

Symantec™ Control Compliance Suite User Guide

Version 9.0.1



Control Compliance Suite User Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 9.0.1

Legal Notice

Copyright © 2010 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, ActiveAdmin, BindView, bv-Control, Enterprise Security Manager, and LiveUpdate are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
<http://www.symantec.com>

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's maintenance offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week
- Advanced features, including Account Management Services

For information about Symantec's Maintenance Programs, you can visit our Web site at the following URL:

www.symantec.com/techsupp/

Contacting Technical Support

Customers with a current maintenance agreement may access Technical Support information at the following URL:

www.symantec.com/techsupp/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system

- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
 - Error messages and log files
 - Troubleshooting that was performed before contacting Symantec
 - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

licensing.symantec.com

Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp/

Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and maintenance contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Maintenance agreement resources

If you want to contact Symantec regarding an existing maintenance agreement, please contact the maintenance agreement administration team for your region as follows:

Asia-Pacific and Japan	contractsadmin@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Symantec Early Warning Solutions	These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.
Managed Security Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Educational Services	Educational Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about Enterprise services, please visit our Web site at the following URL:

www.symantec.com

Select your country or language from the site index.

Contents

Technical Support	4
Chapter 1 Introducing Control Compliance Suite	25
Control Compliance Suite	25
What Control Compliance Suite can do for you	26
How Control Compliance Suite works	26
Components of Control Compliance Suite	27
About the Control Compliance Suite Console	29
About the Control Compliance Suite Application Server	30
About the Control Compliance Suite Directory Server	30
About the Control Compliance Suite Directory	31
About the Control Compliance Suite Data Processing Service	34
About the Control Compliance Suite production database	37
About the Control Compliance Suite reporting database	37
About the Control Compliance Suite evidence database	38
About the Control Compliance Suite Web Portal	38
About the Control Compliance Suite Web portal server	38
About the Control Compliance Suite Management Service	39
About Response Assessment Module	39
Where to get more information	42
Chapter 2 Using the Control Compliance Suite Console	45
About the console features	45
About the menu bar	46
About the tree pane	48
About the Filter by pane	49
About the table pane	49
About the details pane	50
About the taskbar	50
Accessing tasks	51
About the console views	51
About the Home view	51
About the Monitor view	52
About the Manage view	53

About the Settings view	53
About the Reporting view	616
Adding credentials for scheduled jobs	55
About the User preferences page	55
Working in the console	55
Using filters in the Filter by pane	56
Customizing the filter options	56
Managing the table pane	57
Viewing and editing the object details	58
Selecting the columns headings	58
Refreshing the view	59
Searching for objects	59
About working in the tree pane	59
Creating folders in the tree pane	60
About using special characters in folder and job names	60
Moving folders in the tree pane	61
Deleting folders in the tree pane	61
Renaming folders in the tree pane	62
Refreshing folders in the tree pane	62

Chapter 3 Configuring Control Compliance Suite 63

Configuration tasks	64
Managing certificates	68
About Management Services	68
About the Certificates view	69
About managing certificates using the command line	70
Using the Certificate Management Console	70
Configuring roles and permissions	78
About roles	78
About permissions	79
About tasks	79
Predefined roles	80
About custom roles	86
About the Roles view	87
About the Permission Management view	88
Restrictions on collecting data from assets	88
Working with roles	89
Working with permissions	95
Registering and configuring the Data Processing Service	96
About Data Processing Service roles	97
Registering the Data Processing Service	98
Unregistering a Data Processing Service	99

Configuring basic Data Processing Service settings	100
Configuring advanced Data Processing Service settings	100
Assigning a role to a Data Processing Service	102
Synchronizing Data Processing Service settings	103
Working in the System Topology view	103
About the Map view	103
About navigating in the Map view	105
About the Map view icons	105
About the Grid view	106
Modifying the settings of a component	107
Viewing additional component information	107
Saving an image of the configuration layout	108
Adding annotations to the components	108
Deleting annotations	109
Deleting the association between components	109
Viewing the health and the status information	109
Refreshing the health and the status information	110
Monitoring infrastructure jobs	110
Configuring sites	111
What sites can do for you	112
About using sites	112
About planning sites	113
Creating a site	113
Deleting a site	114
Assigning a Data Processing Service to a site	114
Removing a Data Processing Service from a site	115
Modifying the site name	115
Configuring the data collectors	116
Configuring the Windows data collector	117
Configuring the Oracle data collector	118
Configuring the SQL data collector	119
Configuring the UNIX data collector	119
Configuring the ESM data collector	120
Configuring the CSV data collector	129
Configuring the general settings	131
Configuring the data locations	131
Enabling and disabling audit setting	132
Configuring the email Notification Server	132
Selecting the DPS to synchronize the reporting database	133
Synchronizing the reporting database	133
Configuring the evidence purge job	134
About the purge settings	135
Configuring the purge settings	136

Configuring the purge job schedule	137
Configuring the Response Assessment Module database settings	138
Configuring the entitlements settings	139
Configuring the exceptions settings	140
Customizing the report logo and name	141
Configuring the policy settings	142
Configuring the dashboard settings	142
Configuring the remediation settings	143
Configuring the Home view settings	144
Configuring the standards settings	145
Configuring the job count settings	146
Configuring the assets count settings	146
About audits	147
About audit event triggers	147
About viewing the audit logs	148
Managing licenses	148
About the Licenses view	149
Adding a license	150
Adding licenses on the Directory Server	150
Viewing the list of licenses	150
Managing users	151
About the User Management view	151
About adding a user account	151
Importing user accounts	152
Updating a user email address	152
Deleting user accounts	153
Updating user accounts	153
Configuring the application server settings	153
About the security settings for scheduled jobs	154
Configuring the assets batch size	155
Configuring the SQL Server settings	155
Configuring the application server database connection settings	155
Configuring the reporting database connection	156
Configuring the SSIS Server Connection	158
Configuring the application server credentials	159
Configuring service accounts with unconstrained delegation	159
Configuring the S4U and constrained delegation	160
About using special characters in credentials	161
Updating Control Compliance Suite	162
How LiveUpdate works in Control Compliance Suite	163

	About the LiveUpdate view	164
	Enabling and scheduling LiveUpdate	165
	About the host file for Windows LiveUpdate clients	165
	About the LiveUpdate staging location	166
	Performing LiveUpdate on demand	166
	Configuring Response Assessment Module in Control Compliance Suite	167
	Adding a link to Control Compliance Suite	169
	Adding a Response Assessment Module user-defined property	169
	Publishing a questionnaire with invitations in Response Assessment Module	170
	About configuring the Web Portal to contact RAM	171
	About logs and configuration files	172
	About log messages	174
	About log levels	174
Chapter 4	Performing the IT governance tasks with Control Compliance Suite	177
	Preparing for risk assessment	177
	Assessing the compliance and the risk posture of the system	182
	Simplifying the remediation process	186
	Identifying possible threats in the access control system	187
Chapter 5	Managing assets	193
	Getting started with the asset system	193
	About the Asset System view	196
	About the Reconciliation Rules view	198
	Concepts in assets	200
	About assets	201
	Site as scope in asset import	202
	Asset folder hierarchy	202
	Predefined platforms	203
	Asset types	203
	Primary and secondary assets	228
	Reconciliation rules and rule types	229
	Asset import	240
	Asset tagging	246
	Asset groups	247
	Active assets	253
	Creating reconciliation rules	253
	Creating reconciliation rules without manual review	253

Creating reconciliation rules using the manual review	254
Working with reconciliation rules scenarios	255
Importing assets	260
About the first time asset import	262
Importing the assets for the first time	265
Working with asset import scenarios	267
Importing assets from a CSV file	291
Reviewing the assets manually	297
Creating asset groups	299
Creating a dynamic asset group	300
Creating a static asset group	302
Deleting inactive assets using the asset groups	303
Operators (,), AND, OR	304
Performing the tasks in the Asset System view	305
Creating the asset folders	305
Performing the asset group tasks	306
Performing the global tasks	307
Performing the asset tasks	317
Deleting assets or asset groups	319
Viewing asset information in the details pane	319
Using the Filter by pane in the Asset System view	327
Performing the tasks in the Reconciliation Rules view	330
Editing a reconciliation rule	330
Moving a reconciliation rule	331
Copying and pasting a reconciliation rule	331
Deleting a reconciliation rule	331
Viewing rules information in the details pane	331
Using the Filter by pane in the Reconciliation Rules view	332

Chapter 6	Importing assets from Altiris	335
	About importing assets from Altiris	335
	Supported asset types for Altiris	336
	Prerequisites for installing Control Compliance Suite Asset Export Task	337
	Installing Asset Export Task on Altiris Notification Server	337
	Working with the Altiris Asset Export Task solution	338
	Creating the Altiris asset import jobs in Control Compliance Suite Console	339
	Specifying the asset export settings in the Altiris Symantec Management Console	340
	Creating an asset export task in the Altiris Symantec Management Console	341

	Scheduling asset export task in the Altiris Symantec Management Console	342
	About the CSV files on Altiris Notification Server	343
Chapter 7	Managing custom schema	345
	About the custom schema	345
	About the Schema Manager view	346
	About the asset type schema	346
	About the entity schema	347
	About the target type schema	347
	Working with custom asset types	348
	Creating a new asset type	348
	Viewing the custom asset type and the custom fields in the asset system	350
	Extending an existing asset type	351
	Creating an external field to add to the asset type	352
	About the predefined platforms and the primary entities	353
	About the primary, mandatory, and optional fields	354
	About referenced entity fields	354
	About separators in name fields	355
	Working with custom entity	356
	About platforms	356
	About entities	356
	About fields of an entity	357
	About setting tasks to roles for entity schema	357
	About relationships between the predefined entities	358
	Creating a new entity schema	360
	Extending an existing entity schema	364
	Working with custom target type	365
	Creating a new target type	365
	Editing a target type	366
	Working with custom schema scenarios	367
	Creating a custom asset type - Windows Service	368
	Extending the predefined asset type - Windows Machine	370
	Extending Windows Machine to manage inventory and vendor data information	371
	Create a custom entity- Inventory	372
	Extending Windows Machine to include the fields from Inventory	374
	Creating a custom asset type- Printer based on the custom platform- Devices	375

Creating a custom platform- Devices and the custom
entity-Printer 376

Creating a custom asset type- Printer 377

Creating a target type for the asset type - Printer 379

Chapter 8 Managing entitlements 381

About entitlements 381

Reasons for managing entitlements 382

Problems in managing entitlements 382

About the entitlements system workflow 383

About the control point status 387

About the Control Points view 389

About the My Control Points view 390

About the Import Settings view 391

About the Browse Notifications view 393

About the Review Cycle Settings View 394

Concepts in entitlements 394

Control points 395

Data owners 396

Alternative approver 396

Review cycle setting 396

Approval period 397

Tagging 397

Working with control points 398

Marking an asset as a control point 398

Control point type and entitlement type 399

Configuring control points 400

Creating a review cycle setting 402

Deleting a review cycle setting 403

Unmarking a control point 404

Working with entitlements import 404

About entitlements import 405

Configuring the import settings 406

Configuring the automatic entitlements import 407

Importing the entitlements manually 408

Working with approval 410

Requesting approval of entitlements 410

Requesting changes in entitlements 411

Approving the entitlements 411

Configuring the alternative approver 412

Comparing entitlements 413

About the daily approval job 413

Working with notifications	414
About the notification events	414
Configuring entitlements notifications	418
About notification tokens	419
About the entitlements filters	422
Control Point Status filter	422
Tag filter	422
Viewing the control points information in the details pane	423
Control point details pane- General tab	423
Control point details pane- Entitlements tab	424
Control point details pane- Review Cycle tab	424
Control point details pane- Tags tab	425
Control point details pane- Exceptions tab	425
Control point details pane- Workflow Trails tab	425
 Chapter 9	
Managing exceptions	427
Concepts in exception	427
About exceptions	428
About the exception management system	428
About exception validity	429
About exception templates	430
About exception states	431
About the exception filters	432
About the Exceptions view	433
Working with exceptions	433
Viewing exception information in the details pane	433
Requesting an exception	436
Launching the Request Exception Wizard	440
Approving an exception	441
Setting the exception state to In Review	444
Setting the exception state to Request Clarification	444
Setting the exception state to Deny	444
Setting the exception state to Expire	445
Modifying an exception	445
 Chapter 10	
Managing standards	447
Concepts in standards management	447
About standards	448
About predefined standards	449
About sections	453
About checks	453
About data collection jobs	454

About evaluation jobs	454
About target types	455
About compliance score	463
About risk score	463
About gold standard	464
About versioning scheme	465
About the standards filters	466
About policy mapping in ESM	467
About changing an ESM policy name	467
Concepts in checks	467
Field expression	468
Check expression	469
Check formula	469
Preconditions	470
Data Items filter	470
Missing data items	471
Multiple data items	471
Check risk attributes	472
Check Advanced Settings	475
About operators	478
About the Standards view	483
About the standard migration utility for ESM and CCS	485
Working with standards	486
Viewing standard information in the details pane	486
About multi-select functionality	491
Creating a new standard	491
Copying and pasting a standard	492
Moving a standard	493
Importing a standard	493
Exporting a standard	494
Renaming a standard	494
Deleting a standard	495
Running an evaluation job from the Standards view	495
Setting up a data collection job from the Standards view	498
Running a collection-evaluation-reporting job from the Standards view	499
Sizing guidelines for Collection-Evaluation-Reporting job	502
Changing an ESM policy name at the standard level	503
Working with sections	503
Viewing section information in the details pane	503
Creating a new section	505
Copying and pasting a section	506
Moving a section	507

Renaming a section	507
Deleting a section	507
Changing an ESM policy name at the section level	508
Working with checks	508
Viewing check information in the details pane	509
Copying and pasting a check	515
Moving a check	515
Renaming a check	516
Deleting a check	516
Creating a new check	517
Editing a check	520
Viewing the evidence details	521
Changing an ESM policy name at the check level	521
Creating an ESM check	522
Working in the details pane	531
Specifying or editing the description	532
Specifying or editing the check issue	532
Specifying or editing the remediation information	533
Adding the CVE information	533
Editing the CVE information	534
Specifying or editing the check attributes	534
Adding reference information	535
Editing reference information	535
Deleting reference information	536
Working with gold standard	536
Gold standard concepts	536
Creating a gold standard	537
Gold standard job	538
Resolving checks in a gold standard	538
Using the Manual Review dialog box	539
Working with Evaluation Results	541
About exporting the evaluation results	542
Exporting the evaluation results	543
Requesting an exception using the Evaluation Result Details dialog box	544
About risk score calculation	545
Base score calculation	545
Adjusted base score calculation	546
Risk score calculation	546
Average risk score calculation	547

Chapter 11	Remediating assets	549
	About remediation	549
	About automatic remediation	550
	About manual remediation	551
	About closed-loop verification	552
	Remediating the assets manually from the evaluation results	553
	Remediating the assets automatically	555
Chapter 12	Managing baselines	557
	About baseline	557
	About the baselines workflow	558
	About the Baselines view	559
	About setting tasks to roles of baselines	559
	Creating a baseline job	560
	Viewing the comparison results in the Baselines view	561
	Exporting the comparison results	562
	Deleting the baseline record	563
Chapter 13	Managing tags	565
	About tags	565
	About the Tags view	566
	Creating a new tag	566
	Creating a new tag category	566
	Editing a tag category	567
	Deleting a tag category	567
	Moving a tag	568
	Deleting a tag	568
	Renaming a tag	568
Chapter 14	Managing policies	571
	About Policies	571
	About the policy life cycle	572
	About policy status	572
	About audiences	573
	About regulations	574
	About frameworks	574
	About control statements	574
	About policy versioning	575
	About the policies management view	575
	About editing policies	578
	About searching policies	578

Working with policies	578
Creating a new policy	579
Importing a Word policy	581
Moving a policy	582
Deleting a policy	583
Submitting a policy for review	583
Submitting a policy for approval	583
About selecting the policy audience	584
Reviewing and approving policies	584
About policy review	585
Reviewing a policy	585
Viewing the reviewer comments	586
About mapping policies	586
Publishing and unpublishing policies	586
Approving a policy	587
Publishing a policy	587
Unpublishing a policy	588
Responding to policies on the Web Portal	
Responding to policies in the Web Console	588
Accepting or declining a policy	589
Reviewing a policy in the Web Portal	590
Approving a policy in the Web Portal	590
Submitting a policy for approval in the Web Portal	591
Printing a policy from the Web Portal	591
Managing clarifications	592
About clarifications	592
About the clarifications management view	592
Managing clarification requests	593

Chapter 15

Monitoring jobs	595
About jobs	595
About the job types	596
About the job filters	598
About the Jobs view	599
Managing jobs	600
Editing a job	601
Scheduling jobs	602
Deleting jobs	602
Running a job now	603
Searching for a job	604
Refreshing the jobs view	604
Creating jobs	605

Managing job runs	606
Canceling a job run	606
Deleting a job run	607
Viewing jobs information in the details pane	608
Jobs details pane- General tab	608
Jobs details pane- Schedule tab	609
Jobs details pane - Wizard Summary	609
Job run details pane- Summary tab	609
Job run details pane- Failures tab	609
Jobs details pane- Template tab	609

Chapter 16 Monitoring evaluation results 611

About the Evaluation Results view	611
About the evaluation result filters	612
Viewing evaluation jobs in the details pane	612
Evaluation Results details pane - General tab	613
Evaluation Results details pane - Evaluation Summary tab	613
Evaluation Results details pane - Assets Evaluated tab	613

Chapter 17 Managing reports and dashboards 615

About the reports and dashboards	615
About the Reporting view	616
About the Reports Templates view	616
About the My Reports view	618
About the My Dashboards view	619
About the Dashboard Templates view	621
About types of dashboards	622
About predefined report templates	623
About data synchronization	623
About creating user-defined templates	624
About the prerequisites for user-defined report templates	624
About the Report Management jobs	627
About the View My Reports filter option	627
Predefined Reports and Dashboard descriptions	627
Working with reports	635
Scheduling a report	636
Viewing a report	638
Refreshing a report	638
Removing a report	639
Printing a report	639
Exporting a report	639
Copying a report template	640

	Customizing a report template	641
	Customizing a report in report viewer	642
	Deleting a user-defined report template	643
	Adding a user-defined report template	643
	Exporting a report template	644
	Updating a report template	645
	Moving a report template	646
	Editing a report generation job	646
	Working with dashboards	646
	Managing summary dashboards	647
	Managing tiered dashboards	651
	About roles and permissions in tiered dashboard	662
	About threshold settings in tiered dashboard	666
	Configuring tiered dashboards	670
	About trends configuration	675
	Viewing the tiered dashboard reports	678
Chapter 18	Using custom content	681
	Using the custom content tool	681
	About custom content	681
	About the Content view	684
	Creating a custom mandateCreating a custom mandate or section	684
	Modifying a mandate or section	685
	Creating custom control statements	686
	Performing policy analysis	693
	About the Analysis view icons	693
	Viewing the control statements mapped to a regulation, framework, or policy	694
	Performing a gap analysis	695
Chapter 19	Using third-party evidence	697
	About the Evidence Management system	697
	About the Evidence Management View	698
	About a custom evidence provider	698
	General sequence of configuring an evidence provider	698
	Creating a CSV file for evidence data collection	699
	About evidence field format for predefined asset types	701
	Associating a data location with the evidence provider	707
	About setting tasks to roles for evidence collection	707
	Adding a custom evidence provider	708
	Modifying a custom evidence provider	709

	Deleting a custom evidence provider	709
Appendix A	Customizing the Web Portal language	711
	Customizing the Web Portal language	711
	Creating new Web Portal language files	711
	Translating the Web Portal local resource files	713
	Using a new language in the Web Portal	714
	Web Portal string reference	715
Appendix B	Standard Migration Utility	723
	About the Standard Migration Utility	723
	About the Standard Migration Utility system requirements	724
	About the Standard Migration Utility packaging and deployment	725
	Standard Migration Utility	726
	How to use the Standard Migration Utility	727
	About the command-line options	727
	About validation	728
	About the log file configuration settings	728
	About migration summary report	731
	Limitations in the Standard Migration Utility	731
	Troubleshooting evaluation mismatches	734
Appendix C	ESM Policy to CCS Standard Migration utility	741
	About the Symantec ESM Policy to CCS Standard Migration Utility	741
	About packaging and deployment	742
	Additional information about the files	743
	System requirements for the ESM Policy to CCS Standard Migration Utility	743
	About installing the migration utility	744
	Uninstalling the migration utility	744
	About the input file in the ESM Policy to CCS Standard Migration Utility	744
	Executing the migration utility	744
	About the default category IDs for creating the formula	746
	About the log file in the ESM Policy to CCS Standard Migration Utility	747
	About ESM suppressions migration	747
	About the message IDs in ESM Policy to CCS Standard Migration Utility	747

	Advantages and disadvantages of policy migration based on the Message String ID	748
	Advantages and disadvantages of migration based on Message Numeric ID	749
	Limitations of the migration utility	749
	Troubleshooting for ESM Policy to CCS Standard Migration Utility	750
Appendix D	Reporting database schema	755
	About the Reporting database	755
Appendix E	Troubleshooting	769
	About troubleshooting	769
	Deployment troubleshooting	770
	Configuration troubleshooting	771
	Asset import troubleshooting	772
	Data collection troubleshooting	772
	Console and Web Portal troubleshooting	772
	Symantec ESM troubleshooting	774
	Installing Active Directory Application Mode manually	775
	Glossary terms	777
	Index	785

Introducing Control Compliance Suite

This chapter includes the following topics:

- [Control Compliance Suite](#)
- [What Control Compliance Suite can do for you](#)
- [How Control Compliance Suite works](#)
- [Components of Control Compliance Suite](#)
- [About Response Assessment Module](#)
- [Where to get more information](#)

Control Compliance Suite

The Control Compliance Suite (CCS) automates key IT risk and compliance management tasks. The CCS ensures the coverage of external mandates through written policy creation, dissemination, acceptance logs, and exception management. CCS demonstrates compliance to both external regulatory mandates and internal policies. The CCS allows customers to link the written policy to specific technical and procedural standards. Customers can assess those policies using a highly scalable agentless or agent-based tool. The CCS scores assessment results against specified risk criteria. The CCS supports automated assessment of the system security configuration, permissions, patches, and vulnerabilities. The CCS includes system reporting capabilities. CCS also supports the assessment of procedural controls and entitlement review through a manual attestation process.

What Control Compliance Suite can do for you

The Control Compliance Suite (CCS) is an IT risk and compliance management solution.

CCS provides a comprehensive framework that allows customers to do the following:

- Lower the cost of risk and compliance posture assessment.
- Use automated agentless or agent-based capabilities to audit and scan technical controls.
- Provide an ability to attest procedural controls.
- Identify problems with system configuration or internal controls. Guard against policy compliance failure or data breach.
- Define, review, and disseminate written policies to end-users as mapped to specific, measurable controls.
- Determine coverage gaps for multiple, overlapped regulatory, industry-specific, or best practices frameworks.
- Produce evidence of due care in an IT audit process.
- Simplify the remediation process.
- Pull in third-party checks and controls data as evidence and for the integrated assessment of technical standards.
- Help ensure a working review process for the entitlements that are granted to the file system assets and membership of groups.
- Integrate the compliance process with existing asset management systems.

How Control Compliance Suite works

The Control Compliance Suite (CCS) Console lets you create written policies and distribute these policies to users. The console also lets you track user acceptance of policies and lets you manage exceptions to those policies. The console also lets you define evidence of your compliance with the policies.

When you define policy evidence, you use the CCS Console to create jobs to collect data from your network. Servers and other computers on your network are referred to as assets. Data collectors process jobs and gather information from the assets on your network. Collected data is stored in an SQL Server database. The collected data can then be evaluated against the parameters that you specify. Evaluation results are stored in the database. These evaluation results can be reviewed within the CCS Console. Evaluation results are also synchronized to the reporting database.

immediately or on a schedule that you specify. The evaluation results in the reporting database can be processed into reports and printed or displayed in the dashboard.

Figure 1-1 outlines the steps to install, configure, and use the CCS.

Figure 1-1 Using the Control Compliance Suite



Components of Control Compliance Suite

Control Compliance Suite (CCS) consists of several main components.

The following is the list of components with a brief description:

Control Compliance Suite Application Server	<p>The CCS Application Server is responsible for all job executions, work flow, and schedules.</p> <p>See “About the Control Compliance Suite Application Server” on page 30.</p>
Control Compliance Suite Directory Server	<p>The CCS Directory Server hosts the CCS directory, the Encryption Management Service, the Directory Support Service, and the Certificate Management Console.</p> <p>See “About the Control Compliance Suite Directory Server” on page 30.</p>
Control Compliance Suite Directory	<p>The CCS directory stores asset data, user rights and preferences, and information about jobs.</p> <p>See “About the Control Compliance Suite Directory” on page 31.</p>
Control Compliance Suite Console	<p>The CCS console is the primary user interface component that makes data requests and expects data responses.</p> <p>See “About the Control Compliance Suite Console” on page 29.</p>
Data Processing Service (DPS)	<p>A single service that plays multiple roles in CCS. The roles include the DPS Collector, the DPS Evaluator, the DPS Load Balancer, and the DPS Reporter.</p> <p>See “About the Control Compliance Suite Data Processing Service” on page 34.</p>
Encryption Management Service	<p>The Encryption Management Service is a Certificate Authority service that is responsible to generate, manage, and sign certificates.</p> <p>See “About the Control Compliance Suite Management Service” on page 39.</p>
Web Console	<p>The Web portal is used to distribute policy notifications, accept or reject policies, and request policy exceptions.</p> <p>See “About the Control Compliance Suite Web Portal” on page 38.</p>

Production database	<p>The production database is a SQL Server instance that stores the data that is collected from assets. These assets are based on a query and the results of an evaluation job.</p> <p>See “About the Control Compliance Suite production database” on page 37.</p>
Reporting database	<p>The reporting database stores evaluation data. The DPS reporter uses the stored evaluation data.</p> <p>See “About the Control Compliance Suite reporting database” on page 37.</p>
Evidence database	<p>The evidence database stores evidence of your compliance with policies defined in the Control Compliance Suite console.</p> <p>See “About the Control Compliance Suite evidence database” on page 38.</p>
See “Control Compliance Suite” on page 25.	

About the Control Compliance Suite Console

The Control Compliance Suite (CCS) Console is a Windows application that runs on a client computer. The console allows access to the full range of CCS activities. Only users who have been assigned to roles that allow them to work in the console can perform activities in the console.

The computer that hosts the CCS Console and the computer that hosts the Application Server can be in the same domain. If the console and the Application Server are in different domains, the components can communicate successfully if the domains have a two-way trust relationship. Both domains must be a Windows Server 2003 domain or a Windows Server 2008 domain. In addition, the trust relationship must be set up to use Kerberos authentication instead of the default NTLM authentication. Finally, only constrained delegation is supported. Unconstrained delegation is not supported.

For information on setting up delegation, see the *Symantec Control Compliance Suite Installation Guide*.

If no trust relationship exists between the domains, you can use the Windows `runas` command to run the console. When you use the `runas` command, you supply the alternate credentials that the console uses to connect to the Application Server. To use the `runas` command, you must have valid credentials for an account in the same domain as the Application Server.

The `runas` command line should follow the pattern

```
C:\Windows\System32\runas.exe /user:<Domain Name>\<User Name> /netonly  
C:\Users\<User Name on the local machine or  
domain>\AppData\Roaming\Symantec\<Application Server Name>\CCS90.exe.
```

About the Control Compliance Suite Application Server

The Control Compliance Suite (CCS) Application Server is the hub of CCS. CCS jobs flow from the CCS Console to the Application Server and then to one of the Data Processing Service Load Balancers. When reports are complete, the Application Server retrieves the report from the reporting database and sends it to the console for display to the user. In addition, the Application Server manages data storage in the Control Compliance Suite Directory, and manages the scheduled jobs and workflow in the production database.

When you install the Application Server, you must have local administrator-equivalent privileges. In addition, you must have the privileges to read from and write to the Microsoft SQL Servers that host the database components.

The Application Server runs as a service on the server that you specify. The Application Server appears in the **Services** control panel as Symantec Application Server Service. The account that you use for the Application Server must be a local administrator equivalent on the computer that hosts the service. The account can be an Active Directory domain account or a local Windows user account.

Note: The Application Server and the Directory Server must be located in the same domain.

About the Control Compliance Suite Directory Server

The Control Compliance Suite (CCS) Directory Server stores information about business objects, preferences, and other information. In addition, the Control Compliance Suite Directory Server hosts the certificate authority for the CCS system, and issues and validates certificates. Certificates are used to ensure secure communications between the CCS components.

The Directory Server includes the Management Service, the Directory Support Service, and the Certificate Management Console.

Some CCS components contact the Directory Server with no mediation. Other components use the Management Service and the Directory Support Service to communicate with the Directory Server. The Management Service also helps to

manage certificates. The Certificate Management Console is used to create, store, and revoke certificates.

When you install CCS, the Directory Server is installed on a server that you specify. If necessary, you can extend the default schema that ships with CCS. You must have local administrator-equivalent privileges when you install the Directory Server. The account you use for the Directory Server must be a local administrator-equivalent account on the computer that hosts the service. The account can be an Active Directory domain account or a local Windows user account.

Note: The Application Server and the Directory Server must be located in the same domain.

About the Control Compliance Suite Directory

Control Compliance Suite (CCS) stores information about preferences and roles as well as some business objects and other information in the Control Compliance Suite Directory. For other business objects or other information, the object is stored in the production database or the reporting database. The object security descriptor is stored in the Control Compliance Suite Directory. The Control Compliance Suite Directory stores information in a structured way. You can extend the default directory schema to store additional information.

The Application Server can retrieve information from the Control Compliance Suite Directory. For extended permissions, the Application Server also contacts the Directory Support Service. Like the directory, the Directory Support Service runs on the Directory Server. The Directory Support Service is installed automatically when you install the Directory Server. The Directory Support Service has minimal configuration needs.

On Windows Server 2003, the Microsoft Active Directory Application Mode (ADAM) service hosts the Directory Server. ADAM runs as an independent user service, as opposed to an operating system service. ADAM is designed to meet the specific needs of organizations that use directory-enabled applications. ADAM is a directory service subset of the Microsoft Active Directory. ADAM does not replace any existing directory service on your network. This ADAM installation is for the sole use of CCS.

On Windows Server 2008, the Microsoft Active Directory Lightweight Directory Service (AD LDS) hosts the Directory Server. Like ADAM, AD LDS runs as an independent user service, as opposed to an operating system service. AD LDS is a directory service subset of the Microsoft Active Directory. AD LDS does not replace any existing directory service on your network. This AD LDS installation is for the sole use of CCS.

The directory is installed and created automatically when you install the Directory Server.

The account you use for the Directory Support Service must be a local administrator-equivalent account on the computer that hosts the service. The account can be an Active Directory domain account or a local Windows user account.

See [“About objects in the directory”](#) on page 32.

See [“About organizing objects in the directory”](#) on page 32.

About objects in the directory

When you install the Control Compliance Suite, a default hierarchical structure is created to store objects in the directory. All objects are stored under the root folder. The root folder holds subfolders for each object type. For example, a folder is used for assets, for policies, and for standards. Under the individual object type folder, the user can create a hierarchical structure to store the objects that best suits the organizational needs. For example, in the Assets folder, assets can be stored in a hierarchy that is based on the geographical locations of the organization.

See [“About organizing objects in the directory”](#) on page 32.

The following is a list of folders under the root folder:

- Assets
- Exceptions
- Policies
- Reconciliation
- Reporting
- Shared
- Standards
- Tags

See [“About the Control Compliance Suite Directory”](#) on page 31.

About organizing objects in the directory

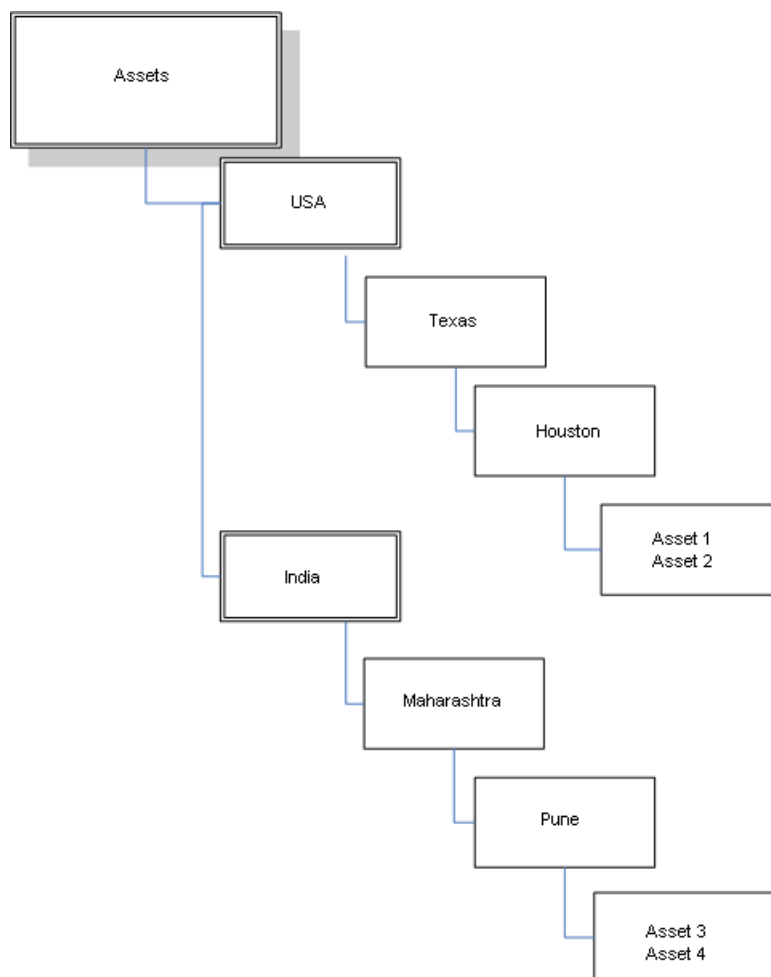
The Control Compliance Suite (CCS) directory is hierarchical in nature, which allows users to create folders and objects in an inverted tree-like structure. This structure provides flexibility to create a hierarchy that allows the user to model the tree that is based on the organizational requirements.

When you install CCS, a default hierarchy is created to store objects. Users should organize the tree to follow the flow of control in the organization.

Beyond the default hierarchy users should organize the tree to follow the flow of control in the organization. This flow is natural for the users to administer permissions on the folders and objects where needed in the tree.

Organizations with branches all over the world, with local administrators responsible for their geographical area, benefit by a hierarchy that mimics their geographical locations. This design helps organizations to administer permissions and roles for the local administrators by following their organizational structure.

Figure 1-2 Example of structure based on geographical locations



See [“About the Control Compliance Suite Directory”](#) on page 31.

See [“About objects in the directory”](#) on page 32.

About the Control Compliance Suite Data Processing Service

The Control Compliance Suite (CCS) Data Processing Service (DPS) is a single service that performs up to four different duties in CCS. Each of these duties is called a role. Which role the DPS serves depends on how the DPS is registered. The DPS runs as a Windows Service. A single instance of the service can provide more than one role simultaneously. Normally, a CCS deployment includes many servers that each hosts a DPS installation. When a deployment contains multiple DPS installations, each DPS performs a single role.

In the **Services** control panel, the service is listed as the Symantec Data Processing Service.

The Data Processing Service performs the following roles:

- Load Balancer
See [“About the Data Processing Service Load Balancer”](#) on page 34.
- Collector
See [“About the Data Processing Service Collector”](#) on page 36.
- Evaluator
See [“About the Data Processing Service Evaluator”](#) on page 37.
- Reporter
See [“About the Data Processing Service Reporter”](#) on page 35.

When you install a Data Processing Service, you must have local administrator-equivalent privileges.

The account you provide for a Data Processing Service to use must be a local administrator-equivalent account on the computer that hosts the service. The account can be an Active Directory user account or a local Windows user account.

About the Data Processing Service Load Balancer

When the Data Processing Service (DPS) acts as a load balancer, the DPS routes data collection jobs from the Application Server to a DPS Collector. In addition, a load balancer routes the evaluation jobs to the DPS Evaluator and the reporting jobs to the DPS Reporter. If your deployment includes multiple load balancers, the Application Server automatically uses each in turn. If a load balancer fails, the Application Server automatically skips the failed load balancer and uses another load balancer. This round robin assignment gives limited fault tolerance.

See [“About the Data Processing Service Collector”](#) on page 36.

See [“About the Data Processing Service Evaluator”](#) on page 37.

See [“About the Data Processing Service Reporter”](#) on page 35.

The DPS Collector retrieves the data from the network. Potentially, your installation of Control Compliance Suite (CCS) can have a large number of DPS Collectors and the associated data collectors. The load balancer assigns jobs to eligible collectors sequentially. The load balancer does not base job assignments on the current load of the collector. If a query requires input from several DPS Collectors, the load balancer distributes the query appropriately. When the DPS Collectors complete the query, the load balancer combines the results and returns the results to the Application Server for storage.

An eligible DPS Collector is any collector that has the ability to complete the data collection job. The collector site assignment and the installed RMS snap-in modules determine the collector eligibility.

The DPS Evaluator compares collected data to the standards that you specify and saves the results for later use. Potentially, your installation of CCS can have multiple DPS Evaluators. The load balancer assigns jobs to evaluators sequentially. The load balancer does not base job assignments on the current load of the evaluator.

The first DPS registered when you deploy CCS should be assigned to the Load Balancer role.

About the Data Processing Service Reporter

The Data Processing Service (DPS) Reporter generates reports and dashboards for display by the Control Compliance Suite (CCS) Console. In addition, a single DPS Reporter is assigned to perform database synchronization between the production database and the reporting database.

The reporter executes the list of queries that are specific to the selected dashboard or the selected report. On the basis of these queries, the reporter retrieves data from the reporting database and creates the report.

The DPS Reporter that is assigned to synchronize data synchronizes the contents of the reporting and the production databases. Synchronization occurs based on a schedule that you specify or when an evaluation job triggers the synchronization.

The computer that hosts the DPS Reporter must have the Crystal Reports engine installed. The Crystal Reports installer is available on the CCS product disc.

See [“About the Data Processing Service Load Balancer”](#) on page 34.

See [“About the Data Processing Service Collector”](#) on page 36.

See [“About the Data Processing Service Evaluator”](#) on page 37.

About the Data Processing Service Collector

The Data Processing Service (DPS) Collector is the interface to the programs that do the actual work of collecting data from the network. Your Control Compliance Suite (CCS) deployment can include multiple data collectors, each linked with a DPS Collector. The DPS Collector receives data collection jobs from the DPS Load Balancer and formats the job for the data collector. When the data collector processes the job and collects the data, the data collector transfers the data to the DPS Collector. The DPS Collector then returns the collected data to the DPS Load Balancer. If necessary, the DPS Load Balancer combines the data with data from one or more other DPS Collectors. Finally, the DPS Load Balancer sends the data to the Application Server for storage in the production database for use by the DPS Evaluator.

The DPS Collector collects the data from the data collectors, which in turn collect data from the network. Potentially, your installation of CCS can have a large number of DPS Collectors and associated data collectors. The DPS Load Balancer assigns jobs to the eligible DPS Collectors sequentially. The DPS Load Balancer does not base job assignments on the current load of a DPS Collector. If an eligible DPS Collector is unavailable, the DPS Load Balancer skips it and uses another eligible DPS Collector. This round robin assignment gives limited fault tolerance.

An eligible DPS Collector is any collector that has the ability to complete the data collection job. The DPS Collector site assignment or installed RMS snap-in modules can make the DPS Collector ineligible.

CCS supports the following data collectors:

- Symantec RMS
- Symantec Enterprise Security Manager (ESM)
- CSV files
- ODBC databases

Used with a custom schema, the CSV files let you create any custom data collector and schema. This ability lets you use any custom data on your network, including data not ordinarily supported by CCS.

The data that the DPS Collector collects is compressed before the data is returned to the other CCS components.

See [“About the Data Processing Service Load Balancer”](#) on page 34.

See [“About the Data Processing Service Evaluator”](#) on page 37.

See [“About the Data Processing Service Reporter”](#) on page 35.

About the Data Processing Service Evaluator

Evaluation jobs are sent from the Application Server to one of the Data Processing Service (DPS) Load Balancers. The DPS Load Balancer then sends the evaluation job to the DPS Evaluator. The evaluator compares the data to the specifications in the Standards that you select and then stores the evaluation results in the production database.

If you have more than one evaluator, the DPS Load Balancer assigns evaluation jobs to the evaluators sequentially. If a DPS Evaluator is unavailable, the load balancer skips it and uses the next available evaluator. This round robin assignment gives limited fault tolerance.

See [“About the Data Processing Service Load Balancer”](#) on page 34.

See [“About the Data Processing Service Collector”](#) on page 36.

See [“About the Data Processing Service Reporter”](#) on page 35.

About the Control Compliance Suite production database

A Microsoft SQL Server instance hosts the production database. The database stores the data that is collected from the assets. The database also stores the results of evaluation jobs. The database stores information about the policies that you create and about the entitlement control points. If you use the Symantec Response Assessment module with the Control Compliance Suite (CCS), the Response Assessment data is also stored in the production database.

The production database requires Microsoft SQL Server 2005 SP2. CCS requires a single production database. The production database can share a host server with the Control Compliance Suite Directory, or you can use a dedicated server as the host. The production database can be hosted on the same SQL Server as the reporting database, or on another SQL Server.

About the Control Compliance Suite reporting database

A Microsoft SQL Server instance hosts the reporting database. The reporting database is periodically synchronized with the data that is stored in the production database and the evidence database. In addition, the database stores data specific to individual dashboards or reports. The DPS Reporter monitors the synchronization of data between the production database, evidence database and the reporting database.

The reporting database requires Microsoft SQL Server 2005 SP2. CCS requires a single reporting database. The reporting database can share a host server with the Control Compliance Suite Directory, or you can use a dedicated server as the

host. The reporting database can be hosted on the same SQL Server as the production database, or on another SQL Server.

The reporting database also needs to be accessible to an SQL Server with Integration Services (SSIS) installed. SSIS can be installed on the same server that hosts the reporting database, or SSIS can be installed on another SQL Server. Normally, SSIS should be installed on the server that hosts the reporting database. CCS requires SSIS SP2.

SSIS is a technology from Microsoft that lets Microsoft SQL Server consolidate data from multiple sources.

For more information about SSIS, see the Microsoft SSIS Web site.

<http://www.microsoft.com/sql/technologies/integration/default.mspx>

About the Control Compliance Suite evidence database

A Microsoft SQL Server instance hosts the evidence database. The evidence database stores evidence of your compliance with the policies or standards that are defined in the Control Compliance Suite (CCS) Console. The Data Processing Service Evaluator stores the evidence in this database.

The evidence database requires Microsoft SQL Server 2005 SP2. CCS requires a single evidence database. The evidence database must share a host SQL Server with the production database.

About the Control Compliance Suite Web Portal

The Control Compliance Suite (CCS) Web portal lets users access a subset of the CCS functionality using Internet Explorer 6 or Internet Explorer 7.

In the Web portal, users can do the following:

- Review policies.
- Accept or reject policies.
- Request policy exceptions.

About the Control Compliance Suite Web portal server

The same computer that hosts the Control Compliance Suite (CCS) Web portal server must also host the Microsoft Internet Information Server (IIS). The Web portal allows access to some CCS content without requiring the full CCS Console.

The Control Compliance Suite (CCS) Web portal lets you do the following:

- Distribute policy notifications to end users across the enterprise and track when users read and acknowledge the policies.
- Request exceptions to policies.
- Request exceptions from control points.

By default, the Web portal uses integrated Windows security. If the user domain and the Web portal domain have a trust relationship, the Web portal uses the existing user credentials. The user does not need to enter a name and password to access the Web portal. If no trust relationship exists, the user is prompted for a name and a password.

If the same computer hosts the Web portal, the Application Server, and the Directory Server, CCS uses Windows NTLM authentication. If the Web portal, the Application Server, and the Directory Server are hosted on multiple computers, you must enable Kerberos authentication on all components. Kerberos authentication lets credentials be passed from the Web portal client to the Web portal server, then on to the Application Server. The Application Server can then pass the credentials to the Directory Server.

For information about Kerberos authentication, see the Microsoft knowledge base.

<http://support.microsoft.com/kb/326985>.

About the Control Compliance Suite Management Service

The Control Compliance Suite (CCS) Management Service is the root certificate authority service that generates, manages, and signs certificates for the CCS components.

The Directory Server hosts the Management Service. The Management Service is installed and configured automatically when you install the Directory Server. The root certificate that the Management Service uses is created during installation. In addition, half of the key that is used for double encryption is created. The only user interface to the Management Service is the Certificate Management Console.

The account you use for the Management Service must be a local administrator-equivalent account on the computer that hosts the service. The account can be an Active Directory domain account or a local Windows user account.

About Response Assessment Module

The Response Assessment Module (RAM) is a set of innovative components and services and is part of the Symantec Control Compliance Suite (CCS) strategy.

RAM is an optional, external module for CCS. RAM formalizes, standardizes, and documents the assessments and audits that are a part of an organization. You can construct a complex business evaluation from prepackaged content packs. RAM lets you create questionnaires to answer your business challenges.

The following are your business challenges:

- Complexity of regulatory compliance
- Cost of regulatory compliance
- Increased accountability from the shareholders, government, and industry
- Increased civil and criminal liabilities for noncompliance

With the results gathered from the questionnaires, you can make informed decisions. Often, the results are used to gain an understanding of the beliefs and behaviors of a target population under a given set of circumstances. The results provide a snapshot, which reflects these beliefs and behaviors. In the past, to create an assessment was a complicated process that returned inconsistent results.

Previous approaches to assessments typically meant that each executive or manager would have their own Excel spreadsheet. The spreadsheets had no uniformity because they reflected each executive or manager's particular concerns. One assessment may conflict with other collected assessments. The assessment may not reflect an important concern. The members of upper management must spend the time to compile the assessments to gain an overall view of the organization. To create and store assessments can create technical problems.

The following are some of the assessment issues:

- Not standardized
- Not accessible from other applications
- Difficult to manage
- Difficult to store
- Not secure

RAM extends the assessment strategy. Everyone sees the same questions. Executives and managers can provide uniform responses. The responses are compiled easily and the members of upper management can make more informed business decisions. RAM is a comprehensive assessment solution. When the RAM Server is installed, assessments are stored in an SQL Server database and are accessible from the Web. Invited users can create responses from any Web connection. With the necessary permissions, users can generate reports, export report detail information, and create the charts that visualize the information. RAM increases an organization's ability to manage the flow of information.

RAM is a management tool that collects the following:

Assessments	Current and new assessments
Audits	Current and new audits
Risk alignment	Supports a risk analysis process

Executives and managers can accomplish the following:

- Measure and evaluate their operations
- Distribute the questionnaires at regular intervals
- Improve their organization's operations based on the results

Executives and managers can measure and evaluate the aspects of the following business processes:

- Compliance
- Business continuity
- Information security
- Physical security
- Governance
- Protection of intellectual property

A Response Assessment Module assessment is taken through the assessment lifecycle.

The following are the parts of the assessment lifecycle:

Questionnaire creation	The process that defines the questionnaire. The creation process may include questionnaire property definitions and the questionnaire layout.
Questionnaire delivery	The process to deliver the questionnaire to the intended attesters.
Response creation	The activities that focus on the response.
Report management	Responses can be grouped together, exported to an Excel spreadsheet, and used to create charts.
Questionnaire management	The activities that focus on the administration of an assessment.

See [“Configuring Response Assessment Module in Control Compliance Suite”](#) on page 167.

Where to get more information

You can access the Control Compliance Suite documents from the product disc and the Symantec Web site. The documents are also installed at the *<install directory>\Documentation* folder.

Control Compliance Suite (CCS) provides the following documents:

<i>Control Compliance Suite Planning and Deployment Guide</i>	The guide informs users about the decisions that they need to make before the installation.
<i>Control Compliance Suite Installation Guide</i>	The guide assists users in installing the product and its components.
<i>Control Compliance Suite User's Guide</i>	The guide describes the various features and indicates when they are performed. The user's guide contains procedures for all the key tasks.
<i>Control Compliance Suite Online Help</i>	<p>The Help file describes the various features and indicates when they are performed. The help file contains procedures for all the key tasks.</p> <p>The Help file is accessible from within the Control Compliance Suite Console.</p>
<i>Control Compliance Suite Release Notes</i>	The release notes contain any installation or other issues that users should know before they install the Control Compliance Suite product.
<i>Control Compliance Suite Quick Reference Card</i>	The quick reference card provides users with enough information to prepare to deploy the product.
<i>CCS_API_Reference_Guide</i>	The reference guide provides APIs to integrate the third-party clients to the core functionality of CCS within their own business processes.

The Control Compliance Suite user's guide, planning and deployment guide, installation guide, quick reference card, and release notes are available in a PDF format.

For information about installing and using the Symantec Enterprise Security Manager (ESM), see the documentation that is provided with the CCS Symantec Enterprise Security Manager.

The Documentation directory includes the following Symantec ESM documentation:

- *Symantec Enterprise Security Manager Release Notes*

- *Symantec Enterprise Security Manager Installation Guide*
- *Symantec Enterprise Security Manager User's Guide*
- *Symantec Enterprise Security Manager Online Help*

Note: To view the online documentation, you must have Acrobat Reader 5.0 or later.

You can also check the Symantec Web site and the Knowledge Base for answers to frequently asked questions, troubleshooting tips, and the latest product information.

On the Internet, go to: www.symantec.com/support/

See “[Control Compliance Suite](#)” on page 25.

Using the Control Compliance Suite Console

This chapter includes the following topics:

- [About the console features](#)
- [Accessing tasks](#)
- [About the console views](#)
- [Adding credentials for scheduled jobs](#)
- [About the User preferences page](#)
- [Working in the console](#)

About the console features

The Control Compliance Suite console provides several control features to help you work with ease and efficiency.

The console provides the following control features:

Menu bar	The menu bar appears across the top of the console window. You can access the Control Compliance Suite features using the menu options.
Navigation bar	The navigation bar appears under the menu bar across the top of the console window. The navigation bar groups the common tasks that you can perform.

Tree pane	<p>The tree pane appears on the left side of the console window under the navigation bar. The tree pane does not appear in all views. The tree pane displays a hierarchical, a folder-based navigation structure that lists the objects that are stored in the Directory. When you select an asset group from the tree pane, the list of assets is displayed in the table pane.</p> <p>See “About the tree pane” on page 48.</p> <p>See “About working in the tree pane” on page 59.</p>
Filter by pane	<p>The Filter by pane appears in the lower-left side of the console window under the tree pane. You can narrow the list of objects that are displayed in the table pane by selecting the filter options. The filter options vary based on the view selected.</p> <p>See “About the Filter by pane” on page 49.</p> <p>See “Using filters in the Filter by pane” on page 56.</p> <p>See “Customizing the filter options” on page 56.</p>
Taskbar	<p>The taskbar appears across the top of the tree pane and the table pane in the console window. The taskbar displays a list of tasks that are relevant to the current object that is selected in the table pane.</p>
Table pane	<p>The table pane appears in the right side of the console window under the taskbar . The table pane lists all the objects for the selected folder in the tree pane.</p> <p>See “About the table pane” on page 49.</p> <p>See “Managing the table pane” on page 57.</p>
Details pane	<p>The details pane appears in the lower-right side of the console window under the table pane. The details pane displays information about the object that is selected in the table pane.</p> <p>See “Viewing and editing the object details” on page 58.</p>

About the menu bar

You can access the Control Compliance Suite (CCS) features by using the menu bar that appears across the top of the Console window. The menu bar offers a traditional approach to using the application’s features. Some options are available only after an item is selected.

Table 2-1 Menu options

Menu	Menu item	Description
File	Print Preview	Opens the Print Preview dialog box.
	Print	Invokes the Print dialog box and lets you print the information in the view area to a selected printer.
	Export to	Opens the Export to dialog box . The Export to dialog box lets you export the information in the view area. The Export to menu item is not available in all views.
	Export options	Opens the Export Options dialog box. The Export options dialog box is not available in all views.
	Send	Link by E-mail invokes your email application and lets you send a mail recipient a link to the view. Shortcut to Desktop lets you save the state of a particular view to your desktop for quick access at a later time.
Edit	Exit	Closes the CCS application.
	Cut	Cuts the currently selected item to the clipboard.
	Copy	Copies the currently selected item to the clipboard.
	Paste	Pastes the current contents of the clipboard.
View	Back	Returns to the previous view.
	Forward	Returns to the view you were in when you selected Back.
	Refresh	Displays the most current information in the view you are in.
	Show/Hide	Acts as a toggle to show or hide the following: <ul style="list-style-type: none">■ Tree pane■ Filter by pane■ Table pane■ Details pane
Go	Home	Opens the CCS Home view.

Table 2-1 Menu options (continued)

Menu	Menu item	Description
	Monitor	Opens the CCS Monitor view.
	Manage	Opens the CCS Manage view.
	Settings	Opens the CCS Settings view.
	Reporting	Opens the CCS Reporting view
Tasks	The Tasks menu appears only for certain features.	Displays the list of available tasks that are relevant to the item that is selected in the view. The tasks in the list are the same tasks available from the taskbar .
Help	Help Topic	Opens the Control Compliance Suite Online Help.
	Index	Opens the help file Index tab.
	Search	Opens the help file Search tab.
	About	Opens the CCS About box. The About box provides information such as version number, copyright information, product information, and system information.

See [“About the console features”](#) on page 45.

About the tree pane

The tree pane displays a hierarchical, folder-based structure of the objects as stored in the Directory. The tree pane displays the objects that are relevant to the view in the console. For example, if you are in the Assets view, the tree pane displays only assets and the asset groups.

The tree pane appears on the left side of the console window under the navigation bar.

The tree pane contains the predefined folder and user-defined folders:

Predefined	Displays the built-in business objects that are installed along with the product. All users can access the Predefined folder. When you select a folder, the list of objects within the folder is displayed in the table pane. The objects in the Predefined folder cannot be modified.
------------	---

User-defined	Displays the hierarchical structure of folders as defined in the Directory. You can also create a folder structure from here. The hierarchy can be based on requirements such as platform and geographical locations. When you select a folder in the tree pane, the list of objects within that folder is displayed in the table pane.
--------------	---

See [“About working in the tree pane”](#) on page 59.

See [“About the console features”](#) on page 45.

About the Filter by pane

The **Filter by** pane displays the predefined filter options that correspond to each view in the console. You can select different options from the filter pane and click the Update icon to view the updated results in the table pane.

When filtering assets, you can only filter on the assets that are displayed in the table pane. You cannot filter on the assets that are in the asset store.

See [“Asset folder hierarchy”](#) on page 202.

The **Filter by** pane appears in the lower left side of the console window under the tree pane.

The filter pane has the following icons:

Customize	You can choose which filter options appear in the filter pane and the order in which the options appear. To choose the options that appear in the filter pane, you click the Customize icon.
Reset to last	You can reset the values of the filter options to the last saved values. When you make changes to the filter options and then decide to revert back to the previously selected filter options you click Reset to last icon. Once you navigate away from the view you cannot reset the options to the previous selection.
Update	When you modify the filter options and their values, you must click the Update icon to update the results in the table pane.

See [“Customizing the filter options”](#) on page 56.

See [“Using filters in the Filter by pane”](#) on page 56.

About the table pane

The table pane lists all the objects for the selected folder in the tree pane.

The table pane appears in the right side of the console window under the taskbar. You can select the object that you want to work with from the table pane. After the object is selected, all associated tasks are enabled on the taskbar. You can also use the context menu to do the tasks. Right-click the object in the table menu and the context menu appears.

You can also select multiple objects to work within the table pane. Select the check box next to the objects that you want to work with. Only the tasks that are associated with multiple selections are enabled.

When you edit multiple objects, the previous values of all the selected objects are replaced with the new values.

Use the **Filter by** pane and the other features of the console to manage and refine the results in the table pane.

See [“Managing the table pane”](#) on page 57.

See [“Viewing and editing the object details”](#) on page 58.

See [“Selecting the columns headings”](#) on page 58.

See [“About the console features”](#) on page 45.

About the details pane

The details pane displays the various properties of the object that is selected in the table pane. The object details are grouped in various tabs. The details pane appears in the lower-right side of the console window under the table pane. In the details pane, the object details are shown grouped in various tabs.

The details pane has the following icons:

Save	You can make changes to certain values in the details pane. To save any changes that are made in the tabs, you click Save .
Revert	You can reset the values of any changes that are made in the details pane. Revert only resets those values that have not been saved.
Refresh	You can refresh the details pane to display any properties that has changed since the view was selected.

See [“About the console features”](#) on page 45.

About the taskbar

The taskbar displays the tasks that are relevant to the object that are selected in the current view. The taskbar appears across on top of the tree pane and the table pane in the console window.

In some views, where there are larger number of tasks, the taskbar contains a drop-down menu. You can click on the drop-down menu to view the additional tasks.

See [“About the console features”](#) on page 45.

Accessing tasks

You can access tasks in the console from the following console features:

- Menu bar
- Navigation bar
- Taskbar
- Context menu

See [“About the console features”](#) on page 45.

About the console views

The console consists of several main views where you do your work. The views and tasks available to you are based on the roles and permissions that your administrator assigns to you.

The following are the main views of the console:

- Home view
- Monitor view
- Manage view
- Reports view
- Settings view

See [“About the console features”](#) on page 45.

About the Home view

The **Home** view is the default view that appears when you log on to the Control Compliance Suite (CCS) Console. The Home view contains the **Home** page and the **User Preferences** page.

The Home page displays items such as your preferred reports, and your preferred dashboards. You can customize the Home view to display a default report and a default dashboard.

The Home page displays your preferred reports. You can customize the Home page to display a default report.

The Home view contains the following information:

My Reports	<p>The reports panel lists the first ten most recent reports you have viewed. You can change the number of reports to be listed in the Settings > General view.</p> <p>See “Configuring the Home view settings” on page 144.</p> <p>You can click the View All link to view all the reports from the My Reports view.</p>
My Dashboards	<p>The dashboards panel lists all the summary dashboards for which you have permissions. The tiered dashboards are not displayed here. You can choose a dashboard from the drop-down list and make it your default dashboard.</p> <p>You can click on the View All link to view all the dashboards from the My Dashboards view.</p>
User Preferences	<p>The User Preferences page allows users with the role to schedule jobs to store their password. The credentials are used to run the scheduled jobs at a later time.</p>

See [“About the User preferences page”](#) on page 55.

See [“Adding credentials for scheduled jobs”](#) on page 55.

See [“About the console views”](#) on page 51.

About the Monitor view

The **Monitor** view displays the information that is related to Jobs and Evaluation Results.

The **Monitor** view consists of the following views:

- **Jobs**
- **Evaluation Results**

See [“About the Jobs view”](#) on page 599.

See [“About the Evaluation Results view”](#) on page 611.

About the Manage view

The Manage view lets you perform all the tasks that are related to assets, entitlement, exceptions, standards, tags, and policies in the Control Compliance Suite.

The Manage view consists of the following views:

- Assets
- Entitlements
- Exceptions
- Standards
- Baselines
- Tags
- Content
- Policies

About the Settings view

The Settings view contains the tools that help the administrator to easily and efficiently configure and manage the Control Compliance Suite infrastructure.

The Settings view is displayed only to users with the Administrator role.

You can do the following from the Settings view:

- Configure and manage the infrastructure components.
- Deploy infrastructure updates, content updates, and patches.
- Report on the configuration and the health status of the infrastructure components.
- Configure and manage users, roles, and credentials.
- View component certificates
- Collect evidence
- Manage asset and entity schema

Settings contains the following views:

- General
- Roles
See [“About the Roles view”](#) on page 87.
- Permissions Management

See [“About the Permission Management view”](#) on page 88.

- Licenses
See [“About the Licenses view”](#) on page 149.
- LiveUpdate
See [“About the LiveUpdate view”](#) on page 164.
- System Topology
See [“About the Map view”](#) on page 103.
See [“About the Grid view”](#) on page 106.
- Certificates
See [“About the Certificates view”](#) on page 69.
- User Management
See [“About the User Management view”](#) on page 151.
- Schema Manager
See [“About the Schema Manager view”](#) on page 346.
- Extended Evidence Source

About the Reporting view

Control Compliance Suite provides a rich set of presentation-level reports. A report is a business document that contains a predefined, organized collection of data. A report can be viewed, printed, or analyzed. Reports are viewed in the Reporting view. You schedule reports in the Job Management view. The reporting features let you distill the data and publish the results.

To view dashboards, you are required to install a Flash player with the CCS console.

You can do the following in the Reporting view:

- Manage reports and dashboard templates
- Manage reports
- Export reports to a different format
- Manage historical data in My Reports view
- Generate reports on compliance-relevant areas in the Control Compliance Suite

The Reporting view comprises the following:

- Reports Templates view
- Dashboard Templates view
- My Reports view

See [“About the Reports Templates view”](#) on page 616.

See [“About the Dashboard Templates view”](#) on page 621.

See [“About the My Reports view”](#) on page 618.

Adding credentials for scheduled jobs

Users with the role to schedule jobs can store their passwords. The password is required for asset resolution on the jobs that are scheduled to run at a later time.

This feature is available only if the administrator has selected the option to store password in Control Compliance Suite.

See [“About the security settings for scheduled jobs”](#) on page 154.

Only users with the role to schedule jobs can store their passwords.

To add user preferences

- 1 Go to the **Home > User Preferences**.
- 2 In the **User Preferences** view, type the password.
- 3 Click **Update password**.

About the User preferences page

Users with the role to schedule jobs can store their passwords. The password is required for asset resolution on the jobs that are scheduled to run at a later time. Only users with the role to schedule jobs can store their passwords.

This feature is available only if the administrator has selected the option to store password in Control Compliance Suite.

See [“About the security settings for scheduled jobs”](#) on page 154.

See [“About the Home view”](#) on page 51.

Working in the console

You can perform various tasks in the console views based on the roles and permissions that are assigned to you.

See [“Using filters in the Filter by pane”](#) on page 56.

See [“Customizing the filter options”](#) on page 56.

Using filters in the Filter by pane

When configuring your console, you can set filters in each view to limit the number of objects that display in the table pane. Each view has a set of predefined filters that correspond to the type of information in the view. The **Filter by** pane also provides a customize feature where you can choose the filter options that appear in the **Filter by** pane.

See [“Customizing the filter options”](#) on page 56.

To use filters

- 1 In the **Filter by** pane, select the check box that corresponds to the required filter.
- 2 If applicable, select the filter value from the associated list box.
- 3 For certain filters, you must provide the upper and lower limit values to obtain the results that exist within the range.
- 4 Click the **Update** icon to view the results in the table pane.

See [“About the Filter by pane”](#) on page 49.

Customizing the filter options

You can choose which filter options and the order the options appear in the **Filter by** pane.

To customize the filter options

- 1 In the **Filter by** pane, click the **Customize** icon.
- 2 In the **Customize Filters** dialog box, from the list box select the filter type to edit.
- 3 For the selected filter type, you can do any of the following:
 - Select or deselect the Display filter type check box. If you deselect the filter type, the filter type and its options are not displayed in the **Filter by** pane.
 - Use the arrow icons to move the options between Display and Do not display boxes.
 - Use the **Move up** and **Move Down** icons to change the order of the options that is displayed in the **Filter by** pane.
- 4 Click **Save Changes**.

See [“About the Filter by pane”](#) on page 49.

See [“Using filters in the Filter by pane”](#) on page 56.

Managing the table pane

Use the Filter by pane and other areas of the console to manage and refine the results that are displayed in the table pane.

To manage the table pane

- 1 In the tree pane, navigate to the required folder.
- 2 Use any of the following to manage the objects that are shown in the table pane:

Filter by pane	Select the filter options in the Filter by pane to refine the results in the table pane.
Display list box	<p>The Display list box lists the different types of content that can be displayed in the table. For example, in the Assets view, some of the Display selections are: Assets and Asset Groups, Asset Groups Only, and Assets Only.</p> <p>The Display list box is displayed on the top-left side of the table pane. The Display selection remains when you navigate away from the view and return.</p>
Column chooser	Select the column headings that you want to see or hide in the table pane. To select the column headings, you click the column chooser icon. The options available in the Column Chooser dialog box depend on what is selected in the Display list box. The column chooser icon is displayed in the top-right side of the table pane.
Column sort	The content of table can be arranged based on the content of the columns that compose the table. Contents can be arranged in ascending or in descending order. The up or down arrow in the column heading indicates the order in which the table is sorted.
Column order	The columns can be rearranged in any order. To move a column, you drag the heading of the column to move to the new location in the column header.
Column groups	Some tables have the capability to group the table results by any column heading. This feature is available when the blue text “Drag a column heading here to group by that column” appears above the column headings. To group the results by column heading, you drag the heading of the column to group on to the Drag a column heading here area.

See [“About the table pane”](#) on page 49.

See [“Viewing and editing the object details”](#) on page 58.

Viewing and editing the object details

You can view and edit some of the object details from the details pane or from the details dialog box. The object details are grouped and displayed in tabs. Not all object details can be edited.

You can also select multiple objects to edit. Select the check box next to the objects that you want to edit. When you edit multiple objects, the previous values of all the selected objects are replaced with the new values.

To view and edit the object details in the details pane

- 1 In the table pane, select the object.
- 2 In the details pane, the object details are shown grouped in various tabs.
- 3 Select the required tab and edit the details.
- 4 Click the **Save** icon.

To view and edit the object details using the details dialog box

- 1 In the table pane, select the check box next to the object.
- 2 Do one of the following:
 - Click **Edit Details** in the taskbar.
 - Double-click the object.
 - Right-click the object, and click **Details**.
- 3 In the details dialog box, edit the details if required.
- 4 Click **Save**.

See [“About the table pane”](#) on page 49.

See [“Managing the table pane”](#) on page 57.

Selecting the columns headings

You can select the column headings that you want to see or hide in the table pane.

To select the column headings

- 1 In the view, click the **column chooser** icon.
- 2 In the **Column Chooser** dialog box, check the column headings.

See [“About the table pane”](#) on page 49.

Refreshing the view

You can refresh the view to update the currently displayed information with new information.

To refresh the view

- ◆ Do one of the following:
 - On the keyboard, press **F5**.
 - In the Menu bar, click **View > Refresh**.

See [“About the console features”](#) on page 45.

Searching for objects

You can perform a quick search or an advanced search to search for an object in the table pane. The search is performed on the contents of the selected folder in the tree pane. The type of objects you can look for depends on the current view. For example, if you are in the **Standards** view, you can search for standards, sections, checks, or all three.

When searching for assets in the **Assets** view, you can only search for the assets that are displayed in the table pane. You cannot search for the assets that are in the asset store.

See [“Asset folder hierarchy”](#) on page 202.

To perform a quick search

- 1 In the table pane, in the **Search** text box, type a text string.
- 2 To narrow the search to a certain type, select the type from the Search drop-down box.
- 3 Click the **Search** icon.

To perform an advanced search

- 1 In the table pane, click the **Expand** icon that is on the top-right of the table pane.
- 2 In the **Advanced Search** pane, select the details and click **Search**.

See [“About the console features”](#) on page 45.

About working in the tree pane

The tree pane provides a context menu for doing the common tasks on the folders. The menu options that are displayed are different in each view. Right-click the folder in the tree pane and the context menu appears.

The following common tasks are available in most views:

- Move folder
See [“Moving folders in the tree pane”](#) on page 61.
 - Create new folder
See [“Creating folders in the tree pane”](#) on page 60.
 - Delete folder
See [“Deleting folders in the tree pane”](#) on page 61.
 - Rename folder
See [“Renaming folders in the tree pane”](#) on page 62.
 - Refresh folder
See [“Refreshing folders in the tree pane”](#) on page 62.
- See [“About the tree pane”](#) on page 48.

Creating folders in the tree pane

You create folders to organize the business objects in a hierarchical manner.

To create a folder in the tree pane

- 1 In the tree pane, right-click the root folder or an existing folder.
- 2 Select **New Folder**.
- 3 In the **Create New Folder** dialog box, type the name of the folder.
- 4 Click **OK**.

See [“About using special characters in folder and job names”](#) on page 60.

See [“Creating the asset folders”](#) on page 305.

See [“About the tree pane”](#) on page 48.

About using special characters in folder and job names

When you create folders in the tree pane from any view, you need to ensure that you do not use certain special characters. The usage of special characters is not allowed in cases where a folder is created dynamically by the name of some value.

Consider the following example:

You create a Post Rule. Add an action to move the assets to the folder. You choose to create the folder dynamically based on the name of the value of the selected field. In this case, if the value of the field contains a special character that is not supported the folder is created with a different name.

Note: If a folder name contains a special character that is not supported by Control Compliance Suite, the character is replaced with - (hyphen).

Control Compliance Suite does not support the following special characters in the folder name and the job name:

- *
- (
-)
- \
- /
- ,
- +
- "
- <
- >
- ;
- =
- #
- \r

See [“Creating folders in the tree pane”](#) on page 60.

Moving folders in the tree pane

The move feature lets you easily change the location of a folder in the tree pane. When you move a folder, all the child folders are also moved.

To move a folder in the tree pane

- 1 In the tree pane, right-click the folder to move and select the **Move** task.
- 2 In the **Move** dialog box, select the new location in the tree pane.
- 3 Click **OK**.

See [“About working in the tree pane”](#) on page 59.

Deleting folders in the tree pane

When you delete a folder, all the child folders and objects are deleted.

To delete a folder in the tree pane

- 1 In the tree pane, right-click the folder to delete.
- 2 Select the **Delete** task.
- 3 In the message dialog box, click **OK**.

See [“About the tree pane”](#) on page 48.

Renaming folders in the tree pane

You can rename a folder in the tree pane.

To rename a folder in the tree pane

- 1 In the tree pane, right-click the folder to rename.
- 2 Select the **Rename** task.
- 3 In the **Rename** dialog box, type the new name of the folder.
- 4 Click **OK**.

See [“About the tree pane”](#) on page 48.

Refreshing folders in the tree pane

You must refresh the folder to display any changes in the directory objects.

To refresh a folder in the tree pane

- 1 In the tree pane, right-click the folder to refresh.
- 2 Select the **Refresh** task.

See [“About the tree pane”](#) on page 48.

Configuring Control Compliance Suite

This chapter includes the following topics:

- [Configuration tasks](#)
- [Managing certificates](#)
- [Configuring roles and permissions](#)
- [Registering and configuring the Data Processing Service](#)
- [Working in the System Topology view](#)
- [Configuring sites](#)
- [Configuring the data collectors](#)
- [Configuring the general settings](#)
- [About audits](#)
- [Managing licenses](#)
- [Managing users](#)
- [Configuring the application server settings](#)
- [About the security settings for scheduled jobs](#)
- [Configuring the assets batch size](#)
- [Configuring the SQL Server settings](#)
- [Configuring the application server credentials](#)

- [Updating Control Compliance Suite](#)
- [Configuring Response Assessment Module in Control Compliance Suite](#)
- [About configuring the Web Portal to contact RAM](#)
- [About logs and configuration files](#)

Configuration tasks

The administrator must perform certain tasks before the system users can use Control Compliance Suite (CCS) to collect and report on the compliance data from across the organization.

You can access the Configuration tasks topic from the **Help > Configuration** menu item.

You do the following tasks to configure CCS. Click on the links to learn more about how to perform each task.

See [Table 3-1](#) on page 64.

See [Table 3-2](#) on page 65.

See [Table 3-3](#) on page 66.

See [Table 3-4](#) on page 67.

Table 3-1 Initial configuration tasks

Tasks and links	Description
Create asset folders in the Manage > Asset System view.	<p>The user-defined folders store business objects in a hierarchical manner that reflects your organizational structure. The user-defined folders let you effectively assign permissions.</p> <p>When you install CCS, a default hierarchy structure is created to store objects. Users should organize the tree to follow the flow of control in the organization.</p> <p>See “Creating the asset folders” on page 305.</p>
Assign users to roles.	<p>The role determines what you can see and perform in the CCS Console. In addition to the role, you must have permission on the required folders and objects to successfully perform a task.</p> <p>See “Adding users and groups to a role” on page 89.</p>

Table 3-1 Initial configuration tasks (*continued*)

Tasks and links	Description
Assign permissions to trustees.	You must manually assign permissions to the user-defined folders. When a role is assigned to a user, permissions are automatically granted to the objects in the predefined folders. See “Assigning permissions from the Permission Management view” on page 95.
Create sites to match the structure in the deployment plan.	You create sites to manage logical groups of assets. Grouping of assets facilitate data collection and other CCS operations. See “Creating a site” on page 113.
Register installed Data Processing Service instances.	Before the Application Server can use a newly installed Data Processing Service (DPS), you must register the DPS with the Application Server. When you register the DPS, you also assign the DPS to a site and specify the DPS roles. Where appropriate, specify data types to collect. See “Registering the Data Processing Service” on page 98.

You do the following tasks to discover assets, and then collect and evaluate data from the imported assets.

Table 3-2 Assets, data collection, and evaluation tasks

Task	Description and task links
Create asset import reconciliation rules as specified in the deployment plan.	The reconciliation rules let you filter the potential assets before they enter the asset system. The reconciliation rules also help to update the field values of the existing assets. See “Creating reconciliation rules using the manual review” on page 254. See “Creating reconciliation rules without manual review” on page 253.

Table 3-2 Assets, data collection, and evaluation tasks (*continued*)

Task	Description and task links
Create asset import jobs.	<p>You must import assets from the network before you can collect data from the assets and evaluate the assets against specific standards and checks.</p> <p>You can import the assets in one of the following ways:</p> <p>See “Importing the assets for the first time” on page 265.</p> <p>See “Importing asset-specific fields from the default data collector” on page 272.</p> <p>See “Importing asset-specific and common fields using the default data collector” on page 275.</p> <p>See “Importing asset-specific and common fields using the CSV data collector” on page 278.</p> <p>See “Importing the specific and common fields for custom asset using the CSV data collector” on page 281.</p> <p>See “Working with asset import scenarios” on page 267.</p>
Set up data collection jobs.	<p>After you have imported the assets you create jobs to collect data from the imported assets.</p> <p>See “Setting up a data collection job from the Assets view” on page 310.</p>
Create evaluation jobs.	<p>After you have collected the data from the imported assets you create jobs to evaluate the assets.</p> <p>See “Running an evaluation job from the Asset System view” on page 311.</p>

You do the following tasks to discover control points and create reports and dashboards.

Table 3-3 Entitlements, reports, and dashboards tasks

Task	Description and task links
Mark and configure entitlement control points.	<p>You mark an asset as a control point to monitor the entitlements of the asset through the approval workflow.</p> <p>See “Marking an asset as a control point” on page 398.</p> <p>You configure a control point to assign a data owner, an approver, the tags, and the review cycle to the control point</p> <p>See “Configuring control points” on page 400.</p>

Table 3-3 Entitlements, reports, and dashboards tasks (*continued*)

Task	Description and task links
Create report jobs.	<p>The report job generates a report with the data from the reporting database.</p> <p>You must synchronize the reporting database to view the latest data before you run a report job.</p> <p>The Reporting Database Synchronization job is an existing job in the Monitor > Jobs view.</p> <p>See “Running a job now” on page 603.</p> <p>See “Scheduling a report ” on page 636.</p>
Create dashboard jobs.	<p>The dashboard job generates the dashboard with the data from the reporting database.</p> <p>In order to see data, you must run the Scheduled Reporting Synchronization Job from the Monitor > Jobs view before you open a dashboard or panel for the first time.</p> <p>The Reporting Database Synchronization Job job is an existing job in the Monitor > Jobs view.</p> <p>See “Running a job now” on page 603.</p>

You do the following tasks to create and publish policies across the organization.

Table 3-4 Policies and RAM tasks

Task	Description and task links
Create policies.	<p>Policies are rules established by an organization. Policies are designed to guide their employees. You can create a policy from scratch or import a Microsoft Word document as a policy.</p> <p>See “Creating a new policy” on page 579.</p> <p>See “Importing a Word policy” on page 581.</p>
Publish policies.	<p>After a policy is created and approved, the policy is published to the selected audience members in the organization. The audience members can access the policy from the CCS Web Console.</p> <p>See “Publishing a policy” on page 587.</p>

Table 3-4 Policies and RAM tasks (continued)

Task	Description and task links
Optionally publish Response Assessment module questionnaires.	See <i>Symantec Response Assessment module User Guide</i> for information on publishing questionnaires. See “About Response Assessment Module ” on page 39.

Managing certificates

In Control Compliance Suite (CCS), a unique certificate is created for each installable component on each host. Certificates secure the environment by using a unique identifier for communications between Control Compliance Suite core components. If any host or certificate becomes compromised, the compromised single certificate can be revoked using the **Certificate Management Console**. When the certificate is revoked, only the compromised component is effected. The certificate of the single component must be regenerated and bound with the Control Compliance Suite system, and the component is fully functional again. If a host or certificate is compromised no other components are affected. Certificates are kept and maintained in the certificate store.

If any host or certificate becomes compromised, the compromised single certificate can be unbound using the **Certificate Management Console**. When the certificate is unbound, the compromised component can communicate with other CCS components. The **Symcert** `untrust` command places the certificate in an untrusted store and revokes communications with that certificate. The certificate of the single component must be regenerated and bound with the Control Compliance Suite system, and the component is fully functional again.

You can review the certificates in the following locations:

- **Certificates** view in the CCS Console
- **Certificate Management Console**

See [“About Management Services”](#) on page 68.

See [“About the Certificates view”](#) on page 69.

See [“Registering the Data Processing Service”](#) on page 98.

About Management Services

Management Services is the root certificate authority service that is used to generate, manage, and sign certificates for the CCS components.

The **Certificate Management Console** is installed on the same system as Management Services to manage certificates. Using the console, users can create, renew, revoke, or remove certificates.

Symcert is a command-line utility that provides an optional method of managing certificates and is installed when a certified component is installed.

The Certificate MMC Snap-in component should not be used to install or remove CCS component certificates.

See [“About the Certificates view”](#) on page 69.

See [“Using the Certificate Management Console”](#) on page 70.

About the Certificates view

The **Certificates** view lists the certificates that have not been removed from the system. You can review the specific properties for each certificate.

You can do the following:

- **Search** for a specific certificate by any of the certificate properties
- **Clear** the results of the search
- Use **Column Chooser** to select if specific columns are visible
- Quickly view the number of certificates that are available in the view and for each of the categories

You can rearrange the columns for the view. If you rearrange the columns, the rearranged layout does not persist. The columns return to their default locations when you open or refresh the view.

If you want to modify a certificate, you must use the **Certificate Management Console**.

You can view the following categories:

Table 3-5 Categories and descriptions

Category	Description
Bound	The certificate is connected to a certain component
Root Certificate	The top level of the certificate hierarchy
Unbound	The certificate is not connected to a component
Disabled/Unbound	The certificate is no longer needed but not removed

The **Disabled/Unbound** status is used for the certificates that should no longer be bound due to the uninstallation of a component. A certificate with this status can safely be removed. You can rebind a certificate in the **Disabled/Unbound** state in the **Certificate Management Console**. **Disabled/Unbound** DPS certificates may only be bound if the component has been registered in the CCS Console.

You can review the following properties for each certificate:

Table 3-6 Certificate properties

Name	Description
Component Name	The component that is used during the certificate creation.
Expiration Date	Date and time when the certificate is no longer valid
Host Name	The fully qualified domain address for the component
Serial Number	The serial number is a unique identifier for a certificate. The number lets you identify a certificate if multiple certificates exist for the same component.

About managing certificates using the command line

SymCert is a command-line tool that is used to manage the certificates. When a component that requires certification is installed on a computer, the command-line tool is also installed. You must have local administrator rights on the computer. You can install or delete a certificate using the command-line tool. If you delete a certificate, the certificate can be reinstalled using the install command.

See [“About Management Services”](#) on page 68.

See [“About the Certificates view”](#) on page 69.

See [“Using the Certificate Management Console”](#) on page 70.

Using the Certificate Management Console

The Certificate Management Console is installed on the same system as the Management Services. The user must have local administrator rights to work with the Certificate Management Console.

Table 3-7 Certificate life cycle

Action	Description	More information
Creation	You create the certificate based on the service type.	

Table 3-7 Certificate life cycle (*continued*)

Action	Description	More information
Renewal	You can renew the certificate, which extends the life of the certificate.	See “Renewing certificates” on page 75.
Bind	In certain circumstances, you can bind a certificate. The system trusts a component with a bound certificate.	
Unbind	A certificate can become invalid before the expiration date. Under such circumstances, you should unbind the certificate.	
Removal	You should remove the disabled/unbound certificates or expired certificates when you perform a periodic system cleanup.	

The user uses the **Certificate Management Console** to do the following:

- Create a certificate.
- Renew certificates.
- Review certificate status.
- Revoke certificates.
- Remove certificates.

See [“Managing certificates”](#) on page 68.

About the Certificate Management Console

The **Certificate Management Console** is used to manage certificates for Control Compliance Suite. The **Certificate Management Console** is installed on the same system as the Management Services. The console cannot be accessed remotely. Users must be logged on to the system that hosts the Management Services to access the **Certificate Management Console**.

You can view the following information on each certificate:

- Issued to
- Expiration Date
- Host Name
- IP Address
- Status

You can do a search on the certificates on any of the columns. You can drag a column header to group the certificates by that column.

Using the **Certificate Management Console**, certificates can be created, renewed, revoked, or removed. The user views the status of the issued certificates.

The type of installation determines the number of certificates that are created automatically. A directory service (DSS) installation always creates the root certificate. The DSS install also creates and binds the Management Service certificate. The DSS installation does not create the certificates that are needed to install the application server or the DPS servers. You must create the service type certificate for each installed component. For example, if your system has 50 DPS components, you must create 50 certificates. Each CCS component has a host registration in ADAM. In a single system installation, the certificates are created and bound for each component during installation. The DPS certificate is not bound during the single system installation. The certificate is created but it's host record is not created during installation so the certificate cannot be bound until the DPS registration occurs. The registration process both creates the host record and binds the certificate to the host record. In a distributed installation, you create the application server and DPS certificates manually using the **Certificate Management Console**. The application server certificate is unbound until the component is installed. The DPS Certificate is unbound until registered in **System Topology** in the CCS Console.

In a single system installation, the following certificates are created automatically:

CA	Root certificate
ManagementServices-<computer name>	Trusted
AppServer-<computer name>	Trusted
DPS-<computer name>	Trusted

In a distributed installation, the following certificates are created:

CA	Root certificate
ManagementServices-<computer name>	Trusted

See [“Using the Certificate Management Console”](#) on page 70.

See [“About Management Services”](#) on page 68.

Creating a DPS or an application server certificate

You create the certificate that is based on the service type. You should verify that the service type that you select creates the appropriate certificate. You can create multiple certificates. Certain property items are used as the default information from the previous certificate, but all of the items can be edited. Every item in the **Create Certificates** dialog box is required. The information that you provide in the certificate is not validated. You should verify that the information is accurate.

You must have local administrator rights to create a certificate and you must be a CCS administrator and know the root certificate password.

You are not prompted for a root certificate password if one of the following events has occurred:

- You have previously opened the **Certificate Management Console**
- You are logged on in the context of the user who installed the system

You can create certificates for either the Data Processing Service (DPS) or application server. You should verify that the service type that you select creates the appropriate certificate.

On Windows Server 2008 with UAC enabled, use the **run as administrator** option when launching the **Certificate Management Console**.

You can find a list of the **Country** codes at:

http://www.iso.org/iso/country_codes/iso_3166_code_lists/english_country_names_and_code_elements.htm

See “[Using the Certificate Management Console](#)” on page 70.

See “[Managing certificates](#)” on page 68.

See “[Renewing certificates](#)” on page 75.

To create a DPS or an application server certificate

- 1 Click **Start > All Programs > Symantec Control Compliance**, and then select **Certificate Management Console**.
- 2 You may be prompted to provide the **Root Certificate Password**.
The password is used during installation.
- 3 Click **OK**.
- 4 In the **Certificate Management Console** toolbar, click **Create Certificates**.
- 5 In the **Create Certificates** dialog box, in the **Service Type** area, do one of the following:
 - Click **AppServer**

■ Click **DPS**

The default selection is DPS.

- 6 In the **Expired In** box, select the number of years.
The default value is 25.
- 7 In the **Organization** box, provide a name.
You can change the default name during certification creation.
- 8 In the **Division** box, provide a name.
You can change the default name during certification creation.
- 9 In the **City** box, provide a name.
You can change the default name during certification creation.
- 10 In the **State/Province** box, provide a name.
You can change the default name during certification creation.
- 11 In the **Country** box, provide a name.
You can change the default code during certification creation.
- 12 In the **NetBIOS Name** box, provide the name.
The NetBIOS Name must be less than 15 bytes in length.
You can browse to select a **NetBIOS name**
- 13 In the **FQDN** box, provide the name.
- 14 In the **IP Address** box, provide the information.
- 15 Click (+) plus icon to add multiple TCP/IP addresses, if needed.
- 16 In the **Destination folder** box, provide the location for the saved certificate file.
You can browse to select the location.
- 17 In the **Password** box, type a password.
- 18 In the **Retype Password** box, type the same password to confirm the spelling.
- 19 Click **Create Certificate**.
- 20 In the **Success** message box, click **OK**.
- 21 In the **Create Certificate** message box, click **Yes** to create another certificate, if needed.

Renewing certificates

If a particular certificate is about to expire, you can renew the certificate. A renewal extends the date of the certificate. You must know the location and password for the current version to renew the certificate. You cannot change the password. The default value for the renewal is 25 years. When the certificate is renewed, its new expiration date must be less than January 1, 2038. The **Expires In** selection adds the number of years to the number of years that remain for that certificate.

When you open the console, you may be prompted to provide the root certificate password. The password is created during the installation of Control Compliance Suite (CCS).

The root certificate password is not required if either of the following conditions have occurred:

- You have previously opened the console
- You are logged on in the context of the user who installed CCS

All information in the **Renew Certificate** dialog box is required.

Table 3-8 Renew Certificate options

Name	Description	Default value
Current Certificate	Location of the current certificate. You can use Browse to navigate to the location.	None
Password	The password that is assigned to the certificate during the certificate creation.	None
Destination folder	The folder to store the certificate. You can accept the current location or provide another location. You can use Browse to navigate to a location.	<InstallDir> \ManagementServices\ DefaultCerts
Expires In	The number of years for the certificate's lifetime	25

See [“Managing certificates”](#) on page 68.

See [“Using the Certificate Management Console”](#) on page 70.

To renew a certificate

- 1 Click **Start > All Programs > Symantec Control Compliance > Certificate Management Console**.
- 2 Provide the **Root Certificate Password** and click **OK**, if needed.
The password is used during installation.
- 3 In the **Certificate Management Console**, select the check box for the appropriate certificate and then click **Renew Certificates**.
- 4 In the **Renew Certificate** dialog box, complete the form. The description for the options is available in [Table 3-8](#)
- 5 Click **Renew Certificate**.
- 6 In the **Success** message box, click **OK**.

Revoking certificates

The administrator or the certificate authority (CA) can revoke a certificate. Revocation prevents use of the public key for decryption.

Certificates are issued with a planned lifetime. That lifetime is defined in the **Years until expired** field when the certificate is created. A certificate is valid until its expiration date. However, circumstances may cause a certificate to become invalid before the expiration date. Under such circumstances, the issuing certificate authority (CA) or the administrator should revoke the certificate.

The certificate status is changed to revoked.

See [“Removing revoked certificates”](#) on page 77.

See [“Creating a DPS or an application server certificate”](#) on page 73.

See [“Renewing certificates”](#) on page 75.

See [“Removing revoked certificates”](#) on page 77.

To open the Certificate Management Console

- 1 Click **Start > All Programs > Symantec Control Compliance > Certificate Management Console**.
- 2 Provide the **Root Certificate Password** and click **OK**, if needed.
The password is used during installation.

To revoke a certificate

- 1 Click Start > All Programs > Symantec Control Compliance, and select **Certificate Management Console**.
- 2 In the **Certificate Management Console**, provide the **Root Certificate Password**.
The root certificate password is created during installation.
- 3 Click **OK**.
- 4 In the **Certificate Management Console**, select the certificate.
- 5 Click **Revoke Certificates**.
- 6 In the **Warning** message box, click **Yes**.

Removing revoked certificates

The administrator removes revoked certificates. A removed certificate is no longer available to the users.

See [“Managing certificates”](#) on page 68.

See [“Creating a DPS or an application server certificate”](#) on page 73.

See [“Renewing certificates”](#) on page 75.

See [“Revoking certificates”](#) on page 76.

To remove a revoked certificate

- 1 Click Start > All Programs > Symantec Control Compliance, and select **Certificate Management Console**.
- 2 In the **Certificate Management Console**, provide the **Root Certificate Password**.
The root certificate password is created during installation.
- 3 Click **OK**.
- 4 In the **Certificate Management Console**, select the certificate.
The certificate must have the revoked status.
- 5 Click **Remove Certificates**.
- 6 In the **Warning** message box, click **Yes**.

Configuring roles and permissions

Control Compliance Suite (CCS) supports a combination of roles and permissions-based access control. When the users log on, they see only a filtered application that is based on their role. The role defines the access privileges for the views and tasks. The permissions that the user has on the objects in the CCS directory determine the tasks that the user can perform on an object.

Access control in CCS works in the following order:

- Related and relevant tasks are collected to define a role. Role and task association is predefined and cannot be modified.
- Roles are assigned to users or groups who access the application.
- Users are then assigned the permissions to objects to perform certain tasks. Only users with permissions can perform certain tasks on the objects.

CCS provides the interface to assign the predefined roles and permissions to the CCS users. If a user's role assignment is modified, the user must quit and then restart the CCS console. When the console restarts, the user can see the new views and tasks that are associated with the role.

CCS also provides the facility to create custom roles if the predefined roles do not fit the needs of your organization.

See [“About custom roles”](#) on page 86.

See [“About roles”](#) on page 78.

See [“About tasks”](#) on page 79.

See [“About permissions”](#) on page 79.

See [“Predefined roles”](#) on page 80.

About roles

In Control Compliance Suite (CCS) a role is a collection of predefined tasks or functions. The user may perform each task that is a specific action, such as Create a policy or Run an evaluation. The role determines what a user can see and perform in the CCS console.

To have a role does not automatically grant the user the rights that are required to perform the task on the directory objects. In addition to the role, the user must have access rights on the required directory objects to successfully perform a task.

For example, if the user is in the Evaluators role, the user is allowed to set up and run evaluation jobs. But when the evaluation job is run, the results are based only on the assets for which the user has been granted the Evaluate permission.

CCS provides a number of predefined roles to suit your organizational needs. The predefined role and task association cannot be modified. However, CCS lets you create custom roles.

See [“About custom roles”](#) on page 86.

See [“Predefined roles”](#) on page 80.

See [“About permissions”](#) on page 79.

See [“About tasks”](#) on page 79.

See [“Configuring roles and permissions”](#) on page 78.

About permissions

Control Compliance Suite (CCS) lets you control which users have what access to which directory objects. When a user account is authenticated, the type of access granted to the objects is determined by the permissions that are attached to the objects.

When a role is assigned to a user, permissions are automatically granted to the directory objects in the predefined folders. The administrator must manually assign permissions to the user-defined folders at a later time.

Every directory object has a set of effective rights that is either assigned directly to or is inherited from the parent folder. The effective rights determine what kind of directory operations a specific user can perform on that object.

Objects are stored in the CCS directory. The directory is hierarchical in nature. You can create folders and objects in an inverted tree-like structure. The directory gives the user the flexibility to create a hierarchy that allows them to model the tree that is based on their organizational needs.

See [“About roles”](#) on page 78.

See [“About tasks”](#) on page 79.

See [“Configuring roles and permissions”](#) on page 78.

See [“Predefined roles”](#) on page 80.

About tasks

A task is an action that a user performs. CCS provides numerous tasks at a detailed level of granularity. For example, Create a policy or Run an evaluation are tasks provided by CCS. A collection of predefined tasks define a role. When a user is assigned to a role, the user can perform the tasks that are associated with the role.

See [“About roles”](#) on page 78.

See [“Predefined roles”](#) on page 80.

See [“About permissions”](#) on page 79.

See [“Configuring roles and permissions ”](#) on page 78.

Predefined roles

Control Compliance Suite (CCS) includes several predefined roles that you can assign to users. These roles specify the level of interaction that the users have when they log on to the console.

An administrator can allow or block user access to features and functionality in the product by assigning different roles to the console users. Predefined roles cannot be edited.

Various CCS roles are based on the features and functionality of the product.

Table 3-9 Administrative roles

Role	Description
CCS Administrator	The CCS Administrator has full access to all the features of CCS. You can view the list of available tasks from the Settings > Roles view.
Power User	The Power User role lets the user do everything the CCS Administrator can do except the following tasks: <ul style="list-style-type: none">■ Configure application.■ Manage audits.■ Manage licenses.■ Assign policy audience. You can view the list of available tasks from the Settings > Roles view.

Table 3-9 Administrative roles (*continued*)

Role	Description
Auditor	<p>The Auditor role lets the user view the following:</p> <ul style="list-style-type: none">■ View all jobs.■ View assets and asset reconciliation rules.■ View baselines and baseline comparison results.■ View control points.■ View evaluation results.■ View notification templates.■ View roles and permissions.■ View policies, policy comments, and policy content.■ View reports and report templates■ View dashboards and dashboard templates■ View dashboards and tiered dashboards.■ View review cycles■ View standards

Table 3-10 Default CCS user role

Role	Description
Guest User	<p>By default, all the authenticated CCS users have the Guest User role.</p> <p>The Guest User role lets the user do the following:</p> <ul style="list-style-type: none">■ Accept or decline policies.■ Request exceptions.■ View policies and policy comments.

Table 3-11 Assets roles

Role	Description
Assets Viewer	<p>The Assets Viewer role lets the user do the following:</p> <ul style="list-style-type: none">■ View asset details.■ View asset group details.

Table 3-12 Standards roles

Role	Description
Standards Administrator	<p>The Standards Administrator role lets the user do the following:</p> <ul style="list-style-type: none"> ■ Manage configuration settings. ■ Manage standards, sections, and checks. ■ Manage jobs. ■ Collect data. ■ Evaluate standards. ■ Manage tags. ■ Request exceptions. ■ Generate reports and dashboards. ■ Manage tiered dashboards. ■ View assets. ■ View standards. ■ View evaluation results. ■ View roles and permissions. ■ View reports and report templates. ■ View dashboards and dashboard templates. ■ Customize report templates. ■ View roles and permissions.
Standards Evaluator	<p>The Standards Evaluator role lets the user do the following:</p> <ul style="list-style-type: none"> ■ Manage jobs. ■ Collect data. ■ Evaluate standards. ■ Manage jobs. ■ Manage tags. ■ Manage tiered dashboard. ■ Request exceptions. ■ Generate reports and dashboards. ■ View evaluation results. ■ View dashboards and reports. ■ View assets. ■ View standards. ■ View and customize dashboard and report templates.

Table 3-12 Standards roles (*continued*)

Role	Description
Remediation Administrator	<p>The Remediator role lets the user do the following:</p> <ul style="list-style-type: none">■ Collect data.■ Manage jobs.■ Execute remediation action.■ Evaluate standards.■ Evaluate assets.■ Manage jobs.■ Manage tags.■ Manage configuration settings■ Manage tiered dashboards■ Request exceptions.■ Generate reports and dashboards.■ View configuration settings■ View dashboards, tiered dashboards, and reports.■ View dashboard templates and report templates.■ Customize report templates.■ View evaluation results.■ View assets.■ View standards.

Table 3-13 Exception roles

Role	Description
Exception Approver	<p>The Exception Approver role lets the user do the following:</p> <ul style="list-style-type: none">■ Approve exceptions.■ Manage tags. <p>Note: The exception approver must have the required tasks and permissions to view assets.</p>
Exception Requestor	<p>The Exception Requestor role lets the user do the following:</p> <ul style="list-style-type: none">■ Request exceptions on behalf of a user without an assigned CCS role.■ Manage tags. <p>Note: The exception requestor must have the required tasks and permissions to add assets, standards, and entitlements.</p>

Table 3-14 Entitlements roles

Role	Description
Entitlements Administrator	<p>The Entitlements Administrator role lets the user do the following:</p> <ul style="list-style-type: none"> ■ Manage the control points. ■ Assign the data owners and the alternate data owners to the control points . ■ Import entitlements. ■ Manage control points. ■ Manage users. ■ Manage review cycles. ■ Manage jobs. ■ Manage tags. ■ Manage tiered dashboards. ■ Manage users. ■ Request entitlements approval. ■ Request exceptions. ■ Generate reports and dashboards. ■ Customize report templates. ■ Manage configuration settings. ■ Update and view notification templates. ■ View assets and asset reconciliation rules. ■ View review cycles. ■ View control points. ■ View dashboards and dashboard templates. ■ View reports and report templates. ■ View evaluation results. ■ View roles and permissions. ■ View tiered dashboards.
Entitlements Data Owner	<p>The Entitlements Data Owner role lets the user do the following:</p> <ul style="list-style-type: none"> ■ Request exceptions. ■ Manage entitlements. ■ Assign the alternate data owner to the control points. ■ View roles.

Table 3-15 Policy roles

Role	Description
Policy Administrator	<p>The Policy Administrator role lets the user do the following:</p> <ul style="list-style-type: none">■ Manage policies.■ Manage jobs.■ Manage tags.■ Manage policy comments.■ Manage policy clarifications.■ Manage policy content.■ Manage tiered dashboard■ Request exceptions.■ Publish policies.■ Manage configuration settings.■ Customize report templates.■ Generate reports and dashboards.■ View assets.■ View standards.■ View policies, policy comments, and policy content.■ View dashboards and dashboard templates.■ View reports and report templates.■ View roles and permissions.■ View tiered dashboard
Policy Approver	<p>The Policy Approver role lets the user do the following:</p> <ul style="list-style-type: none">■ Approve policies.■ Manage policy comments.■ View asset and asset group details.■ View policy and policy content details.■ View roles.
Policy Reviewer	<p>The Policy Reviewer role lets the user do the following:</p> <ul style="list-style-type: none">■ Manage policy comments.■ Review policies.■ View asset and asset group details.■ View policy, policy comments, and policy content details.■ View roles.

Table 3-16 Reports and dashboards roles

Role	Description
Reporting Administrator	<p>The Reporting Administrator role lets the user do the following:</p> <ul style="list-style-type: none">■ Generate reports and dashboards.■ Customize report templates.■ View dashboards and dashboard templates.■ View reports and report templates.■ Manage dashboards■ Manage jobs.■ Assign permissions to folders.■ Manage tags.■ Request exceptions.■ Manage configuration settings.■ View assets and asset reconciliation rules.■ View standards.■ View review cycles.■ View baselines.■ View evaluation results.■ View roles and permissions.■ View tiered dashboards
Report Result Viewer	<p>The Report Result Viewer role lets the user do the following:</p> <ul style="list-style-type: none">■ View all jobs.■ View the report templates and dashboard templates.■ View reports and dashboards.■ View tiered dashboards.

See [“About roles”](#) on page 78.

About custom roles

Control Compliance Suite (CCS) comes with a number of predefined roles that typically suit most organizations. CCS also provides the ability to create custom roles if the predefined roles do not fit the needs of your organization. However, the custom roles can only be created using a combination of tasks that come built-in with CCS.

You can create new roles or base them on existing roles. Some caution is called for when you create custom roles, because of the dependency between tasks.

For example, you create a custom role to manage the roles. If you add only the Manage Roles task to the custom role, the user is not able to view the roles. To view the roles, you must also add the View Roles task.

Note: The Manage Roles task must be assigned only to users with the administrative privileges as this task implicitly gives permissions to all folders in the directory.

See [“Creating a custom role”](#) on page 92.

See [“Copying a role”](#) on page 93.

See [“Editing a custom role”](#) on page 93.

See [“Deleting a role”](#) on page 94.

About the Roles view

The **Roles** view lets you assign roles to users and create custom roles.

The **Roles** view contains the following panes:

Table pane	The table pane lists the predefined roles and the custom roles.
Details pane	The details pane lists the tasks that are associated to a role and the users who are assigned to a role.

You can do the following from the Roles view:

- Add user to a role.
See [“Adding users and groups to a role”](#) on page 89.
- Remove user from a role.
See [“Removing a user or a group from a role”](#) on page 90.
- Assign permissions to the directory folders.
See [“Assigning permissions from the Roles view”](#) on page 91.
- View the tasks that are associated to a role.
See [“Viewing tasks associated to a role”](#) on page 91.
- View the users assigned to a role.
See [“Viewing users assigned to a role”](#) on page 90.
- Create a custom role.
See [“Creating a custom role”](#) on page 92.
- Edit a custom role.
See [“Editing a custom role”](#) on page 93.

- Delete a custom role.
See [“Deleting a role”](#) on page 94.
- Copy a custom role.
See [“Copying a role”](#) on page 93.

About the Permission Management view

The **Permission Management** view lets you assign permissions to the directory folders and items. Once you assign a role to a user, the permissions must be assigned to the folders before the user can perform any tasks on the folder.

The **Permission Management** view contains the following panes:

Tree pane	The tree pane displays a hierarchical, folder-based structure of the folders that are stored in the CCS directory.
Table pane	The table pane lists any subfolders of the folder that is selected in the tree pane.
Details pane	The details pane lists the users who have permissions over the selected folder in the table pane.

You can do the following from the Permission Management view:

- Assign permissions.
See [“Assigning permissions from the Permission Management view”](#) on page 95.
- Remove permissions.
See [“Removing permissions”](#) on page 96.
- View users who have permissions on a folder.

Restrictions on collecting data from assets

To assign permissions to users over assets in the console gives users the logical permissions over the assets. To successfully perform a task on an asset the user must also have the physical permission over the asset in the network.

If a user has permission to collect data from an asset but does not have the credentials on the physical asset, the data collection task fails.

For example, if a user is assigned the Evaluator permission over a computer, but is not given the required credentials to query the computer to collect data, the user cannot run the evaluation.

Working with roles

Control Compliance Suite (CCS) provides a number of predefined roles that can be assigned to the CCS users.

A role is a collection of predefined tasks. The user may perform each task that is a specific action, such as Create a policy or Run an evaluation. The role determines what a user can see and perform in the Control Compliance Suite console.

See [“Adding users and groups to a role”](#) on page 89.

See [“Removing a user or a group from a role”](#) on page 90.

See [“Viewing users assigned to a role”](#) on page 90.

See [“Viewing tasks associated to a role”](#) on page 91.

See [“Assigning permissions from the Roles view”](#) on page 91.

See [“Creating a custom role”](#) on page 92.

See [“Copying a role”](#) on page 93.

See [“Editing a custom role”](#) on page 93.

See [“Deleting a role”](#) on page 94.

Adding users and groups to a role

You must add user and groups to roles in Control Compliance Suite. After you add a user to a role you must grant the user permissions to the folders or the objects in the folders. You must grant the permissions for the user to perform the tasks.

Permissions to the predefined folders are automatically granted when the user is added a role.

You can assign permissions from the **Roles** view or the **Permissions** view.

See [“Assigning permissions from the Roles view”](#) on page 91.

See [“Assigning permissions from the Permission Management view”](#) on page 95.

To add a user or a group to a role

- 1 Go to **Settings > Roles**.
- 2 In the **Roles** view, select the check box next to the role to which you want to add the users or groups.
- 3 Click **Add Users and Groups**.
- 4 In the **Select Users or Groups** dialog box, type the name of the user or group to add and click **OK**.

The new user is listed in the **Users and Groups** list for the role.

See [“Removing a user or a group from a role”](#) on page 90.

See [“Configuring roles and permissions ”](#) on page 78.

Removing a user or a group from a role

After a user is removed from a role, the user can no longer perform the tasks that are associated with the role. All the assigned permissions over the directory folders are also removed.

To remove a user or a group from a role

- 1 Go to **Settings > Roles**.
- 2 In the **Roles** view, select the check box next to the role that you want to remove.
- 3 Click **Remove Users and Groups**.
- 4 In the **Remove Trustees** dialog box, select the user that you want to remove.
- 5 Click **Remove**.
- 6 Click **OK**.

See [“Adding users and groups to a role”](#) on page 89.

See [“Configuring roles and permissions ”](#) on page 78.

Viewing users assigned to a role

User with the Administrator role can assign users and groups to a role. Each role can have any number of users assigned to it.

To view users and groups assigned to a role

- 1 Go to **Settings > Roles**.
- 2 In the **Roles** view, do one of the following:
 - Select the role. The **Users and Groups** tab lists all the users who are assigned to the role.
 - Right-click the role and select **View Details**.
The **View Details - Settings** dialog box lists the users who are assigned to the role and the tasks that are associated with the role.

See [“Adding users and groups to a role”](#) on page 89.

See [“Configuring roles and permissions ”](#) on page 78.

See [“Viewing tasks associated to a role”](#) on page 91.

Viewing tasks associated to a role

Each role has a list of tasks that are associated to it. The tasks are predefined and cannot be modified.

To view tasks associated to a role

- 1 Go to **Settings > Roles**.
- 2 In the **Roles** view, do one of the following:
 - Select the role, the **Tasks** tab lists tasks that are associated to the role.
 - Right-click the role and select **View Details**.
The **View Details - Settings** dialog box lists the tasks that are associated with the role and the users who are assigned to the role.

See [“Adding users and groups to a role”](#) on page 89.

See [“Configuring roles and permissions ”](#) on page 78.

See [“Viewing users assigned to a role”](#) on page 90.

Assigning permissions from the Roles view

After you add a user or a group to a role you must grant permissions to folders and its objects. You cannot grant a user the permissions to a folder unless the user has been added to the appropriate role.

See [“Adding users and groups to a role”](#) on page 89.

When you assign permissions to a parent folder, the subfolders automatically inherit the parent folder permissions.

When you add a user to a role, the system automatically assigns permissions to any predefined folders.

Note: There may be time delay for permissions to propagate through the directory.

To assign permissions

- 1 Go to **Settings > Roles**.
- 2 In the **Roles** view, select the role.
- 3 In the **Users and Groups** tab, select the user or group.
- 4 Click **Assign Permissions**.
- 5 In the **Assign Permissions** panel, in the left pane, navigate to the required folder.

All the subfolders are listed in the right pane.

- 6 Do one of the following:
 - To add a folder that is listed in the right pane, select the folder and click **Add**.
 - To add all folders that are listed in the right pane, click **Add All**.You can use the search feature to quickly find the required folder.
- 7 The newly added folders are listed in the **Selected Items** list.
- 8 Click **Next**.
- 9 In the **Review Assigned Permissions** panel, confirm if the folder selection is accurate.
- 10 Click **Finish**.

See [“Assigning permissions from the Permission Management view”](#) on page 95.

See [“Configuring roles and permissions ”](#) on page 78.

Creating a custom role

You can create new roles or copy an existing role and make changes to suit your needs.

See [“Copying a role”](#) on page 93.

Note: The Manage Roles task must be assigned only to users with the administrative privileges as this task implicitly gives permissions to all folders in the directory.

To create a custom role

- 1 Go to **Settings > Roles** view.
- 2 In the **Roles** view, on the taskbar, click **Create Role**.
- 3 In the **Create or Edit Custom role wizard > Specify Custom Role details** panel, type the name of the role.
- 4 Type a brief description of the new role and then click **Next**.
- 5 In the **Specify tasks for custom role** panel, select the tasks for the new role. To select the tasks do the following:
 - From the roles list, select a role. The tasks for the selected role are listed in the tasks list.
 - From the tasks list, select the tasks. Click **Add** for each task you select or you can click **Add all** to select all tasks from the tasks list.

The **Selected Items** section lists all the tasks that you added from the tasks list.

- 6 Repeat step 5 to select tasks from a different role.
- 7 Click **Next**.
- 8 In the **Summary** panel, review the tasks that you have selected for the custom role and click **Back** to make changes.
- 9 Click **Finish** to close the wizard.

See [“Configuring roles and permissions”](#) on page 78.

Copying a role

You can copy a predefined role or a custom role to create a new role. You can make the required changes to the name and description.

To modify the tasks that are associated with a custom role, you must select **Edit Role** on the taskbar.

To copy a role

- 1 Go to **Settings > Roles**.
- 2 In the **Roles** view, select the role that you want to copy.
- 3 On the taskbar, click **Copy Role**.
- 4 In the **Copy Role View** dialog box, type a unique name for the new role.
- 5 Change the description of the role.
- 6 Click **OK** to save.

See [“Configuring roles and permissions”](#) on page 78.

See [“Creating a custom role”](#) on page 92.

Editing a custom role

You can edit the name, the description, and the tasks that are associated with the role.

When you modify the tasks in a role, the system automatically updates the permissions on the directory folders and objects for the user with the role.

Note: The Manage Roles task must be assigned only to users with the administrative privileges as this task implicitly gives permissions to all folders in the directory.

To edit a custom role

- 1 Go to **Settings > Roles**.
- 2 In the **Roles** view, select the role that you want to edit.
- 3 On the taskbar, click **Edit Role**.
- 4 In the **Create or Edit Custom Role wizard > Specify Custom Role details** panel, change the name and description of the role if required.
- 5 Click **Next**.
- 6 In the **Specify Tasks for Custom Role** panel, add or remove the tasks for the role.
- 7 To add tasks, do the following:
 - From the roles list, select a role. The tasks for selected role are listed in the tasks list.
 - From the tasks list, select the tasks. Click **Add** for each task that you select or you can click **Add all** to select all tasks from the tasks list.
- 8 Repeat step 6 to select tasks from a different role.
- 9 To remove tasks, in the **Selected Tasks** list, select the task to remove, click **Remove** or you can click **Remove All** to remove all tasks.
- 10 Click **Next**.
- 11 In the **Summary** panel, review the tasks that you have selected for the role.
- 12 Click **Back** to make changes or click **Finish** to close the wizard.

See [“Creating a custom role”](#) on page 92.

Deleting a role

You can only delete custom roles.

When you delete a role, the system automatically updates the permissions on the directory folders and objects for the users with the role.

To delete roles

- 1 Go to **Settings > Roles**.
- 2 In the **Roles** view, select the check boxes next to the roles you want to delete.
- 3 On the taskbar, click **Delete Roles**.

See [“Creating a custom role”](#) on page 92.

Working with permissions

Control Compliance Suite lets you control which users have what access to which directory objects. When a user account is authenticated, the type of access that is granted to the objects is determined by the permissions that are attached to the object.

When a role is assigned to a user, permissions are automatically granted to the directory objects in the predefined folders. The administrator must manually assign permissions to the user-defined folders.

See [“Assigning permissions from the Permission Management view”](#) on page 95.

See [“Removing permissions”](#) on page 96.

Assigning permissions from the Permission Management view

After you add a user or group to a role in the Roles view, you must grant permissions to folders to perform tasks. You cannot grant a user the permissions to a folder unless the user has been added to the appropriate role.

See [“Adding users and groups to a role”](#) on page 89.

When you add a user to a role, the system automatically assigns permissions to any predefined folders.

When you assign permissions to a parent folder, the subfolders automatically inherit the parent folder permissions.

Note: There may be time delay for permissions to propagate through the directory.

To assign permission

- 1 Go to **Settings > Permission Management**.
- 2 In the **Permission Management** view, in the tree pane, navigate to the required folder.
- 3 In the table pane, select the folder to assign the permissions.
- 4 In the **User and Groups** tab, click **Assign Permissions**.
- 5 In the **Assign Permissions** dialog box, click **Add**.
- 6 In the **Select Users/Groups** dialog box, select the role name and click **OK**.
The newly added user is listed in the **Assign Permissions** dialog box.
- 7 To add more users or groups, go to step 5.

- 8 Click **OK**.
- 9 Click the **refresh** icon on the details pane to list all the newly assigned users.
See [“Assigning permissions from the Roles view”](#) on page 91.
See [“Configuring roles and permissions ”](#) on page 78.

Removing permissions

You can remove permissions that are assigned to a user over a directory folder.

To remove permission

- 1 Go to **Settings > Permission Management**.
- 2 In the **Permission Management** view, in the tree pane, navigate to the required folder.
- 3 In the table pane, select the folder.
- 4 In the **Users and Group** tab, select the user or group.
- 5 Click **Remove Permissions**.
- 6 In the **Remove Permission View** dialog box, select the role name and click **Remove**.
- 7 Click **Update** to confirm the removal of permission.

See [“Assigning permissions from the Permission Management view”](#) on page 95.

See [“Assigning permissions from the Roles view”](#) on page 91.

See [“Configuring roles and permissions ”](#) on page 78.

Registering and configuring the Data Processing Service

After you install a Data Processing Service (DPS) instance, you must register it. Until you register it, the Application Server cannot contact the DPS. When you register the DPS, you import a copy of the certificate that is associated with the DPS and store it. You can also configure the DPS to fit your environment when you register the DPS.

Changes to the DPS Settings can help to optimize the performance of the Control Compliance Suite (CCS). Changes to the settings that you make in error can make it impossible to collect data from the data collectors on your network. Changes to the settings can also harm the performance of CCS.

The settings lets you change how the DPS Collector interacts with the following:

- RMS data collector Information Server
- ESM data collector managers
- Data that another tool collects and stores in a file (CSV files)

For each DPS, you can configure the following:

- DPS roles
- Site assignment

You can also change the data collector settings for any DPS assigned to the DPS Collector role.

See [“Configuring the data collectors”](#) on page 116.

See [“Configuring the Windows data collector”](#) on page 117.

See [“Configuring the Oracle data collector”](#) on page 118.

See [“Configuring the SQL data collector”](#) on page 119.

See [“Configuring the UNIX data collector”](#) on page 119.

See [“Configuring the CSV data collector”](#) on page 129.

See [“Configuring the assets batch size”](#) on page 155.

See [“About the Control Compliance Suite Data Processing Service”](#) on page 34.

About Data Processing Service roles

The Data Processing Service (DPS) must be assigned one or more roles within the Control Compliance Suite (CCS). The assigned role or roles control what tasks the DPS performs in your CCS deployment. Any DPS can be assigned to multiple roles, but more often a DPS plays a single role.

A DPS can be assigned to one or more of the following roles:

- DPS Load Balancer
 See [“About the Data Processing Service Load Balancer”](#) on page 34.
- DPS Collector
 See [“About the Data Processing Service Collector”](#) on page 36.
- DPS Evaluator
 See [“About the Data Processing Service Evaluator”](#) on page 37.
- DPS Reporter
 See [“About the Data Processing Service Reporter”](#) on page 35.

For information on how to choose which DPS computers to assign to which roles, see the *Symantec Control Compliance Suite Planning and Deployment Guide*.

Registering the Data Processing Service

Before the Application Server can use a newly installed Data Processing Service (DPS), you must register the DPS with the Application Server. When you register a DPS, the Directory Server verifies a copy of the certificate that is assigned to the DPS host. The certificate is then used to secure communications with the DPS. When you register the DPS, you can also configure the DPS settings.

The DPS icon in the **Map View** and **Grid View** does not reflect the updated DPS status until you refresh the view.

Note: Assign the first DPS that you register to the Load Balancer role.

To register the Data Processing Service

- 1 In the **System Topology > Map View** or **System Topology > Grid View**, click **Register DPS**.
- 2 In the **Data Processing Service Selection** panel, select one or more DPS hosts to register and click **Next**.
- 3 In the **Site Selection** panel, select the site to which the DPS hosts should be assigned. You can use an existing site or create a new site. To create a new site, click **Create Site** and enter a site name and click **Next**.
- 4 In the **Role Selection** panel, select the roles to which the DPS should be assigned. You must assign the DPS to at least one role.

You can also change the port the DPS uses to communicate with the Application Server. The default port is 3993. Click **Next**.
- 5 In the **Confirm or change the DPS to Use for Synchronizing the Reporting Database** panel, select the DPS that should perform synchronization of the reporting database, then click **Next**.
- 6 If you selected the DPS Collector role, in the **Data Collector Selection** panel, select the data collectors that the DPS should use, then click **Next**.
- 7 In the **Summary** panel, click **Next**.
- 8 Do one of the following:
 - If you assigned a DPS to the DPS Collector role, in the **Finished** panel, click **Advanced Settings for registered components**.
 - If you did not assign a DPS to the DPS Collector role and need to register another DPS, in the **Finished** panel, click **Register another DPS**.
 - If you did not assign a DPS to the DPS Collector role, in the **Finished** panel, click **Close**.

- 9 If you clicked **Advanced Settings for registered components**, in the **Categories** area of the **Component Settings** dialog box, configure any DPS Collectors to collect data.
- 10 Click the name of the setting to configure.
 Enter any information that is required on the panel.
 See [“Configuring the Windows data collector”](#) on page 117.
 See [“Configuring the Oracle data collector”](#) on page 118.
 See [“Configuring the SQL data collector”](#) on page 119.
 See [“Configuring the UNIX data collector”](#) on page 119.
 See [“Configuring the CSV data collector”](#) on page 129.
 See [“Configuring basic Data Processing Service settings”](#) on page 100.
 See [“Configuring advanced Data Processing Service settings”](#) on page 100.
- 11 In the **Component Settings** dialog box, click **OK** to close the dialog box and save the changes.
- 12 In the **Finished** panel, click **Close**.

Unregistering a Data Processing Service

If needed, you can unregister a Data Processing Service (DPS) instance. When you do so, you remove the DPS from the list of Data Processing Services that the Application Server contacts. Before you unregister a DPS, make sure that another DPS is assigned to take over the duties of the unregistered DPS.

To unregister a Data Processing Service

- 1 In the **System Topology > Map View** or **System Topology > Grid View**, click **Unregister DPS**.
- 2 In the **Data Processing Service Selection** panel, select one or more DPS hosts to unregister, then click **Next**.
- 3 In the **Summary** panel, click **I understand the above DPS and associated data collector configurations will be removed permanently and I understand this action is irrevocable**, and then click **Next**.
- 4 In the **Finish** panel, click **Close**.

Configuring basic Data Processing Service settings

You can configure the Data Processing Service (DPS) settings when you register the DPS. You can also configure the DPS settings at a later time. You use one of the system topology views to select the DPS to configure.

When you configure the DPS settings, the panels that appear vary depending on the components that are deployed on the host system. In addition, the DPS settings determine what information appears. For example, options to enable data sources only appear if the DPS is assigned to the DPS Collector role.

If you modify more than one DPS at a time, only the common setting tabs and fields appear. Select each DPS individually to view all settings that apply to the DPS.

Note: If you make a change to the basic Data Processing Service settings, the changes do not appear immediately. You must close and reopen the **Component settings** dialog box before the new options appear.

See [“Configuring the data collectors”](#) on page 116.

See [“About the Control Compliance Suite Data Processing Service”](#) on page 34.

To configure the basic Data Processing Service settings

- 1 Go to the **System Topology > Grid View** or **System Topology > Map View**.
- 2 In the **System Topology > Grid View** or the **System Topology > Map View**, right-click the Data Processing Service component and click **Edit Settings**.
- 3 In the **Data Processing Service** area of the **Component settings** dialog box, click **Basic**.
- 4 On the **DPS - Basic** panel, click the roles to assign the DPS to.
- 5 If the DPS is assigned to the DPS Collector role, select the data collectors to enable on the DPS.
- 6 Click **OK** to save the changes and close the dialog box.

Configuring advanced Data Processing Service settings

You can change the advanced Data Processing Service (DPS) settings.

You can configure the Data Processing Service settings when you register the DPS. You can also make changes to the settings of an existing DPS from the **System Topology > Map View** or **System Topology > Grid View** views.

If you modify more than one DPS at a time, only the common setting tabs and fields appear. Select each DPS individually to view all settings that apply to the DPS.

See “[Registering the Data Processing Service](#)” on page 98.

See “[Configuring the data collectors](#)” on page 116.

See “[About the Control Compliance Suite Data Processing Service](#)” on page 34.

Warning: When you change the advanced settings, you can render the Data Processing Service invisible to other components. You can also harm the speed of data collection and job processing on the DPS. Only change these settings when asked to do so by Symantec Technical Support.

The Advanced settings include the following:

- TCP/IP port settings
- Session Manager settings
- Scheduler settings

You can change the following TCP/IP port setting:

Port	The TCP/IP Port other components use to communicate with the DPS.
------	---

You can change the following settings that the Data Processing Service uses internally to define how the Session Manager behaves:

Command Threads	The minimum number and maximum number of processor threads available for the Session Manager. This thread pool is used to collect job results and perform other maintenance tasks. These settings are appropriate for most installations. If a very high performance computer hosts the Data Processing Service, more available threads may improve performance.
Job Poll Interval	The time, in seconds, the Data Processing Service waits between attempts to collect job results.

You can change the following settings the Data Processing Service uses internally to define how the Scheduler behaves:

Command Threads	The minimum number and maximum number of processor threads available for the Data Processing Service Scheduler. If a very high performance computer hosts the Data Processing Service, more available threads may improve performance.
-----------------	--

- | | |
|----------------|---|
| Submit Threads | The minimum number and maximum number of processor threads available for the scheduler Job Submission thread pool. This thread handles newly submitted jobs. |
| Resume Threads | The minimum number and maximum number of processor threads available for the scheduler Job Resumption thread pool. This thread handles any jobs that were submitted, transferred to the scheduler, and later resumed. |

To configure the advanced Data Processing Service settings

- 1 Go to the **System Topology > Grid View** or **System Topology > Map View**.
- 2 In the **System Topology > Grid View** or the **System Topology > Map View**, right-click the Data Processing Service component and click **Edit Settings**.
- 3 In the **Data Processing Service** area of the **Component Settings** dialog box, click **Advanced**.
- 4 On the DPS - Advanced panel, make any required changes to the advanced settings.
- 5 Click **OK** to save the changes and close the dialog box.

Assigning a role to a Data Processing Service

Each instance of the Data Processing Service (DPS) is assigned to one or more roles. A role controls what tasks the DPS performs.

You can assign a DPS to one or more of the following roles:

- DPS Load Balancer
- DPS Collector
- DPS Evaluator
- DPS Reporter

DPS Collectors list the enabled data collectors. Only enabled data collectors have configuration tabs available. If you make changes to the selected data collectors, you must close and reopen the dialog for the changes to take effect.

For information on how to choose which DPS computers to assign to which roles, see the *Symantec Control Compliance Suite Planning and Deployment Guide*.

See [“About the Control Compliance Suite Data Processing Service”](#) on page 34.

To assign a role to a Data Processing Service

- 1 Go to the **System Topology > Grid View** or **System Topology > Map View**.
- 2 In the **System Topology > Grid View** or the **System Topology > Map View**, right-click the Data Processing Service component and click **Edit Settings**.
- 3 In the **Data Processing Service** area of the **Component Settings** dialog box, click **Basic**.
- 4 On the **DPS - Basic** panel, click the roles the DPS should be assigned to.
- 5 Click **OK**.

Synchronizing Data Processing Service settings

The Application Server periodically synchronizes settings on all registered Data Processing Service hosts. You can also synchronize settings manually if needed.

To manually synchronize settings

- ◆ Do one of the following:
 - In the **System Topology > Map View**, click **Infrastructure Tasks > Sync Configuration**.
 - In the **System Topology > Grid View**, click **Sync Configuration**.

Working in the System Topology view

The System Topology view contains the Map view and the Grid view. Both views read data from the Control Compliance Suite Directory. The Map view displays a graphical representation of all the deployed infrastructure components. The Grid view displays the same information in a tabular format. Using both the views you can inspect and query the various deployed components.

See [“About the Map view”](#) on page 103.

See [“About the Grid view”](#) on page 106.

See [“About navigating in the Map view”](#) on page 105.

See [“About the Map view icons”](#) on page 105.

About the Map view

The **Map** view reads data from the Control Compliance Suite (CCS) Directory and displays a graphical representation of all deployed components. When you navigate to the view, a map is drawn with a balanced spacing between all the components.

You can use the mouse to move the components around the view to draw a different layout.

The **Map** view displays the association between the application server and all the load balancers. The load balancers show their association with the other data processing servers that are assigned to various sites.

When you exit from the **Map** view, the configuration layout is automatically saved. The next time you navigate to the **Map** view, the saved configuration layout is displayed. If a component is deleted or added, the **Map** view reconciles any differences with the CCS Directory and dynamically displays the updated configuration.

You can do the following from the **Map** view:

- Register and unregister DPS.
See “[Registering the Data Processing Service](#)” on page 98.
See “[Unregistering a Data Processing Service](#)” on page 99.
- Sync configuration.
See “[Synchronizing Data Processing Service settings](#)” on page 103.
- Modify or view the settings of each component.
See “[Modifying the settings of a component](#)” on page 107.
- Create sites.
See “[Creating a site](#)” on page 113.
- View health and status information.
- Monitor system jobs.
See “[Monitoring infrastructure jobs](#)” on page 110.
- Create and delete annotations.
See “[Adding annotations to the components](#)” on page 108.
- Save an image of the components layout.
See “[Saving an image of the configuration layout](#)” on page 108.
- Zoom in and zoom out of the layout.
- Display a balanced view of the components layout.
- Modify the layout of the components.
See “[About navigating in the Map view](#)” on page 105.
See “[About the Map view icons](#)” on page 105.
See “[About the Grid view](#)” on page 106.

About navigating in the Map view

The Map view provides the following features to adjust the layout and view of the components:

Zoom in and zoom out	You can use the zoom icons to zoom in or zoom out of the component layout.
Fit in Window	The Fit in Window feature redraws the map with a balanced spacing between all the components and zooms out so that the whole map is visible.
Move	You can manually move a specific component or multiple components in the view area. To move a specific component, you click the component and drag and drop it to the new location. To move multiple components, you click in an empty area on the view. Hold down the left mouse key and drag the mouse until the frame is around the objects to be moved. All the component icons are highlighted inside the frame. You click on any of the highlighted icons and drag the icon to the new location.
Reset	If the layout of all the components is not well balanced, clicking Auto Layout redraws the map.
Refresh	<p>You can refresh the Map view to display any changes to the component configurations since the view was selected.</p> <p>After a Data Processing Service is registered, the DPS status in the Map view and the Grid view does not reflect the updated status until you refresh the view.</p> <p>You can also view the status of the current configuration jobs that are running from the Infrastructure Job Monitor dialog box..</p> <p>See “Monitoring infrastructure jobs” on page 110.</p>

See [“About the Map view”](#) on page 103.

About the Map view icons

The Map view icons help visually to identify the different roles of the Data Processing Service (DPS) and the health status of the components.

The following table displays the DPS role icons:



DPS Load Balancer

The DPS with a blue icon depicts a DPS Load Balancer.

When the DPS acts as a load balancer, the DPS routes data collection jobs from the application server to a DPS Collector. In addition, a load balancer routes the evaluation jobs to the DPS Evaluator and the reporting jobs to the DPS Reporter.



DPS Collector

The DPS with a green icon depicts a DPS Collector.

The DPS Collector is the interface to the programs that do the actual work of collecting data from the network.



DPS Evaluator

The DPS with a red icon depicts a DPS Evaluator.

Evaluation jobs are sent from the application server to one of the Data Processing Service (DPS) Load Balancers. The DPS Load Balancer then sends the evaluation job to the DPS Evaluator. The evaluator compares the data to the specifications in the Standards that you select and then stores the evaluation results in the production database.



DPS Reporter

The DPS with a yellow icon depicts a DPS Reporter.

The Data Processing Service (DPS) Reporter generates reports and dashboards for display by the Control Compliance Suite Console. In addition, a single DPS Reporter is assigned to perform database synchronization between the production database and the reporting database test.

After a Data Processing Service is registered, the DPS status in the Map view and the Grid view does not reflect the updated status until you refresh the view.

You can also view the status of the current configuration jobs that are running from the **Infrastructure Job Monitor** dialog box..

See [“Monitoring infrastructure jobs”](#) on page 110.

See [“About the Control Compliance Suite Data Processing Service”](#) on page 34.

About the Grid view

The **Grid** view reads data from the Control Compliance Suite Directory and displays a tabular representation of all deployed components. The information that is displayed in the **Map** view and the grid view is the same except for the format that displays the information.

You can do the following from the **Grid** view:

- Register and unregister DPS.
See [“Registering the Data Processing Service”](#) on page 98.

See “ [Unregistering a Data Processing Service](#) ” on page 99.

- Sync configuration.
See “ [Synchronizing Data Processing Service settings](#) ” on page 103.
- Modify or view the settings of each component.
See “[Modifying the settings of a component](#) ” on page 107.
- Create site.
See “[Creating a site](#)” on page 113.
- Monitor system jobs
See “[Monitoring infrastructure jobs](#)” on page 110.
- Select the columns to be displayed in the grid.
- Sort the grid.

See “[About the Map view](#)” on page 103.

Modifying the settings of a component

You can modify the component settings from the Map view or from the Grid view.

To modify the settings of a component from the Map view

- 1 Go to **Settings > System Topology**.
- 2 In the **Map** view, right-click the component to modify the settings.
- 3 Click **Edit Settings**.
- 4 In the **Edit Settings** dialog box, modify the required properties.
- 5 Click **OK** to save.

To modify the settings of a component from the Grid view

- 1 Go to **Settings> System Topology**.
- 2 In the **Grid** view, right-click the component in the grid.
- 3 Click **Edit Settings**.
- 4 In the **Edit Settings** dialog box, modify the required properties.
- 5 Click **OK** to save.

See “[About the Map view](#)” on page 103.

See “[About the Grid view](#)” on page 106.

Viewing additional component information

You can view additional information about a component from the Map view.

The additional information window displays the details of the component and the health and status of the component.

To view additional information of a component

- 1 Go to **Settings > System Topology > Map view**.
- 2 In the Map view, do one of the following:
 - Right-click the component.
 - Pause the mouse over the component. You can view information of the selected component in the balloon window that appears.

See [“Modifying the settings of a component ”](#) on page 107.

Saving an image of the configuration layout

You can save the image of the **Map** view layout and print it for later use.

To save an image of the configuration layout

- 1 Go to **Settings > System Topology**.
- 2 In the **Map** view, click **Save Image**.
- 3 In the **Save as** dialog box, navigate to the location to save the image file.
- 4 Modify the name of the file, and click **Save**.

See [“About the Map view”](#) on page 103.

Adding annotations to the components

You can add an annotation to the link that connects two components in the **Map** view. You can add comments, notes, or any text that is relevant to the linked components.

To add an annotation

- 1 Go to **Settings > System Topology**.
- 2 In the **Map** view, right-click the blue link between the two components and select **Annotate**.
- 3 In the text box, type the notes.
- 4 Click outside the text box to save.

If required, you can move the text box to a location in the view.

See [“Deleting annotations”](#) on page 109.

See [“Deleting the association between components”](#) on page 109.

Deleting annotations

You can delete the annotations that are added to the components.

To delete an annotation

- 1 Go to **Settings > System Topology**.
- 2 In the **Map** view, right-click the annotation text and select **Delete Label**.

See [“Adding annotations to the components”](#) on page 108.

See [“Deleting the association between components”](#) on page 109.

Deleting the association between components

You can delete the link between two components in the Map view.

To delete the link between components

- 1 Go to **Settings > System Topology**.
- 2 In the **Map** view, right-click the link between the two components select **Delete Link**.

See [“Deleting annotations”](#) on page 109.

See [“Adding annotations to the components”](#) on page 108.

Viewing the health and the status information

The health information and status information lets users view the current state and configuration details of the infrastructure. The information can also be used to detect and diagnose issues

The following health and status information is available:

- Communication settings
- Application server settings
- CCS directory Settings
- Data Processing Service settings
- Infrastructure logs

The following are the different health status icons that are displayed in the top left corner of the various infrastructure components in the Map view:

Green check circle Indicates a healthy status.

Yellow warning triangle Indicates that the component needs attention.

Red stop sign	Indicates that the component has failed the health status check.
Pink question mark	Indicates that system cannot get a status on the component.

To view health and status of a component

- 1 Go to Settings > System Topology > Map view.
- 2 In the Map view, pause the mouse over the component.
You can view information of the selected component in the balloon window that appears.
- 3 Click on the (+) plus icon in the status section to view complete health information.

Refreshing the health and the status information

The scheduled health and status information is posted every 24 hrs at midnight. You can manually refresh the Map view at anytime to see the latest health information of a component.

To refresh the health and status information

- ◆ Do one of the following:
 - In the **Settings > System Topology > Map view**, on the taskbar, click **Infrastructure Tasks > Refresh Health Status**.
 - In the **Settings > System Topology > Grid view**, on the taskbar, click **Refresh Health Status**.

See [“Refreshing the health and the status information”](#) on page 110.

See [“About the Map view”](#) on page 103.

See [“About the Grid view”](#) on page 106.

Monitoring infrastructure jobs

You can monitor the status of any system configuration jobs that are currently running.

To monitor the infrastructure jobs

- 1 Do one of the following:
 - In the **Settings > System Topology > Map view**, on the taskbar, click **Infrastructure Tasks > Monitor System Jobs**.
 - In the **Settings > System Topology > Grid view**, on the taskbar, click **Monitor System Jobs**.

The **Infrastructure Job Monitor** dialog box displays any jobs that are running.

- 2 You can choose to refresh the **Map** view when the job completes. You can also modify the time interval to refresh the **Map** view when the job completes.

See [“About the Map view”](#) on page 103.

See [“About the Grid view”](#) on page 106.

Configuring sites

A site is a logical grouping of assets and servers. Sites are organizational tools. Sites help you configure how data is collected and which DPS Collector performs the collection.

Each asset is assigned to a single site.

All instances of the Data Processing Service (DPS) are assigned to one or more sites. Every site must have at least one DPS Collector assigned.

Data is collected from the assets that are assigned to a site by the DPS Collectors that are also assigned to the site. Any DPS Collector can be assigned to more than one site.

Multiple, identically configured DPS Collectors can be assigned to a single site. When multiple DPS Collectors are assigned to a site, the DPS Load Balancers assign jobs in a round robin fashion. An asset is assigned to a single site.

A site can represent a physical location that is separated from the remainder of your Control Compliance Suite deployment by slow network links. A site can also represent a logical subdivision of a single location such as a single department, a single building, or a single floor.

See [“What sites can do for you”](#) on page 112.

See [“About using sites”](#) on page 112.

See [“About planning sites”](#) on page 113.

See [“Creating a site”](#) on page 113.

See [“Deleting a site”](#) on page 114.

See [“Assigning a Data Processing Service to a site”](#) on page 114.

See [“Removing a Data Processing Service from a site”](#) on page 115.

What sites can do for you

Sites let you group assets together with the Data Processing Services that handle the assets. Sites let you adapt Control Compliance Suite (CCS) data collection to your needs. You can use sites to represent physical groups of your assets.

Sites can represent a physical grouping of assets. When the deployment spans multiple locations and the locations have slow network links, sites help to optimize data collection. In this model, the site groups all assets at a single physical location with the DPS Collectors that retrieve data from the assets. The DPS Collectors collect data from the assets over local, high-speed network connections. Only communications with other CCS components cross the slow link to the remainder of the network. Further, communications between the collector and other components are designed to accommodate these slow links. Data is compressed before transmission and broken into chunks to facilitate the transmission.

As a variation, you can group the assets that share a single type of network access into a group. A site that groups assets by network speed can help to optimize data collection performance. For example, any assets that are accessible over a low-speed virtual private network (VPN) access can be grouped in a single site. This model isolates assets with slower data collection. In this model, the DPS Collector that collects data from the remote access site is hosted in the same location as the VPN router.

You can also subdivide assets at a single location into multiple sites that are based on their physical location. At a campus with multiple buildings, you can group all assets from a single building into a site. You can also group all assets from a portion of a building into a single site.

Sites can also represent a logical grouping of assets. For example, you can assign all assets in a single department or a small group of departments to a site.

Finally, sites can be used to group DPS Load Balancers, Evaluators, and Reporters. A site without a DPS Collector cannot include any assets. This type of phantom site can be useful when you plan and document the CCS deployment.

About using sites

All assets and all Data Processing Service (DPS) instances are assigned to a site. Assets are always assigned to a single site. A DPS must be assigned to a site and can be assigned to more than one site. If a site has assets assigned, the site must have at least one DPS Collector assigned to collect data from the assets. You use the Control Compliance Suite (CCS) console to create, assign, and manage sites. Only users with appropriate privileges can make changes to sites.

All CCS deployments must include at least a single site. A default site is created when you install CCS. You can create as many additional sites as you need. You can also rename or delete any site except the default site.

Note: If a DPS is removed from a site, it cannot collect data from the assets you assigned to that site.

About planning sites

Sites benefit from careful plans. Before you begin your Control Compliance Suite (CCS) deployment, you should evaluate your network and consider the best way to divide it into sites.

You begin with a diagram of your network. Your diagram should include a note of the speed of the links that connect parts of your network. This analysis suggests how your assets should be divided into sites.

Site planning is integrated into the deployment planning process. You must consider your site plans in light of your comprehensive deployment plans.

Creating a site

You create a site to organize a group of assets.

By default, all the Data Processing Services are assigned to the Default site.

See [“About the Control Compliance Suite Data Processing Service”](#) on page 34.

To create a site from the Map view

- 1 Go to **Settings > System Topology**.
- 2 In the **Map** view, right-click on an empty area of the map.
- 3 Click **Create Site**.
- 4 In the **Create Site** dialog box, type the name of the site.
- 5 Click **OK**.

To create a site from the Grid view

- 1 Go to **Settings > System Topology**.
- 2 In the **Grid** view, on the taskbar, click **Create Site**.
- 3 In the **Create Site** dialog box, type the name of the site.
- 4 Click **OK**.

See [“What sites can do for you”](#) on page 112.

See [“About using sites”](#) on page 112.

See [“Deleting a site”](#) on page 114.

See [“Modifying the site name”](#) on page 115.

Deleting a site

You must first remove any Data Processing Service that is assigned to the site before you delete the site.

See [“Removing a Data Processing Service from a site”](#) on page 115.

You must also reassign the assets that are assigned to the site. You can manually assign the assets one at a time or you can use the reconciliation rule.

Do the following to reassign the assets:

- Create an Update reconciliation rule.
See [“Creating reconciliation rules”](#) on page 253.
- Reimport the assets.
See [“Importing assets”](#) on page 260.

To delete a site from the Map view

- 1 Go to **Settings > System Topology**.
- 2 In the **Map** view, right-click on the site name.
- 3 Click **Delete site**.

See [“Creating a site”](#) on page 113.

See [“Modifying the site name”](#) on page 115.

See [“About using sites”](#) on page 112.

Assigning a Data Processing Service to a site

You assign a Data Processing Service (DPS) that is responsible for load balancing, data collection, evaluation, and reporting from the assets in the site. A DPS can be assigned to multiple sites. By default all DPS are assigned to the Default Site.

If a DPS is removed from a site, the DPS cannot collect data from the assets that are assigned to that site.

To assign a DPS to a site from the Map view

- 1 Go to **Settings > System Topology**.
- 2 In the **Map** view, right-click the DPS to assign.
- 3 Click **Assign to site**, and then select the name of the site.

To assign a DPS to a site from the Grid view

- 1 Go to **Settings > System Topology**.
- 2 In the **Grid** view, click **by Sites**.
- 3 Right-click the DPS to assign.
- 4 Click **Assign to site** and then select the name of the site.
- 5 Click .

See [“About the Control Compliance Suite Data Processing Service”](#) on page 34.

See [“Creating a site”](#) on page 113.

See [“About using sites”](#) on page 112.

Removing a Data Processing Service from a site

Whenever a Data Processing Service (DPS) is removed from a site the DPS is automatically added to its last default site.

If a DPS is removed from a site, the DPS cannot collect data from the assets that are assigned to that site.

To remove a DPS from a site in the Map view

- 1 Go to **Settings > System Topology**.
- 2 In the **Map** view, right-click the DPS in the site from which you want it removed.
- 3 Click **Remove from site**, and then select the name of the site.

To remove a DPS from a site in the Grid view

- 1 Go to **Settings > System Topology**.
- 2 In the **Grid** view, click **by Sites**.
- 3 Right-click the DPS in the site from which you want it removed.
- 4 Click **Remove from site**.

See [“Assigning a Data Processing Service to a site”](#) on page 114.

See [“About the Control Compliance Suite Data Processing Service”](#) on page 34.

See [“About using sites”](#) on page 112.

Modifying the site name

You can modify the site name at anytime.

The site name can contain a maximum of 256 characters.

To modify the name of a site

- 1 Go to Settings > System Topology.
- 2 In the Map view, click on the site name to modify the name.
- 3 In the text box, modify the name of the site.
- 4 Click anywhere outside the text box to save.

See [“Creating a site”](#) on page 113.

See [“Deleting a site”](#) on page 114.

See [“About using sites”](#) on page 112.

Configuring the data collectors

In Control Compliance Suite, the Data Processing Service (DPS) component is configured as a data collector. The DPS in the role of a data collector collects data from the data collection components such as RMS, ESM, and CSV files.

The RMS data collection component comprises the RMS Console and Information Server into which snap-in modules of predefined platforms are registered. The snap-in modules are equipped to collect data from the computers that are installed with any of the predefined platforms. RMS Console and Information Server supports data collection from the computers that are installed with the predefined platforms such as Windows, UNIX, SQL, and Oracle. In Control Compliance Suite, for every predefined platform a predefined data collector is defined. The data collector routes the Control Compliance Suite data collection query through the Information Server and collects the data that is queried and gathered by the snap-in module. The collected data is routed through the data collector to the Control Compliance Suite infrastructure.

The ESM data collection component comprises the ESM Manager and the agent.

The ESM Manager does the following:

- Controls and stores policy data and passes the data to the agents or to the console.
- Gathers and stores security data from the agents and passes the data to the console.

The manager uses the control information files (CIF) server to communicate with the agents and the ESM Console. The control information files (CIF) server is the primary component of the manager and is an important part of the ESM information exchange process. Control Compliance Suite defines an ESM data collector that routes the query through the ESM Manager to collect data from the

agents. The collected data is routed through the ESM data collector to the Control Compliance Suite infrastructure.

Table 3-17 Predefined platforms and the corresponding data collectors

Platform	Data collector
ESM	ESM data collector
Oracle	Oracle data collector
SQL	SQL data collector
UNIX	UNIX data collector
Windows	Windows data collector
CSV	CSV data collector

See “[Configuring the Oracle data collector](#)” on page 118.

See “[Configuring the SQL data collector](#)” on page 119.

See “[Configuring the UNIX data collector](#)” on page 119.

See “[Configuring the Windows data collector](#)” on page 117.

See “[Configuring the CSV data collector](#)” on page 129.

Configuring the Windows data collector

The Control Compliance Suite can use Symantec Information Server to retrieve data from your enterprise network. The Information Server passes the collected data to the Data Processing Service (DPS) Collector. The collector then returns the collected data to the Control Compliance Suite infrastructure for further processing. The Information Server uses the bv-Control for Windows snap-in module to collect data from the Windows computers.

The Control Compliance Suite uses the Windows data collector to collect data from RMS. Before you use the Windows data collector on the DPS computer, you must configure this data collector. The Windows data collector must be associated with an Information Server.

You can configure the Windows Data Collector components either from the Grid View or from the Map View.

See “[Configuring the data collectors](#)” on page 116.

To configure the Windows data collector

- 1 Go to Settings > System Topology.
- 2 Do one of the following:
 - In the System Topology > Grid View, right-click **Data Collection Service** and click **Edit Settings**.
 - In the System Topology > Map View, right-click a registered DPS component and click **Edit Settings**.
- 3 In the **Component Settings** dialog box, under Data Collector, click **Windows - Information Server**.
- 4 In the Windows - Information Server panel, enter the required information.

Configuring the Oracle data collector

The Control Compliance Suite uses the Information Server to retrieve data from the enterprise network. The Information Server passes the collected data to the Data Processing Service (DPS) Collector. The collector then returns the collected data to the Control Compliance Suite infrastructure for further processing. The Information Server uses the bv-Control for Oracle snap-in module to collect data from the Oracle databases.

The Control Compliance Suite uses the Oracle data collector to collect data from the Information Server. Before you use the Oracle data collector on the DPS computer, you must configure this data collector. The Oracle data collector must be associated with an Information Server.

You can configure the Oracle Data Collector components either from the Grid View or from the Map View.

See [“Configuring the data collectors”](#) on page 116.

To configure the Oracle data collector

- 1 Go to Settings > System Topology.
- 2 Do one of the following:
 - In the System Topology > Grid View, right-click **Data Collection Service** and click **Edit Settings**.
 - In the System Topology > Map View, right-click a registered DPS component and click **Edit Settings**.
- 3 In the **Component Settings** dialog box, click **Oracle - Information Server**.
- 4 On the Oracle - Information Server panel, enter the required information.

Configuring the SQL data collector

The Control Compliance Suite uses the Information Server to retrieve data from your enterprise network. The Information Server passes the collected data to the Data Processing Service (DPS) Collector. The collector then returns the collected data to the Control Compliance Suite infrastructure for further processing. The Information Server uses the bv-Control for Microsoft SQL Server snap-in module to collect data from the SQL Server databases.

The uses the SQL data collector to collect data from the Information Server. Before you use the SQL data collector on the DPS computer, you must configure this data collector. The SQL data collector must be associated with an Information Server.

You can configure the SQL Data Collector components either from the Grid View or from the Map View.

See “[Configuring the data collectors](#)” on page 116.

To configure the SQL data collector

- 1 Go to **Settings > System Topology**.
- 2 Do one of the following:
 - In the **System Topology > Grid View**, right-click **Data Collection Service** and click **Edit Settings**.
 - In the **System Topology > Map View**, right-click a registered DPS component and click **Edit Settings**.
- 3 In the **Component Settings** dialog box, click **SQL - Information Server**.
- 4 On the SQL - Information Server panel, enter the required information.

Configuring the UNIX data collector

The Control Compliance Suite can use the Information Server to retrieve data from the enterprise network. The Information Server passes the collected data to the Data Processing Service (DPS) Collector. The collector then returns the collected data to the Control Compliance Suite infrastructure for further processing. The Information Server uses the bv-Control for UNIX snap-in module to collect data from the UNIX target computers.

The Control Compliance Suite uses the UNIX data collector to collect data from the Information Server. Before you use the UNIX data collector on the DPS computer, you must configure this data collector for an Information Server.

See “[Configuring the data collectors](#)” on page 116.

To configure the UNIX data collector

- 1 Go to **Settings > System Topology**.
- 2 Do one of the following:
 - In the **System Topology > Grid View**, right-click **Data Collection Service** and click **Edit Settings**.
 - In the **System Topology > Map View**, right-click a registered DPS component and click **Edit Settings**.
- 3 In the **Component Settings** dialog box, click **UNIX - Information Server**
- 4 On the **UNIX - Information Server** panel, enter the required information.

Configuring the ESM data collector

You must configure the ESM data collector before you use the ESM data collector on a computer where Data Processing Service (DPS) is installed. The ESM data collector must be associated with one or more ESM managers.

Before you configure the ESM data collector, you must provide the details about the ESM components that the data collector is configured to communicate with. At any point of time after you configure the ESM data collector, you can re-configure the settings to make changes to the data collector.

See [“Configuring the data collectors”](#) on page 116.

To configure the ESM data collector

- 1 Go to **Settings > System Topology**.
- 2 Do one of the following:
 - In the **System Topology > Grid View**, right-click **Data Collection Service** and click **Edit Settings**.
 - In the **System Topology > Map View**, right-click a registered DPS component and click **Edit Settings**.
- 3 In the **Component Settings** dialog box, click **ESM**.
- 4 On the **ESM** panel, configure the ESM Manager by providing the required information.
- 5 In the **Edit Settings** dialog box, navigate to **Data Collector > ESM**.
Provide the required information to configure the thread settings and poll settings of the ESM data collector.

See [“Modifying the settings of a component ”](#) on page 107.

See [“Configuring basic Data Processing Service settings”](#) on page 100.

See [“Configuring the ESM manager settings”](#) on page 121.

See [“Configuring the ESM general settings ”](#) on page 125.

Configuring the ESM components

You must configure the ESM data collector before you use the ESM data collector on the Data Processing Service computer. The ESM data collector must be associated with one or more ESM managers.

The ESM manager settings are specific to a site. The configurations that you do for the ESM manager is specific to the site where you have configured the ESM data collector. You can view or update the ESM data collector configuration for a site by selecting the site from the **Site** drop-down list. The drop-down list displays the list of sites that have at least one DPS that is configured as the ESM data collector.

To configure the ESM components

- 1 In the CCS console, go to **Settings > System Topology**.
- 2 Do one of the following:
 - In the **System Topology > Grid View**, right-click **Data Collection Service** and then click **Edit Settings**.
 - In the **System Topology > Map View**, right-click the site where DPS is installed and then click **Edit Settings**.

3

See [“Configuring the ESM manager settings”](#) on page 121.

See [“Configuring the ESM general settings ”](#) on page 125.

See [“Configuring an ESM manager for custom messages”](#) on page 122.

See [“Collecting suppressed ESM messages ”](#) on page 123.

Configuring the ESM manager settings

The ESM managers that are configured for the data collector of a site are displayed in the **List of configured ESM Managers** list box.

To configure the ESM manager settings

- ◆ On the right pane, provide the required information to configure an ESM manager.

Adding, modifying, or removing an ESM manager

To add or modify an ESM manager

- 1
- 2 In the ESM Manager Credentials dialog box, in the Manager details section, provide the required information.

To remove an ESM manager

- 1 On the panel, select an ESM manager from the **List of configured ESM managers** pane.
- 2 Click **Remove**.

See [“Configuring the ESM manager settings”](#) on page 121.

Configuring an ESM manager for custom messages

You can configure the ESM data collector to use the custom messages during data collection, if you have customized ESM messages. You can select only one ESM manager per site as a source for custom messages.

The message schema includes the following:

- Message description
- Message title
- Message format

You can customize the message schema on the selected ESM manager. The ESM data collector uses the message schema during data collection for the specified site.

To specify an ESM manager for custom messages

- 1 Navigate to **Settings > Map View** or **Settings > Grid View** of the console and right-click on a DPS and click **Edit Settings**.
- 2

- 3 On the right pane of the dialog box, for the **Manager for custom messages** section, click the **Manager Name** drop-down list.

You can select the ESM manager that maintains the custom messages, which you have configured. The schema of the custom messages, such as description, title, format and so on are also collected from the selected ESM manager.

- 4 Keep **Report error if custom messages manager not available** checked.

If you check **Report error if custom messages manager not available**, then the data collection job fails with an error if the specified custom messages manager is unavailable.

If you uncheck **Report error if custom messages manager not available**, then the ESM data collector collects data even if the specified custom messages manager is unavailable.

If the custom messages manager is not available, a message prompt appears in the job failures tab, which states about the unavailability of the manager.

See [“Configuring the ESM manager settings”](#) on page 121.

Collecting suppressed ESM messages

You can configure the ESM data collector to do the following:

- Collect suppressed ESM messages
- Filter suppressed messages

The data collector configuration to collect suppressed messages applies to the ESM managers that are configured for the selected site.

Note: When you uncheck **Do not collect suppressed messages**, the checks which were successful in the previous data collection might fail in the subsequent data collection.

To collect suppressed messages

- 1 Navigate to **Settings > Map View** or **Settings > Grid View** of the console and right-click on a DPS and click **Edit Settings**.
- 2
- 3 On the right pane of the dialog box, for the **Collection of suppressed messages** section, uncheck **Do not collect suppressed messages**.

See [“Configuring the ESM manager settings”](#) on page 121.

About CCS ESM policy run configurations

Every check in a CCS ESM standard is mapped to an ESM policy. A CCS ESM Standard is mapped to one or more ESM policies. Policy run options let you specify the data that the ESM data collector must collect for a given policy.

The default setting for all policies is "Do not run policy, collect data from last successful policy run." However, you can add exceptions to the default setting by adding an entry in the policy run settings for each policy that you want to customize. The ESM data collector executes a policy run on the basis of the policy run configuration.

You can configure the number of messages that you want ESM data collector to fetch for each policy run. The `Symantec.CSM.ESM.Integration.dll.config` file contains the `MaximumPolicyRunMessageCount` parameter, where you can specify the value for the message count. The `Symantec.CSM.ESM.Integration.dll.config` file that is located in the following location:

`<Install_Directory>\CCS\Reporting and Analytics\DPS\Data Collectors\ESM`

The default value is 3000.

The ESM data collector collects policy run data on the basis of the policy run configuration. The ESM data collector does not verify the agents and the modules in the policy run when it fetches the latest policy run data. The data collections job completes successfully even if the selected policy run does not contain the modules or the agents that you have specified. However, the result for the data collection job displays the corresponding errors if the policy run data is not present on the ESM manager.

The available modes for data collection are:

- Collect data from the last policy run on the ESM manager.
- Run the ESM policy on the ESM manager and collect the policy run data.
- Run policy on the ESM manager only if the last policy run is older than the <number of> days.

For example, consider that the 'Security essentials W2K3MS v2.0' policy includes the 'Account Integrity' and 'Password Strength' modules. Consider the two agents, 'W2k3Server1-USA' and 'W2k3Server2-USA.' You have run all the modules of 'Security essentials W2K3MS v2.0' on both the agents on 28th September, 2008, at 11:00 a.m. Later, you fix certain violations and then run only the Password Strength module of 'Security essentials W2K3MS v2.0' policy on W2k3Server2-USA on the 29th September, 2008, at 01:00 p.m. You schedule a data collection job on the 30th September, 2008, at 11:00 a.m. to collect data for ESM agents W2k3Server1-USA and W2k3Server2-USA for the same policy and the modules.

In CCS 9.0, you configure the ESM policy 'Security essentials W2K3MS v2.0' as 'Run policy if data is older than 1 days.'

During data collection, ESM data collector retrieves the timestamp of the last policy run of the selected agents for all the selected modules.

In the given scenario, the policy run timestamps for the 'Security essentials W2K3MS v2.0' policy on W2k3Server1-USA and W2k3Server2-USA agents are as follows:

ESM agent	ESM policy	ESM module	Timestamp of the last policy run
W2k3Server1-USA	Security essentials W2K3MS v2.0	Account Integrity	28th September, 2008, 11:00 a.m.
W2k3Server1-USA	Security essentials W2K3MS v2.0	Password Strength	28th September, 2008, 11:00 a.m.
W2k3Server2-USA	Security essentials W2K3MS v2.0	Account Integrity	28th September, 2008, 11:00 a.m.
W2k3Server2-USA	Security essentials W2K3MS v2.0	Password Strength	29th September, 2008, 01:00 p.m.

The most recent timestamp of the values that the ESM data collector retrieves in this case is 29th September, 2008, 01:00 p.m. Assume that the data collection job is initiated as per its schedule. The ESM data collector compares the 29th September, 2008, 01:00 p.m. timestamp with the current timestamp on the DPS computer, which is 30th September, 2008, 11:00am. Since the data is not older than 1 day, the ESM data collector imports the messages from the last policy run from all the ESM agents.

Configuring the ESM general settings

To configure the ESM general settings

- ◆ In the panel, provide the following information:

Thread settings

- In the Thread count text box, type the number of ESM managers that the ESM data collector can communicate in parallel.
The default value is 5.
- In the Thread timeout seconds text box, type the time in seconds after which the ESM data collector should terminate an idle thread.
The default value is 600.

See [“About the thread settings for ESM data collector ”](#) on page 126.

Poll settings

- In the ESM manager polling seconds text box, type the manager polling time in seconds.
The default value is 30 seconds.
- In the ESM policy run submit retry seconds text box, type the policy run retry submit time in seconds.
The default value is 300 seconds.

See [“About the poll settings for ESM data collector ”](#) on page 127.

See [“Configuring the ESM manager settings”](#) on page 121.

About the thread settings for ESM data collector

A thread is a connection that an ESM data collector creates to communicate with an ESM manager to collect data. The ESM data collector can communicate with multiple ESM managers in parallel. The thread settings let you define the number of ESM managers the ESM data collector can contact in parallel.

You can configure the following parameters for the ESM thread settings:

Thread count

Specify the number of ESM managers that the ESM data collector can communicate in parallel.

The default value is 5.

Thread Timeout Seconds

The ESM data collector terminates a thread that continues to be idle for longer than the specified time. Specify the time in seconds after which the ESM data collector must terminate an idle thread.

The default value is 600 seconds.

Note: The **Thread Timeout Seconds** setting impacts data collection only when the ESM data collector queries more than one manager in a data collection request.

See [“Configuring the ESM manager settings”](#) on page 121.

See [“Configuring the ESM general settings ”](#) on page 125.

About the poll settings for ESM data collector

Sometimes, the ESM data collector initiates policy runs before the ESM manager starts data collection from the agents. You can configure the polling frequency of the ESM data collector to initiate the policy runs through the general settings configuration of the data collector.

The scenarios for which the ESM data collector uses the poll setting configurations are as follows:

- Establish contact with the ESM manager when the ESM data collector starts a new policy run.
- Determine the policy completion status.

The ESM manager lets only four concurrent policy runs in the starting state on the ESM manager. If you initiate the fifth policy run, the ESM manager displays the following error:

```
Could not start job: server too busy. Reschedule job for a later time.
```

You can configure the following parameters for the ESM poll settings:

ESM manager polling seconds

Specify the interval period after which the ESM data collector must query the ESM manager to find the policy completion status.

The default value is 30 seconds.

ESM policy run submit retry seconds	<p>The ESM data collector re-submits a policy run if the data collector encounters an error when it starts the policy run. Specify the interval period after which the ESM data collector must try to re-submit a policy run on the ESM manager.</p> <p>The default value is 300 seconds.</p>
-------------------------------------	---

See [“Configuring the ESM manager settings”](#) on page 121.

See [“Configuring the ESM general settings ”](#) on page 125.

Recommended Data Processing Service settings for ESM data collector

Symantec recommends that you change the settings of the DPS that is configured for ESM data collection. You can configure the DPS settings from the computer where the Data Processing Server service is installed.

To change the Data Processing Service settings

- 1 Open the DPS configuration file from the following location:
`<Install Directory>\Symantec\CCS\Reporting and Analytics\DPS\Symantec.CSM.DPS.exe.config`
- 2 Add the keys in the <appSettings> section of the configuration file.

You can restrict the maximum number of concurrent jobs that the DPS handles to four when you specify the values that are mentioned in the table.
- 3 Restart the DPS Service.

Table 3-18 Keys for appSettings and their description

Key to add in <appSettings>	Description
<add key="WPM_MinimumWorkerProcesses" value="1">	Configures the DPS to have at least one worker process at any given point of time.
<add key="WPM_MaximumWorkerProcesses" value="2">	Configures the DPS to create maximum of two concurrent worker processes for processing the data collection job.
<add key="WPM_MaximumJobsPerWorkerProcess" value="1">	Configures the DPS to assign maximum of one job to a single worker process.

The configuration of the DPS for the ESM data collector with other roles such as evaluation or reporting may affect the data collection performance. Symantec recommends that you install a DPS only with the DPS Collection role for the ESM data collector.

Configuring the CSV data collector

In the Control Compliance Suite, you can store assets in a CSV file and import them using a CSV data collector. The assets and their relevant data must be arranged in a specific format in the CSV file for importing them into the infrastructure using the CSV data collector.

See [“About format of the CSV file headers”](#) on page 291.

In the Control Compliance Suite, a DPS that is registered to a site can be configured as a CSV data collector. The DPS can be configured as a CSV data collector either from the Grid View or from the Map View of the console. Before configuring the DPS, ensure that the CSV file containing the assets is placed in a network share path of the computer that hosts the DPS.

Note: If a CSV file is shared on a DPS collector computer, then ensure that the user has either log on locally or log on as a batch job permission. This permission is required for the CSV data collector of both the single setup and distributed setup modes. The user is the one whose credentials are required to access the network share path. The same user credentials are also specified for the selected platform of the CSV option in the **Component Settings** dialog box.

The CSV data collector is used to collect data in the following scenarios:

- To collect data for the common fields of the predefined asset types.
You must use the platform, Common in the Common settings dialog box for the CSV configuration.
See [“Configuring Common platform through CSV settings”](#) on page 271.
- To collect data for assets that are stored in the CSV files for any predefined asset type or a custom application.

See [“Configuring the data collectors”](#) on page 116.

To configure the CSV data collector

- 1 Go to Settings > System Topology.
- 2 Do one of the following:
 - In the System Topology > Grid View, right-click the Data Collection Service and click **Edit Settings**.

- In the System Topology > Map View, right-click a registered DPS component and click **Edit Settings**.

- 3 In the **Component Settings** dialog box, select **CSV** under the Data Collector Sites option on the left pane of the dialog box.
- 4 Select the site to which the DPS is registered from the Site Name drop-down box on the right side pane of the dialog box.
- 5 Enter values for the fields to configure the CSV data collector.

The fields and the descriptions are as follows:

Platform	<p>Enter the platform of the application whose data is to be queried .</p> <p>You can use the drop-down box to select the platform of the application.</p>
CSV File(s) Path	<p>Enter the path where the CSV file is placed.</p> <p>If you are importing assets from the Altiris CMDB, the file path should point to location of the CSV file on Altiris Notification Server. The CSV file is created by the CCS Asset Export Task solution on Altiris Notification Server.</p> <p>See “About importing assets from Altiris” on page 335.</p> <p>Click the browse button and in the Browse for folder dialog box, browse to the path where the CSV file is located. You must ensure that the CSV file path is specified in the UNC format, \\<server name>\<share name>\<path>\<filename>.csv.</p>
Windows Domain	<p>Enter the domain of the Windows computer, where the CSV file is located.</p> <p>You need to provide the credentials of the Windows domain user in the dialog box, Credentials for the Platform.</p>
User Name	<p>Enter the user name of the specific domain.</p>

Search Pattern

Enter the search pattern of the CSV file.

For example, in a given share path there can be several CSV files for the same platform. In such a case, if you want to have data from the CSV file that starts with the alphabet, m, then the search option can be, m*.csv.

File Encoding

Enter the encoding type of the file. For example, Unicode (UTF -8).

You can use the drop-down box to select the unicode of the CSV file.

6 Click **Apply**.

7 Click **OK**.

See [“Creating a CSV file for custom application”](#) on page 295.

See [“Creating a CSV file for predefined asset types”](#) on page 293.

Configuring the general settings

The Control Compliance Suite Console comes configured with default values for the various system settings. You can change the values to meet your organization's requirements. Only users with the Administrator role can configure the settings.

You can configure the settings from the Settings > General view.

Configuring the data locations

Note: If you change the data location configuration, then you must synchronize the DPS with the latest configuration. You can synchronize DPS using the Sync Configuration option from the **Settings > General > Data Processing Service** view.

To configure the data location

- 1** Go to **Settings > General**.
- 2** In the **General** view, on the left panel, click **System Configuration > Data Locations**.
- 3** On the right panel, click **Add**.

- 4 In the **Add Data Location** dialog box, provide the required information.
To edit an existing data location, select the data location and click **Edit**.
To delete an existing data location, select the data location and click **Delete**.
- 5 Click **OK** to save.

Enabling and disabling audit setting

Configuring the audit settings is a system-wide setting that applies to all CCS users.

To configure auditing

- 1 Go to **Settings > General**.
- 2 In the **General** view, on the left panel, click **System Configuration > Auditing**.
- 3 On the right panel, do one of the following:
 - To enable auditing, check **Enable Auditing**.
 - To disable auditing, uncheck **Enable Auditing**.

See [“About audits”](#) on page 147.

Configuring the email Notification Server

You must specify the server and the port number to send and receive notifications in Control Compliance Suite (CCS).

CCS can be configured to send notifications for the following events:

- Completion of the asset import jobs.
- Completion of the data collection and data evaluation jobs.
- Expiration of an exception.
- Change in the status of a policy.
- Response to policy clarification requests.
- Change in status of a dashboard or a dashboard update job.
- State transitions of the control points.
- Asset remediation.

To configure the email notification settings

- 1 Go to **Settings > General**.
- 2 In the **General** view, on the left panel, click **System Configuration > Email Notifications**.
- 3 On the right panel, provide the following information:

Notification Server	Type the name of the computer that hosts the SMTP server. The name is specified in any format: computer name, IP address, or host name.
From Email Address	Type the default email address that is used in the Job wizards to send notifications. If required, at the time of creating the job you can change the address in the wizard.
Notification Port	Type the port number of the computer that hosts the SMTP server.

See [“About the job types”](#) on page 596.

Selecting the DPS to synchronize the reporting database

You can select the Data Processing Service (DPS) that is used for synchronizing the reporting database. The reporting database is periodically synchronized with the data that is stored in the production database. Data is synchronized when the Reporting Database Synchronization job is run.

To select the DPS for data synchronization

- 1 Go to **Settings > General**.
- 2 In the **General** view, on the left panel, click **System Configuration > DPS for Reporting Synchronization**.
- 3 On the right panel, select the DPS that can be used for synchronization of the reporting database.

See [“About the Control Compliance Suite Data Processing Service”](#) on page 34.

Synchronizing the reporting database

Configuring the report server settings is a system-wide setting that applies to all Control Compliance Suite (CCS) users.

You can choose to synchronize the reporting database immediately after certain jobs are completed.

To perform data synchronization

- 1
- Go to **Settings > General**.
- 2
- In the **General** view, on the left panel, click **System Configuration > Reporting Synchronization**.
- 3
- On the right panel, you can do the following:

Check/uncheck jobs for synchronization	Check or uncheck the jobs for the reporting database synchronization. By default, all the jobs are selected. If you uncheck any of the jobs, the corresponding job data is synchronized when the scheduled reporting data synchronization job is run. If you check any of the jobs, the corresponding job information is synchronized in the reporting database immediately after the jobs are completed.
Synchronize Configuration to Integration Services Server	Click this option to verify the connection to the computer that has the SQL Server with Integration Services (SSIS) installation.
Synchronize Application Server Credentials	Click this option to verify the authentication of the user connecting to the computer that has the SQL Server with Integration Services (SSIS) installation.

See [“About data synchronization”](#) on page 623.

Configuring the evidence purge job

You can configure the purge job schedule for the custom evidence providers that are registered with the system. Purge settings applies to all custom evidence providers and is not specific to individual custom evidence providers.

Any evidence data that exceeds the retention age for the registered custom evidence providers is deleted at the specified time.

See [“About the Evidence Management system”](#) on page 697.

You can monitor the purge job using the SQL Server agent.

To configure the evidence data purge schedule

- 1 Go to **Settings > General**.
- 2 In the **General** view, on the left panel, click **Data Purge > Evidence Purge**.
- 3 On the right panel, check **Purge evidence data at** and select the time to run the evidence purge job.

About the purge settings

When objects in the Directory are deleted, the corresponding information and results are stored in the database. The database must be purged regularly to maintain optimum performance. As the database grows, the results are longer queries, corrupt databases, and depleted disk space.

Control Compliance Suite (CCS) includes a default global purge setting. Some modules have their own purge settings. You can schedule the purge job to run periodically.

You can configure the purge settings from the **System > General > Data Purge > Other Purge Settings** panel.

The following are the different purge settings tabs in the **Other Purge Settings** panel:

Stale Data	<p>Settings for the global purge.</p> <p>The number of days after which data is purged. The default value is 180 days.</p>
Exceptions	<p>Settings for purging the exceptions data.</p> <p>The exceptions data older than the number of days that is specified in the Exceptions tab is deleted. The default value is 180 days.</p>
Standards	<p>Settings for purging the standards data.</p> <p>The standards data older than the number that is specified in the Stale Data tab are deleted.</p> <p>Data can also be deleted if it is younger than the number that is specified. The data collection results and the data evaluation results for runs greater than the number that is specified in the Standards tab are deleted.</p> <p>Note: A purge of evaluations results does not re-compute summary statistics until another evaluation is executed.</p>

Entitlements	<p>Settings for purging the historical entitlements data.</p> <p>The entitlements historical data older than the number of days that is specified in the Entitlements tab is deleted. The default value is 180 days.</p> <p>The minimum value is 100 days and the maximum value is 9999 days.</p>
System Audit Log	<p>Settings for purging the historical audit log data.</p> <p>The audit log historical data older than the number of days that is specified in the System Audit log tab is deleted. The default value is 365 days.</p> <p>See “About audits” on page 147.</p>
Baselines	<p>Settings for purging the comparison results.</p> <p>The comparison results older than the number of days that is specified in the Baselines tab is deleted. The default is 60 days.</p>
Reports	<p>Settings for purging the report results in the reporting database.</p> <p>The report results older than the number that is specified in the Reports tab are deleted. Report results are also deleted for runs greater than the number that is specified in the Reports tab.</p>

See [“Configuring the purge settings”](#) on page 136.

See [“Configuring the purge job schedule”](#) on page 137.

Configuring the purge settings

Control Compliance Suite (CCS) comes configured with default purge settings. You can change the values if you prefer different settings.

See [“About the purge settings”](#) on page 135.

To configure the purge settings

- 1 Go to **Settings > General**.
- 2 In the **General** view, on the left panel, click **Data Purge > Other Purge Settings**.

3 On the right panel, do the following:

Stale Data	<p>Type the number of days after which the information in the production database is purged. The default value is 180 days.</p> <p>The stale data setting is used as the default global purge setting. Some modules have their own purge settings.</p> <p>Select the purge schedule options.</p>
Exceptions	<p>Type the number of days after which the exceptions data is purged. The default value is 180 days.</p>
Standards	<p>Type the number of data collection job runs, the results of which must be retained. The default value is 10</p> <p>Type the number of data evaluation job runs, the results of which must be retained. The default value is 10.</p>
Entitlements	<p>Type the number of days after which the entitlements historical data is purged. The default value is 180 days.</p> <p>The minimum value is 100 days and the maximum value is 9999 days.</p>
System Audit Log	<p>Type the number of days after which the historical audit log data is purged. The default value is 365 days.</p>
Baselines	<p>Type the number of days after which the baselines comparison result is deleted. The default is 60 days.</p>
Reports	<p>Type the number of report job runs, the results of which must be retained. The default value is 10.</p> <p>Type the number of days after which the information in the reporting database is deleted.</p>

4 On the **Other Purge Settings > State Data** tab, click **Schedule Job** to run the job according to the selected schedule options.

See [“Configuring the purge job schedule”](#) on page 137.

Configuring the purge job schedule

You can check the status of a purge job from the **Monitor > Job Management** view.

To configure the purge schedule

- 1 Go to **Settings > General**.
- 2 In the General view, on the left panel, click **Data Purge > Other Purge Settings**.

- 3
- On the **Stale Data** tab, Select one of the following schedule options:
- **Run now**

Select this option to run the job immediately after you click Schedule Job.

■ **Run periodically**

Select this option to run the job on a specified date and time.
Provide the following information:

Start on

Select the date and time to run the evaluation job.

Run once

Select this option to run the job one time on the specified date and time.

Run every

Select this option to specify how often (in days) the scheduled purge job runs.

4

Click **Schedule Job** to save the settings and run the job that is based on the settings.

See [“About the purge settings”](#) on page 135.

See [“Configuring the purge settings”](#) on page 136.
- ## Configuring the Response Assessment Module database settings
- You can modify the SQL Server settings that are used to connect to the Response Assessment Module (RAM) database.
- To configure the RAM settings
- 1

Go to **Settings > General**.

2

In the **General** view, on the left panel, click **Application Configuration > RAM DB Configuration**.

3

On the right panel, provide the following information:
- | | |
|--|--|
| Enable RAM database configuration | Select the check box to configure the SQL server settings that are used to connect to the Response Assessment module (RAM) database. |
| SQL Server | Type the computer name that hosts the SQL Server. |
| Database Name | The default database name can be changed, if needed. |

Instance name	Type the SQL Server instance name. The default SQL Server instance name appears in the text box.
Port number	Type the port number of the SQL Server instance. If the port is enabled, the SQL Server default instance listens on TCP port 1433.
Use SSL	Check this option if you want SQL Server to use SSL to encrypt network transmissions independent of the network protocol.
Use Windows NT Integrated Security	Select this option if you connect to the SQL Server instance using Windows Authentication.
Use a SQL user name and password	Select this option if you connect to the SQL Server instance using SQL Server Authentication. You must specify the authentication details of the user in the respective text boxes. You cannot specify the following special characters for the User name and the Password fields: <ul style="list-style-type: none"> ■ Semicolon (;) ■ Double quotes (")

See [“About Response Assessment Module ”](#) on page 39.

Configuring the entitlements settings

Configuring the entitlements settings is a system-wide setting that applies to all Control Compliance Suite users.

To configure the entitlements settings

- 1 Go to **Settings > General**.
- 2 In the **General** view, on the left panel, click **Application Configuration > Entitlements**.
- 3 On the right panel, provide the following information:

Multi select approval tasks	Select the check box to allow data owners to change and approve multiple control points at the same time.
Daily Approval Job run time	Select the time to schedule the entitlements approval job. The approval job starts and ends the review cycles.
Automatically Import Entitlements	Select the check box if you want the system to automatically import the entitlements at a scheduled time.
Automatic Import Job Runtime	If you have selected to automatically import entitlements, select the time to schedule the job.
Connection timeout interval	Select the database timeout interval. The database terminates the session when it reaches the specified time.
Revert Import Pending Control Point Status	<p>Due to system failure the status of some control points are left in the Entitlement Import Pending status.</p> <p>Select this option to change the status of the control points with status Entitlement Import Pending to Entitlement Import Required.</p>

See “[About entitlements](#)” on page 381.

Configuring the exceptions settings

Configuring the exceptions settings is a system-wide setting that applies to all Control Compliance Suite users.

To configure the exceptions settings

- 1 Go to **Settings > General**.
- 2 In the **General** view, on the left panel, click **Application Configuration > Exceptions**.
- 3 On the right panel, provide the following information:

Expiration notification period	Type the number of days before the expiration date when a notification must be sent.
Run the exceptions update job at	Select the time to schedule the exception management job.
From address for exception details	Type the email address from which the email notification is sent.

See [“About exceptions”](#) on page 428.

Customizing the report logo and name

You can select the company logo and the company name to replace the existing logo and the name that appear on the report.

The following is the recommended logo size:

For the company logo	The maximum size is 44 x 42 pixels at 72 DPI resolution.
For the company banners that contain both the logo and name	The maximum size is 570x42 pixels at 72 DPI resolution.

To customize the report logo and name

- 1 Go to **Settings > General**.
- 2 In the **General** view, on the left panel, click **Application Configuration > Report Customization**.
- 3 On the right panel, click **Add** to select the logo and the company name.
- 4 To set the default logo, select the logo and click **Set Default**.
- 5 To set the default company name, select the company name and click **Set Default**.

See [“Working with reports ”](#) on page 635.

Configuring the policy settings

Configuring the policy settings is a system-wide setting that applies to all Control Compliance Suite users.

To configure the policy settings

- 1 Go to **Settings > General**.
- 2 In the **General** view, on the left panel, click **Application Configuration > Policies**.
- 3 On the right panel, provide the following information:

Policies expiry period	Type the default number of days of a policy 's life span. When a policy is created, this number is used to calculate the policy expiration date.
Policies review period	Type the default number of days for reviewing a policy. When a policy is created, this number is used to calculate the date by when a policy must be reviewed.
Clarifications are due within	Type the default number of days for submitting a clarification.
Policies daily job time	Select the daily scheduled time to run a policy job.
Email from address	Type the email address from which the email notification is sent.

See [“Working with policies”](#) on page 578.

Configuring the dashboard settings

Configuring the dashboards is a system-wide setting that applies to all the tiered dashboards. You can configure the security assessment status level settings to all the evaluation nodes and the dashboard job settings.

To configure the dashboard settings

- 1 Go to **Settings > General**.
- 2 In the **General** view, on the left panel, click **Application Configuration > Tiered Dashboards**.
- 3 On the right panel, provide the following information:

Global Threshold Settings tab	<p>Define a threshold for each status level of Standards and bv-Control query.</p> <p>The four possible security assessment status levels for the dashboard are:</p> <ul style="list-style-type: none"> ■ Critical ■ Danger ■ Warning ■ Normal <p>The build-up of the security assessment of the evaluation nodes for both bv-Control and Standards evaluation results determine a dashboard's security assessment status.</p> <p>See “Example of status calculation for bv-Control Query Results node” on page 669.</p> <p>See “Example of status calculation for Standards Evaluation Results node” on page 669.</p>
Global Job Settings tab	<p>Type the maximum number of update jobs that can be assigned to each Data Processing Service (DPS) in the Reporting role.</p> <p>See “About the Control Compliance Suite Data Processing Service” on page 34.</p>

See [“About threshold settings in tiered dashboard”](#) on page 666.

See [“About status calculation”](#) on page 668.

See [“About the threshold types ”](#) on page 667.

Configuring the remediation settings

You must configure the remediation settings to create the ServiceDesk tickets and to send email notifications for asset remediation.

To configure the remediation settings

- 1 Go to **Settings > General**.
- 2 In the **General** view, on the left panel, click **Application Configuration > Remediation Settings**.
- 3 On the right panel, provide the following information:

Service Desk Incident Web Service URL	Type the fully qualified URL of the Web Service. http://<serverName>/SD.Remediation.RemediationService.asmx Control Compliance Suite (CCS) uses the URL to create ServiceDesk tickets for asset remediation.
CCS Web Server	Type the name of the computer that hosts the CCS Web server. The Web server is used to communicate with the ServiceDesk application to reevaluate the assets that required remediation. The Web server is also used to send email notifications for the assets that require remediation. The name is specified in any of the following formats: IP address, the fully qualified DNS, or the computer.
Submitting contact email	Type the contact email address. The email address is used as the From address in the email notifications that are sent for asset remediation. The email account must exist in the ServiceDesk application as the account is the primary contact for the ServiceDesk tickets that are submitted from CCS.
Maximum assets per ticket	Type the maximum number of assets that can be included in a remediation ticket for each asset type. The default value is 20. The minimum value is 1.

See [“About remediation”](#) on page 549.

Configuring the Home view settings

Configuring the report settings is a system-wide setting that applies to all Control Compliance Suite (CCS) users.

You can configure the number of reports that are displayed in the **Home** view. By default, 10 reports are displayed. The reports that are displayed are the most recently run reports.

To configure the number of reports in the Home view

- 1 Go to **Settings > General**.
- 2 In the **General** view, on the left panel, click **Application Customization > Home**.
- 3 On the right panel, type the maximum number of reports that can be displayed in the **Home > Home Page** view.

See [“About the Home view”](#) on page 51.

See [“Working with reports ”](#) on page 635.

Configuring the standards settings

You can configure the maximum number of job runs that are displayed for each asset. You can also set the number of data collection results that are displayed for each category of the standard.

By default, the 10 most recent job runs are displayed.

To configure the standards settings

- 1 Go to **Settings > General**.
- 2 In the **General** view, on the left panel, click **Application Customization > Standards**.
- 3 On the right panel, provide the following information:
 - Type the number of job runs to be displayed in **Evaluation** tab for each asset.
The **Evaluation** tab is displayed in the **Manage > Assets > Asset System** view and in the **Manage > Standards** view.
 - Type the number of job runs to be displayed in **Data Collection** tab for each asset.
The **Data Collection** tab is displayed in the **Manage > Assets > Asset System** view.
 - Type the number of data collection results to be displayed in the **Data Collection Details** dialog box for each category of the standard.
The **Data Collection Details** dialog box is displayed when you click the view icon on the **Data Collection** tab in the details pane of **Manage > Assets > Asset System** view.
The details pane displays the details of the assets that are evaluated against a standard.

See [“Viewing asset information in the details pane”](#) on page 319.

See [“Viewing standard information in the details pane”](#) on page 486.

Configuring the job count settings

You can configure the number of jobs and the job runs that are displayed in the **Monitor > Jobs** view.

By default, 20 jobs and 10 job runs are displayed. For each job, the most recent job runs are displayed. Entering the value zero displays all jobs and job runs.

To configure the job count settings

- 1 Go to **Settings > General**.
- 2 In the **General** view, on the left panel, click **Application Customization > Job Count**.
- 3 On the right panel, provide the following information:

Number of Jobs	Type the number of jobs to be displayed in the Monitor > Jobs view.
Number of Job Runs	Type the number of job runs to be displayed in the Monitor > Jobs view. For each job, the specified number of job runs are displayed.

See [“About the Jobs view”](#) on page 599.

Configuring the assets count settings

You can configure the number of assets that are displayed in the **Manage > Assets > Assets System** view.

By default, 2000 imported assets are displayed. Entering the value zero displays all the assets in the system.

To configure the assets count setting

- 1 Go to **Settings > General**.
- 2 In the **General** view, on the left panel, click **Application Customization > Assets Count**.
- 3 On the right panel, type the number of assets.

The assets are displayed in the **Manage > Assets > Assets System** view.

See [“Performing the tasks in the Asset System view”](#) on page 305.

About audits

An audit of the Control Compliance Suite (CCS) involves tracking and logging the events that occur on the system. You can change the audit settings to comply with your organization's standards. You can either enable or disable auditing in the **Settings > General** view. Auditing is a system-wide setting. Auditing tracks the changes to standards, policies, and assets and captures the data to an audit log. The log captures the information on who changed what and when the change was made. The log can track the changes to permissions on the objects.

An audit usually includes the following tracking information:

- Insertions of new records
- Deletions of existing records
- Modifications of existing records

See [“About audit event triggers”](#) on page 147.

See [“Enabling and disabling audit setting”](#) on page 132.

See [“About viewing the audit logs”](#) on page 148.

About audit event triggers

The following are the actions that trigger an audit event:

Table 3-19 Audit Event Triggers

Event type	Module	Triggering Action
Asset Change	C1 Core	An attribute of an asset is changed.
Job Execution	C1 Core	At the successful completion of every job that the application server launches.
Job Creation/Deletion	C1 Core	Log the creation or deletion of a job
Role Member Change	C1 Core	A person or group is added to and or removed from a role.
Role Create/Delete	C1 Core	A role is created or deleted.
Role Power Change	C1 Core	A power is added to or removed from a role.
Policy Change	Policy	Any component of a Policy is modified.
Standard Change	Standards	Any component of a Standard is modified. Each modification creates a separate log entry of this type.

Table 3-19 Audit Event Triggers (continued)

Event type	Module	Triggering Action
Policy Module Control Statement Create/Change/Delete	Policy	A control statement is created, changed, or deleted.
Policy Module Control Statement Assignment/De-Assignment	Policy	A control point is linked to or delinked from a policy.
Control Point Configuration Change	Entitlement	The configuration for a control point is changed. The configuration may include a change in published status, data owner, management classification, department, or review cycle.
Control Point Approval or Rejection/Request for Change	Entitlement	A control point entitlement approval or request for change occurred.
Control Point Approval Violation	Entitlement	A control point review cycle ended without the required approval event.

See [“About audits”](#) on page 147.

About viewing the audit logs

You can generate audit reports and view the reports in the **My Reports** view after they are scheduled.

You cannot open or view an audit log within the console. A SQL Server database maintains the audit logs. With the appropriate permissions and third-party tools, you can view the log data.

See [“About audits”](#) on page 147.

See [“About audit event triggers”](#) on page 147.

Managing licenses

You can add licenses at the time of Control Compliance Suite (CCS) installation or at a later time from the console's **Licenses** view. You must provide the core license during installation. The core license, CCS_Core.slf, is required for installing the Directory Support Service and the CCS Application Server components.

The CCS licenses are stored in the ELS (Enterprise License Store) store of the product (C:\Program Files\Common Files\Symantec Shared\Licenses).

In the CCS Console, users can view and add CCS license files from the **Licenses** view. Users can view only those features that have a valid license.

You cannot open the CCS Console if the core license expires. The core license can be renewed from the stand-alone utility Symantec.CSM.LicenseUtil.exe that is stored in the following location:

```
<install_directory>\CCS\Reporting and Analytics\Directory Support  
Service\
```

See [“Adding licenses on the Directory Server”](#) on page 150.

The CCS Console does not display any expired component's features. The system displays a message to indicate that a license has expired.

See [“About the Licenses view”](#) on page 149.

See [“Adding a license”](#) on page 150.

See [“Viewing the list of licenses”](#) on page 150.

About the Licenses view

In the **Settings > Licenses** view, the user can view, and add licenses. You can check the status, the type, the product ID, and the expiration dates of licenses.

You can use the **Licenses** view for the following tasks:

- View registered licenses for the installed Control Compliance Suite components.
- Add a new license.

The **Licenses** view displays the following information for each license:

Feature	Component name and its version
Status	Valid or Invalid license
Product ID	Component name
Expires	Expiration date of the license. Some licenses never expire.

See [“Managing licenses”](#) on page 148.

See [“Adding a license”](#) on page 150.

See [“Adding licenses on the Directory Server”](#) on page 150.

See [“Viewing the list of licenses”](#) on page 150.

Adding a license

When you add a license you enable an installed feature.

To add a license

- 1 Go to **Settings > Licenses**.
- 2 In the **Licenses** view, click **Add License**.
- 3 In the **Add Licenses** dialog box, click **Import** to add the license.
- 4 Locate and open the license file, then select the license or licenses to add and click **Open**, or double-click a license.
- 5 Click **OK**.

See [“Managing licenses”](#) on page 148.

See [“About the Licenses view”](#) on page 149.

See [“Adding licenses on the Directory Server”](#) on page 150.

See [“Viewing the list of licenses”](#) on page 150.

Adding licenses on the Directory Server

When you add a license you enable an installed feature. You can use the `Symantec.CSM.LicenseUtil.exe` utility on the Control Compliance Suite Directory Server to add license files. The tool imports a Symantec License File (.slf) and activates the software.

The tool is available on the Directory Server host at `<install directory>\CCS\Reporting and Analytics\Directory Support Service\Symantec.CSM.LicenseUtil.exe`.

See [“Managing licenses”](#) on page 148.

To add a license on the Directory Server

- 1 On the Directory Server host, open the `Symantec.CSM.LicenseUtil.exe` tool.
- 2 In the **Licensing** dialog, click **Add Licenses**.
- 3 Locate and open the license file, then select the license or licenses to add and click **Open**, or double-click a license.
- 4 In the **Licensing** dialog, click **Done** to close the utility.

Viewing the list of licenses

You can view the list of licenses and their status.

To view a list of licenses

- 1 Go to **Settings > Licenses**.
- 2 The **Licenses** view lists the Control Compliance Suite licenses and their status.
See [“Managing licenses”](#) on page 148.
See [“About the Licenses view”](#) on page 149.
See [“Adding a license”](#) on page 150.
See [“Adding licenses on the Directory Server”](#) on page 150.

Managing users

Control Compliance Suite (CCS) lets you store the CCS user and group accounts. The user accounts are automatically added when the users are assigned to roles. The user and the group accounts can also be imported from a CSV file. The accounts store the user and the group email addresses that are used to send any updates.

See [“About the User Management view”](#) on page 151.

About the User Management view

The **User Management** view lists all the Control Compliance Suite (CCS) users and groups.

You can do the following from the User Management view:

- Import user and group accounts from a CSV file
See [“Importing user accounts”](#) on page 152.
- Update email addresses
See [“Updating a user email address”](#) on page 152.
- Delete user and group accounts
See [“Deleting user accounts”](#) on page 153.
- Update all users and groups from the domain
See [“Updating user accounts”](#) on page 153.

See [“Managing users”](#) on page 151.

About adding a user account

When a user is assigned a role in the Settings > Roles view, an account for the user is automatically created in the system. All of the Control Compliance Suite users and groups are displayed in the **Settings > User Management** view.

See [“About the User Management view”](#) on page 151.

See [“Managing users”](#) on page 151.

Importing user accounts

Control Compliance Suite lets you import user and group accounts from a CSV file.

The CSV file should contain fields in the following format:

<DomainName\SAM Account name>,<Display name>,<Mail ID>

Table 3-20 Example

CSV field	Example
SAM Account name	ABC\jsmith
Display name	John Smith
Mail ID	jsmith@abc.com

To import user and group accounts

- 1 Go to **Settings > User Management**.
- 2 In the **User Management** view, on the taskbar , click **Import from CSV**.
- 3 In the **Open** dialog box, browse to the location of the CSV file.
- 4 Select the file and click **Open**.

See [“About the User Management view”](#) on page 151.

See [“Managing users”](#) on page 151.

Updating a user email address

You can update a user email address from the User Management view.

To update user information

- 1 Go to **Settings > User Management**.
- 2 In the **User Management** view, select the user or the group account to update the email ID.
- 3 Click on the **Mail ID** cell of the user account, and type the email address.

The system displays a message if the ID is invalid.

See [“About the User Management view”](#) on page 151.

See [“Managing users”](#) on page 151.

Deleting user accounts

You can only delete the user or the group accounts that are not responsible for any critical functions of the system. A message appears when you try to delete a user or the group account that is responsible for executing certain functions of the system.

To delete user accounts

- 1 Go to **Settings > User Management**.
- 2 In the **User Management** view, right-click the user or the group account to be deleted, and select **Delete**.

See [“About the User Management view”](#) on page 151.

See [“Managing users”](#) on page 151.

Updating user accounts

You can update all the Control Compliance Suite user and group accounts with current information from Active Directory.

To update user accounts

- 1 Go to **Settings > User Management**.
- 2 In the **User Management** view, select the check boxes of the user and group accounts to be updated.
- 3 From the **Common Tasks** menu, select **Update**.

See [“About the User Management view”](#) on page 151.

See [“Managing users”](#) on page 151.

Configuring the application server settings

You can change the authentication type for storing the security settings.

To configure the application server settings

- 1 Go to **Settings > System Topology**.
- 2 Do one of the following:
 - In the **System Topology > Grid View**, right-click the application server component and click **Edit Settings**.

- In the **System Topology > Map View**, right-click the application server component and click **Edit Settings**.
- 3 In the **Component Settings** dialog box, click **Application Server**.
- 4 On the **Application Server** panel, select one of the following authentication types:

Use controlled delegation of security rights	Select this option if you want to use the Constrained Delegation feature of Windows 2003.
Use Control Compliance Suite to store the password	Select this option if you want to use the built-in storage to store the encrypted password.
- 5 Type the name of the email server.
- 6 Click **Apply**.
- 7 Click **OK**.

See [“About the security settings for scheduled jobs”](#) on page 154.

See [“Adding credentials for scheduled jobs”](#) on page 55.

About the security settings for scheduled jobs

Control Compliance Suite (CCS) provides the option to store the user password that is required for asset resolution when running scheduled jobs.

During installation, the administrator can choose from one of the following security settings:

- Use controlled delegation of security rights
CCS uses the Constrained Delegation feature of Windows 2003
- Use Control Compliance Suite to store the password
CCS uses the built-in secured storage to the encrypted password

Administrator can later choose to change the security setting from the **Settings > System Topology > Map** view.

See [“Configuring the application server settings”](#) on page 153.

Only users with the role to schedule jobs can store their passwords from the **Home > User Preferences** view.

See [“Adding credentials for scheduled jobs”](#) on page 55.

Configuring the assets batch size

You can control the number of assets that are imported from data collectors in a single batch. Each data collector size is set separately. These settings let you optimize the collection of data from your network.

Symantec recommends that you use the default batch size to ensure better performance.

See [“Configuring the data collectors”](#) on page 116.

To configure the assets batch size

- 1 Go to **Settings > System Topology**.
- 2 Do one of the following:
 - In the **System Topology > Grid View**, right-click the Data Processing Service component and click **Edit Settings**.
 - In the **System Topology > Map View**, right-click the Data Processing Service component and click **Edit Settings**.
- 3 In the **Component Settings** dialog box, click **Assets Batch Size**.
- 4 On the **Assets Batch Size** panel, provide the number of assets that are imported in a batch from each data collector.
- 5 Click **Apply**.
- 6 Click **OK**.

Configuring the SQL Server settings

You can modify the SQL Server settings of the reporting database, production database, and the SSIS connection. The SQL Server settings are initially configured in the Installation Wizard.

You can modify the settings from the **Settings > Secure Configuration** view.

See [“Configuring the application server database connection settings”](#) on page 155.

See [“Configuring the reporting database connection”](#) on page 156.

See [“Configuring the SSIS Server Connection”](#) on page 158.

Configuring the application server database connection settings

The application server uses the production database to store the queried data.

You can modify the SQL Server settings of the production database that is initially configured in the Installation Wizard.

Use the settings to set up a new server. The data is not automatically migrated to the new database.

To configure the application server settings

- 1
- Go to **Settings > Secure Configuration > AppServer Database Connection**.
- 2
- Provide the following information:

SQL Server	Type the computer name that hosts the SQL Server.
Database name	Type the name of the database. By default, the existing database name is displayed in the text box.
Instance name	Type the SQL Server instance name if the SQL Server database is not the default instance.
Port number	Type the port number of the computer that hosts the SQL Server. By default, Control Compliance Suite Application Server connects through the port, 1433 of the SQL Server computer.
Use SSL	Check this option if your computer that hosts the SQL Server is SSL enabled for communication.
Use Windows NT Integrated Security	Select this option if you have installed the SQL Server in the Windows NT user context.
Use a SQL user name and password	Select this option if you have installed the SQL Server in a different user context. Specify the authentication details of the user in the respective text boxes. You cannot specify the following special characters for the User name and the Password fields: <ul style="list-style-type: none">■ Semicolon (;)■ Double quotes (")

- 3
- Click **Update** to save.

See [“About the Control Compliance Suite production database”](#) on page 37.

Configuring the reporting database connection

You can modify the SQL Server settings of the reporting database that is initially configured in the Installation Wizard .

The application server uses the settings to communicate with the reporting database. The reporting database stores the evaluated data that is used for generating reports.

Use the settings to set up a new server. The data is not automatically migrated to the new database.

To configure the reporting database settings

1 Go to **Settings > Secure Configuration > Report Database Connection**.

2 Provide the following information:

SQL Server	Type the computer name that hosts the SQL Server.
Database name	Type the database name. The default database name appears in the text box.
Instance name	Type the SQL Server instance name. The default SQL Server instance name appears in the text box.
Port number	Type the port number of the SQL Server instance. If the port is enabled, the SQL Server default instance listens on TCP port 1433.
Use SSL	Check this option if you want SQL Server to use SSL to encrypt network transmissions independent of the network protocol.
Use Windows NT Integrated Security	Select this option if you connect to the SQL Server instance using Windows Authentication.
Use a SQL user name and password	Select this option if you connect to the SQL Server instance using SQL Server Authentication. You must specify the authentication details of the user in the respective text boxes. You cannot specify the following special characters for the User name and the Password fields: <ul style="list-style-type: none"> ■ Semicolon (;) ■ Double quotes (")

3 Click **Update** to save.

See [“About the Control Compliance Suite reporting database”](#) on page 37.

Configuring the SSIS Server Connection

You can modify the SQL server settings of the SSIS connection that is initially configured in the Installation Wizard .

The reporting database uses the SSIS platform to sync with the production database. The information that is provided on this panel is used to connect to the msdb database and deploy SSIS packages. You must enable the SQL Agent on the selected database.

To configure the application server settings

- 1
- Go to **Settings > Secure Configuration > SSIS Server Connection**.
- 2
- Provide the following information:

SQL Server	Type the computer name that hosts the SQL Server.
Instance name	Type the SQL Server instance name. The default SQL Server instance name appears in the text box.
Port number	Type the port number of the SQL Server instance. If the port is enabled, the SQL Server default instance listens on TCP port 1433.
Use SSL	Check this option if you want SQL Server to use SSL to encrypt network transmissions independent of the network protocol.
Use Windows NT Integrated Security	Select this option if you connect to the SQL Server instance using Windows Authentication.
Use a SQL user name and password	Select this option if you connect to the SQL Server instance using SQL Server Authentication. You must specify the authentication details of the user in the respective text boxes. You cannot specify the following special characters for the User name and the Password fields: <ul style="list-style-type: none">■ Semicolon (;)■ Double quotes (")■ Curly bracket ({})■ Single quotes (')■ Hyphen (-)■ Forward slash (/)

- 3
- Click **Update** to save.

Configuring the application server credentials

Provide the credentials of the user in whose context the application server is run on the computer. You must also set the Service Principal Name for the Application Server service account.

See [“Configuring service accounts with unconstrained delegation”](#) on page 159.

See [“Configuring the S4U and constrained delegation”](#) on page 160.

To modify application server credentials

- 1 Go to **Settings > Secure Configuration > AppServer Credentials**.
- 2 Type the user name in whose context the application server Service is run on the computer.

See [“About using special characters in credentials”](#) on page 161.
- 3 Type the password that authenticates the specified user account.
- 4 Click **Update** to save.

Configuring service accounts with unconstrained delegation

You need to configure the service accounts for the Directory Support Service (DSS) and the Application Server to operate with unconstrained delegation in distributed and single setup modes.

Note: Setting up of Service Principal Names (SPNs) is important for a successful installation and configuration of a distributed setup. You must execute the procedure to configure the service accounts for unconstrained delegation before you install the CCS components.

To configure the service accounts with unconstrained delegation

- 1 Identify the user accounts that you want to use as the service accounts for DSS and Application Server.

The user accounts must have the necessary privileges.
- 2 Create the Service Principal Name (SPN) for the Application Server and the DSS services.

The SPN for both the short NetBIOS name and the fully-qualified host name (FQDN) is created. While delegation can work without SPN in Windows Server 2000 domains, it can also fail depending on the operating system that is in use.

You must associate an SPN to a single user account.

The service-name portion of the SPN must match the following:

- SetSpn -A Symantec.CSM.AppServer/appserver_machine domain\appserver_account
- SetSpn -A Symantec.CSM.AppServer/appserver_machine.fqn domain\appserver_account
- SetSpn -A Symantec.CSM.DSS/dss_machine domain\dss_account
- SetSpn -A Symantec.CSM.DSS/dss_machine.fqn domain\dss_account
- SetSpn.exe -a http/IIS_computer's_NetBIOS_name DomainName\UserName
This is applicable only for Windows Server 2003.
- SetSpn.exe -a http/IIS_computer's_FQDN DomainName\UserName
This is applicable only for Windows Server 2003.

3 Enable delegation for the Application Server's service account.

The following service accounts are to be enabled:

Windows Server 2000 Domain	In the user properties for the Application Server account, go to Account tab and check the option, Account is trusted for delegation .
Windows Server 2003 Domain	In the user properties, go to the Delegation tab and select the option, Trust this user for delegation to any service (Kerberos only) .

4 When installing the Application Server, specify the FQDN when prompted by the setup for the computer that installed the DSS. It is not mandatory to specify the FQDN, but sometimes specifying a short NetBIOS name can cause problems.

Configuring the S4U and constrained delegation

Before configuring the Service for User (S4U) and constrained delegation, ensure that you configure the service accounts with unconstrained delegation. The S4U configuration is a modification of the unconstrained delegation configuration and is therefore an optional task for you to perform.

See [“Configuring service accounts with unconstrained delegation”](#) on page 159.

To configure S4U with constrained delegation

1 Set up delegation on the Application Server account.

For AD users and computers, open the properties for the Application Server's service account and make the following changes on the Delegation tab:

- Select **Trust this user for delegation to specified services only**
- Select **Use any authentication protocol**
- Under **Services to which this account can provide delegated credentials** do the following:
 - Click **Add** and type in the name of the machine where DSS is installed. From the list of services, select the service, LDAP that has the same port number as the port where the ADAM instance is running and click **OK**.
 - Click **Add** and type the name of the service account for which the DSS service is running. You can view the custom SPN that was created for the DSS before installation. Select the service and click **OK**.

2 On the Application Server computer, open the Local Security Policy editor.

Navigate to **Under Local Policies > User Rights Assignment** and grant the privilege, Act as part of the operating system to the Application Server.

3 Configure the Application Server in the following manner to use S4U authentication:

- In the CCS Console, go to **Settings > System Topology**.
- Select the Application Server component, and right-click on **Edit Settings**.
- In the **Edit Settings** dialog box, select the **Application Server > Basic** option.
- For the **Authentication type** option, select **Use controlled delegation of security rights**.

4 Reboot the Application Server computer so that the delegation settings can take effect.

About using special characters in credentials

Control Compliance Suite supports using specific special characters in the credentials of the user accounts when you install the product components. Using any unsupported special characters in the credential of the user account can cause the component installation to fail.

The supported special characters are applicable to the Windows user accounts for the following services:

- Directory Support Service
- Application server Service
- Data Processing service (DPS) running in the reporter role

The supported special characters are applicable to the following databases:

- Production database
- Reporting database
- SQL Server integration Service (SSIS)

The following special characters are supported in the user account user name:

- A-Z, a-z
- 0-9
- At sign (@)
- Hash (#)

The following special characters are supported in the user account password:

- A-Z, a-z
- 0-9
- At sign (@)
- Hash (#)
- Less-than (<)
- Greater-than (>)

See [“Configuring the application server credentials”](#) on page 159.

Updating Control Compliance Suite

Symantec releases system patches and updates for the Control Compliance Suite (CCS) components, which are downloaded using LiveUpdate. LiveUpdate is a core Symantec technology that is used to simplify maintenance and updates of Symantec software after deployment.

Symantec hosts an online database of all possible product updates. The LiveUpdate client contacts the Symantec LiveUpdate Server and submits a list of products that are currently installed on the LiveUpdate client. The LiveUpdate server returns a list of appropriate updates.

Various LiveUpdate client types are available, but Control Compliance Suite uses only the Windows LiveUpdate Client. In CCS, the LiveUpdate client is automatically installed on the computer on which the CCS Application Server component and the Data Processing Service are installed.

The LiveUpdate client also requires the LiveUpdate Administrator (LUA) for downloading the patches. You can install the LUA on any computer where Internet access is available, including a computer that runs the LiveUpdate client. The LUA is equipped with a distribution mechanism to distribute the updates to a distribution area. The LiveUpdate client is responsible for picking up the updates from the distribution area for the components that are installed on the LiveUpdate client computer. All computers that host a LiveUpdate client must be configured with a host file that points to the LUA distribution area.

See [“About the host file for Windows LiveUpdate clients”](#) on page 165.

The administrator needs to decide whether content or system updates are required for the installed components and to configure the LUA appropriately.

The following two types of updates are available for the CCS components:

- Content updates
- System patches and service pack updates

See [“How LiveUpdate works in Control Compliance Suite”](#) on page 163.

See [“About the LiveUpdate view”](#) on page 164.

How LiveUpdate works in Control Compliance Suite

Control Compliance Suite (CCS) uses Symantec LiveUpdate to get the latest product updates. Other distribution methods such as direct download from the Symantec Web site are available per Symantec policies.

Do the following to set up LiveUpdate:

- Configure a host file on the LUA.
See [“About the host file for Windows LiveUpdate clients”](#) on page 165.
- Copy the host file to the LiveUpdate client computers.
You must copy the client settings host file to the LiveUpdate installation folder on the client computer. By default, LiveUpdate is installed to C:\Program Files\Symantec\LiveUpdate.
- Enable and schedule LiveUpdate.
See [“Enabling and scheduling LiveUpdate”](#) on page 165.

In CCS, LiveUpdate works in the following way:

- The LiveUpdate client detects new update and copies the package to the CCS LiveUpdate staging location on the LiveUpdate client.
See [“About the LiveUpdate staging location”](#) on page 166.
- From the staging location, the CCS administrators must install the updates manually on each computer that hosts the LiveUpdate client.

Before you install updates, confirm that the staging progress is 100% complete in the **System > LiveUpdate** view.

Symantec recommends that you first install the updates on the Application Server.

When the updates are installed, the **Percent Deployed** column in the System > LiveUpdate view shows 100%.

If the Directory Server is not installed on the same computer as the Application Server, the update status of the Directory Server is not calculated. A 100% does not include the Directory Server status.

See [“About the LiveUpdate view”](#) on page 164.

See [“Updating Control Compliance Suite”](#) on page 162.

About the LiveUpdate view

In the LiveUpdate view, you can view the status of the deployed version and the latest update of the component that is available for download. The view also displays the Readme file of the latest update.

The LiveUpdate view displays the following information for each update:

Component name	The name of the installed component.
Current Version	The version of the component that is currently deployed.
Percent Deployed	<p>The percentage of successful deployment of the target component in the Control Compliance Suite environment.</p> <p>A 100% would mean that the update is deployed successfully on all the computers that hosts the target component.</p> <p>If the Directory Server is not installed on the same computer as the Application Server, the deployed status of the Directory Server is not calculated. A 100% does not include the Directory Server status.</p>
Available Version	A newer version of the component that is available on the LiveUpdate client.

Percent Staged The percentage of successful downloads of the latest update package in all computers that host the target component.

If the Directory Server is not installed on the same computer as the Application Server, the staged status of the Directory Server is not calculated. The percentage does not include the Directory Server status.

Detection Date The date when the newer version is available for download.

See [“How LiveUpdate works in Control Compliance Suite”](#) on page 163.

See [“Updating Control Compliance Suite”](#) on page 162.

Enabling and scheduling LiveUpdate

You can enable LiveUpdate to run automatically at a scheduled time interval to ensure that Symantec CCS always has the most current updates. By default, when LiveUpdate clients are installed on the CCS computers, the clients are not scheduled to run automatically. You must manually configure the schedule to run LiveUpdate on the CCS computers.

To enable and configure LiveUpdate

- 1 Run LuConfig.exe from \Program Files\Symantec\LiveUpdate folder.
- 2 In the LiveUpdate Configuration console, click **Automatic LiveUpdate** tab.
- 3 In the Automatic LiveUpdate box, check **Use Automatic LiveUpdate**.
- 4 In the Update Frequency box, type the number in hours or minutes to set the frequency that you want Automatic LiveUpdate to run.

The default is every 240 minutes.

See [“How LiveUpdate works in Control Compliance Suite”](#) on page 163.

See [“Updating Control Compliance Suite”](#) on page 162.

See [“Performing LiveUpdate on demand”](#) on page 166.

About the host file for Windows LiveUpdate clients

When a LiveUpdate client is installed, the client is configured to use a Symantec LiveUpdate server. You must generate a new client settings host file to redirect LiveUpdate clients to retrieve updates from a Distribution server. The host file must then be distributed to each client computer on the network. When the client computer runs LiveUpdate, LiveUpdate connects to the server that you designate in the host file and downloads the updates from that location.

In Control Compliance Suite (CCS), the LiveUpdate client is installed on the computer on which the Application Server and the Data Processing Service are installed.

You must copy the client settings host file to the LiveUpdate installation folder on the client computer. By default, LiveUpdate is installed to C:\Program Files\Symantec\LiveUpdate.

For information on how to generate a host file, refer to *Symantec LiveUpdate Administrator User's Guide*.

See [“How LiveUpdate works in Control Compliance Suite”](#) on page 163.

See [“Updating Control Compliance Suite”](#) on page 162.

About the LiveUpdate staging location

When LiveUpdate runs, it copies the latest update package to the staging location.

The staging location is user-definable. The location is specified by creating a text file with a single line of text that contains the fully qualified path to the staging location. The file is named LUSTagingLocation.txt and should be located in the following directory: <common_app_data>\Symantec\CCS

If LUSTagingLocation.txt does not exist, cannot be read, or is empty, LiveUpdate uses the default staging location, which is
<common_app_data>\Symantec\CCS\LiveUpdateStaging.

See [“How LiveUpdate works in Control Compliance Suite”](#) on page 163.

See [“Updating Control Compliance Suite”](#) on page 162.

See [“Performing LiveUpdate on demand”](#) on page 166.

Performing LiveUpdate on demand

You can run LiveUpdate on demand to force an immediate update of a component or the content.

To perform LiveUpdate on demand

- 1 Run LuALL.exe from \Program Files\Symantec\LiveUpdate folder.
- 2 Follow the on-screen instructions to run LiveUpdate.

See [“How LiveUpdate works in Control Compliance Suite”](#) on page 163.

See [“Updating Control Compliance Suite”](#) on page 162.

Configuring Response Assessment Module in Control Compliance Suite

Control Compliance Suite (CCS) lets you connect to the Response Assessment Module (RAM) and assign the CCS assets to questionnaires to collect the evidence data.

[Table 3-21](#) lists all the tasks that you must do to successfully view the evidence data from the questionnaires.

Table 3-21 Collect data from RAM

Task	Description
Assign roles	<p>Assign the Asset Viewer role to users answering the questionnaire about CCS assets. The role determines what you can see and perform in the CCS Console.</p> <p>See “Adding users and groups to a role” on page 89.</p>
Configure the RAM database	<p>Configure the SQL Server settings to connect to the RAM database.</p> <p>See “Configuring the Response Assessment Module database settings” on page 138.</p>
Create asset groups	<p>Create the asset groups to use in the questionnaires. Individual assets can be used but they must be part of an asset group for the Policy module to use.</p> <p>An asset group consists of assets of one or more types. The grouping is represented in a hierarchical fashion with nested subsets. You can create dynamic and static asset groups to organize the assets into logical groups.</p> <p>See “Creating a dynamic asset group” on page 300.</p> <p>See “Creating a static asset group” on page 302.</p>
Enable the CCS connection	<p>Enable the connection to the CCS application server to collect the evidence data.</p> <p>See “Adding a link to Control Compliance Suite” on page 169.</p>
Create a questionnaire	<p>Create a questionnaire or choose a questionnaire from the predefined content folders.</p> <p>Refer to the <i>Response Assessment module User Guide</i> for steps on how to create a questionnaire.</p>

Table 3-21 Collect data from RAM (*continued*)

Task	Description
Add an asset group variable	Create a user-defined property and assign it to a CCS asset. See “Adding a Response Assessment Module user-defined property” on page 169.
Invite questionnaire users	Invite users to the new questionnaire and select the CCS asset to link to the questionnaire. See “Publishing a questionnaire with invitations in Response Assessment Module” on page 170.
Create a policy	After the evidence data is in the database, create a policy for the questionnaire from the CCS console. Create a policy and link it to the same asset group that is linked to the questionnaire. The policy reports do not work if not linked to the same asset group. See “Creating a new policy” on page 579. See “Importing a Word policy” on page 581.
Map control statements	After the policy is created, map the control statements to the policy. The control statements are mapped to the frameworks and regulations that your enterprise must adhere to. The policy reports do not work if the policy and questions in the questionnaire are not linked to the same control statements. See “Mapping policies to control statements” on page 688.
Publish the policy	After the policy is mapped to the control statements, publish the policy for user acceptance. See “Publishing a policy” on page 587.
Synchronize the reporting database	After the policy is published, synchronize the reporting database to run reports. Note: Evidence from RAM is only imported if it exists in the Evidence table of the RAM database. See “Synchronizing the reporting database” on page 133. See “Running a job now” on page 603.

Table 3-21 Collect data from RAM (continued)

Task	Description
Run reports	<p>After data is synchronized, run the following reports to view the RAM data:</p> <ul style="list-style-type: none"> ■ Policy Compliance by Asset ■ Policy Results by Control ■ Policy Control Statement Mappings <p>See “Scheduling a report” on page 636.</p> <p>See “Viewing a report” on page 638.</p>

Adding a link to Control Compliance Suite

You can link the Response Assessment Module (RAM) to Control Compliance Suite (CCS). After you have linked the systems, you can assign the CCS assets to a RAM questionnaire and view RAM evidence in CCS. You must have the RAM Server installed and have a connection to it.

See [“Configuring Response Assessment Module in Control Compliance Suite”](#) on page 167.

To add a link to Control Compliance Suite

- 1 In **Start > All Programs > Symantec Corporation**, select **Response Assessment module > Response Assessment module**.
- 2 In the **RAM Server** toolbar in the **RAM Console**, click **Settings**.
- 3 In the **Settings** dialog box, check **CCS present in the environment**.
- 4 In **Application Server** box, provide the server name.
- 5 In the **Port** box, provide the number.
- 6 In the **UPN** box, provide a valid email address.

Adding a Response Assessment Module user-defined property

In the Response Assessment module (RAM), you can add a user-defined property to an object. You can populate a drop-down list that is displayed in the Web client or the Windows client. You can assign a default value. The default value is displayed at the top of the list. You can set the values to read-only.

User-defined properties are displayed in the RAM **Invitation Manager** and the RAM **Response Wizard** reports.

See [“Configuring Response Assessment Module in Control Compliance Suite”](#) on page 167.

To add a Response Assessment Module user-defined property

- 1 In the **RAM Console**, click **Properties**.
- 2 In the **Selected Object's Properties** dialog box, in the **User Defined Properties** node, click **Add**.
- 3 In the **Create New User Defined Property** dialog box, type the name.
- 4 Click **Add**.
- 5 In the **DropDown Definition** box, type a value. Click **OK**.
- 6 Repeat steps 4 and 5, if necessary.
- 7 Click **OK** to add the property.

Publishing a questionnaire with invitations in Response Assessment Module

In the Response Assessment module (RAM), you can publish a questionnaire and invite users to respond. To create the invitations, you use the **RAM Server** toolbar in the **RAM Console**. You must have the **RAM Server** installed to use the **RAM Server** toolbar and **Invitation Manager**.

You should have the user names available. You can search for the email address in the **RAM Server users** dialog box.

When you create the invitations, you can also set the following options:

- **Enable Expiration Date**
- **Enable Email Notifications**
- **Enable Quizzing**
- **Number of Questions Per Page**

These options are not required.

If you select **Enable Expiration Date** option, you must provide an expiration date.

You should select **Enable Email Notifications**, if you want emailed invitations. You must have your mail server configured to send emails.

If you want to quiz your users and allow them to answer a questionnaire a specific number of times, select the **Enable Quizzing** option. You must also provide the minimum passing percentage and the number of extra chances. The minimum passing percentage is the percentage of correct answers in the quiz. The number

of extra chances is the number of times that a user can take the same quiz before it is automatically submitted.

You can change the number in the **Number of Questions Per Page** option. This option is the number of questions a user may see in one page of the **RAM Web Client**. The default number per page is 10. The number may be different if you have used the **Next Hops** tool. The **Next Hops** tool lets you design a different flow to the questionnaire. For example, a **Next Hops** question could be if the server room is always locked. If the user responds "Yes", then the user skips any questions about the server room being unlocked.

See [“Configuring Response Assessment Module in Control Compliance Suite”](#) on page 167.

To publish a questionnaire with invitations in RAM

- 1 In the **RAM Console**, in the **RAM Server** toolbar, click **Publish**.
- 2 In the **Publish a Questionnaire to the RAM Server** page, click **Publish**.
- 3 In the **Success** message, click **OK**.
- 4 In the **Invite Users** message, click **Yes**.
- 5 In the **Create Questionnaire Invitations** page, provide a title or accept the default.
- 6 Click **Add Users**.
- 7 In the **RAM Server users** dialog, select the users and click **Add Selected Users**.
- 8 Click **Close** to close the dialog.
- 9 Click **Invite**.
- 10 In the **Invitations Created** message, click **OK**.
- 11 In the **Create Questionnaire Invitations** page, click **Close**.

About configuring the Web Portal to contact RAM

The Control Compliance Suite (CCS) Web Portal works with the Response Assessment module (RAM) Web client. Several settings may be changed to enable connection with RAM.

The IIS CCS application pool uses the Network Server account as the identity. The account is a local account. The account may or may not connect to RAM. You should use the same account that is used as the identity in the RAM application pool.

The identity account has the following requirements:

- Member of the IIS_WPG local group
- Full permissions to the .NET directory
- Full permissions to the Windows\Temp directory

The Control Compliance Suite Web Portal is installed with anonymous access setting for the CCS_Web site. You should change the setting to use Windows Integrated authentication. You should disable anonymous access.

In the web.config file for the Control Compliance Suite Web Portal, you must set the SPN value. The format for the value should be

account@domain_name.com

Verify that the computer name is used in the following settings:

- AppServer
- RAMServer

If you use Control Compliance Suite assets with the RAM questionnaires, you must use Kerberos authentication.

About logs and configuration files

The application adds a message to the log when an event occurs. The type of event that triggers a message is based on the level of severity setting. Logs may include event data from the servers. You view the log information to troubleshoot security problems in the network. You delete the events that are no longer needed.

You can use Notepad.exe or another text editor to read a log file or a configuration file.

The logs are found in the following locations:

Table 3-22 Log location based on operating system

Operating system	Location
Windows 2003 Server	%ALLUSERSPROFILE%\Application Data\Symantec.CSM\Logs
Windows 2008 Server	%ALLUSERSPROFILE%\Symantec.CSM\Logs

The logging system is configured on a per-application basis. You must edit the configuration file to change the settings. The configuration file is commonly known as an app.config file.

The Control Compliance Suite Console configuration information location is based on operating system.

The configuration files are found in the following locations:

Table 3-23 Console configuration information based on operating system

Operating system	Configuration name
Windows 2003 Server/XP	%USERPROFILE%\Local Settings\Apps\2.0\[HASH]\[HASH]\syma..tion_[HASH]\SymConsole.exe.config
Windows 2008 Server/Vista	%USERPROFILE%\AppData\Local\Apps\2.0\[HASH]\[HASH]\syma..tion_[HASH]\SymConsole.exe.config

The following lists the Control Compliance Suite components and the name of their app.config file:

Table 3-24 Component and configuration name

Component	Configuration name
Application Server	<installation directory>\Application Server\AppserverService.exe.config
Data Processing Service	<installation directory>\DPS\Symantec.CSM.DPS.exe.config
Worker Process	<installation directory>\DPS\Blade.WorkerProcess.exe.config
Encryption Management Service	<installation directory>\EncryptionManagement Service\Symantec.CSM.EncryptionManagement.Service.exe.config
Certificate Management console	<installation directory>\Management Services\CertificateMgrConsole.exe.config
Directory Support Service	<installation directory>\Directory Support Service\Symantec.CSM.DSS.Service.exe.config

See [“About log messages”](#) on page 174.

See [“About log levels”](#) on page 174.

About log messages

The log messages conform to a standard logging format. The date and time are based on the UTC or the appropriate time zone information is attached. The category section is optional.

Each log message contains the following:

- Date
- Time
- Category
- Severity level
- Identity of the logging computer
- Message text

Message text can be used to supply text or additional parameters to a log message.

See [“About logs and configuration files”](#) on page 172.

See [“About log levels”](#) on page 174.

About log levels

Control Compliance Suite has a hierarchical logging system. The system uses a standard set of levels that are used to capture the required information. You can control how much information is written to the log when you adjust the log level threshold. When you enable logging at a given level, you also enable logging at the lower levels.

The log levels are as follows:

Table 3-25 Log levels

Level	Description	Levels captured in log
Verbose	The component operates properly. The level provides additional information.	This level is the highest level in the hierarchy.
Error	Operation cannot complete because of an error condition.	The error level logs all unhandled exceptions.
Warning	A recoverable error occurred.	A warning is often used for handled exceptions.

Table 3-25 Log levels (*continued*)

Level	Description	Levels captured in log
Informational	The component operates correctly. The level provides general feedback.	The level is used to capture the information that is useful for system management.
None	No log information is stored.	No log is kept.

The following are the details that each levels writes to the log:

Table 3-26 Log level details

Level	Verbose	Error	Warning	Informational
Verbose	X	X	X	X
Error		X	X	X
Warning			X	X
Informational				X

See [“About logs and configuration files”](#) on page 172.

See [“About log messages”](#) on page 174.

Performing the IT governance tasks with Control Compliance Suite

This chapter includes the following topics:

- [Preparing for risk assessment](#)
- [Assessing the compliance and the risk posture of the system](#)
- [Simplifying the remediation process](#)
- [Identifying possible threats in the access control system](#)

Preparing for risk assessment

The organization of all the known assets into the system is a crucial step in the process of governance in IT. Control Compliance Suite lets you collect the data for the assets, manage and monitor the assets, and evaluate the assets against a set of standards. You can collect the asset data either from the data collection components in the system or from a CSV file. Control Compliance Suite lets you reconcile the collected asset data based on certain rules.

The Control Compliance Suite supports certain predefined platforms and predefined asset types. The Control Compliance Suite also provides the flexibility to create your own asset types and perform the risk assessment on the custom asset types.

See [“Predefined platforms”](#) on page 203.

See [“Predefined asset types”](#) on page 204.

You are ready for the risk assessment when you have imported all the known assets into the asset system. Before you begin the asset import, it is recommended that you review the basic concepts in the asset system.

See [“Concepts in assets”](#) on page 200.

Table 4-1 Preparing for risk assessment

Task	Description
Register Data Processing Service	<p>Before the Application Server can use a newly installed Data Processing Service (DPS), you must register the DPS with the Application Server. When you register the DPS, you also assign the DPS to a site and specify the DPS roles.</p> <p>See “Registering the Data Processing Service” on page 98.</p> <p>See “Importing the specific and common fields for custom asset using the CSV data collector” on page 281.</p> <p>Go to Settings > Map View > Register DPS.</p>

Table 4-1 Preparing for risk assessment (*continued*)

Task	Description
Configure data collectors	<p>Go to Settings > Map View > Right-click the site > Edit settings.</p> <p>In the Data Processing Service dialog box, configure the following data collectors:</p> <ul style="list-style-type: none"> ■ Navigate to Collector - General Settings tab. Configure at least one data collection component to collect the assets. You can configure the data collector for the platform for which you want to import the assets. For example: If you want to collect the data for the Windows platform, you must configure the Windows Information Server settings. See “Configuring the data collectors” on page 116. ■ Navigate to Collector settings by site and click CSV Settings. Select Common from the platform list. Configure the Common platform through CSV settings if you want to collect the data for the fields that are common for all the asset types. See “Configuring Common platform through CSV settings” on page 271.

Table 4-1 Preparing for risk assessment (continued)

Task	Description
Set up the reconciliation rules	<p>Go to Manage > Asset System > Reconciliation Rules > Create Rule.</p> <p>See “Asset reconciliation” on page 245.</p> <p>Perform one of the following tasks to use the reconciliation rules:</p> <ul style="list-style-type: none">■ Use the predefined reconciliation rules to add the assets into the asset system for the first time. However, the predefined reconciliation rules add all the imported assets into the default folder, Asset System. See “Predefined reconciliation rules” on page 238.■ Create your own reconciliation rules to organize the assets into the asset system in a specific folder hierarchy. See “Creating reconciliation rules without manual review” on page 253. See “Reconciliation rules and rule types” on page 229.

Table 4-1 Preparing for risk assessment (*continued*)

Task	Description
Import the assets	<p>Go to Manage > Assets > Asset System > Asset Tasks > Import Assets.</p> <p>Perform the following tasks to import the assets into the asset system:</p> <ul style="list-style-type: none"> ■ Identify the primary assets of the asset type that you want to import. See “Primary and secondary assets” on page 228. ■ Import the primary assets either with the predefined reconciliation rules or with the custom reconciliation rules. See “Importing the assets for the first time” on page 265. ■ Import the secondary assets either from the default data collector or from the CSV data collector. See “Importing asset-specific fields from the default data collector” on page 272. See “Importing asset-specific and common fields using the default data collector” on page 275. See “Importing asset-specific and common fields using the CSV data collector” on page 278. See “Importing the specific and common fields for custom asset using the CSV data collector” on page 281.

Table 4-1 Preparing for risk assessment (continued)

Task	Description
Create asset groups	<p>Go to Manage > Assets > Asset System > Asset Group Tasks > Create Asset Group.</p> <p>Perform the following tasks with the asset groups:</p> <ul style="list-style-type: none">■ Create static and dynamic asset groups to create asset clusters on the basis of a common logical criteria. See “Creating a static asset group” on page 302. See “Creating a dynamic asset group” on page 300.■ Use the predefined dynamic asset groups. Copy a relevant predefined asset group to the folder in which you want to create an asset cluster. See “Predefined asset groups” on page 248.

See [“Assessing the compliance and the risk posture of the system”](#) on page 182.

Assessing the compliance and the risk posture of the system

The assessment of the compliance and the risk posture of the system begins when you import all the known assets into the system. Control Compliance Suite lets you proactively assess the assets against a set of standards. The assessment is done based on the data that is collected from the data collection components of the Control Compliance Suite. This comparison of the computer settings to predefined Standards is called an evaluation.

Before you begin the evaluation of the imported assets against the Standards, it is recommended that you review the basic concepts in Standards.

See [“Concepts in standards management”](#) on page 447.

Table 4-2 Compliance and risk posture assessment

Task	Description
Understand and identify the predefined standard for assessment	<p>Go to Manage > Standards .</p> <p>Consider the following to understand the predefined standards:</p> <ul style="list-style-type: none"> ■ Browse through the predefined standards in the tree pane under the Standards node. ■ Identify the predefined standard that you want to use for assessment of the imported assets. <p>See “About standards” on page 448.</p>
Collecting data for evaluation	<p>Go to Manage > Assets > Asset System > Global Tasks.</p> <p>Consider the following when you collect the data for evaluation:</p> <ul style="list-style-type: none"> ■ Select the asset type or the asset group for which you want to collect the data for evaluation and select Setup Data Collection. <p>See “Setting up a data collection job from the Assets view” on page 310.</p>

Table 4-2 Compliance and risk posture assessment (*continued*)

Task	Description
Evaluating the assets against the standards	<p>Go to Manage > Assets > Asset System > Global Tasks.</p> <p>Consider the following to evaluate the assets against the standards:</p> <ul style="list-style-type: none">■ Create an evaluation job to evaluate the assets for which data is collected. <p>The information that you specify during the evaluation process is saved in the evaluation job. Hence, an evaluation job lets you perform the evaluation process repeatedly without having to specify the evaluation criteria again. Evaluation jobs can be scheduled to run at predefined intervals.</p> <p>See “Running an evaluation job from the Asset System view” on page 311.</p>
Viewing the evaluation results	<p>Go to Manage > Assets > Asset System.</p> <p>Consider the following to view the evaluation results:</p> <ul style="list-style-type: none">■ View the details of the assets that are evaluated against a standard in the Details pane. <p>The details pane presents the following information about the evaluation:</p> <ul style="list-style-type: none">■ Standard against which the evaluation job was run■ Evaluation date■ Checks evaluated■ Checks not evaluated■ Compliance score■ Risk score <p>See “Running an evaluation job from the Asset System view” on page 311.</p> <p>See “Viewing the evaluation results in the details pane” on page 325.</p>

Table 4-2 Compliance and risk posture assessment (*continued*)

Task	Description
Generate reports based on evaluation	<p>Go to Reporting > Report Templates</p> <p>Consider the following while generating the compliance reports</p> <ul style="list-style-type: none"> ■ Generate reports that provide a summary of the compliance of assets against the required standards. See “Predefined Reports and Dashboard descriptions” on page 627. See “Working with reports ” on page 635.
Create dashboard reports for the evaluated data	<p>Go to Reporting > My Dashboards</p> <p>You can do the following to create and generate dashboard reports:</p> <ul style="list-style-type: none"> ■ Create a tiered dashboard through the Create Tiered Dashboards wizard. See “Creating a tiered dashboard” on page 657. ■ Add a Standards Evaluation Results node to the dashboard. See “Adding an evaluation node” on page 672. Select the asset and the appropriate standard to assess and create the scope for the evaluation node. ■ Schedule the tiered dashboard update job through the Create Tiered Dashboards wizard. ■ View the dashboard details and trends report in the report viewer. See “Viewing the tiered dashboard reports” on page 678.

See [“Simplifying the remediation process”](#) on page 186.

Simplifying the remediation process

After you evaluate the assets against standards, you get the evaluation results and the risk score. You can now identify the assets in the organization that are compliant with the set guidelines. Control Compliance Suite lets you create baselines based on the evaluation results. The baselines make it easier to compare the assets.

Table 4-3 Remediation process

Task	Description
Create baseline	<p>Go to Monitor > Jobs.</p> <p>Create a baseline job.</p> <p>You can mark an asset as a baseline for other assets. Or you can mark the result of an entire job run as a baseline for further jobs.</p> <p>See “Creating a baseline job” on page 560.</p>
View comparison results	<p>Go to Manage > Baselines.</p> <p>View comparison results for an asset against the baselined asset.</p> <p>See “Viewing the comparison results in the Baselines view” on page 561.</p>
Create remediation reports	<p>Go to Reporting >Report Templates.</p> <p>Select and schedule the Remediation Report to execute at a specific time interval.</p> <p>The remediation report lets you view the remediation information and the detailed evidence of failed checks for one or more asset groups or asset folders.</p> <p>See “Scheduling a report ” on page 636.</p>

Table 4-3 Remediation process (*continued*)

Task	Description
Setting exceptions	<p>Go to Manage > Exceptions.</p> <p>Identify the assets that you want to mark as exceptions to following certain standards.</p> <p>See “Requesting an exception for assets on checks” on page 436.</p> <p>Exceptions are the temporary permissions that exempt an asset from following an organizational policy for a specific time period. The exemption should be made for a valid business reason.</p>
Create a gold standard	<p>Go to Manage > Standards.</p> <p>Create a gold standard.</p> <p>See “Working with gold standard” on page 536.</p>
Create evidence for an IT audit process	<p>Go to Reporting > Report Templates.</p> <p>Generate various compliance summary reports to get a snapshot of the over compliance of your system.</p> <p>See “Scheduling a report ” on page 636.</p>

Identifying possible threats in the access control system

In a typical environment, IT compliance is confined to configuration management, the firewall, the antivirus systems, and the vulnerability assessment. However, there is a difference between managing security configurations and vulnerabilities and managing access controls and data entitlements. Incidents can occur when a valid user can have access to the data that the user should not access.

Control Compliance Suite facilitates the monitoring of access rights in the organization. The Control Compliance Suite identifies false entitlements. The Entitlements view in the Control Compliance Suite lets you define the data a user is entitled to access. The Entitlements view also monitors whether the system adheres to the defined access controls.

Before you begin to monitor the entitlements of the control points, it is recommended that you review the basic concepts in entitlements management. See [“Concepts in entitlements”](#) on page 394.

Table 4-4 Identifying threats in access control

Task	Description
Locating the potential control points in the asset system	<p>Go to Manage > Assets > Asset system.</p> <p>Consider the following to locate the potential control points in the asset system:</p> <ul style="list-style-type: none">■ Control points are the data locations in the system at which the access permissions are granted and approved. Locate the type of assets that should be marked as control points. You can decide the potential control points based on the Confidentiality, Integrity, and Availability values of the assets or any other criteria. <p>For example:</p> <p>You might want to frequently review the permissions granted to the assets that belong to the Finance department. In this case, consider the creation of a tag, Finance for a set of assets so that you can easily locate the potential control points.</p> <ul style="list-style-type: none">■ You cannot mark the Windows machines and the UNIX Machines assets as control points. <p>See “Control points” on page 395.</p>

Table 4-4 Identifying threats in access control (*continued*)

Task	Description
Mark the assets as control points	<p>Go to Manage > Assets > Asset System > Global Tasks > Mark as Control Point.</p> <p>Consider the following to mark the assets as control points:</p> <ul style="list-style-type: none"> ■ After you locate the assets as potential control points, you can mark the assets as control points. ■ After you mark the assets as control points, they are available for monitoring of entitlements in the Manage > Entitlements view. <p>See “Marking an asset as a control point” on page 398.</p>
Create Review Cycle Setting	<p>Go to Manage > Entitlements > Review Cycle Settings.</p> <p>Consider the following to create a review cycle setting:</p> <ul style="list-style-type: none"> ■ You must have the Entitlements Administrator role to create a review cycle setting. See “Predefined roles” on page 80. ■ Create a review cycle setting to monitor the control points over a specific time period. See “Review cycle setting” on page 396. ■ You can create a Recurring or a Non-recurring review cycle. <p>See “Creating a review cycle setting” on page 402.</p>

Table 4-4 Identifying threats in access control *(continued)*

Task	Description
Configure the control point	<p>Go to Manage > Entitlements > Control Points.</p> <p>Consider the following to configure the control points:</p> <ul style="list-style-type: none">■ You must have the Entitlements Administrator role to configure control points. See “Predefined roles” on page 80.■ You configure the control point to associate a data owner and a review cycle to the control point. See “Configuring control points” on page 400.

Table 4-4 Identifying threats in access control (*continued*)

Task	Description
Monitor the control point status throughout the review cycle	<p>Go to Manage > Entitlements > Control Points</p> <p>Before you begin monitoring the control points in the review cycle, it is recommended that you understand the various control point states.</p> <p>See “About the control point status” on page 387.</p> <p>Perform the following tasks in the given order as an Entitlements Administrator:</p> <ul style="list-style-type: none"> ■ Import the entitlements of the control point whenever the control point is in the Entitlement Import Required state. See “Importing the entitlements manually” on page 408. See “Configuring the automatic entitlements import” on page 407. ■ Send an approval request to the data owner <p>The control points are then approved by the data owners or the data owners request changes in the control point entitlements.</p> <p>To know more about the entire approval workflow visit the following link: See “About the entitlements system workflow” on page 383.</p>

Table 4-4 Identifying threats in access control (*continued*)

Task	Description
Generate entitlements report	<p>Go to Reporting > Report Templates</p> <p>You can generate the following types of entitlements reports:</p> <ul style="list-style-type: none">■ Entitlement changes report■ Trustee report■ Effective permissions report■ Simple permissions report <p>See “Predefined Reports and Dashboard descriptions” on page 627.</p>

Managing assets

This chapter includes the following topics:

- [Getting started with the asset system](#)
- [About the Asset System view](#)
- [About the Reconciliation Rules view](#)
- [Concepts in assets](#)
- [Creating reconciliation rules](#)
- [Importing assets](#)
- [Creating asset groups](#)
- [Performing the tasks in the Asset System view](#)
- [Performing the tasks in the Reconciliation Rules view](#)

Getting started with the asset system

To define the known assets that need protection is the first step in the IT process governance. The primary goal of the asset management system is to present a consolidated view of the assets that are present in the organization. The asset system lets you manage the assets in the organization. The system also lets you exchange the context-specific information about the assets so that you can look at your organization from different perspectives. You can use the asset system to manage and monitor the assets that are valuable to your organization.

To understand how the asset system works, review the concepts that you must understand before you begin to use the asset system.

See [“Concepts in assets”](#) on page 200.

Table 5-1 Primary tasks to get started with asset system

Task	Description
Registering the Data Processing Service	<p>Before the Application Server can use a newly installed Data Processing Service (DPS), you must register the DPS with the Application Server. When you register the DPS, you also assign the DPS to a site and specify the DPS roles. Where appropriate, specify data types to collect.</p> <p>See “ Registering the Data Processing Service” on page 98.</p>
Configuring the data collectors	<p>You must configure the data collector for the platform for which you want to import the assets.</p>
Configure Common platform to import common fields	<p>In Control Compliance Suite, the data for the common fields of an asset type is not collected from the default data collector.</p> <p>See “About the working of default data collectors in asset import” on page 268.</p> <p>To collect data for the common fields, you must manually create a CSV file and define all the common fields in a specific format.</p> <p>See “Creating a CSV file for custom application” on page 295.</p> <p>If you do not have the Common platform configured, the assets are still imported into the asset system without the common fields data.</p> <p>See “Configuring Common platform through CSV settings” on page 271.</p>

The asset system workflow starts with the creation of reconciliation rules. The asset system workflow ends with the evaluation results of the assets that are a part of the asset system. Asset import is the most crucial step in the asset system. You must have reconciliation rules, tags, and the asset groups before you import the assets.

Table 5-2 Asset system tasks

Task	Description
Import the primary assets for the first time with the predefined reconciliation rules	<p>The day zero asset import is the most important step to get started with the asset system.</p> <p>The asset system facilitates the process of the day zero asset import with predefined rules. The day zero asset import implies the import of primary assets into the asset system.</p> <p>See “Primary and secondary assets” on page 228.</p> <p>See “About the first time asset import” on page 262.</p> <p>See “Importing the assets for the first time” on page 265.</p>
Create reconciliation rules for further asset imports	<p>If you have imported assets without the common fields data, you can set the values of the common fields with the reconciliation rules.</p> <p>See “Using a Pre rule to set the values of the common fields” on page 256.</p> <p>See “Creating reconciliation rules” on page 253.</p>
Apply tags to the assets	<p>You can now create tags to assign to the assets. You can create tags on the basis of Department, Confidentiality, Location, and so on.</p> <p>See “Asset tagging” on page 246.</p> <p>See “Applying a tag to the asset” on page 326.</p>
Create asset groups	<p>After you create the tags, you can group the assets on the basis of the tags or any other logical grouping.</p> <p>You can create static and dynamic asset groups or use the predefined asset groups.</p> <p>See “Creating asset groups” on page 299.</p>

Table 5-2 Asset system tasks (continued)

Task	Description
Import the secondary assets	<p>After you import the primary assets, you can now proceed with the further asset imports with the reconciliation rules and asset groups.</p> <p>See “Working with asset import scenarios” on page 267.</p>

About the Asset System view

The Asset System view lets you manage the assets in the Control Compliance Suite.

You can access the Asset System view from Manage > Assets > Asset System.

The Asset System view contains the following panes:

Tree pane	<p>This pane appears on the left side of the console window under the navigation bar.</p> <p>This pane displays the assets under the Asset System node. Under the Asset System node, you can view the Asset Group Templates that contain the predefined asset groups.</p> <p>See “Creating the asset folders” on page 305.</p>
Filter by pane	<p>This pane appears in the lower left side of the console window under the tree pane.</p> <p>You can use the following filters in the asset management view:</p> <ul style="list-style-type: none">■ Select tags■ Risk Ratings■ Created Between■ Modified Between <p>See “Using the Filter by pane in the Asset System view” on page 327.</p>
Taskbar	<p>The taskbar appears across the top of the tree pane and the table pane in the console window.</p> <p>See “Performing the tasks in the Asset System view” on page 305.</p>

Table pane

The table pane appears in the right side of the console window under the taskbar .

This pane displays the assets and the asset groups.

On the top right corner of the table pane, the active assets are displayed.

See [“Active assets”](#) on page 253.

Details pane

The details pane appears in the lower-right side of the console window under the table pane.

This pane displays the details of the asset or the asset group that is selected in the tables pane.

See [“Viewing asset information in the details pane”](#) on page 319.

The taskbar of the Asset System view is divided into the following major tasks:

Asset Group Tasks

You can perform the following asset group tasks:

- Create Asset Group
 See [“Creating a dynamic asset group”](#) on page 300.
 See [“Creating a static asset group”](#) on page 302.
- Edit Asset Group
- See [“Editing an asset group”](#) on page 306.
- Copy Asset Group
 See [“Copying and pasting an asset group”](#) on page 307.
- Paste Asset Group
 See [“Copying and pasting an asset group”](#) on page 307.
- Rename Asset Group

Global Tasks

You can perform the following global tasks:

- Mark as Control Point
See [“Marking an asset as a control point”](#) on page 398.
- Request Exception
See [“Requesting an exception”](#) on page 436.
- Set up Data Collection
See [“Setting up a data collection job from the Assets view”](#) on page 310.
- Run Evaluation
See [“Running an evaluation job from the Asset System view”](#) on page 311.
- Run Collection-Evaluation-Reporting
See [“Running a collection-evaluation-reporting job from the Asset System view”](#) on page 314.

Asset Tasks

You can perform the following asset tasks:

- Import Assets
See [“Working with asset import scenarios”](#) on page 267.
- Edit Assets
See [“Editing assets”](#) on page 317.
- Move Assets
See [“Moving an asset”](#) on page 318.
- Export CSV Headers
See [“Exporting CSV headers”](#) on page 319.

Common Tasks

You can perform the following common tasks:

- Delete
See [“Deleting assets or asset groups”](#) on page 319.
- View permissions

About the Reconciliation Rules view

The Reconciliation Rules view lets you manage the rules in the Control Compliance Suite.

You can access the Reconciliation Rules view from Manage > Assets > Reconciliation Rules.

Tree pane	<p>This pane appears on the left side of the console window under the navigation bar.</p> <p>This pane displays the reconciliation rules under the Reconciliation Rules node. Under the Reconciliation Rules node, you can view the predefined Rules.</p>
Filter by pane	<p>This pane appears in the lower left side of the console window under the tree pane.</p> <p>You can use the following filters in the rules management view:</p> <ul style="list-style-type: none"> ■ Asset Type ■ Rule Type
Taskbar	<p>The taskbar appears across the top of the tree pane and the table pane in the console window.</p> <p>See “Performing the tasks in the Reconciliation Rules view” on page 330.</p>
Table pane	<p>The table pane appears in the right side of the console window under the taskbar .</p> <p>This pane displays the rule types and the rules.</p>
Details pane	<p>The details pane appears in the lower-right side of the console window under the table pane.</p> <p>This pane displays the details of the rule that is selected in the tables pane.</p>

The rules management view lets you perform the following tasks:

- Create Rule
 - See [“Creating reconciliation rules using the manual review”](#) on page 254.
 - See [“Creating reconciliation rules without manual review”](#) on page 253.
- Moving Rule
 - See [“Moving a reconciliation rule”](#) on page 331.
- Editing Rule

See [“Editing a reconciliation rule”](#) on page 330.

- Copy Rule
See [“Copying and pasting a reconciliation rule”](#) on page 331.
- Paste Rule
See [“Copying and pasting a reconciliation rule”](#) on page 331.
- Delete Rule
See [“Deleting a reconciliation rule”](#) on page 331.
- Mark as Default Rule
- Unmark as Default Rule

Concepts in assets

To understand the workflow of managing the assets in Control Compliance Suite, you need to understand some of the concepts in the assets.

The following are the concepts of the assets:

- About assets
See [“About assets”](#) on page 201.
- Site
See [“Site as scope in asset import”](#) on page 202.
- Asset folder hierarchy
See [“Asset folder hierarchy”](#) on page 202.
- Predefined platforms
See [“Predefined platforms”](#) on page 203.
- Asset types
See [“Asset types”](#) on page 203.
- Primary and secondary assets
See [“Primary and secondary assets”](#) on page 228.
- Reconciliation rules
See [“Reconciliation rules and rule types”](#) on page 229.
- Asset tagging
See [“Asset tagging”](#) on page 246.
- Asset import
See [“Asset import”](#) on page 240.
- Asset groups
See [“Asset groups”](#) on page 247.

- Active assets
See “Active assets” on page 253.

About assets

With reference to Control Compliance Suite, an asset is defined as an object in the organization that has certain properties.

Table 5-3 Features of assets

Feature	Description
Value	An object must have a value in the organization to become an asset. Without a value, the object is a liability.
Owner	The owner of the asset carries the responsibility to secure and maintain the value of the asset.
Restricted access	An asset must also have limited access to safeguard its value. Because an asset has value, some benefit can be derived from its use. Any unlimited access that is granted to assets implies zero value.

In a broader perspective, assets fall into the following major non-technical groups:

- | | |
|--------------------|--|
| People assets | ■ Human capital |
| Information assets | <ul style="list-style-type: none"> ■ Financial data ■ HR data ■ Patent records ■ Business plans ■ Disaster recovery plans |
| Physical assets | <ul style="list-style-type: none"> ■ Furniture ■ Office campus |

Control Compliance Suite deals with the technology assets.

Technology assets are important because of the following reasons:

- Technology assets store information.
- Technology assets have role-based access control.
People are granted various levels of authority over these assets.

- Technology assets often control other physical systems.

Primitive technology assets include User accounts, Computers, Printers, Network Infrastructure, and Services. Control Compliance Suite collects data on these primitive assets.

See [“Site as scope in asset import”](#) on page 202.

See [“Asset folder hierarchy”](#) on page 202.

Site as scope in asset import

In the asset system, the sites are used as scopes to limit the number of assets to be imported into the asset system. A site is a default scope for asset import for the first time. When you import the assets for the first time, you must select the Site to which the Data Processing Server is associated, as a scope. The asset import job collects the assets from the configured sites.

See [“Configuring sites”](#) on page 111.

Asset folder hierarchy

When you install Control Compliance Suite, a default hierarchy structure is created to store objects in the CCS directory. All objects are stored under the root folder. The root folder holds subfolders for each object type. With the individual object type folder, you can create a hierarchical structure that best suits your organizational needs to store objects.

In case of the asset system, the objects that are stored in the CCS directory include the assets and the reconciliation rules.

After installation, the following hierarchical structure is created for storing the assets:

- Asset System
 - Asset Group templates

After installation, the following hierarchical structure is created for storing the reconciliation rules:

- Reconciliation Rules
 - Predefined Reconciliation Rules

See [“About organizing objects in the directory”](#) on page 32.

Predefined platforms

Control Compliance Suite lets you collect the asset data in the form of categories that are specific to the predefined platforms.

Control Compliance Suite supports the data collection, analysis, and reporting on the following platforms:

- Enterprise Security Manager
- Oracle
- SQL
- UNIX
- Windows

Each predefined platform has certain primary entities. Control Compliance Suite by default supports some of the primary entities of the predefined platforms as asset types. In addition to the primary entities that the predefined platforms support as asset types, you can create your own asset types with other primary entities.

The predefined platforms are not extensible.

See [“About platforms”](#) on page 356.

See [“About entities”](#) on page 356.

See [“Predefined asset types”](#) on page 204.

See [“Probable asset types”](#) on page 227.

Asset types

An asset type is an entity of the platform that the asset system supports for the asset import. For example, all directories of the Windows platform can constitute to be the assets. You can categorize the assets into a single category of an asset type called Windows directory.

By default, the asset system supports certain entities of the predefined platforms as asset types. You can perform the asset import operation with the predefined asset types without any customization.

See [“Predefined asset types”](#) on page 204.

The asset system does not support certain entities of the predefined platforms by default. But, the asset system makes these entities available for customization to create custom asset types. Probable asset types are created from the entities that the Control Compliance Suite does not support by default as asset types.

See [“Probable asset types”](#) on page 227.

The asset system lets you create an entirely new platform and define the entity that the new platform supports. You can use these newly created entity and create a new asset type that is based on the custom entity. The asset types that are created from the custom platform and custom entities are custom asset types.

See [“Custom asset types”](#) on page 228.

Predefined asset types

Control Compliance Suite lets you collect the asset data in the form of categories that are specific to the supported platforms. Control Compliance Suite supports the data collection, analysis, and reporting on the ESM, Windows, UNIX, Oracle, and SQL platforms.

To gather more specific data for the purpose of monitoring, Control Compliance Suite lets you select the asset types that belong to the supported platforms.

Predefined asset types are based on the entities of the predefined platforms.

See [“Predefined platforms”](#) on page 203.

In Control Compliance Suite, a platform is defined to be the category to which a group of entities belong.

See [“About platforms”](#) on page 356.

A group of fields that define the common functions of the network element form an entity.

See [“About entities”](#) on page 356.

Each asset type has some specific primary, mandatory, and optional fields.

The predefined asset types that are associated with the predefined platforms are as follows:

See [“Probable asset types”](#) on page 227.

See [“Custom asset types”](#) on page 228.

Fields for ESM Agent

The Control Compliance Suite lets you create your own asset type schema and extend the existing asset type schema to manage your assets.

[Table 5-4](#) lists the primary, mandatory, and optional fields for the ESM agents asset type.

Table 5-4 Fields for ESM Agent

Display name	Description	Type	Is single valued?	Field type
Registered Name	The name that is used to register agent with ESM manager	String	True	Primary
OS details	Operating system details	String	True	Mandatory
OS Version	Operating system version	String	True	Mandatory
Platform	Operating system platform	String	True	Mandatory
ESM Manager	Associated ESM Manger	String	True	Mandatory
ESM SU Version	Security Update version on the ESM agent	String	True	Optional
ESM Domains	The ESM domains to which the agent belongs	String	False	Optional
ESM version	ESM version that is installed on the agent	String	True	Optional
FQDN	Fully Qualified Domain Name of the ESM agent	String	True	Optional
Host Name	Agent's NETBIOS or Host name	String	True	Optional
IP Address	IP Address of the ESM agent computer	String	False	Optional

Fields for Oracle Configured Databases

Table 5-5 Oracle Configured Databases

Display name	Description	Type	Single valued or multi valued	Field type
Domain/Workgroup Name	This field returns the domain or the workgroup name of the computer that hosts the Oracle Server.	String	Single valued	Primary
Server Name (Instance)	This field returns the name of the Oracle Server instance, not the name of the host.	String	Single valued	Primary
Host Name (Node)	This field returns the name of the Windows NT server that hosts the instance of Oracle Server.	String	Single valued	Primary
Database Name	This field returns the name of the database.	String	Single valued	Primary
Windows Domain Name or Unix IP Address	This field reports Domain Name for the Windows server and IP Address for a Unix server.	String	Single valued	Primary
Server Name	This field reports the name of the Oracle server	String	Single valued	Primary

Table 5-5 Oracle Configured Databases (*continued*)

Display name	Description	Type	Single valued or multi valued	Field type
Server NetBIOS Name	This field reports the NetBIOS name of the Oracle server	String	Single valued	Primary
OS Type	This field reports the Operating System type of the Oracle server.	String	Single valued	Mandatory

Fields for Oracle Configured Servers

Table 5-6 Fields for Oracle Configured Servers

Display name	Description	Type	Single valued or multi valued	Field type
Server Name	This field reports the name of the Oracle server.	String	Single valued	Primary
Server NetBIOS Name	This field reports the NetBIOS name of the Oracle server.	String	Single valued	Primary
Windows Domain Name or UNIX IP Address	This field reports Domain Name for Windows server and IP Address for a UNIX Server	String	Single valued	Primary

Table 5-6 Fields for Oracle Configured Servers (*continued*)

Display name	Description	Type	Single valued or multi valued	Field type
OS Type	This field reports the Operating System type of the Oracle server	String	Single valued	Mandatory

Fields for SQL Databases

Table 5-7 Fields for SQL Database

Display name	Description	Type	Single valued or multi valued	Field type
Domain/Workgroup Name	This field returns the domain or the workgroup name of the computer that hosts the SQL Server.	String	Single valued	Primary
Server Name (Instance)	This field returns the name of the SQL Server instance, not the name of the host.	String	Single valued	Primary
Host Name (Node)	This field returns the name of the Windows NT server that hosts the instance of SQL Server.	String	Single valued	Primary
Database Name	This field returns the name of the database.	String	Single valued	Primary

Table 5-7 Fields for SQL Database (*continued*)

Display name	Description	Type	Single valued or multi valued	Field type
Owner	The owner of the SQL server element.	String	Single valued	Optional

Fields for SQL Server

Table 5-8 Fields for SQL Server

Display name	Description	Type	Single valued or multi valued	Field type
Domain/Workgroup Name	This field returns the domain or the workgroup name of the computer that hosts the SQL Server.	String	Single valued	Primary
Server Name (Instance)	This field returns the name of the SQL Server instance, not the name of the host.	String	Single valued	Primary
Host Name (Node)	This field returns the name of the Windows NT server that hosts the instance of SQL Server.	String	Single valued	Primary
Major Version	The major version of the SQL server instance.	Integer	Single valued	Mandatory
Minor Version	The minor version of the SQL server instance.	Integer	Single valued	Optional

Table 5-8 Fields for SQL Server (continued)

Display name	Description	Type	Single valued or multi valued	Field type
Login Mode	The default login mode for the server. The valid values are Integrated, Mixed, Normal and Unknown	String	Single valued	Optional
Operating System	The underlying operating system.	String	Single valued	Optional
Platform	The platform.	String	Single valued	Optional
Product Level	The SQL Server product level. The possible values include B1 and RTM. This field is applicable only for SQL server 2000 and above.	String	Single valued	Optional
Product Version	The SQL server product version.	String	Single valued	Optional
Version String	The complete version of the SQL server product instance.	String	Single valued	Optional

Fields for UNIX File

Table 5-9 Fields for UNIX File

Display name	Description	Type	Single valued or multi valued	Field type
Machine Name	This field returns the name of the target.	String	Single valued	Primary
Host IP Address	This field returns the host IP address.	String	Single valued	Primary
File Name (With Path)	This field returns the file name (with path).	String	Single valued	Primary

Fields for UNIX Group

Table 5-10 Fields for UNIX Group

Display name	Description	Type	Single valued or multi valued	Field type
Machine Name	This field returns the name of the computer that hosts the group.	String	Single valued	Primary
IP Address	This field returns the IP address used to connect to the target.	String	Single valued	Primary
Group Database	This field returns the database from where the group information is retrieved.	String	Single valued	Primary

Table 5-10 Fields for UNIX Group *(continued)*

Display name	Description	Type	Single valued or multi valued	Field type
Group Name	This field returns the name of the group.	String	Single valued	Primary

Fields for UNIX Machine

Table 5-11 Fields for UNIX Machine

Display name	Description	Type	Single valued or multi valued	Field type
Machine Name	This field returns the name of the target.	String	Single valued	Primary
IP Address	This field returns the IP address that is used to connect to the target.	String	Single valued	Primary
Open Distribution Field	This field returns the operating distribution field that is running on this target. For example: Red Hat Linux i686	String	Single valued	Mandatory
Operating System	This field returns the operating system that is running on this target. For example: Linux, SunOS	String	Single valued	Mandatory

Table 5-11 Fields for UNIX Machine *(continued)*

Display name	Description	Type	Single valued or multi valued	Field type
Operating System Version	This field returns the operating system version that is running on this target.	String	Single valued	Mandatory

Fields for Windows Domain

Table 5-12 Fields for Windows Domain

Display name	Description	Type	Single valued or multi valued	Field type
Domain Name	This field returns the Pre-Windows 2000 name of the domain	String	Single valued	Primary
Domain Full Name	This field contains the distinguished name of the reported domain. This field returns [N/A] for NT4 domains.	String	Single valued	Optional

Table 5-12 Fields for Windows Domain (continued)

Display name	Description	Type	Single valued or multi valued	Field type
Domain Mode	This field returns the mode in which the domain is running. For Windows NT 4.0 domains the field returns 'Pre-Windows 2000 mode'. For the domains that are running in Mixed mode the field returns Mixed Mode otherwise Native Mode. This field is only accurate when the Query Engine is installed on a Windows 2000 or later OS.	Integer	Single valued	Optional
Domain Type	This field returns the type of the operating system that is installed on the Primary Domain Controller.	Integer	Single valued	Optional
DNS Forest Name	This field returns the name of the forest (in the DNS format) where the domain resides.	String	Single valued	Optional

Table 5-12 Fields for Windows Domain (*continued*)

Display name	Description	Type	Single valued or multi valued	Field type
Description	This field returns the description text that is associated with the Domain from the Active Directory. This field returns N/A for NT4 domains.	String	Single valued	Optional
Domain Functional Level	This field returns the domain functionality level. The domain functionality activates the features that affect the whole domain and that domain only.	Integer	Single valued	Optional
Forest Functional Level	This fields returns the forest functionality level. The forest functionality level activates the features across all the domains in your forest.	Integer	Single valued	Optional

Fields for Windows Directory

Table 5-13 Fields for Windows Directory

Display name	Description	Type	Single valued or multi valued	Field type
Domain/Workgroup Name	This field returns the domain or the workgroup membership (which ever is appropriate for that computer) of the computer that contains the directory. This field obtains the name from the Query Engine's reporting domain settings. Use the field 'domain Workgroup Name (Machine Setting)' to determine the domain or workgroup that the computer is a member of.	String	Single valued	Primary
Machine Name	This field returns the name of the directory's computer.	String	Single valued	Primary
Directory Name	This field returns the full path name of the directory.	String	Single valued	Primary

Table 5-13 Fields for Windows Directory (*continued*)

Display name	Description	Type	Single valued or multi valued	Field type
Owner	This field returns the name of the account that currently owns the directory. The owner has the ability to change the permission assignments to the directory.	String	Single valued	Optional
Member of Domain	This field returns True, if the computer that contains the directory is the member of the domain	Boolean	Single valued	Optional

Fields for Windows File

Table 5-14 Fields for Windows File

Display name	Description	Type	Single valued or multi valued	Field type
Domain/Workgroup Name	This field returns the domain or the workgroup membership (which ever is appropriate for that computer) of the computer that contains the directory. This field obtains the name from the Query Engine's reporting domain settings. Use the field 'Domain / Workgroup Name (Machine Setting)' to determine the domain or workgroup that the machine is a member of.	String	Single valued	Primary
Machine Name	This field returns the name of the machine that contains the file.	String	Single valued	Primary
File Name (With Path)	This field returns the full path name of the file.	String	Single valued	Primary

Table 5-14 Fields for Windows File (*continued*)

Display name	Description	Type	Single valued or multi valued	Field type
Last Modified Date/Time	This field returns the date and time the file was last modified.	DateTime	Single valued	Optional
Owner	This field returns the name of the account that currently owns the file. The owner has the ability to change permission assignments for the file.	String	Single valued	Optional
Size (MB)	This field returns the logical size of the file in megabytes.	Double	Single valued	Optional
Member of Domain	This field returns true if the machine that contains the file is a member of a domain.	Boolean	Single valued	Optional

Fields for Windows Group

Table 5-15 Fields for Windows Group

Display name	Description	Type	Single valued or multi valued	Field type
Domain/Workgroup Name	This field returns the domain or workgroup membership (which ever is appropriate for that machine) of the machine containing the directory. This field obtains the name from the Query Engine's reporting domain settings. Use the field 'Domain / Workgroup Name (Machine Setting)' to determine the domain or workgroup that the machine is a member of.	String	Single valued	Primary
Group Name (Pre-Windows 2000) -	This field returns the Pre-Windows 2000 name of the group object.	String	Single valued	Primary
Machine Name	This field returns the name of the machine that contains the file.	String	Single valued	Primary

Table 5-15 Fields for Windows Group (*continued*)

Display name	Description	Type	Single valued or multi valued	Field type
Group Name	This field returns the name of the group object.	String	Single valued	Primary
Group Type	This field returns group type, i.e. domain local, domain global, universal local.	Integer	Single valued	Optional
Owner	This field returns the name of the account that currently owns the file. The owner has the ability to change permission assignments for the file.	String	Single valued	Optional
Host Machine Member of Domain	This field returns true if the group is owned by a machine that is a member of a domain.	Boolean	Single valued	Optional

Fields for Windows Machine

Table 5-16 Fields for Windows Machine

Display name	Description	Type	Single valued or multi valued	Field type
Domain/Workgroup Name	This field returns the domain or workgroup membership (which ever is appropriate for that machine) of the machine containing the directory. This field obtains the name from the Query Engine's reporting domain settings. Use the field 'Domain / Workgroup Name (Machine Setting)' to determine the domain or workgroup that the machine is a member of.	String	Single valued	Primary
Machine Name	This field returns the name of the machine that contains the file.	String	Single valued	Primary

Table 5-16 Fields for Windows Machine (*continued*)

Display name	Description	Type	Single valued or multi valued	Field type
OS Major Version Number	This field returns the major version number of the machine's NT operating system. Ex. For NT 3.51, the major version is 3. The "OS Major Version Number (Browser)" field is a faster method of retrieving the same information, but avoids directly accessing the machine by getting the data from the browser if the browser is available.	Integer	Single valued	Mandatory

Table 5-16 Fields for Windows Machine (continued)

Display name	Description	Type	Single valued or multi valued	Field type
OS Minor Version Number	This field returns the minor version number of the machine's NT operating system. Ex. For NT 3.51, the minor version is 51. The "OS Minor Version Number (Browser)" field is a faster method of retrieving the same information, but avoids directly accessing the machine by getting the data from the browser if the browser is available/	Integer	Single valued	Mandatory
OS Type	This field returns machine's Windows operating system type. It also indicates if the machine has Terminal Services capability.	String	Single valued	Mandatory

Table 5-16 Fields for Windows Machine (*continued*)

Display name	Description	Type	Single valued or multi valued	Field type
Machine Is Server	This field returns true if the machine is running the NT Server operating system. The "Machine Is Server? (Browser)" field is a faster method of retrieving the same information, but avoids directly accessing the machine by getting the data from the browser if the browser is available.	Boolean	Single valued	Mandatory

Table 5-16 Fields for Windows Machine (*continued*)

Display name	Description	Type	Single valued or multi valued	Field type
Machine Is BDC	This field returns true if the machine is a backup domain controller. The "Machine Is BDC? (Browser)" field is a faster method of retrieving the same information, but avoids directly accessing the machine by getting the data from the browser if the browser is available.	Boolean	Single valued	Mandatory
Machine Is PDC	This field returns true if the machine is a primary domain controller. The "Machine Is PDC? (Browser)" field is a faster method of retrieving the same information, but avoids directly accessing the machine by getting the data from the browser if the browser is available.	Boolean	Single valued	Mandatory

Table 5-16 Fields for Windows Machine (*continued*)

Display name	Description	Type	Single valued or multi valued	Field type
Member of Domain	This field returns true if the machine is a member of a domain.	Boolean	Single valued	Optional

Probable asset types

The probable asset types are the entities for the predefined platforms that the asset system does not support by default.

The Control Compliance Suite supports certain entities of the predefined platforms to be the asset types. The predefined asset types are the entities of the predefined platforms.

See [“Predefined asset types”](#) on page 204.

In Control Compliance Suite, a platform is defined to be the category to which a group of entities belong.

See [“Predefined platforms”](#) on page 203.

See [“About platforms”](#) on page 356.

A group of fields that define the common functions of the network element form an entity.

See [“About entities”](#) on page 356.

In addition to the predefined asset types, Control Compliance Suite provides certain probable asset types. You can use the Schema Manager view and create your own asset type with the entities that are not supported by default.

See [“About the Schema Manager view”](#) on page 346.

The probable asset types for the SQL platform are as follows:

- Stored procedure
- Database Users

The probable asset types for the UNIX platform are as follows:

- User

The probable asset types for the Windows platform are as follows:

- IIS virtual directories

- IIS Web sites
- Registry
- Service

See [“Custom asset types”](#) on page 228.

Custom asset types

Control Compliance Suite lets you create custom asset types from the custom platforms and custom entities that you can create from the Schema Manager view.

See [“About the entity schema ”](#) on page 347.

You can import the assets from the custom asset types in the same way as you import the assets from any other asset type.

Asset types are based on the entities of the platform. In Control Compliance Suite, a platform is defined to be the category to which a group of entities belong. A group of fields that define the common functions of the network element form an entity.

See [“About platforms”](#) on page 356.

See [“About entities”](#) on page 356.

When you create your own platform and define fields for the platform to create an entity, you can define an asset type also. The custom asset type imports the data of the fields that are defined in the custom entity.

See [“Creating a new asset type”](#) on page 348.

See [“Extending an existing asset type”](#) on page 351.

Primary and secondary assets

Primary assets are the assets that should be imported first to import certain other kind of assets. Primary assets act as the default scope to import the other asset types. The assets that are imported after the primary assets are the secondary assets. Primary assets constitute the super-set of the secondary assets.

For example, in the Control Compliance Suite, you must import the Windows Domain before you import the Windows Machines. In this example, Windows Domain is the primary asset and the Windows Machine is the secondary asset. In the asset system Windows Domain is the default scope for the Windows Machines.

See [“Default scope and supported scope”](#) on page 289.

In the asset system, Site is the primary asset for all the asset types. When you import the assets of any asset type, you can use the Site as the scope. But, it is not

recommended to use the Site as a scope even if it is a supported scope for all the asset types. You are recommended to use the default scopes.

Using the default scope implies the import of the primary assets before the secondary assets.

See [“About scopes in asset import”](#) on page 287.

Table 5-17 Predefined asset types and primary assets

Asset type	Primary asset
ESM Agents	Site ESM Agents
Oracle Configured Databases	Site
Oracle Configured Servers	Site
SQL Databases	SQL Server
SQL Server	Site
UNIX Machine	Site
UNIX Group	UNIX Machine
UNIX File	UNIX Machine
Windows Domain	Site
Windows Machine	Windows Domain
Windows Group	Windows Machine
Windows Directory	Windows Machine
Windows File	Windows Machine

The primary asset for the SQL asset types is SQL Server.

The primary asset for the UNIX asset types is UNIX Machine.

The primary asset for the Windows asset types is Windows Domain.

Reconciliation rules and rule types

The asset reconciliation helps you organize the assets that already exist in the asset store in a logical hierarchy. Reconciliation provides you the flexibility to manage the asset records conditionally when the records get into the assets system. The reconciliation rule lets the administrator manage the asset information when

imported into the system. A reconciliation rule consists of a condition and an action. A set of actions is executed when the imported asset satisfies the specified set of conditions.

Reconciliation is based on the priority. A reconciliation rule that is enabled and is at the top in order, takes highest priority. If the rule is not satisfied, then the second rule takes priority with succeeding rules, if necessary. If an asset does not satisfy any reconciliation rule, the asset is forwarded to the manual review store. Control Compliance Suite performs the asset reconciliation that is based on some rules. Every rule that you create must be compliant with one of the rule-types that the asset system defines. All the reconciliation rules are displayed in Manage > Assets > Reconciliation Rules view.

Table 5-18 Types of reconciliation rules

Rule type	Rule description
Pre rule See “Pre rule” on page 231.	<p>A Pre rule is executed on the assets that are in the process of import before the assets are brought into the assets system.</p> <p>The Pre rule lets you set a value for a particular asset field. The Pre rule also lets you discard the asset.</p>
Add rule See “Add rule” on page 233.	<p>An Add rule is executed to add the assets that are in the process of import to the asset system</p> <p>The Add rule lets you add new assets to the asset system at a specific location. The Add rule also lets you add assets to the manual review store.</p>

Table 5-18 Types of reconciliation rules (*continued*)

Rule type	Rule description
Update rule See “Update rule” on page 234.	An Update rule is applied on the existing assets to update their fields with the values of the assets that in the process of import. The update rule updates the assets that already exist in the system. The update rule also lets you add assets to the manual review store.
Post rule See “Post rule” on page 237.	A Post rule is executed at the end in the order of the reconciliation rules. The Post rule is executed only for the imported asset records for which there is a corresponding addition or update in the asset system.

Note: Every asset import job must have at least one add or update rule.

In addition to the rules that you can create, Control Compliance Suite also provides predefined rules. You can use any of the predefined rules to import the assets for the very first time.

See [“Predefined reconciliation rules”](#) on page 238.

See [“Creating reconciliation rules without manual review”](#) on page 253.

See [“Creating reconciliation rules using the manual review”](#) on page 254.

Pre rule

A Pre rule is executed on the assets being imported before the assets are brought into the assets system.

[Table 5-19](#) are as follows:

Table 5-19 Conditions for Pre rule

Condition	Description
Always	The specified action is performed on the assets every time.
If an asset being imported does not exist in the asset system	The action is performed only if the asset that is being imported does not exist already in the asset system.
If an asset being imported exists in the asset system	The action is performed only if the asset that is being imported already exists in the asset system.
If field of an asset being imported is not set	The action is performed only if the asset field is not set.
If field of an asset being imported has a relation with a specified value	<p>The action is performed only if the field of the asset that is being imported has a specified relation with the specified value</p> <p>For example, <field> <operator><value> <Asset Custodian><equals><ABC></p>

[Table 5-20](#) are as follows:

Table 5-20 Actions for Pre rule

Action	Description
Discard an asset being imported	<p>Ignores the asset that is being imported.</p> <p>The asset is not added to the asset system if no Add Rule is specified.</p>

Table 5-20 Actions for Pre rule (*continued*)

Action	Description
Set the field value of an asset being imported as specified	<p>Sets the field value of the asset that is being imported as the value that you specify.</p> <p>Lets you select the asset field for which you want to set the value. You can also specify the value that you want to set.</p> <p>If you select Asset Tags as the field, you can also select the Tag Set Options that work as follows:</p> <ul style="list-style-type: none"> ■ Clear Removes all the tags from the asset before the asset is imported to the asset system. ■ Append Adds the tag to the asset alongwith the existing tags before the asset is imported to the asset system. This option is selected by default. If you do not select any tag set option, the new tag is appended to the asset. ■ Overwrite Replaces the existing tag with the new tag.

Example for the Pre rule:

If an asset being imported exists in the asset system THEN Set the field value of an asset being imported as specified.

This rule condition checks if the asset to be imported exists in the system. If the asset already exists, it sets the value of the selected field for that asset according to the given value.

See [“Using a Pre rule to set the values of the common fields”](#) on page 256.

Add rule

The Add rule is executed to add the assets being imported to the asset system.

[Table 5-21](#) are as follows:

Table 5-21 Conditions for Add rule

Condition	Description
If an asset being imported does not exist in the asset system	The action is performed only if the asset that is being imported does not exist already in the asset system.
If field of an asset being imported has a relation with a specified value	<div>The action is performed only if the field of the asset that is being imported has a specified relation with the specified value</div> <div>For example, <field> <operator><value></div> <div><Asset Custodian><equals><ABC></div>

Table 5-22 are as follows:

Table 5-22 Actions for Add rule

Action	Description
Add an asset being imported to the specified folder	Adds the asset that is being imported to the folder that you specify.
Add to manual review store	<div>Adds the asset to the manual review store</div> <div>See “Manual review” on page 246.</div>

Example for the Add rule:

If field of an asset being imported has a relation with a specified value THEN Add an asset being imported to the specified folder.

This rule condition checks the value of the selected field of the asset being imported with the existing asset. If the value matches the existing asset, it adds the asset to the specified folder.

See “[Using an Add rule to dynamically create asset folders](#)” on page 257.

Update rule

Update rule is applied on the existing assets to update their fields with the values of the assets being imported.

Table 5-23 are as follows:

Table 5-23 Conditions for Update rule

Condition	Description
If an asset being imported exists in the asset system	The action is performed only if the asset that is being imported already exists in the asset system.
If an existing asset field has a relation with a specified value	<p>The action is performed if the existing asset field has a specified relation with the specified value</p> <p>For example, <imported asset field> <operator> <value></p>
If field of an asset being imported has a relation with a specified value	<p>The action is performed only if the field of the asset that is being imported has a specified relation with the specified value</p> <p>For example, <field> <operator> <value></p> <p><Asset Custodian><equals><ABC></p>
If field of an asset being imported has a relation with an existing asset field	<p>The action is performed only if the field of an asset that is being imported has a specified relation with the field of an existing asset.</p> <p>For example, <current asset field><operator><imported asset field></p> <p><Asset Custodian><equals><Asset Owner></p>

[Table 5-24](#) are as follows:

Table 5-24 Actions for Update rule

Update rule- action	Description
Set the field value of an existing asset as specified	<p>Sets the field value of an existing asset as that you specify.</p> <p>Lets you select the asset field for which you want to set the value. You can also specify the value that you want to set.</p> <p>If you select Asset Tags as the field, you can also select the Tag Set Options that work as follows:</p> <ul style="list-style-type: none">■ Clear Removes all the tags from the asset before the asset is imported to the asset system.■ Append Adds the tag to the asset along with the existing tags before the asset is imported to the asset system. This option is selected by default. If you do not select any tag set option, the new tag is appended to the asset.■ Overwrite Replaces the existing tag with the new tag.
Update specified fields of an existing asset with the fields of the asset being imported	<p>Replaces the values of the selected fields of an existing asset with the values of the fields of the asset that is being imported.</p> <p>Note: This action has a different behavior in case you choose to update the tags of an asset. This action adds the new tags of an asset being imported to the tags of the existing asset. The existing tags remain intact and do not get overwritten.</p>
Add to manual review store	<p>Adds the asset to the manual review store.</p> <p>See “Manual review” on page 246.</p>

Examples for Update rule:

If field of an asset being imported has a relation with a specified value THEN
Update specified fields of an existing asset with the fields of the asset being imported.

This condition updates the values of the assets that are present in the asset system.
See [“Using an Update rule to update the existing field values”](#) on page 258.

Post rule

The Post rule is executed at the end in the order of the reconciliation rules.

[Table 5-25](#) are as follows:

Table 5-25 Conditions for Post rule

Condition	Description
If an asset being imported exists in the asset system	The action is performed only if the asset that is being imported already exists in the asset system.
If an asset being imported is added in the asset system	The action is performed only if the asset that is being imported is added in the asset system.
If an asset being imported is updated in the asset system	The action is performed only if the asset that is being imported is updated in the Asset System
If an existing asset field has a relation with the specified value	The action is performed if the field of the existing asset has a specified relation with the specified value For example, <imported asset field> <operator> <value>
If field of an asset being imported has a relation with a specified value	The action is performed only if the field of the asset that is being imported has a specified relation with the specified value For example, <field> <operator><value> <Asset Custodian><equals><ABC>

Table 5-25 Conditions for Post rule *(continued)*

Condition	Description
If field of an asset being imported has a relation with an existing asset field	<p>The action is performed only if the field of an asset that is being imported has a specified relation with the field of an existing asset.</p> <p>For example, <current asset field><operator><imported asset field></p> <p><Asset Custodian><equals><Asset Owner></p>

[Table 5-26](#) are as follows:

Table 5-26 Actions for Post rule

Action	Description
Move the existing asset to the specified folder	Moves the existing asset from its current location to the specified location in the asset system.

Example for Post rule:

IF an asset being imported is updated in the asset system THEN Move the existing asset to the specified folder.

This condition moves the assets that are already present in the asset store to the specified folder.

See [“Using a Post rule to mark the assets as control points”](#) on page 259.

Predefined reconciliation rules

To create an asset import job for the first time, Control Compliance Suite provides predefined rules. You can use the predefined rules for importing the assets for the first time without creating custom reconciliation rules.

See [“Asset folder hierarchy”](#) on page 202.

See [“About organizing objects in the directory”](#) on page 32.

See [“Creating the asset folders”](#) on page 305.

See [“Creating reconciliation rules without manual review”](#) on page 253.

See [“Creating reconciliation rules using the manual review”](#) on page 254.

Asset being imported

The term 'assets being imported' is used with reference to the creation of reconciliation rules. The reconciliation rules are applied on the assets being imported.

An asset being imported is a potential asset, which is yet not a part of the asset system. It is the asset that is collected from the data collector but can only be called the asset when it passes through the reconciliation rules. After the reconciliation rules are applied, the asset to be imported becomes an asset.

For example, consider that you want to add Windows Machines from a specific site as assets to the asset system.

Your rule statement reads as follows:

```
If an asset being imported does not exist in the asset system  
THEN Add an asset being imported to the specified folder
```

In this case, the Windows Machines remain the 'asset being imported' until the rule verifies that the computers are not present in the asset system and adds those into the asset system. The Windows Machines that are already present in the system are not added to the asset system and do not become assets.

Existing assets

The term existing assets is used with reference to the creation of reconciliation rules. The existing assets are the assets that are already a part of the asset system. The existing assets are present in the asset store in the CCS directory.

The objects that are collected from the data collectors are referred to as asset being imported until the reconciliation rules are applied.

See [“Asset being imported”](#) on page 239.

When the rules are applied on the asset being imported, the assets that satisfy the rules criteria become a part of the asset system. These assets are then referred to as the existing assets.

For example, consider that you want to update the values of specific asset fields with the Update rule.

Your rule statement reads as follows:

```
IF an asset being imported exists in the asset system  
THEN Update specified fields of an existing asset with the fields of  
the asset being imported
```

In this case, the rule checks the field values of the existing assets which are the assets that are already in the asset store. If the asset being imported exists in the

asset system, the rule overwrites the values of the existing assets with those of the asset being imported.

Asset import

In the asset system, asset import involves the import of the following data:

- Data for the common fields
Common fields are the fields that are common across all the asset types.
See [“Common fields for all asset types”](#) on page 285.
The data for the common fields is imported from the CSV data collector.
- Data for the asset-specific fields
Asset-specific fields are the fields that are specific to the asset type that you select to import.
See [“Predefined asset types”](#) on page 204.
The data for the asset-specific fields is imported from the default data collector.

Go through the following concepts to perform the asset import more effectively:

- Default data collectors
See [“Default data collectors”](#) on page 240.
- Data collectors and asset types
See [“Data collectors and asset types”](#) on page 241.
- Asset field filters
See [“Examples of asset filters”](#) on page 242.
- Filter statement operators
See [“Filter statement operators”](#) on page 243.
- Asset reconciliation
See [“Asset reconciliation”](#) on page 245.
- Manual review
See [“Manual review”](#) on page 246.

Default data collectors

You can choose to import the assets from the default or the CSV data collector.

The asset system assigns the following default data collectors for various platforms:

Table 5-27 Platform and data collectors

Platform	Data collector
ESM platform	ESM data collector
Oracle platform	Oracle data collector
SQL platform	SQL data collector
UNIX platform	UNIX data collector
Windows platform	Windows data collector
Custom platform	You can use the following data collector for the custom platform: <ul style="list-style-type: none">■ CSV data collector
Common platform The Common platform is the platform that is used to import the common fields across the asset types.	The following data collector can be used to collect the Common fields: <ul style="list-style-type: none">■ CSV data collector

See [“About the working of default data collectors in asset import”](#) on page 268.

Data collectors and asset types

The asset types associated with the available data collectors are as follows:

- CSV
 - SQL Database
 - SQL Server
 - ESM Agent
 - Oracle Configured Databases
 - Oracle Configured Servers
 - UNIX File
 - UNIX Group
 - UNIX Machine
 - Windows Directory
 - Windows Domain
 - Windows File

- Windows Machine
- ESM
 - ESM Agent
- Oracle
 - Oracle Configured Databases
 - Oracle Configured Servers
- SQL
 - SQL Database
 - SQL Server
- UNIX
 - UNIX File
 - UNIX Group
 - UNIX Machine
- Windows
 - Windows Directory
 - Windows Domain
 - Windows File
 - Windows Machine

Examples of asset filters

You create the filter statements that are based on the asset fields when you create an asset group and an asset import job.

In case of creation of an asset import job, you need to create the filters that are based on the asset type that you select.

The following table describes certain filter statements that you can use to import assets under specific scenarios.

Table 5-28 Examples of asset filters

Scenario	Filter statement	Job result
To import assets of the Windows Directory with Machine 1 and Machine 2 as scope	<i>((Root Path EqualTo D: Or Root Path EqualTo C:) and depth GreaterThanOrEqualTo 1) and Is Shared? = True</i>	The job returns all the shared folders under the C:\ and the D:\ drive.
To import the Files and the Directories with name like *Accounting*	<i>(Root Path EqualTo D:\directory and depth GreaterThanOrEqualTo 1) and Directory Name Like %Accounts%</i>	The job returns all the directories and the files that contain Accounting in the name.
To import all the directories and the files "n" level below the directory, D:\DATA	<i>Root Path EqualTo D:\directory and depth GreaterThanOrEqualTo 1</i>	The job returns all the e directories under the D:\ directory as per the available depth.
To import the Windows Directories with Machine 1 and domain as a scope	<i>(Root Path EqualTo D:\directory and depth GreaterThanOrEqualTo 1) and PermissionsDifferentThanParent(include Owner) / (Ignore Owner) EqualTo Different</i>	The job returns all the directories of which the permissions differ from the parent.
To import UNIX Files under the directory, etc and the sub-directories	<i>Filename(With Path) like /etc%</i>	The job returns all the UNIX files under the directory, etc and from under the sub-directories.

Filter statement operators

The filter statement operators are the operators that are used for creating filter statements in the asset import job and the asset groups. These operators are used to make a comparison between the two given values.

Table 5-29 Filter statement operators

Operator Name	Description	Filter Statement examples
Equal To (=)	A must be equal to B	Directory Name EqualTo 'Admin'

Table 5-29 Filter statement operators (*continued*)

Operator Name	Description	Filter Statement examples
NotEqualTo (!=)	A must not be equal to B	Directory Name NotEqualTo 'HR'
Like	The SQL like operator, with same syntax and semantics.	Database Name like DB2
Not Like	The SQL not like operator. Note the space between not and like. Any amount of white space (blanks, tabs, new lines, or carriage returns) is allowed here. The white space is not strictly required, but it is best not to omit it.	Database Name NotLike DB2
Match (=~)	The regular expression matching operator.	Directory Name Match 'CM'
NoMatch (!~)	The negative of the expression matching operator.	Directory Name NotMatch 'CM'
IsNull	The SQL is null operator. A filter statement that uses this operator must not have a value specified. At least one white space character is required between is and null.	Depth IsNull
IsNotNull	The negative of is null. The white space between not and null is not strictly required, but it is best not to omit it.	Depth IsNotNull
Exact	Forces case-sensitive string comparison.	Directory Name Exact 'ERCT'
Inexact	Forces case-insensitive string comparison.	Directory Name Inexact 'ERCT'
Contains (%)	In case of single valued field, value on RHS has to be partially or completely matching with LHS. In case of multi valued field, every value on RHS has to be present on the LHS.	Owner Contains John

Table 5-29 Filter statement operators (*continued*)

Operator Name	Description	Filter Statement examples
ContainsMatch (%~)	In case of single valued field, the regular expression on RHS should match field value on LHS. In case of multi valued field, every regular expression on RHS should match at least one element on LHS.	Owner ContainsMatch John
NotContains (!%)	The negative of the Contains operator.	A NotContains B
NotContainsMatch (!%~)	The negative of the ContainsMatch operator.	A NotContainsMatch B

For example, if you select Description as the field to be used as the filter for the ESM Agent asset type, your filter statement could be as follows:

IF Description <Operator> <Value>

Asset reconciliation

The asset reconciliation helps you organize the assets that already exist in the asset store in a logical hierarchy. Reconciliation provides you the flexibility to manage the asset records conditionally when the records get into the assets system.

A reconciliation rule that you specify in the asset import job decides the action that should be taken on the asset that is being imported.

The reconciliation rules are executed in the following order:

- Pre rule
See “[Pre rule](#)” on page 231.
- Add rule
See “[Add rule](#)” on page 233.
- Update rule
See “[Update rule](#)” on page 234.
- Post rule
See “[Post rule](#)” on page 237.

The reconciliation process performs the following tasks on the assets that are imported into the asset system:

- Perform actions like discarding the asset, setting CIA values before the asset is added to the asset system.
- Add the newly discovered assets to the asset store.
- Update the properties of the assets that already exist.
- Mark the assets for the manual review that is based on the rule conditions.

See [“Reconciliation rules and rule types”](#) on page 229.

See [“Creating reconciliation rules without manual review”](#) on page 253.

See [“Creating reconciliation rules using the manual review”](#) on page 254.

Manual review

Control Compliance Suite lets you review the assets manually before you choose to add the assets to the asset system. The assets that are marked for manual review are added to the manual review store.

The assets form a part of the manual review store in any of the following cases:

- If you choose to add the assets to the manual review store in the Add Action dialog box during the creation of the Add Rule.
- If you choose to add the assets to the manual review store in the Update Action dialog box during the creation of the Update Rule.
- If the assets do not satisfy any of the reconciliation rules that are associated with the import job.
- If you associate more than one Add or Update rule with an asset import job and one of the rules marks the assets for manual review.

After the asset is stored in the manual review store, the following actions are possible:

- Edit the import job and add new reconciliation rules.
- Re-run the reconciliation on the manual review records from the Monitor > Jobs view using the Reconcile Records option.

See [“Viewing the manual review records”](#) on page 298.

See [“Reconciling the manual review records”](#) on page 298.

Asset tagging

Control Compliance Suite provides a mechanism to tag and identify assets for report and scope purposes.

Tagging is a way to define an asset with meta information. Tagging helps you identify assets in some context that might prove helpful to determine the value of the asset. You can use the tags to filter the assets.

For example, you can create a tag that is called SOX and associate it with a relevant asset.

Asset groups

An asset group consists of the assets of one or more types. For example, Windows servers, UNIX servers, or Oracle databases can become asset groups.

The asset groups may be created based on various criteria. You can attach the tags to the asset groups and create an asset group that is based on the tags. Similarly, you can create the asset groups that are based on location, owner, risk rating and so on.

The asset groups are of the following types:

- **Dynamic asset group**
See [“Dynamic asset groups”](#) on page 247.
- **Static asset group**
See [“Static asset groups”](#) on page 248.
- **Predefined asset group**
See [“Predefined asset groups”](#) on page 248.

See [“Creating a dynamic asset group”](#) on page 300.

See [“Creating a static asset group”](#) on page 302.

See [“Editing an asset group”](#) on page 306.

Dynamic asset groups

A dynamic asset group is updated with every asset import job if more assets meet the criteria that is specified in the dynamic group definition. The update to the asset group is done on the basis of the criteria of the group. After the import job, the new assets become a part of the asset group if they match the dynamic filters of that asset group. At the time of query execution, the asset groups are resolved to discrete assets.

The dynamic groups can be created on the basis of the following criteria:

- **Common fields of all the asset types**
You can create the asset groups on the basis of the common field values of all the asset types. The common fields include the asset name, location, department, custodian, owner, tags, and risk rating.

- Specific fields of the asset type
- Both

See [“Creating a dynamic asset group”](#) on page 300.

Static asset groups

You can create static asset groups on the basis of the asset type.

The asset count in the static asset groups does not change automatically with the import job. You manually add assets to the static asset groups.

See [“Creating a static asset group”](#) on page 302.

Predefined asset groups

The asset system provides predefined asset groups for all the predefined platforms.

See [“Predefined platforms”](#) on page 203.

The predefined asset groups are dynamic in nature. The predefined dynamic asset groups are created by default at the time of installation. The predefined asset groups are based on certain asset-specific field filters. The filters for the asset groups form the definitions for the assets that are included in the asset group.

Note: You can use the predefined asset groups only after you copy the asset group to the folder in which you want to group the assets.

You can use the predefined asset groups to provide scope for asset import.

The predefined asset groups for the ESM platform are as follows:

Table 5-30 Predefined asset groups for the ESM platform

Group name	Filter / Definition of the dynamic group
All ESM Windows Agents	ESM Agent – OS Version = 'WIN*'
All ESM UNIX Agents	ESM Agent – OS Version= 'UNIX'
All ESM Windows 2003 Agents	ESM Agent – OS Version= 'WIN2003'
All ESM OPenVMS Agents	ESM Agent – OS Version = 'VMS'

The predefined asset groups for the Oracle platform are as follows:

Table 5-31 Predefined asset groups for the Oracle platform

Group name	Filter / Definition of the dynamic group
All Oracle Servers	-
All Oracle 9i Databases	Oracle Configured Databases- Database Version = '9*'
All Oracle 10g Databases	Oracle Configured Databases- Database Version = '10*'
All Oracle 8i Databases	Oracle Configured Databases- Database Version = '8*'
All Oracle 11g Databases	Oracle Configured Databases- Database Version = '11*'
All Oracle installations on UNIX Machines	Oracle Configured Databases- OS Type = 'UNIX' or Oracle Configured Servers- OS Type='UNIX'
All Oracle installations on Windows Machines	Oracle Configured Databases- OS Type = 'Windows' or Oracle Configured Servers- OS Type='Windows'
All Oracle objects	-
All Oracle Databases	-

The predefined asset groups for the SQL platform are as follows:

Table 5-32 Predefined asset groups for the SQL platform

Group name	Filter / Definition of the dynamic group
All SQL Server 7 Instances	SQL Server- Major Version = '7'
All SQL Server 2005 Instances	SQL Server- Major Version = '9'
All SQL Server Instances	-

Table 5-32 Predefined asset groups for the SQL platform (*continued*)

Group name	Filter / Definition of the dynamic group
All SQL Server 2000 Instances	SQL Server- Major Version = '8'

The predefined asset groups for the UNIX platform are as follows:

Table 5-33 Predefined asset groups for the UNIX platform

Group name	Filter / Definition of the dynamic group
All UNIX Servers	-
AIX 5.1 Servers	UNIX Machine- Operating Distribution Field = '*AIX*' and UNIX Machine- Operating System Version= '5.1'
Sun Solaris Servers	UNIX Machine- Operating Distribution Field = '*SunOS*' and UNIX Machine- Operating System Version= '5.1'
Red Hat Linux Servers	UNIX Machine- Operating Distribution Field = '*Red Hat Linux*' and UNIX Machine- Operating System Version= '5.2'
AIX 5.2 Servers	UNIX Machine- Operating Distribution Field = '*AIX*' and UNIX Machine- Operating System Version= '5.2'
Red Hat Servers	UNIX Machine- Operating Distribution Field = '*Red Hat*' and UNIX Machine- Operating System Version= '5.3'
All AIX Servers	UNIX Machine- Operating Distribution Field = '*AIX*' and UNIX Machine- Operating System Version= '5.3'
AIX 5.3 Servers	UNIX Machine- Operating Distribution Field = '*AIX*' and UNIX Machine- Operating System Version= '5.3'

Table 5-33 Predefined asset groups for the UNIX platform (*continued*)

Group name	Filter / Definition of the dynamic group
Red Hat Enterprise Linux Servers	UNIX Machine- Operating Distribution Field = '*Red Hat Enterprise Linux*'
SuSE Linux Servers	UNIX Machine- Operating Distribution Field = '*SuSE Linux*' and Not UNIX Machine- Operating Distribution Field = '*SuSE Linux Enterprise Server*'
HP-UX Servers	UNIX Machine- Operating Distribution Field = '*HP-UX*'
SuSE Enterprise Linux Servers	UNIX Machine- Operating Distribution Field = '*SuSE Linux Enterprise Server*'
All SuSE Servers	UNIX Machine- Operating Distribution Field = '*SuSE*'
AIX 6.1 Servers	UNIX Machine- Operating Distribution Field = '*AIX*' and UNIX Machine- Operating System Version= '6.1'
Red Hat Enterprise Linux 2.1 Servers	UNIX Machine- Operating Distribution Field = '*Red Hat Enterprise Linux*' and UNIX Machine- Operating System Version= '2.1'
Red Hat Enterprise Linux 3.0 Servers	UNIX Machine- Operating Distribution Field = '*Red Hat Enterprise Linux*' and UNIX Machine- Operating System Version= '3.0'

Table 5-33 Predefined asset groups for the UNIX platform (*continued*)

Group name	Filter / Definition of the dynamic group
Red Hat Enterprise Linux 4.0 Servers	UNIX Machine- Operating Distribution Field = '*Red Hat Enterprise Linux*' and UNIX Machine- Operating System Version= '4.0'
Red Hat Enterprise Linux 5.0 Servers	UNIX Machine- Operating Distribution Field = '*Red Hat Enterprise Linux*' and UNIX Machine- Operating System Version= '5.0'
VMware ESX 3 Servers	UNIX Machine- Operating Distribution Field = '*Vmware ESX*' and UNIX Machine- Operating System Version= '3'
Vmware ESX 3.5 Servers	UNIX Machine- Operating Distribution Field = '*Vmware ESX*' and UNIX Machine- Operating System Version= '3.5'
Vmware ESX 4 Servers	UNIX Machine- Operating Distribution Field = '*Vmware ESX*' and UNIX Machine- Operating System Version= '4'
VMware ESX Servers	UNIX Machine- Operating Distribution Field = '*Vmware ESX*'

The predefined asset groups for the Windows platform are as follows:

See [“Creating a dynamic asset group”](#) on page 300.

See [“Creating a static asset group”](#) on page 302.

See [“Editing an asset group”](#) on page 306.

Active assets

The active assets are the assets that are created or updated in the past six months. The Asset System view displays the number of active assets in the top right corner of the table pane.

You can configure the period for which the active assets should be displayed. You can specify the number of days for which the active assets should be displayed in the `ActiveAssetsConfig.xml`. The XML can be found at the `<installdir>\CCS\Reporting And Analytics\Applications\AssetSystem`.

The active assets are displayed only for the following asset types:

- Windows Machines
- UNIX Machines
- ESM Agents

Creating reconciliation rules

The asset reconciliation helps you organize the assets that already exist in the asset store in a logical hierarchy. Reconciliation provides you the flexibility to manage the asset records conditionally when the records get into the assets system.

You can use the reconciliation rules to facilitate the process to add the assets to the asset system. You use the reconciliation rules to update the field values of the existing assets too.

See [“Asset reconciliation”](#) on page 245.

See [“Creating reconciliation rules using the manual review”](#) on page 254.

See [“Creating reconciliation rules without manual review”](#) on page 253.

See [“Using a Pre rule to set the values of the common fields”](#) on page 256.

Creating reconciliation rules without manual review

The creation of reconciliation rules is a crucial step in the asset system workflow. You can create the reconciliation rules with the use of the Create or Edit Reconciliation Rules wizard.

To create reconciliation rules

- 1 Go to **Manage > Assets > Reconciliation Rules**.
- 2 On the taskbar, click **Create Rule**.
- 3 In the **Specify Rule Details** panel of the **Create Reconciliation Wizard**, type the rule name and select the rule type.

You can select from the following rule types:

- Pre rule
- Add rule
- Update rule
- Post rule

See [“Reconciliation rules and rule types”](#) on page 229.

- 4 Select the asset type to associate the rule with.
You can also create the reconciliation rule for all the asset types.
- 5 Select the folder to save the reconciliation rule in.
- 6 Type the description for the reconciliation rule and click **Next**.
- 7 In the **Select Rule Conditions and Actions** panel, click the **Add Condition**.
- 8 In the Add Condition dialog box, select a condition from the drop-down list and click **OK**.
- 9 In the **Select Rule Conditions and Actions** panel, click **Add Action**.
- 10 In the **Add Action** dialog box, select an action that should be performed on the imported asset when it meets the specified condition and click **OK**.
- 11 Click **Next** in the **Select Rule Conditions and Actions** panel after you set the condition and the action.
- 12 In the **Summary** panel, review the rule and click **Finish**.

You can choose to go back and edit the rule any time.

See [“Creating reconciliation rules using the manual review”](#) on page 254.

See [“Working with reconciliation rules scenarios”](#) on page 255.

Creating reconciliation rules using the manual review

Manual review is the process of manually reviewing the assets that are imported into the system by an import job.

See [“Manual review”](#) on page 246.

The assets are added into the asset system with the Add Rule. The field values for the newly imported assets are updated in the asset system with the Update Rule.

See [“Reconciliation rules and rule types”](#) on page 229.

The Add and the Update type of reconciliation rules let you mark the assets for manual review.

To create a reconciliation rule using the manual review

- 1 Go to Manage >Assets >Reconciliation Rules.
- 2 On the taskbar , click **Create Rule**.
- 3 In the **Specify Rule Details** panel, type the rule name and select the rule type.
To mark the assets to add to the manual review store, you can select from the following rule types:
 - Add rule
 - Update rule
- 4 Select the asset type to associate the rule with.
You can also create the reconciliation rule for all the asset types.
- 5 Select the folder to save the reconciliation rule in.
- 6 Type the description for the reconciliation rule and click **Next**.
- 7 In the **Select Rule Conditions and Actions** panel, click the **Add Condition** icon.
- 8 In the **Add Condition** dialog box, select a condition from the drop-down list and click **OK**.
- 9 In the **Select Rule Conditions and Action** panel, click the Add Action icon.
- 10 In the **Add Action** dialog box, select **Add to manual review store** and click **OK**.
- 11 In the **Select Rule Conditions and Actions** panel, click **Next**.
- 12 In the **Summary** panel, review the rule and click **Finish**.

You can choose to go back and edit the rule at any time.

See [“Viewing the manual review records”](#) on page 298.

See [“Working with reconciliation rules scenarios”](#) on page 255.

See [“Creating reconciliation rules without manual review”](#) on page 253.

Working with reconciliation rules scenarios

The reconciliation rules help you handle the situations of organizing the assets effectively in the asset system.

Go through the following scenarios to learn how reconciliation rules work:

- Using a Pre rule to set the values of the common fields
See [“Using a Pre rule to set the values of the common fields”](#) on page 256.

- Using an Add rule to dynamically create asset folders
See [“Using an Add rule to dynamically create asset folders”](#) on page 257.
- Using an Update rule to update the existing field values
See [“Using an Update rule to update the existing field values”](#) on page 258.
- Using a Post rule to dynamically create folders and move assets to the folders
See [“Using a Post rule to mark the assets as control points”](#) on page 259.

Using a Pre rule to set the values of the common fields

Pre rule is the rule that is executed before the assets are added to the asset system. Use the Pre rule to discard the asset before it is added to the asset system or to set the values of the fields before the asset is added. The asset system provides a Predefined rule that sets the values of the Confidentiality, Integrity, and Availability fields to NotDefined. The rule is applicable to all the asset types.

See [“Common fields for all asset types”](#) on page 285.

Similarly, you can create a Pre Rule to set the values of the common fields.

Consider the following scenario:

Assume, that you want to set the name of the asset owner as **xyz** before the asset is added to the asset system.

To set the values of the common fields

- 1 Go to Manage > Reconciliation Rules.
- 2 From the taskbar, select **Create Rule**.
- 3 In the Create or Edit Reconciliation Rule wizard, in the Specify Rule details panel type the rule name.
- 4 From the Rule type drop-down list, select **Pre Rule**.
- 5 From the Asset type drop-down list select the asset type for which you want to create the rule.
- 6 In the Save in box, browse and select the folder where you want to save the rule and click **Next**.
- 7 In the Select Rule Conditions and Actions panel, select **Add Condition**.
- 8 In the Add Condition dialog box, select **If an asset being imported exists in the asset system** and click **OK**.
- 9 In the Select Rule Condition and Actions panel, select **Add Action**.

- 10 In the Add Action dialog box, select **Set the field value of an existing asset as specified**.

Select the field **Asset Owner** and type the value **xyz** and click **OK**.

- 11 Click **Finish** in the Summary panel.

Go to Manage > Assets > Reconciliation Rules. Browse to the folder where you created the rule and check if the rule appears in the folder.

See [“Using an Add rule to dynamically create asset folders”](#) on page 257.

See [“Using an Update rule to update the existing field values”](#) on page 258.

See [“Using a Post rule to mark the assets as control points”](#) on page 259.

Using an Add rule to dynamically create asset folders

Add rule is the rule that lets you add the assets to the asset system in a specified folder. The Add rule is executed on the assets that are being imported. You can also create folders dynamically based on the common field values of the assets.

Consider the following scenario:

Assume that you want to categorize the assets of the Oracle Configured Databases based on the name of the database. The Add rule lets you create the folders dynamically based on the field value. The assets are then added to the folder that is created based on the field value.

To create asset folders dynamically with an Add rule

- 1 Go to Manage > Reconciliation Rules.
- 2 From the taskbar, select **Create Rule**.
- 3 In the Create or Edit Reconciliation Rule wizard, in the Specify Rule details panel type the rule name.
- 4 From the Rule type drop-down list, select **Add Rule**.
- 5 From the Asset type drop-down list select **Oracle Configured Databases**.
- 6 In the Save in box, browse and select the folder where you want to save the rule and click **Next**.
- 7 In the Select Rule Conditions and Actions panel, select **Add Condition**.
- 8 In the Add Condition dialog box, select **If an asset being imported does not exist in the asset system** and click **OK**.
- 9 In the Select Rule Condition and Actions panel, select **Add Action**.

- 10 In the Add Action dialog box, select **Add an asset being imported to the specified folder**.

Click the Browse (...) icon and click **New** in the Select Folder dialog box.

In the Custom Folder dialog box, select **Folder based on field value**.

In the Fields list, select **Database Name** and click **OK**.

Click **OK** in the Select Folder dialog box and click **Next** in the Specify Rule Conditions and Actions panel.

- 11 Click **Finish** in the Summary panel.

If you add this rule to the asset import job for the Oracle Configured Databases, different folders are created with the name of the databases and the assets are added to the proper folders.

Go to Manage > Assets > Reconciliation Rules. Browse to the folder where you created the rule and check if the rule appears in the folder.

See [“Using a Pre rule to set the values of the common fields”](#) on page 256.

See [“Using an Update rule to update the existing field values”](#) on page 258.

See [“Using a Post rule to mark the assets as control points”](#) on page 259.

Using an Update rule to update the existing field values

The Update rule lets you update the field values of the existing assets with new values. The Update rule is executed on the existing assets during an asset import job to check the existing field values.

Consider the following scenario:

Assume that the Operating System of the assets in your enterprise that belongs to the Finance Department, changes from Windows to Linux. You have the asset group based on the tag,, Finance Department. The Update rule lets you update the value of the operating system field.

To update the existing field value with an update rule

- 1 Go to Manage > Reconciliation Rules.
- 2 From the taskbar, select **Create Rule**.
- 3 In the Create or Edit Reconciliation Rule wizard, in the Specify Rule details panel type the rule name.
- 4 From the Rule type drop-down list, select **Add Rule**.
- 5 From the Asset type drop-down list select **Windows Machine**.

- 6 In the Save in box, browse and select the folder where you want to save the rule and click **Next**.
- 7 In the Select Rule Conditions and Actions panel, select **Add Condition**.
- 8 In the Add Condition dialog box, select **If an asset being imported exists in the asset system** and click **OK**.
- 9 In the Select Rule Condition and Actions panel, select **Add Action**.
- 10 In the Add Action dialog box, select **Set the field value of an existing asset as specified**.

In the Fields list, select **OS Type**.

In the Value box, type **Linux** and click **OK**.

- 11 Click **Finish** in the Summary panel.

Go to Manage > Assets > Reconciliation Rules. Browse to the folder where you created the rule and check if the rule appears in the folder.

See [“Using a Pre rule to set the values of the common fields”](#) on page 256.

See [“Using an Add rule to dynamically create asset folders”](#) on page 257.

See [“Using an Update rule to update the existing field values”](#) on page 258.

Using a Post rule to mark the assets as control points

The Post rule lets you move an asset to a specified folder after the asset is added to the asset system. The Post rule is executed on the assets that are already a part of the asset system.

Consider the following scenario:

Assume that you have imported the assets for the Oracle Configured Databases. You want to mark all the assets as control points. You can create a Post rule to mark the assets for Oracle Configured Databases as control points.

To create folders dynamically and move assets to the folders

- 1 Go to Manage > Reconciliation Rules.
- 2 From the taskbar, select **Create Rule**.
- 3 In the Create or Edit Reconciliation Rule wizard, in the Specify Rule details panel type the rule name.
- 4 From the Rule type drop-down list, select **Post Rule**.
- 5 From the Asset type drop-down list select **Oracle Configured Database**.
- 6 In the Save in box, browse and select the folder where you want to save the rule and click **Next**.

- 7 In the Select Rule Conditions and Actions panel, select **Add Condition**.
- 8 In the Add Condition dialog box, select **If an asset being imported exists in the asset system** and click **OK**.
- 9 In the Select Rule Condition and Actions panel, select **Add Action**.
- 10 In the Add Action dialog box, select **Mark an existing asset as control point**.
Click **OK** and click **Next** in the Specify Rule Conditions and Actions panel.
- 11 Click **Finish** in the Summary panel.

Go to Manage > Assets > Reconciliation Rules. Browse to the folder where you created the rule and check if the rule appears in the folder.

See [“Using a Pre rule to set the values of the common fields”](#) on page 256.

See [“Using an Add rule to dynamically create asset folders”](#) on page 257.

See [“Using an Update rule to update the existing field values”](#) on page 258.

Importing assets

In the asset system, asset import involves the import of the following data:

- Data for the asset-specific fields
Asset-specific fields are the fields that are specific to the asset type that you select to import.
See [“Predefined asset types”](#) on page 204.
- Data for the common fields
Common fields are the fields that are common across all the asset types.
See [“Common fields for all asset types”](#) on page 285.

Table 5-34 How data collectors work in asset import

Selected data collector	How the data collector works
Default	<p>Asset import from default data collector involves the import from the data collection components as well as the CSV data collector.</p> <ul style="list-style-type: none"> ■ The default data collector gathers the information about the asset-specific fields from the data collection components in the Control Compliance Suite. ■ A data collection component is assigned to the import query internally, depending on the platform for which the asset import should be performed. A separate data collector is assigned to each platform for data collection. ■ The default data collector gathers information about the common fields from the CSV. ■ The data for the common fields is imported from the Common platform. You must configure the Common platform with a CSV share to import the data for the common fields of the assets. See “Configuring Common platform through CSV settings” on page 271.
CSV	<ul style="list-style-type: none"> ■ The CSV data collector gathers the information about the asset-specific fields from a CSV file. ■ The CSV data collector reads from the CSV files that are specific to platforms. You must create different CSV files for different platforms, if you want to import the asset-specific fields data from the CSV file. To know more about configuring the CSV data collector, click on the following link: See “Configuring the CSV data collector” on page 129. ■ In addition to the CSV file specific to the platform, you also need the CSV file that is configured for the Common platform to import the information about the common fields. See “Configuring Common platform through CSV settings” on page 271.

See [“Importing the assets for the first time”](#) on page 265.

See [“Importing asset-specific fields from the default data collector”](#) on page 272.

See [“Importing asset-specific and common fields using the default data collector”](#) on page 275.

See [“Importing asset-specific and common fields using the CSV data collector”](#) on page 278.

See [“Importing the specific and common fields for custom asset using the CSV data collector”](#) on page 281.

About the first time asset import

The first time asset import implies the asset import on the first day after you install and configure Control Compliance Suite.

Before you import the assets for the first time, you must review the following concepts that are related to asset import.

- Predefined platforms
See [“Predefined platforms”](#) on page 203.
- Predefined asset types
See [“Predefined asset types”](#) on page 204.
- Primary and secondary assets
See [“Primary and secondary assets”](#) on page 228.
- Default data collectors for the supported platforms
See [“Default data collectors”](#) on page 240.
- Working of the default data collector in asset import
See [“About the working of default data collectors in asset import”](#) on page 268.
- Working of the CSV data collector in asset import
See [“About the working of CSV data collector in asset import”](#) on page 269.

When you import the assets for the first time, you import the primary assets into the asset system.

Note: You might not have the Common platform configured through the CSV settings when you import the assets for the first time. In this case, the asset import job does not import the data for the common fields. You must have at least one data collector configured.

See [“Configuring Common platform through CSV settings”](#) on page 271.

Table 5-35 First time asset import steps

Task	Description
Launch the Create or Edit Asset Import Job wizard	Go to Manage > Assets > Asset System > Import Assets to launch the Create or Edit Asset Import Job wizard.
Identify the primary assets to be imported	<p>You must first identify the type of assets that you want to import and then identify the primary assets for the asset type that should be imported first.</p> <p>For example, if you want to import the Windows Files, you must first import the Windows Machines. To import the Windows Machines, you must first import the Windows Domain.</p> <p>Note: You can import the primary assets only for the data collector that you have configured.</p> <p>For example, if you have installed the bv-Control for Windows for data collection, you can import only Windows assets.</p> <p>See “Primary and secondary assets” on page 228.</p>
Select the scope to import the assets	<p>You must select the correct scope to import the assets. After you identify the primary assets to import, you can select the correct scope.</p> <p>It is recommended that you select the default scope.</p> <p>See “About scopes in asset import” on page 287.</p> <p>See “Default scope and supported scope” on page 289.</p>

Table 5-35 First time asset import steps (*continued*)

Task	Description
Select the Add Rule from the predefined reconciliation rules	<p>You can use the Add rule from the predefined reconciliation rules when you import the assets for the first time.</p> <p>The Add rule checks if the asset that is being imported is already in the asset system. If the asset is not in the asset system, the Add rule adds the asset to the asset system.</p> <p>See “Predefined reconciliation rules” on page 238.</p>
Complete the Create or Edit Asset Import Wizard	<p>You need not create any asset field filters when you import the assets for the first time. After you add the reconciliation rules, you can proceed through the Create or Edit Asset Import Job wizard till the Summary page.</p> <p>Make sure that you select the Run Now option in the Schedule panel to run the import job immediately.</p>
Monitor the job status	<p>You can monitor the status of the asset import job from the Jobs view.</p> <p>Go to Manage > Jobs to monitor the status.</p>
View the assets in the asset system	<p>After the asset import job completes, you can view the primary assets in the asset system.</p> <p>Go to Manage > Assets > Asset System</p> <p>You can use the Display filter in the table pane and select the asset type for which you have created the import job. The assets for the selected asset type are displayed in the table pane.</p>

Table 5-35 First time asset import steps (*continued*)

Task	Description
Set the common field values with the reconciliation rules	<p>The asset import job on the first day does not import the common fields if the Common platform is not configured through CSV settings.</p> <p>You can set the values of the common fields with the reconciliation rules after the asset import job.</p> <p>See “Using a Pre rule to set the values of the common fields” on page 256.</p>

See [“Importing the assets for the first time”](#) on page 265.

Importing the assets for the first time

When you import the assets into the asset system for the first time, the scenario can be as follows:

- You have a DPS registered to a site.
- You have at least one data collector configured.
The configuration of the CSV data collector and the configuration of the Common platform through CSV settings are optional.
- You have identified the asset type for which you want to import the assets.
- You have at least one Add rule created through the reconciliation rule to add the assets of the identified asset type in the system.
See [“Creating reconciliation rules without manual review”](#) on page 253.
If you do not have any custom rule, you can use the Add rule from the predefined rules.
See [“Predefined reconciliation rules”](#) on page 238.

Note: On the first day, if you do not have the CSV data collector configured, the data for the fields that are common across all asset types is not imported. You can set the common fields data later using the reconciliation rules.

See [“Using a Pre rule to set the values of the common fields”](#) on page 256.

The asset import involves the following steps:

- Creating an asset import job

■ Executing the asset import job

To import the assets for the first time

- 1 Go to Manage > Assets > Asset System.
- 2 On the taskbar, from the **Asset Tasks** select **Import Assets**.
- 3 In the **Specify Name and Description** panel, in the Name box, type the name for the import job.

You can optionally type the description for the import job and click **Next**.

- 4 In the **Select Platform, Asset Type, and Data Collector** panel, select the platform and the asset type to import the assets.
- 5 In the **Select Platform, Asset Type, and Data Collector** panel, from the **Data Collector** drop-down list, select **Default** and click **Next**.

See [“About the working of default data collectors in asset import”](#) on page 268.

- 6 In the **Select Asset Import Scope** panel, select the default scope with the **Add** option and click **Next**.

See [“About scopes in asset import”](#) on page 287.

Depending upon the asset type that you select in the previous panel, the default scope is selected as a Site or an asset type.

Click **Browse (...)** to view and select the scope.

In the **Limit Asset Import Scope** dialog box, you can select the additional scope from the list of the supported scopes and click **OK**.

See [“Default scope and supported scope”](#) on page 289.

- 7 In the **Add Reconciliation Rules** panel, click **Add Rules**.
- 8 In the Select Reconciliation Rules panel, from the left pane, navigate to Reconciliation Rules > predefined rules .

In the right pane, select **Add asset to the Asset System** and click **Add**. Click **OK**.

The rule adds all the assets to the asset system.

See [“Predefined reconciliation rules”](#) on page 238.

- 9 In the **Specify Asset Field Filters** panel click **Next**.

You do not need to filter the assets with the field filters when you import the assets for the first time.

- 10 In the **Schedule** panel, click **Run now**.

- 11 In the **Specify Notification Details** panel, if you want to send the notification of job completion or job failure, do the following:
 - Type the subject and message of the notification mail.
 - Type the email ID of the sender and the receiver.
- 12 In the **Summary** panel, review the configurations for the import job and click **Finish**.

Go to the Monitor > Jobs view to monitor the current status of the job.

See [“About the first time asset import”](#) on page 262.

Working with asset import scenarios

After you import the primary assets on day zero, you can proceed with the creation of further asset import jobs for the secondary assets.

See [“About the first time asset import”](#) on page 262.

Table 5-36 Asset import scenarios

Data collector	Asset import objective
Default data collector See “About the working of default data collectors in asset import” on page 268.	<p>The scenarios are as follows:</p> <ul style="list-style-type: none">■ To import the asset-specific fields See “Importing asset-specific fields from the default data collector” on page 272.■ To import the asset-specific and common fields See “Importing asset-specific and common fields using the default data collector” on page 275. <p>The import of common fields from the default data collector involves the configuration of CSV data collector for Common platform. See “Configuring Common platform through CSV settings” on page 271.</p>

Table 5-36 Asset import scenarios (continued)

Data collector	Asset import objective
CSV data collector See “About the working of CSV data collector in asset import” on page 269.	The scenarios are as follows: <ul style="list-style-type: none">■ To import the asset-specific and common fields from the CSV data collector See “Importing asset-specific and common fields using the CSV data collector” on page 278.■ To import the custom asset-specific fields and common fields from the CSV data collector See “Importing the specific and common fields for custom asset using the CSV data collector” on page 281.

About the working of default data collectors in asset import

See [“Data collectors and asset types”](#) on page 241.

The default data collector imports the data for the asset fields that are specific to the asset type from the data collection components. A data collection component is internally assigned to the import query based on the selected platform to collect the asset-specific data.

Table 5-37 Platform and data collectors

Platform	Data collector
ESM platform	ESM data collector
Oracle platform	Oracle data collector
SQL platform	SQL data collector
UNIX platform	UNIX data collector
Windows platform	Windows data collector
Custom platform of a custom application	You can use the following to collect data from the custom platforms: <ul style="list-style-type: none">■ CSV data collector

Table 5-37 Platform and data collectors (*continued*)

Platform	Data collector
Common platform The Common platform is the platform that is used to import the common fields across the asset types.	CSV data collector By default, the CSV data collector is used to import the common fields of the Common platform.

Consider the following example:

You select Oracle Configured Servers as the asset type and select the default data collector. The default data collector imports the data for the fields like Server Name, Server NetBIOS Name, Windows Domain Name or UNIX IP Address, OS Type. These fields are specific to the Oracle Configured Servers asset type.

The default data collector imports the data for the common fields from the CSV data collector. To import the data for the common fields of the selected asset type, you must configure the Common platform through CSV settings.

See [“Configuring Common platform through CSV settings”](#) on page 271.

See [“Importing the assets for the first time”](#) on page 265.

See [“Importing asset-specific fields from the default data collector”](#) on page 272.

See [“Importing asset-specific and common fields using the default data collector”](#) on page 275.

About the working of CSV data collector in asset import

See [“Data collectors and asset types”](#) on page 241.

Table 5-38 Role of CSV data collector

Role of the CSV data collector	Description
To import the data of a predefined platform and you explicitly select the CSV data collector for asset import.	<p>To import the entire data in case you explicitly select the CSV data collector for asset import.</p> <p>In this case, the data for the asset-specific fields and for the common fields, is imported from the CSV data collector.</p> <p>If you want to import the entire asset data from the CSV data collector, you need to create a CSV file with a specific format.</p> <p>After you create the CSV file, you need to configure the CSV data collector.</p> <p>See “Importing asset-specific and common fields using the CSV data collector” on page 278.</p>
To import the data for the common fields even if you select the Default data collector for asset import.	<p>To import the data for the common fields even if you select the Default data collector for asset import.</p> <p>In this case, the data for the common fields only is imported from the CSV data collector. The default data collector imports the data for the asset-specific fields.</p> <p>To import the data for the common fields, you must configure the Common platform through CSV settings.</p> <p>See “Configuring Common platform through CSV settings” on page 271.</p> <p>See “About the working of default data collectors in asset import” on page 268.</p>
To import the data in case you import the data for the custom asset type.	<p>In this case, the CSV data collector becomes the default data collector.</p> <p>See “Importing the specific and common fields for custom asset using the CSV data collector” on page 281.</p>

See [“Creating a CSV file for custom application”](#) on page 295.

See [“Configuring the CSV data collector”](#) on page 129.

Configuring Common platform through CSV settings

In Control Compliance Suite, the default data collector does not collect the data for the common fields such as Confidentiality, Integrity, Availability and so on. To collect data for the common fields, you must manually create a CSV file and define all the common fields in a specific format. You must then configure a DPS as a CSV data collector to collect data for the common fields of the predefined asset type. So, to import the predefined asset types even if you select a default data collector you still require a CSV data collector to collect the common fields data.

The overall sequence to collect data for the common fields of an asset type are as follows:

- Export the data fields of an asset type into a CSV file.
- Create a CSV file that contains the data for the common fields.
See [“Common fields for all asset types”](#) on page 285.
Ensure that you know the primary fields of the predefined asset type for which the common fields are to be specified in the CSV file. The primary fields are asset type identifiers that are used to map the common fields of the asset type correctly. For example, for the predefined asset type, Windows directory of the predefined platform, you must know the primary fields, Host and DomainName.
See [“Predefined asset types”](#) on page 204.
- Configure the CSV data collector.
See [“Configuring the CSV data collector”](#) on page 129.
- Import the asset type using the Asset Import wizard.
See [“About the working of default data collectors in asset import”](#) on page 268.

To create and configure the common fields of an asset type through CSV settings

- 1 Select the platform and the asset type for which the common fields must be defined.
- 2 Get the primary fields of the asset type.
If you want to specify the common fields of the predefined asset types, then you must know the primary fields of those asset types.
See [“Predefined asset types”](#) on page 204.

3 Create a CSV file with headers in the following format:

```
<platform.entity. primaryfield1>, <platform.entity.primaryfield2>,  
<Common.platformentity.baseattributefield1>,  
<Common.platform.entity.baseattributefield2>
```

For example, for the common fields of a predefined asset type, Windows directory, the CSV file headers are as follows:

```
Wnt.Domain.DomainName, Wnt.Domain.Host,  
Common.WntDomain.Confidentiality, Common.WntDomain.Integrity,...
```

Here, DomainName and Host are the primary fields of the predefined asset type and Wnt is the platform.

For an asset type, it is important that you ensure the correct correlation between the primary fields and the common fields. The data of the common fields correspond to the assets, whose unique identifiers are the primary fields.

For example, for an asset type, Windows directory, the data representation for the primary and common fields in the CSV file are as follows:

Wnt.Domain. DomainName	Wnt.Domain. HostName	Common. WntDomain. Confidentiality	Common. WntDomain. Integrity
TestDomain	Test1Machine	High	High
TestDomain	Test2Machine	Low	High

As per the example, common fields data for the assets, Test1Machine and Test2Machine are collected.

- 4 Place the CSV file in the network share path of the Windows computer.
- 5 In the console, go to **System Topology > Grid View** and configure the DPS as CSV data collector.
See “[Configuring the CSV data collector](#)” on page 129.
- 6 In the console, go to Settings > System Topology > Map View and click **Infrastructure Tasks > Sync Configuration**.

Importing asset-specific fields from the default data collector

To import the data for the asset-specific fields from the default data collector is a simple task.

The import of the asset-specific fields from the default data collector works on the basis of the following assumptions:

- You select an asset type
- You select the Default data collector
- You want to import the data of the fields that are specific to the asset type that you select.

See [“About the working of default data collectors in asset import”](#) on page 268.

To import asset-specific fields from the default data collector

- 1 Go to Manage > Assets > Asset System.
- 2 On the taskbar, from the Asset Tasks select **Import Assets**.
- 3 In the **Specify Name and Description** panel, in the Name box, type the name for the import job.

You can optionally type the description for the import job and click **Next**.

- 4 In the **Select Platform, Asset Type, and Data Collector** panel, select the platform and the asset type to import the assets for.
- 5 In the **Select Platform, Asset Type, and Data Collector** panel, from the **Data Collector** drop-down list, select **Default** and click **Next**.

See [“About the working of default data collectors in asset import”](#) on page 268.

- 6 In the **Select Asset Import Scope** panel, click the ... option to select the scope for the asset type.

Depending upon the asset type that you select in the previous panel, the default scope is selected as a Site or an asset type.

Click **Browse (...)** to view and select the scope.

In the **Limit Asset Import Scope** dialog box, you can select the additional scope from the list of the supported scopes and click **OK**.

See [“About scopes in asset import”](#) on page 287.

- 7 In the **Select Asset Import Scope** panel, browse through the assets hierarchy and select a folder to add the assets from. Click **Add** to add it as a scope and click **Next**.
- 8 In the **Add Reconciliation Rules** panel, you can do one of the following:
 - Use the **Add Rule** option to add a rule to the import job from the existing rules.
The **Add Rule** option displays the Select Reconciliation Rules panel.

- Use the **Delete Rule** option to delete the rule that is already added and click **Next**.
 - Use the **Move Up** and **Move Down** options to arrange the rules in an order and click **Next**.
- 9 In the **Select Reconciliation Rules** panel, browse through the Reconciliation Rules folder and use the **Add** option to add the existing reconciliation rules to the import job.
- Click **OK**.
- 10 In the **Specify Asset Field Filters** panel you can do one of the following:
- Use the **Edit Selected Statement** option to edit the existing filter and click **Next**.
 - Use the **Delete Selected Statement** option to delete the existing filter and click **Next**.
 - Use the **Add Statement** option to create a new statement.
Click the icon next to the fields drop-down menu to launch the Field Information Browser. The Field Information Browser lets you browse through the list of fields that are supported in the entity schema for the selected data collector. You can also view the fields and its information to build a meaningful asset field filter.
The **Add Statement** option displays the **Create Filter Statement** dialog box.
- 11 In the **Create Filter Statement** dialog use the parameter type and the conditions to create a filter statement.
- See [“Examples of asset filters”](#) on page 242.
- See [“Filter statement operators”](#) on page 243.
- 12 In the **Schedule** panel, select any one of the following:
- If you want to run the job after the wizard closes, check **Run now**.
 - If you want to run the job at a specified interval, check **Run periodically** and enter the following information:
 - In the **Start On** box, enter the start date and time to run the job.
 - Under **Run periodically** options, if you want to run the job only one time, select **Run Once**. If you want to run the job after specific days, select the number of days in the **Run Every Day** list box. Click **Next**.
- 13 In the **Specify Notification Details** panel, if you want to send the notification of job completion or job failure, do the following:

- Type the subject and message of the notification mail.
- Type the email ID of the sender and the receiver.

14 In the Summary panel, review the configurations for the import job and click **Finish**.

You can go back to the previous panels and edit the configurations any time.

You can go to the Monitor > Jobs view to monitor the current status of the job.

The asset import job can be in one of the following states:

- Custom
This state indicates that the state of the asset import job run is Awaiting Manual Review.
- Completed
This state indicates that the job is complete.

The asset import job run can be in one of the following states:

- Executing
This state indicates that the job is running.
- Awaiting manual review
This state indicates that the records that are returned by the data collector should be manually reviewed. The job goes into the Awaiting for manual review status, if the reconciliation rule marks the asset for manual review or if the assets do not satisfy any condition in the reconciliation rules.
See [“Reviewing the assets manually”](#) on page 297.

Importing asset-specific and common fields using the default data collector

If you want to import the asset-specific and common fields from the default data collector, it is mandatory that you configure the Common platform from the CSV settings.

See [“Configuring Common platform through CSV settings”](#) on page 271.

See [“About the working of default data collectors in asset import”](#) on page 268.

See [“About the working of CSV data collector in asset import”](#) on page 269.

You must also ensure that the default data collector for the platform for which you want to import the assets, is configured.

See [“Default data collectors”](#) on page 240.

To import asset-specific and common fields from the default data collector

- 1 Go to Manage > Assets > Asset System.
- 2 On the taskbar, from the Asset Tasks select **Import Assets**.
- 3 In the **Specify Name and Description** panel, in the Name box, type the name for the import job.

You can optionally type the description for the import job and click **Next**.

- 4 In the **Select Platform, Asset Type, and Data Collector** panel, select the platform and the asset type to import the assets for.
- 5 In the **Select Platform, Asset Type, and Data Collector** panel, from the **Data Collector** drop-down list, select **Default** and click **Next**.

See [“About the working of default data collectors in asset import”](#) on page 268.

- 6 In the **Select Asset Import Scope** panel, click the ... option to select the scope for the asset type.

Depending upon the asset type that you select in the previous panel, the default scope is selected as a Site or an asset type.

Click **Browse (...)** to view and select the scope.

In the **Limit Asset Import Scope** dialog box, you can select the additional scope from the list of the supported scopes and click **OK**.

See [“About scopes in asset import”](#) on page 287.

- 7 In the **Select Asset Import Scope** panel, browse through the assets hierarchy and select a folder to add the assets from. Click **Add** to add it as a scope and click **Next**.
- 8 In the **Add Reconciliation Rules** panel, you can do one of the following:
 - Use the Add Rules option to add a rule to the import job from the existing rules.
The Add Rule option displays the Select Reconciliation Rules panel.
 - Use the Delete Rule option to delete the rule that is already added and click **Next**.
 - Use the Move Up and Move Down options to arrange the rules in the order and click **Next**.
- 9 In the **Select Reconciliation Rules** panel, browse through the Reconciliation Rules folder and use the **Add** option to add the existing reconciliation rules to the import job.

Click **OK**.

- 10 In the **Specify Asset Field Filters** panel you can do one of the following:

- Use the Edit Selected Statement option to edit the existing filter and click **Next**.
 - Use the Delete Selected Statement option to delete the existing filter and click **Next**.
 - Use the Add Statement option to create a new statement.
The Add Statement option displays the Create Filter Statement dialog box.
Click the icon next to the fields drop-down menu to launch the Field Information Browser. The Field Information Browser lets you browse through the list of fields that are supported in the entity schema for the selected data collector. You can also view the fields and its information to build a meaningful asset field filter.
- 11 In the **Create Filter Statement** dialog box, use the parameter type and the conditions to create a filter statement.
See [“Examples of asset filters”](#) on page 242.
See [“Filter statement operators”](#) on page 243.
- 12 In the Schedule panel, select any one of the following:
- If you want to run the job after the wizard closes, check **Run now**.
 - If you want to run the job at a specified interval, check **Run periodically** and enter the following information:
 - In the Start On box, enter the start date and time to run the job.
 - Under Run periodically options, if you want to run the job only one time, select **Run Once**. If you want to run the job after specific days, select the number of days in the Run Every Day list box. Click **Next**.
- 13 In the **Specify Notification Details** panel, if you want to send the notification of job completion or job failure, do the following:
- Type the subject and message of the notification mail.
 - Type the email ID of the sender and the receiver.
- 14 In the Summary panel, review the configurations for the import job and click **Finish**.
You can go back to the previous panels and edit the configurations any time.
You can go to the Monitor > Jobs view to monitor the current status of the job.
The asset import job can be in one of the following states:
- Custom

This state indicates that the state of the asset import job run is Awaiting Manual Review.

- Completed

This state indicates that the job is complete.

The asset import job run can be in one of the following states:

- Executing

This state indicates that the job is running.

- Awaiting manual review

This state indicates that the records that are returned by the data collector should be manually reviewed.

See [“Reviewing the assets manually”](#) on page 297.

Importing asset-specific and common fields using the CSV data collector

You can use the CSV data collector as any other default data collector to import the assets of a predefined platform.

Before you start using the CSV data collector for asset import, ensure that you have performed the following tasks:

- Create a CSV file in the supported format.

See [“Creating a CSV file for predefined asset types”](#) on page 293.

- Share the CSV file on the computer where you have installed the Control Compliance Suite Console.

Consider the following cases when you share the CSV file:

- You create a single CSV file to import the common fields and asset-specific fields. You configure different CSV share path for common platform and default platform. In this case, the CSV file must be copied at both the locations.

- You create two separate CSV files to import the common fields and asset-specific fields. You configure different CSV share path for common platform and default platform. In this case, the CSV file for the common fields data must be copied to the share location of the common platform and the CSV file for the default platform must be copied to the share location of the default platform.

- Configure the CSV settings for the platform for which you want to import the assets.

See [“Configuring the CSV data collector”](#) on page 129.

To import asset-specific and common fields from the CSV data collector

- 1 Go to Manage > Assets > Asset System.
- 2 On the taskbar, from the Asset Tasks select **Import Assets**.
- 3 In the **Specify Name and Description** panel, in the Name box, type the name for the import job.

You can optionally type the description for the import job and click **Next**.

- 4 In the **Select Platform, Asset Type, and Data Collector** panel, select the platform and the asset type to import the asset.
- 5 In the **Select Platform, Asset Type, and Data Collector** panel, from the **Data Collector** drop-down list, select **CSV Data Collector** and click **Next**.

See [“About the working of CSV data collector in asset import”](#) on page 269.

- 6 In the **Select Asset Import Scope** panel, click the ... option to select the scope for the asset type.

Depending upon the asset type that you select in the previous panel, the default scope is selected as a Site or an asset type.

Click **Browse (...)** to view and select the scope.

In the **Limit Asset Import Scope** dialog box, you can select the additional scope from the list of the supported scopes and click **OK**.

See [“About scopes in asset import”](#) on page 287.

- 7 In the **Select Asset Import Scope** panel, browse through the assets hierarchy and select a folder to add the assets from. Click **Add** to add it as a scope and click **Next**.
- 8 In the **Add Reconciliation Rules** panel, you can do one of the following:
 - Use the Add Rules option to add a rule to the import job from the existing rules.

The Add Rule option displays the Select Reconciliation Rules panel.
 - Use the Delete Rule option to delete the rule that is already added and click **Next**.
 - Use the Move Up and Move Down options to arrange the rules in the order and click **Next**.
- 9 In the **Select Reconciliation Rules** panel, browse through the Reconciliation Rules folder and use the **Add** option to add the existing reconciliation rules to the import job.

Click **OK**.

- 10 In the **Specify Asset Field Filters** panel you can do one of the following:

- Use the Edit Selected Statement option to edit the existing filter and click **Next**.
 - Use the Delete Selected Statement option to delete the existing filter and click **Next**.
 - Use the Add Statement option to create a new statement.
The Add Statement option displays the Create Filter Statement dialog box.
Click the icon next to the fields drop-down menu to launch the Field Information Browser. The Field Information Browser lets you browse through the list of fields that are supported in the entity schema for the selected data collector. You can also view the fields and its information to build a meaningful asset field filter.
- 11** In the **Create Filter Statement** dialog box, use the parameter type and the conditions to create a filter statement.
See [“Examples of asset filters”](#) on page 242.
See [“Filter statement operators”](#) on page 243.
- 12** In the Schedule panel, select any one of the following:
- If you want to run the job after the wizard closes, check **Run now**.
 - If you want to run the job at a specified interval, check **Run periodically** and enter the following information:
 - In the Start On box, enter the start date and time to run the job.
 - Under Run periodically options, if you want to run the job only one time, select **Run Once**. If you want to run the job after specific days, select the number of days in the Run Every Day list box. Click **Next**.
- 13** In the Specify Notification Details panel, if you want to send the notification of job completion or job failure, do the following:
- Type the subject and message of the notification mail.
 - Type the email ID of the sender and the receiver.
- 14** In the Summary panel, review the configurations for the import job and click **Finish**.
You can go back to the previous panels and edit the configurations any time.
You can go to the Monitor > Jobs view to monitor the current status of the job.
The asset import job can be in one of the following states:
- Custom

This state indicates that the state of the asset import job run is Awaiting Manual Review.

- **Completed**

This state indicates that the job is complete.

The asset import job run can be in one of the following states:

- **Executing**

This state indicates that the job is running.

- **Awaiting manual review**

This state indicates that the records that are returned by the data collector should be manually reviewed.

See [“Reviewing the assets manually”](#) on page 297.

Importing the specific and common fields for custom asset using the CSV data collector

To import the asset data for the custom asset type, you use the CSV data collector. For the new asset type, CSV data collector works as the default data collector.

See [“Default data collectors”](#) on page 240.

Before you start using the CSV data collector for asset import, ensure that you have performed the following tasks:

- **Create a CSV file in the supported format.**

See [“Creating a CSV file for custom application”](#) on page 295.

- **Share the CSV file on the computer where you have installed the Control Compliance Suite Console.**

Consider the following cases when you share the CSV file:

- You create a single CSV file to import the common fields and asset-specific fields. You configure different CSV share path for common platform and default platform. In this case, the CSV file must be copied at both the locations.

- You create two separate CSV files to import the common fields and asset-specific fields. You configure different CSV share path for common platform and default platform. In this case, the CSV file for the common fields data must be copied to the share location of the common platform and the CSV file for the default platform must be copied to the share location of the default platform.

- **Configure the CSV settings for the platform for which you want to import the assets.** You must configure the CSV settings if you have created a new platform. See [“Configuring the CSV data collector”](#) on page 129.

To import custom asset-specific and common fields from the CSV data collector

- 1 Go to Manage > Assets > Asset System.
- 2 On the taskbar, from the Asset Tasks select **Import Assets**.
- 3 In the **Specify Name and Description** panel, in the Name box, type the name for the import job.

You can optionally type the description for the import job and click **Next**.

- 4 In the **Select Platform, Asset Type, and Data Collector** panel, select the platform and the asset type that you have created.
- 5 In the **Select Platform, Asset Type, and Data Collector** panel, from the **Data Collector** drop-down list, select **CSV Data Collector** and click **Next**.

See [“About the working of CSV data collector in asset import”](#) on page 269.

- 6 In the Select Asset Import Scope panel, click the ... option to select the scope for the asset type.

Depending upon the asset type that you select in the previous panel, the default scope is selected as a Site or an asset type.

Click **Browse (...)** to view and select the scope.

In the **Limit Asset Import Scope** dialog box, you can select the additional scope from the list of the supported scopes and click **OK**.

See [“About scopes in asset import”](#) on page 287.

- 7 In the **Select Asset Import Scope** panel, browse through the assets hierarchy and select a folder to add the assets from. Click **Add** to add it as a scope and click **Next**.
- 8 In the **Add Reconciliation Rules** panel, you can do one of the following:
 - Use the Add Rules option to add a rule to the import job from the existing rules.
The Add Rule option displays the Select Reconciliation Rules panel.
 - Use the Delete Rule option to delete the rule that is already added and click **Next**.
 - Use the Move Up and Move Down options to arrange the rules in the order and click **Next**.
- 9 In the **Select Reconciliation Rules** panel, browse through the Reconciliation Rules folder and use the **Add** option to add the existing reconciliation rules to the import job.

Click **OK**.

- 10 In the **Specify Asset Field Filters** panel you can do one of the following:

- Use the Edit Selected Statement option to edit the existing filter and click **Next**.
 - Use the Delete Selected Statement option to delete the existing filter and click **Next**.
 - Use the Add Statement option to create a new statement.
The Add Statement option displays the Create Filter Statement dialog box.
Click the icon next to the fields drop-down menu to launch the Field Information Browser. The Field Information Browser lets you browse through the list of fields that are supported in the entity schema for the selected data collector. You can also view the fields and its information to build a meaningful asset field filter.
- 11 In the **Create Filter Statement** dialog box, use the parameter type and the conditions to create a filter statement.
See [“Examples of asset filters”](#) on page 242.
See [“Filter statement operators”](#) on page 243.
- 12 In the Schedule panel, select any one of the following:
- If you want to run the job after the wizard closes, check **Run now**.
 - If you want to run the job at a specified interval, check **Run periodically** and enter the following information:
 - In the Start On box, enter the start date and time to run the job.
 - Under Run periodically options, if you want to run the job only one time, select **Run Once**. If you want to run the job after specific days, select the number of days in the Run Every Day list box. Click **Next**.
- 13 In the Specify Notification Details panel, if you want to send the notification of job completion or job failure, do the following:
- Type the subject and message of the notification mail.
 - Type the email ID of the sender and the receiver.
- 14 In the Summary panel, review the configurations for the import job and click **Finish**.
You can go back to the previous panels and edit the configurations any time.
You can go to the Monitor > Jobs view to monitor the current status of the job.
The asset import job can be in one of the following states:
- Custom

This state indicates that the state of the asset import job run is Awaiting Manual Review.

- **Completed**

This state indicates that the job is complete.

The asset import job run can be in one of the following states:

- **Executing**

This state indicates that the job is running.

- **Awaiting manual review**

This state indicates that the records that are returned by the data collector should be manually reviewed.

See [“Reviewing the assets manually”](#) on page 297.

Updating the assets in the system after the import

Once you import the assets in the asset system, you can use the Update rule to update the field values of the existing assets.

Consider the following scenario:

Assume that the operating system of the assets in your enterprise that belonged to the Finance Department, changes from Windows to Linux. You have the asset group based on the tag, Finance Department. The Update rule lets you update the value of the operating system field.

To update the existing field value with an update rule

- 1 Go to Manage > Reconciliation Rules.
- 2 From the taskbar, select **Create Rule**.
- 3 In the **Create or Edit Reconciliation Rule** wizard, in the Specify Rule details panel type the rule name.
- 4 From the Rule type drop-down list, select **Add Rule**.
- 5 From the Asset type drop-down list select **Windows Machine**.
- 6 In the Save in box, browse and select the folder where you want to save the rule and click **Next**.
- 7 In the **Select Rule Conditions and Actions** panel, select **Add Condition**.
- 8 In the **Add Condition** dialog box, select **If an asset being imported exists in the asset system** and click **OK**.
- 9 In the **Select Rule Condition and Actions** panel, select **Add Action**.

- 10 In the **Add Action** dialog box, select **Set the field value of an existing asset as specified**.

In the Fields list, select **OS Type**.

In the Value box, type **Linux** and click **OK**.

- 11 Click **Finish** in the Summary panel.

Go to Manage > Assets > Reconciliation Rules. Browse to the folder where you created the rule and check if the rule appears in the folder.

Common fields for all asset types

Control Compliance Suite supports certain predefined asset types.

See [“Predefined asset types”](#) on page 204.

See [“Configuring Common platform through CSV settings”](#) on page 271.

All the asset types have the following common fields:

- **Confidentiality**

Confidentiality is the act of limiting the access and disclosure of information to only authorized users. The impact of unauthorized disclosure of confidential information can lead to security risk, loss of public confidence, or legal action against the organization.

You can set the value of this field as one of the following:

- Not Defined
- Low
- Medium
- High

- **Integrity**

Integrity refers to the genuineness of the information. Integrity dictates that information must be protected from improper modification. Integrity is lost if unauthorized changes are made to the data by either intentional or accidental acts. Continuous use of corrupted data can result in inaccuracy, fraud, or erroneous decisions.

You can set the value of this field as one of the following:

- Not Defined
- Low

This is represented by 1 in the CCS directory. You must specify 1 in the CSV file, in case you want to define the asset value of Integrity as Low after the asset import.

- Medium
- High
- Availability

Availability refers to the accessibility of information resources. Attacks that consume network bandwidth, processor cycles, or disk space affect the availability of a system. If a mission-critical asset is unavailable to its end users, the organization's mission may be affected.

You can set the value of this field as one of the following:

 - Not Defined
 - Low
 - Medium
 - High
- Tags

Tagging is a way to define an asset with meta information. Tagging helps you identify assets in some context that might prove helpful to determine the value of the asset. You can use the tags to filter the assets.

For example, you can create a tag that is called SOX and associate it with a relevant asset.
- Asset Custodian

User who is the business owner of the asset data. There can be one or more custodians for a set of assets. For example, Finance Manager and the Human Resource Manager can be the custodians for the data of all the assets that include the data related to the employee's salary.
- Asset Department

The department to which the asset belongs.
- Asset Location

The location of the asset in the organization.
- Asset Owner

Asset owner is the user who has the permissions to import, update, rename, and delete the assets in the asset system.
- Asset Site

The site to which the asset belongs.

You can set the values of the common fields with the Pre rule.

See [“Using a Pre rule to set the values of the common fields”](#) on page 256.

See [“Importing asset-specific and common fields using the default data collector”](#) on page 275.

See [“Importing asset-specific and common fields using the CSV data collector”](#) on page 278.

See [“Importing the specific and common fields for custom asset using the CSV data collector”](#) on page 281.

About scopes in asset import

You add a scope to the asset import job to gather more specific asset data.

To provide a scope for the asset import, you first limit the scope to a location in the system. The location can be a site, a domain in case of Windows, or a database in case of SQL and Oracle. When you specify a scope at the location level, the asset import query returns the specified asset type from the specified location only.

After you provide the scope at the location level, you can select a specific folder, an asset group, or an asset. The asset import query looks for the specified folder, the asset group, or the asset at the specified location and returns the asset type. Provide asset groups or containers as scopes instead of providing individual assets as scopes.

Consider the following example:

Assume that you want to import the Windows Files. You limit the scope to Windows Machine, which is the default scope for the Windows Files. You select a folder as a scope that contains the Windows Machine and Windows Domain. In this case, the asset import query does not consider the Windows Domain as you have limited the scope to Windows Machine only.

[Table 5-39](#) explains how the default scopes and the supported scopes work in the asset import.

You can scope the assets in the following ways:

- **Use the default scope**
The default scope includes the primary assets for the asset type that you want to include. You import the selected asset type from the primary asset for that asset type.
See [“Primary and secondary assets”](#) on page 228.
- **Use any or all the supported scopes**
The supported scopes include all the asset types or sites from which you can import the selected asset type.

Table 5-39 Asset import scope options

Scope	Scenario	Results
Default scope	<ul style="list-style-type: none">■ You select Windows File as the asset type to import.■ The supported scopes for the Windows File asset type are Domain, Machine, Directory, and File.■ The default scope for the Windows File asset type is Machine.■ You use the default scope.■ The asset import query looks for the Windows files only in the machines.■ If you explicitly select the machines A, B, C, and D, the asset import query looks for the Windows files only in the machines. In the scope, the asset import query looks for the Windows files on the specified machines only.	<ul style="list-style-type: none">■ With the default scope, you can obtain more specific asset data.■ The query execution is comparatively faster due to specific scope.■ You can use the default scope effectively if you want to update the fields of certain existing assets.■ The order of asset type import is important if you want to use the default scope. <p>For example, to import the Windows file with the default scope, you should have the Windows machines already imported in the asset system.</p> <p>See “Default scope and supported scope” on page 289.</p>

Table 5-39 Asset import scope options (*continued*)

Scope	Scenario	Results
Supported scope	<ul style="list-style-type: none">■ The supported scopes for the Windows File asset type are Domain, Machine, Directory, and File.■ The default scope for the Windows File asset type is Machine.■ You use Domain, Machines, and Directory from the supported scope.■ The asset import query looks for the Windows files in domains, machines, and directories.	<ul style="list-style-type: none">■ The query execution takes longer if you do not scope the query properly. See “Default scope and supported scope” on page 289.

See [“Default scope and supported scope”](#) on page 289.

Default scope and supported scope

You add a scope to the asset import job to gather more specific asset data.

You can scope the assets in the following ways:

- Use the default scope
The default scope includes the primary assets for the asset type that you want to include. You import the selected asset type from the primary asset for that asset type.
See [“Primary and secondary assets”](#) on page 228.
- Use any or all the supported scopes
The supported scopes include all the asset types or sites from which you can import the selected asset type.

Table 5-40 Supported and default scopes for the asset types

Asset type	Default scope	Supported scope
Custom In case you create a custom asset type from a custom platform	<ul style="list-style-type: none">■ Site■ Asset type	<ul style="list-style-type: none">■ Site■ Asset type

Table 5-40 Supported and default scopes for the asset types (*continued*)

Asset type	Default scope	Supported scope
ESM Agent	<ul style="list-style-type: none"> ■ ESM Agent ■ Site 	<ul style="list-style-type: none"> ■ ESM Agent ■ Site
Oracle Configured Databases	Site	<ul style="list-style-type: none"> ■ Site ■ Oracle Configured Databases ■ Oracle Configured Servers
Oracle Configured Servers	Site	<ul style="list-style-type: none"> ■ Site ■ Oracle Configured Servers
SQL Database	SQL Server	<ul style="list-style-type: none"> ■ SQL Database ■ SQL Server
SQL Server	Site	<ul style="list-style-type: none"> ■ SQL Server ■ Site
UNIX File	UNIX Machine	<ul style="list-style-type: none"> ■ UNIX Machine ■ UNIX File
UNIX Group	UNIX Machine	<ul style="list-style-type: none"> ■ UNIX Machine ■ UNIX Group
UNIX Machine	Site	<ul style="list-style-type: none"> ■ UNIX Machine ■ Site
Windows Directory	Windows Machine	<ul style="list-style-type: none"> ■ Windows Machine ■ Windows Domain ■ Windows Directory
Windows Domain	Site	<ul style="list-style-type: none"> ■ Windows Domain ■ Site
Windows File	Windows Machine	<ul style="list-style-type: none"> ■ Windows Machine ■ Windows Domain ■ Windows Directory ■ Windows File

Table 5-40 Supported and default scopes for the asset types (*continued*)

Asset type	Default scope	Supported scope
Windows Group	Windows Machine	<ul style="list-style-type: none">■ Windows Group■ Windows Machine■ Windows Domain
Windows Machine	Windows Domain	<ul style="list-style-type: none">■ Windows Domain■ Windows Machine■ Site

See [“About scopes in asset import”](#) on page 287.

Importing assets from a CSV file

In Control Compliance Suite, you can maintain assets in a CSV file, which can be imported into the infrastructure for data collection. The assets are categorized into various asset types, which are imported into Control Compliance Suite through the Create or Edit Asset Import Job wizard. The assets of any application can either belong to a predefined asset type or you can define a new asset type.

See [“Predefined asset types”](#) on page 204.

Before performing an asset import operation from a CSV file, you must first export the assets into a CSV file. You can use any third-party utility to export the assets into the CSV file. The assets that are exported into the CSV file must be arranged in a specific format. You must configure the CSV data collector before you import the assets into Control Compliance Suite.

See [“Creating a new asset type”](#) on page 348.

See [“Configuring the CSV data collector”](#) on page 129.

See [“About format of the CSV file headers”](#) on page 291.

About format of the CSV file headers

After you export the assets and the data that is related to the assets into a CSV file, you must arrange them in a specific format. A single CSV file can contain assets that belong to a specific asset type. Assets can belong either to a predefined asset type or to the asset types that are defined by you through Control Compliance Suite.

See [“Creating a new asset type”](#) on page 348.

The CSV file must contain headers under which the assets along with the data that is related to the assets are arranged. A header is defined containing the name

of the platform, the name of the asset type or entity, and the property or field that defines the asset. For every asset, you scan categorize the properties or fields into asset-specific and common.

The format of the headers for the asset-specific and common fields are as follows:

- **Asset-specific fields**

The asset-specific fields of an asset type comprise the unique identifiers of the asset type along with all fields that define the asset type.

The header format for the asset-specific fields is as follows:

`<platform>.<entity>.<field>`

The details of the fields are as follows:

- The platform header represents the platform to which the asset type belongs. For example, the platform of a predefined asset type, Windows Domain is Windows.

See [“About platforms”](#) on page 356.

- The entity header represents the asset type. For example, Windows Domain can be an asset type for all computers or assets of the Windows domain. See [“About entities”](#) on page 356.

- The field header represents the property that defines the asset. For example, an asset can have properties such as machine name, IP address, domain name.

See [“About fields of an entity”](#) on page 357.

An example of the header of the asset-specific fields of an asset that belongs to a predefined asset type, Windows Domain is as follows:

`Wnt.Domain.Host, Wnt.Domain.IPaddress, Wnt.Domain.DomainName`

The properties of the asset are Host (computer name), IP address, and DomainName.

Every asset is identified easily with their unique identifiers such as IP address, machine name, or domain name. In Control Compliance Suite, these identifiers are known as primary and mandatory fields. You must identify the primary and mandatory fields of an asset type during creation. These primary and mandatory fields are a part of the asset-specific fields and must be specified in the CSV file for every asset.

- **Common fields**

The common fields of an asset type are confidentiality, integrity, availability, and tags.

The header format for the common fields is as follows:

`<common>.<platformentity>.<field>`

See [“Common fields for all asset types”](#) on page 285.

An example header format for the common fields of an asset type, Windows Domain is as follows:

```
Common.WntDomain.Confidentiality, Common.WntDomain.Integrity
```

The common fields of the asset are confidentiality and integrity.

For the predefined asset types, you can retrieve the headers directly into a CSV file from the Asset View of the console. You can use the option, Export CSV Headers of the Asset View to export the headers into the CSV file.

See [“Exporting CSV headers”](#) on page 319.

For example, the assets that belong to a predefined asset type, Windows File, the headers that are exported using the option, Export CSV Headers are as follows:

```
Wnt.File.DomainWorkgroupName,Common.WntFile.DomainWorkgroupName
,Wnt.File.Host,Common.WntFile.Host,Wnt.File.FullyQualifiedNameResolved
,Common.WntFile.FullyQualifiedNameResolved,Wnt.File.LastModifiedDatetime
,Wnt.File.Owner,Wnt.File.SizeMB,Wnt.File.HOSTMACHINEINDOMAIN,
Common.WntFile.Confidentiality,Common.WntFile.Integrity,
Common.WntFile.Availability,Common.WntFile.Tags,
Common.WntFile.AssetCustodian,Common.WntFile.AssetDepartment,
Common.WntFile.AssetLocation,Common.WntFile.AssetOwner,
Common.WntFile.AssetNSResourceID
```

Note: To import assets of the asset type, Windows File with directory as the scope using the CSV data collector, add a new column in the CSV file. The column, WntFile.PARENTDIRECTORYINT is added in the CSV file besides the other fields that are required for the asset type. The data for this column must contain the directory names, which are specified as the scope during the asset import.

For the custom applications, you need to define the headers for the asset type through the Create New Entity Schema wizard.

See [“Creating a new entity schema”](#) on page 360.

See [“Predefined asset types”](#) on page 204.

See [“About the list field format in CSV file”](#) on page 297.

See [“Creating a CSV file for custom application”](#) on page 295.

See [“Creating a CSV file for predefined asset types”](#) on page 293.

Creating a CSV file for predefined asset types

A comma-separated value (CSV) file is one of the means to import data into the Control Compliance Suite. Data is arranged in a specific format in the CSV file for easy interpretation by the infrastructure. A CSV data collector is configured to

collect data from the CSV file. Reports of the collected data is generated and displayed in the Control Compliance Suite console. In the CSV file, you must organize data in a comma-separated manner as per a specific format.

See [“About format of the CSV file headers”](#) on page 291.

You can create a CSV file for any custom application or for any of the predefined asset types of Control Compliance Suite.

See [“Creating a CSV file for custom application”](#) on page 295.

Note: To import assets of the ESM asset type, Agent, you can use the file, ESMAgentAsset.csv. This file is located in the directory, <install directory>\Symantec\CCS\Reporting and Analytics\Applications\Data Collectors\ESM.

To create a CSV file

- 1 Go to **Manage > Assets > Asset System**.
- 2 On the right-hand side table pane of the Asset System view, select a predefined asset type from the **Display** drop-down box.
- 3 From the taskbar select **Asset Tasks > Export CSV Headers**.

The CSV headers for the selected predefined asset type is exported to a .csv file that is created instantaneously. The .csv file contains headers for the asset-specific and common fields of an asset type.

- 4 In the CSV file, arrange the assets and the corresponding data of the predefined asset type.

For example, for the predefined asset type, Windows Directory, the data representation of the asset-specific and common fields of the asset type is as follows:

Wnt.Domain. DomainName	Wnt.Domain. HostName	Common. WntDomain. Confidentiality	Common. WntDomain. Integrity
TestDomain	Test1Machine	High	High
TestDomain	Test2Machine	Low	High

- 5 Import the assets of the predefined asset type through the **Create or Edit Asset Import Job** wizard.

See [“Importing asset-specific and common fields using the CSV data collector”](#) on page 278.

Ensure that you select CSV data collector in the **Create or Edit Asset Import Job** wizard.

See [“Configuring the CSV data collector”](#) on page 129.

Creating a CSV file for custom application

A comma-separated value (CSV) file is one of the means to import data into the Control Compliance Suite. Data is arranged in a specific format in the CSV file for easy interpretation by the infrastructure. A CSV data collector is configured to collect data from the CSV file. Reports of the collected data is generated and displayed in the Control Compliance Suite console. In the CSV file, you must organize data in a comma-separated manner in a specific format.

For a custom application, you must define an entity, which maps to an asset type. An entity is defined in the entity schema, which is created using the Create New Entity Schema wizard. The entity schema contains the blueprint of the asset type. The assets that you import can either belong to any of the predefined asset types or you can create a new asset type. If the assets belong to a predefined asset type, then you must know the details of the fields of the predefined asset type.

See [“Predefined asset types”](#) on page 204.

To create a CSV file

- 1 Export the data of the custom application into a CSV file.
- 2 Identify whether the asset type or entity of the custom application belongs to any of the predefined asset type.
- 3 If the asset type or entity does not belong to any of the predefined asset type, then identify the following for the asset type:

- Platforms

See [“About platforms”](#) on page 356.

- Entity

See [“About entities”](#) on page 356.

- Fields

See [“About fields of an entity ”](#) on page 357.

- 4 For a custom application, you must first define an entity schema before creating the CSV file.

See [“Creating a new entity schema”](#) on page 360.

The schema is created using the Create New Entity Schema wizard. In the entity schema, you must specify the primary fields of the entity besides defining the other asset-specific and common fields.

- 5 Copy the CSV file headers from the Summary panel of the Create New Entity Schema wizard and paste it in the CSV file.

Ensure that the CSV headers are arranged in the supported format. The best practice is to specify the header information of the primary fields as the starting columns in the CSV file.

See [“About format of the CSV file headers”](#) on page 291.

For example, you can have a network of servers that are installed with a custom application, DB2 and you want to collect the server name of all the servers. In the entity schema, you can define the platform as DB2, the entity as Server and the field as Server Name.

The header information for the DB2 application in the CSV file is of the following format:

```
DB2.Server.ServerName
```

If the asset type or entity belongs to a predefined asset type or an already defined asset type, then export the CSV headers from the console. The header information of the asset type can be retrieved from the Asset view of the console.

See [“Exporting CSV headers”](#) on page 319.

6 Arrange the data of the custom application for the defined CSV headers in the CSV file.

7 Configure the CSV data collector.

See [“Configuring the CSV data collector”](#) on page 129.

See [“Creating a new asset type”](#) on page 348.

See [“Creating a CSV file for predefined asset types”](#) on page 293.

About the list field format in CSV file

The Control Compliance Suite accepts data from the CSV file for data collection only if the data is specified in a specific format.

See [“About format of the CSV file headers”](#) on page 291.

If you want to define a string type data, which is an array in the CSV file, then you must ensure that the data is represented in a specific list field format. Control Compliance Suite does not report on string type array data, which is not specified as per the list field format in the CSV file.

Control Compliance Suite supports the following list field formats in a CSV file:

- Multi-line text enclosed in double quotes
- The format, @:<total number of items in the list>:<char count>:<char text>

For example, @:3:10:TestDomain:7:Domain1:9:ESMDomain

The list field details of the format in the example are as follows:

- The number, 3 represents the total number of items in the list.
The items in the list are, TestDomain, Domain1, and ESMDomain.
- The number, 10 is the character count of the list item, TestDomain. Similarly, the number, 7 is the character count of the list item, Domain1.
- The character text is the name of the list item such as TestDomain, Domain1, and ESMDomain.

Reviewing the assets manually

The assets that are marked for manual review in the reconciliation rules are added to the manual review store. The assets that do not satisfy any reconciliation rules are also included in the manual review store.

See [“Manual review”](#) on page 246.

See [“Creating reconciliation rules using the manual review”](#) on page 254.

You must manually review the records in the manual review store and decide whether the records should be added to the asset system or not.

The manual review of assets involve the following steps:

- Viewing the manual review records
See [“Viewing the manual review records”](#) on page 298.
- Reconciling the manual review records
See [“Reconciling the manual review records”](#) on page 298.

Viewing the manual review records

The assets that are marked for manual review in the asset import job appear in the Monitor > Jobs view. The status of the job run of the asset import job, that is marked for manual review is, Awaiting Manual Review. The parent asset import job, that is marked for manual review is, Custom.

To view the manual review records

- 1 Go to Monitor > Jobs.
- 2 In the table pane, navigate to the asset import job for which you want to view the manual review records.
- 3 In the table pane, right-click the job run that displays the status, **Awaiting Manual Review**.
- 4 Select **Review Records**.

View the records in the Review Records - Monitor dialog box.

See [“Manual review”](#) on page 246.

See [“Reconciling the manual review records”](#) on page 298.

Reconciling the manual review records

After viewing the asset records that await the manual review, you can reconcile those assets again.

To reconcile the manual review records

- 1 Go to Monitor > Jobs.
- 2 In the table pane, right-click the job run that displays the status Awaiting Manual Review.

3 Select **Review Records**.

- 4** In the **Review Records - Monitor** dialog box, review the records. If you want to execute the add rule or the update rule that is associated with the asset import job on all the records, click **Reconcile Records**.

When you reconcile the records, another job run is created in the Jobs view. The status of the job that was marked as Awaiting Manual Review is not updated. The new job run shows the updated status after the records are reconciled according to the reconciliation rules. You can view the number of job runs in the original job with the status Awaiting Manual Review.

When you decide to reconcile the records, the job query ignores the manual review entry in the reconciliation rules. The job query only considers the original rule definition of the add rule or the update rule. The asset records for manual review are then added to the asset system or the field values are updated depending on the rule.

If you want to add another reconciliation rule to the records that await manual review, you can edit the parent asset import job. You can then associate a new reconciliation rule with the job and then reconcile the manual review records.

See [“Manual review”](#) on page 246.

See [“Viewing the manual review records”](#) on page 298.

Creating asset groups

An asset group consists of the assets of one or more types. For example, Windows servers, UNIX servers, or Oracle databases can become asset groups. The grouping is represented in a hierarchical fashion with nested subsets.

You can create dynamic and static asset groups to organize the assets into logical groups. You can create asset groups on the basis of tags, CIA values, asset types, and other asset fields.

See [“Dynamic asset groups”](#) on page 247.

See [“Creating a dynamic asset group”](#) on page 300.

See [“Static asset groups”](#) on page 248.

See [“Creating a static asset group”](#) on page 302.

See [“Editing an asset group”](#) on page 306.

Creating a dynamic asset group

You create a dynamic asset group, if you want the assets in a folder to be organized dynamically based on certain properties. The dynamic asset group gets updated with every asset import job if more assets from the relevant asset folder meet the dynamic group filters.

Note: You can add assets to the asset group only from the folder that contains the asset group or from the folders in the same hierarchy.

To create a dynamic asset group

- 1 In the taskbar, from the Asset Group Tasks, select Create Asset Group.
- 2 In the **Specify Asset Group Details** panel, specify the following:
 - Name of the asset group
 - Description of the asset group
 - Folder path from which to include the assets
- 3 Select **Dynamic group** in the Asset Group Type section:
- 4 Click **Next**.
- 5 In the **Select Asset Type** panel, select the asset type for which you want to create an asset group and click **Next**.

- 6** In the **Create Common Asset Field Filters** panel, specify the value for the common asset field filters and click **Next**.

The **Create Common Asset Field Filters** panel lets you create a filter that is based on the values of the common fields. The panel presents a list of common asset fields. You can specify the values for the selected fields. The asset group is formed based on the values that you specify in this panel.

The **Create Common Asset Field Filters** panel presents the following options:

Name	<p>Lets you specify the asset name.</p> <p>Assets with the specified name are included in the asset group.</p>
Location	<p>Lets you specify the asset location.</p> <p>Assets that reside at the specified location are included in the group.</p>
Department	<p>Lets you specify the asset department.</p> <p>Assets that belong to the specified department are included in the asset group.</p>
Owner	<p>Lets you specify the asset owner.</p> <p>Assets with the specified owner are included in the asset group.</p>
Custodian	<p>Lets you specify the custodian for the assets.</p> <p>Assets with the specified custodian are included in the asset group.</p>
Tags	<p>Lets you specify the tag name and the tag path.</p> <p>Assets that have the specified tag are included in the asset group.</p>
Risk rating	<p>Lets you specify the risk rating.</p> <p>Assets with the specified risk rating are included in the asset group.</p>
Include assets with any of the above filters	<p>Includes the asset in the asset group if the asset meets the criteria that is specified in any of the above filters.</p>

- 7 In the **Create Specific Asset Type Filters** panel, select a field from the drop-down list on the basis of which you want to create the dynamic asset group. Click **Add Statement**.

The **Create Specific Asset Type Filters** panel lets you edit, delete, arrange, and configure the asset field filters. You can select a field that should be used as a filter for the selected asset type and create a filter statement. You can use the Add Statement option on the panel to create a new filter statement.

You can edit or delete the existing filter statement using the Edit option and the Delete option.

The asset field that you can select depends on the asset type that you selected.

You can use the AND and OR operators to specify the filter after adding the filter statements.

See [“Operators \(, \), AND, OR”](#) on page 304.

- 8 In the **Filter Statement** dialog box, select the parameter, the operator and the value for the field to form a filter statement and click **OK**.
 - 9 In the **Create Specific Asset Type Filters**, click **Next**.
 - 10 Review the configuration information in the **Summary** panel and click **Finish**.
- See [“Creating a static asset group”](#) on page 302.

Creating a static asset group

You create a static asset group for the assets that do not undergo frequent updates. The asset count in the static asset group remains constant unless you edit the group and manually add more assets to the group.

Note: You can add assets to the asset group only from the folder that contains the asset group or from the folders in the same hierarchy.

Consider the following example:

- Under the Asset System folder you have another folder - US-CA.
- You have a static asset group, WindowsServer2003 under the folder US-CA.
- You can add the assets to the asset group WindowsServer2003 from the folder US-CA or from the folders under the US-CA folder.

To create a static asset group

- 1 In the task bar, from the Asset Group Tasks, select **Create Asset Group**.
- 2 In the **Specify Asset Group Details** panel, specify the following:

- Name of the asset group
 - Description of the asset group
 - Folder path from which to include the assets
- 3 Select **Static group** in the Asset Group Type section.
 - 4 Click **Next**.
 - 5 In the **Select Asset Type** panel, select the asset type for which you want to create an asset group and click **Next**.
 - 6 In the **Select Assets** panel, navigate to the folder in the asset system hierarchy, select the assets that you want to add to the asset group and click **Add**.
This is an optional step.
 - 7 Review the configuration information in the Summary panel and click **Finish**.
- See [“Creating a dynamic asset group”](#) on page 300.

Deleting inactive assets using the asset groups

The Asset System view displays the number of active assets in the top right corner of the table pane. The active assets are the assets that are created or updated during the last six months. The active assets are displayed only for the Windows Machines, the UNIX Machines, and the ESM Agents.

You might want to delete the inactive assets from the asset system. You can use the asset groups feature to form a dynamic group of assets that are not modified for the last six months. You can then delete this group.

To create an asset group based on the last modified date

- 1 In the task bar, from the Asset Group Tasks, select **Create Asset Group**.
- 2 In the Specify Asset Group Details panel, specify the following:
 - Name of the asset group
 - Description of the asset group
 - Folder path where the asset group should be saved
- 3 Select **Dynamic group** in the Asset Group Type section.
- 4 Click **Next**.
- 5 In the Select Asset Type panel, select the asset type for which you want to create an asset group and click **Next**.

- 6 In the Create Common Asset Field Filters panel, specify the value for the common asset field filters and click **Next**.

The Create Common Asset Field Filters panel lets you create a filter that is based on the values of the fields that are common across all the asset types. The panel presents a list of common asset fields. You can specify the values for the selected fields. The asset group is formed based on the values that you specify in this panel.
- 7 In the Create Specific Asset Type Filters panel, select **All Asset Types- Asset last modified date** and click **Add Statement**.

You can use the AND and OR operators to specify the filter after adding the filter statements.

See “[Operators \(, \), AND, OR](#)” on page 304.
- 8 In the Filter Statement dialog box, select **Specific Value**.

Select **EqualTo (=)** as the operator and from the Specify value drop-down list select a date.

The assets that were modified till the specified date are included in the asset group.
- 9 Review the configuration information in the Summary panel and click **Finish**.

Operators (,), AND, OR

In the asset system you can use the opening and closing parentheses, AND, and OR operators to join the filter statements. You need to specify the filters on the basis of which the asset import job or the asset groups is created.

You can use more than one filter and create a combined filter expression with the operators.

Consider the following example:

- You create the following filter statements:
 - **A Equal To (=) B**
 - **C Greater Than or Equal To [<=] D**
 - **A Equal To (=) B**
 - **C Equal To (=) F**
- You can use opening and closing parentheses, AND, OR operators in the following ways to specify the relation among the given filter statements:
 - **A Equal To (=) B and C Greater Than or Equal To [<=] D**

The AND operator is the default operator that is used to join the two filter statements.

- **A Equal To (=) B or C Greater Than or Equal To [\leq] D**
You can switch between the AND/OR operators using the same option.
- **(A Equal To (=) B) and (C Greater Than or Equal To [\leq] D) or (A Equal To (=) B) and (C Equal To (=) F)**
With the opening and closing parentheses, you can create more complex filter expressions.

Performing the tasks in the Asset System view

You can perform the following tasks from the Manage > Assets > Asset System view:

- Creation of asset folders in the tree pane
See [“Creating the asset folders”](#) on page 305.
- Asset group tasks
See [“Performing the asset group tasks”](#) on page 306.
- Global tasks
See [“Performing the global tasks”](#) on page 307.
- Asset tasks
See [“Performing the asset tasks”](#) on page 317.
- Common tasks
See [“Deleting assets or asset groups”](#) on page 319.
- View asset details pane
See [“Viewing asset information in the details pane”](#) on page 319.
- Use Filter by pane
See [“Using the Filter by pane in the Asset System view”](#) on page 327.

Creating the asset folders

You create folders to store new assets. You use folders to organize the business objects in a hierarchical manner. The organization of the assets in a hierarchical manner is the most crucial step in the asset system. You can model the default hierarchy that is created during the installation of Control Compliance Suite, to suit your organizational requirements. Asset hierarchy can also be created based on the location, the department, the platform, or any other criteria.

See [“Asset folder hierarchy”](#) on page 202.

You can effectively administer the permissions on the folders and the objects within the folder if the hierarchy is created properly.

See [“Assigning permissions from the Permission Management view”](#) on page 95.

You can use reconciliation rules to help you arrange the assets in a specific hierarchical form.

To create a folder in the tree pane

- 1 Go to Manage > Asset System.
- 2 In the Asset System view, in the tree pane, right-click Asset System folder.
- 3 Select **New Folder**.
- 4 In the Create new container dialog box, type the name of the container.
- 5 Click **OK**.

See [“About using special characters in folder and job names”](#) on page 60.

Performing the asset group tasks

You can perform the following asset group tasks from the Asset System view:

- Create asset group.
See [“Creating asset groups”](#) on page 299.
- Edit asset group.
See [“Editing an asset group”](#) on page 306.
- Copy and paste asset group.
See [“Copying and pasting an asset group”](#) on page 307.
- Rename Asset Group

Editing an asset group

You can edit the asset groups with the use of the **Create or Edit Asset Group Wizard**.

To use the Create or Edit Asset Group Wizard

- 1 In the table pane, select an asset group that you want to edit.
- 2 From the **Common Tasks**, select **Edit Asset Group**.
- 3 Edit the selections as you want and complete the wizard.

Copying and pasting an asset group

You can copy and paste the asset group to the same folder or any other folder under the Asset System in the tree pane. If you copy the asset group to the same folder, the group is created as **Copy of <Name of the original asset group>**.

You can also select and copy multiple asset groups from the table pane.

Note: When you copy and paste an asset group, the assets in the asset group are not retained. The filters for the asset group are retained. This is because you can include the assets to the asset group only from the folder where the asset group is present.

To copy and paste the asset group

- 1 In the table pane, right-click the asset group that you want to copy.
- 2 Select **Copy Asset Group**.
- 3 In the tree pane, right-click the folder in which you want to paste the asset group.
- 4 Select **Paste Asset Group**.

Performing the global tasks

You can perform the following global tasks from the Asset System view:

- Mark as control point.
See [“Marking an asset as a control point”](#) on page 398.
- Request exceptions.
See [“Requesting an exception for assets on checks”](#) on page 436.
- Set up data collection.
See [“Setting up a data collection job from the Assets view”](#) on page 310.
- Run evaluation.
See [“Running an evaluation job from the Asset System view”](#) on page 311.
- Run collection-evaluation-reporting
See [“Running a collection-evaluation-reporting job from the Asset System view”](#) on page 314.

Marking an asset as a control point

An asset that is marked as a control point appears in the Entitlements > Control Points view.

You can mark only the following asset types as control points:

- Windows File
- Windows Directory
- Windows Groups
- UNIX File
- UNIX Group
- SQL Database
- Oracle Database
- ESM Agents

See [“Control points”](#) on page 395.

Note: You cannot mark Windows Machines, UNIX Machines, SQL Servers, and Oracle Servers as control points.

To mark an asset as a control point

- 1 Go to Manage > Assets > Asset System.
- 2 In the table pane, right-click the asset that you want to mark as a control point.
- 3 Select **Mark as Control Point**.
- 4 In case you mark an asset that belongs to Oracle, SQL, or ESM platforms as a control point, you must select the entitlement type.
See [“Control point type and entitlement type”](#) on page 399.
- 5 In the Entitlement Type Selector dialog box, select one or more entitlement types and click **OK**.
- 6 In the confirmation message box, click **OK**.
- 7 Go to Manage > Entitlements > Control Points and verify the control point in the table pane.

See [“Unmarking a control point”](#) on page 404.

See [“Control points”](#) on page 395.

Requesting an exception for assets on checks

A requestor can request an exception on the checks for specific assets in the organization.

To request an exception

- 1 Go to Manage > Exceptions.
- 2 In the Exceptions view, do either of the following:
 - On the taskbar, click **Request Exception**.
 - In the table pane, right-click anywhere on the grid and select **Request Exception**.
- 3 In the Request Exception Wizard, in the Specify Exception Details panel, enter the following details and click **Next**:
 - In the Title box, enter the name of the exception.
 - In the Type box, select **Standards**.
In the Template box, the displayed template is Evaluation Exception.
 - In the Description box, type a description for the exception.
 - In the Attachment box, browse to enter the name of the file that you want to attach.
 - In the Exception Validity group box, in the Effective Date box, select the date on which the exception becomes applicable. In the Expiration Date box, select the date on which the exception becomes invalid. Click **Next**.
- 4 In the Select Checks and Assets panel, click **Add** to select the standards, sections, or checks.
All the checks within the selected standard or section are displayed.
- 5 In the Select Standards or Sections or Checks dialog box, expand the Standards folder and select a folder. The standards within the selected folder are displayed in the right pane. Select a standard, section, or check and click **Add**. Click **Add All** to select all the standards. To remove one or more standards from the Selected Items list, click **Remove** or **Remove All**. Click **OK**.
All the checks within the selected standard or section are displayed in the Select Checks and Assets Panel.
- 6 In the Select Checks and Assets panel, click **Add** to select the assets. In the Select Assets or Asset Groups or Folders dialog box, expand the Assets folder and select a folder. The assets within the selected folder are displayed in the right pane. Select an asset and click **Add**. Click **Add All** to select all the assets. To remove one or more assets from the Selected Items list, click **Remove** or **Remove All**. Click **OK**.
- 7 In the Specify Exception Type Information panel, click **Next**.

- 8 In the Specify Requestor Information panel, type or browse to enter the Requestor and the Requestor Group. Enter the Requestor Email ID and Comments.
- 9 In the Summary panel, verify the details that you have entered in the wizard. Click **Back** to modify any data. Click **Finish** to exit the wizard.

The exception is created and its state is set to Requested.

Similarly, you can request an exception by launching the Request Exception Wizard from the Standards view, Assets view, and the Evaluation Results dialog box.

See [“Launching the Request Exception Wizard”](#) on page 440.

See [“About exception states ”](#) on page 431.

Setting up a data collection job from the Assets view

You can run a data collection job from the asset management view. You can use the Create or Edit Data Collection Job wizard to create a job to start the process of collecting data for the specified standards.

Ensure that you already have some assets in the asset store before you proceed with the data collection.

To set up a data collection job

- 1 Go to Manage > Asset System.
- 2 In the table pane, select the assets or the asset group for which you want to run the data collection job.
- 3 From the Global Tasks select, **Setup Data Collection**.
- 4 In the Create or Edit data Collection Job, in the Specify Job Name and Description panel, in the Name field, type the name of the data collection job.
- 5 In the Description box, type a description for the evaluation job and click **Next**.
- 6 In the Select Standards panel, navigate through the Standards and select a standard against which you want to set up a data collection.

The predefined standards or the custom standards that are relevant to the asset type selected only are available for selection.
- 7 Click **Add** to add the standard to the data collection job and click **Next**.
- 8 In the **Schedule Job** panel, select any one of the following:
 - If you want to run the job after the wizard closes, check **Run Now**.

- If you want to run the job at a specified interval, check **Run Periodically** and enter the following information.
In the Start On box, enter the start date and time to run the job.
Under Run periodically options, if you want to run the job only one time, select **Run Once**. If you want to run the job after specific days, select the number of days in the Run every Day list box. Click **Next**.
- 9 In the Specify Notification Details panel, select **Send notification** and type the information for sending the notification and click **Next**.
- 10 In the Summary panel review all the selections that you made and click **Finish**.
You can monitor the status of the job from the Monitor > Jobs view.
See [“Running an evaluation job from the Asset System view”](#) on page 311.

Running an evaluation job from the Asset System view

See [“Viewing the evaluation results in the details pane”](#) on page 325.

You run an evaluation job wizard to evaluate the assets in your organizations against specific standards or checks.

See [“About evaluation jobs”](#) on page 454.

To run an evaluation job

- 1 Go to Manage > Assets.
- 2 In the Assets view, do one of the following:
 - In the table pane, right-click and select **Run Evaluation**.
 - From the Global Tasks, select **Run Evaluation**.
- 3 In the Specify Job Name and Description panel, in the Job Name box, type a name for the evaluation job that you want to create.
- 4 In the Description box, type a description for the evaluation job and click **Next**.
- 5 In the Select Standards panel, in the tree pane, select a folder. You can further select from the displayed folder contents.
The selected standards are displayed in the Selected Items list.

- 6 After this step, you can configure automatic remediation.

If you do not want to configure remediation, you can skip the **Select Asset Types for Remediation** panel and click **Next** to reach the **Schedule Job** panel.

For a detailed procedure of configuring the automatic remediation visit the following link:

See [“To remediate the assets automatically”](#) on page 313.

- 7 In the Schedule Job panel, select any one of the following:

- If you want to run the evaluation job after the wizard closes, check **Run Now**.

- If you want to run the job at a specified interval, check **Run Periodically** and enter the following information.

In the Start On box, enter the start date and time to run the job.

Under the Run periodically options, if you want to run the job only one time, select **Run Once**. If you want to run the job after specific days, select the number of days in the Run every Day list box. Click **Next**.

You must set a password in the System Management > User Preferences > Data Collection Password. If you fail to set the password, a warning message appears when you schedule the job. You can click OK in the message box and specify the scheduling details. But you must set the password before the scheduled time for running the job.

- 8 In the **Add Result Viewers** panel, add the users or the groups that have the permissions to view the evaluation results and reports.

It is recommended to add the groups as the result viewers.

- 9 In the Specify Notification Details panel, enter the job completion notification details on the Job Success tab. Enter the job failure notification details on the Job Failure tab. Both the tabs on this panel contain the same options. Check **Send notification**, enter the following information and then click **Next**:

- Enter the subject and message of the notification mail.
- Enter the sender and the receiver email ID.
Notification can be sent to multiple recipients.

To remediate the assets automatically

- 1 In the **Select Asset Type for Remediation Ticketing** panel, check the **Enable Automatic Remediation Ticketing** option to configure the automatic remediation details.

Select the asset types that correspond to the assets that were evaluated and click **Next**.

- 2 In the **Specify Remediation Ticketing Criteria** panel, specify the combination of risk score and compliance score that you want to use to identify the assets for remediation.

You can select **Apply to all standards** if you want to apply the specified remediation criteria to all the standards for remediation.

If you do not select **Apply to all standards**, you must specify the remediation ticketing criteria for each standard.

Click **Next**.

- 3 In the **Select Remediation Ticket Type** panel, select one of the following:

- Create an email notification.

This option lets you create an email notification that you want to send for notification.

- Create a service desk ticket.

This action opens a service desk ticket request directly at the end of the evaluation results for the non-compliant assets.

You can choose the **Enable closed-loop verification** option. With the closed-loop verification, the non-compliant assets data is re-evaluated after the service desk request is met.

See [“About closed-loop verification”](#) on page 552.

Click **Next**.

- 4 If you choose to send an email notification as a remediation action, specify the message that you want to send as an email notification in the **Configure Notification Details for Remediation Ticketing** panel. Click **Next**.

If you select **Consolidate multiple assets in a single ticket/email**, a single notification is sent that includes all the non-compliant assets.

You can check **Make this the default Email Notification template** if you want to use the same message for all the service desk ticket requests.

- 5 If you choose to create a service desk ticket as a remediation action, specify the message that you want to send as a service desk request in the **Configure Service Desk Ticket** panel. Click **Next**.

If you select **Consolidate multiple assets in a single ticket/email**, a single service desk ticket is generated that includes all the non-compliant assets.

You can check **Make this the default Service Desk Ticket template** if you want to use the same message for all the service desk ticket requests.

- 6 Proceed with the Create or Edit Evaluation Job Wizard till the Summary panel.

Running a collection-evaluation-reporting job from the Asset System view

The collection-evaluation-reporting job lets you create a common job to schedule data collection, evaluation, and report generation. Control Compliance Suite provides different jobs for data collection, evaluation, and report generation tasks. In case of environments where thousands of such jobs are scheduled, a collection-evaluation-reporting job makes it easy to manage all the tasks from a single wizard.

See [“About evaluation jobs”](#) on page 454.

To run a collection-evaluation-reporting job

- 1 Go to Manage > Asset System.
- 2 In the Asset System view, right-click an asset in the table pane and select **Run Collection-Evaluation-Reporting**.
- 3 In the Specify Job Name and Description panel, in the Job Name box, type a name for the evaluation job that you want to create.
- 4 In the Description box, type a description for the evaluation job and click **Next**.
- 5 In the Select Standards panel, from the list of standards that appear in the left section, select the standard against which you want to evaluate the assets.
Click **Add** to add the selected standard and click **Next**.
Click **Add All** to add all the standards that appear in the right section and click **Next**.
- 6 In the **Select Report Templates** panel, do one of the following:
 - Select **Synchronize evaluation results with reporting database** to sync the evaluation results with the reporting database and click **Next**.
 - Select **Generate reports for this evaluation results** to select the report template for the evaluation results.

You can also use the **Define Scope and Add Template** option to define the scope for the report.

7 After this step, you can configure automatic remediation.

If you do not want to configure remediation, you can skip the **Select Asset Types for Remediation** panel and click **Next** to reach the **Schedule Job** panel.

For a detailed procedure of configuring the automatic remediation visit the following link:

See [“To remediate the assets automatically”](#) on page 316.

8 In the **Schedule Job** panel, select any one of the following:

- If you want to run the evaluation job after the wizard closes, check **Run Now**.
- If you want to run the job at a specified interval, check **Run Periodically** and enter the following information.
 In the Start On box, enter the start date and time to run the job.
 Under the Run periodically options, if you want to run the job only one time, select **Run Once**. If you want to run the job after specific days, select the number of days in the Run every Day list box. Click **Next**.

You must set a password in the **Home > User Preferences > Schedule Job Credentials**. If you fail to set the password, a warning message appears when you schedule the job. You can click OK in the message box and specify the scheduling details. But you must set the password before the scheduled time for running the job.

9 In the **Add Result Viewers** panel, add the users or the groups that have the permissions to view the evaluation results and reports.

It is recommended to add the groups as the result viewers.

10 In the Specify Notification Details panel, enter the job completion notification details on the Job Success tab. Enter the job failure notification details on the Job Failure tab. Both the tabs on this panel contain the same options. Check **Send notification**, enter the following information and then click **Next**:

- Enter the subject and message of the notification mail.
- Enter the sender and the receiver email ID.
 Notification can be sent to multiple recipients.

11 In the **Summary** panel, view the summary and click **Finish**.

The Create or Edit Collection-Evaluation-Reporting wizard also lets you configure the details to remediate the assets that are non-compliant.

To remediate the assets automatically

- 1 In the **Select Asset Type for Remediation Ticketing** panel, check the **Enable Automatic Remediation Action** option to configure the automatic remediation details.

Select the asset types that correspond to the assets that were evaluated and click **Next**.

- 2 In the **Specify Remediation Ticketing Criteria** panel, specify the combination of risk score and compliance score that you want to use to identify the assets for remediation.

You can select **Apply to all standards** if you want to apply the specified remediation criteria to all the standards for remediation.

If you do not select **Apply to all standards**, you must specify the remediation ticketing criteria for each standard.

Click **Next**.

- 3 In the **Select Remediation Ticket Type** panel, select one of the following:

- Create an email notification.

This option lets you create an email notification that you want to send for notification.

- Create a service desk ticket.

This action opens a service desk ticket request directly at the end of the evaluation results for the non-compliant assets.

You can choose the **Enable closed-loop verification** option. With the closed-loop verification, the non-compliant assets data is re-evaluated after the service desk request is met.

See [“About closed-loop verification”](#) on page 552.

Click **Next**.

- 4 If you choose to send an email notification as a remediation action, specify the message that you want to send as an email notification in the **Configure Notification Details for Remediation Ticketing** panel. Click **Next**.

If you select **Consolidate multiple assets in a single ticket/email**, a single notification is sent that includes all the non-compliant assets.

You can check **Make this the default Email Notification template** if you want to use the same message for all the service desk ticket requests.

- 5 If you choose to create a service desk ticket as a remediation action, specify the message that you want to send as a service desk request in the **Configure Service Desk Ticket** panel. Click **Next**.

If you select **Consolidate multiple assets in a single ticket/email**, a single service desk ticket is generated that includes all the non-compliant assets.

You can check **Make this the default Service Desk Ticket template** if you want to use the same message for all the service desk ticket requests.

- 6 Proceed with the Create or Edit Evaluation Job Wizard till the Summary panel.

Performing the asset tasks

You can perform the following asset tasks from the Asset System view:

- Import assets.
See [“Importing assets”](#) on page 260.
- Edit assets.
See [“Editing assets”](#) on page 317.
- Move assets.
See [“Moving an asset”](#) on page 318.
- Export CSV headers.
See [“Exporting CSV headers”](#) on page 319.

Editing assets

You can edit the asset field values using the Edit Assets dialog box.

The Edit Assets dialog box lets you edit the mandatory and the optional field values along with the common fields for the selected asset. You can also add or remove the tags from the Edit Assets dialog box.

Note: You can edit multiple assets of the same asset type collectively if you want to specify common field values and tags to all assets.

To edit assets

- 1 In the table pane, right-click an asset that you want to edit.
You can also select multiple assets at a time for editing.
- 2 Select **Edit Assets**.

- 3 In the **Edit Assets** dialog box, under the **Properties** tab specify or change the values of the fields.

The **Properties** tab presents the list of the editable fields for the selected asset type. The editable fields include the mandatory fields, the optional fields, and the common fields.

The Properties tab presents checkboxes for the optional fields that have a string value. You can select the check box if you want to use blank value for the optional field. You do not need to type any value for the optional string field, in case you select the check box. If you select the check box and still type the value in the optional string field, then the value that you type takes precedence over the blank value.

The boxes for all the fields are empty by default. The current value is retained if you do not specify any value for a field.

- 4 Under the Tags tab, click **Add Tag**.
- 5 In the Select Tags dialog box, select a tag that you want to apply to the asset and click **Add**.
- 6 Click **OK** in the Select Tags dialog box.
- 7 In the Tags tab, under the **Tag Set Options**, select one of the following:
 - **Append**
To add the selected tag to the existing asset. This option adds the tag in addition to the existing tags of the assets.
 - **Overwrite**
To overwrite the existing tag. This option removes the existing tag and adds the selected tag to the asset.
 - **Clear**
To clear all the existing tags. This option removes all the existing tags from the asset.
- 8 Click **OK**

Moving an asset

You use the right-click menu or the menu bar in the Control Compliance Suite Manage > Asset System view to move an asset from one location to another.

To move an asset

- 1 In the table pane, right-click an asset that you want to move.
- 2 Select **Move**.

- 3 In the **Move Asset** dialog box, select the destination folder to which you want to move the asset.
- 4 Click **OK**.

Exporting CSV headers

You can export the CSV headers of the asset type for which you want to import the assets through the CSV data collector. With the list of CSV headers, you can create your own CSV files with more accuracy to import the assets of a particular asset type.

You can use the CSV headers to create the CSV file that can be used for importing the assets from the CSV data collector.

To export the CSV headers

- 1 Go to Manage > Assets > Asset System.
- 2 Select an asset type from the **Display** drop-down list.
- 3 From the **Asset Tasks** in the taskbar , select **Export CSV Headers**
- 4 Select the location where you want to save the CSV file.

See [“Importing asset-specific and common fields using the CSV data collector”](#) on page 278.

Deleting assets or asset groups

You can delete one or more assets or asset groups from the Asset System view.

Note: You cannot delete an asset that is used as a control point for which the review cycle is progress.

To delete the assets or the asset groups

- 1 Go to Manage > Assets > Asset System.
- 2 From the table pane select the assets or the asset groups that you want to delete.
- 3 From the Common Tasks, click **Delete**.

See [“Moving an asset”](#) on page 318.

Viewing asset information in the details pane

You can view the information about the assets in the details pane.

To view the asset information

- 1
- In the table pane, select the asset for which you want to view the information.
- 2
- View the information for the selected asset in the details pane.

The details pane displays all the information about the selected asset in the following tabs:

-
- General
- See “[Asset details pane- General tab](#)” on page 320.
-
- Asset-type Properties
- See “[Asset details pane- Asset-type Properties tab](#)” on page 322.
-
- Custom Properties
- See “[Asset details pane- Custom Properties tab](#)” on page 323.
-
- Errors
- See “[Asset details pane- Errors tab](#)” on page 324.
-
- Data Collection
- See “[Asset details pane- Data Collection tab](#)” on page 324.
-
- Evaluation
- See “[Asset details pane- Evaluation tab](#)” on page 324.
-
- Tags
- See “[Asset details pane- Tags tab](#)” on page 325.
-
- Exceptions
- See “[Asset details pane- Exceptions tab](#)” on page 326.

Asset details pane- General tab

The General tab of the asset details pane provides general information about the selected asset.

The General tab contains the following details about the assets:

Asset name	Displays the name of the asset.
Asset type	Displays the asset type.
Creation Date	Displays the date when the asset or the asset group was created.
Last modified date	Displays the date when the asset or the asset group was last modified.

Last evaluation date	Displays the date when the asset or the asset group was last evaluated.
Confidentiality	<p>Displays one of the following states for confidentiality:</p> <ul style="list-style-type: none"> ■ Not Defined This is represented by 0 in the CCS directory. ■ Low This is represented by 1 in the CCS directory. ■ Medium This is represented by 2 in the CCS directory. ■ High This is represented by 3 in the CCS directory. <p>Note: If you specify the value of this field in the CSV file as anything greater than 3, the asset system marks it as NotDefined.</p>
Integrity	<p>Displays one of the following states for integrity:</p> <ul style="list-style-type: none"> ■ Not Defined This is represented by 0 in the CCS directory. ■ Low This is represented by 1 in the CCS directory. ■ Medium This is represented by 2 in the CCS directory. ■ High This is represented by 3 in the CCS directory. <p>Note: If you specify the value of this field in the CSV file as anything greater than 3, the asset system marks it as NotDefined.</p>

Availability	<p>Displays one of the following states for availability:</p> <ul style="list-style-type: none">■ Not Defined This is represented by 0 in the CCS directory.■ Low This is represented by 0 in the CCS directory.■ Medium This is represented by 0 in the CCS directory.■ High This is represented by 0 in the CCS directory. <p>Note: If you specify the value of this field in the CSV file as anything greater than 3, the asset system marks it as NotDefined.</p>
Compliance score	<p>Displays the overall compliance score of the assets in the asset group that is derived from all the sources.</p>
Risk Score	<p>Displays the overall risk score of the assets in the asset group that is derived from all the sources.</p>
Risk Rating	<p>Displays the risk rating.</p> <p>The risk rating is the highest risk score of all the risk scores that are derived from all the sources.</p>

- See [“Using a Pre rule to set the values of the common fields”](#) on page 256.
- See [“Asset details pane- General tab”](#) on page 320.
- See [“Asset details pane- Asset-type Properties tab”](#) on page 322.
- See [“Asset details pane- Custom Properties tab”](#) on page 323.
- See [“Asset details pane- Errors tab”](#) on page 324.
- See [“Asset details pane- Data Collection tab”](#) on page 324.
- See [“Asset details pane- Evaluation tab”](#) on page 324.
- See [“Asset details pane- Tags tab”](#) on page 325.

Asset details pane- Asset-type Properties tab

The Asset-type properties tab of the Asset details pane provides information about the asset type.

The Asset-type Properties tab contains the primary, mandatory, and optional fields for the selected asset types.

The Asset-type Properties tab contains the information about the following common fields:

- Asset Custodian
- Asset Department
- Asset Location
- Asset Owner
- Asset Site

You can set the values of the common fields, mandatory fields, and optional fields from the Asset-type Properties tab.

See [“Predefined asset types”](#) on page 204.

See [“Using a Pre rule to set the values of the common fields”](#) on page 256.

See [“Asset details pane- General tab”](#) on page 320.

See [“Asset details pane- Custom Properties tab”](#) on page 323.

See [“Asset details pane- Errors tab”](#) on page 324.

See [“Asset details pane- Data Collection tab”](#) on page 324.

See [“Asset details pane- Evaluation tab”](#) on page 324.

See [“Asset details pane- Tags tab”](#) on page 325.

Asset details pane- Custom Properties tab

The Custom Properties tab presents the fields that are newly added to the asset type from the Schema Manager.

The Custom Properties tab includes the following fields:

- New external fields that are added to the asset type
- New optional fields that are added to the asset type

See [“Extending an existing asset type”](#) on page 351.

See [“Using a Pre rule to set the values of the common fields”](#) on page 256.

See [“Asset details pane- General tab”](#) on page 320.

See [“Asset details pane- Asset-type Properties tab”](#) on page 322.

See [“Asset details pane- Errors tab”](#) on page 324.

See [“Asset details pane- Data Collection tab”](#) on page 324.

See [“Asset details pane- Evaluation tab”](#) on page 324.

See [“Asset details pane- Tags tab”](#) on page 325.

Asset details pane- Errors tab

The Errors tab lists the errors that occur while running a job for the selected asset.

See [“Using a Pre rule to set the values of the common fields”](#) on page 256.

See [“Asset details pane- General tab”](#) on page 320.

See [“Asset details pane- Asset-type Properties tab”](#) on page 322.

See [“Asset details pane- Custom Properties tab”](#) on page 323.

See [“Asset details pane- Data Collection tab”](#) on page 324.

See [“Asset details pane- Evaluation tab”](#) on page 324.

See [“Asset details pane- Tags tab”](#) on page 325.

Asset details pane- Data Collection tab

The Data Collection tab contains the details of the assets for which the data has been collected.

See [“Using a Pre rule to set the values of the common fields”](#) on page 256.

See [“Asset details pane- General tab”](#) on page 320.

See [“Asset details pane- Asset-type Properties tab”](#) on page 322.

See [“Asset details pane- Custom Properties tab”](#) on page 323.

See [“Asset details pane- Errors tab”](#) on page 324.

See [“Asset details pane- Evaluation tab”](#) on page 324.

See [“Asset details pane- Tags tab”](#) on page 325.

Asset details pane- Evaluation tab

The Evaluations tab contains the list of the evaluations.

You can view the details of the assets that are evaluated against a standard in the Details pane.

The Details pane presents the following information about the evaluation:

- Standard against which the evaluation job was run
- Evaluation date
- Checks evaluated
- Checks not evaluated
- Compliance score
- Risk score

See [“Using a Pre rule to set the values of the common fields”](#) on page 256.

See [“Asset details pane- General tab”](#) on page 320.

See [“Asset details pane- Asset-type Properties tab”](#) on page 322.

See [“Asset details pane- Custom Properties tab”](#) on page 323.

See [“Asset details pane- Errors tab”](#) on page 324.

See [“Asset details pane- Data Collection tab”](#) on page 324.

See [“Asset details pane- Tags tab”](#) on page 325.

Viewing the evaluation results in the details pane

You can view the details of the assets that are evaluated against a standard in the Details pane.

The details pane presents the following information about the evaluation:

- Standard against which the evaluation job was run
- Evaluation date
- Checks evaluated
- Checks not evaluated
- Compliance score
- Risk score

To get the asset based view of the evaluation results

- 1 Go to Manage > Assets > Asset System.
- 2 Select the assets for which you have run the evaluation job.
- 3 In the Details pane, select the **Evaluation** tab.
- 4 Click the View Details icon at the top right corner of the Details pane.
- 5 View the asset-based detailed information about the evaluation.

See [“Working with Evaluation Results”](#) on page 541.

See [“Running an evaluation job from the Asset System view”](#) on page 311.

Asset details pane- Tags tab

The Tags tab contains the list of all the tags that are associated with the selected asset.

The Tags tab also lets you add a new tag to associate with the selected asset.

You can also remove a tag that is already associated with the asset from the Tags tab.

See [“Using a Pre rule to set the values of the common fields”](#) on page 256.

See [“Asset details pane- General tab”](#) on page 320.

See [“Asset details pane- Asset-type Properties tab”](#) on page 322.

See [“Asset details pane- Custom Properties tab”](#) on page 323.

See [“Asset details pane- Errors tab”](#) on page 324.

See [“Asset details pane- Data Collection tab”](#) on page 324.

See [“Asset details pane- Evaluation tab”](#) on page 324.

Applying a tag to the asset

You can apply one or more tags to a single asset.

To assign a tag to the assets

- 1 In the table pane, select one or more assets to which you want to assign a tag.
- 2 Right-click the assets and select **Edit Assets**.
- 3 In the Edit Assets dialog, in the Tags tab click **Add**.
- 4 In the Apply Tag dialog, select the tag from the Tags folder and click **Add**.
- 5 Click **OK**.

Removing a tag from the asset

You can remove the tag that is associated with the asset.

To remove a tag

- 1 In the table panel, select the asset for which you want to remove the tag.
- 2 Right-click the asset and select **Edit Assets**.
- 3 In the Edit Assets dialog, under the Tags tab select the tag that you want to remove and click **Remove**.
- 4 Click **OK** in the Edit Assets dialog.

Asset details pane- Exceptions tab

The Exceptions tab lists all the exceptions that are applied to the selected asset.

See [“Using a Pre rule to set the values of the common fields”](#) on page 256.

See [“Asset details pane- General tab”](#) on page 320.

See [“Asset details pane- Asset-type Properties tab”](#) on page 322.

See [“Asset details pane- Custom Properties tab”](#) on page 323.

See [“Asset details pane- Errors tab”](#) on page 324.

See [“Asset details pane- Data Collection tab”](#) on page 324.

See [“Asset details pane- Evaluation tab”](#) on page 324.

See [“Asset details pane- Tags tab”](#) on page 325.

Using the Filter by pane in the Asset System view

The Filter by pane contains the filters that you can use to display only the required assets.

The Control Compliance Suite provides the following default filters for filtering the assets:

Select tags

Lets you filter the assets according to the specified tags. You can browse to add the tags in the Tags list.

You can select either of the following options:

- **Match any**
Displays the assets that match any one of the listed tags.
- **Match all**
Displays the assets that match all the listed tags.

See [“Select tags filter”](#) on page 329.

Risk Ratings

Lets you filter the existing assets according to the specific risk rating that is associated with the assets.

You can select the rating of Confidentiality, Integrity, and Availability from the drop-down list that is shown at each of the risk types.

The assets that possess the selected risk rating are displayed in the table pane.

See [“Risk Rating filter”](#) on page 329.

Created Between

Lets you select the dates to display the assets that are created between the selected dates.

See [“Created Between filter”](#) on page 329.

Modified Between

Lets you select the dates to display the assets that are updated between the selected dates.

See [“Modified Between filter”](#) on page 329.

If you specify values for more than one filters, all the selected filters are considered when the assets are displayed in the table pane. In case you select more than one values for a single filter only one of the values is considered when the assets are displayed in the table pane.

For example:

If you specify values for the Tags, Risk Ratings, Created Between, and Modified Between filters, all the filters are considered. If you select two tags in the tags filter only one of the tags is considered. If you select values for the Confidentiality, Integrity, and Availability rating, only one of the values is considered.

You can customize the filter options in the Filter by pane.

To customize the filter options

- 1 In the Filter by pane, click the **Customize** icon.
- 2 In the **Customize Filters** dialog box, from the list box select the filter type to edit.
- 3 For the selected filter type, you can do any of the following:
 - Select or deselect the Display filter type check box. If you deselect the filter type, the filter type and its options are not displayed in the Filter by pane.
 - Use the arrow icons to move the options between Display and Do not display boxes.
 - Use the Move up and Move Down icons to change the order of the options that is displayed in the Filter by pane.
- 4 Click **Save Changes**.

See [“Customizing the filter options”](#) on page 56.

See [“Select tags filter”](#) on page 329.

See [“Risk Rating filter”](#) on page 329.

See [“Created Between filter”](#) on page 329.

See [“Modified Between filter”](#) on page 329.

Risk Rating filter

You can use the Risk rating filter when you want to filter the existing assets according to the specific risk rating that is associated with the assets. You can select the rating of Confidentiality, Integrity, and Availability from the drop-down list that is shown at each of the risk types. The assets that possess the selected risk rating are shown in the table pane.

To edit the filter, click the Customize icon at the top of the Filter by pane.

See [“Using the Filter by pane in the Asset System view”](#) on page 327.

See [“Customizing the filter options”](#) on page 56.

Select tags filter

You can use the Select tags filter when you want the assets with specific tags to be displayed in the tree pane.

In the Filter by pane, under the Select tags section, you can either choose the options "Match any" or "Match all".

You can also use the Browse option to browse and select specific tags.

You can also edit the filter, with the Customize icon at the top of the Filter by pane.

See [“Using the Filter by pane in the Asset System view”](#) on page 327.

See [“Customizing the filter options”](#) on page 56.

Created Between filter

The Created Between filter lets you select a time period to display the assets that were created between the specified dates.

See [“Using the Filter by pane in the Asset System view”](#) on page 327.

See [“Customizing the filter options”](#) on page 56.

Modified Between filter

The Modified Between filter lets you select two dates. The assets that were modified between the specified dates are displayed in the table pane.

See [“Using the Filter by pane in the Asset System view”](#) on page 327.

See [“Customizing the filter options”](#) on page 56.

Performing the tasks in the Reconciliation Rules view

You can perform the following tasks from the Manage > Assets > Reconciliation Rules view:

- Create rule.
See [“Creating reconciliation rules”](#) on page 253.
- Copy and paste rule
See [“Copying and pasting a reconciliation rule”](#) on page 331.
- Delete rule.
See [“Deleting a reconciliation rule”](#) on page 331.
- Move rule
See [“Moving a reconciliation rule”](#) on page 331.
- Edit rule.
See [“Editing a reconciliation rule”](#) on page 330.
- View reconciliation rules details pane.
See [“Viewing rules information in the details pane”](#) on page 331.
- Use Filter by pane.
See [“Using the Filter by pane in the Reconciliation Rules view ”](#) on page 332.

Editing a reconciliation rule

You can edit only one reconciliation rule at a time. You cannot edit the rule type, the asset type, and the rule folder. You can edit the name of the rule, and the conditions and the actions associated with the rule.

To edit the reconciliation rule

- 1 Use the check box to select a rule from the table pane.
- 2 Click **Edit Rule** from the menu bar.
- 3 In the **Edit Reconciliation Rules** wizard, in the Select Rule Type and Name panel, edit the name of the rule.
- 4 Click **Next**.
- 5 In the **Select Rule Condition and Action** panel, add or remove the conditions and actions.
- 6 Click **Next**.
- 7 Click **Finish** in the Summary panel.

Moving a reconciliation rule

You use the right-click menu or the menu bar in the Control Compliance Suite Console to move a rule from one location to another.

To move a rule

- 1 In the table pane, use the check box to select a rule.
- 2 Select **Move Rules** from the menu bar.
- 3 In the **Move Rules** dialog box, select the destination folder to which you want to move the rule.
- 4 Click **OK**.

Copying and pasting a reconciliation rule

You can copy and paste a reconciliation rule to any other folder under the Reconciliation Rules in the tree pane.

To copy and paste the reconciliation rule

- 1 In the table pane, right-click the rule that you want to copy.
You can select multiple rules to copy.
- 2 Select **Copy Rule**.
- 3 In the tree pane, right-click the folder in which you want to paste the rule.
- 4 Select **Paste Rule**.

Deleting a reconciliation rule

You delete the reconciliation rules with the Delete Rule option in the task bar.

To delete a rule

- 1 Go to Manage > Assets > Reconciliation Rules.
- 2 In the table pane, select one or more rules of the same rule type.
- 3 From the task bar, click **Delete Rule**.
- 4 Click **OK** on the confirmation message box.

Viewing rules information in the details pane

You can view the information about the reconciliation rules in the details pane.

To view the rules information

- 1 In the table pane, select the rule for which you want to view the information.
- 2 View the information for the selected asset in the details pane.
See [“Creating reconciliation rules without manual review”](#) on page 253.
See [“Creating reconciliation rules using the manual review”](#) on page 254.

Using the Filter by pane in the Reconciliation Rules view

The Filter by pane of the Manage > Assets > Reconciliation Rules view contains the filters that you can use to display only the required reconciliation rules.

The Control Compliance Suite provides the following default filters for filtering the reconciliation rules:

Asset Types

Lets you filter the reconciliation rules to display only the rules that are associated with a particular asset type.

See [“Asset Type filter”](#) on page 333.

Rule Types

Lets you filter the reconciliation rules to display only a particular type of rules.

See [“Rule Type filter”](#) on page 333.

You can customize the filter options in the Filter by pane.

To customize the filter options

- 1 In the Filter by pane, click the **Customize** icon.
- 2 In the **Customize Filters** dialog box, from the list box select the filter type to edit.
- 3 For the selected filter type, you can do any of the following:
 - Select or deselect the Display filter type check box. If you deselect the filter type, the filter type and its options are not displayed in the Filter by pane.
 - Use the arrow icons to move the options between Display and Do not display boxes.
 - Use the Move up and Move Down icons to change the order of the options that is displayed in the Filter by pane.
- 4 Click **Save Changes**.

See [“Customizing the filter options”](#) on page 56.

Rule Type filter

The Rule Type filter lets you select a type of the rule from the Pre, Add, Update, and Post. The rules of the selected type only are displayed in the table pane.

See [“Customizing the filter options”](#) on page 56.

See [“Using the Filter by pane in the Reconciliation Rules view ”](#) on page 332.

Asset Type filter

You can use the Asset Type filter when you want to filter the existing assets according to the specific asset types. From the list of asset types, you can select the corresponding check boxes to select the specific asset types. The assets of the selected asset type are shown in the table pane.

To edit the filter, click the Customize icon at the top of the Filter by pane.

See [“Using the Filter by pane in the Asset System view”](#) on page 327.

See [“Customizing the filter options”](#) on page 56.

See [“Using the Filter by pane in the Reconciliation Rules view ”](#) on page 332.

Importing assets from Altiris

This chapter includes the following topics:

- [About importing assets from Altiris](#)
- [Supported asset types for Altiris](#)
- [Prerequisites for installing Control Compliance Suite Asset Export Task](#)
- [Installing Asset Export Task on Altiris Notification Server](#)
- [Working with the Altiris Asset Export Task solution](#)
- [Creating the Altiris asset import jobs in Control Compliance Suite Console](#)
- [Specifying the asset export settings in the Altiris Symantec Management Console](#)
- [Creating a asset export task in the Altiris Symantec Management Console](#)
- [Scheduling asset export task in the Altiris Symantec Management Console](#)
- [About the CSV files on Altiris Notification Server](#)

About importing assets from Altiris

Control Compliance Suite (CCS) provides the CCS Asset Export Task solution to import certain types of assets from the Altiris Configuration Management Database (CMDB) to the CCS database. Windows and UNIX are the predefined asset types that are supported.

The CCS Asset Export Task solution must be installed on the Altiris Notification Server before you can export the assets.

See [“Installing Asset Export Task on Altiris Notification Server”](#) on page 337.

When you install the CCS Asset Export Task solution, it becomes part of the Altiris Symantec Management Console. Most of the functionality appears in the **Manage > Jobs and Tasks > Notification Server** option.

The **Altiris Symantec Management Console** is a Web-based user interface that is the primary tool for interacting with Notification Server and installed solutions.

The CCS Asset Export Task solution does the following:

- Exports assets from the Altiris CMDB to a CSV file.
- Runs an asset import job on CCS. The asset import job imports assets from the CSV file to the CCS asset system. The assets are imported using a CSV data collector.

If any resource is deleted from the Altiris CMDB, the corresponding asset is not deleted from the CCS asset system.

See [“Supported asset types for Altiris”](#) on page 336.

See [“Working with the Altiris Asset Export Task solution”](#) on page 338.

Supported asset types for Altiris

Only the Windows and UNIX asset types are exported from the Altiris Configuration Management Database (CMDB) database.

If the required attributes for Control Compliance Suite (CCS) are not available in the Altiris CMDB, those assets are not imported.

The following attributes are exported for the Windows computers:

- Domain\workgroup name
- Machine name
- Operating system Major version number
- Operating system Minor version number
- Operating system Type
- Machine Is Server
- Machine Is BDC
- Machine Is PDC
- SourceID
- Source

The following attributes are exported for the UNIX computers:

- Machine name
- IP address
- Operating system
- Operating Distribution Field
- Operating system Version
- SourceID
- Source

See [“About importing assets from Altiris”](#) on page 335.

Prerequisites for installing Control Compliance Suite Asset Export Task

You must have the following products to successfully download and install the Control Compliance Suite (CCS) Asset Export Task solution:

- Symantec Install Manager
You must use the latest Symantec Install Manager to install the CCS solution.
- Altiris Notification Server 7.0
You must have the Altiris Notification Server 7.0 on which to install the CSS solution.

See [“About importing assets from Altiris”](#) on page 335.

Installing Asset Export Task on Altiris Notification Server

You use Symantec Installation Manager to install the Control Compliance Suite (CCS) Asset Export Task solution.

You must install the solution on Altiris Notification Server 7.0.

To install the CCS Asset Export Task

- 1 Start Symantec Installation Manager.
- 2 On the **Installed Products** page, click **Install new products**.
- 3 On the **Install New Products** page, check **CCSAssetExport**, and then click **Review selected products**.

- 4 On the **Selected Products and Features** page, verify that you selected the correct product, and then click **Next**.
- 5 On the **End User License Agreement** page, check **I accept the terms in the license agreements**, and then click **Next**.
- 6 On the **Contact Information** page, type the required information, and then click **Next**.
- 7 On the **Computers to Manage** page, click **Begin install** to begin the installation.
- 8 On the **Installation Complete** page, click **Finish**.

You can now launch the Symantec Management Console to access the CCS Asset Export Task solution.

See [“Working with the Altiris Asset Export Task solution”](#) on page 338.

See [“About importing assets from Altiris”](#) on page 335.

Working with the Altiris Asset Export Task solution

You must perform certain tasks on Control Compliance Suite (CCS) and Altiris Notification Server to import assets successfully from the Altiris CMDB.

In the CCS console, perform the following tasks:

- Configure a CSV data collector to import assets from the CSV file on Altiris Notification Server.
See [“Configuring the CSV data collector”](#) on page 129.
- Create asset import jobs for Windows and UNIX asset types.
See [“Creating the Altiris asset import jobs in Control Compliance Suite Console”](#) on page 339.

In the **Altiris Symantec Management Console**, perform the following tasks:

- Provide the Web Service URL to import assets into the CCS asset system.
See [“Specifying the asset export settings in the Altiris Symantec Management Console”](#) on page 340.
- Create a CCS asset export task.
See [“Creating a asset export task in the Altiris Symantec Management Console”](#) on page 341.
- Schedule the CCS asset export task.
See [“Scheduling asset export task in the Altiris Symantec Management Console”](#) on page 342.

See [“About importing assets from Altiris”](#) on page 335.

Creating the Altiris asset import jobs in Control Compliance Suite Console

The CSV data collector is used to import the assets from the Altiris CMDB database to the Control Compliance Suite (CCS) asset system. You must configure the CSV settings for the Windows and UNIX platforms to import the assets.

See [“Configuring the CSV data collector”](#) on page 129.

To create an Altiris asset import job

- 1 In the CCS console, go to **Manage > Assets > Asset System**.
- 2 On the taskbar, from the **Asset Tasks** select **Import Assets**.
- 3 In the **Specify Name and Description** panel, in the Name box, type the name for the import job.

You can optionally type the description for the import job and click **Next**.

- 4 In the **Select Platform, Asset Type, and Data Collector** panel, do the following:
 - Select the platform and the asset type for which to import the assets. Windows and UNIX are the predefined asset types that are supported.
 - From the Data collector drop-down list, select **CSV Data Collector** and click **Next**.
- 5 In the **Select Asset Import Scope** panel, do the following:
 - Click the browse ... icon to select the scope for the asset type. Depending upon the asset type that you select in the previous panel, the default scope is selected as a Site or an asset type. See [“About scopes in asset import”](#) on page 287.
 - In the **Limit Asset Import Scope** dialog box, select the additional scope from the list of the supported scopes and click **OK**.
 - In the **Select Asset Import Scope** dialog box, in the left pane, browse through the assets hierarchy and select a folder to add the assets from. In the right pane, select the folder, asset group, or asset and then click **Add** to add it as a scope. Click **Next**.
- 6 In the **Add Reconciliation Rules** panel, you can add, delete, and move the order of the reconciliation rules.

To add rules, do the following:

- Click **Add Rules**.

- In the **Select Reconciliation Rules** panel, browse through the Reconciliation Rules folder and use the **Add** option to add the existing reconciliation rules to the import job.
Click **OK**.
 - In the **Add Reconciliation Rules** panel, click **Next**.
- 7 In the **Specify Asset Field Filters** panel, you can configure the asset field filters.
- The fields in this panel are specific to the asset type that you want to import. You can select a field that should be used as a filter for the selected asset type and create a filter statement.
- To add a filter, do the following:
- Select a statement from the drop-down list , and click **Add Statement**.
 - In the **Create Filter Statement** dialog box, use the parameter type and the conditions to create a filter statement and click **OK**.
See [“Examples of asset filters”](#) on page 242.
See [“Filter statement operators”](#) on page 243.
 - After you add the filters, click **Next**.
- 8 In the **Schedule** panel, select any one of the schedule options.
- 9 In the **Specify Notification Details** panel, if you want to send the notification of job completion or job failure, do the following:
- Type the subject and message of the notification mail.
 - Type the email ID of the sender and the receiver.
- 10 In the **Summary** panel, review the configurations for the import job and click **Finish**.
- You can go to the Monitor > Jobs view to monitor the current status of the job.
- See [“About importing assets from Altiris”](#) on page 335.

Specifying the asset export settings in the Altiris Symantec Management Console

You must specify the Control Compliance Suite (CCS) asset export task settings to run the CCS asset import jobs.

The asset import job in CCS is run using a CCS Web Service. You must provide the URL to the Web Service to import the assets into the CCS asset system.

To specify the settings

- 1 In the Altiris Notification Server Management Console, in the **Settings** menu, click **Notification Server > CCS Asset Export Task Setting**.
- 2 Type the Web Service URL. If SSL is enabled, use https://.
 http://<webservicehostname>/CCS_WebServices/AssetImportService.asmx
- 3 Type the number of days that you want to retain a CSV file. Any CSV files that are older than the number of days entered is deleted from the folder.
- 4 Click **OK** to save.

See [“About importing assets from Altiris”](#) on page 335.

Creating a asset export task in the Altiris Symantec Management Console

The Control Compliance Suite (CCS) Asset Export Task must be installed on Notification Server before you can run the task.

See [“Installing Asset Export Task on Altiris Notification Server”](#) on page 337.

When you create a new task, there may be a time delay to store the credentials. Therefore, if you schedule to run a job immediately after you create a new task, the job might fail. You may have to reschedule the job.

To create a CCS asset export task

- 1 In the Altiris Notification Server Management Console, in the **Manage** menu, click **Jobs and Tasks**.
- 2 In the left pane, expand **Jobs and Tasks > System Jobs and Tasks > Notification Server**.
- 3 Right-click **Notification Server** and select **New > Job or Task**.

- 4 On the **Create New Task** page, type the following information:

Specify export location	Type the location where the CSV files are stored. See “About the CSV files on Altiris Notification Server” on page 343.
Specify credentials	Type the user name and the password that is required to access the CSV file and run the asset import job on CCS.
Specify import job to run	Select the asset import job. The listed asset import jobs are created in CCS. See “Creating the Altiris asset import jobs in Control Compliance Suite Console” on page 339.

- 5 Click **Apply**.
 - 6 Select the computers for which you want to run the asset import job.
 - 7 Click **OK**.
- After you create an export task, you must set up the schedule to run the task.
- See [“Scheduling asset export task in the Altiris Symantec Management Console”](#) on page 342.
- See [“About importing assets from Altiris”](#) on page 335.

Scheduling asset export task in the Altiris Symantec Management Console

After you create a Control Compliance Suite (CCS) asset export task, you must schedule the task to export the assets to a CSV file. The assets are then imported into the CCS asset system from the CSV file.

When you create a new task, there may be a time delay to store the credentials. Therefore, if you schedule to run a job immediately after you create a new task, the job might fail. You may have to reschedule the job.

To schedule the CCS asset export task

- 1 In the Altiris Notification Server Management Console, in the **Manage** menu, click **Jobs and Tasks**.
- 2 In the left pane, expand **Jobs and Tasks > System Jobs and Tasks > Notification Server**.

- 3 In the left pane, under **Notification Server**, select the task to schedule.
- 4 In the **New Schedule** page, provide the following information:

Now	Select this option if you want to run the job immediately.
Schedule	Select this option if you want to run the job at a specified time.

- 5 Click **Schedule**.

You can now go to the CCS console's **Monitor > Jobs** view to monitor the status of the job.

See [“Creating a asset export task in the Altiris Symantec Management Console”](#) on page 341.

See [“About importing assets from Altiris”](#) on page 335.

About the CSV files on Altiris Notification Server

When the scheduled Control Compliance Suite asset export task runs, the resources from the Altiris Configuration Management Database (CMDB) are exported to a CSV file. The resources that are exported depends on the type of asset import job that is selected in the task. A CSV file is created per asset type. The CSV files are purged according to the settings in the CCS Asset Export Task Setting page.

See [“Specifying the asset export settings in the Altiris Symantec Management Console”](#) on page 340.

On the Notification Server, the CSV files are created with the following syntax
CCS_<AssetType>_<DateTime>_<GUID>.csv.

See [“About importing assets from Altiris”](#) on page 335.

See [“Creating a asset export task in the Altiris Symantec Management Console”](#) on page 341.

Managing custom schema

This chapter includes the following topics:

- [About the custom schema](#)
- [Working with custom asset types](#)
- [Working with custom entity](#)
- [Working with custom target type](#)
- [Working with custom schema scenarios](#)

About the custom schema

Control Compliance Suite provides certain predefined asset types that you can use to import the assets into the asset system. Asset types let you import the asset data for a collection of fields that belong to a specific entity. In the process of managing the assets in the system, you might need to create your custom asset types to manage the assets that are outside the scope of the predefined asset types.

Control Compliance Suite lets you create your own schema for the asset types and the entities. In addition, you can also extend the schema for the predefined asset types and extend the custom entity schema. You can also create new target types and edit the newly created target types.

In addition, you can also edit the existing asset type and existing entity schema. The Schema Manager gives you the option to switch the CSV or ODBC data collectors for the custom and common platforms.

You can create and edit the following types of schema

- Asset type schema
See [“About the asset type schema”](#) on page 346.
- Entity schema

See [“About the entity schema ”](#) on page 347.

- Target type schema

See [“About the target type schema”](#) on page 347.

See [“Working with custom schema scenarios”](#) on page 367.

See [“Working with custom asset types”](#) on page 348.

See [“Working with custom entity”](#) on page 356.

See [“Working with custom target type”](#) on page 365.

About the Schema Manager view

The Schema Manager view lets you create or extend the asset type schema and the entity schema. The view also lets you create a new target type or edit an existing target type.

You can access the Schema Manager view from Settings > Schema Manager.

You can do the following from the Schema Manager view:

See [“About the asset type schema”](#) on page 346.

See [“About the entity schema ”](#) on page 347.

See [“About the target type schema”](#) on page 347.

About the asset type schema

The assets are stored in the asset store in the CCS directory. Each asset type in the CCS directory has its own schema. Control Compliance Suite supports some predefined asset types.

See [“Predefined asset types”](#) on page 204.

The assets schema includes the following types of schema:

- Asset type schema

Each asset type is a separate entity and has no relation with the other asset types. Each asset type has some primary fields. The primary fields are used to uniquely identify the asset in the CCS directory.

- Asset base schema

The asset base schema represents the asset fields that are common across all the asset types. The common fields of the asset type include, Integrity, Confidentiality, Availability, Tags, Asset Custodian, Asset Department, Asset Owner, Asset Location, and Asset Site.

Control Compliance Suite lets you create your own asset type schema and extend the existing asset type schema to manage your assets.

See [“Creating a new asset type”](#) on page 348.

See [“Extending an existing asset type”](#) on page 351.

About the entity schema

An entity schema in Control Compliance Suite is the blueprint that contains the asset information, which is used to create an asset type. Once the asset type is defined, the registered data collectors import the assets into the infrastructure based on the defined schema. The data collectors of Control Compliance Suite also collect data from the imported assets.

An entity schema interprets data only if the data is defined in a specific format. For every asset, data must be defined in a format that contains attributes such as platform, entity, and fields. The entity schema is a set of XML definitions, which represent the defined attributes.

In Control Compliance Suite, you can define an entity schema for any custom application for which you want to collect data. Data for the application must be imported to a comma-separated value (CSV) file and arranged in a specific format for the entity schema. The CSV data collector of Control Compliance Suite collects data from the CSV file.

You can also define an entity schema for any custom application and collect data for the asset using the ODBC data collector.

See [“About the predefined platforms and the primary entities”](#) on page 353.

You can create a new entity schema or extend an existing entity schema using the appropriate tools from Settings > Schema Manager view of the console.

See [“Creating a new entity schema”](#) on page 360.

See [“Extending an existing entity schema”](#) on page 364.

About the target type schema

You select a target type to evaluate a set of assets against a standard. The standards are based on the asset types. You cannot evaluate an asset of the type Oracle Configured Database against an ESM standard.

Control Compliance Suite lets you create your own target types to filter the assets of a particular asset type for evaluation.

Consider the following example:

Windows machines is a predefined asset type. If you want to evaluate a standard only for the Windows XP machines, the Windows XP machines can be your target type.

See [“Creating a new target type”](#) on page 365.

See [“Editing a target type”](#) on page 366.

Working with custom asset types

Control Compliance Suite lets you create custom asset types from the custom platforms and custom entities that you can create from the Schema Manager view.

See [“About the entity schema”](#) on page 347.

You can import the assets from the custom asset types in the same way as you import the assets from the predefined or probable asset types.

Asset types are based on the entities of the platform. In Control Compliance Suite, a platform is defined as the category to which a group of entities belong. A group of fields that define the common functions of the network element form an entity.

See [“About platforms”](#) on page 356.

See [“About entities”](#) on page 356.

When you create your own platform and defined fields for the platform to create an entity, you can define an asset type also. The custom asset type imports the data of the fields that are defined in the custom entity.

You can create the custom asset types from the Schema Manager view. Go to Settings > Schema Manager > Add new asset type to get started with the creation of a custom asset type.

See [“Creating a new asset type”](#) on page 348.

See [“Extending an existing asset type”](#) on page 351.

Creating a new asset type

Control Compliance Suite lets you create a custom asset type that you can use for importing assets.

The creation of a new asset type involves the following steps:

- Choose your own platform and the primary entity to create the asset type.
See [“Asset types”](#) on page 203.
- Specify the fields that should be included in the newly created asset type.
You can specify the fields for the referenced entity also.
See [“About referenced entity fields”](#) on page 354.
- Mark the fields as mandatory or optional.
See [“About the primary, mandatory, and optional fields”](#) on page 354.

- Add a new field that has no reference to the entity schema.
See [“About separators in name fields”](#) on page 355.
- Add asset name fields.
See [“About separators in name fields”](#) on page 355.
- Close the Control Compliance Suite Console, Restart the Symantec Application Server Service, and re-launch the Console.

Note: Before creating a new asset type you must know that an asset type once created or a field once added to the asset type cannot be deprecated.

To create a new asset type

- 1 Go to Settings > Schema Manager.
- 2 Select **Add new asset type**.
- 3 In the Specify Asset Type Details panel, do the following:
 - Type the name of the asset type that you want to create in the Name field.
The asset type name should not include spaces and should not exceed 10 characters.
 - Type the display name and the description for the asset type in the Display name and Description fields and click **Next**.
- 4 In the Select Platform and Primary Entity panel, do the following:
 - From the Platform drop-down list, select a platform for which you want to create an asset type.
The list of platforms includes the predefined platforms and any custom platform that you have already created.
 - From the Primary entity drop-down list, select a primary entity for the selected platform and click **Next**.
See [“About the predefined platforms and the primary entities”](#) on page 353.
- 5 In the Specify Fields panel, select the fields from the Available fields list and add the fields in the Selected fields list with the Add icon.

By default, the primary fields for the primary entity are listed in the Available fields list.

- 6 Select **Include referenced entities** if you want to add the fields for the referenced entities and click **Next**.

If you select this option, the referenced entities appear in the Entity drop-down list. You can then select a referenced entity and add the fields for the referenced entities.

See [“About referenced entity fields”](#) on page 354.

- 7 In the Customize Field Attributes panel, you can mark the fields as mandatory or optional and click **Next**.

You mark the fields as mandatory or optional that are not primary fields. You can also specify if the field is a part of the asset import and if the field is editable.

See [“About the primary, mandatory, and optional fields”](#) on page 354.

- 8 In the Add External Fields panel, click **Add** to add an external field.

See [“Creating an external field to add to the asset type”](#) on page 352.

- 9 In the Specify Asset Name Fields, select the fields from the Available fields list. Use the Add icon to add to add the fields to the Selected fields list.

Click **Next**.

You can use the separators to add multiple asset name fields and to specify the relation among the multiple fields.

See [“About separators in name fields”](#) on page 355.

- 10 In the Summary panel, review the selections that you made for the custom asset type and click **Finish**.

- 11 Restart the Symantec Application Server service and relaunch the Console.

See [“Viewing the custom asset type and the custom fields in the asset system”](#) on page 350.

See [“Extending an existing asset type”](#) on page 351.

Viewing the custom asset type and the custom fields in the asset system

You can view the custom asset type in the asset system after you create an asset type from the Create new Asset Type wizard.

To view the custom asset type in the asset system

- 1 Go to Start > Run and type **services.msc**.
- 2 In the Services console, right-click the Symantec Application Server Service and select **Restart**.
- 3 Close the Control Compliance Suite Console and relaunch the console after waiting for two minutes.
- 4 Go to Manage > Assets > Asset System.
- 5 Check if the newly created asset type appears in the Display drop-down list that appears in the taskbar .

You can view the newly added mandatory, optional, or external fields after you import the assets from the custom asset type.

To view the custom fields in the asset system:

- 1 Go to Manage > Assets > Asset System.
- 2 Select the asset type for which you imported the assets.
- 3 Select an asset for which you want to view the custom field information.
- 4 In the details pane, go to Custom Properties tab.

The newly added fields appear.

See [“Creating a new asset type”](#) on page 348.

Extending an existing asset type

Control Compliance Suite lets you extend the existing asset types by modification of the default fields and addition of the optional fields to the asset types.

Note: Before extending an existing asset type you must know that a field once added to the asset type cannot be deprecated.

To extend an existing asset type

- 1 Go to Settings > Schema Manager.
- 2 Select **Extend existing asset type**.
- 3 In the Select Asset Type panel, select an asset type that you want to extend and click **Next**.

The primary, mandatory, and optional fields for the selected asset type are displayed.

- 4 In the Select Optional Fields panel, select the fields from the Available fields list and add the fields in the Selected fields list with the Add icon.
- 5 Select **Include referenced entities** if you want to add the fields for the referenced entities and click **Next**.

If you select this option, the referenced entities appear in the Entity drop-down list. You can then select a referenced entity and add the fields for the referenced entities.

See [“About referenced entity fields”](#) on page 354.

- 6 In the Customize Field Attributes panel, you can choose to include the fields in the data collection job and mark them editable.

When you extend an existing asset type, you can only add the optional fields. The optional fields are not required for data collection. You can explicitly mark the field to include in the data collection job.

Click **Next**.

- 7 In the Add External Fields panel, click **Add** to add an external field.

See [“Creating an external field to add to the asset type”](#) on page 352.

- 8 In the Summary panel, review the selections that you made for the custom asset type and click **Finish**.

See [“Creating a new asset type”](#) on page 348.

Creating an external field to add to the asset type

Control Compliance Suite gives you a flexibility to create external fields that have no reference to the entity schema. The data for the external fields cannot be imported from the data collectors. You can manually specify values for the external fields from the details pane or use the pre reconciliation rules to set the value.

To create an external field to add to the asset type

- 1 From the Add External Fields panel in the Create New Asset Type wizard, click **Add**.
- 2 In the Add New Field dialog box, type the name of the new field in the Field name box.
- 3 Type the display name and the description for the field.
- 4 Select the type of the field from the following options:
 - String
 - Integer

- Boolean
 - DateTime
- 5 Check **Allow editing of field** to mark the field as editable.
- 6 Check **Is case sensitive** to mark the field as case sensitive.
- 7 Check **Is array** to mark the field as an array.
- See [“Creating a new asset type”](#) on page 348.
- See [“Creating a new entity schema”](#) on page 360.

About the predefined platforms and the primary entities

The Control Compliance Suite provides certain primary entities for the predefined platforms as predefined asset types.

See [“Predefined asset types”](#) on page 204.

In addition to the predefined asset types, the Control Compliance Suite also defines certain primary entities that you can use to create custom asset types.

See [“Probable asset types”](#) on page 227.

Control Compliance Suite provides the following primary entities for the predefined platforms to create asset types:

Enterprise Security Manager	Agent
Oracle	<ul style="list-style-type: none">■ CONFIGUREDDATABASES■ CONFIGUREDSERVERS
SQL	<ul style="list-style-type: none">■ Database■ Server■ Stored Procedure■ User
UNIX	<ul style="list-style-type: none">■ File■ Group■ Machine■ User

Windows

- Directory
- Domain
- File
- Group
- IISVirtualDirectories
- IISWebSite
- Machine
- Registry
- Service

See [“Creating a new asset type”](#) on page 348.

See [“Creating a new entity schema”](#) on page 360.

About the primary, mandatory, and optional fields

The primary fields are the identifier fields. The primary fields are used to identify the asset type exclusively.

The mandatory fields are the fields that are required for data collection and evaluation. Without the presence of the mandatory fields, the asset is not imported into the asset system.

The optional fields are the fields that are not required for asset import, data collection, or evaluation. The new fields that you can add to the custom asset type are optional fields. They have no reference to the entity schema.

See [“Creating a new asset type”](#) on page 348.

See [“Creating a new entity schema”](#) on page 360.

About referenced entity fields

A referenced entity is a parent entity. You can choose to include the fields of the referenced entity along with the fields of the primary entity in the custom schema.

Consider the following example:

- You select Windows File as the primary entity to create a new asset type.
- You choose to include the referenced entity fields also in the new asset type. The parent or referenced entities for the Windows File are Domain, Machine, and Group.
- You create a new asset type. When you run a job that is based on the new asset type, the job also collects the information about the referenced fields.

- If the data for the Windows File asset type contains information about the Domain, the import job also returns the data for the domain.

See [“Creating a new asset type”](#) on page 348.

See [“Creating a new entity schema”](#) on page 360.

About separators in name fields

You use the separators to set the format to display the asset name on the Control Compliance Suite console.

For the assets that belong to the predefined asset types, the default format to display the asset name is as follows:

```
domain name\machine name\file name with full path
For example, CMCT\2k3-105-133\c:\boot.ini
```

The backslash mark (\) is a separator that is used to display the asset name. The domain name, the machine name, and the file name are the name fields that are used to form the asset name.

When you create a custom asset type, you can use one or more available asset name fields and use a separator from the given list. The asset name for the custom asset type that you create is displayed in the format that you specify.

Consider the following selections:

Platform	SQL
Primary entity	Database
Asset name fields	Database name, Host name (node), and Server name (instance)
Separator	#

In case of the selections that are specified, the asset name format should be as follows:

```
Database name#Host name (node)#Server name (instance)
```

Note: You cannot edit the naming convention once you create an asset type with the convention.

See [“Creating a new asset type”](#) on page 348.

See [“Extending an existing asset type”](#) on page 351.

Working with custom entity

A custom entity comprises a group of fields.

See [“About entities”](#) on page 356.

The entity schema can be created using the Create new entity schema tool of the Schema Manager. The Schema Manager can be accessed through the Settings > Schema Manager option of the console.

A custom entity must have unique identifiers known as primary keys, which are defined in the entity schema. Control Compliance Suite lets you extend an already created custom entity through the Extend entity schema tool of the Schema Manager.

See [“Creating a new entity schema”](#) on page 360.

See [“Extending an existing entity schema”](#) on page 364.

About platforms

In Control Compliance Suite, a platform is defined as the category to which a group of entities belong. For example, SQL can be a platform, which contains entities that define the SQL application.

See [“About entities”](#) on page 356.

The Control Compliance Suite supports certain predefined platforms that are recognized by the infrastructure for data collection. For every predefined platform, a default data collector of Control Compliance Suite performs the data collection. An entity schema contains the blueprint of a data collector and drives the data collector for data collection.

The predefined platforms of Control Compliance Suite are as follows:

- Windows
- UNIX
- SQL
- Oracle
- ESM

About entities

An entity is formed by a group of fields that define the common functions of the network element. The entity encapsulates the properties of an asset type, based on which an asset type can be created.

For example, for a Windows platform, you can define an entity such as Machines, which contains fields that define the entity. Fields such as machine name, IP address, netmask, and CPU usage, and so on can define the Machine entity.

See [“About platforms”](#) on page 356.

See [“About fields of an entity ”](#) on page 357.

About fields of an entity

A field contains definitions of a network element. A network element can be a router, directory, server, desktop, or any entity that functions on set parameters.

For example, in Windows server computer, the directories can be the entities. The directories can be defined by parameters such as the disk-occupied size in bytes, directory location in the computer, and user privileges to access. The fields such as disk space, location, and users can be used to define the directory parameters.

Fields are an integral part of the entity schema for defining an asset type. In an entity schema, fields are defined for an entity. An entity can contain as many fields as are required to define the asset type. A configured data collector collects data for the fields that are specified in the entity schema.

See [“About the entity schema ”](#) on page 347.

See [“About platforms”](#) on page 356.

See [“About entities”](#) on page 356.

About setting tasks to roles for entity schema

To create an entity schema through the Control Compliance Suite console, you must have permission to execute specific tasks. The tasks are associated with the role that is assigned to you.

You must have the following tasks associated with your role to create an entity schema:

- Manage Configuration Settings
- Manage Schema

By default, the role, CCS_Administrator is provided permission for all the tasks to create an entity schema. If you are not assigned the CCS_Administrator role, then create a custom role through the Settings >Role view of the console.

See [“Creating a custom role”](#) on page 92.

See [“Creating a new entity schema”](#) on page 360.

About relationships between the predefined entities

In Control Compliance Suite, there is defined relationship between the predefined entities of the predefined platforms. The relationship is between the fields of the predefined entities. Such relationships between the predefined entities facilitate broader scope of collecting data for a custom entity. The scope of collecting data broadens whenever a custom entity extends a predefined entity.

You must know the relation between the predefined entities of all the predefined platforms. You can use the relationship between the predefined entities to reference the custom entity. The Create new entity schema wizard is used to reference a custom entity during creation.

See [“Creating a new entity schema”](#) on page 360.

Table 7-1 relationship details of the predefined entities for the Oracle platform

Predefined entity	Relation entity
CONFIGUREDDATABASES	CONFIGUREDSERVERS of the Oracle platform
CONFIGUREDSERVERS	The CONFIGUREDSERVERS entity is referenced to the following predefined entities: <ul style="list-style-type: none">■ Machine entity of the Windows platform■ Machine entity of the UNIX platform

Table 7-2 relationship details of the predefined entities for the SQL platform

Predefined entity	Relation entity
Database	Server of the SQL platform
Server	Machine of the Windows platform
Stored Procedure	The Stored Procedure entity is referenced to the following predefined entities: <ul style="list-style-type: none">■ Database of the SQL platform■ Server of the SQL platform
User	The User entity is referenced to the following predefined entities: <ul style="list-style-type: none">■ Database of the SQL platform■ Server of the SQL platform

Table 7-3 relationship details of the predefined entities for the UNIX platform

Predefined entity	Relation entity
File	Machine of the UNIX platform
Group	Machine of the UNIX platform
Machine	No defined relationship
User	Machine of the UNIX platform

Table 7-4 relationship details of the predefined entities for the Windows platform

Predefined entity	Relation entity
Directory	<p>The Directory entity is referenced to the following predefined entities:</p> <ul style="list-style-type: none"> ■ Machine of the Windows platform ■ Domain of the Windows platform
Domain	No defined relationship
File	<p>The File entity is referenced to the following predefined entities:</p> <ul style="list-style-type: none"> ■ Machine of the Windows platform ■ Domain of the Windows platform ■ Directory of the Windows platform
Group	<p>The Group entity is referenced to the following predefined entities:</p> <ul style="list-style-type: none"> ■ Machine of the Windows platform ■ Domain of the Windows platform
IISVirtualDirectories	<p>The IISVirtualDirectories entity is referenced to the following predefined entities:</p> <ul style="list-style-type: none"> ■ Machine of the Windows platform ■ Domain of the Windows platform
IISWebSite	<p>The IISWebSite entity is referenced to the following predefined entities:</p> <ul style="list-style-type: none"> ■ Machine of the Windows platform ■ Domain of the Windows platform
Machine	Domain of the Windows platform

Table 7-4 relationship details of the predefined entities for the Windows platform *(continued)*

Predefined entity	Relation entity
Registry	<div>The Registry entity is referenced to the following predefined entities:</div> <div><div>■ Machine of the Windows platform</div><div>■ Domain of the Windows platform</div></div>
Service	<div>The Service entity is referenced to the following predefined entities:</div> <div><div>■ Machine of the Windows platform</div><div>■ Domain of the Windows platform</div></div>

Creating a new entity schema

You can create a new entity schema for a custom application through the Schema Manager of the Control Compliance Suite Console. The entity schema defines the platform, entities, and fields of an asset for which data is to be collected. You can create a new entity schema only when you do not want to use any of the predefined platforms for data collection.

Note: Before you create a new entity schema you must know that the entities and platforms cannot be deprecated.

See [“About platforms”](#) on page 356.

After you create an entity, you must create the custom asset types, which are later imported into Control Compliance Suite using the Asset Import wizard.

See [“Creating a new asset type”](#) on page 348.

Note: Every custom asset type that you create from a custom entity can scope to Site and the asset type itself when importing assets. The assets are imported using the Asset Import wizard.

To create a new entity schema

- 1 Go to Settings > Schema Manager.
- 2 Select **Create new entity schema** to launch the **Create New Entity Schema** wizard.

- 3 In the **Select or Create New Platform** panel, select either option and click **Next**.

Specify the values for the following fields:

- Create new platform
- Use existing platform

- 4 In the **Specify Entity Details** panel, enter the values for the fields and click **Next**.

Specify the values for the following fields:

- Name
- Display name
- Description
- Extend an existing entity
- Folder path

- 5 In the Add Fields panel, click **Add** to add new fields for the entity.

- 6 In the Create New Field dialog box, enter the values for the fields and click **OK**.

Specify the values for the following fields:

- Field name
- Display name
- Description
- Type
- Is case sensitive
- Is array

The added field details are displayed in the **Add Fields** panel. You must check the option, **Is primary key** if you want to declare the field as a primary key. Unchecking the option makes the added fields optional.

If you have extended a predefined entity (in the **Specify Entity Details** panel), then you must ensure that the number of primary keys for the creating entity is same as that of the extended entity.

- 7 In the **Add Fields** panel, click **Next**.

- 8 In the **Specify Entity Name Fields** panel, select the primary fields that are listed in the Available fields column and use the Add icon to add them to the **Selected fields** column.

The fields that are selected constitute the name of the assets that are created for the entity, which in turn defines the asset type.

Click **Next**.

- 9 In the **Specify References** panel, associate the fields of the entity with a parent entity and click **Next**.

Select the Platform, Parent entity, and fields from the drop-down boxes for associating the created entity as a child entity and click **Add**.

The panel lets you create relationship between the new entity and an entity of the predefined platform. A parent-child relationship is created between the entity of the predefined platform and the new entity that you are creating. You can associate the primary fields of the new entity with the primary fields of the parent entity to create a parent-child relationship. The parent-child relationship lets you collect data for the parent entity along with the child entity.

When you extend an entity, you must create a reference with the extended entity. You can also create a reference with the entity with which the extended entity shares a relationship. The relationship between the predefined entities are defined in Control Compliance Suite.

See [“About relationships between the predefined entities”](#) on page 358.

10 In the Summary panel, review the details of the created entity and click **Finish**.

The entity schema creates three XML files for the new platform, new entity, and the common platform respectively. You must put the XML files in the specific directories of every computer on which a CCS component is installed and restart the services.

The directories where the XML files are to be placed are as follows:

Installation directory of the Reporting and Analytics	<div><install directory> \Symantec\CCS\Reporting And Analytics</div> <div>For example, C:\Program Files\Symantec\CCS\Reporting And Analytics</div>
Installation directory of the Application Server	<div><install directory>\Symantec\CCS\Reporting And Analytics\Application Server</div> <div>For example, C:\Program Files\Symantec\CCS\Reporting And Analytics\Application Server</div>
Installation directory of the Data Processing Service (DPS)	<div><install directory>\Symantec\CCS\Reporting And Analytics\DPS</div> <div>For example, C:\Program Files\Symantec\CCS\Reporting And Analytics\DPS</div> <div>Note: For a distributed setup mode, if you have more than one DPS, then copy all the schema XML files to the computers on which DPS is installed.</div>

See [“Extending an existing entity schema”](#) on page 364.

Extending an existing entity schema

Control Compliance Suite lets you extend an existing entity schema to add new fields. You can extend a schema that you have earlier created.

Note: Before you edit the existing entity schema you must know that the entities once edited cannot be deprecated.

To extend an existing schema

- 1 Go to Settings > Schema Manager.
- 2 Select **Extend existing entity schema** to launch the Extend Entity Schema wizard.
- 3 In the Select Entity panel, select an existing platform and provide details for the entity that is to be extended.
Click **Next**.
- 4 In the Select Fields panel, click **Add** to add new fields for the entity.
The added fields are optional for the entity.
- 5 Click **Next**.
- 6 In the Summary panel, review the details of the fields and click **Finish**.

See [“Creating a new entity schema”](#) on page 360.

Working with custom target type

A target type is used to filter the assets during the data collection and the evaluation process.

See [“About target types”](#) on page 455.

A custom target type must be created when you want to collect data and run an evaluation for the custom asset type.

See [“Creating a new asset type”](#) on page 348.

See [“Working with custom asset types”](#) on page 348.

You can create a target type from the Schema Manager view.

The Schema Manager view lets you perform the following tasks that are related to target types:

- Create a new target type
See [“Creating a new target type”](#) on page 365.
- Edit a target type
See [“Editing a target type”](#) on page 366.

Creating a new target type

You need to create a custom target type to be able to collect data and run an evaluation for the custom asset type. You can create a new target type for both predefined as well as custom asset types.

To create a target type

- 1 Go to Settings > Schema Manager.
- 2 Click **Create New Target Type**.
- 3 In the Specify Name and Description for Target Type panel, type the name and description for the new target type. Click **Next**.
- 4 In the Select Platform and Asset Type panel, select an asset platform in the Platform list. Select an asset type in the Asset Type list.

The custom platform, the custom asset types, and the predefined asset types are available for selection in the drop-down list.
- 5 In the Create Asset Type filters panel, click **Add Statement** to add a filter statement.
- 6 In the Filter Statement dialog box, select an operator and in the Specify Value box, type a value. Click **OK**.
- 7 In the Create Asset Type filters panel, click **Next**.
- 8 In the Summary panel, review the information that you have entered in the wizard. Click **Back** to make any modifications or click **Finish** to exit the wizard.

Go to Manage > Standards. The new target type is available for selection in the Specify Name and Target Type panel of the Create Check wizard.

Editing a target type

You can edit only the custom target types. You cannot edit a predefined target type.

To edit a target type

- 1 In the **Select Target Type** panel, select the relevant asset platform and the asset type.
- 2 In the **Target Type** box, check the target type that you want to edit. Click **Next**.
- 3 In the **Specify Name and Description for Target Type** panel, you can edit the name and the description of the target type. Click **Next**.
- 4 In the **Edit Asset Type** filters panel, you can do either of the following:
 - To edit a filter statement, select the statement and click **Edit**.
 - To delete a filter statement, select the statement and click **Delete**.
- 5 To add a filter statement, click **Add Statement**.

- 6 In the **Filter Statement** dialog box, select an operator and in the Specify Value box, type a value. Click **OK**.
- 7 In the **Edit Platform and Asset Type** panel, click **Next**.
- 8 In the **Summary** panel, review the information that you have entered in the wizard. Click **Back** to make any modifications or click **Finish** to exit the wizard.

Working with custom schema scenarios

You use the Schema Manager to create or extend the entity schema, asset type, and the target type.

Go through the following scenarios and perform the tasks in the given order to understand the application of the custom schema functionality in the process of managing assets.

Table 7-5 Custom schema scenarios

Scenario	How to achieve?
You want to create a custom asset type, Windows Service.	<p>Use the Add new asset type option on the Schema Manager view.</p> <p>For a detailed procedure of how to create a custom asset type, Windows Service, click on the link:</p> <p>See “Creating a custom asset type - Windows Service” on page 368.</p>
You want to add a new field, TCP/IP Address to the Windows Machine asset type.	<p>Use the Extend existing asset type option on the Schema Manager view.</p> <p>For a detailed procedure of how to add TCP/IP Address to the Windows Machine, click on the link:</p> <p>See “Extending the predefined asset type - Windows Machine” on page 370.</p>

Table 7-5 Custom schema scenarios (continued)

Scenario	How to achieve?
You want to extend the Windows Machine asset type to manage the inventory information.	<ul style="list-style-type: none">■ Use the Create new entity schema option on the Schema Manager view.■ Create a new entity Inventory with relevant fields that are required to manage the inventory.■ Use the Extend existing asset type option.■ Add the inventory fields to the Windows Machine asset type. <p>For a detailed procedure click on the link:</p> <p>See “Extending Windows Machine to manage inventory and vendor data information” on page 371.</p>
You want to create custom asset types printers, scanners, monitors, and so on to manage the physical devices in the enterprise.	<ul style="list-style-type: none">■ Use the Create new entity schema option on the Schema Manager view,■ Create a new platform Devices and a new entity Printer.■ Use the Add new asset type option on the Schema Manager view.■ Create a new asset type, Printer based on the custom platform, Devices. <p>For a detailed procedure click on the link:</p> <p>See “Creating a custom asset type-Printer based on the custom platform-Devices” on page 375.</p>

Creating a custom asset type - Windows Service

In the scenario, create a custom asset type, Windows Service. You must use the Add new asset type option in the Schema Manager view to create the custom asset type.

Windows is one of the predefined platforms that the Control Compliance Suite supports.

See [“Predefined platforms”](#) on page 203.

Service is one of the primary entities that is not supported as a predefined asset type. Service can be a probable asset type.

See [“Probable asset types”](#) on page 227.

To create a Windows Service asset type

- 1 Go to Settings > Schema Manager.
- 2 Select **Add new asset type**.
- 3 In the Specify Asset Type Details panel of the Create New Asset Type wizard, type **WindowsService** in the Name field.
- 4 In the Select Platform and Primary Entity panel, do the following:
 - From the Platform drop-down list, select **Windows**.
 - From the Primary entity drop-down list, select **Service** .
By default, the primary fields are listed in the Primary fields list.
The primary fields for the Windows Service are as follows:
 - Domain/Workgroup Name
 - Machine Name
 - Service NameClick **Next**
- 5 In the Specify Fields panel, add the following fields from the Available fields list.
 - Startup type
This field returns the method by which the service is started (automatic or manual)
 - Owner
This field returns the name of the account that currently owns the Service.
 - Status
This field returns the current status of the service process.
 - Service Type
This field returns the internal type of the service process. Valid values are Shared Process and Own Process.

- 6 In the Customize Field Attributes panel, mark, **Owner** as the mandatory field and mark **startup type**, **service type**, and **status** as the optional fields and click **Next**.
See [“About the primary, mandatory, and optional fields”](#) on page 354.
- 7 In the Add External Fields panel, click **Next**.
- 8 In the Specify Asset Name Fields, select all the fields from the Available fields list and use the Add icon to add the fields to the Selected fields list.
Click **Next**.
From the Separator drop-down list, select #.
See [“About separators in name fields”](#) on page 355.
- 9 In the Summary panel, review the selections that you made for the custom asset type and click **Finish**.
- 10 Close the Control Compliance Suite Console and restart the Symantec Application Server Service, Symantec Data Processing Server Service, and the Symantec Directory Support Service.
- 11 Launch the Control Compliance Suite Console and go to Manage > Assets > Asset System.
In the table pane, from the Display drop-down list, view the Windows Service asset type.

Extending the predefined asset type - Windows Machine

In the scenario, add the field TCP/IP Address to the predefined asset type, Windows Machine. You must use the Extend Asset Type wizard to add the field to the existing asset.

Control Compliance Suite lets you extend the existing asset types by modification of the default fields and addition of the optional fields to the asset types.

You can extend the predefined asset types and the custom asset types also.

To extend an existing asset type

- 1 Go to Settings > Schema Manager.
- 2 Select **Extend existing asset type** and click **Next**.
- 3 In the Select Asset Type panel of the Extend Asset Type wizard, from the Asset Type drop-down list, select **Windows Machine** and click **Next**.

The primary, mandatory, and optional fields for Windows Machine are displayed.

- 4 In the Select Optional Fields panel, select **TCP/IP Address (First)** from the Available fields list and add to the Selected fields list with the Add icon.
- 5 In the Customize Field Attributes panel, check the options **Is field part of job** and **Allow editing of field**.

When you extend an existing asset type, you can only add the optional fields. The optional fields are not required for data collection. You can explicitly mark the field to include in the data collection job.

Click **Next**.

- 6 In the Add External Fields panel, click **Next** without adding any external field.
- 7 In the Summary panel, review the selections that you made for the custom asset type.

Make sure that the field TCP/IP Address is available under the heading New Optional Fields and click **Finish**.

- 8 Close the Control Compliance Suite Console and restart the Symantec Application Server Service.
- 9 Launch the Control Compliance Suite Console and go to Manage > Assets > Asset System.
- 10 Select the Windows Machine asset type.

If you already have the assets for the Windows Machine, select an asset. In the details pane, under the Custom Properties tab, view the newly added field TCP/IP Address.

To import the values of the newly added field TCP/IP Address, go to Monitor > Jobs view and re-run the asset import job for Windows Machine.

Extending Windows Machine to manage inventory and vendor data information

Assume that you want to use the predefined asset type Windows Machine to manage the inventory and the vendor data.

Perform the following tasks:

- Create a new custom entity, Inventory using the Create new entity schema option from the Schema Manager view.
Click on the link to create a new entity, Inventory.
See [“Create a custom entity- Inventory”](#) on page 372.
- Extend the Windows Machine asset type to include the fields from the custom entity, Inventory, using the Extend asset type option from the Schema Manager view.

Click on the link to extend Windows Machine to include the fields from Inventory

See [“Extending Windows Machine to include the fields from Inventory”](#) on page 374.

Create a custom entity- Inventory

The entity schema defines the platform, entities, and fields of an asset for which the data collector collects data. You can create a new entity schema only when you do not want to use any of the predefined platforms for data collection.

To create a custom entity- Inventory

- 1 Go to Settings > Schema Manager.
- 2 Select **Create new entity schema** to launch the Create New Entity Schema wizard.
- 3 In the Select or Create New Platform panel, select **Create a new platform**.
In the Name box, type **Custom** and click **Next..**
- 4 In the Specify Entity Details panel, in the Name box, type **Inventory** as the name of the entity.
- 5 In the Specify Entity Details pane, select **Extend an existing entity**.
From the platform drop-down list, select **Windows**.
From the entity drop-down list, select **Machine**.
Select the folder path where you want to create the entity schema xml files and click **Next**.
- 6 In the Add Fields panel, click **Add** to add new fields for the entity.

- 7 In the Create New Field dialog box, create four fields as follows.

The number of primary fields for the new entity, Inventory must match the number of primary fields of Windows Machine. The objective to create the custom entity is to include the fields to the Windows Machine asset type. You must add the primary fields of Windows Machine as the primary fields of the entity, Inventory.

Let us add the four fields with the following details:

Domain/Workgroup Name - Primary	String data type
Machine Name- Primary	String data type
Vendor Name	String data type
Address of the Vendor	String data type
Date/Time of Contract Expiry	DateTime

Click **Next**.

- 8 In the Specify Entity Name Fields panel, select **Domain/Workgroup Name** and **Machine Name** from the Available fields list and add them to the Selected fields list.

The added primary fields form the name of the new entity.

From the list of Separators, select # and click **Next**.

- 9 In the Specify References panel, from platform list, select **Windows** and in the Parent entity list, select **Machine**.

Associate the fields of the <Windows>.<Machine> with the fields of the <Custom>.<Inventory> as follows:

Domain/Workgroup Name	Domain/Workgroup Name
Machine Name	Machine Name

The panel lets you create relation between the new entity and an entity of the predefined platform. A parent-child relation is created between the entity of the predefined platform and the new entity that you are creating. You can associate the primary fields of the new entity with the primary fields of the parent entity to create a parent-child relation. The parent-child relation lets you collect data for the parent entity along with the child entity.

See [“About referenced entity fields”](#) on page 354.

- 10 In the Summary panel, review the details of the created entity and click **Finish**.

- 11 Close the Control Compliance Suite Console.
- 12 Copy the XMLs at the following paths:
 - <installdir>\Symantec\CCS\Reporting and Analytics
 - <installdir>\Symantec\CCS\Reporting and Analytics\Application Server
 - <installdir>\Symantec\CCS\Reporting and Analytics\DPS
- 13 Restart the Symantec Application Server Service and the Symantec Data Processing Service and launch the Control Compliance Suite Console again.

Now that you have a custom entity Inventory that extends from Windows Machine, you can include the newly added fields to the Windows Machine.

See [“Extending Windows Machine to include the fields from Inventory”](#) on page 374.

Extending Windows Machine to include the fields from Inventory

After you create the entity Inventory and extend it from the Windows Machine asset type, you must now include the Inventory fields to the Windows Machine asset type.

Use the Extend existing asset type option on the Schema Manager view to include the Inventory fields to the Windows Machine.

To extend the Windows Machine to include the fields from Inventory

- 1 Go to Settings > Schema Manager.
- 2 Select **Extend existing asset type**.
- 3 In the Select Asset Type panel, select **Windows Machine** and click **Next**.

The primary, mandatory, and optional fields for the selected asset type are displayed.
- 4 In the Select Optional Fields panel, Select **Include referenced entities** and select **Inventory** from the list of entities.
- 5 Select **Vendor Name**, **Address of Vendor**, and **Date/Time of Contract Expiry** from the Available fields column. Use the Add icon to add the fields to the Selected fields column.

Click **Next**.

See [“About referenced entity fields”](#) on page 354.

- 6 In the Customize Field Attributes panel, check **Is field part of job** for all the three fields and mark them editable.

When you extend an existing asset type, you can only add the optional fields. The optional fields are not required for data collection. You can explicitly mark the field to include in the data collection job.

Click **Next**.

- 7 In the Add External Fields panel, click **Next**.
- 8 In the Summary panel, review the selections that you made for the custom asset type and click **Finish**.
- 9 Close the Control Compliance Suite Console, restart the Symantec Application Server Service and relaunch the Control Compliance Suite Console.

To import data from the CSV file for the newly added fields, create a CSV file with the following format:

```
Custom.Inventory.DomainName,  
Custom.Inventory.MachineName,  
Custom.Inventory.VendorName,  
Custom.Inventory.VendorAddress,  
Custom.Inventory.Date-TimeofContractExpiry
```

After you create a CSV file, share the file, and specify the share path for the CSV settings. After you create a CSV file, share the file and specify the share path in the CSV settings. You can then perform an asset import for the new fields.

See [“Configuring the CSV data collector”](#) on page 129.

See [“Importing assets”](#) on page 260.

Creating a custom asset type- Printer based on the custom platform- Devices

Assume that you want to manage the physical devices assets such as, printers, scanners, monitors, keyboards and so on. The predefined asset types cannot manage these assets. The predefined platforms and the data collectors cannot help you gather data about these assets. Now, you must create custom asset types for printers, scanners and so on. You must first create a new platform and a custom entity based on which the custom asset types can be created.

Perform the following tasks:

- Create a new platform, Devices and a new entity, Printer
See [“Creating a custom platform- Devices and the custom entity-Printer”](#) on page 376.

- Create a new asset type, Printer
See [“Creating a custom asset type- Printer”](#) on page 377.

Creating a custom platform- Devices and the custom entity-Printer

Let us use the Create new entity schema option and create an entirely new platform and entity for managing the physical assets or devices in the enterprise. You can create a new platform, Devices and create multiple entities that are based on the platform as Printer, Scanner, Monitors, Keyboard and so on. You can then create asset types based on each of the entities and use the asset types to import the data for the entities.

You must use the Create new entity schema option from the Schema Manager view to create a new platform and an entity.

To create a custom platform- Devices and the custom entity- Printer

- 1 Go to Settings > Schema Manager.
- 2 Select **Create new entity schema** to launch the Create New Entity Schema wizard.
- 3 In the Select or Create New Platform panel, select **Create a new platform**.
In the Name box, type **Devices**.
In the Display Name box, type **Devices** and click **Next**.
- 4 In the Specify Entity Details panel, in the Name box, type **Printer** as the name of the entity
In the Display Name box, type **Printer** and click **Next**.
The display name of the entity appears in the evaluation report that is generated for the collected data of the asset.
- 5 In the Add Fields panel, click **Add** to add new fields for the entity.
- 6 In the Create New Field dialog box, create fields with the following details:

Name:	String data type
Printer Name	Mark as primary field
Name:	String data type
Printer Type	
Name:	Boolean data type
Is double sided?	

In the Add Fields panel, click **Next**.

- 7 In the Specify Entity Name Fields panel, **PrinterName** from the Available fields list and add them to the Selected fields list.
Click **Next**.
- 8 In the Specify References panel, click **Next**.
Let us not specify any field from the existing entities as the reference fields for <Devices><Printer>.
You can alternatively specify a field from the existing entity and establish a relation between the two fields. In this case, the field from the parent entity becomes the primary asset type if you want to import the assets from the Printer asset type.
See [“Primary and secondary assets”](#) on page 228.
See [“About referenced entity fields”](#) on page 354.
- 9 In the Summary panel, review the details of the created entity and click **Finish**.
- 10 Close the Control Compliance Suite Console.
- 11 Copy the XMLs at the following paths:
 - <installldir>\Symantec\CCS\Reporting and Analytics
 - <installldir>\Symantec\CCS\Reporting and Analytics\Application Server
 - <installldir>\Symantec\CCS\Reporting and Analytics\DPS
- 12 Go to Start > Run, type **services.msc**, restart the Symantec Application Server Service and re-launch the Console after two minutes.

Creating a custom asset type- Printer

Let us create a custom asset type, Printer that is based on the custom platform, Devices and the custom entity, Printer that you created in

To create a Windows Service asset type

- 1 Go to Settings > Schema Manager.
- 2 Select **Add new asset type**.
- 3 In the Specify Asset Type Details panel of the Create New Asset Type wizard, type **Printer** in the Name field and in the Display name field and click **Next**.
- 4 In the Select Platform and Primary Entity panel, do the following:
 - From the Platform drop-down list, select **Devices**.
 - From the Primary entity drop-down list, select **Printer** and click **Next**.

- 5 In the Specify Fields panel, add the following fields from the Available fields list to the Selected fields list and click **Next**.
 - Type of the printer
 - Is double sided?
- 6 In the Customize Field Attributes panel, mark the field **Type of the printer** as **Mandatory** and the field **Is double sided?** as **Optional**.
Select **Is field part of job** for both the fields and click **Next**.
See [“About the primary, mandatory, and optional fields”](#) on page 354.
- 7 In the Add External Fields panel, click **Add**.
- 8 In the Add New Field dialog box, type **Location** and select **String** as the data type.
- 9 In the Specify Asset Name Fields, select **Name of the printer** from the Available fields list and add it to the Selected fields list.
Click **Next**.
- 10 In the Summary panel, review the selections that you made for the custom asset type and click **Finish**.
- 11 Close the Control Compliance Suite Console and restart the Symantec Application Service.
- 12 Launch the Control Compliance Suite Console and go to Manage > Assets > Asset System.

In the table pane, from the Display drop-down list, view the Printer as the new asset type.

To import the data for the Printer fields using a CSV data collector, create a CSV file with the following format:

```
Devices.Printer.Printername,
Devices.Printer.PrinterType,
Devices.Printer.IsdoubleSided,
```

To learn the procedure to import the assets for the asset type, printer click on the following links:

See [“Importing the specific and common fields for custom asset using the CSV data collector”](#) on page 281.

See [“Creating a target type for the asset type - Printer”](#) on page 379.

Creating a target type for the asset type - Printer

After you import the assets for the custom asset type, Printer you might want to collect the data for the Printer.

See [“Setting up a data collection job from the Assets view”](#) on page 310.

To evaluate the assets for the Printer, you must create custom checks and build a standard. To create custom checks for the custom asset type, Printer you must create a target type.

You can create a target type that is based on the fields of the asset type, Printer. PrinterName is the primary field and the PrinterType and Is DoubleSided are the other fields of the Printer asset type.

Let us create a target type that is based on the field, PrinterType.

To create a target type for the asset type - Printer

- 1 Go to Settings > Schema Manager.
- 2 Click **Create New Target Type**.
- 3 In the Specify Name and Description for Target Type panel, type **DotNet** and click **Next**.
- 4 In the Select Platform and Asset Type panel, select **Devices** as the platform and **Printer** as the asset type.
- 5 In the Create Asset Type filters panel, select **PrinterType** from the drop-down list and click **Add Statement** to add a filter statement.
- 6 In the Filter Statement dialog box, select **Specific Value** as the parameter type.

Select **EqualTo (=)** as the operator and type **DotNet** in the Specify Value box.

Click **OK**.

- 7 In the Create Asset Type filters panel, click **Next**.
- 8 In the Summary panel, review the information that you have entered in the wizard. Click **Back** to make any modifications or click **Finish** to exit the wizard.

Go to Manage > Standards and create the custom checks that are based on the newly created target type.

See [“Creating a new check”](#) on page 517.

Managing entitlements

This chapter includes the following topics:

- [About entitlements](#)
- [Concepts in entitlements](#)
- [Working with control points](#)
- [Working with entitlements import](#)
- [Working with approval](#)
- [Working with notifications](#)
- [About the entitlements filters](#)
- [Viewing the control points information in the details pane](#)

About entitlements

The Entitlements view in Control Compliance Suite facilitates the monitoring of access rights in the organization. The Entitlements view provides the means to efficiently gather the permissions data from the various platforms and enables the user to generate reports.

In a typical environment, IT compliance is confined to configuration management, the firewall, the antivirus systems, and the vulnerability assessment. However, there is a difference between managing security configurations and vulnerabilities and managing access controls and data entitlements. The IT department can implement processes for managing and auditing entitlements. The decision about who has access to what data lies with the business owner of that data. Incidents can occur when a valid user can have access to the data that the user should not access. The Entitlements view identifies these false entitlements. The Entitlements

view lets you define the data that user X is entitled to access. The Entitlements view also monitors whether the system adheres to the defined access controls.

The Entitlements view lets you configure the control points and assign the review periods. The view also ensures the frequent approvals of the control points by the respective data owners. To know where an individual user and groups have rights is critical to safeguard the data. Merely the documentation of those rights is insufficient to safeguard the data. This information must correspond to the internal business processes and must be directly linked to data ownership. The ability to confirm the entitlements at regular intervals gives additional support to the organizations for demonstrating good stewardship. This confirmation ability includes internal and external data security, confidentiality, integrity, and availability.

See [“Creating a review cycle setting”](#) on page 402.

See [“Problems in managing entitlements”](#) on page 382.

Reasons for managing entitlements

User and group entitlements is one of the most significant and the most difficult aspects of IT security. In an organization, the protection of data is highly important, not only from external exploitation but also from internal misuse. A person in an organization who has illegal access to sensitive data can lead to undesirable effects. To determine who should have access to which data can be difficult, especially in large companies with a number of users. Large companies maintain many identity management roles and also maintain multiple databases that contain sensitive information. The concern that arises is to how entitlements should be determined.

See [“Problems in managing entitlements”](#) on page 382.

Problems in managing entitlements

Many companies maintain an Access Control List (ACL). This approach might serve the purpose of restricting access to sensitive information to a limited number of users. Equally important is to ensure that the authentic users have access to all the relevant data. This type of management requires extensive effort to gather information about users, to look at the data flows, and to conduct frequent analyses.

The following questions must be answered while monitoring entitlements in an organization:

Where does user X have access in the network?	When an employee leaves the company or is terminated for serious reasons, it becomes important to identify the risk exposure that the employee contributes.
Where in the network do the members of group X have access?	When a user is added to the group, the user inherits all the permissions that are assigned to that group. These inherited permissions should be audited diligently.
Who has access to the data X?	When all the access grants are finalized, the review of the complete list of read, write, and execute permissions on a regular basis is important.
Who validates that the access grants are appropriate?	Apart from a strong security model for the network, the proof of an ongoing review process is also needed to comply with various government regulations. To serve this purpose, organizations must be able to associate critical data with appropriate business data owners who can validate the access grants.

The approval of the entitlements on a periodic basis is in the core of the entitlements system.

See [“Creating a review cycle setting”](#) on page 402.

About the entitlements system workflow

To understand the workflow of the entitlements system, you must review the concepts that are related to the entitlements system.

See [“Concepts in entitlements”](#) on page 394.

The workflow of the entitlements system starts with marking an asset as a control point and ends with the generation of the entitlements reports.

The entitlements reports include the Effective Permissions Report, the Simple Permissions Report, the Entitlement Changes Report, and the Trustee Report.

See [“About the control point status”](#) on page 387.

The users in the role of an entitlement administrator and the entitlements data owner perform the tasks in the entitlements system.

See [“Predefined roles”](#) on page 80.

The tasks in the entitlements system can be divided as follows:

Manual tasks	<ul style="list-style-type: none">■ Performed by the user■ Require user input and user action.
System tasks	<ul style="list-style-type: none">■ System tasks■ Require no user input and user action.

You can perform the following manual tasks in the entitlements system based on your role:

<p>Mark an asset as a control point</p> <p>See “Marking an asset as a control point” on page 398.</p>	<p>You mark an asset as a control point if you want to monitor the entitlements of the asset through the approval workflow.</p> <p>The entitlement administrator can mark assets as control points from the asset system.</p> <p>When the assets are marked as control points they appear in the Manage > Entitlements > Control Points view.</p> <p>By default, the control points are in the No Review Configured state.</p>
<p>Create a review cycle setting</p> <p>See “Creating a review cycle setting” on page 402.</p>	<p>You create a review cycle setting to define a review period for the approval of the entitlements of the control points.</p> <p>The entitlement administrator can create a review cycle setting from the Manage > Entitlements > Review Cycle Settings view.</p>
<p>Assign the role of data owner to a trustee</p> <p>See “Adding users and groups to a role” on page 89.</p>	<p>You select a trustee who can review and approve the entitlements for the control points.</p> <p>You must assign the role of an entitlements data owner to the trustee from > Settings > Roles view.</p>

Configure the control point

See [“Configuring control points”](#) on page 400.

You configure a control point to assign a data owner or an approver, the tags, and the review cycle to the control point.

The entitlements administrator can configure the control points from the Manage > Entitlements > Control Points view.

The control points status changes to Review Start Awaited when the control point is configured with a review cycle

When you configure the control point with a review cycle the entitlements system transitions the control points in various states. The states are based on the review cycle status.

The control point status changes from Review Start Awaited to Review Started when the review cycle starts. The system starts the review cycle on the start date that is specified in the review cycle setting.

The system then changes the control point status from Review Started to Entitlement Import Required. The Entitlement Import Required status is set according to the number of days specified for importing the entitlements before the approval starts.

Import entitlements

See [“Importing the entitlements manually”](#) on page 408.

See [“Configuring the automatic entitlements import”](#) on page 407.

The entitlements administrator must import the entitlements before the approval starts. The entitlements are then available for the data owner to approve.

If the automatic entitlements import is not configured, then the entitlements administrator must import the entitlements manually.

The control point status changes from Entitlement Import Required' state to Entitlement Import Pending when the entitlements import is in progress.

When the entitlement import is complete the system changes the control point status to Approval Start Awaited.

The control points status changes from Approval Start Awaited to Request for Approval when the approval period starts. The approval period starts on the approval start date that is specified in the review cycle setting.

Request for Approval

See [“Requesting approval of entitlements”](#) on page 410.

The entitlement administrator requests the approval of entitlements when the approval period starts.

After the entitlement administrator requests for approval, the data owner can either approve the entitlements or request changes in the entitlements.

Approve the control points

See [“Approving the entitlements”](#) on page 411.

The data owner can view the entitlements for the control points and approve the control points from the My Control Points view.

The alternative approver can also approve the control points if the alternative approver is enabled.

After the approval, the control point status changes to Approved.

Request changes in entitlements

See [“Alternative approver”](#) on page 396.

The data owner can request changes in the entitlements of the control points.

The control points status changes to Request for Change.

Request for Approval

See [“Requesting approval of entitlements”](#) on page 410.

The entitlement administrator can request for approval again when the IT department implements the change requests of the data owner.

The entitlement administrator must import the entitlements again.

When the entitlement administrator requests for approval of the control points for which a change is requested, the status changes to Entitlement Import Required.

Import entitlements

See [“Importing the entitlements manually”](#) on page 408.

See [“Configuring the automatic entitlements import”](#) on page 407.

The entitlement administrator must import the entitlements before the approval starts. The entitlements are then available for the data owner for approval.

If the automatic entitlement import is not configured, the entitlement administrator must import the entitlements manually.

The control point status changes from 'Entitlement Import Required' state to 'Entitlement Import Pending' when the entitlements import is in progress.

When the entitlement import is complete the system changes the control point status to Request for Approval.

The data owner can now approve if the entitlements are as expected or again request for change if the entitlements are not as expected.

About the control point status

In the process of the approval of the entitlements, a control point moves through various states.

At any given time, a control point can be in any of the following states in the entitlements system:

No Review Configured	<p>Indicates that the control point has no review cycle that is associated with it.</p> <p>No Review Configured is the default status of the control point, when an asset is marked as the control point.</p> <p>A control point cannot be monitored for its entitlements in the approval workflow unless a review cycle is associated with it.</p>
Review Start Awaited	<p>Indicates that the review cycle is associated with a control point and the review start date is awaited.</p> <p>The review cycle start depends on the date that you indicate in the review cycle settings.</p>

Review Started	<p>Indicates that the review cycle for the control point has started.</p> <p>The review cycle starts after the daily approval job runs on the review cycle start date.</p> <p>Status changes from Review Start Awaited to Review Started when the review cycle starts.</p>
Entitlement Import Required	<p>Indicates that the entitlements should be imported before the approval period begins.</p> <p>The control point status changes to the Entitlement Import Required in the following cases:</p> <ul style="list-style-type: none">■ The status changes from Review Started to Entitlements Import Required according to the review cycle setting. In the review cycle setting, you mention the number of days before the approval start when you want to import the entitlements.■ The status changes from Request For Change to Entitlement Import Required when the entitlements administrator requests for the approval of control point after the entitlements are changed according to the change requests.
Entitlement Import Pending	<p>Indicates that the entitlement import is in progress.</p> <p>Status changes from Entitlement Import Required to Entitlement Import Pending.</p> <p>Note: Sometimes, in case of system failure during the entitlement import, control points are left in the Entitlement Import Pending status even after the system is up. You must revert the status to the Entitlement Import Required status to re-import the entitlements of these control points. To revert the status to the Entitlement Import Required status, go to Settings > General > Entitlements> Revert Import Pending Control Point Status. You cannot revert the status if another entitlement import job is running.</p> <p>The system runs an approval job on a daily basis. The approval job changes the status to Entitlement Import Pending.</p>
Approval Start Awaited	<p>Indicates that the approval period for the control points is yet to start after Entitlement Import.</p>

Request for Approval	<p>Indicates that the request for approval is sent to the data owner of the control points.</p> <p>The control point status changes to the Request for Approval in the following cases:</p> <ul style="list-style-type: none"> ■ The status changes from Approval Start Awaited to Request for Approval when the approval starts. ■ The status changes from Entitlement Import Required to Request for Approval when the entitlement import is complete. This is in case of the re-importing of entitlements after the implementation of the change requests.
Request for Change	<p>Indicates that the data owner has requested changes in the entitlements of the control points.</p> <p>Status changes from Request for Approval to Request for Change.</p>
Approved	<p>Indicates that the data owner has approved the entitlements of the control points.</p>

See [“Working with control points”](#) on page 398.

About the Control Points view

The Control Points view lets you manage the control points in the Control Compliance Suite.

You can access the Control Points view from Manage > Entitlements > Control Points.

The Control Points view contains the following panes:

Tree pane	<p>This pane appears on the left side of the console window under the navigation bar.</p> <p>This pane displays the asset folders and asset groups under the Asset System node.</p>
Filter by pane	<p>This pane appears in the lower left side of the console window under the tree pane.</p> <p>You can use the following filters in the Control Points view:</p> <ul style="list-style-type: none"> ■ Control point status ■ Select tags

Table pane	<p>This pane appears on the right side of the console window under the taskbar .</p> <p>This pane displays the assets that are marked as control points. You can use the Display filters to view the control points of a particular type.</p> <p>You cannot multi-select the control points that belong to the different approval status from the table pane. You can only select multiple control points that belong to the same approval status to perform a common action on those.</p>
Details pane	<p>This pane appears in the lower right side of the console window under the table pane.</p> <p>This pane displays the details of the control point that is selected in the table pane.</p>

You can perform the following tasks from the Control Points view:

- Import entitlements
See [“Importing the entitlements manually”](#) on page 408.
- Unmark a control point
See [“Unmarking a control point”](#) on page 404.
- Configure control points
See [“Configuring control points”](#) on page 400.
- Request exceptions
See [“Requesting an exception”](#) on page 436.
- Request approval
See [“Requesting approval of entitlements”](#) on page 410.
- Comparing entitlements
See [“Comparing entitlements”](#) on page 413.
- Viewing control point details

About the My Control Points view

The My Control Points view lets the data owner manage the control points that require the data owner's approval.

You can access the My Control Points view from **Manage > Entitlements > My Control Points**.

The My Control Points view contains the following panes:

Tree pane	<p>This pane appears on the left side of the console window under the navigation bar.</p> <p>This pane displays the asset folders and asset groups under the Asset System node.</p>
Filter by pane	<p>This pane appears in the lower left side of the console window under the tree pane.</p> <p>You can use the following filters in the Control Points view:</p> <ul style="list-style-type: none">■ Control point status■ Select tags
Table pane	<p>This pane appears on the right side of the console window under the taskbar .</p> <p>This pane displays the control points that are assigned to the user who is logged-in as the data owner. You can use the Display filters to view the control points of a particular type.</p> <p>The table pane displays the control points according to the current status.</p>
Details pane	<p>This pane appears in the lower right side of the console window under the table pane.</p> <p>This pane displays the details of the control point that is selected in the table pane.</p>

See [“About the Control Points view”](#) on page 389.

About the Import Settings view

You can refine the entitlements import process from the network with the help of rules that are called import settings.

The Import Settings view lets you configure the analysis options for the following entitlement types:

- Windows File or Directory
- ESM File or Folder
- ESM User Group

You use the analysis options to narrow down the scope of the job when you import the entitlements.

Note: The import settings are applicable to all the entitlement import jobs for the selected control point type. For example, if you specify the import settings for Windows File and Directory, the settings are considered every time when the entitlements for the Windows File or Directory are imported.

You can set the following analysis options for the Windows File / Directory:

Analysis types

You can select one of the following analysis types:

- Local and network analysis
Performs the full analysis of effective permissions whether they are obtained by logging on locally or by accessing the file system object through a share. This option executes a local analysis and a network analysis and combines the results.
- Security descriptor only
Calculates the effective permissions to the file system object by analyzing only the security descriptor.

Analysis options

You can select any one or all the following analysis options:

- Report groups
Includes the Groups in the entitlement import
- Report users
Includes only the users in the entitlement import
- Skip logon workstations

Group analysis

You can select one of the following group analysis options:

- **Report members of all groups**
Reports the members of all the groups that are contained in the scope of the entitlement import
- **Do not report members of these groups**
Lets you type the names of the groups separated by semicolon. The members of the specified groups are not reported on in the entitlement import job.

You can set the following analysis options for ESM File, Folder entitlements and User Group entitlements:

Policy name

Lets you enter the ESM policy name.

The policy name that you specify is case sensitive.

See [“Configuring the import settings”](#) on page 406.

About the Browse Notifications view

The Notifications view lets you enable or disable notifications to be sent to the data owners. The notifications are sent to the data owners at certain time intervals during the review cycle.

You can access the Notifications view from Manage > Entitlements > Notifications.

You can configure the following types of notification:

- Review End
- Approval Start
- Approval End
- Approval Requested
- Review Start
- Data Owner Change
- Alternative Approver Changed

The Notifications view also lets you configure and customize the notifications.

See [“Configuring entitlements notifications”](#) on page 418.

About the Review Cycle Settings View

The Review Cycle Settings view lets you create review cycle settings. The review cycles that you create in this view, are used when you configure the control points. You can only assign a review cycle that is already created in the view.

See [“Creating a review cycle setting”](#) on page 402.

The Review Cycle Settings view contains the following panes:

Table pane	<p>This pane appears under the taskbar .</p> <p>This pane displays all the review cycle settings that you create.</p>
Details pane	<p>This pane appears in the lower right side of the console window under the table pane.</p> <p>This pane displays the control points that are associated with the review cycle setting that is selected in the table pane.</p>

Concepts in entitlements

To understand the workflow for managing the entitlements in Control Compliance Suite, you must first understand the concepts in the entitlements.

The following are the concepts in the Entitlements view:

- Control points
See [“Control points”](#) on page 395.
- Data owners
See [“Data owners”](#) on page 396.
- Alternative approver
See [“Alternative approver”](#) on page 396.
- Review cycle setting
See [“Review cycle setting”](#) on page 396.
- Approval period
See [“Approval period”](#) on page 397.
- Tagging
See [“Tagging”](#) on page 397.

Control points

A control point is the data location in the system at which the access permissions are granted and approved. You can mark an asset that is imported into the Control Compliance Suite system as a control point.

Consider the following directory structure:

```
C:\
C:\Data
C:\Data\Accounting
C:\Data\Accounting\Site 01
C:\Data\Accounting\Site 02
C:\Data\Accounting\Site 03
```

In the directory structure, the permissions for the Accounting folder are assigned at the data location, C:\Data\Accounting. The rights that are assigned at this point in the directory are also assigned down to any file or folder that exists under this directory. You can assign additional rights lower in this directory for a specific file or a folder. The file is the lowest level of control point.

You can also define a control point for a group. A group of users can have the same type of permissions for a certain directory or a file.

Note: You cannot mark Windows Machines or UNIX Machines as control points.

The entitlements system supports certain predefined asset types as control point types. In addition to the supported asset types, the entitlements cannot be imported for any custom asset type that you create. But, the entitlements system supports an extended predefined asset type that is supported as a control point type.

The entitlements system lets you mark the following asset types as control points:

- Oracle Configured Databases
- SQL Databases
- UNIX File
- UNIX Group
- Windows File
- Windows Group
- Windows Directory
- ESM Agents

The entitlements system supports the following entitlement types:

- ESM Agents
 - ESM File, Folder entitlements
 - ESM User Group entitlements
- Oracle Configured Databases
 - Stored procedure entitlements
 - Table entitlements
 - View entitlements
- SQL
 - Database entitlements
 - Stored procedure entitlements
 - Table entitlements
 - View entitlements

See [“Working with control points”](#) on page 398.

Data owners

Data owners are the business owners of the data.

Control Compliance Suite assumes that a person who is theoretically the business owner of the data- also owns the data in the system. The data owner has the responsibility to approve or decline permissions on the control points.

See [“Configuring control points”](#) on page 400.

Alternative approver

Control Compliance Suite lets you configure an alternative approver for the control points. The alternative approver performs the role of the data owner to approve the entitlements, in case the data owner is not available.

See [“Configuring the alternative approver”](#) on page 412.

Review cycle setting

The review cycle setting is the time frame for which the entitlements are validated. The entitlement administrator can define different review cycle settings for different types of data.

For example, an organization might want to validate the entitlements of the financial data two times in a year. However, the HR data might be validated only one time in a year.

The definition of the review cycle setting can be based on the organizational policies of approving entitlements.

A review cycle setting can be set as recurrent or non-recurrent. If you mark a review cycle setting as recurrent, the same review cycle setting repeats after the end of the review cycle setting. For example, if you define a review cycle setting for three months and mark it as recurrent, then the cycle is repeated every three months. Each review cycle setting that is completed becomes a review cycle instance.

See [“Creating a review cycle setting”](#) on page 402.

Approval period

The approval period of a control point is a subset of the review period.

The data owner should approve or request a change in the entitlements within the specified approval period. For example, consider that the review period for a set of control points is from January 1 to March 31. The approval period may be between February 1 and February 28.

See [“Working with approval”](#) on page 410.

Tagging

The assets that are marked as control points must be defined with reference to some context. You can define the control points according to their sensitivity, confidentiality, and value to the organization. The purpose of defining control points is such that the data owner understands the relevance of the control points. Each organization may have its own ways to classify the data. Control Compliance Suite lets you tag the control points. Tags are used to categorize data so that uniform permissions can be assigned to the data in the same category. This categorization is important for the most effective and the most efficient use of the data.

Tags can be based on the critical value of the data such as confidential, public, or classified. Tags can be also based on how often the data needs to be accessed. You can define the tags according to the department, such as human resources, finance, and marketing. Well-planned tags make the essential data easy to find. The tags can be of particular importance in risk management, legal discovery, and compliance with government regulations.

The Entitlements view lets you assign tags to the control points and categorize the control points as required. You can assign multiple tags to a control point. The tagging of a control point is not mandatory.

Working with control points

In Control Compliance Suite, you mark an asset as a control point to monitor the entitlements on that control point.

In the entitlement system, you perform the following tasks with the control points:

- Mark an asset as a control point
See [“Marking an asset as a control point”](#) on page 398.
- Unmark a control point
See [“Unmarking a control point”](#) on page 404.
- Configure a control point
See [“Configuring control points”](#) on page 400.
- Create review cycle settings
See [“Creating a review cycle setting”](#) on page 402.

Marking an asset as a control point

An asset that is marked as a control point appears in the Entitlements > Control Points view.

You can mark only the following asset types as control points:

- Windows File
- Windows Directory
- Windows Groups
- UNIX File
- UNIX Group
- SQL Database
- Oracle Database
- ESM Agents

See [“Control points”](#) on page 395.

Note: You cannot mark Windows Machines, UNIX Machines, SQL Servers, and Oracle Servers as control points.

To mark an asset as a control point

- 1 Go to Manage > Assets > Asset System.
- 2 In the table pane, right-click the asset that you want to mark as a control point.
- 3 Select **Mark as Control Point**.
- 4 In case you mark an asset that belongs to Oracle, SQL, or ESM platforms as a control point, you must select the entitlement type.
See [“Control point type and entitlement type”](#) on page 399.
- 5 In the Entitlement Type Selector dialog box, select one or more entitlement types and click **OK**.
- 6 In the confirmation message box, click **OK**.
- 7 Go to Manage > Entitlements > Control Points and verify the control point in the table pane.

See [“Unmarking a control point”](#) on page 404.

See [“Control points”](#) on page 395.

Control point type and entitlement type

The entitlements system supports certain predefined asset types as control point types. In addition to the supported asset types, the entitlements cannot be imported for any custom asset type that you create. But, the entitlements system supports an extended predefined asset type that is supported as a control point type.

The entitlements system supports the following control point types and entitlement types:

- ESM Agents
 - ESM File, Folder entitlements
 - ESM User Group entitlements
- Oracle Configured Databases
 - Stored Procedure entitlements
 - Table entitlements
 - View entitlements
- SQL
 - Database entitlements
 - Stored procedure entitlements

- Table entitlements
- View entitlements
- Windows
 - Windows Files entitlements
 - Windows Directories entitlements
 - Windows Groups entitlements
- UNIX
 - UNIX Files entitlements
 - UNIX Groups entitlements

See [“Importing the entitlements manually”](#) on page 408.

Configuring control points

You can configure the control points to make them available for monitoring in the approval workflow. The configuration of the control points associates the control points with the data owner, the alternative approver, the tags, and the review cycle.

Note: You can associate the review cycle setting to the control point only if the date of entitlements import before the approval start is yet to arrive.

Make sure that you have at least one review cycle setting created before you configure a control point.

See [“Creating a review cycle setting”](#) on page 402.

To launch the Configure Control Points wizard

- 1 Go to Manage > Entitlements > Control Points.
- 2 From the table pane, right-click a control point and select **Configure Control Point**.

To configure the data owners

- 1 In the Configure Data Owners panel, type a description.
The description is optional.
- 2 Under the Data owner details section, click **Browse** and select a data owner to associate with the control points.
You can use the Clear option to remove the associated data owner.
The user that you select as a data owner is a primary data owner.
- 3 Select **Enable Alternative Approver** to allow the secondary data owner to approve the control points in the absence of the primary data owner.
The assignment of the alternative approver is an optional step.
- 4 Under the Alternative approver details section, click **Browse** and select a user as an alternative approver.
- 5 Click **Next**.

To assign tags to the control points

- 1 In the Assign Tags panel, click **Add**.
- 2 In the Select Tags dialog, select a tag from the Tags node and click **Add**.
- 3 Click **OK**.
- 4 In the Assign Tags panel, click **Next**.

To configure a review cycle

- 1 In the Specify Review Cycle Details panel, select one of the following:

No Review Required	Lets you choose not to associate the control point with any review cycle. The selected control points do not follow the approval-based reviews.
Retain Existing Review Cycle	Lets you retain the existing review cycle. This option is enabled only if the control points have the previous review cycles configured.
Assign a New Review Cycle	Lets you select a review cycle from the existing review cycles.
- 2 Click **Next**.

To assign a new review cycle

- 1
- In the Assign a Review Cycle panel, select a review cycle setting from the existing review cycles to associate with the control points.
- 2
- Click **Next**.
- 3
- In the Summary panel, click **Finish**.

See [“Marking an asset as a control point”](#) on page 398.

See [“Unmarking a control point”](#) on page 404.

See [“Control points”](#) on page 395.

Creating a review cycle setting

Only the entitlement administrator can configure a review cycle setting.

The review cycle setting is a time period during which you want to monitor the entitlements of a set of control points.

See [“Review cycle setting”](#) on page 396.

To create a review cycle setting

- 1
- Go to Manage > Entitlements > Review Cycle Setting.
- 2
- In the taskbar, click **Create**.
- 3
- In the Create Review Cycle Setting dialog box, specify the following information and click **OK**.

Name	Lets you type a name for the review cycle.
Duration	Lets you select a duration for the review cycle. You can select the duration from the following options: <div><div>■</div>1 Week</div> <div><div>■</div>2 Weeks</div> <div><div>■</div>1 Month</div> <div><div>■</div>3 Months</div> <div><div>■</div>6 Months</div> <div><div>■</div>1 year</div>
Next Review Start Date	Lets you choose a date from when the review cycle should start.

Approval Start	<p>Lets you select a period before the review end date to start the approval.</p> <p>Approval start indicates that the data owner has to approve the control points within the specified limit before the review ends.</p> <p>You can select from the following options:</p> <ul style="list-style-type: none"> ■ 1 Week ■ 2 Weeks ■ 1 Month ■ 3 Months ■ 6 Months ■ 1 year
Approval Duration	<p>Lets you select a duration for the approval period.</p> <p>You can select from the following options:</p> <ul style="list-style-type: none"> ■ 1 Week ■ 2 Weeks ■ 1 Month ■ 3 Months ■ 6 Months ■ 1 year
Is Recurring?	<p>Lets you select a True or False value to make the review cycle recurring.</p>
Import Entitlements before # days of Approval Start	<p>Lets you select the number of days before the approval start date, to import the entitlements.</p> <p>You can choose to import the entitlements from 0 to 150 days before the approval start.</p>

See [“Deleting a review cycle setting”](#) on page 403.

Deleting a review cycle setting

The entitlement administrator can delete the review cycle setting from the Review Cycle Settings view.

Note: You can delete the review cycle setting if the control points are not associated with the review cycle. In case of non-recurring review cycles, you can delete the review cycle setting after the end of the review cycle even if the control points are associated with it.

To delete a review cycle setting

- 1 Go to Manage > Entitlements > Review Cycle Setting.
- 2 Select a review cycle setting that you want to delete.
- 3 From the taskbar, click **Delete**.
- 4 In the message box, click **Yes** if you want to delete the review cycle setting and click **No** if you want to retain the review cycle setting.

See [“Creating a review cycle setting”](#) on page 402.

Unmarking a control point

You can unmark a control point from the entitlements management view. To unmark a control point, you must be the entitlements administrator.

To unmark a control point

- 1 Go to Manage > Entitlements > Control Points.
- 2 In the table panel, right-click a control point and select **Unmark as control point**.

See [“Marking an asset as a control point”](#) on page 398.

See [“Control points”](#) on page 395.

Working with entitlements import

In the entitlements system workflow, you import the entitlements of the control points in any of the following states:

- Before the approval period begins the entitlement administrator imports the entitlements of the control points.
- After the entitlements are changed according to the change request by the data owner, the entitlement administrator imports the entitlements of the control points.

See [“About the control point status”](#) on page 387.

In the entitlement system, you perform the following tasks with the entitlement import:

- Configure the import settings.
See [“Configuring the import settings”](#) on page 406.
- Configure the automatic entitlements import.
See [“Configuring the automatic entitlements import”](#) on page 407.

- Import the entitlements manually.
See [“Importing the entitlements manually”](#) on page 408.

About entitlements import

Only the entitlement administrator can perform the task of entitlement import.

In the entitlements system workflow, you import the entitlements of the control points in any of the following states:

- Before the approval period begins
- After the entitlements are changed according to the change request by the data owner

To get the latest entitlements of the control points that await the entitlements import, you can also manually create an entitlement import job. You can manually import the entitlements of the control points in any state.

The manual and automatic entitlements import work as follows:

Manual entitlement import

To manually import the entitlements of the control points, you create an entitlements import job.

You can run the entitlements import job immediately or schedule the job to run when the approval period of the control points is about to begin.

See [“Importing the entitlements manually”](#) on page 408.

Automatic entitlement import

To automatically import the entitlements of the control points, you configure the automatic entitlements import job.

The automatic entitlement import job runs daily at a specified time. The job imports entitlements for all the control points that display the status as Entitlements Import Required.

See [“Configuring the automatic entitlements import”](#) on page 407.

Configuring the import settings

You can refine the entitlements import process with the help of the rules that are called as the import settings.

The Import Settings view is divided into the following tabs:

- Windows File or Directory
- ESM File or Folder
- ESM User Group

Note: The import settings are applicable to all the entitlement import jobs for the selected control point type. For example, if you specify the import settings for Windows File and Directory, the settings are considered every time when the entitlements for the Windows File or Directory are imported.

To configure the import settings

- 1 Go to Manage > Entitlements > Import Settings.
- 2 To specify the import settings for the Windows File or Directory, use the following options and click **Save**.

Analysis types

You can select one of the following analysis types:

- Local and network analysis.
Performs the full analysis of effective permissions whether they are obtained by logging on locally or by accessing the file system object through a share. This option executes a local analysis and a network analysis and combines the results.
- Security descriptor only.
Calculates the effective permissions to the file system object by analyzing only the security descriptor.

Analysis options

You can select any one or all the following analysis options:

- Report groups.
Includes the Groups in the entitlement import
- Report users
Includes only the users in the entitlement import
- Skip logon workstations.

Group analysis

You can select one of the following group analysis options:

- Report members of all groups.
Reports the members of all the groups that are contained in the scope of the entitlement import
- Do not report members of these groups.
Lets you type the names of the groups in the separated by a semicolon. The members of the specified groups are not reported on in the entitlement import job.

- 3 To specify the import settings for ESM- File, Folder Entitlements and ESM-User Group Entitlements, type the policy name and click **Save**.

The policy name that you type is case-sensitive. The policy name that you type is used when you import the entitlements for the ESM Agents control points.

Configuring the automatic entitlements import

You configure the automatic entitlements import to get the latest entitlements of the control points on daily basis.

The automatic entitlement import job imports the entitlements for the control points that are in the Entitlement Import Required state.

Consider the following case:

- You have a control point that is in the Entitlements Import Required state.
- The automatic entitlement import job is scheduled to run at 12 midnight.

- You import the entitlements of the control points manually at 8 PM before the automatic entitlement import job runs.
- The automatic entitlement import does not fetch any entitlements as the control point is not in the state of Entitlement Import Required.

Note: In case of importing the entitlements for ESM Agents, it is recommended that you customize the templates to limit the entitlement import only for specific objects. The entitlement import for ESM Agents may generate a large amount of data unless you restrict it to a specific scope. The results are stored in the production database (CSM_DB) which may lead to the increase in the size of the database.

See [“About entitlements import”](#) on page 405.

To configure the automatic entitlements import

- 1 Go to **Settings > General > Application Configuration > Entitlements**.
- 2 Under the **Automatic import settings**, check **Automatically import entitlements**.
- 3 In the **Automatic import job run time**, specify the time when you want the daily entitlement job to run.

See [“Importing the entitlements manually”](#) on page 408.

Importing the entitlements manually

You can import the entitlements for the control points using the Create or Edit Entitlements Import Job wizard. The import of entitlements with the wizard is manual import.

You can also configure an automatic entitlement import job to run on a periodic basis. The automatic import job imports the entitlements of the control points that are in the Entitlement Import Required state.

See [“Configuring the automatic entitlements import”](#) on page 407.

Consider the following case:

- You have a control point that is in the Entitlements Import Required state.
- The automatic entitlement import job is scheduled to run at 12 midnight.
- You import the entitlements of the control points manually at 8 PM before the automatic entitlement import job runs.
- The automatic entitlement import does not fetch any entitlements as the control point is not in the state of Entitlement Import Required.

To import the entitlements manually

- 1 Go to **Manage > Entitlements > Control Points**.
- 2 Right-click in the table pane and select **Import Entitlements**.
- 3 In the Specify Job Name and Description panel, type the name for the import job in the Name box and click **Next**.

You can alternatively type the description for the import job.

- 4 In the Select Platform, Asset Type, and Entitlement Type panel, select the platform, the control point type, and the entitlement type to import.

Click **Next**.

See [“Control point type and entitlement type”](#) on page 399.

- 5 In the Add Asset Scope panel, select the control points by navigating through the asset hierarchy.

Click **Add** to add the selected control points to the import job and click **Next**.

In case of importing the entitlements for ESM Agents, it is recommended that you customize the templates to limit the entitlement import only for specific objects. The entitlement import for ESM Agents may generate a large amount of data unless you restrict it to a specific scope. The results are stored in the production database (CSM_DB) which may lead to the increase in the size of the database.

- 6 In the Specify Filters panel, under the Data Owners click **Add** and select a data owner.

Only the control points with the selected data owner are included in the imported job. You can select the **Consider Alternate Approver** option if you want to filter on the alternative approver.

- 7 Under the Tags click **Add** and select the tags.

Only the control points with the selected tags are included in the import job. If you select more than one tag, you can also select the **Include only if all tags assigned** option. The selection of this option includes the control points only if all the tags that are added are assigned to the control point. If you do not select the **Include only if all tags assigned** option, the import job includes the control points with any selected tags.

- 8 In the Specify Filters panel, click **Next**.
- 9 In the Schedule panel, select any one of the following:

- If you want to run the job after the wizard closes, check **Run now**.

- If you want to run the job at a specified interval, check **Run periodically** and enter the following information:
 - In the Start On box, enter the start date and time to run the job.
 - Under the Run Periodically options, if you want to run the job only one time, select **Run Once**. If you want to run the job after specific days, select the number of days in the Run Every Day list box. Click **Next**.
- 10 In the Specify Notification Details panel, enter the job completion notification details.

Check **Send notification** and enter the following information:

 - Enter the subject and message of the notification mail.
 - Enter the sender's and the receivers email ID.

Notification can be sent to multiple recipients.
- 11 Click **Next**.
- 12 In the Summary panel, review the configurations that you made for the import job and click **Finish**.

See [“Configuring the automatic entitlements import”](#) on page 407.

Working with approval

The approval-related tasks of the control point include the following:

- Request approval
See [“Requesting approval of entitlements”](#) on page 410.
- Request change
See [“Requesting changes in entitlements”](#) on page 411.
- Approve
See [“Approving the entitlements”](#) on page 411.
- Configure alternative approver
See [“Configuring the alternative approver”](#) on page 412.

Requesting approval of entitlements

Only the entitlements administrator can perform the task of sending an approval request.

You, as an entitlement administrator can send an approval request to the data owner, when the entitlements for control point in status Request for Change are

modified as per the change request. The control points change their status to Entitlement Import Required. After the entitlement import is complete for these control points, the status changes to Request for Approval.

To request approval of entitlements

- 1 Go to Manage > Entitlements > Control Points.
- 2 In the table pane, right-click a control point with the Request for Change status and select **Request Approval**.

See [“Requesting changes in entitlements”](#) on page 411.

See [“Approving the entitlements”](#) on page 411.

Requesting changes in entitlements

Only the data owner or the alternative approver can request changes in entitlements.

You, as an entitlements data owner, can request changes in the entitlements of the control points, if you are in the role of the entitlements data owner for those control points. The control points status changes to Request for Change.

To request changes in entitlements

- 1 Log on as an entitlements data owner.
- 2 Go to Manage > Entitlements > My Control Points.
- 3 In the table pane, select the control point with the status Request for Approval.
- 4 In the details pane, under the Entitlements tab, review the entitlements of the selected control point.
- 5 In the table pane, right-click the control point for which changes should be requested and select **Request Change**.
- 6 In the Request Change for Control Points dialog box, type the change request in the Comments field and click **Request Change**.

See [“Approving the entitlements”](#) on page 411.

Approving the entitlements

Only the data owner or the alternative approver approves the entitlements of the control points, depending on who is the active approver.

You as a data owner, approve the entitlements of the control points, if you are in the role of the entitlements data owner for those control points. The control points status changes to Approved after the control points are approved.

To approve the entitlements

- 1 Log on as an entitlements data owner.
- 2 Go to Manage > Entitlements > My Control Points.
- 3 In the table pane, select the control point with the status Request for Approval.
- 4 In the details pane, under the Entitlements tab, review the entitlements of the selected control point.
- 5 In the table pane, right-click the control point for which changes should be requested and select **Approve**.
- 6 In the Approve Control Points dialog box, type the comments and click **Approve**.

See [“Requesting changes in entitlements”](#) on page 411.

Configuring the alternative approver

The data owner can configure an alternative approver for the control point. You can choose to configure an alternative trustee who can perform the role of the data owner to approve the entitlements in case the data owner is not available.

An entitlement administrator can configure and enable an alternative approver when the control point is configured.

See [“Configuring control points”](#) on page 400.

An entitlement data owner can also configure an alternative approver for the control points that the data owner owns.

To configure the alternative approver

- 1 Log on as an entitlement data owner.
- 2 Go to Manage > Entitlements > My Control Points.
- 3 Right-click the control point for which you want to configure an alternative approver and select Configure Alternative Approver.
- 4 In the Assign Alternative Approver dialog box, select a user from the Available Users list and click **Add**.
- 5 Check **Enable alternative approver** if you want the alternative approver to review the entitlements and approve or request for change in the entitlements.
- 6 Click **OK**

See [“Alternative approver”](#) on page 396.

Comparing entitlements

You can compare the entitlements of a control point, only if the control point is approved at least once.

The current entitlements are compared with the latest approved entitlements.

To compare the entitlements

- 1 Go to > Manage > Entitlements > Control Points.
- 2 In the table pane, select a control point that you want to compare and select **Compare Entitlements**.
- 3 The Compare Entitlements dialog box presents the following details.

Control Point Details

Presents the following details about the control points:

- Asset type
- Domain/ Workgroup name
- Machine name
- Directory name

Entitlement Comparison

Lets you select the entitlement type that you want to compare.

Summary

Displays a record of the change in entitlements in the form of rows added, removed, changed, and unchanged.

View Rows

Lets you select a filter from the drop-down list. You can choose to view only the rows that were added, removed, changed, or unchanged.

- 4 Click **OK** to close the dialog box.

About the daily approval job

The daily approval job is a hidden system job that runs daily at a specified time. You can specify the time for the daily approval job to run daily in the Entitlement Global Settings.

See [“Configuring the entitlements settings”](#) on page 139.

The daily approval job is responsible for the state transitions of the control points in a review cycle.

The notifications about the control point status are sent to the responsible owner after the daily approval job runs.

Working with notifications

Only the entitlement administrator can configure the notification events.

The data owners get the notifications about the important state transitions of the control points that need the attention of the data owner.

In the entitlements system, the control point acquires its status based on where the control point lies in the entitlements workflow. The entitlements system lets you configure the notifications that are sent to the data owners who own the control points. The notifications are sent as an email to the data owner.

See [“About the notification events”](#) on page 414.

See [“Configuring entitlements notifications”](#) on page 418.

About the notification events

In the entitlements system, the control point acquires its status that is based on where it lies in the entitlements workflow. The entitlements system lets you configure the notifications that are sent to the data owners who own the control points. The notifications are meant to inform the data owner about the status of the control point. The notifications are sent as an email to the data owner.

You can configure the following types of notifications:

Review Cycle Start

This notification event is generated at the beginning of the review cycle for the set of control points.

This notification is sent to the user who is mentioned in the To field of the notification.

You can choose to send the notification immediately after the daily approval job runs. The notifications are sent separately for each control point that belongs to the same review cycle.

Or, you can choose to send a single notification after consolidation. The notifications for all the control points that belong to the same review cycle are consolidated in a single notification and sent within an hour.

See [“Configuring entitlements notifications”](#) on page 418.

Approval Period Start

This notification is generated at the beginning of the approval period.

This notification is sent to the user who is mentioned in the To field of the notification.

You can choose to send the notification immediately after the daily approval job runs. The notifications are sent separately for each control point that belongs to the same review cycle.

Or, you can choose to send a single notification after consolidation. The notifications for all the control points that belong to the same review cycle are consolidated in a single notification and sent within an hour.

See [“Configuring entitlements notifications”](#) on page 418.

Approval Period End

This notification is generated at the end of the approval period.

This notification is sent to the user who is mentioned in the To field of the notification.

You can choose to send the notification immediately after the daily approval job runs. The notifications are sent separately for each control point that belongs to the same review cycle.

Or, you can choose to send a single notification after consolidation. The notifications for all the control points that belong to the same review cycle are consolidated in a single notification and sent within an hour.

See [“Configuring entitlements notifications”](#) on page 418.

Review Cycle End

This notification is generated at the end of the review cycle.

This notification is sent to the user who is mentioned in the To field of the notification.

You can choose to send the notification immediately after the daily approval job runs. The notifications are sent separately for each control point that belongs to the same review cycle.

Or, you can choose to send a single notification after consolidation. The notifications for all the control points that belong to the same review cycle are consolidated in a single notification and sent within an hour.

See [“Configuring entitlements notifications”](#) on page 418.

Approval Requested

This notification is generated when the status of the control point changes to Request for Approval.

This notification is sent to the user who is mentioned in the To field of the notification.

You can choose to send the notification immediately after the daily approval job runs. The notifications are sent separately for each control point that belongs to the same review cycle.

Or, you can choose to send a single notification after consolidation. The notifications for all the control points that belong to the same review cycle are consolidated in a single notification and sent within an hour.

See [“Configuring entitlements notifications”](#) on page 418.

Change in Data Owner or Alternative Approver Configuration

This notification is generated when the data owner or the alternative approver is assigned to a control point, or the data owner or the alternative approver changes.

This notification is sent to the user who is mentioned in the To field of the notification.

You can choose to send the notification immediately after the daily approval job runs. The notifications are sent separately for each control point that belongs to the same review cycle.

Or, you can choose to send a single notification after consolidation. The notifications for all the control points that belong to the same review cycle are consolidated in a single notification and sent within an hour.

Approver Activated

This notification is sent to the user who is mentioned in the To field of the notification.

This notification can be sent in any of the following cases:

- When the entitlement administrator configures a data owner.
- When the data owner configures an alternative approver for the control point and enables the alternative approver.

This notification is sent to user that is mentioned in the To field. You can choose to send the notification immediately after the daily approval job runs. The notifications are sent separately for each control point that belongs to the same review cycle.

Or, you can choose to send a single notification after consolidation.

The notifications for all the control points that belong to the same review cycle are consolidated and sent within an hour.

See [“Configuring entitlements notifications”](#) on page 418.

Configuring entitlements notifications

You configure the email notifications from the Manage > Entitlements > Browse Notification Events view.

Note: The notifications are sent to the data owner email addresses that are specified as tokens in the email configuration. The token for the email address reads the email address from the User Management view. Ensure that the User Management view reflects the updated email address of the user to whom the notification should be sent.

To configure notifications

- 1 Go to Manage > Entitlements > Browse Notification Events.
- 2 Right-click the notification event that you want to configure and click **Edit Notification**.
- 3 In the Edit Notification Events dialog box, in the Send notification option, do one of the following:
 - **Immediately**
Sends the notification immediately after the daily approval job runs on the event date.
For example, if the approval period for a control point starts today at 12 PM, the notification is sent immediately when the daily approval job runs after 12 PM. In this case, if another nine control points belong to the same review cycle, then separate notification is sent for each control point for the same event.
 - **After consolidation**
Consolidates the notifications of all the control points that belong to the same review cycle.
For example, if the approval period for ten control points that belong to the same review cycle starts today at 12 PM a consolidated notification is sent within an hour after the daily approval job runs.
- 4 Select **Disable notification for this event** if you want to disable the notification for this event.
- 5 In the **Send reminder notification # days before event date** option, select the number of days. The reminder notification is sent before the specified number of days of the event date.
- 6 Create a notification text with the tokens.
See [“About notification tokens”](#) on page 419.
- 7 To preview the notification, click **Preview** and then click **OK**.

About notification tokens

You use tokens to configure the notification text in the entitlement system. You can customize the notifications that are sent to the data owners when the control point status changes. To create a standard text that should be sent to the data owner, you use the tokens.

Tokens are similar to variables. The actual value replaces the tokens when the notification is sent.

The token with their descriptions are as follows:

DataOwnerMailAddress	<p>Address token that is used in the To field.</p> <p>The email ID of the data owner replaces the token</p>
AlternateApproverMailAddress	<p>Address token that is used in the To field.</p> <p>The email ID of the alternative approver replaces the token.</p>
DataOwnerName	<p>Body or Subject token that can either be used in the subject line or the message body.</p> <p>The name of the data owner replaces the token.</p>
AlternateApproverName	<p>Body or Subject token that can be used either in the subject line or in the message body.</p> <p>The name of the alternative approver replaces the token</p>
ReviewCycleName	<p>Body or Subject token that can be used either in the subject line or in the message body.</p> <p>The name of the review cycle replaces the token.</p>
ReviewCycleStartDate	<p>Body or Subject token that can be used either in the subject line or in the message body.</p> <p>The review cycle start date replaces the token.</p>
ApprovalStartDate	<p>Body or Subject token that can either be used in the subject line or the message body.</p> <p>The approval period start date replaces the token.</p>
ApprovalEndDate	<p>Body or Subject token that can be used either in the subject line or in the message body.</p> <p>The approval period end date replaces the token.</p>

ReviewCycleEndDate	<p>Body or Subject token that can be used either in the subject line or in the message body.</p> <p>The review cycle end date replaces the token.</p>
AutomaticImportRequiredDate	<p>Body or Subject token that can be used either in the subject line or in the message body.</p> <p>The date when the control point status changes to Entitlement Import Required replaces the token.</p>
ReviewCycleSettingsDetails	<p>Body or Subject token that can be used either in the subject line or in the message body.</p> <p>The details of the review cycle settings replace the token.</p>
ReviewCycleDates	<p>Body or Subject token that can be used either in the subject line or in the message body.</p> <p>The dates that are applicable in case of the review cycle replace the token. This includes the approval start, approval end, review start, review end, and the import required dates.</p>
ControlPointIdentifier	<p>Body token that can be used in the message body.</p> <p>The name of the control point replaces the token.</p>
ApproverName	<p>Body or Subject token that can be used either in the subject line or in the message body.</p> <p>The name of the alternative approver replaces the token .</p>
ApproverMailAddress	<p>Body or Subject token that can be used either in the subject line or in the message body.</p> <p>The email ID of the alternative approver replaces the token.</p>

About the entitlements filters

The Filter pane shows the filters that you can use to display only the required control points.

Control Compliance Suite provides the following default filters for filtering the control points:

- Control point status
See [“Control Point Status filter”](#) on page 422.
- Tags
See [“Tag filter”](#) on page 422.

Control Point Status filter

During the entitlements workflow a control point can display a different status at a different point of time. You can use the Control Point Status filter to filter the control points that display a particular status.

You can select from any of the following control point states to filter the control points of your choice:

- Request for Change
- Request for Approval
- Approved
- No Review Configured
- Review Start Awaited
- Approval Start Awaited
- Entitlement Import Required
- Entitlement Import Pending
- Review Started

Tag filter

You can use the Tag filter when you want to filter the existing control points that display a specific tag. From the list of tags, you can select the corresponding check boxes to select the specific tags. The control points that display the selected tag are shown in the table pane.

To edit the filter, you click on the Customize icon at the top of the Filter by pane.

Viewing the control points information in the details pane

You can view the information about the control points through the details pane.

To view the control point information

- 1 In the table pane, select the control point for which you want to view the information.
- 2 View the information for the selected control point in the details pane.

The details pane displays all the information about the selected control point in the following tabs:

- General
See [“Control point details pane- General tab”](#) on page 423.
- Entitlements
See [“Control point details pane- Entitlements tab”](#) on page 424.
- Review Cycle
See [“Control point details pane- Review Cycle tab”](#) on page 424.
- Entitlement Import Details
- Review Cycle Dates
- Tags
See [“Control point details pane- Tags tab”](#) on page 425.
- Exceptions
See [“Control point details pane- Exceptions tab”](#) on page 425.
- Workflow Trails
See [“Control point details pane- Workflow Trails tab”](#) on page 425.

Control point details pane- General tab

The General tab of the control point details pane provides the general information about the selected control point.

The General tab contains the following details about the control points:

Description	Displays the description of the control point that you provide while you configure the control point.
Asset type	Displays the asset type of the control point.

Status	Displays the current status of the control point.
Review cycle name	Displays the name of the review cycle if a review cycle is associated with the control point.
Configuration change date	Displays the last date when the control point configuration was changed.
Creation date	Displays the date when the asset was marked as a control point.
Data owner display name	Displays the display name of the data owner, wherever applicable.
Data owner SAM account name	Displays the SAM account name of the data owner in the domain\username format.
Alternative approver display name	Displays the name of the alternative approver.
Alternative approver SAM account name	Displays the SAM account name of the alternative approver in the domain\username format.
Alternative approver active	Displays Yes if the alternative approver is enabled and No if the alternative approver is not enabled.

Control point details pane- Entitlements tab

The Entitlements tab of the control points details pane presents the entitlements in case the entitlements are imported for the control point.

You can select the entitlement type in case of the Oracle, the SQL, and the ESM control points. You can view the entitlement details of the selected entitlement type.

You can also choose to view the simple or the effective permissions.

Control point details pane- Review Cycle tab

The Review Cycle tab presents all the details of the review cycle that are associated with the selected control point.

The details include the following:

- Name
- Review duration
- Next review start date
- Approval start
- Approval duration
- Import entitlements # days before the approval start
- Is recurring (Yes or No)

See [“Creating a review cycle setting”](#) on page 402.

Control point details pane- Tags tab

The Tags tab of the control point details pane contains a list of all the tags that are associated with the selected asset.

The Tags tab also lets you add a new tag to associate with the selected asset.

You can also remove a tag that is already associated with the asset from the Tags tab.

Control point details pane- Exceptions tab

The Exceptions tab lists all the exceptions that are applied to the selected control point.

Control point details pane- Workflow Trails tab

The Workflow Trails tab of the control point details pane provides information about the control point status changes.

The Workflow Trails tab presents a tabular view that contains the date and the time details about the control point status transition.

Managing exceptions

This chapter includes the following topics:

- [Concepts in exception](#)
- [About the Exceptions view](#)
- [Working with exceptions](#)

Concepts in exception

Before you begin to perform the exception-related tasks, you should review the following concepts in exceptions:

- Exception Management System
See [“About the exception management system”](#) on page 428.
- Exceptions
See [“About exceptions”](#) on page 428.
- Exception validity
See [“About exception validity ”](#) on page 429.
- Exception templates
See [“About exception templates”](#) on page 430.
- Exception states
See [“About exception states ”](#) on page 431.
- Exception filters
See [“About the exception filters”](#) on page 432.

About exceptions

Exceptions are the temporary permissions that exempt an asset from following an organizational policy for a specific time period. Make an exception for a valid business reason.

For example, consider a check that verifies whether the latest Microsoft patch is installed on Windows Server 2003. The mailing server administrator may only be able to apply the patch over the weekend. Because applying the patch requires the computer to be restarted, which can have an effect on the mailing infrastructure of the company. Under such a situation, the mailing administrator can request an exception to be made.

The exception management system creates and tracks exceptions in Control Compliance Suite.

Before creating exceptions, complete the settings available in the Settings > General Settings > Exceptions.

The following permissions must be assigned while creating exceptions:

Exception for asset on check or an exception for check on asset View Asset and View Standard

Exception for control points View Asset

Exception for policy on asset or an exception for asset on policy View Asset and View Policies

Certain predefined roles are required for exceptions.

See [“Predefined roles”](#) on page 80.

See [“About the exception management system”](#) on page 428.

About the exception management system

Exception management is a well-defined system that is used to create, manage, track, and report the exceptions in the Control Compliance Suite.

The exception management system provides a central place for handling exceptions of different modules in Control Compliance Suite.

At the present time, the following modules are permitted the use of exceptions:

- Standards
- Entitlements
- Policies

See [“About exceptions”](#) on page 428.

About exception validity

Exceptions are applicable only for a specific time period. This time period is specified when the exception is requested. You can modify the time period when you edit the exception.

The exception validity time period consists of the following terms:

Effective date	<p>The start date when the exception is applied to the specified objects.</p> <p>When you modify an exception, you can only postpone the effective date. For example, if the validity period is 24th Aug to 26th Aug, you can change the effective date to 25th or 26th Aug. You cannot change the date to 23rd Aug.</p>
Effective time	<p>The local time at which the exception validity period begins. The exception is applied to the specified objects at this time on the specified effective date.</p> <p>When an exception is created or modified, the effective time by default is 12:00 a.m. local time.</p>
Expiration date	<p>The end date when the exception no longer remains valid. From this date onward, the exception is not applied to the specified objects.</p> <p>The expiration date must be equal to or greater than the effective date. You can change this date when you modify an exception.</p> <p>When the current date exceeds the expiration date, the exceptions are marked as expired automatically.</p>

Expiration time	<p>The local time at which the exception validity period ends. The exception becomes invalid at this time on the specified expiration date.</p> <p>When an exception is created or modified, the expiration time by default is 11:59 p.m. local time.</p> <p>An internal system job runs at 12 a.m. by default to mark all the exceptions due for expiration as Expired.</p> <p>Ensure that your scheduled jobs such as an Evaluation job, Collection-Evaluation-Reporting job and so on do not clash with the scheduled time of the system job.</p> <p>The system job is internal and is not visible in the Jobs view. However, you can change the scheduled time of the system job.</p>
-----------------	--

About exception templates

Each module that registers with the exceptions management system has a template. A template governs the kind of information that is stored in the exception. The template specifies the objects that are exempted from following the normal organizational process. A module can have more than one template.

Table 9-1 Templates

Module	Template	Objects
Standards	Evaluation Exception	<p>The objects are as follows:</p> <ul style="list-style-type: none">■ Standards■ Sections■ Checks <p>The objects can be associated with assets, asset groups, and asset containers.</p>
Entitlements	Entitlement Exception	Control Points

Table 9-1 Templates (*continued*)

Module	Template	Objects
Policies	Policy Exception	Policies The objects can be associated with assets, asset groups, and asset containers.

About exception states

The exception workflow with reference to the exception states can be explained as follows:

- A requestor requests an exception for a particular object. An exception request is created and the initial state is set to Requested.
- An approver must then review the requested exception. The approver can go through the exception details and act in one of the following ways:
 - The approver can set the exception state to In Review to show that the exception is under consideration.
 - The approver may want more information regarding the exception. The Approver can then set the exception state to Request Clarification.
 - The approver can review the exception details and approve the exception. The exception state is set to Approved.
 - If the approver does not want to approve the exception request, the approver can set the exception state to Deny.
- If the approver takes no action on the exception request until the specified effective date, then the system sets the state to Approval Overdue.
- If the expiration date of the exception is reached, then the system sets the exception state to Expired. A requestor can also set the state to Expired if the exception is no longer required. An approver cannot set the exception state to Expired.

An exception can be in one of the following states:

Table 9-2 Exception states

Exception State	Description
Requested	This state indicates that a requestor has requested or modified an exception.
Approved	This state indicates that an approver has approved the exception.

Table 9-2 Exception states *(continued)*

Exception State	Description
Request Clarification	This state indicates that the approver requires additional information about the exception.
In Review	This state indicates that the approver has the exception under consideration.
Deny	This state indicates that the approver has rejected the exception request.
Approval Overdue	This state indicates that the approver has performed no action on the exception request until the effective date of the exception.
Expired	<p>This state indicates that the exception is now invalid.</p> <p>The system sets the status of an exception as expired when the current date has exceeded the expiration date of the exception.</p> <p>A requestor can set the status of an exception as expired at any time.</p>

About the exception filters

The Filter by pane contains the filters that you can use to display only the required exceptions.

The Control Compliance Suite provides the following default filters for filtering the exceptions:

Exception Types	Lets you filter the exceptions according to the type of module for which the exception is created.
Exception States	Lets you filter the exceptions according to the specified exception state.
Others	Lets you filter the exceptions according to the specified requestors.
Select Tags	<p>Lets you filter the exceptions according to the specified tags.</p> <ul style="list-style-type: none">■ Match Any. Select the Match Any option to display the exceptions that match any one of the listed tags.■ Match All. Select the Match All option to display the exceptions that match all the listed tags.

About the Exceptions view

The exception management view is used to manage and track all the exceptions in the Control Compliance Suite.

You can access the exception management view from Manage > Exceptions.

The exception management view lets you perform the following tasks:

- Request an exception for specific objects.
- Approve an exception request.
- Edit an exception.
- Change the exception state.

Working with exceptions

You can perform the following tasks using exceptions:

- View exception information in the details pane
See [“Viewing exception information in the details pane”](#) on page 433.
- Request an exception
See [“Requesting an exception”](#) on page 436.
- Approve an exception
See [“Approving an exception”](#) on page 441.
- Set the exception state to In Review
See [“Setting the exception state to In Review”](#) on page 444.
- Set the exception state to Request Clarification
See [“Setting the exception state to Request Clarification”](#) on page 444.
- Set the exception state to Deny
See [“Setting the exception state to Deny”](#) on page 444.

Viewing exception information in the details pane

You can view the information about an exception through the details pane.

To view the exception information

- 1 In the table pane of the Exceptions view, select the exception for which you want to display the information.
- 2 View the information for the selected exception in the details pane.

The exception details are contained in the following tabs:

- General
See “Exceptions details pane - General tab” on page 434.
- Associations
See “Exceptions details pane - Associations tab” on page 435.
- Tags
See “Exceptions details pane - Tags tab” on page 435.
- Workflow Trails
See “Exceptions details pane - Workflow Trails tab” on page 435.

Exceptions details pane - General tab

The General tab of the Exceptions details pane provides general information about the selected exception.

The General tab presents the following information:

Title	The name of the exception.
Type	The module that contains the objects that should be exempted.
Requestor	The name of the requestor.
Effective Date	The start date of the exception validity period. The exception is applied to the specified objects from this date onward.
Effective Time	The local time at which the exception validity period begins. The exception is applied to the specified objects at this time on the specified effective date.
Expiration Date	The end date of the exception validity period. From this date onward, the exception is no longer applicable on the specified objects.
Expiration Time	The local time at which the exception validity period ends. The exception becomes invalid at this time on the specified expiration date.
Requestor Group	The name of the requestor group.
Requestor Email ID	The email address of the requestor.
Attachment	The name of the files that are attached with the exception.
Description	The description for the exception.

See [“Viewing exception information in the details pane”](#) on page 433.

Exceptions details pane - Associations tab

The Associations tab of the exceptions details pane provides information about the selected objects.

The Associations tab presents a list of selected checks and assets.

You may not be able to see any objects on the Associations tab if either of the following situations is present:

- The requestor has not entered the object information.
- You do not have the required permissions to view all the objects that the requestor has selected.

If guid is visible or associations are not visible then the following permissions must be given:

Exception for asset on check or an exception View Asset and View Standard
for check on asset

Exception for control points View Asset

Exception for policy on asset or an exception View Asset and View Policies
for asset on policy

See [“Viewing exception information in the details pane”](#) on page 433.

Exceptions details pane - Tags tab

The Tags tab contains a list of all the tags that are associated with a selected exception.

The Tags tab lets you apply the tags that can be associated with a selected exception. You can also remove the tags that are already associated with an exception.

See [“Viewing exception information in the details pane”](#) on page 433.

Exceptions details pane - Workflow Trails tab

The Workflow Trails tab lets you keep track of all the state changes that an exception has gone through.

The Workflow Trails tab contains the following information:

Modifier Name	The name of the user who has initiated the state change of the exception.
Modifier SAM Account name	The SAM Account name of the modifier. The format for the SAM Account name is domain name\user name.
Changed Status	The state of the exception.
Comments	The remarks that the user entered.
Status Changed on	The date and time at which the state of the exception was changed.

See [“Viewing exception information in the details pane”](#) on page 433.

Requesting an exception

A requestor can request an exception through the Request Exception Wizard.

A requestor can request an exception on the following objects:

- Standards, sections, or checks
See [“Requesting an exception for assets on checks”](#) on page 436.
- Control points
See [“Requesting an exception for control points”](#) on page 438.
- Policies
See [“Requesting an exception for assets on policies”](#) on page 439.

Similarly, you can request an exception by launching the Request Exception Wizard from the Standards view, Assets view, and the Evaluation Results dialog.

See [“Launching the Request Exception Wizard”](#) on page 440.

See [“About exception states ”](#) on page 431.

Requesting an exception for assets on checks

A requestor can request an exception on the checks for specific assets in the organization.

To request an exception

- 1 Go to Manage > Exceptions.
- 2 In the Exceptions view, do either of the following:
 - On the taskbar, click **Request Exception**.
 - In the table pane, right-click anywhere on the grid and select **Request Exception**.

- 3 In the Request Exception Wizard, in the Specify Exception Details panel, enter the following details and click **Next**:
 - In the Title box, enter the name of the exception.
 - In the Type box, select **Standards**.
In the Template box, the displayed template is Evaluation Exception.
 - In the Description box, type a description for the exception.
 - In the Attachment box, browse to enter the name of the file that you want to attach.
 - In the Exception Validity group box, in the Effective Date box, select the date on which the exception becomes applicable. In the Expiration Date box, select the date on which the exception becomes invalid. Click **Next**.
- 4 In the Select Checks and Assets panel, click **Add** to select the standards, sections, or checks.

All the checks within the selected standard or section are displayed.
- 5 In the Select Standards or Sections or Checks dialog box, expand the Standards folder and select a folder. The standards within the selected folder are displayed in the right pane. Select a standard, section, or check and click **Add**. Click **Add All** to select all the standards. To remove one or more standards from the Selected Items list, click **Remove** or **Remove All**. Click **OK**.

All the checks within the selected standard or section are displayed in the Select Checks and Assets Panel.
- 6 In the Select Checks and Assets panel, click **Add** to select the assets. In the Select Assets or Asset Groups or Folders dialog box, expand the Assets folder and select a folder. The assets within the selected folder are displayed in the right pane. Select an asset and click **Add**. Click **Add All** to select all the assets. To remove one or more assets from the Selected Items list, click **Remove** or **Remove All**. Click **OK**.
- 7 In the Specify Exception Type Information panel, click **Next**.

- 8 In the Specify Requestor Information panel, type or browse to enter the Requestor and the Requestor Group. Enter the Requestor Email ID and Comments.
- 9 In the Summary panel, verify the details that you have entered in the wizard. Click **Back** to modify any data. Click **Finish** to exit the wizard.

The exception is created and its state is set to Requested.

Similarly, you can request an exception by launching the Request Exception Wizard from the Standards view, Assets view, and the Evaluation Results dialog box.

See [“Launching the Request Exception Wizard”](#) on page 440.

See [“About exception states ”](#) on page 431.

Requesting an exception for control points

A requestor can request an exception for specified control points in the organization.

To request an exception

- 1 Go to Manage > Exceptions.
- 2 In the Exceptions view, do either of the following:
 - On the taskbar , click **Request Exception**.
 - In the table pane, right-click anywhere on the grid and select **Request Exception**.
- 3 In the Request Exception Wizard, in the Specify Exception Details panel, enter the following details and click **Next**:
 - In the Title box, enter the name of the exception.
 - In the Type box, select **Entitlements**.
In the Template box, let the displayed template name remain as Entitlement Exception.
 - In the Description box, type a description for the exception.
 - In the Attachment box, browse to enter the name of the file that you want to attach.
 - In the Exception Validity group box, in the Effective Date box, select the date on which the exception becomes applicable. In the Expiration Date box, select the date on which the exception becomes invalid. Click **Next**.
- 4 In the Select Control Points panel, click **Add** to select the control points.

- 5 In the Select Control Points dialog box, expand the Asset System folder and select a folder. Select the control points that you want to exempt and click **Add**. Click **Add All** to select all the control points. To remove one or more control points from the Selected Items list, click **Remove** or **Remove All** respectively. Click **OK**.
- 6 In the Select Control Points panel, click **Next**.
- 7 In the Specify Requestor Information panel, type or browse to enter the Requestor and the Requestor Group. Enter the Requestor Email ID and Comments.
- 8 In the Summary panel, verify the details that you have entered in the wizard. Click **Back** to modify any data. Click **Finish** to exit the wizard.

The exception is created and its state is set to Requested.

See [“Launching the Request Exception Wizard”](#) on page 440.

See [“About exception states ”](#) on page 431.

Requesting an exception for assets on policies

A requestor can request an exception on the policies for specific assets in the organization.

To request an exception

- 1 Go to Manage > Exceptions.
- 2 In the Exceptions view, do either of the following:
 - On the taskbar , click **Request Exception**.
 - In the table pane, right-click anywhere on the grid and select **Request Exception**.
- 3 In the Request Exception Wizard, in the Specify Exception Details panel, enter the following details and click **Next**:
 - In the Title box, enter the name of the exception.
 - In the Type box, select **Policies**.
In the Template box, let the displayed template name remain as Policy Exception.
 - In the Description box, type a description for the exception.
 - In the Attachment box, browse to enter the name of the file that you want to attach.

- In the Exception Validity group box, in the Effective Date box, select the date on which the exception becomes applicable. In the Expiration Date box, select the date on which the exception becomes invalid. Click **Next**.
- 4 In the Select Policies and Assets panel, click **Add** to select the policies.
- 5 In the Select Policies dialog box, expand the Policies folder and select a folder. Select the policies and click **Add**. Click **Add All** to select all the policies. To remove one or more policies or all the policies from the Selected Items list, click **Remove** or **Remove All**. Click **OK**.
- 6 In the Select Policies and Assets panel, click **Add** to select the assets. In the Asset Object Chooser dialog box, expand the Assets folder and select a folder. Select the assets and click **Add**. Click **Add All** to select all the assets. To remove the assets from the Selected Items list, select the assets and click **Remove**. Click **Remove All** to remove all the assets. Click **OK**.
- 7 In the Select Policies and Assets panel, click **Next**.
- 8 In the Specify Requestor Information panel, type or browse to enter the Requestor and the Requestor Group. Enter the Requestor Email ID and Comments.
- 9 In the Summary panel, verify the details that you have entered in the wizard. Click **Back** to modify any data. Click **Finish** to exit the wizard.

The exception is created and its state is set to Requested.

See [“Launching the Request Exception Wizard”](#) on page 440.

See [“About exception states ”](#) on page 431.

Launching the Request Exception Wizard

You can request an exception through the Request Exception Wizard. The Request Exception Wizard can be launched from various views.

To launch the Request Exception Wizard from the Standards view

- 1 Go to Manage > Standards
- 2 In the Standards view, select the standards, sections, or checks for which you want to request an exception and do one of the following:
 - On the taskbar , click **Request Exception**.
 - On the Tasks menu, click **Request Exception**.
 - In the table pane, right-click the selection and select **Request Exception**.

To launch the Request Exception Wizard from the Assets view

- 1 Go to Manage > Asset Management > Assets.
- 2 In the Assets view, select the assets for which you want to create an exception and do one of the following:
 - On the taskbar, click **Request Exception**.
 - On the Tasks menu, click **Request Exception**.
 - In the table pane, right-click the selection and select **Request Exception**.

To launch the Request Exception Wizard from the Exceptions view

- 1 Go to Manage > Exceptions.
- 2 In the Exceptions view, do one of the following:
 - On the taskbar, click **Request Exception**.
 - In the table pane, right-click anywhere on the grid and select **Request Exception**.

Approving an exception

An approver can approve an exception through the Approve Exception Wizard.

An approver can approve an exception request on the following objects:

- Standards, sections, or checks
See [“Approving an exception for assets on checks”](#) on page 441.
- Control points
See [“Approving an exception for control points”](#) on page 442.
- Policies
See [“Approving an exception for policies”](#) on page 443.

See [“About exception states ”](#) on page 431.

Approving an exception for assets on checks

An approver can approve an exception request on the checks for specific assets in the organization.

To approve an exception

- 1 Go to Manage > Exceptions.
- 2 In the table pane of the Exceptions view, do either of the following:
 - Select the exception that you want to approve, right-click, and select **Approve Exception**.

- Select the exception that you want to approve and select **Approve Exception** on the taskbar.
- 3 In the View Exception Details panel, view the exception information that the requestor has entered. Click **Next**.
 - 4 In the View or Select Checks and Assets panel, view the information that the requestor has entered. All the objects (checks and assets) may not be visible in case of either of the following situations:
 - The requestor has not entered the object information.
In this case, click **Add** to specify the objects for which the exception must be created.
 - You do not have the required permissions to view all the objects that the requestor has selected. In this case, ensure that you get the required permissions.
 - 5 Click **Next**.
 - 6 In the Specify Comments panel, in the Comments box, enter your comments.
 - 7 In the Summary panel, verify the details that you have entered in the wizard. Click **Back** to modify any data. Click **Finish** to exit the wizard.
- The state of the exception is set to Approved. In the table pane, the exception is present under the Approved list.

Approving an exception for control points

An approver can approve an exception request for specific control points in the organization.

To approve an exception

- 1 Go to Manage > Exceptions.
- 2 In the table pane of the Exceptions view, do either of the following:
 - Select the exception that you want to approve, right-click, and select **Approve Exception**.
 - Select the exception that you want to approve and select **Approve Exception** on the taskbar.
- 3 In the View Exception Details panel, view the exception information that the requestor has entered. Click **Next**.
- 4 In the View or Select Control Points panel, view the information that the requestor has entered. All the objects (control points) may not be visible in case of either of the following situations:

- The requestor has not entered the object information.
In this case, click **Add** to specify the objects for which the exception must be created.
 - You do not have the required permissions to view all the objects that the requestor has selected. In this case, ensure that you get the required permissions.
- 5 Click **Next**.
 - 6 In the Specify Comments panel, in the Comments box, enter your comments.
 - 7 In the Summary panel, verify the details that you have entered in the wizard. Click **Back** to modify any data. Click **Finish** to exit the wizard.
- The state of the exception is set to Approved. In the table pane, the exception is present under the Approved list.

Approving an exception for policies

An approver can approve an exception request on the policies for specific assets in the organization.

To approve an exception

- 1 Go to Manage > Exceptions.
- 2 In the table pane of the Exceptions view, do either of the following:
 - Select the exception that you want to approve, right-click, and select **Approve Exception**.
 - Select the exception that you want to approve and select **Approve Exception** on the taskbar.
- 3 In the View Exception Details panel, view the exception information that the requestor has entered. Click **Next**.
- 4 In the View or Select Policies and Assets panel, view the information that the requestor has entered. All the objects (policies and assets) may not be visible in case of either of the following situations:
 - The requestor has not entered the object information.
In this case, click **Add** to specify the objects for which the exception must be created.
 - You do not have the required permissions to view all the objects that the requestor has selected. In this case, ensure that you get the required permissions.
- 5 Click **Next**.

- 6 In the Specify Comments panel, in the Comments box, enter your comments.
- 7 In the Summary panel, verify the details that you have entered in the wizard. Click **Back** to modify any data. Click **Finish** to exit the wizard.

The state of the exception is set to Approved. In the table pane, the exception is present under the Approved list.

Setting the exception state to In Review

An approver can set the exception state to In Review to show that the exception is under the review process.

To set the In Review state

- 1 Go to Manage > Exceptions.
- 2 In the Exceptions view, select the exception, right-click, and select **Set Status to In Review**.
- 3 In the Comments dialog box, type your comments and select **In Review**.

See [“About exception states ”](#) on page 431.

Setting the exception state to Request Clarification

An approver can set the exception state to Request Clarification to show that some additional information is required before the exception can be approved.

To set the Request Clarification state

- 1 Go to Manage > Exceptions.
- 2 In the Exceptions view, select the exception, right-click, and select **Request Clarification**.
- 3 In the Comments dialog box, type your comments and select **Request Clarification**.

See [“About exception states ”](#) on page 431.

Setting the exception state to Deny

An approver can set the exception state to Deny to show that the exception request has been rejected.

To set the Deny state

- 1 Go to Manage > Exceptions.
- 2 In the Exceptions view, select the exception, right-click, and select **Deny Exception**.
- 3 In the Comments dialog box, type your comments and select **Deny**.

See “[About exception states](#)” on page 431.

Setting the exception state to Expire

A requestor can set the exception state to Expire to make the exception invalid.

To set the Expire state

- 1 Go to Manage > Exceptions.
- 2 In the Exceptions view, select the exception, right-click, and select **Terminate Exception**.
- 3 In the Confirm Expire dialog box, click **Expire**.

See “[About exception states](#)” on page 431.

Modifying an exception

A requestor can modify the exception information through the details pane.

You cannot edit an expired exception.

Note: When an exception is modified, the state of the exception is set to Requested.

To modify an exception

- 1 Go to Manage > Exceptions.
- 2 In the Exception view, select the exception that you want to modify.
- 3 In the details pane, on the general tab, you can edit the following information:
 - Effective Date
 - Expiration Date
 - Requestor Email ID
 - Description
- 4 On the Associations tab, click **Add** to select and add the objects to the exception. To remove the objects, select the objects and click **Remove**.

- 5 On the Tags tab, click **Add Tag** to add a tag for the exception. To remove tags, select the tags and click **Remove Tag**.
- 6 Click the save icon to save your changes.

Managing standards

This chapter includes the following topics:

- [Concepts in standards management](#)
- [Concepts in checks](#)
- [About the Standards view](#)
- [About the standard migration utility for ESM and CCS](#)
- [Working with standards](#)
- [Working with sections](#)
- [Working with checks](#)
- [Working in the details pane](#)
- [Working with gold standard](#)
- [Working with Evaluation Results](#)
- [About risk score calculation](#)

Concepts in standards management

Standards, sections, and checks form the backbone of the Standards module.

Before you begin to perform the standards tasks, you must go through the following concepts:

- Standards
See [“About standards”](#) on page 448.
- Predefined standards
See [“About predefined standards”](#) on page 449.

- Sections
See [“About sections”](#) on page 453.
- Checks
See [“About checks”](#) on page 453.
- Gold standard
See [“About gold standard”](#) on page 464.
- Data collection job
See [“About data collection jobs”](#) on page 454.
- Evaluation job
See [“About evaluation jobs”](#) on page 454.
- Compliance score
See [“About compliance score”](#) on page 463.
- Risk score
See [“About risk score”](#) on page 463.

About standards

Standards provide the means for assessing the compliance of an asset. In Control Compliance Suite, a standard is a hierarchical organizational structure of sections and checks.

Control Compliance Suite makes available a set of predefined standards that are installed along with the product. These standards are mostly derived from some published guidelines by established organizations such as CIS or NSA.

You can also create new standards that are based on your specific requirements. In Control Compliance Suite, the standards hierarchy is explained as follows:

- A standard contains one or more sections.
- Each section can further contain other sections or checks.
- A check is always contained within a section in a standard.

See [“About sections”](#) on page 453.

See [“About checks”](#) on page 453.

See [“About predefined standards”](#) on page 449.

See [“Working with standards”](#) on page 486.

See [“About versioning scheme”](#) on page 465.

About predefined standards

Predefined standards are the standards that are installed along with Control Compliance Suite. These standards are present in the Predefined folder in the tree pane of the Standards view. The predefined standards are not editable, but can be copied to the user-defined folder. The copies can then be modified.

You can perform only the following actions on the predefined standards:

- Copy
- Export
- Set up a data collection job
- Run an evaluation job
- Request an exception
- Run collection-evaluation-reporting job

Control Compliance Suite ships with the predefined standards for the following platforms:

- ESM
See [“Predefined standards for ESM”](#) on page 449.
- Oracle
See [“Predefined standards for Oracle”](#) on page 451.
- SQL
See [“Predefined standards for SQL”](#) on page 451.
- UNIX
See [“Predefined standards for UNIX”](#) on page 452.
- Windows
See [“Predefined standards for Windows”](#) on page 452.
- NetWare
- Exchange
See [“Predefined standards for Exchange”](#) on page 453.

See [“About standards”](#) on page 448.

See [“Working with standards”](#) on page 486.

Predefined standards for ESM

The predefined standards are the standards that are installed along with the product. The predefined standards are present in the predefined folder in the tree pane. These standards are not editable.

Each check expression in a standard is mapped to an ESM policy. You can also map multiple checks of an ESM policy to one CCS standard. The checks that a predefined standard contains map to only one ESM policy. However, in customized standards, you can map each check to different CCS standards.

Note: You cannot edit a predefined standard. You can copy the predefined standards and then customize them as per your requirement.

See [“Copying and pasting a standard”](#) on page 492.

Table 10-1 contains the following information:

- The name of the predefined CCS standards.
- The corresponding ESM policies, which contain the checks that map to each CCS standard.
- The location of the policy installer.

Table 10-1 CCS standard to ESM policy mapping

Predefined CCS standard	ESM policy	ESM policy installer in the product disc
ESM - CIS Legacy Security Settings Benchmark for Windows 2003 Domain Controller v2.0	Security essentials W2K3DC v2.0	Content_Updates\Policies\Security Essentials\Policies\Windows_2003_Security Essentials.exe
ESM - CIS Windows Server 2003 Legacy Security Settings for Domain Member Servers v2.0	Security essentials W2K3MS v2.0	Content_Updates\Policies\Security Essentials\Policies\Windows_2003_Security Essential.exe
ESM - CIS for Solaris 10 Benchmark v4.0	Security essentials Sol 10 v4.0	Content_Updates\Policies\Security Essentials\Policies\Solaris\Solaris10_Security Essentials.exe
ESM - Change Notifications for Windows	WS3 Server SOA Change	Content_Updates\Policies\Sarbanes-Oxley\Policies\Microsoft\Intel\w3s-ix86 \Windows_2003_SOA_Change_Notification.exe

Table 10-1 CCS standard to ESM policy mapping (*continued*)

Predefined CCS standard	ESM policy	ESM policy installer in the product disc
ESM - Change Notifications for UNIX	Sol 8-9 SOA Change	Content_Updates\Policies\Sarbanes-Oxley\Policies\Solaris\Solaris_SOA_Change_Notification.exe
File, Folder Entitlements	File, Folder Entitlements	Content_Updates\Policies\Sarbanes-Oxley\Policies\BestPractice_Entitlement_Reporting.exe
User, Group Entitlements	User, Group Entitlements	Content_Updates\Policies\Sarbanes-Oxley\Policies\BestPractice_Entitlement_Reporting.exe

Note: The ESM - Change Notifications for Windows and ESM - Change Notifications for UNIX standards are based on the Change Notification category of messages in Enterprise Security Manager.

Predefined standards for Oracle

The predefined standards for the Oracle platform are present at the following location in the tree pane of the Standards view:

Standards > Predefined > Oracle

See [“About predefined standards”](#) on page 449.

The following predefined standard for the Oracle platform is installed with the product:

- CIS Oracle 9i and 10g Database Security Benchmark v2.0

Predefined standards for SQL

The predefined standards for the SQL platform are present at the following location in the tree pane of the Standards view:

Standards > Predefined > Sql

See [“About predefined standards”](#) on page 449.

The following predefined standards for the SQL platform are installed with the product:

- Security Essentials for Microsoft SQL Server 2005
- CIS Security Configuration Benchmark for Microsoft SQL Server 2005 v1.1.1
- The Australian Government Information and Communications Technology Security Manual for MS-SQL Server
- Security Essentials for SQL Server 2008

Predefined standards for UNIX

The predefined standards for the UNIX platform are present at the following location in the tree pane of the Standards view:

Standards > Predefined > Unix

See [“About predefined standards”](#) on page 449.

The following predefined standards for the UNIX platform are installed with the product:

- Security Essentials for AIX 5.1 and Above
- Security Essentials for Solaris 10
- Security Essentials for HP-UX
- Security Essentials for Red Hat Enterprise Linux 2.1 and Above
- Security Essentials for SuSE Linux Enterprise Server

Predefined standards for Windows

The predefined standards for the Windows platform are present at the following location in the tree pane of the Standards view:

Standards > Predefined > Windows

See [“About predefined standards”](#) on page 449.

The following predefined standards for the Windows platform are installed with the product:

- CIS Legacy Security Settings Benchmark for Windows 2003 Domain Controller v2.0
- CIS Legacy Settings Benchmark for Windows XP Professional v2.0
- CIS Windows 2000 Server Operating System Server Level Two Benchmark for Stand-alone and Member Servers v2.2.1

- CIS Windows Server 2003 Legacy Security Settings for Domain Member Servers v2.0
- Security Essentials for IIS
- The Australian Government Information and Communications Technology Security Manual for Windows
- US Federal Desktop Core Configuration Standard (FDCC) V1.0.1 for Windows Vista
- Windows Patch Assessment Check Library

Predefined standards for Exchange

The predefined standards for the Exchange platform are present at the following location in the tree pane of the Standards view:

Standards >Predefined > Exchange

See [“About predefined standards”](#) on page 449.

The following predefined standards for the Exchange platform are installed with the product:

- Security Essentials for Exchange 2007

About sections

You use a section to organize or to group related checks. A section can contain another section. Hence, a section can be a collection of checks and other sections.

For example, consider that you have one set of checks that relate to account passwords. Another set of checks concern the account lockout policy. You can create two separate sections for each set of checks and place these sections within another section for overall account handling.

See [“About standards”](#) on page 448.

See [“About checks”](#) on page 453.

See [“About versioning scheme”](#) on page 465.

See [“Working with sections”](#) on page 503.

About checks

A check is a test that is performed against one or more assets to determine a pass or a fail status.

A check is composed of one or more check expressions. Multiple check expressions can be joined through operators to form a check formula.

See [“About standards”](#) on page 448.

See [“About sections”](#) on page 453.

See [“About versioning scheme”](#) on page 465.

See [“Working with checks”](#) on page 508.

See [“About operators”](#) on page 478.

About data collection jobs

You create a data collection job to collect data from the assets for specific standards.

The information that you specify during the data collection process is saved in the data collection job. Hence you do not need to specify the collection criteria every time you perform the collection process. Data collection jobs can be scheduled to run at predefined intervals. The jobs can also be modified and deleted.

You can create or edit a data collection job through the **Create or Edit Data Collection Job** wizard.

You can create a collection job from the Standards view, Assets view, and the Job Management view. You can modify, delete, or track the status of a data collection job only from the Job Management view.

See [“Setting up a data collection job from the Standards view”](#) on page 498.

About evaluation jobs

You create an evaluation job to evaluate the assets in your organization against specific standards.

The information that you specify during the evaluation process is saved in the evaluation job. Hence, an evaluation job lets you perform the evaluation process repeatedly without having to specify the evaluation criteria again. Evaluation jobs can be scheduled to run at predefined intervals. You can modify and delete the evaluation jobs.

You can create or edit an evaluation job through the Create or Edit Evaluation Job wizard.

Note: Before you run an evaluation job, you must run a data collection job to obtain accurate evaluation results.

You can create an evaluation job from the Standards view, the Assets view, and the Job Management view. You can edit or delete an evaluation job only from the Job Management view.

See [“Running an evaluation job from the Standards view”](#) on page 495.

About target types

You use a target type to filter the assets during the data collection and the evaluation process. The target type filters the assets on the basis of the asset type. You specify the target type at the time of check creation. A check with a specific target type is applicable only on the specific asset type. For example, an asset of the type Windows Machine cannot be evaluated against a check of the UNIX target type.

The target type can be defined only at the check level. The target type for a standard lists the target type of the checks that are present within the standard. For example, consider a standard that contains two checks. The target type of one check is Windows 2000 Machines and the target type of the other check is Windows 2003 Machines. Then the list of target types for the concerned standard contains both Windows 2000 Machines and Windows 2003 Machines.

The target types that exist for the checks within the predefined standards are known as predefined target types.

Control Compliance Suite contains predefined target types for the following platforms:

- SQL
See [“About SQL predefined target types”](#) on page 455.
- Windows
See [“About Windows predefined target types”](#) on page 456.
- UNIX
See [“About UNIX predefined target types”](#) on page 457.
- Oracle
See [“About Oracle predefined target types”](#) on page 461.
- Enterprise Security Manager
See [“About ESM predefined target types”](#) on page 462.

About SQL predefined target types

The SQL predefined target types are as follows:

Table 10-2 Supported SQL target types

Target type	Description
SQL Server 2005 Instances	All Microsoft SQL Server 2005 instances.
SQL Server 2000 Instances	All Microsoft SQL Server 2000 instances.
SQL Server 7 Instances	All Microsoft SQL Server 7 instances.
SQL Server Instances	All Microsoft SQL Server instances.

See [“About target types”](#) on page 455.

About Windows predefined target types

The Windows predefined target types are listed as follows:

Table 10-3 Supported Windows predefined target types

Target type	Description
Windows 2000 or Later Member Servers	All Windows 2000 or later Server Machine Types (no domain controllers)
Windows 2000 Member Servers	All Windows 2000 Server Machine Types (no domain controllers)
All Windows Machines	All Windows computers
Windows 2000 Advanced Servers	Windows 2000 Advanced Server computers (no domain controllers)
Windows 2000 Machines	Windows 2000 computers only
Windows 2000 or Later Machines	All Windows 2000 or later computers.
Windows 2000 Professional Machines	Windows 2000 Professional computers
Windows 2003 Domain Controller Servers	Windows 2003 Domain Controller Server computers
Windows 2003 Machines	Windows 2003 computers only
Windows 2003 Member Servers	Windows 2003 Domain Member Server computers (no domain controllers)
Windows Vista Machines	Windows Vista computers only
Windows XP Professional Machines	Windows XP computers only

Table 10-3 Supported Windows predefined target types (*continued*)

Target type	Description
Windows 2000 Domain Controller Servers	All Windows 2000 Server Machine Types (Domain Controllers)
Windows 7 Machines	All Windows 7 computers
Windows server 2008 Machines	All Windows server 2008 computers

See [“About target types”](#) on page 455.

About UNIX predefined target types

The UNIX predefined target types are as follows:

Table 10-4 Supported UNIX target types

Target type	Description
AIX 5.1 and later Machines	All computers that are installed with version AIX 5.1 or later
AIX 5.1 Machines	All computers that are installed with AIX 5.1
AIX 5.2 Machines	All computers that are installed with AIX 5.2
AIX 5.3 Machines	All computers that are installed with AIX 5.3
AIX 6.1 Machines	All computers that are installed with AIX 6.1
All AIX Machines	All computers that are installed with AIX
All HP-UX Machines	All computers that are installed with HP-UX computers
All Redhat non Enterprise Linux Machines	All computers that are installed with RedHat Linux excluding theRedHat Enterprise Linux.
All SuSE Linux Enterprise Server Machines	All computers that are installed with SuSE Linux Enterprise Server
All SuSE Linux Machines	All computers that are installed with SuSE Linux
Fedora Machines	All the Fedora computers.
HP-UX 11.00 and 11.23 Machines	All computers that are installed with HP-UX 11.00 or 11.23

Table 10-4 Supported UNIX target types (*continued*)

Target type	Description
HP-UX 11.00 and 11.11 Machines	All computers that are installed with HP-UX 11.00 or 11.11
HP-UX 11.00 Machines	All computers that are installed with HP-UX 11.00
HP-UX 11.00, 11.11 and 11.23 Machines	All computers that are installed with HP-UX 11.00, 11.11, or 11.23
HP-UX 11.11 and 11.23 Machines	All computers that are installed with HP-UX 11.11 or 11.23
HP-UX 11.11 Machines	All computers that are installed with HP-UX 11.11
HP-UX 11.23 Machines	All computers that are installed with HP-UX 11.23
HP-UX 11.x Machines	All computers that are installed with HP-UX 11.x
Red Hat Enterprise Linux 2.1 and 3.0 Machines	All computers that are installed with Red Hat Enterprise Linux 2.1 or 3.0
Red Hat Enterprise Linux 2.1 and 4.0 Machines	All computers that are installed with Red Hat Enterprise Linux 2.1 or 4.0
Red Hat Enterprise Linux 2.1 and Later Machines	All computers that are installed with Linux 2.1 or later
Red Hat Enterprise Linux 2.1 Machines	All computers that are installed with Linux 2.1
Red Hat Enterprise Linux 2.1, 3.0 and 4.0 Machines	All computers that are installed with 2.1, 3.0, or 4.0
Red Hat Enterprise Linux 3.0 and 4.0 Machines	All computers that are installed with Red Hat Enterprise Linux 3.0 or 4.0
Red Hat Enterprise Linux 3.0 and Later Machines	All computers that are installed with Red Hat Enterprise Linux 3.0 or later
Red Hat Enterprise Linux 3.0 Machines	All computers that are installed with Red Hat Enterprise Linux 3.0
Red Hat Enterprise Linux 4.0 and Later Machines	All computers that are installed with Red Hat Enterprise Linux 4.0 or Later

Table 10-4 Supported UNIX target types (*continued*)

Target type	Description
Red Hat Enterprise Linux 4.0 Machines	All computers that are installed with Red Hat Enterprise Linux 4.0
Red Hat Enterprise Linux 5.0 and Later Machines	All computers that are installed with Red Hat Enterprise Linux 5.0 or Later
Red Hat Enterprise Linux 5.0	All computers that are installed with Red Hat Enterprise Linux 5.0
Red Hat Enterprise Linux Machines	All computers that are installed with Red Hat Enterprise Linux
Redhat 7.0 Machines	All computers that are installed with RedHat 7.0
Redhat 7.1 Machines	All computers that are installed with RedHat 7.1
Redhat 7.2 Machines	All computers that are installed with Redhat 7.2
Redhat 7.3 Machines	All computers that are installed with Redhat 7.3
Redhat 8.0 Machines	All computers that are installed with Redhat 8.0
Solaris 10 Machines	All computers that are installed with Solaris 10
Solaris 2.6 and later Machines	All computers that are installed with Solaris 2.6 or later
Solaris 2.6, 7 and 8 Machines	All computers that are installed with Solaris 2.6, 7, or 8
Solaris 7 and earlier Machines	All computers that are installed with Solaris 7 or earlier
Solaris 7 and later Machines	All computers that are installed with Solaris 7 or later
Solaris 7 Machines	All computers that are installed with Solaris 7
Solaris 7,8 and 9	All computers that are installed with Solaris 7, 8, or 9

Table 10-4 Supported UNIX target types (*continued*)

Target type	Description
Solaris 7,8,9 and 10	All computers that are installed with Solaris 7, 8, 9, or 10
Solaris 7,8	All computers that are installed with Solaris 7 or 8
Solaris 8 and 9	All computers that are installed with Solaris 8 or 9
Solaris 8 and earlier Machines	All computers that are installed with Solaris 8 or earlier
Solaris 8 and later Machines	All computers that are installed with Solaris 8 or later
Solaris 8 Machines	All computers that are installed with Solaris 8
Solaris 8,9 and 10	All computers that are installed with Solaris 8, 9, or 10
Solaris 9 and 10	All computers that are installed with Solaris 9 or 10
Solaris 9 and later Machines	All computers that are installed with Solaris 9 or later.
Solaris 9 Machines	All computers that are installed with Solaris 9
Solaris Servers	All computers that are installed with Solaris Servers
SuSE Linux 8.0, 8.1 and 8.2 Machines	All computers that are installed with SuSE Linux 8.0, 8.1, or 8.2
SuSE Linux 9.0, 9.1, 9.2 and 9.3 Machines	All SuSE Linux 9.0, 9.1, 9.2 or 9.3 computers
SuSE Linux Enterprise Server 10 Machines	All SuSE Linux Enterprise Server 10 computers
SuSE Linux Enterprise Server 9 Machines	All SuSE Linux Enterprise Server 9 computers
SuSE Linux Enterprise Server 8.1 and 10 Machines	All computers that are installed with SuSE Linux 8.1, or 10

Table 10-4 Supported UNIX target types (*continued*)

Target type	Description
SuSE Linux Enterprise Server 8.1 and 9 Machines	All computers that are installed with SuSE Linux 8.1, or 9
SuSE Linux Enterprise Server 8.1 Machines	All computers that are installed with SuSE Linux 8.1
SuSE Linux Enterprise Server 9 and 10 Machines	All computers that are installed with SuSE Linux 9 or 10
UNIX Machines - All UNIX Machines	All UNIX computers
VMware 3.0 and Later Machines	All computers that are installed with VMware 3.0 or later
VMware ESX Server 3.0 Machines	All computers that are installed with VMware ESX Server 3.0
VMware ESX Server 3.5 Machines	All computers that are installed with VMware ESX Servers 3.5
VMware ESX Server 3.x Machines	All computers that are installed with VMware ESX Server 3.x
VMware ESX Server 4.x Machines	All computers that are installed with VMware ESX Server 4.x
All VMware ESX Machines	All computers that are installed with VMware ESX

See “[About target types](#)” on page 455.

About Oracle predefined target types

The predefined target types for Oracle are listed as follows:

Table 10-5 Supported Oracle target types

Target type	Description
Oracle 10g Databases	All Oracle 10g databases.
Oracle 8i Databases	All Oracle 8i databases.
Oracle 9i and 10g Databases	All Oracle 9i and 10g databases.
Oracle 9i Databases	All Oracle 9i databases.

Table 10-5 Supported Oracle target types (*continued*)

Target type	Description
Oracle 10g and 11g Databases	All Oracle 10g and 11g databases.
Oracle 11g Databases	All Oracle 11g Databases
Oracle 9i, 10g, and 11g Databases	All Oracle 9i, 10g, and 11g databases.
Oracle Databases	All Oracle databases.
Oracle Unix Databases	All Oracle databases on UNIX operating system.
Oracle Windows Databases	All Oracle databases on Windows operating system.
Oracle Windows Servers	All Oracle Servers with Windows operating system.
Oracle Servers	All Oracle Servers.
Oracle Unix Servers	All Oracle Servers with UNIX operating system.

See [“About target types”](#) on page 455.

About ESM predefined target types

Table 10-6 Supported ESM target types

Target type	Description
All ESM Agent Machines	All ESM agents running on any operating system
All UNIX ESM Agent Machines	All ESM agents running on any UNIX operating system
Sun Solaris 10 ESM Agent Machines	All ESM agents running on Solaris 10 operating system
Windows 2003 ESM Agent Machines	All ESM agents running on Windows 2003 operating system
Windows XP ESM Agent Machines	All ESM agents running on Windows XP operating system
Windows Vista ESM Agent Machines	All ESM agents running on Windows Vista operating system

Table 10-6 Supported ESM target types (*continued*)

Target type	Description
Windows 2008 ESM Agent Machines	All ESM agents running on Windows 2008 operating system
AS/400 ESM Agent Machines	All ESM agents running on AS/400 operating system
All Windows ESM Agent Machines	All ESM agents running on any Windows operating system
All Windows 2000 ESM Agent Machines	All ESM agents running on Windows 2000 operating system
OpenVMS ESM Agent Machines	All ESM agents running on OpenVMS operating system

Note: To create customized checks for ESM application modules, such as DB2 or SQL Server, you must use the underlying OS platform target type.

About compliance score

The compliance score is a percentage value between 0 and 100 that represents the level of adherence to a standard. This score is derived from the checks that are present in a standard.

The checks in the Not Applicable status are not considered when you calculate the compliance score.

The compliance score is available when you evaluate an asset against one or more standard. The result of the evaluation process provides the compliance and the risk score.

See [“Working with Evaluation Results”](#) on page 541.

See [“About risk score”](#) on page 463.

About risk score

In Control Compliance Suite, a risk score is used to quantify the risk that is associated with an asset in your organization.

The risk score is calculated on the basis of the CIA values for an asset and the risk attributes of a check. You should give due consideration before you specify these values in the product.

You can specify the asset CIA values through the assets details pane or with the pre rules in the asset view.

See [“Using a Pre rule to set the values of the common fields”](#) on page 256.

You can specify the check risk attributes through the checks details pane or at the time of check creation.

See [“Specifying or editing the check attributes”](#) on page 534.

The risk calculations are based on the Common Vulnerabilities Scoring System version 2.

See [“About risk score calculation”](#) on page 545.

About gold standard

You may have an asset in your enterprise that is set up exactly as per the security guidelines or policies of your organization. You may want to create a standard that is based on the values of this reference asset.

Control Compliance Suite partially automates this process of creating a standard from values of a reference asset and hence saves you valuable time. Such a standard that is built from the values present in a reference asset is known as a gold standard.

For example, consider that you have a computer in your network that is configured in accordance with the security practices adopted by the organization. You want the values of this computer to act as a benchmark for the other computers in the enterprise. Then Control Compliance Suite can create a gold standard for you by replacing the expression values in a reference standard with data from the reference computer.

Assume that a check in a reference standard has the following expression:

Min password length = 8

The reference asset has the minimum password length as 10.

The resulting gold standard check has the following expression:

Min password length = 10

Control Compliance Suite may not be able to replace the expression values in a reference standard if the data is ambiguous or the check is complex.

See [“Resolving checks in a gold standard”](#) on page 538.

See [“Gold standard concepts”](#) on page 536.

See [“Creating a gold standard”](#) on page 537.

About versioning scheme

Each standard, section, and check follows a versioning scheme. The version consists of three numerical values that are separated by a period.

The components of the versioning scheme are explained as follows:

Major version	<p>The first digit in the versioning scheme represents the major version.</p> <p>This value tells us the schema version of the specific check, section, or standard xml. The schema may need to be changed to support a new feature. In such cases, only the major version number changes.</p>
Minor version	<p>The second digit in the versioning scheme represents the minor version.</p> <p>This version changes when a standard, section, or check is modified, for example, added, deleted, moved, or copied. But this version does not change if the standard, section, or check is modified for fixing a bug.</p>
Fix version	<p>The third digit in the versioning scheme represents the fix version. This version changes when the standard, section, or check is modified with respect to its description, expression, the CIA values or any other property.</p>

Following is the syntax for a version number:

(Major Version).(Minor Version).(Fix Version)

The change in version number is propagated to the top in the hierarchy. If a check is added to a section, the minor version of the parent section and the parent standard is incremented. If the version of a child section is incremented, then the respective version of the parent section is also incremented. This process helps in identifying precisely what has changed in a standard.

The following table lists the effect on the version number of actions such as creating, modifying, and deleting:

Create a check	The minor version of the parent section and the parent standard changes.
Modify a check	If a check is modified , then the fix version of the check, the parent section and the parent standard changes.
Delete a check	The minor version of the parent section and the parent standard changes.
Create a section	The minor version of the parent section (if any) and the parent standard changes.
Modify a section	If a section is modified , then the fix version of the section, the parent section, and the parent standard changes.

Delete a section The minor version of the parent section (if any) and the parent standard changes.

See “[About sections](#)” on page 453.

See “[About checks](#)” on page 453.

See “[About standards](#)” on page 448.

About the standards filters

The Filter by pane in the Standards view contains the filters that you can use to display only the required standards.

The Control Compliance Suite provides the following default filters for filtering the standards, sections, and checks:

Target Platform	Lets you filter the standards according to the specified target type.
Author	Lets you filter the standards according to the specified author name.
Compliance Score	Lets you filter the standards according to the specified range of compliance score.
Evaluated Between	Lets you filter the standards according to the specified range of evaluation dates. The last evaluation date is considered for filtering the standards.
Select tags	Lets you filter the standards according to the specified tags. You can browse to add the tags in the Tags list. You can select either of the following options: <ul style="list-style-type: none">■ Match Any. Select the Match Any option to display the standards that match any one of the listed tags.■ Match All. Select the Match All option to display the standards that match all the listed tags.

See “[About the Filter by pane](#)” on page 49.

See “[Customizing the filter options](#)” on page 56.

See “[Using filters in the Filter by pane](#)” on page 56.

About policy mapping in ESM

The check expressions in a standard are mapped with the policies in Enterprise Security Manager. When you execute a data collection job for a standard on ESM assets, the ESM data collector collects messages for the corresponding ESM policy from the ESM manager. Each check expression within a section of a CCS standard is mapped to an ESM policy.

If you create a custom standard, then you must change the name of the ESM policy that corresponds to the CCS standard.

See [“About CCS ESM policy run configurations ”](#) on page 124.

About changing an ESM policy name

Every check in the CCS standard is linked to an ESM policy. You can rename an existing ESM policy name for some checks in an ESM standard from the CCS console. You can change the ESM policy name for a whole standard, a section, or a check level.

Note: You cannot rename the pre-defined ESM policies.

See [“Changing an ESM policy name at the standard level”](#) on page 503.

See [“ Changing an ESM policy name at the section level ”](#) on page 508.

See [“ Changing an ESM policy name at the check level ”](#) on page 521.

Concepts in checks

Before you begin to perform the checks-related operations, you should familiarize yourself with the following concepts in checks:

- Field expression
See [“Field expression”](#) on page 468.
- Check expression
See [“Check expression”](#) on page 469.
- Preconditions
See [“Preconditions”](#) on page 470.
- Check formula
See [“Check formula”](#) on page 469.
- Data Items filter
See [“Data Items filter ”](#) on page 470.

- Missing data items
See “Missing data items” on page 471.
- Multiple data items
See “Multiple data items” on page 471.
- Check risk attributes
See “Check risk attributes” on page 472.

Field expression

In a field expression, an operator is used to compare a field with a particular value that a user specifies.

A field expression is composed of the following:

- Field
Name of the field whose value you want to compare.
- Value
The value against which you want to compare a specified field. This value is also known as a field value.
- Operator
The operator specifies the action that must be performed. For example, if you want to obtain a field A that has the exact value of 100, you must use the equal (=) operator. Every field value has a defined set of operators. You can only select an operator from the range of operators that are defined for the selected field value.
See “Field expression operators” on page 479.

The syntax for a field expression is as follows:

<Field><Operator><Value>

The following table lists some examples of a field expression:

Table 10-7 Examples of field expressions

Field	Operator	Value	Field expression
Domain Name	=	SOUTH REGION	Domain Name=SOUTH REGION
Auditing Enabled	!=	Yes	Auditing Enabled!=Yes

See “About checks” on page 453.

See “Concepts in checks” on page 467.

See [“Check expression”](#) on page 469.

See [“Creating a new check”](#) on page 517.

See [“Check Advanced Settings”](#) on page 475.

Check expression

A check expression compares a property of an asset against a data value that a user specifies. The result of the comparison is a pass, a fail, or an unknown value.

A check expression is composed of the following:

- Field expression (mandatory)
See [“Field expression”](#) on page 468.
- Data Items filter (optional)
See [“Data Items filter ”](#) on page 470.

See [“About checks”](#) on page 453.

See [“Concepts in checks”](#) on page 467.

See [“Creating a new check”](#) on page 517.

Check formula

A check formula is created by using check expressions.

A check formula is composed of either of the following:

- A single check expression
See [“Check expression”](#) on page 469.
- Multiple check expressions that are connected by the use of check formula operators.
See [“Check formula operators”](#) on page 481.

When a check formula is composed of only one check expression, then the check formula and the check expression are the same. Hence, their outcome is the same.

See [“About checks”](#) on page 453.

See [“Concepts in checks”](#) on page 467.

See [“Check Advanced Settings”](#) on page 475.

See [“Creating a new check”](#) on page 517.

Preconditions

A precondition is a logical condition that must be met before a check can be evaluated against the target asset.

In Control Compliance Suite, a check consists of a precondition and the actual check formula. If the check has a precondition, then the precondition is evaluated before the execution of check formula. If the precondition is not met then the check formula is not evaluated and the check outcome is set to Not Applicable.

The common use of a precondition is to verify some condition on the target asset before the assessment of the asset for compliance.

For example, consider the check: Is directory 'XYZ' owned by 'PQR' and has group set to 'ABC'? You may want to first verify if the specified directory 'XYZ' exists on the target computer before checking for the ownership. In this case, the precondition would be a verification of the fact whether the directory 'XYZ' exists.

See [“About checks”](#) on page 453.

See [“Concepts in checks”](#) on page 467.

See [“Creating a new check”](#) on page 517.

Data Items filter

A data items filter lets you filter the data against which the field expression is evaluated in a check.

A data items filter is composed of one or more filter statement. Each filter statement is a field expression.

See [“Field expression”](#) on page 468.

You can specify a data items filter in the Advanced Settings dialog box when you create or edit a check.

See [“Check Advanced Settings”](#) on page 475.

If you specify multiple filter statements, then the final data for evaluation is determined by the following options:

- Return only the data that matches all of the filter statements.
The AND operator is applied on the result of each filter statement to determine the final data for evaluation purpose.
- Return only the data that matches any one of the filter statements.
The OR operator is applied on the result of each data item to determine the final data for evaluation purpose.

See [“About checks”](#) on page 453.

See [“Concepts in checks”](#) on page 467.

See [“Creating a new check”](#) on page 517.

Missing data items

Data items are termed as 'missing' in the following situations:

- No value for the field is present.
- Application of an evaluation condition filter returns no data values.

You must specify the outcome for missing data in the evaluation results. You can set this value when you create a check in the Advanced Settings dialog box of the Create Check wizard. You can also modify the Missing Data Outcome value after the check is created.

See [“Check Advanced Settings”](#) on page 475.

You can set the following values as the outcome for missing data items:

- Pass
- Fail
- Unknown

The default value for a missing data outcome is Unknown.

See [“About checks”](#) on page 453.

See [“Concepts in checks”](#) on page 467.

See [“Creating a new check”](#) on page 517.

Multiple data items

An evaluation condition consists of a field expression. When you specify an evaluation condition, all data items of the specified field are matched against the condition.

The result of each tested data item is one of the following:

- Pass
- Fail
- Unknown

To calculate the final result for all the tested data items, you must specify the action to take for multiple data items. You can specify this action in the Advanced Settings dialog box of the Create Check wizard.

See [“Check Advanced Settings”](#) on page 475.

In the Advanced Settings dialog box, you can select either of the following options to specify the action for multiple data items:

- All must meet the evaluation condition
The AND operator is applied on the individual results of each data item.
- At least one must meet the evaluation condition
The OR operator is applied on the individual results of each data item.

See [“Operators AND and OR”](#) on page 481.

See [“About checks”](#) on page 453.

See [“Concepts in checks”](#) on page 467.

See [“Creating a new check”](#) on page 517.

Check risk attributes

The attributes of a check that are used to calculate the risk are known as the risk attributes.

A check has the following risk attributes:

- Confidentiality Impact
This attribute measures the impact to confidentiality if a specified check fails. Confidentiality is the act of limiting the access and disclosure of information to only authorized users. The impact of unauthorized disclosure of confidential information can lead to security risk, loss of public confidence, or legal action against the organization.

You can assign the following values to this attribute:

No Impact	No impact to the confidentiality of the system. The corresponding weight that is assigned to this value is 0.0.
Partial	Considerable information disclosure has occurred. Access to some system files is possible but the attacker does not have control over the data that is obtained. The scope of the loss is constrained. The corresponding weight that is assigned to this value is 0.275.
Complete	Total information disclosure has occurred. All the system files are revealed. The attacker has access to all the system data. The corresponding weight that is assigned to this value is 0.66.

■ Integrity Impact

This attribute measures the impact to integrity if a specified check fails.

Integrity refers to the genuineness of the information. Integrity dictates that information must be protected from improper modification. Integrity is lost if unauthorized changes are made to the data by either intentional or accidental acts. Continuous use of corrupted data can result in inaccuracy, fraud, or erroneous decisions.

You can assign the following values to this attribute:

No Impact	No impact to the integrity of the system. The corresponding weight that is assigned to this value is 0.0.
Partial	Modification of some information has occurred but the attacker does not have control over what can be modified. Modification scope is limited. The corresponding weight that is assigned to this value is 0.275.
Complete	Total compromise of system integrity has occurred. The attacker is able to modify any files on the target system. The corresponding weight that is assigned to this value is 0.66.

■ Availability Impact

This attribute measures the impact to availability if a specified check fails.

Availability refers to the accessibility of information resources. Attacks that consume network bandwidth, processor cycles, or disk space affect the availability of a system. If a mission-critical asset is unavailable to its end users, the mission of the organization may be affected.

You can assign the following values to this attribute:

No Impact	No impact to the availability of the system. The corresponding weight that is assigned to this value is 0.0.
Partial	Reduced performance or interruptions in availability of information. The corresponding weight that is assigned to this value is 0.275.

Complete	Total shut down of the affected resource. The attacker can render the resource completely unavailable. The corresponding weight that is assigned to this value is 0.66.
----------	--

- Access Vector
This attribute reflects how vulnerability is exploited in a system.
According to the type of access that is required for the attacker to exploit the vulnerability, this attribute can be assigned the following values:

Local Accessible	The attacker has either physical access to the vulnerable system or a local (shell) account. The corresponding weight that is assigned to this value is 0.395.
Adjacent Network Accessible	The attacker has access to either the broadcast or the collision domain of the vulnerable software. The corresponding weight that is assigned to this value is 0.646.
Network Accessible	The vulnerable software is bound to the network stack and the attacker does not require local network access or local access. The corresponding weight that is assigned to this value is 1.0.

- Access Complexity
This attribute measures the complexity of the attack that is required to exploit the vulnerability in a system.
The possible values for this attribute are as follows:

Low	Specialized access conditions do not exist. The corresponding weight that is assigned to this value is 0.71
Medium	The access conditions are specialized to a limited degree. The corresponding weight that is assigned to this value is 0.61.

High

Specialized access conditions exist.

The corresponding weight that is assigned to this value is 0.35.

- Authentication
- This attribute measures the number of times an attacker must authenticate to a target for exploiting the vulnerability. This attribute does not measure the strength or complexity of the authentication process. Authentication gauges only the fact whether an attacker is required to provide credentials before the exploration of the vulnerability.
- The possible values for this attribute are as follows:

Multiple Instances	<div>The attacker is required to authenticate two or more times to exploit the vulnerability. The same credentials may be used each time.</div> <div>The corresponding weight that is assigned to this value is 0.45</div>
Single Instance	<div>The attacker needs to log into the system such as at a command line or through a desktop session or Web interface.</div> <div>The corresponding weight that is assigned to this value is 0.56.</div>
No Authentication	<div>Authentication is not required to exploit the vulnerability.</div> <div>The corresponding weight that is assigned to this value is 0.704</div>

See “[About checks](#)” on page 453.

See “[About risk score calculation](#)” on page 545.

Check Advanced Settings

The check fundamentals such as evaluation condition, data items filters, and multiple data items are important concepts to understand the process of creating a check. You can set these values in the Advanced Settings dialog box when you create a check.

For example, assume a table exists in the database with the name EXAMPLE. You can treat t his table equivalent to a category in an evaluation condition.

[Table 10-8](#) contains the following fields and values:

Table 10-8 EXAMPLE

A	B	C	D
9	X	P	50
10	Y	Q	60
11	Z	R	70

CASE I: The following evaluation condition is set and no filter is applied on the evaluation condition:

Evaluation Condition	In the table EXAMPLE, the value of the field A should be greater than 9.
Equivalent field expression for the evaluation condition	A > 9
Data items filter	--

For the field A, three data values (9, 10, and 11) are present in the table. Each data value is tested against the specified evaluation condition and the following results are obtained:

A = 9	Result = FAIL
A = 10	Result = PASS
A = 11	Result = PASS

To calculate the final result for the tested data, you must specify the action that should be taken for multiple data items.

You can select either of the following options to specify the action for multiple data items:

- All must meet the evaluation condition.
The AND operator is applied on the individual results of each data item.
- At least one must meet the evaluation condition.
The OR operator is applied on the individual results of each data item.

If the AND operator is applied for the sample check, then the final result is as follows:

Final test result	FAIL
(Applying the All must meet the evaluation condition option)	(FAIL AND PASS AND PASS)

CASE II: The same evaluation condition is set and a data items filter that consist of a single filter statement is applied:

Evaluation Condition	In the table EXAMPLE, the value of the field A should be greater than 9.
Equivalent field expression for the evaluation condition	$A > 9$
Evaluation condition filter	$D > 50$

On applying the filter statement, only those values of the field A are tested that match the filter statement. In the example, now only the values 10 and 11 are checked against the evaluation condition.

The individual results for the tested data values are as follows:

A = 10	Result = PASS
A = 11	Result = PASS

If you now specify the action for multiple data items as "All must meet the evaluation condition", then the final result is as follows:

Final test result	PASS
(Applying the All must meet the evaluation condition option)	(PASS AND PASS)

CASE III: The same evaluation condition is set and two filter statements are specified in the data items filter as follows:

Evaluation Condition	In the table EXAMPLE, the value of the field A should be greater than 9.
Equivalent field expression for the evaluation condition	$A > 9$
Filter statement 1	$D > 50$
Filter statement 2	$C = P$

In the CASE III, the following values are returned on applying each filter statement:

D > 50	The following values are returned: A = 10 A = 11
C = P	The following values are returned: A = 9

When you apply more than one filter statement on the evaluation condition, you must specify the behavior for multiple filter statements. This behavior is used to determine the data items that would be considered for evaluation purpose.

You can select either of the following options to specify the behavior for multiple filter statements:

- Return only the data that matches all of the filter statements.
The AND operator is applied on each data item.
- Return only the data that matches any one of the filter statements.
The OR operator is applied on each data item.

If you consider only the data items that match any one of the filter statements, then the final data values are obtained as follows:

Applying OR operator as follows: (A = 10) OR (A = 11) OR (A = 9)	All the three data values are available for testing. A=9 A=10 A=11
---	---

You can then proceed to test each data item against the evaluation condition.

See [“About checks”](#) on page 453.

See [“Concepts in checks”](#) on page 467.

See [“Creating a new check”](#) on page 517.

About operators

An operator is used to indicate an action that is performed on one or more elements. An operator can be a symbol or a word that signifies a particular action.

In the Standards module, the following operators are used:

- Field expression operators

See “Field expression operators” on page 479.

- Check formula operators
- See “Check formula operators” on page 481.

Field expression operators

The operators that are allowed in a field expression are known as the field expression operators. These operators are used to make a comparison between two given values.

Table 10-9 lists the descriptions of the available field expression operators.

Table 10-9 Field expression operators

Operator	Operator Name	Expression using sample values A, B, and the operator	Description
=	The equality operator	A = B	A must be equal to B
!= or <>	The inequality operator	A!=B	A must not be equal to B
<	The less than operator	A < B	A must be less than B
<=	The less than or equal operator	A <= B	A must be less than or equal to B
>	The greater than operator	A > B	A must be greater than B
>=	The greater than or equal operator	A >= B	A must be greater than or equal to B
Like	The like operator	A Like B	The SQL like operator (same syntax and semantics).
Not Like	The not like operator	A Not Like B	The SQL not like operator. Note the space between not and like. Any amount of white space (blanks, tabs, new lines, or carriage returns) is allowed here. The white space is not strictly required, but it is best not to omit it.
=~	The match operator	A=~B	The regular expression matching operator.

Table 10-9 Field expression operators (*continued*)

Operator	Operator Name	Expression using sample values A, B, and the operator	Description
!~	The no match operator.	A!~B	The negative of the expression matching operator.
is null	The is null operator	A is null	The SQL is null operator. A field expression employing this operator must not have a value specified. At least one white-space character is required between is and null.
is not null	The is not null operator	A is not null	The negative of is null. The white space between not and null is not strictly required, but it is best not to omit it.
Exact	The exact operator		Forces case-sensitive string comparison.
Inexact	The inexact operator		Forces case-insensitive string comparison.
%	Contains operator	A%B	In case of a single valued field, value on RHS has to be partially or completely matching with LHS. In case of a multi valued field, every value on RHS has to be present on the LHS.
!%	The Not Contains operator	A!%B	The negative of the Contains operator.
%~	The Contains Match operator	A%~B	In case of a single valued field, the regular expression on RHS should match field value on LHS. In case of a multi valued field, every regular expression on RHS should match at least one element on LHS.
!%~	The Not Contains Match operator	A!%~B	The negative of the Contains Match operator.

See [“About operators”](#) on page 478.

Check formula operators

The operators that are allowed to be used in a check formula are known as the check formula operators.

The check formula operators are as follows:

- AND
- OR
- NOT
- IF
- THEN
- ELSE

See [“Operators AND and OR”](#) on page 481.

See [“Operator NOT”](#) on page 482.

See [“Operators IF, THEN, ELSE”](#) on page 482.

When you create a check, you can specify the operators in the Create Expression(s) panel of the Create Check wizard. By default, the AND operator is used to connect two or more expressions. You can specify the operators in the Formula box by either typing or selecting the displayed operators.

See [“About operators”](#) on page 478.

See [“Concepts in checks”](#) on page 467.

Operators AND and OR

The AND and OR operators are used to connect two or more check expressions in a check formula.

[Table 10-10](#) defines the outcome of the check formula when AND and OR operators are used to define logical combinations of check expressions. In the table, A and B represent check expressions.

Table 10-10 Use of AND and OR operators

If A equals	If B equals	Then A AND B equals	Then A OR B equals
PASS	PASS	PASS	PASS
PASS	FAIL	FAIL	PASS

Table 10-10 Use of AND and OR operators (continued)

If A equals	If B equals	Then A AND B equals	Then A OR B equals
PASS	MANUAL REVIEW	MANUAL REVIEW	PASS
FAIL	PASS	FAIL	PASS
FAIL	FAIL	FAIL	FAIL
FAIL	MANUAL REVIEW	FAIL	MANUAL REVIEW
MANUAL REVIEW	PASS	MANUAL REVIEW	MANUAL REVIEW
MANUAL REVIEW	FAIL	FAIL	MANUAL REVIEW
MANUAL REVIEW	MANUAL REVIEW	MANUAL REVIEW	MANUAL REVIEW

See “[Check formula operators](#)” on page 481.

See “[About operators](#)” on page 478.

Operator NOT

The NOT operator can be used in a check formula.

[Table 10-11](#) defines the outcome of the check formula when the NOT operator is used to define logical combinations of check expressions. In the table, A represents a check expression.

Table 10-11 Usage of NOT operator

If A equals	Then NOT A equals
PASS	FAIL
FAIL	PASS
MANUAL REVIEW	MANUAL REVIEW

See “[Check formula operators](#)” on page 481.

See “[About operators](#)” on page 478.

Operators IF, THEN, ELSE

An IF, THEN, ELSE operator is defined as follows:

If (condition)

Then (true expression)

Else (false expression)

The value is obtained in the following way when you use this operator:

- The value is unknown if the condition evaluates to unknown.
- The value is true if the condition evaluates to true.
- The value is false if the condition evaluates to false.

See [“Check formula operators”](#) on page 481.

See [“About operators”](#) on page 478.

About the Standards view

The Standards view lets you manage the standards, sections, and checks in the Control Compliance Suite.

You can access the standards management view from Manage > Standards.

The Standards view contains the following panes:

Tree pane	<p>The tree pane appears on the left side of the console window under the navigation bar.</p> <p>The pane displays a hierarchical, folder-based structure of the standards that are stored in the CCS directory.</p>
Filter by pane	<p>The Filter by pane appears in the lower left side of the console window under the tree pane.</p> <p>You can specify filters in this pane so that only the required standards, sections, and checks are displayed in the table pane.</p> <p>You can use the following filters in the standards view:</p> <ul style="list-style-type: none">■ Target Platform■ Author■ Compliance Score■ Evaluated Between■ Select Tags
Table pane	<p>The table pane appears in the right side of the console window under the taskbar .</p> <p>This pane displays the standards, sections, and checks.</p>

Details pane

The details pane appears in the lower-right side of the console window under the table pane.

This pane displays the details of the standard, section, or check that is selected in the details pane.

The taskbar of the Standards view is divided into the following major tasks:

Standard Tasks

- Create Standard
See [“Creating a new standard”](#) on page 491.
- Import Standard
See [“Importing a standard”](#) on page 493.
- Export Standard
See [“Exporting a standard”](#) on page 494.
- Create Check
See [“Creating a new check”](#) on page 517.
- Create Section
See [“Creating a new section”](#) on page 505.

Gold Standard Tasks

- Create Gold Standard
See [“Creating a gold standard”](#) on page 537.
- Manual Review
See [“Resolving checks in a gold standard”](#) on page 538.

Evaluation Tasks

ESM Tasks

Change ESM Policy Name

See [“Changing an ESM policy name at the standard level”](#) on page 503.

Common Tasks

- Move
 - See [“Moving a standard”](#) on page 493.
 - See [“Moving a section”](#) on page 507.
 - See [“Moving a check”](#) on page 515.
- Delete
 - See [“Deleting a standard”](#) on page 495.
 - See [“Deleting a section”](#) on page 507.
 - See [“Deleting a check”](#) on page 516.
- Request Exception
 - See [“Requesting an exception”](#) on page 436.
 - See [“Launching the Request Exception Wizard”](#) on page 440.

See [“About the standards filters”](#) on page 466.

See [“Working with standards”](#) on page 486.

See [“Working with sections”](#) on page 503.

See [“Working with checks”](#) on page 508.

See [“Viewing standard information in the details pane”](#) on page 486.

About the standard migration utility for ESM and CCS

Symantec has developed independent utilities to migrate the following to CCS 9.0.1 or later format:

- Customized ESM policies
- Customized CCS 8.60 standards

Both the utilities use command-line functionality to migrate the policies or standards. Once you migrate the policies or standards to CCS 9.0.1 or later format, you can import them into CCS 9.0.1 or later.

For more information on how to use the utilities, see the guide available with the utility.

For 9.0.1 or later release, the web package of the utilities is available along with the web package of CCS 9.0.1 or later . The web package of CCS 9.0.1 or later is available on the Platinum site.

To gain access to the latest utilities, contact Technical Support for assistance.

Working with standards

You can perform the following tasks on standards:

- View standard information in the details pane
See [“Viewing standard information in the details pane”](#) on page 486.
- Create a new standard.
See [“Creating a new standard”](#) on page 491.
- Copy and paste a standard.
See [“Copying and pasting a standard”](#) on page 492.
- Move a standard.
See [“Moving a standard”](#) on page 493.
- Import a standard.
See [“Importing a standard”](#) on page 493.
- Export a standard.
See [“Exporting a standard”](#) on page 494.
- Rename a standard.
See [“Renaming a standard”](#) on page 494.
- Delete a standard.
See [“Deleting a standard”](#) on page 495.
- Evaluate an asset against a standard.
See [“Running an evaluation job from the Standards view”](#) on page 495.
- Create a chained job
See [“Running a collection-evaluation-reporting job from the Standards view”](#) on page 499.

Viewing standard information in the details pane

You can view the information about a standard through the details pane in the standards view.

To view the standards information

- 1 Go to Manage > Standards.
- 2 In the table pane of the Standards view, select the standard for which you want to display the information.
- 3 View the information for the selected standard in the details pane.

The standards details are contained in the following tabs:

- General
See “[Standard details pane - General tab](#)” on page 487.
- Description
See “[Standard details pane - Description tab](#)” on page 488.
- Evaluations
See “[Standard details pane - Evaluations tab](#)” on page 488.
- References
See “[Standard details pane - References tab](#)” on page 489.
- Exceptions
See “[Standard details pane - Exceptions tab](#)” on page 489.
- Tags
See “[Standard details pane - Tags tab](#)” on page 489.
- Gold Standard Properties
This tab is present only for a gold standard.
See “[Standard details pane - Gold Standard Properties tab](#)” on page 490.

See “[About the details pane](#)” on page 50.

Standard details pane - General tab

The General tab of the Standards details pane provides general information about the selected standard.

The General tab contains the following information:

Standard Name	The name of the standard. This value is editable. See “ Renaming a standard ” on page 494.
Target Type(s)	This list reflects the target type of all the checks that are present within the standard. See “ About target types ” on page 455.
Version	The current version of the standard. See “ About versioning scheme ” on page 465.
Author	For a predefined standard, the value of Author is Symantec. For a user-defined standard, this value refers to the user who created the standard.
Creation Date	The date and time of creation of the standard.
Last Updated	The date and time when the standard was last updated.

Number of Checks	The total number of checks in the standard.
Last Evaluation	The date and time when the standard was last evaluated.
#Assets Evaluated	The number of assets against which the standard was evaluated.
Compliance Score	The Compliance score of the standard. See “About compliance score” on page 463.
Risk Score	The risk score of the standard. See “About risk score” on page 463.

See [“About the details pane”](#) on page 50.

See [“Viewing standard information in the details pane”](#) on page 486.

See [“Working in the details pane”](#) on page 531.

Standard details pane - Description tab

The Description tab of the Standard details pane lets you describe the standard.

The Description tab has the following views:

- Read only
This view lets you only read the standard description.
- Edit
This view lets you make changes to the standard description.

See [“About the details pane”](#) on page 50.

See [“Viewing standard information in the details pane”](#) on page 486.

See [“Working in the details pane”](#) on page 531.

Standard details pane - Evaluations tab

The evaluations tab of the standard details pane provides the history of the last ten evaluation results for the standard.

The evaluations tab contains the following information:

Evaluation Date	Specifies the date and time at which the evaluation job was run.
Evaluated against	The name of all the assets against which the standard was evaluated. A comma (,) is used to separate the assets.
Compliance (%)	The compliance value in percentage for all the assets against which the standard was evaluated.

Risk score	The risk score of the asset.
------------	------------------------------

Standard details pane - References tab

The References tab lists the hyperlinks that lead to additional information about the standard.

The References tab contains the following information:

Name	The reference name
URL	The hyperlink for locating the reference information

You can perform the following tasks using the References tab:

- Add reference information
See [“Adding reference information”](#) on page 535.
 - Edit reference information
See [“Editing reference information”](#) on page 535.
 - Delete reference information
See [“Deleting reference information”](#) on page 536.
- See [“Viewing section information in the details pane”](#) on page 503.
- See [“About the details pane”](#) on page 50.
- See [“Working in the details pane”](#) on page 531.

Standard details pane - Tags tab

The Tags tab contains the list of all the tags that are associated with the selected standard.

The Tags tab lets you add a new tag to associate with the selected standard. You can also remove a tag that is already associated with the standard.

Standard details pane - Exceptions tab

The Exceptions tab lets you view the exception-related details of the checks within the standard.

The Exceptions tab contains the following information:

Title	The title that was specified at the time of creating the exception.
-------	---

Effective Date	The start date of the exception validity period. The exception becomes valid from this date.
Expiration Date	The last day of the exception validity period. The exception becomes invalid after this date.
Last Modified On	The date and time when the exception was modified the last time.

See [“About the details pane”](#) on page 50.

See [“Viewing standard information in the details pane”](#) on page 486.

See [“Working in the details pane”](#) on page 531.

Standard details pane - Gold Standard Properties tab

The Gold Standard Properties tab is available only for a gold standard. This tab lets you view the information regarding the gold standard.

The Gold Standard Properties tab contains the following information:

Reference Asset	The name of the reference asset.
Reference Standard	The name of the reference standard.
Reference Standard Version	The version of the reference standard.
Number of Unresolved Checks	The number of checks that are unresolved in the gold standard.
Last Synchronization Job Completion Date	The date and time at which the synchronization job was last completed.

See [“About the details pane”](#) on page 50.

See [“Viewing standard information in the details pane”](#) on page 486.

See [“Working in the details pane”](#) on page 531.

See [“About gold standard”](#) on page 464.

See [“Gold standard concepts”](#) on page 536.

See [“Creating a gold standard”](#) on page 537.

About multi-select functionality

You can select more than one standard, section, or check at a time to perform the common tasks.

The following tasks can be performed when you select multiple standards:

- Move
- Copy
- Delete
- Request exception
- Evaluate
- Set up a data collection job
- Set up collection-evaluation-reporting job

The following tasks can be performed when you select multiple sections or only multiple checks:

- Move
- Copy
- Delete
- Request exception

The following tasks can be performed when you select standards, sections, or checks simultaneously:

- Delete
- Request exception

Creating a new standard

You can create a new standard in the Standards view.

To create a new standard

- 1 Go to Manage > Standards.
- 2 In the Standards view, in the tree pane, select the folder in which you want to create the new standard.
- 3 Do one of the following:
 - On the taskbar, select **Create Standard**.
 - On the Tasks menu, select **Create Standard**.

- In the table pane, right-click on an empty grid and select **Create Standard**.
- 4 In the Create Standard dialog box, in the Name box, type the name of the new standard.
- 5 In the Description box, enter the description information.
- 6 Click **OK**.

After you click OK, the Edit Standard dialog box is displayed. This dialog box lets you create a new section or a new check within the recently created standard. You can choose to close the dialog box and create a section or a check later.

Copying and pasting a standard

You can copy the predefined and the user-defined standards. You can copy multiple standards at a time to any folder except the predefined folder.

To copy and paste a standard using the context menu

- 1 Go to Manage > Standards.
- 2 In the table pane of the Standards view, right-click the standard that you want to copy and select **Copy**.
- 3 In the tree view, select the folder where you want to locate the copied standard. In the table pane, right-click in the empty space in the grid and select **Paste**.

You can paste a standard only within a folder. The paste option is disabled when you try to paste a standard within a section, or a check.

After you paste a standard, a Progress Status bar is displayed. This bar shows the progress of the paste operation. A message appears when the paste operation is successful.

To copy and paste a standard using the menu bar

- 1 Go to Manage > Standards.
- 2 In the table pane of the Standards view, select the standard that you want to copy and on the menu bar, click **Edit** and then **Copy**.
- 3 Place the cursor where you want to place the copied standard. On the menu bar, click **Edit** and then **paste**.

Moving a standard

You can move the user-defined standards to any location except the predefined folder. The predefined standards cannot be moved.

To move a standard

- 1 Go to Manage > Standards.
- 2 In the table pane of the Standards view, do either of the following:
 - Right-click the standard that you want to move and select **Move**.
 - Select the standard that you want to move and on the taskbar, click **Common Tasks > Move**.
 - Select the standard that you want to move and on the Tasks menu, select **Move**.
- 3 In the Move Standard - Manage dialog box, select the destination folder to which you want to move the standard. Click **OK**.

See [“About multi-select functionality”](#) on page 491.

See [“Working with standards”](#) on page 486.

Importing a standard

You can import a standard that is compliant with the Control Compliance Suite. You can import the standard to any folder except the predefined container.

Note: When a standard is imported, the version of the standard is taken into consideration. Therefore, changing the name of the standard in the XML does not lead to creation of a new standard.

To import a standard

- 1 Go to Manage > Standards.
- 2 In the tree pane of the Standards view, select the folder to which you want to import the standard.
- 3 Do either of the following:
 - On the Tasks menu, select **Import Standard**.
 - On the taskbar, click **Import Standard**.

- 4 In the Import Standard dialog box, in the File Path box, type or browse to the standard file that you want to import.

The Container Folder displays the folder to which the standard is to be imported.

- 5 Click **OK**.

See [“Working with standards”](#) on page 486.

Exporting a standard

You can export a standard to a file system that is located outside the Control Compliance Suite. Exporting a standard can assist you in creating a backup of the standard. You cannot export a section or a check.

To export a standard

- 1 Go to Manage > Standards.
- 2 In the table pane of the Standards view, do one of the following:
 - Select the standard that you want to export and on the Tasks menu, select **Export Standard**.
 - Select the standard that you want to export and on the taskbar, click **Standard Tasks > Export Standard**.
 - Right-click the standard that you want to export and select **Export Standard**.
- 3 In the Export Standard - Manage dialog box, enter the name of the file that you want to export and the folder path.
- 4 Click **OK**.

See [“Working with standards”](#) on page 486.

Renaming a standard

You can change the standard name through the General tab of the details pane.

To rename a standard

- 1 Go to Manage > Standards.
- 2 In the table pane of the Standards view, select the standard that you want to rename.
- 3 In the details pane, on the General tab, type the new name in the Standard Name text box.
- 4 Click the save icon.

See [“Working with standards”](#) on page 486.

Deleting a standard

You can delete only the user-defined standards. The predefined standards cannot be deleted.

To delete a standard

- 1 Go to Manage > Standards.
- 2 In the table pane of the Standards view, do either of the following:
 - Right-click the standard that you want to delete and select **Delete**.
 - Select the standard that you want to delete and on the Tasks menu, click **Common Tasks > Delete**.
 - Select the standard that you want to delete and on the taskbar, click **Delete**.
- 3 In the Manage Standards box, select **Yes** to delete the selected standard.

See [“About multi-select functionality”](#) on page 491.

See [“Working with standards”](#) on page 486.

Running an evaluation job from the Standards view

You can evaluate the assets in your organizations against specific standards. The Create or Edit Evaluation Job wizard lets you create or edit an evaluation job.

See [“About evaluation jobs”](#) on page 454.

To run an evaluation job

- 1 Go to Manage > Standards.
- 2 In the Standards view, do one of the following:
 - Right-click the standard that you want to evaluate and select **Run Evaluation**.
 - Select the standard that you want to evaluate and on the taskbar, click **Run Evaluation**.
 - Select the standard that you want to evaluate and on the Tasks menu, select **Run Evaluation**.
- 3 In the Specify Job Name and Description panel, in the Job Name box, type a name for the evaluation job that you want to create.
- 4 In the Description box, type a description for the evaluation job and click **Next**.

- 5 In the Select Targets panel, in the tree pane, select a folder. You can further select from the displayed folder contents.

The selected assets are displayed in the Selected Items list.

- 6 After this step, you can configure automatic remediation.

If you do not want to configure remediation, you can skip the **Select Asset Types for Remediation** panel and click **Next** to reach the **Schedule Job** panel.

For a detailed procedure of configuring the automatic remediation visit the following link:

See [“To remediate the assets automatically”](#) on page 497.

- 7 In the Schedule Job panel, select any one of the following:

- If you want to run the evaluation job after the wizard closes, check **Run Now**.
- If you want to run the job at a specified interval, check **Run Periodically** and enter the following information.

In the Start On box, enter the start date and time to run the job.

Under the Run periodically options, if you want to run the job only one time, select **Run Once**. If you want to run the job after specific days, select the number of days in the Run every Day list box. Click **Next**.

You must set a password in the System Management > User Preferences > Data Collection Password. If you fail to set the password, a warning message appears when you schedule the job. You can click OK in the message box and specify the scheduling details. But you must set the password before the scheduled time for running the job.

- 8 In the **Add Result Viewers** panel, add the users or the groups that have the permissions to view the evaluation results and reports.

It is recommended to add the groups as the result viewers.

- 9 In the Specify Notification Details panel, enter the job completion notification details on the Job Success tab. Enter the job failure notification details on the Job Failure tab. Both the tabs on this panel contain the same options. Check **Send notification**, enter the following information and then click **Next**:

- Enter the subject and message of the notification mail.
 - Enter the sender and the receiver email ID.
- Notification can be sent to multiple recipients.

- 10 In the Summary panel, review the information that you have entered. Click **Back** to make any changes, else click **Next**.
- 11 Click **Finish** to exit the wizard.

To monitor the current status of the job, go to Monitor > Jobs.

To remediate the assets automatically

- 1 In the **Select Asset Type for Remediation Ticketing** panel, check the **Enable Automatic Remediation Ticketing** option to configure the automatic remediation details.

Select the asset types that correspond to the assets that were evaluated and click **Next**.

- 2 In the **Specify Remediation Ticketing Criteria** panel, specify the combination of risk score and compliance score that you want to use to identify the assets for remediation.

You can select **Apply to all standards** if you want to apply the specified remediation criteria to all the standards for remediation.

If you do not select **Apply to all standards**, you must specify the remediation ticketing criteria for each standard.

Click **Next**.

- 3 In the **Select Remediation Ticket Type** panel, select one of the following:

- Create an email notification.

This option lets you create an email notification that you want to send for notification.

- Create a service desk ticket.

This action opens a service desk ticket request directly at the end of the evaluation results for the non-compliant assets.

You can choose the **Enable closed-loop verification** option. With the closed-loop verification, the non-compliant assets data is re-evaluated after the service desk request is met.

See [“About closed-loop verification”](#) on page 552.

Click **Next**.

- 4 If you choose to send an email notification as a remediation action, specify the message that you want to send as an email notification in the **Configure Notification Details for Remediation Ticketing** panel. Click **Next**.

If you select **Consolidate multiple assets in a single ticket/email**, a single notification is sent that includes all the non-compliant assets.

You can check **Make this the default Email Notification template** if you want to use the same message for all the service desk ticket requests.

- 5 If you choose to create a service desk ticket as a remediation action, specify the message that you want to send as a service desk request in the **Configure Service Desk Ticket** panel. Click **Next**.

If you select **Consolidate multiple assets in a single ticket/email**, a single service desk ticket is generated that includes all the non-compliant assets.

You can check **Make this the default Service Desk Ticket template** if you want to use the same message for all the service desk ticket requests.

- 6 Proceed with the Create or Edit Evaluation Job Wizard till the Summary panel.

See [“Working with standards”](#) on page 486.

Setting up a data collection job from the Standards view

You can run a data collection job from the Standards view. You can use the New Data Collection Job wizard to create a job to start the process of collecting data for the specified standards.

To set up a data collection job

- 1 Go to Manage > Standards.
- 2 In the table pane, select the standard for which you want to run the data collection job. On the taskbar, click **Evaluation Tasks > Setup Data Collection**.
- 3 In the Create or Edit Data Collection Job wizard, in the Specify Job Name and Description panel, in the Name field, type the name of the data collection job.
- 4 In the Description box, type a description for the evaluation job and click **Next**.
- 5 In the Select Assets panel, navigate through the assets and select an asset for which you want to set up a data collection.
- 6 Click **Add** to add the asset to the data collection job and click **Next**.
- 7 In the **Schedule Job** panel, select any one of the following:
 - If you want to run the job after the wizard closes, check **Run Now**.

- If you want to run the job at a specified interval, check **Run Periodically** and enter the following information.
In the Start On box, enter the start date and time to run the job.
Under Run periodically options, if you want to run the job only one time, select **Run Once**. If you want to run the job after specific days, select the number of days in the Run every Day list box. Click **Next**.
- 8 In the Specify Notification Details panel, select **Send notification** and type the information for sending the notification and click **Next**.
- 9 In the Summary panel, review all the selections that you made and click **Finish**.

You can monitor the status of the job from the Monitor > Jobs view.

Running a collection-evaluation-reporting job from the Standards view

The collection-evaluation-reporting job lets you create a common job to schedule data collection, evaluation, and report generation. Control Compliance Suite provides different jobs for data collection, evaluation, and report generation tasks. In case of environments where thousands of such jobs are scheduled, a collection-evaluation-reporting job makes it easy to manage all the tasks from a single wizard.

See [“About evaluation jobs”](#) on page 454.

To run a collection-evaluation-reporting job

- 1 Go to **Manage > Standards**.
- 2 In the Standards view, do one of the following:
 - Right-click in the table pane and select **Run Collection-Evaluation-Reporting**.
 - Select the standard that you want to evaluate and on the taskbar, from the Evaluation Tasks, select **Run Collection-Evaluation-Reporting**.
- 3 In the Specify Job Name and Description panel, in the Job Name box, type a name for the evaluation job that you want to create.
- 4 In the Description box, type a description for the evaluation job and click **Next**.
- 5 In the Select Targets panel, navigate through the assets hierarchy, select the assets and click **Next**.

You can select an asset, asset group, or an asset folder to evaluate.

- 6 In the Select Standards panel, from the list of standards that appear in the left section, select the standard against which you want to evaluate the assets.

Click **Add** to add the selected standard and click **Next**.

Click **Add All** to add all the standards that appear in the right section and click **Next**.

- 7 In the **Select Report Templates** panel, select one or more report templates for the evaluation job report.

- 8 After this step, you can configure automatic remediation.

If you do not want to configure remediation, you can skip the **Select Asset Types for Remediation** panel and click **Next** to reach the **Schedule Job** panel.

For a detailed procedure of configuring the automatic remediation visit the following link:

See [“To remediate the assets automatically”](#) on page 501.

- 9 In the **Schedule Job** panel, select any one of the following:

- If you want to run the evaluation job after the wizard closes, check **Run Now**.
- If you want to run the job at a specified interval, check **Run Periodically** and enter the following information.

In the Start On box, enter the start date and time to run the job.

Under the Run periodically options, if you want to run the job only one time, select **Run Once**. If you want to run the job after specific days, select the number of days in the Run every Day list box. Click **Next**.

You must set a password in the **System Management > User Preferences > Data Collection Password**. If you fail to set the password, a warning message appears when you schedule the job. You can click **OK** in the message box and specify the scheduling details. But you must set the password before the scheduled time for running the job.

- 10 In the **Add Result Viewers** panel, add the users or the groups that have the permissions to view the evaluation results and reports.

It is recommended to add the groups as the result viewers.

- 11 In the Specify Notification Details panel, enter the job completion notification details on the Job Success tab. Enter the job failure notification details on the Job Failure tab. Both the tabs on this panel contain the same options. Check **Send notification**, enter the following information and then click **Next**:

- Enter the subject and message of the notification mail.
- Enter the sender and the receiver email ID.

Notification can be sent to multiple recipients.

The Create or Edit Collection-Evaluation-Reporting wizard also lets you configure the details to remediate the assets that are non-compliant.

To remediate the assets automatically

- 1 In the **Select Asset Type for Remediation Ticketing** panel, check the **Enable Automatic Remediation Ticketing** option to configure the automatic remediation details.

Select the asset types that correspond to the assets that were evaluated and click **Next**.

- 2 In the **Specify Remediation Ticketing Criteria** panel, specify the combination of risk score and compliance score that you want to use to identify the assets for remediation.

You can select **Apply to all standards** if you want to apply the specified remediation criteria to all the standards for remediation.

If you do not select **Apply to all standards**, you must specify the remediation ticketing criteria for each standard.

Click **Next**.

- 3 In the **Select Remediation Ticket Type** panel, select one of the following:

- Create an email notification.

This option lets you create an email notification that you want to send for notification.

- Create a service desk ticket.

This action opens a service desk ticket request directly at the end of the evaluation results for the non-compliant assets.

You can choose the **Enable closed-loop verification** option. With the closed-loop verification, the non-compliant assets data is re-evaluated after the service desk request is met.

See [“About closed-loop verification”](#) on page 552.

Click **Next**.

- 4 If you choose to send an email notification as a remediation action, specify the message that you want to send as an email notification in the **Configure Notification Details for Remediation Ticketing** panel. Click **Next**.

If you select **Consolidate multiple assets in a single ticket/email**, a single notification is sent that includes all the non-compliant assets.

You can check **Make this the default Email Notification template** if you want to use the same message for all the service desk ticket requests.

- 5 If you choose to create a service desk ticket as a remediation action, specify the message that you want to send as a service desk request in the **Configure Service Desk Ticket** panel. Click **Next**.

If you select **Consolidate multiple assets in a single ticket/email**, a single service desk ticket is generated that includes all the non-compliant assets.

You can check **Make this the default Service Desk Ticket template** if you want to use the same message for all the service desk ticket requests.

- 6 Proceed with the Create or Edit Evaluation Job Wizard till the Summary panel. See [“Sizing guidelines for Collection-Evaluation-Reporting job”](#) on page 502.

Sizing guidelines for Collection-Evaluation-Reporting job

The Collection-Evaluation-Reporting job supports only a certain report templates. The reports that are available for the Collection-Evaluation-Reporting job are divided into two groups. The reports that are resource intensive and contain a large amount of data may overload the Crystal Report API during report generation. These reports are classified as heavy-weight reports. The reports that contain less data may not overload the Crystal Report API during report generation. These reports are classified as light-weight reports.

The heavy-weight reports are as follows:

- Compliance by Asset
- Gold Standard report
- Compliance by Technical Check

The light-weight reports are as follows:

- Compliance Summary
- Asset Risk Summary
- Asset Evaluation Result Change
- Assets at Highest Risk Report
- Top Failed Technical Checks

A heavy-weight report always fails to generate when the number of assets are above the 200 assets data point. The collection-evaluation-reporting job may succeed, but the report is not generated.

A light-weight report can handle between 200 and 500 assets. The Asset Evaluation Result Change report fails above the 500 asset data point.

See [“Running a collection-evaluation-reporting job from the Standards view”](#) on page 499.

Changing an ESM policy name at the standard level

You can rename an existing ESM policy name at the standard level. The policy name in the expressions of all the checks in the standard that you have selected is changed to the newly entered policy name.

Note: The ESM policy name is case sensitive.

To change an ESM policy name at the standard level

- 1 Right-click a standard and click **Change ESM Policy Name**.
- 2 In the Change ESM Policy Name dialog box, enter the new policy name.
- 3 Click **OK**.

See “[About changing an ESM policy name](#)” on page 467.

See “[Changing an ESM policy name at the section level](#)” on page 508.

See “[Changing an ESM policy name at the check level](#)” on page 521.

Working with sections

You can perform the following tasks on sections:

- View section information in the details pane
See “[Viewing section information in the details pane](#)” on page 503.
- Create a new section.
See “[Creating a new section](#)” on page 505.
- Copy and paste a section.
See “[Copying and pasting a section](#)” on page 506.
- Move a section.
See “[Moving a section](#)” on page 507.
- Rename a section.
See “[Renaming a section](#)” on page 507.
- Delete a section.
See “[Deleting a section](#)” on page 507.

Viewing section information in the details pane

You can view the information about a section from the details pane.

To view the section information

- 1
- Go to **Manage > Standards**.
- 2
- In the table pane of the Standards view, select the section for which you want to display the information.
- 3
- View the information for the selected section in the details pane.

The section details are contained in the following tabs:

-
- General
- See [“Section details pane - General tab”](#) on page 504.
-
- Description
- See [“Section details pane - Description tab”](#) on page 505.
-
- References
- See [“Section details pane - References tab”](#) on page 505.
-
- Exceptions

See [“About the details pane”](#) on page 50.

Section details pane - General tab

The General tab of the Section details pane provides general information about the selected section.

The General tab contains the following information:

Section Name	Name of the section. You can modify the name of the section. This value is editable. See “Renaming a section” on page 507.
Version	The current version of the section. See “About versioning scheme” on page 465.
Author	For a section that is contained within a predefined standard, the value of Author is Symantec. For a section that is contained within a user-defined standard, this value refers to the user who created the standard.
Creation Date	The date and time of creation of the section.
Last Updated	The date and time when the section was last updated.
Number of Checks	The total number of checks in the section.

See [“Viewing section information in the details pane”](#) on page 503.

See [“About the details pane”](#) on page 50.

See [“Working in the details pane”](#) on page 531.

Section details pane - Description tab

The Description tab of the Section details pane lets you describe the standard.

The Description tab has the following views:

- Read only
This view lets you only read the section description.
- Edit
This view lets you make changes to the section description.

See [“Viewing section information in the details pane”](#) on page 503.

See [“About the details pane”](#) on page 50.

See [“Working in the details pane”](#) on page 531.

Section details pane - References tab

The References tab lists the hyperlinks that lead to additional information about the section.

The References tab contains the following information:

Name	The reference name
URL	The hyperlink for locating the reference information

You can perform the following tasks using the References tab:

- Add reference information
See [“Adding reference information”](#) on page 535.
- Edit reference information
See [“Editing reference information”](#) on page 535.
- Delete reference information
See [“Deleting reference information”](#) on page 536.

Creating a new section

You can create a new section only with reference to a standard or another section. Therefore, before you create a new section, you identify the standard or the section to which you want to add the new section.

To add a new section to a standard or to another section

- 1 Go to Manage > Standards.
- 2 In the Standards view, right-click the standard or the section to which you want to add the new section and select **Create Section**.
- 3 In the Section Name dialog box, enter the name of the new section. Click **OK**.
The new section is added to the standard. You can enter further information for the section such as description and references through the details pane.

See [“Working with sections”](#) on page 503.

Copying and pasting a section

You can copy the predefined and the user-defined sections to custom standards. You can copy one or more sections at a time to any folder except the predefined folder.

To copy and paste a section using the context menu

- 1 Go to Manage > Standards.
- 2 In the table pane of the Standards view, right-click the section that you want to copy and select **Copy**.
This step lets you copy the selected section. But to view the copied section, you must perform the paste operation as explained in the next step.
- 3 Place the cursor under the standard or the section where you want to paste the copied section. Right-click the mouse and select **Paste**.

The Progress Status bar is displayed. This bar shows the progress of the paste operation. A message appears when the section is pasted.

To copy and paste a section using the menu bar

- 1 Go to Manage > Standards.
- 2 In the table pane of the Standards view, right-click the section that you want to copy and on the menu bar, click **Edit** and then **Copy**.
- 3 Put the cursor where you want to place the copied section. On the menu bar, click **Edit** and then **paste**.

See [“About multi-select functionality”](#) on page 491.

See [“Working with sections”](#) on page 503.

Moving a section

You can move the user-defined sections to any location except the predefined folder. You cannot move the predefined sections.

To move a section

- 1 Go to Manage > Standards.
- 2 In the table pane of the Standards view, do one of the following:
 - Right-click the section that you want to move and select **Move**.
 - Select the section that you want to move and on the taskbar, click **Common Tasks > Move**.
 - Select the section that you want to move and on the Tasks menu, select **Move**.
- 3 In the Move Standard - Manage dialog box, select the destination folder to which you want to move the section. Click **OK**.

See [“About multi-select functionality”](#) on page 491.

See [“Working with sections”](#) on page 503.

Renaming a section

You can change the section name through the General tab of the details pane.

To rename a section

- 1 Go to Manage > Standards.
- 2 In the table pane of the Standards view, select the section that you want to rename.
- 3 In the details pane, on the General tab, type the new name in the Section Name text box.
- 4 Click the save icon.

See [“Working with sections”](#) on page 503.

Deleting a section

You can delete only the user-defined sections. You cannot delete the predefined sections.

To delete a section

- 1 Go to Manage > Standards.
- 2 In the table pane of the Standards view, do one of the following:

- Right-click the section that you want to delete and select **Delete**.
 - Select the section that you want to delete and on the taskbar, click **Common Tasks > Delete**.
 - Select the section that you want to delete and on the Tasks menu, select **Delete**.
- 3 In the Manage Standards box, select **Yes** to delete the selected section.
- See [“About multi-select functionality”](#) on page 491.
- See [“Working with sections”](#) on page 503.

Changing an ESM policy name at the section level

You can rename an existing ESM policy name at the standard level. The policy name in the expressions of all the checks in the section that you have selected is changed to the newly entered policy name.

To change an ESM policy name at the section level

- 1 Right-click a section and click **Change ESM Policy Name**.
- 2 In the Change ESM Policy Name dialog box, enter the new policy name.
- 3 Click **OK**.

See [“About changing an ESM policy name”](#) on page 467.

See [“Changing an ESM policy name at the standard level”](#) on page 503.

See [“Changing an ESM policy name at the check level”](#) on page 521.

Working with checks

You can perform a number of tasks with checks. You can cut, copy, paste, create, and delete checks. You can also create new check expressions to customize the checks.

You can perform the following tasks on checks:

- View check information in the details pane
See [“Viewing check information in the details pane”](#) on page 509.
- Create a new check.
See [“Creating a new check”](#) on page 517.
- Copy and paste a check.
See [“Copying and pasting a check”](#) on page 515.
- Move a check.

See [“Moving a check”](#) on page 515.

- Rename a check.
See [“Renaming a check”](#) on page 516.
- Delete a check.
See [“Deleting a check”](#) on page 516.
- Modify a check.
See [“Editing a check”](#) on page 520.

Viewing check information in the details pane

You can view the information about a check through the details pane.

To view the check information

- 1 Go to Manage > Standards.
- 2 In the table pane of the Standards view, navigate to the check for which you want to display the information and select the check.
- 3 View the information for the selected check in the details pane.

The check details are contained in the following tabs:

- General
See [“Check details pane - General tab”](#) on page 510.
- Description
See [“Check details pane - Description tab”](#) on page 512.
- Expression
See [“Check details pane - Expression tab”](#) on page 512.
- Parameters
See [“Check details pane - Parameters tab”](#) on page 512.
- Remediation
See [“Check details pane - Remediation tab”](#) on page 513.
- Issue
See [“Check details pane - Issue tab”](#) on page 513.
- CVE
See [“Check details pane - CVE tab”](#) on page 514.
- References
See [“Check details pane - References tab”](#) on page 514.
- Target Type

- Exceptions
See “[Check details pane - Exceptions tab](#)” on page 514.

See “[About the details pane](#)” on page 50.

Check details pane - General tab

The General tab of the Check details pane provides general information about the selected check.

The General tab contains the following information:

Check Name	<p>The name of the check. This value is editable.</p> <p>See “Renaming a check” on page 516.</p>
Target Type	<p>The type of asset to which the check is applicable.</p> <p>See “About target types” on page 455.</p>
Author	<p>The value of Author is Symantec for a check that is contained within a predefined standard.</p> <p>For a check that is contained within a user-defined standard, this value refers to the user who created the check.</p>
Version	<p>The current version of the check.</p> <p>See “About versioning scheme” on page 465.</p>
Creation Date	<p>The date and time of creation of the check.</p>
Last Updated	<p>The date and time when the check was last updated.</p>
Confidentiality	<p>Confidentiality value has one of the following states:</p> <ul style="list-style-type: none">■ Not Defined■ No Impact■ Partial■ Complete
Integrity	<p>Integrity value has one of the following states:</p> <ul style="list-style-type: none">■ Not Defined■ No Impact■ Partial■ Complete

Availability	<p>Availability value has one of the following states:</p> <ul style="list-style-type: none"> ■ Not Defined ■ No Impact ■ Partial ■ Complete
Access Vector	<p>Access Vector has one of the following states:</p> <ul style="list-style-type: none"> ■ Not Defined ■ Local Accessible ■ Adjacent Network Accessible ■ Network Accessible
Access Complexity	<p>Access Complexity has one of the following states:</p> <ul style="list-style-type: none"> ■ Not Defined ■ Low ■ Medium ■ High
Authentication	<p>Authentication has one of the following states:</p> <ul style="list-style-type: none"> ■ Not Defined ■ Multiple Instances ■ Single Instance ■ No Authentication

For a user-defined check, you can modify the following information about the check through the General tab:

- Check Name
See [“Renaming a check”](#) on page 516.
- Confidentiality
- Integrity
- Availability
- Access Vector
- Access Complexity
- Authentication

See [“Viewing check information in the details pane”](#) on page 509.

See [“About the details pane”](#) on page 50.

See [“Working in the details pane”](#) on page 531.

Check details pane - Description tab

The Description tab of the Check details pane lets you describe the standard. The Description tab has the following views:

- Read only
This view lets you only read the check description.
- Edit
This view lets you make changes to the check description.

See [“Viewing check information in the details pane”](#) on page 509.

See [“About the details pane”](#) on page 50.

See [“Working in the details pane”](#) on page 531.

Check details pane - Expression tab

The Expression tab of the check details pane states the check formula and the specified pre-conditions.

The Expression tab contains the following information:

Pre-Condition	States the pre-condition.
Formula	States the check formula.

Click the Switch to expanded mode icon to expand the individual expressions in the formula and view the complete formula.

To view information for each expression in the formula, click the expression in the formula. The Expression text dialog box appears. This dialog box contains the selected expression.

You can also edit the pre-condition and the check formula through the Expression tab.

See [“Viewing check information in the details pane”](#) on page 509.

See [“About the details pane”](#) on page 50.

See [“Working in the details pane”](#) on page 531.

Check details pane - Parameters tab

Some checks in the predefined standards use complex algorithms. The custom algorithms make use of named procedures. You must use the Parameters tab in the details pane to modify the values of the parameter.

Name	The name of the parameter.
Value	The value of the parameter.

See [“Viewing check information in the details pane”](#) on page 509.

See [“About the details pane”](#) on page 50.

See [“Working in the details pane”](#) on page 531.

Check details pane - Remediation tab

The Remediation tab of the check details pane states the recommended fixes for the issue.

The Remediation tab has the following views:

- Read only
This view lets you only read the remediation information that was entered when the check was created.
- Edit
This view lets you make changes to the remediation information.

See [“Viewing check information in the details pane”](#) on page 509.

See [“About the details pane”](#) on page 50.

See [“Working in the details pane”](#) on page 531.

Check details pane - Issue tab

The Issue tab of the check details pane states the reason for creating the check.

The Issue tab has the following views:

- Read only
This view lets you only read the issue information that was entered when the check was created.
- Edit
This view lets you make changes to the issue information.

See [“Viewing check information in the details pane”](#) on page 509.

See [“About the details pane”](#) on page 50.

See [“Working in the details pane”](#) on page 531.

Check details pane - CVE tab

The CVE tab of the check details pane lists the number for the common vulnerabilities and exposures information.

See [“Viewing check information in the details pane”](#) on page 509.

See [“About the details pane”](#) on page 50.

See [“Working in the details pane”](#) on page 531.

Check details pane - References tab

The References tab lists the hyperlinks that lead to additional information about the check.

The References tab contains the following information:

Name	The reference name
URL	The hyperlink for locating the reference information

You can perform the following tasks using the References tab:

- Add reference information
See [“Adding reference information”](#) on page 535.
- Edit reference information
See [“Editing reference information”](#) on page 535.
- Delete reference information
See [“Deleting reference information”](#) on page 536.

See [“Viewing check information in the details pane”](#) on page 509.

See [“About the details pane”](#) on page 50.

See [“Working in the details pane”](#) on page 531.

Check details pane - Exceptions tab

The Exceptions tab lets you view the exception-related details of the check.

The Exceptions tab contains the following information:

Title	The title that was specified at the time of creating the exception.
Effective Date	The start date of the exception validity period. The exception becomes valid from this date.

Expiration Date	The last day of the exception validity period. The exception becomes invalid after this date.
Last Modified On	The date and time when the exception was last modified.

Copying and pasting a check

You can copy the predefined and the user-defined checks. You can copy one or more checks at a time to any folder except the predefined folder.

To copy and paste a check using the context menu

- 1 Go to Manage > Standards.
- 2 In the table pane of the Standards view, right-click the check that you want to copy and select **Copy**.

This step lets you copy the selected check. But to view the copied check, you must perform the paste operation as explained in the next step.

- 3 Place the cursor under the section where you want to paste the copied check. Right-click the mouse and select **Paste**.

The Progress Status bar is displayed. This bar shows the progress of the paste operation. A message appears when the check is pasted.

To copy and paste a check using the menu bar

- 1 Go to Manage > Standards.
- 2 In the table pane of the Standards view, right-click the check that you want to copy and on the menu bar, click **Edit** and then **Copy**.
- 3 Place the cursor where you want to locate the copied check. On the menu bar, click **Edit** and then **paste**.

See [“About multi-select functionality”](#) on page 491.

See [“Working with checks”](#) on page 508.

Moving a check

You can move the user-defined checks to any location except the predefined folder. The predefined checks cannot be moved.

To move a check

- 1 Go to Manage > Standards.
- 2 In the table pane of the Standards view, do one of the following:

- Right-click the check that you want to move and select **Move**.
 - Select the check that you want to move and on the taskbar, click **Common Tasks > Move**.
 - Select the check that you want to move and on the Tasks menu, select **Move**.
- 3 In the Move Standard - Manage dialog box, select the destination folder to which you want to move the check. Click **OK**.

See [“About multi-select functionality”](#) on page 491.

See [“Working with checks”](#) on page 508.

Renaming a check

You can change the check name through the General tab of the details pane.

To rename a check

- 1 Go to Manage > Standards.
- 2 In the table pane of the Standards view, select the check that you want to rename.
- 3 In the details pane, on the General tab, type the new name in the Check Name text box.
- 4 Click the save icon.

See [“Working with checks”](#) on page 508.

Deleting a check

You can delete only the user-defined checks. You cannot delete the predefined checks.

To delete a check

- 1 Go to Manage > Standards.
- 2 In the table pane of the Standards view, do one of the following:
 - Right-click the check that you want to delete and select **Delete**.
 - Select the check that you want to delete and then on the taskbar, click **Common Tasks > Delete**.
 - Select the check that you want to delete and then in the Tasks menu, select **Delete**.
- 3 In the Manage Standards dialog box, select **Yes** to delete the selected check.

See [“About multi-select functionality”](#) on page 491.

See [“Working with checks”](#) on page 508.

Creating a new check

You must use the Create Check wizard to create a new check.

The Create Check wizard provides you the following options to create a new check:

Quick Check Builder	This option lets you create a check that does not include a pre-condition.
Advanced Check Builder	This option lets you create a check that includes a pre-condition.

To create a new check

- 1 Go to Manage > Standards.
- 2 In the table pane of the Standards view, navigate to the section to which you want to add the new check. Right-click the section and select **Create Check**.
- 3 In the Specify Name and Target panel of the Create Check wizard, enter the following information:
 - In the Name text box, type the name of the new check.
 - In the Description text box, type a description for the new check. This information is optional.
 - In the Target Type text box, select the type of asset to which the new check is applicable.
You can also create custom target types to evaluate specific standards against a targeted set of assets.
 - Select either the **Quick Check Builder** option or the **Advanced Check Builder** option.
The Quick Check Builder option lets you create a check without a precondition.
The Advanced Check Builder option lets you add a precondition to the new check.
- 4 Click **Next**

To proceed with check creation using the Quick Check Builder option

- 1 In the Create Expression(s) panel, enter the following information to create an evaluation condition.
 - In the Category list box, select the category of the field.

- In the Field list box, select the name of the field.
 - In the Operator list box, select the operator.
 - In the Value text box, specify a value for the field.
To specify values for a LIST field, you must enclose all the values in a curly bracket and use a comma to separate each value. For example, {sam, ram, mac}.
- 2 Click the icon at the top right corner of the Value box to launch the Field Information Browser. The Field Information Browser lets you browse through the list of fields that are supported in the entity schema for the selected data collector. You can also view the fields and its information to build a meaningful check expression.
 - 3 Click the plus (+) sign to add the recently created field expression to the Expression(s) list.
The new expression is added to the Formula box by default. If a check includes only a single expression, then the check formula is the same as the expression.
 - 4 Repeat step 1 and step 3 to create any number of expressions.
 - 5 In the Formula text box, you can use the check formula operators to connect the various expressions.
By default, the new expressions are connected using the AND operator.
 - 6 Click the Validate Formula icon to validate the check formula that you have created. Click **Next**.
 - 7 In the Check Summary panel, you can view the information that you have entered. Click **Back** to make any changes and click **Finish** to exit the wizard.

To proceed with check creation using the Advanced Check Builder option

- 1 In the Create a Precondition panel, enter the following information to create an evaluation condition.
 - In the Category list box, select the category of the field.
 - In the Field list box, select the name of the field.
 - In the Operator list box, select the operator.
See “[About operators](#)” on page 478.
 - In the Value text box, specify a value for the field.

To specify values for a LIST field, you must use a comma to separate the multiple values and enclose all the values in a curly bracket. For example, {sam, ram, mac}.

- 2 Click the icon at the top right corner of the Value box to launch the Platform Browser. The Platform Browser lets you browse through the list of entities that are supported in the entity schema for all the data collectors. You can also view the entity and its information to build a meaningful check expression.

- 3 Click the plus (+) sign to add the recently created field expression to the Expression(s) list.

The new expression is added to the Formula box by default. If a check includes only a single expression then the check formula is the same as the expression.

- 4 Repeat steps 1 and 2 to create any number of expressions.

- 5 In the Formula text box, you can use the check formula operators to connect the various expressions.

By default, the new expressions are connected using the AND operator.

- 6 Click the Validate Formula icon to validate the check formula that you have created. Click **Next**.

- 7 In the Create Expression(s) panel, enter the information in the same manner as in steps 1 to 6. Click **Next**.

- 8 In the Specify Check Content panel, enter the optional information such as risk rating, remediation, issue, CVE, and references. Click **Next**.

See [“Editing a check”](#) on page 520.

- 9 In the Check Summary panel, you can view the information that you have entered. Click **Back** to make any changes and click **Finish** to exit the wizard.

See [“Viewing check information in the details pane”](#) on page 509.

See [“Check details pane - Remediation tab”](#) on page 513.

See [“Check details pane - Issue tab”](#) on page 513.

See [“Check details pane - CVE tab”](#) on page 514.

See [“Check details pane - References tab”](#) on page 514.

See [“About the target type schema”](#) on page 347.

See [“Creating a new target type”](#) on page 365.

See [“Editing a target type”](#) on page 366.

Editing a check

You can make changes to an existing check.

The following features of a check can be edited:

- **Name and risk attributes**
You can change the name, target type, and the risk rating values of the check from the General tab of the details pane.
See [“Renaming a check”](#) on page 516.
See [“Specifying or editing the check attributes”](#) on page 534.
- **Description**
You can change the description of the check from the Description tab of the details pane.
See [“Specifying or editing the description ”](#) on page 532.
- **Remediation, issue, and references**
You can change the remediation, issue, and references information from the respective tabs on the details pane.
See [“Specifying or editing the remediation information”](#) on page 533.
See [“Specifying or editing the check issue ”](#) on page 532.
See [“Editing reference information”](#) on page 535.
- **Pre-condition and Check formula**
You can change the pre-condition and the check formula from the Edit Check wizard.

Note: You cannot edit the pre-condition and the check formula of a custom check.

To change the pre-condition and the check formula

- 1 In the table pane of the Standards view, do either of the following:
 - Right-click the check that you want to modify and select **Edit**.
 - Select the check that you want to modify and on the Expressions tab of the details pane, click **Edit**.
 - Go to the **Expressions** tab in the check details pane.
- 2 In the Specify a target filter panel of the Edit Check wizard, enter the following information to create a field expression:
 - In the Category list box, select the category of the field.
 - In the Field list box, select the name of the field.
 - In the Operator list box, select the operator.

- In the Value text box, specify a value for the field.
- 3 Click the icon at the top right corner of the Value box to launch the Platform Browser. The Platform Browser lets you browse through the list of entities that are supported in the entity schema for the selected data collector. You can also view the entity and its information to build a meaningful check expression.
- 4 Click the plus (+) sign to add the recently created field expression to the Expression(s) list.

The new expression is added to the Formula box by default. If a check includes only a single expression then the check formula is the same as the expression.
- 5 Repeat step 2 and step 4 to create any number of expressions.
- 6 In the Formula text box, you can use the check formula operators to connect the various expressions.

By default, the new expressions are connected using the AND operator.
- 7 Click **Validate Formula** to validate the check formula that you have created.
- 8 In the Expressions panel, enter the information in the same manner as in steps 1 to 6.
- 9 In the Review panel, you can view the information that you have entered. Click **Back** to make any changes and click **Finish** to exit the wizard.

See [“Working with checks”](#) on page 508.

See [“Creating a new check”](#) on page 517.

Viewing the evidence details

You can view the evidence details for a check that has a failed, an error, or an unknown outcome.

To view the evidence details

- 1 In the Evaluation Result Details dialog box, select **Asset based** view.
- 2 Select an asset and then select the check for which you want to view the evidence.
- 3 Right-click the check and select **Show Detailed Evidence**.

Changing an ESM policy name at the check level

You can rename an existing ESM policy name at the check level. The policy name in the expressions of the check that you have selected is changed to the newly entered policy name.

To change an ESM policy name at the check level

- 1 Right-click a check and click **Change ESM Policy Name**.
- 2 In the Change ESM Policy Name dialog box, enter the new policy name.
- 3 Click **OK**.

See [“About changing an ESM policy name”](#) on page 467.

See [“Changing an ESM policy name at the standard level”](#) on page 503.

See [“Changing an ESM policy name at the section level ”](#) on page 508.

Creating an ESM check

You can create the CCS ESM checks using the Check Builder wizard.

The Check Builder wizard provides you with the following options to create checks:

The Quick Check Builder option	Lets you create a check without a precondition.
The Advanced Check Builder option	Lets you add a precondition to the new check.

The check execution process in ESM includes the following:

- The CCS evaluation engine checks if the ESM agent reports the security messages that the corresponding CCS ESM check generates.
- If the ESM agents reports security messages, then the CCS check is reported as "Fail."

In case of a failed check, the evidence report includes the following:

 - The ESM message title
 - The message name
 - The message information
- If the ESM agent does not report any security message, then the CCS evaluation engine checks if the agent reports any error message.
- If the ESM agents reports error messages, then the CCS check is reported as "Unknown" and the evidence report includes the ESM error messages.
- If the ESM agent does not report any security message or any error message, then the CCS check is reported as "Pass."

Note: You must include the policy name and the module name in the data filter when you create an expression in an ESM check. The ESM data collector uses the policy name and module name that you specify when it collects data for the checks.

See [“Creating a CCS ESM check by using the Quick Check Builder option”](#) on page 523.

See [“Creating a CCS ESM check by using the Advanced Check Builder option”](#) on page 528.

Creating a CCS ESM check by using the Quick Check Builder option

You can create CCS ESM checks by using the Quick Check Builder option.

To create a CCS ESM check by using the Quick Check Builder option

- 1 In the **Standards** pane, right-click the section to which you want to add the new check and click **Create Check**.
- 2 In the **Specify Name and Target Type** panel of the Check Builder, enter the following information:
 - In the **Name** text box, type a name for the new check.
 - In the **Description** text box, type a description for the check. This field is optional.
 - From the **Target Type** drop-down list, expand the Enterprise Security Manager Platform node, and then click the type of asset that you want to be evaluated.
See [“About ESM predefined target types”](#) on page 462.
 - Click **Quick Check Builder**.
- 3 Click **Next**.
- 4 In the **Create Expressions** panel, add a message expression for each message that the corresponding CCS ESM check can generate.
See [“Creating a message expression for a new CCS ESM check”](#) on page 524.
See the *Symantec_Enterprise_Security_Manager_Checks_Reference.chm* for information on the messages that ESM checks generate. This file is located in the Documentation folder in the product disc.
- 5 Add data filters for ESM module name and ESM policy name.
See [“Adding the policy name and the module name data filters for a new CCS ESM check”](#) on page 525.

- 6 Add an error expression to the check that you want to create. The error expression checks if an ESM agent reports any error message.
See “[Creating an ESM error expression for a new ESM check](#)” on page 526.
- 7 Update the CCS check formula so that the CCS check behaves as per the check execution rules.
See “[Creating an ESM check](#)” on page 522.
See “[Editing the check formula for a new CCS ESM check](#)” on page 527.
- 8 Click **Next**.
- 9 In the **Review** panel, view the information that you have entered and then click **Finish**.
See “[Creating an ESM check](#)” on page 522.
See “[Creating a CCS ESM check by using the Advanced Check Builder option](#)” on page 528.

Creating a message expression for a new CCS ESM check

You need to add a message expression for each message that the corresponding CCS ESM check generates.

To create a message expression

- 1 In the Standards pane, right-click the section to which you want to add the new check and click **Create Check**.
- 2 In the Specify Name and Target panel of the Check Builder, provide the necessary information and then click one of the following options:
 - Quick Check Builder
 - Advanced Check Builder
- 3 Click **Next**.
- 4 In the Create Expressions panel, create a message expression by performing the following steps:
 - In the **Category** drop-down list, select **Message**.
 - In the **Field** drop-down list, select **Message String ID**.
 - In the Operator drop-down list, select the **!=** operator.
 - In the Value text box, select the message ID. For example, select **ESM_DISABLED_ACCOUNT**.

See the *Symantec_Enterprise_Security_Manager_Checks_Reference.chm* for information on the respective message ID that each ESM check generates for

an ESM compliance message. This file is located in the Documentation folder in the product disc.

- 5 Click the **Add** icon to add the recently created check expression to the Expression(s) list.

By default, the new expressions are connected using the **AND** operator.

- 6 Select the expression that you have created from the Expression(s) list box and click **Advanced Settings**. Alternatively, double-click the expression in the Expression(s) list.

See [“Adding the policy name and the module name data filters for a new CCS ESM check”](#) on page 525.

See [“Adding the policy name and the module name data filters for a new CCS ESM check”](#) on page 525.

Adding the policy name and the module name data filters for a new CCS ESM check

You must add the policy name and the module name to the ESM check that you want to create.

To configure the advanced settings for a CCS ESM message

- 1 In the Standards pane, right-click the section to which you want to add the new check and click **Create Check**.
- 2 In the Specify Name and Target panel of the Check Builder, provide the necessary information and then click one of the following options:
 - Quick Check Builder
 - Advanced Check Builder
- 3 Click **Next**.
- 4 In the **Create Expression(s)** panel of the CCS Check Builder wizard, do the following:
 - In the Category drop-down list, click **ESM Message**.
 - In the Field drop-down list, click **ESM Module Name**.
 - Select the = operator and then select a module name from the Value drop-down list.
 - Click the plus (+) sign to add the expression to the Expression(s) list.
 - In the Expression(s) list, double-click the expression.
- 5 To add a data filter for policy name, do the following:

- From the Field drop-down list, select **ESM Policy**.
 - Select the = operator and then type a policy name in the Value drop-down list. For example, type **Security essentials W2K3MS v2.0**.
ESM policy names are case sensitive.
The = operator is the only operator that ESM data collector supports for ESM policy data filter.
 - Click the plus sign (+) to add the expression.
- 6 In the Advanced Settings dialog box, do the following to add a data filter for the module name:
- From the Field drop-down list, select **ESM Module Name**.
 - Select the = operator and then select a module name from the Value drop-down list. For example, select **Account Integrity**.
 - Click the plus sign (+) to add the expression.
- 7 In the **Data items filter** section, click **Return only the data which matches ALL of the filter statements**. This option is mandatory to create a valid CCS ESM check.
- 8 In the Specify behavior if multiple data items were evaluated against Evaluation Condition area, click **ALL must meet the evaluation condition**.
- Click **All must meet the evaluation condition**, if you want the check to meet all the values that you have specified in the evaluation condition.
 - Click **At least ONE must meet the evaluation condition** if you want the check to meet any one of the values that you have specified in the evaluation condition.
- 9 In the Specify the expression outcome when no data items were found to evaluate against the Evaluation Condition area, click **Unknown**.
- 10 Click **OK**.

See “[Creating an ESM check](#)” on page 522.

Creating an ESM error expression for a new ESM check

You must add an error expression to the ESM check that you want to create. An error expression checks if an ESM agent reports any error message.

To create an ESM error expression

- 1 In the Standards pane, right-click the section to which you want to add the new check and click **Create Check**.
- 2 In the Specify Name and Target panel of the Check Builder, provide the necessary information and then click one of the following options:
 - Quick Check Builder
 - Advanced Check Builder
- 3 Click **Next**.
- 4 In the Create Expressions panel, enter the following information to create an error expression:
 - In the Category drop-down list, select **Message**.
 - In the Field drop-down list, select **Is Error Message**.
 - In the Operator drop-down list, select the “=” operator.
 - In the Value text box, select **False**.

An expression that contains "Is Error Message = False" lets you mark a check for manual review if an ESM module generates error messages.
- 5 Click the plus sign (+) to add the recently created field expression to the Expression(s) list.

The new expression is added to the Formula box by default. If a check includes only a single expression then the check formula is the same as the expression. You can create as many expressions as you want.
- 6 Select the expression from the Expression(s) list box and click **Advanced Settings**. Alternatively, double-click the expression in the Expression(s) list.

For every expression that you create on a Message entity, you must add data filters for module name and policy name.

See [“Adding the policy name and the module name data filters for a new CCS ESM check”](#) on page 525.

See [“Creating an ESM check”](#) on page 522.

Editing the check formula for a new CCS ESM check

After you create the message expression and the error expression, you must edit the check formula to ensure that the check that you create behaves as per the specifications.

To edit the check formula for a new CCS ESM check

- 1

In the Standards pane, right-click the section to which you want to add the new check and click **Create Check**.
- 2

In the Specify Name and Target panel of the Check Builder, provide the necessary information and then click one of the following options:

■ Quick Check Builder

■ Advanced Check Builder
- 3

Click **Next**.
- 4

In the Create Expressions panel, enter the necessary information to create an error expression.

See “[Creating an ESM error expression for a new ESM check](#)” on page 526.
- 5

In the Formula box, edit the predicate as follows:

Type **If [(message expression)] THEN (IF ([error expression]) THEN (True) ELSE (Unknown)) ELSE ([False])**

Following is the explanation for the message expression and error expression:

Message expression	<p>Name of the message expressions that you have created, which corresponds to the messages that an ESM check generates.</p> <p>If the check generates multiple messages, you must specify the message expressions by using the logical AND operator. For example, E1 AND E2.</p>
Error expression	<p>Name of the error expression.</p>

Creating a CCS ESM check by using the Advanced Check Builder option

You can create CCS ESM checks by using the Advanced Check Builder option.

To create a CCS ESM check by using the Advanced Check Builder option

- 1

In the Standards pane, right-click the section to which you want to add the new check and click **Create Check**.
- 2

In the **Specify Name and Target Type** panel of the Check Builder, enter the following information:

- In the **Name** text box, type a name for the new check.
 - In the **Description** text box, type a description for the check. This field is optional.
 - From the **Target Type** drop-down list, expand the Enterprise Security Manager Platform node, and then click the type of ESM asset that you want to evaluate.
See “[About ESM predefined target types](#)” on page 462.
 - Click **Advanced Check Builder**.
- 3 ■ From the **Category** drop-down list, select the category of the ESM entity.
- From the **Field** drop-down list, select the field for the category that you want the check to report on.
 - From the **Operator** drop-down list, select the operator.
 - From the **Value** drop-down list, select the value for the field that you have selected.
 - Click the **Add** icon to add the pre-condition to the **Expressions** list box. You can see the name of the check formula that you create in the **Formula** box.
 - Double-click the evaluation condition and configure the advanced settings for the check expression and then **Next**.
- 4 In the Create Expressions panel, create a message expression by performing the following steps:
- In the **Category** drop-down list, select **Message**.
 - In the **Field** drop-down list, select **Message String ID**.
 - In the Operator drop-down list, select the **!=** operator.
 - In the Value text box, select the message ID. For example, select **ESM_DISABLED_ACCOUNT**.
See the *Symantec_Enterprise_Security_Manager_Checks_Reference.chm* for information on the messages that ESM checks generate. This file is located in the Documentation folder in the product disc.
 - Click the **Add** icon to add the recently created check expression to the Expression(s) list.
By default, the new expressions are connected using the **AND** operator.
- 5 Add data filters for ESM module name and ESM policy name.
See “[Adding the policy name and the module name data filters for a new CCS ESM check](#)” on page 525.

- 6

Add an error expression to the check that you want to create. The error expression checks if an ESM agent reports any error message.
See “[Creating an ESM error expression for a new ESM check](#)” on page 526.
- 7

Update the CCS Check formula so that the CCS check behaves as per the check execution rules.
See “[Creating an ESM check](#) ” on page 522.
See “[Editing the check formula for a new CCS ESM check](#)” on page 527.
- 8

Click **Next**.
- 9

In the **Specify Check Content** panel, enter the information on the content of the check. This information is optional.

Risk Rating	Lets you enter the check attributes. These values are used to calculate the Risk Score.
Remediation	Lets you enter the remediation for the issue.
Issue	Lets you enter more information on the issue.
CVE	Lets you enter the ID for common vulnerabilities and exposures.
References	Lets you enter the URL for a Web site for more information.

- 10

In the Review panel, view the information that you have entered and then click **Finish**.
See “[Creating an ESM check](#) ” on page 522.
See “[Creating a CCS ESM check by using the Quick Check Builder option](#)” on page 523.

Specifying the content for a new CCS ESM check

You can specify the check content when you create an ESM check by using the Specify Check Content panel.

To specify the content for a new CCS ESM check

- 1 In the Standards pane, right-click the section to which you want to add the new check and click **Create Check**.
- 2 In the Specify Name and Target panel of the Check Builder, provide the necessary information and then click **Advanced Check Builder**.
- 3 Click **Next**.
- 4 In the Create Expressions panel, enter the necessary information to create an error expression and then click **Next**.
See “[Creating an ESM error expression for a new ESM check](#)” on page 526.
- 5 In the Specify Check Content panel, enter the information on the content of the check. This information is optional.

Risk Rating	Lets you enter the check attributes. These values are used to calculate the Risk Score.
Remediation	Lets you enter the remediation for the issue.
Issue	Lets you enter more information on the issue.
CVE	Lets you enter the ID for common vulnerabilities and exposures.
References	Lets you enter the URL for a Web site for more information.

See “[Creating a CCS ESM check by using the Advanced Check Builder option](#)” on page 528.

See “[Creating a CCS ESM check by using the Quick Check Builder option](#)” on page 523.

Working in the details pane

You can perform the following tasks using the details pane:

- Rename a standard, section, or check
See “[Renaming a standard](#)” on page 494.
See “[Renaming a section](#)” on page 507.
See “[Renaming a check](#)” on page 516.
- Enter or edit the description for a standard, section, or check.

See [“Specifying or editing the description ”](#) on page 532.

- Add, edit, or delete the reference information for a standard, section, or check.
See [“Adding reference information”](#) on page 535.
See [“Editing reference information”](#) on page 535.
See [“Deleting reference information”](#) on page 536.
- Enter or edit the remediation information for a check.
See [“Specifying or editing the remediation information”](#) on page 533.
- Enter or edit the issue information for a check.
See [“Specifying or editing the check issue ”](#) on page 532.
- Add or edit the CVE information for a check.
See [“Adding the CVE information”](#) on page 533.
See [“Editing the CVE information”](#) on page 534.
- Enter or edit the risk attributes of a check
See [“Specifying or editing the check attributes”](#) on page 534.

Specifying or editing the description

You can specify the description when you create a standard, section, or check. You can also enter the description from the details pane after creating a standard, section, or check. You can edit the description only through the details pane.

To specify or edit the description using the details pane

- 1 Go to **Manage > Standards**.
- 2 In the **Standards** view, select the standard, section, or check for which you want to enter or modify the description.
- 3 On the **Description** tab, click the **Switch between Edit and Read-only view** icon.

This icon lets you switch between the Read-only and the Edit view.
- 4 Enter a description or modify the existing description.

You can use the Bold, list item, and the Web link icon on the taskbar.
- 5 Click the save icon.

See [“Working in the details pane”](#) on page 531.

Specifying or editing the check issue

You can enter or edit the issue information for a check through the details pane. You can also enter the check issue at the time of creating a check.

To specify or edit the issue information using the details pane

- 1 Go to **Manage > Standards**.
- 2 In the table pane, navigate to the check for which you want to edit the issue information. Select the check.
- 3 In the details pane, on the Issue tab, click the icon with two arrows.
This icon lets you switch between the Read-only and the Edit view.
- 4 Enter the issue or edit the existing issue.
You can use the Bold, list item, and the Web link icon on the taskbar.
- 5 Click the Save icon.

See [“Working in the details pane”](#) on page 531.

Specifying or editing the remediation information

You can specify or edit the remediation information for a check through the details pane.

To edit the remediation information

- 1 Go to **Manage > Standards**.
- 2 In the table pane, navigate to the check for which you want to edit the remediation information. Select the check.
- 3 In the details pane, on the Remediation tab, click the Switch between Edit and Read-only view icon.
This icon lets you switch between the Read-only and the Edit view.
- 4 Enter or edit the remediation information.
You can use the Bold, list item, and the Web link icon on the taskbar.
- 5 Click the save icon.

See [“Working in the details pane”](#) on page 531.

Adding the CVE information

You can add the CVE information for a check through the details pane. You can also enter the CVE information at the time of creating a check.

To add the CVE information using the details pane

- 1 Go to **Manage > Standards**.
- 2 In the table pane, navigate to the check for which you want to edit the CVE information. Select the check.

- 3 In the details pane, on the CVE tab, click the add (+) icon.
- 4 In the Add CVE dialog box, enter the CVE text that you want to add.
- 5 Click **Add**.
- 6 Click the save icon.

See [“Working in the details pane”](#) on page 531.

Editing the CVE information

You can edit the CVE information for a check through the details pane.

To edit the CVE information

- 1 Go to Manage > Standards.
- 2 In the table pane, navigate to the check for which you want to edit the CVE information. Select the check.
- 3 Select the CVE text that you want to edit and click the edit icon.
- 4 In the Edit CVE dialog box, enter the CVE text and click **Update**. Click the save icon.
- 5 To delete the CVE information, select the required text and click the delete icon. Click the save icon.

See [“Working in the details pane”](#) on page 531.

Specifying or editing the check attributes

You can specify or edit the risk attributes of a check through the details pane.

See [“Check risk attributes”](#) on page 472.

To specify or edit the risk attributes

- 1 Go to Manage > Standards.
- 2 In the table pane, navigate to the check for which you want to edit the risk attributes. Select the check.
- 3 In the details pane, on the General tab, select the values for the following:
 - Confidentiality
 - Integrity
 - Availability
 - Access Vector
 - Access Complexity

- Authentication

- 4 Click the save icon.

See [“Working in the details pane”](#) on page 531.

Adding reference information

You can add reference information through the Reference tab in the details pane.

To add the reference information

- 1 Go to Manage > Standards.
- 2 In the Standards view, select the standard, section, or check for which you want to add the reference information.
- 3 In the details pane, on the References tab, click the add icon.
- 4 In the Add References window, in the Link Text box, type the name for the reference text.
- 5 In the Link box, type the URL path.
- 6 Click **Add** in the Add References window.

The reference link information is added on the Reference tab.

- 7 Click the save icon.

See [“Working in the details pane”](#) on page 531.

Editing reference information

You can edit the reference information through the Reference tab in the details pane.

To edit the reference information

- 1 Go to Manage > Standards.
- 2 In the Standards view, select the standard, section, or check for which you want to edit the reference information.
- 3 In the details pane, on the References tab, select the reference that you want to edit.
- 4 Click the edit icon.
- 5 In the Edit References window, in the Link Text box, edit the name for the reference text.
- 6 In the Link box, edit the URL path.

7 Click Update.

The reference is updated with the new information.

8 Click the save icon.

See [“Working in the details pane”](#) on page 531.

Deleting reference information

You can delete the reference information through the Reference tab in the details pane.

To delete the reference information

- 1** Go to Manage > Standards.
- 2** In the Standards view, select the standard, section, or check for which you want to add the reference information.
- 3** In the details pane, on the References tab, select the reference that you want to delete.
- 4** Click the delete icon.
- 5** In the Delete Row message box, click **Yes** to delete the selected reference link.
- 6** Click the save icon.

See [“Working in the details pane”](#) on page 531.

Working with gold standard

Once a gold standard has been created, you can treat the gold standard in the same manner as a regular standard. You can perform the same operations on a gold standard that you perform on a regular standard. You can create, delete, modify, copy, and paste the sections and checks within a gold standard. You can also collect data and run an evaluation job for a gold standard.

■ Create a gold standard

See [“Creating a gold standard”](#) on page 537.

■ Manually resolve checks in a gold standard

See [“Resolving checks in a gold standard”](#) on page 538.

Gold standard concepts

The following terms are used with reference to gold standards:

- Reference asset

The asset whose values are used to create a gold standard. The reference asset can be of any type. For example, the reference asset can be a Windows computer, a UNIX computer, or an Oracle database.

■ **Reference standard**

The standard whose values are modified according to the values that exist in the reference asset.

■ **Synchronization**

In a gold standard, synchronization is required when any parameter in the reference asset changes.

During the synchronization process, values in the gold standard are refreshed on the basis of the values in the reference asset. The values in Manually Resolved state are not changed. The synchronization process indicates that new data is available and you can manually resolve the check.

See [“About gold standard”](#) on page 464.

See [“Creating a gold standard”](#) on page 537.

Creating a gold standard

You create a gold standard through the Create Gold Standard wizard.

To create a gold standard

- 1 Go to Manage > Standards.
- 2 In the Standards view, do one of the following:
 - On the taskbar , click **Create Gold Standard**.
 - On the Tasks menu, point to Gold Standard Tasks, and then click **Create Gold Standard**.
- 3 In the Create Gold Standard wizard, in the Specify Name and Reference Information panel, enter a name for the gold standard in the Name box.
- 4 Click (...) to specify a reference standard. In the Select Reference Standard dialog box, select a standard and click **Add**. The selected standard is added to the Selected Items list. Click **OK**.
- 5 In the Specify Name and Reference Information panel, to specify a reference asset, click (...) against the Reference Asset box. In the Select Reference Asset dialog box, select an asset and click **Add**. The selected asset is added to the Selected Items list. Click **OK**.
- 6 In the Specify Name and Reference Information panel, click **Next**.

- 7 In the Specify Destination Location panel, in the Destination Location box, browse to specify the location of the gold standard. Click **Next**.
 - 8 In the Summary panel, view the details that you have specified for the gold standard. Click **Back** to make any changes or click **Finish** to exit the wizard.
- You can view the gold standard that you have created in the table pane of the Standards view.

See [“About gold standard”](#) on page 464.

See [“Gold standard job”](#) on page 538.

Gold standard job

You create a gold standard through the Create Gold Standard wizard. After you specify all the values in the wizard, the system runs a gold standard job to create the gold standard.

The gold standard job is available in the list of jobs in the job management view.

You can only perform the following operations on a gold standard job:

- Refresh.
- Delete.

When you delete a gold standard job, the corresponding gold standard is also deleted. Similarly when you delete a gold standard, the corresponding gold standard job is also deleted.

See [“About gold standard”](#) on page 464.

See [“Creating a gold standard”](#) on page 537.

Resolving checks in a gold standard

Control Compliance Suite creates a gold standard by replacing the expression values in a reference standard with data from a reference asset.

Control Compliance Suite cannot resolve the checks in a gold standard in the following conditions:

- Data is ambiguous.
In this case, Control Compliance Suite gives you the provision to manually resolve the checks in the gold standard.
- Check is complex.
You cannot manually resolve the check.

You can manually review and resolve the checks in a gold standard through the Manual Review dialog box.

To manually resolve checks in a gold standard

- 1 Go to Manage > Standards.
- 2 In the Standards view, select the gold standard whose checks you want to manually review and do one of the following:
 - Right-click the selected gold standard and select **Manual Review**.
 - On the taskbar, select **Manual Review**.The Manual Review dialog box is displayed.
- 3 In the Manual Review dialog box, select the check that you want to resolve.
- 4 Select the Resolve Check icon on the top.
- 5 In the Resolve Check dialog box, under the Expression(s) list, select the expression that you want to modify.
- 6 In the Value(s) list, select the required value. Click the Update icon.
- 7 Repeat steps 3 and 4 to modify any further expressions.
- 8 Click **OK**.

See [“Using the Manual Review dialog box”](#) on page 539.

See [“About gold standard”](#) on page 464.

Using the Manual Review dialog box

You can perform the following functions on the checks in the gold standard using the Manual Review dialog box:

- Delete checks.
- Edit checks.
- Change status.
- Resolve checks.
- View the check details.

To launch the Manual Review dialog box

- 1 Go to Manage > Standards.
- 2 In the Standards view, select the gold standard whose checks you want to manually review and do one of the following:
 - Right-click the selected gold standard and select **Manual Review**.
 - On the taskbar, select **Manual Review**.

- On the Tasks menu, point to Gold Standard Tasks, and then select **Manual Review**.

The Manual Review dialog box is displayed.

To delete a check

- 1 In the Manual Review dialog box, select the check that you want to delete.
- 2 Click the Delete Check(s) icon on the top.

The selected check is deleted.

To edit a check

- 1 In the Manual Review dialog box, select the check that you want to edit and click the Edit Check icon on the top.
- 2 In the Create or Edit Check wizard, make the necessary changes and click **Finish**.

To modify the check status

- 1 In the Manual Review dialog box, select the check whose status you want to change.
- 2 Click **Mark As** and select the status from the list.
- 3 In the Change Status message box, click **Yes**.

The status of the check is modified.

To resolve a check

- 1 In the Manual Review dialog box, select the check that you want to resolve.
- 2 Select the Resolve Check icon on the top.
- 3 In the Resolve Check dialog box, under the Expression(s) list, select the expression that you want to modify.
- 4 In the Value(s) list, select the required value. Click the Update icon.
- 5 Repeat step 3 and 4 to modify any further expressions.
- 6 Click **OK**.

To view the check details

- 1 In the Manual Review dialog box, select the check whose details you want to view.
- 2 To view the check details, click the General, Description, and the Expression(s) tab.

See [“About gold standard”](#) on page 464.

See [“Creating a gold standard”](#) on page 537.

Working with Evaluation Results

The Evaluation Result Details dialog box lets you view the results of an evaluation job run.

When you select the Standard based view option in this dialog box, the following information is available:

- Asset Name
- Failed
- Check in Error
- Manual Review
- Not Applicable
- Passed
- Compliance %
- Risk Score
- Data Collection Date

When you select the Asset based view option in this dialog box, the following information for a check against a specific asset is available:

- Check name
- Status
- Exception
- Risk score
- Confidentiality
- Integrity
- Availability
- Access Complexity
- Access Vector
- Authentication

See [“Check risk attributes”](#) on page 472.

You can also view the evidence details for a failed or an unknown check.

You can perform the following tasks using the Evaluation Result Details dialog box:

- Export the evaluation results.

See [“Exporting the evaluation results”](#) on page 543.

- Request exception on assets.

See [“Requesting an exception using the Evaluation Result Details dialog box”](#) on page 544.

You can export the evaluation results either through the menu bar or the context menu.

About exporting the evaluation results

You can export the evaluation results that are available in the Evaluation Result Details dialog box.

The Evaluation Result Detail dialog box consists of three panes.

The top left pane lets you select the view that you want to display. Based on the view that you select, the relevant information is displayed in the other two panes.

The top right pane displays the summary of the evaluation results in the form of a pie chart.

The bottom pane displays the evaluation results in the form of data columns.

You can export the evaluation result details that are available in the bottom pane in either of the following ways:

- Export results using the menu bar

You can use the menu bar to export the evaluation result details that pertain to both the Standard based view and the Asset based view.

However, for the Asset based view, you can export the results for only one asset at a time using the menu bar option. Also, you cannot export the evidence details information through this option.

You can export the evaluation results in the following formats:

- Excel
- PDF
- Word
- XML

- Export results using the context menu

You can use the context menu that is available when you right-click a particular asset to export all check information. This information includes the evidence details.

Using the context menu options, you can export the evaluation results of multiple assets at a time but you can export only in the Excel format.

Note: You must have Excel installed on your computer to be able to export the evaluation results using the context menu.

The generated report layout is different for both the discussed options.

See [“Exporting the evaluation results”](#) on page 543.

Exporting the evaluation results

You can export the evaluation results that are available in the Evaluation Result Details dialog box.

To launch the Evaluation Result Details dialog box

- 1 Go to Manage > Standards.
- 2 In the table pane of the Standard view, select the standard for which you want to view the evaluation results.
- 3 In the details pane, on the Evaluations tab, click the View Detail icon.

The Evaluation Result Details dialog box is launched.

To export the evaluation results using the menu bar for asset based view

- 1 In the Evaluation Results dialog box, select **Asset based view**.
- 2 Select the asset for which you want to export the result.
- 3 On the File menu, select **Export to** and then select the format in which you want to export.
- 4 In the Export to dialog box, in the file name box, specify the name of the file where you want to save the evaluation results. Click **Save**.

To export the evaluation results using the menu bar for standard based view

- 1 In the Evaluation Results dialog box, select **Standard based view**.
- 2 Select the standard for which you want to export the result.
- 3 On the File menu, select **Export to** and then select the format in which you want to export.
- 4 In the Export to dialog box, in the file name box, specify the name of the file where you want to save the evaluation results. Click **Save**.

To export the evaluation results using the context menu

- 1 In the Evaluation Results dialog box, select **Asset based view**.
- 2 Select the assets for which you want to export the result, right-click, and select **Export Results**.
- 3 In the Save result as dialog box, in the file name box, specify the name of the file where you want to save the evaluation results. Click **Save**.

See [“About exporting the evaluation results”](#) on page 542.

Requesting an exception using the Evaluation Result Details dialog box

You can request an exception through the Evaluation Result Details dialog box.

To launch the Evaluation Result Details dialog box

- 1 Go to Manage > Standards.
- 2 In the table pane of the Standard view, select the standard for which you want to view the evaluation results.
- 3 In the details pane, on the Evaluations tab, click the View Detail icon.

The Evaluation Result Details dialog box is launched.

To request an exception from the standard-based view

- 1 In the Evaluation Result Details dialog box, do either of the following.
 - Select Standard-based view.
 - Select Asset-based view. Go to step 3.
- 2 In the left pane, select a standard or a check . In the lower pane, select the assets that you want to exempt from the selected standard or check. Right-click the selected assets and select **Request Exception**. Go to step 4.
- 3 In the left pane, select an asset. In the lower pane, select the checks for which you want to exempt the selected asset. Right-click the selected checks and select **Request Exception**.
- 4 In the Request Exception wizard, in the Specify Exception Details panel, enter the title, description, and any attachment for the exception.
- 5 Enter the effective date and the expiration date. Click **Next**.
- 6 In the Select Checks and Assets panel, view the selected checks and assets. Click **Next**.

- 7 In the Specify Requestor Information panel, browse to enter the requestor and the requestor group information. Also, enter the requestor email ID and any comments.
- 8 In the Summary panel, view the details that you have specified. Click **Back** to make any changes and click **Finish** to exit the wizard.

About risk score calculation

The Control Compliance Suite follows the Common Vulnerabilities Scoring System (CVSS) version 2 to calculate the risk that is associated with a particular asset.

Control Compliance Suite performs the following calculations in the scoring process:

- Base score calculations
See [“Base score calculation”](#) on page 545.
- Adjusted base score calculations
See [“Adjusted base score calculation”](#) on page 546.
- Risk score calculations
See [“Risk score calculation”](#) on page 546.
- Average risk score calculations
See [“Average risk score calculation”](#) on page 547.

Base score calculation

The base score is calculated using the following attributes that are assigned to each check:

- Confidentiality Impact (C)
- Integrity Impact (I)
- Availability Impact (A)
- Access Vector (Av)
- Access Complexity (Ac)
- Authentication (Au)

See [“Check risk attributes”](#) on page 472.

The formula that is used to calculate the base score is as follows:

Base score = round_to_1_decimal (((0.6*Impact) + (0.4*Exploitability) – 1.5) * f(Impact))

The Impact, Exploitability, and the $f(\text{Impact})$ values in the base score formula are calculated from the check attributes as follows:

$$\text{Impact} = 10.41 * (1 - (1 - \text{Confidentiality Impact}) * (1 - \text{Integrity Impact}) * (1 - \text{Availability Impact}))$$

$$\text{Exploitability} = 20 * (\text{Access Vector}) * (\text{Access Complexity}) * (\text{Authentication})$$

$f(\text{impact}) = 0$ if $\text{Impact} = 0$, $f(\text{impact}) = 1.176$ if Impact is not equal to 0.

The range of the base score values is from 0.0-10.0.

See [“About risk score calculation”](#) on page 545.

Adjusted base score calculation

The Adjusted base score is calculated for an asset and a check pair. This score is calculated using the attributes of the asset and the check.

The following formula is used to calculate the adjusted base score:

$$\text{Adjusted base score} = \text{round_to_1_decimal} (((0.6 * \text{Adjusted Impact}) + (0.4 * \text{Exploitability}) - 1.5) * f(\text{Adjusted Impact}))$$

The Adjusted Impact, Exploitability, and the $f(\text{Adjusted Impact})$ values in the Adjusted base score formula are calculated as follows:

$$\text{Adjusted Impact} = \min(10, 10.41 * (1 - (1 - \text{Confidentiality Impact} * \text{Confidentiality Required}) * (1 - \text{Integrity Impact} * \text{Integrity Required}) * (1 - \text{Availability Impact} * \text{Availability Required})))$$

$$\text{Exploitability} = 20 * \text{Access Vector} * \text{Access Complexity} * \text{Authentication}$$

$f(\text{Adjusted impact}) = 0$ if $\text{Adjusted Impact} = 0$, $f(\text{impact}) = 1.176$ if Impact is not equal to 0.

The Adjusted base score values range from 0.0-10.0

See [“About risk score calculation”](#) on page 545.

Risk score calculation

The risk score term is applicable to an asset as well as to a standard.

For a given standard, the risk score of an asset is defined as the average of the adjusted base score of every failed check in the standard for the specific asset.

$$\text{Risk score} = (\text{Total adjusted base score for all failed checks in the standard}) / (\text{Total number of failed checks})$$

See [“Adjusted base score calculation”](#) on page 546.

For example, consider an asset A and a standard S that contains five checks (C1, C2, C3, C4, and C5). When the asset A is evaluated against the standard S, only checks C4 and C5 are passed. The checks C1, C2, and C3 are failed.

To determine the risk score of asset A, calculate the adjusted base score of every failed check in the standard S with respect to asset A.

Assume that the following values are obtained:

Adjusted base score for check C1 with reference to asset A = 1

Adjusted base score for check C2 with reference to asset A = 2

Adjusted base score for check C3 with reference to asset A = 3

The average of the adjusted base score = $(1 + 2 + 3) / 3 = 2$

This average adjusted base score value is the Risk score of the asset A with reference to a standard S.

See [“About risk score calculation”](#) on page 545.

Average risk score calculation

The Average risk score of an asset is calculated for all the standards against which the asset is evaluated. This score is the average of the individual risk scores of the asset for each of the standards against which the asset is evaluated.

Average risk score = (Total risk score for all standards) / (Total number of standards)

See [“Risk score calculation”](#) on page 546.

For example, consider an asset A that is evaluated against standards S1 and S2. Assume that the risk score of asset A for standard S1 is 3, and the risk score of asset A for standard S2 is 5.

The Average risk score = $(3 + 5) / 2 = 4$

See [“About risk score calculation”](#) on page 545.

Remediating assets

This chapter includes the following topics:

- [About remediation](#)
- [About automatic remediation](#)
- [About manual remediation](#)
- [About closed-loop verification](#)
- [Remediating the assets manually from the evaluation results](#)
- [Remediating the assets automatically](#)

About remediation

Control Compliance Suite (CCS) provides a remediation feature that lets you identify the assets that are not in compliance. The remediation feature helps you resolve the issues that is caused by the non-compliance by sending the notification to the appropriate personnel. Remediation lets you specify the criteria to identify the non-compliant assets and then lets you choose the method of notification for the identified assets. You can either notify the appropriate personnel with a ServiceDesk ticket or with an email. The appropriate personnel resolves the issue and then closes the ticket.

You must configure the remediation settings to create the ServiceDesk tickets and to send email notifications.

See [“Configuring the remediation settings”](#) on page 143.

Control Compliance Suite provides a closed-loop verification feature where the assets that were remediated earlier are reevaluated for compliance. The closed-loop verification feature is available only when you select the ServiceDesk ticket method of notification.

See “[About closed-loop verification](#)” on page 552.

You have the option to remediate the assets automatically or to select the assets to remediate manually.

See “[About automatic remediation](#)” on page 550.

See “[About manual remediation](#)” on page 551.

See “[About remediation](#)” on page 549.

About automatic remediation

Control Compliance Suite provides a feature to remediate the assets that are non-complaint. You can remediate the assets automatically or manually.

To automatically remediate the assets, you can schedule a specific remediation action as a part of the evaluation job or the collection-evaluation-reporting job. Automatic remediation immediately triggers a specified remediation action on the non-compliant assets that satisfy a specified criteria at the end of the job.

The automatic remediation works in the following way:

- Create a new evaluation job or a collection-evaluation-reporting job.
- Specify the evaluation job details.
- Enable automatic remediation and select the asset types.
- Specify remediation criteria.
- Select a remediation action.
- Schedule the evaluation job or the collection-evaluation-reporting job.
- Specify the notification details.

You must configure the remediation settings to create ServiceDesk tickets and to send email notifications for asset remediation. You can configure the settings from **Settings > General > Application Configuration- Remediation Settings**.

Table 11-1 Remediation options

Option	Description
ServiceDesk URL	The hyperlink that is used to create ServiceDesk tickets for asset remediation. <i>http://servername/WebServicename</i>

Table 11-1 Remediation options (*continued*)

Option	Description
CCS Web server	Name of the computer that hosts the Web server . The name can be specified in any format: computer name, IP address, or the fully qualified DNS.
Submitting contact	The email address from which the email notifications are sent for asset remediation.
Maximum assets per ticket	The Maximum number of assets that is included in a remediation ticket for each asset type. The default value is 20. The minimum value is 1.

See [“Configuring the remediation settings”](#) on page 143.

See [“About remediation”](#) on page 549.

See [“Remediating the assets automatically”](#) on page 555.

See [“About manual remediation”](#) on page 551.

About manual remediation

Control Compliance Suite provides a feature to remediate the assets that are non-complaint. You can remediate the assets automatically or manually.

To manually remediate the assets, you can select specific assets from the Evaluation Result Details dialog box and specify the remediation action.

The Evaluation Result Details dialog box can be launched from the Monitor > Evaluation Results view or from the Evaluations tab in the details pane of the Asset System view.

See [“Remediating the assets manually from the evaluation results”](#) on page 553.

The manual remediation works in the following way:

- Navigate to the evaluation results details dialog box.
- Select the remediate task.
- Select the asset types.
- Specify remediation criteria.
- Select remediation action.

- Select the assets to perform the remediation action from the assets that match the criteria.

You must configure the remediation settings to create the ServiceDesk tickets and to send email notifications.

See [“Configuring the remediation settings”](#) on page 143.

See [“About automatic remediation”](#) on page 550.

See [“About remediation”](#) on page 549.

About closed-loop verification

The Control Compliance Suite provides the closed-loop verification feature where the assets once remediated are reevaluated for compliance. The closed-loop verification feature is available only for the ServiceDesk remediation action. The verification is optional and can be enabled at any time.

When an evaluation job identifies an asset that is out of compliance, a ServiceDesk ticket is opened, and then sent to the appropriate personnel to fix the issue. After the ticket is resolved, Control Compliance Suite recollects and reevaluates the asset data based on the original evaluation scope.

You must configure the remediation settings to create ServiceDesk tickets and to send email notifications for asset remediation. You can configure the settings from **Settings > General > Application Configuration- Remediation Settings**.

Table 11-2 Remediation options

Option	Description
ServiceDesk URL	The hyperlink that is used to create ServiceDesk tickets for asset remediation. <i>http://servername/WebServiceName</i>
CCS Web server	Name of the computer that hosts the Web server . The name can be specified in any format: computer name, IP address, or the fully qualified DNS.
Submitting contact	The email address from which the email notifications are sent for asset remediation.
Maximum assets per ticket	The Maximum number of assets that is included in a remediation ticket for each asset type. The default value is 20. The minimum value is 1.

You can view the remediation verification job status from the Manage > Jobs view. You cannot modify, schedule, or delete the job because the job is a system-job.

See [“About remediation”](#) on page 549.

See [“Remediating the assets manually from the evaluation results”](#) on page 553.

See [“Remediating the assets automatically”](#) on page 555.

See [“Configuring the remediation settings”](#) on page 143.

Remediating the assets manually from the evaluation results

You can remediate the assets using the Evaluation Result Details dialog box. Manual remediation involves remediating the assets after you obtain the evaluation results..

After you evaluate the assets against standards, you receive the evaluation results and the risk score. You can now specify the criteria to identify the assets that require remediation and then take action to remediate. You can further choose specific assets from the list of assets that match the specified criteria. Remediation occurs only on the selected assets. The criteria can be the risk score or by compliance score or a combination of both the scores. You can choose to send email notifications or open service desk tickets for the assets that require remediation.

To launch the Evaluation Result Details dialog box

- 1 Go to Manage > Standards.
- 2 In the table pane of the Standards view, select the standard for which you want to view the evaluation results.
- 3 In the details pane, on the **Evaluations** tab, click the **View Detail** icon.
or
- 4 Go to Monitor > Evaluation Results.

To remediate the assets manually

- 1 In the **Evaluation Result Details** dialog box, click **Remediation Ticketing**.
- 2 In the **Select Asset Type for Remediation Ticketing** panel, select the asset types that correspond to the assets that were evaluated and click **Next**.

- 3 In the **Specify Remediation Ticketing Criteria** panel, specify the combination of risk score and compliance score that you want to use to identify the assets for remediation.

You can select **Apply to all standards** if you want to apply the specified remediation criteria to all the standards for remediation.

If you do not select **Apply to all standards**, you must specify the remediation ticketing criteria for each standard.

Click **Next**.

- 4 In the **Select Remediation Ticket Type** panel, select one of the following:
 - Create an email notification.
This option lets you create an email notification that you want to send for notification.
 - Create a ServiceDesk ticket.
This action opens a ServiceDesk ticket request directly at the end of the evaluation results for the non-compliant assets.
You can choose the **Enable closed-loop verification** option. With the closed-loop verification, the non-compliant assets data is re-evaluated after the ServiceDesk request is met.
See [“About closed-loop verification”](#) on page 552.

Click **Next**.

- 5 If you choose to send an email notification as a remediation action, specify the message that you want to send as an email notification in the **Configure Notification Details for Remediation Ticketing** panel. Click **Next**.

If you select **Consolidate multiple assets in a single ticket/email**, a single notification is sent that includes all the non-compliant assets.

You can check **Make this the default Email Notification template** if you want to use the same message for all the ServiceDesk ticket requests.

- 6 If you choose to create a ServiceDesk ticket as a remediation action, specify the message that you want to send as a ServiceDesk request in the **Configure Service Desk Ticket** panel. Click **Next**.

If you select **Consolidate multiple assets in a single ticket/email**, a single ServiceDesk ticket is generated that includes all the non-compliant assets.

You can check **Make this the default Service Desk Ticket template** if you want to use the same message for all the ServiceDesk ticket requests.

- 7 In the **Select Assets for Remediation Ticketing** panel, select specific assets from the list of assets that is displayed in the panel. The list contains the assets that match the specified remediation criteria. You can further select specific assets from the filtered assets.
Click **Next**.
- 8 In the **Summary** panel, view the details that you specified. Click **Back** to make any changes and click **Finish** to exit the

Remediating the assets automatically

You can remediate the assets as a part of the evaluation or the collection-evaluation-reporting job. Automatic remediation is scheduling the remediation of assets, as a sequential step, in the evaluation job..

You can configure the remediation details in the Create or Edit Evaluation Job Wizard and in the Create or Edit Collection-Evaluation-Reporting Job Wizard.

The panels to configure the remediation details in the Create or Edit Evaluation Job wizard appear after the **Specify Notification Details** panel.

You can also remediate the assets from the Assets view.

See [“Running an evaluation job from the Asset System view”](#) on page 311.

To remediate the assets automatically from the Standards view

- 1 Go to Manage > Standards.
- 2 Right-click the standard that you want to evaluate and select **Run Evaluation** or **Run Collection-Evaluation-Reporting** according to your requirement.

Provide the necessary information until you reach the **Select Asset Type for Remediation Ticketing** panel.

- 3 In the **Select Asset Type for Remediation Ticketing** panel, check the **Enable Automatic Remediation Ticketing** option to configure the automatic remediation details.

Select the asset types that correspond to the assets that were evaluated and then click **Next**.

- 4 In the **Specify Remediation Ticketing Criteria** panel, specify the combination of risk score and compliance score that you want to use to identify the assets for remediation.

You can select **Apply to all standards** if you want to apply the specified remediation criteria to all the standards for remediation.

If you do not select **Apply to all standards**, you must specify the remediation ticketing criteria for each standard.

Click **Next**.

- 5 In the **Select Remediation Ticket Type** panel, select one of the following:
 - Create an email notification.
This option lets you create an email notification that you want to send for notification.
 - Create a ServiceDesk ticket.
This action opens a ServiceDesk ticket request directly at the end of the evaluation results for the non-compliant assets.
You can choose the **Enable closed-loop verification** option. With the closed-loop verification, the non-compliant assets data is re-evaluated after the ServiceDesk request is met.
See [“About closed-loop verification”](#) on page 552.

Click **Next**.

- 6 If you choose to send an email notification as a remediation action, specify the message that you want to send as an email notification in the **Configure Notification Details for Remediation Ticketing** panel. Click **Next**.

If you select **Consolidate multiple assets in a single ticket/email**, a single notification is sent that includes all the non-compliant assets.

You can check **Make this the default Email Notification template** if you want to use the same message for all the ServiceDesk ticket requests.

- 7 If you choose to create a ServiceDesk ticket as a remediation action, specify the message that you want to send as a ServiceDesk request in the **Configure Service Desk Ticket** panel. Click **Next**.

If you select **Consolidate multiple assets in a single ticket/email**, a single ServiceDesk ticket is generated that includes all the non-compliant assets.

You can check **Make this the default Service Desk Ticket template** if you want to use the same message for all the ServiceDesk ticket requests.

- 8 Proceed with the Create or Edit Evaluation Job Wizard or the Create or Edit Collection-Evaluation-Reporting Job Wizard.

Managing baselines

This chapter includes the following topics:

- [About baseline](#)
- [About the baselines workflow](#)
- [About the Baselines view](#)
- [About setting tasks to roles of baselines](#)
- [Creating a baseline job](#)
- [Viewing the comparison results in the Baselines view](#)
- [Exporting the comparison results](#)
- [Deleting the baseline record](#)

About baseline

A baseline is a reference data. You use the baseline feature to compare the asset data with a previous reference data or a previous reference job. In the Control Compliance Suite, when you run a baseline job, the records in the newer dataset are compared against the records in the older dataset.

Baselines let you compare the assets either with an asset that is marked as baseline or with a job-run that is marked as baseline.

Control Compliance Suite supports the following types of baselines:

Asset-based baseline

Control Compliance Suite lets you mark an asset as a baseline. You collect the data for an asset and use that data as a baseline to compare or monitor the assets in the further job runs.

The asset-based baseline lets you compare multiple assets of the same type with a single reference asset periodically.

Job-based baseline

Control Compliance Suite lets you mark the entire data that is collected by the baseline job as a baseline.

The job-based baseline serves the purpose of monitoring the same set of assets. When you create a baseline job and select a job-based baseline to compare against, the entire result data for the baseline job is compared.

See [“Creating a baseline job”](#) on page 560.

See [“Viewing the comparison results in the Baselines view”](#) on page 561.

About the baselines workflow

The end-to-end sequence of using the baselines is as follows:

- Create a primary baseline job to mark the job run or an asset as a baseline.
If you use the baseline feature for the first time, you create a baseline job and use the same job-run as a baseline. Or you create a baseline job and mark an asset from the job as a baseline.
See [“Creating a baseline job”](#) on page 560.
- Create subsequent baseline jobs to compare the results or the assets with the created baselines.
You need to create baselines jobs to compare the assets with a job run or an asset that is marked as baseline.
- View the comparison results
You can view the results of the baseline job in the form of comparison with the baseline.
See [“Viewing the comparison results in the Baselines view”](#) on page 561.

About the Baselines view

The baseline management view lets you manage the baselines in the Control Compliance Suite.

Note: To view the Baselines view, you should assign the View Baselines task explicitly to the user to manage the baselines.

You can access the baseline management view from Manage > Baseline.

You can perform the following tasks from the baseline management view:

- Delete a baseline.
See [“Deleting the baseline record”](#) on page 563.
 - View comparison results.
See [“Viewing the comparison results in the Baselines view”](#) on page 561.
- See [“Creating a baseline job”](#) on page 560.

About setting tasks to roles of baselines

To run the baselines job from the Jobs view, you must create a custom role that is configured to perform specific tasks. In Control Compliance Suite, you can create a custom role for the baselines system through the Settings >Role view of the console.

See [“Creating a custom role”](#) on page 92.

The following are the required baseline tasks that should be assigned to the user with the custom role for baselines:

- Manage baseline
- View baseline
- Compare baseline
- View comparison results

The following dependency tasks should be assigned to the user with the custom role for baselines:

- Manage jobs
- View assets
- View all jobs

See [“Configuring roles and permissions ”](#) on page 78.

Creating a baseline job

You create a baseline job for one of the following purposes:

- To mark the job or an asset as a baseline.
If you use the baseline feature for the first time, you create a baseline job and use the same job-run as a baseline. Or you create a baseline job and mark an asset from the job as a baseline.
- To compare the records with the previous baselines.
You need to create baselines jobs to compare the assets with a job run or an asset that is marked as baseline.

You can create the baseline job for the assets for which the data collection and the evaluation is complete.

Note: To view the Baselines view, you must assign the View Baselines task explicitly to the user to manage the baselines.

To create a baseline job

- 1 Go to Monitor > Jobs and from the Common Tasks select, **Baseline Job**.
- 2 In the **Specify Job Name and Description** panel, type the name and the description for the baseline job and click **Next**.
- 3 In the **Compare with Baseline** panel do one of the following:
 - If you create the baseline job for the first time, click **Next**.
 - If you already have a baseline created, select **Compare with baseline** and select a baseline from the list.
Click **Next** and go to step [5](#)
- 4 In the **Select Platform, Asset Type, and Data Collector** panel, select the platform, the asset type, and the data collector for which the baseline data should be collected.
- 5 In the **Add Asset Scope** panel, browse through the available assets and add the assets to the baseline job.

You can select one or more assets of the selected asset type as scope.
Click **Next**.
- 6 In the **Select Fields** panel, select the fields for the asset type.

The fields that you select in this panel are used to collect the relevant data for the selected asset type.
Click **Next**.

- 7 In the Specify Asset Field Filters panel you can do one of the following:
 - Use the Edit Selected Statement option to edit the existing filter and click **Next**. Go to step 9
 - Use the Delete Selected Statement option to delete the existing filter and click **Next**. Go to step 9
 - Use the Add Statement option to create a new statement.
The Add Statement option displays the Create Filter Statement dialog box. Go to step 9
- 8 In the Create Filter Statement dialog use the parameter type and the conditions to create a filter statement.
See [“Examples of asset filters”](#) on page 242.
See [“Filter statement operators”](#) on page 243.
- 9 In the Schedule panel, select any one of the following:
 - If you want to run the job after the wizard closes, check **Run Now**.
 - If you want to run the job at a specified interval, check **Run Periodically** and enter the following information:
 - In the Start On box, enter the start date and time to run the job.
 - Under Run periodically options, if you want to run the job only one time, select **Run Once**. If you want to run the job after specific days, select the number of days in the Run Every Day list box. Click **Next**.
- 10 In the Specify Notification Details panel, if you want to send the notification of job completion or job failure, do the following:
 - Type the subject and message of the notification mail.
 - Type the email ID of the sender and the receiver.
- 11 In the Summary panel, review the configurations for the baseline job and click **Finish**.
You can go back to the previous panels and edit the configurations any time.
You can go to the Monitor > Jobs view to monitor the current status of the job.

Viewing the comparison results in the Baselines view

You view the comparison results that are gathered from the baselines job in the Manage > Baselines view.

You can view the comparison results of the baseline job runs that are completed.
You can view the comparison results of only one job-run at a time.

To view the comparison results in the Baselines view:

- 1 Go to Manage > Baselines.
- 2 In the table pane select a job run for which you want to view the comparison results.
- 3 From the taskbar , select **View Comparison Results**.
- 4 In the View Comparison Results dialog box, view the following details:

Number of Assets	Displays the total number of assets that are compared.
Search	Lets you search a particular asset. Note: If you search an asset immediately after you launch the View Comparison Results dialog box, only the asset name are searched. After you perform any action in the View Comparison Results dialog box, the search applies to the entire baselined data.
Details	Displays the list of changed and unchanged assets.

See [“Creating a baseline job”](#) on page 560.

Exporting the comparison results

You can export the comparison results to the following formats:

- Excel
- Word
- PDF
- XML
- CSV

To export the comparison results

- 1 In the **View Comparison Results** dialog box, go to File > Menu > Export to.
- 2 Select the format to which you want to export the comparison results.
- 3 In the Save In dialog box, type the file name by which the comparison results must be saved.

If you export the comparison results in the XML format and if the results contain linefeeds or other XML-specific characters , then use the IE or other XML rendering browser to view the results. In this case, the multi-valued fields are separated by space. In case, you use the default viewer as notepad the XML contains special characters that indicate newline.

Deleting the baseline record

You can delete the baseline from the Manage > Baselines view.

To delete the baseline

- 1 Go to Manage > Baselines.
- 2 Right-click the baseline record that you want to delete and select **Delete**.

Managing tags

This chapter includes the following topics:

- [About tags](#)
- [About the Tags view](#)
- [Creating a new tag](#)
- [Creating a new tag category](#)
- [Editing a tag category](#)
- [Deleting a tag category](#)
- [Moving a tag](#)
- [Deleting a tag](#)
- [Renaming a tag](#)

About tags

Control Compliance Suite provides a method to tag and identify the business objects such as the assets, standards, the exceptions, the policies with respect to their severity, confidentiality, utility or any other area.

Tagging the assets is a way to apply meta-information to an asset. Tags help you identify the assets in some context that might prove helpful to determine the value of the asset. You can also use the tags to filter the assets.

For example, you can create a tag that is called SOX and associate it with a relevant asset.

See [“Creating a new tag category”](#) on page 566.

See [“Creating a new tag”](#) on page 566.

About the Tags view

You can access the tags management view from **Manage > Tags**.

The tags management view lets you perform the following tasks:

- Create Tag
- Rename Tag
- Delete Tags
- Move Tags

The tag categories are listed in the tree pane under the Tags node. You can create or edit a tag category using the right-click option from the tree pane. When you select a tag category in the tree pane, a list of tags under the selected category appears in the table pane.

See [“About tags”](#) on page 565.

Creating a new tag

You can access the Create Tag dialog box from **Manage > Tags > Create Tag**.

To create a new tag

- 1 Go to **Manage > Tags**.
- 2 In the tables pane, right-click the tag category under which you want to create a new tag and click **CreateTag**.
- 3 In the Create Tag dialog box, type the name of the new tag that should be created.
- 4 Click **OK**.

See [“Creating a new tag category”](#) on page 566.

See [“Renaming a tag”](#) on page 568.

See [“Moving a tag”](#) on page 568.

See [“Deleting a tag”](#) on page 568.

Creating a new tag category

You can create a new tag category from the tree pane.

To create a tag category

- 1 Right-click the Tags node in the tree pane.
- 2 Select **Create Tag Category**.
- 3 Type the name of the tag in the Name field.
- 4 Type the description for the tag category in the Description field.
- 5 Click **OK**.

See [“Creating a new tag”](#) on page 566.

See [“Editing a tag category”](#) on page 567.

See [“Deleting a tag category”](#) on page 567.

Editing a tag category

You can edit an existing tag category from the tree pane.

To edit a tag category

- 1 Right-click the category that should be edited under the Tags node in the tree pane.
- 2 Select **Edit Tag Category**.
- 3 Edit the Name and the Description fields in the Edit Tag Category dialog box.
- 4 Click **OK**.

See [“Creating a new tag category”](#) on page 566.

See [“Deleting a tag category”](#) on page 567.

Deleting a tag category

You can delete a tag category using the option in the menu bar.

To delete a tag

- 1 Select a tag category that you want to delete.
- 2 Select **Delete tag category** from the menu bar.
- 3 Select **Yes** in the confirmation dialog box to delete the tag.

See [“Creating a new tag category”](#) on page 566.

See [“Editing a tag category”](#) on page 567.

Moving a tag

You can move a tag using the option from the menu bar.

To move a tag

- 1 Select a tag that you want to move.
- 2 Select **Move Tag** from the Common Tasks .
- 3 In the Move selected tags to dialog box, select the tag category to which you want to move the tags.
- 4 Click **OK**.

See [“Creating a new tag”](#) on page 566.

See [“Renaming a tag”](#) on page 568.

See [“Deleting a tag”](#) on page 568.

Deleting a tag

You can delete a tag using the option in the menu bar.

To delete a tag

- 1 Select a tag that you want to delete.
- 2 Select **Delete tag** from the menu bar.
- 3 Select **Yes** in the confirmation dialog box to delete the tag.

See [“Creating a new tag”](#) on page 566.

See [“Renaming a tag”](#) on page 568.

See [“Moving a tag”](#) on page 568.

Renaming a tag

You can access the Rename Tag dialog from Manage > Tags > Rename Tags.

To rename a tag

- 1 Go to Manage > Tags.
- 2 In the tables pane, right-click the tag that you want to rename and select **Rename tag**.
- 3 In the Rename Tags dialog box, type a new name for the selected tag.
- 4 Click **OK**.

See [“Creating a new tag”](#) on page 566.

See [“Moving a tag”](#) on page 568.

See [“Deleting a tag”](#) on page 568.

Managing policies

This chapter includes the following topics:

- [About Policies](#)
- [About the policies management view](#)
- [Working with policies](#)
- [Reviewing and approving policies](#)
- [About mapping policies](#)
- [Publishing and unpublishing policies](#)
- [Responding to policies on the Web Portal](#)[Responding to policies in the Web Console](#)
- [Managing clarifications](#)

About Policies

Using the policies features of the Control Compliance Suite (CCS), you can manage, publish, and track your policies across the organization. You can also collect evidence of due care of policy compliance.

Policies are mapped to the control statements that in turn are mapped to regulations and frameworks. Mapping helps you to see the existing gaps in the current policies of your organization. These gaps can exist between your current policies and the mandates with which your organization must comply. Mapping also helps you to meet the requirements of the mandates with which the organization must comply.

About the policy life cycle

Policies are rules established by an organization that are designed to guide their employees. In an IT environment, policies are used to guide the decisions that relate to the management of the IT infrastructure. Policies have an arbitrary hierarchy and may map to one or many control statements.

A policy with no control statements can indicate an unimportant policy or a policy where compliance cannot be monitored. A control statement with no policy can indicate a gap showing noncompliance with one or more regulations.

The following tasks are typical of the life cycle of a policy:

- Create a new policy.
See [“Creating a new policy”](#) on page 579.
- Review the policy.
See [“Reviewing a policy”](#) on page 585.
- Approve the policy.
See [“Approving a policy”](#) on page 587.
- Publish the policy.
See [“Publishing a policy”](#) on page 587.
- Accept or decline the policy.
See [“Accepting or declining a policy”](#) on page 589.
- Manage clarifications.
See [“Managing clarification requests”](#) on page 593.

About policy status

Every policy has a status that is assigned to it at all times.

The status is one of the following:

Draft	<p>A policy that is authored in its initial form. The policy has not been reviewed. The policy may or may not be complete in the view of the author.</p> <p>Also, a policy that has been reviewed but which has change requests, or a policy that has been unpublished.</p> <p>Policies can only be changed while in Draft status.</p>
In Review	<p>A policy in its first draft that is considered complete by the author. The policy is automatically submitted to the policy reviewers for their comments. Reviewer comments and change requests can be made while the policy is In Review.</p>

Awaiting Approval	<p>A policy that may or may not have reviewer comments. If a policy does not have change requests from reviewers, the status changes to Awaiting Approval. The status changes automatically when the review deadline that was set during the policy creation passes.</p> <p>If a policy does have change requests, its status reverts automatically to Draft when the review deadline passes. After the change requests are addressed, the author can submit it for review again.</p>
Policy Approved	<p>A policy is Approved when the author has incorporated all the reviewer comments and is completely satisfied. A policy that is marked as Approved is ready for publication.</p>
Published	<p>A policy administrator with rights to the policy can publish an approved policy. A published policy is accessible to members of the audience from the Control Compliance Suite Web portal .</p>
Archived	<p>A policy that is archived and no longer in effect. An archived policy is not visible in the Policy view. Inactive policies are stored in the database.</p>

About audiences

The audience consists of a group of people within an organization. The audience members are selected when a user creates a policy. Audience members become aware of the published policies applicable to them when they log on to the Control Compliance Suite Web Portal home page. The security manager or security analyst is made aware of the user acceptance status of the policy. The manager or analyst responds to any exception request or clarification request that is submitted for the policy.

The users and the groups that are assigned to the **Guest User** role with permission to a policy make up the policy audience. The audience can consist of one or more users and groups.

You can use the Roles feature and Permission Management feature to assign users to the audience of a policy.

Note: Only a user who is assigned to the CCS Administrator role can assign roles and permissions.

See [“Configuring roles and permissions”](#) on page 78.

See [“Adding users and groups to a role”](#) on page 89.

See [“Assigning permissions from the Roles view”](#) on page 91.

See [“Assigning permissions from the Permission Management view”](#) on page 95.

About regulations

Regulations are published government mandates such as HIPAA, Sarbanes-Oxley, or GLBA. These regulations describe the business functions and security functions that must be performed, usually with limited information on the implementation details.

The following are some of the regulations for which predefined policies exist:

HIPAA	Health Insurance Portability and Accountability Act
FISMA	Federal Information Security Management Act
GLBA	Gramm-Leach-Bliley Act
SOX	Sarbanes-Oxley Act of 2002

About frameworks

Frameworks are published best practices such as COBIT, COSO, and the ISO series. These frameworks describe implementation details. An example of such details is that the password policy should contain entries for length, complexity, and rotation.

The following are some of the frameworks for which predefined policies exist:

COBIT	Control Objectives for Information and related Technology
NIST	National Institute of Standards and Technology
ISO	International Standards Organization
COSO	Committee of Sponsoring Organizations of the Treadway Commission
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission

About control statements

A control statement is a concise statement of a discrete portion of a regulation or framework. Because regulations and frameworks have large areas of overlap, the control statements reduce repetition by stating each portion a single time. For example, where differences exist between regulation or framework statement requirements, a single control statement can exist to which each of the entries is mapped. Since both the regulation and the framework are mapped to the single control statement, the single control statement meets the requirements of both.

A control statement is mapped when it is linked to a policy. Control statements are also mapped to mandates. Through the control statement, the policy is indirectly linked to the regulation and the framework.

About policy versioning

A policy version is independent of its position in the policy tree structure.

The version numbers are assigned and used based on the following policy states:

Create	When a policy is created, its status is Draft and the policy is assigned version number 1. A child policy is created with version number 1. A parent may have a higher version number than a child.
Review	When a policy is reviewed, the policy reviewer comments are specific to the current policy and the policy version. The reviewers are not allowed to edit their comments from the previous versions of the policy.
Publish	When a policy is published, it is published with the current version number.
Unpublish	When a published policy is recalled or saved to update, the policy is automatically unpublished. When an unpublished policy is saved, the saved policy is marked as Draft and the version automatically increments by 1. For example, if version 2 of a policy is unpublished, the new version number is 3.
Awareness and clarification	When a user accepts, declines, or asks for a clarification, the task is specific to the current version.
Exceptions	An exception to a policy is not specific to the version. For example, if an exception is approved for version 1 of a policy, then the same exception holds for version 2. The exception remains in place as long as the exception has not expired.

About the policies management view

The policies management view lets you manage the policies in the Control Compliance Suite. The policies management view displays a hierarchical tree structure of all policies. The policies management view lets you view the attributes of a selected policy or filter the displayed policies.

You can access the policies management view from Manage > Policies.

The policies management view contains the following panes:

Tree pane	<p>This pane appears on the left side of the console window under the navigation bar.</p> <p>This pane displays a hierarchical, folder-based structure of the policies that are stored in the CCS directory.</p>
Filter by pane	<p>This pane appears in the lower left side of the console window under the tree pane.</p> <p>You can specify filters in this pane so that only the required policies are displayed in the table pane.</p>
Table pane	<p>The table pane appears in the right side of the console window under the taskbar.</p> <p>This pane displays the policies.</p>
Details pane	<p>The details pane appears in the lower-right side of the console window under the table pane.</p> <p>This pane displays the details of the policy that is selected in the details pane.</p>

You can perform the following tasks from the policies management view:

- Create a new policy.
- Import a Microsoft Word document as the basis for a new policy.
- View the details of an existing policy.
- Edit a policy.
- Copy a policy.
- Move a policy.
- Rename a policy.
- Delete a policy.
- Submit a policy for review.
- Submit a policy for approval.
- Approve a policy.
- Publish a policy.
- Unpublish a policy.

The details pane of the policies management view lets you review and edit policies.

The details pane includes the following tabs:

General	The General tab includes the policy name, version, author, status, review by date, expiration date, priority level, and rationale.
Content	The Content tab contains the text of the policy. You can use formatting tools to edit the policy or edit the policy with HTML tags. You can also preview how the policy appears in a Web browser.
Statements	The Statements tab displays any control statements that are mapped to the policy. Control statements are mapped to the policy in the Content Studio tool. The Statements tab contains a link that lets you open the Content Studio.
Audience	The Audience tab lists the users assigned the Guest User role in Control Compliance Suite that have permissions to the policy.
Approvers	The Approvers tab lists the users who are assigned the Policy Approver role who also have permission to this policy. A policy must have at least one assigned approver. If no approver is assigned, the policy can never be set to In Review . Only approved policies can be published.
Reviewers	The Reviewers tab lists the users who are assigned to the Policy Reviewer role who also have permission to this policy. A policy must have at least one assigned reviewer. If no reviewer is assigned, the policy can never be set to In Review .
Reviewer Comments	The Reviewer Comments tab lets reviewers review the policy and create comments or change requests for the policy.
Clarifications	<p>The Clarifications tab lets you review and respond to clarification requests for the policy by an audience member.</p> <p>The Clarifications tab lists all the clarification requests that are submitted by the end users. By default, the requests are grouped based on status: Open or Closed. Use the sort, group, or filter feature to quickly access a specific policy clarification.</p>
Tags	The Tags tab lets you review the tags that are assigned to the policy. You can also add tags to the policy and remove tags from the policy using this tab.
Exceptions	<p>The Exceptions tab lists any exceptions that are granted to this policy. Use the Exceptions Management view to manage these exceptions.</p> <p>See “About exceptions” on page 428.</p> <p>See “About the exception management system” on page 428.</p>

Note: Only a user who is assigned to the CCS Administrator role can assign roles and permissions.

About editing policies

Before a policy has been set to **In Review**, you can continue to make changes to the policy. You can make changes to all aspects of the policy, including the name and the content. Only the author name and the policy version cannot be changed manually.

After a policy has been approved or published, you can issue clarifications to a policy without additional review and approval.

To make changes to a published policy, you must unpublish it. You then make changes to the new policy version. The changed policy reverts to draft status and the version number increments.

All changes to an approved or published policy require the policy to be reviewed again, then approved and published.

About searching policies

The **policies** view contains the tools that help you locate specific policies.

In the top right corner of the view, the **Search** box lets you search for policy names.

In the bottom left, the filter pane lets you filter the policies displayed based on a number of criteria.

Working with policies

You must set up the policies that suit the needs of your enterprise. The Policies view lets you manage policies and their relationships.

You can do the following:

- Create a policy.
See [“Creating a new policy”](#) on page 579.
- Import a Microsoft Word file as a policy.
See [“Importing a Word policy”](#) on page 581.
- Move a policy.
See [“Moving a policy”](#) on page 582.
- Delete a policy.
See [“Deleting a policy”](#) on page 583.
- Select the policy audience.
See [“About selecting the policy audience”](#) on page 584.

Creating a new policy

You can create a policy from the start or copy from an existing policy template.

The asterisks (*) indicate that the fields are required.

To create a new policy

- 1 In the Policies view, navigate in the tree pane and click the folder where you want to store the new policy.

You can only create a policy in a folder where you have appropriate rights.

- 2 Do one of the following:

- Click **New Policy**.
- Click **Policy Tasks > New Policy**.
- Right-click the folder, then click **New Policy**.

- 3 In the **Create New Policy** panel, do one of the following:

- Click **Create a New Policy** and then click **Next**.
- Click **Create a Policy Based on a Predefined Policy**, then click the policy to base the new policy on and then click **Next**.

- 4 In the **Specify Policy Properties** panel, enter the following information and then click **Next**:

Policy Name	The name of the new policy. A name is required.
Review By Date	The date by which reviewers of the policy must submit comments. The default review by date is calculated based on the value that is set in System Management > General Settings > Policies Settings. You can select a different date.
Expiration Date	The date the policy expires and is no longer valid. The default expiration date is calculated based on the value that is set in System Management > General Settings > Policies Settings. You can select a different date.
Priority Level	The importance you assign to the policy. The default priority is low.
Allow User Response	<p>When this option is checked, the policy can be published to the Control Compliance Suite Web Portal. Users can then read and respond to the policy.</p> <p>When unchecked, the policy can be published to the Web Portal. Users can request clarifications, but cannot accept or decline the policy or request an exception from the policy. From the user perspective, the policy is read-only.</p>
Rationale	The reason for the existence of the new policy. The rationale can be as comprehensive as your needs require. A rationale is required.

- 5 In the **Add Policy Content** panel, type the policy. You can use the formatting toolbars or click **HTML** to edit the HTML code manually.

See [“Getting started with the asset system”](#) on page 193.

Click **Next**.

- 6 In the **Choose Policy Targets** panel, locate the asset folders that are the targets of the policy. Click the targets and click **Add** or **Add All** to add the targets to the **Selected Items** list. Click **Next**.
- 7 In the **Summary** panel, review the properties of the new policy. If you need to change any properties, click **Back**. If you want to map control statements to the policy, ensure that **Launch Content Studio to map Control Statements** is checked.

See [“Mapping policies to control statements”](#) on page 688.

- 8 In the **Summary** panel, click **Finish**.

Importing a Word policy

You can import a Microsoft Word .doc file as a Control Compliance Suite policy. When you import a Word document, the name of the source Word document is assigned to the new Policy. You can manually change this name.

If the policy name already exists as a policy, the Control Compliance Suite follows rules to determine how to handle the new policy. If the policy status is Draft or In Review, you have a choice to overwrite the existing policy or to create a new policy. If the policy status is Reviewed, Approved, or Published, a new policy is created with a different name.

The new policy name includes the existing policy name and one of the following:

- Folder name of the Word document
- A random number
- Current date and time

The text of the Word document is set as the content of the new policy.

When you import one or more Word documents, the following properties are explicitly set for the newly imported policies:

Policy name	Same as the source Word document name
Policy content	Contents of the source Word document
Policy status	Draft

All other properties have their default values.

Before approving or publishing the new policy, you should make any necessary changes to the policy.

You must install Microsoft Word and the Microsoft Office Primary Interop Assembly on the same computer as your CCS client to import Word documents.

The Microsoft Office Primary Interop Assembly may or may not be installed, depending on the version of Microsoft Office and how it is installed.

Use one of the following URLs to download the correct version of the Microsoft Office Primary Interop Assembly for your Office version:

Office 2003 <http://www.microsoft.com/downloads/details.aspx?familyid=39a983a-ac14-4125-8ba0-d36d67e0f4ad&displaylang=en>

Office XP <http://www.microsoft.com/downloads/details.aspx?FamilyId=C41BD61E-3060-4F71-A6B4-01FEBA508E52&displaylang=en>

Note: Microsoft Office 2007 is not supported.

To import a Word policy

- 1 In the Policies view, navigate in the tree pane and click the folder where you want to store the new policy.
- 2 Do one of the following:
 - Click **Import Policies**.
 - Click **Policy Tasks > Import Policies**.
 - Right-click a folder in the tree, then click **Import Policies**.
- 3 Click **Next**.
- 4 In the **Select Word Documents** panel, click **Add**.
- 5 In the **Select Word Documents to Import** dialog box, click the Word .doc file to import, then click **Open**.
- 6 Repeat step 4 and step 5 to add additional Word files to import.
Click **Next** to continue when all files are added.
- 7 In the **Select a Target Folder** panel, click the folder into which the imported files should be saved, then click **Next**.
- 8 In the **Input Rationale** panel, enter the rationale for the imported policies.
Click **Next**.
- 9 In the **Completing the Import Policies Wizard** panel, review the choices you have made, then click **Finish**.

Moving a policy

When you create a policy, you may want to move it to another folder at a later time. To move a policy, you can use the move task or copy and paste the policy.

To move a policy

- 1 In the Policies view, do one of the following:
 - Right-click any policy and click **Move**.
 - In the table pane, click the check box beside one or more policies, then click **Policy Tasks > Move Policies**.
- 2 In the **Move Policies** dialog box, click the folder where the policies should move to, then click **OK**.

To copy and paste a policy

- 1 In the Policies view, right-click any policy and click **Copy**.
- 2 In the **Tree** pane, click the folder where you want to paste the policy.
- 3 In the Policies view, in the **Details** pane, right-click then click **Paste**.

Deleting a policy

If you decide not to proceed with a draft policy you may delete the policy.

To delete a policy

- 1 In the Policies view, do one of the following:
 - Right-click any policy in the Draft state and click **Delete Policies**.
 - In the table pane, click the check box beside one or more policies in the Draft state, then click **Policy Tasks > Delete Policies**.
- 2 In the **Delete Policies** dialog box, click **Yes**.

Submitting a policy for review

After you have created a policy and it is ready for review, it must be submitted to the policy reviewers.

Note: Only the policies that you have permissions to in the folder selected in the tree pane can be submitted for review.

To submit a policy for review

- 1 In the Policies view, click a folder in the tree pane, and do one of the following:
 - Click **Submit Policy For Review**
 - Click **Workflow Tasks > Submit Policy For Review**
 - Right-click an object in the tree, then click **Submit Policy For Review**
- 2 In the **Submit Policy For Review** dialog box, click the check box beside the name of the policies to submit for review, then click **Submit**.

Submitting a policy for approval

After a policy has been reviewed, the policy is submitted for approval automatically when the review period expires. If you choose, you can manually submit the policy for approval after all reviewers have commented on it.

Note: Only the policies that you have permissions to in the folder selected in the tree pane can be submitted for approval.

To submit a policy for approval

- 1 In the Policies view, click a folder in the tree pane, and do one of the following:
 - Click a policy in the details pane and then click **Submit Policy For Approval**
 - Click **Workflow Tasks > Submit Policy For Approval**
 - Right-click an object in the tree, then click **Submit Policy For Approval**
- 2 In the **Submit Policy For Approval** dialog box, click the check box beside the name of the policies to submit for review, then click **Submit**.

About selecting the policy audience

The users and the groups that are assigned to the **Guest User** role with permission to a policy make up the policy audience. The audience can consist of one or more users and groups.

You use the Roles feature and Permission Management feature to assign users to the audience of a policy.

Note: Only a user that is assigned to the CCS Administrator role can assign roles and permissions.

See [“Configuring roles and permissions”](#) on page 78.

See [“Adding users and groups to a role”](#) on page 89.

See [“Assigning permissions from the Roles view”](#) on page 91.

See [“Assigning permissions from the Permission Management view”](#) on page 95.

Reviewing and approving policies

Before it can be published, experts must review any policy for fitness, suitability, legal aspects, relevance, and other matters. Policy review lets you obtain those comments and retain the feedback through the life of the policy.

About policy review

The policy review feature assists reviewers by providing a central location to view and comment about the policies. Reviewers can also view other reviewer comments and refer to comments that are made in the previous versions of a policy.

When a policy is ready for review, the policy administrator marks the status as In Review. The Control Compliance Suite mails information about the policy to the reviewers. The reviewers view and comment about a policy using the Reviewer Comments tab of the policy details. When the review period expires, the policy state automatically changes. The policy administrator can also change the state manually if all reviewers have reviewed the policy. If a reviewer submitted a change request, the state reverts to **Draft**. The policy author views all the comments and updates the policy if a reviewer submitted a change request. After the author makes any required change, the author can submit the policy for review again.

If no change request was submitted, the status changes to "Pending Approval."

After a policy is approved or published or when the Review By date has passed, review comments are not editable. The original comments become part of the policy history. The policy history provides a record of the comments that led to a particular version of the policy.

Reviewing a policy

To review a policy, you must have the required roles and permissions, and the policy status must be marked as In Review. After a policy is approved or published or when the Review By date has passed, review comments are not editable.

Note: Only a user that is assigned to the CCS Administrator role can assign roles and permissions.

To review a policy

- 1 In the Policies view, select the policy to review.
- 2 In the details pane, click **Comments**.
- 3 In the **Comments** pane, click **Add Comment**.
- 4 In the **Reviewer Comment Details** dialog box, type your comments in the My Comments section. If the comment requests a change to the policy, click **Change Request**. If a change is requested, the policy status automatically changes to **Draft** when the review by date passes.
- 5 Click **OK**.

Viewing the reviewer comments

To view the review comments for a policy, you must have the required roles and permissions. In addition, the policy status must be marked as In Review.

Note: Only a user that is assigned to the CCS Administrator role can assign roles and permissions.

To view the reviewer comments for a policy

- 1 In the Policies view, select the policy to review.
- 2 In the details pane, click **Comments**.
- 3 In the **Comments** pane, double-click the reviewer comment you want to read.
- 4 Click **OK**.

About mapping policies

Policy mapping is the process of linking policies to control statements. These control statements are themselves mapped to the frameworks and regulations that your enterprise must adhere to. The control statements express the behaviors that the Control Compliance Suite can monitor and report on.

You can use the Symantec Content Studio to map policies to control statements.

See [“Using the custom content tool”](#) on page 681.

See [“Mapping policies to control statements”](#) on page 688.

Publishing and unpublishing policies

By publishing policies, you send approved policies to their respective audiences and make them accessible to members of the organization. Policies are viewable on the Control Compliance Suite Web Portal. After a policy is created, reviewed, and approved, it is ready to be published to the selected audience members.

A policy can be published only if the status is marked as Approved. A policy that has expired cannot be published.

When a policy is published, the selected audience members can access the policy from the Control Compliance Suite Web Portal. If you want to modify or update a published policy, you must first unpublish the policy. The policy is set to **Draft** status with a new version number. You can edit this new version. The published version of the policy cannot be modified.

When a policy is published, the selected audience members can access the policy from the Control Compliance Suite Web Console. If you want to modify or update a published policy, you must first unpublish the policy. The policy is set to **Draft** status with a new version number. You can edit this new version. The published version of the policy cannot be modified.

When a policy is unpublished, the current version of the policy is archived and is no longer displayed in the Web Portal home page. The policy is available for future publication under a new version number.

Approving a policy

Before you can publish policies, they must be approved. Policies can only be approved after they have been reviewed. In addition, the policy review by date must be in the past. Policies can be rejected as well. A rejected policy returns to the draft state.

Exceptions can be approved for approved policies just as with published policies.

Note: Only the policies that you have permissions to in the folder selected in the tree pane can be approved.

To approve or reject a policy

- 1 In the Policies view, click a folder in the tree pane, and do one of the following:
 - Click **Approve Policy**
 - Click **Workflow Tasks > Approve Policy**
 - Right-click an object in the tree, then click **Approve Policy**
- 2 In the **Approve Policy** dialog box, click the check box beside the name of the policies to publish, then click **Approve** or **Reject**.

Publishing a policy

Only approved policies can be published.

When you publish policies, you transmit the policies to the policy audience on the Control Compliance Suite Web Portal. Members of the audience can then accept or reject the policy. The audience members can also request exceptions to the policy or clarifications of the policy.

A policy can be published only if the status is marked as Approved. A policy that has expired cannot be published.

When a policy is published, the selected audience members can access the policy from the Control Compliance Suite Web Portal.

Note: Only the policies that you have permissions to in the folder selected in the tree pane can be published.

To publish a policy

- 1 In the Policies view, click a folder in the tree pane, and do one of the following:
 - Click **Workflow Tasks > Publish Policy**.
 - Right-click an object in the tree, then click **Publish Policy**.
- 2 In the **Publish Policy** dialog box, click the check box beside the name of the policies to publish, then click **Publish**.

Unpublishing a policy

Only published policies can be unpublished. When you unpublish a policy, the policy is removed from the Web Portal. An unpublished policy is no longer accessible to the policy audience. The policy state changes to **Archived**. A new version of the policy is created with the **Draft** state.

Note: Only the policies to which you have permissions in the currently-selected folder selected in the tree pane can be unpublished.

To unpublish a policy

- 1 In the Policies view, click a folder in the tree pane, and do one of the following:
 - Click **Workflow Tasks > Unpublish Policy**.
 - Right-click an object in the tree, then click **Unpublish Policy**.
- 2 In the **Unpublish Policy** dialog box, click the check box beside the name of the policies to unpublish, then click **Unpublish**.

Responding to policies on the Web PortalResponding to policies in the Web Console

The Web Portal home page displays a list of all published policies applicable to the currently logged on user. Here the user can select to view any policy details and decide to accept or decline the policy. The user can also request an exception





or a clarification for any policy. More than one exception or clarification can be made for each policy.

Note: If a policy is designated as read-only, the options to accept or decline a policy are not available. Also, no exception requests can be submitted for read-only policies.

Access the Web Portal home page using the following URL:

`http://servername/CCS_Web`

The following icons next to the policy indicates the user acceptance status for the policy:

- | | |
|---|---|
|  | Unread Policy |
|  | Read Policy - Not Accepted or Declined |
|  | Accepted Policy |
|  | Declined Policy |

The Policies area displays a list of all policies applicable to the currently logged on user. Click on a policy to view the details.

The My Exception Requests area displays any user-requested exceptions and the policy manager's response to the exceptions. The user can request an exception for any policy that they cannot comply with.

The My Clarification Requests area displays any user-requested clarifications and the policy manager's response to the clarifications. The user can request a clarification for any policy that they have questions about.

Accepting or declining a policy

The Web Portal home page displays a list of all published policies applicable to the currently logged on user. You can accept or decline a policy using the Web Portal home page.

Note: If a policy is designated as read-only, the options to accept or decline a policy are not available. No exception requests can be submitted for read-only policies.

To accept or decline a policy

- 1 Go to the **Web Portal** home page using the following URL:
`http://servername/CCS_Web`
- 2 In the **Web Portal** home page, under **Policies**, click the policy that you want to accept or decline. The icon next to the policy indicates the user acceptance status for the policy.
- 3 The policy details page displays the policy content. After you have read the policy and are ready to respond, click one of the following options:
 - **I have read this policy, but not accepted or declined yet**
 - **I accept this policy**
 - **I decline this policy**
- 4 Click **Submit Response**.

Reviewing a policy in the Web Portal

The Web Portal home page displays a list of all policies the currently logged on user is assigned to review. You can review any policy that is assigned to you for review using the Web Portal home page.

If you are assigned to review a policy, the policy appears in the **Review Policies** page.

To review a policy

- 1 Go to the **Web Portal** home page using the following URL:
`http://servername/CCS_Web`
- 2 In the **Web Portal** home page, click **Policies**.
- 3 Click **Review Policies**.
- 4 In the **Review Policies** page, review the policy content, targets, statements, and audience.
- 5 Click **Add Comments** to add your comments for the policy.

Approving a policy in the Web Portal

If you are assigned to the administrator role and have rights to a policy, the policy appears on the **Approve Policies** page in the Web Portal.

To approve a policy

- 1 Go to the **Web Portal** home page using the following URL:
`http://servername/CCS_Web`
- 2 In the **Web Portal** home page, click **Policies**.
- 3 Click **Approve Policies**.
- 4 In the **Approve Policies** page, select the policy to approve.
- 5 Do one of the following:
 - Click **Approve**.
 - Click **Reject**.
 - Click **Add Comments** to add your comments for the policy.

Submitting a policy for approval in the Web Portal

If you are assigned to the reviewer role and have rights to a policy, the policy appears in the **Policy Review Complete** page in the Web Portal. If all assigned reviewers have commented on the policy and there are no required changes, you can submit the policy for approval.

You must explicitly assign users to the **Policy Administrator**, **Policy Reviewers**, **Policy Approvers**, and **Policy Audience** roles. No users are assigned to these roles by default, including the **CCS Administrator**.

To submit a policy for approval

- 1 Go to the **Web Portal** home page using the following URL:
`http://servername/CCS_Web`
- 2 In the **Web Portal** home page, click **Policies**.
- 3 Click **Policy Review Complete**.
- 4 In the **Policy Review Complete** page, select the policy to submit for approval.
- 5 Click **Submit for Approval**.

Printing a policy from the Web Portal

The Web Portal home page displays a list of all published policies applicable to the currently logged on user. You can print a policy using the Web Portal home page.

The following items are included in the printed policy:

- Policy name

- Policy content
- Page number
- Time and date the policy was printed

To print a policy

- 1 Go to the **Web Portal** home page using the following URL:
`http://servername/CCS_Web`
- 2 In the **Web Portal** home page, under **Policies**, click the policy that you want to print .
- 3 Do one of the following:
 - Click **File > Print**.
 - Right-click, then click **Print**.

Managing clarifications

Clarifications let members of the policy audience request more information about a policy that they do not understand. Users can also request clarification for any policies which they may not be able to accept without further information. You manage clarifications in the policy clarifications view. You open the policy clarifications view by clicking **Manage > Policies > Clarifications**.

About clarifications

The clarification feature lets users request any clarification on the policies that they have questions about, using the Web Portal home page. More than one clarification request can be made to a policy. Users can view the status of those clarification requests that they have asked for.

The following clarification statuses exist:

Open	A clarification request that is submitted, but for which no response exists
Closed	A security manager has responded

About the clarifications management view

The **Clarifications Management** view lets you manage and respond to the policy clarification requests from users. The **Clarifications Management** view displays all policy clarification requests. The **Clarifications Management** view lets you

view the attributes of a selected policy clarification or filter the displayed policy clarifications.

You can access the **Policy Clarifications Management** view from Manage > Policies > Clarifications.

The **Policy Clarifications Management** view contains the following panes:

Blank pane	<p>This pane appears on the left side of the console window under the navigation bar.</p> <p>This pane displays a hierarchical, folder-based structure of the clarifications that are stored in the CCS directory.</p>
Filter by pane	<p>The filter by pane appears in the lower left side of the console window under the tree pane.</p> <p>You can specify filters in this pane so that only the required policy clarifications are displayed in the table pane.</p>
Table pane	<p>The table pane appears in the right side of the console window under the taskbar.</p> <p>This pane displays the policy clarifications.</p>
Details pane	<p>The details pane appears in the lower-right side of the console window under the table pane.</p> <p>This pane displays the details of the policy clarification that is selected in the details pane.</p>

You can perform the following tasks from the **Clarifications management** view:

- Review the policy clarifications.
- Respond to policy clarifications.

Managing clarification requests

You use the policy clarification view to view the clarification details or to respond to the clarification request.

To manage clarification requests

- 1 In the policy clarification view, select the clarification to manage.
- 2 Click **Open Clarification**.

3 The clarification editor displays the following information:

Submitted	Displays the date and time when the request was created.
By	Displays the name of the user who requested the clarification.
Email	<p>Displays the email address of the user to send a notification to. The email address is optional.</p> <p>If you send an email, you must configure the From email address in the Email Notifications tab in the General Settings.</p> <p>See “Configuring the email Notification Server ” on page 132.</p>
Details	Displays the question that the user submitted regarding the policy.
Due By	Displays the date by when the security manager should send a response.
Responded (date)	Displays the date and time of the response.
By	Displays the account name of the security manager who responded to the request.
Details	Displays a text box where you can enter an explanation to the clarification that the user submitted.

4 Click **OK** to save.

A notification is sent to the user if an email address is provided.

Monitoring jobs

This chapter includes the following topics:

- [About jobs](#)
- [Managing jobs](#)
- [Managing job runs](#)
- [Viewing jobs information in the details pane](#)

About jobs

A job is a specified set of operations. These operations are performed sequentially by various components of Control Compliance Suite. A job is also called a query with a scope. For example, a query with a scope in the form of assets in a particular domain is called a job. A job is uniquely defined.

When you execute a job, the particular instance of a job is called a job run. The job run is displayed when you expand a job in the table pane.

You can perform the following operations on jobs:

- Create a job
See [“Creating jobs”](#) on page 605.
- Edit a job
See [“Editing a job”](#) on page 601.
- Run a job now
See [“Running a job now”](#) on page 603.
- Schedule a job
See [“Scheduling jobs”](#) on page 602.
- Delete a job
See [“Deleting jobs”](#) on page 602.

- Refresh the jobs view
See [“Refreshing the jobs view”](#) on page 604.
- Cancel a job run
See [“Canceling a job run”](#) on page 606.
- Delete a job run
See [“Deleting a job run”](#) on page 607.

Select the job and use the right-click option to perform the stated operations. The menu options available at the right-click option are specific to the job type. You can select multiple jobs by using check boxes.

The stated options are also available on the taskbar and the menu bar under the Tasks menu. The tasks are enabled when the check box is checked.

You can even set up a job count. When you set up the job count, you can choose the number of jobs to be displayed in the Job view. These changes are made through the **Settings > General Settings**. Similarly, you can even set up a job run count.

To expand all the rows of jobs, press Ctrl + Right Arrow.

To collapse all the rows of jobs, press Ctrl + Left Arrow.

Control Compliance Suite does not support the following special characters in the job name:

* () \ / , + " > < ; = #

See [“About using special characters in folder and job names”](#) on page 60.

See [“About the job types”](#) on page 596.

See [“About the job filters”](#) on page 598.

About the job types

The jobs that are automatically created by Control Compliance Suite are known as System jobs. The System jobs perform certain predefined functions. Some of the System jobs may be hidden.

The jobs that are created by the user are known as user-defined jobs.

Control Compliance Suite contains the following job types:

Asset import job	<p>The Asset import job imports assets. You can also add assets in the hierarchy through the job, which helps you to manage the assets.</p> <p>See “Importing asset-specific fields from the default data collector” on page 272.</p> <p>See “Importing asset-specific and common fields using the CSV data collector” on page 278.</p>
Baseline job	<p>Initially, the Baseline job is the same as the data collection job, as it collects data based on the query. Then a job run of this job is marked as a baseline. You can compare another job run with the job run that is marked as a baseline. Similarly, you can compare two types of assets.</p> <p>See “Creating a baseline job” on page 560.</p>
Entitlements import job	<p>The Entitlements import job fetches the entitlements for a particular control point.</p> <p>See “Importing the entitlements manually” on page 408.</p>
Automatic entitlements import job	<p>The Automatic entitlements import job is created during installation. This job fetches the entitlements for the import-required control points.</p> <p>See “Configuring the automatic entitlements import” on page 407.</p>
Evidence collection job	<p>The Evidence collection job imports third-party evidence data.</p>
Report generation job	<p>The Report generation job creates different types of reports.</p> <p>See “Editing a report generation job” on page 646.</p>
Summary dashboard update job	<p>The Summary dashboard update job updates an existing Summary dashboard through the Edit Dashboard Schedule Job wizard. Summary dashboards are created using the dashboard templates.</p> <p>See “Editing a summary dashboard update job” on page 651.</p>
Tiered dashboard update job	<p>The Tiered dashboard update job updates an existing Tiered dashboard through the Edit Tiered Dashboards wizard.</p> <p>See “Editing a tiered dashboard” on page 658.</p>
Reporting database synchronization job	<p>The Report data synchronization job synchronizes between the production database and the reporting database.</p>
Report data purge job	<p>The Report data purge job purges data from the reporting database.</p>

Evaluation job	<p>The Evaluation job evaluates a standard or a set of standards against the assets or the assets group, or the assets folder.</p> <p>See “Running an evaluation job from the Standards view” on page 495.</p> <p>Data collection must be performed before running an Evaluation Job.</p> <p>See “About remediation” on page 549.</p>
Data collection job	<p>The Data collection job collects required data for a standard or a set of standard. The job collects the data against the assets or the assets group, or the assets folder.</p> <p>See “Setting up a data collection job from the Standards view” on page 498.</p>
Gold standard job	<p>The Gold standard job creates and synchronizes the gold standard. This job creates a gold standard, collects data for this gold standard, and auto-resolves and evaluates the standard.</p> <p>See “Gold standard job” on page 538.</p>
Collection-Evaluation-Reporting job	<p>The collection-evaluation-reporting lets you create a chained job to collect data for a set of assets, to evaluate the assets, and to generate reports for those assets.</p> <p>You can also schedule to remediate the assets automatically at the end of the evaluation.</p> <p>See “Running a collection-evaluation-reporting job from the Standards view” on page 499.</p>
Remediation verification job	<p>The remediation verification job is a system job.</p> <p>The remediation verification job recollects and reevaluates the asset data after the remediation action is taken on the assets. This job appears only if you enable the closed-loop remediation.</p> <p>See “About jobs” on page 595.</p> <p>See “Creating jobs” on page 605.</p>

About the job filters

The Filter by pane at the left in the Jobs view shows numerous filters. You can use these filters to display the required jobs. If none of the job type is selected then jobs of all job types are shown.

Control Compliance Suite provides the following default filters for filtering the jobs:

Job Type	<p>Lets you filter the jobs according to the type of the job.</p> <p>The following types of jobs can be filtered:</p> <ul style="list-style-type: none">■ Asset import job■ Baseline job■ Entitlements import job■ Automatic entitlements import job■ Evidence collection job■ Report generation job■ Summary dashboard update job■ Report data synchronization job■ Report data purge job■ Tiered dashboard update job■ Evaluation job■ Data collection job■ Gold standard job■ Collection-Evaluation-Reporting job■ Remediation verification job
Last Run Date	<p>Lets you filter the jobs according to the last completed job run date or time.</p> <p>You can select one of the following options:</p> <ul style="list-style-type: none">■ Any■ Before■ After■ Between

Select the filter and click update to view the jobs in the table pane.

See [“About jobs”](#) on page 595.

See [“About the job types”](#) on page 596.

See [“Customizing the filter options”](#) on page 56.

About the Jobs view

The Jobs view is used to view all the jobs that are created in Control Compliance Suite.

You can access the Jobs view from **Monitor > Jobs**.

Manage Jobs and View all Jobs permissions are needed to navigate to jobs view.

The jobs view displays the following three panes:

Table pane	The table pane displays the list of the jobs. When you expand the jobs, you can view the job run.
Details pane	The details pane displays the details of the job. When you select the job in the table pane, the job details are displayed in the details pane.
Filter by pane	The filter by pane is used to filter the jobs. When you set the filters and update, the jobs are listed in the table pane.

The taskbar of the Jobs view is divided into the following major tasks:

Common Tasks

Job Tasks

- Run job now
See [“Running a job now”](#) on page 603.
- Refresh selected job
See [“Refreshing the jobs view”](#) on page 604.
- Delete job
See [“Deleting jobs”](#) on page 602.
- Edit job
See [“Editing a job”](#) on page 601.
- Schedule job
See [“Scheduling jobs”](#) on page 602.

Job Run Tasks

- Cancel job run
See [“Canceling a job run”](#) on page 606.
- Delete job runs
See [“Deleting a job run”](#) on page 607.
See [“Manual review”](#) on page 246.

You can search for a job through the Jobs view.

See [“Searching for a job”](#) on page 604.

See [“About jobs”](#) on page 595.

See [“About the job filters”](#) on page 598.

See [“Viewing jobs information in the details pane”](#) on page 608.

Managing jobs

You can perform the following operations in the **Jobs** view:

- Create jobs
See [“Creating jobs”](#) on page 605.

- Edit a job
See [“Editing a job”](#) on page 601.
- Run a job now
See [“Running a job now”](#) on page 603.
- Schedule a job
See [“Scheduling jobs”](#) on page 602.
- Delete a job
See [“Deleting jobs”](#) on page 602.
- Refresh the jobs view
See [“Refreshing the jobs view”](#) on page 604.
- Search for a job
See [“Searching for a job”](#) on page 604.

Editing a job

You can edit a job by using the right-click menu option available at the job. You can even edit the jobs by using the taskbar and the **Tasks** menu.

You can edit only one job at a time. Each job type has unique edit options. You can only edit user-defined jobs. The user who has created the job and the CCS administrator can edit the job.

To edit jobs

- 1 In the **Monitor > Job** view, select the job.
- 2 Right-click and select **Edit Job**.
- 3 In the wizard of the respective job, make the required changes. Complete the wizard. The job is edited.

See [“About jobs”](#) on page 595.

See [“Scheduling jobs”](#) on page 602.

See [“Deleting jobs”](#) on page 602.

See [“Running a job now”](#) on page 603.

See [“Canceling a job run”](#) on page 606.

See [“Searching for a job”](#) on page 604.

See [“Refreshing the jobs view”](#) on page 604.

See [“Deleting a job run”](#) on page 607.

See [“Creating jobs”](#) on page 605.

Scheduling jobs

You can schedule a job by using the right-click menu option available at the job. You can even schedule the jobs by using the taskbar and the **Tasks** menu.

You can schedule only one job at a time.

To schedule a job

- 1 In the **Monitor** > **Job** view, select the job.
- 2 Right-click and select **Schedule Job**.
- 3 In the Schedule dialog box, select either or both of the following:
 - If you want to run the job now, check **Run Now**.
 - If you want to run the job at a specified interval, check **Run Periodically** and enter the following information:
 - In the Start On box, enter the start date and time to run the job.
 - Under Run periodically options, if you want to run the job only one time, select **Run Once**. If you want to run the job after specific days, select the number of days in the Run every Day list box.
- 4 Click **OK**.

See [“About jobs”](#) on page 595.

See [“Editing a job”](#) on page 601.

See [“Deleting jobs”](#) on page 602.

See [“Running a job now”](#) on page 603.

See [“Canceling a job run”](#) on page 606.

See [“Searching for a job”](#) on page 604.

See [“Refreshing the jobs view”](#) on page 604.

See [“Deleting a job run”](#) on page 607.

See [“Creating jobs”](#) on page 605.

Deleting jobs

You can delete a job by using the right-click menu option available at the job. You can even delete the jobs by using the taskbar and the **Tasks** menu.

You can delete multiple jobs. You can delete only the user-defined jobs.

To delete a job

- 1 In the **Monitor > Job** view, select the job.
- 2 Right-click and select **Delete Job**. In the confirmation message, click **Yes** and the job is deleted.

See [“About jobs”](#) on page 595.

See [“Editing a job”](#) on page 601.

See [“Scheduling jobs”](#) on page 602.

See [“Running a job now”](#) on page 603.

See [“Canceling a job run”](#) on page 606.

See [“Searching for a job”](#) on page 604.

See [“Refreshing the jobs view”](#) on page 604.

See [“Deleting a job run”](#) on page 607.

See [“Creating jobs”](#) on page 605.

Running a job now

You can run a job by using the right-click menu option available at the job. You can even run the jobs by using the taskbar and the **Tasks** menu.

To run a job now

- 1 In the **Monitor > Job** view, select the job.
- 2 Right-click and select **Run Job Now**. A corresponding Job run is created and the job starts to run. The column Last Run Status displays the last run status of the job. The column Last Run Date displays the timestamp of the last completed job run.

See [“About jobs”](#) on page 595.

See [“Editing a job”](#) on page 601.

See [“Scheduling jobs”](#) on page 602.

See [“Deleting jobs”](#) on page 602.

See [“Canceling a job run”](#) on page 606.

See [“Searching for a job”](#) on page 604.

See [“Refreshing the jobs view”](#) on page 604.

See [“Deleting a job run”](#) on page 607.

See [“Creating jobs”](#) on page 605.

Searching for a job

You can use the **Search** box to search for a job. You can even search by any of the columns. For example, you can type Failed and see the job runs with the Failed status.

You can even use the Filter by pane to filter the jobs. Search is performed only on the records visible in User Interface.

To search for a job

- 1 In the **Monitor > Job** view, type the name of the job in the Search box available in the table pane.
- 2 Click the **search** icon. The jobs are listed in the table pane.

See [“About jobs”](#) on page 595.

See [“Editing a job”](#) on page 601.

See [“Scheduling jobs”](#) on page 602.

See [“Deleting jobs”](#) on page 602.

See [“Running a job now”](#) on page 603.

See [“Canceling a job run”](#) on page 606.

See [“Refreshing the jobs view”](#) on page 604.

See [“Deleting a job run”](#) on page 607.

See [“Creating jobs”](#) on page 605.

Refreshing the jobs view

You can refresh the jobs view or the selected jobs.

To see the current status of the job or the job run, you can perform the refresh option manually.

To refresh the whole view, you can press F5.

To refresh a specific job

- 1 Select the job that you want to refresh.
- 2 Do one of the following:
 - On the **Tasks** menu, point to Job Tasks and then select **Refresh Selected Job**.
 - Right-click the selected job and select **Refresh Selected Job**.
 - On the taskbar, select **Refresh Selected Job**.

See [“About jobs”](#) on page 595.

See [“Editing a job”](#) on page 601.

See [“Scheduling jobs”](#) on page 602.

See [“Deleting jobs”](#) on page 602.

See [“Running a job now”](#) on page 603.

See [“Canceling a job run”](#) on page 606.

See [“Searching for a job”](#) on page 604.

See [“Deleting a job run”](#) on page 607.

See [“Creating jobs”](#) on page 605.

Creating jobs

You can create few jobs from the jobs view by using the right-click option in the table pane. You can even create the jobs through the **Tasks** bar.

You can create the following jobs from the jobs view:

- Baseline job
See [“Creating a baseline job”](#) on page 560.
- Evaluation job
See [“Running an evaluation job from the Standards view”](#) on page 495.
- Data collection job
See [“Setting up a data collection job from the Standards view”](#) on page 498.
- Entitlements import job
See [“Importing the entitlements manually”](#) on page 408.
- Import assets job
See [“Importing asset-specific and common fields using the CSV data collector”](#) on page 278.
See [“Importing asset-specific fields from the default data collector”](#) on page 272.

To create a job from the jobs view

- 1 In the **Monitor > Job** view, right-click in the empty grid in the table pane and select the job that you want to create.

The wizard that is associated with the respective job is launched.

- 2 Complete the wizard to create the job.

See [“About jobs”](#) on page 595.

See [“Editing a job”](#) on page 601.

See [“Scheduling jobs”](#) on page 602.

See [“Deleting jobs”](#) on page 602.

See [“Running a job now”](#) on page 603.

See [“Canceling a job run”](#) on page 606.

See [“Searching for a job”](#) on page 604.

See [“Deleting a job run”](#) on page 607.

See [“Refreshing the jobs view”](#) on page 604.

Managing job runs

You can perform the following operations on job runs:

- Cancel a job run
See [“Canceling a job run”](#) on page 606.
- Delete a job run
See [“Deleting a job run”](#) on page 607.
See [“Manual review”](#) on page 246.

Canceling a job run

You can cancel a job run by using the right-click menu option available at the job run. You can even cancel the job run by using the taskbar and the **Tasks** menu.

You can simultaneously cancel job runs of the same type. Job runs of the same type that belong to different jobs can also be canceled.

For example, if you select two asset import job runs, the cancel option is enabled. If you select asset import job run and data collection job run for cancelation, then the cancel option is disabled. These job runs are not canceled because the jobs are not of the same type.

You can cancel Job runs in Executing states.

You cannot cancel Job runs in the following states:

- Aborted
- Complete
- Faulted
- Custom

To cancel a job run

- 1 In the **Monitor > Job** view, expand the job container under which the job run resides.
- 2 Select the job run you want to cancel, right-click, and then click **Cancel Job**. The job run is canceled.

See [“About jobs”](#) on page 595.

See [“Editing a job”](#) on page 601.

See [“Scheduling jobs”](#) on page 602.

See [“Deleting jobs”](#) on page 602.

See [“Running a job now”](#) on page 603.

See [“Searching for a job”](#) on page 604.

See [“Refreshing the jobs view”](#) on page 604.

See [“Deleting a job run”](#) on page 607.

See [“Creating jobs”](#) on page 605.

Deleting a job run

You can delete a job run by using the right-click menu option that is available at the job run. You can even delete the job runs by using the taskbar and the **Tasks** menu.

You can delete only the job runs in completed, aborted, and faulted states.

To delete a job run

- 1 In the **Monitor > Job** view, expand the job in the table pane.
- 2 Select the job run, right-click, and select **Delete Job Run**. The job run is deleted.

See [“About jobs”](#) on page 595.

See [“Editing a job”](#) on page 601.

See [“Scheduling jobs”](#) on page 602.

See [“Deleting jobs”](#) on page 602.

See [“Running a job now”](#) on page 603.

See [“Canceling a job run”](#) on page 606.

See [“Searching for a job”](#) on page 604.

See [“Refreshing the jobs view”](#) on page 604.

See [“Creating jobs”](#) on page 605.

Viewing jobs information in the details pane

You can view the information about the jobs through the details pane.

The details pane displays all the information about the selected job or the job run in the following tabs:

- General tab
See “Jobs details pane- General tab” on page 608.
- Schedule tab
See “Jobs details pane- Schedule tab” on page 609.
- Wizard Summary tab
See “Jobs details pane - Wizard Summary” on page 609.
- Summary tab
See “Job run details pane- Summary tab” on page 609.
- Failures tab
See “Job run details pane- Failures tab” on page 609.
- Templates tab
See “Jobs details pane- Template tab” on page 609.

To view jobs information

- 1 In the **Monitor** > **Jobs** view, select the job or the job run in the table pane for which you want to view the information.
- 2 View the information for the selected job or the job run in the details pane.

Jobs details pane- General tab

The **General** tab of the Jobs details pane provides general information about the selected job. The information in this tab is read-only.

The **General** tab contains the following details about the jobs:

Job type	Displays the job type
Created by	Displays the identity of who has created the job
Next run date	Displays the date and the time when the job runs next
Created on	Displays the date and the time when the job was created
Last run status	Displays the status of the latest job run
Last run date	Displays the last completed job run date and time

Last modified on

Displays the date and the time when the job was last modified

Jobs details pane- Schedule tab

The **Schedule** tab of the Jobs details pane provides information about the scheduling of the selected job. The information in this tab is read-only.

The **Schedule** tab contains the following details about the jobs:

Run on	Displays the date and time for the job to run or displays the next job execution time
Recurring	Displays the status for a recurring job
Run every	Displays the duration between two scheduled runs

Jobs details pane - Wizard Summary

This tab shows the configuration details of the job. The data that is displayed in this tab varies with the job type.

Job run details pane- Summary tab

The **Summary** tab provides details about the selected job run. The information that is displayed in the tab pertains to the type of the job. The information in this tab is read-only.

Job run details pane- Failures tab

The **Failures** tab provides information about the data collector errors of the selected job run. The information in this tab is read-only.

The **Failure Details** column of the job run in the tables pane displays the details about other errors.

Jobs details pane- Template tab

The **Template** tab of the Jobs details pane specifies the template that is used for creating the report. The information in this tab is read-only.

The **Template** tab contains the following information of the report:

Report title	Displays the name of the report
Report type	Displays the type of report

Description	Displays the description of the report
Author	Displays the name of the author of the report
Version	Displays the version of the report

Monitoring evaluation results

This chapter includes the following topics:

- [About the Evaluation Results view](#)
- [About the evaluation result filters](#)
- [Viewing evaluation jobs in the details pane](#)

About the Evaluation Results view

The Evaluation Results view is used to view the details of each evaluation job run.

For example, assume that you have evaluation jobs A and B. You run the job A two times and the job B three times. The Evaluation Results view lists the details of each job run. In this case, job A is listed twice and job B is listed three times.

Note: You must have the Standard Administrator or Standard Evaluator role to view the evaluation results.

The Evaluation Results view displays content in the following panes:

Tables pane	Lists each instance of the job run for all the evaluation jobs.
Details pane	Provides the details of each evaluation job run.
Filter by pane	Provides the filters to display only selected evaluation jobs in the table pane.

See [“Evaluation Results details pane - General tab”](#) on page 613.

See “Evaluation Results details pane - Evaluation Summary tab” on page 613.

See “Evaluation Results details pane - Assets Evaluated tab” on page 613.

About the evaluation result filters

The filter by pane contains the Last Run Date filter that you can use to display only the required evaluation jobs.

The Last Run Date filter contains the following options for filtering the evaluation jobs:

All	Lists all the evaluation jobs.
Last One Day	Lists all the evaluation jobs that were run during the last one day.
Last One Week	Lists all the evaluation jobs that were run during the last one week.
Last One Month	Lists all the evaluation jobs that were run during the last one month.
Between	Lists all the evaluation jobs that were run during a specific time period.
And	Provide the start date and time in the Between box. Provide the end date and time in the And box.

The time that is used to calculate the specified options is 12:00 am.

For example, consider that on 23 Aug 2008 at 4:00 p.m. you select the Last One Day option for filtering the jobs. Then all the jobs that were run from 22 Aug 2008 (at 12:00 a.m.) to 23 Aug 008 (at 4:00 p.m.) are displayed.

Viewing evaluation jobs in the details pane

You can view the information about an evaluation job through the details pane of the Evaluation Results view.

To view the evaluation job information

- 1 In the table pane, select the evaluation job for which you want to display the information.
- 2 View the information for the selected evaluation job in the details pane.

The evaluation job details are contained in the following tabs:

- General
See [“Evaluation Results details pane - General tab”](#) on page 613.
- Evaluation Summary
See [“Evaluation Results details pane - Evaluation Summary tab”](#) on page 613.
- Assets Evaluated
See [“Evaluation Results details pane - Assets Evaluated tab”](#) on page 613.

See [“About the details pane”](#) on page 50.

Evaluation Results details pane - General tab

The General tab of the Evaluation Results details pane provides general information about the selected evaluation job.

The General tab contains the following information:

Name	The name of the evaluation job. This value is editable.
Description	The description of the evaluation job.
Evaluation Date	The date when the job was evaluated.
Submitted by	The user name of the user who submitted the job.

Evaluation Results details pane - Evaluation Summary tab

The Evaluation Summary tab of the Evaluation Results details pane provides information about the standards that were evaluated in the evaluation job.

The Evaluation Summary tab contains the following information:

Name	Lists the name of the standards that were evaluated in the evaluation job.
Version	Lists the version of the standards.
Risk Score	Lists the risk score of the standard.
Compliance Score	Lists the compliance score of the standard.

Evaluation Results details pane - Assets Evaluated tab

The Assets Evaluated tab of the Evaluation Results details pane provides information about the assets that are evaluated in the evaluation job. This tab contains a list of the names of the assets that were evaluated.

Managing reports and dashboards

This chapter includes the following topics:

- [About the reports and dashboards](#)
- [Working with reports](#)
- [Working with dashboards](#)

About the reports and dashboards

Control Compliance Suite (CCS) provides a rich set of presentation-level reports. A report lets you collect and present the data in a format that conforms to the organizational needs. A report is a business document that contains a predefined, organized collection of data. A report can be viewed, printed, or analyzed. You can create and customize reports from the Reporting view. You can schedule the report generation or dashboard update jobs from the Jobs view. You can schedule reports and dashboard jobs to run at a specified time. If the report supports the feature, you can export a report in several formats.

Organizations collect vast amounts of information in the course of completing business transactions. Management studies the data to make decisions. The Reporting feature gives you the timely information that you need to make informed decisions about the organization.

The reporting database stores the data that is needed for the reports and dashboards.

The collection-evaluation-reporting job lets you create a chained job. A chained job collects data for a set of assets, evaluates the assets, and generates reports from the results.

You can create a report template or modify a report template using Crystal Reports Developer 2008. An installation of the Crystal Reports Developer 2008 is required. Crystal Reports Developer 2008 is not a component of the Symantec Control Compliance Suite installation.

See [“About the Reporting view”](#) on page 616.

See [“Working with reports ”](#) on page 635.

See [“Working with dashboards”](#) on page 646.

About the Reporting view

Control Compliance Suite provides a rich set of presentation-level reports. A report is a business document that contains a predefined, organized collection of data. A report can be viewed, printed, or analyzed. Reports are viewed in the Reporting view. You schedule reports in the Job Management view. The reporting features let you distill the data and publish the results.

To view dashboards, you are required to install a Flash player with the CCS console.

You can do the following in the Reporting view:

- Manage reports and dashboard templates
- Manage reports
- Export reports to a different format
- Manage historical data in My Reports view
- Generate reports on compliance-relevant areas in the Control Compliance Suite

The Reporting view comprises the following:

- Reports Templates view
- Dashboard Templates view
- My Reports view

See [“About the Reports Templates view”](#) on page 616.

See [“About the Dashboard Templates view”](#) on page 621.

See [“About the My Reports view”](#) on page 618.

About the Reports Templates view

The Reports Templates view lists the report templates that you can access. The Reports folder has the Predefined subfolder. You can create a user-defined subfolder to store the customized report templates. You can copy the predefined

templates to the user-defined folder. If the report template supports the feature, you can customize the predefined report template.

The Report Templates view has the following panes:

- Folder
- Filter by
- Table
- Details

In the folder pane, you can do the following:

- Add user-defined subfolders
- Select a folder to view the report templates in the table pane

In the **Filter by** pane, you can do the following:

- Create a report type filter.
- Create a tag filter.

In the table pane, you can do the following:

- Schedule a selected template
- Copy and paste a predefined template to the user-defined folder
- Customize a report template, if the report template supports the feature
- Export a report template to a Crystal Reports Developer 2008 file
- Add a report template that is created in Crystal Reports Developer 2008
- Update a report template that is created in Crystal Reports Developer 2008
- Apply a filter to the template list
- View the name, description, and version number of each report template
- Verify if a report supports customization and can be generated using the chained job
- In a user-defined folder, you can delete a report template
- In a user-defined folder, you can move a report template to another user-defined folder
- Add or update a report template
- Export a report template
- Move a report template

In the details pane > General tab, you can view the following information about a selected report template:

- Report title
- Report type
- Description
- Author
- Version

In the details pane > Tags tab, you can add a tag to a report.

- Add a tag.
- Remove a tag.

See [“Copying a report template”](#) on page 640.

See [“Customizing a report template”](#) on page 641.

See [“Deleting a user-defined report template”](#) on page 643.

See [“About the Reporting view”](#) on page 616.

See [“Exporting a report”](#) on page 639.

See [“Adding a user-defined report template”](#) on page 643.

See [“Updating a report template”](#) on page 645.

See [“Exporting a report template”](#) on page 644.

See [“Moving a report template”](#) on page 646.

About the My Reports view

The My Reports view lists the successful report runs that you can access. The view displays only the successful report runs. These reports are only accessible by the user who created the report. The Report Viewer role can only see reports in the My Reports view.

Members of the CCS Administrators role cannot remove a report. If you are assigned as a viewer for the report, you can remove the report from the **My Reports** view.

The My Reports view has the following panes:

- Filter by
- Table

In the **Filter by** pane, you can filter the reports by the following: by using a last run date and the selected type of report.

- Last run date
- Report type

The last run date can be one of the following:

- Any date
- Before a selected date
- After a selected date
- Within a specific date range

The report type can be one of the following:

- Assets
- Standards
- Entitlements
- Policy
- Audit

You can do the following in the table pane:

- View a selected report.
- Remove a report.
- Apply a filter to the report list.

You can base the filter on the report template type or date run.

When you view a report, you can export the report to a supported format.

See [“About the Reporting view”](#) on page 616.

About the My Dashboards view

The **My Dashboards** view lists the tiered and summary dashboards that you can access. A summary dashboard is listed every time the summary dashboard update job runs. A tiered dashboard is listed after creating the dashboard job using the Create Tiered Dashboards wizard.

Members of the CCS Administrators role cannot remove a summary dashboard update job run. If you are assigned as a viewer for the dashboard, you can remove any tiered and summary dashboard from the My Dashboards view.

In the taskbar, you can select the following:

- **View**
- **Dashboard Tasks**
- **Create Tiered Dashboard**
- **Delete**
- **Manage Tiered Dashboards**
- **View Details Report**
- **View Trends Report**
- **Tiered Dashboards Reports**

The **My Dashboards** view has the following panes:

- **Filter by**
- **Table**

In the **Filter by** pane, you can create a filter on the **Last Run Date**.

You can have the following options for the **Last Run Date**:

- Any
- Before a selected date
- After a selected date
- Between selected dates

You can filter by the following status categories:

- **Critical**
- **Danger**
- **Warning**
- **Normal**
- **Information**
- **No Data**

The table pane columns are as follows:

- **Dashboard Name**
- **Last Run Date**
- **Status**

You can select a column and drag the column name to the header to group the remaining columns by that column.

You can **Search** by any of the table pane columns.

In the table pane, you can do the following with a selected dashboard:

- View
- Delete
- Rename
- Copy
- Edit
- Edit Schedule
- Edit Dashboard Job Notification
- Export
- View Details Report
- View Trends Report

See [“About the Reporting view”](#) on page 616.

See [“About types of dashboards”](#) on page 622.

About the Dashboard Templates view

The **Dashboard Templates** view lists the predefined dashboard templates. These predefined dashboard templates are known as summary dashboards. You can schedule a dashboard template, which executes as a summary dashboard update job. You cannot delete, customize, or copy the dashboard templates. You cannot add user-defined folders in the **Dashboard Templates** view.

The **Dashboard Templates** view is divided between the table pane and the details pane.

You can do the following in the table pane:

- Select a template and schedule a summary dashboard update job.
- View the name, the description, and the version number of each dashboard template.

In the details pane, you can view the following information:

- Dashboard title
- Dashboard type
- Description
- Author

- Version
- See [“About the Reporting view”](#) on page 616.
- See [“Scheduling a summary dashboard update job”](#) on page 649.

About types of dashboards

Control Compliance Suite defines the summary dashboard and tiered dashboard.

Table 17-1 Dashboard types and descriptions

Type	Description	Available in
Tiered	A dashboard that is based on hierarchical dashboards with the sections and the nodes that logically represent your organization in different ways.	Control Compliance Suite Console
Web-based	A dashboard that is based on selected key elements of an organization and can be adapted for each viewer.	Control Compliance Suite Web Console

A summary dashboard is about a set of defined static dashboard templates that you can use to gather specific information. You can access the summary dashboard templates from **Reporting Dashboards Templates**.

You can do the following for a summary dashboard:

- Use the defined templates for gathering specific information
- Schedule and execute the summary dashboard update jobs

You can do the following for a tiered dashboard:

- Create the dashboards that contain evaluation sections and nodes.
- Schedule and execute the tiered dashboard update jobs.
- Edit a tiered dashboard and the evaluation sections and nodes.
- Delete a tiered dashboard.

The dashboard that is created in the Web Console is not based on a scheduled job. A dashboard that is created in the Web Console consists of independent elements, called panels. Each panel has two levels. The top level is typically a chart or a grid. You can drill down to see the detail in a second-level grid.

See [“Managing summary dashboards”](#) on page 647.

See [“Managing tiered dashboards”](#) on page 651.

About predefined report templates

The predefined report templates are installed with the Control Compliance Suite. The predefined report templates are in the **Predefined** folder in the tree pane of the Report Template view. You can schedule a report template. You can customize a template, if the template supports the feature. You can customize a report template in the predefined node or copy the report template to a user-defined folder in the Report Templates view.

You can export the template as an RPT file and then open the file with Crystal Reports Developer 2008. You can modify the RPT file and add the file as a user-defined report template.

You cannot delete a predefined report template.

See [“Scheduling a report”](#) on page 636.

See [“Copying a report template”](#) on page 640.

See [“Customizing a report template”](#) on page 641.

See [“Predefined Reports and Dashboard descriptions”](#) on page 627.

See [“Exporting a report template”](#) on page 644.

About data synchronization

Reports and dashboards use the data that is stored in the reporting database. The data that is required for reports and dashboards is synchronized with the production database using the synchronization job. The reporting database synchronization job is located in the Job Management view.

The prerequisite for the Reporting Database Synchronization Job requires SQL Server 2005 Integration Services (SSIS) SP2 to be installed.

The synchronization job operates in the following modes:

- Automatic
- Scheduled

The automatic mode synchronizes data between the production and reporting databases after the completion of selected jobs. You can select the jobs in the Settings > General > System Configuration > Reporting Synchronization.

The synchronization job can be set to start at a specific time. You can request an administrator to schedule a synchronization job to run immediately. Only administrators run the synchronization job. You must run a synchronization job before you schedule a report or dashboard.

See [“About the Report Management jobs”](#) on page 627.

See [“Synchronizing the reporting database”](#) on page 133.

About creating user-defined templates

You can create a template with Crystal Reports 2008 SP1 and then add the template into Control Compliance Suite. You can also update an existing template by exporting the template to Crystal Reports 2008 SP1. To add or update a template, you must be a Report Administrator.

An installation of the Crystal Reports 2008 SP1 is required. Crystal Reports 2008 SP1 is not a component of the Symantec Control Compliance Suite installation.

You can find more information on developing your reports at:

<http://www.symantec.com/business/support/overview.jsp?pid=53741>

See [“Adding a user-defined report template”](#) on page 643.

See [“About the prerequisites for user-defined report templates”](#) on page 624.

About the prerequisites for user-defined report templates

You can register user-defined reports. User-defined reports are reports created with Crystal Reports 2008 SP1. To create a user-defined report, you must have access to the reporting database.

You must have the following permissions:

- Access to the SQL Server instance
- Read-only access to the Reporting database
- An installation of the Crystal Reports 2008 SP1 is required. Crystal Reports 2008 SP1 is not a component of the Symantec Control Compliance Suite installation.

If you create a report that combines business objects, you must add all of the required parameters. The report template is validated based on the type of business objects. For example, if you create a report template for assets and standards, then you must add the required asset parameters and the required standards parameters to the report template. You do not add a required parameter twice. The ReportRunBy parameter and the ReportRunDate parameter must appear only once in the report.

If you create a report that needs information from RMS, the legacy default RMS database name is ComplianceManager.

To create a new asset or asset group report template in Crystal Reports 2008 SP1, you must have the following parameters:

AssetJobID	The unique identifier joins related tables to the ReportJob table in the CSM_Reports database.
AssetGroup	The unique identifier of the asset group present in the report scope.
Folders	The unique identifier of the asset system folder within the report scope.
ReportRunBy	The user who executes the reporting job for the report.
ReportRunDate	The date for the reporting job

To create a new standards report template in Crystal Reports 2008 SP1, you must have the following parameters:

StandardJobID	The unique identifier joins related tables to the ReportStandardJob table in the CSM_Reports database.
ReportRunBy	The user who executes the reporting job for the report.
ReportRunDate	The date for the reporting job

To create a new entitlements control points report template in Crystal Reports 2008 SP1, you must have the following parameters:

ControlPointType	The display name of the control point type.
Status	The control point status
DataOwner	The control point owner
Tags	The tags that are associated with the control point
EntitlementControlPointJobID	The unique identifier joins related tables to the ReportJob table in the CSM_Reports database. The parameter is a part of the filter set definition XML. The definition filters control point types.
ReportRunBy	The user who executes the reporting job for the report.
ReportRunDate	The date for the reporting job
AssetGroup	The unique identifier of the asset group present in the report scope.

Folders	The unique identifier of the asset system folder within the report scope.
---------	---

To create a new entitlements review cycles report template in Crystal Reports 2008 SP1, you must have the following parameters:

CurrentOrSnapshoted	The parameter determines if the report scope contains current review cycles or snapshot review cycles
Status	The status of the review cycle
ReviewCycleID	The unique identifier of the review cycle
ControlPointType	The display name of the control point type.
DataOwner	The control point owner
Tags	The tags that are associated with the control point
EntitlementsReviewCycleJobID	The unique identifier joins related tables to the ReportJob table in the CSM_Reports database. The parameter is a part of the filter set definition XML. The definition filters control point types.
ReportRunBy	The user who executes the reporting job for the report.
ReportRunDate	The date for the reporting job
AssetGroup	The unique identifier of the asset group present in the report scope.
Folders	The unique identifier of the asset system folder within the report scope.

To create a new policy report template in Crystal Reports 2008 SP1, you must have the following parameters:

PolicyJobID	The unique identifier joins related tables to the PM_PolicyUser table in the CSM_Reports database.
ReportRunBy	The user who executes the reporting job for the report.

ReportRunDate	The date for the reporting job
---------------	--------------------------------

See [“About creating user-defined templates”](#) on page 624.

See [“Adding a user-defined report template”](#) on page 643.

About the Report Management jobs

In the Monitor > Jobs view, you can view the run status and details for the Report Management jobs.

The Report Management jobs are the following:

Report generation	The job schedules a report.
Dashboard update	The job schedules a dashboard.
Scheduled Reporting Database Purge	The job purges historical and summary data from the reporting database.
Reporting Database Synchronization	The job synchronizes the data from the production database into the reporting database.

See [“Scheduling a report ”](#) on page 636.

See [“Viewing a report”](#) on page 638.

About the View My Reports filter option

If the report supports the filter option, you can filter a report in the **View My Report - Reporting**. A report may not support the filter option. The types of filter that you can apply to a report are different and based on the report.

Predefined Reports and Dashboard descriptions

The Control Compliance Suite Reports and Dashboards include the default reports and dashboards that let you determine the state of the installation. Settings are selected before the report is run.

The result of a report or dashboard may vary based on your permission level.

Table 17-2 Report and Dashboard Descriptions

Name	Description	Location	Customization Support	Job Chaining support
Asset based Policy Completion Status	The report displays data on the policy completion status.	Report Templates	Yes	No
Asset Change Report	The report lets the user compare the two most recent results and display the differences.	Report Templates	Yes	no
Asset Compliance by Technical Check	The report lets users identify the most common failed or passed technical checks.	Report Templates	Yes	Yes
Asset Details Report	The report displays detailed information about the user's managed assets.	Report Templates	No	No
Asset Exception Status Report	The report displays a summary of exceptions that are in place across the IT infrastructure. The report can be used as an auditor report.	Report Templates	Yes	No
Asset Risk Summary	The report displays the asset type, the risk level, and the related technical controls for one standard.	Report Templates	Yes	Yes
Assets at Highest Risk	The report displays the assets that are given a rank that is based on the remediation order that is based on a risk score.	Report Templates	Yes	Yes

Table 17-2 Report and Dashboard Descriptions (*continued*)

Name	Description	Location	Customization Support	Job Chaining support
Comparison of Control Statement Mapping Report	<p>The report lets you compare control statement mappings between the policies or between the policies and a mandate. The title of the generated report is based on your selection.</p> <p>A report that compares policies has the Comparison of Control Statement Mappings between Policies Report title.</p> <p>A report that compares policies and a mandate has the Comparison of Control Statement Mappings between Policies and Mandate Report title.</p>	Report Templates	No	No
Compliance-Exception Impact Analysis	<p>The dashboard displays the compliance level of the selected asset group or folder using two pie charts.</p> <p>The first chart displays the current compliance level with the 'pass', 'fail', and 'other' categories. The 'other' category is comprised of the checks that are exempted, manual review, and N/A.</p> <p>The second chart displays the projected compliance level if all current outstanding exception requests were approved.</p> <p>The dashboard also displays a risk gauge with the current risk score for the selected asset group or folder.</p>	Dashboard Templates	No	No

Table 17-2 Report and Dashboard Descriptions (continued)

Name	Description	Location	Customization Support	Job Chaining support
Compliance Summary	The report lets users view risk scores and compliance status for an asset or an asset group.	Report Templates	No	Yes
Compliance Trend by Technical Standard	<p>The dashboard displays the compliance trends for a maximum of four standards at a time. The dashboard displays two trend charts and a pie chart.</p> <p>The first trend chart displays the 'pass', 'fail', and 'other' trends over time. The second chart displays the corresponding data as a percentage value.</p> <p>The pie chart summarizes the current counts of 'pass', 'fail', and 'other' categories for all of the selected standards. The 'other' category is comprised of the checks that are unmapped, exempted, manual review, and N/A.</p> <p>Ten trend points are plotted on the trend charts.</p>	Dashboard Templates	No	No

Table 17-2 Report and Dashboard Descriptions (*continued*)

Name	Description	Location	Customization Support	Job Chaining support
Compliance Trends for Asset Group(s) or Folder(s)	<p>The dashboard displays the compliance trends for a maximum of four asset groups or folders at a time. The dashboard displays two trend charts and a pie chart. The first trend chart displays the 'pass', 'fail', and 'other' trends over time. The second chart displays the corresponding data as a percentage value. The pie chart summarizes the current counts of 'pass', 'fail', and 'other' categories for all of the selected asset groups or folders. The 'other' category is comprised of the checks that are unmapped, exempted, manual review, and N/A. Procedural and technical controls are considered in the compliance scores and control status counts.</p> <p>Ten trend points are plotted on the trend charts.</p>	Dashboard Templates	No	No
Control Statement Mapping Report	<p>The report lets policy content managers provide details on the interrelationships between a policy and the control statements. Auditors may use the report as documentation of the policy process. The report includes information on checks, questions, entitlements, and third party evidence.</p>	Report Templates	No	No

Table 17-2 Report and Dashboard Descriptions (*continued*)

Name	Description	Location	Customization Support	Job Chaining support
CCS System Change Auditing Report	The report displays key Control Compliance Suite (CCS) change events. The change events may affect either the security of the CCS system and the configuration of the security assessment or policy-related information.	Report Templates	Yes	No
Effective Permissions Report	The report generates information about the detailed effective permissions of one or more control points.	Report Templates	No	No
Failure Trends	The dashboard summarizes the failure trends of the selected asset groups or folders for a specific standard. The failure trends are displayed for the past 13 months which includes the current month.	Dashboard Templates	No	No
Gold Standard	The report assesses the compliance of a system to a Gold Standard system.	Report Templates	Yes	Yes
Overall Compliance	The report displays the individual check results for an asset or an asset group. The user can view, sort, or print the results.	Report Templates	Yes	Yes
Compliance by Asset	The report displays the individual check results for a set of assets.			
Overall Compliance by Standard	The report displays the compliance status of technical checks for a single asset.	Report Templates	Yes	No

Table 17-2 Report and Dashboard Descriptions (*continued*)

Name	Description	Location	Customization Support	Job Chaining support
Overall Policy Compliance Score	The report lets users view roll-up compliance scores for technical checks and lists of technical checks. The report also displays procedural content for the assets that are mapped to the selected policies.	Report Templates	No	No
Evaluation Results Report	This report details about the evaluation job results such as the compliant assets, maximum number of failed checks for a given evaluation job run. The evaluation results report is generated based on the latest job run.	Report Templates	No	Yes
Policy Compliance	The dashboard displays the compliance levels of a maximum of four regulatory mandates. The mandates include regulations and frameworks. Each selected mandate is displayed with a pie chart. The 'other' category is comprised of the checks that are unmapped, exempted, manual review, and N/A. Procedural and technical controls are considered in the compliance score.	Dashboard Templates	No	No

Table 17-2 Report and Dashboard Descriptions (*continued*)

Name	Description	Location	Customization Support	Job Chaining support
Policy Results Report	<p>The report displays information for selected policies. The report lets the user view asset information.</p> <p>The user can view the following for selected policies:</p> <ul style="list-style-type: none"> ■ Risk score ■ Risk rating ■ Technical checks ■ Procedural controls 	Report Templates	No	No
Policy Summary Report	The report displays a summary of a policy.	Report Templates	Yes	No
Remediation Report	The report displays remediation information and detailed evidence information for one or more asset groups or folders for the latest evaluation.	Report Templates	No	No
Simple Permissions Report	The report displays an audit trail of the explicit ACL on control points. The report displays the raw permissions that are granted in the operating system and the application. You can use the report to reconcile effective permissions with the ACL itself.	Report Templates	No	No
Technical Checks Report	The report reviews the technical checks that are applied to the IT infrastructure.	Report Templates	No	No

Table 17-2 Report and Dashboard Descriptions (*continued*)

Name	Description	Location	Customization Support	Job Chaining support
Technical Checks Results Details	The report displays risk scores and compliance status or technical checks for an asset group for the last evaluation.	Report Templates	Yes	Yes
Technical Control Compliance -Risk for Asset Groups or Folders	The dashboard lets you view the risk and the compliance for a maximum of four asset groups or folders. The risk and the compliance information for each asset group or folder is displayed in a separate pie chart or gauge.	Dashboard Templates	No	No
Top Failed Technical Checks	The report identifies the checks that failed most frequently across a set of assets for the latest evaluation during the date range.	Report Templates	Yes	No
Trustee Permissions Report	The report displays information about the permissions of a trustee within the context of managed control points in the Entitlements module.	Report Templates	No	No

Working with reports

You can do the following with a report template:

- Schedule a report template to create a report
See [“Scheduling a report”](#) on page 636.
- View a report
See [“Viewing a report”](#) on page 638.
- Copy a report template
See [“Copying a report template”](#) on page 640.
- Customize a user-defined report template

See [“Customizing a report template”](#) on page 641.

- Customize a report in the report viewer
See [“Customizing a report in report viewer”](#) on page 642.
- Refresh a report in the report viewer
See [“Refreshing a report”](#) on page 638.
- Export a report in the report viewer
See [“Exporting a report”](#) on page 639.
- Print a report in the report viewer
See [“Printing a report”](#) on page 639.
- Delete a user-defined report template
See [“Deleting a user-defined report template”](#) on page 643.
- Add a user-defined report template
See [“Adding a user-defined report template”](#) on page 643.
- Export a user-defined report template
See [“Exporting a report template”](#) on page 644.
- Update a user-defined report template
See [“Updating a report template”](#) on page 645.
- Move a report template
See [“Moving a report template”](#) on page 646.
- Remove a report
See [“Removing a report”](#) on page 639.

Scheduling a report

The Schedule Report wizard generates a report by creating a report generation job. A report is generated on the current data in the reporting database. The reports are generated only on the evaluated assets and standards. After you have created the job, you can view the current job status in Monitor > Jobs view. You can view the report in My Reports.

You must run the Reporting Database Synchronization job before you schedule the report. The synchronization job populates the database with the data in the production database. The synchronization job is an existing job and is in the Monitor > Jobs view. If you create the report before the synchronization job completes its run, you may see a blank report.

If you attach a report, the report displays the date and time of the operating system where the Application Server is installed. In a remote console, the report displays the date and time of the operating system where the Application Server is installed.

Each report has different scalability limitations. For example, the remediation report is designed to handle large result sets. For most of the predefined reports, you should be sure that your report fits within the limitation. A report may fail or cause a system slowdown if the limitation is exceeded.

The report job may fail or cause a system slowdown if the following conditions are met:

- Asset group or folder contains more than 800 assets for a standard
- Standard contains more than 300 checks

You should verify that the total value of the result of the report is within the scalability limits. The total value is found by multiplying the number of assets in the asset group or folder and the number of checks in the standard. The total value should not exceed 240,000.

If you have changed the locale or the time zone on the Application Server, you must restart the Application Server. After you have restarted the service, you should launch the Control Compliance Suite. You should run the Reporting Database Synchronization job and then run your report generation jobs.

The report generation job may send an email to selected users when the report is ready. Report notification must be implemented as a part of the reporting job workflow. The report notification has SMTP requirements.

Each schedule report wizard has a different sequence of panels. The panels that you complete depend on the business logic of the report.

Note: As a prerequisite for the CCS System Auditing report, you must enable auditing from the Settings > General > System Configuration area.

See [“Running a job now”](#) on page 603.

See [“Viewing a report”](#) on page 638.

To schedule a report

- 1 In the **Report Templates** view, select a report template.
- 2 Right-click and select **Schedule Report**.

The wizard that is associated with that report is launched.

- 3 Complete the wizard to create the report generation job.
- 4 You can monitor the status in the Jobs view.

Viewing a report

After a successful report generation job run, the report is listed in My Reports view. The result of a report may vary based on your permission level.

You must synchronize data in the reporting database by running the sync report job before you run the report. The sync report job is in the Jobs > Monitor view.

The report process takes several minutes to generate a view if the selected report has large numbers of the following:

- Assets
- Checks
- Control points
- Policies

You must have sufficient disk space available in the user temp folder on the computer that runs the CCS console in the following conditions:

- You select a report that has a large number of assets, checks, control points, or policies
- You select multiple reports simultaneously

See [“Working with reports”](#) on page 635.

See [“About the My Reports view”](#) on page 618.

To view a report

- 1 In Reporting > My Reports, select a report
- 2 Right-click and select **View**.

The selected report opens in the viewer.

Refreshing a report

You refresh a report in the report viewer. The report must support the refresh option.

See [“Viewing a report”](#) on page 638.

See [“Printing a report”](#) on page 639.

See [“About the My Reports view”](#) on page 618.

To refresh a report

- 1 In the Reporting view, click **My Reports**.
- 2 Select a report and right-click.

- 3 Click **View**.
- 4 In the report viewer, click the Refresh icon.
- 5 In the **Enter Parameter Values** dialog box, provide the required information.
- 6 Select **OK**.

Removing a report

You can remove a report from the My Reports view.

Members of the CCS Administrators role cannot remove a report. If you are assigned as a viewer for the report, you can remove the report from the **My Reports** view.

See [“Working with reports”](#) on page 635.

To remove a report

- 1 In the table pane of Reporting > My Reports, select a report
- 2 Right-click and select **Remove**.
- 3 In the **Confirm** message box, click **Yes**.

Printing a report

You print a report in **View My Report - Reporting** dialog.

See [“Viewing a report”](#) on page 638.

See [“Refreshing a report”](#) on page 638.

See [“About the My Reports view”](#) on page 618.

To print a report

- 1 In Reporting > My Reports, select a report in the table pane.
- 2 Right-click and select **View**.
- 3 In the report viewer, click the **Print Report** icon.
- 4 In the **Print** dialog, select the options and click **OK**.

Exporting a report

After a report generation job run has completed, you can export a report.

You can export the report in the following formats:

Crystal Reports

.rpt

Adobe Reader	.pdf
Microsoft Excel 97 - 2003	.xls
Microsoft Excel 97 - 2003 Data-Only	.xls
Microsoft Word 97 - 2003	.doc
Microsoft Word 97 - 2003 Editable	.rtf
Rich Text	.rtf
XML	.xml

See [“Viewing a report”](#) on page 638.

See [“Printing a report”](#) on page 639.

See [“About the My Reports view”](#) on page 618.

To export a report

- 1 In the Reporting view, click **My Reports**.
- 2 Select a report and right-click.
- 3 Select **View**
- 4 In the report viewer, click the Export Report icon.
- 5 In the **Export Report** dialog box, browse to a folder, if needed.
- 6 Select a format, if needed.
- 7 Click **Save**.

Copying a report template

You can copy a report template to a user-defined folder. If the report template supports customization, you can customize a predefined report template or a user-defined report template.

See [“Working with reports ”](#) on page 635.

See [“Customizing a report template”](#) on page 641.

To copy a report template

- 1 In the table pane of the Report Templates view, select a template.
- 2 Right-click the report template and select **Copy**.

- 3 Navigate to a user-defined folder.
- 4 Right-click in the table panel, and select **Paste** to add the template to the folder.

Customizing a report template

You can customize a report in the user-defined folder or predefined folder. Only certain report templates support customization.

Based on your permission level, you can customize the following report templates in the predefined folder:

- Asset Evaluation Result Change
- Compliance by Technical Check
- Assets at Highest Risk
- Asset Exceptions Status
- Asset Risk Summary
- Gold Standard
- Compliance by Asset
- Overall Compliance by Standard
- Asset Based Policy Completion Status
- Policy Summary Report
- CCS System Auditing
- Asset Group Compliance
- Top Failed Technical Checks

See [“Copying a report template”](#) on page 640.

To customize a report template

- 1 Select a template.
- 2 Right-click and select **Customize**.
- 3 In the **Specify Report Title, Company Name, and Logo** panel, provide a report title for the report. Click **Next**.

You can add a company name and logo, if they are available in the Settings > General view.

- 4 In the **Specify Report Content** panel, you can add or remove the fields from the report. You can reorder the fields.

- 5 Click **Add Fields** to add fields to the report.
The report template must support the feature.
- 6 In the **Add Fields** dialog box, select the fields. Click **OK**.
You can add a maximum of 10 fields.
- 7 Click **Next**.
- 8 In the **Specify Report Group By Information** panel, select the fields that are used to group the displayed results. Click **Next**.
- 9 In the **Select the Location for the Saved Report** panel, navigate to the folder where you want to save the report. Click **Next**.
- 10 In the **Summary** panel, click **Finish**.

Customizing a report in report viewer

You can customize certain reports in the **My Reports** view in **Reporting**. You can find which reports support customization in the Predefined report and dashboard descriptions section. Every report does not support customization. Using the viewer, you may be able to interact with the report by drilling down into charts and table summaries.

When a report is customized in the report viewer, a report is not generated. The selected report is updated with the customized settings. This process is known as Post Customization. If you want to save the settings that you have customized, you must export the report. If you close and relaunch the report, the customized settings are not saved.

See [“Predefined Reports and Dashboard descriptions”](#) on page 627.

To customize a report in report viewer

- 1 In the **My Reports** view, select a report.
- 2 Right-click and select **View**.
- 3 In the report viewer, click **Customize**.
- 4 In the **Specify Report Title, Description, and Logo** page, provide a name for the report.
You can add a company name and logo, if they are available in the Settings > General view.
- 5 In the **Specify Report Content** page, you select the fields for the report. Click **Add** to add fields.
- 6 In the **Add Fields** message box, select a maximum of 10 fields to add to the report.

- 7 Click **OK**.
- 8 Click **Next**
In the **Specify Grouping of Information** page, and then select the groups that should be displayed.
- 9 In the **Summary** page, click **Finish**.

Deleting a user-defined report template

You can delete a user-defined report template. A report template is not saved before deletion. If you delete the template, you must recreate the template if you want to use the template again. You can only delete a template in the user-defined folder.

You must have the appropriate permissions on the user folder to delete a template. If you delete a user-defined template, the deletion does not affect the predefined report template.

You cannot delete a predefined report template.

See [“Working with reports”](#) on page 635.

See [“Copying a report template”](#) on page 640.

See [“Customizing a report template”](#) on page 641.

To delete a user-defined report template

- 1 In the Report Templates tree view, navigate to a user-defined folder
- 2 In the table pane, select a template.
- 3 Right-click and select **Delete**.
- 4 In the **Confirm** message box, click **Yes**.

Adding a user-defined report template

With Crystal Reports 2008 SP1, you can create a report and then add the report to the Control Compliance Suite. You must be a member of the Report Administrator role to add a template.

An installation of the Crystal Reports 2008 SP1 is required to create the template. Crystal Reports 2008 SP1 is not a component of the Symantec Control Compliance Suite installation.

To add a user-defined report template

- 1 In the Reports view, select **Common Tasks**. Click **Add or Update** to open the **Add or Update a report template** wizard.
- 2 In the **Choose an Option - Add or Update a Report Template** panel, select **Add a report template**.
- 3 In the **Specify the Name, Description, and other Properties of the New, User-Defined Report Template** panel, provide the **Report template name**.
- 4 Provide the **Report template description**
- 5 In the **Import template from** box, navigate to and select the report template location.
- 6 In the **Save template to** box, navigate to and then select the folder to save the template.
- 7 Click **Next**.
- 8 In the **Select the Business Objects** panel, select the business objects that are included in the template.
- 9 Check **Allow multiple** if the template supports multiple instances of a business object.
- 10 Select the category type from the **Report template category** drop-down box. The category type is based on the selected business object.
- 11 Click **Next**.
- 12 In the **Summary** panel, click **Finish**.

Exporting a report template

You can export a report template to an RPT file. You can open the file in Crystal Reports 2008 SP1 to modify the file. You can export either user-defined templates or predefined templates.

An installation of the Crystal Reports 2008 SP1 is required to view the exported file. Crystal Reports 2008 SP1 is not a component of the Symantec Control Compliance Suite installation.

To export a report template

- 1 In the table pane, right-click a report template.
- 2 Select **Export Report Template**.
- 3 In the **Save As** dialog box, select the destination and provide a file name.
- 4 Click **Save**.

Updating a report template

You can update an existing report template in the user-defined folder using the **Add or Update a Report Template** wizard. The wizard validates the template's mandatory parameters for each update. A successful validation overwrites the existing template.

We recommend that you should update a template only if you make the following changes:

- Change the field labels
- Change header and footer information
- Add static text
- Change the layout
- Add fields
- Remove fields

The update fails if you alter the template's mandatory parameters. The template update process validates the number of mandatory parameters and the type of mandatory parameters. Parameters that are not mandatory are not checked. If the number of mandatory parameters is incorrect or if you have added mandatory parameters then the update fails.

If you want to change the template's mandatory parameters or if you want to add information to the report we recommend that you create a new template.

The validation only checks the report template's mandatory parameters. If you have two report templates with different information but the same mandatory parameters, you may overwrite the template. For example, if you have two asset reports, report A and report B, and you modify report A. You select report B when you do the update. Report B is overwritten. The report contents may be different but the validation succeeds and one template overwrites the selected template.

An installation of the Crystal Reports 2008 SP1 is required to modify the template. Crystal Reports 2008 SP1 is not a component of the Symantec Control Compliance Suite installation.

To update a user-defined report template

- 1 In the Reports view, select **Common Tasks**. Click **Add or Update** to open the **Add or Update a report template** wizard.
- 2 In the **Choose an Option - Add or Update a Report Template** panel, select **Update a report template**.
- 3 In the **Browse for the Updated .RPT and Choose the Template to Update** panel, navigate to the modified RPT file.

- 4 Select a folder and add the report template to be updated.
- 5 Click **Next**.
- 6 In the **Summary** panel, click **Finish**.
- 7 In the message, click **OK**.

Moving a report template

You can move a user-defined report template from one location to another location. You can move a user-defined template from one user-defined folder to another user-defined folder.

To move a report template

- 1 In the table pane, right-click a report template.
- 2 Select **Move**.
- 3 In the **Move Report Template** dialog box, select the destination folder.
- 4 Click **OK**.
- 5 In the **Reporting** message box, click **OK**.

Editing a report generation job

You can edit a report generation job in the Job view. The job can have only one scheduled run in a 24 hour period. Any changes to the schedule overwrite the existing schedule. If you select the **Run now** option, the option does not affect the scheduled job run. By default, the schedules begin on the current date and the current time.

The Report type determines which steps are available.

To edit a report generation job

- 1 In the Monitor > Jobs view, existing jobs are shown in the table pane. Select a report generation job.
- 2 Right-click and select **Edit job**
The wizard that is associated with that report is launched.
- 3 Complete the wizard to edit the report generation job.

Working with dashboards

Dashboards are a visual analysis that provides a summary of your organization's compliance. Dashboards provide the capability to view the security posture and

assessment trends at a glance. You can also drill down through the hierarchy that represents your organization to see the compliance percentage of each level.

In the **Dashboard Templates** view, you create a dashboard job when you schedule a dashboard template. The dashboard jobs that are created using the dashboard templates are known as summary dashboards.

You can also create the dashboards that contain roll-up data, which is a summary result of the standards' checks and the bv-Control query results. Dashboards consume the summary data from the bv-Control XML export format and the evaluation results of the standards. The dashboard jobs that are created from the roll-up data are known as tiered dashboards.

Note: Tiered dashboards do not summarize results of ESM message data for display.

In the My Dashboards view, you can view the dashboards. In the **Monitor > Jobs** view, you can edit a dashboard update job.

Note: Do not stop the script run, if you see a warning message about the Flash program running slowly. The message sometimes appears when a dashboard is generated.

- Scheduling a summary dashboard
See [“Editing a summary dashboard update job”](#) on page 651.
- Viewing a dashboard
See [“Viewing a tiered dashboard”](#) on page 653.
- Editing a dashboard update job
See [“Editing a summary dashboard update job”](#) on page 651.
- Exporting a dashboard
See [“Exporting a summary dashboard”](#) on page 648.
- Removing a dashboard
See [“Removing a summary dashboard”](#) on page 650.

Managing summary dashboards

Summary dashboards are template-based predefined dashboards of Control Compliance Suite. The predefined dashboard templates are created to address the basic risk and compliance assessment requirement of business organizations. The templates display the compliance level, risks, failure trends, or compliance trends of the selected assets or asset groups.

You can use the dashboard templates and schedule a dashboard job from the **Dashboards Templates** view of the console. You can schedule a Summary dashboard update job on any assets or asset groups from the **Schedule Dashboard** wizard.

See [“Scheduling a summary dashboard update job”](#) on page 649.

See [“Exporting a summary dashboard”](#) on page 648.

See [“Removing a summary dashboard”](#) on page 650.

Viewing a summary dashboard

All the summary dashboards that you schedule from the Dashboard Templates view are listed in the **My Dashboards** view. To view a dashboard, you must have Adobe Flash installed.

You must synchronize data in the reporting database by running the Scheduled Reporting Database Synchronization Job before you run the dashboard job. The job is in the **Jobs > Monitor** view.

The result of a dashboard may vary based on the permission level. From the dashboard window, you can export a dashboard.

To view a summary dashboard

- 1 Go to **Reporting > My Dashboards** view of the console.
- 2 In the My Dashboards view, select a summary dashboard from the list, right-click it, and select **View**.
- 3 To export the summary dashboard to any folder on your local computer, click **Export**.

In the **My Dashboard Preview Pane View - Reporting** window, you can find the following details of the selected summary dashboard:

- Number of assets that were assessed by the summary dashboard.
- Name of the summary dashboard.
- User in whose context the summary dashboard is executing.
- Run date of the summary dashboard.

See [“Exporting a summary dashboard”](#) on page 648.

Exporting a summary dashboard

You can export the dashboards to a folder. You can export from the Home page view or **My Dashboards Preview Pane view - Reporting**.

The result of a dashboard may vary based on your permission level. To view a dashboard, you must have Adobe Flash installed.

You must synchronize data in the reporting database by running the Scheduled Reporting Database Synchronization Job before you run the dashboard. The job is in the **Jobs > Monitor** view.

See [“Viewing a tiered dashboard”](#) on page 653.

To export a summary dashboard

- 1 In My Dashboards, select a dashboard.
- 2 Right-click and select **View**.
- 3 In the **My Dashboards Preview Pane View - Reporting**, click **Export**.
- 4 Navigate to the folder.
- 5 Click **OK**.

Scheduling a summary dashboard update job

The Schedule Dashboard wizard generates a dashboard by creating a dashboard update job. A dashboard views the current data in the Reporting database that is based on a specific criteria. The dashboards are generated only on the evaluated assets and standards.

You start the schedule dashboard wizard in the **Dashboard Templates** view. The wizard guides you through each step necessary for the creation of the dashboard. When the wizard is finished, you remain in the **Dashboard Templates** view. You can view the dashboard in the **My Dashboards** view after the job has completed. You can monitor the job status in the **Monitor > Jobs** view.

You must run the Scheduled Reporting Database Synchronization job before you create the dashboard update job. The dashboard update job populates the database with the last successful synchronization of the data in the production database. The Scheduled Reporting Database Synchronization job is an existing job. If you create the dashboard before the Scheduled Reporting Database Synchronization job completes its run, you may see a blank dashboard.

The dashboard run date is displayed in the Application Server date format. The Failure Trend dashboard has a date range that is always displayed in the English (US) long date format.

If you change the locale or the time zone on the Application Server, you must restart the Application Server. After you restart the service, launch the Control Compliance Suite. You must run the Scheduled Reporting Database Synchronization job and then run the summary dashboard update jobs.

You may not see each step in the procedure. The type of dashboard determines which steps are needed.

See [“Running a job now”](#) on page 603.

To schedule a summary dashboard update job

- 1 In the **Dashboard Templates** view, select a dashboard template.
- 2 Right-click and select **Schedule Dashboard**.
The **Schedule Dashboard** wizard appears.
- 3 In the **Specify Dashboard Name and Description** panel of the wizard, enter the name and description for the summary dashboard update job and click **Next**.
- 4 In the **Select Asset Groups and Folders** panel, select the assets for which you want to run the summary dashboard update job and click **Add**.
- 5 Click **Next**.
- 6 In the **Select Trend Date and Trend Time** panel, set the trend date and time and click **Next**.
Based on the set trend date and time, the evaluation results are displayed on the dashboard.
- 7 In the **Add/Remove Viewers** panel, add or remove the viewers who can be notified through emails to view the dashboard and click **Next**.
- 8 In the **Job Schedule** panel, schedule the summary dashboard update job and click **Next**.
- 9 In the **Set Notification** panel, specify the email addresses of the users who must be notified when the job fails or succeeds, and click **Next**.
- 10 In the **Summary** panel of the wizard, review the details of the created job and click **Finish**.

See [“Editing a summary dashboard update job”](#) on page 651.

Removing a summary dashboard

You can remove a summary dashboard from the **My Dashboards** view.

Members of the CCS Administrators role cannot remove a dashboard. If you are assigned as a viewer for the dashboard, you can remove the dashboard from the **My Dashboards** view.

To remove a dashboard

- 1 Go to **Reporting > My Dashboards** view and select a dashboard.
- 2 Right-click and select **Remove**.
- 3 In the **Confirm** message box, click **Yes**.

See [“Managing summary dashboards”](#) on page 647.

Editing a summary dashboard update job

A dashboard update job can be edited in the Monitor > Job view. The job can only have one scheduled run in a 24 hour period. Any changes to the schedule overwrite the current schedule. It does not affect the scheduled job run if you want to have the job run immediately. By default, the schedule begins on the current date and the current time.

To edit a Summary dashboard update job

- 1 In the Monitor > Jobs view, existing jobs are shown in the table pane.
- 2 In the Jobs view, right-click a Summary dashboard update job, and select **Edit job**
- 3 In the Edit Dashboard Schedule Job wizard, navigate through the panels to edit the Summary dashboard job.

See [“About the job types”](#) on page 596.

See [“Scheduling a summary dashboard update job”](#) on page 649.

Managing tiered dashboards

Tiered dashboard is the hierarchical representation of roll-up data. The roll-up data is a summary of the evaluation results of the Standards checks and the bv-Control query results. Hierarchy in tiered dashboards refers to the creation of sections and nodes, which are scopes representing either a geographical location or a business unit. A tiered dashboard consumes the summary data from the bv-Control reports that are in XML format and the Standards evaluation results.

You can configure multiple dashboards to define the hierarchy that logically represents your organization in different ways. For example, you can configure the dashboards that are based on your corporate network topology, department structures, or geographical locations.

See [“Viewing a tiered dashboard”](#) on page 653.

See [“Creating a tiered dashboard”](#) on page 657.

See [“Editing a tiered dashboard”](#) on page 658.

Getting started with tiered dashboards

Tiered dashboard collects data from either an evaluation result of the Standards module or from an export file of the bv-Control snap-in.

Before you create a tiered dashboard, you must have either of the following completed:

- Evaluation results of assets that are evaluated against a standard
- Query results of any bv-Control snap-in

All users of dashboards must be assigned a role before they can use the application

Use the following table to get you started quickly with dashboards:

Assigning roles	<p>Assign appropriate roles and permission to the users of dashboards.</p> <p>See “About roles and permissions in tiered dashboard” on page 662.</p>
Collecting data	<p>Do one of the following:</p> <ul style="list-style-type: none">■ For bv-Control query results data that are exported to an XML file, you need to set up a data location where the file is stored. The data location must be a network share path of the computer from where the export file is accessed by the dashboard. See “Configuring the data locations” on page 131.■ For the Standards module evaluation data, create and run a scheduled evaluation job. Dashboard update jobs that are scheduled for evaluation nodes of standards module evaluate the assets based on the selected standard at run time. The evaluation results are used for data collection by the dashboard.
Creating dashboard	<p>Create a new dashboard. When you create a dashboard you first configure the settings for the dashboard that define the evaluation criteria for the assessment.</p> <p>See “Creating a tiered dashboard” on page 657.</p>
Configuring an evaluation node	<p>Configuration settings for an evaluation node include selecting the following:</p> <ul style="list-style-type: none">■ Select the evaluation results for the Standards Evaluation Results node or the export file for the bv-Control Query Results node.■ Set the thresholds for the evaluation node.■ Schedule the collection of summary results for assessment. <p>See “Adding an evaluation node” on page 672.</p>

Assessing and
analyzing

After the data is collected and is available to the dashboard, you can begin to view, assess, and analyze the information.

See [“Viewing a tiered dashboard”](#) on page 653.

See [“About trends configuration”](#) on page 675.

See [“Viewing the tiered dashboard reports”](#) on page 678.

Viewing a tiered dashboard

All the tiered dashboards that you create are listed in the **My Dashboards** view. You can view the status and details of the dashboard sections provided you have the requisite view permissions.

You must synchronize data in the reporting database by running the **Scheduled Reporting Database Synchronization Job** before you run the dashboard. The job is in the **Jobs > Monitor** view.

To view a tiered dashboard

- 1 Go to **Reporting > My Dashboards** view of the console.
- 2 In the **My Dashboards** view, select a tiered dashboard from the list, right-click it, and select **View**.
- 3 In the **View Dashboard- Reporting** window, you can find the following tabs for the selected tiered dashboard:
 - Status
 - Details
 - Evaluation Results

This tab is displayed only when you select a Standards Evaluation Results evaluation node.

See [“About the Status tab view”](#) on page 653.

See [“About the Details tab view”](#) on page 656.

About the Status tab view

The **Status** tab of the **View Dashboard - Reporting** window captures the essence of the security assessment information. You can view the current roll-up of the security assessment status in the graphical form for a specific dashboard.

The status of the evaluation node is automatically updated at the time the Standards module evaluation job completes its execution. The status is also updated when the bv-Control schedule is completed.

The dashboard and the section status are also updated if the data collected crosses any threshold values. The last evaluated date-time stamp is displayed for an evaluation node.

When you select a dashboard or an evaluation section on the left pane of the window, the Status tab displays the following information:

Current Overall Status	<p>The dashboard analyzes and summarizes the lower level security assessment details. The dashboard provides a roll-up of the security assessment of the organization that is based on all data that is collected for this dashboard or for individual sections.</p> <p>The overall status display indicate the following security assessment status levels:</p> <ul style="list-style-type: none">■ Critical■ Danger■ Warning■ Normal■ No Data■ Information
Status Trend	<p>This bar chart indicates the security posture of your organization, showing improvement or degradation over a time period. The status is based on the maximum status that the evaluation nodes have attained in a time interval. If there are multiple evaluations in a day, the latest status on that day is considered. The time scale can be changed to suit the needs of your analysis period.</p>
Current Evaluations by Status	<p>This bar chart depicts the security assessment status of all evaluation nodes in this dashboard or the evaluation sections. The evaluation nodes are grouped based on criticality. By grouping, you can quickly determine if there are too many evaluation nodes in the critical or danger status that require immediate attention. The threshold conditions determine the status of the evaluation nodes.</p>
Evaluations Trend	<p>The line graph indicates the number of evaluation nodes that have attained a specific assessment status for a time period. The time period is based on the Trend Window option. The specific assessment status is the average status that the evaluation nodes have attained in a time interval. The average is used because data collection schedules can be different for different evaluation nodes.</p> <p>Note: If an evaluation node does not exist or contains no data then the status, No Data is displayed for the dashboard or the section.</p>

When you select an evaluation node in the left-side pane of the window, the Status tab displays the following information:

Trend Window	<p>Select a trend from the Trend window option, which determines the amount of historical data that is to be displayed in the dashboard.</p>
Node Details	<p>Review the details of the node that you have selected.</p> <p>The following Node Details are displayed for both the bv-Control Query Results and Standards Evaluation Results node.</p> <ul style="list-style-type: none"> ■ Type Displays the type of the selected node. ■ Status Displays the status such as critical, warning, danger, and normal of the selected node. ■ Scope Displays the scope for the selected node. For example, for a bv-Control node, the path of location for the XML file is displayed.
Data	<p>Review the summary data that is collected for the selected node.</p> <p>For the bv-Control Query Results node, the details are as follows:</p> <ul style="list-style-type: none"> ■ Not Found Percent Refers to data of the selected node that is not found ■ Found Percent ■ Objects Not Found Refers to not retrieving the target computers on which bv-Control queries are executed. ■ Objects Found Refers to retrieving the target computers on which bv-Control queries are executed. ■ Objects in Scope Refers to the scope for target computers on which bv-Control queries are executed. <p>For the Standards Evaluation Results node, the details are as follows:</p> <ul style="list-style-type: none"> ■ Compliance Score ■ Risk Score ■ Total Checks ■ Checks Unknown ■ Checks Passed ■ Checks Failed
Custom Thresholds	<p>Review the value of the custom threshold that you have set for the node.</p>

Status Trend	<p>Review the bar chart that shows the status trend of the selected node.</p> <p>Select the time period for which you want to view the status trend from the Time Scale drop-down box.</p> <p>See “About trends configuration” on page 675.</p>
Summary Result Trends	<p>Review the bar chart that shows the current status of the evaluation data for the node.</p> <p>Select the time period for which you want to view the summary results trend from the Time Scale drop-down box.</p>

See [“About the Details tab view”](#) on page 656.

About the Details tab view

The **Details** tab displays the evaluation results of the Standards and the bv-Control query results. You can print or export the grid information to a file.

When you select a dashboard or an evaluation section on the left pane of the **View Dashboard - Reporting** window, the **Details** tab displays the following:

- The roll-up of the evaluation results from all the nodes or sections in the dashboard or evaluation section.
- The evaluation node name, hierarchical path, and the time when the evaluation node was last updated.
- The results that are grouped based on the security assessment status. You can regroup the evaluation nodes based on the status or the type of evaluation node. You can drag the columns to group the evaluation nodes in the window.

When you select an evaluation node on the left pane of the window, the tab displays the assets in the evaluation results. The predefined assigned attributes and values of the assets are also displayed for the evaluation node. If you add new attributes to an asset, then the details of the new fields are also listed for the evaluation node.

You can click on the column chooser icon to select or unselect the attribute columns.

Note: You can view the data of only those assets for which you have the requisite permission.

See [“About the Status tab view”](#) on page 653.

See [“Viewing a tiered dashboard”](#) on page 653.

About the Evaluation Results tab view

The **Evaluation Results** tab displays the evaluation results of a standard that is evaluated on an asset. The tab displays the details of the number of assets that are evaluated and the properties of the checks that are executed on the assets. The tab also contains a graphical representation of the risk score, compliance score, and the result summary of the assets.

The various fields of the tab and their descriptions are as follows:

Standard Evaluated	Name of the standard that evaluated the asset.
Asset Name	Name of the asset.
Data Collection Date	Date when data is collected from the assets for the selected standard.
Evaluation Date	Date when evaluation of the collected data for the selected standard is performed.
Column Chooser	<div>Lets you select the properties of the checks to display at the bottom pane of the view.</div> <div>You can right-click a check and select Export to export the check details to a file.</div> <div>Click the column chooser icon to display the dialog box.</div>

See [“Working with Evaluation Results”](#) on page 541.

Creating a tiered dashboard

A tiered dashboard can be created and listed in the **My Dashboards** view of the console. A tiered dashboard is executed as a tiered dashboard update job from the My Dashboards or from the **Monitor> Jobs** view of the console.

Note: You must synchronize data in the reporting database by running the **Scheduled Reporting Database Synchronization Job** before you run the tiered dashboard update job. The job is in the **Monitor> Jobs** view.

To create a tiered dashboard

- 1 Go to **Reporting > My Dashboards** in the console.
- 2 In the **My Dashboards** view, right-click on the table pane and select **Create Tiered Dashboard**.

- 3 In the **Specify Name and Description** panel of the **Create Tiered Dashboard** wizard, enter the name and description and then click **Next**.
The **Description** is optional.
- 4 In the **Create Dashboard Nodes** panel, you can do the following and then click **Next**.
 - Create a section.
 - Create and edit node.
 - Add and manage a trustee.
 - Set up a notification for the dashboard.
 - Copy, paste, rename, and delete a dashboard.
- 5 In the **Job Schedule** panel, select an option of scheduling the dashboard job that you create and then click **Next**.
- 6 In the **Job Notification** panel, setup the notification for the success or failure of the scheduled dashboard job and then click **Next**.
- 7 In the Summary panel, review the details of the dashboard job that you create and then click **Finish**.

See [“Editing a tiered dashboard”](#) on page 658.

See [“Configuring an email notification alert for tiered dashboards”](#) on page 674.

Editing a tiered dashboard

You can edit a tiered dashboard from the My Dashboards view of the console.

To edit a tiered dashboard

- 1 Go to **Reporting > My Dashboards** view in the console.
- 2 In the My Dashboards view, do one of the following:
 - Right-click on the selected tiered dashboard and select **Edit**.
 - Click **Manage Tiered Dashboards > Edit**
- 3 In the **Edit Dashboard** dialog box you can edit any of the following and then click **OK**.
 - Create and edit an evaluation node.
 - Add and manage a trustee.
 - Set up a notification for the dashboard.

- Copy, paste, and delete a dashboard.

See [“Creating a tiered dashboard”](#) on page 657.

See [“Viewing a tiered dashboard”](#) on page 653.

Copying and pasting a tiered dashboard

You can create a copy of an existing tiered dashboard that is displayed in the **My Dashboards** view. When you copy and paste a dashboard, all the permissions assigned to the user are also copied.

Note: On copying a tiered dashboard, the permissions stamped on the dashboard are also copied.

To copy a tiered dashboard

- 1 Go to **Reporting > My Dashboards** view and select a tiered dashboard.
- 2 In the My Dashboards view, do one of the following:
 - Right-click on the selected tiered dashboard and select **Copy**.
 - Click **Manage Tiered Dashboards > Copy**
- 3 On the same My Dashboards view do one of the following to paste the copied dashboard:
 - Right-click on the workspace and select **Paste Tiered Dashboard**
 - Click **Manage Tiered Dashboards > Paste Tiered Dashboard**

See [“Copying and pasting an evaluation section”](#) on page 674.

See [“Copying and pasting an evaluation node”](#) on page 674.

Renaming a tiered dashboard

You can change the current name of a tiered dashboard by renaming it in the **My Dashboards** view.

To rename a tiered dashboard

- 1 Go to **Reporting > My Dashboards** view of the console.
- 2 In the **My Dashboards** view, do one of the following:
 - Select a tiered dashboard to rename and click **Rename**
 - Click **Manage Tiered Dashboards > Rename**
- 3 In the **Rename Dashboard** dialog box, provide the new name.

See [“Managing tiered dashboards”](#) on page 651.

Editing a tiered dashboard job schedule

You can edit the job schedule of a tiered dashboard from the **My Dashboards** view of the console. Initially, you can schedule the dashboard update job when creating it using the **Create Tiered Dashboards** wizard.

To edit a tiered dashboard job schedule

- 1 Go to **Reporting > My Dashboards** view of the console.
- 2 In the **My Dashboards** view, do one of the following:
 - Select a tiered dashboard and then click **Edit Schedule**
 - Click **Manage Tiered Dashboards > Edit Schedule**
- 3 In the **Schedule Dashboard** dialog box, edit the job schedule options, and then click **OK**.

Editing a tiered dashboard job notification

You can edit the job notification of a tiered dashboard from the **My Dashboards** view of the console. Initially, you can set the dashboard update job notification when creating it using the **Create Tiered Dashboards** wizard. Control Compliance Suite sends an email notification whenever a dashboard job succeeds or fails.

To edit a tiered dashboard job notification

- 1 Go to **Reporting > My Dashboards**.
- 2 In the **My Dashboards** view, do one of the following:
 - Select a tiered dashboard and then click **Edit Dashboard Job Notification**
 - Click **Manage Tiered Dashboards > Edit Dashboard Job Notification**
- 3 In the **Job Notification** dialog box, edit the job notification for the **Success** and the **Failure** tabs, and click **OK**.

Importing a tiered dashboard

You can import a tiered dashboard from an XML file into the **My Dashboards** view. The XML file must adhere to a specific schema. A new dashboard is created after you import an XML file provided that no dashboard of the same name already exists.

You can import multiple XML files to create multiple dashboards. An hour glass icon appears during the import operation of the selected dashboard. A status dialog box appears when the import operation completes.

Note: Depending on the type of XML editor, the threshold operators, < or > might appear in the exported XML file as < or >, respectively. You must retain the operators as < or > in the XML file during dashboard import.

To import a tiered dashboard

- 1 Go to **Reporting > My Dashboards** view of the console.
- 2 In the **My Dashboards** view, do one of the following:
 - Right-click on the table pane and select **Import Tiered Dashboard**.
 - Click **Manage Tiered Dashboards > Import Tiered Dashboard**.
- 3 In the **Select File to Import** dialog box, select the xml file, and then click **Open**.

See [“Exporting a tiered dashboard”](#) on page 661.

Exporting a tiered dashboard

You can export a tiered dashboard to an XML file. You can use an XML editor to read and edit the file later. The exported dashboard XML file contains all the required and mandatory information to recreate a dashboard. The XML file contains comments for each element for you to edit the XML file. You must have the appropriate permissions to export specific evaluation sections of a dashboard.

An XML file is saved in the location that you select. An hour glass appears while the export operation is in progress. A status dialog box appears when the export operation completes.

Note: Depending on the type of XML editor, the threshold operators, < or > might appear in the exported XML file as, < or > respectively. You must retain the operators as < or > in the XML file during dashboard import.

The exported XML file contains the following information:

- Dashboard attributes
- Event notification
- View permissions
- Evaluation node and evaluation section attributes

To export a tiered dashboard

- 1 Go to **Reporting > My Dashboards** view.
 - 2 In the **My Dashboards** view, do one of the following:
 - Click **Manage Tiered Dashboards > Export**.
 - right-click a dashboard and select **Export**
 - 3 Save the dashboard as an XML file when the **File Save** dialog box opens.
- See [“Importing a tiered dashboard”](#) on page 660.

Editing a tiered dashboard update job

You can edit a tiered dashboard update job from the **Monitor > Jobs** view.

See [“Creating a tiered dashboard”](#) on page 657.

See [“About jobs”](#) on page 595.

To edit a tiered dashboard update job

- 1 Go to **Monitor > Jobs** view of the console.
- 2 In the **Jobs** view, right-click a dashboard update job and select **Edit Job**.
- 3 In the **Edit Tiered Dashboards** wizard, edit the properties of the job and reschedule it.

About roles and permissions in tiered dashboard

Control Compliance Suite can restrict permission for any user or group to any specific network data. This restriction of permission is leveraged in tiered dashboards through roles that are defined with permission to perform specific tasks.

The following default roles are defined for the tiered dashboard:

- Report Result Viewer
- Reporting Administrator
- CCS Administrator

Using the role-based access control feature, permissions can be given at the dashboard level or at the section level of a dashboard.

By default, view permissions over dashboards and sections are assigned to all users who belong to any of the default roles. Dashboard trustees are created to assign permissions to few selected users to view a dashboard or a dashboard section. The Manage Trustees option of the Edit Dashboard dialog box creates the dashboard trustee for the tiered dashboard.

Users with the following roles can modify the View permissions:

- CCS Administrator role
- Report Result Viewer role
- Reporting Administrator role

See [“About the predefined roles in tiered dashboards”](#) on page 663.

See [“About view permissions for users in Report Result Viewer role”](#) on page 664.

See [“About manage permission for users in Reporting Administrator role”](#) on page 665.

About the predefined roles in tiered dashboards

The tiered dashboards provide predefined roles that you can use to delegate permissions for your users.

The tiered dashboards related tasks that a user of a specific role can perform are as follows:

Report Result Viewer	<p>User who is added in the Report Result Viewer role can do the following at the dashboard and section level:</p> <ul style="list-style-type: none">■ View the tiered dashboard■ View the dashboard details report■ View the dashboard trends report■ View the jobs, the job runs, and the details of a job in the Job Management view of the console.
----------------------	--

Reporting Administrator

User who is added in the Reporting Administrator role and is the creator of a dashboard can do the following at the dashboard and section level:

- Create a dashboard
- Edit a dashboard
- Rename a dashboard
- Copy and paste a dashboard
- Edit the dashboard job notification
- Import and export a dashboard
- Setup a dashboard status notification
- View the dashboard details and trends report
- View the dashboard
- Assign permission to another user to manage the dashboard
- Run and schedule the tiered dashboard update job

User who is added in the Reporting Administrator role and assigned permission on a dashboard or a section can do the following:

- Create a dashboard
- Edit a dashboard or a section
- View the dashboard

You can view the section of the dashboard for which you have the permission.
- View the dashboard details and trends report

You can view the reports for the section of the dashboard for which you have the permission.
- Import and export a dashboard
- Run a tiered dashboard update job

See [“Predefined roles”](#) on page 80.

About view permissions for users in Report Result Viewer role

A CCS Administrator or a Reporting Administrator user can edit the view permission of a user that belongs to the Report Result Viewer role. You can edit the view permission of a tiered dashboard user using the Manage Trustees option of the Edit Dashboard dialog box.

The user with view permission at the dashboard level can do the following:

- View the dashboard details report and the dashboard trends report for a tiered dashboard.

The dashboard details and trends report are accessed for a Tiered dashboard that is selected in the My Dashboards view.

- Require requisite permission to view the assets and standards for a Standards Evaluation Results node in the View Dashboard - Reporting window.
The user must have read permission on assets and standards to view the Details and the Evaluation Results tabs of the Standard Evaluation Results node.
See [“Predefined roles”](#) on page 80.
- Status tab
- Details tab
- Evaluation Results tab

The user with view permission at the section level of a dashboard can do the following:

- View the section and its evaluation nodes in the View Dashboard-Reporting window. The child sections can also be viewed.
The user cannot view the evaluation nodes of the parent dashboard or the parent section.
- The user must have read permission on assets and standards to view the Details and the Evaluation Results tabs of the Standard Evaluation Results node.

See [“About manage permission for users in Reporting Administrator role”](#) on page 665.

See [“About the predefined roles in tiered dashboards”](#) on page 663.

About manage permission for users in Reporting Administrator role

A CCS Administrator or a Reporting Administrator user can assign permission to users to manage a tiered dashboard. You can assign permission to a user using the Manage Trustees option of the Create or Edit Tiered Dashboards wizard.

The following points apply to the user with permission to manage a tiered dashboard:

- Create a new dashboard and have permission on all the tasks that are related to the dashboard and the dashboard update job.
- The following tasks cannot be performed by the user who is not a creator of the dashboard but is assigned permission to manage the tiered dashboard:
 - Edit Dashboard Job Notification
 - Edit Schedule
 - Delete
 - Rename

- Set up notification

The following points apply to the user with permission to manage at the section level of a dashboard:

- Create a new dashboard and have permission on all the tasks that are related to the dashboard and the dashboard update job.
- The following tasks cannot be performed by the user who is not a creator of the dashboard but is assigned permission to manage the section of a tiered dashboard:
 - Edit Dashboard Job Notification
 - Edit Schedule
 - Delete a dashboard
 - Rename a dashboard
 - Setup dashboard notification
- Any tasks that are to be performed for the parent section or dashboard

See [“About view permissions for users in Report Result Viewer role”](#) on page 664.

See [“About the predefined roles in tiered dashboards”](#) on page 663.

About threshold settings in tiered dashboard

You can define thresholds for all the security assessment status levels of a Tiered dashboard's evaluation node. If the set threshold condition for an evaluation node does not evaluate to true, then the node's security assessment status is Normal. If the set threshold condition for an evaluation node evaluates to true, then the associated status level is the security assessment status of the evaluation node.

Configuring the threshold for a status level involves defining the check fields, relational operator, and the check reference value. The check fields vary depending on whether you have selected a Standards Evaluation Results node or a bv-Control Query Results node. The check field values are derived from the evaluation results of the Standards module and the summary results' data fields of the bv-Control queries.

We recommend that you use the same check field for the different status levels that are defined for the evaluation node. Also, define thresholds in such a way that one of them always evaluates to true.

See [“About the threshold types ”](#) on page 667.

See [“About status calculation”](#) on page 668.

About the threshold types

Threshold conditions are configured for the evaluation nodes to generate customized dashboard reports and information about the dashboard status. The types of thresholds that can be configured for an evaluation node are Global Threshold, Custom Threshold and No Thresholds (Information only node). All the threshold types can be set and associated with the evaluation nodes when you create the nodes through the **Create Tiered Dashboards** wizard.

The types of thresholds and their descriptions are as follows:

Global Threshold	<p>Use this threshold type to set conditions and apply them to all the evaluation nodes of the same type.</p> <p>You can set the global thresholds from the General view of the console. You can access the option, Settings > General > Tiered Dashboards > Global Thresholds Settings to configure the global thresholds.</p>
Custom Threshold	<p>Use this threshold type to set the threshold conditions specific to an evaluation node. You can set the threshold conditions for the evaluation node through the Create Tiered Dashboards wizard.</p>
No Thresholds (Information only node)	<p>Use this threshold type when you want to retrieve summary data of evaluation nodes for which no threshold conditions are set.</p>

See [“About the threshold check fields”](#) on page 667.

See [“About status calculation”](#) on page 668.

About the threshold check fields

Check fields are threshold parameters for which the threshold values are set for a node.

The following check fields are available for the Standards Evaluation Results node:

- Compliance Score (%)
- Total Checks
- Checks Passed
- Checks Failed
- Checks Unknown
- Risk Score

The following check fields are available for the bv-Control Query Results node:

- Objects in Scope
- Objects Found
- Objects Not Found
- Found Percent
- Not Found Percent

See [“About the relational operators”](#) on page 668.

About the relational operators

The dashboard evaluation node configuration supports the following relational operators for comparing the check field values and the reference:

< (Less Than)	Values that are smaller than the user-selected value.
> (Greater Than)	Values that exceed the user-selected value
<= (Less Than or Equal To)	Values that are smaller than or are equal to the user-selected value.
= (Equal To)	Values that match the user-selected value.
>= (Greater Than or Equal To)	Values that exceed or are equal to the user-selected value.

See [“About status calculation”](#) on page 668.

About status calculation

The summary data collected by an evaluation node is evaluated against the reference values as configured in the threshold settings. If a threshold condition does not evaluate to true, then the evaluation node's security assessment status is Normal. If a threshold condition evaluates to true, then the associated status level is the security assessment status of the evaluation node.

See [“Example of status calculation for Standards Evaluation Results node”](#) on page 669.

See [“Example of status calculation for bv-Control Query Results node”](#) on page 669.

Example of status calculation for Standards Evaluation Results node

You can set the criticality of your environment in different ways. For example, you can define the criticality for your environment, based on a percentage of compliance.

To set the status condition that is based on 85% compliance, you can use the Standards evaluation results

Table 17-3 Criticality status based on compliance percentage

Status	Condition	Operator	Value
Critical	Compliance Score (%)	<	50.00
Danger	Compliance Score (%)	<	70.00
Warning	Compliance Score (%)	<	85.00
Normal	Compliance Score (%)	>=	85.00

To set the status condition that is based on the total number of checks that are passed, you can use the Standards evaluation results.

Table 17-4 Criticality status based on the total number of checks passed

Status	Condition	Operator	Value
Critical	Compliance Score (%)	<	50.00
Danger	Checks Failed	>=	50.00
Warning	Check Unknown	>=	20.00
Normal	Checks Passed	>=	50.00

See [“Managing tiered dashboards”](#) on page 651.

Example of status calculation for bv-Control Query Results node

You can use bv-Control query results to set the status condition that is based on 85% of found objects.

Table 17-5 bv-Control query configuration

Status	Condition	Operator	Value
Critical	Objects Found	<	15.00
Danger	not used	not used	not used
Warning	not used	not used	not used
Normal	Objects Found	>=	85.00

See [“Managing tiered dashboards”](#) on page 651.

Configuring tiered dashboards

Dashboard configuration involves tasks that are related to creating and modifying the sections and nodes of the dashboard.

Dashboard configuration includes the following:

- Adding a node
See [“Adding an evaluation node”](#) on page 672.
- Editing a node
See [“Editing an evaluation node”](#) on page 673.
- Deleting a node
See [“Deleting an evaluation node”](#) on page 673.
- Copying and pasting an evaluation section
See [“Copying and pasting an evaluation section”](#) on page 674.
- Copying and pasting an evaluation node
See [“Copying and pasting an evaluation node”](#) on page 674.
- Configuring the email alerts
See [“Configuring an email notification alert for tiered dashboards”](#) on page 674.

See [“Managing tiered dashboards”](#) on page 651.

About types of evaluation nodes

An evaluation node represents a scope of assets or query reports, which are to be assessed by Control Compliance Suite.

A Standards Evaluation Results node represents a scope of assets that are evaluated against a specific standard.

A bv-Control Query Results node represents a scope of query reports. The query reports are exported into the XML files after executing the bv-Control queries on the assets.

See [“Adding an evaluation node”](#) on page 672.

Assigning roles and permissions to users of tiered dashboard

You can associate a user or group with any predefined role that is specific to dashboard and assign permissions. The predefined roles that are specific to dashboard are Report Result viewer and Reporting Administrator. You can assign or revoke permission to a user or a group using the Manage Trustee option of the Create Tiered Dashboards wizard. You can edit the permissions in the **Edit Dashboard** dialog box.

To revoke permission completely for a user, you must remove the user from the dashboard specific role in the Roles view of the console.

To assign permission to users or groups on a specific dashboard or an evaluation section

- 1 Go to Settings > Roles view of the console.
- 2 In the Roles view, right-click any of the dashboard related roles and select **Add Users and Groups** and add a user or group.
See [“Adding users and groups to a role”](#) on page 89.
- 3 Go to **Reporting > My Dashboards** view of the console
- 4 In the **My Dashboards** view, right-click a dashboard and select **Edit**.
- 5 In the **Edit Dashboard** dialog box select the dashboard or section and then click **Manage Trustees**.
- 6 In the **Manage Trustees** dialog box, click **Add Users and Groups** to assign a user or group to a role.
In the **Manage Trustees** dialog box, you can view the list of users and groups that are associated with a role.
- 7 In the **Select Users or Groups** dialog box, select a role name and associate the users or groups that are configured for the role and click, **Update Users and Groups**.
- 8 In the **Manage Trustees** dialog box, click **Update Permissions**.
- 9 In the **Edit Dashboard** dialog box, click **OK**.

To revoke permission for a user or group from a specific dashboard or an evaluation section

- 1 Go to **Reporting > My Dashboards** view of the console
- 2 In the **My Dashboards** view, right-click a dashboard and select **Edit**.
- 3 In the **Edit Dashboard** dialog box select the dashboard or section for which you want to revoke permission and click **Manage Trustees**.
- 4 In the **Manage Trustees** dialog box, select the user name or group name and the corresponding role name and click **Remove**.
- 5 In the **Manage Trustees** dialog box, click **Update Permissions**.
- 6 In the **Edit Dashboard** dialog box, click **OK**.

Adding an evaluation node

You can use the **Edit Dashboard** dialog box to add evaluation nodes to an existing tiered dashboard. You can also use the **Create Tiered Dashboards** wizard to add a new evaluation node to the tiered dashboard.

A tiered dashboard can contain evaluation nodes of the following types:

- Standards Evaluation Results
- bv-Control Query Results

To add an evaluation node

- 1 Go to **Reporting > My Dashboards** view of the console.
- 2 In the **My Dashboards** view, right-click a dashboard and select **Edit**.
- 3 In the **Edit Dashboard** wizard, select the type of node from the drop-down box, and click **Add Node**.

You can select either **bv-Control Query Results** node or **Standards Evaluation Results** node from the drop-down box.

- 4 In the displayed dialog box, enter the required values to create the following nodes:
 - For a Standards Evaluation Results node, enter the required values in the dialog box.
 - For a bv-Control Query Results node, enter the required values in the dialog box.

See [“Editing an evaluation node”](#) on page 673.

Editing an evaluation node

You can edit either the bv-Control Query Results node or the Standards Evaluation Results node of a tiered dashboard.

To edit an evaluation node

- 1 Go to **Reporting > My Dashboards** view of the console.
- 2 In the **My Dashboards** view, right-click a dashboard, and select **Edit**.
- 3 In the **Edit Dashboard** dialog box, select and expand the dashboard to the level of the evaluation node.
- 4 Select the evaluation node and click **Edit Node**.
A dialog box corresponding to the selected node type is displayed.
- 5 In the displayed dialog box, edit the required values for the following evaluation nodes:
 - For a Standards Evaluation Results node, enter the required values in the dialog box.
 - For a bv-Control Query Results evaluation node, enter the required values in the dialog box.

See [“Adding an evaluation node”](#) on page 672.

See [“Deleting an evaluation node”](#) on page 673.

Deleting an evaluation node

You can delete an evaluation node that is added to a tiered dashboard. When creating a tiered dashboard, you can delete an evaluation node from the **Create Tiered Dashboards** wizard. You can also delete an existing evaluation node through the **Edit Dashboard** dialog box.

Note: Data of the evaluation node is deleted once you delete the evaluation node.

To delete an evaluation node

- 1 Go to **Reporting > My Dashboards** view of the console.
- 2 In the **My Dashboards** view, right-click a dashboard and select **Edit**.
- 3 In the **Edit Dashboard** dialog box, select and expand the dashboard to the level of the evaluation node.
- 4 Select the evaluation node and click **Delete**.

See [“Editing an evaluation node”](#) on page 673.

Copying and pasting an evaluation section

You can copy and paste an evaluation section when creating a tiered dashboard using the **Create Tiered Dashboards** wizard. You can also copy and paste a section when editing the tiered dashboard using the **Edit Dashboard** dialog box.

Note: On copying a section of the dashboard, all the permissions that are stamped on the section are also copied.

To copy and paste an evaluation section

- 1 Go to **Reporting > My Dashboards** view of the console.
- 2 In the **My Dashboards** view, do one of the following:
 - Click **Create Tiered Dashboards** to create a dashboard.
 - Right-click a dashboard and select **Edit** to edit a dashboard.
- 3 In the wizard or the **Edit Dashboard** dialog box, select the section of a dashboard that you want to copy and click **Copy**.
- 4 Navigate to the level of a dashboard and then click **Paste**.

See [“Copying and pasting an evaluation node”](#) on page 674.

Copying and pasting an evaluation node

You can copy and paste an evaluation node of a tiered dashboard through the **Create Tiered Dashboard** wizard and the **Edit Dashboard** dialog box.

To copy and paste an evaluation node

- 1 Go to **Reporting > My Dashboards** view of the console.
- 2 In the **My Dashboards** view, right-click a dashboard and then select **Edit**.
- 3 In the **Edit Dashboard** dialog box, select a section of a dashboard and navigate to the node that you want to copy and click **Copy**.
- 4 Navigate to the level of a section and then click **Paste**.

See [“Copying and pasting an evaluation section”](#) on page 674.

Configuring an email notification alert for tiered dashboards

You can configure an email notification alert for the tiered dashboards.

You can configure an email notification for the following tasks:

- Status change of a tiered dashboard update job

The status of the tiered dashboard update job can change to either success or failure.

■ Status change of a dashboard.

A dashboard's status can change if the status of a section or an evaluation nodes changes.

To configure email notification for a tiered dashboard job

- 1 Go to **Reporting > My Dashboards** in the console.
- 2 In the **My Dashboards** view, right-click a dashboard and select **Edit Dashboard Job Notification**.
- 3 In the **Job Notification** dialog box, enter the values for the required fields.

To configure email notification for a tiered dashboard

- 1 Go to **Reporting > My Dashboards** in the console.
- 2 In the **My Dashboards** view, select **Manage Tiered Dashboards > Create Tiered Dashboards** or **Manage Tiered Dashboards > Edit**.
- 3 In the **Create Tiered Dashboards** wizard or **Edit Dashboard** dialog box navigate to the **Create Dashboards** Node panel and click **Setup Notification**.
- 4 In the **Setup Notification** dialog box, enter the values of the fields for setting an email notification.

About trends configuration

The tiered dashboard lets you view the trends in the security assessment posture of your organization over a period of time. To view the trends, you must add an evaluation node and schedule data collection for a tiered dashboard.

See [“Adding an evaluation node”](#) on page 672.

Trends define the amount of historical data that is displayed for an evaluation node. You can set the default trends for an evaluation node when creating it using the **Create Tiered Dashboards** wizard. The trends are displayed based on the time scale that is set for the evaluation node. The time-scale setting defines the frequency of display of the data. You can configure various types of trends and time-scale for an evaluation node.

By default, in the tiered dashboard's reporting view, all data that you collect from the dashboard's creation date to the current date are displayed. You can view the status trends of the evaluation node for the selected time scale in the Status tab of the **View Dashboard- Reporting** window.

Dashboard details and trends reports can also be generated and viewed for the configured trends.

See [“About configuring trends for evaluation nodes ”](#) on page 676.

See [“Calculation of time interval - Example 1”](#) on page 676.

See [“Calculation of time interval - Example 2”](#) on page 678.

About configuring trends for evaluation nodes

Evaluation node trends are the latest evaluation data that is collected by the evaluation node. For example, if you want to view the trends for the last week on a daily basis, then the latest data that is collected in the week is displayed.

You can configure trends for an evaluation node of the tiered dashboard in the following ways:

- Set the default trends and time scale for the evaluation nodes when creating it through the **Create Tiered Dashboards** wizard.
You can set the default trend and time scale in the **Create Dashboard Nodes** panel of the wizard. Data is collected for the evaluation node based on this default trends and time-scale configuration.
- Set the trends for the evaluation nodes when viewing it in the **View Dashboard-Reporting** window.
You can modify the status trends of the evaluation node when viewing the dashboard in the **View Dashboard-Reporting** window. In the **View Dashboard - Reporting** window, the view at the dashboard or section level displays the status trends of the latest updated evaluation node.
- Set the trends and time scale of the evaluation nodes in the Dashboard Details and Trends report.
The Dashboard Details and Trends reports updates and displays the report instantly as per the configured trends.

See [“Viewing the tiered dashboard reports”](#) on page 678.

See [“Calculation of time interval - Example 1”](#) on page 676.

See [“Calculation of time interval - Example 2”](#) on page 678.

Calculation of time interval - Example 1

The Trend Window is given as the Last Month, with the Current Date given as the date of entry, in this example 3/1/2007. The Trend Start Date would then be 2/1/2007 and the Trend End Date would be 2/28/2007.

If the Time Scale value is Weekly, the time intervals are based on the days in the week. For calculation purposes, Weekly starts on Sunday and ends on Saturday. The first date is the Trend Start Date, which is as per this example is 2/1/2007(Thursday). The last date is Trend End Date, which as per this example

is 2/28/2007 (Wednesday). The complete calendar weeks between the first and the last date start on Sundays and end on Saturdays.

Based on the example the five time intervals and their display dates are as follows:

2/1/2007 (Thursday) - 2/3/2007 (Saturday)	Displays as 2/3/2007
2/4/2007 (Sunday) - 2/10/2007 (Saturday)	Displays as 2/10/2007
2/11/2007 (Sunday) - 2/17/2007 (Saturday)	Displays as 2/17/2007
2/18/2007 (Sunday) - 2/24/2007 (Saturday)	Displays as 2/24/2007
2/25/2007 (Sunday) - 2/28/2007 (Wednesday)	Displays as 3/03/2007

The time interval shows the time period in the **Trend Window** for which data is grouped and the trends are calculated. The display value is the value shown as X-axis labels.

If the Time scale value is Daily, then the time intervals are based on the days in the month.

The 28 time intervals and their display dates are the following:

2/1/2007	Displays as 2/1/2007
2/2/2007	Displays as 2/2/2007
2/3/2007	Displays as 2/3/2007
2/4/2007	Displays as 2/4/2007
2/5/2007	Displays as 2/5/2007
...	..
...	..
2/27/2007	Displays as 2/27/2007
2/28/2007	Displays as 2/28/2007

The time interval shows the time period in the Trend Window for which data is grouped and the trends are calculated. The display value is the value shown as X-axis labels.

See [“Managing tiered dashboards”](#) on page 651.

Calculation of time interval - Example 2

The Trend Window is given as Last 30 Days, with the Current Date given as the date of entry, in this case 3/1/2007. The Trend Start Date would then be 1/31/2007 and the Trend End Date would be 3/1/2007.

If the time scale value is Monthly, the three time intervals and their display dates are as follows:

1/31/2007 - 1/31/2007 Displays as Jan 2007

2/1/2007 - 2/28/2007 Displays as Feb 2007

3/1/2007 - 3/1/2007 Displays as Mar 2007

The time interval shows the time period in the Trend Window for which data is grouped and the trends are calculated. The display value is the value shown as X-axis labels.

See [“Managing tiered dashboards”](#) on page 651.

Viewing the tiered dashboard reports

Tiered dashboard reports show the trends and the summary details of the evaluation nodes. The dashboard reports are displayed in a new window. You can export the details and the trends report to any format such as a PDF, XLS, RTF.

The following are the types of tiered dashboards reports:

Dashboard Details report	Displays the details of the evaluation node, the summary results data and the assessment status for the node. The information is in a graphical format.
Dashboard Trends report	Displays the graphical view of the security assessment posture of your organization for the specified time period. Prints the Status Trend and the Evaluations Trends for all the levels of the dashboard.

See [“Viewing the dashboard details report ”](#) on page 679.

See [“Viewing the dashboard trends report”](#) on page 679.

Viewing the dashboard details report

You can view the dashboard details report for a tiered dashboard from the **My Dashboards** view.

The details report is displayed in the **Dashboard Details Report** window.

You can view the following details in the window:

- Current overall status
- Status trends
- Current evaluation by status
- Evaluation trends

To view the dashboard details report

- 1 Go to **Reporting > My Dashboards** view of the console.
- 2 In the **My Dashboards** view, select a tiered dashboard and then right-click to select **View Details Report**.
- 3 In the **Dashboard Details Report** view, select the following options and check **Show Details**.
 - Set the trend of the data collection from the **Trend window** drop-down box.
 - Set the frequency scale of displaying the data in the **Time scale** drop-down box.
- 4 Click **Apply**.

See [“Viewing the dashboard trends report”](#) on page 679.

Viewing the dashboard trends report

You can view the dashboard trends report for a tiered dashboard from the **My Dashboards** view.

The trends report is displayed in the **Dashboard Trends Report** window in which you can view the following details of the dashboard:

- Status trends
The status trends are displayed for the dashboard, section, and the evaluation node levels.
- Evaluation trends
The evaluation trends are displayed for the dashboard and the section level only.

To view the dashboard trends report

- 1** Go to **Reporting > My Dashboards** view of the console.
- 2** In the **My Dashboards** view, select a tiered dashboard and right-click to select **View Trends Report**.
- 3** In the **Dashboard Trends Report** window select the following options and click **Apply**
 - Set the trend of the data collection from the **Trend window** drop-down box.
 - Set the frequency scale of displaying the data in the **Time scale** drop-down box.

See [“Viewing the dashboard details report ”](#) on page 679.

Using custom content

This chapter includes the following topics:

- [Using the custom content tool](#)

Using the custom content tool

Custom content consists of the regulations, the frameworks, or the control statements that you create to match your unique Policy needs.

Generally, you do the following when you create custom content:

- Create custom regulations or frameworks.
- Create any needed custom control statements.
- Map the subsections of your custom regulations or frameworks to control statements.
- Map control statements to questions, policies, or standards, or all three.
- Use the custom content in the Control Compliance Suite (CCS).

You create and modify custom content with the Symantec Content Studio. Click **Manage > Content > Content Studio** to open the Content Studio.

About custom content

The Symantec Content Studio lets you create and use the custom content that fits the needs of your enterprise. The custom control statements and the custom regulatory content help you create the policies that suit the regulatory environment that your enterprise must inhabit. You can map the custom control statements to the custom regulatory content as well as to the Symantec-provided regulatory content. You also use the Content Studio to map the policies that you create to relevant control statements.

Control statements are included in Symantec-created content, and the Content Studio lets you create your own control statements. Any control statements can be mapped to the regulations or frameworks that you create. The Content Studio also lets you map control statements to questions from the Response Assessment module or to standards.

After you have created your custom content, you can use it in the Control Compliance Suite (CCS).

When you use Content Studio, you can start from the high-level regulations or frameworks that you require. Alternatively, you can begin from the individual control statements, then build from control statements into regulations or frameworks. Normally, you start by carefully analyzing the regulation or framework to determine the control statements that are required. This analysis lets you reuse control statements in multiple sections of the regulation or framework.

After these pieces are in place, you map policies, standards, and questions to control statements. Next, you map the control statements to the regulations or frameworks that you created. When you are satisfied with new content, you can use this content.

You can do the following using the custom content feature:

- Create custom control statements.
- Create custom regulatory content.
- Map custom control statements and Symantec provided control statements to custom regulatory content.
- Map policies to control statements.

About mandates

A mandate is a regulation or framework with which you must comply. The Symantec Content Studio lets you create the custom mandates that fit your specific needs. You can also map custom mandates to control statements in the Content Studio. Any regulation or framework is a mandate.

A mandate is made up of one or more sections, each of which can optionally have one or more subsections.

A mandate has the following attributes:

Heading	Use the heading to assign a name to the mandate.
---------	--

Prefix	Use to store any section number the mandate has. When the mandate is displayed in the Mandates area, the Content Studio displays the prefix, then the heading.
Levels	If the mandate has multiple levels, you can create and assign levels to the mandate or to the sections. A mandate and its subsections all use the same group of levels. If you edit levels in any part of a mandate, the levels change in every section.
Author	The user name that was logged on when the mandate was created.
Path	The path in the mandate list to the mandate or to the section.
Body	The text of the mandate or the section.
Statement mappings	A list of the statements that you have mapped to the mandate or the section.
Category	A list of the categories that you have assigned to the mandate or the section. Policies do not use categories, but they can be used to help you group like items in the Content Studio. You can group items with categories to make them easier for you to locate.

About custom control statements

A control statement is a concise statement of a discrete portion of a regulation or framework. Since regulations and frameworks have large areas of overlap, the control statements reduce repetition by stating each portion a single time. For example, where differences exist between regulation or framework statement requirements, a single control statement exists that each of the entries is mapped to. The organizational mapping of policies to the control statement satisfies both the regulation and the framework requirements.

A control statement is mapped when it is linked to a policy. Through the policy, the control statement is indirectly linked to the regulation and framework.

A custom control statement is a control statement that you create to suit your enterprise needs. It may have none or minimal overlap with the control statements that Symantec provides with the Control Compliance Suite (CCS) content. The primary attribute of the custom control statement is that it meets your needs.

About Symantec Content Studio

The Symantec Content Studio lets you manage Symantec-created content in the Control Compliance Suite (CCS). It also lets you create your own custom content that can be used in the same way that you use Symantec-created content. Content consists of the regulations, frameworks, and control statements that underlie the

policies that you create and publish. Custom content lets you fit CCS to your unique regulatory or framework needs.

You use the Content Studio in the Manage > Content view to map mandates, policies, and control statements, and to create custom content.

You can create the following custom content types:

- Regulations
- Frameworks
- Control statements

You can map any Symantec-created control statements that are included with CCS to the regulations or frameworks that you create. You can also map control statements you create to the regulations or frameworks that you create. You can also map to questions from the Response Assessment module or to standards.

After you have created your custom content, you can use this content in CCS.

When you use the Content Studio, you can start from the high-level regulations or frameworks that you require. Alternatively, you can begin from the individual control statements, then build from control statements into regulations or frameworks. You start by carefully analyzing the regulation or framework to determine the control statements that are required. This analysis lets you reuse control statements in multiple sections of the regulation or framework, or in multiple policies. You can also use Symantec-created control statements in your custom regulations, frameworks, or policies.

After these pieces are in place, you map control statements, policies, standards, and questions to the regulations or frameworks that you created. When you are satisfied with new content, you can use it in CCS.

See [“Using the custom content tool”](#) on page 681.

About the Content view

The Content view let you manage custom content in the Control Compliance Suite.

You can access the Content view from **Manage > Content**.

You can use the view to start the Symantec Content Studio. You can click **Content Studio** to open the Symantec Content Studio.

See [“About the Content view”](#) on page 684.

Creating a custom mandateCreating a custom mandate or section

A mandate is a regulation or framework that you must comply with. The Symantec Content Studio lets you create the custom mandates that fit your specific needs.

You can also map custom mandates to control statements in the Content Studio. Any regulation or framework is a mandate.

To create a custom mandate

- 1 In the navigation bar in the lower left corner of the **Symantec Content Studio** window, click **Mandates**.
- 2 Do one of the following:
 - Click **New**, then click **Regulation** or **Framework**.
 - In the Mandates area, right-click, then click **New Regulation** or **New Framework**.
 - Click the mandate to add a section to, then click **New**, then click **Section**, then click **Under**, **Before**, or **After**.
 - In the Mandates area, right-click the mandate to add a section to, then click **New Section**.
- 3 In the Heading field of the details pane, you can type a name for the new regulation or framework.
- 4 In the Prefix field of the details pane, you can type a section number for the new regulation or framework.
- 5 To add levels to the mandate, click **Edit**.
- 6 In the **Edit Levels** dialog box, click the add icon with the yellow plus (+) symbol to add a level. Then type a name and description of the level. Click **OK** to close the dialog box and save the new levels.
- 7 In the details pane, type the text of the mandate in the body field.
- 8 Click **Save**.

See [“Mapping control statements to mandates”](#) on page 686.

Modifying a mandate or section

After you have created a mandate or section, you can make changes to it in the Symantec Content Studio. You can change any of the mandate attributes or section attributes. You can also add new sections to the mandate or section.

To modify a mandate or section

- 1 In the navigation bar in the lower left corner of the **Symantec Content Studio** window, click **Mandates**.
- 2 Click the mandate or section to which you want to make changes.

- 3 Make any needed changes to the mandate or section.
- 4 Click **Save**.

Creating custom control statements

Custom control statements let you define how you meet the requirements of mandates.

To create a custom control statement

- 1 In the navigation bar in the lower left corner of the **Symantec Content Studio** window, click **Statements**.
- 2 Do one of the following:
 - Click **New**, then click **Statement**.
 - In the Statements area, right-click, then click **New Statement**.
- 3 In the **Heading** box of the **Details** pane, you can type a name for the new statement.
- 4 In the **Body** box of the **Details** pane, you can type the control statement content.
- 5 Select a status for the control statement from the Status options.
- 6 Click **Save**.

See [“About control statements”](#) on page 574.

See [“Mapping control statements to mandates”](#) on page 686.

See [“Mapping policies to control statements”](#) on page 688.

See [“Mapping checks to control statements”](#) on page 689.

See [“Mapping questions to control statements”](#) on page 690.

Mapping control statements to mandates

The Symantec Content Studio lets you map multiple control statements to a single mandate. When you do so, you tie the mandate to every control statement that is relevant to the mandate. You can also map a single control statement to one or more mandates.

To map one or more control statements to a single mandate

- 1 In the navigation bar in the lower left corner of the **Symantec Content Studio** window, click **Mandates**.
- 2 Click the mandate section that you want to map control statements to.

- 3 Click **Statement Mappings**.
- 4 Locate the statement that you want to map to the section in the Available Statements table and do one of the following:
 - Click the statement, then click the up arrow icon to map it to the section.
 - Click the statement and drag it to the Mapped Statements table.
- 5 Click **Save**.

To remove a mapped control statement from a mandate

- 1 In the navigation bar in the lower left corner of the **Symantec Content Studio** window, click **Mandates**.
- 2 Click the mandate section that you want to remove the mapped control statements from.
- 3 Click **Statement Mappings**.
- 4 Locate the statement that you want to remove from the mandate section in the Mapped Statements table and do one of the following:
 - Click the statement, then click the down arrow icon to remove the mapping to the mandate section.
 - Click the statement and drag the statement to the Available Statements table.
- 5 Click **Save**.

To map a single control statement to one or more mandates

- 1 In the navigation bar in the lower left corner of the **Symantec Content Studio** window, click **Statements**.
- 2 Click the control statement that you want to map to one or more mandates.
- 3 Click **Mandate Mappings**.
- 4 Click **All Mandates** to display the list of mandates in the Content Studio.
- 5 Select a mandate section the control statement should be mapped to, and click the add icon with the yellow plus (+) symbol.

The added mandate sections are shown grouped by mandate in the Mapped Sections area.

To remove one or more mandates from a single control statement

- 1 In the navigation bar in the lower left corner of the **Symantec Content Studio** window, click **Statements**.
- 2 Click the control statement that you want to remove one or more mandates from.

- 3 Click **Mandate Mappings**.
- 4 Click **All Mandates** to display the list of mandates in the Content Studio.
- 5 Select a mandate to remove, and do one of the following:
 - Click the remove icon with the red X symbol.
 - Drag the mandate from the Mapped Sections area to the All Mandates area.

See [“About Symantec Content Studio”](#) on page 683.

See [“Creating custom control statements”](#) on page 686.

See [“Mapping policies to control statements”](#) on page 688.

See [“Mapping checks to control statements”](#) on page 689.

See [“Mapping questions to control statements”](#) on page 690.

Mapping policies to control statements

By mapping policies to control statements, you connect the mandates that you must comply with to the policies that validate compliance.

To map one or more control statements to a policy

- 1 In the navigation bar in the lower left corner of the **Symantec Content Studio** window, click **Policies**.
- 2 Click the policy that you want to map control statements to.
- 3 Locate the statement that you want to map to the mandate in the Available Statements table and do one of the following:
 - Click the statement, then click the up arrow icon to map it to the mandate.
 - Click the statement and drag it to the Mapped Statements table.
- 4 Click **Save**.

To remove a mapped control statement from a policy

- 1 In the navigation bar in the lower left corner of the **Symantec Content Studio** window, click **Policies**.
- 2 Click the policies that you want to remove the mapped control statements from.
- 3 Locate the statement that you want to remove from the mandate in the Mapped Statements table and do one of the following:
 - Click the statement, then click the down arrow icon to remove the mapping to the mandate.

- Click the statement and drag the statement to the Available Statements table.

4 Click **Save**.

See [“About Symantec Content Studio”](#) on page 683.

See [“Using the custom content tool”](#) on page 681.

See [“Creating custom control statements”](#) on page 686.

See [“Mapping control statements to mandates”](#) on page 686.

See [“Mapping checks to control statements”](#) on page 689.

See [“Mapping questions to control statements”](#) on page 690.

Mapping checks to control statements

By mapping checks to control statements, you connect the mandates that you must comply with to the checks that validate compliance.

To map a single control statement to one or more checks

- 1 In the navigation bar in the lower left corner of the **Symantec Content Studio** window, click **Statements**.
- 2 Click the control statement that you want to map one or more checks to.
- 3 Click **Check Mappings**.
- 4 Click **All Checks** to display the list of checks in groups by standard in the Content Studio.
- 5 Select a check that should be mapped to the control statement, and do one of the following:
 - Click the add icon with the yellow plus (+) symbol.
 - Drag the check to the Mapped Checks area.

The added checks are shown grouped by standard in the Mapped Checks area.

To remove one or more checks from a single control statement

- 1 In the navigation bar in the lower left corner of the **Symantec Content Studio** window, click **Statements**.
- 2 Click the control statement that you want to remove one or more checks from.
- 3 Click **Check Mappings**.
- 4 Click **All Checks** to display the list of checks that in groups by standard in the Content Studio.
- 5 Select a check to remove, and do one of the following:

- Click the remove icon with the red X symbol.
- Drag the check from the Mapped Checks area to the All Checks area.

To map a single check to one or more control statements

- 1 In the navigation bar in the lower left corner of the **Symantec Content Studio** window, click **Standards**.
- 2 Click the check that you want to map one or more control statements to.
- 3 Select a statement that should be mapped to the check, and do one of the following:
 - Click the statement, then click the up arrow icon to map it to the check.
 - Drag the statement to the **Mapped Statements** area.

To unmap one or more control statements from a single check

- 1 In the navigation bar in the lower left corner of the **Symantec Content Studio** window, click **Standards**.
- 2 Click the check that you want to remove one or more control statements from.
- 3 Select a statement to remove, and do one of the following:
 - Click the statement, then click the down arrow icon to unmap it from the check.
 - Drag the statement from the **Mapped Statements** area to the **Available Statements** area.

See [“About Symantec Content Studio”](#) on page 683.

See [“Using the custom content tool”](#) on page 681.

Mapping questions to control statements

By mapping a Response Assessment question to a control statement, you take advantage of the built-in Response Assessment ability to track policy acceptance.

To map one or more questions to a single control statement

- 1 In the navigation bar in the lower left corner of the **Symantec Content Studio** window, click **Statements**.
- 2 Click the control statement that you want to map one or more questions to.
- 3 Click **Question Mappings**.
- 4 Click **All Questions** to display the list of Questions in the Content Studio.
- 5 Select a question that should be mapped to the control statement, and do one of the following:

- Click the add icon with the yellow plus (+) symbol.
- Drag the check to the Mapped Questions area.

To remove one or more questions from single control statement

- 1 In the navigation bar in the lower left corner of the **Symantec Content Studio** window, click **Statements**.
- 2 Click the control statement that you want to remove one or more questions from.
- 3 Click **Question Mappings**.
- 4 Click **All Questions** to display the list of questions in the Content Studio.
- 5 Select a question to remove, and do one of the following:
 - Click the remove icon with the red X symbol.
 - Drag the question from the Mapped Questions area to the All Questions area.

To map a single question to one or more control statements

- 1 In the navigation bar in the lower left corner of the **Symantec Content Studio** window, click **Questions**.
- 2 Click the question that you want to map one or more control statements to.
- 3 Select a control statement that should be mapped to the question, and do one of the following:
 - Click the statement, then click the up arrow icon to map it to the question.
 - Drag the statement to the Mapped Statements area.

To unmap one or more control statements from a single question

- 1 In the navigation bar in the lower left corner of the **Symantec Content Studio** window, click **Questions**.
- 2 Click the question that you want to remove one or more control statements from.
- 3 Select a statement to remove, and do one of the following:
 - Click the statement, then click the down arrow icon to unmap it from the question.
 - Drag the statement from the Mapped Statements area to the Available Statements area.

See [“About Symantec Content Studio”](#) on page 683.

See [“Using the custom content tool”](#) on page 681.

Mapping control statements to third-party evidence

You can use the Symantec Content Studio to help you map control statements to evidence from third-party providers. Evidence for third-party providers is imported from a .csv file the third-party data collector creates. When you map third-party evidence to the control statements, you can use the third-party evidence to support your compliance.

See [“About the Evidence Management system”](#) on page 697.

See [“About a custom evidence provider ”](#) on page 698.

See [“General sequence of configuring an evidence provider ”](#) on page 698.

Note: When you map control statements to third-party evidence, you must modify the Microsoft SQL Server databases that the Control Compliance Suite (CCS) uses. You should exercise caution when making these changes.

When you map the control statements, you must do the following:

- Determine the ID of the statement you map to.
- Identify the evaluation instance of the third-party evidence provider.
- Create an SQL script to perform the mapping.

Symantec Professional Services supplies the evaluation instance when you create the third-party evidence database.

To determine a control statement ID in Symantec Content Studio

- 1 In the **Symantec Content Studio** window, click a control statement.
- 2 In the details pane, click **Properties**.
- 3 In the **Properties** dialog, click **Properties** to copy the control statement ID.

To use SQL Server Management Studio to determine a control statement ID

- ◆ In SQL Server Management Studio, use the following T-SQL statements to retrieve all control statements in the system:

```
Use [CSM_DB]
Go
SELECT ID, Heading, Body from [content].[Statement]
GO
```

To create a SQL script to perform the mapping

- ◆ In SQL Server Management Studio, create a mapping between a control statement with the ID you specify and a third-party evaluation instance.

The following T-SQL statement creates the correct mapping:

```
INSERT INTO [CSM_DB].[content].[StatementCustomEvidenceProvider]
    ([ID]
    , [StatementID]
    , [ThirdPartyEvaluationInstanceID]
    , [Author]
    , [CreatedDate]
    , [ModifiedDate])
VALUES
    (newid()
    , <StatementID, uniqueidentifier,>
    , <ThirdPartyEvaluationInstanceID, uniqueidentifier,>
    , <Author, nvarchar(256),>
    , getdate()
    , getdate())
```

Performing policy analysis

The **Symantec Content Studio** lets you analyze your policies to see the gaps in compliance between your organization's current policies and the security regulations.

The Content Studio analysis view helps you to identify any control statements that are not mapped to a policy. You can then use the Content Studio to create relationships between those policies and control statements. When you link a policy to a control statement, you establish a relationship between the policy and the control statement. The control statement is also linked to one or more regulations or frameworks.










See [“About the Analysis view icons”](#) on page 693.

See [“Viewing the control statements mapped to a regulation, framework, or policy”](#) on page 694.

See [“Performing a gap analysis”](#) on page 695.

About the Analysis view icons

In the **Map Policies** dialog box, the following icons and links are used to represent the different objects and their relationships on the map area:

	Depicts a control statement
	Depicts a regulation
	Depicts a policy or a policy template
	Depicts a framework
	Displays the links between the selected policy and the control statements that are linked to the policy
	Displays the links between the selected policy template and the control statements that are linked to the policy template.
	Displays the links between a regulation and the control statements
	Displays the links between a framework and the related control statements
	Displays the links between a parent node and its children

See [“Performing policy analysis”](#) on page 693.

See [“Performing a gap analysis”](#) on page 695.

See [“Viewing the control statements mapped to a regulation, framework, or policy”](#) on page 694.

Viewing the control statements mapped to a regulation, framework, or policy

You can use the Analysis view to review the control statements that are mapped to one or more regulations, best-practice frameworks, or policies. You can use this view to determine the gaps between the regulations and frameworks with which you must comply and the policies you use to enforce those requirements.

You can view regulations, frameworks, and policies one at a time or in groups. You should use the content studio to map your frameworks and regulations to the control statements and map the control statements in turn to your policies. When mapping is complete, every framework or regulation should map to one or more control statements. Every control statement should in turn map to one or more policies. Through their mutual maps to shared control statements, every framework or regulation will be linked to one or more policies.

To view the control statements that are mapped to a regulation, framework, or policy

- 1 In the **Symantec Content Studio** window, on the navigation bar, click **Analysis**.
- 2 In the tree view, drag and drop any regulation, framework, or policy to the map area.
- 3 In the Analysis View, do one of the following:
 - Right-click a control statement, and then click **Expand > Regulation** to display the regulations mapped to the control statement.
 - Right-click a control statement, and then click **Expand > Frameworks** to display the frameworks mapped to the control statement.
 - Right-click a control statement, and then click **Expand > Policies** to display the policies mapped to the control statement.
 - Right-click a control statement, and then click **Expand > All** to display all regulations, frameworks, and policies linked to the control statement.
 - Right-click any object and click **Remove** to remove it from the **Analysis** view.
- 4 If desired, return to 2 and add an additional regulation, framework, or policy.

See [“Performing policy analysis”](#) on page 693.

See [“About the Analysis view icons”](#) on page 693.

See [“Performing a gap analysis”](#) on page 695.

Performing a gap analysis

By performing a gap analysis you can see the existing gaps in the policies your organization follows.

To perform a gap analysis

- 1 In the **Symantec Content Studio** window, click **Analysis**.
- 2 In the tree view, expand the Policies node.
- 3 Locate the required policy and drag it to the map area.
- 4 In the tree view, expand the Regulation or Framework node.
- 5 Locate the section relevant to the policy and drag it to the map area.

- 6 Click **Auto Layout**. The Auto Layout feature redraws the map with a balanced spacing between all the objects and zooms out so that the whole map is visible.
- 7 You can see the control statements that are not mapped to the policy. Use the Content Studio to map these Statements to the policy.

See [“Performing policy analysis”](#) on page 693.

See [“About the Analysis view icons”](#) on page 693.

See [“Viewing the control statements mapped to a regulation, framework, or policy”](#) on page 694.

Using third-party evidence

This chapter includes the following topics:

- [About the Evidence Management system](#)
- [About the Evidence Management View](#)
- [About a custom evidence provider](#)
- [General sequence of configuring an evidence provider](#)
- [Creating a CSV file for evidence data collection](#)
- [About evidence field format for predefined asset types](#)
- [Associating a data location with the evidence provider](#)
- [About setting tasks to roles for evidence collection](#)
- [Adding a custom evidence provider](#)
- [Modifying a custom evidence provider](#)
- [Deleting a custom evidence provider](#)

About the Evidence Management system

Evidence is the data that defines whether an asset in an enterprise is configured, managed, and secured as per the governance requirement. Validation checks are run on assets and the information that provides data after a validation check passes or fails on an asset, is called evidence. Evidence information that is collected from a validation check failure is known as negative evidence. Positive evidence information contains more data about the asset on which a validation check passes.

See [“About a custom evidence provider”](#) on page 698.

See [“General sequence of configuring an evidence provider”](#) on page 698.

About the Evidence Management View

The Evidence Management view lets you manage the evidence data that is collected using an evidence provider.

You can access the Evidence Management view by navigating through the **Settings > Evidence Management** menus of the console.

The Evidence Management view contains the following columns:

Display Name	Displays the names of the evidence providers that are added.
Description	Displays the description of the evidence providers that are added.
Is Custom Provider?	Displays whether the registered evidence providers are custom applications or not.
Retention Age In Day(s)	Displays the time period for retaining the evidence data in the evidence database.
Evidence Collection Schedule	Displays the schedule that is set for the evidence collection job.

See [“Adding a custom evidence provider”](#) on page 708.

See [“Modifying a custom evidence provider ”](#) on page 709.

See [“Deleting a custom evidence provider”](#) on page 709.

About a custom evidence provider

See [“Creating a CSV file for evidence data collection ”](#) on page 699.

See [“Associating a data location with the evidence provider”](#) on page 707.

See [“Adding a custom evidence provider”](#) on page 708.

See [“General sequence of configuring an evidence provider ”](#) on page 698.

See [“Creating a CSV file for evidence data collection ”](#) on page 699.

General sequence of configuring an evidence provider

You must know the end-to-end process of creating a custom evidence provider, populating the evidence database, and running the Evidence Collection job.

The end-to-end sequence of collecting evidence data is as follows:

- Add a custom evidence provider through the Evidence Management system.
See [“Adding a custom evidence provider”](#) on page 708.
- Populate the table, ThirdPartyEvaluationInstances with data of the EvaluationType field of the CSV file.
The Symantec's Professional Services would perform the task of populating the table for you.
- By default, the role, CCS_Administrator has the permission to run the Evidence Collection job. You can also create a specific role and assign the tasks to the role that are required to run the Evidence Collection job.
See [“About setting tasks to roles for evidence collection”](#) on page 707.
- Set the password for the Data Collection User Name and Password option in the Home > User Preference view of the console.
See [“Adding credentials for scheduled jobs”](#) on page 55.
- Run the Evidence Collection job from the Manage > Jobs view of the console.
See [“Scheduling jobs”](#) on page 602.
You must have scheduled the Evidence Collection job when adding the custom evidence provider.
See [“Mapping control statements to third-party evidence”](#) on page 692.

Creating a CSV file for evidence data collection

The Control Compliance Suite collects evidence data of any custom application from a custom evidence provider such as a CSV file. Data must be stored in a specific format in the CSV file for easy interpretation by the infrastructure. The collected evidence data is stored in the evidence database of the Control Compliance Suite. By default, the database, CSM_EvidenceDB is created for storing the evidence data of the custom application.

To create a CSV file for evidence data collection

- 1 Gather the primary and mandatory fields of the asset type that you have created.

If the asset type is same as the predefined asset type of a predefined platform, then you must know the primary and mandatory fields of the predefined asset type.

See [“Predefined asset types”](#) on page 204.
- 2 Create the headers for the created asset type in the CSV file.

The headers in a CSV file must be of a specific format that is supported by the Control Compliance Suite. The headers must contain fields specific to the asset type and to the asset evidence.

The format of the headers is as follows:

```
Evidence.Record.AssetkeyClass, Evidence.Record.Assetkeyfield1,
Evidence.Record.Assetkeyfield2,...Evidence.Record.Assetkeyfield8
,Evidence.Record.Status, Evidence.Record.EvaluationType,
Evidence.Record.EvaluationName, Evidence.Record.EvaluationID,
Evidence.Record.GeneratedDate, Evidence.Record.AssetSite,
Evidence.Record.EvidenceDescription,
Evidence.Record.Confidentiality, Evidence.Record.Integrity,
Evidence.Record.Availibility
```

You must know the header format for the predefined asset types and also the descriptions of the evidence-related fields to create the CSV file.

See [“About evidence field format for predefined asset types”](#) on page 701.

For example, you can have a UNIX Machine asset type, whose health status is to be evaluated. You must identify the primary fields of the asset type and arrange them in the ascending alphabetical order against the headers in the CSV file.

The primary and mandatory fields of the asset type are as follows:

Machine Name (for example, primary field
TestMachine)

Host IP address (for example, primary field
132.34.56.78)

The headers and the tentative data for the UNIX Machine asset type are as follows:

Evidence.Record.Assetkeyfield1	132.34.56.78
Evidence.Record.Assetkeyfield2	TestMachine
Evidence.Record.Status	Pass
Evidence.Record.EvaluationType	healthcheckup
Evidence.Record.EvaluationName	IsMachinehealthfine
Evidence.Record.EvaluationID	07ADFG-98
Evidence.Record.GeneratedDate	10/12/2008

Evidence.Record.AssetSite	Defaultsite
Evidence.Record.EvidenceDescription	to check the health status
Evidence.Record.Confidentiality	2
Evidence.Record.Integrity	1
Evidence.Record.Availability	3

- 3
- Place the CSV file in the network share path of the computer.
See [“Associating a data location with the evidence provider”](#) on page 707.
- 4
- Populate the table, ThirdPartyEvaluationInstances with data for the field, EvaluationType, manually.
See [“General sequence of configuring an evidence provider ”](#) on page 698.

About evidence field format for predefined asset types

In the CSV file header format, the fields, Assetkeyfield1 to Assetkeyfield8 represent the primary and mandatory fields of the asset type. The remaining header fields represent the evidence properties of the assets. Data for the Assetkeyfields must be arranged in the ascending alphabetical order in the CSV file. If the asset type belongs to any of the predefined asset type, then you must map the key fields appropriately with the Assetkeyfield headers. For example, for a Windows Directory asset type, the key fields, Directory Name, Domain Name, and Machine Name must map to Assetkeyfield1, Assetkeyfield2, and Assetkeyfield3, respectively.

You must know the following for creating the CSV file:

- Mapping between the primary and mandatory fields and the Assetkeyfield headers.
- Descriptions of the evidence-related fields that are specified in the CSV file.

The mapping between the fields and the headers is as follows:

Table 19-1 Lists the headers of the CSV file for the primary and mandatory fields of the predefined asset types

Predefined asset type	Primary and mandatory fields	Header format
SQL Database	<p>The following fields that are listed in the ascending order are to be mapped to the headers:</p> <ul style="list-style-type: none">■ Database Name■ Domain/Workgroup Name■ Host Name (Node)■ Server Name (Instance)	<p>The headers to which the fields are to be mapped are as follows:</p> <ul style="list-style-type: none">■ Evidence.Record.AssetField1■ Evidence.Record.AssetField2■ Evidence.Record.AssetField3■ Evidence.Record.AssetField4
SQL Server	<p>The following fields that are listed in the ascending order are to be mapped to the headers:</p> <ul style="list-style-type: none">■ Domain/Workgroup Name■ Host Name (Node)■ Major Version■ Server Name (Instance)	<p>The headers to which the fields are to be mapped are as follows:</p> <ul style="list-style-type: none">■ Evidence.Record.AssetField1■ Evidence.Record.AssetField2■ Evidence.Record.AssetField3■ Evidence.Record.AssetField4
ESM Agent	<p>The following fields that are listed in the ascending order are to be mapped to the headers:</p> <ul style="list-style-type: none">■ ESM Manager■ OS Details■ OS Version■ Platform■ Registered Name	<p>The headers to which the fields are to be mapped are as follows:</p> <ul style="list-style-type: none">■ Evidence.Record.AssetField1■ Evidence.Record.AssetField2■ Evidence.Record.AssetField3■ Evidence.Record.AssetField4■ Evidence.Record.AssetField5

Table 19-1 Lists the headers of the CSV file for the primary and mandatory fields of the predefined asset types *(continued)*

Predefined asset type	Primary and mandatory fields	Header format
Oracle Configured Databases	<p>The following fields that are listed in the ascending order are to be mapped to the headers:</p> <ul style="list-style-type: none"> ■ Database Name ■ Database Version ■ OS Type ■ Server Name ■ Windows Domain Name or UNIX IP address 	<p>The headers to which the fields are to be mapped are as follows:</p> <ul style="list-style-type: none"> ■ Evidence.Record.AssetField1 ■ Evidence.Record.AssetField2 ■ Evidence.Record.AssetField3 ■ Evidence.Record.AssetField4 ■ Evidence.Record.AssetField5
Oracle Configured Servers	<p>The following fields that are listed in the ascending order are to be mapped to the headers:</p> <ul style="list-style-type: none"> ■ OS Type ■ Server Name ■ Windows Domain Name or UNIX IP address 	<p>The headers to which the fields are to be mapped are as follows:</p> <ul style="list-style-type: none"> ■ Evidence.Record.AssetField1 ■ Evidence.Record.AssetField2 ■ Evidence.Record.AssetField3
UNIX File	<p>The following fields that are listed in the ascending order are to be mapped to the headers:</p> <ul style="list-style-type: none"> ■ File Name (with path) ■ Host IP Address ■ Machine Name 	<p>The headers to which the fields are to be mapped are as follows:</p> <ul style="list-style-type: none"> ■ Evidence.Record.AssetField1 ■ Evidence.Record.AssetField2 ■ Evidence.Record.AssetField3
UNIX Group	<p>The following fields that are listed in the ascending order are to be mapped to the headers:</p> <ul style="list-style-type: none"> ■ Group Database ■ Group Name ■ IP Address ■ Machine Name 	<p>The headers to which the fields are to be mapped are as follows:</p> <ul style="list-style-type: none"> ■ Evidence.Record.AssetField1 ■ Evidence.Record.AssetField2 ■ Evidence.Record.AssetField3 ■ Evidence.Record.AssetField4

Table 19-1 Lists the headers of the CSV file for the primary and mandatory fields of the predefined asset types *(continued)*

Predefined asset type	Primary and mandatory fields	Header format
UNIX Machine	<p>The following fields that are listed in the ascending order are to be mapped to the headers:</p> <ul style="list-style-type: none"> ■ IP Address ■ Machine Name ■ Operating Distribution Field ■ Operating System ■ Operating System Version 	<p>The headers to which the fields are to be mapped are as follows:</p> <ul style="list-style-type: none"> ■ Evidence.Record.AssetField1 ■ Evidence.Record.AssetField2 ■ Evidence.Record.AssetField3 ■ Evidence.Record.AssetField4 ■ Evidence.Record.AssetField5
Windows Directory	<p>The following fields that are listed in the ascending order are to be mapped to the headers:</p> <ul style="list-style-type: none"> ■ Directory Name ■ Domain/Workgroup Name ■ Machine Name 	<p>The headers to which the fields are to be mapped are as follows:</p> <ul style="list-style-type: none"> ■ Evidence.Record.AssetField1 ■ Evidence.Record.AssetField2 ■ Evidence.Record.AssetField3
Windows Domain	Domain Name	Evidence.Record.AssetField1
Windows File	<p>The following fields that are listed in the ascending order are to be mapped to the headers:</p> <ul style="list-style-type: none"> ■ Domain/Workgroup Name ■ File Name (with path) ■ Machine Name 	<p>The headers to which the fields are to be mapped are as follows:</p> <ul style="list-style-type: none"> ■ Evidence.Record.AssetField1 ■ Evidence.Record.AssetField2 ■ Evidence.Record.AssetField3

Table 19-1

Lists the headers of the CSV file for the primary and mandatory fields of the predefined asset types *(continued)*

Predefined asset type	Primary and mandatory fields	Header format
Windows Group	<div>The following fields that are listed in the ascending order are to be mapped to the headers:</div> <div><div>■ Domain/Workgroup Name</div><div>■ Group Name (with path)</div><div>■ Machine Name</div></div>	<div>The headers to which the fields are to be mapped are as follows:</div> <div><div>■ Evidence.Record.AssetField1</div><div>■ Evidence.Record.AssetField2</div><div>■ Evidence.Record.AssetField3</div></div>
Windows Machine	<div>The following fields that are listed in the ascending order are to be mapped to the headers:</div> <div><div>■ Domain/Workgroup Name</div><div>■ Machine Name</div><div>■ Machine is BDC</div><div>■ Machine is PDC</div><div>■ Machine is server</div><div>■ OS Major Version</div><div>■ OS Minor Version</div><div>■ OS Type</div></div>	<div>The headers to which the fields are to be mapped are as follows:</div> <div><div>■ Evidence.Record.AssetField1</div><div>■ Evidence.Record.AssetField2</div><div>■ Evidence.Record.AssetField3</div><div>■ Evidence.Record.AssetField4</div><div>■ Evidence.Record.AssetField5</div><div>■ Evidence.Record.AssetField6</div><div>■ Evidence.Record.AssetField7</div><div>■ Evidence.Record.AssetField8</div></div>

The evidence property fields and the descriptions that are to be specified in the CSV file are as follows:

Evaluation Type	<div>This field indicates the type of evaluation that is performed on the asset.</div> <div>For example, a health check-up of the asset can be a type of evaluation.</div> <div>The data type for this field must be a string.</div>
-----------------	--

Evaluation Name	<p>This field indicates the evaluation that was executed on the asset.</p> <p>For example, the evaluation name, Is average memory consumption high on machine, can generate evidence record.</p> <p>The data type for this field must be a string.</p>
Status	<p>This field indicates the status of the asset such as pass, fail, and error.</p> <p>The data type for this field must be an integer.</p>
GeneratedDate	<p>This field indicates the date of evaluation of the data.</p> <p>The data type for this field must be a date/time.</p>
Evaluation ID	<p>This field indicates the identity of the evaluation check that was executed on the asset.</p> <p>The data type for this field must be a string.</p>
AssetSite	<p>This field indicates the asset site.</p> <p>The data type for this field must be a string.</p>
EvidenceDescription	<p>This field indicates the description of the evidence for the evaluated data.</p> <p>The data type for this field must be a string.</p>
Confidentiality	<p>This field indicates the confidentiality of the evaluated data.</p> <p>The data type for this field must be an integer.</p>
Availability	<p>This field indicates the availability of the evaluated data.</p> <p>The data type for this field must be an integer.</p>
Integrity	<p>This field indicates the integrity of the evaluated data.</p> <p>The data type for this field must be an integer.</p>

Evidence Data

This field provides information about the failure or the error that is generated after executing the evaluation check.

The data type for this field must be a string.

Associating a data location with the evidence provider

Note: At any given point of time, you must not use the same data location for two different evidence providers.

To associate a data location with an evidence provider

- 1 Go to Settings > General.
- 2 Under System Configuration click **Data Locations**.
- 3 In the right pane of the console, click **Add**.
- 4 In the Add Data Location dialog box, enter the required values.
- 5 Go to Settings > Evidence Management.
- 6 In the Evidence Management view, right-click and select **Add Custom Evidence Provider**.
- 7 In the Add New Evidence Provider dialog box, enter the required values for the General tab.
- 8 In the Advanced tab, for the Data Location field, select the configured data location from the drop-down list.
- 9 Click **OK**.

See [“Adding a custom evidence provider”](#) on page 708.

See [“Creating a CSV file for evidence data collection ”](#) on page 699.

About setting tasks to roles for evidence collection

To run the Evidence Collection job from the Jobs view of the console, you must create a custom role that is configured to perform specific tasks. In Control Compliance Suite, you can create a custom role for the Evidence Management system through the Settings > Role view of the console.

See [“Creating a custom role”](#) on page 92.

The following tasks must be associated with the custom role that is created for the Evidence Management system:

- Manage Configuration Settings
- View Assets
- View All Jobs
- Manage Evidence definitions
- View Asset Reconciliation Rules
- Manage Jobs
- Import Assets

See [“Configuring roles and permissions”](#) on page 78.

Adding a custom evidence provider

You must register the evidence provider with the Control Compliance Suite for initiating evidence data collection. The evidence provider is a CSV file. The file must be placed in the network share path and configured through the Data Location option of the console's System Configuration view.

See [“Associating a data location with the evidence provider”](#) on page 707.

To add a custom evidence provider

- 1 Go to Settings > Evidence Management.
- 2 In the Evidence Management view, right-click and select **Add Custom Evidence Provider**.
- 3 In the Add New Evidence Provider dialog box, provide the values for the following tabs:
 - General
 - Schedule
You can schedule the Evidence Collection job in this dialog box and run the job from the Job Management view of the console.
 - Advanced
- 4 Click **OK**.

An evidence collection job is created. The evidence collection job collects the evidence data at the configured scheduled time.

See [“About jobs”](#) on page 595.

See [“Modifying a custom evidence provider”](#) on page 709.

See [“Deleting a custom evidence provider”](#) on page 709.

Modifying a custom evidence provider

You can modify the properties such as schedule, retention age, site, data location and so on of the evidence provider. The modifying operation can be performed through the Control Compliance Suite Console.

To modify an evidence provider

- 1 Go to Settings > Evidence Management.
- 2 In the Evidence Management view, select an evidence record and right-click to select **Edit Evidence Provider**.
- 3 In the Edit Evidence Provider dialog box, modify any of the following:
 - Description of the evidence provider
 - Evidence collection schedule
 - Retention age of the evidence data
 - Site of the asset
 - Reconciliation rules for the asset.
- 4 Click OK.

See [“Adding a custom evidence provider”](#) on page 708.

See [“Deleting a custom evidence provider”](#) on page 709.

Deleting a custom evidence provider

You can delete a registered evidence provider from the Evidence Management view of the console.

Note: Deleting the custom evidence provider also deletes the evidences.

To delete an evidence provider

- 1 Go to Settings > Evidence Management.
- 2 In the Evidence Management view, select an evidence provider and right-click to select **Delete Evidence Provider**.
- 3 In the message dialog box, click **Yes**.

Customizing the Web Portal language

This appendix includes the following topics:

- [Customizing the Web Portal language](#)

Customizing the Web Portal language

If the users of the Control Compliance Suite Web Console prefer a language other than English, you can create custom language resource files. The Web console uses these custom language files to create the Web console user interface.

The custom language resource files contain a string name for each customizable element along with the custom value you specify for that value. When you create a custom translation, you should first translate each element manually, then create the resource files.

Creating new Web Portal language files

You can add a new language to the Web console using the Visual Studio 2005 application.

The resource files you create must have particular, well-defined names.

The names must match the following patterns:

- `PolicyModule.language code.resx`
- `SiteMapLocations.language code.resx`

You create one of each these resource file types for each custom language you create.

The language code is the ISO 639-1 standard two-letter abbreviation for the language, such as es for Spanish or fr for French.

The following are valid example names for language files and site map location files:

- `PolicyModule.es.resx`
- `SiteMapLocations.es.resx`

To create a resource project file

- 1 In Visual Studio 2005 click **Create New Project**.
- 2 In the **New Project** dialog box, create a Visual C# Windows class library. Name the project `App_GlobalResources`.
- 3 Click **OK**.

To create a new language file for the Web console

- 1 In Visual Studio 2005, right-click the project name and click **Add > New Item**.
- 2 In the **Add New Item** dialog box, click **Resource File**. Type a valid name for the file in the form `PolicyModule.language code.resx`
- 3 Click **Add**.
- 4 In the resource editor, add the necessary Names and Values.
See [Table A-2](#) on page 715.
- 5 After you have entered all of the names and values, close and save the file.

To create the site map location resource file

- 1 In Visual Studio 2005, right-click the project name and click **Add > New Item**.
- 2 In the **Add New Item** dialog box, click **Resource File**. Type a valid name for the file in the form `SiteMapLocations.language code.resx`.
- 3 In the resource editor, add the required string names and values.
See [Table A-3](#) on page 720.
- 4 After you have entered all of the names and values, close and save the file.

To set the resource project properties

- 1 In Visual Studio 2005, right-click the project name and click **Properties**.
- 2 In the project properties dialog, change the default namespace to **Resources**.

- 3 In Visual Studio 2005, press F6 to build the solution.
The output directory contains a resource folder that you name with the language code of the `resx` file.
- 4 Copy the resource folder to the `Reporting and Analytics\WebPortal\bin` directory on the Control Compliance Suite Application Server.

Translating the Web Portal local resource files

To use the Web console with a custom language, you must translate the local resource files that the Web console uses to the target language.

Each file is named in the pattern `filename.aspx.resx`. You copy each file and rename it in the pattern `filename.aspx.language code.resx`

The language code is the ISO 639-1 standard two-letter abbreviation for the language, such as `es` for Spanish or `fr` for French.

You then use Visual Studio 2005 to open and translate each of the files.

[Table A-1](#) lists the files you must copy and translate. The table groups the files by directory.

Table A-1 Web console local resource files

Directory	Files
<i>Installation Directory</i> \ Symantec\CCS\Reporting and Analytics\WebPortal\ App_LocalResources:	MainPage.aspx.resx
<i>Installation Directory</i> \Symantec\CCS\Reporting and Analytics\WebPortal\Errors\ App_LocalResources:	■ Error.aspx.resx ■ PMError.aspx.resx ■ RAMError.aspx.resx

Table A-1 Web console local resource files (continued)

Directory	Files
<i>Installation Directory</i> \ Symantec\CCS\Reporting and Analytics\WebPortal\PolicyModule\ App_LocalResources:	<div>■ AddCommentsPage.aspx.resx</div> <div>■ ClarificationDetail.aspx.resx</div> <div>■ ClarificationPolicy.aspx.resx</div> <div>■ Default.aspx.resx</div> <div>■ ExceptionDetail.aspx.resx</div> <div>■ ExceptionPolicy.aspx.resx</div> <div>■ PolicyApprove.aspx.resx</div> <div>■ PolicyDetail.aspx.resx</div> <div>■ PolicyPendingApproval.aspx.resx</div> <div>■ PolicyReview.aspx.resx</div> <div>■ RequestException.aspx.resx</div>
<i>Installation Directory</i> \ Symantec\CCS\Reporting and Analytics\WebPortal \QuestionnaireModule \App_LocalResources	Questionnaire.aspx.resx

To translate the local resource files

- 1
- On the computer that hosts the Web console server, use Windows Explorer or a similar tool to locate the directories in [Table A-1](#).
- 2
- Using Windows Explorer or a similar tool, make a copy of each file in [Table A-1](#). Rename each copy *filename.aspx.xx.resx*.
- 3
- Open each copied file in Visual Studio 2005, and translate the items in the **Values** column to the target language.
- 4
- Save the translated files in the same directories as the original files on the Web console server.

Using a new language in the Web Portal

You can use the language files and customized local resources to view the Web Client in the target language.

To use the language files in the Web console

- 1
- Open Internet Explorer and click **Tools > Internet Options**.
- 2
- In the **Internet Options** dialog box, click **Languages**.
- 3
- In the **Language Preferences** dialog, click **Add**.

- 4 In the **Add Language** dialog box, select the language that matches the language code for the resource. Click **OK**.
- 5 In the **Language Preference** dialog box, select the language and click **Move Up**.
- 6 In the **Language Preference** dialog box, click **OK**.
- 7 In the **Internet Options** dialog box, click **OK**.
- 8 In Internet Explorer, Navigate to the Web console. The Web console should appear in the new language.

Web Portal string reference

[Table A-2](#) lists the string names for the Policy Module and the default English values for each string.

[Table A-3](#) lists the string names for the Web console uses and the default English values for each string.

Your custom language resource files contain these string names and your translation of the default values.

Table A-2 Policy Module Resource Strings

Name	Value
AddCommentsPageTitle	Add Comments to Policy
AddCommentPopupHeader	Add Comment
AddComments	Add Comments...
AddCommentsPageTitle	Add Comments to Policy
ApproverComment	Approver Comment
ApproverCommentDes	Enter your approval comments about the policy
Attachment	Attachment
CalendarFooterFormat	Today
Cancel	Cancel
Category	Category
ChangeRequest	Change Request
ClarificationDetails	Clarification Details

Table A-2 Policy Module Resource Strings (*continued*)

Name	Value
ClarificationRequest	Clarification Request
ClarificationRequestNotification	Clarification Request Notification
ClarificationRequestNotificationBody_1	Clarification has been requested to the policy
ClarificationRequestNotificationBody_2	on the date of
ClearCommentMessage	Are you sure you want to clear the comment?
ClearComments	Clear Comments
Comment	Comment
Commented	My Comments Added
Commented_False	No
Commented_True	Yes
CommentType	Comment Type
Description	Description
EffectivDate	Effective Date
Email	Email
EmailBodyLine1_1	The status of the policy
EmailBodyLine1_2	changed
EmailBodyLine2	The policy status changed on
EmailBodyLine3	Previous status :
EmailBodyLine4	Current status :
EmailBodyLine5	The Symantec Control Compliance Suite generated this email automatically. Do not reply to this email. The mail box is not set up to receive emails.
EmailSubject	Notification of policy status changes
Exception	Exception

Table A-2 Policy Module Resource Strings (*continued*)

Name	Value
ExceptionRequest	Exception Request
ExceptionStatus_ApprovalOverdue	Approval Overdue
ExceptionStatus_Approved	Approved
ExceptionStatus_Deny	Denied
ExceptionStatus_InReview	In Review
ExceptionStatus_RequestClarification	Request Clarification
ExceptionStatus_Requested	Requested
ExceptionDetails	Exception Details
ExpirationDate	Expiration Date
Help	Help
HomePagePolicyDetail	Provides you with the list of all policies that are applicable to the logged-on user. Here the user can select to view any policy detail and decide to accept or decline the policy. The user can also request an exception or a clarification for any policy.
HomePagePolicyHeader	Policies
HomePagePolicyLinkText	View your Policies
HomePageRAMDetail	View invitations to answer questionnaires created in the CCS Response Assessment module (RAM). Select a questionnaire to begin responding to questions through the RAM Web Console.
HomePageRAMheader	Questionnaires
HomePageRAMLinkText	View your Questionnaire Invitations
HomePageText	The Control Compliance Suite (CCS) Web Console provides you with an online resource for activities related to the CCS Policy and the Response Assessment modules

Table A-2 Policy Module Resource Strings (*continued*)

Name	Value
HomePageTitle	Welcome to the Symantec Control Compliance Suite Web Console
LastModified	Last Modified
Name	Name
NoDataToDisplay	No data to display
Path	Path
Policy	Policy
PolicyAcceptanceStatus_Accepted	Accepted
PolicyAcceptanceStatus_Declined	Declined
PolicyAcceptanceStatus_Read	Read
PolicyAcceptanceStatus_UnRead	Not Read
PolicyAuthor	Author
PolicyDetails	Policy Details
PolicyExpirationDate	Expiration Date
PolicyLevel	Policy Level
PolicyLevel_High	High
PolicyLevel_Low	Low
PolicyLevel_Medium	Medium
PolicyName	Policy Name
PolicyStatus	Status
PolicyStatus_Approved	Approved
PolicyStatus_Archived	Archived
PolicyStatus_Draft	Draft
PolicyStatus_InReview	In Review
PolicyStatus_PendingApproval	Pending Approval

Table A-2 Policy Module Resource Strings (*continued*)

Name	Value
PolicyStatus_Published	Published
PolicyStatus_Rejected	Rejected
PolicyVersion	Version
Rationale	Rationale
ReceivedDate	Received Date
RequestChange	Request Change
RequesterName	Requested By
RequestText	Request Text
RequestTime	Date Submitted
ResponseDueDate	Response Due
ReviewByDate	Review By Date
ReviewedDate	Reviewed Date
Reviewer	Reviewer
ReviewerComment	Reviewer Comment
ReviewerCommentDes	Enter your review comments about the policy
SendEmailDes	Send response notifications to following e-mail address
Show	Show
ShowStatus	Show Status
Space	:
Status_Closed	Closed
Status_Open	Open
Submit	Submit
TabApproverComments	Comments
TabApproversTitle	Approvers

Table A-2 Policy Module Resource Strings (*continued*)

Name	Value
TabAudienceTitle	Audience
TabClarificationsTitle	Clarifications
TabContentTitle	Content
TabGeneralTitle	General
TabReviewerComments	Comments
TabReviewersTitle	Reviewers
TabStatementsTitle	Statements
TabTagsTitle	Tags
TabTargetsTitle	Targets
Title	Title

Table A-3 Site Map Localization Resource Strings

Name	Value
ClarificationPage.description	Clarifications
ClarificationPage.title	Clarifications
ExceptionPage.description	Exceptions
ExceptionPage.title	Exceptions
Home.description	Home page
Home.title	Home
PoliciesMenu.description	Policies
PoliciesMenu.title	Policies
PolicyAcceptancePage.description	Accept Policies
PolicyAcceptancePage.title	Accept Policies
PolicyApprovalPage.description	Approve Policies
PolicyApprovalPage.title	Approve Policies
PolicyManagerSite.title	Policy Manager

Table A-3 Site Map Localization Resource Strings (*continued*)

Name	Value
PolicyPendingApprovalPage.description	Policy Review Complete
PolicyPendingApprovalPage.title	Policy Review Complete
PolicyReviewPage.description	Review Policies
PolicyReviewPage.title	Review Policies
Questionnaires.description	Questionnaires
Questionnaires.title	Questionnaires

Standard Migration Utility

This appendix includes the following topics:

- [About the Standard Migration Utility](#)
- [About the Standard Migration Utility system requirements](#)
- [About the Standard Migration Utility packaging and deployment](#)
- [Standard Migration Utility](#)
- [How to use the Standard Migration Utility](#)
- [About the log file configuration settings](#)
- [About migration summary report](#)
- [Limitations in the Standard Migration Utility](#)
- [Troubleshooting evaluation mismatches](#)

About the Standard Migration Utility

The Standard Migration Utility (SMU) lets you migrate the following to Control Compliance Suite (CCS) 9.0.1 or later format:

- Custom standards of the existing Technical Standard Packs (TSP)
- Custom standards that you have created

You can use the migrated standards in CCS 9.0.1 or later after you migrate the standards to the CCS 9.0.1 or later format.

You can migrate the complex checks of the custom standards of the following TSPs:

- Security Essentials for Red Hat Enterprise Linux 5.0

- CIS Security Benchmark for HP-UX v1.3.1
- CIS AIX Benchmark v1.0.1
- CIS Solaris 10 Benchmark v4.0
- CIS Oracle 9i and 10g Database Security Benchmark v2.0
- Security Essentials for Microsoft SQL Server 2005
- CIS Legacy Security Settings Benchmark for Windows 2003 Domain Controller v2.0
- CIS Legacy Settings Benchmark for Windows XP Professional v2.01
- CIS Windows 2000 Server Operating System Level Two Benchmark for Stand-alone and Member Servers v2.2.1
- CIS Windows Server 2003 Legacy Security Settings for Domain Member Servers v2.0
- CIS Benchmark for IIS 5.0 and 6.0 for Microsoft Windows 2000, XP and Server 2003 v1.0
- US Federal Desktop Core Configuration Standard (FDCC) V1.0.1 for Windows Vista

You can migrate all the generic checks of all the TSPs available to the CCS 9.0.1 or later format. After migration to the 9.0.1 or later format, you can import standards, perform data collection, and evaluate the migrated checks in CCS 9.0.1 or later. You cannot migrate the complex checks of the standards that are present in CCS 8.60 but are not present in CCS 9.0.1 or later. You can find the messages for the checks in the log file.

The utility can migrate only one standard at a time.

About the Standard Migration Utility system requirements

You must ensure that the workstation meets the following hardware requirements:

- 3.0 GHz CPU
- 1 GB RAM
- 1 GB free disk space
- Monitor resolution set to 1024x768 pixels or greater

You must ensure that the workstation meets the following software requirements:

- Microsoft Windows Server 2003 SP1 or later

- Microsoft Windows XP SP2 or later
- Microsoft .NET 3.0
- Microsoft Jet OLE DB 4.0

Note: You can download the Microsoft Jet OLE DB 4.0 utility from the Internet.

About the Standard Migration Utility packaging and deployment

The utility is present in the Symantec_Control_Compliance_Suite_Migration_Utility_9.0.1_Win.exe Web package.

You can extract the content of the Web package to any location. The installation of the Control Compliance Suite (CCS) 9.0.1 or later is not mandatory on the computer where you want to migrate the standard. The extraction of the package creates the following folders:

- bin
- Documentation
- MetaData
- Output
- Schema

The bin folder contains the binaries that you must have for migration. The Documentation folder contains the Symantec Standard Migration Utility Guide. The MetaData folder contains password-protected .mdb files for the four platforms. These .mdb files are required to migrate complex checks and for replacing target types. The utility generates the migrated files in the CCS 9.0.1 or later format in the output folder. The output file is an .xml file that is time stamped. The Schema folder contains PolicyTree.xsd, which is the XSD for CCS 8.6. The Schema folder also contains standard.xsd, which is the XSD for CCS 9.0.1 or later. These files are required for validation.

Note: The .mdb files in the MetaData folder are password-protected.

Standard Migration Utility

The following notes describe the known issues in the Standard Migration Utility:

- Checks that have the following fields are not migrated:

ACCOUNTTYPE	GROUP data source
RELATIVEADSIPATH	IISVIRTUALDIRECTORIES data source
BROWSINGENABLED	IISVIRTUALDIRECTORIES data source

The checks that are created by using these fields are also not migrated.

- The utility does not look into the values that are sent to various operators in the input standard expressions, for example, Match operator. The utility does not perform any corrective action on the operators. It does not correct improper regular expressions too. The utility migrates the expressions and may display an error during evaluation.
- If the 8.60 input standard has the predicates that have any one of the following, then you must correct the standard as per 9.0.1 format before migration :
 - Unequal number of open and closed brackets
 - Individual expressions that are not in brackets
For example, <predicate>IF NOT [A2] THEN [A2] ELSE [A1]</predicate>
instead of <predicate>IF (NOT [A2]) THEN [A2] ELSE [A1]</predicate>.
Otherwise, the checks are not migrated.
- The Standard Migration Utility does not migrate a standard that contains checks to scan multiple platforms such as UNIX, Windows, SQL, and Oracle. Ensure that the checks in a standard pertain to single platform.
- The check Are Deleted Database pages Zeroed out? of the standard Security Essentials for Exchange 2007 is properly migrated using the utility. However, the migrated check will not function as expected.
- In CCS 8.60 when server related checks were evaluated against a administrative group or organization target the checks used to be evaluated against all servers under the administrative group/organization. This behavior is no longer supported in CCS 9.0.1. The user will not be able to evaluate a server related check on any target other than a server. Similarly, checks applicable to organizations and administrative groups can only be evaluated against an organization and an administrative group assets respectively.
- Some of the fields required in the Exchange 2000 standard are not available in the product and migration utility. Any check using any of the following fields will not be migrated by the Standard Migration Utility:

- MAILADMIN.EXCHANGE2KDIRECTORY.CHANNEL_EVERYONEACCESS
- MAILADMIN.EXCHANGE2KDIRECTORY.CLASS_MSEXCHCHATMAXCONNECTIONS
- MAILADMIN.EXCHANGE2KDIRECTORY.ADSI_MSEXCHAUTHENTICATIONFLAGS_NONRMS
- MAILADMIN.EXCHANGE2KDIRECTORY.FILTER_ENABLED
- MAILADMIN.EXCHANGE2KDIRECTORY.COMMUNITY_EVERYONEACCESS
- MAILADMIN.EXCHANGE2KDIRECTORY.ADSI_MSEXCHSMTPRELAYRESTRICTION

How to use the Standard Migration Utility

The Standard Migration Utility is a command-line tool. This tool accepts command-line options and produces a standard that is consistent with CCS 9.0.1 or later standard schema. The tool provides a logging facility because CCS 8.60 or older standard can have a large number of procedures, checks, and sections to migrate. The details about each item that the tool migrates is successfully logged. The utility also logs any item that does not migrate and includes reasons for not migrating the item.

A user who has the permissions to import a standard can import the migrated standard into CCS 9.0.1 or later.

About the command-line options

You must provide the following command-line options to the utility:

- -standard
- -platform

You must type the following in the command prompt and press enter to start the migration:

```
StandardMigrator.exe -standard <fully qualified name of the standard file> -platform <Unix/Oracle/Windows/SQL/Exchange>
```

Note: You must run the command from the StandardMigrationTool\bin folder.

For example,

```
StandardMigrator.exe -standard "D:\build_drops\5th  
Dec\StandardMigrationtool\SampleOldStandards\Old_CISAIXV101.std" -platform  
UNIX
```

The possible values for the platform are UNIX, Oracle, Windows, SQL, and Exchange. The option is case insensitive.

About validation

The Standard Migration Utility validates the following:

- **Input Standard**
 After you provide the details to the utility, the utility checks whether the input file exists and if the platform is valid. The input standard file is then validated against the PolicyTree.xsd. The process of migration continues if the input file is valid. If the input standard file is invalid then the message "Input standard is invalid" appears. The utility then prompts whether you want to continue with the migration. The log file is updated with the details of the validation error in the input standard. If you choose to continue, then the migration continues with an invalid input standard.
- **Migrated Standard**
 The utility logs all successful migration of standards to the log file. The errors are also logged in the log file. The final standard in the CCS 9.0.1 or later format that is migrated is validated against the CCS 9.0.1 or later standard that is shipped with the tool. If invalid, a message appears that states that the standard has been migrated but it is invalid. Otherwise, a valid standard is generated. A migration without an error indicates the generation of a valid CCS 9.0.1 or later standard.
 You can still receive a valid standard that may contain invalid checks. For example, if during migration the utility fails to migrate a particular check, then the log file contains the migration errors of that check. But because the tool skips that check and continues the migration of other checks, the final migrated standard is valid. However, the standard does not contain the invalid check.

About the log file configuration settings

The details of logging is configurable through the StandardMigrator.exe.config file that is located in the bin folder. Open the configuration file in a standard text editor to make the changes.

The configuration file has the following settings:

- **add key="CheckTypeToMigrate" value=**
 You can use this option to specify whether all checks or only the generic checks are to be migrated.
 For example, `<add key="CheckTypeToMigrate" value="generic" />`

The setting has the following possible values:

All	Migrates all the checks in the standard.
Generic	Migrates only the generic checks in the standard.

The default value is All.

■ Log.Disable

You can use this option to disable the entire logging subsystem. When you enable this option, all of the log messages written by the application and its support assemblies are ignored.

Note: Enabling this option can provide a performance gain. However, no diagnostic output exists, regardless of severity.

The setting has the following possible values:

- True
- False

The default value is false.

■ Log.FileLogger.Severity

Each diagnostic message written to the logging subsystem has a severity associated with it. Severity is defined as one of the following values:

Error	These messages indicate that some type of critical error has occurred. Messages with a severity of Error usually indicate that a component is no longer capable of functioning. The component also operates under reduced functionality or may have lost data.
Warning	Messages with a severity of Warning usually indicate that a potential problem has occurred that may cause more serious consequences later if not corrected.
Information	Informational messages are used to indicate normal flow of execution. These messages are usually employed to mark milestone events during normal execution.
Verbose	Verbose messages provide more in-depth details about normal or abnormal execution and are intended to aid in diagnosing problems in the field.

The Log.FileLogger.Severity option provides a way to filter the messages that get output based upon a severity threshold. The following four possible values exist for Log.FileLogger.Severity:

Error	Messages with a severity of Error is the output.
Warning	Messages with severity of Warning or Error is the output.
Information	Messages with severity of Information, Warning, or Error is the output.
Verbose	Messages with severity of Verbose, Information, Warning, and Error is the output.

The default value is Error.

- **Log.FileLogger.BaseFilename**
This parameter defines the base file name that is used for log files of this application. Log file names take the following form:
base_filename.timestamp.pid.sequence_number.extension
This option defines the base_filename portion of the log file name.
The default value is name of the executing assembly without the extension..
- **Log.FileLogger.LogDirectory**
This parameter specifies the location to which log files for this application are written. You may specify either a relative path or an absolute (rooted) path for this option. The behavior differs depending upon the path that you specify. If you specify an absolute (rooted) path, log files are written to that directory. Do not use this method except in situations where the base logging directory is undesirable.
If you specify a relative path, that path is added to the base logging directory and log files are written into that directory. Use this method because it allows all log files to be written under a common directory structure.
By default, the base logging directory is:
<common_app_data>\Symantec.CSM\Logs
The <common_app_data> directory is a special directory defined by Windows. Its location varies depending upon the operating system. <common_app_data> resolves in the following location on different versions of Windows:

Windows 2000/XP/2003	<systemdrive>\Documents and Settings\All Users\ApplicationData
Windows Vista/2008	<systemdrive>\ProgramData

If <common_app_data> is undesirable as a location for the base logging directory, you can change the base logging directory.
The default value is Empty (logs are written to <common_app_data>\Symantec.CSM\Logs).

- `add key="MetadataLocation" value=`
You can use this option to specify metadata location and name in the configuration file.
For example, `<add key="MetadataLocation" value="C:\patch_chk_metadata.mdb" />`
The setting has the following possible values:
 - Metadata location with name.
 - If value of this key is empty then the Standard Migration Utility uses the default metadata depending upon the platform specified.

About migration summary report

The migration summary report is generated after migration of the standards. This summary report is generated in the Output folder. The summary report name is same as the name of the migrated standard with “MigrationSummary” prefixed before the file name.

For example,

MigrationSummary_Symantec_2_6_2009 11_37_17 AM.csv

The output file is a .csv file that has the following columns:

Check	Section	Status
-------	---------	--------

Limitations in the Standard Migration Utility

The utility has the following limitations:

- Constant upgrade or changes are needed to the Standard Migration Utility as upgrade or changes occur in CCS 9.0.1 or later content.
- The utility migrates only “procedures” and “policy” tags under the “tree” tag of the custom standards that are migrated. The utility does not migrate “refmachine” and “scopes” tags under the “tree” tag. If “refmachine” and “scopes” tags are present then the utility discards the tags as they are not required for migration in CCS 9.0.1 or later.
- In CCS 8.60 through scopes you can specify the following:
 - Where to get files from
 - Whether to get content
 - Sub folders to be included

9.0.1 does not have scopes. The Standard Migration Utility performs the function of scopes for most of the cases.

Otherwise, you need to specify these parameters in the check itself (in the selectors and filters of the checks).

If the input check does not have the following fields, then post migration such a check fetches files from default location (\ root and one level below root):

- UNIX.File.Parent Directory
- UNIX.File.Fully Qualified Name
- UNIX.File.Base Name

To correct this problem modify the migrated check as shown:

An input check (Search for world writable directories with sticky bit set in whole box) with expression

```
<expression name="n0" ...>
<text>"UNIX.FILE.ISWOTH" = True</text>
<selectors>
<text>"UNIX.FILE.TYPE" = "directory"</text>
<text>"UNIX.FILE.ISWOTH" = True</text>
</selectors>
</expression>
```

Is migrated to check with expression

```
<datacollectionqueries>
<datacollectionquery mosentityname="Unix.File">
<mosfields>
...
</mosfields>
<filters>
<filter filteroperator="And">
<filtertext>Unix.File.Type = 'directory'</filtertext>
<filtertext>Unix.File.IsWOTH = 'True'</filtertext>
</filter>
</filters>
</datacollectionquery>
</datacollectionqueries>
<procedure>
<expressions>
<expressions>
<expression name="n0" ...>
<text>Unix.File.IsWOTH = 'True'</text>
<selectors>
```

```

<text>Unix.File.Type = 'directory'</text>
<text>Unix.File.IsWOTH = 'True'</text>
</selectors>
</expression>
</expressions>
</expressions>
It should be changed to
<datacollectionqueries>
<datacollectionquery mosentityname="Unix.File">
<mosfields>
...
</mosfields>
<filters>
<filter filteroperator="And">
<filtertext>Unix.File.Type = 'directory'</filtertext>
<filtertext>Unix.File.IsWOTH = 'True'</filtertext>
<filtertext>Unix.File.FullyQualifiedName LIKE '/%'</filtertext>
<filtertext>Unix.File.FindOptions = '-type d -perm +022'</filtertext>
</filter>
</filters>
</datacollectionquery>
</datacollectionqueries>
<procedure>
<expressions>
<expressions>
<expression name="n0" ...>
<text>Unix.File.IsWOTH = 'True'</text>
<selectors>
<text>Unix.File.Type = 'directory'</text>
<text>Unix.File.IsWOTH = 'True'</text>
<text>Unix.File.FullyQualifiedName LIKE '/%'</text>
<text>Unix.File.FindOptions = '-type d -perm +022'</text>
</selectors>
</expression>
</expressions>
</expressions>

```

- Change LIKE to "match" in the input check if the input check has the LIKE operator with a value that has patterns other than the patterns recognized by SQL equivalent LIKE operator, for example %, _, [a-z], [%]. Otherwise, you might receive a run time error during evaluation.

For example, you should change Field1 LIKE 'ab.*c' to Field1 match 'ab.*c'

Troubleshooting evaluation mismatches

Some evaluation mismatches may occur while the product evaluates the migrated standard. The following resolutions exist for the problem:

Problem Consider a check with two or more expressions, where some, but not all, have the same selectors and the MOS field. This check can give an incorrect evaluation result.

For example, if we have a check such as:

```
<procedure>

<precondition>

<procedure>

<description>Description</description>

<expressions>

<expression name="A1" default="Unknown" rollup="Or"
selectorOperator="AND">

<text>Wnt.Service.Name %~ '/alerter/I'</text>

</expression>

</expressions>

<predicate>[A1]</predicate>

</procedure>

</precondition>

<description>Description</description>

<expressions>

<expression name="A2" default="False" rollup="And"
selectorOperator="OR">

<text>Wnt.Service.StartupType = 'Automatic'</text>

<selectors>

<text>Wnt.Service.Name = 'Error Reporting
Service'</text>
```

```
</selectors>  
</expression>  
</expressions>  
<predicate>[A2]</predicate>  
</procedure>
```

Where the expression A1 does not have a selector and A2 has selector and both deal with same field (Wnt.Service.Name). The reason is that the selector in A2 creates a filter and the utility will filter data as per the filter tag. So in the example given the data for "alerter" Service (expression A1) is never retrieved.

Resolution To resolve this problem, you should include a selector in A1 as shown:

```
<procedure>
<precondition>
<procedure>
<description>Description</description>
<expressions>
<expression name="A1" default="Unknown" rollup="Or"
selectorOperator="AND">
<text>Wnt.Service.Name %~ '/alerter/I'</text>
<selectors>
<text>Wnt.Service.Name = 'Alerter'</text>
</selectors>
</expression>
</expressions>
<predicate>[A1]</predicate>
</procedure>
</precondition>
<description>Description</description>
<expressions>
<expression name="A2" default="False" rollup="And"
selectorOperator="OR">
<text>Wnt.Service.StartupType = 'Automatic'</text>
<selectors>
<text>Wnt.Service.Name = 'Error Reporting
Service'</text>
</selectors>
</expression>
</expressions>
<predicate>[A2]</predicate>
</procedure>
```


Problem If a check calls a procedure 1 and that procedure 1 calls another procedure 2 that accepts argument. But the procedure 1 calls procedure 2 without the arguments, then the check can give an incorrect evaluation result.

For example, if we have a procedure such as;

```
<procedure name="P2">
  <expressions>
    <expression name="A1" default="True" rollup="OR"
      selectorOperator="AND">
      <text>"WNT.PATCHASSESSMENT.BPM_PRODUCT_NAME" =
        !ProductName</text>
    </expression>
  </expressions>
  <predicate>[A1]</predicate>
</procedure>
<procedure name="P1">
  <precondition>
    <procedurename custom="False">P2</procedurename>
  </precondition>
  <expressions>
    <expression name="A1" default="Unknown" rollup="AND"
      selectorOperator="AND">
      <text>"WNT.PATCHASSESSMENT.BPM_PATCH_STATUS" != Missing
        Service Pack</text>
    <selectors>
      <text>"WNT.PATCHASSESSMENT.BPM_PRODUCT_NAME" =
        !ProductName</text>
```

```
</selectors>  
</expression>  
</expressions>  
<predicate>[A1]</predicate>  
</procedure>
```

Where the procedure P2 accepts an argument and it is called from procedure “P1” without providing any argument. Procedure “P1” is called from check, so in this case the check results in “Not Applicable”. As procedure “P2” is called from the “Predicate” tag of the procedure “P1” without providing argument and “P2” does not receive the value of the argument that the procedure expects.

Resolution To resolve this problem you must call procedure “P2” by providing argument as shown:

```
<procedure name="P2">
  <expressions>
    <expression name="A1" default="True" rollup="OR"
      selectorOperator="AND">
      <text>"WNT.PATCHASSESSMENT.BPM_PRODUCT_NAME" =
        !ProductName</text>
    </expression>
  </expressions>
  <predicate>[A1]</predicate>
</procedure>

<procedure name="P1">
  <precondition>
    <procedure>
      <predicate>[proc:P2 (ProductName = !
        ProductName)]</predicate>
    </procedure>
  </precondition>
  <expressions>
    <expression name="A1" default="Unknown" rollup="AND"
      selectorOperator="AND">
      <text>"WNT.PATCHASSESSMENT.BPM_PATCH_STATUS" != Missing
        Service Pack</text>
    <selectors>
      <text>"WNT.PATCHASSESSMENT.BPM_PRODUCT_NAME" =
        !ProductName</text>
    </selectors>
    </expression>
  </expressions>
  <predicate>[A1]</predicate>
</procedure>
```


ESM Policy to CCS Standard Migration utility

This appendix includes the following topics:

- [About the Symantec ESM Policy to CCS Standard Migration Utility](#)
- [About packaging and deployment](#)
- [System requirements for the ESM Policy to CCS Standard Migration Utility](#)
- [About installing the migration utility](#)
- [Uninstalling the migration utility](#)
- [About the input file in the ESM Policy to CCS Standard Migration Utility](#)
- [Executing the migration utility](#)
- [About the log file in the ESM Policy to CCS Standard Migration Utility](#)
- [About ESM suppressions migration](#)
- [About the message IDs in ESM Policy to CCS Standard Migration Utility](#)
- [Limitations of the migration utility](#)
- [Troubleshooting for ESM Policy to CCS Standard Migration Utility](#)

About the Symantec ESM Policy to CCS Standard Migration Utility

The Symantec ESM Policy to CCS Standard Migration Utility lets you map the existing ESM policies to CCS standards. You can also migrate ESM policies to the

CCS standards by using the CCS Check Builder. However, the CCS Check Builder is time consuming and the level of complexity is high.

To make the ESM policy migration procedure seamless, Symantec has designed the migration utility that automates the process of CCS standard creation from an ESM policy.

The Symantec ESM Policy to CCS Standard Migration Utility is a command-line utility that takes the ESM Policy XML as an input. The utility then generates a CCS Standard XML as an output. At a time, the utility can take only one ESM Policy XML as an input.

Table C-1 ESM and CCS content mapping

ESM	CCS
ESM policy name	CCS standard name
ESM module name	CCS section
ESM OS platform	CCS section
ESM check title	CCS check name
ESM check description	CCS check description
ESM message, message string ID, or message numeric ID	CCS check expression

About packaging and deployment

A Web package by the name Symantec_Control_Compliance_Suite_ESM_SU_39_Migration_UTILITY_9.0.1_Win.exe contains the migration utility. You can run the Web package on your local computer to extract the content. The utility creates a folder by the name "ESMPolicyToCCSStandard," which contains the following binaries:

File	Function
ESMPolicyToCCSStandard.exe	Migration Utility
ESMPolicyToCCSStandard.exe.config	Migration Utility Configuration file
Security-content.xml	Security Content XML
Symantec.CSM.Resources.SUResources.dll	SU Resources Assembly
ESMTargetTypeMapping.xml	ESM Target Type Mapping XML

File	Function
Symantec™ ESM Policy to CCS Standard Migration Utility User's Guide	Documentation

Additional information about the files

The additional information of the files is as follows:

security-content.xml	<p>The security-content.xml file contains the metadata information about the ESM checks and the ESM security messages. In addition, it contains the mapping of all the ESM security messages that an ESM check generates.</p> <p>The Security Content XML is located in the update package that is created for Reporting Database Link (RDL). The Security Content XML is updated and is shipped with every ESM Security Update release.</p>
Symantec.CSM.Resources.ESMSUResources.dll	<p>The security-content.xml file contains the numeric codes for all the metadata information about the ESM checks and the ESM security messages. The SU Resource assembly contains the actual text for each of these codes.</p>

System requirements for the ESM Policy to CCS Standard Migration Utility

The computer on which you want to install the migration utility must meet the following hardware requirements:

- 3.0 GHz CPU
- 1 GB RAM
- 1 GB free disk space

The computer on which you want install the migration utility must meet the following software requirements:

- Microsoft Windows Server 2003 SP1 or later
- Microsoft Windows Server 2003 x64 SP1 or later
- Microsoft Windows XP Professional SP2 or later
- Microsoft Windows XP Professional x64 SP2 or later
- Microsoft Windows Vista

- Microsoft Windows Vista x64
- Windows Server 2008
- Microsoft Windows Server 2008 x64

About installing the migration utility

Run the Web package to extract the content. You may copy all the files from the ESMPolicyToCCSStandard folder to a new folder under any of the following folders:

- CCS console installation folder from
%APPDATA%\Symantec\CCS-<hostname>\<New folder for the migration utility>
- DPS installation directory, that is, from <CCS Installation Directory>\DPS\<New folder for the migration utility>
- Any other folder. In this case, you have to configure the 'ReferencedAssemblyLocation' attribute in configuration file viz. ESMPolicyToCCSStandard.exe.config. Read the comments in configuration file to understand what value you should specify for this attribute.

Uninstalling the migration utility

To remove this utility, delete the folder ESMPolicyToCCSStandard that the utility Web package has created.

About the input file in the ESM Policy to CCS Standard Migration Utility

The migration utility requires the ESM Policy XML. You can generate the ESM Policy XML by using the Policy Tool, which is provided with ESM. The Policy Tool utility exports ESM policies as XML formatted files.

Executing the migration utility

To start using the migration utility, you have to copy all the files in an installation folder and then run the utility.

Executing the migration utility

- ◆ You must run the following format from the command prompt for the utility to start migrating data:

```
ESMPolicyToCCSStandard.exe -e <esmpolicy.xml> -m {NUMERIC |  
STRING} [-c {message categories}] [-o {ccsstandard.xml}] [-xs]
```

The following table describes the parameters and their corresponding descriptions:

-e	ESM Policy XML file path. You must specify the path of the ESM Policy XML using this option. The path must exist and be accessible.
-m	<p>This option is mandatory. You can specify either NUMERIC or STRING. If NUMERIC is specified, the utility creates CCS check expression based on ESM security message's numeric ID. If you specify the string, the utility creates CCS check expression based on ESM security message's string ID.</p> <p>See “About the message IDs in ESM Policy to CCS Standard Migration Utility” on page 747.</p>
-o	This parameter is optional. Output Standard XML file path. You can specify the path for this output standard XML file by using this option. The path must exist and be accessible. The path can be a directory, a filename, or an entire path of a file. By default, output standard XML is created in the current directory and the filename is Standard-<ESM Policy>.xml.
-xs	<p>This parameter is optional. If you specify this option, then the migration utility does not migrate the ESM suppressions to CCS Standard.</p> <p>See “About ESM suppressions migration” on page 747.</p>

-c

This parameter is optional. You can customize the default list of the messages categories that are migrated to the standard.

For example, if you do not want to migrate the messages whose categories are system Information, then you can use the -c option with the list of comma separated message categories in addition to the other regular options whilst executing the migration tool.

```
ESMPolicyToCCSStandard.exe -e "policy.xml" -m STRING -c 1,2,3,8,500
```

In the above example,-c 1,2,3,8,500 refers to migration of all messages that belong to the following categories: Policy Compliance, Patch Assessment, Change Notification, ICE, Network Assessment respectively.

See [“About the default category IDs for creating the formula”](#) on page 746.

The following is the example of the format:

```
ESMPolicyToCCSStandard.exe -e "D:\ESM\ESM Policies\CIS\Window2003\ciswin2k3DC.xml" -m STRING -o "D:ESM\CCS Standards\CIS\CIS Win2K3 Domain Controller.xml" -c 1,2,3,8,500.
```

About the default category iDs for creating the formula

By default, the Migration utility uses the messages with the following category IDs for creating the formula:

[Table C-2](#) lists the default category iDs for creating the formula

Table C-2 Default category iDs	
Category ID	Category
1	Policy Compliance
2	Patch Assessment
3	Change Notification
7	System Information
8	ICE
500	Network Assessment

About the log file in the ESM Policy to CCS Standard Migration Utility

The migration utility creates a log file in the same location from where you execute the utility. The name of the log file is as follows:

ESMPolicyToCCSStandard.<ESMPolicyFilename>.<DateTime>.<Process ID>.<Sequence Number>.csv

About ESM suppressions migration

If you run the migration utility without specifying the -xs option, then the ESM suppressions gets migrated to CCS Standard. The utility creates the "Is any ESM message suppressed?" check for each module. The "Is any ESM message suppressed?" check fails if any ESM message is suppressed. The migration utility does not create multiple CCS checks per suppressed message in ESM. It creates one such check per ESM module for each ESM OS version. As evidence for the check failure, you can see the suppressed messages for the corresponding ESM module. You can mark the CCS check as exception and use the features that the CCS Exception Management application provides.

Note: For the "Is any ESM message suppressed?" check to work as explained, you must uncheck the 'Do not collect suppressed messages' check box in ESM data collector configuration before data collection. When you uncheck the 'Do not collect suppressed messages' check box, the ESM data collector collects the suppressed messages during data collection.

About the message IDs in ESM Policy to CCS Standard Migration Utility

Every security message that an ESM check generates has a distinct numeric ID. The string ID is the string representation for the numeric message ID and is platform independent.

For example, for the ESM security message “System allows blank passwords,” the numeric IDs for different OS Versions are as follows:

OS Version	Message Numeric ID
Windows 2000	105336

OS Version	Message Numeric ID
Windows 2003	205336
Windows 2008	248336
Windows Vista	228336
Windows XP	200336

However, the message string ID across all OS versions is “ESM_PASSNOPASS”.

Only the Message IDs that belong to one of the following message categories are included for migration:

- Policy compliance
- Patch Assessment
- Change notification
- System information
- ICE
- Network assessment

Advantages and disadvantages of policy migration based on the Message String ID

Using the ‘-m STRING’ option creates CCS check expression based on the Message String ID.

The advantage of policy migration based on the Message String ID is that the Message String ID is platform independent. Hence, you can copy the check and use it for the ESM assets that are running on different operating systems by changing the target type.

The disadvantage is that the raw reports of the policy runs contain only the Message Numeric ID of the security messages. The ESM data collector retrieves the Message String ID from the Message Schema XML which is deployed with the ESM data collector. For 2010-2 Update, this Message Schema XML is generated from the security-content.xml of SU 2010.03.01 (SU 39).

Sometimes, the ESM data collector may fail to retrieve the Message String ID of the security message. This happens when an ESM agent with a higher SU version reports a security message that is newly added in the specified SU. In such a scenario, the check may not evaluate as expected. As a resolution, you must obtain the ESM data collector upgrade package and upgrade the SU version of the Message Schema XML and the SU Resources assembly.

Advantages and disadvantages of migration based on Message Numeric ID

Using the '-m NUMERIC' option creates CCS check expression based on Message Numeric ID.

The advantages of policy migration based on the Message Numeric is that if the ESM data collector cannot find the metadata for an ESM message in its Message Schema XML, it requests the ESM manager to format the messages. Hence, irrespective of the SU version of the ESM data collector, the CCS check is always evaluated as expected. The ESM data collector gathers the details from the ESM manager if an ESM agent with a higher SU reports a security message, which is new in the specified SU. In such a scenario, the CCS check is evaluated as expected even though metadata for that message is not available with the ESM data collector.

The disadvantages is that the Message Numeric ID is platform-dependent. Hence, the same check cannot be used across ESM agents that are installed on different operating systems.

Limitations of the migration utility

The migration utility has the following limitations:

- This utility does not support automatic synchronization of modified ESM policies and CCS standards. For example, if you translate ESM policy "ESM_A" CCS standard "CCS_A". Afterward, if you modify "ESM_A", you have to re-run the utility to create a new version of the standard.
- Only one CCS check is created for an ESM check that is based on a name-list or a template. Therefore, the ESM messages that are reported for an entry in a name-list or a template are reported as evidence.
- You cannot use the utility to migrate the ESM policies for the following ESM platforms:
 - NDS/NetWare
 - Tru642010-2 Update does not support the NDS/NetWare and Tru64 target types for ESM data collector.
- To migrate ESM suppressions to CCS, the utility creates the CCS check "Is any ESM message suppressed?" for each module. The "Is any ESM message suppressed?" check fails if any ESM message is suppressed. The utility does not create multiple CCS checks per suppressed message in ESM. Also, the utility does not convert the ESM suppressions to CCS exceptions. However,

you can manually mark the check “Is any ESM message suppressed?” as CCS exception.

- You cannot choose the message categories to be considered when you migrate the ESM checks. The utility uses all the categories that are mentioned in the About Message string ID.
See “[About the message IDs in ESM Policy to CCS Standard Migration Utility](#)” on page 747.
- The utility migrates only the enabled ESM checks from the ESM policy.

Troubleshooting for ESM Policy to CCS Standard Migration Utility

You may encounter problems when you use the migration utility. This chapter includes information on the problems that may occur and their resolution.

Table C-3 Migration utility problems and their resolution

Problem	Resolution
Could not find file <path>\Symantec.CCS.Apps.Standards.Exceptions.dll CCS Console pulls assemblies dynamically to the CCS installation folder (i.e. %APPDATA%\Symantec\CCS-<hostname>) as and when it needs them.	If you have not yet visited Standards view from the CCS console, assemblies related to standards do not exist in the console installation folder. Launch the 2010-2 Update console and go to the Standards UI. Go to Manage > Standards .

Table C-3 Migration utility problems and their resolution (continued)

Problem	Resolution
Could not retrieve module long name for '<module short name>', skipping all checks for this module. Use the updated Symantec.CSM.Resources.ESMSUResources.dll	<p>The ESM Policy XML contains the module short name for the ESM modules that are included in the policy. The utility first retrieves the code for the module long name from the Security Content XML. The utility then retrieves the actual module long from the SU Resources assembly.</p> <p>If either of them is out-dated, it may not contain information for the modules that were recently added in ESM content. Without the module long name, the utility cannot create 2010-2 Update checks because the 2010-2 Update ESM Message entity schema only understands module long names.</p> <p>To resolve this issue, you need to use the utility with the latest Security Content XML and latest SU Resources assembly.</p>

Table C-3 Migration utility problems and their resolution (*continued*)

Problem	Resolution
Cannot locate the latest Security Content XML	<p>Security Content XML is present in the update package that is created for RDL and is shipped with every Security Update released by ESM Content.</p> <p>You can find the update package for RDL in the following location on the ESM manager:</p> <p><ESM Installation Folder>\update\ble\<Latest SU Version>\en\UpdatePackage.rdl</p> <p>Perform the following in the given order:</p> <ul style="list-style-type: none"> ■ Create a copy of the package. Do not tamper the original file because RDL may give errors if it fails to find the file UpdatePackage.rdl. ■ Rename it from UpdatePackage.rdl to UpdatePackage.zip. ■ Extract the content of this compressed file. ■ Copy the security-content.xml file from the extracted folder. Save the XML in the 2010-2 Update Console installation folder from where you intend to run the Symantec ESM Policy to CCS Standard Migration Utility. <p>Note: If a new module is added in the latest SU update, you need the corresponding ESM data collector upgrade package.</p>
Cannot locate the latest SU Resources Assembly	<p>Copy the latest Symantec.CSM.Resources.ESMSUResources.dll from the <DPS installation Folder>\Data Collectors\ESM to the 2010-2 Update console installation folder from where you intend to run the Symantec ESM Policy to CCS Standard Migration Utility.</p> <p>If the Symantec.CSM.Resources.ESMSUResources.dll in the <DPS Installation Folder>\Data Collectors\ESM is also outdated, you need to update CCS content.</p>

Table C-3
Migration utility problems and their resolution (*continued*)

Problem	Resolution
Warning message: ESM OS Version '[ESM OS Version]' is not supported. Skipping migration of checks enabled for it.	<p>This warning message is displayed in case of the following:</p> <ul style="list-style-type: none"> ■ A different ESM OS version is encountered. ■ Migration of all checks that are enabled for that ESM OS version is skipped.
Warning message: The description information for the CCS Check may be blank as the utility could not retrieve the ESM Check Description.	<p>The ESM check description is migrated as CCS check description. First the migration utility retrieves the check description code from the Security Content XML. Then the utility retrieves the actual text for the check description from the SU Resources assembly. This error may occur if either of them is out-dated.</p> <p>To resolve this problem, use the updated Security Content XML and updated SU Resources Assembly.</p>

Reporting database schema

This appendix includes the following topics:

- [About the Reporting database](#)

About the Reporting database

The topic describes the module-specific classification of the reporting database (CSM_Reports) tables. The reporting database has several modules.

Standards, sections, and checks form the backbone of the Standards module. The system lets you evaluate one or more standards on one or more assets. The result information is available to verify compliance of the standards against those assets.

Most of the standard module reports accept the Report job identifier and standard information as inputs. The report identifier is stored in the ReportJobs table of the Reporting database. The ReportJobs table contains the Job identifier and the Asset identifiers, which correspond to the assets that are given as input to the report. The ReportJobs table is linked to the other tables to generate reports based on the assets and standard, which are inputs in the latest evaluation. The Report identifies the latest evaluation with the current row column in the Facts table. The rows in the Facts table that have the current row value as 1 represent the latest evaluation for the assets and standard checks combination. To generate reports on the current as well as the historical data, the user has to consider the archive tables. Every report accepts the Report ID as input to display the report tags.

Table D-1 Standards Table Descriptions

Table Name	Description
Asset_Std_Summ, Asset_Std_Summ_Archive	<p>Each row has the following information:</p> <ul style="list-style-type: none"> ■ Total count of the passed or failed or other checks ■ Passed or failed or other compliance score ■ An aggregate risk score of an asset against a standard <p>The archive table contains historical data that is not used in the reports.</p>
Asset_Summary, Asset_Summary_Archive	<p>Each row has the following information:</p> <ul style="list-style-type: none"> ■ Total count of the passed or failed or other checks ■ Passed or failed or other compliance score ■ Composite risk score of an asset against all standards <p>The archive table contains historical data that is not used in the reports.</p>
AuditLoad	<p>The table tracks synchronization start time, end time, and source update time. Each row in all of the Standards module tables is linked to one row in the AuditLoad table.</p>
EvalChecksToExceptions	<p>The tables have all of the exceptions that are associated with an asset that is evaluated against a check.</p>
Evaluation_Jobs	<p>Each row has information about the evaluation job and the evaluation job details.</p>
Fact_table	<p>Each row has the following information:</p> <ul style="list-style-type: none"> ■ Total count of the passed or failed or other checks ■ Passed or failed or other compliance score ■ An aggregate risk score of an asset against a standard

Table D-1 Standards Table Descriptions (*continued*)

Table Name	Description
TargetsToExceptions,TargetsToExceptions_Archive	<p>The table has all of the exceptions that are associated with an asset that a standard evaluates.</p> <p>The archive table contains historical data that is not used in the reports.</p>
Sections	Each row represents a section of a standard
Standards_Summary, Standards_Summary_Archive	<p>Each row has the following information:</p> <ul style="list-style-type: none"> ■ Total count of the passed or failed or other checks ■ Passed or failed or other composite score ■ The composite risk score of a standard against all assets <p>The archive table contains historical data that is not used in the reports.</p>
Status_LKP	Lookup table for check outcome status ordinal numbers to status strings
SM_FailureTrend_DB	<p>This table is the Failure Trend dashboard summary source.</p> <p>Each row has the one-row-for-one-month information for an asset against a standard:</p> <ul style="list-style-type: none"> ■ Count of new checks ■ Count of carried over checks ■ Count of reopened checks ■ Count of total checks
SM_FailureTrend_Map	The table is used internally to represent the states and transitions of the SM_Failure_DB table.

Table D-1 Standards Table Descriptions (*continued*)

Table Name	Description
Standard_ComplianceTrend_DB	<p>The table is the Remediation Dashboard Summary source.</p> <p>Each row has the following information about a standard evaluated against all of the assets:</p> <ul style="list-style-type: none"> ■ Daily compliance ■ Weekly compliance ■ Monthly compliance

Standard module-related reports read data from the following tables:

- Assets
- Asset_STD_SUMM
- Checks
- Standards
- Fact_Table

The common tables, ReportTags, and Company, contain the configuration information for each report.

The Entitlements in Control Compliance Suite facilitates the monitoring of the access rights in the organization. The Entitlements view provides the means to efficiently gather the permissions data from the various platforms and enable the user to generate reports.

Table D-2 Entitlements Table Descriptions

Table name	Description
EM_AuditLoad	Internal Use: Tracks the synchronization start time, end time, and source update time. Every row in the other Entitlement Module table is linked to one row in this table.
EM_ControlPoint_Fact	Contains the current configuration and the snapshot information of the control points for an ongoing or a completed review cycle respectively.
EM_ControlPointStatusOrdinal	A lookup table for control point status ordinal numbers to actual Status strings.

Table D-2 Entitlements Table Descriptions (*continued*)

Table name	Description
EM_DisplayNameLookUp	Internal use: Lookup table for different keywords to their display names.
EM_Entitlement_FACT	Each row represents a trustee and its permissions on a particular control point. It contains the current entitlements that are imported and snapshot entitlements for a completed review cycle.
EM_EntitlementChange_FACT	Each row gives the difference in the current and the last snapshot permissions for a trustee on a control point.
EM_EntitlementChangeTypeOrdinal	Internal use: Lookup table for the change type ID ordinal numbers that are associated with each row in EM_EntitlementChange_FACT table.
EM_EntitlementType	Lookup table for entitlement type ordinal numbers to actual type strings.
EM_Exceptions	Each row gives the control point that is exempted from review in a particular review cycle.
EM_FrequencySettings	Contains the different duration frequencies that are used in defining a review cycle setting.
EM_ReviewCycle	Each row gives information about a review cycle.
EM_ReviewCycle_FACT	Contains the state transition for each control point in a completed review cycle.
EM_ReviewCycleSettings	Each row is a Review Cycle Setting. The review cycle setting is the time frame for which the entitlements are validated.
EM_ReviewCycleStatusOrdinal	Lookup table for review cycle status ordinal numbers to actual status strings.

Entitlements reports accept either control points or review cycles as input along with the Reportjob identifier. The Report identifier is stored in the ReportJobs table of the Reporting database with control point IDs. This table is linked to other

entitlement-related tables such as, EM_Entitlement_FACT, EM_EntitlementChange_FACT, EM_ControlPoint_Fact, EM_ReviewCycleSettings, EM_ReviewCycle_FACT, and EM_ReviewCycle.

If the reports are based on the control points, then use the following selection criteria: EM_ControlPoint_FACT.CurrentRow = 1 and EM_Entitlement_FACT.CurrentRow= 1.

If the reports are based on the Review Cycle, then use the following selection criteria:

- EM_ControlPoint_FACT.CurrentRow <> 1
- The control point details are stored in the Assets and Asset_details table

Using the policies features of the Control Compliance Suite, you can manage, publish, and track your policies across the organization. You can also collect evidence of due care of policy compliance.

Policies include the control statements that are mapped to regulations and frameworks. Mapping helps you to see the existing gaps in the current policies of your organization. Mapping also helps you to meet the requirements of each regulation that the organization must comply.

Table D-3 Policy Table Descriptions

Table Name	Description
PM_Comment	Each row represents the reviewer comments of each policy.
PM_Content	Contains the regulations and frameworks and all sections within the regulations and frameworks.
PM_ContentStatement	Contains the mapping between the mandates (PM_Content) and the control statement (PM_Statement).
PM_ContentStatementLevel	Contains the mapping between the content statement mapping and the level. You can find the importance or level of the mapped statement; for example, if a statement is optional.
PM_Policy	Each row gives the definition of a policy.
PM_PolicyStatement	Contains the mapping between the policy(PM_Policy) and the control statement (PM_Statement).

Table D-3 Policy Table Descriptions (*continued*)

Table Name	Description
PM_PolicyTarget	Each row represents an asset that is the target for the policy.
PM_PolicyTargetAssetCollection	Each row represents an asset group or folder that is the target for the policy.
PM_PolicyUser	Internal Use: contains the recipients for a policy. The table is populated during the policy report run.
PM_Statement	Contains all control statements.
PM_StatementCheck	Contains the mapping between the control statements (PM_Statement) and Entitlements in EM.
PM_StatementCustomEvidenceProvider	Contains the mapping between control statements (PM_Statement) and third-party evaluation instances for the providers that are registered in the Evidence System.
PM_StatementEntitlement	Contains the mapping between the control statements (PM_Statement) and the Entitlements in EM.
PM_StatementQuestion	Contains the mapping between the control statements (PM_Statement) and the questions in RAM.
PM_UserResponse	Contains the user response of each recipient of the policy.
PM_Clarification	Contains the user-requested clarification and the corresponding responses. A user may request a clarification to a policy before the policy is accepted.
PM_AuditLoad	Internal use: Used to track synchronization start time, end time, and source update time. Every row in all the other Policy Module tables is linked to one row in this table.
RM_AuditLoad	Internal use: Used to track synchronization start time, end time, and source update time. Every row in all the other RAM Module tables is linked to one row in this table.

Table D-3 Policy Table Descriptions (*continued*)

Table Name	Description
RM_Fact_Table	Each row gives the status of a questionnaire\question for a particular asset on a particular day.
RM_StatusOrdinal	Lookup table for question response status ordinal numbers to actual status strings.
TP_AuditLoad	Internal use: Used to track synchronization start time, end time, and source update time. Every row in all the other Third Party Module tables is linked to one row in this table.
TP_Fact_Table	Each row gives the status of a third-party evaluation instance for a particular provider on an asset on a particular day.
TP_StatusOrdinal	Lookup table for third-party evaluation instance status ordinal numbers to actual status strings.
Mandate_Compliance_DB	Compliance for Regulatory Mandates Dashboard summary source. Each row represents an asset along with passed or failed or other. Each row also has a count for the checks or the questions or the review cycle or the third-party instances. This information is mapped to the control statements that are part of a particular mandate.
Asset_ComplianceTrend_DB	Compliance Trends for Asset Groups Dashboard summary source. Each row represents an asset along with passed or failed or other. Each row also has a count for latest checks or questions or review cycle or the third-party instances. This information is evaluated against that asset per day, per week, and per month.

Policy reports accept Report Job ID, Policy ID, and Policy version as inputs along with the Assets business objects to which these policies are applicable. These business object IDs are stored as AssetIDs in the ReportJobs table along with the Report Job ID. These AssetIDs are linked to the TargetID of the PM_PolicyTarget

table. In this manner, data is filtered for the given input policy, which is applied to all the targets (for example, Policy Results Report).

Exceptions are the temporary permissions that exempt an asset from following an organizational policy for a specific time period. The exemption should be made for a valid business reason.

Exception reports accept Report job identifier, Exception types, and Date Range. The ReportJobs table contains the Job identifier and the Asset IDs, which correspond to the assets that are given as input to the report. The Exception Types for a given exception is stored in the EX_EXCEPTIONS table.

Exception reports show the exceptions that are applicable to the assets. These reports are filtered based on the exception types and the date range (for example, Exception status report).

Table D-4 Exceptions Table Descriptions

Table Name	Description
EX_Exceptions	Each row represents an Exception along with its details.
EX_AssociationFor	Gives the type and its details for which an exception can be applied (Assets, Users).
EX_AssociationTo	Gives the type and its details to which an exception can be associated
EX_ExceptionAssociationFor	Gives the mapping between Exceptions and Association_For types.
EX_ExceptionAssociationTo	Gives the mapping between Exceptions and Association_To types.
EX_Identity	Gives the user details involved in the Exception workflow.
EX_AuditLoad	Internal use: Used to track synchronization start time, end time, and source update time. Every row in all the other Exception Module tables is linked to one row in this table.

Table D-5 Change Log Table Descriptions

Table Name	Description
ChangeLogEntries	Each row represents information about a particular event in a module.

Table D-5 Change Log Table Descriptions (*continued*)

Table Name	Description
ChangeLogEventTypes	Contains the list of different events for which entries are made.
ChangeLogModules	Contains the list of modules for which Auditing entries are made.

Different modules use the workflow trail tables to store the audit trail of their workflow.

Table D-6 Workflow Trail Table Descriptions

Table Name	Description
CM_AuditLoad	Internal use: Used to track synchronization start time, end time, and source update time. Every row in all the other Workflow Trail Module tables is linked to one row in this table.
CM_WorkflowTrail_Entry	Each row represents a state of an object (Exception) and the user responsible for changing the object state.
CM_WorkflowTrail_ObjectTypeOrdinal	Each row represents the module that is registered to store its object trail in CM_WorkflowTrail_Entry.

Table D-7 Reporting Metadata

Table Name	Description
Company	Internal Use: Stores the company information that is used for report customization.
Language	Internal Use: Stores the language information that is used for report customization.
Report_Tags	Internal Use: Stores display names or labels for various reports.

Table D-8 Reporting Dashboard Processing Framework

Table Name	Description
ReportJob	Internal Use: Passes the report parameters that are used during report generation.
DisplayInfo	Internal Use: Stores the report footer information.
DB_AssetGrp	Internal Use: Passes the report parameters that are used during report generation.
SM_FailureTrend_Dashboard	Internal Use: Used for Failure Trend dashboard generation.
TrusteeJob	Internal Use: Used for EM Trustee report generation

Table D-9 Synchronization Metadata

Table Name	Description
SSIS_Configuration	Internal Use: Contains the configuration information like log file path, history count, etc. picked by SSIS packages during its execution.
Sync_Modules	Internal Use: Each row represents a module synchronized into the Reporting database. This table is used to pick up the Audit-Table to be used for a module

Table D-10 Temporary Business Objects

Table Name	Description
TempAssets	Internal Use: An intermediate store for synchronization of assets from ADAM into the reporting database table Assets.
TempAssetDetails	Internal Use: An intermediate store for synchronization of Asset Details from ADAM into the reporting database table Asset_Details.
TempBOAssetsToTags	Internal Use: An intermediate store for synchronization of tags from ADAM into the reporting database table BO_AssetsToTags.

Table D-10 Temporary Business Objects (*continued*)

Table Name	Description
TempTags	Internal Use: An intermediate store for synchronization of tags from ADAM into the reporting database table BO_Tags.
TempStandards	Internal Use: An intermediate store for synchronization of standards from ADAM into the reporting database table Standards.
TempChecks	Internal Use: An intermediate store for synchronization of checks from ADAM into the reporting database table Checks.

The Business Object tables represent information about the various Control Compliance Suite business objects that are stored in ADAM.

Table D-11 Business Objects Table Descriptions

Table Name	Description
Assets	Each row represents an asset along with the common attributes.
Asset_Details	Stores the information about all optional attributes of an asset. The custom attributes are also stored in this table.
BO_AssetsToTags	Gives all tags that are associated with an asset.
BO_AuditLoad	Internal use: Used to track synchronization start time, end time, and source update time. Every row in all the other Business Object Module table is linked to one row in this table.
BO_Tags	Each row represents tag information and tag attribute information.
Checks	Each row represents a check along with its attributes.
CheckType_LKP	Lookup table for check type ordinal value (Third Party or Symantec).

Table D-11 Business Objects Table Descriptions (*continued*)

Table Name	Description
Standards	Each row represents a check along with its attributes.

Troubleshooting

This appendix includes the following topics:

- [About troubleshooting](#)

About troubleshooting

Your Control Compliance Suite deployment is a complex of interlocking pieces. From time to time, it is possible that some part of the system may fail. If a failure occurs, the troubleshooting guide can help you to correct it.

In addition to the troubleshooting guide, you should consult the Technical Support Knowledge Base. The Knowledge Base includes references to additional issues and includes additional symptoms and corrective actions.

The Knowledge Base is available at the following URL:

<http://www.symantec.com/business/support/overview.jsp?pid=53741&view=kb>

You may require troubleshooting assistance with the following types of issues:

- Control Compliance Suite deployment
See “[Deployment troubleshooting](#)” on page 770.
- Control Compliance Suite configuration
See “[Configuration troubleshooting](#)” on page 771.
- Asset import
See “[Asset import troubleshooting](#)” on page 772.
- Data collection
See “[Data collection troubleshooting](#)” on page 772.
- Control Compliance Suite Console and Web Portal
See “[Console and Web Portal troubleshooting](#)” on page 772.
- Symantec ESM

See [“Symantec ESM troubleshooting”](#) on page 774.

Deployment troubleshooting

[Table E-1](#) lists possible deployment problems and their associated causes and resolutions.

Table E-1 Deployment troubleshooting

Problem	Cause	Resolution
Failed Directory Server Installation	The domain account credentials that are used for the component are not valid.	Supply valid credentials.
	The c:\Windows directory does not allow software to be installed.	Change the permissions on the c:\Windows directory to allow software installation.
	Active Directory is not available.	Install and configure Active Directory before installing the Control Compliance Suite.
	The C:\Program Files directory on the Directory server host is compressed.	Uncompress the C:\Program Files directory on the Directory server host. Reinstall the ADAM instance. See “Installing Active Directory Application Mode manually” on page 775.
Certificate does not match specified computer	The ping utility has different results for the target computer when run from the Directory Server and from the target computer itself.	Correct network errors to ensure that the same information appears when you use the ping utility from all computers.
	An incorrect certificate type was specified during certificate creation.	Create a new certificate of the correct type.
Application Server install wizard rejects Directory Server credentials	The domain account credentials that are used for the component are not valid.	Supply valid credentials.
	The credentials that were used to log on when the Directory Server was installed should be used. The credentials that were supplied during the installation should not be used.	Supply the user credentials that were used to log on when the Directory Server was installed.

Table E-1 Deployment troubleshooting (*continued*)

Problem	Cause	Resolution
Application Server, Directory Server, or Data Processing Service fail to start	Host computer does not have Internet connectivity or connection to the VeriSign web server is blocked.	Provide access to the VeriSign Web server the first time the service starts. You can also disable certificate checking for all components on the host. Finally, you can manually download the Certificate Revocation List from VeriSign and install it on the host.
When you install with Remote Desktop Connection, installation logs are deleted when the user logs off.	Logs are stored in the %temp%\csmsetup. The folder that is used for the %temp% folder varies depending on the type of user logon. Files in the %temp% folder are deleted automatically when a Remote Desktop Connection user logs out.	Manually copy the log file to another folder after the installation is complete but before logging out.
During the installation, an error message appears. The error message indicates that the state of the secure channel cannot be verified.	The computer has lost its secure channel with the domain.	Rejoin the computer to the domain.

Configuration troubleshooting

[Table E-2](#) lists possible configuration problems and their associated causes and resolutions.

Table E-2 Configuration troubleshooting

Problem	Cause	Resolution
The user is unable to start the Certificate Management Console	A password error appears when the Certificate Management Console is started.	Verify that the user supplies the same password that was supplied during installation of the Directory Server.
	The Certificate Management Console fails to start.	Verify that the user is an administrator of the ADAM or AD LDS installation on the Directory Server. Verify that the user is a Control Compliance Suite Administrator.

Table E-2 Configuration troubleshooting (continued)

Problem	Cause	Resolution
The user is unable to create certificates using the Certificate Manager console.	On Windows Server 2008 computers, the Certificate Manager console is unable to create certificates if it is not run as an administrator.	Run the Certificate Manager as an administrator.

Asset import troubleshooting

The following table lists possible asset import problems and their associated causes and resolutions.

Data collection troubleshooting

The following table lists possible data collection problems and their associated causes and resolutions.

Console and Web Portal troubleshooting

[Table E-3](#) lists possible problems with the console and the Web Portal and their associated causes and resolutions.

Table E-3 Console and Web Portal troubleshooting

Problem	Cause	Resolution
The user cannot start the Control Compliance Suite Console	Cannot locate the Control Compliance Suite Console installer.	The installer is hosted on the Application Server in the \\ <i>Application Server Name</i> \CCS directory.
	The console is unable to contact the Application Server computer by name.	Ensure that the Domain Name Service is properly configured, or use the IP address of the Application Server.

Table E-3 Console and Web Portal troubleshooting (*continued*)

Problem	Cause	Resolution
	The console is unable to successfully start.	<p>Verify that the Application Server service account is trusted for delegation.</p> <p>Verify that the Service Principal Names are properly registered.</p> <p>See “Configuring service accounts with unconstrained delegation” on page 159.</p> <p>See “Configuring the S4U and constrained delegation” on page 160.</p>
The Web Portal is unable to connect to the Response Assessment module	Web Portal is not configured to connect to the Response Assessment module.	<p>Configure the Web Portal to connect to the Response Assessment module.</p> <p>Note: You must configure the Web Portal to connect to the Response Assessment Module when you install the Web Portal.</p> <p>See “About configuring the Web Portal to contact RAM” on page 171.</p>
	All jobs fail to run.	Verify that the Production database host works properly.
The Web Portal does not correctly display Response Assessment module pages	Internet Explorer Enhanced Security Components are installed and cookies are blocked from the Web Portal Internet Information Services (IIS) server.	Allow the Web Portal IIS server to set cookies.
Configuration changes do not appear.	If two users simultaneously make changes to the same settings, only the changes by the first user take effect.	The second user should navigate to a different view, then return to the settings page and repeat any required settings changes.
Correct time does not appear on reports.	The time setting or locale setting was changed on the Application Server host, but the changed time or locale does not appear on reports.	Restart the Application Server service then restart the Control Compliance Suite Console and run Scheduled Reporting Database Synchronization job. Then run the report again. The updated time appears correctly.

Table E-3 Console and Web Portal troubleshooting (continued)

Problem	Cause	Resolution
Reports may cause a system slowdown or may fail.	The complexity of the report exceeds the scalability limitations.	Reduce the complexity of the report.
The error HTTP Error 401.1 - Unauthorized: Access is denied appears when you access the Web Portal.	The Service Principal Names (SPNs) used by the Web Portal are misconfigured.	Properly configure the Service Principal Names (SPNs). See http://support.microsoft.com/kb/871179
Blank reports appear	When you run a report, the report contents may not appear. The report appears to be blank. This error occurs because the Scheduled Reporting Database Synchronization job must run before you can run a report.	You should run the Scheduled Reporting Database Synchronization job before you schedule the report. The synchronization job populates the database with the data in the production database. The synchronization job is an existing job and is in the Monitor > Jobs view.

Symantec ESM troubleshooting

[Table E-4](#) lists possible problems with Symantec ESM and their associated causes and resolutions.

Table E-4 Symantec ESM troubleshooting

Problem	Cause	Resolution
Cannot classify ESM 6.0 agents as different UNIX computers.	ESM 6.0 uses the OS details field in a different way than ESM 9.0 does.	<p>Update the ESM agents with SU 34 or later, then execute the Agent Information module on each ESM 6.0 agent.</p> <p>In Control Compliance Suite 9.0, import all ESM 6.0 Assets. Then create an Update reconciliation rule. Include the "If an asset being imported exists in the asset system" condition. You must also include the "Update the specifying fields of an existing asset with the fields of an asset being imported" action. Use the Only Selected fields option when you add the update type and select OS details in the Available Fields list.</p> <p>Update the <code>ESM.Agent.RegisteredName,</code> <code>ESM.Agent.ESMManager,</code> <code>ESM.Agent.OSVersion,</code> <code>ESM.Agent.Platform,</code> and <code>ESM.Agent.OSDetails</code> fields in the file <code><Install directory>\Symantec\CCS\Reporting and analytics\Applications\Data Collectors\ESM\ESMAgentAsset.csv</code>.</p> <p>Configure the CSV data collector and import the <code>ESMAgentAsset.csv</code> file.</p>

Installing Active Directory Application Mode manually

If the Control Compliance Suite installer is unable to create an Active Directory Application Mode (ADAM) instance because the Program Files folder is compressed, you must manually install ADAM.

To install ADAM manually

- 1 In the Windows Explorer double click the file
%Windows%\adam\adaminstall.exe to start the **Active Directory Application Mode Setup Wizard**.
- 2 In the **Welcome to the Active Directory Application Mode Setup Wizard** panel, click **Next**.
- 3 In the **Select Options** panel, click **A unique instance**, then click **Next**.
- 4 In the **Instance Name** panel, enter **SymantecCCS**, then click **Next**.
- 5 In the **Ports** panel, enter the LDAP port and SSL port the ADAM instance should use. The ports should range from 1024 to 65535.
Click **Next**.
- 6 In the **Application Directory Partition** panel, click **Yes, create an application directory partition**. In the **Partition name** field, enter **O=Symantec**, then click **Next**.
- 7 In the **File Locations** panel, click **Next**.
- 8 In the **Service Account Selection** panel, click **Network service account**, then click **Next**.
- 9 In the **ADAM Administrators** panel, click **Currently logged on user**, then click **Next**.
- 10 In the **Importing LDIF Files** panel, click **Do not import LDIF files for this instance of ADAM**, then click **Next**.
- 11 In the **Ready to Install** panel, click **Next**.
- 12 In the **Completing the Active Directory Application Mode Setup Wizard** panel, click **Finish**.

Glossary

Access Complexity	The attribute that measures the complexity of the attack that is required to exploit the vulnerability. The values are High, Medium, and Low.
Access Vector	The metric that reflects how the vulnerability is exploited. The values are Local, Adjacent Network, and Network.
Add Rule	A type of reconciliation rule that is applied on the current assets to add the current asset to a specified location.
approval period	The subset of the entitlements review period.
asset group	A collection of assets of one or more types for evaluation and reporting. A user-defined group can be static or dynamic.
asset reconciliation	The resolution of the existing assets with the newly imported assets in the asset store.
asset store	The location in the Directory Support Service where all the assets that are discovered and reconciled are stored.
asset system	The overall CCS system that includes all the assets and the features to manage the assets. The assets include groupings, filters, tags, folders, credentials, and asset authorization.
asset type	A form of categories that are specific to the supported platforms to gather more specific data for the purpose of monitoring the network.
asset	A managed object in the system that has value, has an owner, has controlled access, and can have authority. The authority occurs when the asset is a person or a query engine.
attestation	The reply, the answer, or the additional information that is returned to a questionnaire author.
attester	The creator and owner of the response.
audience	The users to whom a policy applies.
Authentication	The attribute that measures the complexity of the attestation that is required to exploit the vulnerability. The values are Multiple, Single, and None.
automatic remediation	A process that involves identifying the assets that are not in compliance and selecting a remediation notification method as part of the evaluation job.

Availability Impact	The attribute that measures the effect to availability of a successfully exploited vulnerability. The values are None, Partial, and Complete.
certificate	A file that the cryptographic systems uses as proof of identity. The file contains a user's name and a public key.
check expression	An expression that is used to compare a property of an asset to a specified data value.
check formula	A formula that is created by using check expressions. Operators connect multiple check expressions to create a single check expression.
check	A statement that tests a condition for an asset, such as a test if passwords have a certain length.
clarification	A user request for additional details about a policy before the user accepts a policy or requests an exception.
compliance score	The percentage value of 0 to 100 that represents the level of adherence to a standard. The score is derived from the technical checks.
Confidentiality Impact	The attribute that measures the effect on confidentiality of a successfully exploited vulnerability. The values are None, Partial, and Complete.
content pack	The prepackaged questionnaire that is based on common standards.
Control Compliance Suite Application Server	The server that is responsible for all job executions, workflow, and schedules.
Control Compliance Suite Console	A GUI component of CCS.
Control Compliance Suite Directory Server	The server that stores the asset data, user rights and preferences, and information about jobs.
Control Compliance Suite Directory	Active Directory Application Mode, a Lightweight Directory Access Protocol (LDAP) directory service. Lets the applications store information in a directory, rather than in a flat file or in a database. ADAM is separate from any Active Directory domains that are deployed on the network. In CCS, ADAM/ADLDS is the Directory Server.
control point	The data location in the system where the access permissions are granted and approved.
control statement	A single-sentence description of an activity, concept, or requirement called out by a regulation or a best-practice framework. These descriptions are a means of mapping related tasks and requirements between various regulations and best practices.
custom threshold	The threshold type that you use to set threshold conditions specific to a type of evaluation node.

dashboard	The high-level view that provides a summary roll-up of your organization's compliance.
data collector	The CCS component that retrieves information about assets from the network.
data item filter	A file that the cryptographic systems use as proof of identity. The file contains a user's name and a public key.
data location	The location of the CSV file.
Data Processing Service Collector	A role of the Data Processing Service. The DPS collector transmits data collection jobs to the data collector and retrieves results when the job is complete.
Data Processing Service Evaluator	A role of the Data Processing Service. The DPS evaluator compares data that is collected from the network to specified conditions, then stores the evaluation result for reporting.
Data Processing Service Load Balancer	A role of the Data Processing Service. The DPS load balancer distributes data collection jobs to the DPS collectors and to the DPS evaluators on the network.
Data Processing Service Reporter	A role of the Data Processing Service. The DPS reporter processes the evaluated data from the DPS data evaluator into the reports and the dashboards that are suitable for users.
Data Processing Service	A single service that has multiple roles in CCS. The roles include the DPS Collector, the DPS Evaluator, the DPS Load Balancer, and the DPS Reporter.
Directory Support Service	The service that works with the CCS Directory to check user rights on the directory items.
entitlement	The permission to access the control point.
ESM (Enterprise Security Manager)	An agent-based data collector for CCS.
evaluation	The process that is used to test the compliance of an asset with a standard, a section, or a check in the organization.
evidence database	The database that stores the proof of compliance with the policies and the checks.
evidence definition	A description of the information that is collected from the network that serves as proof of compliance with a particular policy.
evidence	The information that is collected from the network that proves that an organization is compliant with the policies that the organization has defined.
exception request	A user request for permission to defer compliance with a control statement that is included in a policy. The exception request can include the rationale for the request.
exception	The temporary permission that allows a user with a valid business reason to violate an organizational policy or a technical standard.

field expression	An expression that uses an operator to compare a field with a particular value that a user specifies.
framework	A collection of the policies that define best practices. An organization voluntarily uses the policy best practices.
gap analysis	The analysis that lets you review how the policies that are defined for an organization match up to a regulation or a framework.
global threshold	The threshold type that you use to set conditions and then apply those conditions to all the evaluation nodes of the same type.
gold standard	The standard that is built from the values that are present in a reference asset. A gold standard is the standard configuration against which other systems are benchmarked.
Integrity Impact	The attribute that measures the effect to integrity of a successfully exploited vulnerability. The values are None, Partial, and Complete.
job run	A particular instance of a job.
key field	The field in an evidence definition that lets you filter evidence results.
live data collection	The ESM configuration option for the site that tells the ESM collector to execute an ESM policy run.
location	An attribute of an asset. CCS users can create locations to represent geographical locations. Assets are associated with the appropriate location as well as with the services that work with those assets.
manual remediation	A process that involves identifying the assets that are not in compliance and selecting a remediation notification method from existing evaluation results.
MOS (Managed Object System)	An abstract representation of the network resources that are managed. A managed object can be a physical entity or a network service.
MOS schema	The object model that is used to represent network data.
no threshold (Information only node)	The threshold type that you use to retrieve summary data of evaluation nodes for which no threshold conditions are set.
object	A type of entity that is contained within the Directory Support Service. These entities include policy, asset, or standard. Objects are always the final level of the tree.
overall compliance score	The percentage value of 0 to 100 that represents the level of adherence to regulations. The compliance score is derived from the technical checks and the procedural controls.
policy mapping	The process of matching the policies that an organization defines to the frameworks or the regulations that the organization must comply with.

policy state	The status of a policy. The different states of a policy are planning, review, use, or retired.
policy template	A sample policy that is created by Symantec that can be used to create the custom policies that suit an organization's needs.
policy	A set of guidelines that are issued by a company to its employees to keep the company compliant with certain government regulations. The guidelines help to maintain the company's standards and reputation.
Post Rule	A type of reconciliation rule that is applied on the current assets after the asset becomes a part of the asset store.
Pre Rule	A type of reconciliation rule that is applied on the current assets before the asset becomes a part of the asset store.
predefined rules	Reconciliation rules that are built in the asset system. The asset system has Add, Pre, and Update types of rules.
production database	The database that stores collected data from the data collectors. The DPS evaluator uses the stored data.
question type	The question categorization that is based on the method that is used to provide a solution.
questionnaire author	The creator and owner of the questionnaire.
questionnaire	The set of questions that ask for responses from the attester that are created by the questionnaire author. The questionnaire hierarchy contains the questionnaire, the groups, the questions, and the answers.
reconciliation rule	A rule that defines a condition and a course of action that is to be taken when an asset is imported into the system. A set of actions is executed when the imported asset satisfies the specified set of conditions.
reference asset	The asset values that are used to create a gold standard. See also gold standard
reference standard	The standard whose values are modified according to the values existing in the reference asset.
regulation	A collection of the policies that define an organization's compliance with a governmental rule or regulation. Compliance is mandatory, which an outside body imposes.
remediation	A process that involves identifying the assets that are not in compliance and sending notifications to the appropriate personnel to resolve the issues.
Report Template	A report definition that is used by CCS for generating a report. The user can make a copy of a predefined template to create a new customized template.
reporting database	The database that stores the evaluation data. The DPS reporter uses the stored evaluation data.

retention age	The time period for retaining the evidence data in the evidence database.
review cycle	The time frame during which the data owner must complete the entitlement approval process.
risk impact	A check's risk level that is calculated by computing the total Confidentiality, Integrity, Availability, and Vulnerability settings.
risk rating	An asset's risk level that is calculated by computing the total Confidentiality, Integrity, Availability, and Vulnerability settings.
risk score	The percentage value of 0 to 100 for an asset that is calculated by computing the total Confidentiality, Integrity, and Availability settings. Risk scores are used to compute the severity of a failure of a particular check for a given asset.
RMS	A data collector that retrieves data from a bv-Control installation.
role	A designation that is based on a collection of predefined tasks that defines what a user is able to do in CCS.
section	A collection of subsections and checks. Sections are used to organize the checks and the subsections into logical groups.
site	A set of assets assigned to one or more Data Processing Services (DPS). Assigning sites to a DPS facilitates load balancing, data collection, data evaluation, and reporting from the assets that are assigned to a site.
standard	A collection of sections that contain checks and subsections. Assets are evaluated against a standard to provide a compliance score.
tag	An attribute that can be attached to an item such as an asset, policy, group, standard, evaluation result, query, or query result. The user can then search by such items as "My SOX assets." The tag is sometimes referred to as a label.
task	A specific action such as Create a policy or Run an evaluation that the user performs. A collection of predefined tasks defines a role.
threshold check field	Threshold parameters for which the threshold values are set for a node.
tiered dashboard	The hierarchical representation of roll-up data.
trend analysis	An analysis that shows an organization's frameworks, regulations, and policies information and helps organizations to determine the extent of their policy compliance.
trend	A graphical representation of data that is collected for a dashboard. A trend displays the security assessment posture of the organization over a given period of time.
TSP (Technical Standard Pack)	A collection of checks that can be run by a user to verify compliance with industry security and configuration best practices for various operating systems and applications.

Update Rule

A type of reconciliation rule that is applied on the imported assets to update their properties with the values of the current assets that are newly imported.

Index

A

- access control 78
- add rule 257
 - conditions and actions 233
- alternative approvers 396
- Altiris
 - asset types 336
 - CCS Asset Export Task settings 340
 - creating import job 339, 341
 - CSV file 343
 - importing assets 335
 - installing 337
 - tasks 338
- Analysis view 693
- annotations
 - adding 108
 - deleting 109
- application server 30
 - authentication type 153
 - credentials 159
- approve entitlements 411
- architecture 26
- asset groups 247
 - copying and pasting 307
 - creating 299
 - dynamic 247
 - editing 306
 - predefined 248
 - static 248
- asset import 240
 - Altiris 335
 - default and supported scope 289
 - default data collector 268
 - first time 262
 - scenarios 267
 - scope 287
 - specific and common fields for custom asset 281
 - specific and common fields from CSV data collector 278
 - specific and common fields from default collector 275
 - asset import (*continued*)
 - specific fields from default data collector 272
 - using a CSV file 291
 - using csv data collector 269
- asset system tasks 305
 - asset group tasks 306
 - asset tasks 317
 - global tasks 307
- asset type fields
 - ESM 204
- asset types 203
 - common fields 285
 - create 348
 - custom 228
 - extend 351
 - predefined 204
 - probable 227
- assets 201
 - active 253
 - Altiris 336
 - applying tags 326
 - asset groups 247
 - basic concepts 200
 - batch size 155
 - count settings 146
 - custom asset types 228
 - editing 317
 - field filters 242
 - folder hierarchy 202
 - getting started 193
 - importing 240
 - importing for the first time 265
 - importing specific and common fields for custom asset 281
 - importing specific and common fields from CSV data collector 278
 - importing specific and common fields from default data collector 275
 - importing specific fields from default data collector 272
 - manual review 246
 - moving 318

assets *(continued)*

- predefined asset types 204
- predefined platforms 203
- primary and secondary 228
- probable asset types 227
- reconciliation 245
- reconciliation rules 229
- removing tags 326
- reviewing manually 297
- site scope 202
- tagging 246
- types 203
- updating 284

audience

- about 573
- accepting a policy 589
- declining a policy 589
- responding to policies 588
- selecting 578, 584

audits

- about 147
- event triggers 147
- setting 132
- viewing 148

B

baseline jobs

- deleting 563

baselines

- create 560

best practices 574

C

CCS

- documents 42

CCS Asset Export Task

- creating 341
- installing 337
- scheduling 342
- settings 340

CCS custom standard migration utility 485

CCS ESM policy run options

- about 124

certificate management console

- about 71

certificates

- creating 73
- managing 68

certificates *(continued)*

- removing 77
- renewing 75
- revoking 76
- tasks 70

Check

- risk attributes 472

check 453

- concepts 467
- copying and pasting 515
- creating 517
- deleting 516
- expression 469
- formula 469
- mapping to control statements 689
- modifying 520
- moving 515
- renaming 516
- version 465

clarifications

- about 592
- management view 592
- managing 592
- managing requests 593
- reviewing 592

client 29, 38

closed-loop verification

- about 552

collector 34

columns

- heading 58

common fields 285

common platform

- default data collector 271
- fields 271
- predefined asset types 271

compliance score 463

components

- additional information 107
- application server 30
- client 29
- collector 34, 36
- console 29
- Control Compliance Suite Directory 30–31
- data processing service 34
- deleting association 109
- evaluator 34, 37
- evidence database 38
- list 27

- components *(continued)*
 - load balancer 34
 - management service 39
 - modify settings 107
 - production database 37
 - reporter 34–35
 - reporting database 37
 - SQL Server 37–38
 - web portal 38
- configuration layout
 - saving 108
- configuring
 - alternative approver 412
 - automatic entitlement imports 407
 - control points 400
 - CSV data collector 129
 - Data Processing Service 96, 98, 100, 102
 - entitlements notifications 418
 - ESM components 121
 - ESM custom messages manager 122
 - ESM data collector 120
 - ESM general settings 125
 - ESM manager settings 121
 - ESM poll settings 127
 - ESM thread settings 126
 - import settings 406
 - Oracle data collector 118
 - SQL data collector 119
 - UNIX data collector 119
 - Windows data collector 117
- console 29
 - features 45
 - views 51
- Content Studio 683
- Control Compliance Suite
 - architecture diagram 26
 - defined 25–26
- Control Compliance Suite Directory 30–31
- control points 395
 - approval period 397
 - configuring 400
 - details pane 423
 - marking 307, 398
 - status 387
 - unmarking 404
- control statements 574
 - Content Studio 683
 - creating custom 686
 - custom 681, 683
- control statements *(continued)*
 - mapping to checks 689
 - mapping to mandates 686
 - mapping to policies 586, 688
 - mapping to third-party evidence 692
- copy-paste
 - asset group 307
 - reconciliation rules 331
- create
 - asset folders 305
 - asset groups 299
 - asset types 348
 - baselines 560
 - dynamic asset group 300
 - reconciliation rules 253
 - static asset group 302
 - tag category 566
 - tags 566
- create reconciliation rules
 - with manual review 254
 - without manual review 253
- credentials
 - scheduled jobs 55
- CSV
 - exporting resources from Altiris 343
- CSV file
 - importing assets 291
- CSV file format
 - collecting evidence data 699
 - data collection 295
 - list field format 297
 - predefined asset types 293
 - user account 152
- CSV headers
 - exporting 319
- custom asset
 - importing specific and common fields
 - information 281
- custom content 681–682
 - about 681
 - Content Studio 683
 - control statements 683, 686
 - framework 684–685
 - frameworks 682
 - mandate 684–685
 - mapping checks to control statements 689
 - mapping control statements to mandates 686
 - mapping control statements to third-party
 - evidence 692

- custom content (*continued*)
 - mapping policies to control statements 688
 - mapping questions to control statements 690
 - regulation 684–685
 - regulations 682
- custom evidence provider
 - about 698
 - adding 708
 - associating data location 707
 - configuration sequence 698
 - deleting 709
 - modifying 709
- custom roles
 - about 86
 - creating 92
 - deleting 94
 - editing 93
 - entity schema 357
 - evidence collection 707
- custom schema 348

D

- dashboard
 - about tiered 646
 - descriptions 627
 - job settings 142
 - threshold settings 142
- dashboard reports
 - viewing 678
 - viewing details report 679
 - viewing trends report 679
- dashboard section
 - copying and pasting 674
- dashboards
 - types 622
- data collection
 - restrictions 88
- data collection job 454
- data collector
 - SQL 119
- data collectors
 - about configuration 116
 - default 240
- data filter 470
- data location
 - associating custom evidence provider 707
 - configuring 131
- data owners 396

- Data Processing Service
 - advanced settings 100
 - assigning 114
 - configuring 100
 - registering 96, 98
 - removing 99, 115
 - roles 97, 102
 - settings 100
 - synchronizing
 - reporting database 133
 - synchronizing settings 103
- data processing service 34–37
 - collector 36
 - evaluator 37
 - load balancer 34
 - reporter 35
- data synchronization 623
- databases
 - jobs 627
 - reporting
 - synchronizing 133
- delete
 - assets or asset groups 319
 - reconciliation rules 331
 - tag 568
 - tag category 567
- details pane
 - about 50
 - assets 319
 - control points 423
 - reconciliation rules 331
- directory 31
 - objects 32
- DPS 34–37
 - collector 34, 36
 - evaluator 34, 37
 - load balancer 34
 - reporter 34–35
 - settings for ESM 128
- dynamic asset groups
 - creating 300

E

- edit
 - asset group 306
 - assets 317
 - category 567
 - reconciliation rules 330

- email address
 - updating 152
- email notification
 - settings 132
- entitlements
 - settings 139
- entity
 - defination in Control Compliance Suite 356
- entity schema
 - about 347
 - creating 360
 - extending 364
- ESM
 - adding, modifying, removing manager 122
 - policy mapping 467
 - policy name change 467
 - target types 462
- ESM Check Builder
 - adding an error expression 526
 - adding the data filters 525
 - editing check formula 527
 - message expression 524
 - specifying content 530
- ESM checks
 - Advanced Check Builder 528
 - creating 522
 - Quick Check Builder 523
- ESM custom policy migration utility 485
- ESM policy
 - renaming at the check level 521
 - renaming at the section level 508
 - renaming at the standard level 503
- evaluation job 454
 - creating 495
- evaluation node
 - adding 672
 - bv-Control Query Results 670
 - copying and pasting 674
 - deleting 673
 - editing 673
 - Standards Evaluation Results 670
- evaluator 34, 37
- evidence
 - mapping third- party to control statements 692
- Evidence Management system
 - collecting evidence data 697
- Evidence Management view 698
- evidence provider
 - adding 708

- evidence provider *(continued)*
 - modifying 709
- exception 428
 - approving 441
 - concepts 427
 - filters 432
 - modifying 445
 - requesting 436
 - states 431
 - templates 430
 - validity 429
- exception state 431
 - Deny 444
 - Expire 445
 - In Review 444
 - Request Clarification 444
- exceptions
 - settings 140
- export
 - CSV headers 319
- expression
 - check 469
 - field 468

F

- field expression 468
- fields of an entity
 - defination in Control Compliance Suite 357
- Filter by pane
 - about 49
 - assets 327
 - customizing 56
 - Evaluation Result view 612
 - reconciliation rules 332
 - using 56
- filters
 - asset system 327
 - entitlement 422
 - reconciliation rules 332
 - reports 627
- folders
 - creating 60
 - deleting 61
 - moving 61
 - refreshing 62
 - renaming 62
 - special characters 60
- framework
 - viewing 694

- frameworks 574
 - Content Studio 683
 - creating custom 684
 - custom 681–682
 - modifying custom 685

G

- gap analysis
 - performing 695
- general
 - settings 131
- gold standard 464
 - concepts 536
 - creation 537
 - job 538
- Grid view
 - about 106

H

- health and status
 - refreshing 110
 - viewing 109
- Home
 - setting 144
- host file 165

I

- imports 405
 - automatic 407
 - configuring 406
 - manual 408
- infrastructure jobs
 - monitoring 110
- initial tasks
 - configuring 64

J

- job run
 - about 595
 - canceling 606
 - deleting 607
- jobs
 - about 595
 - about filters 598
 - count settings 146
 - creating through jobs view 605
 - deleting 602
 - editing 601

- jobs *(continued)*
 - refreshing the view 604
 - running 603
 - scheduling 602
 - searching 604
 - types 596
- jobs view
 - about 599

L

- licenses
 - about 148
 - adding 150
 - expiration date 149
 - viewing 150
- LiveUpdate
 - about 162
 - enable and schedule 165
 - host file 165
 - run 166
 - staging
 - location 166
 - using 163
 - view 164
- load balancer 34
- logs
 - about 172
 - levels 174
 - locations 172
 - messages 174

M

- management service 39
- management services
 - about 68
- mandate
 - creating custom 684
 - modifying custom 685
- mandates 682
 - mapping custom to control statements 686
- manual review 246
 - reconciling records 298
 - viewing records 298
- Map view
 - about 103
 - icons 105
 - navigating 105

menu bar

about 46

monitor view

about 52

N

notifications

configuring 418

entitlements 414

events 414

tokens 419

O

objects

directory 32

editing 58

organizing 32

searching 59

operators 478

check formula 481

Field expression 479

P

permissions

about 79

assigning 91, 95

removing 96

platform

definition in Control Compliance Suite 356

policies

about 571

about clarifications 592

accepting 589

approval 583

approving 575, 587

audience 573

changing 575

clarification 575

clarifications 575

clarifications management 592

control statements 574

copying 575, 582

create 575

creating 575, 578–579

declining 589

deleting 575, 578, 583

edit 578

editing 575

policies *(continued)*

exception 575

exceptions 575

frameworks 574

importing 575, 578, 581

life-cycle 572

managing clarification requests 593

managing clarifications 592

mapping to control statements 586, 688

moving 575, 578, 582

pasting 582

policy management view 575

printing from the web portal 591

publish 575

publishing 575, 586–587

regulations 574

renaming 575

responding on web portal 588

review 575

reviewing 583–585

search 578

searching 575

selecting audience 578, 584

status 572, 578, 586–588

submitting for approval 583

submitting for review 575, 583

tags 575

unpublish 575

unpublishing 575, 588

versioning 575

viewing 575

viewing reviewer comments 586

policy

custom 485

settings 142

policy mapping

ESM 467

post rule 259

conditions and actions 237

pre rule 256

conditions and actions 231

preconditions 470

predefined platforms 203

predefined standards 449

ESM 449

Oracle 451

SQL 451

UNIX 452

Windows 452

predefined target type

- Oracle 461
- SQL 455
- UNIX 457
- Windows 456

production database 37

purge

- about 135
- evidence 134
- job schedule 137
- settings 136

Q

questions

- mapping to control statements 690

RRAM. *See* Response Assessment Module

- adding link 169
- adding property 169
- evidence 167
- publishing questionnaire 170

RAM database

- settings 138

reconciliation rules 229

- assets being imported 239
- copying and pasting 331
- creating 253
- deleting 331
- editing 330
- moving 331
- predefined 238
- types 229
- with manual review 254
- without manual review 253

reconciliation rules tasks 330

reconciliation rules

- existing assets 239

reference information

- adding 535
- deleting 536
- editing 535

regulation

- viewing 694

regulations 574

- Content Studio 683
- creating custom 684
- custom 681–682

regulations *(continued)*

- modifying custom 685

relationships

- defined between entities 358

remediation

- about 549
- automatic 555
- closed-loop verification 552
- manual 553
- settings 143

report templates

- adding 643
- copying 640
- creating 624
- customizing 641
- deleting 643
- exporting 644
- importing 643, 645
- moving 646
- predefined 623
- prerequisites 624
- updating 645

reporter 34–35

reporting database 37–38

- settings 156
- synchronizing 133

reports

- CCS 615
- copying custom 640
- creating 636
- customizing 141, 642
- data synchronization 623
- descriptions 627
- editing 646
- exporting 639
- filters 627
- job 627
- printing 639
- refreshing 638
- removing 639
- scheduling 636
- viewing 638

request approval 410

request changes 411

Response Assessment Module. *See* description of

risk calculations 545

- Adjusted base score 546
- average risk score 547
- base score 545

risk calculations *(continued)*

 risk score 546

risk score 463

roles

 about 78

 adding user 89

 copying 93

 Data Processing Service 102

 permissions 95

 predefined 80

 removing user 90

 viewing tasks 91

 viewing users 90

roles and permissions

 configuring 78

S

S4U

 configuring 160

 constrained delegation 160

scheduled jobs

 setting 154

section 453

 copying and pasting 506

 creating 505

 deleting 507

 moving 507

 renaming 507

 version 465

security

 settings 154

service accounts

 configuring 159

 unconstrained delegation 159

setting

 review cycle 396

settings

 Data Processing Service 99–100, 102

 synchronizing Data Processing Service 103

sites

 assigning Data Processing Service 114

 configuring 111

 creating 113

 deleting 114

 modifying name 115

 planning 113

 removing Data Processing Service 115

 use of 112–113

special characters

 credentials 161

SQL Server 37–38

 settings 155

SQL Server Integration Service

 settings 158

SSIS 37

standard 448

 copying and pasting 492

 creating 491

 custom 485

 deleting 495

 exporting 494

 filters 466

 Importing 493

 moving 493

 predefined 449

 renaming 494

 version 465

standards

 settings 145

static asset groups

 creating 302

summary dashboard

 about 647

 creating dashboard job 649

 editing dashboard update job 651

 exporting 648

 removing 650

 scheduling 649

 viewing 648

suppressed ESM messages

 collecting 123

System Topology view

 about 103

T

table pane

 about 49

 managing 57

tag category

 creating 566

 deleting 567

 editing 567

tags 565

 creating 566

 deleting 568

 moving 568

 renaming 568

- target type 455
- taskbar
 - about 50
- tasks
 - about 79
 - accessing 51
- thresholds
 - about setting thresholds 666
- tiered dashboard
 - about check fields 667
 - about predefined roles 663
 - about relational operators 668
 - about status calculation 668
 - about threshold types 667
 - about thresholds 666
 - about trends configuration 675
 - about types of evaluation nodes 670
 - assigning permissions 671
 - configuring email alerts 674
 - configuring nodes 670
 - copying 659
 - copying and pasting node 674
 - copying section 674
 - creating 657
 - editing 658
 - editing dashboard update job 662
 - editing job notification 660
 - editing job schedule 660
 - evaluation nodes 676
 - exporting 661
 - getting started 652
 - importing 660
 - managing 651
 - managing permission 665
 - pasting section 674
 - renaming 659
 - roles and permissions 662
 - viewing 653
 - viewing details tab 656
 - viewing evaluation results tab 657
 - viewing permissions 664
 - viewing reports 678
 - viewing status tab 653
- tree pane
 - about 48
 - using 59
- trends
 - configuring 675
 - viewing reports 679

- troubleshooting 769

U

- update
 - assets 284
- update rule 258
 - conditions and actions 234
- user account
 - adding 151
 - deleting 153
 - importing 152
 - updating 153
- User Management
 - view 151
- user-defined templates
 - prerequisites 624
- users
 - about 151
 - adding role 89
 - assigning permission 91
 - removing role 90
 - viewing roles 90

V

- view
 - comparison results 561
- views 51
 - certificates 69
 - Dashboard Templates 621
 - Grid 106
 - Home 51
 - license 149
 - LiveUpdate 164
 - Map 103
 - My Dashboards 619
 - My Reports 618
 - refreshing 59
 - Report Templates 616
 - Reporting 54, 616
 - Settings 53
 - System Topology 103
 - User Management 151

W

- web portal 38
 - accepting a policy 588–589
 - adding a new language 711
 - declining a policy 588–589

web portal (*continued*)
 printing a policy 591
 strings 715
 using 588