Symantec™ Control Compliance Suite 11.0 User Guide

Control Compliance Suite 11.0 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: 11.0

Legal Notice

Symantec and the Symantec Logo, ActiveAdmin, BindView, bv-Control, 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.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

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
350 Ellis Street
Mountain View, CA 94043

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 support 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/or web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our web site at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

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

www.symantec.com/business/support/

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:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as 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 support 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

Support agreement resources

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

Asia-Pacific and Japan	customercare_apac@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:

Managed Services — Managed 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.

Education Services — Education 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/business/services/

Select your country or language from the site index.

Contents

Section 1

About Control Compliance Suite

Chapter 1

Introducing Control Compliance Suite

This chapter includes the following topics:

About the Control Compliance Suite

Symantec Control Compliance Suite (CCS) automates key IT risk and compliance management tasks. 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. CCS allows customers to link the written policy to specific technical and procedural standards. Customers can assess these policies using a highly scalable agent-less or agent-based tool.

CCS scores assessment results against specified risk criteria. CCS supports automated assessment of the system security configuration, permissions, patches, and vulnerabilities. CCS also supports the assessment of procedural controls and entitlement review through a manual attestation process. CCS includes system reporting capabilities.

CCS is an integrated solution comprising of different modules. You can use a combination of these modules to meet your business objectives.

Refer to the following link, to understand how you can use CCS to achieve your business goal.

The CCS Suite is the host infrastructure in CCS. It is mandatory to deploy the CCS Suite to use any of the CCS capabilities.

You can use CCS to collect raw-data based content using agent-less or agent-based methods, message based content using agent-based method or security assessment data from external data systems.

CCS provides out of the box connectors for integration with the following products:

- Symantec CCS Vulnerability Manager for vulnerability assessment.
- Symantec Data Loss Prevention for data loss assessment.
- Symantec Response Assessment Module for response assessment.

For details about external data systems,

See "How Control Compliance Suite works" on page 44.

See " What Control Compliance Suite can do for you " on page 45.

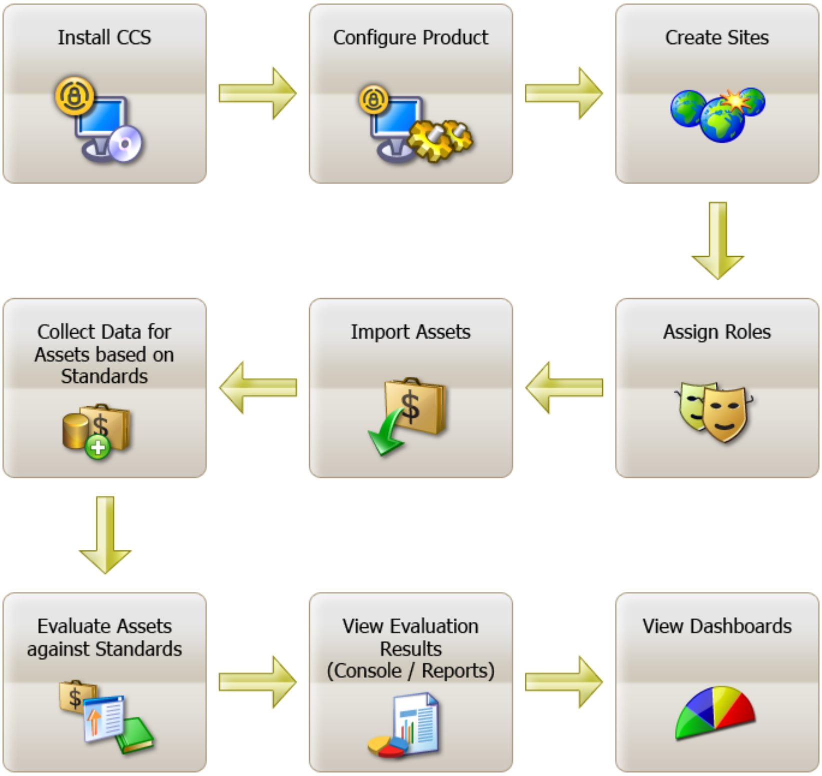
How Control Compliance Suite works

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


Install CCS
Configure Product
Create Sites
Assign Roles
Import Assets
Collect Data for Assets based on Standards
Evaluate Assets against Standards
View Evaluation Results (Console / Reports)
View Dashboards

What Control Compliance Suite can do for you

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.
- 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.

Chapter 2

Components of Control Compliance Suite

This chapter includes the following topics:

CCS Home page

You can achieve the following most common business objectives using the workflows that are displayed on the Control Compliance Suite (CCS) home page:

- Security Compliance
- Policy Management

Using the optimized home page you can do the following:

- Get a quick glance of the flow of tasks.
- Navigate easily through the application using the workflow.

The quick links that are provided in each task helps you navigate to the specific view or module in CCS.

- Access the quick links to CCS documentation and CCS Support.

See “Assessing the security compliance” on page 399.

See “Assessing the policy compliance” on page 400.

CCS Console

The 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 CCS Application Server can be in the same domain. If the console and the CCS 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*.

See “CCS Web Console” on page 48.

CCS Web Console

The CCS Web Console lets users access a subset of the CCS functionality using Internet Explorer 7.0 or Internet Explorer 8.0.

In the Web console, users can do the following:

- Accept or reject policies.
- Request policy exceptions.
- Request policy clarifications.
- Review policies.
- Approve policies.
- Respond to CCS questions.
- Review data in dashboards.

- Create dashboards.
- Connect to the CCS Web client to respond to questionnaires.
- Set Web console user preferences.
- Download CCS thick console from the **Downloads** page.

Note: You must enable SSL if you want to launch the CCS Web console in a FIPS-enabled environment.

CCS Application Server

The CCS Application Server includes the Directory Service, the Encryption Management Service, the Application Server Service, and the Certificate Management Console.

The CCS Application Server is the hub of CCS. The Directory Service in the CCS Application Server stores information about business objects, preferences, and other information. In addition, the Directory Service hosts the certificate authority for the CCS system, and issues and validates certificates. Certificates are used to ensure secure communications between the CCS components.

CCS jobs flow from the CCS Console to the CCS Application Server and then to one of the CCS Manager 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 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 CCS Application Server runs as a service on the server that you specify. In the **Services** control panel, the CCS Application Server services are listed as Symantec Application Server Service, Symantec Directory Support Service and Symantec Encryption Management 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.

The same computer hosts both the Application Server and the Web Console server.

CCS Manager

CCS Manager is a component of Control Compliance Suite that performs different roles. CCS Manager runs as a Windows service where a single instance of the service can provide multiple roles simultaneously.

The different roles that CCS Manager performs are as follows:

- CCS Manager in the role of a load balancer
  See "About the CCS Manager Load Balancer" on page 51.
- CCS Manager in the role of a collector
  See "About the CCS Manager Collector" on page 51.
- CCS Manager in the role of an evaluator
  See "About the CCS Manager Evaluator" on page 53.
- CCS Manager in the role of a reporter
  See "About the CCS Manager Reporter" on page 53.
- CCS Manager in the role of an external data collector
  See "About the CCS Manager External Data Connector" on page 54.

CCS Manager controls agent based functionality and performs various agent related activities such as Agent Registration, Live Update, Remote upgrade. CCS Manger enables raw data based collection as well as message based data collection depending on the agent registration.

The CCS Manager performs the following functions:

- Agent registration and asset import.
  The CCS Manager collects agent and asset information from the agents. During an agent registration job, the agent is registered with the CCS Manager and the assets are imported into the asset system.
- Granular Live Update of the registered agents.
  The App Server creates granular Live Update packages for the CCS agents and sends them to the CCS Manager. During a data collection job, only the files required for the current job are pushed from the LU packages to the agents.
- Performs remote upgrade of agents
  The remote upgrade packages are sent to the CCS Manager, which in turn send them to the agents and perform the agent upgrade.

CCS Manager controls agent based functionality and performs various agent related activities such as Agent Registration, Live Update, Remote upgrade. CCS Manger enables raw data based collection as well as message based data collection depending on the agent registration.

About the CCS Manager Load Balancer

When the CCS Manager acts as a load balancer, the CCS Manager routes data collection jobs from the Application Server to a CCS Manager Collector. In addition, a load balancer routes the evaluation jobs to the CCS Manager Evaluator and the reporting jobs to the CCS Manager 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 CCS Manager Collector" on page 51.

See "About the CCS Manager Evaluator" on page 53.

See "About the CCS Manager Reporter" on page 53.

See "About the CCS Manager External Data Connector" on page 54.

The CCS Manager Collector retrieves the data from the network. Potentially, your installation of CCS can have a large number of CCS Manager 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 CCS Manager Collectors, the load balancer distributes the query appropriately. When the CCS Manager Collectors complete the query, the load balancer combines the results and returns the results to the Application Server for storage.

An eligible CCS Manager 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 CCS Manager 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 CCS Manager 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 CCS Manager when you deploy CCS should be assigned to the Load Balancer role.

About the CCS Manager Collector

The CCS Manager Collector is the interface to the programs that do the actual work of collecting data from the network. Your CCS deployment can include multiple data collectors, each linked with a CCS Manager Collector. The CCS Manager Collector receives data collection jobs from the CCS Manager 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 CCS Manager Collector. The CCS Manager Collector then returns the collected data to the CCS Manager Load Balancer. If necessary, the CCS Manager Load Balancer combines the data with data from one or more other CCS Manager Collectors. Finally, the CCS Manager Load Balancer sends the data to the Application Server for storage in the production database for use by the CCS Manager Evaluator.

The CCS Manager 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 CCS Manager Collectors and associated data collectors. The CCS Manager Load Balancer assigns jobs to the eligible CCS Manager Collectors sequentially. The CCS Manager Load Balancer does not base job assignments on the current load of a CCS Manager Collector. If an eligible CCS Manager Collector is unavailable, the CCS Manager Load Balancer skips it and uses another eligible CCS Manager Collector. This round robin assignment gives limited fault tolerance.

CCS Manager can perform both agent-less and agent-based data collection. Agent-based data collection is performed with the use of CCS Agents installed on target computers.

An eligible CCS Manager Collector is any collector that has the ability to complete the data collection job.

CCS supports the following data collectors:

- The CCS Manager can be configured as the following data collectors:
- Windows data collector
- UNIX data collector
- SQL data collector
- Oracle data collector
- ESM data collector
- Exchange data collector
- NDS data collector
- NetWare data collector
- CSV data collector
- ODBC data collector
- Directory Server data collector

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 CCS Manager Collector collects is compressed before the data is returned to the other CCS components.

See "About the CCS Manager Load Balancer" on page 51.

See "About the CCS Manager Evaluator" on page 53.

See "About the CCS Manager Reporter" on page 53.

See "About the CCS Manager External Data Connector" on page 54.

About the CCS Manager Evaluator

Evaluation jobs are sent from the Application Server to one of the CCS Manager Load Balancers. The CCS Manager Load Balancer then sends the evaluation job to the CCS Manager 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 CCS Manager Load Balancer assigns evaluation jobs to the evaluators sequentially. If a CCS Manager 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 CCS Manager Load Balancer" on page 51.

See "About the CCS Manager Collector" on page 51.

See "About the CCS Manager Reporter" on page 53.

See "About the CCS Manager External Data Connector" on page 54.

About the CCS Manager Reporter

The CCS Manager Reporter generates reports and dashboards for display by the CCS Console. In addition, a single CCS Manager 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 CCS Manager 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 CCS Manager Reporter must have the Crystal Reports engine installed. The Crystal Reports installer is available on the CCS product disc.

See "About the CCS Manager Load Balancer" on page 51.

See "About the CCS Manager Collector" on page 51.

See "About the CCS Manager Evaluator" on page 53.

See "About the CCS Manager External Data Connector" on page 54.

About the CCS Manager External Data Connector

The CCS Manager External Data Connector is responsible for hosting the external data integration framework and serves as a means to collect data from any external data system. You must enable the External Data Connector role of the CCS Manager if you want to import external data into CCS.

When you register a CCS Manager External Data Connector, all the pre-integrated connectors such as ODBC, CSV, Web services, Symantec Data Loss Prevention, and Symantec CCS Vulnerability Manager get registered.

See "CCS Manager" on page 50.

See "About the CCS Manager Load Balancer" on page 51.

See "About the CCS Manager Collector" on page 51.

See "About the CCS Manager Evaluator" on page 53.

See "About the CCS Manager Reporter" on page 53.

CCS Agent

CCS Agent is a component that is installed on every computer in your enterprise network to perform agent-based data collection. The CCS agent can perform raw data-based as well as message-based data collection to assess security compliance.

The agent configuration parameters control the behavior of the agents installed on the computers. The configuration parameters for each agent are stored in the agent.conf file on the agent computer at the following location:

C:\Program Files\Symantec\Control Compliance Suite\

The CCS agent is registered to a CCS Manager using the agent registration utility. During agent registration, the agent information is stored on the CCS Manager. The CCS Manager passes the agent information to the Application Server through an Agent Registration Job (ARJ). The ARJ creates the agents and the corresponding assets in the asset system .

CCS agent management consists of the following tasks:

- Agent registration
  See "Agent registration" on page 145.
- LiveUpdate
  See "LiveUpdate" on page 145.
  See "Configuring LiveUpdate" on page 562.
- Remote Upgrade
  See "Remote Upgrade" on page 145.
  See "Performing a remote upgrade of ESM agents" on page 559.
- Agent configuration
  See "Agent configuration" on page 145.
  See "Configuring agents" on page 558.

Databases

CCS hosts the following types of databases:

- Production
  See "Production database" on page 55.
- Reporting
  See "Reporting database" on page 56.

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 CCS, the Response Assessment data is also stored in the production database.

The production database requires Microsoft SQL Server 2005 SP2 or Microsoft SQL Server 2008. CCS requires a single production database. The production database can share a host server with CCS, 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.

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. In addition, the database stores data specific to individual dashboards or reports. The CCS Manager Reporter monitors the synchronization of data between the production database and the reporting database.

The reporting database requires Microsoft SQL Server 2005 SP2 or Microsoft SQL Server 2008. CCS requires a single reporting database. The reporting database can share a host server with CCS, 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.

About the Control Compliance Suite Web Console server

The computer that hosts the CCS Web Console server host must have the Microsoft Internet Information Server (IIS). The CCS Web Console allows access to some CCS content without requiring the full CCS Console. The same computer hosts the Web Console server and the Application Server.

The CCS Web Console lets users do the following:

- Accept or reject policies.
- Request policy exceptions.
- Request policy clarifications.
- Review policies.
- Approve policies.
- Respond to Response Assessment module questions.
- Review data in dashboards.
- Connect to the Response Assessment module Web client to respond to questionnaires.
- Set Web console user preferences.
- Download Control Compliance Suite thick console from the Downloads page.

The computer that hosts the Application Server also always hosts the CCS Web Console server.

If the same computer hosts the Web console, the Application Server, and the Directory Server, CCS uses Windows NTLM authentication. If the Web console, 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 Console client to the Web Console server which is the same as 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.

See “CCS Application Server” on page 49.

Chapter 3

Concepts in Control Compliance Suite

This chapter includes the following topics:

- About jobs
- Concepts in routing rules
- Concepts in risk management
- About Dynamic Dashboards

About data collection models

You can perform data collection from your enterprise network in different ways based on the type of data collected. You can either collect raw data or message based data.You must configure your environment for the different data collection models based on the type of data collection method that you plan to adopt.

The data collection models can be of the following types:

- Raw data based
  In the raw data based data collection model, the CCS Manager or the CCS agent collects data from the network. The collected data is then evaluated against a standard.
  Raw data based data collection can be done using the agent based or the agentless method..
  See " Configuring data collectors for raw data based data collection" on page 327.
- Message based
  In the message based data collection model, the CCS agent installed on each computer in the enterprise network performs the actual task of data collection. The security content executables installed on the agents collect and evaluate the data and report the conformance of the assets with the security policies.The evaluated data is collected and presented in the form of messages.
  Message based data collection requires a CCS agent to be installed on every computer in the enterprise neotwork.

See "CCS Manager" on page 50.

See "CCS Agent" on page 54.

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 61.

- Site
  See "Site as scope in asset import" on page 64.
- Asset folder hierarchy
  See "Asset folder hierarchy" on page 64.
- Predefined platforms
  See "Predefined platforms" on page 65.
- Asset types
  See "Asset types" on page 65.
- Primary and secondary assets
  See "Primary and secondary assets" on page 104.
- Reconciliation rules
  See "Reconciliation rules and rule types" on page 106.
- Asset tagging
  See "Asset tagging" on page 131.
- Asset import
  See "Asset import" on page 122.
- Asset groups
  See "Asset groups" on page 131.
- Active assets
  See "Active assets" on page 141.

About assets

With reference to Control Compliance Suite, an asset is defined as an object in the organization that has certain properties.

Table 3-1 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.

Table 3-1 Features of assets *(continued)*

Feature	Description
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	■ Financial data ■ HR data ■ Patent records ■ Business plans ■ Disaster recovery plans
Physical assets	■ 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 64.

See "Asset folder hierarchy" on page 64.

About business assets

The asset system in CCS represents the following kinds of assets:

- Technical and tangible assets as computers and databases

- Business assets that are non-technical and more intangible as people and processes

Business assets fall into the following categories:

- Business Units as Investment, Corporate, Consumer, Commercial, or Treasury
- Departments as Credit Card, Trading, or Retail
- Business Processes as GRC, Shipment, or Security

The following features characterize business assets:

- Business assets are unique. The asset system prevents the duplication of a business asset within the system.
- Business assets can be tagged.
- A business asset can be available only in one asset folder at a time.

Business assets add value to the organization, and are vulnerable to security threats. Risk is the possibility of a business incurring loss from security threats. CCS uses business assets to model risk. CCS associates business assets and controls to risk objectives. Through associations with policies and questionnaires, business assets also make the evaluation of compliance possible.

See “About types of business assets” on page 63.

See “About the management of business assets” on page 141.

About types of business assets

A business asset type represents a group of business assets. A set of shared attributes defines the type. For example, the asset system provides a new asset type, Business Asset (BA) to represent all business entities. Types enhance the ease of managing business assets. For example, use the type of a business asset to filter business assets or to search for business assets.

CCS provides the following predefined business asset types:

- Business Units
- Business Process
- Business Application

To manage asset types, you require the following permissions:

- Permissions of CCS Administrator
- Privileges that are associated with the Manage Schema task

Use the CCS Administrator role to add user-defined attributes during the creation or edit of a business asset type.

System attributes are attributes available to all business assets. A set of predefined attributes defines every type of business asset. System attributes are also available to custom business assets.

CCS disallows the following actions on business assets:

- Remove attributes to edit the business asset type in the asset system.
- During the edit of a business asset type, mark the user-defined attributes that were added as mandatory attributes.
- Remove mandatory attributes.
- Deprecate a custom business asset type as deprecation affects all areas of CCS.

See "About business assets" on page 62.

See "About the management of business assets" on page 141.

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.

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

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
- Exchange
- NDS
- NetWare

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 583.

See "Predefined asset types" on page 66.

See "Probable asset types" on page 103.

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 66.

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 103.

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 104.

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 65.

In Control Compliance Suite, a platform is defined to be the category to which a group of entities belong.

See “About platforms” on page 583.

A group of fields that define the common functions of the network element form an entity.

See “About entities” on page 583.

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:

Table 3-2 Predefined asset types

Platform	Predefined asset type
Enterprise Security Manager Platform	■ ESM Agent

Table 3-2 Predefined asset types *(continued)*

Platform	Predefined asset type
Exchange	■ Administrative Groups MS-Exchange See "Fields for Administrative Groups MS-Exchange" on page 94. ■ Exchange Server See "Fields for Exchange Server" on page 95. ■ Organization MS-Exchange See "Fields for Organization MS-Exchange" on page 96.
NDS	■ NDS Tree See "Fields for NDS Tree" on page 102.
NetWare	■ NetWare Server See "Fields for NetWare File Server" on page 103.
Oracle Platform	■ Oracle Configured Databases See "Fields for Oracle Configured Databases" on page 73.
SQL Platform	■ SQL Database See "Fields for SQL Databases" on page 70. ■ SQL Server See "Fields for SQL Server" on page 71.
UNIX Platform	■ UNIX File See "Fields for UNIX File" on page 75. ■ UNIX Group See "Fields for UNIX Group" on page 76. ■ UNIX Machine See "Fields for UNIX Machine" on page 76.

Table 3-2 Predefined asset types *(continued)*

Platform	Predefined asset type
Windows Platform	■ IIS Virtual Directory See "Fields for IIS Virtual Directory" on page 96. ■ IIS Web Site See "Fields for IIS Web Site" on page 99. ■ Windows Directory See "Fields for Windows Directory" on page 81. ■ Windows Domain See "Fields for Windows Domain" on page 78. ■ Windows File See "Fields for Windows File" on page 83. ■ Windows Group See "Fields for Windows Group" on page 86. ■ Windows Machine See "Fields for Windows Machine" on page 88. ■ Windows Share

See "Probable asset types" on page 103.

See "Custom asset types" on page 104.

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 3-3 lists the primary, mandatory, and optional fields for the ESM agents asset type.

Table 3-3 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

Table 3-3 Fields for ESM Agent *(continued)*

Display name	Description	Type	Is single valued?	Field type
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 SQL Databases

Table 3-4 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
Owner	The owner of the SQL server element.	String	Single valued	Optional
Host name (DNS)	The name of the Windows NT server that hosts the SQL server database.	String	Single valued	Optional

Table 3-4 Fields for SQL Database *(continued)*

Display name	Description	Type	Single valued or multi valued	Field type
IP Addresses	This field returns all the TCP/IP addresses that are configured for the computer that contains the database.	String	Multi valued	Optional

See "Predefined asset types" on page 66.

Fields for SQL Server

Table 3-5 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

Table 3-5 Fields for SQL Server *(continued)*

Display name	Description	Type	Single valued or multi valued	Field type
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
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

Table 3-5 Fields for SQL Server *(continued)*

Display name	Description	Type	Single valued or multi valued	Field type
Host Name (DNS)s	The name of the Windows NT server that hosts the SQL server database.	String	Single valued	Optional

See “Predefined asset types” on page 66.

Fields for Oracle Configured Databases

Table 3-6 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

Table 3-6 Oracle Configured Databases *(continued)*

Display name	Description	Type	Single valued or multi valued	Field type
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
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
IP Addresses	List of IP network addresses of the Oracle server	String	Multi-valued	Optional
Database Version	This field reports on the database version	String	Single valued	Mandatory

Table 3-6 Oracle Configured Databases *(continued)*

Display name	Description	Type	Single valued or multi valued	Field type
Port	The port number used by the listener service for the configured database.	Integer	Single valued	Optional

See “Predefined asset types” on page 66.

Fields for UNIX File

Table 3-7 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
IP Addresses	The list of IP network addresses on the target	String	Multi valued	Optional

See “Predefined asset types” on page 66.

Fields for UNIX Group

Table 3-8 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
Group Name	This field returns the name of the group.	String	Single valued	Primary

See "Predefined asset types" on page 66.

Fields for UNIX Machine

Table 3-9 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

Table 3-9 Fields for UNIX Machine *(continued)*

Display name	Description	Type	Single valued or multi valued	Field type
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
Operating System Version	This field returns the operating system version that is running on this target.	String	Single valued	Mandatory
IP Addresses	The list of IP network addresses on the target	String	Multi valued	Optional

See “Predefined asset types” on page 66.

See “About fields of an entity ” on page 584.

Fields for Windows Domain

Table 3-10 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
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

Table 3-10 Fields for Windows Domain *(continued)*

Display name	Description	Type	Single valued or multi valued	Field type
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
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

Table 3-10 Fields for Windows Domain *(continued)*

Display name	Description	Type	Single valued or multi valued	Field type
Forest Functional Level	These fields return the forest functionality level. The forest functionality level activates the features across all the domains in your forest.	Integer	Single valued	Optional

See "Predefined asset types" on page 66.

See "About fields of an entity " on page 584.

Fields for Windows Directory

Table 3-11 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 3-11 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

See “Predefined asset types” on page 66.

See “About fields of an entity ” on page 584.

Fields for Windows File

Table 3-12 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 3-12 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

Table 3-12 Fields for Windows File *(continued)*

Display name	Description	Type	Single valued or multi valued	Field type
Host Name (DNS)	This field returns the host name of the computer by querying the name server. The configured name server of the Query Engine computer is used to resolve the host name query.	String	Single valued	Optional
TCP/IP Addresses (List)	This field returns a list of the TCP/IP addresses that are configured for the computer.	String	Multi valued	Optional

See "Predefined asset types" on page 66.

See "About fields of an entity " on page 584.

Fields for Windows Group

Table 3-13 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 3-13 Fields for Windows Group *(continued)*

Display name	Description	Type	Single valued or multi valued	Field type
Group Type	This field returns group type, i.e. domain local, domain global, universal local.	Integer	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

See “Predefined asset types” on page 66.

See “About fields of an entity ” on page 584.

Fields for Windows Machine

Table 3-14 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 3-14 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 3-14 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 3-14 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 3-14 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 3-14 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
Host Name (DNS)	This field returns the host name of the computer by querying the name server. The configured name server of the Query Engine computer is used to resolve the host name query.	String	Single valued	Optional
TCP/IP Addresses (List)	This field returns a list of the TCP/IP addresses that are configured for the computer.	String	Multi valued	Optional

See “Predefined asset types” on page 66.

See “About fields of an entity ” on page 584.

Fields for Administrative Groups MS-Exchange

Table 3-15 Fields for Administrative Groups MS-Exchange

Display name	Description	Type	Single valued or multi valued	Field type
Administrative Group DN	This field returns the full distinguished name of the Administrative Group.	String	Single valued	Primary
Administrative Group Name	This field returns the common name value of the object. Typically, this is identical to the admin display name and name values.	String	Single valued	Optional
Object Class Type	This field returns the object class type.	String	Single valued	Optional

Note: If you want to import the assets of the Administrative Groups MS Exchange asset type from a CSV file with Organization MS Exchange as scope, you must enter Organization DN field manually in the CSV file.

See “Predefined asset types” on page 66.

See “About fields of an entity ” on page 584.

Fields for Exchange Server

Table 3-16 Fields for Exchange Server

Display name	Description	Type	Single valued or multi valued	Field type
Server DN	This field returns the full distinguished name of this object that is system created.	String	Single valued	Primary
Exchange Version / Build (String)	This field returns version and the build number of Microsoft Exchange on that server. If the Internet Explorer version is older than 4.0, then the data returns as `<unknown>`.	String	Single valued	Optional
Server Roles	This field returns all the roles that are currently configured for the Exchange 2007 server..	String	Single valued	Optional
Server name	This field returns the computer name, as per the registry.	String	Single valued	Optional

Note: If you want to import the assets of the Exchange Server asset type from a CSV file with Organization MS Exchange as scope, you must enter Organization DN field manually in the CSV file.

See "Predefined asset types" on page 66.

See "About fields of an entity " on page 584.

Fields for Organization MS-Exchange

Table 3-17 Fields for Organization MS-Exchange

Display name	Description	Type	Single valued or multi valued	Field type
Organization DN	This field returns the full distinguished name of the organization.	String	Single valued	Primary
Organization Name	This field returns the organization name from the organization DN.	String	Single valued	Optional

See "Predefined asset types" on page 66.

See "About fields of an entity " on page 584.

Fields for IIS Virtual Directory

Table 3-18 Fields for IIS Virtual Directory

Display name	Description	Type	Single valued or multi valued	Field type
Virtual Directory Name	This field returns the name (without path) of the virtual directory, directory, or the file object.	String	Single valued	Mandatory

Table 3-18 Fields for IIS Virtual Directory *(continued)*

Display name	Description	Type	Single valued or multi valued	Field type
ADSI Path	This field returns the ADSI path of the IISAdmin object that is associated with the record.	String	Single valued	Primary
Parent Web Site Name	This field returns the user-friendly name of the item's parent Web Site.	String	Single valued	Mandatory
Domain/Workgroup Name	This field returns the name of the domain or workgroup that contains the computer on which the device driver is found. This field obtains the name from the Query Engine's reporting domain settings.	String	Single valued	Mandatory
PrimKey Machine	This field returns the primary key of the machine.	String	Single valued	Primary

Table 3-18 Fields for IIS Virtual Directory *(continued)*

Display name	Description	Type	Single valued or multi valued	Field type
Is In Domain (internal)	This field returns the domain membership of the computer on which the process is running. If the computer is not the member of the domain, this field returns "N/A." This field obtains the domain from the Query Engine's reporting domain settings. Use the Domain / Workgroup Name (Machine Settings) field to determine the domain or a workgroup of which the computer is a member.	String	Single valued	
PrimKey Domain	This field returns the primary key of the domain.	String	Single valued	Primary

See "Predefined asset types" on page 66.

See "About fields of an entity " on page 584.

Fields for IIS Web Site

Table 3-19 Fields for IIS Web Site

Display name	Description	Type	Single valued or multi valued	Field type
Web Site Name	This field returns the name of the object.	String	Single valued	Primary
ADSI Path	This field returns the ADSI path of the IISAdmin object that is associated with the record.	String	Single valued	Primary
Domain/Workgroup Name	This field returns the name of the domain or workgroup that contains the computer on which the device driver is found. This field obtains the name from the Query Engine's reporting domain settings.	String	Single valued	Mandatory
PrimKey Machine	This field returns the primary key of the machine.	String	Single valued	Primary

Table 3-19 Fields for IIS Web Site *(continued)*

Display name	Description	Type	Single valued or multi valued	Field type
Is In Domain (internal)	This field returns the domain membership of the computer on which the process is running. If the computer is not the member of the domain, this field returns "N/A." This field obtains the domain from the Query Engine's reporting domain settings. Use the Domain / Workgroup Name (Machine Settings) field to determine the domain or a workgroup of which the computer is a member.	String	Single valued	
PrimKey Domain	This field returns the primary key of the domain.	String	Single valued	Primary

Fields for Windows Share

Table 3-20 Fields for Windows Share

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
Share Name	This field returns the name assigned to the share.	String	Single valued	Primary

Table 3-20 Fields for Windows Share *(continued)*

Display name	Description	Type	Single valued or multi valued	Field type
Hidden	This field returns True if the Windows share is hidden for normal browsing. The Shares are hidden by adding a "$" at the end of the share name.	Boolean	Single valued	Optional
Comment	This field returns the comment text that is assigned to the share. This is usually a description of the share.	String	Single valued	Optional

See “Predefined asset types” on page 66.

See “About fields of an entity ” on page 584.

Fields for NDS Tree

Table 3-21 Fields for NDS Tree

Display name	Description	Data type	Single valued or multi-valued	Field type
Tree name	This field contains the name of the NDS tree.	String	Single valued	Primary

See “Predefined asset types” on page 66.

See “About fields of an entity ” on page 584.

Fields for NetWare File Server

Table 3-22 Fields for NetWare File Server

Display name	Description	Data type	Single values or multi valued	Field type
Object name (DN)	This field contains the Distinguished Name of the report object. The DN is the unique name of the object including all the folders up to the root folder.	String	Single valued	Primary
Tree name	This field contains the name of the NDS tree.	String	Single valued	Primary

See “Predefined asset types” on page 66.

See “About fields of an entity ” on page 584.

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 66.

In Control Compliance Suite, a platform is defined to be the category to which a group of entities belong.

See “Predefined platforms” on page 65.

See “About platforms” on page 583.

A group of fields that define the common functions of the network element form an entity.

See “About entities” on page 583.

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 568.

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:

- Registry
- Service

See "Custom asset types" on page 104.

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.

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 583.

See "About entities" on page 583.

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 569.

See "Extending an existing asset type" on page 575.

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 483.

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 481.

Table 3-23 Predefined asset types and primary assets

Asset type	Primary asset
ESM Agents	Site ESM Agents
Oracle Configured Databases	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
IIS Virtual Directory	Windows Machine
IIS Web Site	Windows Machine

Table 3-23 Predefined asset types and primary assets *(continued)*

Asset type	Primary asset
Windows Share	Windows Machine
Administrative Group MS-Exchange	Organization MS-Exchange
Exchange Server	Organization MS-Exchange
Organization MS-Exchange	Site

Site is the primary asset for ESM Agents, Oracle Configured Databases, SQL Servers, UNIX Machine, Windows Domain, and Organization MS-Exchange.

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 3-24 Types of reconciliation rules

Rule type	Rule description
Pre rule See "Pre rule" on page 108.	A Pre rule is executed on the assets that are in the process of import before the assets are brought into the assets system. The Pre rule lets you set a value for a particular asset field. The Pre rule also lets you discard the asset.
Add rule See "Add rule" on page 109.	An Add rule is executed to add the assets that are in the process of import to the asset system 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.
Update rule See "Update rule" on page 110.	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 113.	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 114.

See "Creating reconciliation rules without manual review" on page 437.

See "Creating reconciliation rules using the manual review" on page 438.

Pre rule

A Pre rule is executed on the assets being imported before the assets are brought into the assets system.

Table 3-25 are as follows:

Table 3-25 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	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 3-26 are as follows:

Table 3-26 Actions for Pre rule

Action	Description
Discard an asset being imported	Ignores the asset that is being imported. The asset is not added to the asset system if no Add Rule is specified.
Set the field value of an asset being imported as specified	Sets the field value of the asset that is being imported as the value that you specify. 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.

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.

Add rule

The Add rule is executed to add the assets being imported to the asset system.

Table 3-27 are as follows:

Table 3-27 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	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 3-28 are as follows:

Table 3-28 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	Adds the asset to the manual review store See "Manual review" on page 130.

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.

Update rule

Update rule is applied on the existing assets to update their fields with the values of the assets being imported.

Table 3-29 are as follows:

Table 3-29 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	The action is performed if the existing asset field has a specified relation with the specified value For example,<imported asset field> <operator> <value>

Table 3-29 Conditions for Update rule *(continued)*

Condition	Description
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>
If field of an asset being imported has a relation with an existing asset field	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. For example, <current asset field><operator><imported asset field> <Asset Custodian><equals><Asset Owner>

Table 3-30 are as follows:

Table 3-30 Actions for Update rule

Update rule- action	Description
Set the field value of an existing asset as specified	Sets the field value of an existing asset as that you specify. 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. If you select Asset Tags as the field, you can also select the Tag Set Options that work as follows: ■ 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	Replaces the values of the selected fields of an existing asset with the values of the fields of the asset that is being imported. **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.
Add to manual review store	Adds the asset to the manual review store. See "Manual review" on page 130.

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.

Post rule

The Post rule is executed at the end in the order of the reconciliation rules.

Table 3-31 are as follows:

Table 3-31 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>
If field of an asset being imported has a relation with an existing asset field	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. For example, <current asset field><operator><imported asset field> <Asset Custodian><equals><Asset Owner>

Table 3-32 are as follows:

Table 3-32 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.

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 64.

See "Creating the asset folders" on page 505.

Table 3-33 Predefined reconciliation rules

Rule type	Rule statement	Rule description
Add Rule Rule Name: Add asset to the asset system	IF *an asset being imported does not exist in the asset system* THEN *Add an asset being imported to the Asset System folder*	The rule is applicable to all the asset types. The rule adds all the assets that are being imported to the asset system if they do not exist already in the system. The assets are added to the Asset System folder.

Table 3-33 Predefined reconciliation rules *(continued)*

Rule type	Rule statement	Rule description
Add Rule for Vulnerability Manager Rule Name: Add UNIX Machine	IF Device Operating System Subcategory equals Linux AND UNIX Machine asset does not exist where {(Machine Name equals Device Host Name) OR (IP Address equals Device IP Address)} THEN Create UNIX Machine asset using {(Machine Name with Device Host Name), (IP Address with Device IP Address), (Operating System with Device Operating System Type), (Operating Distribution Field with [Undefined]), (Operating System Version with Device Operating System Version)} and place the asset in the Asset System folder	Add UNIX Machine while importing data from Symantec CCS Vulnerability Manager.

Table 3-33 Predefined reconciliation rules *(continued)*

Rule type	Rule statement	Rule description
Add Rule for Vulnerability Manager Rule Name: Add Windows Machine	IF Device Operating System Subcategory contains Windows AND Windows Machine asset does not exist where {(Machine Name equals Device Host Name) OR (Host Name (DNS) equals Device Fully Qualified Name)} THEN Create Windows Machine asset using {(Domain/Workgroup Name with [Undefined]), (Machine Name with Device Host Name), (OS Major Version Number with 0), (OS Minor Version Number with 0), (OS Type with Device Operating System Type), (Machine Is Server with False), (Machine Is PDC with False), (Machine Is BDC with False), (TCP/IP Addresses <LIST> with Device IP Address), (Host Name (DNS) with Device Fully Qualified Name)} and place the asset in the Asset System folder	Add Windows Machine while importing data from Symantec CCS Vulnerability Manager.

Table 3-33 Predefined reconciliation rules *(continued)*

Rule type	Rule statement	Rule description
Pre Rule Rule Name: Set CIA values before adding asset to the asset system.	IF an asset being imported does not exist in the asset system THEN Set the value of the Confidentiality field as NotDefined Set the value of the Integrity field as NotDefined Set the value of the Availability field as NotDefined	The rule is applicable to all the asset types. The rule checks if the asset that is the process of import is in the asset system or not. If the asset is not in the asset system, it sets the value of the Confidentiality, Integrity, and Availability attributes of the assets to NotDefined.
Pre Rule for Exchange Rule Name: Filter Exchange Administrative Groups	IF object class type does not equal msExchAdminGroup THEN discard an asset being imported	The rule is applicable to the Administrative Groups MS-Exchange asset type only. The rule checks if the asset that is in the process of import is an administrative group or not. If the asset is not an administrative group, the rule discards the asset.
Pre Rule for Exchange Rule Name: Filter Exchange Edge Servers	IF object class type does not equal msExchEdgeServer THEN discard an asset being imported	The rule is applicable to the Exchange Server asset type only. The rule checks if the asset that is in the process of import is an Exchange Edge Server or not. If the asset is an Exchange Server, the rule discards the asset.

Table 3-33 Predefined reconciliation rules *(continued)*

Rule type	Rule statement	Rule description
Pre Rule for UNIX Rule Name: Set UNIX machine SSH port to default value	IF the incoming data field does not have value THEN Set the field value of an asset being imported as specified	The rule is applicable to the UNIX Machine asset type only. The rule checks if the asset that is in the process of import does have specific value or not. If not then set the value of an asset being imported or specified to default value.
Pre Rule for UNIX Rule Name: Set UNIX machine SSH version to default value	IF the incoming data field does not have value THEN Set the field value of an asset being imported as specified	The rule is applicable to the UNIX Machine asset type only. The rule checks if the asset that is in the process of import does have specific value or not. If not then set the value of an asset being imported or specified to default value.
Pre Rule for Oracle Rule Name: Set Oracle database connection type to default value	IF the incoming data field does not have value THEN Set the field value of an asset being imported as specified	The rule is applicable to the Oracle Configured Databases asset type only. The rule checks if the asset that is in the process of import does have specific value or not. If not then set the value of an asset being imported or specified to default value.

Table 3-33 Predefined reconciliation rules *(continued)*

Rule type	Rule statement	Rule description
Pre Rule for Oracle Rule Name: Set Oracle database SSH version to default value	IF the incoming data field does not have value THEN Set the field value of an asset being imported as specified	The rule is applicable to the Oracle Configured Databases asset type only. The rule checks if the asset that is in the process of import does have specific value or not. If not then set the value of an asset being imported or specified to default value.
Pre Rule for Oracle Rule Name: Set Oracle database port to default value	IF the incoming data field does not have value THEN Set the field value of an asset being imported as specified	The rule is applicable to the Oracle Configured Databases asset type only. The rule checks if the asset that is in the process of import does have specific value or not. If not then set the value of an asset being imported or specified to default value.
Pre Rule for Oracle Rule Name: Set Oracle database protocol to default value	IF the incoming data field does not have value THEN Set the field value of an asset being imported as specified	The rule is applicable to the Oracle Configured Databases asset type only. The rule checks if the asset that is in the process of import does have specific value or not. If not then set the value of an asset being imported or specified to default value.

Table 3-33 Predefined reconciliation rules *(continued)*

Rule type	Rule statement	Rule description
Pre Rule for Oracle Rule Name: Set Oracle database name type to default value	IF the incoming data field does not have value THEN Set the field value of an asset being imported as specified	The rule is applicable to the Oracle Configured Databases asset type only. The rule checks if the asset that is in the process of import does have specific value or not. If not then set the value of an asset being imported or specified to default value.
Pre Rule for Oracle Rule Name: Set Oracle database SSH port to default value	IF the incoming data field does not have value THEN Set the field value of an asset being imported as specified	The rule is applicable to the Oracle Configured Databases asset type only. The rule checks if the asset that is in the process of import does have specific value or not. If not then set the value of an asset being imported or specified to default value.
Update Rule Rule Name: Update asset	IF an asset being imported exists in the asset system THEN update all fields of the existing asset with the values of the current asset.	The rule is applicable to all the asset types. The rule checks if the asset that in the process of import exists in the asset system or not. If the asset is in the asset system, the rule overwrites the values of all the existing asset fields with the values of the asset being imported.

Table 3-33 Predefined reconciliation rules *(continued)*

Rule type	Rule statement	Rule description
Update Rule for ESM Rule Name: Update Host Name, IP Address, and FQDN for ESM agents	IF an asset being imported exists in the asset system THEN update only selected fields Host Name, IP Address, FQDN of an existing asset with the fields of the asset being imported. (Manual review enabled)	The rule is applicable only to the ESM Agent asset type. The rule checks if the asset that in the process of import exists in the asset system or not. If the asset exists in the asset system, the rule overwrites the values of the fields Host Name, IP Address, and FQDN with the values of the new asset. The asset records are sent to the manual review store.
Update Rule for Vulnerability Manager Rule Name: Update Windows Machine IP Address	IF Windows Machine asset exists where {(Machine Name equals Device Host Name)} THEN Update the fields of Windows Machine asset with the incoming data {(TCP/IP Addresses <LIST> with Device IP Address)}	Update Windows Machine IP Address while importing data from Symantec CCS Vulnerability Manager.

See “Creating reconciliation rules without manual review” on page 437.

See “Creating reconciliation rules using the manual review” on page 438.

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 121.

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 477.
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 66.
  The data for the asset-specific fields is imported from the default data collector.

  Note: The default data collector is not applicable for fresh installation of CCS.

Go through the following concepts to perform the asset import more effectively:

- Default data collectors
  See "Default data collectors" on page 123.

  Note: The default data collector is not applicable for fresh installation of CCS.

- Data collectors and asset types
  See "Data collectors and asset types" on page 124.
- Asset field filters
  See "Examples of asset filters" on page 127.
- Filter statement operators
  See "Filter statement operators" on page 128.
- Asset reconciliation
  See "Asset reconciliation" on page 129.
- Manual review
  See "Manual review" on page 130.

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 3-34 Platform and data collectors

Platform	Data collector
ESM platform	ESM data collector

Table 3-34 Platform and data collectors *(continued)*

Platform	Data collector
Oracle platform	Oracle data collector
SQL platform	SQL data collector
UNIX platform	UNIX data collector
Windows platform	Windows data collector
Exchange platform	Exchange data collector
NDS platform	NDS data collector
NetWare platform	NetWare data collector
Custom platform	You can use the following data collector for the custom platform: ■ CSV data collector ■ ODBC data collector **Note:** For custom platforms, if you select CSV or ODBC data collector during entity schema creation, then the selected data collector becomes the default data collector. When importing assets of the custom platform, the option, Default appears in the drop-down list of the Create or Edit Asset Import wizard.
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: ■ CSV data collector ■ ODBC data collector

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
  - Windows Share
  - Organization MS-Exchange
  - Administrative Groups MS-Exchange
  - Exchange Server
  - NDS Tree
  - NetWare File Server
- 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
- Windows Share
- Exchange
  - Organization MS-Exchange
  - Administrative Groups MS-Exchange
  - Exchange Server
- NetWare
  - NetWare File Server
- ODBC
  - 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
  - Windows Share
  - Organization MS-Exchange
  - Administrative Groups MS-Exchange
  - Exchange Server
  - NDS Tree
  - NetWare File Server

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 3-35 Examples of asset filters

Scenario	Filter statement	Job result
To import assets of the Windows Directory with Machine 1 and Machine 2 as scope	*((Root Path EqualTo D: Or Root Path EqualTo C:) and depth GreaterThanOrEqualTo 1) and Is Shared? = True*	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*	*(Root Path EqualTo D:\directory and depth GreaterThanOrEqualTo 1) and Directory Name Like %Accounts%*	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	*Root Path EqualTo D:\directory and depth GreaterThanOrEqualTo 1*	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	*(Root Path EqualTo D:\directory and depth GreaterThanOrEqualTo 1) and Permissions DifferentThan Parent(Include Owner) / (Ignore Owner) EqualTo Different*	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	*Filename(With Path) like /etc%*	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 3-36 Filter statement operators

Operator Name	Description	Filter Statement examples
Equal To (=)	A must be equal to B	**Directory Name EqualTo 'Admin'**
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'**

Table 3-36 Filter statement operators *(continued)*

Operator Name	Description	Filter Statement examples
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**
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>

See “Operators (,), AND, OR” on page 504.

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 108.
- Add rule

See “Add rule” on page 109.

- Update rule
  See “Update rule” on page 110.
- Post rule
  See “Post rule” on page 113.

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 106.

See “Creating reconciliation rules without manual review” on page 437.

See “Creating reconciliation rules using the manual review” on page 438.

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 496.

See “Reconciling the manual review records” on page 497.

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.

See “About tags” on page 213.

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:

- Asset groups with assets based on criteria
  See “Asset groups with assets based on criteria ” on page 131.
- Asset groups with specific assets
  See “Asset groups with specific assets” on page 132.
- Predefined asset group
  See “Predefined asset groups” on page 132.

See “Creating an asset group with assets based on criteria” on page 498.

See “Creating an asset group with specific assets” on page 502.

See “Editing an asset group” on page 513.

Asset groups with assets based on criteria

An asset group with assets based on criteria is updated with every asset import job if more assets meet the criteria that is specified in the query. 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 asset groups with assets based on criteria 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 an asset group with assets based on criteria" on page 498.

Asset groups with specific assets

You can create the asset groups with specific assets on the basis of the asset group criteria.

The asset count in these asset groups does not change automatically with the import job. You manually add assets to these asset groups.

See "Creating an asset group with specific assets" on page 502.

Predefined asset groups

The asset system provides predefined asset groups for all the predefined platforms.

See "Predefined platforms" on page 65.

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 3-37 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 Exchange platform are as follows:

Table 3-38 Predefined asset groups for the Exchange platform

Group name	Filter / Definition of the dynamic group
Exchange 2000 Server	Exchange Server – Exchange Version/Build = 'Version 6.0'
All Exchange Organizations	-
Exchange 2007 Hub transport Servers	Exchange Server – Exchange Version/Build = 'Version8' and Exchange Server - Server Role(s) ='Hub transport'
All Exchange Servers	-
Exchange 2007 Unified Messaging Servers	Exchange Server – Exchange Version/Build = 'Version8' and Exchange Server - Server Role(s) ='Unified Messaging'
Exchange 2007 Client Access Servers	Exchange Server – Exchange Version/Build = 'Version8' and Exchange Server - Server Role(s) ='Client Access'
All Exchange Administrative Groups	-
Exchange 2007 Mailbox Servers	Exchange Server – Exchange Version/Build = 'Version8' and Exchange Server - Server Role(s) ='Mailbox'

Table 3-38 Predefined asset groups for the Exchange platform *(continued)*

Group name	Filter / Definition of the dynamic group
Exchange 2003 Servers	Exchange Server – Exchange Version/Build = 'Version 6.5'
Exchange 2007 Servers	Exchange Server – Exchange Version/Build = 'Version 8.0'
Exchange 2007 Edge Transport Servers	Exchange Version= '*Version 8*'

The predefined asset groups for the NDS platform are as follows:

Table 3-39 Predefined asset groups for the NDS platform

Group name	Filter / definition of the dynamic group
All NDS Trees	NDS Tree - Tree name Equal To (=) '*'

The predefined asset groups for the NetWare platform are as follows:

Table 3-40 Predefined asset groups for the NetWare platform

Group name	Filter / definition of t he dynamic group
All NetWare Servers	NetWare Server- Object Name (DN) Equal To (=) '*'
NetWare 6.5 Servers	NetWare Server- Object Name (DN) Equal To (=) '*' and NetWare Server-NetWare Version = '*NetWare 5.70*'
NetWare 5.X Servers	NetWare Server- Object Name (DN) Equal To (=) '*' and NetWare Server-NetWare Version = '*NetWare 5.00*'
NetWare 4.X Servers	NetWare Server- Object Name (DN) Equal To (=) '*' and NetWare Server-NetWare Version = '*NetWare 4.*'
NetWare 6 Servers	NetWare Server- Object Name (DN) Equal To (=) '*' and NetWare Server-NetWare Version = '*NetWare 5.60*'

The predefined asset groups for the Oracle platform are as follows:

Table 3-41 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'
All Oracle installations on Windows Machines	Oracle Configured Databases- OS Type = 'Windows'
All Oracle objects	-
All Oracle Databases	-

The predefined asset groups for the SQL platform are as follows:

Table 3-42 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	-
All SQL Server 2000 Instances	SQL Server- Major Version = '8'
All SQL Server 2008 Instances	SQL Server- Major Version = '10'

The predefined asset groups for the UNIX platform are as follows:

Table 3-43 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*'
Red Hat Linux Servers	UNIX Machine- Operating Distribution Field ='*Red Hat Linux*'
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*'
All AIX Servers	UNIX Machine- Operating Distribution Field ='*AIX*'
AIX 5.3 Servers	UNIX Machine- Operating Distribution Field ='*AIX*' and UNIX Machine- Operating System Version= '5.3'
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*'

Table 3-43 Predefined asset groups for the UNIX platform *(continued)*

Group name	Filter / Definition of the dynamic group
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'
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'

Table 3-43 Predefined asset groups for the UNIX platform *(continued)*

Group name	Filter / Definition of the dynamic group
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*'
All UNIX Servers with Apache Installed	Unix Machine -Is Apache Installed = 'True'

The predefined asset groups for the Windows platform are as follows:

Table 3-44 Predefined asset groups for the Windows platform

Group name	Filter / Definition of the dynamic group
Windows Domain Controllers	Windows Machine - Machine Is Server= 'True' and (Windows Machine- Machine Is PDC= 'True' or Windows Machine- Machine Is BDC= 'True'

Table 3-44 Predefined asset groups for the Windows platform *(continued)*

Group name	Filter / Definition of the dynamic group
Windows Backup Domain Controllers	Windows Machine- Machine Is BDC= 'True'
Windows 2003 Machines	Windows Machine- OS Major Version Number= '5' and Windows Machine OS Minor Version Number= '2'
All IIS Web Sites	IIS Web Site - Name Equal To(=) "*" or IIS Web Site- ADSI Path Equal To(=) "*"
Windows XP Machines	Windows Machine- OS Major Version Number= '5' and Windows Machine OS Minor Version Number= '1'
Windows Primary Domain Controllers	(Windows Machine- Machine Is PDC= 'True'
Windows 2000 Professional	Windows Machine - OS Type= 'Windows 2000 Professional'
Windows Workstations	Windows Machine - Machine Is Server= 'False'
All Windows Machines	-
Windows 2000 Servers	Windows Machine- OS Type= 'Windows 2000*Server*'
Windows Servers	Windows Machine- Machine Is Server= 'True'
Windows NT 4.x Machines	Windows Machine - OS Major Version Number = '4'

Table 3-44 Predefined asset groups for the Windows platform *(continued)*

Group name	Filter / Definition of the dynamic group
Windows 2008 Machines	Windows Machine - Machine Is Server Equal To(=) 'True' and Windows Machine - OS Major Version Number Equal To (=) '6' and Windows Machine - OS Minor Version Number Equal To (=)'0'
All IIS Virtual Directories	IIS VIrtual Directory - ADSI Path Equal To(=) '*'
Windows Vista Machines	Windows Machine- OS Major Version Number= '6' and Windows Machine OS Minor Version Number= '0' and Windows Machine - Machine Is Server= 'False'
Windows 2000 Machines	Windows Machine- OS Major Version Number= '5' and Windows Machine OS Minor Version Number= '0'
Windows 2008 R2 Machine	Windows Machine-
Windows 7 Machine	Windows Machine- Machine Is Server = ’False’ and Windows Machine- OS Major Version Number =’6’ and Windows Machine- OS Minor Version Number =’1’
Windows SharePoint Servers 2007	Wnt.machine.sharepointversion = =~ '^12\..*'

See “Creating an asset group with assets based on criteria” on page 498.

See “Creating an asset group with specific assets” on page 502.

See “Editing an asset group” on page 513.

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

See “About the Asset System view ” on page 434.

About the management of business assets

Use the asset system in CCS to view and manage business assets.

You manage business assets in the following ways:

- View business assets.
- Edit business assets.
- Delete business assets.
- Manage associations: Form associations with business or network assets, or remove associations.
  CCS makes available the new tasks, **Associate with Business Asset**and **Remove Association**.
- Move business assets.
  To move a business asset, right-click the business asset in the Assets table, and click **Move Assets**.
- Assign and remove permissions on business assets.
- Search for business assets.

To view business assets, you require the following permissions:

- Roles that are associated with the **View Asset** task
- Requisite permissions on the business assets

CCS provides you the following view options:

- View types of business assets.
  Move your pointer over a business asset in the Assets table to see its name and type.
- Select an asset group in the assets pane to view the assets in the group in the Assets table.
- In the **Assets** pane, select a business asset with associations to view the assets that are associated with the selected business asset in the Assets table.
- Select a folder in the **Assets** pane to view all assets within the folder in the Asset table.
- View the permissions on a business asset.
  To view the permissions on a business asset, right-click the business asset, and click **View Permissions** or on **Common Tasks**, click **View Permissions**.

The Advanced Search functionality of the asset system facilitates the search for a specific set of assets. On the search results, you can perform all those operations that are possible on business assets in the asset system.

The asset system supports the searches that are based on the following criteria:

- Common attributes like name, owner, department, and location
- Tags
- Asset types
- The properties or attributes that are specific to an asset type as computer name, and application name
- A specific folder or a branch in the directory

See “About business assets” on page 62.

See “About types of business assets” on page 63.

See “Editing business assets” on page 509.

See “Associating with a business asset” on page 510.

See “Removing the association with a business asset” on page 510.

See “Assigning permissions on business assets” on page 511.

See “Removing permissions from a business asset” on page 512.

About associations with business assets

To form associations with business assets, in the asset system, use the task, **Associate with Business Asset**, under **Asset Tasks**. Association helps to aggregate the risk scores for all associated assets.

To form associations, you require the following permissions:

- View Assets
- Permissions that are associated with the 'Manage Assets and Asset groups' task

Control Compliance Suite supports the following:

- Association of business assets with other business assets and network assets
  The maximum number of business or network assets with which a business asset can form associations is 1500. To associate with more than 1500 business or network assets, a business asset needs to expand its association capability. A business asset forms an association with another business asset to expand its association capability.
- Association to evaluate risk
  Evaluation of risk involves the definition of a risk objective, and the association of the business asset with the risk objective. Effective evaluation of risk also requires the association of the business asset with other business assets and physical assets. Dynamic Dashboards display the aggregated risk of the business asset and all associated business assets.
- Association to evaluate compliance
  The evaluation of the compliance of a business asset to a policy needs the following: The aggregation of the compliance of all assets with direct or indirect associations with that business asset. Compliance involves technical and procedural controls. Technical controls link policy to control statements, and the control statements to checks, rules, and EDI. Procedural compliance control involves the creation of questionnaires for the business asset, and the association of the questionnaires with the business assets.
- Association by means of reconciliation rules
  The asset system provides an action for a Post Rule for the import of network assets as well as third-party assets: Associate asset with specified business asset.
- Associations by means of integration services
  Invoke the related API to form the association.
- Removal of associations with business assets
  Use the **Remove Association** task to remove associations.

CCS support does not extend to the following:

- Use of reconciliation rules to import network assets and thereby create business assets.
- Circular dependency in associations: A can associate with B, and B with C, but C cannot associate with A to form a ring.

See "Associating with a business asset" on page 510.

See "Removing the association with a business asset" on page 510.

About queries

Control Compliance Suite queries collect data about the objects in your network. Queries collect data for the parameters you configure. Queries bypass the asset system to provide a direct method of data collection.

Control Compliance Suite provides two kinds of queries:

- Custom queries: Queries for which you configure all parameters
- Predefined queries: Sample queries for Windows, SQL, UNIX, and Oracle platforms with preselected entity and fields, besides default scope
  You can edit predefined queries.

The number of entities that platforms support for queries are as follows:

Platform	Number of supported entities
UNIX	23
SQL	43
Oracle	43
Windows	54

See "Configuring queries" on page 355.

Concepts in agent management

To understand the sequence of tasks to be carried out in agent management, you must understand the concepts in agent management.

Concepts in agent management are as follows:

- CCS Manager
  See "CCS Manager" on page 50.

- CCS Agent
  See "CCS Agent" on page 54.
- Data collection models in Control Compliance Suite
  See "About data collection models" on page 60.

Agent registration

The CCS agent is registered to the CCS Manager using the agent registration utility. The agent information is stored in an agent information file on the CCS Manager. The CCS Manager sends the agent information to the Application Server through an Agent Registration Job (ARJ). The agents and assets are created and imported into the Asset system through an Agent Registration Job. Asset import is also done for the application modules installed on the agents.

LiveUpdate

The LiveUpdate mechanism ensures that during data collection the agent has the latest content updates. The application server downloads the latest content update packages from the LiveUpdate Server. The Application server creates granular LiveUpdate packages for the agents and sends them to the CCS Manager. Depending on the data collection job that the agent executes, the required content files are updated on the agent

Remote Upgrade

The remote upgrade mechanism is used to upgrade CCS agents remotely from the CCS console. The Remote Upgrade (RU) packages that are available with the CCS Manager are pushed to the CCS agents. The upgrade process is initiated on the respective CCS agents.

Agent configuration

Agent configuration parameters control the behavior of the CCS agents. You can remotely set the CCS agent configuration parameters from the CCS console.

You can set the following properties using agent configuration parameters:

- Log level
- Number of jobs that can be run in parallel
- Number of log files
- Job expiry time
- Files to fetch for troubleshooting

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 146.
- Entity schema
  See "About the entity schema " on page 147.
- Target type schema
  See "About the target type schema" on page 148.

See "Working with custom schema scenarios" on page 589.

See "Working with custom asset types" on page 567.

See "Working with custom entity" on page 578.

See "Working with custom target type" on page 587.

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 66.

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 569.

See "Extending an existing asset type" on page 575.

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.

See "Creating a CSV file for custom application" on page 487.

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 572.

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 578.

See "Editing an existing entity schema" on page 582.

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 587.

See “Editing a target type” on page 588.

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 148.
- Data owners
  See “Data owners” on page 150.
- Alternative approver
  See “Alternative approver” on page 150.
- Review cycle setting
  See “Review cycle setting” on page 150.
- Approval period
  See “Approval period” on page 151.
- Tagging
  See “Tagging” on page 151.

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 616.

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 616.

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 631.

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 618.

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 629.

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.

See "Concepts in entitlements" on page 148.

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 153.
- Exceptions
  See "About exceptions" on page 152.
- Exception validity
  See "About exception validity " on page 153.
- Exception templates
  See "About exception templates" on page 154.
- Exception states
  See "About exception states " on page 155.
- Exception filters
  See "About the exception filters" on page 157.

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 “About the exception management system” on page 153.

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:

- SCAP
- Standards
- Entitlements
- Policies

See “About exceptions” on page 152.

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	The start date when the exception is applied to the specified objects. 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.

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.

When an exception is created or modified, the effective time by default is 12:00 a.m. local time.

Expiration date

The end date when the exception no longer remains valid. From this date onward, the exception is not applied to the specified objects.

The expiration date must be equal to or greater than the effective date. You can change this date when you modify an exception.

When the current date exceeds the expiration date, the exceptions are marked as expired automatically.

Expiration time

The local time at which the exception validity period ends. The exception becomes invalid at this time on the specified expiration date.

When an exception is created or modified, the expiration time by default is 11:59 p.m. local time.

An internal system job runs at 12 a.m. by default to mark all the exceptions due for expiration as **Expired**.

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.

The system job is internal and is not visible in the Jobs view. However, you can change the scheduled time of the system job.

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 3-45 Templates

Module	Template	Objects
SCAP	SCAP Exception	SCAP exceptions can be requested on the rules of an SCAP benchmark profile. If you select a profile to request an exception, then all the rules of the profile are considered for an exception. The objects can be associated with assets, asset groups, and asset containers.
Standards	Evaluation Exception	The objects are as follows: ■ Standards ■ Sections ■ Checks The objects can be associated with assets, asset groups, and asset containers.
Entitlements	Entitlement Exception	Control Points
Policies	Policy Exception	Policies The objects can be associated with assets, asset groups, and asset containers.

See "About exceptions" on page 152.

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 3-46 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.
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	This state indicates that the exception is now invalid. The system sets the status of an exception as expired when the current date has exceeded the expiration date of the exception. A requestor can set the status of an exception as expired at any time.

See “About exceptions” on page 152.

See “About exception states ” on page 155.

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	Lets you filter the exceptions according to the specified tags. ■ 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.

See “About exceptions” on page 152.

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 158.
- Predefined standards
  See “About predefined standards” on page 158.
- Sections
  See “About sections” on page 162.
- Checks

See “About checks” on page 163.

- Data collection job
  See “About data collection jobs” on page 163.
- Evaluation job
  See “About evaluation jobs” on page 164.
- Compliance score
  See “About compliance score” on page 175.
- Risk score
  See “About risk score” on page 175.

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 162.

See “About checks” on page 163.

See “About predefined standards” on page 158.

See “Working with standards” on page 654.

See “About versioning scheme” on page 176.

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:

- Oracle
  See "Predefined standards for Oracle" on page 159.
- UNIX
  See "Predefined standards for UNIX" on page 159.
- Windows
  See "Predefined standards for Windows" on page 160.

See "About standards" on page 158.

See "Working with standards" on page 654.

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 158.

The following predefined standard for the Oracle platform is installed with the product:

- CIS Oracle 9i and 10g Database Security Benchmark v2.0
  You must ensure that you configure bv-Control for Windows SQL Server, bv-Control for UNIX, and bv-Control for Windows with the Information Server for this standard.
- CIS Oracle Database Server 11g Security Benchmark v1.0.1

See "Predefined reconciliation rules" on page 114.

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 158.

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
- Security Essentials for SuSE Linux Enterprise Server 10 and SuSE Linux Enterprise Server 11

Note: Along with the predefined standards, the regulatory standards for the UNIX platform are also installed with the product.

See “Predefined reconciliation rules” on page 114.

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 158.

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
- 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
- Security Essentials for Windows Server 2008
- Security Essentials for Windows Server 2008 R2
- Security Essentials for Symantec Endpoint Protection

Note: Along with the predefined standards, the regulatory standards for the Windows platform are also installed with the product.

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.

Table 3-47 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 3-47 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

Table 3-47 CCS standard to ESM policy mapping *(continued)*

Predefined CCS standard	ESM policy	ESM policy installer in the product disc
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
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.

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 158.

See "About checks" on page 163.

See "About versioning scheme" on page 176.

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 158.

See "About sections" on page 162.

See "About versioning scheme" on page 176.

See "Working with checks" on page 669.

See "About operators" on page 197.

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 "About advanced options for data collection" on page 164.

About advanced options for data collection

The Control Compliance Suite provides you with the ability to collect data only for the assets for which data was never collected in the previous job runs. When you specify a periodic schedule to run a data collection job after specific intervals, some assets may be down. Due to this, the data for those assets may not be collected during the specified periodic schedule.

The advanced options for data collection lets you specify a sub-schedule within the main schedule of the periodic data collection. You can specify the number of days after which the job must be repeated within the main schedule. The job is run after every specified interval until the specified day.

These options help you get the most updated data for all the available assets in the scope for the data collection job.

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.

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:

- Windows
  See "About Windows predefined target types" on page 165.
- UNIX
  See "About UNIX predefined target types" on page 166.
- Oracle
  See "About Oracle predefined target types" on page 171.

About SQL predefined target types

The SQL predefined target types are as follows:

Table 3-48 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.
SQL Databases	All SQL databases.
SQL Server 2008 Instances	All Microsoft SQL Server 2008 instances.

About Windows predefined target types

The Windows predefined target types are listed as follows:

Table 3-49 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
Windows 2000 Domain Controller Servers	All Windows 2000 Server Machine Types (Domain Controllers)
Windows 2008 R2 Machine	All Windows 2008 R2 computers
Windows 7 Machines	All Windows 7 computers
Windows server 2008 Machines	All Windows server 2008 computers
Windows Domains	All Windows domains
Windows SharePoint Servers 2007	All Windows SharePoint 2007 servers

See “About target types” on page 164.

About UNIX predefined target types

The UNIX predefined target types are as follows:

Table 3-50 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
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

Table 3-50 Supported UNIX target types *(continued)*

Target type	Description
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
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

Table 3-50 Supported UNIX target types *(continued)*

Target type	Description
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
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

Table 3-50 Supported UNIX target types *(continued)*

Target type	Description
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
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
SuSE Linux Enterprise Server 10 and Later Machines	All computers with SuSE Linux Enterprise Server 10 and later
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

Table 3-50 Supported UNIX target types *(continued)*

Target type	Description
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
UNIX Machines With Apache Installed	All UNIX computers that have Apache installed

See "About target types" on page 164.

About Oracle predefined target types

The predefined target types for Oracle are listed as follows:

Table 3-51 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.
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.

Table 3-51 Supported Oracle target types *(continued)*

Target type	Description
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 164.

About ESM predefined target types

Table 3-52 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
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
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 Exchange predefined target types

The Exchange predefined target types are as follows:

Table 3-53 Supported Exchange target types

Target type	Description
Exchange Server	All Exchange servers
Exchange Organization	The entire Exchange organization
Exchange Administrative Group	All administrative groups in the Exchange organization
Exchange 2000 Servers	All Exchange 2000 servers in the organization
Exchange 2003 Servers	All Exchange 2003 servers in the organization
Exchange 2007 Servers	All Exchange 2007 servers in the organization
Exchange 2007 Mailbox Servers	All Exchange 2007 mailbox servers.
Exchange 2007 Client Access Servers	All Exchange 2007 Client Access Servers
Exchange 2007 Hub Transport Servers	All Exchange 2007 Hub Transport Servers
Exchange 2007 Unified Messaging Servers	All Exchange 2007 Unified Messaging Servers
Exchange 2007 Edge Transport Servers	All Exchange 2007 Edge transport Servers

See “About target types” on page 164.

About NetWare predefined target types

The NetWare predefined target types are listed as follows:

Table 3-54 Supported NetWare predefined target types

Target type	Description
NetWare 5.1 Machines with NDS 7.x	All the computers that are installed with NetWare version 5.1 with NDS 7.X.
NetWare 5.1 Machines with NDS 8.x	All the computers that are installed with NetWare version 5.1 with NDS 8.X.
NetWare 5.1, 6.0, and 6.5 Machines	All the computers that are installed with NetWare version 5.1, 6.0, or 6.5.
NetWare 5.1 Machines	All the computers that are installed with NetWare version 5.1.
NetWare 6.0 and 6.5 Machines	All the computers that are installed with NetWare version 6.0 or 6.5.
NetWare 6.0 Machines	All the computers that are installed with NetWare version 6.0.
NetWare 6.5 Machines	All the computers that are installed with NetWare version 6.5.
NetWare 4.11 and 4.2 Machines	All the computers that are installed with NetWare version 4.11 and 4.2.
NetWare 4.11 and 4.2 Machines with NDS 6.x	All the computers that are installed with NetWare version 4.11 or 4.2 with NDS 6.x.
NetWare Machines with eDirectory 8.6.2	All the computers that are installed with NetWare eDirectory 8.6.2.
NetWare Machines with eDirectory 8.7.0	All the computers that are installed with NetWare eDirectory 8.7.0.
NetWare Machines with eDirectory 8.7.1	All the computers that are installed with NetWare eDirectory 8.7.1.
NetWare Machines with eDirectory 8.7.3	All the computers that are installed with NetWare eDirectory 8.7.3.
NetWare Machines with eDirectory 8.8	All the computers that are installed with NetWare eDirectory 8.8.
NetWare Machines with NDS 6.x	All the NetWare computers that are installed with NDS 6.x.
NetWare Machines with NDS 7.x	All the NetWare computers that are installed with NDS 7.x.

Table 3-54 Supported NetWare predefined target types *(continued)*

Target type	Description
NetWare Machines with NDS 8.x	All the NetWare computers that are installed with NDS 8.x.
All NetWare Servers	All NetWare Servers.

About NDS predefined target types

The NDS predefined target types are listed as follows:

Table 3-55 Supported NDS target types

Target type	Description
All NDS Trees	All the NDS trees

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 697.

See “About risk score” on page 175.About compliance

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.

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 695.

The risk calculations are based on the Common Vulnerabilities Scoring System version 2.

See "About risk score calculation" on page 702.

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 — The first digit in the versioning scheme represents the major version.

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.

Minor version — The second digit in the versioning scheme represents the minor version.

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.

Fix version — 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.

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 162.

See "About checks" on page 163.

See "About standards" on page 158.

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: ■ 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 261.

See “Customizing the filter options” on page 267.

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 1121.

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 669.

See “ Changing an ESM policy name at the check level ” on page 687.

List of standards

Following is the List of standards for the Control Compliance Suite11.0 version:

Table 3-56

Standard	Overview
CIS Oracle Database Server 11g Security Benchmark v1.0.1	The benchmark for Oracle Database Server 11g Security Benchmark v1.0.1 contains Consensus Baseline Security Settings for various database system components.
Security Essentials for Microsoft SQL Server 2008	The Security Essentials for Microsoft SQL Server 2008 document is derived from research conducted utilizing the SQL Server 2008 environment on Windows XP Desktops and Windows 2003 servers.
CIS Solaris Benchmark v4.0	The CIS Benchmark for Solaris evaluates systems against CIS Solaris 10 Benchmark v4.0 and provides compliance status and the hardening recommendations to improve security of Solaris systems.
Security Essentials for Red Hat Enterprise Linux	The Securing the Red Hat Enterprise Linux environment provides guidelines for securing Red Hat Enterprise Linux versions 2.1,3,4.0 and 5.0.
CIS Security Configuration Benchmark For Microsoft Windows Server 2008 v1.1.0	The CIS Security Configuration Benchmark for Microsoft Windows Server 2008 v1.1.0 evaluates systems and provides compliance status and recommendations to improve security of Windows 2008 systems.
CIS Oracle 9i and 10g Database Security Benchmark v2.0	The Center for Internet Security (CIS) publishes an Oracle 9i and 10g Database Security Benchmark v2.0 contains Consensus Baseline Security Settings for various database system components.
CIS Oracle Database Server 11g Security Benchmark v1.0.1	The Center for Internet Security (CIS) publishes an CIS Oracle Database Server 11g Security Benchmark v1.0.1 contains the Consensus Baseline Security Settings for various database system components.

Table 3-56 *(continued)*

Standard	Overview
CIS Security Configuration Benchmark for Microsoft SQL Server 2005 v1.1.1	The CIS Security Configuration Benchmark for Microsoft SQL Server 2005 v1.1.1 document is derived from research conducted utilizing the SQL Server 2005 environment on Windows XP Desktops and Windows 2003 servers. This document provides the necessary settings and procedures for the secure installation, setup, configuration, and operation of an MS SQL Server 2005 system. With the use of the settings and procedures in this document, an SQL Server 2005 database may be secured from conventional “out of the box” threats. Recognizing the nature of security cannot and should not be limited to only the application; the scope of this document is not limited to only SQL Server 2005 specific settings or configurations, but also addresses backups, archive logs, “best practices” processes and procedures that are applicable to general software and hardware security. The Level column indicates the following: - Level 1 settings are generally considered “safe” to apply to most systems. The use of these configuration recommendations is not likely to have a negative impact on performance or functionality unless otherwise noted in the Comments. - Level 2 settings provide a higher level of security, but will result in a negative impact to performance and functionality. It is extremely important to conduct testing of security configurations on non-production systems prior to implementing them on production systems.
Security Essentials for Microsoft SQL Server 2008	The Security Essentials for Microsoft SQL Server 2008 is based on the Security Essentials for Microsoft SQL Server 2008 Version 1.0 guidelines.

Table 3-56 *(continued)*

Standard	Overview
The Australian Government Information and Communications Technology Security Manual for MS-SQL Server	This Technical Standard Pack (TSP) contains checks for a set of baseline configuration parameters recommended by Australian Government Information and Communications Technology Security Manual.
Security Essentials for Red Hat Enterprise Linux	The Securing Essentials Red Hat Enterprise Linux environment contains many of the common challenges in the area of Unix security administration. The recommendations are applicable in most cases to Red Hat Enterprise Linux versions 2.1,3,4.0 and 5.0.
CIS Security Benchmark for HP-UX v1.3.1	The CIS HP-UX Benchmark v1.3.1 (for HP-UX 11.i) contains consensus baseline security settings for HP-UX systems.
CIS Solaris 10 Benchmark v4.0	The CIS Solaris Benchmark v4.0 (for Solaris 10 release) contains consensus baseline security settings for Solaris systems.
CIS VMware ESX Server 3.x Benchmark v1.0	The CIS VMware ESX Server 3.x Benchmark Version 1.0 contains consensus baseline security settings for VMware ESX Server 3.x systems.
Security Essentials for CIS VMware ESX Server 4.x	The Security Essentials for CIS VMware ESX Server 4.x contains compliance status and recommendations to improve security of VMware ESX Server 4.x systems.
Security Essentials for SuSE Linux Enterprise Server	The Security Essentials for SuSE Linux Enterprise Server contains a configuration benchmark for SuSE Linux 9.0 that defines the recommended security configurations for various operating system components.

Table 3-56 *(continued)*

Standard	Overview
Security Essentials for SuSE Linux Enterprise Server 10 and SuSE Enterprise Linux 11	TheSecurity Essentials for SuSE Linux Enterprise Server 10 and SuSE Enterprise Linux 11 provides compliance status and recommendations to improve security of Security Essentials for SuSE Linux Enterprise Server 10 and SuSE Enterprise Linux Server 11 systems.
CIS Benchmark for IIS 5.0 and 6.0 for Microsoft Windows 2000, XP and Server 2003 v1.0	The CIS Benchmark for IIS 5.0 and 6.0 for Microsoft Windows 2000, XP and Server 2003 v1.0 provides guidelines for securing IIS 5.0 and 6.0 for Microsoft Windows 2000 Server, XP, and Server 2003.
CIS Legacy Security Settings Benchmark for Windows 2003 Domain Controller v2.0	The Center for Internet Security (CIS) publishes a configuration benchmark for Windows Server 2003 domain Controller servers that defines Consensus Baseline Security Settings for various operating system components. CIS considers these recommended configurations safe for administrators of any security skill level to implement. The CIS Legacy Security Settings Benchmark for Windows 2003 Domain Controller v2.0 includes legacy recommendations for Windows Server 2003 Domain Controller systems that consists of four major categories: ■ Additional Security Protection ■ Auditing and Account Policies ■ Microsoft Service Packs and Security Updates ■ Security Settings To harden Windows Server 2003 security for domain controller servers, networks should at a minimum comply with the recommendations published by CIS.

Table 3-56 *(continued)*

Standard	Overview
CIS Legacy Settings Benchmark for Windows XP Professional v2.01	The Center for Internet Security (CIS) publishes a configuration benchmark for Windows XP Professional that defines Consensus Baseline Security Settings for various operating system components. CIS considers these recommended configurations as safe for administrators of any security skill level to implement. The CIS Legacy Settings Benchmark for Windows XP Professional v1.3.0 includes recommendations for Windows XP Professional Legacy systems that consists of four major categories: ■ Additional Security Protection ■ Auditing and Account Policies ■ Microsoft Service Packs and Security Updates ■ Security Settings To harden Windows XP Professional security for Legacy workstations, networks should comply with the recommendations published by CIS.
CIS Security Configuration Benchmark For Microsoft Windows Server 2008 v1.1.0	The CIS Security Configuration Benchmark For Microsoft Windows Server 2008 v1.1.0 evaluates systems and provides compliance status and recommendations to improve security of Windows 2008 systems.
CIS Security Configuration Benchmark For Windows 7 v1.1.0	The CIS Security Configuration Benchmark For Windows 7 v1.1.0 contains checks for security settings and recommendations.

Table 3-56 *(continued)*

Standard	Overview
CIS Windows 2000 Server Operating System Level Two Benchmark for Stand-alone and Member Servers v2.2.1	The Center for Internet Security (CIS) publishes a configuration benchmark for Windows 2000 stand-alone and member servers that defines Consensus Baseline Security Settings for various operating system components. CIS considers these recommended configurations safe for administrators of any security skill level to implement. The CIS Windows 2000 Server Operating System Level Two Benchmark for Stand-alone and Member Servers v2.2.1 consists of four major categories: ■ Additional Security Protection ■ Auditing and Account Policies ■ Microsoft Service Packs and Security Updates ■ Security Settings To harden Windows 2000 Server security for stand-alone and member servers, networks should comply with the recommendations published by CIS.

Table 3-56 *(continued)*

Standard	Overview
CIS Windows Server 2003 Legacy Security Settings for Domain Member Servers v2.0	The Center for Internet Security (CIS) publishes a configuration benchmark for Windows Server 2003 domain member servers that defines Consensus Baseline Security Settings for various operating system components. CIS considers these recommended configurations safe for administrators of any security skill level to implement. The CIS Windows Server 2003 Legacy Security Settings for Domain Member Servers v2.0 includes legacy recommendations for Windows Server 2003 systems that consists of four major categories: ■ Additional Security Protection ■ Auditing and Account Policies ■ Microsoft Service Packs and Security Updates ■ Security Settings To harden Windows Server 2003 security for domain member servers, networks should at a minimum comply with the legacy recommendations published by CIS.
Security Essentials for Windows Server 2008 R2	The Security Essentials for Windows Server 2008 R2 evaluates systems and provides compliance status and recommendations to improve security of Windows 2008 R2 systems.
The Australian Government Information and Communications Technology Security Manual for Windows	This Technical Standard Pack (TSP) contains checks for a set of baseline configuration parameters recommended by Australian Government Information and Communications Technology Security Manual.

Table 3-56 *(continued)*

Standard	Overview
US Federal Desktop Core Configuration Standard (FDCC) V1.0.1 for Windows Vista	The US Federal Desktop Core Configuration Standard (FDCC) V1.0.1 for Windows Vista contains a set of baseline configuration parameters for Microsoft Windows Vista systems.

See "About standards" on page 158.

See "About predefined standards" on page 158.

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 186.
- Check expression
  See "Check expression" on page 188.
- Preconditions
  See "Preconditions" on page 187.
- Check formula
  See "Check formula" on page 188.
- Data Items filter
  See "Data Items filter " on page 189.
- Missing data items
  See "Missing data items" on page 189.
- Multiple data items
  See "Multiple data items" on page 190.
- Check risk attributes
  See "Check risk attributes" on page 191.

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 197.

The syntax for a field expression is as follows:

<Field><Operator><Value>

The following table lists some examples of a field expression:

Table 3-57 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 163.

See "Concepts in checks" on page 186.

See "Check expression" on page 188.

See "Creating a new check" on page 682.

See "Check Advanced Settings" on page 194.

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 163.

See “Concepts in checks” on page 186.

See “Creating a new check” on page 682.

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 186.
- Data Items filter (optional)
  See “Data Items filter ” on page 189.

See “About checks” on page 163.

See “Concepts in checks” on page 186.

See “Creating a new check” on page 682.

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 188.
- Multiple check expressions that are connected by the use of check formula operators.
  See “Check formula operators” on page 199.

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 163.

See “Concepts in checks” on page 186.

See “Check Advanced Settings” on page 194.

See “Creating a new check” on page 682.

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 186.

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 194.

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 163.

See “Concepts in checks” on page 186.

See “Creating a new check” on page 682.

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 194.

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 163.

See "Concepts in checks" on page 186.

See "Creating a new check" on page 682.

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 194.

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 200.

See "About checks" on page 163.

See "Concepts in checks" on page 186.

See "Creating a new check" on page 682.

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	The attacker is required to authenticate two or more times to exploit the vulnerability. The same credentials may be used each time. The corresponding weight that is assigned to this value is 0.45
Single Instance	The attacker needs to log into the system such as at a command line or through a desktop session or Web interface. The corresponding weight that is assigned to this value is 0.56.
No Authentication	Authentication is not required to exploit the vulnerability. The corresponding weight that is assigned to this value is 0.704

See "About checks" on page 163.

See "About risk score calculation" on page 702.

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 this table equivalent to a category in an evaluation condition.

Table 3-58 contains the following fields and values:

Table 3-58 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 163.

See “Concepts in checks” on page 186.

See “Creating a new check” on page 682.

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 197.
- Check formula operators
  See “Check formula operators” on page 199.

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 3-59 lists the descriptions of the available field expression operators.

Table 3-59 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.
!~	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.

Table 3-59 Field expression operators *(continued)*

Operator	Operator Name	Expression using sample values A, B, and the operator	Description
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 197.

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 200.

See "Operator NOT" on page 201.

See "Operators IF, THEN, ELSE" on page 201.

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 197.

See "Concepts in checks" on page 186.

Operators AND and OR

The AND and OR operators are used to connect two or more check expressions in a check formula.

Table 3-60 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 3-60 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
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

Table 3-60 Use of AND and OR operators *(continued)*

If A equals	If B equals	Then A AND B equals	Then A OR B equals
MANUAL REVIEW	FAIL	FAIL	MANUAL REVIEW
MANUAL REVIEW	MANUAL REVIEW	MANUAL REVIEW	MANUAL REVIEW

See “Check formula operators” on page 199.

See “About operators” on page 197.

Operator NOT

The NOT operator can be used in a check formula.

Table 3-61 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 3-61 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 199.

See “About operators” on page 197.

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 199.

See "About operators" on page 197.

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

See "Working with standards" on page 654.

Concepts in SCAP Content

Before you work with SCAP Content, that includes SCAP benchmarks and OVAL definitions, you must read through SCAP-related concepts.

The SCAP-related concepts are covered in the following topics:

- About SCAP content in CCS
  See "About SCAP content in CCS" on page 203.

- About supported SCAP specifications in CCS
  See "About supported SCAP specifications in CCS" on page 205.
- About supported SCAP capabilities in CCS
  See "About supported SCAP capabilities in CCS" on page 204.
- About usage of XCCDF in CCS
  See "About usage of XCCDF in CCS" on page 205.
- About usage of CCE in CCS
  See "About usage of CCE in CCS" on page 206.
- About usage of CVE-CVSS in CCS
  See "About usage of CVE in CCS" on page 207.
- About usage of CVSS in CCS
  See "About usage of CVSS in CCS" on page 207.
- About usage of CPE in CCS
- About usage of OVAL in CCS
  See "About usage of OVAL in CCS" on page 208.
- About the supported OVAL objects in CCS
  See "About the supported OVAL objects in CCS" on page 209.

About SCAP content in CCS

CCS adopted the Security Content Automation Protocol (SCAP) which is a method for using specific standards that are defined by the National Institute of Standards and Technology (NIST). SCAP uses the standards to enable automated vulnerability management, measurement, and policy compliance evaluation of the enterprise organization.

SCAP is a suite of specifications that standardize the format and nomenclature by which security software products communicate software flaws and security configuration information. Adoption of SCAP facilitates an organization's automation of security monitoring, vulnerability management, and security policy compliance evaluation and reporting.

For more details on SCAP, refer to http://scap.nist.gov/

CCS supports implementation of SCAP 1.0 specification.

The SCAP 1.0 specification comprises the following six component specifications:

- eXtensible Configuration Checklist Description Format (XCCDF) v1.1.4
- Open Vulnerability and Assessment Language (OVAL) v5.3
- Common Platform Enumeration (CPE) v2.2

- Common Configuration Enumeration (CCE) v5
- Common Vulnerabilities and Exposures (CVE)
- Common Vulnerability Scoring System (CVSS) v2

CCS facilitates import of SCAP content that you download from the Website of NIST, http://fdcc.nist.gov/download.cfm. The content that you import into CCS cannot be edited. CCS lets you leverage the in-built functionality to execute the SCAP evaluation job that collects data from assets and evaluates them against the SCAP content. The Data Processing Service (DPS) that is configured as a Windows data collectort performs the task of data collection and evaluation of SCAP content.

After data evaluation completes, use the report generation feature of CCS to generate the Asset Details report for the SCAP evaluation results. The evaluated data are also rendered on CCS dashboards such as, Compliance Administration - SCAP profile benchmark.

See "About import of SCAP benchmarks into CCS" on page 743.

See "Viewing the imported SCAP benchmarks in CCS" on page 748.

See "Evaluating assets against the SCAP benchmarks" on page 750.

See "Generating reports of the SCAP evaluated results" on page 759.

See "Accessing dashboards of SCAP benchmarks" on page 759.

About supported SCAP capabilities in CCS

CCS uses few of the SCAP capabilities that are defined by NIST.

The SCAP capabilities that CCS supports are as follows:

- FDCC Scanner
  The capability to audit and assess a target computer to determine its compliance with the FDCC requirements.
- Authenticated Configuration Scanner
  The capability to audit and assess a target computer to determine its compliance with a defined set of configuration requirements using the logon privileges.
- Authenticated Vulnerability and Patch Scanner
  The capability to scan a target computer to locate and identify the presence of known vulnerabilities and evaluate the software patch status. The patch status is evaluated to determine the compliance with a defined patch policy using the target computer's logon privileges.

CCS also has the capability to collect and evaluate data from the target computers that have remote registry service disabled or unavailable.

See "About supported SCAP specifications in CCS" on page 205.

About supported SCAP specifications in CCS

CCS adheres to the SCAP 1.0 specification to govern the risk and the compliance posture of the enterprise network.

Refer to the Web site, http://scap.nist.gov/revision/1.0/index.html for details about the SCAP 1.0 specification.

The standards of SCAP 1.0 specification and their descriptions are as follows:

Standard	Description
Extensible Configuration Checklist Description Format (XCCDF 1.1.4)	An Extensible Markup Language (XML) specification for the structured collections of security configuration rules. The operating system (OS) and the application platforms uses these rules.
Open Vulnerability and Assessment Language (OVAL - 5.3)	An XML specification for exchanging the technical details on how to check systems for security-related software flaws, configuration issues, and patches.
Common Configuration Enumeration (CCE - 5.0)	A dictionary of names for software security configuration issues such as access control settings and password policy settings.
Common Platform Enumeration (CPE - 2.2)	A naming convention for hardware, operating system, and application products
Common Vulnerability Scoring System (CVSS - 2.0)	A method for classifying characteristics of software flaws and assigning severity scores that are based on these characteristics.
Common Vulnerabilities and Exposures (CVE - no version)	A dictionary of names for the security-related software flaws.

See "About supported SCAP capabilities in CCS" on page 204.

About usage of XCCDF in CCS

The eXtensible Configuration Checklist Description Format (XCCDF v1.1.4) is an XML specification and language that provides a common framework for developing security checklists and benchmarks. The National Institute of Standards and Technology (NIST) hosts and maintains the XCCDF specification and language.

For more details about XCCDF, refer to http://scap.nist.gov/specifications/xccdf

The SCAP v1.0 specification requires an SCAP benchmark to use an XCCDF document to define the checklist or benchmark of an SCAP data stream.

CCS supports XCCDF as part of an SCAP v1.0 data stream. During import of the SCAP data stream, CCS validates the XCCDF document against the official XCCDF schema. If an XCCDF benchmark contains multiple profiles, then CCS imports all the profiles.

CCS uses XCCDF specification in the following manner:

- Imports XCCDF v1.1.4 as part of the SCAP data stream
  See "Importing SCAP data stream into CCS" on page 744.
- Evaluates the assets against the XXCDF benchmarks through the SCAP evaluation job execution.
  See "Evaluating assets against the SCAP benchmarks" on page 750.
- Displays the evaluation results in the **Evaluation Results** view of the console.
- Exporting the evaluation results in the following formats:
  - XCCDF
  - FDCC XCCDF

See "Concepts in SCAP Content" on page 202.

About usage of CCE in CCS

Common Configuration Enumeration v5 (CCE) is a standard that defines a common identification for computer security configuration issues and exposures. The Mitre Corporation, whose Web site, http://cce.mitre.org, hosts and maintains the CCE standard. The standard is officially maintained as a CCE list, which in the XML format. The CCE list provides all currently identified CCE identifiers (IDs), a description, and references for more information.

CCS lets you import the CCE v5 XML list and store them in the database. CCS also provides the CCE IDs, which the SCAP content or OVAL content references in the evaluation result details of the SCAP or OVAL content. The CCS SCAP evaluation details let you search asset or evaluation results for specific CCE IDs.

CCS uses CCE standard in the following manner:

- Imports the CCE list independent of the SCAP data stream.
  See "Importing CCE list into CCS" on page 744.

- Displays the CCE IDs in the evaluation results.
- Exports the evaluation results that also contain the CCE ID details.

See "Concepts in SCAP Content" on page 202.

About usage of CVE in CCS

Common Vulnerabilities and Exposures (CVE) is a standard that defines a common identification and dictionary for computer and information security vulnerabilities. The Mitre Corporation, whose Web site is http://cve.mitre.org, hosts and maintains the CVE standard.

The National Vulnerability Database (NVD) publishes the vulnerability summaries that provide detailed information for most known computer and information security vulnerabilities. These vulnerability summaries can be accessed using the CVE identifier (IDs) for a given vulnerability.

CCS lets you import the CVE 2.0 list and store them in the database. CCS also provides the CVE IDs, which the SCAP or OVAL content references in the evaluation result details of the SCAP or OVAL content. The evaluation result details provide link to the NVD vulnerability summaries for the CVE IDs. You can also use the **Search** option of the **SCAP Evaluation Result Details** dialog box to search the CVE IDs in the generated evaluation results.

CCS uses CVE standard in the following manner:

- Imports the CVE list independent of the SCAP data stream.
  See "Importing CVE-CVSS list into CCS" on page 745.
- Displays the CVE IDs in the evaluation results.
- Exports the evaluation results that also contains the CVE ID details.

See "Concepts in SCAP Content" on page 202.

About usage of CVSS in CCS

CVSS v2 (Common Vulnerability Scoring System) is a standard that is defined by the Forum of Incident Response and Security Teams (FIRST). FIRST, whose Web site is http://www.first.org/cvss, defines methods for scoring and rating the computer vulnerabilities. The National Vulnerability Database (NVD) defines and publishes the CVSS base scores and vector strings for the most known vulnerabilities.

NVD publishes the vulnerability summaries that provide detailed information, which includes the CVSS base score and vector strings. These vulnerability summaries can be accessed using the CVE (Common Vulnerabilities and Exposures) identifier (ID) for a given vulnerability.

CCS lets you import the CVE 2.0 and store the CVSS base scores and vector string data in the database. Links to the NVD vulnerability summaries through the CVE IDs are displayed for the SCAP evaluation result details.

CCS uses the CVE-CVSS standard in the following manner:

- Imports the CVE list independent of the SCAP data stream.
  See "Importing CVE-CVSS list into CCS" on page 745.
- Displays the evaluation results in the **Evaluation Results** view of the console.
- Exports the evaluation results.

See "Concepts in SCAP Content" on page 202.

See "About risk and compliance score calculation for SCAP assets" on page 753.

About usage of OVAL in CCS

Open Vulnerability and Assessment Language v5.3 (OVAL) is used to express standardized, machine-readable rules that can be used to assess the state of a system. Under SCAP, OVAL is commonly used to determine the presence of vulnerabilities and insecure configurations. A set of instructions used to check for a security problem, such as an incorrect minimum password length setting, is known as an OVAL Definition. A file containing one or more OVAL Definitions (often hundreds or even thousands) is known as an OVAL Definition file. The Mitre Corporation, whose Web site is http://cpe.mitre.org hosts and maintains OVAL.

The SCAP v1.0 specification requires that an SCAP benchmark use OVAL for both compliance definitions and for inventory checks within a CPE OVAL file. An SCAP benchmark can also contain an OVAL patch file that evaluates an asset for patch compliance. OVAL files can also be used to evaluate an asset independently without the need for an SCAP data stream. CCS supports both OVAL as part of an SCAP v1.0 data stream, as well as stand-alone OVAL definition evaluations.

CCS provides full support for OVAL definitions on Microsoft Windows XP and Microsoft Vista operating systems. During import of the SCAP data streams or stand-alone OVAL definition files, the OVAL definition files are validated against the official OVAL schema and schematrons. If validation errors result during validation of the OVAL definitions, then CCS reports them. After you execute an SCAP evaluation job or an SCAP OVAL evaluation job, CCS lets you export the OVAL definitions. The OVAL definitions can be exported as OVAL Thin or OVAL Full results.

CCS uses stand-alone OVAL in the following manner:

- Imports the OVAL definition file.
  See "Importing OVAL definitions" on page 746.

- Evaluates the assets against OVAL.
  See "Evaluating assets against OVAL definitions" on page 752.
- Displays the evaluation results in the **Evaluation Results** view of the console.
- Exporting the evaluation results.

See "About SCAP content in CCS" on page 203.

About the supported OVAL objects in CCS

To support the SCAP capability, Authenticated vulnerability and patch scanner, CCS supports all OVAL objects for the Windows definition file of OVAL 5.3 schema. CCS also supports the independent definition file of OVAL 5.3 schema.

CCS supports the following OVAL objects in the product:

- accesstoken_object
- activedirectory_object
- auditeventpolicy_object
- auditeventpolicysubcategories_object
- file_object
- fileauditedpermissions53_object
- fileauditedpermissions_object
- fileeffectiverights53_object
- fileeffectiverights_object
- group_object
- interface_object
- lockoutpolicy_object
- metabase_object
- passwordpolicy_object
- port_object
- printereffectiverights_object
- process_object
- registry_object
- regkeyauditedpermissions53_object
- regkeyauditedpermissions_object

- regkeyeffectiverights53_object
- regkeyeffectiverights_object
- sharedresource_object
- sid_object
- uac_object
- user_object
- volume_object
- wmi_object
- filemd5_object
- filehash_object
- environmentvariable_object
- textfilecontent_object
- xmlfilecontent_object

About External Data Integration

External data integration lets you seamlessly assimilate data from an external application to Control Compliance Suite (CCS). The external data is represented as a data schema in CCS. You can use this data schema for the following purposes:

- Assess the Policy Compliance:
  You can use the imported data to correlate with the CCS assets. You can then gauge the compliance over the assets based on policies, mandates, and regulations.
  See "Policy compliance in correlation with CCS assets" on page 804.
- Contribute to CCS Asset Risk Score:
  A risk score is used to quantify the risk that is associated with an asset in your organization. You can import external data and use it for contributing to the CCS asset risk score.
  See "Contributing to the CCS asset Risk Score" on page 805.
- View Dynamic Dashboards and Reports:
  You can view external data in the CCS dashboards in the following ways:
  - You can import external data and view the data using CCS dashboards without correlating the external data to CCS assets.

  - You can import external data and view the data using CCS dashboards in correlation with the CCS assets. By means of correlation, you basically establish an association between the imported data schema and the existing CCS assets. CCS provides you with the capability to define new schema, which you can map to a CCS schema by matching attributes.

  See “Viewing the data in dashboards” on page 807.

- Correlate data with CCS:

  Data correlation lets you establish an association between the data fields in the imported data and the CCS data.

  See “Correlating data with CCS” on page 809.

- Reconcile assets:

  You can use the reconciliation rules to add new assets, update existing asset fields and update the data schema.

  See “Reconciling assets based on external system data” on page 811.

Before you import data, you must identify the data that you want to import into CCS. This data is represented in CCS as a data schema. You may use an existing schema to import data, or create a new data schema for first-time import. This data schema may then be used for any of the purposes that are mentioned above.

CCS represents imported data in terms of the following three attributes of the data schema:

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.
Assessment	A statement that tests a condition for an asset, such as a test if passwords have a certain length.
Status	A status is the outcome or the resultant value of an assessment.

The data schema is comprised of Asset , Asessment and Status, or Asset and Status.

CCS provides pre-integrated solutions for:

- Vulnerability assessment
- Response assessment
- Data loss assessment

To import external system data, you need to first add the external system to the Control Compliance Suite and create a data connection.

See “Configuring data systems” on page 761.

See “Configuring data connections” on page 773.

You must have appropriate permissions to integrate external data.

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 890.

See “Viewing the comparison results in the Baselines view” on page 892.

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 895.

See "Creating a new tag" on page 896.

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 can 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 may also 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 902.
- Review the policy.
  See "Reviewing a policy" on page 916.

- Approve the policy.
  See “Approving a policy” on page 917.
- Publish the policy.
  See “Publishing a policy” on page 911.
- Manage clarifications.
  See “Managing clarification requests” on page 914.

About policy versioning

Every policy has a version number assigned. The version number is assigned and incremented automatically during the policy life cycle. Most policy life cycle events are specific to a particular policy version number.

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.

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.

Approved
When a policy is approved, it is approved with the current version number.

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.

See “About policies” on page 213.

See “About the policy life cycle” on page 213.

See “About policy status” on page 215.

About policy status

Every policy has a status that is assigned to it at all times.

The status is one of the following:

Draft

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.

Also, a policy that has been reviewed but which has change requests, or a policy that has been unpublished.

Policies can only be edited while in Draft status.

In Review

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.

Pending Approval

A policy that may or may not have reviewer comments. If a policy does not have change requests from reviewers, the status changes to Pending Approval. The status changes automatically when the review deadline that was set during the policy creation passes.

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.

Approved

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.

Published

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 Console. The policy audience includes all the users assigned to the Policy Audience role in the CCS Console who also have permission to access the policy.

Archived

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.

Note: 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**.

See “About policies” on page 213.

See “About the policy life cycle” on page 213.

See “About policy versioning” on page 214.

See “About policy approval” on page 217.

See “About policy review” on page 216.

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 Controls Studio to map policies to control statements.

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.

Note: You must explicitly assign users to the **Policy Reviewers** role. No users are assigned to this role by default, including the **CCS Administrator**.

See "About the policy life cycle" on page 213.

See "About policy status" on page 215.

See "Submitting a policy for review" on page 907.

See "Submitting a policy for review and approval" on page 909.

See "Reviewing a policy" on page 916.

See "Viewing the reviewer comments" on page 916.

About policy reviewers

Any user who is assigned to the **Policy Reviewer** role who also has permission to access the policy is a policy reviewer for the policy. Every policy reviewer must review the policy before it can be approved. The policy reviewer can comment on policies or request a change before they agree with the statement of the policy.

Policy reviewers can use the Control Compliance Suite Console or the Control Compliance Suite Web Console to review policies.

The Control Compliance Suite notifies each affected policy reviewer when a policy is submitted for review.

See "About the policy life cycle" on page 213.

See "About policy review" on page 216.

About policy approval

The policy approval feature helps you stage the release of your policies. All policies must be approved before they are eligible for publishing. You can centralize the policy approval process, with authority to approve the policies granted to select users who are responsible for the policies.

The policy approvers must have both the Policy Approver role and permission to access the policy.

When a policy is ready for approval, the policy administrator marks the status as Reviewed. The Control Compliance Suite notifies the approver about the policy. The policy approver can use the Control Compliance Suite Console to approve the policy.

Note: You must explicitly assign users to the **Policy Approvers** role. No users are assigned to this role by default, including the **CCS Administrator**.

See "Approving a policy" on page 917.

See "About the policy life cycle" on page 213.

See "Submitting a policy for approval" on page 908.

See "Submitting a policy for review and approval" on page 909.

About policy approvers

Any user who is assigned to the **Policy Approver** role who also has permission to access the policy is a policy Approver for the policy. A policy approver can approve and publish the policy when all reviewers have reviewed the policy and all change requests have been addressed. Policy approvers can use the Control Compliance Suite Console or the Control Compliance Suite Web Console to approve policies.

The Control Compliance Suite notifies each affected policy approver when a policy is submitted for approval.

See "About the policy life cycle" on page 213.

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.

To make changes to the content of the policy, you must download the policy document, edit the document and attach the document again.

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.

See "Working with policies" on page 902.

See "Editing a policy" on page 905.

See "Deleting a policy" on page 906.

See “Moving, copying, and pasting a policy” on page 907.

About using policies

When you create a policy, you can assign an audience to the policy.

The policy audience uses the Control Compliance Suite (CCS) Web Console to do the following:

- Accept the policy.
- Decline the policy.
- Request a clarification of the policy.
- Request an exception to the policy.
- Review the status of clarification and exception requests.
- Review administrator responses to the clarification and exception requests.

When a policy is published, the CCS sends an email notification to the members of the policy audience. In addition, if an audience member requests a clarification, the CCS notifies the requestor when the policy administrator responds to the request.

About clarifications

The clarification feature lets members of the policy audience request any clarification on the policies that they have questions about, using the Control Compliance Suite Web Console home page. More than one clarification request can be made to a policy. Users can view the status of the clarification requests that they have made. When the policy administrator responds to the request, the user can view the response as well..

The following clarification statuses exist:

Open	A clarification request that is submitted, but for which no response exists
Closed	A policy administrator has responded

See “Managing clarifications” on page 913.

See “Managing clarification requests” on page 914.

About custom content

The Symantec Controls Studio lets you customize content to fit the needs of your enterprise. The custom control statements and the custom mandates help you create the policies that suit the regulatory environment that your enterprise must inhabit. You use the Controls Studio to map Symantec-created control statements and custom control statements to the custom mandates that you create and to your policies. You also map any of the control statement to checks, questions, or extended controls. You can also use the Controls Studio to analyze your policies to help understand the scope of your policy coverage.

The Controls Studio includes a large number of Symantec-created control statements. In addition, the Controls Studio lets you create your own control statements. Any control statements can be mapped to the regulations or frameworks that you create. You can also map control statements to any Control Compliance Suite (CCS) policy in the **Draft** state. The Controls Studio also lets you map control statements to checks, to questions from the Response Assessment module or to extended controls.

When you use Controls 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 checks, questions, and extended controls to control statements. Next, you map the control statements to the regulations or frameworks that you created. Then you map the control statements to your draft policies and perform policy analysis.

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 control statements to checks, questions, and extended controls.
- Map policies to control statements.

See “Creating custom content” on page 1009.

About Symantec Controls Studio

The Symantec Controls 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 Controls Studio to map mandates and policies to control statements and control statements to checks, questions, and extended controls. Mappings link the regulations and frameworks that affect your enterprise, the policies you create to meet those mandates, and the underlying control statements, checks, questions, and extended controls.

You use the Controls 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 or to the CCS policies. You can also map control statements to checks, to questions from the Response Assessment module or to extended controls.

After you have created your custom content, you can use this content in CCS.

When you use the Controls 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 the regulations or frameworks you created to the control statements. You then map the control statements to the checks, questions, and extended controls. Finally, you create the new policies that match the mandates you use and map the control statements to those policies.

See “About custom content” on page 220.

See “Creating custom content” on page 1009.

About mandates

A mandate is a regulation or framework with which you must comply. The Symantec Controls Studio includes predefined mandates you can use as a model for your custom mandates. The Controls Studio also lets you create the custom mandates that fit your specific needs. You can also map custom mandates to Symantec-created or custom control statements in the Controls Studio. Any regulation or framework is a mandate.

You can activate or deactivate a mandate as per your organizational requirements. Only an active mandate is taken into consideration for metric calculation for Policy Manager, reports, and dashboards. However, when you deactivate a mandate, the entry of the mandate is not deleted from the reporting database. An inactive mandate is still used for the trending panels.

You can activate or deactivate a mandate by selecting the relevant option from the right-click menu. The right-click menu also contains the options to view all the mandates or only the active mandates in your organization.

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 Controls 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 name of the user who created the mandate. The author for all Symantec-created content is “Symantec.” The author for all custom content is the name of the 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.

You can perform the following tasks by right-clicking a mandate:

Open in a new window	Lets you open the selected regulation or framework in a new window.
New Regulation	Lets you create a new regulation.
New Framework	Lets you create a new framework.
New Section	Lets you create a new section.
Delete	Lets you delete the selected regulation or framework.
Filter	Lets you choose which mandate you want to be displayed.
Expand All	Lets you expand all the mandates.
Collapse All	Lets you collapse all the mandates.
Show All	Lets you view all the mandates.
Show Active Only	Lets you view only the active mandates.
Activate	Lets you activate the selected mandate.
Deactivate	Lets you deactivate the selected mandate.

See “About custom content” on page 220.

See “Creating custom content” on page 1009.

See “Modifying the details of a custom mandate or section” on page 1011.

See “Mapping mandates to control statements” on page 1015.

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

See "About frameworks" on page 224.

See "About mapping policies" on page 216.

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

See "About regulations" on page 223.

About 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 mandate, policy, check, question, or extended control. Policies and mandates are mapped to control statements. In turn, control statements are mapped to checks, questions, and extended controls.

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.

See "About custom content" on page 220.

See "Creating custom content" on page 1009.

See "Mapping mandates to control statements" on page 1015.

See "Mapping policies to control statements" on page 1017.

See "Mapping checks to control statements" on page 1019.

See "Mapping questions to control statements" on page 1021.

See "Viewing the control statements mapped to a regulation, framework, or policy " on page 1024.

About Controls Framework

Controls Framework provides you the means to organize all the control statements in a logical structure. Using controls framework you can group the control statements in the form of control categories and controls.

In Control Compliance Suite (CCS) a set of predefined control categories and controls are available. Relevant control statements are mapped to controls.

You can also create new control categories and controls based on your specific requirements.

In CCS the controls framework is explained as follows:

- Controls framework contains one or more control categories.
- A control category contains one or more controls.
- A control is mapped to one or more control statements.

About Control Categories

Control categories are used to organize or group related controls. A control category can have one or more than one predefined or custom controls.

You can perform the following tasks on control categories:

- Create a new controls.
- Delete a custom control category. Predefined control categories cannot be deleted.
- Search for components in the controls framework.

About Controls

Controls are used to organize and group control statements. One or many control statements can be mapped to a control.

You can perform the following tasks on controls:

- Map control statements to controls.
- Delete a custom control. Predefined controls cannot be deleted.
  A control cannot be deleted if even one control statement is mapped to that control.
- Move a control from one control category to another control category.
- Search for components in the controls framework.

About jobs

A job is a specified set of operations. Various components of Control Compliance Suite perform these operations sequentially. 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.

A job run is a particular instance of any job execution. Expand a job in the table pane to see its job run.

Control Compliance Suite provides the following operations on jobs:

- Create a job
  See "Creating jobs" on page 1046.
- Edit a job
  See "Editing a job" on page 1042.
- Run a job now
  See "Running a job now" on page 1044.
- Schedule a job
  See "Scheduling jobs" on page 1043.
- Delete a job
  See "Deleting jobs" on page 1043.
- Configure desktop notification for a job
- Refresh the jobs view
  See "Refreshing the jobs view" on page 1045.
- Cancel a job
  See "Canceling a job run" on page 1057.
- Delete a job run
  See "Deleting a job run" on page 1058.

Select any job and right-click it to see the menu with operations available for the job. The options available are specific to the job type. Use the check boxes to select multiple jobs.

The taskbar and the menu bar under the Tasks menu also provide the same options. Check a check box to enable the tasks.

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. Use **Settings** > **General Settings** to make these changes. 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 a job name:

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

See " About job types" on page 227.

See "About job filters" on page 1039.

About job types

The jobs that Control Compliance Suite automatically creates are known as System jobs. System jobs perform certain predefined functions. Some of the System jobs may be hidden.

User-defined jobs are the jobs that users create.

Control Compliance Suite provides the following types of jobs:

Asset import	The Asset import job imports assets. You can also add assets in the hierarchy through the job, which helps you to manage the assets. See "About Asset import job" on page 1032.
Baseline job	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. See "About Baseline job" on page 1033.
Entitlement import	The Entitlement import job fetches the entitlements for a particular control point. See "About Entitlement import job" on page 1034.

Automatic entitlements import

The Automatic entitlements import job is created during installation. This job fetches the entitlements for the import-required control points.

See "About Automatic entitlements import job" on page 1033.

Report generation

The Report generation job creates different types of reports.

See "About Report generation job" on page 1037.

Tiered dashboard update

The Tiered dashboard update job updates an existing Tiered dashboard by means of the Edit Tiered Dashboards wizard.

See "About Tiered dashboard update job" on page 1039.

Report data synchronization

The Report data synchronization job synchronizes the production database with the reporting database.

See "About Report data synchronization job" on page 1037.

Report data purge

The Report data purge job purges data from the reporting database.

See "About Report data purge job" on page 1036.

Global Metrics and Trend Computation Job

The Global Metrics and Trend Computation job is a system job that computes metrics for standards, policies, and mandate-specific rollups that dashboards use on the Web console.

To know more about the job See "About Global metrics and trend computation job" on page 1031.

Note: The Global Metrics and Trend Computation job now replaces the Policy and Mandates Metrics Computation job .

Queries

Queries collect data about the objects in your network. Run a predefined or custom query to get data for the parameters that you configure.

See "About Queries job" on page 1032.

Queries baseline

A query baseline job compares the results of two selected query runs. The older run acts as the baseline for the comparison.

Evaluation

The Evaluation job evaluates a standard or a set of standards against the assets or the assets group, or the assets folder.

See "About evaluation jobs" on page 164.

Perform data collection before you run an Evaluation Job.

See "About remediation" on page 533.

Data collection

The Data collection job collects required data for a standard or a set of standards. The job collects the data against the assets or the assets group, or the assets folder.

See “About data collection jobs” on page 163.

Collection-Evaluation-Reporting

The collection-evaluation-reporting job lets you create a chained job. The job collects data for a set of assets, evaluates the assets, and generates reports for those assets.

You can also schedule to remediate the assets automatically at the end of the evaluation.

See “Running a collection-evaluation-reporting job from the Standards view” on page 663.

Remediation verification

The remediation verification job recollects and reevaluates the asset data after the remediation action is taken on the assets.

See “About Remediation verification job” on page 1036.

SCAP evaluation

The SCAP evaluation job lets you evaluate assets against the SCAP Benchmarks. The SCAP benchmarks comprise a set of rules that NIST predefines.

See “About SCAP evaluation job” on page 1038.

SCAP OVAL evaluation

The SCAP OVAL evaluation job lets you evaluate a valid OVAL Definition file against the SCAP Benchmarks.

See “About SCAP OVAL evaluation job” on page 1039.

Automatic updates installation

The Automatic updates installation job automatically installs the CCS updates on the CCS components in a particular sequence.

See “About Automatic updates installation job” on page 1032.

External data integration

The External data integration job collects data from the third-party systems that have been integrated with Control Compliance Suite.

See “About External data integration job” on page 1035.

Import assets and agents

The Import assets and agents job imports the agents that are registered with the CCS Manager and the assets associated with these agents.

See “About Import assets and agents job” on page 1035.

See “About jobs” on page 226.

See “Creating jobs” on page 1046.

Concepts in routing rules

CCS introduces a new functionality called routing rules, which allows you to define a particular site or CCS manager to perform tasks that are related to assets.

A few tasks that you can manage with routing rules are as follows :

- Agent tasks such as remote upgrade and retrieving agent logs
- SCAP collection and evaluation
- Host cache refresh

See “Routing rules based on IP address range” on page 230.

See “Routing rules based on subnet ” on page 231.

See “Routing rules based on expression” on page 231.

See “Routing rules based on asset groups” on page 233.

See “Routing rules based on active directory site” on page 234.

See “Scope in routing rules ” on page 234.

See “About resolving IP addresses” on page 235.

See “Routing rules evaluation ” on page 236.

Routing rules based on IP address range

You can create rules based on the IP address range. The jobs for the assets that are found within a specified range are routed to the CCS manager or site that you specify in the rule.

Consider this example, you want to performa job on the assets that are on different floors in your organization.

10.216.40.1 - 10.216.47.254	CCS Manager 1
10.216.96.1 - 10.216.103.254	Site A

You can define IP address range routing rules for the jobs as follows:

- Route jobs for the assets that fall within 10.216.40.1 - 10.216.47.254 to CCS Manager 1.
- Route jobs for the assets that fall within 10.216.96.1 - 10.216.103.254 to Site A.

See “Routing rules based on subnet ” on page 231.

See “Routing rules based on expression” on page 231.

See “Routing rules based on asset groups” on page 233.

See “Routing rules based on active directory site” on page 234.

See “Creating routing rules based on IP address range” on page 1069.

Routing rules based on subnet

You can create rules based on the subnet ID and subnet mask. The jobs for the assets that have a specified subnet ID and subnet mask are routed to the CCS manager or site that you specify in the rule.

Consider this example, you want to perform a job on the assets that are on different subnets in your organization.

Subnet ID: 10.216.0.0 Subnet mask : 255.255.128.0	CCS Manager 1
Subnet ID: 10.216.46.0 Subnet mask : 255.255.255.0	Site A

You can define subnet routing rules as follows:

- Route jobs for the assets that have subnet ID: 10.216.0.0 and subnet mask: 255.255.128.0 to CCS Manager 1.
- Route jobs for the assets that have subnet ID: 10.216.46.0 and subnet mask: 255.255.255.0 to CCS Site A.

See “Routing rules based on expression” on page 231.

See “Routing rules based on asset groups” on page 233.

See “Routing rules based on active directory site” on page 234.

See “Routing rules based on IP address range” on page 230.

See “Creating routing rules based on subnet ” on page 1070.

Routing rules based on expression

You can create routing rules based on host name, FQDN, and domain. It includes the operators that you can use to create the rules.

The following table lists the operators and their descriptions:

Table 3-62 Operators and descriptions

Operator	Description
Equals	Route assets that match all the words in the search string.
Starts with	Route assets that starts with the specified search string.
Ends with	Route assets that ends with the specified search string.
Like	Route assets that match a search string, which includes regular expressions.
Contains	Route assets that contain the search string, which can be a word, word fragment, or a phrase. For example, if you use the word 'Critical' in the search string, the Contains operator searches for the words critical, srvcritical, and so on. The operator searches for these terms regardless of where they appear in a sentence.

Consider this example, you want to perform a job on the servers that are in your organization and 2000 are critical servers and another 2000 are in the Medical domain.

CriticalSrv	CCS Manager 1
Medical	Site A

You can define routing rules based on expressions as follows:

- Route jobs for the assets whose host name begins with CriticalSrv to CCS Manager 1.
- Route jobs for the assets who are in the Medical domain to Site A.

See "Routing rules based on asset groups" on page 233.

See "Routing rules based on active directory site" on page 234.

See "Routing rules based on IP address range" on page 230.

See "Routing rules based on subnet " on page 231.

See "Creating routing rules based on expression " on page 1071.

Routing rules based on asset groups

You can create routing rules based on the asset group. The jobs for the asset groups are routed to the CCS manager or site that you specify in the rule.

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.

Consider this example, you want to perform a job on the assets in your organization where 2000 are Oracle databases and 1000 are UNIX servers.

Oracle	CCS Manager 1
UNIX	Site A

You can define asset group routing rules for jobs as follows:

- Route jobs for assets in Oracle group to CCS Manager 1
- Route jobs for assets in UNIX group to Site A.

See "Routing rules based on active directory site" on page 234.

See "Routing rules based on IP address range" on page 230.

See "Routing rules based on subnet " on page 231.

See "Routing rules based on expression" on page 231.

See "Creating routing rules based on asset group" on page 1073.

Scope in routing rules

You can use site and CCS manager as scope to route jobs.

Sites are used as scope to route jobs. You can choose to send jobs to group of CCS managers in a site. At least one CCS manager in the collectors role must be present in the default site or the site that you create.

If you are new to CCS 11.0, a default site is created after you have installed and configured CCS 11.0 on your computer. By default, a system-defined rule is also created and is displayed as disabled in the **Manage Routing Rules - Settings** view. If you do not create any routing rules, the jobs for your assets are routed to the default site.

If you are an existing CCS user, when you upgrade from your current CCS version to CCS 11.0, the site-based rules that you had created earlier are displayed in the **Manage Routing Rules - Settings** view. By default, these rules are enabled. The job related to data collection mechanism in CCS 11.0 is backward-compatible. Therefore, if you opt on not creating routing rules, the job is performed using the existing mechanism. You can override the existing data collection mechanism by disabling the system-defined rules and creating new routing rules.

Note: The jobs for the assets that cannot be routed are sent to the fall back options as described in the section, About routing rule evaluation.

See "Concepts in routing rules" on page 230.

See "Routing rules evaluation " on page 236.

Routing rules based on active directory site

You can create routing rules based on the subnets that are present in the active directory site. When the information on the subnets are obtained, you can create the subnet-based routing rules. You can then assign sites or CCS managers to the rule. An active directory site can have multiple subnets and a subnet can be part of only one active directory site. Each active directory site represents a logical boundary and all subnets in an active directory site are physically close, a CCS manager that is installed in an active directory site can be used to collect data from all assets in that site.

After you are connected to the domain, CCS displays the following information:

- Displays the sites that are present in the active directory.
- Displays the subnets that are present in the sites.
- Displays any routing rules that are you have created.
- Displays the CCS managers that are installed in the site.

See "Creating routing rules based on active directory site" on page 1074.

See "Routing rules based on IP address range" on page 230.

See "Routing rules based on subnet " on page 231.

See "Routing rules based on expression" on page 231.

See "Routing rules based on asset groups" on page 233.

Scope in routing rules

You can use site and CCS manager as scope to route jobs.

Sites are used as scope to route jobs. You can choose to send jobs to group of CCS managers in a site. At least one CCS manager in the collectors role must be present in the default site or the site that you create.

If you are new to CCS 11.0, a default site is created after you have installed and configured CCS 11.0 on your computer. By default, a system-defined rule is also created and is displayed as disabled in the **Manage Routing Rules - Settings** view. If you do not create any routing rules, the jobs for your assets are routed to the default site.

If you are an existing CCS user, when you upgrade from your current CCS version to CCS 11.0, the site-based rules that you had created earlier are displayed in the **Manage Routing Rules - Settings** view. By default, these rules are enabled. The job related to data collection mechanism in CCS 11.0 is backward-compatible. Therefore, if you opt on not creating routing rules, the job is performed using the existing mechanism. You can override the existing data collection mechanism by disabling the system-defined rules and creating new routing rules.

Note: The jobs for the assets that cannot be routed are sent to the fall back options as described in the section, About routing rule evaluation.

See "Concepts in routing rules" on page 230.

See "Routing rules evaluation " on page 236.

About resolving IP addresses

Assets are imported through various mechanisms such as LDAP connector and third-party providers however not all assets have an IP associated with them. A host IP cache is created on the CCS Manager in the load balancer role, to avoid a manual update of the IP address of these assets.

See "Host IP cache update job" on page 235.

See "Host IP cache refresh job" on page 236.

Host IP cache update job

This job help resolve the IP address of the assets that do not have an IP address. On every job run, the unresolved assets that are present in the CCS asset system are sent to all the CCS managers that are present in the system. A DNS query is fired to create the cache. By default, this job is scheduled to run once a day however you can modify the job run interval.

See "Scheduling a host IP cache update job" on page 1080.

See "About resolving IP addresses" on page 235.

Host IP cache refresh job

This job help update the IP address of the all assets. On every job run, the assets that are present in the database are sent to all the CCS managers that are present in the system. A DNS query is fired to create the cache. By default, this job is disabled.

See "Scheduling a host IP cache refresh job" on page 1080.

See "About resolving IP addresses" on page 235.

Routing rules evaluation

Routing rule evaluation lets you view the scope for the assets and the rules against which the assets are evaluated.

If for any reason, the jobs for the assets are not satisfied by the rules that you specify, the jobs for the assets are then routed to the following fall back options:

- Network affinity
  This is the first fall back option.

  Note: The assets must be in the same or accessible subnet as that of the CCS manager.

- Default site
  This is the second fall back option.

  Note: The default site must have CCS manager in the collector role.

The jobs that do not satisfies the mentioned criteria are displayed in the **Failures** tab.

See "Evaluating routing rules" on page 1078.

See "Routing rules workflow" on page 1081.

See "Concepts in routing rules" on page 230.

Concepts in risk management

To understand how risk can be managed by using CCS, you need to understand the following concepts that are related to risks:

- Risk and the components of a risk.

- Assets and business assets with reference to risk.
- Controls, weights, residual risk, and compensating controls.
- Risk modeling, risk assessment, and risk management workflow.
- Analyzing and monitoring risks, treating risks, and risk treatment workflow.

See “Risks” on page 238.

See “Assets” on page 238.

See “Controls” on page 239.

See “Residual risk and compensating controls” on page 239.

See “Weight” on page 240.

See “Components of a risk” on page 240.

See “Risk manager - Workflow” on page 240.

See “Risk treatment - Workflow” on page 248.

About environmental challenges and risk management

Today's highly connected IT infrastructures exist in an environment that is increasingly malicious—attacks are being mounted with increasing frequency and are demanding ever shorter reaction times. Often, organizations cannot react to new security threats before their business is affected. Managing the security of their infrastructures—and the business value that those infrastructures deliver—has become a primary concern for IT departments. Failure to proactively manage security may put executives and whole organizations at risk.

See “About role of CCS in risk management” on page 237.

About role of CCS in risk management

CCS delivers a clear, actionable guidance on how to implement a security risk management process that delivers a number of benefits, including:

- Helps you to move to a proactive risk posture and frees you from a reactive, frustrating process.
- Makes risk measurable.
- Helps you to efficiently mitigate the risks to your organization.

See “About CCS risk manager” on page 238.

About CCS risk manager

CCS risk manager is a Web-based and data-driven approach to manage and communicate the risks to your business.

Risk manager lets you do the following:

- Understand the risk posture of the critical assets in different areas in your organization and mitigate it to attain your business objectives.
- Define objectives and create a risk model to understand the risk level that is associated with the objective.
- Define and identify critical assets and risk areas for which you want to determine the risk level.
- Assess and measure risk to know the risk level that is associated with it.
- Monitor and prioritize risks by using risk dashboards.
- Define an action plan to treat risks.
- Visualize risks in multiple dimensions such as risk areas, security objectives, asset organization, controls and so on.
- View the risk trends in key risk areas.

See “Concepts in risk management” on page 236.

Risks

Risk is a probable frequency and magnitude of future loss, which is measurable. The measure of an IT risk can be determined as a product of threat, vulnerability, and asset values.

Managing risks involves rationally making choices under uncertainty.

See “Concepts in risk management” on page 236.

Assets

An asset for a business organization is anything that has a value, an owner, and restricted access. Business organizations can have physical and business assets.

- Physical assets are the ones that are accessible over a computer network. For example, desktop and laptop computers, servers, printers, files, folders and so on.
- Business assets are typically real world business entities such as business units, departments, business processes and so on.

See “Concepts in assets” on page 60.

See “About business assets” on page 62.

See “Creating business assets” on page 507.

See “Associating with a business asset” on page 510.

See “Concepts in risk management” on page 236.

Controls

Controls are safeguards or the measures that are put into place to protect against a specific risk or threat. Organizations deploy controls to protect physical and business assets from various threats and mitigate risks. CCS provides a Controls Studio that lets you manage controls, map controls to assessment data, policies, and create new regulations and controls.

Following are a few examples of controls:

- Employees must be trained and prepared to notify the management in case of accidental data loss or a malicious attack
- Apply latest security patch every week.
- Enforce a strong password.
- Data must be encrypted when transmitting over a public network.

See “Creating Control Categories” on page 1012.

See “Creating Controls” on page 1013.

See “Mapping Control Statements to Controls” on page 1015.

See “Concepts in risk management” on page 236.

Residual risk and compensating controls

Organizations can analyze the extent of the risk reduction generated by the new or enhanced controls in terms of the reduced threat likelihood or impact, the two parameters that define the mitigated level of risk to the organizational mission.

In an IT environment that has multiple security controls, one security control can compensate another. There can be an exposure to loss remaining even after other known risks are eliminated. The risk remaining after the implementation of new or enhanced controls is the residual risk.

If there is any residual risk on the control, there can be a new or an enhanced control that reduces the risk by a factor of its effectiveness. This is called a compensating control.

See “Defining monitoring parameters for security objective” on page 1095.

See "About risk aggregation and analytics" on page 242.

See "Concepts in risk management" on page 236.

Weight

Weight is the importance that you can assign as a percentage to the controls that you associate with the security objective. Weight is a relative term and you can determine the weight percentage that you want to assign to a control.

Components of a risk

It is important for everyone involved in the risk management process to understand how different components form a risk definition. Only with a thorough understanding of risk will the business be able to take specific action when managing it. Table 3-63 explains the components that form a risk.

Table 3-63 Components of a risk

Risk			
Impact What is the impact to the business?		**Likelihood** How likely is the threat given the controls?	
Asset What are you trying to protect?	**Threat** What are you afraid of happening?	**Vulnerability** How can the threat occur?	**Mitigation** What is currently reducing the risk?

See "Concepts in risk management" on page 236.

Risk manager - Workflow

Risk manager involves four major components that are risk modeling, risk analytics, risk dashboards, and risk-based remediation.

Prerequisites

1. Asset hierarchy must be created in the asset system.
2. Control categories and controls must be created in the controls framework of the controls studio. Control statements must be mapped to the controls.
3. Evaluation and data collection job must be already run and the results must be available.

See "Prerequisites to use risk manager" on page 241.

End-to-end sequence of operations in risk manager

1. Risk Modeling

   Risk modeling is a process where you can create a security objective, associate the business assets and controls to the security objective, and publish the security objective.

2. Risk Analytics

   CCS runs a scheduled job Global Metrics and Trends Computation that is made available with the CCS installation, for risk manager to determine the correct risk score. The risk calculation logic in risk manager calculates the risk score, based on the evaluation and the assessment data that is collected from the following:

   - Checks, questions, and extended tests and assessment procedures that are available in the reporting database for the corresponding assets and the controls.
   - Configured systems in the external data integration workspace like CCS VM, response assessment evidences, DLP, and any user-defined third-party system. .

3. Risk Dashboards

   The risk-related data that is stored in the reporting database after the risk score is calculated presents the risk posture of the business. By using the risk dashboards, you can visualize risks with the help of panels.

4. Action to treat risks

   Risk dashboards enable you to analyze risks and create an action plan to treat the risks. You can opt for the following remediation systems:

   - Symantec Workflow
   - Symantec ServiceDesk
   - Email

See “Concepts in risk management” on page 236.

Prerequisites to use risk manager

To use the risk manager, you must install all the CCS components that are available with the CCS core license.

You must have an asset hierarchy created in the asset system of CCS.

See “About the management of business assets” on page 141.

See “Asset folder hierarchy” on page 64.

You must have controls defined and control statements mapped to the controls, in the controls studio.

See “Creating Control Categories” on page 1012.

See “Creating Controls” on page 1013.

See “Mapping Control Statements to Controls” on page 1015.

Evaluation and data collection job must be already run and the results must be available.

See “About data collection jobs” on page 163.

See “About evaluation jobs” on page 164.

Appropriate roles must be assigned to users to access various components of the risk manager.

See “Predefined roles” on page 285.

Risk manager uses this existing evaluation data and helps you to determine the risk on the assets.

About risk assessment

CCS risk manager analyzes data and derives the risk score based on the following:

- The risk score that CCS Vulnerability Manager and CCS Standards Manager generates.
- The incident data that Symantec Data Loss Protection generates.
- Data generated by user responses to the Symantec Response Assessment Module.
- Data that is generated by the assessment procedures of any external systems.
- Data that is generated by any user-defined tests.

Internally, CCS applies the risk aggregation and analytics logic on the collected data and calculates the risk to your business. By using CCS risk dashboards, you can then view the risk score.

See “About External Data Integration” on page 210.

See “About risk aggregation and analytics” on page 242.

About risk aggregation and analytics

CCS calculates the base risk score that is based on the technical assessments, user response to response assessment evidences, incidents, vulnerabilities and so on. The base risk score is a product of likelihood and impact.

Risk manager builds the risk aggregation and analytics logic over the base risk score. This is based on the following:

- Asset characteristics
  Importance of the assets across multiple dimensions and information classification.
- Controls effectiveness
  Realistic ability to model risks.
- Weights and compensating controls
  Weight in terms of percentage, the compensating controls, and the compensation percentage.

The final risk score is calculated after applying the risk aggregation and analytics logic to the base risk score. The risk score is represented numerically on the scale of 1 to 10. 1 being the lowest and 10 being the highest.

Following are the types of risk scores:

- Base risk score
- Weighted base risk score
- Risk score - with controls
- Weighted risk score - with controls
- Compensated risk score

Note: Risk score with controls considers the controls that are defined at the security objective level. Base risk score considers all tests like threats, vulnerabilities, incidents, response assessment evidences, and technical assessments, irrespective of whether they are associated with a control or not.

See "About risk score - With controls" on page 243.

See "About aggregated weighted risk score - With controls" on page 245.

See "About weighted base risk score" on page 245.

See "About compensated risk score" on page 246.

About risk score - With controls

Table 3-64 explains the logic behind how the base risk score on a security objective that has controls that are associated gets calculated.

Table 3-64 Risk score with controls

Controls	Tests	Asset Group A		Average
		Asset A	Asset B	
C1	T1	7	0	**3.5**
	T2	6	0	**3.0**
Average:		**6.5**	**0**	**3.25**

Let us assume the following:

- You have a security objective SO1.
- Asset Group A (contains assets Asset A and Asset B) and C1 (contains tests T1 and T2) are associated with SO1.
- Asset A and Asset B are evaluated against the tests T1 and T2.
- Tests T1 and T2 have failed for Asset A and passed for Asset B.

Risk score of C1 is calculated as follows:

- Risk Score of T1 on Asset A and Asset B is 7 and 0, respectively. Therefore, the aggregated risk score of T1 is (Risk score of Asset A evaluation + Risk score of Asset B evaluation)/2 that is (7 + 0)/2 = 3.5.
- Risk Score of T2 on Asset A and Asset B is 6and 0, respectively. Therefore, the aggregated risk score of T2 is (Risk score of Asset A evaluation + Risk score of Asset B evaluation)/2 that is (6 + 0)/2 = 3.0.
- Risk score of C1 is (Risk score of T1 + Risk score of T2)/2 that is (3.5 + 3.0)/2 = 3.25.

Risk score of Asset Group A is calculated as follows:

- The risk score for Asset A and Asset B is calculated as the (Evaluation score of T1 + Evaluation score of T2)/2. Therefore, in the case of Asset A it is (7 + 6)/2 = 6.5 and for Asset B it is 0.
- Risk score of Asset Group A is (Risk score of Asset A + Risk score of Asset B)/2 that is (6.5 + 0)/2 = 3.25.

Risk score of SO1 is calculated as the (Risk score of Asset group A + Risk score of C1)/2 that is (3.25 + 3.25)/2 = 3.25.

See “About aggregated weighted risk score - With controls” on page 245.

See “About weighted base risk score” on page 245.

See “About compensated risk score” on page 246.

About aggregated weighted risk score - With controls

Table 3-65 explains the logic behind how the aggregated weighted risk score of a security objective that has controls that are associated gets calculated

Table 3-65 Aggregated Weighted Risk Score with Controls

Asset Group A	Controls	Weight%	Risk Score
Asset A	C1	80%	7
	C2	20%	6

Let us assume the following:

- You have a security objective SO1.
- SO1 is associated with Asset Group A (contains Asset A).
- SO1 is associated with two controls C1 and C2.
- C1 and C2 are assigned a weight percentage of 80% and 20%, respectively.
- Asset A is evaluated against C1 and C2 and the risk scores are 7 and 6, respectively.

Risk score of SO1 is calculated as follows:

- (Risk Score of C1 x Weight%) + (Risk Score of C2 x Weight%) that is (7 x 80%) + (6 x 20%) = 6.8

See "About weighted base risk score" on page 245.

See "About compensated risk score" on page 246.

See "About risk score - With controls" on page 243.

About weighted base risk score

Table 3-66 explains the logic of how a weighted average risk score gets calculated for a security objective without controls.

Table 3-66 Aggregated Weighted Risk Score

Asset Group A	Tests	Source System	Weight%	Risk Score
Asset A	Vulnerability (V1)	CCS VM	80%	7
	Data loss incident (DL1)	DLP	20%	6

Let us assume the following:

- You have a security objective SO1.
- SO1 is mapped to Asset Group A that contains one asset, Asset A.
- Asset A is evaluated against a vulnerability test (V1) and a data loss test (DL1).
- The source system of V1 is CCS VM and the source system of DL1 is Symantec DLP.
- Risk score of V1 and DL1 on Asset A is 7 and 6, respectively.
- The weight percentages that you have set while defining the source systems CCS VM and DLP are 80% and 20%, respectively.

Risk score of SO1 is calculated as follows:

- (Risk score of V1 x Weight % of its source system) + (Risk score of DL1 x Weight % of its source system) that is (7 x 80%) + (6 x 80%) = 6.8

See "About aggregated weighted risk score - With controls" on page 245.

See "About risk score - With controls" on page 243.

See "About compensated risk score" on page 246.

About compensated risk score

To understand the logic behind how a compensated risk score gets calculated, let us consider the following scenario:

- Security objective (SO1) - Account for and protect all IT assets.
- Control (C1) - Protect application.
- Control (C2) - Protect computer.
- Control (C3) - protect network.

To access the application, the user has to access the computer that is protected and pass through the network that is also secured. Therefore, even though C1 is vulnerable, the risk on C1 gets reduced because of C2 and C3. Therefore, C2 and C3 are the compensating controls because they compensate the risk on C1.

Let us assume the following data consisting of risk scores, weights, and compensating factor for the controls.

Table 3-67 Compensated risk score

Controls	Compensating Whom	Compensating By	Current Risk (Scale 1 to 10)	Weight Percentage
C1			4	30%
C2	C1	80%	6	30%
C3	C1	40%	9	40%

In the table Table 3-67, C3 compensates C1 by 40% only when C3 is 100% effective. The formula that the risk manager uses to calculate the risk is:

```
Compensation effect = risk score of the control getting compensated
x [ compensation percentage x {(10 - risk score of the compensating
control)/10% }]
```

According to the formula the compensation effect of C2 is:

```
4 x [(80/100) x {(10-6)/10%}] = 1.28
```

According to the formula the compensation effect of C3 is:

```
4 x [(40/100) x {(10-9)/10%}] = 0.16
```

Net compensation effect of the controls C2 and C3 is the maximum of the two that is 1.28.

The formula to derive the net risk score is:

```
Net risk score of the control getting compensated = current risk
score - maximum of the compensation effect
```

that is

```
4 - 1.28 = 2.72
```

Apply the compensation as explained to get the following risk scores:

- C1 = 2.72
- C2 = 6
- C3 = 9

The risk score of the security objective is derived by taking the weighted sum of all the controls that are mapped to the security objective. The formula that the risk manager uses to calculate the risk score is:

```
Risk score of the security objective = (total weight x net risk score
of the control)/100
```

that is

```
[(2.72 x 30) + (6 x 30) + (9 x 40)]/100 = 6.216
```

See "About aggregated weighted risk score - With controls" on page 245.

See "About risk score - With controls" on page 243.

See "About weighted base risk score" on page 245.

Risk treatment - Workflow

Once you define and publish a security objective, risk manager lets you analyze the risk score and define an action plan to treat the risks.

Sequence of operations for treating risks

1. Define and publish a security objective.
2. After the security objective is published, risk manager calculates the current risk score and the projected risk score for the following:
   - Each risk element that is associated with the security objective.
   - Aggregated risk for the overall security objective.
3. Based on your analysis of the risk score, you can decide on an action to treat risks, by using dashboards.

   Note: Before you proceed with an action to treat risks, you must select a default system under Settings > Risk Remediation. You can select either email, Symantec Workflow, or Symantec ServiceDesk as the default system for treating risks.

4. Create and submit either a remediation plan or an exception plan by selecting risks for remediation or risks for exception, respectively.

What happens once you submit the plan?

- If you opt for email , an email with the remediation details is sent to the specified recipients.
- If you opt for Symantec Workflow, you can submit the remediation plan to the desired workflow in Symantec Workflow. Symantec Workflow handles the action and provides a status update to CCS. This status is displayed on the **Action Plans** page, under the **Status** column.
- If you opt for Symantec ServiceDesk , a ticket is generated and submitted to the Symantec ServiceDesk . When Symantec ServiceDesk updates the status of the ticket, the status is displayed on the **Action Plans** page under the **Status** column.

See “About risk treatment” on page 1102.

About Dynamic Dashboards

A dynamic dashboard is a business tool that displays key performance indicators (KPI), business trends, and other relevant information to management and employees. The panels in a dashboard use 2D and 3D charts to provide high level and relevant information at a glance.

A dashboard provides the following abilities:

Table 3-68 Dashboard abilities

Name	Description
Monitor	Critical business activities, processes, and trends can be monitored with the performance metrics that can trigger an alert when potential problems occur.
Manage	People and processes can be visually managed to improve decisions and optimize performance.
Analyze	A dashboard user can explore the timely and the relevant information that is gathered from multiple sources at one location.

From the Web Console you can view the different dashboards in the sidebar, predefined dashboards and created dashboards to fit the organization’s needs.

A dashboard definition consists of the following:

- Dashboard name
- A category for the dashboard
- A dashboard contains at least one panel
- The dashboard can have a mix of Published Panels and Private Panels

The following dashboard tasks may be available, depending on the permissions you have:

Table 3-69 Dashboard tasks

Tasks	Description
Create	Design and create a dashboard to fit your organization's needs.
Publish	Publish the dashboard so that other users can view it. Publishing a dashboard publishes private panels. In the Dashboard sidebar the icon next to the selected dashboard changes from the private icon to the public icon.
Edit	Modify the dashboard.
Delete	Delete the selected dashboard from the system. You cannot delete a predefined dashboard.
Copy	Copy a dashboard to the Private filter of the Dashboards sidebar. Only the CCS Administrator or the dashboard creator can see the copied dashboard.
Unpublish	Move the dashboard from Published filter to Private filter so that only the CCS Administrator or the dashboard creator can view unpublished dashboard. In the sidebar the icon next to the selected dashboard changes from the public icon to the private icon.

The following table lists what you can do with dashboards:

Table 3-70 What you can do with dashboards

What you can do	Link
Create a dashboard.	See “Creating a dashboard” on page 973.
Create a panel.	See “Creating a panel” on page 984.
Edit a dashboard.	See “Editing a dashboard” on page 977.
Change the setting of the dashboard refresh interval.	See “Setting a dashboard refresh interval ” on page 974.
Applying filters to a dashboard.	See “Applying filters to a dashboard” on page 975.

Table 3-70 What you can do with dashboards *(continued)*

What you can do	Link
Add a panel to a dashboard.	See "Adding a panel to a dashboard" on page 974.
Publish a dashboard.	See "Publishing a dashboard" on page 975.
Resizing a panel in a dashboard.	See "Maximizing a panel in a dashboard" on page 1002.
Send a dashboard link.	See "Emailing a dashboard URL" on page 978.
Print a dashboard.	See "Printing a dashboard" on page 978.
Copy a dashboard.	See "Copying a panel" on page 1000.
Delete a dashboard.	See "Deleting a dashboard" on page 979.

See "About panels" on page 251.

See "About key performance indicators" on page 253.

See "Roles and permissions" on page 969.

About panels

A panel uses 2D and 3D charts to display high level and relevant information at a glance to the user.

Some panels are designed to provide multiple levels of information. The top level is displayed in one of the following manner:

- Chart
- Text
- Table

An important feature of the panels is the ability to easily add interactivity. This interactivity can be in the form of drilldown or drill through. Either interactivity lets you view more details about a particular element of a chart in a panel.

The drilldown feature lets you graphically penetrate down in the hierarchy to provide information across various categories. A drill through refers to showing details from the context of drilldown which display the detail information about the KPI measures.

Note: You can only implement the drilldown feature when you create or edit a risk panel.

A panel definition consists of the following:

- Panel name
- A KPI or area of interest
- A measure based on the KPI
- A dimension of measurement which is the X axis
- A category for the panel
- Scopes or pre-filters, if available
- Post-filters, if available
- Content, which can be displayed as either a chart or a table

The following panel tasks may be available, depending on the permissions you have:

Table 3-71 Panel tasks

Tasks	Description
Create	Design and create a panel to fit your organization's needs.
Publish	Publish the panel so that other users can view it. In the Panels sidebar the icon associated with the selected panel changes from the private icon to the public icon.
Edit	Modify the panel.
Delete	Delete the selected panel from the system. You cannot delete a predefined panel.
Copy	Copy a panel to the Private filter of the Panel sidebar. Only the CCS Administrator or the panel creator can see the copied panel.
Unpublish	Move the panel from Published filter to Private filter so that only the CCS Administrator or the panel creator can view unpublished panel. In the sidebar the icon next to the selected panel changes from the public icon to the private icon.

The following table lists what you can do with panels:

Table 3-72 What you can do with panels

What you can do	Link
Create a panel.	See "Creating a panel" on page 984.
Edit a panel.	See "Editing a panel" on page 999.
Add a panel to a dashboard.	See "Adding a panel to a dashboard" on page 974.
Publish a panel.	See "Publishing a panel" on page 997.
Unpublish a panel.	See "Unpublishing a panel" on page 997.
Apply filters to a panel.	See "Applying filters to a panel in a dashboard" on page 1002.
Maximizing a panel in a dashboard.	See "Maximizing a panel in a dashboard" on page 1002.
Viewing properties of a panel.	See "Viewing properties of a panel" on page 998.
Extracting a panel to Excel.	See "Extracting a panel to Excel" on page 1001.
Copy a panel.	See "Copying a panel" on page 1000.
Delete a panel.	See "Deleting a panel" on page 1001.

See "About Dynamic Dashboards" on page 249.

See "Difference between drilldown and drill through" on page 976.

See "About key performance indicators" on page 253.

See "Roles and permissions" on page 969.

About key performance indicators

A panel in a dashboard is a key performance indicator (KPI). A KPI is a measure of the performance of an organization's goals or individual goals. The KPI can be critical for the current success and future success of the organization. An important characteristic of a KPI is that what is measured can be changed.

For example, if the asset compliance indicators show a downward trend, you need to implement corrective actions to improve performance.

A KPI has no purpose if it measures an activity that the organization cannot change.

See “About panels” on page 251.

Section 2

Working with the Control Compliance Suite Console

Navigating through Control Compliance Suite console

This chapter includes the following topics:

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

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.

See "About the tree pane" on page 260.

See "About working in the tree pane" on page 270.

Filter by pane

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.

See "About the Filter by pane" on page 261.

See "Using filters in the Filter by pane" on page 266.

See "Customizing the filter options" on page 267.

Taskbar

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.

Table pane

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.

See "About the table pane" on page 261.

See "Managing the table pane" on page 267.

Details pane

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.

See "Viewing and editing the object details" on page 269.

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 4-1 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.
	Exit	Closes the CCS application.
Edit	**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: ■ Tree pane ■ Filter by pane ■ Table pane ■ Details pane
Go	**Home**	Opens the CCS Home view.

Table 4-1 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 257.

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 270.

See "About the console features" on page 257.

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.

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 267.

See "Using filters in the Filter by pane" on page 266.

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 267.

See "Viewing and editing the object details" on page 269.

See "Selecting the columns headings" on page 269.

See "About the console features" on page 257.

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 257.

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 257.

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 257.

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 is a static page that displays a brief introduction of the product and contains links that helps you to quickly get started with the product. The **Home** page also displays the link to launch CCS Web Console.

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.

See "Adding credentials for scheduled jobs" on page 308.

See "About the console views" on page 263.

About the Monitor view

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

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

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

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 data
- Manage asset and entity schema

Settings contains the following views:

- General

- Roles
- Permissions Management
- Licenses
- LiveUpdate
- System Topology
  See "About the Map view" on page 408.
  See "About the Grid view" on page 411.
- Certificates
- User Management
- Schema Manager

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
- 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
- My Reports view

See "About the Reports Templates view" on page 942.

See "About the My Reports view" on page 943.

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.

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 418.

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

See "About the Home view" on page 263.

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 266.

See "Customizing the filter options" on page 267.

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 257.

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 267.

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 261.

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 261.

See “Using filters in the Filter by pane” on page 266.

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

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.

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.

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 261.

See "Viewing and editing the object details" on page 269.

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 261.

See "Managing the table pane" on page 267.

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 261.

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 257.

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.

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 257.

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 272.
- Create new folder
  See "Creating folders in the tree pane" on page 271.
- Delete folder
  See "Deleting folders in the tree pane" on page 272.
- Rename folder
  See "Renaming folders in the tree pane" on page 273.
- Refresh folder
  See "Refreshing folders in the tree pane" on page 273.

See "About the tree pane" on page 260.

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 special characters in folder and job names" on page 271.

See "About the tree pane" on page 260.

About 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 271.

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 270.

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 260.

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 260.

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 260.

Optimizing the console layout

When working in a view you can choose to show or hide the tree pane, filter pane, table pane, and details pane. By optimizing the layout of the view you can create more work area and focus on your current area of interest. For example, once you've set your filter options, you can hide the filter pane to increase the display area of tree pane, table pane, and the details pane.

The show or hide option is available only for certain views of the console.

To optimize the console layout

1. Go to the view you want to work in.
2. On the menu bar, click **View > Show/Hide**.
3. Select the pane you want to hide.

   You click the same option again to show the pane. This action acts like a toggle.

   The name of the pane varies depending on the view.

Section 3

Configuring Control Compliance Suite

Getting started with configuration

This chapter includes the following topics:

- Quick start with minimum configuration
- Configuration tasks

Quick start with minimum configuration

The quick start helps you to get started with the minimum initial configuration that is required to collect and evaluate data, and to view the reports with compliance information.

The quick start applies to single setup mode installation.

The Configuration tasks topic provides more information and links to procedures that help you configure the system to suit your organization's infrastructure.

See "Configuration tasks" on page 278.

Table 5-1 Tasks to get you started with Control Compliance Suite (CCS)

Task	Description
Register CCS Manager	You must register the CCS Manager with the application server. When you register the CCS Manager, you also assign the CCS Manager to the default site or create your own site and specify the CCS Manager roles. Where appropriate, specify data types to collect.

Table 5-1 Tasks to get you started with Control Compliance Suite (CCS) *(continued)*

Task	Description
Create asset folders (optional)	You can store the objects in the default **Asset System** folder that is created when you install CCS or create user-defined folders. If you store objects in the default **Asset System** folder, you can later use the reconciliation rules to move the objects to a user-defined folder structure. The user-defined folders help to store business objects in a hierarchical manner that reflects your organizational structure. The user-defined folders let you effectively assign permissions.
Create asset import reconciliation rules (optional)	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. You can use the predefined reconciliation rules or create your own reconciliation rules to filter the assets.
Create an asset import job	You must import assets from the network before you can collect data from the assets and evaluate the assets against specific standards and checks.
Create a common data collection, data evaluation, and a reporting job	After you have imported the assets, you create a job to collect, evaluate, and report data from the imported assets.
Run Scheduled Reporting Synchronization Job	In order to see data, you must run the Scheduled Reporting Synchronization Job from the **Monitor > Jobs** view before you open a report, dashboard or panel for the first time.
View a report	You can now view the report.

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 5-2 on page 279.

See Table 5-3 on page 280.

See Table 5-4 on page 281.

See Table 5-5 on page 281.

Table 5-2 Initial configuration tasks

Tasks and links	Description
Create asset folders in the Manage > Asset System view.	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. 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. See "Creating the asset folders" on page 505.
Assign users to roles.	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. See "Adding users and groups to a role" on page 294.
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 300.
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 323.
Register installed CCS Manager instances.	Before the Application Server can use a newly installed CCS Manager, you must register the CCS Managerwith the Application Server. When you register the CCS Manager, you also assign the CCS Manager to a site and specify the roles. Where appropriate, specify data types to collect.

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

Table 5-3 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 438. See "Creating reconciliation rules without manual review" on page 437.
Create asset import jobs.	You must import assets from the network before you can collect data from the assets and evaluate the assets against specific standards and checks. You can import the assets in one of the following ways: See "Importing the assets for the first time" on page 444. See "Importing asset-specific fields from the default data collector" on page 455. See "Importing asset-specific and common fields using the default data collector" on page 458. See "Importing asset-specific and common fields using the CSV data collector" on page 461. See "Importing the specific and common fields for custom asset using the CSV data collector" on page 467.
Set up data collection jobs.	After you have imported the assets you create jobs to collect data from the imported assets. See "Setting up a data collection job from the Asset System view" on page 517.
Create evaluation jobs.	After you have collected the data from the imported assets you create jobs to evaluate the assets. See "Running an evaluation job from the Asset System view" on page 519.

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

Table 5-4 Entitlements, reports, and dashboards tasks

Task	Description and task links
Mark and configure entitlement control points.	You mark an asset as a control point to monitor the entitlements of the asset through the approval workflow. See "Marking an asset as a control point" on page 514. You configure a control point to assign a data owner, an approver, the tags, and the review cycle to the control point See "Configuring control points" on page 616.
Create report jobs.	The report job generates a report with the data from the reporting database. You must synchronize the reporting database to view the latest data before you run a report job. The Reporting Database Synchronization job is an existing job in the **Monitor > Jobs** view. See "Scheduling a report " on page 957.
Create dashboard jobs.	The dashboard job generates the dashboard with the data from the reporting database. 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. The Reporting Database Synchronization Job job is an existing job in the **Monitor > Jobs** view.

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

Table 5-5 Policies and RAM tasks

Task	Description and task links
Create policies.	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. See "Creating a new policy" on page 902. See "Importing a Word policy" on page 904.
Publish policies.	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.

Table 5-5 Policies and RAM tasks *(continued)*

Task	Description and task links
Optionally publish Response Assessment module questionnaires.	See *Symantec Response Assessment module User Guide* for information on publishing questionnaires. See "About Response Assessment Module " on page 391.

Chapter 6

Configuring roles and permissions

This chapter includes the following topics:

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 292.

See "Predefined roles" on page 285.

See "About permissions" on page 284.

See "About tasks" on page 284.

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 283.

See "About tasks" on page 284.

See "Predefined roles" on page 285.

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 283.

See "Predefined roles" on page 285.

See "About permissions" on page 284.

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 6-1 Administrative roles

Role	Description
CCS Administrator	The CCS Administrator can perform most of the tasks in CCS. **Note:** In CCS v 10.0 the administrator can no longer review or approve policies. To review and approve policies, you must assign at least one user to the Policy Reviewer role and the Policy Approver role.
Power User	The Power User role lets the user do everything the CCS Administrator can do except the following tasks: ■ Configure application. ■ Manage audits. ■ Manage licenses. ■ Assign policy audience. You can view the list of available tasks from the **Settings > Roles** view.

Table 6-1 Administrative roles *(continued)*

Role	Description
Auditor	The Auditor role lets the user view the following: ■ View all jobs. ■ View assets and asset reconciliation rules. ■ View baselines and baseline conparision 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 review cycles ■ View standards

Table 6-2 CCS user role and Policy Audience role

Role	Description
CCS User	The CCS User role lets the user create dashboards in the Web console. **Note:** To view the assets in the dashboards, the CCS User must be assigned the Asset Viewer role and have permissions to the assets.
Policy Audience	By default, all the authenticated CCS users have the Policy Audience role. **Note:** When you upgrade from version 9.0.1 to 10.0, the Guest User role is removed in version 10.0. The user accounts of the Guest User role are now placed in the Policy Audience role. The Policy Audience role lets the user do the following: ■ Accept or decline policies. ■ Request exceptions. ■ View policies and policy comments.

Table 6-3 Assets roles

Role	Description
Assets Viewer	The Assets Viewer role lets the user do the following: ■ View asset details. ■ View asset group details.

Table 6-4 Standards roles

Role	Description
Standards Administrator	The Standards Administrator role lets the user do the following: ■ Manage configuration settings. ■ Manage standards, sections, and checks. ■ Manage jobs. ■ Collect data. ■ Evaluate standards. ■ Manage tags. ■ Request exceptions. ■ View assets. ■ View standards. ■ View evaluation results. ■ View roles and permissions. ■ View reports and report templates. ■ Customize report templates. ■ View roles and permissions.
Standards Evaluator	The Standards Evaluator role lets the user do the following: ■ Manage jobs. ■ Collect data. ■ Evaluate standards. ■ Manage jobs. ■ Manage tags. ■ Request exceptions. ■ Generate reports and dashboards. ■ View evaluation results. ■ View dashboards and reports. ■ View assets. ■ View standards.

Table 6-5 Exception roles

Role	Description
Exception Approver	The Exception Approver role lets the user do the following: ■ Approve exceptions. ■ Manage tags. **Note:** The exception approver must have the required tasks and permissions to view assets.
Exception Requestor	The Exception Requestor role lets the user do the following: ■ Request exceptions on behalf of a user without an assigned CCS role. ■ Manage tags. **Note:** The exception requestor must have the required tasks and permissions to add assets, standards, and entitlements.

Table 6-6 Entitlements roles

Role	Description
Entitlements Administrator	The Entitlements Administrator role lets the user do the following: ■ 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 users. ■ Request entitlements approval. ■ Request exceptions. ■ Customize report templates. ■ Manage configuration settings. ■ Update and view notification templates. ■ View assets and asset reconciliation rules. ■ View review cycles. ■ View control points. ■ View reports and report templates. ■ View evaluation results. ■ View roles and permissions.
Entitlements Data Owner	The Entitlements Data Owner role lets the user do the following: ■ Request exceptions. ■ Manage entitlements. ■ Assign the alternate data owner to the control points. ■ View roles.

Table 6-7 Policy roles

Role	Description
Policy Administrator	The Policy Administrator role lets the user do the following: ■ Manage policies. ■ Manage jobs. ■ Manage tags. ■ Manage policy comments. ■ Manage policy clarifications. ■ Manage policy content. ■ Request exceptions. ■ Publish policies. ■ Manage configuration settings. ■ Customize report templates. ■ View assets. ■ View standards. ■ View policies, policy comments, and policy content. ■ View reports and report templates. ■ View roles and permissions.
Policy Approver	The Policy Approver role lets the user do the following: ■ Approve policies. ■ Manage policy comments. ■ View asset and asset group details. ■ View policy and policy content details. ■ View roles.
Policy Reviewer	The Policy Reviewer role lets the user do the following: ■ Manage policy comments. ■ Review policies. ■ View asset and asset group details. ■ View policy, policy comments, and policy content details. ■ View roles.

Table 6-8 Reports and dashboards roles

Role	Description
Reporting Administrator	The Reporting Administrator role lets the user do the following: ■ Customize report templates. ■ View reports and report templates. ■ 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.
Report Result Viewer	The Report Result Viewer role lets the user do the following: ■ View all jobs.

Table 6-9 Risk manager roles

Module	Roles	Description
Risk modeling	Risk Author	The risk author role lets you do the following: ■ Create, edit, and delete your risk objectives.
	CCS Administrator	The CCS Administrator role lets you: ■ Create, update, and delete all risk objectives.

Table 6-9 Risk manager roles *(continued)*

Module	Roles	Description
Risk dashboards	Any CCS user	Any CCS user can view risk dashboards for risk objectives where the user is a stakeholder, owner, or creator.
	CCS Administrator	The CCS Administrator role lets you do the following: ■ View the risk dashboards for all risk objectives.
Remediation management	Any CCS user	Any CCS user can initiate and view remediation plans for risk objectives where the user is a stakeholder, owner, or creator.
	CCS Administrator	The CCS Administrator role lets you do the following: ■ Initiate and view a risk remediation plan for all the risk objectives.

See “About roles” on page 283.

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 297.

See “Copying a role” on page 298.

See “Editing a custom role” on page 299.

See “Deleting a role” on page 299.

About the Roles view

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

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

Taskbar	The taskbar appears across the top of the tree pane and the table pane in the console window.
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.

The taskbar of the Roles view is divided in to the following major tasks:

Common tasks	■ Add Users and Groups ■ Remove Users and Groups ■ Create Role ■ Delete Role ■ Edit Role ■ Copy Role ■ View Details
Export tasks	■ Roles To Tasks List ■ Roles To Users List

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:

Task bar	The taskbar appears across the top of the tree pane and the table pane in the console window.

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.
- Remove permissions.
- View users who have permissions on a folder.
- View permissions on the folders at all levels.

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 294.

See “Removing a user or a group from a role” on page 295.

See “Viewing users assigned to a role” on page 296.

See “Viewing tasks associated to a role” on page 295.

See “Assigning permissions from the Roles view” on page 296.

See “Creating a custom role” on page 297.

See “Copying a role” on page 298.

See “Editing a custom role” on page 299.

See “Deleting a role” on page 299.

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 296.

See "Assigning permissions from the Permission Management view" on page 300.

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 295.

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 294.

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 294.

See "Viewing users assigned to a role" on page 296.

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 294.

See "Viewing tasks associated to a role" on page 295.

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 294.

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 300.

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 298.

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.

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 “Creating a custom role” on page 297.

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 297.

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 297.

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 300.

See "Removing permissions" on page 301.

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 294.

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 296.

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 300.

See "Assigning permissions from the Roles view" on page 296.

Chapter 7

Configuring the application server

This chapter includes the following topics:

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 **Edit Settings** dialog box, click **Application Server**.

4 On the **Application Server - Basic** 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 On the **Application Server - Integration Services** panel, provide the following information:

Algorithm Suite	Lets you select the algorithm suite that you want the bridge manager to use. The default algorithm suite for TCP, HTTPS, and HTTP is Basic256. You can also configure the algorithm suite for the following communication layers: ■ TCP/IP (HTTP, Windows Security) ■ WS_HTTP (Windows Security) ■ WS_HTTP over SSL (HTTPS, Windows Security) ■ WS_HTTP over SSL (HTTPS, Username Security) ■ Basic HTTP over SSL (HTTPS, Username Security) The default algorithm suite for the mentioned communication layers is set to **Inherited**. If you retain the default value, the communication layers inherit the algorithm suite that you select for the bridge manager. However, if you select a different algorithm for the communication layers, then the algorithm selection for the bridge manager is overridden.

Enabled	Enables the TCP/HTTPS/HTTP protocol if checked. **Note:** The field is not editable for the TCP.
Metadata Enabled	Enables the metadata if checked. **Note:** You must select the checkbox, if you want to use the Integration Services APIs over TCP or HTTPS or HTTP binding.

Port Number

Lets you type the port number.

- The default port for TCP is 1431.
- The default port for HTTPS is 12431.

  If you change the port number for the HTTPs, you must use the httpcfg (Windows 2003 support tools) or netsh (Windows 2008) to rebind the certificate to the new port.

  On the Windows 2003, use the following command:

  ```
  httpcfg delete ssl -i
  0.0.0.0:<install_port>
  httpcfg set ssl -i
  0.0.0.0:<new_port>
  -c Symantec_Components
  -h
  <certificate_thumbprint>
  -g <guid>
  ```

  On the Windows 2008, use the following command:

  ```
  netsh http delete
  sslcert
  ipport=0.0.0.0:<install_port>
  netsh http add sslcert
  ipport=0.0.0.0:<new_port>
  certstorename=Symantec_Components
  certhash=<certificate_thumbprint>
  appid=<application_id>
  ```
- The default port for HTTP is 80.

Enabled

Enables the Windows Security or the Username Security based on how you want to make the API calls.

In case of TCP/IP and HTTP, you can only use the Windows Security. In case of HTTPS, you can use either the Windows Security or Username Security.

BindingFactory	The field is not editable. The transport name is populated from the Directory Server.
ClientBindingFactory	The field is not editable. The transport name is populated from the Directory Server.
UriSuffix	The field is not editable. The transport name is populated from the Directory Server.
Public Transport	Lets you select from the Yes or No options. If you select Yes, only the public APIs are exposed. If you select No, both the public and the internal APIs are exposed.
Exception Details In Faults	Lets you select from the Yes or No options. If you select Yes, the internal error details that occur on the Server side also are included in Faults.

6 Click **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.

To modify application server credentials

1 Go to **Settings > Secure Configuration > AppServer Credentials**.

2 Type the password that authenticates the specified user account.

3 Click **Update password** to save.

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 Service
- Application server Service
- CCS Manager running in the reporter role

The supported special characters are applicable to the following databases:

- Production database
- Reporting database

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 (>)

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 418.

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**.

Registering and configuring the CCS Manager

This chapter includes the following topics:

About CCS Manager roles

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

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

- CCS Manager Load Balancer
- CCS Manager Collector

- CCS Manager Evaluator
- CCS Manager Reporter

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

Registering the CCS Manager

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

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

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

To register the CCS Manager

1. In the **System Topology > Map View** or **System Topology > Grid View**, click **Register CCS Manager**.
2. In the **CCS Manager Selection** panel, select one or more CCS Manager hosts to register and click **Next**.
3. In the **Site Selection** panel, select the site to which the CCS Manager 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 CCS Manager should be assigned. You must assign the CCS Manager to at least one role.

   You can also change the port the CCS Manager uses to communicate with the Application Server. The default port is 3993. Click **Next**.
5. In the **Confirm or change the CCS Manager to Use for Synchronizing the Reporting Database** panel, select the CCS Manager that should perform synchronization of the reporting database, then click **Next**.
6. If you selected the CCS Manager Collector role, in the **Data Collector Selection** panel, select the data collectors that the CCS Manager should use, then click **Next**.

7 In the **Summary** panel, click **Next**.

8 Do one of the following:

- If you assigned a CCS Manager to the CCS Manager Collector role, in the **Finished** panel, click **Advanced Settings for registered components**.
- If you did not assign a CCS Manager to the CCS Manager Collector role and need to register another CCS Manager, in the **Finished** panel, click **Register another CCS Manager**.
- If you did not assign a CCS Manager to the CCS Manager Collector role, in the **Finished** panel, click **Close**.

9 Click the name of the setting to configure.

Enter any information that is required on the panel.

10 In the **Edit Settings** dialog box, click **Save** to close the dialog box and save the changes.

11 In the **Finished** panel, click **Close**.

See “ Configuring the Windows data collector” on page 1112.

See “ Configuring the Oracle data collector” on page 1114.

See “ Configuring the SQL data collector” on page 1113.

See “ Configuring the UNIX data collector” on page 1113.

See “ Configuring the Exchange data collector” on page 1115.

See “ Configuring the NetWare data collector” on page 1116.

See “ Configuring the NDS data collector” on page 1115.

See “ Data collection using ESM data collectors” on page 1117.

See “ Configuring the CSV data collector” on page 329.

See “Configuring the ODBC data collector” on page 331.

Registering the CCS Manager with minimum custom configuration

Before the application server can use a newly installed CCS Manager, you must register the CCS Manager with the application server. When you register a CCS Manager, the Directory Server verifies a copy of the certificate that is assigned to the CCS Manager host. The certificate is then used to secure communications with the CCS Manager. When you register the CCS Manager, you can also configure the CCS Manager settings.

To register the CCS Manager Service

1. In the **System Topology > Map View** click **Register CCS Manager**.
2. In the **CS Manager Selection** panel, select the CCS Manager host to register and click **Next**.
3. In the **Site Selection** panel, select the Default Site option. You can also 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, click **Select ALL Items** link and click **Next**.

   The CCS Manager is assigned to all the roles.

   See “ About CCS Manager roles” on page 311.
5. In the **Confirm or change the CCS Manager to Use for Synchronizing the Reporting Database** panel, select the CCS Manager that should perform synchronization of the reporting database, then click **Next**.
6. In the **Data Collector Selection** panel, select the data collectors that the CCS Manager should use, then click **Next**.
7. In the **Summary** panel, click **Next**.
8. In the **Finished** panel, click **Change advanced settings for registered components** to change the settings of the CCS Manager Collectors to collect data.
9. In the **Edit Settings** dialog box, select the data collector and configure the settings.
10. Click **Save** to close the dialog box and save the changes.

See “ Registering the CCS Manager” on page 312.

Unregistering a CCS Manager

If needed, you can unregister a CCS Manager instance. When you do so, you remove the CCS Manager from the list of CCS Managers that the Application Server contacts. Before you unregister a CCS Manager, make sure that another CCS Manager is assigned to take over the duties of the unregistered CCS Manager.

To unregister a CCS Manager

1. In the **System Topology > Map View** or **System Topology > Grid View**, click **Unregister CCS Manager**.
2. In the **CCS Manager Selection** panel, select one or more CCS Manager hosts to unregister, then click **Next**.

3 In the **Summary** panel, click **I understand the above CCS Manager 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, do one of the following:

- Click **Unregister another CCS Manager**.
- Click **Close**

See " Registering the CCS Manager" on page 312.

Configuring basic CCS Manager settings

You can change the basic CCS Manager settings to assign roles and configure the data collectors.

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

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

Note: If you make a change to the basic CCS Manager settings, the changes do not appear immediately. You must close and reopen the **Edit Settings** dialog box before the new options appear.

See "Configuring advanced CCS Manager settings " on page 316.

See " Configuring data collectors for raw data based data collection" on page 327.

See "CCS Manager" on page 50.

To configure the basic CCS Manager settings

1 Double-click the shortcut icon of the CCS Console on the computer desktop.

2 In the launched **Select Symantec Control Compliance Suite Server** dialog box, enter the following:

- Application Server
  Enter the name of the computer on which the CCS Application Server is installed.
- TCP\IP port

Enter the port number of the computer that hosts the CCS Application Server. By default, the port is 1431.

3 Click **OK** to launch the CCS Console.

4 Go to the **System Topology > Grid View** or **System Topology > Map View**.

5 Right-click the CCS Manager and click **Edit Settings**.

6 In the **Edit Settings** dialog box, in the left pane, under **Symantec CCS Manager**, click **Basic**.

7 On the **CCS Manager - Basic** panel, click the roles to assign the CCS Manager to.

8 If the CCS Manager is assigned to the CCS Manager Collector role, select the data collectors to enable on the CCS Manager.

9 If you want to configure the CCS Manager for message based data collection, enter the ESM password to enable message based data collection. Confirm the ESM password, and then click **Apply**

You need to provide the ESM password while registering a CCS Agent for message based data collection.

10 Click **Save** to save the changes.

Configuring advanced CCS Manager settings

You can change the advanced CCS Manager settings to change the number of threads the CCS Manager uses internally.

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

You can change the settings of a CCS Manager from the **System Topology > Map View** or **System Topology > Grid View** views.

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

See “Configuring basic CCS Manager settings” on page 315.

See “ Configuring data collectors for raw data based data collection” on page 327.

See “CCS Manager” on page 50.

The Advanced settings include the following:

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

You can change the following communication settings:

Port	The TCP/IP Port other components use to communicate with the CCS Manager.

You can change the following settings the CCS Manager uses internally to define how the Scheduler behaves:

Command Threads	The minimum number and maximum number of processor threads available for the CCS Manager Scheduler. If a very high performance computer hosts the CCS Manager, 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.

You can change the following settings that the CCS Manager 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 CCS Manager, more available threads may improve performance.
Job Poll Interval	The time, in seconds, the CCS Manager waits between attempts to collect job results.

To configure the advanced Data Processing Service settings

1. Double-click the shortcut icon of the CCS Console on the computer desktop.
2. In the launched **Select Symantec Control Compliance Suite Server** dialog box, enter the following:

- Application Server
  Enter the name of the computer on which the CCS Application Server is installed.
- TCP\IP port
  Enter the port number of the computer that hosts the CCS Application Server. By default, the port is 1431.

3 Click **OK** to launch the CCS Console.

4 Go to the **System Topology > Grid View** or **System Topology > Map View**.

5 Right-click the CCS Manager and click **Edit Settings**.

6 In the **Edit Settings** dialog box, in the left pane, under **Symantec CCS Manager**, click **Advanced**.

7 On the CCS Manager - Advanced panel, make any required changes to the advanced settings.

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

8 Click **Save** to save the changes.

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 data collectors for raw data based data collection” on page 327.

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 CCS Manager component and click **Edit Settings**.
- In the **System Topology > Map View**, right-click the CCS Manager component and click **Edit Settings**.

3. In the **Edit 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 **Save**.

Assigning a role to a CCS Manager

Each instance of the CCS Manager is assigned to one or more roles. A role controls what tasks the CCS Manager performs.

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

- Load Balancer
- Collector
- Evaluator
- Reporter
- External Data Connector

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

See “Configuring basic CCS Manager settings” on page 315.

See “Configuring advanced CCS Manager settings ” on page 316.

See “CCS Manager” on page 50.

To assign a role to a CCS Manager

1. Double-click the shortcut icon of the CCS Console on the computer desktop.
2. In the launched **Select Symantec Control Compliance Suite Server** dialog box, enter the following:
   - Application Server
     Enter the name of the computer on which the CCS Application Server is installed.
   - TCP\IP port
     Enter the port number of the computer that hosts the CCS Application Server. By default, the port is 1431.
3. Click **OK** to launch the CCS Console.
4. Go to the **System Topology > Grid View** or **System Topology > Map View**.
5. Right-click the CCS Manager and click **Edit Settings**.

6. In the **Edit Settings** dialog box, in the left pane, under **Symantec CCS Manager**, click **Basic**.
7. On the **CCS Manager - Basic** panel, click the roles to assign the CCS Manager to.
8. Click **Save** to save the changes.

Synchronizing CCS Manager settings

The Application Server periodically synchronizes settings on all registered CCS Manager 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**.

Chapter 9

Configuring sites

This chapter includes the following topics:

What sites can do for you

Sites let you group assets together with the CCS Managers that handle the assets. Sites let you adapt 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 CCS Manager Collectors that retrieve data from the assets. The CCS Manager 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 CCS Manager 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 CCS Manager Load Balancers, Evaluators, and Reporters. A site without a CCS Manager 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 CCS Manager instances are assigned to a site. Assets are always assigned to a single site. A CCS Manager 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 CCS Manager Collector assigned to collect data from the assets. You use the 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 CCS Manager 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 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 CCS Managers are assigned to the Default site.

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 "Deleting a site" on page 323.

See "Modifying the site name" on page 325.

Deleting a site

You must first remove any CCS Manager that is assigned to the site before you delete the site.

See "Removing a CCS Manager from a site" on page 324.

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 437.

- Reimport the assets.
  See "Importing assets" on page 440.

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 323.

See "Modifying the site name" on page 325.

See "About using sites" on page 322.

Assigning a CCS Manager to a site

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

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

To assign a CCS Manager to a site from the Map view

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

See "Creating a site" on page 323.

Removing a CCS Manager from a site

Whenever a CCS Manager is removed from a site the CCS Manager is automatically added to its last default site.

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

To remove a CCS Manager from a site in the Map view

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

See “Assigning a CCS Manager to a site” on page 324.

See “CCS Manager” on page 50.

See “About using sites” on page 322.

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 323.

See “Deleting a site” on page 323.

Configuring data collectors

This chapter includes the following topics:

Configuring data collectors for raw data based data collection

In Control Compliance Suite, the CCS Manager component is configured as a data collector. The CCS Manager 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 components comprise the ESM Manager and the ESMagent.

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.

A CSV file or an ODBC compliant database are defined as data collection components that facilitate import of any custom application data. In Control Compliance Suite, a CSV data collector is defined and configured to collect data of the application from the CSV files. An ODBC data collector is defined and configured to collect data from the ODBC compliant databases.

Table 10-1 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
Exchange	Exchange data collector
NDS	NDS data collector
NetWare	NetWare data collector
CSV	CSV data collector
ODBC	ODBC data collector

See “ Data collection using ESM data collectors” on page 1117.

See “ Configuring the Oracle data collector” on page 1114.

See “ Configuring the SQL data collector” on page 1113.

See “ Configuring the UNIX data collector” on page 1113.

See “ Configuring the Windows data collector” on page 1112.

See “ Configuring the Exchange data collector” on page 1115.

See “ Configuring the NDS data collector” on page 1115.

See “ Configuring the NetWare data collector” on page 1116.

See “ Configuring the CSV data collector” on page 329.

See “Configuring the ODBC data collector” on page 331.

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.

In the Control Compliance Suite, a CCS Manager that is registered to a site can be configured as a CSV data collector. The CCS Manager can be configured as a CSV data collector either from the Grid View or from the Map View of the console. Before configuring the CCS Manager, ensure that the CSV file containing the assets is placed in a network share path of the computer that hosts the CCS Manager.

Note: If a CSV file is shared on a CCS Manager 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 **Edit 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.
- To collect data for assets that are stored in the CSV files for any predefined asset type or a custom application.

See “ Configuring data collectors for raw data based data collection” on page 327.

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 CCS Manager component and click **Edit Settings**.

3 In the **Edit 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 CCS Manager 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

Enter the platform of the application whose data is to be queried .

You can use the drop-down box to select the platform of the application.

CSV File(s) Path

Enter the path where the CSV file is placed.

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.

Windows Domain

Enter the domain of the Windows computer, where the CSV file is located.

You need to provide the credentials of the Windows domain user in the dialog box, Credentials for the Platform.

User Name

Enter the user name of the specific domain.

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 **Save**.

Configuring the ODBC data collector

You can configure a CCS Manager as an ODBC data collector to collect data from the ODBC compliant databases.

See "About the ODBC data collector" on page 331.

See " Configuring data collectors for raw data based data collection" on page 327.

To configure an ODBC 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 CCS Manager component and click **Edit Settings**.

3 In the **Edit settings** dialog box, under the **CCS Manager**section, select **Basic** and check **ODBC Data Collector**.

4 In the **Edit settings** dialog box, select **ODBC** under the **Data Collector Sites** option on the left pane of the dialog box.

5 Select the site to which the CCS Manager is registered from the **Site Name** drop-down box on the right side pane of the dialog box.

6 Enter values for the fields to configure the ODBC data collector.

7 Click **Save**.

About the ODBC data collector

The ODBC data collector is used to import assets and collect data from the Open Database Connectivity (ODBC) compliant databases. For example, you maintain an Oracle database that stores asset details of various Oracle computers, which you can import using an ODBC data collector. In Control Compliance Suite, you must configure a CCS Manager as an ODBC data collector.

The ODBC data collector is equipped to import assets of predefined platforms or custom platforms and also collect data for the assets. The data collector interprets data only if the database table or view names and the column names are defined in a specific format.

The end-to-end sequence to import assets and collect data using the ODBC data collector is as follows:

- Identify the assets for which data is to be collected using the ODBC data collector.
  Assets belonging to either the predefined platforms or custom platforms can be imported.
- Create ODBC compliant database, which contain the assets that you want to import and their data. The ODBC compliant database tables or view names and the column names must be of the defined format for easy interpretation by the Control Compliance Suite for asset import or data collection.

  Note: If the database table or column names are not as per the naming convention, then you can manually map them through a dialog box.
- Register a CCS Manager as the ODBC data collector through the **Edit Settings** dialog box.
- Configure the CCS Manager as the ODBC data collector.
- Import the assets through the **Create or Edit Asset Import Job** wizard.

See "Configuring the ODBC data collector" on page 331.

Switching between CSV and ODBC data collectors

For custom platforms, even after you configured a default data collector, you can still switch over to another data collector to do asset import or data collection. This switching of data collector function is performed through the dialog box, **Switch CSV or ODBC Data Collector**. You can switch between a configured CSV data collector and an ODBC data collector to import assets and collect data for any custom platform.

After you switch, the data collector to which you switched the selected platform becomes the default data collector for importing assets. For example, you have configured a CSV data collector to collect data for a custom platform, DB2. Later, you want to switch to ODBC data collector to import assets and collect data for the same platform, DB2. You use the dialog box to switch between the CSV and the ODBC data collector.

You can also switch the common platform fields alone from one configured data collector to another. The common platform contains the common fields of an asset type.

To switch between CSV and ODBC data collectors

1. Go to **Settings > Schema Manager** in the console.
2. In the **Schema Manager** view, click **Switch CSV or ODBC data collector**.
3. In the **Switch CSV or ODBC Data Collector** dialog box, provide the details to switch a data collector.

Configuring the Directory Server data collector

You can configure a CCS Manager as a Directory Server data collector to collect data.

To configure the Directory Server 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 CCS Manager component and click **Edit Settings**.
3. In the **Edit settings** dialog box, under the **CCS Manager**section, select **Basic** and check **Directory Server** .
4. In the **Edit settings** dialog box, select **Directory Server** under the **Data Collector Sites** option on the left pane of the dialog box.

5 In the **Directory Server Configuration** area of the Directory Server panel, enter the following information:

Site	Lets you select a site from the drop-down list. The Direcotry Server configuration is applicable only for the selected site.
Asset type	Lets you select an asset type to which the Directory Server data collector configuration is applicable. You can select any of the pre-defined asset types for which you want to collect data. See "Predefined asset types" on page 66. You can select an asset type from a drop-down list.
Directory Server name and port	Lets you specify the name of the Directory Server and port. The required format to specify the servername and port is as follows: <servername>:port
Distinguished name	Lets you specify the distinguished name.

6 In the **Credentials** area of the Directory Server panel. enter the following information:

Username	Lets you enter the username for the Directory Server that you want to use.
Password	Lets you enter the password.
Confirm password	Lets you re-enter the password for confirmation.

Configuring data collectors for message-based data collection

In Control Compliance Suite 11.0, you must install a CCS agent to perform message based data collection.

The CCS agent installed on each computer in the enterprise network performs the actual task of data collection. The security content executables installed on the agents collect and evaluate the data and report the conformance of the assets with the security policies.The evaluated data is collected and presented in the form of messages.

You must configure your CCS setup for message based data collection.

To perform message based data collection

1. Register the CCS agent to a CCS Manager

2. Import assets and agents into the CCS Asset system.

   See "Importing assets and agents " on page 556.

3. Enable Message based content.

   Refer to Enabling message based data collection from the *Symantec Control Compliance Suite Installation Guide Version 11.0.*

Configuring platforms for data collection

This chapter includes the following topics:

Configuring data collection on UNIX platform

Configuring data collection on Windows platform

Installing Oracle Instant Client for data collection on Oracle

If you are collecting data on the Oracle platform, you require the Oracle Instant Client 10.2.0.4 files to run on the CCS Manager. If the files are not present on the CCS Manager then the data collection job for Oracle fails and the following error message is displayed:

```
Error(s) were encountered starting the BindView Information Server:

Module Control\Oracle\BVOOCCILoader.dll failed to load, reason:
```

```
Ensure that the Oracle Instant Client files are present on the
computer.
```

To install Oracle Instant Client 10.2.0.4

1. Locate the **Oracle Instant Client version 10.2.0.4** files on your Oracle product support website and download the **Instant Client Package - Basic** package.
2. Unzip the contents of the package to a directory at a known location.

   Note: Symantec reccomends that the Oracle Instant Client files must not be stored in the Control Compliance Suite installation directory.

3. Add the directory path to the PATH environment variable at system level.
4. Restart the CCS Manager.

See "Configuring data collection on UNIX platform" on page 337.

See "Configuring data collection on Windows platform" on page 338.

Configuring data collection on Oracle platform

Chapter 12

Configuring the general settings

This chapter includes the following topics:

- Configuring the job count settings
- Configuring the assets count settings

Configuring the data locations

Note: If you change the data location configuration, then you must synchronize the CCS Manager with the latest configuration. You can synchronize CCS Manager using the Sync Configuration option from the **Settings > General > CCS Manager** 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 418.

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.
- Remediation plan in risk management.
- Exception plan in risk management.

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 job types” on page 227.

See “About risk treatment” on page 1102.

Selecting the CCS Manager to synchronize the reporting database

You can select the CCS Manager 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 CCS Manager for data synchronization

1. Go to **Settings > General**.
2. In the **General** view, on the left panel, click **System Configuration > CCS Manager for Reporting Synchronization**.
3. On the right panel, select the CCS Manager that can be used for synchronization of the reporting database.

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.

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 > Purge Settings** panel.

The following are the different purge settings tabs in the **Purge Settings** panel:

Stale Data Settings for the global purge.

The number of days after which data is purged. The default value is 180 days.

Exceptions Settings for purging the exceptions data.

The exceptions data older than the number of days that is specified in the **Exceptions** tab is deleted. The default value is 180 days.

Standards Settings for purging the standards data.

The standards data older than the number that is specified in the **Stale Data** tab are deleted.

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 this tab are deleted.

The SCAP data evaluation results for job runs greater than the number that is specified in this tab are deleted.

Note: A purge of evaluations results does not re-compute summary statistics until another evaluation is executed.

Entitlements Settings for purging the historical entitlements data.

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.

The minimum value is 100 days and the maximum value is 9999 days.

System Audit Log

Settings for purging the historical audit log data.

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.

Baselines

Settings for purging the comparison results.

The comparison results older than the number of days that is specified in the **Baselines** tab is deleted. The default is 60 days.

Reports

Settings for purging the report results in the reporting database.

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.

The report results for runs greater than the number specified in the Reports tab are deleted.

Historical results form the reporting database are purged after the specified number of days.

Trend information from the reporting database is purged after the specified number of days.

See “About data purging in the reporting database” on page 346.

See “Configuring the purge settings” on page 344.

See “Configuring the purge job schedule” on page 346.

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 343.

To configure the purge settings

1 Go to **Settings > General**.

2 In the **General** view, on the left panel, click **Data Purge > Purge Settings**.

3 On the right panel, do the following:

Stale Data

Type the number of days after which the information in the production database is purged. The default value is 180 days.

The stale data setting is used as the default global purge setting. Some modules have their own purge settings.

Select the purge schedule options.

Exceptions

Type the number of days after which the exceptions data is purged. The default value is 180 days.

Standards

Type the number of data collection job runs, the results of which must be retained. The default value is 10

Type the number of data evaluation job runs, the results of which must be retained. The default value is 10.

Entitlements

Type the number of days after which the entitlements historical data is purged. The default value is 180 days.

The minimum value is 100 days and the maximum value is 9999 days.

System Audit Log

Type the number of days after which the historical audit log data is purged. The default value is 365 days.

Baselines

Type the number of days after which the baselines comparison result is deleted. The default is 60 days.

Reports

Type the number of report job runs, the results of which must be retained. The default value is 10.

Type the number of days after which the information in the reporting database is deleted.

Type the number of report job runs for which data must be retained. The default value is 10.

Type the number of days after which historical results from the reporting database must be purged. The default value is 180 days.

Type the number of days after which trend information from the reporting database must be purged. The default value is 2555 days (7 years).

4 On the **Purge Settings > Stale Data** tab, click **Execute Job** to run the job according to the selected schedule options.

See “Configuring the purge job schedule” on page 346.

About data purging in the reporting database

The data in the reporting database is classified into the following types, from the perspective of data purging :

- Historical results data
  The historical results data contains the historical results of the security assessment of an organization. This type of data is stored for a short period of time and archived, to be retrieved at a later stage, if required for audit purposes.
  The purge setting for historical results data is **Purge setting for purging historical results data**, and has a default value of 180 days.
- Trend data
  Trend data contains the trend information of the security assessment data of the organization over a period of time. This type of data is retained for a long period of time, as the trend information helps organizations to determine the extent of security policy compliance over a period of time.
  The new purge setting for trend data is **Purge setting for purging trend information**, which has a default value of 2555 days (7 years).

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 > 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 **Execute Job** to save the settings and run the job that is based on the settings.

Note: If you run the purge job while a reporting synchronization job is running, then the purge job fails. If a reporting synchronization job is running, then you must run the purge job only after the synchronization job is complete.

See "About the purge settings" on page 343.

See "Configuring the purge settings" on page 344.

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 Due to system failure the status of some control points are left in the Entitlement Import Pending status.

Select this option to change the status of the control points with status Entitlement Import Pending to Entitlement Import Required.

See “About entitlements” on page 603.

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 152.

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 956.

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:

Expire policies after

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 must be reviewed within

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.

Run the daily policies update job at

Select the daily scheduled time to run a policy job.

Show expired policies

Select the option to display the list of expired policies.

Notifications

You can configure the notifications that are sent to the assigned policy users at different stages of the policy life cycle. The notifications are meant to inform the user about the status of the policy. The notifications are sent as an email.

- **Notification type**
  Select the type of policy notification.
- **Subject**
  You can type the subject of the email notification.
- **Message**
  You can customize the message of the policy.

Note: Policy notifications are sent only if the **From email address** is specified in **Settings > General > System Configuration > Email Notifications**.

See “Configuring the email Notification Server ” on page 341.

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	Define a threshold for each status level of Standards and bv-Control query. The four possible security assessment status levels for the dashboard are: ■ Critical ■ Danger ■ Warning ■ Normal 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.
Global Job Settings tab	Type the maximum number of update jobs that can be assigned to each CCS Manager in the Reporting role.

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.

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 standard information in the details pane" on page 655.

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.

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 505.

Chapter 13

Configuring queries

This chapter includes the following topics:

Configuring queries

Control Compliance Suite provides the Create or Edit Query wizard to configure queries. Use the panels in the wizard to complete the tasks of query configuration.

Table 13-1 tabulates the tasks that you need to complete to configure queries.

Table 13-1 Tasks in query configuration

Step	Action	Description
Step 1	Configure identifiers and query location	Provide a name and description for the query, along with a location. See "Configuring query name and description" on page 356.
Step 2	Configure query platform and properties	Provide the platform, entity, and fields for the query. See "Configuring platform and query properties" on page 357.
Step 3	Configure query scope	Define the extent of operation for the query. See "Configuring the scope of queries" on page 358.

Table 13-1 Tasks in query configuration *(continued)*

Step	Action	Description
Step 4	Configure query filters	Provide the filters to exclude unwanted data from query results. See "Configuring query filters" on page 359.
Step 5	Configure sort order for query results	Provide an order in which to sort query results. See "Configuring sort order for query results" on page 360.
Step 6	Configure query schedule	Schedule query runs. See "Configuring query schedules" on page 360.
Step 7	Configure actions for query results	Provide the settings for the notification, attachment to emails, and export of query results. See "Configuring actions for query results" on page 361.
Step 8	Review query definition	Review the parameters that you configured for the query. See "Reviewing query configurations" on page 362.

See "About queries" on page 144.

Configuring query name and description

Queries need identifiers. The distinguishing features of a query are its name and description. The identifiers and the folder in which the query is saved help to locate a query.

To configure query name and description

1. To get the Queries page, on the Control Compliance Suite home page, point to **Manage**, and click **Queries**.
2. To get the Create or Edit Query wizard and create a query, do one of the following:.
   - In the **Queries** folder pane, right-click a folder and click **Create Query**.
   - On **Query Tasks**, click **Create Query**.
3. On the **Name and Description** panel, in the **Name** and **Description** fields, enter a name and a description for the query.
4. To enter the location in which to save the query, click the button alongside the **Save in** field.
5. On **Select Folder**, select a folder and click **OK**.
6. Click **Next**.

See “Configuring queries” on page 355.

See “About queries” on page 144.

Configuring platform and query properties

A query configuration needs include the platform, entity, and fields for the query.

Control Compliance Suite supports query operations on the Windows, SQL, UNIX, and Oracle platforms. Every platform has its entities. An entity contains the fields that define the attributes or properties of the objects. A query configuration requires at least one field.

To get the description of a field, select the field. For example: For Windows, select **Device Driver Name** to see the description, 'This field returns the internal name of the device driver.' Selected fields appear ticked.

To configure query attributes

1. On the **Entity and Fields** panel of the Create or Edit Query wizard, in the **Platform** field, enter the platform that you want to query.
2. In the **Entity** field, from the list of entities for the selected platform, enter the entity that you want to query.

   Click the button alongside the **Entity** field to access the **Entity Browser**.
3. In **Available Fields**, select fields and click the right arrow to include them in the list of **Selected fields**.

   To move all fields, click the double arrows.

4 In the **Selected fields** pane, use the up and down arrows to provide the order for the results.

5 To view all platforms, entities and fields in **Entity Browser**, click **View all platforms, entities, and fields**.

Otherwise, the system only displays the entities and the associated fields of the selected platform. Use **Entity Browser** to find the entity and platform of any field.

6 Click **Next**.

See “Configuring queries” on page 355.

See “About queries” on page 144.

Configuring the scope of queries

The scope of a query defines the extent of its operation. Select an asset container, asset group, a single asset, or multiple assets to define the scope of a query. Scope selection filters the assets on the basis of the platform and the entity that you selected. Control Compliance Suite limits the support for scope definition to assets from the asset system. Use the **Additional Scope** option to specify the filters and refine the query down to the level of file path, file name, or service name. **Additional Scope** provides the predefined scope for the selected asset type.

To configure the scope of a query

1 On the **Asset Scope** panel, from the asset system , select the assets, asset groups, or asset containers, and click **Add**.

2 To add all available items, click **Add All**.

3 To remove one scope item, in the **Selected Items** table, select the item and click **Remove**.

4 To remove all items from the **Selected Items** table, click **Remove All**.

5 To get the **Additional Scope** box that displays more items for scope definition, click **Additional Scope**.

6 In the **Scope to** field, select the scope option, and click the Plus (+) button to see the option that is displayed in the **Additional scope** pane.

7 On Additional Scope, click **Add**, and then **Add**.

8 To change the additional scope you that you specified, select the scope item in the **Additional scope** pane.

9 Make the required changes in the **Scope options** pane, and click the button with the save icon.

10 To conclude the configuration at **Asset Scope**, click **Finish**, and then on **Question** click **Yes**.

11 To configure filters for query results, click **Next**.

See "Configuring queries" on page 355.

See "About queries" on page 144.

Configuring query filters

Query management provides filters for the results of data collection. Configure filters for a query to get only the data records that you require. Filters consist of one or more filter terms. Select a value or a group of values to define a filter term. The term values of filters define the data that the query returns.

The list of operators that **Add Filter Statement** displays for a filter depends on the field that you selected for the query.

Control Compliance Suite makes available the following types for condition parameters:

- Specific Value: Finds the records that match a specific criterion
- Special Value: Finds the records that match a specific exception condition
- Ordinal Value: Finds the records that differ for specific users

Note: Filters are optional parameters in query configuration.

To configure filters for a query

1. On the **Result Filter** panel, enter a filter from the list and click **Add Statement**.
2. In **Add Filter Statement**, select a type for the condition parameter.
3. Enter the operator for the filter definition.
4. In the **Specify value** field, enter the value that completes the filter condition.
5. On **Add Filter Statement**, click **OK**.
6. To conclude the configuration at **Result Filter**, click **Finish**, and then on **Question** click **Yes**.
7. To configure a sort order for query results, click **Next**.

See "Configuring queries" on page 355.

See "About queries" on page 144.

Configuring sort order for query results

Configure a sort order to organize the records of query results. A sort order depends on the contents of one or more keys in each record. A key is a unique identifier for a record that Control Compliance Suite collects for an object. The use of the same identifier for many records results in the duplication of keys. Use the options in the **Select Duplicate Key Options** section to define how records with duplicate keys are included in the data that the query returns.

Control Compliance Suite provides the following options for duplicate keys:

- Allow Records with Duplicate Key: Includes all records irrespective of key duplication
- Only Allow Records with Duplicate Key: Includes only the records with duplicate keys
- Suppress Records with Duplicate Key: Includes the first record of a key and excludes the second record

The **Sort order** pane accommodates only six fields. In query configuration, the sort order is an optional parameter.

To configure a sort order for query results

1. On the **Result Sort Order** panel, select fields from **Selected fields**, and click the right arrow to move the fields to the **Sort order** pane.
2. To provide the order for sorting, use the following options:
   - The Ascending option or the Descending option to provide an order for the records of a field
   - The up arrow and the down arrow to move the selected field either up or down the order
3. Select a duplicate key option.
4. To conclude the configuration at **Result Sort Order**, click **Finish**, and then on **Question**, click **Yes**.
5. To configure a schedule for query runs, click **Next**.

See “Configuring queries” on page 355.

See “About queries” on page 144.

Configuring query schedules

Control Compliance Suite facilitates the configuration of a schedule for query runs. If you configure the **Run now** option for a query during its configuration, the query runs upon the completion of the configuration. You also receive a desktop notification of the query start.

To schedule the query run

1 For one immediate run, on the **Query Run Schedule** panel, , select **Run now**.

2 To schedule query runs, select **Run periodically**, and in the **Start on** field, enter the start time for the run.

3 To schedule a one-time run, in **Run Periodically Options**, select **Run once**.

4 To schedule recurrent runs, in the **Run every__ days** field, enter the interval for the runs.

5 To conclude the query configuration at this panel, click **Finish**, and then on **Question**, click **Yes**.

6 To configure actions for query results, click **Next**.

See "Configuring queries" on page 355.

See "About queries" on page 144.

Configuring actions for query results

Control Compliance Suite supports the following actions on query results:

- Notification of the success or failure of query configuration
- Attachment of query results to email messages
- Export of query results
  Control Compliance Suite supports the export of query results in the following formats: PDF, Comma-separated values, Excel, Word, and XML.

To configure notification, attachment to email, and export of results

1 To export the query results or to send them as an email attachment, in the **Notification and Result Format** panel, click **Results**.

2 To send the query results as an email attachment, check **Send query results as email attachment**.

3 In the **From** and **To** fields, enter the email addresses of the sender and the recipient.

4 To export the query results, check **Export query results**.

5 To enter the location in the **Export path** field, click the browse button alongside the field.

6 On **Browse for Folder**, select the location to which you want the results exported, and then click **OK**.

7 In the **Format** field, enter the format in which you want the results exported.

8 To send a notification for the success or failure of the query job, click **Notification**, and then click **Success** or **Failure**.

9 Check **Send Notification**, and in the **From** and **To** fields, enter the email addresses of the sender and the recipient.

10 To conclude the query configuration at this panel, click **Finish**, and then on **Question**, click **Yes**.

11 To review the configuration, click **Next**.

See "Configuring queries" on page 355.

See "About queries" on page 144.

Reviewing query configurations

Control Compliance Suite provides the **Review the selected options** panel to facilitate the review of the query configuration before you commit the configuration.

To review and complete query configuration

1 On the **Review the selected options** panel, review the configurations for the query.

2 To modify the configuration, click **Back** and return to the previous panel.

3 To exit the wizard, click **Cancel**.

4 To cancel the configuration, on **Cancel Wizard**, click **OK** and to confirm the cancellation, click **Yes** on **Warning**.

5 To complete the configuration of the query, and receive confirmation of query configuration, click **Finish**.

6 On **Information**, click **OK**.

See "Configuring queries" on page 355.

See "About queries" on page 144.

Chapter 14

Configuring Symantec Workflow

This chapter includes the following topics:

- Configuring Symantec Workflow with CCS

Configuring Symantec Workflow with CCS

Control Compliance Suite(CCS) can be integrated with an existing installation of Symantec Workflow for handling risk action plans and policy management. You can submit risk action plans and policies by the integrated Symantec Workflow for further action. The workflow handles the action plan and provides a status update to CCS. You can submit the policies for review and approval using the workflow. The status of the action plan can be viewed on the **Action Plans** page.

The status of the policies can be viewed in the Policy view of the CCS Web Console.

To configure a Symantec Workflow

1 Go to **Settings > General**.

2 In the General view, on the left panel, click **System Configuration > Symantec Workflow**.

The **Symantec Workflow** page is displayed in the right pane.

3 On the right panel, do the following:

Workflow Name	Type the name of the workflow. This is a required field.
Workflow Description	Type the description of the workflow.

Workflow URL	Type the correct URL of the workflow system
Workflow Type	Select the type of workflow. ■ Action Plan ■ Policy
User Name	Type the user name to access the workflow system
Password	Type the password to access the workflow system
Re-enter Password	Confirm the password.

4 Click **Add** to create the workflow.

The newly created workflow is displayed in a grid along with the existing workflows.

Select a workflow from the list to **Edit** or **Delete** it.

Note: You must configure a default remediation system where you want to submit the remediation plan. See "Configuring a default system for treating risks" on page 1108.

Configuring credentials

This chapter includes the following topics:

About Credential Management

CCS lets you manage credentials for agent-less and agent-based targets at a central location.

Credentials can be used for the following objectives:

- To configure credentials for assets, for assets in a domain, for asset in a folder, and for all assets of a particular type
- To store user name and password for Windows, UNIX, SQL, and Oracle users centrally and use them in platform configuration

See "RBAC for managing credentials" on page 365.

See "About the Credentials view" on page 369.

See "About the View Saved Passwords panel" on page 382.

RBAC for managing credentials

CCS provides role based access control (RBAC) for managing credentials.

RBAC comprises the roles over the tasks which in turn provide you certain priviledges while accessing a workspace. The following tasks are assigned to CCS Administrator and CCS Power Users for accessing Credentials workspace.

- Manage Credentials
- View Credentials
- Manage Shared Credentials
- View Shared Credentials

CCS does not provide any predefined roles for managing credentials. You can create custom roles using the Roles workspace.

CCS provides the following validations for the predefined tasks:

Table 15-1 Tasks and their validations

Task	Validation
Manage Credentials	You can update assets and platform credentials. You can also save credentials for reuse.
View Credentials	You can only view and use the platform credentials.
Manage Shared Credentials	You can update shared credentials.
View Shared Credentials	You can only view and use the saved credentials. **Note:** For View Shared Credentials task, you must have access rights over the View Credentials task.

See "About the Credentials view" on page 369.

See "About the View Saved Passwords panel" on page 382.

About configuring the credentials for a platform

You need credentials mainly for accessing the network assets and secondary assets. For instance, Windows machine, Windows file. However, you have to configure the credentials which can be used to collect information for the assets.

The configuration of credentials involves the following steps:

- Navigate to **Credentials** view.

- Specify the credentials for the domain and the asset folder for which the data needs to be collected.
- Save the given credentials as passwords.
- Specify name and description for the saved passwords.

See "Adding common credential" on page 372.

See "Editing common credential" on page 375.

See "Deleting credential" on page 376.

About credential usage

CCS data collection requires credentials to collect information from the common platforms. A single platform credential can be used for multiple operations. The usage of crdentials is across platforms.

Saved Passwords

You can save the credential by assigning a user name and a passwords to it. If stored credentials are available then you can reuse it instead of entering the user name and the password again. Hence instead of asking the administrator to enter the credentials at multiple places, you can use the stored credentials seamlessly.

Default credentials

Using General Query Credential in Windows, SQL, UNIX, and Oracle you can use a single account credentials for asset system.

You can use the credentials (User name and Password) for the following objectives:

Windows

- For querying domain or machine information

UNIX

- For querying machine information

Microsoft SQL

- For querying MS SQL database information

Oracle

- For querying Oracle database information

See "About the Credentials view" on page 369.

See "About the View Saved Passwords panel" on page 382.

About credential management for agent-based targets

For a given asset the credentials are required for one of the following objectives:

- For querying the information of the target computer
- For querying the information of the applications such as SQL on the target computer

For agent-based assets, you can do the following:

- Configure credentials locally on the target:

  CCS provides a utility for each platform which lets you configure credentials on the target computer. You can select type of credentials for configuration, specify username and password, specify password expiry. After you configure the credentials using the given utility, the tag Use Local Credentials is set on the target and all data collection jobs for that particular platform start using local credentials.

  For agent-based assets, you can either use agent side credential for a platform, use CCS side credential, or do not use credentials at all. The agent-based credential support is available only for UNIX and Windows platform.
- Use centralized credentials:

  You can use credentials saved in CCS credential database using the Credentials workspace. If local credentials are not configured, data collection job attempts to resolve credentials for the target at CCS Manager. If configured local credentials are available, they passed on to the agent along with the job for reuse.

  CCS Manager fetches information from Application Server.

  Besides the above-mentioned options, for Windows fallback option can be used to collect data.

See "About the Credentials view" on page 369.

About assigning credentials to assets

CCS supports assigning credentials at asset level and at folder level. For most of the platforms the saved passwords are available for reuse.

For example, for SQL you can configure credentials as follows:

- SQL Server level Credential

  You can select required SQL servers and assign the credentials.
- Domain level Credential

  If there is a single domain account which has access to all the SQL Servers then you need not configure the credentials at server level. Instead you can specify the domain name and the credentials. In this case all the SQL Servers in that domain uses the configured credentials. During query execution if you do not find server level credentials for a SQL server, then credentials configured for its domain can be used. So server level credentials can take over domain level credentials.

- General Query Credential
  If there is an account which can be used across all domains in an enterprise, then you can configure that credentials which can be used for all SQL Server instances in the query. During query execution if there are no server level credentials as well as domain level credentials, then credentials configured for General Query can be used.

Note: Asset credential for SQL requires SQL and Windows authentication while platform credential for SQL requires only Windows authentication.

See "Adding asset credential" on page 376.

See "Editing asset credential" on page 381.

See "Removing assets from the platform credential" on page 382.

About the Credentials view

The Credentials view lets you manage the credentials in the Control Compliance Suite.

The **Credentials** view displays the common platform credentials, the assets that are applied to the credentials, and the common platforms. You can access the **Credentials** view by navigating through the **Settings > Credentials** menu of the console.

The following table describes the panes that are available in the **Credentials** view:

Table 15-2 Credentials view

Pane	Description
Filters	This pane appears on the left side of the console window under the navigation bar. This pane displays the platforms. You can select Oracle, SQL, UNIX, and Windows platform for filtering the platform specific credentials.

Table 15-2 Credentials view *(continued)*

Pane	Description
Platform Credentials	This pane appears in the right side of the console window under the taskbar . This pane displays the information on Credential, Platform, Type, Configured for, Created by, Creation date, and Last modified date of the platform credentials.
Assets	This pane appears in the lower-right side of the console window under the Platform Credentails pane. This pane displays the information on the assets which are applied to the platform credentials.

The **Filters** pane displays the following platforms:

- Oracle
- SQL
- UNIX
- Windows

You can add or remove assets for a platform credential in the Applied Assets pane.

You can screen platform wise credentials using the Filters.

The following table contains information on the options that are available on the taskbar of the Platform Credentials view and their descriptions.

Table 15-3 Options in the Credentials taskbar and their descriptions

Options	Descriptions
Add Common Credential	Lets you add a platform credentials to CCS.
Add Asset Credential	Lets you add an asset credential to CCS.
Edit Credential	Lets you edit the asset and platform credentials.
Delete Credential	Lets you delete asset and platform credentials from CCS.
View Saved Passwords	Lets you add and update the shared credentials in CCS.

The following table contains information on the columns available in the **Platform Credentials** pane.

Table 15-4 Columns in the Platform Credentials pane and their descriptions

Column name	Description
Credential	Displays the details of a platform credential.
Platform	Displays the module name of a platform credential.
Type	Displays the type of a platform credential.
Configured for	Displays the number of assets associated with the platform credential.
Created by	Displays the name of an user who created or added the platform credential to CCS.
Creation date	Displays the date on which the platform credential was created.
Last modified date	Displays the date on which the platform credential was modified most recently.

The following table contains information on the assets which are applied to the specified platform credential.

Table 15-5 Columns in the Assets pane and their descriptions

Columns	Descriptions
Asset	Displays the name of an asset.
Asset type	Displays the type of an asset.

Note: In the Assets pane, you can click **Add Assets** to add assets to the selected platform credential and

you can click **Remove Assets** to remove assets from the selected platform credential.

See "About the View Saved Passwords panel" on page 382.

See "About configuring the credentials for a platform" on page 366.

See "About credential usage" on page 367.

See "About credential management for agent-based targets" on page 368.

See "About assigning credentials to assets" on page 368.

See "Adding common credential" on page 372.

See "Editing common credential" on page 375.

See "Deleting credential" on page 376.

See "Adding asset credential" on page 376.

See "Editing asset credential" on page 381.

See "Removing assets from the platform credential" on page 382.

See "RBAC for managing credentials" on page 365.

Adding common credential

You can add common platform credentials using the **Add Common Credential** panel.

To add platform credential

1 Go to **Settings > Credentials**.

2 On the taskbar, click **Add Common Credential**.

3 In the **Add Common Credential** panel, enter the following information and then click **OK**.

Table 15-6 Add Common Credential

Field	Description
Platform	Select the platform type for adding platform credential to CCS. The following platform types are available for selection: ■ SQL ■ Windows ■ UNIX ■ Oracle

Table 15-6 Add Common Credential *(continued)*

Field	Description
Configure for	Configure the selected platform for the given credential options. For details on credential options, refer to Table 15-7 Table 15-8 Table 15-9 Table 15-10 **Note:** For UNIX platform, you need to configure query as well as connection credentials for data collection jobs to work properly.
Authentication	Select the authentication type for the specifed platform. For details on authentication types, refer to Table 15-11
Credentials	Specify the platform specific credentials. For details on platform credentials, refer to Table 15-12 **Note:** You can save password or you can browse password by clicking the arrow button.

Table 15-7 Oracle Platform

Platform Credential option	Description
All databases	Configures credential for all Oracle databases.

Table 15-8 SQL Platform

Platform Credential option	Description
All servers in the domain	Configures credential for all SQL servers in specified domain.
All servers	Configures credential for all SQL servers.

Table 15-9 UNIX Platform

Platform Credential option	Description
Connecting to all UNIX machines	Configures credential for connecting to all UNIX machines.
Performing data collection from all UNIX machines	Configures credential for performing data collection from all UNIX machines.

Table 15-10 Windows Platform

Platform Credential option	Description
All machines in the domain	Configures credential for all Windows machines in the specified domain.
All machines	Configures credential for all Windows machines.

Table 15-11 Authentication Type

Platform	Authentication Type
Oracle	Oracle
SQL	SQL
UNIX	UNIX or Certificate
Windows	Windows

Table 15-12 Credentials

Field	Value
Domain **Note:** Domain field is applicable only for Windows and SQL.	Specify the domain for the selected platform.
User name	Specify the user name for the selected platform.
Certificate **Note:** Certificate field is applicable only for UNIX.	Browse and select the certificate if you have selected Certificate authentication type for UNIX platform.

Table 15-12 Credentials *(continued)*

Field	Value
Password or Passphrase	Specify the password or passphrase for the selected platform or Specify the passphrase for UNIX certificate.
Confirm Password or Confirm Passphrase	Specify the same password or passphrase which you entered in the Password or Passphrase field.

See "Editing common credential" on page 375.

See "Deleting credential" on page 376.

Editing common credential

You can edit common platform credentials using the **Edit Platform Credential** panel.

To edit platform credential

1 Go to **Settings > Credentials**.

2 On the taskbar, click **Edit Credential**.

3 In the **Edit Credential** panel, enter the following information and then click **OK**.

Table 15-13 Edit Common Credential

Field	Description
Credentials	Specify the platform specific credentials. For details on platform credentials, refer to Table 15-12 **Note:** You can save password or you can browse password by clicking the arrow button. For more information, refer to See "About assigning credentials to assets" on page 368.

Table 15-14 Credentials

Field	Value
Domain **Note:** Domain field is applicable only for Windows and SQL.	Specify the domain for the selected platform.
User name	Specify the user name for the selected platform.
Certificate **Note:** Certificate field is applicable only for UNIX.	Browse and select the certificate if you have selected Certificate authentication type for UNIX platform.
Password or Passphrase	Specify the password or passphrase for the selected platform or Specify the passphrase for UNIX certificate.
Confirm Password or Confirm Passphrase	Specify the same password or passphrase which you entered in the Password or Passphrase field.

See "Adding common credential" on page 372.

See "Deleting credential" on page 376.

Deleting credential

You can delete platform credentials using the Delete Platform Credential panel.

To delete platform credential

1 Go to **Settings > Credentials**.

2 In the **Platform Credentials** pane, select the credential which you want delete.

3 On the taskbar, click **Delete Credential**.

The selected credential disappears from the **Platform Credentials** pane.

See "Adding common credential" on page 372.

See "Editing common credential" on page 375.

Adding asset credential

You can add asset credentials using the Add Asset Credential wizard.

Note: You must have user access rights to View Assets task for adding asset credentials.

To add asset credential

1. Go to **Settings > Credentials**.
2. On the taskbar, click **Add Asset Credential**.
3. In the **Add Asset Credential: Specify Platform Credential** panel, enter the required information and then click **Next**.

   See "Specifying platform credentials" on page 378.

   Note: If Oracle is hosted on an UNIX platform, you must configure query as well as connection credentials for data collection jobs to work properly.

4. For UNIX platform, in the **Add Asset Credential: Select Action** panel, select the required option and then click **Next**

   Note: For UNIX platform, you need to configure query as well as connection credentials for data collection jobs to work properly.

   See "Using asset credentials for UNIX platform" on page 381.

5. In the **Add Asset Credential: Select Assets** panel, select and add assets. You can select one or more specific assets of the selected asset type as the asset scope. If credential conflict occurs for the selected assets, in the **Add Asset Credential: Resolve Credential Conflict** panel select the required option and then click **Next**.

   See "Resolving credential conflict" on page 380.

6. In the **Summary** panel, click **Finish**. You can use the **Back** option to go back and change the configurations.

Note: You can also add asset credential to the asset container level from Assets view.

See "Editing asset credential" on page 381.

See "Removing assets from the platform credential" on page 382.

Specifying platform credentials

You need to specify platform credentials while adding asset credentials.

The **Add or Edit Asset Credential: Specify Platform Credential** panel lets you select the platform for updating an asset credential.

Table 15-15 Add or Edit Asset Credential: Specify Platform Credential

Field	Description
Platform	Select the platform type for adding platform credential to CCS. The following platform types are available for selection: ■ SQL ■ Windows ■ UNIX ■ Oracle **Note:** This field is not available for editing an asset credential.
Configure for	Configure the selected platform for the given credential options. For details on credential options, refer to Table 15-7 Table 15-8 Table 15-9 Table 15-10 **Note:** This field is not available for editing an asset credential.
Authentication	Select the authentication type for the specifed platform. For details on authentication types, refer to Table 15-11 **Note:** This field is not available for editing an asset credential.

Table 15-15 Add or Edit Asset Credential: Specify Platform Credential *(continued)*

Field	Description
Credentials	Specify the platform specific credentials. For details on platform credentials, refer to Table 15-12 **Note:** You can save password or you can browse password by clicking the arrow button.

Table 15-16 Oracle Platform

Platform Credential option	Description
All databases	Configures credential for all Oracle databases.

Table 15-17 SQL Platform

Platform Credential option	Description
All servers in the domain	Configures credential for all SQL servers in specified domain.
All servers	Configures credential for all SQL servers.

Table 15-18 UNIX Platform

Platform Credential option	Description
Connecting to all UNIX machines	Configures credential for connecting to all UNIX machines.
Performing data collection from all UNIX machines	Configures credential for performing data collection from all UNIX machines.

Table 15-19 Windows Platform

Platform Credential option	Description
All machines in the domain	Configures credential for all Windows machines in the specified domain.
All machines	Configures credential for all Windows machines.

Table 15-20 Authentication Type

Platform	Authentication Type
Oracle	Oracle
SQL	SQL
UNIX	UNIX or Certificate
Windows	Windows

Table 15-21 Credentials

Field	Value
Domain **Note:** Domain field is applicable only for Windows and SQL.	Specify the domain for the selected platform.
User name	Specify the user name for the selected platform.
Certificate **Note:** Certificate field is applicable only for UNIX.	Browse and select the certificate if you have selected Certificate authentication type for UNIX platform.
Password or Passphrase	Specify the password or passphrase for the selected platform or Specify the passphrase for UNIX certificate.
Confirm Password or Confirm Passphrase	Specify the same password or passphrase which you entered in the Password or Passphrase field.

See “Adding asset credential” on page 376.

See “Editing asset credential” on page 381.

Resolving credential conflict

You need to resolve the credential conflict while adding the asset credentials.

The **Add or Edit Asset Credential: Resolve Credential Conflict** panel lets you resolve credential conflict for all assets.

Table 15-22 Add or Edit Asset Credential: Resolve Credential Conflict

Action	Description
Preserve configuration for all assets	Preserves previous credential configuration for all assets and ignores the current credential configuration.
Overwrite configuration for all assets	Overwrites previous credential configuration for all assets and applies the current credential configuration.

See "Adding asset credential" on page 376.

See "Editing asset credential" on page 381.

Using asset credentials for UNIX platform

You have to specify the credential usage for UNIX while updating asset credentials.

The **Add or Edit Asset Credential: Select Action** panel lets you select an action for credential usage.

Table 15-23 Add or Edit Asset Credential: Select Action

Field	Description
Establish connection	Establishes a connection with the asset.
Perform data collection	Performs data collection from the asset.

Note: For UNIX platform, you need to configure query as well as connection credentials for data collection jobs to work properly.

See "Adding asset credential" on page 376.

See "Editing asset credential" on page 381.

Editing asset credential

You can edit asset credentials using the **Edit Credential** wizard.

To edit asset credential

1 Go to **Settings > Credentials**.

2 On the taskbar, click **Edit Asset Credential**.

3 In the **Edit Asset Credential** panel, enter the required information and then click **Next**.

See “Specifying platform credentials” on page 378.

4 For UNIX platform, in the **Edit Asset Credential: Select Action** panel, select the required option and then click **Next**

See “Using asset credentials for UNIX platform” on page 381.

5 In the **Edit Credential Association: Select Assets** panel, add or remove assets for the association. You can select one or more specific assets of the selected asset type as the asset scope. If credential conflict occurs for the selected assets, in the **Edit Asset Credential: Resolve Credential Conflict** panel select the required option and then click **Next**.

See “Resolving credential conflict” on page 380.

6 In the **Summary** panel, click **Finish**. You can use the **Back** option to go back and change the configurations.

See “Adding asset credential” on page 376.

See “Removing assets from the platform credential” on page 382.

Removing assets from the platform credential

You can remove assets which are applied to the platform credentials from the **Applied Assets** pane.

To remove asset

1 Go to **Settings > Credentials**.

2 In the **Assets** pane, select the assets which you want remove.

3 Click **Remove Assets**.

The selected assets disappear from the **Assets** pane.

See “Adding asset credential” on page 376.

See “Editing asset credential” on page 381.

About the View Saved Passwords panel

The View Saved Passwords panel lets you manage the passwords in the Control Compliance Suite.

The **View Saved Passwords** panel displays the shared credentials. You can access the **View Saved Passwords** panel by navigating through the **Settings > Credentials > View Saved Passwords** menu of the console.

The following table describes the panes that are available in the **View Saved Passwords** panel:

Table 15-24 View Saved Passwords panel

Pane	Description
Count	This pane appears in the console window under the taskbar . This pane displays the information on Name, Credential, Type, Description, Created by, Creation date, and Last modified date of the shared credentials.

The following table contains information on the options that are available on the taskbar of the View Saved Passwords panel and their descriptions.

Table 15-25 Options in the View Saved Passwords taskbar and their descriptions

Options	Descriptions
Add	Lets you add a password to CCS.
Edit	Lets you edit a password.
Delete	Lets you delete a password from CCS.

The following table contains information on the columns available in the **Count** pane.

Table 15-26 Columns in the Count pane and their descriptions

Column name	Description
Name	Displays the name of a shared credential.
Credential	Displays the details of a shared credential.
Type	Displays the type of a shared credential.
Description	Displays the information related to the shared credential.
Created by	Displays the name of an user who created or added the shared credential to CCS.
Creation date	Displays the date on which the shared credential was created.

Table 15-26 Columns in the Count pane and their descriptions *(continued)*

Column name	Description
Last modified date	Displays the date on which the shared credential was modified most recently.

See "About the Credentials view" on page 369.

See "Adding password" on page 384.

See "Editing password" on page 385.

See "Deleting password" on page 385.

Adding password

You can add password using the **Add Password** panel.

To add password

1 Go to **Settings > Credentials**.

2 Click **View Saved Passwords**.

3 Right-click and select **Add**.

In the **Add** panel, enter the following information and then click **OK**.

Table 15-27 Add Password

Field	Description
Name	Specify the name of the shared credential.
Description	Specify the description of the shared credential.
Type	Select the type of credential which is to be shared. The following credentials are available for selection: ■ Oracle User ■ SQL User ■ UNIX User ■ Windows User
User Name	Specify the user name.
Password	Specify the password.

Table 15-27 Add Password *(continued)*

Field	Description
Confirm Password	Specify the same password which you entered in the Password field.

See "Editing password" on page 385.

See "Deleting password" on page 385.

Editing password

You can edit password using the **Edit Password** panel.

To edit saved password

1. Go to **Settings > Credentials**.
2. Click **View Saved Passwords**.
3. Right-click and select **Edit**.

In the **Edit** panel, enter the following information and then click **OK**.

Table 15-28 Edit Password

Field	Description
Name	Edit the name of the shared credential.
Description	Edit the description of the shared credential.
User Name	Specify the user name.
Password	Specify the password.
Confirm Password	Specify the same password which you entered in the Password field.

See "Adding password" on page 384.

See "Deleting password" on page 385.

Deleting password

You can delete password using the **Delete Password** panel.

To delete password

1. Go to **Settings > Credentials**.
2. In the **View Saved Passwords** panel, select the credential which you want delete.
3. On the taskbar, click **Delete**.

The selected credential disappears from the **View Saved Passwords** panel.

See “Adding password” on page 384.

See “Editing password” on page 385.

Configuring the databases

This chapter includes the following topics:

Configuring the production database connection settings

You can modify the SQL Server settings of the production database that is initially configured in the Installation Wizard.

Note: If you change the SQL Server credentials, you must recycle the CCS_WebAppPool from the IIS manager on the Web server computer.

Use the settings to set up a new server. The data is not automatically migrated to the new database.

To configure the production database settings

1. Go to **Settings > Secure Configuration > Production 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.

If you change the SQL Server credentials, you must recycle the CCS_WebAppPool from the IIS manager on the Web server computer.

You cannot specify the following special characters for the User name and the Password fields:

- Semicolon (;)
- Double quotes (")

Connection timeout interval

Type the number of minutes after which the server terminates the connection attempt.

The default timeout interval is 30 minutes.

3 Click **Update** to save.

See “Production database” on page 55.

Configuring the reporting database connection

You can modify the SQL Server settings of the reporting database that is initially configured in the Installation Wizard .

Note: If you change the SQL Server credentials, you must recycle the CCS_WebAppPool from the IIS manager on the Web server computer.

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.

If you change the SQL Server credentials, you must recycle the CCS_WebAppPool from the IIS manager on the Web server computer.

You cannot specify the following special characters for the User name and the Password fields:

- Semicolon (;)
- Double quotes (")

Connection timeout interval	Type the number of minutes after which the server terminates the connection attempt and the query execution. The default timeout interval is 120 minutes.

3 Click **Update** to save.

See “Reporting database” on page 56.

Configuring Response Assessment Module

This chapter includes the following topics:

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.

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.

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.

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.

Section 4

Achieving your business goals with Control Compliance Suite

Evaluating assets

This chapter includes the following topics:

Evaluating assets

Evaluation of assets lies in the core of the Control Compliance Suite. CCS offers capabilities to evaluate the assets against mapped control statements, predefined and custom standards, and against external data systems.

To use CCS for evaluating the assets in your organization, perform the following steps in the given order:

- Configure for asset import
  The configuration for asset import includes configuration based on the data collection mode that you want to use for collecting data on assets.
  See "Configuring for asset import" on page 452.
  You must configure the following data collectors for asset import if you select an agent-less way of data collection:
  - CSV
    See " Configuring the CSV data collector" on page 329.
  - ODBC
    See "Configuring the ODBC data collector" on page 331.
  - LDAP
    See "Configuring the Directory Server data collector" on page 333.

  If you want to use the raw-data based collection type for asset import, then you must configure the following data collectors:
  - Raw-data based collectors
    See " Configuring data collectors for raw data based data collection" on page 327.

If you want to use CCS agents to import assets and collect data, you must first register the CCS Agents with CCS Manager and perform the following steps:

■

- Import assets
  See “Importing assets” on page 440.
- Collect data about the imported assets based on your method of data collection and configure credentials for the imported assets before data collection.
  See “RBAC for managing credentials” on page 365.
  See “About the Credentials view” on page 369.
  See “About the View Saved Passwords panel” on page 382.
- Evaluate the data

Assessing compliance posture

This chapter includes the following topics:

- Assessing the security compliance
- Assessing the policy compliance

Assessing the security compliance

In CCS, the process of assessment of the compliance posture of your system begins with asset import and ends with creating a remediation plan.

To use CCS for assessing the compliance posture of your system, perform the following steps in the given order:

- Configure for asset import
  The configuration for asset import includes configuration based on the data collection mode that you want to use for collecting data on assets.
  See "Configuring for asset import" on page 452.
  You must configure the following data collectors for asset import if you select an agent-less way of data collection:
  - CSV
    See " Configuring the CSV data collector" on page 329.
  - ODBC
    See "Configuring the ODBC data collector" on page 331.
  - LDAP
    See "Configuring the Directory Server data collector" on page 333.

  If you want to use the raw-data based collection type for asset import, then you must configure the following data collectors:

  - Raw-data based collectors

    See " Configuring data collectors for raw data based data collection" on page 327.

  If you want to use CCS agents to import assets and collect data, you must first register the CCS Agents with CCS Manager and perform the following steps:

  -

- Import assets

  See "Importing assets" on page 440.

- Create standards

  You can create your own standard based on the pre-defined standards that are shipped with CCS or you can create a custom standard.

  See "Creating a new standard" on page 659.

- Collect data and configure credentials for the imported assets before data collection.

  See "RBAC for managing credentials" on page 365.

  See "About the Credentials view" on page 369.

  See "About the View Saved Passwords panel" on page 382.

- Evaluate the data

- View the evaluation results

  See "About the Evaluation Results view" on page 1063.

- Creating a remediation plan

Assessing the 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 with which the organization must comply.

To use CCS for assessing the policy compliance of your system, perform the following steps in the given order:

- Create a policy

  See "Creating a new policy" on page 902.

- Review the policy

  See "Reviewing a policy" on page 916.

- Create exceptions on policy

- Approve the policy

See “Approving a policy” on page 917.

- Map control statements to the policy
  See “Mapping policies to control statements” on page 1017.
- Map checks, questionnaires, and assessment procedures
  See “Mapping checks to control statements” on page 1019.
- View dashboards and report

Chapter 20

Working with external data

This chapter includes the following topics:

Managing the external data systems

- Define a new data system
  See "Configuring data systems" on page 761.
- Import a data system
  See "Importing an external data system " on page 769.
- Export a data system
  See "Exporting an external data system " on page 769.
- Import data from CSV
  See "Importing data using a CSV connector" on page 779.
- Get a risk score
  See "Using external data to contribute to the CCS asset Risk Score" on page 805.
- Get policy compliance
  See "Using external data for policy compliance" on page 804.

Section 5

Working with the Control Compliance Suite views

Chapter 21

Managing the Control Compliance Suite views

This chapter includes the following topics:

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 408.

See "About the Grid view" on page 411.

See "Navigating in the Map view" on page 409.

See "About the Map view icons" on page 410.

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 tasks from the **Map** view:

- Common tasks
  - Refresh
  - Configure platform settings
  - Save an image of the components layout.
    See "Saving an image of the configuration layout" on page 413.
  - Auto layout
  - Zoom in
  - Zoom out
  - Fit in window
- Infrastructure tasks
  - Register CCS Manager.
  - Unregister CCS Manager
  - Create sites.
    See "Creating a site" on page 323.
  - Sync configuration.
  - Refresh health and status information.
    See "Viewing the health and the status details" on page 416.
  - Monitor system jobs.

- Routing tasks
  - Configure routing

In addition to the above tasks, you can also perform the following tasks from the graphics that is displayed in the Map view.

- Modify the settings of a component
  See "Modifying the settings of a component " on page 412.
- View the details of the component
  See "Viewing additional component information" on page 412.

See "Navigating in the Map view" on page 409.

See "About the Map view icons" on page 410.

See "About the Grid view" on page 411.

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.
Auto layout	If the layout of all the components is not well balanced, clicking Auto Layout redraws the map.

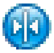
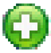
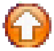
Refresh	You can refresh the Map view to display any changes to the component configurations since the view was selected. After a CCS Manager is registered, the CCS Manager status in the Map view and the Grid view does not reflect the updated status until you refresh the view. You can also view the status of the current configuration jobs that are running from the **Infrastructure Job Monitor** dialog box..

See “About the Map view” on page 408.

About the Map view icons

The Map view icons help visually to identify the different roles of the CCS Manager and the health status of the components.

The following table displays the CCS Manager role icons:

 CCS Manager Load Balancer	The CCS Manager with a blue icon depicts a CCS Manager Load Balancer. When the CCS Manager acts as a load balancer, the CCS Manager routes data collection jobs from the application server to a CCS Manager Collector. In addition, a load balancer routes the evaluation jobs to the CCS Manager Evaluator and the reporting jobs to the CCS Manager Reporter.
 CCS Manager Collector	The CCS Manager with a green icon depicts a CCS Manager Collector. The CCS Manager Collector is the interface to the programs that do the actual work of collecting data from the network.
 CCS Manager Evaluator	The CCS Manager with a red icon depicts a CCS Manager Evaluator. Evaluation jobs are sent from the application server to one of the CCS Manager Load Balancers. The CCS Manager Load Balancer then sends the evaluation job to the CCS Manager 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.

🟡	The CCS Manager with a yellow icon depicts a CCS Manager Reporter.
CCS Manager Reporter	The CCS Manager Reporter generates reports and dashboards for display by the Control Compliance Suite Console. In addition, a single CCS Manager Reporter is assigned to perform database synchronization between the production database and the reporting database test.
🟣	The CCS Manager with a purple icon depicts a CCS Manager External Data Connector.
CCS Manager External Data Connector	The CCS Manager External Data Connector is responsible for hosting the external data integration framework and serve as a means to collect data from any external data system.

The following table displays the heath status icons of the components:

✅	Indicates a healthy status.
⚠	Indicates that the component needs attention. For example: There can be a version mismatch of the application server and the CCS Manager server.
❗	Indicates that the component has failed the health status check.
❓	Indicates that system cannot get a status on the component.

After a CCS Manager is registered, the CCS Manager 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..

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 CCS Manager.
- Sync configuration.

- Modify or view the settings of each component.
  See “Modifying the settings of a component ” on page 412.
- Create site.
  See “Creating a site” on page 323.
- Monitor system jobs
- Select the columns to be displayed in the grid.
- Sort the grid.

See “About the Map view” on page 408.

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 **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 **Save**.

See “About the Map view” on page 408.

See “About the Grid view” on page 411.

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 412.

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 408.

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 414.

See "Associating components" on page 414.

See "Deleting the association between components" on page 414.

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 413.

See "Associating components" on page 414.

See "Deleting the association between components" on page 414.

Associating components

You can create associations between the infrastructure components. By default, the association between components are drawn in the Map view. The links between components help to add annotations.

The Map view lets you draw association that you may have deleted.

To add a link between components

1. Go to **Settings > System Topology**.
2. In the Map view, roll the mouse over the arrow icon that is displayed on the component image that you want to associate.

   When the cursor changes from an arrow to a hand, drag the mouse to the other component that you want to associate with. A blue link is created, associating the two components.

   You can now add annotation to the link.

See "Deleting the association between components" on page 414.

See "Deleting annotations" on page 414.

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 "Associating components" on page 414.

See “Deleting annotations” on page 414.

See “Adding annotations to the components” on page 413.

About the health and status of a component

You can view the configuration information of all the Control Compliance Suite (CCS) services that are installed. The health and the status jobs are run only on CCS Manager and the application server components.

The following health and status information is available:

- Communication settings
- Application server settings
- CCS directory Settings
- CCS Manager settings
- Infrastructure logs

The health information that is displayed is not live and is based on the scheduled jobs and the manual job runs. The health and the status jobs are run at the following time intervals:

Full status	The information is posted every 24 hours at midnight. You can manually refresh the information at anytime from the **Settings > Map** view and the **Settings > Grid** view. See “Refreshing the health and the status information” on page 417. The information is purged after 90 days.
Quick status	The information is posted every hour and is purged after seven days. The quick status is not displayed for the report server and the application configuration files.

You can export the data format.

You can view the health status of multiple CCS Manager at the same time.

In the **Health and Status Details** dialog box, the component name is color coded to indicate the health status of the component. You can also export the data.

Green	Indicates a healthy status.
Yellow	Indicates that the component needs attention.
Red	Indicates that the component has failed the health status check.

Pink	Indicates that system cannot get a status on the component.

See "Viewing the health and the status details" on page 416.

See "Refreshing the health and the status information" on page 417.

See "About the Map view" on page 408.

Viewing the health and the status details

The health information and status information lets users view the configuration details of the infrastructure components. The information can be used to detect and diagnose any issues. You can also the export the data to an XML format.

See "About the health and status of a component" on page 415.

If an error appears, manually run the **Refresh Health Status** task from the **Settings > Map** view or the **Settings > Grid** view.

See "Refreshing the health and the status information" on page 417.

To view health and status of a component

1. Go to **Settings > System Topology**.
2. In the **Map** view or the **Grid** view, right-click a component and then select **Health and Status Details**.
3. In the **Health and Status Details** dialog box, you can view the following information:

LiveUpdate	Displays the updates that are downloaded and are ready to be installed.
Host Machine Details	Displays the details of the host machine on which the selected Control Compliance Suite component is installed.
Service Details	Displays the details about the selected component.
Production Database Details	Displays the details of the SQL Server host and the list of the databases that are installed on the SQL Server host.
Report Server Details	Displays the details of the SQL Server host, the reporting database, and the schema versions of the various modules.
Logging Details	Displays the logging settings and statistics. If the default log location is modified, then the log file information is not displayed here. Only the log files that are stored in the default location appear here.
App. Config Details	Displays the details of the application configuration files.
Integration Bridge Details	Displays all the integration bridge interfaces and the available endpoints.
Data Collector Configuration Details	Displays the data collectors that are configured on the CCS Manager.

See "About the health and status of a component" on page 415.

See "About the Map view" on page 408.

See "About the Grid view" on page 411.

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 "About the health and status of a component" on page 415.

See "Refreshing the health and the status information" on page 417.

See "About the Map view" on page 408.

See "About the Grid view" on page 411.

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.

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 308.

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 419.

See "About viewing the audit logs" on page 420.

About audit event triggers

The following are the actions that trigger an audit event:

Table 21-1 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.
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.

Table 21-1 Audit Event Triggers *(continued)*

Event type	Module	Triggering Action
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 418.

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 418.

See "About audit event triggers" on page 419.

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.

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, Data Processing Service, and the Directory Support 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 424.

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 421.

See "About the LiveUpdate view" on page 422.

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 424.
- 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 423.

In CCS, LiveUpdate works in the following way:

- The LiveUpdate client detects new updates and copies the package to the CCS LiveUpdate staging location on the LiveUpdate client.
  See "About the LiveUpdate staging location" on page 424.
- CCS automatically deploys the updates packages on the CCS components.

Symantec recommends that you first install the updates on the Application Server.

See "About the LiveUpdate view" on page 422.

See "Updating Control Compliance Suite" on page 420.

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:

Table 21-2 Details of the LiveUpdate package

Column name	Description
Update Name	Name of the updates package that is available for download.
Update Version	The version of the updates package that is available for download.
Update Type	The type of the updates package. The updates type can be about CCS content, system patches, and service pack updates.
Host	Name of the computer on which the CCS component is installed.
Component	Name of the CCS component such as Application Server.
Current Version	The current version of the CCS component that is installed on the computer.
Is Update Downloaded at Default Location?	Displays if the latest available updates package is downloaded at a default location on the CCS component from the LiveUpdate server.

Table 21-2 Details of the LiveUpdate package *(continued)*

Column name	Description
Is Update Installed?	Displays if the downloaded updates package is installed on the CCS component.
Is Update Applicable?	Displays if the updates package is applicable for the specific CCS component. When a CCS updates package is released, the package need not be applicable for all the CCS components. Hence, you do not require to take any action if a package is not applicable for a specific CCS component.
Deployment Mode	Displays the status, Manual deployment, Auto deployment, or Not Applicable. The status, **Manual deployment** means that you must manually install the updates on the CCS component because the automatic updates installation job does not install the updates automatically. The status, **Auto deployment** means that the automatic updates installation job installs the updates automatically on the CCS component. The status, **Not Applicable** means that the update is not applicable for the specific CCS component.

See "How LiveUpdate works in Control Compliance Suite" on page 421.

See "Updating Control Compliance Suite" on page 420.

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 421.

See “Updating Control Compliance Suite” on page 420.

See “Performing LiveUpdate on demand” on page 425.

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.

In Control Compliance Suite (CCS), the LiveUpdate client is installed on the computer on which the Application Server, Data Processing Service, and the Directory Support 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 421.

See “Updating Control Compliance Suite” on page 420.

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 421.

See "Updating Control Compliance Suite" on page 420.

See "Performing LiveUpdate on demand" on page 425.

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 421.

See "Updating Control Compliance Suite" on page 420.

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 21-3 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 21-4 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 21-5 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 427.

See "About log levels" on page 427.

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 425.

See "About log levels" on page 427.

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 21-6 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 21-6 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 21-7 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 425.

See "About log messages" on page 427.

About configuring the Web Console to contact RAM

The Control Compliance Suite (CCS) Web Console 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 Console 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 Console, 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.

Chapter 22

Managing assets

This chapter includes the following topics:

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 60.

Table 22-1 Primary tasks to get started with asset system

Task	Description
Registering CCS Manager	Before the Application Server can use a newly installed CCS Manager, you must register the CCS Manager with the Application Server. When you register the CCS Manager, you also assign the CCS Manager to a site and specify the CCS Manager roles. Where appropriate, specify data types to collect.
Configuring the data collectors	You must configure the data collector for the platform for which you want to import the assets. **Note:** The data collectors are not applicable for fresh installation of CCS.
Configure Common platform to import common fields	In Control Compliance Suite, the data for the common fields of an asset type is not collected from the default data collector. To collect data for the common fields, you must manually create a CSV file and define all the common fields in a specific format. If you do not have the Common platform configured, the assets are still imported into the asset system without the common fields data.

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 22-2 Asset system tasks

Task	Description
Import the primary assets for the first time with the predefined reconciliation rules	The day zero asset import is the most important step to get started with the asset system. 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. See "Primary and secondary assets" on page 104. See "About the first time asset import" on page 443. See "Importing the assets for the first time" on page 444.
Create reconciliation rules for further asset imports	If you have imported assets without the common fields data, you can set the values of the common fields with the reconciliation rules. See "Creating reconciliation rules" on page 437.
Apply tags to the assets	You can now create tags to assign to the assets. You can create tags on the basis of Department, Confidentiality, Location, and so on. See "Asset tagging" on page 131. See "Applying a tag to the asset" on page 529.
Create asset groups	After you create the tags, you can group the assets on the basis of the tags or any other logical grouping. You can create asset groups based on criteria and specific assets or use the predefined asset groups. See "Creating asset groups" on page 498.

Table 22-2 Asset system tasks *(continued)*

Task	Description
Import the secondary assets	After you import the primary assets, you can now proceed with the further asset imports with the reconciliation rules and asset groups. See "Working with asset import scenarios" on page 446.

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

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

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.

See "Creating the asset folders" on page 505.

Filter by pane

This pane appears in the lower left side of the console window under the tree pane.

You can use the following filters in the asset management view:

- Select tags
- Risk Ratings
- Created Between
- Modified Between

Taskbar

The taskbar appears across the top of the tree pane and the table pane in the console window.

See "Performing the tasks in the Asset System view" on page 505.

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 141.

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.

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
- Edit Asset Group
- Copy Asset Group
- Paste Asset Group
- Rename Asset Group

Global Tasks

You can perform the following global tasks:

- Mark as Control Point
- Request Exception
- Set up Data Collection
- Run Evaluation
- Run Collection-Evaluation-Reporting

Asset Tasks

You can perform the following asset tasks:

- Import Assets
- Edit Assets
- Move Assets
- Export CSV Headers

Common Tasks

You can perform the following common tasks:

- Delete
- 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

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

This pane displays the reconciliation rules under the Reconciliation Rules node. Under the Reconciliation Rules node, you can view the predefined Rules.

Filter by pane

This pane appears in the lower left side of the console window under the tree pane.

You can use the following filters in the rules management view:

- Asset Type
- Rule Type

Taskbar

The taskbar appears across the top of the tree pane and the table pane in the console window.

See "Performing the tasks in the Reconciliation Rules view" on page 531.

Table pane

The table pane appears in the right side of the console window under the taskbar .

This pane displays the rule types and the rules.

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 rule that is selected in the tables pane.

The rules management view lets you perform the following tasks:

- Create Rule

  See "Creating reconciliation rules without manual review" on page 437.

  See "Creating reconciliation rules using the manual review" on page 438.

- Moving Rule
- Editing Rule
- Copy and Paste Rule
- Delete Rule
- Mark as Default Rule
- Unmark as Default Rule

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 129.

See "Creating reconciliation rules using the manual review" on page 438.

See "Creating reconciliation rules without manual review" on page 437.

See "Creating reconciliation rules for external data" on page 812.

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
  Post rule is not applicable to data schema that you select for external data integration.

See “Reconciliation rules and rule types” on page 106.

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 data schema to associate the rule with.

You can either select the data schema or the asset type for creating the reconciliation rule.

6 Select the folder to save the reconciliation rule in.

7 Type the description for the reconciliation rule and click **Next**.

8 In the **Select Rule Conditions and Actions** panel, click the **Add Condition**.

9 In the Add Condition dialog box, select a condition from the drop-down list and click **OK**.

10 In the **Select Rule Conditions and Actions** panel, click **Add Action**.

11 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**.

12 Click **Next** in the **Select Rule Conditions and Actions** panel after you set the condition and the action.

13 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 438.

See “Working with reconciliation rules scenarios” on page 439.

See “Quick start with minimum configuration” on page 277.

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 130.

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 106.

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 496.

See “Working with reconciliation rules scenarios” on page 439.

See “Creating reconciliation rules without manual review” on page 437.

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
- Using an Add rule to dynamically create asset folders
- Using an Update rule to update the existing field values
- Using a Post rule to dynamically create folders and move assets to the folders

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 66.
- 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 477.

To import assets, you must select either a default data collector, CSV data collector, or an ODBC data collector.

Table 22-3 How data collectors work in asset import

Selected data collector	How the data collector works
Default	Asset import from default data collector involves the import from the data collection components as well as the CSV data collector. ■ The default data collector gathers the information about the asset-specific fields from the data collection components in the Control Compliance Suite. **Note:** The default data collector is not applicable for fresh installation of CCS. ■ 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 data collection components are, Windows data collector, UNIX data collector, SQL data collector, Oracle data collector, ESM data collector, Exchange data collector, NDS data collector, and NetWare data collector. **Note:** For custom platforms, if you select CSV or ODBC data collector during entity schema creation, then the selected data collector becomes the default data collector. ■ 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.

Table 22-3 How data collectors work in asset import *(continued)*

Selected data collector	How the data collector works
CSV	■ 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 329. ■ 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.
ODBC	The ODBC data collector gathers information about the asset-specific fields that are defined in the table columns of the ODBC databases. The ODBC data collector collects both asset-specific and common fields data that are defined for the asset in the database tables. To know more about configuring the ODBC data collector , click on the following link: See "Configuring the ODBC data collector" on page 331. The ODBC data collector reads data from the configured tables of the ODBC compliant databases. The database tables are configured for different platforms as per the entity schema. You must define the table names and the table column names appropriately as per the entity schema for successful data collection.

See "Importing the assets for the first time" on page 444.

See "Importing asset-specific fields from the default data collector" on page 455.

See "Importing asset-specific and common fields using the default data collector" on page 458.

See “Importing asset-specific and common fields using the CSV data collector” on page 461.

See “Importing the specific and common fields for custom asset using the CSV data collector” on page 467.

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.

- CCS Agent
  See “CCS Agent” on page 54.
- Predefined platforms
  See “Predefined platforms” on page 65.
- Predefined asset types
  See “Predefined asset types” on page 66.
- Primary and secondary assets
  See “Primary and secondary assets” on page 104.
- Default data collectors for the supported platforms
  See “Default data collectors” on page 123.

  Note: The default data collector is not applicable for fresh installation of CCS.

- Working of the default data collector in asset import
- Working of the CSV data collector in asset import
  See “About the working of CSV data collector in asset import” on page 448.

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.

To import the assets for the first time, you can do one of the following:

- If you are using CCS agent to import the assets, import the CCS agent and assets.
  See "Importing assets and agents " on page 556.
- If you are not using CCS agent to import the assets, import the assets using the default data sources.
  See "Importing the assets for the first time" on page 444.

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 437.
  If you do not have any custom rule, you can use the Add rule from the predefined rules.
  See "Predefined reconciliation rules" on page 114.

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.

Note: The default data collector is not applicable for fresh installation of CCS.

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 Asset Type, Source, and Scope** panel, select the asset type to import the assets, source, and scope of asset import.

Depending upon the asset type and the source that you select, the scope is available as a site or an asset type. For configuring the data source or the assets, click (+) icon and update the configurations.

5 In the **Add or Edit Configurations** panel, specify the required information and click **OK**.

See "Configuring a data source for asset import" on page 453.

6 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**.

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 481.

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 114.

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 443.

See "Quick start with minimum configuration" on page 277.

See "Configuring for asset import" on page 452.

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 443.

Table 22-4 Asset import scenarios

Data collector	Asset import objective
Default data collector	The scenarios are as follows: ■ To import the asset-specific fields See "Importing asset-specific fields from the default data collector" on page 455. ■ To import the asset-specific and common fields See "Importing asset-specific and common fields using the default data collector" on page 458. The import of common fields from the default data collector involves the configuration of CSV data collector for Common platform. **Note:** The default data collector is not applicable for fresh installation of CCS.

Table 22-4 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 448.	The scenarios are as follows: ■ 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 461. ■ 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 467. ■ To import only the specific assets manually, only once. See "Configuring a data source for asset import" on page 453.
ODBC data collector See "About the working of the ODBC data collector in asset import" on page 450.	The scenario is as follows: ■ To import the asset-specific and common fields from the ODBC data collector See "Importing asset-specific and common fields using the ODBC data collector" on page 470. ■ To import the custom asset-specific fields and common fields from the ODBC data collector. See "Configuring a data source for asset import" on page 453.

Table 22-4 Asset import scenarios *(continued)*

Data collector	Asset import objective
Directory Server	The scenario is as follows: ■ To import the asset-specific and common fields from the Directory Server See "Importing asset-specific and common fields using the directory server" on page 473. ■ To import the custom asset-specific fields and common fields from the Directory Server. See "Configuring a data source for asset import" on page 453. **Note:** The directory server can be configured only for Windows Machine and UNIX Machine asset types.

About the working of CSV data collector in asset import

To import the assets in the asset system, you select a data collector. You can select a default data collector, a CSV data collector, or an ODBC data collector.

See "Data collectors and asset types" on page 124.

Note: The default data collector is not applicable for fresh installation of CCS.

Table 22-5 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.	To import the entire data in case you explicitly select the CSV data collector for asset import. In this case, the data for the asset-specific fields and for the common fields, is imported from the CSV data collector. 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. After you create the CSV file, you need to configure the CSV data collector. See "Importing asset-specific and common fields using the CSV data collector" on page 461.
To import the data for the common fields even if you select the Default data collector for asset import.	To import the data for the common fields even if you select the Default data collector for asset import. 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. To import the data for the common fields, you must configure the Common platform through CSV settings. See "About the working of CSV data collector in asset import" on page 448.
To import the data in case you import the data for the custom asset type.	In this case, the CSV data collector becomes the default data collector. See "Importing the specific and common fields for custom asset using the CSV data collector" on page 467.

See "Creating a CSV file for custom application" on page 487.

See " Configuring the CSV data collector" on page 329.

About the working of the ODBC data collector in asset import

To import the assets in the asset system, you select a data collector. You can select a default data collector, a CSV data collector, or an ODBC data collector.

See "Data collectors and asset types" on page 124.

Table 22-6 Role of an ODBC data collector

Role of the ODBC data collector	Description
To import the data of a predefined or custom platform and you explicitly select the ODBC data collector for asset import.	To import the entire data of an asset and you explicitly select the ODBC data collector for asset import. In this case, the data for the asset-specific fields and the common fields, are imported by the ODBC data collector. See "Importing asset-specific and common fields using the ODBC data collector" on page 470.
To import the data for the common fields and you select ODBC data collector for asset import.	By default, data for the common fields are collected from the CSV files using the CSV data collector. If you want to collect data for the common fields using the ODBC data collector, then switch the CSV to ODBC data collector. See "Switching between CSV and ODBC data collectors" on page 332. To import the data for the common fields, you must configure the Common platform through the ODBC settings.

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.

  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.
- Configure the CSV data collector.

  Note: Ensure that you select the platform, Common in the **Edit Settings** dialog box for configuring the CSV data collector.
- Import the asset type using the Asset Import wizard.

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.

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.

6 In the console, go to Settings > System Topology > Map View and click **Infrastructure Tasks > Sync Configuration**.

Configuring for asset import

You need to configure CCS for agent less or agent based data collection of assets.

You must configure the data source for asset import before data collection. The data sources include CSV, ODBC, and Directory Server. The data sources which are available for selection depend on the asset type that you select for asset import.

Based on asset type and data source, the sites or the assets have to be configured for asset import

See "Configuring a data source for asset import" on page 453.

See "Exporting assets as CSV" on page 530.

See "Importing asset-specific and common fields using the CSV data collector" on page 461.

See "Importing asset-specific and common fields using the ODBC data collector" on page 470.

See "Importing asset-specific and common fields using the directory server" on page 473.

Configuring a data source for asset import

Only CCS Administrator and the users who have the following user task access rights can configure the data source for the site:

- View Configured Settings
- Manage Configured Settings

You can configure a data source for CSV, OBDC database, and Directory Server.

See "Configuring for asset import" on page 452.

To configure a data source for asset import

- ◆ In the **Add or Edit Configuration** panel, specify the following information and click **Ok**.

See "Importing the assets for the first time" on page 444.

The **Add or Edit Configuration: CSV** panel presents the following fields:

Table 22-7 Add or Edit Configuration: CSV

Field	Description
CSV file path	Lets you browse and add the file path to CSV file on your computer.
Windows domain	Lets you select Windows domain from the list.
User name	Lets you specify the user name.
Password	Lets you specify the password.
Search pattern	Lets you specify the search string.

Table 22-7 Add or Edit Configuration: CSV *(continued)*

Field	Description
File encoding	Lets you select the file encodin format.

The **Add or Edit Configuration: Database** panel presents the following fields:

Table 22-8 Add or Edit Configuration: Database

Field	Description
Data Location	Lets you specify the data location or add a new data location.

Note: You can click the link, Entity-Table Mapping to view the field mapping for ODBC.

The **Add or Edit Configuration: Directory Server** panel presents the following fields:

Table 22-9 Add or Edit Configuration: Directory Server

Field	Description
Directory server name and port	Lets you specify the name of the Directory server and port. The required format to specify the servername and port is as follows: <servername>:port
Distinguished name	Lets you specify the distinguished name.
User name	Lets you enter the username for the Directory server that you want to use..
Password	Lets you enter the password.
Confirm Password	Lets you re-enter the password for confirmation.

Note: You can click the link, Entity-Table Mapping to view the field mapping for Directory Server.

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.

To update the existing field value with an update rule

1. Go to **Manage > Asset System > 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 "Importing the assets for the first time" on page 444.

See "About the first time asset import" on page 443.

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.

Note: The default data collector is not applicable for fresh installation of CCS.

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 Asset Type, Source, and Scope** panel, select the asset type to import the assets, source, and scope of asset import.

   Depending upon the asset type and the source that you select, the scope is available as a site or an asset type. For configuring the data source or the assets, click (+) icon and update the configurations.
5. In the **Add or Edit Configurations** panel, specify the required information and click **OK**.

   See “Configuring a data source for asset import” on page 453.
6. 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**.

   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 481.
7. 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**.
8. 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 and click **OK**.

9 Click **Finish** to stop the wizard.

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 or Edit Filter Statement** dialog box.

11 In the **Create or Edit Filter Statement** dialog use the parameter type and the conditions to create a filter statement.

See "Examples of asset filters" on page 127.

See "Filter statement operators" on page 128.

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 Click **Finish** to stop the wizard.

14 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.

15 Click **Finish** to stop the wizard.

16 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 496.

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 "About the working of CSV data collector in asset import" on page 448.

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 123.

Note: The default data collector is not applicable for fresh installation of CCS.

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 Asset Type, Source, and Scope** panel, select the asset type to import the assets, source, and scope of asset import.

   Depending upon the asset type and the source that you select, the scope is available as a site or an asset type. For configuring the data source or the assets, click (+) icon and update the configurations.

5. In the **Add or Edit Configurations** panel, specify the required information and click **OK**.

   See "Configuring a data source for asset import" on page 453.

6. 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**.

   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 481.

7. 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**.

8. In the **Select Reconciliation Rules** panel, browse through the Reconciliation Rules folder, use the **Add** option to add the existing reconciliation rules to the import job and click **OK**.

9. Click **Finish** to stop the wizard.

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 or Edit 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 or Edit Filter Statement** dialog box, use the parameter type and the conditions to create a filter statement.

   See "Examples of asset filters" on page 127.

   See "Filter statement operators" on page 128.

12 Click **Finish** to stop the wizard.

13 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**.

14 Click **Finish** to stop the wizard.

15 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.

16 Click **Finish** to stop the wizard.

17 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 496.

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.

Note: The default data collector is not applicable for fresh installation of CCS.

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 489.
- 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 329.

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 Asset Type, Source, and Scope** panel, select the asset type to import the assets, source, and scope of asset import.

   Depending upon the asset type and the source that you select, the scope is available as a site or an asset type. For configuring the data source or the assets, click (+) icon and update the configurations.
5. In the **Add or Edit Configurations** panel, specify the required information and click **OK**.

   See "Configuring a data source for asset import" on page 453.
6. 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**.

   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 481.
7. 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**.
8. In the **Select Reconciliation Rules** panel, browse through the Reconciliation Rules folder, use the **Add** option to add the existing reconciliation rules to the import job and click **OK**.
9. Click **Finish** to stop the wizard.

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 or Edit 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 or Edit Filter Statement** dialog box, use the parameter type and the conditions to create a filter statement.

See "Examples of asset filters" on page 127.

See "Filter statement operators" on page 128.

12 Click **Finish** to stop the wizard.

13 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**.

14 Click **Finish** to stop the wizard.

15 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.

16 Click **Finish** to stop the wizard.

17 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 496.

Importing asset-specific and common fields using the ODBC data collector

You can use an ODBC data collector as any other default data collector to import the assets of any predefined platform or of a custom platform. The custom platform represents a custom application that is defined through the entity schema for the Control Compliance Suite.

Note: The default data collector is not applicable for fresh installation of CCS.

See "Creating a new entity schema" on page 578.

Before you start using the ODBC data collector for asset import, ensure that you meet the following prerequisites:

- Format the ODBC database table or view names and column names as per the entity schema.
  See "Format to create ODBC compliant database tables" on page 491.

  Note: If you are using ODBC data collector to import assets of predefined asset types, then it is recommended that you use the Entity-Table mapping option. You require to map all the primary and mandatory fields of the asset type for successful data collection.

- Configure a DPS as the ODBC data collector.
  See "Configuring the ODBC data collector" on page 331.

To import asset-specific and common fields using the ODBC 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 Asset Type, Source, and Scope** panel, select the asset type to import the assets, source, and scope of asset import.

   Depending upon the asset type and the source that you select, the scope is available as a site or an asset type. For configuring the data source or the assets, click (+) icon and update the configurations.
5. In the **Add or Edit Configurations** panel, specify the required information and click **OK**.

   See "Configuring a data source for asset import" on page 453.
6. 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**.

   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 481.
7. 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**.
8. In the **Select Reconciliation Rules** panel, browse through the Reconciliation Rules folder, use the **Add** option to add the existing reconciliation rules to the import job and click **OK**.
9. Click **Finish** to stop the wizard.
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 or Edit 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 or Edit Filter Statement** dialog box, use the parameter type and the conditions to create a filter statement.

See "Examples of asset filters" on page 127.

See "Filter statement operators" on page 128.

12 Click **Finish** to stop the wizard.

13 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**.

14 Click **Finish** to stop the wizard.

15 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.

16 Click **Finish** to stop the wizard.

17 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 496.

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.

Note: The default data collector is not applicable for fresh installation of CCS.

See "Default data collectors" on page 123.

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 487.
- 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 329.

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 Asset Type, Source, and Scope** panel, select the asset type to import the assets, source, and scope of asset import.

  Depending upon the asset type and the source that you select, the scope is available as a site or an asset type. For configuring the data source or the assets, click (+) icon and update the configurations.

5 In the **Add or Edit Configurations** panel, specify the required information and click **OK**.

  See "Configuring a data source for asset import" on page 453.

6 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**.

  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 481.

7 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**.

8 In the **Select Reconciliation Rules** panel, browse through the Reconciliation Rules folder, use the **Add** option to add the existing reconciliation rules to the import job and click **OK**.

9 Click **Finish** to stop the wizard.

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 or Edit 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 or Edit Filter Statement** dialog box, use the parameter type and the conditions to create a filter statement.

See “Examples of asset filters” on page 127.

See “Filter statement operators” on page 128.

12 Click **Finish** to stop the wizard.

13 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**.

14 Click **Finish** to stop the wizard.

15 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.

16 Click **Finish** to stop the wizard.

17 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 496.

Importing asset-specific and common fields using the ODBC data collector

You can use an ODBC data collector as any other default data collector to import the assets of any predefined platform or of a custom platform. The custom platform represents a custom application that is defined through the entity schema for the Control Compliance Suite.

Note: The default data collector is not applicable for fresh installation of CCS.

See "Creating a new entity schema" on page 578.

Before you start using the ODBC data collector for asset import, ensure that you meet the following prerequisites:

- Format the ODBC database table or view names and column names as per the entity schema.

See “Format to create ODBC compliant database tables” on page 491.

Note: If you are using ODBC data collector to import assets of predefined asset types, then it is recommended that you use the Entity-Table mapping option. You require to map all the primary and mandatory fields of the asset type for successful data collection.

- Configure a DPS as the ODBC data collector.
  See “Configuring the ODBC data collector” on page 331.

To import asset-specific and common fields using the ODBC 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 Asset Type, Source, and Scope** panel, select the asset type to import the assets, source, and scope of asset import.

   Depending upon the asset type and the source that you select, the scope is available as a site or an asset type. For configuring the data source or the assets, click (+) icon and update the configurations.
5. In the **Add or Edit Configurations** panel, specify the required information and click **OK**.

   See “Configuring a data source for asset import” on page 453.
6. 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**.

   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 481.
7. 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**.

8 In the **Select Reconciliation Rules** panel, browse through the Reconciliation Rules folder, use the **Add** option to add the existing reconciliation rules to the import job and click **OK**.

9 Click **Finish** to stop the wizard.

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 or Edit 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 or Edit Filter Statement** dialog box, use the parameter type and the conditions to create a filter statement.

See “Examples of asset filters” on page 127.

See “Filter statement operators” on page 128.

12 Click **Finish** to stop the wizard.

13 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**.

14 Click **Finish** to stop the wizard.

15 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.

16 Click **Finish** to stop the wizard.

17 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 496.

Importing asset-specific and common fields using the directory server

If you want to import the asset-specific and common fields from the directory server, you must also ensure that the directory server is configured. The directory server can be configured only for Windows Machine and UNIX Machine asset types.

To import asset-specific and common fields from the directory server

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 Asset Type, Source, and Scope** panel, select the asset type to import the assets, source, and scope of asset import.

Depending upon the asset type and the source that you select, the scope is available as a site or an asset type. For configuring the data source or the assets, click (+) icon and update the configurations.

5 In the **Add or Edit Configurations** panel, specify the required information and click **OK**.

See "Configuring a data source for asset import" on page 453.

6 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**.

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 481.

7 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**.

8 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 and click **OK**.

9 Click **Finish** to stop the wizard.

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 or Edit 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 or Edit Filter Statement** dialog box, use the parameter type and the conditions to create a filter statement.

See “Examples of asset filters” on page 127.

See “Filter statement operators” on page 128.

12 Click **Finish** to stop the wizard.

13 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**.

14 Click **Finish** to stop the wizard.

15 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.

16 Click **Finish** to stop the wizard.

17 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 496.

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.

To update the existing field value with an update rule

1 Go to **Manage > Asset System > 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 "Importing the assets for the first time" on page 444.

See "About the first time asset import" on page 443.

Common fields for all asset types

Control Compliance Suite supports certain predefined asset types.

See "Predefined asset types" on page 66.

All the asset types have certain common fields. To import the data for the common fields, you must configure the Common platform either through CSV or ODBC settings. The CSV or ODBC settings can be specified through the **Edit Settings** dialog box while configuring the DPS. In the asset import job, data for the common fields can be imported either through a CSV or an ODBC data collector.

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

    This is represented by 0 in the CCS directory. You must specify 0 in the CSV file or in the ODBC database column based on the data collector that is configured for collecting data. The specified value, 0 defines the asset value of Confidentiality as NotDefined after the asset import.

  - Low

    This is represented by 1 in the CCS directory. You must specify 1 in the CSV file or in the ODBC database column based on the data collector that is configured for collecting data. The specified value, 1 defines the asset value of Confidentiality as Low after the asset import.

  - Medium

    This is represented by 2 in the CCS directory. You must specify 2 in the CSV file or in the ODBC database column based on the data collector that is configured for collecting data. The specified value, 2 defines the asset value of Confidentiality as Medium after the asset import.

  - High

    This is represented by 3 in the CCS directory. You must specify 3 in the CSV file or in the ODBC database column based on the data collector that is configured for collecting data. The specified value, 3 defines the asset value of Confidentiality as High after the asset import.

Note: If you specify the value of this field in the CSV file or in the ODBC database columns as anything greater than 3, the asset system marks it as NotDefined.

- 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

    This is represented by 0 in the CCS directory. You must specify 0 in the CSV file or in the ODBC database column based on the data collector that is configured for collecting data. The specified value, 0 defines the asset value of Integrity as NotDefined after the asset import.
  - 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.

    This is represented by 1 in the CCS directory. You must specify 1 in the CSV file or in the ODBC database column based on the data collector that is configured for collecting data. The specified value, 1 defines the asset value of Integrity as Low after the asset import.
  - Medium

    This is represented by 2 in the CCS directory. You must specify 2 in the CSV file or in the ODBC database column based on the data collector that is configured for collecting data. The specified value, 2 defines the asset value of Integrity as Medium after the asset import.
  - High

    This is represented by 3 in the CCS directory. You must specify 3 in the CSV file or in the ODBC database column based on the data collector that is configured for collecting data. The specified value, 3 defines the asset value of Integrity as High after the asset import.

  Note: If you specify the value of this field in the CSV file or in the ODBC database as anything greater than 3, the asset system marks it as NotDefined.

- 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
    This is represented by 0 in the CCS directory. You must specify 0 in the CSV file or in the ODBC database column based on the data collector that is configured for collecting data. The specified value, 0 defines the asset value of Availability as NotDefined after the asset import.
  - Low
    This is represented by 1 in the CCS directory. You must specify 1 in the CSV file or in the ODBC database column based on the data collector that is configured for collecting data. The specified value, 1 defines the asset value of Availability as Low after the asset import.
  - Medium
    This is represented by 2 in the CCS directory. You must specify 2 in the CSV file or in the ODBC database column based on the data collector that is configured for collecting data. The specified value, 2 defines the asset value of Availability as Medium after the asset import.
  - High
    This is represented by 3 in the CCS directory. You must specify 3 in the CSV file or in the ODBC database column based on the data collector that is configured for collecting data. The specified value, 3 defines the asset value of Availability as High after the asset import.

  Note: If you specify the value of this field in the CSV file or in the ODBC database as anything greater than 3, the asset system marks it as NotDefined.

- 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.
- Risk Score

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.

- Risk Rating
  Risk Rating is the maximum risk score that is calculated based on the maximum weight for a risk property provider.
- 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.
- Source Name
  Name of the source from which the asset is being imported. The source can be one of the pre-defined data collectors, the CSV data collector, the ODBC data collector, or any other source that is used for asset import.
- Source ID
  Unique identification of the asset in the source.

You can set the values of the common fields with the Pre rule.

See “Importing asset-specific and common fields using the default data collector” on page 458.

See “Importing asset-specific and common fields using the CSV data collector” on page 461.

See “Importing the specific and common fields for custom asset using the CSV data collector” on page 467.

See “Importing asset-specific and common fields using the ODBC data collector” on page 470.

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 22-10 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 104.

- 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 22-10 Asset import scope options

Scope	Scenario	Results
Default scope	■ 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.	■ 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. For example, to import the Windows file with the default scope, you should have the Windows machines already imported in the asset system. See "Default scope and supported scope" on page 483.

Table 22-10 Asset import scope options *(continued)*

Scope	Scenario	Results
Supported scope	■ 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.	■ The query execution takes longer if you do not scope the query properly. See “Default scope and supported scope” on page 483.

See “Default scope and supported scope” on page 483.

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 104.
- 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 22-11 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	■ Site ■ Asset type	■ Site ■ Asset type

Table 22-11 Supported and default scopes for the asset types *(continued)*

Asset type	Default scope	Supported scope
ESM Agent	■ ESM Agent ■ Site	■ ESM Agent ■ Site
Oracle Configured Databases	Site	■ Site ■ Oracle Configured Databases
SQL Database	SQL Server	■ SQL Database ■ SQL Server
SQL Server	Site	■ SQL Server ■ Site
UNIX File	UNIX Machine	■ UNIX Machine ■ UNIX File
UNIX Group	UNIX Machine	■ UNIX Machine ■ UNIX Group
UNIX Machine	Site	■ UNIX Machine ■ Site
Windows Directory	Windows Machine	■ Windows Machine ■ Windows Domain ■ Windows Directory ■ Windows Share
Windows Domain	Site	■ Windows Domain ■ Site
Windows File	Windows Machine	■ Windows Machine ■ Windows Domain ■ Windows Directory ■ Windows File ■ Windows Share
Windows Group	Windows Machine	■ Windows Group ■ Windows Machine ■ Windows Domain

Table 22-11 Supported and default scopes for the asset types *(continued)*

Asset type	Default scope	Supported scope
Windows Machine	Windows Domain	■ Windows Domain ■ Windows Machine ■ Site
Windows Share	Windows Machine	■ Windows Share ■ Windows Domain ■ Windows Machine

See "About scopes in asset import" on page 481.

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 66.

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 569.

See " Configuring the CSV data collector" on page 329.

See "About format of the CSV file headers" on page 485.

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 569.

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 583.

  - 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 583.

  - 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 584.

  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>`

  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.

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 578.

See "About the list field format in CSV file" on page 490.

See "Creating a CSV file for custom application" on page 487.

See "Creating a CSV file for predefined asset types" on page 489.

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 66.

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 583.
   - Entity
     See "About entities" on page 583.
   - Fields
     See "About fields of an entity " on page 584.
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 578.

   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 485.

   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 529.

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 329.

See "Creating a new asset type" on page 569.

See "Creating a CSV file for predefined asset types" on page 489.

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 485.

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 487.

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 “Predefined asset types” on page 66.

   Ensure that you select CSV data collector in the **Create or Edit Asset Import Job** wizard.

See “ Configuring the CSV data collector” on page 329.

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 485.

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.

Importing assets from an ODBC database table

In Control Compliance Suite, you can store the asset information in an ODBC database and import them into the infrastructure for data collection. The assets are categorized into various asset types and are imported into the infrastructure using 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 66.

Before performing an asset import operation from an ODBC database table, ensure that the table contains the asset information. The database table or view names and the column names must be defined in a specific format. The ODBC data collector interprets the database table or view names to import assets from the tables.

See “Creating a new asset type” on page 569.

See “Configuring the ODBC data collector” on page 331.

See “Format to create ODBC compliant database tables” on page 491.

Format to create ODBC compliant database tables

To import data from the ODBC compliant databases using the ODBC data collector, you must configure the database table as per the defined format. The defined format is easily interpreted by the ODBC data collector for effective data collection. As per the defined format, the table name or view name and the column names must be mapped with the entity name and the fields, respectively.

The format of the database table naming convention depends on the attributes of the entity schema that you create for an application. Every entity schema is the blue-print for the data collector to collect data and contains the definition of the platform, entity, and the entity fields.

See "Creating a new entity schema" on page 578.

Configure the ODBC data collector for the custom platform that you define in the entity schema.

See "Configuring the ODBC data collector" on page 331.

Table 22-12 Mapping between an entity schema attribute and the ODBC database table element

Entity schema attribute	ODBC database element	Description
Platform name and entity name	Database table or view name	The database table or view name is a combination of the platform name and the entity name. The format of the table or view name must be in the following format: <platformnameentityname>
Field name	Database table column name	The database table's column name must be same as the field name of the entity.

The format of naming the ODBC database tables are as follows:

- Format to create database table or view names for all platforms
  You manually create the database table or view names based on the attributes of the entity schema. The table or view name is a combination of the platform name and the entity name.
  The format to create the database table or view names is as follows:
  ```
  platformnameentityname
  ```
  For example, you want to configure an ODBC data collector for the platform, DB2, whose entity is Server. As per the defined format, the database table or view name must be DB2Server.
- Format to create database table or view names for the Common platform only

The format to create database table or view names for the Common platform is different when compared to the format for other platforms. The Common platform defines the CIA field values and by default, is configured for the predefined asset types. Hence, the table or view name is a combination of the predefined platform name and the entity name.

The format to create the database table or view names for the Common platform is as follows:

```
predefinedplatformnameentityname
```

For example, you want to configure an ODBC data collector for the Common platform of a predefined asset type, Windows Machine. For this asset type, the predefined platform is, Wnt and the entity is, Machine. As per the defined format, table or view name for the Common platform must be WntMachine.

- Format to create database table column names for all platforms

  The fields of an entity that are defined in the entity schema must be the database table column names.

  For example, you want to configure an ODBC data collector for the platform, UNIX, whose entity is, Machine. The entity fields are, IPAddress and Hostname for the entity, Machine. As per the defined format, the database table column names must be IPAddress and Hostname.

- Format to create database tables for the predefined platforms and their asset types

  You can create the database tables for the predefined platforms and their asset types using the following standard naming convention:

  ```
  predefinedplatformnameentityname
  ```

  You must use the internal names of the predefined platforms to define the database table names or view names. For the predefined platforms, the predefined asset types represent the entities. Hence, you can specify the name of the asset type in place of the entity in the defined format. For example, for the Windows platform, the internal name is Wnt. The table or view name for the predefined asset type, Windows Machine is, WntMachine.

  The predefined platforms and their internal names are as follows:

Windows	Wnt
UNIX	Unix
Oracle	ORCL
SQL	Dbif
Exchange	Mailadmin
NDS	NDS

NetWare	NW
ESM	ESM

You must know the predefined asset types of the predefined platform to define the table name or view name for the specific asset type.

See "Predefined asset types" on page 66.

If you do not create table name or view name manually as per the entity schema, then you can use the **Entity Table Mapping** dialog box. This dialog box lets you map the entities to the existing database table or view names for the selected platform. You can also map the database table column names with the field names of the entities. You use this mapping option only if the database table or view names are not compliant with the defined format.

Creating an ODBC database table for custom application

The Control Compliance Suite can import assets of any custom application that are stored in the ODBC compliant databases. The assets are imported using the configured ODBC data collector. For example, you can import assets of a custom application such as DB2 using the ODBC data collector into the infrastructure. Before you import the assets, you must create asset types for the custom application and store the asset information in the ODBC compliant database.

You must define the asset information of the custom application in a specific format for easy interpretation by the ODBC data collector.

To create an ODBC database table

1. Export the data of the custom application into the ODBC database tables.
2. Identify whether the asset type or entity of the custom application belongs to any of the predefined asset type.

   See "Predefined asset types" on page 66.
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 583.
   - Entity
     See "About entities" on page 583.
   - Fields
     See "About fields of an entity " on page 584.

4 For a custom application, you must first define an entity schema before creating the database tables.

See "Creating a new entity schema" on page 578.

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 Based on the entity that you create, you must create asset types for the custom application.

See "Creating a new asset type" on page 569.

6 Create tables with table or view names in a specific format combining the platform and the entity name.

The format is as follows:

<platformnameentityname>

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 define the platform as DB2 and the entity as Server.

One of the table or view name of the ODBC database is as follows:

```
DB2Server
```

7 Arrange the table column names as per the field names that are defined in the entity schema.

For example, you define an entity schema, for platform, DB2, with entity, Server and fields, ServerName, HostName, IPAddress. The database table column names must be same as the field names.

8 Configure the ODBC data collector.

See "Configuring the ODBC data collector" on page 331.

See "Format to create ODBC compliant database tables" on page 491.

About the list field format in ODBC database table

The Control Compliance Suite imports assets and collects data from the ODBC-compliant databases, only if the tables and columns are named in a specific format.

See "Format to create ODBC compliant database tables" on page 491.

If you want to define a string type data, which is an array in the ODBC database table, then the data must be 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 ODBC database.

The format of the list fields for the ODBC databases is as follows:

```
@:<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 130.

See "Creating reconciliation rules using the manual review" on page 438.

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 496.
- Reconciling the manual review records
  See "Reconciling the manual review records" on page 497.

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 130.

See “Reconciling the manual review records” on page 497.

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 130.

See “Viewing the manual review records” on page 496.

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 the asset groups with assets based on criteria or specific assets 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 “Asset groups with assets based on criteria ” on page 131.

See “Creating an asset group with assets based on criteria” on page 498.

See “Asset groups with specific assets” on page 132.

See “Creating an asset group with specific assets” on page 502.

See “Editing an asset group” on page 513.

Creating an asset group with assets based on criteria

You can create an asset group with assets based on criteria, if you want the assets in a folder to be organized dynamically based on certain properties. This asset group gets updated with every asset import job if more assets from the relevant asset folder meet the queries.

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 an asset group with assets based on criteria

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 **Add assets based on criteria** in the Asset Group Criteria 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	Lets you specify the asset name. Assets with the specified name are included in the asset group.
Location	Lets you specify the asset location. Assets that reside at the specified location are included in the group.
Department	Lets you specify the asset department. Assets that belong to the specified department are included in the asset group.
Owner	Lets you specify the asset owner. Assets with the specified owner are included in the asset group.
Custodian	Lets you specify the custodian for the assets. Assets with the specified custodian are included in the asset group.

Tags	Lets you specify the tag name and the tag category. Assets that have the specified tag are included in the asset group. Click the Add icon (+) to add tags and click the Delete icon (X) to remove tags. If you select **Match Any** as a filter, the tag expression is formed with an OR. The assets with either of the specified tags are included in the asset group. **Match Any** is selected by default. If you select **Match All** as a filter, the tag expression is formed with an AND. The assets with either of the specified tags are included in the asset group.
Risk rating	Lets you specify the risk rating. Assets with the specified risk rating are included in the asset group.
Include assets with any of the above filters	Includes the asset in the asset group if the asset meets the criteria that is specified in any of the above filters.

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 asset group with assets based on criteria. 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 504.

8 In the **Create or Edit 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 an asset group with specific assets" on page 502.

Creating an asset group with specific assets

You can create an asset group with specific assets that do not undergo frequent updates. The asset count in this 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 an asset group with specific assets, 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 an asset group with specific assets

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 **Add specific assets** in the Asset Group Criteria 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 an asset group with assets based on criteria" on page 498.

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 an asset group with assets based on criteria 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 **Asset group with assets based on criteria** 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 504.

8 In the **Create or Edit 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 [<=] D**
    You can switch between the AND/OR operators using the same option.
  - **(A Equal To (=) B)** and **© Greater Than or Equal To [<=] D)** or **(A Equal To (=) B)** and **© Equal To (=) F)**
    With the opening and closing parentheses, you can create more complex filter expressions.

See “Filter statement operators” on page 128.

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 505.
- Asset group tasks
  See "Performing the asset group tasks" on page 513.
- Global tasks
  See "Performing the global tasks" on page 514.
- Asset tasks
  See "Performing the asset tasks" on page 526.
- Common tasks
  See "Deleting assets or asset groups" on page 530.
- View asset details pane
- Use Filter by pane

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 64.

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 300.

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 “Quick start with minimum configuration” on page 277.

Adding assets

The **Add Assets** task on **Asset Tasks** simplifies the addition of network assets. The **Add Assets** task facilitates the addition of assets without the requirements of an asset import job and dependent configurations.

To add an asset

1 On the Control Compliance Suite home page, point to **Manage**, and click **Asset System**.

2 On **Asset Tasks**, click **Add Assets** to get the Add Assets wizard.

Alternatively, right-click an assets folder, and click **Add Assets**.

3 On **Provide Asset Information**, click the **Select location** button that is alongside the **Location** field to get the **Select Folder** box.

4 To enter the path to the folder in the **Location** field on **Provide Asset Information**, select the folder in the **Select Folder** box, and then click **OK**.

5 In the **Asset type** field, enter the type of the asset that you want to add.

6 To create a single asset, click **Add asset classification**, and enter the category for the asset that you want to add.

7 Click **Next**.

8 On **Specify Asset Details**, click the Field Chooser icon to get the **Field Chooser** box. .

9 On **Field Chooser**, check the fields for the attributes you want for the asset, and then click **Finish**.

10 On **Progress Details**, click **Close**.

11 On **Information**, click **OK**.

See “Adding multiple assets” on page 507.

See “Running a collection-evaluation-reporting job from the Standards view” on page 663.

See “Associating assets with security objective” on page 1093.

Adding multiple assets

To add more than one asset to Control Compliance Suite, import a CSV file with the assets into CCS.

For the import of assets, select a CSV file that meets the following conditions:

- The file for the specified asset type is available for import.
- Columns in the file match the asset fields.
- No values are missing or extra in the file.

Failure to meet the conditions results in the display of system messages.

To import assets

1. On the Control Compliance Suite home page, point to **Manage**, and click **Asset System**.
2. In the asset system, on **Asset Tasks**, click **Add Assets** to get the Add Assets wizard.
3. On **Provide Asset Information**, click the **Select location** button that is alongside the **Location** field to get the **Select Folder** box.
4. To enter the value in the **Location** field, on **Select Folder**, select the folder to which you want to add the assets, and click **OK**.
5. In the **Asset type** field, enter the type of the assets that you want to add.
6. To import more than one asset, click **Import assets,** and then click the button that is alongside the **Select file** field.
7. To enter the value in the **Select file** field, in the **Open** box, select the CSV file from which to import the assets, and click **Open**.
8. Click **Next** to get the **Preview Asset Details** panel.
9. On **Preview Asset Details**, review the asset fields of the CSV file that you selected, and click **Finish** to get the **Progress Details** panel.
10. On **Progress Details**, click **Finish** to complete the import of assets.

See “Adding assets” on page 506.

See “Running a collection-evaluation-reporting job from the Standards view” on page 663.

See “Associating assets with security objective” on page 1093.

Creating business assets

To create business assets, you require the following permissions:

- Permissions that are associated with the Manage asset and asset group, and View Assets tasks
- Requisite permissions on the asset folder

The asset system stalls the duplication of any business asset. If you attempt the duplication of asset, the system displays a message.

To create a business asset

1. On the CCS home page, click **Manage** > **Asset System**.
2. In the asset system, on **Asset Tasks**, click **Create Business Assets** to get the Create Business Assets wizard.
3. On **Provide Business Asset Information**, to specify the folder in which to create the business asset, click the **Select location** button that is alongside the **Location** field.
4. To enter the path to the folder in the **Location** field, select the folder in the **Select Folder** box, and then click **OK**.
5. If you want to create a single business asset, click **Create a business asset**, and click **Next**.
6. In the **Name** and **Type** fields on **Specify Business Asset Details**, enter the name and the type of the business asset to make available the **Next** button.
7. Enter values for the optional attributes of the business asset in the respective fields.
8. Click **Finish** to get the confirmation that the asset was created.
9. Click **OK** on the confirmation box.

See “About business assets” on page 62.

See “Creating multiple business assets” on page 508.

See “Running a collection-evaluation-reporting job from the Standards view” on page 663.

See “Associating assets with security objective” on page 1093.

Creating multiple business assets

To create multiple business assets, import the business assets into CCS from a CSV file.

For the import of business assets, select a CSV file that meets the following conditions:

- Match between the CSV columns and the business asset fields.

- No extra values or missing values.
- No mandatory fields are missing or incorrect.

To create multiple business assets

1 On the CCS home page, click **Manage** > **Asset System**.

2 In the asset system, on **Asset Tasks**, click **Create Business Assets** to get the Create Business Assets wizard.

3 On **Provide Business Asset Information**, click the **Select location** button to get the **Select Folder** box.

4 In the **Select Folder** box, select the folder in which you want the business assets created, and then click **OK**.

This action enters the path to the folder in the **Location** field.

5 To create multiple business assets from a CSV file, click **Import business assets**.

6 To enter the path to the CSV file in the **Select file** field, click the **Select file** button and get the **Open** box.

7 In **Open**, select the CSV file, and then click **Open**.

8 On **Provide Business Asset Information**, in the **Preview** section, review the values in the fields to verify the attributes for the assets to be added, and click **Finish**.

9 On **Progress Details** that confirms the number of business assets that were created, and the number of failures, click **Finish**.

See “About business assets” on page 62.

See “Creating business assets” on page 507.

See “Running a collection-evaluation-reporting job from the Standards view” on page 663.

See “Associating assets with security objective” on page 1093.

Editing business assets

You add attributes during the editing of business assets to create new types of business assets.

To edit a business asset

1 On the CCS home page, click **Manage** > **Asset System**.

2 Select a folder in the asset system pane , and in the Assets table, select the business asset that you want to edit.

3 Right-click the business asset and click **Edit**.

Alternatively, select the business asset, and on **Common Tasks**, click **Edit**.

4 On **Edit**, click **Properties** to edit attributes, or click **Tags** to add or remove tags.

The following attributes are available for edit: Confidentiality, Integrity, Availability, Custodian, Department, Location, and Owner. Use the following Tag Set Options: Append, Overwrite, or Clear.

5 Make the required modifications, and click **OK**.

See "About business assets" on page 62.

See "About the management of business assets" on page 141.

Associating with a business asset

Association is necessary to arrive at the compliance score or risk score of a business asset. Map the business asset folder to the risk objective to compute the risk score for a business asset. A policy that is applied to the business asset applies to all assets that are associated with the business asset.

To associate with a business asset

1 In the Assets table of the asset system, select the asset for which you want to form an association.

2 Right click the asset and click **Associate with Business Asset**.

Alternatively, on **Asset Tasks**, click **Associate with Business Asset**.

3 In **Associate with Business Asset**, select the business asset with which you want to form the association, and click **Associate**.

4 On the **Associate with business asset** message that confirms the formation of the association, click **OK**.

See "About associations with business assets" on page 143.

See "Removing the association with a business asset" on page 510.

See "Associating assets with security objective" on page 1093.

Removing the association with a business asset

The asset system provides the **Remove Association** task that facilitates the removal of associations with business assets.

To remove the association with a business asset

1. In the Assets table of the asset system, select the business asset whose association you want to remove.
2. Right-click the business asset and click **Remove Association**.

   Alternatively, select the business asset whose association you want to remove. On **Asset Tasks**, click **Remove Association**.
3. On the **Remove Association** message, to confirm that you want to proceed with the removal of the association, click **Yes**.

See "About associations with business assets" on page 143.

See "Associating with a business asset" on page 510.

See "Associating assets with security objective" on page 1093.

Assigning permissions on business assets

CCS controls user access to business assets. The asset system restricts actions on business assets to the roles and permissions that are assigned to users on business assets. A task is an action that a user performs. Many predefined tasks constitute a role. A user that is assigned a role performs the tasks that are associated with the role. Tasks link to privileges or permissions.

The CCS control of business asset users encompasses the following:

- CCS Administrator assigns permission on asset folders and business assets.
- Permissions that are stamped on a business asset pertain to that business asset alone. The permissions do not extend to associated assets.
- The asset folder and business asset permissions are synced in the reporting database.
- Any user who has a permission on a business asset, gets the permission to view all associated network and business assets in Dynamic Dashboards. On drilling down, the user can view all the associated assets and their risk scores and compliance scores.
- A business asset inherits the permissions that are assigned to its folder.

Users with the requisite permissions perform the following permissions-related tasks on business assets:

- Assign permissions on folders and business assets.
- Create roles, and assign permissions on business assets.
- Assign multiple roles to users.

To assign permissions on a business asset

1 On the Control Compliance Suite home page, click **Settings** > **Roles** and assign users or groups to roles for your business assets.

2 Click **Settings** > **Permission Management**.

3 In the Permission Management view, from the Business Objects folders, select the folder that you want displayed in the **Objects** pane.

4 In the **Objects** pane, select the business asset whose details you want displayed in the **Preview** pane.

5 In the **Users and Groups** section in the **Preview** pane, click **Assign Permissions**.

6 Click **Add** to get the **Select Users/Groups** box, select the roles, users or groups, and then click **OK**.

7 On **Assign Permissions**, click **OK**.

See "Removing permissions from a business asset" on page 512.

Removing permissions from a business asset

The control of user access on business assets comprises both the granting and removal of permissions on business assets.

To view the permissions on a business asset, right-click the business asset, and click **View Permissions**. Alternatively, on **Common Tasks**, click **View Permissions**.

To remove permissions on a business asset

1 On the CCS home page, click **Settings** > **Permission Management**.

2 In the Permission Management view, from the Business Objects folders, select the folder that you want displayed in the **Objects** pane.

3 In the **Objects** pane, select the business asset whose details you want displayed in the **Preview** pane.

4 In the Users and Groups section, select the users or groups whose permissions you want to remove, and then click **Remove Permissions**.

5 On **Remove Permissions**, select the roles for the user or group, and click **Remove**.

6 On **Remove Permissions**, click **Update**.

See "Assigning permissions on business assets" on page 511.

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 498.
- Edit asset group.
  See "Editing an asset group" on page 513.
- Copy and paste asset group.
  See "Copying and pasting an asset group" on page 513.
- Rename Asset Group
  See "Renaming an asset group" on page 514.

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**.

Renaming an asset group

To rename the asset group

1. In the tree pane right click the asset group.
2. Select **Rename Asset Group**.
3. In the **Rename Asset Group** dialog box, type a new name for the group.
4. Click **OK**.

Performing the global tasks

You can perform the following global tasks from the Asset System view:

- Mark as control point.
- Request exceptions.
- Set up data collection.
  See "Setting up a data collection job from the Asset System view" on page 517.
- Run evaluation.
  See "Running an evaluation job from the Asset System view" on page 519.
- Run collection-evaluation-reporting
  See "Running a collection-evaluation-reporting job from the Asset System view" on page 521.

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 148.

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 621.
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 616.

See “Control points” on page 148.

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 Specify Notification Information panel, edit the notification information for the notification type. Select the tab of the notification type. Modify the Subject and the Message. Click **Next**.

10 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 647.

See "About exception states " on page 155.

Setting up a data collection job from the Asset System 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 data collection 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 one of the following options:

Run with criteria	Lets you collect the data for the assets for which the data is older than the specified number of days or is missing.
Run now	Runs the job immediately, only once.
Run periodically	Runs the job periodically based on the specified interval. Lets you specify the date and time to being the periodic schedule on. The **Run Periodically** option presents more options within the schedule.

The following table describes the options under the **Run periodically options**:

Run once	Runs the job only once based on the date and time that you specify in the **Start On** option.
Run every # days	Runs the job at regular intervals based on the number of days you specify.
Sub-schedule for data collection	Lets you specify the number of days after which you want to repeat the job. The option also lets you specify the last day until you want the job to continue running periodically. The sub-schedule is a subset of the period that you specify in the **Run every # days** option. This schedule collects the data for the assets for which data was never collected for the standards in the job scopes.

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 519.

Running an evaluation job from the Asset System view

You run an evaluation job wizard to evaluate the assets in your organizations against specific standards or checks.

See "About evaluation jobs" on page 164.

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 520.

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.

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 164.

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 525.

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 **Schedule Job** panel, select one of the following options:

Run with criteria	Lets you collect the data for the assets for which the data is older than the specified number of days or is missing. **Note:** The **Run with criteria** option is applicable only for the data collection job.
Run now	Runs the job immediately, only once.
Run periodically	Runs the job periodically based on the specified interval. Lets you specify the date and time to being the periodic schedule on. The **Run Periodically** option presents more options within the schedule.

The following table describes the options under the **Run periodically options**:

Run once	Runs the job only once based on the date and time that you specify in the **Start On** option.
Run every # days	Runs the job at regular intervals based on the number of days you specify.

Sub-schedule for data collection	Lets you specify the number of days after which you want to repeat the job. The option also lets you specify the last day until you want the job to continue running periodically. The sub-schedule is a subset of the period that you specify in the **Run every # days** option. This schedule collects the data for the assets for which data was never collected for the standards in the job scopes. **Note:** The sub-schedule is applicable only to the data collection 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.

12 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.

   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 "Quick start with minimum configuration" on page 277.

Configuring credentials

You can add and view platform and asset credentials from the Assets view.

To add a credential

1 Go to **Manage > Asset System**.

2 In the Asset System view, in the tree pane, right-click Asset System folder.

3 Select **Add Credential**.

See "Adding asset credential" on page 376.

To view configured credentials

1 Go to **Manage > Asset System**.

2 In the table pane, select the asset group of which you want to view the asset credentials.

3 From the Global Tasks, select **View Credential**.

The **View Credentials** panel lets you view the credentials which are configured from the Credentials view. You can customize the view by selecting any of the following options from the Display list:

- All assets
- Assets with credentials
- Assets without credentials

See "RBAC for managing credentials" on page 365.

Performing the asset tasks

You can perform the following asset tasks from the Asset System view:

- Import assets.

See “Importing assets” on page 440.

- Edit assets.
  See “Editing assets” on page 527.
- Move assets.
  See “Moving an asset” on page 528.
- Export CSV headers.
  See “Exporting CSV headers” on page 529.
- Create Business Assets
  See “Creating business assets” on page 507.
  See “Creating multiple business assets” on page 508.
- Associate with Business Asset
  See “Associating with a business asset” on page 510.
- Remove Association
  See “Removing the association with a business asset” on page 510.
- Add Assets
  See “Adding assets” on page 506.
  See “Adding multiple assets” on page 507.

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 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**.

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.

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 From the **Asset Tasks** in the taskbar , select **Export CSV Headers**

3 Select **Asset type** from the list.

4 Select the **CSV file location** where you want to export the CSV file with headers.

See “Importing asset-specific and common fields using the CSV data collector” on page 461.

Exporting assets as CSV

You can export assets as a CSV file.

To export assets as CSV

1 Go to **Manage > Assets > Asset System**.

2 From the **Asset Tasks** in the taskbar , select **Export Assets as CSV**

3 Select an **Asset Type**.

4 Browse and add the asset folder **Location**.

5 Select the **CSV file location** where you want to save the CSV file.

Performing the common tasks

You can perform the following common tasks from the Asset System view:

- View permissions
- Delete
  See “Deleting assets or asset groups” on page 530.

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 528.

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 437.
- Copy and paste rule
- Delete rule.
- Move rule
- Edit rule.
- View reconciliation rules details pane.
- Use Filter by pane.

Chapter 23

Remediating assets

This chapter includes the following topics:

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.

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.

You have the option to remediate the assets automatically or to select the assets to remediate manually.

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 23-1 Remediation options

Option	Description
ServiceDesk URL	The hyperlink that is used to create ServiceDesk tickets for asset remediation. http://*servername/WebServicename*
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.

Table 23-1 Remediation options *(continued)*

Option	Description
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.

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.

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.

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 23-2 Remediation options

Option	Description
ServiceDesk URL	The hyperlink that is used to create ServiceDesk tickets for asset remediation. http://*servername/WebServicename*
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.

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.

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.

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.

   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.

Chapter 24

Managing queries

This chapter includes the following topics:

- Query management

Query management

Control Compliance Suite provides query tasks to help you manage queries.

Table 24-1 tabulates the tasks you perform to manage queries.

Table 24-1 Tasks in query management

Query task	Task information
Monitor queries	Monitoring queries See "Monitoring queries" on page 542.
Run queries	Running queries See "Running queries" on page 544.
Import queries	Importing queries See "Importing queries" on page 544.
Export queries	Exporting queries See "Exporting queries" on page 545.
Copy and paste queries	Copying and pasting queries See "Copying and pasting queries" on page 546.
Delete queries	Deleting queries See "Deleting queries" on page 546.

Table 24-1 Tasks in query management *(continued)*

Query task	Task information
View query permissions	Viewing query permissions See "Viewing query permissions" on page 547.
View and manage query results	Viewing and managing query results See "Viewing and managing query results" on page 548.
Edit queries	Editing queries See "Editing queries" on page 551.
Purge query information	Scheduling purges of query information See "Scheduling purges of query information" on page 551.

Permissions required for query management

Any Control Compliance Suite user can configure a query. However, only a user who is assigned the Data Collection task can associate scope with a query and run the query. To schedule queries, you need scheduled job credentials.

Table 24-2 lists the tasks that entitle you to the permissions for query management.

Table 24-2 Permissions for query management

Task	What it entitles
Manage Queries	Entitles the user to create, update, and delete queries
Execute Queries	Entitles the user to run queries
View Queries	Entitles the user to view query information

See "Query management" on page 541.

Monitoring queries

Query management includes the monitoring of queries. Monitor queries from the following Control Compliance Suite pages:

- Queries

Use the Queries page to view the status of your queries and query runs. The queries table displays the queries in the folder that you selected in the query folders pane. Use the **Status** filters to filter the display of queries in the Queries table.

To monitor queries from the Queries page

- Jobs

  Use the Jobs page to view the status of your queries and the status details. The Jobs table displays all Control Compliance Suite queries. Under **Job type**, check **Queries** to get queries displayed in the Jobs table. To get only baseline queries in the Jobs table, check **Baseline Queries**. Use the **Last Run Date** filters to filter the display of queries in the Jobs table.

  To monitor queries from the Jobs page

To monitor queries from the Queries page

1. On the Control Compliance Suite home page, point at **Manage** and click **Queries** to get the Queries page.
2. Select the query in the Queries table to view information about the query.
3. Right click the selected query, and click **Refresh Selected Query** to get the query status updated.

   Alternatively, click **Refresh Selected Query** on **Query Tasks**.

The Jobs page provides the following tasks:

- **Job tasks**: Use **Job tasks** to run, refresh, delete, edit a query, or schedule a query run.
- **Job run tasks**: **Job run tasks** provides **Cancel job**, and **Delete job run**.
- **Common tasks**: **Common tasks** provides **Run baseline job**.

Select a query in the Jobs table, and right-click the query to get the following tasks:

- **Run job now**
- **Edit job**
- **Delete job**
- **Schedule job**
- **Refresh selected job**
- **Cancel job**
- **Delete job run**
- **View Results**
- **Run Baseline**

To monitor queries from the Jobs page

1. On the Control Compliance Suite home page, point to **Monitor**, and then click **Jobs** to get the Jobs page.
2. In the **Filters** pane, check **Queries**.
3. To get the query status updated, select the query in the Jobs table, and click the **Update** icon.

See "Query management" on page 541.

Running queries

Query runs are scheduled during query configuration. However, you may run a query without a schedule. To run or schedule query runs, you need the permissions that are associated with the View All Jobs and Manage Jobs tasks. To rerun a query, click the **View Results** task to access the View Results-Manage page, and then click **Run Again**.

To run a query

1. To access the Query management page, on the Control Compliance Suite home page, point to **Manage**, and then click **Queries**.
2. Select a query in the queries table and do one of the following:
   - Right-click the query and click **Run**.
   - On **Query Tasks**, click **Run**.

See "Query management" on page 541.

Importing queries

Control Compliance Suite does not support the duplication of queries through import. To import a query with a name identical to a query name already available in Control Compliance Suite, you must provide a different name. To import queries, you need the permissions that are associated with the Manage Jobs task.

To import a query

1. On the Control Compliance Suite home page, point to **Manage** and click **Queries**.
2. On the Query Management page, do one of the following:
   - Right-click a folder in the query folders pane and click **Import Query**.
   - On **Query Tasks**, click **Import Query**.

3 On **Import Query**, to enter the path in the **File path** field, click the button alongside the field.

4 On **Select the file for import operation**, select the file that you want to import, and click **Open**.

5 To enter the destination for the import in the **Save in** field, click the button alongside the field.

6 On **Select Folder**, select a folder and click **OK**.

7 On **Import Query**, click **OK**.

8 On **Query Import**, in acknowledgement of the message, click **OK**.

See “Query management” on page 541.

See “Exporting queries” on page 545.

Exporting queries

Export helps you take the query to another location, back up the query, or share the query with others.

Control Compliance Suite facilitates the export of queries in the following formats:

- Acrobat format (PDF)
- Comma-separated values (CSV)
- Excel
- Microsoft Word
- XML

To export a query

1 On the Control Compliance Suite home page, point to **Manage** and click **Queries**.

2 In the Queries table, select a query, and do one of the following:

   - Right-click the query, and then click **Export Query**.
   - On **Query Tasks**, click **Export Query**.

3 On **Browse for Folder**, select a folder and click **OK**.

4 If you want to create a new folder for the export, click **Make New Folder**.

5 On the **Query Export** box , in acknowledgement of the export message, click **OK**.

See “Query management” on page 541.

See “Importing queries” on page 544.

Copying and pasting queries

Query management facilitates the copying and pasting of queries. The copy of a query appears with the name 'Copy of...'.

To copy and paste a query

1. To access the Queries page, on the Control Compliance Suite home page, point to **Manage**, and click **Queries**.
2. In the **Queries** pane, select the folder that contains the query that you want to copy.
3. In the queries table, select the query you want to copy, and do one of the following:
   - Right-click the query, and click **Copy Query**.
   - On **Query Tasks**, click **Copy Query**.
4. At the location where you want to paste the query, do one of the following:
   - Right-click and click **Paste Query**.
   - Click, and on **Query Tasks**, click **Paste Query**.

See “Query management” on page 541.

Deleting queries

Control Compliance Suite facilitates the deletion of queries. To delete one query, select one query for the operation. To delete multiple queries, select multiple queries for the operation.

Delete a query from the query management page, or from Jobs view.

To delete a query

1. To access the Queries page, on the Control Compliance Suite home page, point to **Manage**, and click **Queries**.
2. In the queries table, select a query and do one of the following:
   - Right-click the query, and click **Delete Query**.
   - On **Query Tasks**, click **Delete Query**.
3. To confirm your intent to delete the query, on **Delete**, click **Yes**.

See “Query management” on page 541.

Viewing query permissions

The **View Permissions** task of query management facilitates the viewing of the permissions on queries.

The **View Permissions** box lists the trustees and their permissions under the following heads:

- User/Group Name
- Role
- Inherited: Specific to the folder, or inherited from a parent folder

To view user permissions for a query

1. To get the Queries page, on the Control Compliance Suite home page, point to **Manage**, and click **Queries**.
2. Select a query in the queries table, and perform one of the following actions:
   - Right-click the query, and click **View Permissions**.
   - On **Common Tasks**, click **View Permissions**.
3. To see a list of the tasks that are assigned to the role, and the descriptions of the tasks, on the **View Permissions** box, expand **User/Group Name**.
4. To see your permissions, check **View my permissions**.
5. To export the permissions information, click **Export**.
6. On **Save exported file to...**, in the **File Name** field, enter a name for the file to be exported.
7. In the **Save as type** field, provide the format for the export.
8. On **Save exported file to...**, click **Save**.
9. On the **Information** box, in acknowledgement of the export message, click **OK**.
10. On **View Permissions**, click **Close**.

See “Query management” on page 541.

About management of query results

Control Compliance Suite provides the View Results page for the management of query results. Manage query results in the following ways:

- View query results.
- Filter query results.

- Export query results.
- Rerun the query after you have viewed the results.
- Modify the query.
- View the errors in query results.
- Export query failure information.

See “Viewing and managing query results” on page 548.

See “Exporting query results” on page 549.

See “Exporting failure information from query results” on page 549.

Viewing and managing query results

Use the **View Results-Manage** page in query management to view and manage query results.

The **View Results-Manage** page displays the following: Query name, query run time, the platform, and the entity of the query.

To view and manage query results

1. To get the Queries page, on the Control Compliance Suite home page, point to **Manage**, and click **Queries**.
2. To get the **View Results** page, select a query in the queries table, and do one of the following:
   - Right-click the query, and then click **View Results**.
   - On **Common Tasks**, click **View Results**.
3. To filter results, in the **Filter** pane of the View Results page, click the arrows in the **Filter** pane, and then click **Add Statement**.
4. In the **Add Filter Statement** box, select the condition parameter type from the options that are listed.
5. In the fields for the field, operator, and value, enter values to define the filter, and then click **OK**.
6. Click **Apply**.
7. To export results, click **Export**.
8. To rerun the query, click **Run Again**.
9. To edit the query in the Create or Edit wizard, click **Modify**.

10 To view the information about errors, click **View Errors**.

11 View the records for a selected field in the **Query result details** pane.

See “Query management” on page 541.

See “Exporting query results” on page 549.

See “Exporting failure information from query results” on page 549.

Exporting query results

Query management provides the functionality to export query results. When the scope is defined, the query fetches results for all objects that are included in the scope. To get only the required records, use a filter. When filtered query results are exported in the XML format, the XML file provides the number of Records Accepted and the number of Records Rejected. The tiered dashboards of Control Compliance Suite use this information.

To export query results

1 To get the Queries page, on the Control Compliance Suite home page, point to **Manage**, and then click **Queries**.

2 In the Queries table, select a query and do one of the following:

- Right-click the query, and then click **View Results**.
- On **Common Tasks**, click **View Results**.

3 On **View Results**, click **Export**.

4 On **Export Settings**, in the **Format** field, enter the format for the export.

5 To enter the path, click the button alongside the **Path** field, and then on **Browse for Folder**, select a folder and click **OK**.

6 In the **File Name** field, enter a name for the file to be exported.

7 Click **OK**.

8 On **Information**, click **OK**.

See “About management of query results” on page 547.

See “Exporting failure information from query results” on page 549.

Exporting failure information from query results

Query management makes provision for the management of failures in query results. View the failures in query results and take appropriate action. Drag the information in any **Failures** table column to isolate it for viewing. Rerun a query, modify a query, or export the failure information in query results to better manage the failures.

Expand a query to view the asset, type, and the asset owner of the query.

The **View Errors** feature fetches the **Failures** box that provides the following information:

- Date: Displays the query run date
- Error: States the error. For example: 'Windows Data Collection: Information Server query returned with message(s).'
- Error details: Displays the details about the error. For example: 'The RPC server is unavailable.'
- Total assets affected: Provides the number of assets to gauge the extent of the problem
- State: Query failures display two states, Error or Warning. Unlike a warning, an error can stall a query run.

To export failure results

1. In the queries table on the Queries page, select a query and do one of the following:
    - Right-click the query, and click **View Results**.
    - On **Common Tasks**, click **View Results**.
2. On the View Results page, click **View Errors**.
3. On the **Failures** box, click **Export**.
4. On **Save exported file to...**, in the **File name** field, enter a name for the failures file.
5. In the **Save as type** field, enter the format in which you want the file exported.
6. Click **Save**.
7. On **Information**, click **OK**.

See "About management of query results" on page 547.

See "Viewing and managing query results" on page 548.

About modifications to query configurations

Queries require modifications to match changed requirements. Control Compliance Suite provides the means to edit the configurations of a query. Use any of the following methods to edit a query:

- **Edit Query** task
  Use the task to get the Create or Edit Query wizard to modify all configurations of the query.
- Tabs in the query Preview pane
  Use the following tabs in the preview pane to modify queries: **Fields**, **Scope**, **Filter Specification**, **Sort Specification**, **Notification**, and **Result Export**.
- These tabs fetch the configurations on the Create or Edit Query wizard. Make the changes to the configurations, and then click the **Save** icon. To undo the changes, click the **Revert** icon.
- The **Modify** tab on the**View Results** page
  Use **Modify** to fetch the Create or Edit Query wizard, and modify the configurations.

See “Query management” on page 541.

See “Editing queries” on page 551.

Editing queries

Use the **Edit Query** task to modify queries. The **Edit Query** task invokes the **Create or Edit Query** wizard.

To edit a query

1. On the Control Compliance Suite home page, point to **Manage**, and click **Queries**.
2. Select a query in the Queries table and do one of the following:
   - Right-click the query and click **Edit Query**.
   - On **Query Tasks**, click **Edit Query**.
3. On the panels of the **Create or Edit Query** wizard, make the required changes.

See “Configuring queries” on page 355.

See “Query management” on page 541.

See “About modifications to query configurations” on page 550.

Scheduling purges of query information

Purge query information to remove old information and accommodate fresh information. Control Compliance Suite provides you the capability to configure the purge interval for queries, as also the interval to retain query results.

To schedule the purge of query information

1. On the Control Compliance Suite home page, point to **Settings**, and click **General.**
2. In the navigation pane, under **Data Purge**, click **Purge Settings**.
3. On the Purge Settings page, click the **Queries** tab.
4. In the **Purge stale queries every ___ days** field, enter the interval for query purges.
5. In the **Retain query job results for last__ runs** field, enter the number of runs for retention.
6. In the **Purge stale baselines every __ days** field, enter the interval for the purge of query baselines.
7. In the **Retain baseline results for last__ runs** field, enter the number of runs for retention

See "Query management" on page 541.

Chapter 25

Managing agents

This chapter includes the following topics:

About the Agents view

The **Manage** > **Asses System** > **Agents** view lets you import and organize the CCS agents in the Control Compliance Suite.

The Agents view contains the following panes:

Tree pane	This pane appears on the left side of the Console window under the navigation bar. This pane displays the agents under the Agent System node. Under the Agent System node, you can view the node containing agents with no assets.

Filter by pane

This pane appears on the lower left side of the Console window under the tree pane.

You can use the following filters in the agents management view:

- Registered Date
- Platform
- Registered By
- Domain
- Agent Version

Taskbar

The taskbar appears across the top of the tree pane and the table pane in the Console window.

The taskbar includes the various tasks that you can perform from the agents maangement view.

The taskbar of the Agents view presents the following tasks under the group, Agent Tasks:

- Import Assets and Agents

  See “Importing assets and agents ” on page 556.
- Refresh Agents

  See “Refreshing agents” on page 558.
- Configure

  See “Configuring agents” on page 558.
- Remote upgrade

  See “Performing a remote upgrade of ESM agents” on page 559.

  See “Performing a remote upgrade of bv-Control for UNIX agents” on page 560.
- Configure Liveupdate

  See “Configuring LiveUpdate” on page 562.
- Delete
- Show Upgrade Status
- Restart

Table pane	The Table pane appears in the right of the Console window under the taskbar. This pane displays the agents in the agent system if the Agent System node is selected in the tree pane. The table pane displays the agents with no assets if the Agents with no Assets node is selected in the tree pane.
Details pane	The Details pane appears in the lower right side of the Console window under the table pane. The pane displays the details about the agent that is selected in the table pane. The Details pane contains the following tabs: ■ General ■ Content ■ Last Upgrade Details

Performing tasks in the Agents view

You can perform the following tasks from the **Manage** > **Agents** view:

- Import assets and agents
  See "Importing assets and agents " on page 556.
- Configure agents
  See "Configuring agents" on page 558.
- Performing remote upgrade
  See "Performing a remote upgrade of ESM agents" on page 559.
  See "Performing a remote upgrade of bv-Control for UNIX agents" on page 560.
- Configure LiveUpdate
  See "Configuring LiveUpdate" on page 562.
- Unregister the agents
  See "Deleting an agent" on page 562.
- View the upgrade status
- Restart an agent
  See "Restarting an agent" on page 563.

Importing assets and agents

If you want to collect both message-based data and raw data using the CCS agents, then you must import the agents into the agent management system. To import the agents, you must first register the agents that you want to import.

The Create or Edit Import Assets and Agents Job wizard lets you create a job that imports the agents and the assets associated with the agents.

To import assets and agents

1. Go to **Manage** > **Asset System** > **Agents**.
2. On the taskbar, select **Import Assets and Agents**.
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 **Import Assets from ESM Data Collector** panel, you may select the option, **Import Assets from ESM Data Collector**. You can select the option, only if you have the pre-configured ESM Managers from which you want to import the assets.

   Click **Next**.

   If you do not select the checkbox, then the import job by default uses the registered agents to import assets.
5. In the **Select Asset Import Scope** panel, select the scope for the asset import and click **Next**.

   Depending upon the asset type that you select in the previous panel, the default scope is selected as a Site or an asset type. If you add a site as a scope for the import job, then the site must be configured to use CCS Manager.
6. 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**.

7 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**.

8 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**.

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 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 496.

See “Configuring agents” on page 558.

See “Configuring LiveUpdate” on page 562.

See “Restarting an agent” on page 563.

See “Performing a remote upgrade of ESM agents” on page 559.

See “Performing a remote upgrade of bv-Control for UNIX agents” on page 560.

Refreshing agents

The Refresh agents option in the Agents view, fetches information about registered agents. When you click the **Refresh agents** option, it triggers a **Fetch Registered Agents** job. The job fetches information about the agents registered with the CCS Manager.

Configuring agents

You can configure the imported agents from the Agents view. You can configure a single agent or multiple agents using the **Configure** option in the Agents view.

When you select multiple agents for configuration, then the default values of the parameters are displayed.

Agent configuration parameters control the behavior of CCS agents. The parameters are stored in the agent configuration file called as agent.conf. You can set the agent configuration parameters from the Agent view. This eliminates the need for physical access to the agent computer.

To configure agents

1. Go to Manage > Agents.
2. From the taskbar, select **Configure**.
3. In the **Select Configuration Option** panel of the **Configure Parameters for Agent** wizard, select the way you want to configure the agent.

   You can select **Fetch Agent Configuration** option if you want to import the existing configurations of the ESM agent. If you do not select this option, the agent automatically gets the default configuration settings.

   Click **Next**.
4. In the **Configure agent.conf** panel, add, modify, or delete the agent parameters.
5. Select **Restart agent after setting configuration** if you want to restart the agent after the parameters are modified.

6 Click **Next**.

7 Review the summary and finish the wizard.

See "Importing assets and agents " on page 556.

See "Configuring LiveUpdate" on page 562.

See "Deleting an agent" on page 562.

See "Restarting an agent" on page 563.

See "Performing a remote upgrade of ESM agents" on page 559.

See "Performing a remote upgrade of bv-Control for UNIX agents" on page 560.

Performing a remote upgrade of ESM agents

You can use the **Remote Upgrade** task to conveniently upgrade the ESM agent software on Windows or UNIX computers. The **Remote Upgrade** option is available only if you are upgrading from the release previous to Control Compliance Suite 11.0. Remote upgrade can upgrade a single agent or all of the agents in a manager domain.

To perform a remote upgrade of ESM agents

1 While upgrading the ESM Manager to CCS Manager, specify the RemoteUpdate(RU) packages location in the CCS Manager - Service Configuration panel. During the upgrade, if you did not mention the location, you can copy the RemoteUpdate packages on the CCS Manager in the <Install Directory>ESM\Update\Agent folder.

2 Upgrade the ESM Console to CCS 11.0.

3 On the ESM Console, copy the LU_4201 package in the <Install Directory>\ESM Enterprise Console\liveupdate\granularlu folder.

The LU-4201 package is located in the ESM Upgrade folder in the CCS 11.0 product media.

4 Enable LiveUpdate on the ESM Agent.

5 On the ESM Console, run LiveUpdate to push LU_4201 packages to CCS Manager.

6 On the ESM Console, ensure that **Asset Information** and **Prepare RU** policies are listed under the Policies node.

7 Click **Asset Information > Agent Information** policy, right-click the agent platform , select Properties and then check **Asset Information**.

8 On the CCS Console, import assets and agents to get the ESM Agent into CCS.

See "Importing assets and agents " on page 556.

9 On the CCS Console, go to **Manage > Asset System > Agents**.

10 In the table pane, select an agent which you want to remotely upgrade.

11 Right-click the agent and select **Remote Upgrade**.

12 In the **Upgrade Agents** dialog box, select the ESM agent that you want to upgrade from the agents list.

13 Specify the name of the CCS Manager and the port to which the agent must be registered.

For a successful remote upgrade, ensure that the agent that you are trying to upgrade can be resolved using the hostname from the specified CCS Manager. Similarly ensure that CCS Manager can be resolved using the hostname from the agent computer.

14 Go to **Agent Tasks > Show Upgrade Status**, to view the remote upgrade status.

15 Once the remote upgrade is complete, refresh the agent if you have registered the agent to a CCS Manager of the default site. If the agent is registered to a CCS Manager of a different site, import assets and agents to get the upgraded agent into CCS.

See "Importing assets and agents " on page 556.

See "Performing a remote upgrade of bv-Control for UNIX agents" on page 560.

See "Importing assets and agents " on page 556.

See "Configuring agents" on page 558.

See "Configuring LiveUpdate" on page 562.

See "Deleting an agent" on page 562.

Performing a remote upgrade of bv-Control for UNIX agents

You can use the **Remote Upgrade** task to conveniently upgrade the imported bv-Control for UNIX agents. The **Remote Upgrade** option is available only if you are upgrading from the release previous to Control Compliance Suite 11.0.

Before you upgrade the registered bv-Control for UNIX agents, to the version 11.0, you must perform the following steps in the given order:

- Ensure that you apply 2012-1 Update on the bv-Control for UNIX 10.5.1.
- The 2012-1 Update copies the RapidFire file RF10575.rf to the <install_directory>\Symantec\RMS\Control\UNIX\rf folder. Do not change the file name.
- Launch the RMS® Console.

- Expand the BV-Control for UNIX icon located on the left pane tree of the RMS Console.
- Right-click RapidFire Updates folder.
- Select Add RapidFire from the shortcut menu.
- In the File Selection dialog, locate the RapidFire file RF10575.rf saved to the <install_directory>\Symantec\RMS\Control\UNIX\rf folder.
- Select the file and click Open to initiate the RapidFire Update installation process.
- Apply the RF to all the agent computers.
- Import the assets and agents into CCS.
  See "Importing assets and agents " on page 556.
- Before upgrading the bv-Control for UNIX agents, copy the RapidFire file RF11000.rf to the <install_directory>\Symantec\RMS\Control\UNIX\rf folder. Do not change the file name.

Your bv-Control for UNIX agents are now ready for remote upgrade to CCS 11.0

To perform a remote upgrade of bv-Control for UNIX agents

1. Go to **Manage** > **Asset System** > **Agents**.
2. In the table pane, select an agent which you want to remotely upgrade.
3. Right-click the agent and select **Remote Upgrade**.
4. In the **Upgrade Agents** dialog box, select the bv-Control for UNIX agent that you want to upgrade from the agents list.
5. Specify the name of the CCS Manager and the port to which the agent must be registered.
6. Click **OK**.
7. Import the assets and agents into CCS.

   See "Importing assets and agents " on page 556.

See "Performing a remote upgrade of ESM agents" on page 559.

See "Importing assets and agents " on page 556.

See "Configuring agents" on page 558.

See "Configuring LiveUpdate" on page 562.

See "Deleting an agent" on page 562.

Configuring LiveUpdate

See “Importing assets and agents ” on page 556.

See “Configuring agents” on page 558.

See “Deleting an agent” on page 562.

See “Restarting an agent” on page 563.

See “Performing a remote upgrade of ESM agents” on page 559.

See “Performing a remote upgrade of bv-Control for UNIX agents” on page 560.

Deleting an agent

You can delete an agent by selecting **Delete** from the Agent Tasks on the taskbar. When you click the **Delete** option, the Agents view displays a list of the assets associated with the agents. You can delete assets or agents from the list to delete.

When you unregister an agent, it is deleted from the agent management view. To use the agent again, you must register the agent with CCS Manager and then import the agent into the Agent management system .

See “Importing assets and agents ” on page 556.

See “Configuring agents” on page 558.

See “Configuring LiveUpdate” on page 562.

See “Restarting an agent” on page 563.

See “Performing a remote upgrade of ESM agents” on page 559.

See “Performing a remote upgrade of bv-Control for UNIX agents” on page 560.

Viewing the upgrade status

You can view the staus of the upgrade by selecting the **Show Upgrade Status** option from the taskbar.

To view the upgrade status:

◆ Go to **Manage** > **Agents** and select **Show Upgrade Status** from the taskbar.

  The **Show Upgrae Status** dialog displays the status of the remote upgrade of the selected agent.

  The dialog presents the following following information about the agent upgrade status:

  - Upgrade start date
  - Upgrade status

You can select an agent under the **Agent Name** area in the dialog to view the details of the upgrade status in the right side of the dialog.

See "Importing assets and agents " on page 556.

See "Configuring agents" on page 558.

See "Performing a remote upgrade of ESM agents" on page 559.

See "Performing a remote upgrade of bv-Control for UNIX agents" on page 560.

See "Configuring LiveUpdate" on page 562.

See "Deleting an agent" on page 562.

See "Restarting an agent" on page 563.

Restarting an agent

After you make changes to the configuration parameters, you must restart the agent in order to bring into effect the configuration changes. You can use the **Restart Agent** option from the tasks in the Agent view. You can also use the option to restart the agent service.

To restart the agent

1. Go to **Manage** > **Asset System** > **Agents**.
2. Select an agent in the table pane and click **Restart Agent** from the Agent Tasks on the taskbar.

See "Importing assets and agents " on page 556.

See "Configuring agents" on page 558.

See "Configuring LiveUpdate" on page 562.

See "Deleting an agent" on page 562.

See "Performing a remote upgrade of ESM agents" on page 559.

See "Performing a remote upgrade of bv-Control for UNIX agents" on page 560.

Using the Filter by pane in the Agents view

The Filter by pane contains the filters that you can use to display only the required agents.

The Control Compliance Suite provides the following default filters for filtering the agents:

Registered Date	Filters the agents according to the date of registration of agent. You can select two dates. The agents that are registered between the selected dates are displayed in the table pane.:
Platform	Filters the existing agents according to the platform to which they belong. You can specify the platform inthe **Platform** field.
Registered By	Filters the agents based on the name of the user who registered it. You can specify the name of the user in the **Name** field.
Domain	Filters the agents based on the specified domain. You can specify the domain in the **Domain** field.
Agent Version	Filters the agents based on the version.

If you specify values for more than one filters, all the selected filters are considered when the agents are displayed in the table pane.

For example:

If you specify values for the Platform, Registered By, and Domain filters, then all the filters are 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**.

Viewing agent information in the details pane

You can view the detailed information about the selected agent in the details pane.

To view the agent information in the details pane

1. Go to **Manage** > **Asset System** > **Agents**.
2. In the table pane, select the agent to view the information for.
3. In the details pane, view the information in the following tabs:
   - General tab
     See "Agent details pane - General tab" on page 565.
   - Assets tab
     See "Agent details pane - Assets tab" on page 565.
   - Content tab
     See "Agents details pane - Content tab" on page 566.
   - Last upgrade details tab
     See "Agent details pane - Last upgrade details tab" on page 566.

Agent details pane - General tab

The **General** tab of the details pane in the Agents view displays the following information about the selected agent:

- Domain name
- Host name
- NetBIOS name
- OS details

See "Viewing agent information in the details pane" on page 565.

See "Agent details pane - Assets tab" on page 565.

See "Agents details pane - Content tab" on page 566.

See "Agent details pane - Last upgrade details tab" on page 566.

Agent details pane - Assets tab

The **Assets** tab of the details pane in the Agents view presents a list of assets that belong to the selected agent.

The list of assets gives the following details about each asset:

- Name

- Type
- Path
- Creation date
- Last modified dateAgent

See "Viewing agent information in the details pane" on page 565.

See "Agent details pane - General tab" on page 565.

See "Agents details pane - Content tab" on page 566.

See "Agent details pane - Last upgrade details tab" on page 566.

Agents details pane - Content tab

The **Content** tab of the details pane in the Agents view presents the details of the type of content that is associated with the selected agent.

If a selected agent is an upgraded ESM agent, then the Content tab displays the content under the **Module-based data collector**. The **Module-based data collector** contains the details of the SUs, the version of the installed SU, and the Application Module with its version.

If a selected agent is a CCS agent, then the Content tab displays the content under the **Raw data-based data collector.agent**

See "Viewing agent information in the details pane" on page 565.

See "Agent details pane - General tab" on page 565.

See "Agent details pane - Assets tab" on page 565.

See "Agent details pane - Last upgrade details tab" on page 566.

Agent details pane - Last upgrade details tab

The **Last upgrade details** tab of the details pane in the Agents view displays the latest upgrade information about the selected agent.

See "Viewing agent information in the details pane" on page 565.

See "Agent details pane - Assets tab" on page 565.

See "Agent details pane - General tab" on page 565.

See "Agents details pane - Content tab" on page 566.

Chapter 26

Managing custom schema

This chapter includes the following topics:

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 147.

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 583.

See "About entities" on page 583.

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 569.

See “Extending an existing asset type” on page 575.

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:

Add new asset type

You need to create a custom asset type if you want to assess the assets that do not belong to the predefined asset types.

You can create a custom asset type based on the primary entities of the predefined platforms that are not supported as predefined asset types. You can also create a new platform and a new entity, and create a custom asset type based on the new entity.

See “Creating a new asset type” on page 569.

Extend existing asset type

You need to extend the existing asset types if you want to add mandatory or optional fields to the existing asset types. You can also add external fields to the asset types. The data for the external fields is not imported from the entity schema.

See “Extending an existing asset type” on page 575.

Edit existing asset type

The Edit existing asset type option lets you edit the display name, the description, the field attributes of the existing asset type. The option also lets you add the data about the custom fields of the existing asset type.

See “Editing an existing asset type” on page 577.

Create new entity schema

You need to create a new entity schema if you want to assess the assets that do not belong to the predefined platforms. You need to create an asset type that is based on the newly created entity schema to import the asset data.

See “Creating a new entity schema” on page 578.

Edit existing entity schema	You can only edit the custom entity schema. You cannot edit the entity schema for the predefined platforms. You need to edit the custom entity schema, if you want to add more fields to the custom entity that you created. See "Editing an existing entity schema" on page 582.
Create new target type	You can create a custom target type only for the custom asset types. You need to create a target type for the custom asset types to perform the evaluation with a set of checks. See "Creating a new target type" on page 587.
Editing a target type	You can change the name of the target type and the filter for the target type when you edit a custom target type. See "Editing a target type" on page 588.
Switch CSV or ODBC data collector	You can switch between a configured CSV data collector or an ODBC data collector and collect data for any custom platform.

See "About the asset type schema" on page 146.

See "About the entity schema " on page 147.

See "About the target type schema" on page 148.

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 65.
- 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 573.
- Mark the fields as mandatory or optional.
  See "About the primary, mandatory, and optional fields" on page 572.

- Add a new field that has no reference to the entity schema.
  See "About separators in name fields" on page 574.
- Add asset name fields.
  See "About separators in name fields" on page 574.
- 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 572.
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 573.

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 572.

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 573.

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 574.

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 571.

See "Extending an existing asset type" on page 575.

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 569.

About the predefined platforms and the primary entities

The Control Compliance Suite provides certain primary entities for the predefined platforms as predefined asset types.

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.

Control Compliance Suite provides the following primary entities for the predefined platforms to create asset types:

See “Creating a new asset type” on page 569.

See “Creating a new entity schema” on page 578.

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.

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 569.

See "Creating a new entity schema" on page 578.

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 569.

See "Creating a new entity schema" on page 578.

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 569.

See "Creating a new entity schema" on page 578.

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 569.

See "Extending an existing asset type" on page 575.

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 573.
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 573.

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 569.

Registering a platform

The **Settings > Schema Manager** view lets you register a platform to enable the import of the asset types.

Note: The registration of platform is a mandatory step to perform the asset type import.

See “Importing an asset type” on page 576.

To register a platform

1 Go to **Settings > Schema Manager**.

2 From the menu bar, click **Register Platform**.

3 In the **Register Platform** dialog box, browse and select the XML for the platform that you want to register.

You must copy the Platform and the Entity XMLs to the Reporting and Analytics, the Application Server, and the DPS folders. Restart the Symantec Application Server service and the Symantec Data Processing service for all the configured Data Processing Servers. Relaunch the Control Compliance Suite Console.

4 Click **Register.**

Importing an asset type

The import asset type functionality lets you access a custom asset type that another user has created. The user from whom you want to import the asset type must export the asset type.

You must first register the platform of the primary entity of the asset type that you want to import.

See “Registering a platform” on page 576.

To import an asset type

1 Go to **Settings > Schema Manager**.

2 From the menu bar, click **Import Asset Type**.

3 In the **Import Asset Type** dialog box, browse and select the asset type XML to import.

You must have already registered the platform for the primary entity of this asset type.

Note: You must manually copy the custom entity schema and platform XMLs for the primary entity of the asset type that you want to import.

4 Click **Import**.

Editing an existing asset type

You can edit an existing asset type from the **Settings > Schema Manager > Edit existing asset type** option.

The **Edit existing asset type** option lets you edit the attributes of the custom fields for an existing asset type.

To edit the existing asset type

1 Go to **Settings > Schema Manager > Edit existing asset type**.

2 In the **Edit Asset Type Details** panel, select the asset type that you want to edit from the **Asset Type** list.

3 Specify the new display name and the description for the asset type and click **Next**.

4 In the **Edit Attributes** panel, edit the following asset type attributes and click **Next**.

Display Name	This field is editable. You can edit the display name of the attribute from this panel.
Description	This field is editable. You can edit the description of the attribute from this panel.
Data Type	This field it not editable.
Field Type	This field is not editable.
Allow Editing of Field?	This field lets you choose if you want to make the field editable.

5 In the **Summary** panel, review the information that you entered in the wizard. Click **Back** to make any modifications or click **Finish** to exit the wizard.

Working with custom entity

A custom entity comprises a group of fields.

See "About entities" on page 583.

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 578.

See "Editing an existing entity schema" on page 582.

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 583.

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 569.

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 584.

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	<install directory>\Symantec\CCS\Reporting And Analytics For example, C:\Program Files\Symantec\CCS\Reporting And Analytics
Installation directory of the Application Server	<install directory>\Symantec\CCS\Reporting And Analytics\Application Server For example, C:\Program Files\Symantec\CCS\Reporting And Analytics\Application Server
Installation directory of the Data Processing Service (DPS)	<install directory>\Symantec\CCS\Reporting And Analytics\DPS For example, C:\Program Files\Symantec\CCS\Reporting And Analytics\DPS **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.

See “Editing an existing entity schema” on page 582.

Editing an existing entity schema

Control Compliance Suite lets you edit an existing entity schema to add new fields. You can also extend the 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 edit an existing schema

1. Go to Settings > Schema Manager.
2. Select **Edit existing entity schema** to launch the **Edit 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 578.

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 583.

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 583.

See "About fields of an entity " on page 584.

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 147.

See "Creating a CSV file for custom application" on page 487.

See "About platforms" on page 583.

See "About entities" on page 583.

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 578.

Table 26-1 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: ■ Machine entity of the Windows platform ■ Machine entity of the UNIX platform

Table 26-2 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: ■ Database of the SQL platform ■ Server of the SQL platform
User	The User entity is referenced to the following predefined entities: ■ Database of the SQL platform ■ Server of the SQL platform

Table 26-3 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 26-4 relationship details of the predefined entities for the Windows platform

Predefined entity	Relation entity
Directory	The Directory entity is referenced to the following predefined entities: ■ Machine of the Windows platform ■ Domain of the Windows platform
Domain	No defined relationship
File	The File entity is referenced to the following predefined entities: ■ Machine of the Windows platform ■ Domain of the Windows platform ■ Directory of the Windows platform
Group	The Group entity is referenced to the following predefined entities: ■ Machine of the Windows platform ■ Domain of the Windows platform
IISVirtualDirectories	The IISVirtualDirectories entity is referenced to the following predefined entities: ■ Machine of the Windows platform ■ Domain of the Windows platform
IISWebSite	The IISWebSite entity is referenced to the following predefined entities: ■ Machine of the Windows platform ■ Domain of the Windows platform
Machine	Domain of the Windows platform
Registry	The Registry entity is referenced to the following predefined entities: ■ Machine of the Windows platform ■ Domain of the Windows platform
Service	The Service entity is referenced to the following predefined entities: ■ Machine of the Windows platform ■ Domain of the Windows platform

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 new entity schema" on page 578.

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 164.

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 569.

See "Working with custom asset types" on page 567.

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 587.
- Edit a target type
  See "Editing a target type" on page 588.

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 26-5 Custom schema scenarios

Scenario	How to achieve?
You want to create a custom asset type, Windows Service.	Use the Add new asset type option on the Schema Manager view. For a detailed procedure of how to create a custom asset type, Windows Service, click on the link: See “Creating a custom asset type - Windows Service” on page 590.
You want to add a new field, TCP/IP Address to the Windows Machine asset type.	Use the Extend existing asset type option on the Schema Manager view. For a detailed procedure of how to add TCP/IP Address to the Windows Machine, click on the link: See “Extending the predefined asset type - Windows Machine” on page 592.

Table 26-5 Custom schema scenarios *(continued)*

Scenario	How to achieve?
You want to extend the Windows Machine asset type to manage the inventory information.	■ 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. For a detailed procedure click on the link: See “Extending Windows Machine to manage inventory and vendor data information” on page 593.
You want to create custom asset types printers, scanners, monitors, and so on to manage the physical devices in the enterprise.	■ 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. For a detailed procedure click on the link: See “Creating a custom asset type-Printer based on the custom platform-Devices” on page 597.

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 65.

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 103.

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 Name

     Click **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 572.

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 574.

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 “Creating a custom entity- Inventory” on page 594.
- 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 596.

Creating 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**.

   See “Creating a CSV file for custom application” on page 487.
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 573.

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 596.

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 573.

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 329.

See “Importing assets” on page 440.

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 598.

- Create a new asset type, Printer

  See "Creating a custom asset type- Printer" on page 599.

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**.

   See "Creating a CSV file for custom application" on page 487.

   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 104.

   See "About referenced entity fields" on page 573.

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:

    - <installdir>\Symantec\CCS\Reporting and Analytics
    - <installdir>\Symantec\CCS\Reporting and Analytics\Application Server
    - <installdir>\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 572.
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 467.

See "Creating a target type for the asset type - Printer" on page 601.

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 Asset System view" on page 517.

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 682.

Managing entitlements

This chapter includes the following topics:

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 618.

See “Problems in managing entitlements” on page 604.

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 604.

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 618.

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 148.

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 Control Point Effective Permissions, the Control Point Simple Permissions, the Entitlement Changes, the Control Point Permissions by Trustee, and the Entitlement Change Requests.

See "About the control point status" on page 609.

The users in the role of an entitlement administrator and the entitlements data owner perform the tasks in the entitlements system.

The tasks in the entitlements system can be divided as follows:

Manual tasks	■ Performed by the user ■ Require user input and user action.
System tasks	■ System tasks ■ Require no user input and user action.

You can perform the following manual tasks in the entitlements system based on your role:

Mark an asset as a control point See “Marking an asset as a control point” on page 514.	You mark an asset as a control point if you want to monitor the entitlements of the asset through the approval workflow. The entitlement administrator can mark assets as control points from the asset system. When the assets are marked as control points they appear in the Manage > Entitlements > Control Points view. By default, the control points are in the No Review Configured state.
Create a review cycle setting See “Creating a review cycle setting” on page 618.	You create a review cycle setting to define a review period for the approval of the entitlements of the control points. The entitlement administrator can create a review cycle setting from the Manage > Entitlements > Review Cycle Settings view.
Assign the role of data owner to a trustee	You select a trustee who can review and approve the entitlements for the control points. You must assign the role of an entitlements data owner to the trustee from > Settings > Roles view.

Configure the control point See “Configuring control points” on page 616.	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 627. See “Configuring the automatic entitlements import” on page 626.	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 629.	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 630.	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 150.	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 629.	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 627. See "Configuring the automatic entitlements import" on page 626.	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	Indicates that the control point has no review cycle that is associated with it. No Review Configured is the default status of the control point, when an asset is marked as the control point. A control point cannot be monitored for its entitlements in the approval workflow unless a review cycle is associated with it.
Review Start Awaited	Indicates that the review cycle is associated with a control point and the review start date is awaited. The review cycle start depends on the date that you indicate in the review cycle settings.

Review Started

Indicates that the review cycle for the control point has started.

The review cycle starts after the daily approval job runs on the review cycle start date.

Status changes from Review Start Awaited to Review Started when the review cycle starts.

Entitlement Import Required

Indicates that the entitlements should be imported before the approval period begins.

The control point status changes to the Entitlement Import Required in the following cases:

- 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

Indicates that the entitlement import is in progress.

Status changes from Entitlement Import Required to Entitlement Import Pending.

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.

The system runs an approval job on a daily basis. The approval job changes the status to Entitlement Import Pending.

Approval Start Awaited

Indicates that the approval period for the control points is yet to start after Entitlement Import.

Request for Approval

Indicates that the request for approval is sent to the data owner of the control points.

The control point status changes to the Request for Approval in the following cases:

- 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

Indicates that the data owner has requested changes in the entitlements of the control points.

Status changes from Request for Approval to Request for Change.

Approved

Indicates that the data owner has approved the entitlements of the control points.

See “Working with control points” on page 616.

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

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

This pane displays the asset folders and asset groups under the Asset System node.

Filter by pane

This pane appears in the lower left side of the console window under the tree pane.

You can use the following filters in the Control Points view:

- Control point status
- Select tags

Table pane	This pane appears on the right side of the console window under the taskbar . 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. 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.
Details pane	This pane appears in the lower right side of the console window under the table pane. This pane displays the details of the control point that is selected in the table pane.

You can perform the following tasks from the Control Points view:

- Import entitlements
- Unmark a control point
- Configure control points
- Request exceptions
- Request approval
- Comparing entitlements
- 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	This pane appears on the left side of the console window under the navigation bar. This pane displays the asset folders and asset groups under the Asset System node.

Filter by pane	This pane appears in the lower left side of the console window under the tree pane. You can use the following filters in the Control Points view: ■ Control point status ■ Select tags
Table pane	This pane appears on the right side of the console window under the taskbar . 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. The table pane displays the control points according to the current status.
Details pane	This pane appears in the lower right side of the console window under the table pane. This pane displays the details of the control point that is selected in the table pane.

See "About the Control Points view" on page 611.

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.

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.

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.

The Review Cycle Settings view contains the following panes:

Table pane	This pane appears under the taskbar . This pane displays all the review cycle settings that you create.

Details pane	This pane appears in the lower right side of the console window under the table pane. This pane displays the control points that are associated with the review cycle setting that is selected in the table pane.

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 514.
- Unmark a control point
  See "Unmarking a control point" on page 616.
- Configure a control point
  See "Configuring control points" on page 616.
- Create review cycle settings
  See "Creating a review cycle setting" on page 618.

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 514.

See "Control points" on page 148.

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 618.

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 514.

See “Unmarking a control point” on page 616.

See “Control points” on page 148.

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 150.

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: ■ 1 Week ■ 2 Weeks ■ 1 Month ■ 3 Months ■ 6 Months ■ 1 year
Next Review Start Date	Lets you choose a date from when the review cycle should start.
Approval Start	Lets you select a period before the review end date to start the approval. Approval start indicates that the data owner has to approve the control points within the specified limit before the review ends. You can select from the following options: ■ 1 Week ■ 2 Weeks ■ 1 Month ■ 3 Months ■ 6 Months ■ 1 year
Approval Duration	Lets you select a duration for the approval period. You can select from the following options: ■ 1 Week ■ 2 Weeks ■ 1 Month ■ 3 Months ■ 6 Months ■ 1 year
Is Recurring?	Lets you select a True or False value to make the review cycle recurring.

Import Entitlements before # days of Approval Start	Lets you select the number of days before the approval start date, to import the entitlements. You can choose to import the entitlements from 0 to 150 days before the approval start.

See "Deleting a review cycle setting" on page 620.

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 618.

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.

See "Control points" on page 148.

See "Working with control points" on page 616.

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 627.

Viewing control point details

You can view the details of the control point from the **Manage > Entitlements > Control Points** view.

To view the control point details

1. Go to **Manage > Entitlements > Control Points**.
2. In the table pane, select a control point.
3. In the task bar, select **View Details**.
4. View the control points details in the following tabs:
    - General
      See "Control point details pane- General tab" on page 640.
    - Entitlements
      See "Control point details pane- Entitlements tab" on page 641.
    - Review Cycle
      See "Control point details pane- Review Cycle tab" on page 641.
    - Entitlement Import Details
      See "Control points details pane- Entitlement Import Details tab" on page 642.

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 609.

In the entitlement system, you perform the following tasks with the entitlement import:

- Configure the import settings.
  See "Configuring the import settings" on page 624.
- Configure the automatic entitlements import.
  See "Configuring the automatic entitlements import" on page 626.
- Import the entitlements manually.
  See "Importing the entitlements manually" on page 627.

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 627.
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 626.

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.

See "Working with entitlements import" on page 623.

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 623.

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 627.

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 626.

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 621.

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 626.

Working with approval

The approval-related tasks of the control point include the following:

- Request approval
  See "Requesting approval of entitlements" on page 629.
- Request change
  See "Requesting changes in entitlements" on page 630.
- Approve
  See "Approving the entitlements" on page 630.
- Configure alternative approver
  See "Configuring the alternative approver" on page 631.

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 630.

See "Approving the entitlements" on page 630.

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 630.

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 630.

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 616.

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 150.

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.

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 "Configuring entitlements notifications" on page 635.

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	Address token that is used in the To field. The email ID of the data owner replaces the token
AlternateApproverMailAddress	Address token that is used in the To field. The email ID of the alternative approver replaces the token.

DataOwnerName	Body or Subject token that can either be used in the subject line or the message body. The name of the data owner replaces the token.
AlternateApproverName	Body or Subject token that can be used either in the subject line or in the message body. The name of the alternative approver replaces the token
ReviewCycleName	Body or Subject token that can be used either in the subject line or in the message body. The name of the review cycle replaces the token.
ReviewCycleStartDate	Body or Subject token that can be used either in the subject line or in the message body. The review cycle start date replaces the token.
ApprovalStartDate	Body or Subject token that can either be used in the subject line or the message body. The approval period start date replaces the token.
ApprovalEndDate	Body or Subject token that can be used either in the subject line or in the message body. The approval period end date replaces the token.
ReviewCycleEndDate	Body or Subject token that can be used either in the subject line or in the message body. The review cycle end date replaces the token.

AutomaticImportRequiredDate	Body or Subject token that can be used either in the subject line or in the message body. The date when the control point status changes to Entitlement Import Required replaces the token.
ReviewCycleSettingsDetails	Body or Subject token that can be used either in the subject line or in the message body. The details of the review cycle settings replace the token.
ReviewCycleDates	Body or Subject token that can be used either in the subject line or in the message body. 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.
ControlPointIdentifier	Body token that can be used in the message body. The name of the control point replaces the token.
ApproverName	Body or Subject token that can be used either in the subject line or in the message body. The name of the alternative approver replaces the token .
ApproverMailAddress	Body or Subject token that can be used either in the subject line or in the message body. The email ID of the alternative approver replaces the token.

See “About notification tokens” on page 636.

See “Working with notifications” on page 632.

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 636.

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

Address token that is used in the To field.

The email ID of the data owner replaces the token

AlternateApproverMailAddress

Address token that is used in the To field.

The email ID of the alternative approver replaces the token.

DataOwnerName

Body or Subject token that can either be used in the subject line or the message body.

The name of the data owner replaces the token.

AlternateApproverName

Body or Subject token that can be used either in the subject line or in the message body.

The name of the alternative approver replaces the token

ReviewCycleName

Body or Subject token that can be used either in the subject line or in the message body.

The name of the review cycle replaces the token.

ReviewCycleStartDate	Body or Subject token that can be used either in the subject line or in the message body. The review cycle start date replaces the token.
ApprovalStartDate	Body or Subject token that can either be used in the subject line or the message body. The approval period start date replaces the token.
ApprovalEndDate	Body or Subject token that can be used either in the subject line or in the message body. The approval period end date replaces the token.
ReviewCycleEndDate	Body or Subject token that can be used either in the subject line or in the message body. The review cycle end date replaces the token.
AutomaticImportRequiredDate	Body or Subject token that can be used either in the subject line or in the message body. The date when the control point status changes to Entitlement Import Required replaces the token.
ReviewCycleSettingsDetails	Body or Subject token that can be used either in the subject line or in the message body. The details of the review cycle settings replace the token.
ReviewCycleDates	Body or Subject token that can be used either in the subject line or in the message body. 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.

ControlPointIdentifier	Body token that can be used in the message body. The name of the control point replaces the token.
ApproverName	Body or Subject token that can be used either in the subject line or in the message body. The name of the alternative approver replaces the token .
ApproverMailAddress	Body or Subject token that can be used either in the subject line or in the message body. The email ID of the alternative approver replaces the token.

See "About notification tokens" on page 636.

See "Working with notifications" on page 632.

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 638.
- Tags
  See "Tag filter" on page 639.

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

See “Control points” on page 148.

See “Working with control points” on page 616.

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 filer, you click on the Customize icon at the top of the Filter by pane.

See “Tagging” on page 151.

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 640.
- Entitlements
  See “Control point details pane- Entitlements tab” on page 641.
- Review Cycle

See “Control point details pane- Review Cycle tab” on page 641.

- Entitlement Import Details
  See “Control points details pane- Entitlement Import Details tab” on page 642.
- Review Cycle Dates
  See “Control points details pane- Review Cycle Dates tab” on page 643.
- Tags
  See “Control point details pane- Tags tab” on page 642.
- Exceptions
  See “Control point details pane- Exceptions tab” on page 642.
- Workflow Trails
  See “Control point details pane- Workflow Trails tab” on page 642.

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.

See "Working with control points" on page 616.

See "Viewing control point details" on page 622.

See "Viewing the control points information in the details pane" on page 639.

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.

See "Working with control points" on page 616.

See "Viewing control point details" on page 622.

See "Viewing the control points information in the details pane" on page 639.

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 618.

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.

See “Working with control points” on page 616.

See “Viewing control point details” on page 622.

See “Viewing the control points information in the details pane” on page 639.

Control point details pane- Exceptions tab

The Exceptions tab lists all the exceptions that are applied to the selected control point.

See “Working with control points” on page 616.

See “Viewing control point details” on page 622.

See “Viewing the control points information in the details pane” on page 639.

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.

See “Working with control points” on page 616.

See “Viewing control point details” on page 622.

See “Viewing the control points information in the details pane” on page 639.

Control points details pane- Entitlement Import Details tab

The Entitlement Import Details tab of the control point details pane provides information about the entitlements that are imported for the selected control point.

The Entitlement Import Details tab provides the following information:

- Entitlement type
- Last import date
- Last approved date

See "Working with control points" on page 616.

See "Viewing control point details" on page 622.

See "Viewing the control points information in the details pane" on page 639.

Control points details pane- Review Cycle Dates tab

The Review Cycle Dates tab of the control points details pane provides the information about the review cycle dates for the selected control point.

See "Working with control points" on page 616.

See "Viewing control point details" on page 622.

See "Viewing the control points information in the details pane" on page 639.

Managing exceptions

This chapter includes the following topics:

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.

See "Viewing exception information in the details pane" on page 646.

See "About the exception management system" on page 153.

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 646.
- Request an exception
  See "Requesting an exception" on page 646.

- Approve an exception
  See “Approving an exception” on page 647.
- Set the exception state to In Review
  See “Setting the exception state to In Review” on page 648.
- Set the exception state to Request Clarification
  See “Setting the exception state to Request Clarification” on page 648.
- Set the exception state to Deny
  See “Setting the exception state to Deny” on page 648.

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
   - Associations
   - Notifications
   - Tags
   - Workflow Trails

Requesting an exception

A requestor can request an exception through the Request Exception Wizard.

A requestor can request an exception on the following objects:

- SCAP benchmark rules
- Standards, sections, or checks
  See “Requesting an exception for assets on checks” on page 515.
- Control points
- Policies

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 647.

See "About exception states " on page 155.

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**.

See "Requesting an exception" on page 646.

See "About exception states " on page 155.

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:

- SCAP benchmark rules
- Standards, sections, or checks
- Control points
- Policies

See “About exception states ” on page 155.

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 155.

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 155.

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 155.

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.

See "About modifying an exception" on page 649.

See "Working with exceptions" on page 645.

About modifying an exception

A requestor can modify an existing exception. However, any change in the exception puts the exception back into a Requested state. If a requestor edits an approved exception, the state of the exception is set to Requested. The exception has to undergo the approval process again.

See "About exceptions" on page 152.

Chapter 29

Managing standards

This chapter includes the following topics:

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

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

The pane displays a hierarchical, folder-based structure of the standards that are stored in the CCS directory.

Note: The tree pane displays the custom standards, as well as the predefined standards for the supported platforms. The regulatory standards are also displayed for the Windows and the UNIX platform.

Filter by pane

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

You can specify filters in this pane so that only the required standards, sections, and checks are displayed in the table pane.

You can use the following filters in the standards view:

- Target Platform
- Author
- Compliance Score
- Evaluated Between
- Select Tags

Table pane

The table pane appears in the right side of the console window under the taskbar .

This pane displays the standards, sections, and checks.

Note: The simple and the complex checks in the Table pane are tagged differently. You can differentiate between the simple and complex checks visually by the icon. The icon that indicates the complex checks has a red mark on the upper left corner.

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 659. ■ Import Standard See "Importing a standard" on page 662. ■ Export Standard See "Exporting a standard" on page 662. ■ Create Check See "Creating a new check" on page 682. ■ Create Section
Evaluation Tasks	
ESM Tasks	Change ESM Policy Name
Common Tasks	■ Move See "Moving a standard" on page 661. See "Moving a check" on page 681. ■ Delete See "Deleting a standard" on page 663. See "Deleting a check" on page 682. ■ Request Exception See "Requesting an exception" on page 646. See "Launching the Request Exception Wizard" on page 647.

See "About the standards filters" on page 177.

See "Working with standards" on page 654.

See "Working with checks" on page 669.

See "Viewing standard information in the details pane" on page 655.

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 polices 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.

See "About the Standard Migration Utility" on page 704.

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 655.
- Create a new standard.
  See "Creating a new standard" on page 659.
- Copy and paste a standard.
  See "Copying and pasting a standard" on page 660.
- Move a standard.
  See "Moving a standard" on page 661.
- Import a standard.
  See "Importing a standard" on page 662.
- Export a standard.
  See "Exporting a standard" on page 662.
- Rename a standard.
  See "Renaming a standard" on page 660.
- Delete a standard.
  See "Deleting a standard" on page 663.
- Evaluate an asset against a standard.
- Create a chained job
  See "Running a collection-evaluation-reporting job from the Standards view" on page 663.

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 656.
- Description
  See "Standard details pane - Description tab" on page 657.
- Evaluations
  See "Standard details pane - Evaluations tab " on page 657.
- References
  See "Standard details pane - References tab" on page 658.
- Exceptions
  See "Standard details pane - Exceptions tab" on page 655.
- Tags
  See "Standard details pane - Tags tab " on page 658.

See "About the details pane" on page 262.

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 262.

See “Viewing standard information in the details pane” on page 655.

See “Working in the details pane” on page 692.

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 660.
Target Type(s)	This list reflects the target types that are associated with all the checks within the standard. See “About target types” on page 164.
Version	The current version of the standard. See “About versioning scheme” on page 176.
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 175.

Risk Score	The risk score of the standard. See "About risk score" on page 175.

See "About the details pane" on page 262.

See "Viewing standard information in the details pane" on page 655.

See "Working in the details pane" on page 692.

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 "Viewing standard information in the details pane" on page 655.

See "About the details pane" on page 262.

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.
Evaluation Status	Specifies the current status of the evaluation job such as executing, failed, aborted, or completed.
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 version	Displays the version of the standard.

See "Viewing standard information in the details pane" on page 655.

See "Viewing check information in the details pane" on page 670.

See "About the details pane" on page 262.

See "Working in the details pane" on page 692.

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 696.
- Edit reference information
  See "Editing reference information" on page 696.
- Delete reference information
  See "Deleting reference information" on page 697.

See "About the details pane" on page 262.

See "Working in the details pane" on page 692.

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.

See "Viewing standard information in the details pane" on page 655.

See "Viewing check information in the details pane" on page 670.

See "About the details pane" on page 262.

See "Working in the details pane" on page 692.

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

See "Working with standards" on page 654.

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.

See "Creating a new check" on page 682.

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 654.

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**.

   This step lets you copy the selected standard. But to view the copied standard, you must perform the paste operation as explained in the next step.
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**.

See “Moving a standard” on page 661.

See “Copying and pasting a check” on page 680.

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 658.

See "Working with standards" on page 654.

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 654.

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 654.

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 658.

See “Working with standards” on page 654.

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 164.

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 667.

9 In the **Schedule Job** panel, select one of the following options:

Run with criteria	Lets you collect the data for the assets for which the data is older than the specified number of days or is missing. **Note:** This option is applicable to the data collection only.
Run now	Runs the job immediately, only once.
Run periodically	Runs the job periodically based on the specified interval. Lets you specify the date and time to being the periodic schedule on. The **Run Periodically** option presents more options within the schedule.

The following table describes the options under the **Run periodically options**:

Run once	Runs the job only once based on the date and time that you specify in the **Start On** option.
Run every # days	Runs the job at regular intervals based on the number of days you specify.

Sub-schedule for data collection	Lets you specify the number of days after which you want to repeat the job. The option also lets you specify the last day until you want the job to continue running periodically. The sub-schedule is a subset of the period that you specify in the **Run every # days** option. This schedule collects the data for the assets for which data was never collected for the standards in the job scope. **Note:** The sub-schedule is applicable to the data collection only.

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.

   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 668.

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
- Compliance by Technical Check

The light-weight reports are as follows:

- Compliance Summary
- Asset Risk Summary
- Asset Evaluation Result Change
- Assets at Highest Risk
- Asset Group Compliance
- Evaluation Results Asset View
- Evaluation Results Standard View
- Remediation Asset View
- Remediation Standard View

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 663.

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 178.

See " Changing an ESM policy name at the check level " on page 687.

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 670.
- Create a new check.
  See "Creating a new check" on page 682.
- Copy and paste a check.
  See "Copying and pasting a check" on page 680.
- Move a check.
  See "Moving a check" on page 681.
- Rename a check.
  See "Renaming a check" on page 680.

- Delete a check.
  See "Deleting a check" on page 682.
- Modify a check.
  See "Editing a check" on page 685.

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 671.
   - Description
     See "Check details pane - Description tab" on page 673.
   - Expression
     See "Check details pane - Expression tab" on page 674.
   - Parameters
     See "Check details pane - Parameters tab" on page 678.
   - Remediation
     See "Check details pane - Remediation tab" on page 679.
   - Issue
     See "Check details pane - Issue tab" on page 679.
   - CVE
     See "Check details pane - CVE tab" on page 679.
   - References
     See "Check details pane - References tab" on page 673.
   - Target Type
     See "Check details pane - Target Type tab" on page 680.
   - Exceptions
     See "Check details pane - Exceptions tab" on page 671.

See "About the details pane" on page 262.

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.

See “Viewing standard information in the details pane” on page 655.

See “Viewing check information in the details pane” on page 670.

See “About the details pane” on page 262.

See “Working in the details pane” on page 692.

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	The name of the check. This value is editable. See “Renaming a check” on page 680.
Target Type	The target types to which the check is applicable. The drop-down list displays the target types associated with the check based on platforms. You can add or remove a target type by selecting the corresponding checkbox. See “About target types” on page 164.
Author	The value of Author is Symantec for a check that is contained within a predefined standard. For a check that is contained within a user-defined standard, this value refers to the user who created the check.

Version	The current version of the check. See “About versioning scheme” on page 176.
Creation Date	The date and time of creation of the check.
Last Updated	The date and time when the check was last updated.
Confidentiality	Confidentiality value has one of the following states: ■ Not Defined ■ No Impact ■ Partial ■ Complete
Integrity	Integrity value has one of the following states: ■ Not Defined ■ No Impact ■ Partial ■ Complete
Availability	Availability value has one of the following states: ■ Not Defined ■ No Impact ■ Partial ■ Complete
Access Vector	Access Vector has one of the following states: ■ Not Defined ■ Local Accessible ■ Adjacent Network Accessible ■ Network Accessible
Access Complexity	Access Complexity has one of the following states: ■ Not Defined ■ Low ■ Medium ■ High
Authentication	Authentication has one of the following states: ■ 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 680.
- Confidentiality
- Integrity
- Availability
- Access Vector
- Access Complexity
- Authentication

See “Viewing check information in the details pane” on page 670.

See “About the details pane” on page 262.

See “Working in the details pane” on page 692.

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 670.

See “About the details pane” on page 262.

See “Working in the details pane” on page 692.

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 696.
- Edit reference information
  See “Editing reference information” on page 696.
- Delete reference information
  See “Deleting reference information” on page 697.

See “Viewing check information in the details pane” on page 670.

See “About the details pane” on page 262.

See “Working in the details pane” on page 692.

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 670.

See “About the details pane” on page 262.

See “Working in the details pane” on page 692.

About using complex check

Consider the following examples:

- Consider that you have indexed parameters such as "Permission0," "Permission1," and "Permission2. You remove the index parameter "Permission1." The parameter "Permissions2" is renamed to "Permissions1."

- The permissions algorithms parameters for the Windows platform are more complex than those of other complex algorithms.

  The Permissions algorithms for Windows use parameter sets as follows:

  - Accounts
  - Permissions that the account is allowed to use
  - Scope to which the permissions are applied

- The complex checks on the user rights behave in a specific way. The complex checks on the user rights are used when some accounts must be assigned the user right for a check to pass. The other accounts can optionally be assigned the user right. If all accounts are either mandatory or optional, then you can use a generic check.

  You can use two types of checks with different parameters. The usage of the complex algorithms is based on whether a user gets more privileges on the Windows system when assigned with the user right.

- The user gets more privileges on the Windows system if you grant any of the following rights:

  - Increase a process working set
  - Modify an object label
  - Create symbolic links
  - Access Credential Manager as a trusted caller
  - Change the time zone
  - Replace a process level token
  - Generate security audits
  - Back up files and directories
  - Log on as a batch job
  - Bypass traverse checking
  - Create a pagefile
  - Create permanent shared objects
  - Create a token object
  - Debug programs
  - Enable computer and user accounts to be trusted for delegation
  - Increase scheduling priority
  - Adjust memory quotas for a process

- Log on locally
- Load and unload device drivers
- Lock pages in memory
- Add workstations to domain
- Perform volume maintenance tasks
- Access this computer from the network
- Profile single process
- Allow logon through Terminal Services
- Force shutdown from a remote systems
- Restore files and directories
- Manage auditing and security log
- Log on as a service
- Shut down the system
- Synchronize directory service data
- Modify firmware environment values
- Profile system performance
- Change the system time
- Take ownership of files or other objects
- Act as part of the operating system
- Remove computer from docking station
- Impersonate a client after authentication
- Create global objects
- The checks that determine if a user right is assigned appropriately use the following parameters:
  - RequiredAccountSIDs
    A comma-separated list of account SIDs. The accounts in this list must be assigned the user right for the check to pass
  - OptionalAccountSIDs
    A comma-separated list of account SIDs. The accounts in this list may be assigned the user right optionally. In case, an account is not assigned the right, the check passes.

        - UserRight

          The name of the user right. It is the name of the Symantec bv-Control for Windows field that reports the user rights assignment by security identifier (SID).

        - OutcomeForExtraAccount

          The parameter can take the values- Pass and Fail. In case, the accounts other than those specified in the parameters, RequiredAccountSIDs and OptionalAccountSIDs are assigned the user right and the value of this parameter is Fail, then the check Fails.
          In case the value of this parameter is Pass, then check does not fail if the accounts other than those specified in the parameters, RequiredAccountSIDs and OptionalAccountSIDs are assigned the user right.

- The user gets lesser privileges on the Windows system if you grant any of the following rights:
    - Deny logon as a batch job
    - Deny logon locally
    - Deny access to this computer from the network
    - Deny logon through Terminal Services
    - Deny logon as a service
- The checks that determine if a user right is assigned appropriately, use the following parameters:
    - RequiredAccountSIDs

      A comma-separated list of account SIDs. The accounts in this list must be assigned the user right for the check to pass
    - OptionalAccountSIDs

      A comma-separated list of account SIDs. The accounts in this list may be assigned the user right optionally. In case, an account is not assigned the right, the check passes.
    - UserRight

      The name of the user right. It is the name of the Symantec bv-Control for Windows field that reports the user rights assignment by security identifier (SID).
    - OutcomeForExtraAccount

      The parameter can take the values- Pass and Fail. In case, the accounts other than those specified in the parameters, RequiredAccountSIDs and

OptionalAccountSIDs are assigned the user right and the value of this parameter is Fail, then the check Fails.

In case the value of this parameter is Pass, then check does not fail if the accounts other than those specified in the parameters, RequiredAccountSIDs and OptionalAccountSIDs are assigned the user right.

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.

The Parameters tab also lets you add or remove the indexed parameters in case of complex checks. To add or remove the indexed parameters, you must select an indexed parameter, right-click and select **Add new parameter**. Another parameter with the next order in the index is created. You can also remove an indexed parameter. If you remove an indexed parameter, the indexing for the other parameters of the same type changes.

Consider the following examples:

- Consider that you have indexed parameters such as "Permission0," "Permission1," and "Permission2. You remove the index parameter "Permission1." The parameter "Permissions2" is renamed to "Permissions1."
- The permissions algorithms parameters for the Windows platform are more complex than those of other complex algorithms.

  The Permissions algorithms for Windows use parameter sets as follows:
  - Accounts
  - Permissions that the account is allowed to use
  - Scope to which the permissions are applied

See “Viewing check information in the details pane” on page 670.

See “About the details pane” on page 262.

See “Working in the details pane” on page 692.

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 670.

See “About the details pane” on page 262.

See “Working in the details pane” on page 692.

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 670.

See “About the details pane” on page 262.

See “Working in the details pane” on page 692.

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 670.

See “About the details pane” on page 262.

See “Working in the details pane” on page 692.

Check details pane - Target Type tab

The Target Type tab of the check details pane shows a list of target types that are mapped to the selected check. The tab also displays the corresponding filter definition that is used for each target type.

See "Viewing check information in the details pane" on page 670.

See "About the details pane" on page 262.

See "Working in the details pane" on page 692.

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 669.

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.

If you copy a check under the same section, a copy of the check is created once. If you copy the same check again in the same section, the check overwrites the previously copied check. You can copy a check under the same section only once.

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 658.

See “Working with checks” on page 669.

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 658.

See “Working with checks” on page 669.

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 658.

See "Working with checks" on page 669.

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 Type 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 Typedrop-down list, select the target types that must be mapped to the check.

  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 197.
   - 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 685.

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 670.

See “Check details pane - Remediation tab” on page 679.

See “Check details pane - Issue tab” on page 679.

See “Check details pane - CVE tab” on page 679.

See “Check details pane - References tab” on page 673.

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 680.
  See “Specifying or editing the check attributes” on page 695.

- 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 693.

- 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 695.
  See “Specifying or editing the check issue ” on page 693.
  See “Editing reference information” on page 696.

- 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 checks that contain a “proc:”call in the precondition of the check algorithm.

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 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 2 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 **Validate Formula** to validate the check formula that you have created.
7. In the Expressions panel, enter the information in the same manner as in steps 1 to 5.
8. 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 669.

See "Creating a new check" on page 682.

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 178.

See “Changing an ESM policy name at the standard level” on page 669.

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 688.

See “ Creating a CCS ESM check by using the Advanced Check Builder option ” on page 690.

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 172.
   - Click **Quick Check Builder**.
3. Click **Next**.
4. In the **Create Expressions** panel, create a message expression by performing the following steps:

   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.

6. Update the CCS check formula so that the CCS check behaves as per the check execution rules.

   See “ Editing the check formula for a new CCS ESM check” on page 689.

7. Click **Next**.

8. In the **Review** panel, view the information that you have entered and then click **Finish**.

See “ Creating an ESM check ” on page 687.

See “ Creating a CCS ESM check by using the Advanced Check Builder option ” on page 690.

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.

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	Name of the message expressions that you have created, which corresponds to the messages that an ESM check generates. If the check generates multiple messages, you must specify the message expressions by using the logical AND operator. For example, E1 AND E2.
Error expression	Name of the error expression.

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 172.
- Click **Advanced Check Builder**.

3 In the **Create a Precondition** panel, enter the following details to narrow down the scope for targets that the check considers during evaluation. You

can add multiple pre-conditions for a check or you may choose to skip the **Create a Precondition** panel. The information that you provide in the **Create a Precondition** panel are optional.

- 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.
  Click the **Browse Fields** icon to view the description of each field.
- 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:

- From the **Category** drop-down list, select a category for the ESM entity. For example, select **ESM Message**.
- In the **Field** drop-down list, select a field for the ESM message entity that you want the check to report on. For example, select **Message String ID**.
- From the **Operator** drop-down list, select the operator. For example, select **!=**.
- From the Value text box, select a value for the specified value. 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.

6 Do the following to add an error expression to the check that you want to create. The error expression checks if an ESM agent reports any error message.

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 687.

See “ Editing the check formula for a new CCS ESM check” on page 689.

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 687.

See “ Creating a CCS ESM check by using the Quick Check Builder option” on page 688.

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 660.
  See “Renaming a check” on page 680.
- Enter or edit the description for a standard, section, or check.
  See “Specifying or editing the description ” on page 693.
- Add, edit, or delete the reference information for a standard, section, or check.
  See “Adding reference information” on page 696.
  See “Editing reference information” on page 696.

See “Deleting reference information” on page 697.

- Enter or edit the remediation information for a check.
  See “Specifying or editing the remediation information” on page 695.
- Enter or edit the issue information for a check.
  See “Specifying or editing the check issue ” on page 693.
- Add or edit the CVE information for a check.
  See “Adding the CVE information” on page 694.
  See “Editing the CVE information” on page 694.
- Enter or edit the risk attributes of a check
  See “Specifying or editing the check attributes” on page 695.

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 692.

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 692.

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 692.

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 692.

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 692.

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 191.

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 692.

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 692.

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 692.

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 692.

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 191.

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 700.
- Request exception on assets.
  See “Requesting an exception using the Evaluation Result Details dialog box” on page 701.

You can export the evaluation results either through the menu bar or the context menu.

Viewing the evidence details

You can view the evidence details for a check that has failed as well as the check that has passed, 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**.

See “Evaluation Results details pane - General tab” on page 1065.

See “Evaluation Results details pane - Evaluation Summary tab” on page 1065.

See “Evaluation Results details pane - Assets Evaluated tab” on page 1066.

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 700.

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 699.

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.

See “Working with Evaluation Results” on page 697.

See “Evaluation Results details pane - Assets Evaluated tab” on page 1066.

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.

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.

Risk score = (Total adjusted base score for all failed checks in the standard) / (Total number of failed checks)

See "Adjusted base score calculation" on page 703.

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.

Control Compliance Suite performs the following calculations in the scoring process:

- Base score calculations
  See "Base score calculation" on page 702.
- Adjusted base score calculations
  See "Adjusted base score calculation" on page 703.
- Average risk score calculations
  See "Average risk score calculation" on page 704.

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 191.

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(Impact) values in the base score formula are calculated from the check attributes as follows:

Impact = 10.41 * (1- (1-Confidentiality Impact) * (1-Integrity Impact) * (1-Availability Impact))

Exploitability = 20 * (Access Vector) * (Access Complexity) * (Authentication)

f(impact) = 0 if Impact = 0, f(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 702.

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:

Adjusted base score = round_to_1_decimal (((0.6*Adjusted Impact) + (0.4*Exploitability) – 1.5) * f (Adjusted Impact))

The Adjusted Impact, Exploitability, and the f(Adjusted Impact) values in the Adjusted base score formula are calculated as follows:

Adjusted Impact = min(10,10.41 * (1- (1- Confidentiality Impact * Confidentiality Required) * (1-Integrity Impact * Integrity Required) * (1- Availability Impact * Availability Required)))

Exploitability = 20 * Access Vector * Access Complexity * Authentication

f(Adjusted impact) = 0 if Adjusted Impact = 0, f(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 702.

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)

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 702.

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.

See "How to use the Standard Migration Utility" on page 706.

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.

See "About the Standard Migration Utility packaging and deployment" on page 706.

See "About the Standard Migration Utility" on page 704.

About the Standard Migration Utility packaging and deployment

The utility is present in the Symantec_Control_Compliance_Suite_Migration_Utility_10.0_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.

See “About the Standard Migration Utility system requirements” on page 705.

See “About the Standard Migration Utility” on page 704.

See “How to use the Standard Migration Utility” on page 706.

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.

See "About the Standard Migration Utility" on page 704.

See "About the Standard Migration Utility system requirements" on page 705.

See "About the Standard Migration Utility packaging and deployment" on page 706.

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.

See "About the Standard Migration Utility" on page 704.

See "How to use the Standard Migration Utility" on page 706.

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.

See "About the Standard Migration Utility" on page 704.

See "How to use the Standard Migration Utility" on page 706.

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.

See “About the command-line options” on page 707.

See "How to use the Standard Migration Utility" on page 706.

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

See "About the Standard Migration Utility" on page 704.

See "How to use the Standard Migration Utility" on page 706.

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'

See "About the Standard Migration Utility" on page 704.

See "How to use the Standard Migration Utility" on page 706.

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>
```

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 29-1 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

If an ESM policy contains both the application module checks and the operating system module checks, then the CCS standard for the policy is considered for the application module checks only.

About packaging and deployment

A Web package by the name Symantec_Control_Compliance_Suite_ESM_SU_41_Migration_Utility_10.5.1_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
Symantec™ ESM Policy to CCS Standard Migration Utility User Guide	Documentation

Additional information about the files

The additional information of the files is as follows:

security-content.xml	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. 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.
Symantec.CSM.Resources. ESMSUResources.dll	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.

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
- Microsoft Windows 7

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.

Note: Unlike the earlier versions of the migration utility that only required a policy xml as an input, the current version also requires a template folder containing the template files that are included in the ESM policy. The Policy tool when run with the export option for the specified ESM policy, creates the template folder under the parent folder that contains the policy xml.

`-m`

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.

See “About the message IDs in ESM Policy to CCS Standard Migration Utility” on page 725.

`-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`

This parameter is optional. If you specify this option, then the migration utility does not migrate the ESM suppressions to CCS Standard.

See “About ESM suppressions migration” on page 725.

-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 724.

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 29-2 lists the default category IDs for creating the formula

Table 29-2 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
Windows 2003	205336
Windows 2008	248336
Windows Vista	228336

OS Version	Message Numeric ID
Windows XP	200336
Windows 7	258336

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

If you specify the message expression type as 'Numeric' by using the -m switch for a policy that contains application modules, then the migration of all the application module checks is done by using the message expression as 'String'. The migration utility changes the message expression type to 'String' only for the application module checks. The database module checks are migrated by using the message expression type as 'Numeric'. If the ESM policy that you want to migrate contains application module checks, then the migration tool displays the following warning:

“TheESM policy contains at least one application module. The message expression type 'String' will be used to migrate the application module checks”.

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 CCS 10.5.1 Update, this Message Schema XML is generated from the security-content.xml of SU 2011.03.01 (SU 41).

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
  - Tru64

CCS 10.5.1 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 725.
- 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 29-3 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 CCS 10.5.1 Update console and go to the Standards UI. Go to **Manage > Standards**.

Table 29-3 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	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. 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 CCS 10.5.1 Update checks because the CCS 10.5.1 Update ESM Message entity schema only understands module long names. To resolve this issue, you need to use the utility with the latest Security Content XML and latest SU Resources assembly.

Table 29-3 Migration utility problems and their resolution *(continued)*

Problem	Resolution
Cannot locate the latest Security Content XML	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. You can find the update package for RDL in the following location on the ESM manager: <ESM Installation Folder>\update\ble\<Latest SU Version>\en\UpdatePackage.rdl Perform the following in the given order: ■ 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 CCS 10.5.1 Update console installation folder from where you intend to run the Symantec ESM Policy to CCS Standard Migration Utility. **Note:** If a new module is added in the latest SU update, you need the corresponding ESM data collector upgrade package.
Cannot locate the latest SU Resources Assembly	Copy the latest Symantec.CSM.Resources. ESMSUResources.dll from the <DPS installation Folder>\Data Collectors\ESM to the CCS 10.5.1 Update console installation folder form where you intend to run the Symantec ESM Policy to CCS Standard Migration Utility. If the Symantec.CSM.Resources.ESMSUResources.dll in the <DPS Installation Folder>\Data Collectors\ESM is also outdated, you need to update CCS content.

Table 29-3 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.	This warning message is displayed in case of the following: ■ 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.	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. To resolve this problem, use the updated Security Content XML and updated SU Resources Assembly.

Chapter 30

Managing SCAP benchmarks

This chapter includes the following topics:

Working with SCAP benchmarks

You can understand and perform the following tasks on SCAP benchmarks:

- About the SCAP Benchmarks view
  See "About the SCAP Content view" on page 734.
- About OVAL definitions view
  See "About the OVAL Definitions view" on page 740.
- About roles and permissions for SCAP benchmarks
  See "About roles and permissions for SCAP benchmarks" on page 741.
- About import of SCAP benchmarks into CCS
  See "About import of SCAP benchmarks into CCS" on page 743.
- Importing SCAP data stream into CCS
  See "Importing SCAP data stream into CCS" on page 744.
- Importing CCE list into CCS
  See "Importing CCE list into CCS" on page 744.
- Importing CVE-CVSS standards into CCS

See “Importing CVE-CVSS list into CCS” on page 745.

- Importing OVAL definitions
  See “Importing OVAL definitions” on page 746.
- Importing the workgroup computers to report on SCAP content
  See “Importing the workgroup computers to report on SCAP content” on page 747.
- Deleting the imported SCAP content
  See “Deleting the imported SCAP content” on page 748.
- Viewing the imported SCAP benchmarks in CCS
  See “Viewing the imported SCAP benchmarks in CCS” on page 748.
- Evaluating assets against the SCAP Benchmarks
  See “Evaluating assets against the SCAP benchmarks” on page 750.
- Evaluating assets against OVAL definitions
  See “Evaluating assets against OVAL definitions” on page 752.

About the SCAP Content view

The **SCAP Content** view lets you import and manage the SCAP content in the Control Compliance Suite. In CCS, the SCAP content are of two types, such as SCAP Benchmarks and OVAL Definitions. You can import, manage, and view these two content types through the specific console views.

The **SCAP Content** view is displayed when you select this content type from the drop-down list, **Content Type**.

The **SCAP Content** view contains the following:

- Taskbar menus
  Based on the content type that you select from the drop-down list, the appropriate menus are displayed on the taskbar.
- Table pane
  The table pane lists the content type, SCAP benchmarks, and their versions.
- Details pane
  The display pane provides details about the content type that you select in the table pane.
- Filter By pane
  The Filter By pane lets you filter the items listed in the table pane.

  You can use one of the following filters to filter the items in the list:

  - Generated Between

The Generated Between filter lets you specify a date range. The SCAP benchmarks that are generated between the specified date range are displayed in the table pane.

- Imported Between
  The Imported Between filter lets you specify a date range. The SCAP benchmarks that are imported between the specified date range are displayed in the table pane.

The taskbar menus for the **SCAP Content** content type and their descriptions are as follows:

Table 30-1 Taskbar view of SCAP Content content type

Taskbar Menu	Description
Run Evaluation	Lets you run the SCAP evaluation job for the selected profile of a benchmark.
Import Data stream	Lets you import the SCAP FDCC benchmarks into CCS.
Import CVE-CVSS	Lets you import the Common Vulnerability Enumeration (CVE) list and the Common Vulnerabilities Scoring System (CVSS) standard into CCS. You can import the CVE list and the CVSS standard along with the SCAP benchmarks. CCS lets you search and view the CVE IDs in the SCAP evaluation results.
Import CCE	Lets you import the Common Configuration Enumeration (CCE) list into CCS. You can import the CCE list along with the SCAP benchmarks. CCS lets you search and view the CCE IDs in the SCAP evaluation results.
Delete	Let you delete the SCAP benchmarks that are listed in the view.
Request Exception	Lets you request an exception for assets against specific rules of a profile. Request exception lets you manipulate the evaluation result values for the selected rules.

The table pane of the **SCAP Content** view enumerates the benchmarks across two columns such as, **Benchmarks** and **Version**. The **Benchmarks** column represents the name of the SCAP benchmark and the **Version** column displays the benchmark version. The profiles and rules of an SCAP benchmark are listed in a flat structure in the table pane.

The details of the SCAP benchmark, profiles, and the rules are displayed in the details pane of the view.

The details pane of the view displays the following:

- Details of the selected SCAP benchmarks
- Details of the selected SCAP benchmark profiles
- Details of the selected SCAP benchmark rules

See "About the OVAL Definitions view" on page 740.

About display of the SCAP benchmarks detail

The details pane of the **SCAP Benchmarks** view displays details about the benchmarks that you select.

The tabs that are displayed when you select an SCAP benchmark node are as follows:

Table 30-2 SCAP benchmark details

Tab	Description
General	Lets you view the following details of the SCAP benchmarks: ■ Benchmark ID Displays the ID of the benchmark that you select. ■ Title Displays the title of the XCCDF benchmark document. ■ Status Displays the status of the benchmark ■ Generated Date Displays the date the benchmark was generated. ■ Imported Date Displays the date when the benchmark is imported into CCS. ■ Version Displays the version of the benchmark. ■ Platforms Displays the target platform for the benchmark. A URI is displayed that refers to the platform that is listed in the CPE dictionary.

Table 30-2 SCAP benchmark details *(continued)*

Tab	Description
Description	Lets you view the description of the SCAP benchmarks.
Exceptions	Lets you view the exceptions for the selected SCAP benchmarks.

See "About display of the SCAP profile details" on page 737.

See "About display of the SCAP rules" on page 738.

About display of the SCAP profile details

The details pane of the **SCAP Benchmarks** view displays the details of a benchmark profile when you select.

The details of an SCAP benchmark's profile on selection displays the following tabs:

Table 30-3 SCAP profile details

Tab	Description
General	This tab displays the following details of the SCAP benchmark that you select: ■ Profile ID Displays the ID of the profile of the benchmark that you select. ■ Title Displays the title of the profile. ■ Platforms Displays the platform of the target computer on which the profile executes. ■ Extends Displays the ID of the profile on which the profile you select is based upon.
Description	Lets you view the description of the profile of an SCAP benchmark .

Table 30-3 SCAP profile details *(continued)*

Tab	Description
Evaluations	Lets you view the evaluation results of the assets that are evaluated against the selected profile. The **Evaluations** tab displays the following: ■ Evaluation Time ■ Evaluation Against ■ Compliance (%) ■ Risk Score

See "About display of the SCAP benchmarks detail" on page 736.

See "About display of the SCAP rules" on page 738.

About display of the SCAP rules

The details pane of the **SCAP Benchmarks** view displays the details of a rule when you select.

The details of a rule that you select for an SCAP benchmark profile, displays the following tabs in the details pane:

Table 30-4 SCAP rule details

Tab	Description
General	This tab displays the following details of the SCAP benchmark node that you select: ■ Rule ID Displays the rule identifier. For example, for a rule, Allow file and print sharing exception, the rule ID is, allow_file_print_sharing_exception_domain_profile ■ Title Displays the title of the rule. For example, for a rule, Allow file and print sharing exception, the title is same as the rule name. ■ Weight Displays the weight of the rule. ■ Rule path The location path of the rule. ■ Effective Weight Displays the weight that you specify for the rule. The specified weight overrides the actual weight of the rule and is known as the effective weight. The effective weight is the final weight that is applied to the rule in CCS. ■ Effective selection in evaluation Displays the values, True or False based on whether the rule is effective for evaluation or not. A value, True means that the rule is effective for evaluation while a value, False means that the rule is not effective. Even if a rule value is False and is not effective for evaluation, the rule is still reported in the evaluation results. The value set for such rule in the evaluation results is, Not Selected. In the table pane, the selected rule is highlighted and the non-selected rule is not highlighted.
Description	Lets you view the description of the rule of an SCAP benchmark profile.
Exceptions	Lets you view the exceptions for the selected rule.
Remediation	Lets you view the remediation details for the selected SCAP benchmark rules.

See "About display of the SCAP benchmarks detail" on page 736.

About the OVAL Definitions view

The **SCAP Content** view lets you import and manage the SCAP content in the Control Compliance Suite. In CCS, the SCAP content are of two types, such as SCAP Benchmarks and OVAL Definitions. You can import, manage, and view these two content types through the specific console views.

The **OVAL Definitions** view is displayed when you select this content type from the drop-down list, **Content Type**.

The **OVAL Definitions**view contains the following:

- Taskbar menus

  Based on the content type that you select from the drop-down list, the appropriate menus are displayed on the taskbar.
- Table pane

  The table pane lists the content type, OVAL definition files.
- Details pane

  The display pane provides details about the content type that you select in the table pane.

The taskbar menus for the **OVAL Definitions** content type and their descriptions are as follows:

Table 30-5 Taskbar view of OVAL Definitions content type

Taskbar Menu	Description
Run Evaluation	Lets you run the SCAP evaluation job for the selected profile of an OVAL definition.
Import CVE-CVSS	Lets you import the Common Vulnerability Enumeration (CVE) and Common Vulnerability Scoring Systems (CVSS) into CCS. You can import the CVE list and the CVSS standard along with the OVAL definitions. CCS lets you search and view the CVE IDs in the OVAL evaluation results.
Import CCE	Lets you import the Common Configuration Enumeration (CCE) standards into CCS. You can import the CCE list along with the OVAL definitions. CCS lets you search and view the CCE IDs in the OVAL evaluation results.

Table 30-5 Taskbar view of OVAL Definitions content type *(continued)*

Taskbar Menu	Description
Delete	Let you delete the OVAL definitions that are listed in the view.
Import OVAL Definitions	Lets you import the OVAL definitions into CCS.

In the table pane of the **OVAL Definitions** view, the OVAL definition files (XML) are listed. Select a file to read the details in the details pane of the view.

The table pane also displays the following columns for the **OVAL Definitions** view:

Column name	Description
Definition Files	Displays the OVAL definitions files that you import.
Product Name	Displays the name of the organization that introduced the OVAL definitions file. For example, NIST.
Version	Displays the OVAL definitions file version.
Generated Date	Displays the generation date of the OVAL definitions file.
Imported Date	Displays the date the OVAL definitions file was imported into CCS.
Variable File Name	Displays the variable file name that you import. You specify values for the external variables that are imported into CCS.

See “About the SCAP Content view” on page 734.

About roles and permissions for SCAP benchmarks

CCS defines specific roles and permissions to manage the SCAP benchmarks and OVAL definitions of the SCAP Content system. CCS defines the roles, which are associated with specific tasks that you can perform. When you are assigned a role, you can perform those tasks for which you have the required permissions. You can perform the tasks if you have permission on the **SCAP Benchmarks** business object folder in the **Settings > Permission Management** view of the console.

For the SCAP evaluation jobs, the roles that are defined can perform both the data collection and data evaluation tasks.

Note: The name of the roles that are defined for the SCAP Content system are same as that are defined for the CCS Standards system. The tasks that are associated with these roles for the SCAP Content system are specific to SCAP benchmarks.

The roles that are defined for the SCAP benchmarks and the corresponding tasks are as follows:

Table 30-6 SCAP benchmarks roles and their related tasks

Role	Description
Standards Administrator	The tasks that a user of this role can perform for SCAP Content system are as follows: ■ View standards This task lets you view the details of the SCAP benchmarks, profiles, and rules. ■ View evaluation results This task lets you view the evaluation results of the SCAP benchmarks and OVAL definitions. ■ Manage standards This task lets you create, update, and delete the SCAP benchmarks, profiles, and rules. ■ Evaluate standards This task lets you evaluate the assets against the SCAP benchmarks and the OVAL definitions.
Standards Evaluator	The tasks that a user of this role can perform for SCAP Content system are as follows: ■ View standards This task lets you view the details of the SCAP benchmarks, profiles, and rules. ■ View evaluation results This task lets you view the evaluation results of the SCAP benchmarks and OVAL definitions. ■ Manage standards This task lets you create, update, and delete the SCAP benchmarks, profiles, and rules. ■ Evaluate standards This task lets you evaluate the assets against the SCAP benchmarks and the OVAL definitions.

About import of SCAP benchmarks into CCS

CCS lets you import the SCAP-expressed data streams through the **SCAP Benchmarks** view of the console. The data streams are specific to the Federal Desktop Core Configuration (FDCC) standards, which are used to assess and report on the system configurations of computers. The assets are evaluated against the imported SCAP-expressed data streams, which you must download from the following Web site:

http://web.nvd.nist.gov/view/ncp/repository

CCS validates the SCAP-expressed data streams during import to verify if the content is specific to the Windows operating system. Appropriate error messages are displayed if you import invalid benchmarks that CCS does not support. A benchmark ID and version represent every SCAP-expressed data stream that you import. The benchmark ID and version are displayed in the **SCAP Benchmarks** view of the console.

CCS supports the following content:

- FDCC Windows XP
- FDCC Windows Vista
- FDCC Windows XP Firewall
- FDCC Windows Vista Firewall
- FDCC IE 7
- OVAL 5.3

If the data stream already exists in CCS, then you are prompted to overwrite the existing data stream. If the existing data stream is already evaluated then the overwrite operation does not affect the evaluation results. The SCAP evaluation job evaluates against the new data stream in the subsequent job runs.

Beside the FDCC content, CCS supports import and evaluation of the SCAP 1.0 - expressed data stream and OVAL 5.3 definitions.

See “About the supported OVAL objects in CCS” on page 209.

The SCAP-expressed data stream adheres to various specifications that CCS supports. You must import these specifications into CCS that are implicitly applied to the imported SCAP-expressed data stream.

The specifications that you must import into CCS are as follows:

- Open Vulnerability and Assessment Language (OVAL - 5.3)
- Common Platform Enumeration (CPE - 2.2)
- Common Configuration Enumeration (CCE - 5.0)

- Common Vulnerabilities and Exposures (CVE)
- Common Vulnerability Scoring System (CVSS - 2.0)

See "Importing SCAP data stream into CCS" on page 744.

See "Importing CCE list into CCS" on page 744.

See "Importing CVE-CVSS list into CCS" on page 745.

Importing SCAP data stream into CCS

You import the SCAP- expressed benchmarks or data stream through the **SCAP Benchmarks** view of the console. The SCAP data stream must be downloaded from the Web site, http://web.nvd.nist.gov/view/ncp/repository before you import them into CCS. In the Web site, ensure that you select the link, SCAP Content - OVAL 5.3 to download. The downloaded data stream is a set of XML files that are usually stored in a compressed format. However, CCS does not support import of data stream in a zipped format.

See "About import of SCAP benchmarks into CCS" on page 743.

Note: The import of SCAP data stream fails if any rule of the benchmark contains complex checks. For example, if an XCCDF rule contains the element, <xccdf:complex-check>, then you cannot import the benchmark into the SCAP Content system.

To import the SCAP data stream

1. Go to the **Manage > Standards > SCAP Content** view of the console.
2. In the view, for the **Content Type** drop-down list, select **SCAP Benchmarks**.
3. In the taskbar, click **Import Data stream**.
4. In the **Import Data stream** dialog box, click **Browse**.
5. In the **Browse for folder** dialog box, navigate to the directory where the SCAP data stream is located and click **OK**.

   Import the SCAP data stream into CCS.

See "Importing CCE list into CCS" on page 744.

See "Importing CVE-CVSS list into CCS" on page 745.

Importing CCE list into CCS

You import the Common Configuration Enumeration (CCE) list through the **SCAP Content** view of the console. Although, the CCE identifiers (ID) are contained in the SCAP data stream when imported, the CCE ID descriptions are not contained in the data stream. You must download and import the CCE list independently into CCS. You can download the CCE list from the Web site, http://cce.mitre.org/lists/cce_list.html

An independent import of the CCE list lets you import the corresponding descriptions of the CCE IDs. The CCE IDs and their descriptions are displayed for the SCAP or OVAL evaluation job results in the **Monitor > Evaluation Results** view of the console.

Note: During import, ensure that the size of the file that contains the CCE list does not exceed 2 GB.

To import the CCE list

1. Go to the **Manage > Standards > SCAP Content** view of the console.
2. In the **Content Type** drop-down list, select either of the following content types:
   - **SCAP Benchmarks**
   - **OVAL Definitions**
3. In the taskbar, click **Import CCE**.
4. In the **Import CCE** dialog box, for the **Select CCE data file to import** option, click **Browse**.

   Navigate to the folder where the CCE list file is located on the computer to import.
5. In the **Select CCE File** dialog box, select the CCE list file and click **OK**.

   Import the CCE list into CCS.

See “Evaluating assets against the SCAP benchmarks” on page 750.

See “Importing SCAP data stream into CCS” on page 744.

See “Importing CVE-CVSS list into CCS” on page 745.

Importing CVE-CVSS list into CCS

You import the Common Vulnerability and Exposures (CVE) list and Common Vulnerability Scoring System (CVSS) standard through the **SCAP Content** view of the console. The CVE identifiers (ID) represent the software flaws that are defined by the CVE dictionary. The CVSS are used for the risk score calculation of the assets that are evaluated against the SCAP benchmarks or the OVAL definitions.

The SCAP benchmarks or the OVAL definitions that you import does not contain the CVSS base score attributes. You must download and import the CVE-CVSS list into CCS independently. You can download the CVE-CVSS list from the Web site, http://nvd.nist.gov/download.cfm#CVE_FEED.

The CVE IDs are displayed for the evaluation results of the SCAP or OVAL evaluation job results. The results are displayed in the **Monitor > Evaluation Results** view of the console.

Note: During import, ensure that the size of the file that contains the CVE list does not exceed 2 GB.

To import the CVE-CVSS list

1. Go to the **Manage > Standards > SCAP Content** view of the console.
2. In the **Content Type** drop-down list, select either of the following content types:
   - **SCAP Benchmarks**
   - **OVAL Definitions**
3. In the taskbar, click **Import CVE-CVSS**.
4. In the **Import CVE-CVSS** dialog box, for the **Select CVE-CVSS data file to import** option, click **Browse**.

   Navigate to the directory where the CVE-CVSS file is located on the computer to import.
5. In the **Select CVE File** dialog box, select the CVE-CVSS file and click **OK**.

   Import the CVE-CVSS list into CCS.

See "Evaluating assets against the SCAP benchmarks" on page 750.

See "Importing CCE list into CCS" on page 744.

See "Importing SCAP data stream into CCS" on page 744.

Importing OVAL definitions

You import the standalone OVAL definitions into CCS through the **SCAP Content** view of the CCS console.

To import the OVAL definitions

1. Go to the **Manage > Standards > SCAP Content** view of the console.
2. In the **Content Type** drop-down list, select **OVAL Definitions**.
3. In the taskbar, click **Import OVAL Definitions**.
4. In the **Import OVAL Definitions** dialog box, click **Browse** for the **Select OVAL file to import** text field.
5. In the **Select OVAL file** dialog box, select the OVAL definition file and click **OK**.
6. In the same **Import OVAL Definitions** dialog box, click **Browse** for the **Select external variables file to import** text field.
7. In the **Select external variables file** dialog box, select the OVAL external variable file and click **OK**.

See “Importing CCE list into CCS” on page 744.

See “Importing CVE-CVSS list into CCS” on page 745.

Importing the workgroup computers to report on SCAP content

The Control Compliance Suite Data Collection application lets you report on the Windows workgroup computers for the SCAP content. For successful reporting on SCAP content from the workgroup computers, install a bv-Control for Windows Query Engine (QE). You must install a single QE to collect data from all the workgroup computers on which bv-Control for Windows is installed. You use the pass through authentication to query the workgroup computers.

You must refer to the Symantec bv-Control for Windows Online help, NTProductHelp.chm, to perform the configuration for the workgroup computers.

The workgroup computers that are installed with bv-Control for Windows snap-in are resolved by Control Compliance Suite Reporting and Analytics application through asset import method.

To import the workgroup computers into CCS, use either the CSV data collector or the ODBC data collector.

To import workgroup computers into CCS

1. Create a CSV file or an ODBC database table containing all details for asset import.

   Ensure you do the following in the CSV file or the ODBC database table to import the workgroup computers:

- Specify the workgroup names for the fields, Machine.DomainWorkgroupName and Common.WntMachine.DomainWorkgroupName.
- If the workgroup of the computer you import is different from the workgroup of the QE, specify the QE workgroup name for the field, DomainWorkgroupName.
- Specify the values for the fields, Wnt.Machine.HostMachineInDomain and Common.WntMachine.HostMachineInDomain as false.

2 Configure the CSV data collector or the ODBC data collector and perform asset import of the workgroup computers.

Deleting the imported SCAP content

Delete the SCAP benchmarks and the OVAL definitions that you import into CCS through the **SCAP Benchmarks** view or the **OVAL Definitions** view. All the data that are related to the imported SCAP content are deleted from the database by the purge system job. The purge job deletes the stale data from the CCS databases.

Any evaluation results that are generated for the deleted SCAP content are not removed from the database.

To delete an SCAP benchmark or an OVAL definition

1 Go to the **Manage > Standards > SCAP Content** view of the console.

2 In the **Content Type** drop-down list, select either of the following content types:

- **SCAP Benchmarks**
- **OVAL Definitions**

3 In the display pane of the view, select the SCAP content type that you want to delete and click **Delete.**

4 In the **Delete** dialog box, review the number of content that you want to delete and click **Yes**.

See “About SCAP content in CCS” on page 203.

See “About import of SCAP benchmarks into CCS” on page 743.

Viewing the imported SCAP benchmarks in CCS

After you import the SCAP data stream into CCS, the details of the benchmark, profiles, and rules are displayed in the **SCAP Benchmarks** view. A flat list of rules is displayed for a profile of an SCAP benchmark. CCS does not display any abstract rules and rules that are extended from other rules. The **SCAP Benchmarks** view also let you review the rules that are effectively selected for evaluation. The details of a benchmark, profile, or rule are displayed at the bottom pane of the view.

To view the imported SCAP data stream

1. Go to the **Manage > Standards > SCAP Benchmarks** view of the console.
2. From the list of SCAP benchmark, select an SCAP benchmark, a profile, or a rule as per your requirement
3. In the bottom pane, view the details of the selected benchmark, profile, or rule.

See “About display of the SCAP profile details” on page 737.

See “About display of the SCAP rules” on page 738.

Configuring assets for data collection and evaluation against SCAP content

For successful data collection and evaluation of the FDCC-compliant assets against the SCAP content, you must perform few configuration settings for the assets. For both Windows XP and Windows Vista target computers, you must configure the firewalls for communicating using the standard remote administration ports and programs.

To configure Windows XP and Windows Vista domain connected target computers

1. In the Windows XP or Windows Vista computers, navigate to the **Windows Group Policy** dialog box.
2. Under Local Computer Policy, navigate to **Computer Configuration > Administrative Templates > Network > Network Connections > Windows Firewall** and do the following:
   - Disable the setting, **Windows Firewall: Do not allow exceptions**
   - Enable the setting, **Windows Firewall: Allow remote administration exception**
     For more security, you can define the setting with the IP address or addresses of the bv-Control for Windows Query Engines (QE). The QE is configured to collect data from the assets or the target computers.

To configure Windows XP and Windows Vista workgroup target computers

1. In the Windows XP or Windows Vista computers, navigate to the **Local Security Settings** dialog box.
2. Under Security Settings, navigate to **Local Policies > Security Options** and do the following:
   - For the setting, **Network security: LAN Manager authentication level**, change the setting from, **Send NTLMv2 Response Only\Refuse LM & NTLM** to **Send NTLMv2 Response Only\Refuse LM**.

     This setting lets NTLM authentication happen outside a domain. By default, the Windows Vista computers that reside outside a domain cannot be remotely administered because of the User Account Control (UAC) remote restrictions. You must create a registry of DWORD value, **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy** that has a value, 1.

     For more information on this setting, refer to http://support.microsoft.com/kb/951016 and http://support.microsoft.com/kb/942817

Evaluating assets against the SCAP benchmarks

In CCS, you create the SCAP evaluation job to evaluate the assets against the SCAP benchmarks by selecting a profile. Before you evaluate, you must import the SCAP benchmarks into CCS.

See "Importing SCAP data stream into CCS" on page 744.

After the SCAP evaluation job is executed, the evaluation results are displayed in the **Monitor > Evaluation Results** view of the console.

Note: Scope an SCAP evaluation job to the asset group or container that contains 500 assets. Create multiple jobs with this scope to span across more than 500 assets.

To evaluate the assets against the SCAP Benchmarks

1. Go to **Manage > Standards > SCAP Content** view of the console.
2. In the view, from the **Content Type** drop-down list, select **SCAP Benchmarks**.
3. In the **SCAP Benchmarks** view, select the profile of the benchmark against which you want to evaluate the asset.
4. Right-click on the profile and select **Run Evaluation**.

5 In the **Specify Job Name and Description** panel of the **Create or Edit SCAP Evaluation Job** wizard, specify the SCAP evaluation job name and the description and click **Next**.

6 In the **Select Targets** panel of the wizard, select the assets that you want to evaluate against the SCAP Benchmarks and then click **Next**.

7 In the **Schedule Job** panel of the wizard, assign a schedule for the SCAP evaluation job and then click **Next**.

8 In the **Add Results Viewers** panel of the wizard, add the user names who can view the evaluation results of the SCAP evaluation job that you execute.

9 In the **Specify Notification Details** panel of the wizard, specify the notification details to alert when the SCAP evaluation job succeeds or fails and then click **Next**.

10 In the **Summary** panel of the wizard, review the summary details of the SCAP evaluation job and then click **Finish**.

About mapping SCAP rules for policy panels

The SCAP rules can be mapped with policies or mandates by using control statements from the Controls Studio workspace of CCS.

On a successful execution of the SCAP evaluation job, you can view the data in the predefined panels of the Dynamic Dashboards workspace.

You can view the SCAP rule results in policy panels according to the SCAP-PM mappings that are given in the following table:

Table 30-7 Mapping SCAP rules for policy panels

SCAP rule results	Results in the corresponding policy panels
Pass	Pass
Fail	Fail
Error	Error
Unknown	Unknown
Not Applicable	Not Applicable
Fixed	Pass

Table 30-7 Mapping SCAP rules for policy panels *(continued)*

SCAP rule results	Results in the corresponding policy panels
Not Checked	Not Applicable
Not Selected	Not Applicable
Informational	Not Applicable

Evaluating assets against OVAL definitions

In CCS, you create the SCAP OVAL evaluation job to evaluate the assets against the OVAL definitions. The OVAL definitions are imported into CCS before you evaluate the assets against them.

See "Importing OVAL definitions" on page 746.

After the SCAP OVAL evaluation job is executed, the evaluation results are displayed in the **Monitor > Evaluation Results** view of the console.

To evaluate the assets against the OVAL definitions

1. Go to **Manage > Standards > SCAP Content** view of the console.
2. In the view, from the **Content Type** drop-down list, select **OVAL Definitions**.
3. In the **OVAL Definitions** view, select the OVAL file against which you want to evaluate the asset.
4. Right-click on the file and select **Run Evaluation**.
5. In the **Specify Job Name and Description** panel of the **Create or Edit SCAP Evaluation Job** wizard, specify the SCAP OVAL evaluation job name and the description and click **Next**.
6. In the **Select Targets** panel of the wizard, select the assets that you want to evaluate against the OVAL definitions and then click **Next**.
7. In the **Schedule Job** panel of the wizard, assign a schedule for the SCAP OVAL evaluation job and then click **Next**.
8. In the **Add Results Viewers** panel, add the users who can view the evaluation results of the SCAP OVAL evaluation job that you execute.
9. In the **Specify Notification Details** panel, specify the notification details to alert whether the SCAP OVAL evaluation job succeeds or fails and click **Next**.

10 In the **Summary** panel of the wizard, review the summary details of the SCAP OVAL evaluation job and then click **Finish**.

About risk and compliance score calculation for SCAP assets

CCS uses the evaluation results of the assets against the SCAP benchmarks to calculate the compliance score and risk score for the assets. The compliance score of the assets determine the compliance adherence level of the assets with the SCAP benchmarks. The risk score of the assets determine the vulnerability or risk of those assets that have failed in the evaluations against the SCAP benchmarks.

The National Institute of Standards and Technology (NIST) defines the XCCDF's compliance scoring model that CCS implements. As per the recommendation from XCCDF, CCS uses the Default scoring model to calculate the weighted compliance scores of the assets.

See “About compliance score calculation for SCAP assets” on page 753.

CCS uses the Common Vulnerability Scoring System (CVSS) base scores to calculate the risk scores of the assets. The CVSS base scores let you prioritize the remediation of the known security-related software flaws in the assets. Whenever a new vulnerability is announced, a new CVE ID is created for the vulnerability. The software applications that are affected due to the vulnerability are identified using the CPE values. The CVSS base measures and scores are computed and added to the National Vulnerability Database (NVD).

See “About risk score calculation for SCAP assets” on page 756.

About compliance score calculation for SCAP assets

CCS uses the XCCDF's Default scoring model to calculate the weighted compliance scores for the profiles that are evaluated against the assets. The Default scoring model that is supported in XCCDF 1.0 lets you calculate the weighted compliance scores for every benchmark profile. The Default scoring model is indicated implicitly for all the SCAP benchmarks. Weights are assigned to every rule of a profile that are used for calculating the weighted compliance score. If a specific rule is not selected, then the weight of that rule is not considered for the compliance score calculation of the profile. Ensure that you provide weights appropriately to the rules for correct computation of the weighted compliance score using the Default scoring model.

CCS defines the following attributes to calculate the compliance scores of the rules:

- Count

  This attribute is set to either 1 or 0 based on the evaluation result values. The value 1 is set for the result value, Pass, Fail, Error, and Unknown. The value 0 is set for the result values, NotApplicable, NotChecked, NotSelected, Informational, and Fixed.

  The evaluation result values of the SCAP benchmark rules and their contribution to the compliance score calculation are as follows:

  - Pass

    This means that the asset has satisfied all the conditions of the rule. A pass result contributes to the weighted score and maximum possible compliance score.

  - Fail

    This means that the asset did not satisfy all the conditions of the rule. A fail result contributes to the maximum possible compliance score.

  - Error

    This means that the CCS has encountered a system error and is not able to complete the evaluation. Hence, the status of the asset's compliance with the rule is uncertain. For example, if CCS runs with insufficient privileges on the asset, then an error can occur.

  - Unknown

    This means that CCS has encountered some problem and the result is unknown. For example, if CCS was unable to interpret the output of the evaluation.

  - Not Applicable

    This means that the rule is not applicable for the asset that is evaluated. For example, if a rule is specific to an operating system version to which the asset does not belong, then the evaluation result is not applicable. Such kind of evaluation result values do not contribute to the compliance score.

  - Not Checked

    This means that the rule is not evaluated by CCS. Such a result value is designed for the rules that have a role as, unchecked and for the rules that have no properties. Such type of evaluation result values do not contribute to the benchmark compliance score.

  - Not Selected

    This means that the rule is not selected in the benchmark. Such type of evaluation result values do not contribute to the benchmark compliance score.

  - Informational

This means that the rule's result value is simple information that an auditor or administrator uses. Such result is the default value for rules that have a role as, unscored. This result value is designed for rules that can extract information from the asset. This kind of evaluation result values do not contribute to the benchmark compliance score.

  - Fixed

    This means that the rule has failed, but is fixed. Such kind of evaluation result values must contribute to the compliance score similar to the result value, pass.

- Score

  This attribute is set to 100 or 0 based on the evaluation result values. For all the result values whose count is 1, the score is set. No score is set for the result values whose count is 0.

- Accumulator

  This attribute value is the sum total of weights of the rules.

CCS calculates the compliance score for the rules based on the weights that you assign to the rules. CCS also lets you compute the scores for the group to which the rule belongs.

The formula that CCS uses to calculate the compliance score for a rule and group against which an asset is evaluated is as follows

- Rule

  compliance score of a rule = (score of a rule) * (weight of the rule)

- Group

  The normalized score of a group = (Sum of the scores of the rules or groups under the group) / (sum of the weights of the rule or groups under the group)

  Compliance score of a group = (Normalized score)* (Weight of the group)

Note: Even when the data is not available for an asset, the CCS still considers the compliance score(that is zero) for the non-available asset. This is so that the user is informed of the probable risk that might be involved due to the unavailability of the asset.

The formula that CCS uses to calculate the weighted compliance score of a profile is as follows:

- Weighted compliance score of a profile for a single asset

  Weighted compliance score of a profile = (compliance score of the rules) / (sum of weights of the rules)

- Weighted compliance score of a profile for multiple assets

Weighted compliance score of the profile = (sum total of the compliance scores of the profiles evaluated against every asset) / (total number of assets)

- Weighted compliance score of a profile using weights of the group in which the rule exists

  Weighted compliance score of the profile = (Sum of the scores of the rules or groups under the profile) / (sum of the weights of the rule or groups under the profile)

Note: If no weight attribute is set for a rule or group, then the weight is considered as 1. No weight is assigned to a profile.

For example, you calculate the compliance scores (CS) of every asset, A1, A1, A3 against which you evaluate the profile P1. The weighted compliance score that you derive for the assets is as follows:

CS(P1A1)+CS(P1A2)+CS(P1A3)/3

See "About risk score calculation for SCAP assets" on page 756.

See "About adjusted base score calculation for SCAP assets" on page 757.

About risk score calculation for SCAP assets

CCS uses the scoring guidelines published by Common Vulnerability Scoring System (CVSS 2.0) to calculate the risk scores for the assets that failed when evaluated against the SCAP-expressed data stream. You must ensure that you import the CVSS values for the corresponding CVE IDs to calculate the risk scores for the assets.

As per the recommendation of NIST, CCS must use the CVSS base scores to prioritize the remediation of known security-related software flaws. When a new vulnerability is publicly announced, a new CVE ID is created and the CVSS base scores are computed for the vulnerability. The CVSS base scores are then added to the National Vulnerability Database (NVD).

CCS uses the base metrics model of CVSS to calculate the risk scores for the assets.

A rule that represents a software flaw has references to the CVE IDs. As a single rule can point to multiple CVE IDs, the base score of all such CVE IDs are picked up from the CVSS. The Confidentiality (C), Integrity (I) and Availability (A) values of the CVSS entry with the highest base score are used to calculate the adjusted risk score for the assets.

CCS lets you calculate the adjusted base score for a pair of rule and an asset.

See "About adjusted base score calculation for SCAP assets" on page 757.

You can also derive the composite risk score for a single or multiple assets that are evaluated against an SCAP benchmark.

See "About the composite risk score calculation for SCAP assets" on page 758.

See "About compliance score calculation for SCAP assets" on page 753.

About adjusted base score calculation for SCAP assets

The adjusted base score is calculated for a pair of rule and asset. The score is calculated using the 6 risk attributes of a rule and 3 attributes of an asset.

The adjusted base score calculation depends on the following 6 attributes of a rule:

- Confidentiality
- Integrity
- Availability
- Access Vector
- Access Complexity
- Authentication

The 3 attributes of an asset are as follows:

- Confidentiality
- Integrity
- Availability

Note: Ensure that all the 6 values of the rule are defined. If any of the value is Not Defined then the risk score is Not Applicable. It is not compulsory to define the 3 values of the asset because even if not defined then the default value that is considered for the risk score calculation is, Medium.

The following metrics maps to the CVSS values and their respective weightage:

AccessVectorWeightage = { Undefined = -1.0, Local Access = 0.395, Adjacent network accessible = 0.646, Network accessible = 1.0 };

AccessComplexityWeightage = { Undefined = -1.0, Low = 0.71, Medium = 0.61, High = 0.35 };

AuthenticationWeightage = {Undefined = -1.0, Multiple Instance = 0.45, Single Instance = 0.56, No authentication = 0.704 };

CheckCIAWeightage = { undefined = -1.0,none = 0.0, partial = 0.275, complete = 0.660 }

AssetCIAWeightage = { Not Defined = 1.0, Low = 0.5, Medium = 1.0, High = 1.51 }

The following formulae are used to calculate the exploitability, adjusted impact, and fimpact:

Exploitability = 20 * ruleAccessVector * ruleAccessComplexity * ruleAuthentication;

AdjustedImpact = Min(10, 10.41 * (1 - (1 - ruleConfidentiality * assetConfidentiality) * (1 – ruleIntegrity * assetIntegrity) * (1 - ruleAvailability * assetAvailability)));

fImpact = (AdjustedImpact == 0) ? 0 : 1.176;

The following formula is used to calculate the adjusted base score for the rule and asset:

adjustedBase = (((0.6 * AdjustedImpact) + (0.4 * Exploitability) - 1.5) * fImpact);

See “About risk score calculation for SCAP assets” on page 756.

About the composite risk score calculation for SCAP assets

The composite risk score is calculated for one or more assets against the SCAP benchmarks.

The composite risk scores for a single asset against a single benchmark is calculated in the following manner:

- All rules that have failed for an asset. In such case, all the rules have risk scores ranging from 0-10. You can ignore the rules whose result value is Not Applicable.
- All rules that have passed but have the risk scores ranging from 0-10.

  These rules have passed because they are exempted.
- Calculate average of the risk scores for all the rules.

  Note: Exclude the risk score that has the result value as Not Applicable for the failed rules

The composite risk scores for multiple assets against a single benchmark is calculated in the following manner:

- Calculate the risk score of the benchmark for every single asset.
- Take average of the risk scores.

If there are multiple runs of a benchmark against an asset then consider the latest run

Generating reports of the SCAP evaluated results

You use the predefined report template, **Asset Details** to generate reports of the SCAP evaluated results. The report template reports the evaluated results for those assets that are already evaluated against the SCAP benchmarks. You select the assets when scheduling the report template, for which you want to view the details report. The report template details about the SCAP rules and exceptions information for the selected assets.

To generate report for the SCAP evaluated results

1. Go to **Reporting > Report Templates** view of the console.
2. In the **Report Templates** view, select the **Asset Details** report and right-click to select **Schedule Report**.

   Review the scheduled report generation job in the **Monitor > Jobs** view to ensure that the job runs successfully.
3. Go to the **Reporting > My Reports** view of the console.
4. In the **My Reports** view, select the generated **Asset Details** report, right-click and select **View**.

See “Accessing dashboards of SCAP benchmarks” on page 759.

Accessing dashboards of SCAP benchmarks

CCS lets you access the predefined dashboard, **Compliance Administration - SCAP profile benchmark**, which renders the evaluation results of an SCAP evaluation job that you execute. For the SCAP content system, the predefined dashboard is specific only for the **SCAP Benchmarks** content type. The predefined dashboard contains panels that you access for the SCAP benchmark.

The predefined panels of the **Compliance Administration - SCAP profile benchmark** dashboard are as follows:

- Compliance score for SCAP profile (Benchmark)
- Rule status by assets for SCAP profile (Benchmark)
- Top 10 Risk Score by assets for SCAP profile (Benchmark)

CCS also lets you access the panel, Top 10 Risk Score by assets for SCAP profile (Benchmark) through the the existing predefined dashboard, **Compliance Administration - Assets**.

To access a dashboard for an SCAP benchmark

1. Launch the CCS Web Console using the following URL:

   http://<machine name or FQDN name of Application Server>/CCS_Web

2. In the Web Console, in the menu bar, click **Dashboards**.
3. In the Dashboards view, select the **Compliance Administration - SCAP Benchmark** dashboard.

See "Generating reports of the SCAP evaluated results" on page 759.

Chapter 31

Managing external data systems

This chapter includes the following topics:

Configuring data systems

You must add an external data system to CCS before you can import data into CCS. You can add an external system as the data provider. You must then configure any one of the following data connections, based on the external data format, to import the data:

- ODBC data connection
  See "Importing data using an ODBC connector" on page 774.
- CSV data connection
  See "Importing data using a CSV connector" on page 779.
- Web service connection
  See "Importing data using a Web Services connector" on page 785.

Permissions required for External Data Integration

You must have the following permissions to perform external data integration:

Table 31-1 Permissions for CCS

Tasks	Permissions required
Configuring data systems and data connections.	■ Manage External Data Integration ■ Manage Jobs ■ Manage Configuration Settings
Asset Correlation	■ Manage Asset Reconciliation Rules ■ Manage Assets and Asset Groups ■ Import Assets
Policy compliance	■ Manage Content Studio
Viewing and creating dashboards	■ Create Dynamic Dashboards ■ Manage Dynamic Dashboards ■ Publish Dynamic Dashboards

Note: You do not require any asset specific permissions to view asset specific dashboards and panels. While viewing dashboards all external system data related to assets is visible.

Table 31-2 Permissions for external data connections

Tasks	Permissions required
ODBC	■ Read access to the database table or database view
CSV	■ Read permission on the network share where the CSV file is located
Web Service	■ Appropriate permission based on the binding type used for Web Service. For example, Basic HTTP, WSHTTP, or Basic HTTP(SSL).

Adding an external data system

You must add an external data system to CCS before you can import data into CCS. Use the **Add Data System** wizard to add a new data system.

To add an external data system

1. Go to **Manage > External Data Integration**.
2. On the taskbar, click **Add External Data System**.
3. In the **Specify the External Data System** panel, do the following and then click **Next**:

   System name

   Enter a name for the external data system that you want to add.

   Description

   Add a brief description on the external data system.

   This step is optional.

4. In the **Specify Data Connection Parameters** panel, do the following and then click **Next**:

   Connection name

   Enter the name of the external data connection that you want to create.

   Connection type

   Select the type of data connection you want to create.

   The options available in the **Connection Information** section depend on the selection that you make in the **Connection type** drop-down list.

   For ODBC, See "Importing data using an ODBC connector" on page 774.

   For CSV, See "Importing data using a CSV connector" on page 779.

   For Web Service, See "Importing data using a Web Services connector" on page 785.

5. In the **Select Data Fields** panel, select the data fields that you want to include when you import the external data and then click **Next**.

   You must select minimum two fields to import data.

6. In the **Select Data Schema** panel, select one of the following options and then click **Next**:

Create new schema

Schema is a representation of external data in CCS.

Enter the following information:

- In the **Schema name** text box, enter a name for the new schema that you want to create.
- In the **Description** field, enter a brief description of the new schema.

If you click **Create new schema**, then go to 8.

Existing schema

From the **Select CCS schema** drop-down list select the matching CCS schema to the external data.

If you click **Existing schema**, then go to 7.

7 The **Map Data Fields to CCS Schema Fields** panel displays the data fields that you specified in the **Select Data Fields** panel.

Do the following and then click **Next**:

- Drag the data fields from the **Field Name** column in the left-hand box to the **Mapped Field Name** column against the corresponding CCS field in the right-hand box. To identify unique fields in the external data, you must map the external data fields with key fields in the schema. The **Is a Key Field** column in the existing schema displays the key fields in the schema. If all the external data fields are mapped to CCS schema, go to 12.
- Check **Extend CCS Schema to import unmapped fields** if you want to extend the selected CCS schema to import the fields that are unmapped, and click **Next**.

8 The **Associate imported data with CCS** panel displays the data fields that you specified in the **Select Data Fields** panel or the fields that were unmapped in the **Map Data Fields to CCS Schema Fields** panel.

Enter the following information in the **CCS fields** list box and then click **Next**:

CCS Field

Displays the fields that you selected in the **Select Data Fields** panel.

Click the CCS field name to edit the name.

CCS data type

Select the data type from the drop-down list.

For Incremental Data Import select the data type of one of the fields as DateTime.

This field is used for incremental data collection as evaluation date time field. In incremental data import, the records only beyond the maximum date in the evaluation date time field, are fetched in subsequent imports.

Description

Add some description text for the field.

Attribute of

Select the CCS attribute to which you want to map the specified external data field. For example, Asset, Assessment, or Status.

Is a key field

Check to specify if the selected field is a key field. Key field is a mandatory field in CCS schema.

You must specify minimum one field as a key field for asset and assessment.

9 Perform this step only if you have selected a data type as DateTime, in 8

In the **Format and Date Time** panel, provide the following information and then click **Next**:

Evaluation date field

This field is used for incremental data collection. In incremental data import, the records only beyond the maximum date in the evaluation date time field, are fetched in subsequent imports.

Select the evaluate date field from the **Evaluation date field** drop-down list.

Date-time format

Specify the date time format that you want to apply for all DateTime fields in the schema.

To specify the date time format for a particular field, select the date time format in Date Time Format column for that field, in the schema.

Check **Apply to all fields** if you want your selection to be applied to all the DateTime data fields.

Refer to the Date-time formats supported in Control Compliance Suite section to view the datetime formats supported while importing external data.

See "Date-time formats supported in Control Compliance Suite" on page 799.

Time zone

Select the time zone.

To specify the time zone for a particular field, select the time zone in Time Zone column for that field, in the schema.

Check **Apply to all fields** if you want your selection to be applied to all the Time Zone data fields.

10 In the **Data Import Schedule** panel, select one of the following schedule options and then click **Next**:

- **Run now**
  Select this option to run the job immediately after you click **Finish**.

- **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 execute the data import.
Run once	Select this option to execute the data import one time on the specified date and time.
Run every <number of days>	Select this option to specify how often (in days) you want to schedule the data import execution.

11 In the **Email Notification** panel, check **Send Notification** if you want to send a notification upon the success or failure of the data import execution. Both the tabs in the **Email Notification** panel contain the same options. Enter the following information and then click **Next**:

Subject	Enter the subject of the notification mail.
Message	Enter the message of the notification mail.
From (Email ID)	Enter the sender's email ID.
To (Email IDs)	Enter the receiver's email ID. Notification can be sent to multiple recipients. Separate each email ID with a comma.

12 In the **Summary** panel, view the summary and then click **Finish**.

See “Editing an external data system” on page 767.

See “Deleting an external data system” on page 768.

See “Exporting an external data system ” on page 769.

See “Importing an external data system ” on page 769.

See “Viewing external system information in the details pane” on page 770.

Editing an external data system

You can modify an existing external data system from the **Manage > External Data Integration** view.

Note:

You cannot edit a pre-integrated external data system.

To edit an external data system

1. Go to **Manage > External Data Integration.**
2. From the **External Data Systems** list, select a data system and then do one of the following:
   - From the taskbar, select **System Tasks > Edit Data System**.
   - Right-click the data system and then select **Edit Data System**.

See "Adding an external data system" on page 762.

See "Deleting an external data system" on page 768.

See "Exporting an external data system " on page 769.

See "Importing an external data system " on page 769.

See "Viewing external system information in the details pane" on page 770.

Deleting an external data system

You can delete an existing external data system from the **Manage > External Data Integration** view.

Note: You cannot delete a pre-integrated external data system.

To delete an external data system

1. Go to **Manage > External Data Integration.**
2. From the **External Data Systems** list, select a data system and then do one of the following:
   - From the taskbar, select **System Tasks > Delete Data System**.
   - Right-click the data system and then select **Delete Data System**.

See "Adding an external data system" on page 762.

See "Editing an external data system" on page 767.

See "Exporting an external data system " on page 769.

See "Importing an external data system " on page 769.

See "Viewing external system information in the details pane" on page 770.

Importing an external data system

Control Compliance Suite lets you import the configuration file of an external data system that is exported to a specific location. When you import a configuration file, you can use the settings in the XML file to replicate the same configurations of the selected data system.

To import the external system data

1 Go to **Manage > External System Integration**.

2 From the taskbar, select **System Tasks > Import Data System**.

3 In the **Import Data System** dialog box, navigate to the location where the exported file is located, and then click **Import**.

The **System Summary** pane displays the summary of the data system that you have imported.

4 Click **OK**.

See "Adding an external data system" on page 762.

See "Exporting an external data system " on page 769.

See "Editing an external data system" on page 767.

See "Deleting an external data system" on page 768.

See "Viewing external system information in the details pane" on page 770.

Exporting an external data system

Control Compliance Suite lets you export the configuration file of an external data system that you have already added to the CCS infrastructure. You can later import the configuration file into another user environment to replicate the configurations of the data system that you exported.

To export the external system data

1 Go to **Manage > External System Integration** and then select a data system from the **External Data Systems** list.

2 Do one of the following:

- From the taskbar, select **System Tasks > Export Data System**.
- Right-click the data system and then select **Export Data System**.

3 In the **Browse for folder** dialog box, navigate to the location where you want to store the configuration file, and then click **OK**.

4 Click **OK**.

See “Adding an external data system” on page 762.

See “Importing an external data system ” on page 769.

See “Editing an external data system” on page 767.

See “Deleting an external data system” on page 768.

See “Viewing external system information in the details pane” on page 770.

Viewing external system information in the details pane

You can view the detailed information about the imported external system data in the details pane.

To view external system information

1 Go to **Manage > External Data Integration**.

2 In the table pane, select the external data system for which you want to view the information.

The details pane displays the relevant information in the following tabs:

General	Displays the data system name and the description. See “Data system details pane - General tab” on page 771.
Field Mapping	Displays the data fields mapping details between the imported data and the CCS schema. See “Data system details pane - Field Mapping tab” on page 772.
Data Correlation	Displays the asset and the status correlation data for the imported data and the CCS. See “Data system details pane - Data Correlation tab” on page 772.
Risk Aggregation	Displays the risk aggregation settings that you have configured for the selected data system. See “Data system details pane - Risk Aggregation tab” on page 771.

Reconciliation Rules	Displays the reconciliation rules that you have configured for the selected data system. See “Data system details pane - Reconciliation Rules tab” on page 771.

See “Viewing external data connection information in the details pane” on page 801.

Data system details pane - General tab

The General tab of the external data system details pane displays the following information:

External data system name	Displays the name of the external data system.
Description	Displays the details of the selected external data system.
Data schema	Displays the name of the data schema that is used to create the data system.

See “Viewing external system information in the details pane” on page 770.

Data system details pane - Reconciliation Rules tab

The Reconciliation Rules tab of the external data system details pane displays the reconciliation rules grouped according to the rule type. The Reconciliation Rules tab displays the following information for each rule:

Name	Displays the name of the Reconciliation rule.
Rule Definition	Displays the definition of the Reconciliation rule.

See “Viewing external system information in the details pane” on page 770.

Data system details pane - Risk Aggregation tab

The Risk Aggregation tab of the external data system details displays the risk aggregation options that are configured for the data system.

When using CCS to calculate the scores, the Risk Aggregation tab displays the data fields that are mapped to each CVSS attribute, and the weight.

If you use scores from incoming data, the Risk Aggregation tab displays the following information:

Risk score field	Displays the field in the external data that you want to contribute to the risk score calculation.
Minimum scale value	Displays the minimum value for the risk scale.
Maximum scale value	Displays the maximum value for the risk scale.
Weight	Displays the weight for the risk score calculation.

See "Viewing external system information in the details pane" on page 770.

Data system details pane - Field Mapping tab

The Field mapping tab of the external data system details pane displays the following information:

Table name	Fields
External System Fields	■ Field Name ■ Data Type ■ Is Mapped Fields that are selected are mapped from the external data system to the data schema.
Mapping for data schema	■ Mapped External System Field Name ■ Field Name ■ Data Type ■ Is Key Field ■ Field Type

See "Viewing external system information in the details pane" on page 770.

Data system details pane - Data Correlation tab

The Data Correlation tab of the external data system details pane displays the following information:

Correlated target field	Displays the data schema fields mapped to CCS asset fields.

CCS hosted assets	Displays the fields used to find the CCS hosted assets.
Other CCS assets	Displays the mandatory fields for custom assets that you have created.
Status values from external data	Displays the data schema status fields mapped to CCS result values.
CCS result values	Displays the CCS results values.

See “Viewing external system information in the details pane” on page 770.

Configuring data connections

You must add a data connection to import the external system data into Control Compliance Suite. You must have the external data system added to Control Compliance Suite to be able to create a data connection.

You can create only one type of data connection for a data system. For example, if you create an ODBC connection for a data system, the subsequent connections also must be ODBC connections.

Use the **Add Data Connection** wizard to add a connection.

You can add any of the following types of data connections to import external system data:

- ODBC data connection
  Use the ODBC data connection to import data from the systems that store data in databases using ODBC.
- CSV data connection
  Use the CSV data connection to import data from the systems that store data in .csv files.
- Web Services data connection
  Use the Web services data connection to import data from a data system by using a Web service.

See “Importing data using an ODBC connector” on page 774.

See “Importing data using a CSV connector” on page 779.

See “Importing data using a Web Services connector” on page 785.

See “Deleting a data connection” on page 801.

See “Editing a data connection” on page 800.

Importing data using an ODBC connector

Use the ODBC data connection to import data from the systems that store data in databases using ODBC.

To configure an ODBC data connection

1. Go to **Manage > External Data Integration**.
2. From the External Data Systems list, select the data system and then do one of the following:
   - From the taskbar, select **System Tasks > Add Data Connection**.
   - Right-click the data system and then select **Add Data Connection**.
3. In the **Specify the External Data System** panel, do the following and then click **Next**:

System name	Enter a name for the external data system that you want to add.
Description	Add a brief description on the external data system. This step is optional.

4. In the **Specify Data Connection Parameters** panel, do the following and then click **Next**:

Connection name	Enter the name of the external data connection that you want to create.
Connection type	Select **ODBC**. **Note:** To import data from Symantec Response Assessment Module (RAM), select the ODBC data connection.

   The following fields are displayed when you select **ODBC** from the **Connection type** drop-down list:

Data location	Select an existing data location or select **New** to create a new data location for the data connection. In the **Add Data Location** dialog box, do the following and then click **OK**: ■ In the **Name** text box, enter a name for the database location. After you add a data location, you can view the data location in the **Settings > General > System Configuration > Data Locations** pane. ■ In the **Description** text box, enter a brief description on the database location. ■ To enter the connection string, click the browse button (...) to launch the **Data Link Properties** dialog box. ■ On the **Provider** tab, select the database provider and then click **Next**. ■ On the **Connection** tab, provide the necessary information and then click **OK**.
Query type	Select the query type that you want to use for data import.
Table/View/SQL command	Based on the Query type, enter the table name or view name of the database from which you want to import data. You may also specify an SQL command to import data. **Note:** In the external data, if any column names contain special characters, specify the SQL command with escaped column names.

5 In the **Select Data Fields** panel, select the data fields that you want to include when you import the external data and then click **Next**.

You must select minimum two fields to import data.

6 In the **Select Data Schema** panel, select one of the following options and then click **Next**:

Create new schema

Schema is a representation of external data in CCS.

Enter the following information:

- In the **Schema name** text box, enter a name for the new schema that you want to create.
- In the **Description** field, enter a brief description of the new schema.

If you click **Create new schema**, then go to 8.

Existing schema

From the **Select CCS schema** drop-down list select the matching CCS schema to the external data.

If you click **Existing schema**, then go to 7.

7 The **Map Data Fields to CCS Schema Fields** panel displays the data fields that you specified in the **Select Data Fields** panel.

Do the following and then click **Next**:

- Drag the data fields from the **Field Name** column in the left-hand box to the **Mapped Field Name** column against the corresponding CCS field in the right-hand box. To identify unique fields in the external data, you must map the external data fields with key fields in the schema. The **Is a Key Field** column in the existing schema displays the key fields in the schema. If all the external data fields are mapped to CCS schema, go to 12.
- Check **Extend CCS Schema to import unmapped fields** if you want to extend the selected CCS schema to import the fields that are unmapped, and click **Next**.

8 The **Associate imported data with CCS** panel displays the data fields that you specified in the **Select Data Fields** panel or the fields that were unmapped in the **Map Data Fields to CCS Schema Fields** panel.

Enter the following information in the **CCS fields** list box and then click **Next**:

CCS Field

Displays the fields that you selected in the **Select Data Fields** panel.

Click the CCS field name to edit the name.

CCS data type

Select the data type from the drop-down list.

For Incremental Data Import select the data type of one of the fields as DateTime.

This field is used for incremental data collection as evaluation date time field. In incremental data import, the records only beyond the maximum date in the evaluation date time field, are fetched in subsequent imports.

Description

Add some description text for the field.

Attribute of

Select the CCS attribute to which you want to map the specified external data field. For example, Asset, Assessment, or Status.

Is a key field

Check to specify if the selected field is a key field. Key field is a mandatory field in CCS schema.

You must specify minimum one field as a key field for asset and assessment.

9 Perform this step only if you have selected a data type as DateTime, in 8

In the **Format and Date Time** panel, provide the following information and then click **Next**:

Evaluation date field	This field is used for incremental data collection. In incremental data import, the records only beyond the maximum date in the evaluation date time field, are fetched in subsequent imports. Select the evaluate date field from the **Evaluation date field** drop-down list.
Date-time format	Specify the date time format that you want to apply for all DateTime fields in the schema. To specify the date time format for a particular field, select the date time format in Date Time Format column for that field, in the schema. Check **Apply to all fields** if you want your selection to be applied to all the DateTime data fields. Refer to the Date-time formats supported in Control Compliance Suite section to view the datetime formats supported while importing external data. See "Date-time formats supported in Control Compliance Suite" on page 799.
Time zone	Select the time zone. To specify the time zone for a particular field, select the time zone in Time Zone column for that field, in the schema. Check **Apply to all fields** if you want your selection to be applied to all the Time Zone data fields.

10 In the **Data Import Schedule** panel, select one of the following schedule options and then click **Next**:

- **Run now**
  Select this option to run the job immediately after you click **Finish**.
- **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 execute the data import.

Run once	Select this option to execute the data import one time on the specified date and time.
Run every <number of days>	Select this option to specify how often (in days) you want to schedule the data import execution.

11 In the **Email Notification** panel, check **Send Notification** if you want to send a notification upon the success or failure of the data import execution. Both the tabs in the **Email Notification** panel contain the same options. Enter the following information and then click **Next**:

Subject	Enter the subject of the notification mail.
Message	Enter the message of the notification mail.
From (Email ID)	Enter the sender's email ID.
To (Email IDs)	Enter the receiver's email ID. Notification can be sent to multiple recipients. Separate each email ID with a comma.

12 In the **Summary** panel, view the summary and then click **Finish**.

See “Configuring data systems” on page 761.

See “Importing data using a CSV connector” on page 779.

See “Configuring a Web Service” on page 794.

Importing data using a CSV connector

Use the CSV data connection to import data from the systems that store data in .csv files.

Note: When importing external data by using CSV file, use dot [.] as a decimal separator and comma [,] as a CSV field separator. Field values in the CSV file must not contain a comma [,].

To configure a CSV data connection

1 Go to **Manage > External Data Integration**.

2 From the External Data Systems list, select the data system and then do one of the following:

- From the taskbar, select **System Tasks > Add Data Connection**.
- Right-click the data system and then select **Add Data Connection**.

3 In the **Specify the External Data System** panel, do the following and then click **Next**:

System name	Enter a name for the external data system that you want to add.
Description	Add a brief description on the external data system. This step is optional.

4 In the **Specify Data Connection Parameters** panel, do the following and then click **Next**:

Connection name	Enter the name of the external data connection that you want to create.
Connection type	Select **CSV**.

The following fields are displayed if you select **CSV** from the **Connection type** drop-down list:

Data location

Select an existing data location or select **New** to create a new data location for the data connection.

In the **Add Data Location** dialog box, in the **Network share Configuration** section, provide the following information and then click **OK**:

- In the **Name** text box, enter a name for the location where the CSV files are stored.

  After you add a data location, you can view the data location in the **Settings > General > System Configuration > Data Locations** pane.
- In the **Description** text box, enter a brief description on the database location.
- To enter the share path where the CSV file is located, click the browse button (...) to launch the **Browse For Folder** dialog box and then select the folder.

In the **Credentials** section, provide the following information:

- In the **Domain** drop-down list, enter the domain of the network share path where the CSV file is located and then click **OK**.

  Note: Enter the domain name if you accessing a share on a computer in a domain. Enter the workgroup name or computer name if you accessing a share on a computer in a workgroup.
- In the **User name** text box, enter the user name to access the network share path.
- In the **Password** text box, enter the password for the mentioned user account.
- In the **Confirm password** text box, re-enter the password for the mentioned user account.

Sample file path	The first file in the share is automatically chosen as the sample file. This sample file is used to read the header of the CSV file to form a schema. To manually select the sample file, click the browse button (...) to navigate to the location where the CSV file is located.

5 In the **Select Data Fields** panel, select the data fields that you want to include when you import the external data and then click **Next**.

You must select minimum two fields to import data.

6 In the **Select Data Schema** panel, select one of the following options and then click **Next**:

Create new schema	Schema is a representation of external data in CCS. Enter the following information: ■ In the **Schema name** text box, enter a name for the new schema that you want to create. ■ In the **Description** field, enter a brief description of the new schema. If you click **Create new schema**, then go to 8. **Note:** All fields coming from the CSV file are treated as Text data type. Select the appropriate data type for each field for creating appropriate dashboards and representations in CCS.
Existing schema	From the **Select CCS schema** drop-down list select the matching CCS schema to the external data. If you click **Existing schema**, then go to 7.

7 The **Map Data Fields to CCS Schema Fields** panel displays the data fields that you specified in the **Select Data Fields** panel.

Do the following and then click **Next**:

- Drag the data fields from the **Field Name** column in the left-hand box to the **Mapped Field Name** column against the corresponding CCS field in the right-hand box. To identify unique fields in the external data, you must map the external data fields with key fields in the schema. The **Is a Key Field** column in the existing schema displays the key fields in the schema. If all the external data fields are mapped to CCS schema, go to 12.
- Check **Extend CCS Schema to import unmapped fields** if you want to extend the selected CCS schema to import the fields that are unmapped, and click **Next**.

8 The **Associate imported data with CCS** panel displays the data fields that you specified in the **Select Data Fields** panel or the fields that were unmapped in the **Map Data Fields to CCS Schema Fields** panel.

Enter the following information in the **CCS fields** list box and then click **Next**:

CCS Field	Displays the fields that you selected in the **Select Data Fields** panel. Click the CCS field name to edit the name.
CCS data type	Select the data type from the drop-down list. For Incremental Data Import select the data type of one of the fields as DateTime. This field is used for incremental data collection as evaluation date time field. In incremental data import, the records only beyond the maximum date in the evaluation date time field, are fetched in subsequent imports.
Description	Add some description text for the field.
Attribute of	Select the CCS attribute to which you want to map the specified external data field. For example, Asset, Assessment, or Status.
Is a key field	Check to specify if the selected field is a key field. Key field is a mandatory field in CCS schema. You must specify minimum one field as a key field for asset and assessment.

9 Perform this step only if you have selected a data type as DateTime, in 8

In the **Format and Date Time** panel, provide the following information and then click **Next**:

Evaluation date field

This field is used for incremental data collection. In incremental data import, the records only beyond the maximum date in the evaluation date time field, are fetched in subsequent imports.

Select the evaluate date field from the **Evaluation date field** drop-down list.

Date-time format

Specify the date time format that you want to apply for all DateTime fields in the schema.

To specify the date time format for a particular field, select the date time format in Date Time Format column for that field, in the schema.

Check **Apply to all fields** if you want your selection to be applied to all the DateTime data fields.

Refer to the Date-time formats supported in Control Compliance Suite section to view the datetime formats supported while importing external data.

See "Date-time formats supported in Control Compliance Suite" on page 799.

Time zone

Select the time zone.

To specify the time zone for a particular field, select the time zone in Time Zone column for that field, in the schema.

Check **Apply to all fields** if you want your selection to be applied to all the Time Zone data fields.

10 In the **Data Import Schedule** panel, select one of the following schedule options and then click **Next**:

- **Run now**
  Select this option to run the job immediately after you click **Finish**.

- **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 execute the data import.
Run once	Select this option to execute the data import one time on the specified date and time.
Run every <number of days>	Select this option to specify how often (in days) you want to schedule the data import execution.

11 In the **Email Notification** panel, check **Send Notification** if you want to send a notification upon the success or failure of the data import execution. Both the tabs in the **Email Notification** panel contain the same options. Enter the following information and then click **Next**:

Subject	Enter the subject of the notification mail.
Message	Enter the message of the notification mail.
From (Email ID)	Enter the sender's email ID.
To (Email IDs)	Enter the receiver's email ID. Notification can be sent to multiple recipients. Separate each email ID with a comma.

12 In the **Summary** panel, view the summary and then click **Finish**.

See “Configuring data systems” on page 761.

See “Importing data using an ODBC connector” on page 774.

See “Configuring a Web Service” on page 794.

Importing data using a Web Services connector

For importing data using a Web Services connector, you must first implement a new Web service and then configure the Web service in CCS.

- See “About Web Services connector” on page 786.
- See “Implementing a Web Service” on page 786.
- See “Configuring a Web Service” on page 794.

About Web Services connector

The Web services connector lets you import data from external Web services. To get data from an external Web service, you must implement the IDataImporter interface and create a new Web service.

For example, If an external application provides data from a Web service - http://www.securityapp.com/dummyapp/data, you must create a new Web service - http://<machine-name>/securityapp/dataimporter to fetch data from the above mentioned Web service.

The new Web service must implement the IDataImporter interface. The IDataImporter interface provides the following four methods that transform data coming from third-party services into .xml format. CCS uses these methods to fetch data from the external Web service:

- GetSchema
- GetDatapage
- GetParameterInformation
- TestConnection

CCS supports the following binding types for creating a new Web service:

- Basic HTTP
- WSHTTP

See "Implementing a Web Service" on page 786.

See "Configuring a Web Service" on page 794.

Implementing a Web Service

The Web services connector lets you import data from external Web services. To get data from an external Web service, you must implement the IDataImporter interface and create a new Web service.

Add "IDataImporterTemplate.wsdl" as a service reference to get interface definition from http://<<AppServerHostName>>/CCS_Web/IDataImporterTemplate.wsdl.

For example, a code snippet from the service interface generated using the IDataImporterTemplate.wsdl:

```
[ServiceContract]
public interface IDataImporter
{
    [OperationContract]
    string GetParameterInformation();

    [OperationContract]
    string GetSchema();

    [OperationContract]
    string GetDataPage(string parameterXML, string PageInformation);

    [OperationContract]
    void TestConnection();
}
```

You must implement the following four methods provided by the IDataImporter interface. These methods transform data coming from external data services into .xml format. CCS uses these methods to fetch data from the external Web service:

- GetParameterInformation:
  Implement this method to get information about the parameters to be passed to the Web service. You can use the parameters to scope or filter the information received from external data systems.
  - Syntax:
    `string GetParameterInformation()`
  - Input Parameters:
    This method does not require any input parameters.
  - Return Values:
    This method returns the parameter xml which is used to scope and filter external data. The parameters in the xml are displayed on the CCS user interface where you can pass values to those parameters. You have to implement the GetDataPage method to use those values to get filtered data.

    Following is a sample xsd for the return value xml format for GetParameterInformation.

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema attributeFormDefault="unqualified"
elementFormDefault="qualified"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  targetNamespace="http://www.symantec.com/schemas/
  2011/WebServiceConnector/ParametersSchema">
 <xs:element name="parameters">
  <xs:complexType>
   <xs:sequence>
    <xs:element maxOccurs="unbounded" minOccurs="0"
       name="parameter">
```

```
     <xs:complexType>
      <xs:sequence>
       <xs:element name="selectionlist" minOccurs="0" >
        <xs:complexType>
         <xs:sequence>
          <xs:element maxOccurs="unbounded" minOccurs="0"
             name="value" />
         </xs:sequence>
        </xs:complexType>
       </xs:element>
       <xs:element name="valuelist" minOccurs="0">
        <xs:complexType>
         <xs:sequence>
          <xs:element maxOccurs="unbounded" minOccurs="0"
             name="value" />
         </xs:sequence>
        </xs:complexType>
       </xs:element>
      </xs:sequence>
      <xs:attribute name="name" type="xs:string" use="required"/>
      <xs:attribute name="description" type="xs:string" />
      <xs:attribute name="dataType" use="required">
       <xs:simpleType>
        <xs:restriction base="xs:string">
         <xs:enumeration value="Integer"/>
         <xs:enumeration value="String"/>
        </xs:restriction>
       </xs:simpleType>
      </xs:attribute>
      <xs:attribute name="isMandatory" type="xs:boolean" />
      <xs:attribute name="isMultiValued" type="xs:boolean" />
     </xs:complexType>
    </xs:element>
   </xs:sequence>
  </xs:complexType>
 </xs:element>
</xs:schema>
```

Following is a sample xml generated using the above xsd.

```
<?xml version="1.0" encoding="utf-8"?>
<parameters xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns="http://www.symantec.com/schemas/
  2011/WebServiceConnector/ParametersSchema">
  <parameter name="Status"
   description="This is state of vulnerability
   reported at an instance of time"
    dataType="String" isMandatory="false"
     isMultiValued="true">
    <selectionlist>
      <value>Vulanrable</value>
      <value>Not Vulnerable</value>
      <value>Unknown</value>
    </selectionlist>
    <valuelist>
      <value>Vulanrable</value>
      <value>Not Vulnerable</value>
    </valuelist>
  </parameter>
</parameters>
```

- GetSchema:
  Implement this method to get the data schema which contains fields and data types for external data. This method returns the schema in .xml format.
  - Syntax:
    `string GetSchema()`
  - Input Parameters:
    This method does not require any input parameters.
  - Return Values:
    This method returns the schema of the external data which is used for creating new data schema through the CCS user interface.
    Following is a sample xsd for the return value xml format for GetSchema.

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema attributeFormDefault="unqualified"
 elementFormDefault="qualified"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  targetNamespace="http://www.symantec.com/schemas/
  2011/WebServiceConnector/SchemaXMLSchema">
 <xs:element name="schemaXML">
  <xs:complexType>
   <xs:sequence>
```

```
    <xs:element maxOccurs="unbounded" name="field">
     <xs:complexType>
      <xs:attribute name="name" type="xs:string"
      use="required" />
      <xs:attribute name="dataType" use="required" >
       <xsd:simpleType>
        <xsd:restriction base="xs:string">
         <xsd:enumeration value="Boolean"/>
         <xsd:enumeration value="DateTime"/>
         <xsd:enumeration value="Decimal"/>
         <xsd:enumeration value="Guid"/>
         <xsd:enumeration value="Integer"/>
         <xsd:enumeration value="String"/>
        </xsd:restriction>
       </xsd:simpleType>
      </xs:attribute>
     </xs:complexType>
    </xs:element>
   </xs:sequence>
  </xs:complexType>
 </xs:element>
</xs:schema>
```

Following is a sample xml generated using the above xsd.

```
<?xml version="1.0" encoding="utf-8" ?>
<schemaXML xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns="http://www.symantec.com/schemas/
  2011/WebServiceConnector/SchemaXMLSchema">
  <field name="InsidentId" dataType="Integer" />
  <field name="InsidentGuid" dataType="Guid" />
  <field name="OwnerId" dataType="Integer" />
  <field name="MachineName" dataType="String" />
  <field name="IP" dataType="String" />
  <field name="OS" dataType="String" />
  <field name="Department" dataType="String" />
  <field name="CreatedDate" dataType="DateTime" />
  <field name="CreatedBy" dataType="Integer" />
  <field name="LastModifiedDate" dataType="DateTime" />
  <field name="LastModifiedBy" dataType="Integer" />
  <field name="CheckId" dataType="String" />
  <field name="CheckName" dataType="String" />
  <field name="Status" dataType="String" />
</schemaXML>
```

- GetDataPage:
  Implement this method to get data from external application.
  - Description:
  - Syntax:
    `string GetDataPage(string parameterXML, string PageInformation)`
  - Input Parameters:
    The following table describes the input parameters that the API requires:

parameterXML	Parameter xml is used to scope and filter the external data. The parameter values that you provide on the CCS user interface are passed as a part of the parameter xml. You must implement this method to use those values to get filtered data.
PageInformation	This information is used to retrieve the current data page of the data schema.

  - Return Values:
    This method gets the data from the external application. The data is fetched in pages. You must implement the method in such a way that external data is divided into pages and the method returns a single page at time. The method must return the data in xml format.
    Following is a sample xsd for the return value xml format for GetDataPage.

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema attributeFormDefault="unqualified"
  elementFormDefault="qualified"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  targetNamespace="http://www.symantec.com/schemas/
  2011/WebServiceConnector/DataSetSchema">
 <xs:element name="dataset">
  <xs:complexType>
   <xs:sequence>
    <xs:element maxOccurs="unbounded" minOccurs="0"
     name="row">
     <xs:complexType>
      <xs:sequence>
       <xs:element maxOccurs="unbounded" minOccurs="0"
       name="field">
        <xs:complexType>
         <xs:simpleContent>
          <xs:extension base="xs:string">
           <xs:attribute name="name" type="xs:string"
            use="required" />
           <xs:attribute name="dataType" use="required" >
            <xsd:simpleType>
             <xsd:restriction base="xs:string">
              <xsd:enumeration value="Boolean"/>
              <xsd:enumeration value="DateTime"/>
              <xsd:enumeration value="Decimal"/>
              <xsd:enumeration value="Guid"/>
              <xsd:enumeration value="Integer"/>
              <xsd:enumeration value="String"/>
             </xsd:restriction>
            </xsd:simpleType>
           </xs:attribute>
          </xs:extension>
         </xs:simpleContent>
        </xs:complexType>
       </xs:element>
      </xs:sequence>
     </xs:complexType>
    </xs:element>
   </xs:sequence>
   <xs:attribute name="currentPage" type="xs:string"
    use="required" />
   <xs:attribute name="nextPage" type="xs:string"
    use="required" />
  </xs:complexType>
 </xs:element>
</xs:schema>
```

Following is a sample xml generated using the above xsd.

```
<?xml version="1.0" encoding="utf-8"?>
<dataset xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    currentPage="1" nextPage=""
    xmlns="http://www.symantec.com/schemas/
    2011/WebServiceConnector/DataSetSchema">
  <row>
    <field name="InsidentId" dataType="Integer">1</field>
    <field name="InsidentGuid"
     dataType="Guid">766ce3a5-e720-4926-91a5-213753b09ee5</field>
    <field name="OwnerId" dataType="Integer">1</field>
    <field name="MachineName" dataType="String">Symantec2</field>
    <field name="IP" dataType="String">111.111.111.111</field>
    <field name="OS" dataType="String">Win2K8</field>
    <field name="Department" dataType="String">Account</field>
    <field name="CreatedDate"
     dataType="DateTime">2011-03-23T16:57:55.000Z</field>
    <field name="CreatedBy" dataType="Integer">1</field>
    <field name="LastModifiedDate"
     dataType="DateTime">2011-03-23T18:07:37.000Z</field>
    <field name="LastModifiedBy" dataType="Integer">1</field>
    <field name="CheckId" dataType="String">Check-1</field>
    <field name="CheckName"
     dataType="String">SecurityPatchUpdate</field>
    <field name="Status" dataType="String">Pass</field>
  </row>
  <row>
    <field name="InsidentId" dataType="Integer">2</field>
    <field name="InsidentGuid"
     dataType="Guid">766ce3a5-e720-4926-91a5-213753b09ee6</field>
    <field name="OwnerId" dataType="Integer">2</field>
    <field name="MachineName" dataType="String">score</field>
    <field name="IP" dataType="String">111.111.111.112</field>
    <field name="OS" dataType="String">Win2K8-R2</field>
    <field name="Department" dataType="String">Store</field>
    <field name="CreatedDate"
     dataType="DateTime">2011-03-23T18:13:07.000Z</field>
    <field name="CreatedBy" dataType="Integer">2</field>
    <field name="LastModifiedDate"
     dataType="DateTime">2011-03-23T19:52:37.000Z</field>
    <field name="LastModifiedBy" dataType="Integer">2</field>
    <field name="CheckId" dataType="String">Check-3</field>
    <field name="CheckName" dataType="String">IEPatchUpdate</field>
    <field name="Status" dataType="String">Fail</field>
  </row>
</dataset>
```

- TestConnection:

Implement this method to test the connection to the Web service. This method does not require any code definition.

- Syntax:

  ```
  void TestConnection()
  ```

- Input Parameters
  This method does not require any input parameters.
- Return Values:
  This method does not return any value.

Configuring a Web Service

You must add a Web services data connection to import data from a data system by using a Web service.

To configure a Web service data connection

1. Go to **Manage > External Data Integration**.
2. From the External Data Systems list, select the data system and then do one of the following:
   - From the taskbar, select **System Tasks > Add Data Connection**.
   - Right-click the data system and then select **Add Data Connection**.
3. In the **Specify the External Data System** panel, do the following and then click **Next**:

System name	Enter a name for the external data system that you want to add.
Description	Add a brief description on the external data system. This step is optional.

4. In the **Specify Data Connection Parameters** panel, do the following and then click **Next**:

Connection name	Enter the name of the external data connection that you want to create.
Connection type	Select **Web service**.
Data Location	To specify a new data location, click **New**.

5 In the **Add Data Location** dialog box, provide the following information and then click **OK**:

Name

Enter a name for the data location that you want to create.

Description

Enter a brief description about the data location that you want to create.

Discovery URL

Enter the metadata (WSDL) URL of the service.

Click Discover to auto-populate the **Service URL** drop-down list with the available endpoints.

Service URL

Displays the available endpoints that are available at the specified location.

Enter the endpoint URL or select the appropriate endpoint from the list.

Binding Type

Select **Basic HTTP**, **WSHTTP, or Basic HTTP(SSL)**from the drop-down list.

User name

Provide the user name to connect to the service.

Password

Provide the password to authenticate the user account that you have specified.

Confirm password

Re-type the password.

Test Connection

Click to test the connection to the Web service.

6 After specifying the data location, the parameters for scoping the data are displayed in the Parameters grid. This information is fetched from the GetParameterInformation method implemented in the Web service. In the Parameters grid, for each parameter, in the Values column, click the (...) button to add the parameter value.

7 In the **Web Service Parameter** dialog box, from the **Values to add** drop-down list, enter the parameter value or select the appropriate value from the list, and click **Add**.

Note: You cannot set multiple values for a parameter.

8. Click **OK** and then click **Next**.

9. In the **Select Data Fields** panel, select the data fields that you want to include when you import the external data and then click **Next**.

   You must select minimum two fields to import data.

10. In the **Select Data Schema** panel, select one of the following options and then click **Next**:

Create new schema	Schema is a representation of external data in CCS. Enter the following information: ■ In the **Schema name** text box, enter a name for the new schema that you want to create. ■ In the **Description** field, enter a brief description of the new schema. If you click **Create new schema**, then go to 12.
Existing schema	From the **Select CCS schema** drop-down list select the matching CCS schema to the external data. If you click **Existing schema**, then go to 11.

11. The **Map Data Fields to CCS Schema Fields** panel displays the data fields that you specified in the **Select Data Fields** panel.

    Do the following and then click **Next**:

    - Drag the data fields from the **Field Name** column in the left-hand box to the **Mapped Field Name** column against the corresponding CCS field in the right-hand box. To identify unique fields in the external data, you must map the external data fields with key fields in the schema. The **Is a Key Field** column in the existing schema displays the key fields in the schema. If all the external data fields are mapped to CCS schema, go to 16.

    - Check **Extend CCS Schema to import unmapped fields** if you want to extend the selected CCS schema to import the fields that are unmapped, and click **Next**.

12 The **Associate imported data with CCS** panel displays the data fields that you specified in the **Select Data Fields** panel or the fields that were unmapped in the **Map Data Fields to CCS Schema Fields** panel.

Enter the following information in the **CCS fields** list box and then click **Next**:

CCS Field

Displays the fields that you selected in the **Select Data Fields** panel.

Click the CCS field name to edit the name.

CCS data type

Select the data type from the drop-down list.

For Incremental Data Import select the data type of one of the fields as DateTime.

This field is used for incremental data collection as evaluation date time field. In incremental data import, the records only beyond the maximum date in the evaluation date time field, are fetched in subsequent imports.

Description

Add some description text for the field.

Attribute of

Select the CCS attribute to which you want to map the specified external data field. For example, Asset, Assessment, or Status.

Is a key field

Check to specify if the selected field is a key field. Key field is a mandatory field in CCS schema.

You must specify minimum one field as a key field for asset and assessment.

13 Perform this step only if you have selected a data type as DateTime, in 12

In the **Format and Date Time** panel, provide the following information and then click **Next**:

Evaluation date field

This field is used for incremental data collection. In incremental data import, the records only beyond the maximum date in the evaluation date time field, are fetched in subsequent imports.

Select the evaluate date field from the **Evaluation date field** drop-down list.

Date-time format

Specify the date time format that you want to apply for all DateTime fields in the schema.

To specify the date time format for a particular field, select the date time format in Date Time Format column for that field, in the schema.

Check **Apply to all fields** if you want your selection to be applied to all the DateTime data fields.

Refer to the Date-time formats supported in Control Compliance Suite section to view the datetime formats supported while importing external data.

See "Date-time formats supported in Control Compliance Suite" on page 799.

Time zone

Select the time zone.

To specify the time zone for a particular field, select the time zone in Time Zone column for that field, in the schema.

Check **Apply to all fields** if you want your selection to be applied to all the Time Zone data fields.

14 In the **Data Import Schedule** panel, select one of the following schedule options and then click **Next**:

- **Run now**
  Select this option to run the job immediately after you click **Finish**.

- **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 execute the data import.
Run once	Select this option to execute the data import one time on the specified date and time.
Run every <number of days>	Select this option to specify how often (in days) you want to schedule the data import execution.

15 In the **Email Notification** panel, check **Send Notification** if you want to send a notification upon the success or failure of the data import execution. Both the tabs in the **Email Notification** panel contain the same options. Enter the following information and then click **Next**:

Subject	Enter the subject of the notification mail.
Message	Enter the message of the notification mail.
From (Email ID)	Enter the sender's email ID.
To (Email IDs)	Enter the receiver's email ID. Notification can be sent to multiple recipients. Separate each email ID with a comma.

16 In the **Summary** panel, view the summary and then click **Finish**.

See “Configuring data systems” on page 761.

See “Importing data using an ODBC connector” on page 774.

See “Importing data using a CSV connector” on page 779.

Date-time formats supported in Control Compliance Suite

CCS supports the following date-time formats while importing external data:

- yyyy/MM/dd
- dd.MM.YYYY
- M/d/yyyy
- d-M-yyyy

- dd/MM/yyyy
- yyyy-MM-ddThh:mm:ssZ
  For example, 2012-11-11T01:10:23Z
- M/d/yyyy h:mm:ss tt
- yyyy-MM-dd tt h:mm:ss
  For example, 2019-12-10 AM 1:12:32
- yyyy-MM-dd HH:mm:ss
- yyyy-MM-dd HH:mm:ss.fff
  For example, 2019-12-10 11:10:32.600
- yyyy/MM/dd hh:mm:ss tt
  For example, 2019/12/10 01:12:32 AM
- yyyy/M/d HH:mm:ss
- yyyy-M-d H:mm:ss
- d-M-yyyy H:mm:ss
- dd/MM/yyyy hh:mm:ss tt
- dd/MM/yyyy HH:mm:ss
- dd/MM/yyyy h:mm:ss tt
- dd.MM.yyyy H:mm:ss
- d/MM/yyyy h:mm:ss tt
- d/MM/yyyy H:mm:ss
- d/M/yyyy tt h:mm:ss
- dd-MMM-yyyy
- dd-MMM-yyyy hh:mm:ss tt
  For example, 03-Mar-2011 01:22:55 PM
- M/d/yyyy hh:mm:ss tt

Editing a data connection

You can edit an existing data connection by selecting the data connection from the **External Data Systems** view.

Note: When you edit a data connection, you must select the connection that you want to modify, and not the data system.

To edit a data connection

1. Go to **Manage > External Data Integration**.
2. In the **External Data System(s)** pane, expand a data system to view the configured data connections for that system.
3. Right-click the data connection that you want to modify, and click **Edit Data Connection**.
4. In the subsequent panels, make the required changes in the remaining panels and then click **Next** until you reach the Summary panel.
5. In the **Summary** panel, view the summary and then click **Finish**.

See “Configuring data connections” on page 773.

See “Deleting a data connection” on page 801.

Deleting a data connection

You can delete an existing data connection by selecting the data connection from the **External Data Systems** view.

To delete a data connection

1. Go to **Manage** > **External Data Integration**.
2. From the **External Data Systems**, expand a data system to view the configured data connections for that system.
3. From the **Connection Tasks**, click **Delete Data Connection**.

See “Configuring data connections” on page 773.

See “Editing a data connection” on page 800.

Viewing external data connection information in the details pane

You can view the detailed information about an external system data connection in the details pane.

To view external data connection information

1. Go to **Manage > External Data Integration**.
2. In the table pane, select the external data connection for which you want to view the information.

   The details pane displays the relevant information in the following tabs:

General	Displays the data connection name and the description. See "Data connection details pane - General tab" on page 802.
Schedule	Displays the schedule that you have configured for the data connection. See "Data connection details pane - Schedule tab" on page 802.
Email Notification	Displays the email notification configurations for the data connection. See "Data connection details pane - Email Notification tab" on page 803.

See "Viewing external system information in the details pane" on page 770.

Data connection details pane - General tab

The General tab of the data connection details pane displays the following information:

Connection name	Displays the name of the data connection.
Data location	Displays the data location of the data connection which you have created. For example, if you have created a CSV connection, the Data location field displays the data location of the CSV data connection.

See "Viewing external data connection information in the details pane" on page 801.

Data connection details pane - Schedule tab

The Schedule tab of the data connection details pane displays the following information:

Run now	Displays the date and time when the import job is run.
Recurring	Displays Yes if you have set a recurring import job. Displays No if you have not set a recurring import job.
Run every	Displays how often (in days) an import job is scheduled to run.

See "Viewing external data connection information in the details pane" on page 801.

Data connection details pane - Email Notification tab

The Email Notification tab of the data connection details pane displays the email notification messages. The email notification messages are sent upon the success or failure of the data import execution. Both the tabs in the **Email Notification** panel contain the same following options.

Send Notification	The Send notification is checked if you want to send a notification upon the success or failure of the data import execution.
Subject	Displays the subject of the notification mail.
Message	Displays the message of the notification mail.
From (Email ID)	Displays the sender's email ID.
To (Email IDs)	Displays the receiver's email ID. Notification can be sent to multiple recipients. Separate each email ID with a comma.

See "Viewing external data connection information in the details pane" on page 801.

Using external data

External data integration lets you seamlessly assimilate data from an external application to Control Compliance Suite You can represent the data by leveraging the CCS dashboards and reports. Once you import the external data into Control Compliance Suite using a data connection, you can use the data for:

- See "Policy compliance in correlation with CCS assets" on page 804.

- See “Contributing to the CCS asset Risk Score” on page 805.
- See “Viewing the data in dashboards” on page 807.
- See “Correlating data with CCS” on page 809.
- See “Reconciling assets based on external system data” on page 811.

Policy compliance in correlation with CCS assets

You can use the imported data to correlate with the CCS assets. You can then calculate the compliance score of the assets based on policies, mandates, and regulations.

See “Using external data for policy compliance” on page 804.

Using external data for policy compliance

Perform the following procedure to use external data for policy compliance.

To use external data for policy compliance

1. Define the policy.
2. Define the control statements.
3. Add the external data system. See “Adding an external data system” on page 762.
4. Import the external data using the data connectors. See “Configuring data connections” on page 773.

   Note: You must map assessments, that are imported as a part of external data import, to control statements.

5. If required, create assessment procedures for the asset data that you import from external data systems. See “Working with assessment procedures for external data” on page 804.
6. Run the import job.
7. Create dashboards.
8. Create reports.

Working with assessment procedures for external data

Assessments for preshipped or external data systems are imported as a part of external data import. The assessments that are imported as part of the data schema are available under that data schema in Controls Studio. You must map these assessments to control statements.

You can create assessment procedures for the asset data that you import from external data systems. You can assessment procedures on external data to determine the result of the assessment. For example, to determine wether the password length is greater than 8 characters, form the following expression for the assessment procedure.

[Password length < 8]

If the expression evaluates to true, the assessment fails.

If you receive multiple results for the same asset, you can use aggregated functions such as, sum, count, and so on to determine the asset status.

For example, if you have patch assessment results for multiple assets, where assets have multiple patches installed. To create an assessment procedure to check if an asset has all the required patches installed, form the following expression for the assessment procedure.

IF [Count PatchName > 0]

WHERE [Status = Missing]

For information on creating assessment procedures,

See "Using external data for policy compliance" on page 804.

Contributing to the CCS asset Risk Score

A risk score is used to quantify the risk that is associated with an asset in your organization. You can import external data and use it for contributing to the CCS asset risk score. Before contributing to the risk score, you must first correlate the assets with CCS assets. See "Correlating data with CCS" on page 809.

See "Using external data to contribute to the CCS asset Risk Score" on page 805.

Using external data to contribute to the CCS asset Risk Score

Perform the following procedure to use external data to contribute to the CCS asset Risk Score.

To use external data to contribute to the CCS asset Risk Score

1. Add the external data system. See "Adding an external data system" on page 762.
2. Import the external data using the data connectors. See "Configuring data connections" on page 773.

3 Configure asset risk aggregation. See “Configuring asset risk aggregation for external data” on page 806.

4 Run the import job.

5 Create dashboards. For information on creating dashboards,

Configuring asset risk aggregation for external data

Asset risk aggregation lets you contribute to the risk score for an asset associated with an external data system.

For calculating the risk score from external data on associated assets, specify the CVSS attributes to calculate the risk score.

If the external data system already contains the calculated risk score, you can specify a risk score field which CCS uses to contribute to the risk score for an asset.

Note: The fields used for asset risk aggregation appear in the **Set Asset Risk Aggregation** panel only if you have selected the status field while creating the data schema.

To configure asset risk aggregation

1 Go to **Manage > External Data Integration**.

2 From the **Data Systems** list, select a data system, and then do one of the following:

- From the taskbar, select **Data Schema Tasks > Set Asset Risk Aggregation**.
- Right-click the data system and then select **Set Asset Risk Aggregation**.

3 In the **Set Asset Risk Aggregation** panel, check **Enable risk aggregation**.

4 Select **Enable Risk Aggregation for Assessment Procedure** to calculate risk score using assessment procedures.

Select **Enable Risk Aggregation for Assessment** to calculate risk score using assessments.

Note: The **Enable Risk Aggregation for Assessment** option is disabled for the Symantec Data Loss Prevention data system.

5 For risk score calculation for Assessments, select one of the following options:

Use CCS to calculate the scores

Select this option if you want CCS to calculate the risk score on the basis of the Common Vulnerability Scoring System (CVSS) attributes. CCS calculates the risk score on the basis of the CVSS attributes and the weight that you specify.

For each attribute, select the corresponding field from the drop-down list and specify the weight for the risk aggregation. The weight is used if an asset has a risk score from more than one system.

Use scores from incoming data

Select this option if you want to use the risk scores that are specified in the imported data. Specify the following information:

- Risk score field - Select the field in the external data that you want to contribute to the risk score calculation.
- Minimum scale value - Specify the minimum value for the risk scale.
- Maximum scale value - Specify the maximum value for the risk scale.
- Weight - Specify the weight for the risk aggregation. The weight is used if an asset has a risk score from more than one system.

Note: If the external data system has a risk score between 10 to 100, then the minimum scale value is 10 and maximum scale value is 100. CCS converts these values to the range of 0 to 10.

6 Click **OK**.

Viewing the data in dashboards

You can view external data in the CCS dashboards in the following ways:

- You can import external data and view the data using CCS dashboards without correlating the external data to CCS assets.
  See “Viewing external data in CCS dashboards without CCS asset correlation” on page 808.

- You can import external data and view the data using CCS dashboards in correlation with the CCS assets. By means of correlation, you basically establish an association between the data schema and the existing CCS assets. For example, if you import data on vulnerability, you can associate the reported vulnerability to an asset. You can then correlate to an asset in the CCS asset system. CCS provides you the capability to define new data schemas, which you can map to a CCS asset system by matching attributes.

  See "Viewing external data in CCS dashboards in correlation with the CCS assets" on page 808.

Viewing external data in CCS dashboards without CCS asset correlation

Perform the following procedure to view external data in CCS dashboards without CCS asset correlation.

To view external data in CCS dashboards without CCS asset correlation

1. Add the external data system. See "Adding an external data system" on page 762.
2. Import the external data using the data connectors. See "Configuring data connections" on page 773.
3. Create dashboards. For information on creating dashboards,

Viewing external data in CCS dashboards in correlation with the CCS assets

Perform the following procedure to view external data in CCS dashboards in correlation with the CCS assets.

To view external data in CCS dashboards in correlation with the CCS assets

1. Add the external data system. See "Adding an external data system" on page 762.
2. Import the external data using the data connectors. See "Configuring data connections" on page 773.
3. Correlate asset data with Control Compliance Suite. See "Correlating data with CCS" on page 809.
4. Run the import job.
5. Create dashboards. For information on creating dashboards,

Correlating data with CCS

Data correlation lets you establish an association between the data fields in the imported data and the CCS data. By means of correlation, you ensure that CCS is able to consume the data that is imported from an external system. You must correlate data for assets, status and assessments.

In asset correlation, you associate assets in the external data system with assets in CCS. For example, you can correlate assets in external system using the following fields: Host name, IP address, and Fully qualified domain name. For adding new assets to CCS, See "Reconciling assets based on external system data" on page 811.

In status correlation, you associate assessment results in external data system with status in CCS. For example, external systems produce results in different formats such as closed, open, or range 0 to 5, which must be mapped to CCS formats of pass, fail, unknown and not applicable.

In assessment correlation, you provide assessment information to identify assessments in external data. For example, in external data, the Assessments name field contains the assessment name as password length. You must provide this assessment name field to CCS for identifying the assessments in external data.

To correlate external system data with CCS

1. Go to **Manage > External Data Integration**.
2. From the **External Data Systems** list, select a data system and then do one of the following:
   - From the taskbar, select **System Tasks > Correlate Data With CCS**.
   - Right-click the data system and then select **Correlate Data With CCS**.

3 In the **Correlate Asset Data** panel, in the **Asset category** section, select one of the following options:

CCS hosted assets (Identified by IP Address)	Lets you identify assets that are present in the CCS asset system. This option works for CCS supported asset types. Select **CCS hosted assets (Identified by IP address)** if the asset already exists in the CCS system and you can identify the asset. You can identify the asset using the Host name , IP address , or a Fully Qualified Domain Name. From the **Asset Field Name** list, drag the field names and drop them in the Mapped Asset Field Name column against the corresponding CCS asset field. **Note:** Computers having the same IP address across the domain are resolved by providing both, the IP address, and the fully qualified domain name.
Other CCS assets	Lets you select the custom assets that you have created. Once you select the asset type, CCS displays all mandatory fields for that asset type. Select this option if the asset already exists in the system and the asset is a custom asset. From the **Asset Field Name** list, drag the field names and drop them in the Mapped Asset Field Name column against the corresponding CCS asset field.

4 Click **Next**.

5 In the **Correlate Status with CCS Results** panel, in the **Status** field drop-down list, select the status field.

The Status fields appear in the **Status** field drop-down list only if you have selected the status and assessment fields while creating the data schema.

6 Click **Add** to add the status field to CCS results mapping, and then do the following:

- In the **Status values from external data** column, type the value for the result data field in the imported data.

- In the **CCS Result Values** drop-down list, select the CCS result value. The **CCS Result Values** drop-down list contains the following fields: Pass, Fail, Unknown, and Not Applicable. Map all the possible values in the Status field from external data. CCS represents all the values from external data as mapped CCS result values.

7 Click **Next**.

8 Perform this step only if you have selected the CCS status field in 6.

In the **Select Assessment Information for Policy Compliance** panel, specify the following information:

Assessment name field	Select the assessment name from the **Assessment name field** drop-down list. The **Assessment name field** list contains the assessments that are mapped to CCS from imported data. The assessment names appear in the **Assessment name field** field drop-down list only if you have selected the status and assessment fields while creating the data schema.
Assessment message field	Select the status field from the **Assessment message field** drop-down list. The **Assessment message field** list contains the status fields that are mapped to CCS from imported data. The Status field is used as the Assessment message field to display the evidence for the failed status in the Policy Results by Control report.

9 Click **Next**, and then on the **Summary of Correlation of data with CCS** panel, click **Finish**.

Reconciling assets based on external system data

You can use the reconciliation rules to add new assets, update existing asset fields and update the data schema. CCS supports the following rule types for data schema:

- Pre rule - The Pre rule is run before the data is imported into the external system data schema. The pre rule lets you set a temporary value to a particular field in the data schema for reconciliation.
- Add rule - The Add rule lets you add new assets to the asset system at a specific location.

- Update rule - An Update rule is applied on the existing assets to update the asset fields.

Use the reconciliation rules workspace to create data schema based reconciliation rules. For information on creating reconciliation rules, See “Creating reconciliation rules for external data” on page 812.

After you create the reconciliation rules for the data schema, use the **Set Asset Reconciliation** wizard to configure the external data system to use the reconciliation rules.

To set the reconciliation rules for external system

1. Go to **Manage > External Data Integration**.
2. From the **External Data Systems** list, select a data system, and then do one of the following:
   - From the taskbar, select **System Tasks > Set Asset Reconciliation**.
   - Right-click the data system and then select **Set Asset Reconciliation**.
3. In the **Set Asset Reconciliation** panel, click **Add Rules**.
4. In the **Select Reconciliation Rules** panel, expand the **Reconciliation Rules** node and then browse through the folders to select a data schema based rule.

   Note: The rules specific to only the selected external system data schema appear in the right-hand pane.

5. In the right-hand pane, select a rule and then click **Add** or **Add All** as per your requirement and then click **OK**.
6. In the **Set Asset Reconciliation** panel, click **OK**.
7. Use **Move Up** and **Move Down** to reorder the rules.
8. Use **Delete Rule** to remove the rules from the external data system.

Creating reconciliation rules for external data

You can use the reconciliation rules to add new assets, update existing asset fields and update the data schema.

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 or Edit Reconciliation Rule Wizard**, specify the following information and click **Next**.

Rule name	Lets you provide a name for the rule.
Description	Lets you provide a description for the rule.
Data schema	Lets you select the data schema of the external data system, for which you want to create the rule.
Rule type	Lets you select the rule type for the data schema. CCS supports the following rule types for data schema: ■ Pre Rule - The Pre rule is run before the data is imported into the external system data schema. The pre rule lets you set a temporary value to a particular field in the data schema for reconciliation. ■ Add Rule - The Add rule lets you add new assets to the asset system at a specific location. ■ Update Rule - An Update rule is applied on the existing assets to update the asset fields.
Save in	Lets you select a folder to save the rule.

4 The **Select Rule Conditions and Actions** panel, lets you add conditions and actions for the rule.

5 Click **Add Condition** to add a condition for the rule.

- If you have selected Pre Rule in Creating reconciliation rules for external data, from the **Condition type** drop-down list, select one of the following conditions:

Always	The condition is always passed and the related action is always executed.
If the incoming data field does not have value	Select the field of the data schema from the **Field** drop-down list. This condition is passed if the selected incoming data field does not have value.

If the incoming data field has a relation with a specified value	Specify the following information: ■ **Field** : Select the field of the data schema from the **Field** drop-down list. ■ **Operator**: Select the operator from the **Operator** drop-down list. ■ **Value**: In the **Value** text box specify a value for the field. This condition is passed if the selected field has the specified value.

- If you have selected Add Rule in Creating reconciliation rules for external data, from the **Condition type** drop-down list, select one of the following conditions:

If an asset does not exist	Specify the following information: ■ **Asset type**: Select the asset type for which you want to validate the condition. ■ **Asset field**: Select the asset field for the selected asset type. ■ **Operator**: Select the operator. ■ **Data schema field**: Select the data schema field against which you want to validate the condition for the selected Asset type. ■ **Add (+)**: Click **Add (+)** to add the expression. You can add multiple expressions for a condition. ■ **Match all fields**: If you add multiple expression, check **Match all fields** for the condition to pass, only if all expressions evaluate to true. **Note:** You must specify minimum one expression, to check non existence of the asset, for the condition to pass.

If the incoming data field has a relation with a specified value	Specify the following information: ■ **Field** : Select the field of the data schema from the **Field** drop-down list. ■ **Operator**: Select the operator from the **Operator** drop-down list. ■ **Value**: In the **Value** text box specify a value for the field. This condition is passed if the selected field has the specified value.
If the incoming data field has a value	Select the data field of the data schema from the **Field** drop-down list. This condition is passed if the selected incoming data field has a value.

- If you have selected Update Rule in Creating reconciliation rules for external data, from the **Condition type** drop-down list, select one of the following conditions:

If an asset exists	Specify the following information: ■ **Asset type**: Select the asset type for which you want to validate the condition. ■ **Asset field**: Select the asset field for the selected asset type. ■ **Operator**: Select the operator. ■ **Data schema field**: Select the data schema field against which you want to validate the condition for the selected Asset type. ■ **Add (+)**: Click **Add (+)** to add the expression. You can add multiple expressions for a condition. ■ **Match all fields**: If you add multiple expression, check **Match all fields** for the condition to pass, only if all expressions evaluate to true. **Note:** You must specify minimum one expression, to check existence of the asset, for the condition to pass.

If the incoming data field has a relation with a specified value	Specify the following information: ■ **Field** : Select the field of the data schema from the **Field** drop-down list. ■ **Operator**: Select the operator from the **Operator** drop-down list. ■ **Value**: In the **Value** text box specify a value for the field. This condition is passed if the selected field has the specified value.

6 Click **OK** to add the condition.

7 Click **Add Action** to add an action for the rule. You must add minimum one condition to add the related actions.

- If you have selected Pre Rule in Creating reconciliation rules for external data, from the **Action type** drop-down list, select the following action:

Set the field value of incoming data field as specified	Select the data field of the data schema from the **Field** drop-down list. In the **Value** text box specify a value for the field.

- If you have selected Add Rule in Creating reconciliation rules for external data, select the following action:

Create an asset and place the asset in the selected folder	Specify the following information: - **Asset type**: Select the asset type for which you want to set the value from the data schema. The mandatory asset fields are displayed in the grid. for each field, click **Edit** to map to matching data schema fields. If you do not have a matching data schema field, you can define a new value for the asset field. - **Asset field**: To add more asset fields, select the asset field for the selected asset type. - **Data schema field**: Select the data schema field whose value you want to assign to the selected asset field. - **Add (+)**: Click **Add (+)** to add the required values to the asset. You can add multiple asset - data schema mappings. - **Target Folder**: Select the target folder to save the created assets.

- If you have selected Update Rule in Creating reconciliation rules for external data, from the **Action type** drop-down list, select one of the following actions:

Correlate the incoming data with the asset	This action correlates the incoming data with the CCS assets.

Update the fields of an asset with the incoming date	Specify the following information: ■ **Asset type**: Select the asset type for which you want to set the value from the data schema. ■ **Asset field**: To add more asset fields, select the asset field for the selected asset type. ■ **Data schema field**: Select the data schema field whose value you want to assign to the selected asset field. ■ **Add (+)**: Click **Add (+)** to add the required values to the asset. You can add multiple asset - data schema mappings. ■ **Target Folder**: Select the target folder to save the created assets.

8. Click **Next**.
9. In the **Summary** panel, view the summary and then click **Finish**.

Viewing schema data

You can view the details about imported data from an external data system. You can also filter and export the external system schema data.

To view schema data

1. Go to **Manage > External Data Integration**.
2. From the **External Data Systems** list, select a data system and then do one of the following:
   - From the taskbar, select **System Tasks > View Schema Data**.

- Right-click the data system and then select **View Schema Data**.

3 The **Imported Data for <data system name>** panel displays the following:

Filter	Lets you create an expression to view the required data.
Maximum records per page	Lets you configure the number of records that you want to be displayed on each page.
Export	Lets you export the filtered data to a specified location.
Imported Data	Displays the imported data from the selected data system. The fields that you specify when you add the data system are displayed in this pane.

Filtering schema data

You can create an expression to view the required data that is imported from an external data system.

To filter schema data

1 Go to **Manage > External Data Integration**.

2 From the **External Data Systems** list, select a data system and then do one of the following:

- From the taskbar, select **System Tasks > View Schema Data**.
- Right-click the data system and then select **View Schema Data**.

3 In the **Imported Data for <data system name>** panel, click **Filter**.

4 Create an expression to filter data using the respective drop-down fields.

The first drop-down field contains all the field names of the data schema. The second drop-down field contains the operators that are used to create an expression. And the third drop-down field lets you specify the values for a field to create a filter.

5 Click Add (+) to add another expression.

You can add multiple expressions to filter data. Multiple expressions are combined using the AND operator between each expression.

6 Click **Apply** to filter the data.

Exporting schema data

You can export the data from an external data system, to a specified location.

To export schema data

1. Go to **Manage > External Data Integration**.
2. From the **External Data Systems** list, select a data system and then do one of the following:
   - From the taskbar, select **System Tasks > View Schema Data**.
   - Right-click the data system and then select **View Schema Data**.
3. In the **Imported Data for <data system name>** panel click **Export**.
4. In the **Save exported files to** dialog box, browse to the location where you want to export the data.
5. Enter the file name and select the appropriate save as type.

   You can export data in .xls, .doc, .pdf, .xml and .csv formats.
6. Click **Save** to export the data to the specified location.

Working with Symantec CCS Vulnerability Manager integration

Symantec Control Compliance Suite Vulnerability Manager is a unified vulnerability solution.

CCS Vulnerability Manager does the following:

- Scans the network to discover devices running on it.
- Probes vulnerabilities of the discovered devices.
- Discovers the data which is associated with each device. For example, installed software and services running on the devices.

CCS Vulnerability Manager generates the data which is mainly associated with the devices. The data comprises the list of scans which are performed on the network, discovered devices, and associated vulnerabilities for discovered devices.

Symantec CCS Vulnerability Manager integration lets you seamlessly assimilate the data from Symantec CCS Vulnerability Manager into Control Compliance Suite. It lets you represent the imported data by leveraging the CCS dashboards and reports.

With the imported data, you can do any of the following by using the Control Compliance Suite infrastructure:

- Import data and view it in dashboards without correlating to the assets in CCS.
- Import data and view it in dashboards in correlation with the assets present in CCS.
- Import data and use it for assessing the compliance posture in correlation with the assets.
- Import data and use it for asset risk score aggregation.

See "About importing data from Symantec CCS Vulnerability Manager" on page 821.

About importing data from Symantec CCS Vulnerability Manager

Symantec CCS Vulnerability Manager is a preconfigured system available in the External Data Integration workspace. To import data from CCS Vulnerability Manager, you should add a data connection.

You must have a dedicated user account for each CCS Vulnerability Manager data connection.

Using the CCS Vulnerability Manager data connection you can achieve the following:

- Provide the location and credentials to access the CCS Vulnerability Manager Server.
- Provide the scope for data import by selecting the Vulnerability Manager Sites and Groups.
- Provide a schedule for importing data.
- Configure notifications for success and failure of data import.
- Optionally add assets or update existing assets based on imported data by selecting reconciliation rules.

See "Adding a data connection to Symantec CCS Vulnerability Manager " on page 821.

Adding a data connection to Symantec CCS Vulnerability Manager

Use the **Symantec CCS Vulnerability Manager** data connection wizard to add the CCS Vulnerability Manager data Connection and import data into Control Compliance Suite.

To add the CCS Vulnerability Manager data connection

1 Go to **Manage** > **External Data Integration**.

2 From the External Data Systems list, select the **Symantec CCS Vulnerability Manager** system and then do one of the following:

- From the taskbar, select **System Tasks > Add Data Connection**.
- Right-click the **Symantec CCS Vulnerability Manager** system and then select **Add Data Connection**.

3 In the **Specify Connection Parameters for CCS Vulnerability Manager Server** panel, enter the following information, and then click **Test connection** to verify the connection to the CCS Vulnerability Manager Server.

The following message appears if the connection is available: Connection with the CCS Vulnerability Manager system is successful.

An error message appears if the connection is not available.

Connection name	Type the name for the instance of CCS Vulnerability Manager Server connection.
Computer name	Type the name of the computer that hosts the CCS Vulnerability Manager Server or its IP address.
Port	Type the port number on which the server is hosted.
User name	Type the user name to connect to the CCS Vulnerability Manager Server. The user account that you use must have appropriate permissions to connect to the CCS Vulnerability Manager Server.
Password	Type the password of the user account.

4 Click **Next** to continue.

5 In the **Specify CCS Vulnerability Manager Asset Groups and Sites** panel, select the asset groups and the sites for data import, and then click **Next**.

6 In the **Specify CCS Vulnerability Manager advanced settings** panel, do the following and then click **Next**.

The **Specify CCS Vulnerability Manager advanced settings** panel presents the following fields:

Connection timeout (Minutes)	Type the data connection timeout duration for CCS Vulnerability Manager server response.
Assets batch size for import	Type the number for batch size for asset import from CCS Vulnerability Manager to CCS. Batch size is the number of records that are imported in a batch in the database.

7 In the **Data Import Schedule** panel, do one of the following and then click **Next**.

The **Data Import Schedule** panel presents the following options:

Run now	The job runs immediately after the wizard closes.
Run periodically	The Run periodically options are as follows: ■ Start on Lets you select a date from the schedule to start a job run. ■ Run once Lets you run the job only one time on the specified date and time. ■ Run every # day(s). Lets you specify the number of days after which the job runs again automatically.

8 In the **Email Notification** panel, you must enter the notification information.

The **Email Notification** panel contains the following tabs:

- **Success**
- **Failure**

Both the tabs on this panel contain the same options and the options are stated as follows:

When you use email notifications, users receive notification on completion of the data import.

Send notification	Lets you send a notification for the data import job. You must select this check box to be able to enter the notification details.
Subject	Lets you specify the subject of the notification email. You can use the #JobName# token in the Subject of the notification.

Message

Lets you create a message to send. You can use tokens in the message.

Use Ctrl+Enter to go to the next line when you type the notification message.

You can use the following tokens when you create the message for a successful job:

- #Status#
  The success or the failure status of the job.
- #JobStart#
  The date and the time when the job starts.
- #JobSummary#
  The summary of the job.

You can use the following tokens when you create the message for a job failure:

- #FaultMessage#

From (Email ID)

Lets you specify the sender's email ID.

To (Email IDs)

Lets you specify the email ID of multiple recipients of the notification mail.

9 In the **Summary** panel, click **Finish**.

This panel provides the summary of Symantec CCS Vulnerability Manager data connection.

See “About External Data Integration view for Symantec CCS Vulnerability Manager” on page 828.

See “About monitoring jobs” on page 1050.

Editing a data connection to Symantec CCS Vulnerability Manager

Use the **Symantec CCS Vulnerability Manager** data connection wizard to edit the CCS Vulnerability Manager data Connection and import data into Control Compliance Suite.

To edit the CCS Vulnerability Manager data connection

1 Go to **Manage** > **External Data Integration**.

2 From the External Data Systems list, select the **Symantec CCS Vulnerability Manager** system and then do one of the following:

- From the taskbar, select **System Tasks > Edit Data Connection**.

- Right-click the **Symantec CCS Vulnerability Manager** system and then select **Edit Data Connection**.

3 In the **Specify Connection Parameters for CCS Vulnerability Manager Server** panel, enter the following information, and then click **Test connection** to verify the connection to the CCS Vulnerability Manager Server.

The following message appears if the connection is available: Connection with the CCS Vulnerability Manager system is successful.

An error message appears if the connection is not available.

Connection name	Edit the name for the instance of CCS Vulnerability Manager Server connection.
Computer name	Edit the name of the computer that hosts the CCS Vulnerability Manager Server or its IP address.
Port	Edit the port number on which the server is hosted.
User name	Edit the user name to connect to the CCS Vulnerability Manager Server. The user account that you use must have appropriate permissions to connect to the CCS Vulnerability Manager Server.
Password	Edit the password of the user account.

4 Click **Next** to continue.

5 In the **Specify CCS Vulnerability Manager Asset Groups and Sites** panel, select the asset groups and the sites for data import, and then click **Next**.

6 In the **Specify CCS Vulnerability Manager advanced settings** panel, do the following and then click **Next**.

The **Specify CCS Vulnerability Manager advanced settings** panel presents the following fields:

Connection timeout (Minutes)	Edit the data connection timeout duration for CCS Vulnerability Manager server response.
Assets batch size for import	Edit the number of assets that you want to be imported in one batch. The data for specified assets batch size is imported from CCS Vulnerability Manager into CCS.

7 In the **Data Import Schedule** panel, do one of the following and then click **Next**.

The **Data Import Schedule** panel presents the following options:

Run now	The job runs immediately after the wizard closes.
Run periodically	The Run periodically options are as follows: ■ Start on Lets you select a date from the schedule to start a job run. ■ Run once Lets you run the job only one time on the specified date and time. ■ Run every # day(s). Lets you specify the number of days after which the job runs again automatically.

8 In the **Email Notification** panel, you must enter the notification information.

The **Email Notification** panel contains the following tabs:

- **Success**
- **Failure**

Both the tabs on this panel contain the same options and the options are stated as follows:

When you use email notifications, users receive notification on completion of the data import.

Send notification	Lets you send a notification for the data import job. You must select this check box to be able to enter the notification details.
Subject	Lets you specify the subject of the notification email. You can use the #JobName# token in the Subject of the notification.

Message

Lets you create a message to send. You can use tokens in the message.

Use Ctrl+Enter to go to the next line when you type the notification message.

You can use the following tokens when you create the message for a successful job:

- #Status#
  The success or the failure status of the job.
- #JobStart#
  The date and the time when the job starts.
- #JobSummary#
  The summary of the job.

You can use the following tokens when you create the message for a job failure:

- #FaultMessage#

From (Email ID)

Lets you specify the sender's email ID.

To (Email IDs)

Lets you specify the email ID of multiple recipients of the notification mail.

9 In the **Summary** panel, click **Finish**.

This panel provides the summary of Symantec CCS Vulnerability Manager data connection.

See "About External Data Integration view for Symantec CCS Vulnerability Manager" on page 828.

See "About monitoring jobs" on page 1050.

Deleting a data connection to Symantec CCS Vulnerability Manager

You can delete a Symantec CCS Vulnerability Manager data connection from the **External Data Systems**.

To delete a data connection

1 Go to **Manage** > **External Data Integration**.

2 From the **External Data Systems**, select the **Symantec CCS Vulnerability Manager** system.

3 Select the data connection that you want to delete.

4 From the **Connection Tasks**, click **Delete Data Connection**.

See "Adding a data connection to Symantec CCS Vulnerability Manager " on page 821.

About External Data Integration view for Symantec CCS Vulnerability Manager

The **External Data Integration** view displays the preconfigured data systems and the external data systems that you add to CCS. You can access the External Data Integration view for CCS Vulnerability Manager by navigating through the **Manage > External Data Integration > Symantec CCS Vulnerability Manager** menu of the console.

The following table contains information on the options that are available on the taskbar of the External Data Integration view and their descriptions.

Table 31-3 Options in the External Data Integration taskbar and their descriptions

Options	Descriptions
Add Data Connection	Lets you add a new data connection. See "Adding a data connection to Symantec CCS Vulnerability Manager " on page 821.
Edit Data Connection	Lets you modify the configurations of an existing data connection. See "Editing a data connection to Symantec CCS Vulnerability Manager " on page 824.
Delete Data Connection	Lets you delete an existing data connection. See "Deleting a data connection to Symantec CCS Vulnerability Manager" on page 827.
Set Asset Risk Aggregation	Lets you configure asset risk aggregation.
Set Asset Reconciliation	Lets you configure the asset reconciliation rules for external data.
View Data	Lets you view the details about imported data from an external data system.

The following table contains information on the columns available in the **External Data Systems** pane.

Table 31-4 Columns in the **External Data Systems** pane and their descriptions

Column name	Description
External Data System Name	Displays the names of the external data systems that you have configured.
Description	Displays a description for the existing data system.
Data Schema	Displays the data schema names for which you import data from an external data system.
Data Connections	Displays the number of connections that have been configured for a data system.

The External Data Integration view displays the tabs based on the selection of a data system or a data connection.

The following table contains information on the columns that display if you select a data system.

Table 31-5 Columns that are available when you select Symantec CCS Vulnerability Manager and their descriptions

Columns	Descriptions
General	Displays a description of the selected data system.
Field Mapping	Displays the data field mappings for the selected data system.
Data Correlation	Displays the information that is related to data correlation for the selected data system.
Risk Aggregation	Displays the risk aggregation configurations for a selected data system.
Reconciliation Rules	Displays the reconciliation rules that are present for a selected data system.

The following table contains information on the columns that display if you select a data connection.

Table 31-6 Columns that are available when you select a data connection and their descriptions

Columns	Descriptions
General	Displays a description of the selected data connection.
Schedule	Displays the information on the schedule for the data import job that has been configured for the selected data connection.
Email Notification	Displays the information on the email notification configurations for the selected data connection.
Scope	Displays the asset groups and the sites that are selected as the scope for data import.
Advanced Settings	Displays the timeout interval for the data connection and the batch size of assets for the data import.

Viewing data system information in the details pane

You can view the information about the **Symantec CCS Vulnerability Manager** system in the details pane.

To view the data system information

1. Go to **Manage** > **External Data Integration**.
2. In the table pane, select the **Symantec CCS Vulnerability Manager** system for which you want to view the information.
3. View the information for the selected data system in the details pane.

The details pane displays all the information about the selected data system in the following tabs:

- General
- Field Mapping
- Data Correlation
- Risk Aggregation
- Reconciliation rules

See "About External Data Integration view for Symantec CCS Vulnerability Manager" on page 828.

Viewing data connection information in the details pane

You can view the information about the connection in the details pane.

To view the data connection information

1. Go to **Manage** > **External Data Integration**.
2. In the table pane, select the **Symantec CCS Vulnerability Manager** connection for which you want to view the information.
3. View the information for the selected data connection in the details pane.

The details pane displays all the information about the selected data connection in the following tabs:

- General
  See "Data connection details pane - General tab" on page 831.
- Schedule
- Email Notification
- Scope
  See "Data connection details pane - Scope tab" on page 832.
- Advanced Settings
  See "Data connection details pane - Advanced Settings tab" on page 832.

See "About External Data Integration view for Symantec CCS Vulnerability Manager" on page 828.

Data connection details pane - General tab

The General tab of the data connection details pane provides general information about the selected data connection.

The General tab contains the following details about the data connection:

Connection name	Displays the name for the instance of CCS Vulnerability Manager Server connection.
Computer name	Displays the name of the computer that hosts the CCS Vulnerability Manager Server or its IP address.
Port	Displays the port number on which the server is hosted.
User name	Displays the user name to connect to the CCS Vulnerability Manager Server.

See "Viewing data connection information in the details pane" on page 831.

Data connection details pane - Scope tab

The **Scope** tab of the data connection details pane provides data import scope information about the selected asset groups and sites.

The **Scope** tab contains the following details about the assets groups and the sites:

Name	Displays the names of the asset groups and the sites.
Type	Displays the type of data whether all asset groups or all sites.

See "Viewing data connection information in the details pane" on page 831.

Data connection details pane - Advanced Settings tab

The **Advanced Settings** tab of the data connection details pane provides advanced settings information about the timeout interval and the assets batch size.

The **Advanced Settings** tab contains the following details about the timeout interval and the assets batch size:

Timeout interval	Displays the data connection timeout interval for the server response.
Batch size for import	Displays the batch size for asset import from into CCS.

See "Viewing data connection information in the details pane" on page 831.

About the Vulnerability Assessment data schema

CCS represents the vulnerability assessment data in the form of a data schema. The data that is imported from Symantec CCS Vulnerability Manager is mapped to the data schema.

CCS consumes the Vulnerability Assessment data schema for the following:

- To correlate target information available in vulnerability assessment data with assets in CCS.
- To create reconciliation rules for adding assets and for updating assets in CCS based on vulnerability assessment data.
- To create panels based on vulnerability assessment data.

- To create assessment procedures based on the vulnerability assessment data for assessing the compliance posture.
- To identify the vulnerability definitions from the data that can be mapped to control statements.
- To specify the asset risk score aggregation based on the vulnerability assessment data.

CCS provides a default mapping between CCS Vulnerability Manager fields and Vulnerability Assessment data schema which is provided by CCS.

See "About the data mapping of Vulnerability Assessment data schema and Symantec CCS Vulnerability Manager fields" on page 838.

Table 31-7is described as follows:

Table 31-7 Vulnerability Assessment data schema

Field Name	Data Type	Description
Evaluation Date	DateTime	The date on which data evaluation is performed by CCS Vulnerability Manager.
Vulnerability Assessment Status	Text	The status of vulnerability assessment.
Vulnerability Assessment Date	DateTime	The date on which vulnerability assessment is performed by CCS Vulnerability Manager.
Vulnerability Assessment Evidence	Text	The evidence of vulnerability assessment.
Vulnerability Instances	Integer	The number of occurrences of vulnerability on the selected devices.
Device Port	Integer	The service port on which vulnerability is found.
Scan Identifier	Text	The record identifier of a scan.
Service Name	Text	The service name on which vulnerability is found.
Vulnerability Identifier	Text	The record identifier of a vulnerability.

Table 31-7 Vulnerability Assessment data schema *(continued)*

Field Name	Data Type	Description
Vulnerability Name	Text	The name of a vulnerability.
Vulnerability Description	Text	The description of a vulnerability.
Vulnerability Published Date	DateTime	The date on which a vulnerability is published.
Vulnerability Added Date	DateTime	The date on which a vulnerability is added.
Vulnerability Modified Date	DateTime	The date on which a vulnerability is modified.
Vulnerability CVSS Vector	Text	The measurement of vulnerability severity, urgency, and priority of response.
Vulnerability CVSS Access Complexity	Text	The measurement of the complexity of the attack required to exploit the vulnerability once an attacker has gained access to the target system. The lower the required complexity, the higher the vulnerability score. The possible values for this field are as follows: ■ High (H) ■ Medium (M) ■ Low (L)

Table 31-7 Vulnerability Assessment data schema *(continued)*

Field Name	Data Type	Description
Vulnerability CVSS Access Vector	Text	The measurement of vulnerability usage. The more remote an attacker can be to attack a host, the greater the vulnerability score. The possible values for this field are as follows: ■ Local Access (L) ■ Adjacent Network (A) ■ Network (N)
Vulnerability CVSS Authentication	Text	The frequency by which an attacker must authenticate to a target to exploit a vulnerability. The fewer authentication instances that are required, the higher the vulnerability score. The possible values for this field are as follows: ■ Multiple (M) ■ Single (S)
Vulnerability CVSS Availability Impact	Text	The measurement of the impact to availability of a successfully exploited vulnerability. Increased availability impact increases the vulnerability score. The possible values for this field are as follows: ■ None (N) ■ Partial (P) ■ Complete (C)

Table 31-7 Vulnerability Assessment data schema *(continued)*

Field Name	Data Type	Description
Vulnerability CVSS Confidentiality Impact	Text	The measurement of the effect on confidentiality of a successfully exploited vulnerability. Increased confidentiality impact increases the vulnerability score. The possible values for this field are as follows: ■ None (N) ■ Partial (P) ■ Complete (C)
Vulnerability CVSS Integrity Impact	Text	The measurement of the impact to integrity of a successfully exploited vulnerability. Increased integrity impact increases the vulnerability score. The possible values for this field are as follows: ■ None (N) ■ Partial (P) ■ Complete (C)
Vulnerability CVSS Score	Decimal	It provides standard severity ratings of software vulnerabilities. CVSS 2.0 'base score' as a severity rating out of 10 (0 is low, 10 is high) and a risk ranking of "Low", "Medium" or "High".
Vulnerability CVSS Score Range	Text	It represents a particular range of CVSS score for a vulnerability.
Vulnerability Severity	Decimal	It represents the severity of a vulnerability.

Table 31-7 Vulnerability Assessment data schema *(continued)*

Field Name	Data Type	Description
Vulnerability PCI Severity	Decimal	The measurement of assignment of each confirmed vulnerability and potential vulnerability PCI severity level. The severity level is based on the CVSS score assigned to the vulnerability.
Vulnerability References	Text	Vulnerability References are additional references provided by network scan.
Vulnerability Remediation	Text	The measurement of the level of an available solution.
Vulnerability Assessment Status Category	Text	The category of vulnerability assessment status.
Device Status	Text	The device status that indicates whether device is alive.
Device Fully Qualified Name	Text	The fully qualified name of a device.
Device Hardware Address	Text	The hardware address of a device.
Device Operating System Architecture	Text	The information of operating system architecture of a device.
Device Operating System Category	Text	The operating system of a device.
Device Operating System Subcategory	Text	The subcategory of operating system of a device.
Device Operating System Type	Text	The type of operating system of a device.
Device Operating System Vendor	Text	The vendor of operating system of a device.

Table 31-7 Vulnerability Assessment data schema *(continued)*

Field Name	Data Type	Description
Device Operating System Version	Text	The version of the Operating System for a device.
CCS VM Site Identifier	Text	The identifier of a site for CCS Vulnerability Manager.
CCS VM Site Name	Text	The name of a site for CCS Vulnerability Manager.
CCS VM Site Description	Text	The description of a site for CCS Vulnerability Manager.
Device Risk Score Per CCS VM Site	Decimal	The device risk score that is obtained from external data system.
Device Host Name	Text	The host name of a device.
Device IP Address	Text	The IP address of a device.

About the data mapping of Vulnerability Assessment data schema and Symantec CCS Vulnerability Manager fields

CCS provides the default mapping of Vulnerability Assessment data Schema and CCS Vulnerability Manager fields.

Table 31-8 is described as follows:

Table 31-8 Data Mapping of Vulnerability Assessment data schema and CCS Vulnerability Manager fields

Vulnerability Assessment Data Schema Field Name	CCS Vulnerability Manager Field Name
Evaluation Date	Import Date
Vulnerability Assessment Status	Vulnerability Assessment Status
Vulnerability Assessment Date	Vulnerability Assessment Date
Vulnerability Assessment Evidence	Vulnerability Assessment Evidence
Vulnerability Instances	Vulnerability Instances
Device Port	Vulnerability Assessment Port

Table 31-8 Data Mapping of Vulnerability Assessment data schema and CCS Vulnerability Manager fields *(continued)*

Vulnerability Assessment Data Schema Field Name	CCS Vulnerability Manager Field Name
Scan Identifier	Scan Identifier
Service Name	Vulnerability Assessment Service Name
Vulnerability Identifier	Vulnerability Identifier
Vulnerability Name	Vulnerability Title
Vulnerability Description	Vulnerability Description
Vulnerability Published Date	Vulnerability Published Date
Vulnerability Added Date	Vulnerability Added Date
Vulnerability Modified Date	Vulnerability Modified Date
Vulnerability CVSS Vector	Vulnerability CVSS Vector
Vulnerability CVSS Access Complexity	Vulnerability CVSS Access Complexity
Vulnerability CVSS Access Vector	Vulnerability CVSS Access Vector
Vulnerability CVSS Authentication	Vulnerability CVSS Authentication
Vulnerability CVSS Availability Impact	Vulnerability CVSS Availability Impact
Vulnerability CVSS Confidentiality Impact	Vulnerability CVSS Confidentiality Impact
Vulnerability CVSS Integrity Impact	Vulnerability CVSS Integrity Impact
Vulnerability CVSS Score	Vulnerability CVSS Score
Vulnerability CVSS Score Range	Vulnerability CVSS Score Range
Vulnerability Severity	Vulnerability Severity
Vulnerability PCI Severity	Vulnerability PCI Severity
Vulnerability References	Vulnerability References
Vulnerability Remediation	Vulnerability Solution
Vulnerability Assessment Status Category	Vulnerability Assessment Status Category
Device Status	Asset Status
Device Fully Qualified Name	FQDN

Table 31-8 Data Mapping of Vulnerability Assessment data schema and CCS Vulnerability Manager fields *(continued)*

Vulnerability Assessment Data Schema Field Name	CCS Vulnerability Manager Field Name
Device Hardware Address	Hardware Address
Device Operating System Architecture	Operating System Architecture
Device Operating System Category	Operating System Class
Device Operating System Subcategory	Operating System Family
Device Operating System Type	Device Operating System Type
Device Operating System Vendor	Operating System Vendor
Device Operating System Version	Operating System Version
CCS VM Site Identifier	Site Identifier
CCS VM Site Name	Site Name
CCS VM Site Description	Site Description
Device Risk Score Per CCS VM Site	Asset Risk Index Per Site
Device Host Name	Host Name
Device IP Address	IP Address

About the predefined reconciliation rules for Symantec CCS Vulnerability Manager

CCS provides the predefined Add and Update rules as a part of the Symantec CCS Vulnerability Manager integration. You can use these reconciliation rules to add or update the assets in CCS before creating a data connection to import the vulnerability assessment data.

You can view all the Add and Update rules at the following location in the CCS workspace:

Manage > **Reconciliation Rules** > **Pre-defined Rules** > **Data Schema Driven** > **Symantec CCS Vulnerability Manager**.

The following table lists all the predefined reconciliation rules, their descriptions, and their type.

Table 31-9 Predefined reconciliation rules for Symantec CCS Vulnerability Manager

Rule Name	Description	Type of Rule	Rule Definition
Add UNIX Machine	Add UNIX Machine while importing data from Symantec CCS Vulnerability Manager.	Add	IF Device Operating System Subcategory equals Linux AND UNIX Machine asset does not exist where {(Machine Name equals Device Host Name) OR (IP Address equals Device IP Address)} THEN Create UNIX Machine asset using {(Machine Name with Device Host Name), (IP Address with Device IP Address), (Operating System with Device Operating System Type), (Operating Distribution Field with [Undefined]), (Operating System Version with Device Operating System Version)} and place the asset in the Asset System folder

Table 31-9 Predefined reconciliation rules for Symantec CCS Vulnerability Manager *(continued)*

Rule Name	Description	Type of Rule	Rule Definition
Add Windows Machine	Add Windows Machine while importing data from Symantec CCS Vulnerability Manager.	Add	IF Device Operating System Subcategory contains Windows AND Windows Machine asset does not exist where {(Machine Name equals Device Host Name) OR (Host Name (DNS) equals Device Fully Qualified Name)} THEN Create Windows Machine asset using {(Domain/Workgroup Name with [Undefined]), (Machine Name with Device Host Name), (OS Major Version Number with 0), (OS Minor Version Number with 0), (OS Type with Device Operating System Type), (Machine Is Server with False), (Machine Is PDC with False), (Machine Is BDC with False), (TCP/IP Addresses <LIST> with Device IP Address), (Host Name (DNS) with Device Fully Qualified Name)} and place the asset in the Asset System folder
Update Windows Machine IP Address	Update Windows Machine IP Address while importing data from Symantec CCS Vulnerability Manager.	Update	IF Windows Machine asset exists where {(Machine Name equals Device Host Name)} THEN Update the fields of Windows Machine asset with the incoming data {(TCP/IP Addresses <LIST> with Device IP Address)}

Viewing the vulnerability assessment data in the dashboard

After you import the vulnerability assessment data, CCS consumes the data to generate dashboard panels. You can create the dashboard panels by selecting Symantec Vulnerability Assessment as the area of interest.

CCS displays the following predefined dashboard panels for the vulnerabilities:

- Aggregated risk score by CCS Vulnerability Manager sites
- Top 10 Most Common Network Vulnerabilities
- Vulnerabilities by CVSS Score Range
- Vulnerabilities by Severity

Viewing the vulnerability assessment data in the policy compliance report

After you import the vulnerability assessment data, you can view the data in the following policy reports for compliance:

- Comparison of control statement mapping
- Policy compliance by assets
- Policy control statements mapping
- Policy results by controls

About asset risk aggregation using the vulnerability assessment data

The risk score is calculated for an asset based on vulnerability assessment data by using CCS risk scoring algorithm. CCS uses the scoring guidelines published by Common Vulnerability Scoring System (CVSS 2.0) to calculate the risk scores for the assets based on vulnerabilities found on those assets. Every vulnerability has a CVSS base score associated with it. CCS uses the base metrics model of CVSS to calculate the risk scores for the assets.

The rick score can also be calculated using assessment procedures.

Note: For **External Data Integration > Symantec CCS Vulnerability Manager > Set Asset Risk Aggregation**, do not select the option, **Use scores from incoming data** to calculate the asset risk score. Select the option, **Use CCS to calculate the risk score**.

About consuming vulnerability assessment data for compliance

You can map the vulnerability assessment procedures to control statements and control statements to mandates, regulations, or policies. CCS generates the evidence for vulnerability assessment related external data assessments. Based on the mappings and evidence, CCS generates the policy compliance related reports and dashboards.

About procedures for vulnerability assessment data

The following two assessment procedures are available on the Symantec Vulnerability Assessment data schema

- Vulnerability with risk score greater than or equal to 4.

  The procedure evaluates each asset in the scope of data import. The procedure finds whether a vulnerability with risk score greater than or equal to 4 exists on that asset. If the condition is met, the assessment procedure evaluates to Fail otherwise it Passes. Evidence is generated for the asset which fails the assessment.

  The expression for this assessment procedure is, [Vulnerability Assessment Status = Vulnerable] AND [Vulnerability CVSS Score > = 4].

- Vulnerability without risk score

  The procedure evaluates each asset in the scope of data import.The procedure finds whether a vulnerability without CVSS Score exists on that asset. If the condition is met, the assessment procedure evaluates to Fail otherwise it Passes. Evidence is generated for the asset which fails the assessment.

  The expression for this assessment procedure is, [Vulnerability CVSS Score < 0] OR [Vulnerability CVSS Score IS NULL].

About the suggested mappings to control statements

External data assessments in CCS are mapped to Policies by using control statements. Vulnerability assessment related controls need mapping to the respective policies that are related to vulnerability assessment. For the external data assessments that are based on CCS Vulnerability Manager data, CCS provides the mapping suggestions. You can use the mapping suggestions for mapping the external data assessments with CCS Policies.

Scenarios for the vulnerability assessment data integration

You can plan the vulnerability assessment data integration based on the following business objectives:

- Do you want to import vulnerability assessment data and view it in dashboards without correlating to the assets in CCS?
- Do you want to import vulnerability assessment data and view it in dashboards in correlation with the assets in CCS?
- Do you want to import vulnerability assessment data and use it for assessing the compliance posture in correlation with the assets in CCS?
- Do you want to import vulnerability assessment data and use it for asset risk score aggregation?

Table 31-10 Vulnerability assessment data integration model based on your business objective

Scenario	Description	What you need to do
Import vulnerability assessment data and view it in dashboards without correlating to the assets in CCS.	You have to create a data connection to CCS Vulnerability Manager to import the vulnerabilities assessment data into CCS. You can view the imported data directly in the Dashboard panels.	To meet this business goal, you need to do the following: ■ Import vulnerability assessment data. ■ View imported data in the following predefined panels: ■ Aggregated risk score by CCS Vulnerability Manager Sites ■ Top 10 Most Common Network Vulnerabilities ■ Vulnerabilities by CVSS Score Range ■ Vulnerabilities by Severity See "Viewing the vulnerability assessment data in the dashboard" on page 843.

Table 31-10 Vulnerability assessment data integration model based on your business objective *(continued)*

Scenario	Description	What you need to do
Import vulnerability assessment data and view it in dashboards in correlation with the assets in CCS.	You have to create a data connection to CCS Vulnerability Manager to import the vulnerabilities assessment data into CCS. You can view the imported data directly in the Dashboard panels by selecting appropriate asset fields.	To meet this business goal, you need to do the following: ■ Import vulnerability assessment data. ■ Create a panel by selecting Symantec Vulnerability Assessment as the area of interest. ■ Select any of the fields starting with Asset in the display name as the measure or the dimension. The following panel shows the data that is correlated with assets in CCS: ■ Panel Name: Top 10 Count of Vulnerability ID by Asset Name ■ Measure (Y-Axis): Vulnerability ID (Count) ■ Dimension (X-Axis): Asset Name ■ Filter: Assessment Status = Vulnerable ■ Description: This panel shows the top 10 assets with highest number of vulnerabilities found.

Table 31-10 Vulnerability assessment data integration model based on your business objective *(continued)*

Scenario	Description	What you need to do
Import vulnerability assessment data and use it for assessing the compliance posture in correlation with the assets in CCS.	You can use reconciliation rules for adding or updating the assets in CCS before creating a data connection to import data. Then you have to map the vulnerability assessment procedures to control statements and control statements to mandates, regulations, or policies. Finally, the data can be viewed in mandate-based panels or reports.	

Table 31-10 Vulnerability assessment data integration model based on your business objective *(continued)*

Scenario	Description	What you need to do
		To meet this business goal, you need to do the following: ■ Create asset reconciliation rules based on the Vulnerability Assessment data schema. ■ Import vulnerability assessment data. ■ Map the Vulnerability Assessment data schema based on the assessment procedures or vulnerabilities to control statements. ■ Map the control statements to required mandates, regulations, or policies. ■ View the data in the following panels and reports: Mandate-based panels: ■ Control Status by Assets for Mandates ■ Control Status for Mandates ■ Control Status Trends for Mandates ■ Top 10 Failed Control Statements for Mandates Policy panels: ■ Breakdown of Policies by Status ■ Control Status by Assets for Policies ■ Control Status for Policies ■ Control Status for

Table 31-10 Vulnerability assessment data integration model based on your business objective *(continued)*

Scenario	Description	What you need to do
		Policy ■ Top 10 Assets with Highest Risk Score by Policy ■ Top 10 Failed Control Statements for Policies ■ User Acceptance of policies ■ Control status Trends for policies Policy reports: ■ Comparison of control statement mapping ■ Policy compliance by assets ■ Policy control statements mapping ■ Policy results by controls See "Viewing the vulnerability assessment data in the policy compliance report" on page 843.

Table 31-10 Vulnerability assessment data integration model based on your business objective *(continued)*

Scenario	Description	What you need to do
Import vulnerability assessment data and use it for asset risk score aggregation.	You can use reconciliation rules for adding or updating the assets in CCS before creating a data connection to import data. CCS calculates the asset risk score that you can view from the Asset Preview pane.	To meet this business goal, you need to do the following: ■ Create Vulnerability Assessment data schema based on the asset reconciliation rules. ■ Import vulnerability assessment data. ■ Go to **Asset System** > **General** tab of the details pane. Click **Risk Score** to see the exact risk score which is contributed by CCS Vulnerability Manager to the asset risk score.

Working with Symantec Response Assessment Module integration

Symantec Response Assessment Module (RAM) is a unified solution that provides various questionnaires. These questionnaires help you assess the user responses and create the response assessment data. You can use the response assessment data to improve your business processes.

RAM Integration lets you seamlessly assimilate the response assessment data from Symantec Response Assessment Module into Control Compliance Suite. It lets you represent the imported data by leveraging the CCS dashboards and reports.

With the imported data, you can do any of the following by using the Control Compliance Suite infrastructure:

- Import data and view it in dashboards without correlating to the assets in CCS.
- Import data and view it in dashboards in correlation with the assets present in CCS.
- Import data and use it for assessing the compliance posture in correlation with the assets.

See "About importing data from Symantec Response Assessment Module" on page 851.

Before you begin the Symantec Response Assessment Module integration, you can review the information in the *Symantec Response Assessment Module User Guide*

About importing data from Symantec Response Assessment Module

Symantec Response Assessment Module is a preconfigured system available in the External Data Integration workspace. To import data from Symantec Response Assessment Module, you should add a data connection.

You must have an ODBC data location created which stores the RAM database location and the credentials to access the database.

Using the data connection you can achieve the following:

- Provide the ODBC data location for RAM database or create a new data location and specify the table or the view name as RAM.CCS Evidence.
- Provide a schedule for importing data.
- Configure notifications for success and failure of data import.

Use the Add Data Connection wizard to add the RAM data Connection and import data into Control Compliance Suite.

After you add the data connection, a new data connection appears for Symantec Response Assessment Module System in the External Data Integration workspace.

About the Response Assessment data schema

CCS represents the response assessment data in the form of a data schema. The data that is imported from Symantec Response Assessment Module is mapped to the Response Assessment data schema.

CCS provides a default mapping between the RAM fields and Response Assessment data schema which is provided by CCS.

See "About the data mapping of Response Assessment data schema and RAM fields" on page 854.

Table 31-11 Response Assessment Data Schema

Field Name	Data Type	Description
Asset Identifier	GUID	A unique identifier of the asset which is associated with the user's response.
User or Asset Identifier	GUID	This field either contains the User identifier or the asset identifier depending on the type of record.
User Name	Text	The name of a user who responded to the questionnaire. The field is blank for the asset-based records.
Class Type	Text	A category to classify the user based and the asset-based records.
Question Identifier	GUID	The unique identifier of a question.
Question	Text	The name of a question.
Questionnaire Identifier	GUID	A unique identifier of a questionnaire.
Questionnaire	Text	The instance of a questionnaire.
Questionnaire Group Name	Text	The group name of a questionnaire.
Question Type	Text	The type of a question.
Question Importance	Text	It is a priority of the question, which is either of the following ■ Disabled ■ Low ■ Medium ■ High ■ Highest

Table 31-11 Response Assessment Data Schema *(continued)*

Field Name	Data Type	Description
Severity	Text	The weight of the answer that is given by the user. It is either of the following ■ Minimal ■ Moderate ■ Severe ■ Very severe ■ Extreme
Normalized Severity	Decimal	Normalized Severity is a comparison assessment of RAM severity with CCS severity.
Evidence Identifier	GUID	A unique identifier of an evidence.
Comments	Text	The comments provided by the user as a response.
Recommendations	Text	The recommendations provided by the user as a response.
Exceptions	Text	The asset name exceptions requested by the user while answering the CCS asset-based questionnaires.
Answer	Text	The answer that user has provided as a response.

Table 31-11 Response Assessment Data Schema *(continued)*

Field Name	Data Type	Description
Pass State	Bit	The state of user response. The state is Passed for the correct user response. The possible values are as follows: ■ NULL (The value for correlated or grouped records.) ■ 0 (Fail value for non-correlated records.) ■ 1 (Pass value for non-correlated records.)
CCS Status	Integer	The status displayed by CCS on user response. The possible values are as follows: ■ -1 (The value for non-correlated records.) ■ 1 (Fail value for correlated records.) ■ 0 (Pass for correlated records.)
Evidence Created Date	DateTime	The data on which evidence is created.

About the data mapping of Response Assessment data schema and RAM fields

Symantec RAM Integration provides the default mapping of Response Assessment data schema and RAM fields.

Data Mapping of Response Assessment data schema and RAM fields is provided as follows:

Table 31-12 Data Mapping of Response Assessment data schema and RAM fields

Response Assessment Data Schema Field Name	RAM Field Name
Asset Identifier	AssetID
User or Asset Identifier	UserGUID
User Name	UserName
Class Type	ClassType
Question Identifier	QuestionGUID
Question	Question
Questionnaire Identifier	QuestionnaireGUID
Questionnaire	Questionnaire
Questionnaire Group Name	GroupName
Question Type	QuestionType
Question Importance	Importance
Severity	Severity
Normalized Severity	RAMSeverity
Evidence Identifier	EvidenceGUID
Comments	Comments
Recommendations	Recommendations
Exceptions	Exceptions
Answer	Answer
Pass State	PassState
CCS Status	Status
Evidence Created Date	CreatedDate

Viewing the response assessment data in the dashboard

After response assessment data is imported, you can create dashboard panels.

For example, you can create the panels by selecting Symantec Response Assessment Module as the area of interest.

Panel based on the data without asset correlation:

Panel Name	Count Answer by UserName, PassState
Measure (Y-Axis)	Answer
Dimension (X-Axis)	UserName and PassState
Description	The panel displays the information of the total number of answers with respect to the user names and the Pass state.

Panel Name	Count Answer by Question, PassState
Measure (Y-Axis)	Answer
Dimension (X-Axis)	Question and PassState
Description	The panel displays the information of the total number of answers with respect to the questions and the Pass state.

Panel based on the data with asset correlation:

Panel Name	Count Question by Asset Name, CCSStatus
Measure (Y-Axis)	Question
Dimension (X-Axis)	Asset Name and CCSStatus
Description	The panel displays the information of the total number of questions with respect to the asset names and the CCS status.

Viewing the response assessment data in the policy compliance report

After you import the response assessment data, you can view the data in the following policy reports for compliance:

- Comparison of control statement mapping
- Policy compliance by assets
- Policy control statements mapping
- Policy results by controls

Scenarios for the response assessment data integration

You can plan the response assessment data integration based on the following business objectives:

- Do you want to import response assessment data and view it in dashboards without correlating to the assets in CCS?
- Do you want to import response assessment data and view it in dashboards in correlation with the assets in CCS?
- Do you want to import response assessment data and use it for assessing the compliance posture in correlation with the assets in CCS?

Table 31-13 Response assessment data integration model based on your business objective

Scenario	Description	What you need to do
Import response assessment data and view it in dashboards without correlating to the assets in CCS.	You have to create a data location and a data connection to Response Assessment Module to import the response assessment data into CCS. You can view the imported data directly in the Dashboard panels.	To meet this business goal, you need to do the following: ■ Import response assessment data. ■ Create panels based on response assessment data. See "Viewing the response assessment data in the dashboard" on page 855.

Table 31-13 Response assessment data integration model based on your business objective *(continued)*

Scenario	Description	What you need to do
Import response assessment data and view it in dashboards in correlation with the assets in CCS.	You have to create a data location and a data connection to Response Assessment Module to import the response assessment data into CCS. You can view the imported data directly in the Dashboard panels by selecting appropriate asset fields.	To meet this business goal, you need to do the following: ■ Import response assessment data. ■ Create a panel by selecting Symantec Response Assessment Module as the area of interest. ■ Select any of the fields starting with Asset in the display name as the measure or the dimension. See "Viewing the response assessment data in the dashboard" on page 855.

Table 31-13 Response assessment data integration model based on your business objective *(continued)*

Scenario	Description	What you need to do
Import response assessment data and use it for assessing the compliance posture in correlation with the assets in CCS.	You have to create a data location and a data connection to Response Assessment Module to import the response assessment data into CCS. The response assessment data contains the identifiers or the Asset IDs. Then you have to map the questions to mandates, regulations, or policies. Finally, the data can be viewed in mandate-based panels or reports.	

Table 31-13 Response assessment data integration model based on your business objective *(continued)*

Scenario	Description	What you need to do
		To meet this business goal, you need to do the following: ■ Import response assessment data. ■ Map the questions to the control statements. ■ Map the control statements to required mandates, regulations, or policies. ■ View the data in the following panels and reports: Mandate-based panels: ■ Control Status by Assets for Mandates ■ Control Status for Mandates ■ Control Status Trends for Mandates ■ Top 10 Failed Control Statements for Mandates Policy panels: ■ Breakdown of Policies by Status ■ Control Status by Assets for Policies ■ Control Status for Policies ■ Control Status for Policy ■ Top 10 Assets with Highest Risk Score by Policy ■ Top 10 Failed Control Statements for Policies ■ User Acceptance of

Table 31-13 Response assessment data integration model based on your business objective *(continued)*

Scenario	Description	What you need to do
		policies ■ Control status Trends for policies Policy reports: ■ Comparison of control statement mapping ■ Policy compliance by assets ■ Policy control statements mapping ■ Policy results by controls See "Viewing the response assessment data in the policy compliance report" on page 856.

Working with Symantec Data Loss Prevention Integration

Symantec Data Loss Prevention enables you to do the following:

- Locate confidential information on file and Web servers, in databases, and on endpoints like, desktop and laptop systems.
- Protect confidential information through quarantine.
- Monitor network traffic for transmission of confidential data.
- Monitor the use of sensitive data on endpoint computers.
- Prevent transmission of confidential data to outside locations.
- Automatically enforce data security and encryption policies.

The Symantec Data Loss Prevention integration lets you seamlessly import incident data from Symantec Data Loss Prevention into Control Compliance Suite. It lets you represent the imported data in dashboards and reports by leveraging the CCS features.

With the imported data, you can do any of the following by using the Control Compliance Suite infrastructure:

- Import incidents data from the saved reports in Symantec Data Loss Prevention and view it in Dashboards without correlating the data with assets in CCS.
- Import incidents data from the saved reports in Symantec Data Loss Prevention and view it in Dashboards after correlating the data with assets in CCS.
- Import incidents data from the saved reports in Symantec Data Loss Prevention and view it in policy compliance reports after correlating assets in CCS.

See "About importing data from the Symantec Data Loss Prevention" on page 862.

About importing data from the Symantec Data Loss Prevention

The Symantec Data Loss Prevention (DLP) is a pre-integrated system available in the External Data Integration workspace. To import the incident data from DLP, you must create a data connection between your DLP deployment and CCS.

You must also enable and configure the DLP Web Services before you import the DLP incident data into CCS.

The user account that is configured for the connection must have the Reporting API Web Service access permission.

When you create the Symantec Data Loss Prevention data connection, you do the following:

- Specify the address and the credentials that is used to contact the DLP Enforce Server.
  Use the following formats to specify the credentials:
  - <username>
  - <role name>\<username>
  - <username>:<domain name>
    For example, `user1:mydomain`
  - <role name>\<username>:<domain name>
    For example, `role\user1:mydomain`
- Specify the DLP reports to collect incident data from.
- Create a schedule for importing the incidents data.
- Configure email notification to inform about the success and failure of the data import.

After you add a data connection, the new data connection appears under the Symantec Data Loss Prevention system in the External Data Integration workspace.

A new external data integration job with the specified data connection name is created which imports the incidents data in CCS.

See “Adding the Symantec Data Loss Prevention connection” on page 863.

Adding the Symantec Data Loss Prevention connection

You must add a Symantec Data Loss Prevention connection (DLP) to import the Symantec DLP incident data into Control Compliance Suite (CCS).

Use the **Add Data Connection** wizard to add a connection.

To add the Data Loss Prevention connection

1 Go to **Manage > External Data Integration**.

2 Select **Symantec Data Loss Prevention** from the list of pre-integrated external data systems.

3 Click **Add Data Connection**.

4 In the **Specify the Symantec Data Loss Prevention Enforce Server Connection** panel, provide the following information, and then click **Next**:

Connection name	Specify a name for the data connection. The following special characters are not supported in the connection name: * ( ) \ / , + " > < ; = # A new external data integration job with the specified data connection name is created which imports the incidents data in CCS.
Computer name	Type the name of the computer that hosts the Symantec DLP Enforce Server.
Port	Type the port number that the Web service uses on the Enforce Server host. The default port number is 443.

User name

Type the user name that is used to connect to the Enforce Server .

Use the following formats to specify the credentials:

- <username>
- <role name>\<username>
- <username>:<domain name>
  For example, `user1:mydomain`
- <role name>\<username>:<domain name>
  For example, `role\user1:mydomain`

Note: The user account that you use must have the Reporting API Web Service access permission to successfully connect to the Symantec DLP Enforce Server.

Password

Provide the password of the Enforce Server to go to the next panel.

Click **Test Connection** to verify that the connection to the DLP Enforce Server . A message is displayed to show the success or failure of the connection.

5 In the **Specify the Symantec Data Loss Prevention Saved Reports for Incident Collection** panel, do one of the following, and then click **Next**:

Add

Click **Add** to open the **Add Report Details** dialog box.

Add the saved report IDs that the DLP connection must use to collect the incident data.

Modify

Click an existing saved report ID then click **Modify** to open the **Modify Report Details** dialog box.

The **Modify Report Details** dialog box lets you modify the description of an existing report.

Remove

Click an existing saved report ID then click **Remove** to delete a saved report.

6 In the **Data Import Schedule** panel, do one of the following and then click **Next**.

Run now

The job runs immediately after the wizard closes.

Run periodically	The Run periodically options are as follows: ■ **Start on** Lets you select a date from the schedule to start a job run. ■ **Run once** Lets you run the job only one time on the specified date and time. ■ **Run every # days** Lets you specify the number of days after which the job runs automatically.

7 In the **Email Notification** panel, enter the details to send notifications. Email notifications are sent on the success or failure of the data import.

Note: You must set the Notification Server computer and the port details in the CCS general setting page.

The **Email Notification** panel contains the following tabs:

- Success
- Failure

Note: Both the tabs on this panel display the same options.

Enter the following information for the required tabs:

Send notification	Lets you send a notification for the data import job. You must select this option to enable the notification details.
Subject	Specify the subject of the notification email. You can use the #Job Name# token in the subject of the notification.

Message	Compose the email notification message. You can use the following tokens when you create the message for a successful job: ■ #Status# The success or the failure status of the job. ■ #JobStart# The date and the time when the job starts. ■ #JobSummary# The summary of the job. You can use the following token when you create the message for a job failure: ■ #FaultMessage# The message that is displayed after the job fails.
From (Email ID)	Specify the sender's email ID.
To (Email IDs)	Specify the email ID of the recipient of the notification mail. You can specify multiple email IDs by seperating them with a comma.

8 In the **Summary** panel, click **Finish**.

This panel provides the summary of Symantec Data Loss Prevention connection.

See “Deleting the Symantec Data Loss Prevention data connection” on page 867.

Editing the Symantec Data Loss Prevention data connection

You can edit a Symantec Data Loss Prevention data connection with the Edit Data Connection in the taskbar .

To edit a data connection

1 Go to **Manage** > **External Data Integration**.

2 From the **External Data Systems**, select the **Symantec Data Loss Prevention** system.

3 Select the data connection you want to edit. From the taskbar select **Edit Data Connection** option or right-click the connection name and select the **Edit Data Connection** option.

4 In the **Edit Data Connection** wizard, in the **Specify the Symantec Data Loss Prevention Enforce Server Connection** panel, edit the required information, and then click **Next**:

You must provide the password of the Enforce Server to go to the next panel.

5 In the **Specify the Symantec Data Loss Prevention Saved Reports** for Incident Collection panel, add or modify the incident report IDs and their description. Click Next.

6 In the **Data Import Schedule** panel, schedule the data import jobs. Click **Next**.

7 In the **Email Notification** panel, set up notification details. Click **Next**.

8 Click **Finish** in the **Summary** panel.

See "Adding the Symantec Data Loss Prevention connection" on page 863.

See "Deleting the Symantec Data Loss Prevention data connection" on page 867.

Deleting the Symantec Data Loss Prevention data connection

You can delete a Symantec Data Loss Prevention data connection with the Delete Data Connection in the taskbar .

To delete a data connection

1 Go to **Manage** > **External Data Integration**.

2 From the **External Data Systems**, select the **Symantec Data Loss Prevention** system.

3 Select the data connection you want to delete and from the **Connection Tasks** drop-down on the taskbar select **Delete Data Connection** option.

Alternatively, you can right-click the data connection and select **Delete Data Connection** option

See "Adding the Symantec Data Loss Prevention connection" on page 863.

About External Data Integration view for Symantec Data Loss Prevention

The **External Data Integration** view displays the preconfigured data systems and the external data systems that you add to CCS. You can access the External Data Integration view for by navigating through the **Manage > External Data Integration > Symantec Data Loss Prevention** menu of the console.

Table 31-14 contains information on the options that are available on the taskbar of the External Data Integration view and their descriptions.

Table 31-14 Options in the External Data Integration taskbar and their descriptions

Options	Descriptions
Add Data Connection	Lets you add a new data connection. See "Adding the Symantec Data Loss Prevention connection" on page 863.
Edit Data Connection	Lets you modify the configurations of an existing data connection. See "Editing the Symantec Data Loss Prevention data connection" on page 866.
Delete Data Connection	Lets you delete an existing data connection. See "Deleting the Symantec Data Loss Prevention data connection" on page 867.
Set Asset Risk Aggregation	Lets you configure asset risk aggregation.
Set Asset Reconciliation	Lets you configure the asset reconciliation rules for external data. See "About the predefined Reconciliation rules for Symantec Data Loss Prevention" on page 882.
View Data	Lets you view the details about imported data from an external data system.

Table 31-15 contains information on the columns available in the **External Data Systems** pane.

Table 31-15 Columns in the **External Data Systems** pane and their descriptions

Column name	Description
External Data System Name	Displays the names of the external data systems that you have configured.
Description	Displays a description for the existing data system.
Data Schema	Displays the entity names for which you import data from an external data system.

Table 31-15 Columns in the **External Data Systems** pane and their descriptions *(continued)*

Column name	Description
Data Connections	Displays the number of connections that have been configured for a data system.

Options that are displayed in the details pane of the External Data Integration view depend on the data system or a data connection that you select.

Table 31-16 contains information about the columns that are displayed in the details pane, if you select a data system.

Table 31-16 Columns available in the **Symantec Data Loss Prevention data system** details pane

Columns	Descriptions
General	Displays a description of the selected data system.
Field Mapping	Displays the data field mappings for the selected data system. See "About the data mapping of the Symantec Data Loss Prevention fields with the CCS data schema" on page 877.
Data Correlation	Displays the information related to data correlation for the selected data system. This tab is not applicable for the pre-integrated Symantec Data Loss Prevention data system. You can create a new data system using the Symantec Data Loss Prevention Incidents data schema. In which case this field is applicable.
Risk Aggregation	Displays the risk aggregation configurations for a selected data system. This tab is not applicable for the pre-integrated Symantec Data Loss Prevention data system. You can create a new data system using the Symantec Data Loss Prevention Incidents data schema. In which case this field is applicable.

Table 31-16 Columns available in the **Symantec Data Loss Prevention data system** details pane *(continued)*

Columns	Descriptions
Reconciliation Rules	Displays the predefined reconciliation rules that are present for a selected data system. See "About the predefined Reconciliation rules for Symantec Data Loss Prevention" on page 882.
Status Mapping	Displays the mapping of the Symantec Data Loss Prevention statuses to the CCS statuses. You can also add, modify, or remove the mapping from this tab. See "About Symantec Data Loss Prevention Incidents and Control Compliance Suite status mapping" on page 885.

Table 31-17 contains information about the columns that are displayed in the details pane, if you select a data connection.

Table 31-17 Columns available in the **Symantec Data Loss Prevention data connection** details pane

Columns	Descriptions
General	Displays the configuration details of the selected data connection.
Schedule	Displays the information on the schedule of the data import job that is configured for the selected data connection.
Email Notification	Displays the information on the email notification configurations for the selected data connection.
Reports	Displays the report IDs and their descriptions, that are selected for incident data import.

See "Viewing the Symantec Data Loss Prevention data system information in the details pane" on page 871.

See "Viewing the Symantec Data Loss Prevention data connection information in the details pane" on page 871.

Viewing the Symantec Data Loss Prevention data system information in the details pane

You can view information about the **Symantec Data Loss Prevention** data system in the details pane.

To view the data system information

1. From the External Data Systems, select the **Symantec Data Loss Prevention** data system.
2. Click any of the following tabs to view information in the details pane.

- General
  See "Data system details pane - General tab" on page 872.
- Field Mapping
  See "Data system details pane - Field mapping tab" on page 872.
- Data Correlation
  This tab is not applicable for the pre-integrated data system. You can create a new data system using the Symantec Data Loss Prevention data schema. In which case this field is applicable.
- Risk Aggregation
  This tab is not applicable for the pre-integrated data system. You can create a new data system using the Symantec Data Loss Prevention data schema. In which case this field is applicable.
- Reconciliation Rules
  See "Data system details pane - Reconciliation Rules tab" on page 873.
- Status Mapping
  See "Data system details pane - Status Mapping tab" on page 873.

See "Viewing the Symantec Data Loss Prevention data connection information in the details pane" on page 871.

Viewing the Symantec Data Loss Prevention data connection information in the details pane

You can view information about the Symantec Data Loss Prevention data connection in the details pane.

To view the data connection information

1. From the **Symantec Data Loss Prevention** data system, select a data connection.
2. Click any of the following tabs to view information in the details pane.

- General
- Schedule
- Email Notification
- Reports

See "Viewing the Symantec Data Loss Prevention data system information in the details pane" on page 871.

Data system details pane - General tab

The General tab of the Symantec Data Loss Prevention data system displays the following information:

External data system name	Displays the name of the external data system.
Description	Displays the details of the selected external data system.
Data schema	Displays the name of the data schema that is used to create the data system.

See "Viewing the Symantec Data Loss Prevention data system information in the details pane" on page 871.

Data system details pane - Field mapping tab

The Field mapping tab of the Symantec Data Loss Prevention data system displays the mapping of fields between the external data system and the Symantec Data Loss Prevention Incidents data system.

The lists display the following information:

Table name	Fields
External System Fields	■ Field Name ■ Data Type ■ Is Mapped Fields that are selected are mapped from the external data system to Symantec Data Loss Prevention Incidents data system.

Table name	Fields
Mapping for Symantec Data Loss Prevention Incidents	■ Mapped External System Field Name ■ Field Name ■ Data Type ■ Field Type

See "About the data mapping of the Symantec Data Loss Prevention fields with the CCS data schema" on page 877.

See "Viewing the Symantec Data Loss Prevention data system information in the details pane" on page 871.

Data system details pane - Reconciliation Rules tab

The Reconciliation Rules tab of the Symantec Data Loss Prevention data system displays the following information:

Name	Name of the Reconciliation rule
Rule Definition	Definition of the Reconciliation rule

See "About the predefined Reconciliation rules for Symantec Data Loss Prevention" on page 882.

See "Viewing the Symantec Data Loss Prevention data system information in the details pane" on page 871.

Data system details pane - Status Mapping tab

The Status Mapping tab of the Symantec Data Loss Prevention data system displays the mapping of statuses between Symantec DLP and CCS. You can add, modify, or delete the status mappingss from this tab.

The Status Mapping tab displays the following information:

DLP Status ID	Displays the ID of the Status in Symantec DLP
CCS Status	Displays the status to which the DLP status ID is matched to.
Description	Displays the details of the mapping.

See "About Symantec Data Loss Prevention Incidents and Control Compliance Suite status mapping" on page 885.

See “Viewing the Symantec Data Loss Prevention data system information in the details pane” on page 871.

Data connection details pane - General tab

The General tab of the Symantec Data Loss Prevention data connection displays the following information:

Connection Name	Displays the name of the Symantec DLP connection
Enforce Server computer name	Displays the name of the computer that hosts the Symantec DLP Enforce Server.
Enforce Server user name	Displays the user name that is used to connect to the Enforce Server .
Port	Displays the port number that the Web service uses on the Enforce Server host.

See “Adding the Symantec Data Loss Prevention connection” on page 863.

See “Viewing the Symantec Data Loss Prevention data connection information in the details pane” on page 871.

Data connection details pane - Report tab

The Report tab of the Symantec Data Loss Prevention data connection displays the following information:

Report ID	Displays the Report IDs for incident data collection
Description	Displays the detail about the saved report

See “Viewing the Symantec Data Loss Prevention data connection information in the details pane” on page 871.

About the Symantec Data Loss Prevention Incidents data schema

CCS represents the Symantec Data Loss Prevention incidents data in the form of a data schema. The data that is imported from Symantec DLP is mapped to the predefined data schema provided by CCS called Symantec Data Loss Prevention Incidents.

Note: You can create a new external data system using the Symantec Data Loss Prevention Incidents data schema.

Following are fields of the Symantec DLP Incidents data schema.

Table 31-18 Symantec Data Loss Prevention Incidents data schema

Field Name	Data Type	Field Type
Application Name	Text	Assessment
Application Path	Text	Assessment
Assessment Evidence	Text	Assessment
Assessment Message	Text	Assessment
Blocked Status	Text	Assessment
Blocked Status ID	Integer	Assessment
Database Name	Text	Asset
Database Port	Integer	Asset
Database Server Name	Text	Asset
Database Server Type	Text	Asset
Detection Date	DateTime	Assessment
Detection Server	Text	Assessment
Event Date	DateTime	Assessment
File Creation Date	DateTime	Assessment
File Name	Text	Assessment
File Owner	Text	Assessment
File Path	Text	Assessment
FQDN	Text	Asset
Host Name	Text	Asset
Incident Base Type	Text	Assessment
Incident Creation Date	DateTime	Assessment
Incident ID	Integer	Assessment

Table 31-18 Symantec Data Loss Prevention Incidents data schema *(continued)*

Field Name	Data Type	Field Type
Incident Type	Text	Assessment
IP Address	Text	Asset
Last Modification Date	DateTime	Status
Machine ID	Text	Asset
Machine Name	Text	Asset
Message Date	DateTime	Assessment
Source Type	Text	Assessment
Message Type	Text	Assessment
Message Type ID	Integer	Assessment
Originator ID	Text	Assessment
Originator IP	Text	Asset
Policy ID	Integer	Assessment
Policy Name	Text	Assessment
Policy Version	Integer	Assessment
Recipient ID	Text	Assessment
Recipient IP	Text	Assessment
Scan Date	DateTime	Assessment
Severity	Text	Status
Severity ID	Integer	Status
Status	Text	Status
Status ID	Integer	Status
CCS Status ID	Text	Status
Target	Text	Assessment
Target Server	Text	Asset
URL	Text	Assessment

Table 31-18 Symantec Data Loss Prevention Incidents data schema *(continued)*

Field Name	Data Type	Field Type
User Name	Text	Assessment
Violated Policy Rules	Text	Assessment

See "About the data mapping of the Symantec Data Loss Prevention fields with the CCS data schema" on page 877.

About the data mapping of the Symantec Data Loss Prevention fields with the CCS data schema

Symantec Data Loss Prevention integration provides the default mapping of data between the Symantec DLP fields and the CCS data schema.

The following table displays the default mapping of data between the source and the target fields, where:

- Source field name: Symantec DLP fields
- Target field name: CCS data schema

Table 31-19 Default mapping of data for Symantec DLP integration

Source field name	Target field name	Description
IncidentID	Incident ID	Unique ID of the incident.
IncidentType	Incident Type	Class name of the Incident object retrieved by calling DLP reporting APIs. This is required to simplify the asset reconciliation rules definition logic.
IncidentBaseType	Incident Base Type	Base class name of the Incident object retrieved by calling DLP reporting APIs. This is required to simplify the asset reconciliation rules definition logic. Possible values are: ■ EndpointIncidentDetailType (for Endpoint incidents) ■ DiscoverIncidentDetailType (for Discover incidents) ■ NetworkIncidentDetailType (for Network incidents)

Table 31-19 Default mapping of data for Symantec DLP integration *(continued)*

Source field name	Target field name	Description
IncidentCreationDate	Incident Creation Date	Date and time when the incident was added to the Enforce database.
DetectionDate	Detection Date	Date and time at which the Symantec Data Loss Prevention detected the incident.
Severity	Severity	Severity of the incident.
SeverityID	Severity ID	ID that corresponds to the severity of the incident.
Status	Status	Status of the incident.
StatusID	Status ID	ID that corresponds to the status of the incident.
StatusID	CCS Status ID	ID that is obtained as per the specified Status ID mapping with the CCS Status ID.
MessageSource	Source Type	Symantec Data Loss Prevention product that generated the incident. Source type can be one of the following: ■ NETWORK: Network Monitor, Network Prevent (Email), or Network Prevent (Web) ■ DISCOVER: Network Discover or Network Protect ■ ENDPOINT: Endpoint Discover or Endpoint Prevent
MessageType	Message Type	Symantec Data Loss Prevention product component that generated the incident.
MessageTypeID	Message Type ID	ID that corresponds to the Symantec Data Loss Prevention product component that generated the incident.
Policy	Policy Name	Policy that was violated due to which the incident is generated.

Table 31-19 Default mapping of data for Symantec DLP integration *(continued)*

Source field name	Target field name	Description
PolicyID	Policy ID	ID that corresponds to the policy that was violated due to which the incident is generated.
PolicyVersion	Policy Version	Version of the policy that was violated due to which the incident is generated.
ViolatedPolicyRules	Violated Policy Rules	Rules within the policy that was violated due to which the incident is generated.
BlockedStatus	Blocked Status	String value that indicates whether the message was blocked.
BlockedStatusID	Blocked Status ID	ID that corresponds to the blocked status.
DetectionServer	Detection Server	Name of the detection server that created the incident.
IncidentHistory	Last Modification Date	Contains changes to the incident such as change in status or severity. The most recent date included in the history is recorded as Last Modification Date.
MessageDate	Message Date	Date and time at which the network message (for example, an email message, HTTP request, instant message, or other protocol request) was created.
OriginatorIP	Originator IP	IP address of the sender of the network message.
OriginatorID	Originator ID	Identifying string of the sender of the network message.
RecipientIP	Recipient IP	IP Address of the intended recipient of the network message.
RecipientID	Recipient ID	Identifying string of the intended recipient of the network message.
TargetServer	Target Server	Name of the Network Discover Server that performed the scan.

Table 31-19 Default mapping of data for Symantec DLP integration *(continued)*

Source field name	Target field name	Description
Scan	Scan Date	Date and time when the scan started.
Target	Target	Name of the configured Network Discover target.
URL	URL	URL associated with a scan target. (Database connection URL in case of DiscoverSQLDatabaseIncidentDetail incident).
EventDate	Event Date	Date and time at which the violation occurred.
ApplicationName	Application Name	Name of the application that caused the incident.
ApplicationPath	Application Path	Path of the application that caused the incident.
UserName	User Name	Endpoint user name (for example, MYDOMAIN\bsmith)
MachineName	Machine Name	Computer on which the incident occurred.
FileName	File Name	Name of the file that caused the incident.
FilePath	File Path	Path of the file that caused the incident.
FileOwner	File Owner	Owner of the file at the time the incident was created.
FileCreateDate	File Creation Date	Date and time when the file was created.
AssessmentEvidence	Assessment Evidence	A string of the format: Incident [Incident ID] did not comply with the following rules: <list of violated rules>
AssessmentMessage	Assessment Message	A string of the format: Incident [Incident ID] did not comply with the rules.

Table 31-19 Default mapping of data for Symantec DLP integration *(continued)*

Source field name	Target field name	Description
MachineID	Machine ID	Contains value of target server (in case of Discover incidents), originatorIPAddress (in case of Network incidents) or machineName (in case of Endpoint incidents)
IPAddress	IP Address	Populated with Machine ID field value, if it is IP Address. Helps in defining asset reconciliation rules.
FQDN	FQDN	Populated with Machine ID field value, if it is FQDN. Helps in defining asset reconciliation rules.
HostName	Host Name	Populated with Machine ID field value, if it is Host Name. Helps in defining asset reconciliation rules.
DatabaseServerName	Database Server Name	Contains database server name which is read by parsing the URL field, in case of DiscoverSQLDatabaseIncidentDetail incident.
DatabaseServerType	Database Server Type	Contains database server type which is read by parsing the URL field, in case of DiscoverSQLDatabaseIncidentDetail incident. (Possible values are sqlserver, oracle, db2)
DatabaseName	Database Name	Contains database name which is read by parsing the URL field, in case of DiscoverSQLDatabaseIncidentDetail incident.
DatabasePort	Database Port	Contains database port which is read by parsing the URL field, in case of DiscoverSQLDatabaseIncidentDetail incident.

See “About the Symantec Data Loss Prevention Incidents data schema” on page 874.

About the predefined Reconciliation rules for Symantec Data Loss Prevention

CCS provides predefined Add and Update rules as a part of the Symantec Data Loss Prevention integration. You can use these reconciliation rules to add or update the assets in CCS before creating a data connection to import the incidents data.

You can also create reconciliation rules to import the incidents data.

For more information on creating reconciliation rules,

You can view all the Add and Update rules at the following location in the CCS workspace:

Manage > **Reconciliation Rules** > **Pre-defined Rules** > **Data Schema Driven** > **Symantec Data Loss Prevention Incidents**.

The following table lists all the predefined reconciliation rules, their descriptions, and their type.

Table 31-20 Predefined Reconciliation Rules of the Symantec Data Loss Prevention integration

Reconciliation Rule	Description	Type of Rule
Add Windows Machines for Endpoint Incidents	Add Windows computers while importing the Endpoint incident details.	Add
Add Oracle Configured Databases for Discover Database Incidents	Add Oracle Configured Databases while importing the Discover Database incidents.	Add
Add SQL Databases for Discover Database Incidents	Add SQL Databases while importing the Discover Database incident details.	Add
Add Windows Machines for Discover Endpoint Filesystem Incidents	Add Windows computers while importing the Discover Endpoint File System incident details.	Add
Add Windows Machines for Discover Filesystem Incidents	Add Windows computers while importing the Discover File System incident details.	Add

Table 31-20 Predefined Reconciliation Rules of the Symantec Data Loss Prevention integration *(continued)*

Reconciliation Rule	Description	Type of Rule
Correlate with Oracle Configured Databases for Discover Database Incidents	Correlate with Oracle Configured Databases while importing the Discover Database incident details.	Update
Correlate with ESM Agents for Discover Filesystem Incidents	Correlate with ESM Agents while importing the Discover File System incident details.	Update
Correlate with ESM Agents for Discover Filesystem Scanner Incidents	Correlate with ESM Agents while importing the Discover File System Scanner incident details.	Update
Correlate with Windows Machines for Discover Filesystem Scanner Incidents	Correlate with Windows computers while importing the Discover File System Scanner incident details.	Update
Correlate with SQL Databases for Discover Database Incidents	Correlate with SQL Databases while importing the Discover Database incident details.	Update
Correlate with Windows Machines for Discover Filesystem Incidents	Correlate with Windows computers while importing the Discover File System incident details.	Update
Correlate with ESM Agents for Discover Endpoint Filesystem Incidents	Correlate with ESM Agents while importing the Discover Endpoint File System incident details.	Update
Correlate with Oracle Configured Servers for Discover Database Incidents	Correlate with Oracle Configured Servers while importing the Discover Database incident details.	Update
Correlate with Windows Machines for Endpoint Incidents	Correlate with Windows computers while importing the Endpoint incident details.	Update

Table 31-20 Predefined Reconciliation Rules of the Symantec Data Loss Prevention integration *(continued)*

Reconciliation Rule	Description	Type of Rule
Correlate with Windows Machines for Discover Endpoint Filesystem Incidents	Correlate with Windows computers while importing the Discover Endpoint File System incident details.	Update
Correlate with UNIX Machines for Discover Filesystem Scanner Incidents	Correlate with UNIX machines while importing the Discover File System Scanner incident details.	Update
Correlate with ESM Agents for Endpoint Incidents	Correlate with ESM Agents while the importing the Endpoint incident details.	Update
Correlate with SQL Servers for Discover Database Incidents	Correlate with SQL Servers while importing the Discover Database incident details.	Update

Viewing the Symantec Data Loss Prevention incidents data in Dynamic Dashboards

CCS consumes the imported incidents data to generate the dynamic dashboard panels. The data is presented in the panels based on KPIs relevant for DLP.

The following predefined panels are available for Data Loss Prevention:

- Response to Data Loss Prevention Incidents
- Top 10 Data Loss Prevention Incidents by Protocol
- Top 10 Data Loss Prevention Incidents by User

Viewing the Symantec Data Loss Prevention incidents data in Policy Compliance Reports

After you import the incidents data, CCS consumes the data to generate policy compliance reports. As a part of the Symantec Data Loss Prevention integration, CCS generates compliance reports based on Symantec Data Loss Prevention data model.

CCS displays the following predefined policy reports for the compliance:

- Comparison of control statement mapping

- Policy compliance by assets
- Policy control statements mapping
- Policy results by controls

Assessment procedure for Symantec Data Loss Prevention Incidents

The *Symantec Data Loss Prevention Policy Violation* is a pre-shipped assessment procedure for Symantec Data Loss Prevention.

The procedure evaluates whether any incident fails against an asset. If an incident fails for any asset, then that asset is marked as failed for the assessment procedure.

For example:

The procedure evaluates if there are any incidents against an asset in the incoming incident data where the CCS Status ID value is 2. If the CCS Status ID is 2 then that asset is marked Fail for the assessment procedure.

- The CCS status **Pass** is mapped to the CCS status ID **1**.
  When a Symantec DLP status is mapped to the pass status in CCS then the value 1 is saved in the CCS Status ID field.
- The CCS status **Fail** is mapped to the CCS status ID **2**.
  When a Symantec DLP status is mapped to the fail status in CCS then the value 2 is saved in the CCS Status ID field.

About Symantec Data Loss Prevention Incidents and Control Compliance Suite status mapping

Symantec Data Loss Prevention (DLP) creates an incident when it detects a policy violation. The process of handling incidents goes through several stages from discovery to resolution. You may use various status attributes to identify an incident at various stages of the incident, for example "New", "Investigation", “Resolved", and so on. The default status attribute that DLP uses is "New". Each status attribute contains a unique status ID.

Each DLP incident status attribute value has a numeric value that is assigned to it. In DLP the numeric value for the DLP incident status attribute value is mapped to the CCS status.

CCS uses the following statuses:

- Pass.
- Fail.

The status ID is displayed in the DLP console status bar when you place the cursor over the incident status attribute value.

By default, the DLP incident status "New" that has the status ID "1" is mapped to "Fail" in CCS.

To map the DLP incident status ID and the CCS status:

1. Select the Symantec Data Loss Prevention data system from the External Data Integration workspace.
2. From the details view panel, select the Status Mapping tab.
3. Click **Add** to add status mapping.

   Make sure you click **Save** to reflect the changes you make.
4. In the Add Status Mapping panel provide the following information:

DLP Status ID	Lets you enter the ID of the DLP incident status. The Status ID displays on the status bar of the DLP console when you place the cursor on the incident status attribute value.
CCS Status	Lets you select the status that Control Compliance Suite understands.
Description	Lets you enter a brief description about the status mapping. This field is optional.

5. Click **Modify** to edit the status mapping.
6. Click **Remove** to delete the status mapping.

Note: Make sure you click **Save** to reflect the changes you make.

See “Assessment procedure for Symantec Data Loss Prevention Incidents ” on page 885.

About asset risk aggregation using the Data Loss Prevention incidents data

Risk score for the Data Loss Prevention (DLP) incidents can be calculated using assessment procedures. The severity of the DLP incidents is used risk assessment.

See “Configuring asset risk aggregation for external data” on page 806.

Chapter 32

Managing baselines

This chapter includes the following topics:

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 890.
- 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 892.

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.

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

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.
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 890.

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.

See “Viewing the comparison results in the Baselines view” on page 892.

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**.

See “Creating a baseline job” on page 890.

Managing tags

This chapter includes the following topics:

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 896.

See "Editing a tag category" on page 896.

See "Deleting a tag category" on page 897.

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 895.

See "Deleting a tag category" on page 897.

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 895.

See "Renaming a tag" on page 896.

See "Moving a tag" on page 897.

See "Deleting a tag" on page 897.

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 896.

See “Moving a tag” on page 897.

See “Deleting a tag” on page 897.

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 896.

See “Renaming a tag” on page 896.

See “Deleting a tag” on page 897.

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 896.

See “Renaming a tag” on page 896.

See “Moving a tag” on page 897.

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 895.

See “Editing a tag category” on page 896.

Managing policies

This chapter includes the following topics:

About the Policies view

The Policies view lets you manage the policies in the Control Compliance Suite. The Policies view displays a hierarchical tree structure of all policies. The Policies view lets you view the attributes of a selected policy or filter the displayed policies.

You can access the Policies view from Manage > Policies.

The Policies view contains the following panes:

Tree pane	This pane appears on the left side of the console window under the navigation bar. This pane displays a hierarchical, folder-based structure of the policies that are stored in the CCS directory.
Filter by pane	This pane appears in the lower left side of the console window under the tree pane. You can specify filters in this pane so that only the required policies are displayed in the table pane.

Table pane	The table pane appears in the right side of the console window under the taskbar. This pane displays the policies.
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 policy that is selected in the table pane.

You can perform the following tasks from the Policies 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.
- Submit a policy for review and approval.
- Approve a policy.
- Publish a policy.
- Unpublish a policy.

The details pane of the Policies 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, allow user response, and rationale.
Attachments	The **Attachments** tab lists the documents attached to the policy. You can download, attach, or delete policy documents.

Targets	The **Targets** tab lists the Control Compliance Suite assets to which the policy applies. You can use the tab to add and remove assets for policies in the Draft state.
Statements	The **Statements** tab displays any control statements that are mapped to the policy. Control statements are mapped to the policy in the Controls Studio. The **Statements** tab contains a link that lets you open the Controls Studio.
Audience	The **Audience** tab lists the users assigned to the Policy Audience 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**.
Comments	The **Comments** tab lets reviewers review the policy and create comments or change requests for the policy.
Clarifications	The **Clarifications** tab lets you review and respond to clarification requests for the policy by an audience member. 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.
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	The **Exceptions** tab lists any exceptions that are granted to this policy. Use the **Exceptions Management** view to manage these exceptions.

Note: Only a user who is assigned to the CCS Administrator role can assign roles and permissions.

Note: You must explicitly assign users to the **Policy Reviewers** , **Policy Approvers**, and **Policy Audience** roles. No users are assigned to these roles by default, including the **CCS Administrator**.

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 902.
- Import a Microsoft Word file as a policy.
  See "Importing a Word policy" on page 904.
- Move, copy, or paste a policy.
  See "Moving, copying, and pasting a policy" on page 907.
- Delete a policy.
  See "Deleting a policy" on page 906.
- Select the policy audience.

See "About editing policies" on page 218.

Creating a new policy

You can create a policy from the start or create a policy based on a predefined policy.

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 select 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.
Rationale	The reason for the existence of the new policy. The rationale can be as comprehensive as your needs require. A rationale 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	When this option is checked, the policy can be published to the Control Compliance Suite Web Console. Users can then read and respond to the policy. When unchecked, the policy can be published to the Control Compliance Suite Web Console. 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.

5 In the **Add Policy Documents** panel, click **Attach File** to attach the policy documents. You can attach one or more documents in any format, for example: MS Word, HTML, .pdf, .jpeg, etc.

Click **Remove** to remove any of the attached documents.

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 Controls Studio to map Control Statements** is checked.

8 In the **Summary** panel, click **Finish**.

See "Working with policies" on page 902.

See "Importing a Word policy" on page 904.

Importing a Word policy

You can import a Microsoft Word .doc file as a Control Compliance Suite (CCS) 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 CCS prompts you to enter a new name for the policy. You must enter a new name to import the policy.

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 2007	http://www.microsoft.com/downloads/details.aspx?familyid=59DAEBAA-BED4-4282-A28C-B864D8BFA513&displaylang=en
Office 2003	http://www.microsoft.com/downloads/details.aspx?familyid=3c9a983a-ac14-4125-8ba0-d36d67e0f4ad&displaylang=en
Office XP	http://www.microsoft.com/downloads/details.aspx?familyid=C41BD61E-3060-4F71-A6B4-01FEBA508E52&displaylang=en

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 2 and step 4 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**.

See “Working with policies” on page 902.

See “Creating a new policy” on page 902.

Editing a policy

You can use the Control Compliance Suite Console to make changes to a policy. To make changes to a policy, the policy must be in the draft state.

To make changes to a policy that is in review, one or more policy reviewers must request changes to the policy. The change request forces the policy to return to the draft state when the **Review by** period expires. The policy version number does not change.

To make changes to the policy document you must download the policy document, make changes, and then attach the document again to the policy.

To make changes to a published policy, you must unpublish the policy. Unpublishing the policy changes the policy version number and puts the new version in the draft state. You can then review, approve, and publish the new version.

See "About policy status" on page 215.

See "About policy versioning" on page 214.

See "Unpublishing a policy" on page 913.

To edit a policy

1 In the Policies view, navigate in the tree pane and click the policy to select it.

You can only edit a policy to which you have appropriate rights.

2 In the **Details** pane, select the **Attachments** tab. From the list of attachments select the attachment that needs to be edited.

3 Do one of the following:

- Click **Download All** to download the selected attachements.
- Click **Attach File**to attach a new document to the policy.
- Click **Remove File** to deleted the selected attachment.
- Select another policy, then click **Yes** when prompted to save the changes to the policy.
- Select another policy, then click **No** when prompted to save the changes to the policy.

See "About the policy life cycle" on page 213.

See "Working with policies" on page 902.

See "Deleting a policy" on page 906.

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**.

See "About the policy life cycle" on page 213.

See "About policy versioning" on page 214.

See “About policy status” on page 215.

See “Editing a policy” on page 905.

See “Moving, copying, and pasting a policy” on page 907.

Moving, copying, and pasting 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**.

See “Working with policies” on page 902.

See “Creating a new policy” on page 902.

See “Editing a policy” on page 905.

See “Deleting a policy” on page 906.

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.

Note: You must explicitly assign users to the **Policy Reviewers** role. No users are assigned to this role by default, including the **CCS Administrator**.

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 do one of the following:

- Select **Submit via Integrated Workflow**
- Select **Submit via Symantec Workflow**

Click **Submit**.

See "About the policy life cycle" on page 213.

See "About policy status" on page 215.

See "Submitting a policy for review and approval" on page 909.

See "About policy review" on page 216.

See "Reviewing a policy" on page 916.

See "Viewing the reviewer comments" on page 916.

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.

Note: You must explicitly assign users to the **Policy Reviewers** role. No users are assigned to this role by default, including the **CCS Administrator**.

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 approval, then do one of the following:.

- Select **Submit via Integrated Workflow**
- Select **Submit via Symantec Workflow**

Click **Submit**.

See "About the policy life cycle" on page 213.

See "About policy status" on page 215.

See "About policy approvers" on page 218.

See "Submitting a policy for review and approval" on page 909.

See "About policy approval" on page 217.

See "Approving a policy" on page 917.

Submitting a policy for review and approval

After you have created a policy and it is ready for review, you can submit the policy for review and approval.

The policy can be sent for review and approval at the same time.

Note: Only the policies that you have permissions to in the folder selected in the tree pane can be submitted for review and approval.

Note: You must explicitly assign users to the **Policy Reviewers** role. No users are assigned to this role by default, including the **CCS Administrator**.

To submit a policy for review and 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 for Review and Approval**
- Click **Workflow Tasks > Submit for Review and Approval**

- Right-click an object in the tree, then click **Submit for Review and Approval**

2 In the **Submit for Review and Approval** dialog box, click the check box beside the name of the policies to submit for approval, then click **Submit**.

Only the policies that are ready to be sent for review and approval have the checkbox besides the policy name.

3 From the **Select Symantec Workflow** select the workflow that you want to assign the selected policies to.

See "About the policy life cycle" on page 213.

See "About policy status" on page 215.

See "About policy approvers" on page 218.

See "Submitting a policy for review and approval" on page 909.

See "About policy approval" on page 217.

See "Approving a policy" on page 917.

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 in the Control Compliance Suite Web Console. 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 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 Control Compliance Suite Web Console Policy page. The policy is available for future publication under a new version number.

See "About the policy life cycle" on page 213.

See "About policy versioning" on page 214.

See "About policy status" on page 215.

See "Publishing a policy" on page 911.

See “Unpublishing a policy” on page 913.

Publishing a policy

When you publish policies, you transmit the policies to the policy audience in the Control Compliance Suite Web Console. 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.

Note: Only approved policies can be published.

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 Console.

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**.

See “About the policy life cycle” on page 213.

See “About policy versioning” on page 214.

See “About policy status” on page 215.

See “Publishing and unpublishing policies” on page 910.

See “Unpublishing a policy” on page 913.

Publishing a policy from a Web console

The **Publish Policies** page lets you view and publish the approved policies. After a policy is created, reviewed, and approved, it is ready to be published. Once you publish a policy, the policy becomes available to the Policy Audience. The members of the Audience can then Accept or Decline the policy. The audience members can also request Clarifications or Exceptions to the policy.

The Publish Policies page includes the following tabs:

Table 34-1 Tabs on the Publish Policies Page

Tab Name	Description
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.
Targets	The Targets tab lists the entities that are targets of the policy.
Statements	The Statements tab displays any control statements that are mapped to the policy. Control statements are mapped to the policy in the Controls Studio tool.
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.
Comments	The Comments tab lets reviewers view any comments for the policy.
Tags	The Tags tab lets you review the tags that are assigned to the policy.

Unpublishing a policy

Only published policies can be unpublished. When you unpublish a policy, the policy is removed from the Control Compliance Suite Web Console. 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**.

See "About the policy life cycle" on page 213.

See "About policy versioning" on page 214.

See "About policy status" on page 215.

See "Publishing and unpublishing policies" on page 910.

See "Publishing a policy" on page 911.

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.

See "About clarifications" on page 219.

See "Managing clarification requests" on page 914.

About the Clarifications view

The **Clarifications** view lets you manage and respond to the policy clarification requests from users. The **Clarifications** view displays all policy clarification requests. The **Clarifications** view lets you view the attributes of a selected policy clarification or filter the displayed policy clarifications.

You can access the **Clarifications** view from Manage > Policies > Clarifications.

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

Tree pane	The **Tree** pane appears on the left side of the console window under the navigation bar. This pane is not used in the policy clarifications view.
Filter by pane	The **Filter by** pane appears in the lower left side of the console window under the tree pane. You can specify filters in this pane so that only the required policy clarifications are displayed in the table pane.
Table pane	The **Table** pane appears in the right side of the console window under the taskbar. This pane displays the policy clarifications.
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 policy clarification that is selected in the table pane.

You can perform the following tasks from the **Clarifications** 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 Displays the email address of the user to send a notification to. The email address is optional.

If you send an email, you must configure the **From email address** in the **Email Notifications** tab in the **General Settings**.

Details Displays the question that the user submitted regarding the policy.

Due By Displays the date by when the policy administrator should send a response.

Responded (date) Displays the date and time of the response.

By Displays the account name of the policy administrator 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.

See “Managing clarifications” on page 913.

See “About clarifications” on page 219.

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.

See “Submitting a policy for review” on page 907.

See “Submitting a policy for approval” on page 908.

See “Submitting a policy for review and approval” on page 909.

See “Approving a policy” on page 917.

See “Reviewing a policy” on page 916.

See “Viewing the reviewer comments” on page 916.

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.

Note: You must explicitly assign users to the **Policy Reviewers** role. No users are assigned to this role by default, including the **CCS Administrator**.

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**.

See “About the policy life cycle” on page 213.

See “Submitting a policy for review” on page 907.

See “Submitting a policy for review and approval” on page 909.

See “About policy review” on page 216.

See “Viewing the reviewer comments” on page 916.

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.

Note: You must explicitly assign users to the **Policy Reviewers** role. No users are assigned to this role by default, including the **CCS Administrator**.

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**.

See "About the policy life cycle" on page 213.

See "Submitting a policy for review and approval" on page 909.

See "About policy review" on page 216.

See "Reviewing a policy" on page 916.

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**.

See "About the policy life cycle" on page 213.

See "Submitting a policy for approval" on page 908.

See "Submitting a policy for review and approval" on page 909.

Reactivating expired policies

You can reactivate expired policies. The status of a reactivated policy changes from Expired to Draft.

To reactivate an expired policy

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 **Reactivate Expired Policies**
   - Click **Workflow Tasks > Reactivate Expired Policies**
   - Right-click an object in the tree, then click **Reactivate Expired Policies**
2. In the **Reactivate Expired Policies** dialog box, click the check box beside the name of the policies to reactivate, then click **Submit**.

   The Status of the reactivated policy changes to Draft.

Viewing Policy Compliance

You can view the policy reports and policy dashboards to view the overall Policy Complaince posture.

Following are the pre-shipped reports for Policy:

- Policy Summary
- Policy Acceptance Status
- Policy Control Statement Mappings
- Policy Results by Control
- Policy Compliance by Asset

Following are the pre-shipped dashboards and panels for Policy

- Compliance Analysis – Policies
- Control Status for Policies
- Top 10 Failed Control Statements for Policies
- Control Status Trends for Policies
- Active Exceptions for Policies
- Active Exceptions for Policy Controls
- Top 10 Assets with Highest Risk Score by Policy

Chapter 35

Mananging certificates

This chapter includes the following topics:

About Encryption Management Service

Encryption Management Service is responsible for securely encrypting sensitive data.

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

Symcert is a command-line utility for installing and removing certificates on CCS component systems. The utility is installed and automatically executed when a certified component is installed. **Symcert** functions add or remove component certificates in the computer's certificate store. **Symcert** adds necessary certificate data to the component's configuration file. The certificate data in the configuration file is read on service start and defines which CCS systems trust the component. **Symcert** can also be used to review certificate data for all of the CCS components that are installed on a local system. **Symcert** may be used in disaster recovery or migration scenarios without the expense of complete deployment of the DPS systems. Using **Symcert** CCS components can be updated with new certificates issued by the **Certificate Management Console** or from a different CCS root authority. The syntax for **Symcert** is available at the command line.

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

See "About the Certificates view" on page 920.

See "Using the Certificate Management Console" on page 923.

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 35-1 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 35-2 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 utility for installing and removing certificates on CCS component systems. The utility is installed and automatically executed when a certified component is installed. **Symcert** functions add or remove component certificates in the computer's certificate store. Certificate data is also added or removed from the services configuration file. The certificate data in the configuration file is read on service start and defines which CCS systems are trusted by the component. **Symcert** can also be used to read certificate data for all of the CCS components that are installed on a local system. **Symcert** may be used in disaster recovery or migration scenarios without the expense of complete deployment of the DPS systems. Using **Symcert** the systems can be updated with certificates from a different root authority. The syntax for **Symcert** is available at the command line.

See "About Encryption Management Service" on page 919.

See "About the Certificates view" on page 920.

See "Using the Certificate Management Console" on page 923.

About creating certificates

You create certificates in the **Certificate Management Console**. You create the certificate based on the service type and you can create several certificates sequentially. Certain information is reused as the default selections from the previous certificate, but all of the information can be edited. Every item in the

Create Certificates dialog box is required. The information is not validated. You can be an ADAM administrator or have the "Manage Configuration Settings" task in your role to create certificates. You should be a local administrator and be a member of the CCS administrator role.

Note: Computer names should not use any characters that are invalid for a DNS name. The list of characters that are not allowed is available at the following location:

http://support.microsoft.com/kb/909264

Each CCS component has a host registration in ADAM. The CCS Manager certificate is unbound until registered in **System Topology** in the CCS Console.

When you open the **Certificate Management Console**, you may be prompted to provide the root certificate password. The password is created during the installation of CCS. The password is not required if you have previously opened the console. The password is also not required if you are logged on in the context of the user who installed CCS.

You can find a list of the two-character codes at:

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

See “Creating a certificate” on page 926.

About certificate encryption

You create a certificate that uses the Secure Hash Algorithm (SHA) set of cryptographic hash functions. The National Security Agency (NSA) designed the set of functions. The National Institute of Standards and Technology (NIST) publish the set of functions as a Federal Information Processing Standard.

Windows XP and Server 2003 cannot obtain certificates using SHA-2 algorithms unless the operating systems have been updated with the appropriate Windows hotfix. You should review the Microsoft solution to be sure that it is appropriate for your organization.

When you create a certificate for use on a Windows Server 2003 system the password length is limited to a maximum of 31 characters. Certificates that are created for Windows Server 2008 systems may have passwords up to 255 characters.

Table 35-3 Available signature algorithms and key size selections

SHA hash functions	key size	key size	key size
sha1RSA	2048	3072	4096
sha256RSA	2048	3072	4096
sha384RSA	2048	3072	4096
sha512RSA	2048	3072	4096

If you create a certificate with stronger hash function or larger key size, the creation process may take more time on certain computers.

Using the Certificate Management Console

Table 35-4 Certificate life cycle

Action	Description	More information
Creation	You create the certificate based on the service type.	
Renewal	You can renew the certificate, which extends the life of the certificate.	See "Renewing certificates" on page 928.
Bind	In certain circumstances, you can bind a certificate. The system trusts a component with a bound certificate.	See "Binding a certificate" on page 929.
Unbind	A certificate can become invalid before the expiration date. Under such circumstances, you should unbind the certificate.	See "Unbinding certificates" on page 930.
Removal	You should remove the disabled/unbound certificates or expired certificates when you perform a periodic system cleanup.	See "Removing a certificate" on page 931.

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

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

About the Certificate Management Console

The **Certificate Management Console** (CMC) is used to manage certificates for CCS. The console is installed on the same system as the Encryption Management Services. The console cannot be accessed remotely. You must be logged on to the system that hosts the Encryption Management Services to access the CMC. Any user can open the CMC to review the certificates.

You can **Search** on any of the properties. You can **Clear** the results of the search.

Table 35-5 Certificate properties

Name	Description
Issued to	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.
Status	The status of the certificate. The types of status are described in Table 35-6

Table 35-6 Status types 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 uninstall 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** CCS Manager certificates may only be bound if the component has been registered in the CCS Console.

A certificate that is removed no longer is available to the system and is not visible in the CMC.

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.

A user can be a local administrator but must be an ADAM administrator and know the root certificate password to do the following:

- **Create certificates**
- **Renew certificates**
- **Bind certificates**
- **Unbind certificates**
- **Remove certificates**

In the CMC, the user activates a certificate by selecting the appropriate check box. After the check box has been selected, the user can renew, unbound, or remove a certificate. A certificate that is unbound but not removed has a status of disabled/unbound.

The type of installation determines the number of certificates that are created automatically. A CCS Application Server installation always creates the root certificate. The Application Server install also creates and binds the Management Service certificate. If you have installed the CCS Application Server and the CCS Manager on a single computer, the installation creates a certificate for the CCS Manager. The CCS Application Server installation does not create the certificates that are needed to install the stand-alone CCS Managers.For stand-alone CCS Managers, certificates must be created manually using the **Certificate Management Console**. You must create the service type certificate for each installed component. For example, if your system has 50 CCS Managers, you must create 50 certificates. Each CCS component has a host registration in ADAM. The CCS Manager certificate is not bound during the installation. The certificate is created but its host record is not created during installation so the certificate cannot be bound until the CCS Manager registration occurs. The registration process both creates the host record and binds the certificate to the host record. The CCS Manager Certificate is unbound until the CCS Manager is registered in **System Topology** in the **CCS Console**.

In a CCS installation, the following certificates are created automatically:

CA	Root certificate
ManagementServices-<computer name>	Bound
CCS Manager-<computer name>	Unbound

Creating a certificate

You create the certificate based on the service type. You can create multiple certificates. Certain information is reused from the previous certificate, but all of the information can be edited. Every item in the **Create Certificates** dialog box is required. The information is not validated. You must be an ADAM administrator to create certificates. We recommended that you are also a local administrator and a Control Compliance Suite (CCS) administrator.

Table 35-7 Certificate options

Name	Description	Default value
Service Type	The available **Service Type** names are the following: ■ DPS ■ Application Server ■ Application Server (SSL Only) ■ Encryption Management Service You can only create the Encryption Management Service certificate on the computer that hosts the Directory Service. **Note:** For CCS Manager the Service Type is DPS.	**DPS**
Signature Algorithm	A mathematical scheme that demonstrates the authenticity of a digital message. You can find a list of the available signature algorithms and the key sizes in	The signature algorithm that is selected at installation time for the Root certificate.
Key Size	The length that is used in the cryptographic algorithm. You can find a list of the available signature algorithms and the key sizes in	The key size that is selected at installation time for the Root certificate.
Expires In	The number of years before the certificate expires	**25**
Organization	You can accept the value from a previous certificate or you can provide your own.	The information from the previous certificate.

Table 35-7 Certificate options *(continued)*

Name	Description	Default value
NetBIOS Name	You can use **Browse** to add a name. The NetBIOS Name must be less than 16 bytes in length.	None
FQDN	Populated from the **NetBIOS Name** selection.	None
IP Address	Populated from the **NetBIOS Name** selection.	None
(+) plus icon	Add multiple TCP/IP address	None
Destination folder	You can accept the value from a previous certificate or you can provide your own.	`<InstallDir>\ManagementServices\DefaultCerts`
Password	Password for the certificate. You must use this password to modify the certificate.	None
Retype Password	Confirm the password	None

To create a certificate

1 Click **Start** > **All Programs > Symantec Corporation > Symantec Control Compliance Suite > 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** taskbar, click **Create Certificates**.

4 In the **Create Certificates** dialog box, complete the form. All of the information is required.

You can view the option name and descriptions in Table 35-7

5 If the certificate has the same name as an existing file, you are asked if you want to overwrite the file, click **Yes**.

6 In the **Success** message box, click **OK**.

7 In the **Create Certificate** message box, click **Yes** to create another certificate, if needed.

See "About creating certificates" on page 921.

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 35-8 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 “Using the Certificate Management Console” on page 923.

See “Unbinding certificates” on page 930.

See “Removing a certificate” on page 931.

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 35-8
5. Click **Renew Certificate**.
6. In the **Success** message box, click **OK**.

Binding a certificate

If you have registered a component in the CCS Console, and you have unbound the certificate for that component, you can bind the certificate. The certificate status changes to **Bound**.

The DPS certificate cannot be bound if the DPS has not been registered in the console. The certificate is bound when you register the DPS. The application server certificate cannot be bound if the application server has not been installed. The certificate is bound during the installation. A new DPS certificate can be bound in the **Certificate Management Console** if that DPS is registered. An application server certificate can be bound in the **Certificate Management Console** if the application server is installed.

When you open the **Certificate Management 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

Note: You must use **Symcert** on the component's computer to remove the old certificate and add the new certificate to the component.

To bind 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 **Bind Certificates**.

See “About managing certificates using the command line” on page 921.

Unbinding certificates

Certificates are issued with a planned lifetime. That lifetime is defined when the certificate is created and the certificate is valid until its expiration date. Under a variety of circumstances, you can unbind the certificate, if needed. The certificate status is changed to **Disabled/Unbound**. If the certificate is unbound, the component can communicate. The user should log on to the component's computer and use the **Symcert** `untrust` command. The command places the certificate in an untrusted store and revokes communications. The certificate status is changed to disabled/unbound.

When you open the **Certificate Management 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

To unbind 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 certificate.
4. Click **Unbind Certificates**.
5. In the **Warning** message box, click **Yes**.

See “Using the Certificate Management Console” on page 923.

See “Removing a certificate” on page 931.

Removing a certificate

You should remove the unbound or expired certificates when you perform a periodic system cleanup. A removed certificate is not visible in the **Certificates** view or **Certificate Management Console**. The file may exist in the assigned directory. If you have the **Certificates** view open, and remove a certificate in the **Certificate Management Console**, you must refresh the view before you see the change.

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

See “Using the Certificate Management Console” on page 923.

See “Renewing certificates” on page 928.

See “Unbinding certificates” on page 930.

To remove 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.
4. Click **Remove Certificates**.
5. In the **Warning** message box, click **Yes**.

Chapter 36

Managing users

This chapter includes the following topics:

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 934.
- Update email addresses
  See "Updating a user email address" on page 934.
- Delete user and group accounts
  See "Deleting user accounts" on page 935.
- Update all users and groups from the domain
  See "Updating user accounts" on page 935.

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 933.

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 36-1 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 933.

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 933.

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 933.

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 933.

Enumerating users from a group

You can enumerate all the Control Compliance Suite users from a group.

To enumerate the users from a group

1. Go to **Settings > User Management**.
2. In the **User Management** view, select the check boxes of the groups to be updated.
3. On the menu bar, Click **Update**.

Chapter 37

Managing licenses

This chapter includes the following topics:

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 "Adding a license" on page 938.

See "Viewing the list of licenses" on page 938.

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 "About the Licenses view" on page 937.

See "Viewing the list of licenses" on page 938.

Adding licenses to 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`.

To add a license on the Directory Server

1. On the Directory Server host, open the `Symantec.CSM.LicenseUtil.exe` tool.
2. In the **Add Licenses** 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 **Add Licenses** 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 “About the Licenses view” on page 937.

See “Adding a license” on page 938.

Managing reports and dashboards

This chapter includes the following topics:

About 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 adn dashboard jobs to run at a specified time. If the report supports the feature, you can export a report in several formats. Dashboards that are created in the Web Console are real-time, visual representations of selected key elements for an organization. Dashboards that are created in the Web Console are not scheduled.

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 timely information that you need to make informed decisions about the organization.

The reporting database stores the data that is needed for the reports.

See "About the Reporting view" on page 265.

See "Working with reports " on page 956.

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 961.

See “Customizing a report template” on page 961.

See “Deleting a user-defined report template” on page 964.

See “About the Reporting view” on page 265.

See “Exporting a report template” on page 964.

See “Moving a report template” on page 966.

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 265.

About the My Dashboards view

The **My Dashboards** view lists the tiered dashboards that you can access. A tiered dashboard is listed in the table pane after you create the dashboard job using the **Create Tiered Dashboard** wizard.

If you are assigned as a viewer for the dashboard, you can remove any tiered 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

About types of dashboards

Table 38-1 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

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.

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 957.

See "Copying a report template" on page 961.

See "Customizing a report template" on page 961.

See "Predefined reports" on page 951.

See "Exporting a report template" on page 964.

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 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 951.

About creating user-defined templates

ou 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 963.

See "About the prerequisites for user-defined report templates" on page 948.

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:

CurrentOrSnapshotted	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 948.

See “Adding a user-defined report template” on page 963.

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 957.

See "Viewing a report" on page 958.

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.

See "About the My Reports view" on page 943.

Predefined reports

The Control Compliance Suite Reports include the default reports that let you determine the state of the installation. Settings are selected before the report is run.

The result of a report may vary based on your permission level.

Table 38-2 Report Descriptions

Name	Description	Location	Customization Support	Job Chaining support
Asset Evaluation Result Change	The report lets the user compare the two most recent compliance results and display the differences in values.	Report Templates	Yes	Yes

Table 38-2 Report Descriptions *(continued)*

Name	Description	Location	Customization Support	Job Chaining support
Asset Group Compliance	The report displays risk scores and compliance status of check or rule for an asset group or folder for the latest evaluation.	Report Templates	Yes	Yes
Asset Details	The report displays detailed information about the user's managed assets.	Report Templates	No	No
Asset Exception Status	The report displays a summary of exceptions that are in place across the IT infrastructure.	Report Templates	Yes	No
Asset Risk Summary	The report displays asset type, risk level, and related checks for a standard.	Report Templates	Yes	Yes
Assets at Highest Risk	The report displays the assets ranked by remediation order (based on risk score).	Report Templates	Yes	Yes
Compliance by Technical Check	The report lets users filter the failed, passed, unknown, Not applicable, and errored checks.	Report Templates	Yes	Yes
Compliance by Asset	The report displays the individual check results for a set of assets.	Report Templates	Yes	Yes
Compliance Summary	The report lets users view risk scores and compliance status for a set of assets.	Report Templates	No	Yes
Control Point Effective Permissions	The report generates detailed information about the effective permissions for one or more control points.	Report Templates	No	No
Control Point Simple Permissions	The report displays Simple permissions on the control point.	Report Templates	No	No

Table 38-2 Report Descriptions *(continued)*

Name	Description	Location	Customization Support	Job Chaining support
Control Point Permissions by Trustee	The report displays information about the permissions of a trustee for control points in the Entitlements module.	Report Templates	No	No
CCS System Auditing	The report displays key events related to Assets, Standards, Policies, and Entitlements in the CCS system.	Report Templates	Yes	No
Comparison of Control Statement Mappings	The report lets the user compare control statement mappings between policies or between a mandate and a policy. The report displays the control statements mappings that is compared and the checks, the SCAP rules, the external data assessments that are mapped to the control statements.	Report Templates	No	No
Entitlement Change Requests	A report of the change requests made for the control points in the review cycle.	Report Templates	No	No
Evaluation Results Asset view	The report displays evaluation results by Asset for selected evaluation job/run.	Report Templates	No	Yes
Entitlement Changes	The report lets the user access information for the entitlements or group memberships from the current and most recently approved entitlements.	Report Templates	No	No

Table 38-2 Report Descriptions *(continued)*

Name	Description	Location	Customization Support	Job Chaining support
Evaluation Results Standard View	The report displays evaluation results by Standard for selected evaluation job/run.	Report Templates	No	Yes
Policy Compliance by Asset	The report lets users view roll-up compliance scores for the assets assessed against checks and rules or for the external data assessments.	Report Templates	No	No
Policy Results by Control	The report displays asset information for selected policies like risk score, risk rating, checks, and rules against which the asset is assessed or for the external data assessments.	Report Templates	No	No
Policy Control Statement Mappings	The report lets you view the policy, the checks, and the rules mapped to its control statements or the external data assessments mapped to its control statements.	Report Templates	No	No
Policy Summary	The report displays the assets, control statements, and audience for the selected policies.	Report Templates	No	No
Policy Acceptance Status	The report displays the policy acceptance status.	Report Templates	No	No
Remediation Asset View	The report displays remediation information for one or more asset groups or containers for latest evaluation grouped by Asset.	Report Templates	No	Yes

Table 38-2 Report Descriptions *(continued)*

Name	Description	Location	Customization Support	Job Chaining support
Remediation Standard View	The report displays the remediation information for one or more assets groups or containers, for latest evaluation grouped by Standard.	Report Templates	No	Yes
Standard Details	The report reviews the checks that are applied to the IT infrastructure.	Report 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

See “Customizing a report template” on page 961.

About mapping SCAP rules for policy reports

The SCAP rules can be mapped with policies or mandates by using control statements from the Controls Studio workspace of Control Compliance Suite.

On successful execution of SCAP evaluation job, you can run reports job by using pre-defined reports templates from the Reporting workspace of CCS.

You can view the SCAP rule results in policy reports according to SCAP-PM mappings given in the following table:

Table 38-3 SCAP - PM mappings in policy reports

SCAP rule results	Corresponding result value in the policy report
Pass	Pass
Fail	Fail
Error	Unknown
Unknown	Unknown

Table 38-3 SCAP - PM mappings in policy reports *(continued)*

SCAP rule results	Corresponding result value in the policy report
Not Applicable	Not Applicable
Fixed	Pass
Not Checked	Not Applicable
Not Selected	Not Applicable
Informational	Not Applicable

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 957.
- View a report
  See "Viewing a report" on page 958.
- Copy a report template
  See "Copying a report template" on page 961.
- Customize a user-defined report template
  See "Customizing a report template" on page 961.
- Customize a report in the report viewer
  See "Customizing a report in report viewer" on page 962.
- Refresh a report in the report viewer
  See "Refreshing a report" on page 959.
- Export a report in the report viewer
  See "Exporting a report" on page 960.
- Print a report in the report viewer
  See "Printing a report" on page 959.
- Delete a user-defined report template
  See "Deleting a user-defined report template" on page 964.
- Add a user-defined report template
  See "Adding a user-defined report template" on page 963.
- Export a user-defined report template

See “Exporting a report template” on page 964.

- Update a user-defined report template
  See “Updating a report template” on page 965.
- Move a report template
  See “Moving a report template” on page 966.
- Remove a report
  See “Removing a report” on page 959.

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.

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 "Viewing a report" on page 958.

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 956.

See "About the My Reports view" on page 943.

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 958.

See "Printing a report" on page 959.

See "About the My Reports view" on page 943.

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 956.

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 958.

See "Refreshing a report" on page 959.

See "About the My Reports view" on page 943.

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 958.

See “Printing a report” on page 959.

See “About the My Reports view” on page 943.

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 956.

See "Customizing a report template" on page 961.

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
- Compliance by Asset
- CCS System Auditing
- Asset Group Compliance
- Top Failed Technical Checks

See "Copying a report template" on page 961.

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” on page 951.

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**.

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**.

See "About creating user-defined templates" on page 948.

See "About the prerequisites for user-defined report templates" on page 948.

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 956.

See "Copying a report template" on page 961.

See "Customizing a report template" on page 961.

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**.

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**.

See "About creating user-defined templates" on page 948.

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**.

See "About creating user-defined templates" on page 948.

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**.

See "About creating user-defined templates" on page 948.

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.

See "Scheduling a report " on page 957.

Managing dynamic dashboards

This chapter includes the following topics:

Roles and permissions

Control Compliance Suite (CCS) users can view dashboard panels, but not the underlying data. The CCS Administrator or the panel creator grants the Asset Viewer role with permissions for others to view the underlying data.

The following tasks are required to work with dashboards and panels:

Table 39-1 Required tasks to work with dashboards and panels

Tasks	Description
Create Dashboards	Lets you create dashboards and panels.
Manage Dashboards	Lets you can manage dashboards and panels.
Publish Dashboards	Lets you can publish dashboards and panels.

When a CCS Administrator or a Power User publishes a dashboard, others cannot see the dashboards and its panels without appropriate permissions. The CCS Administrator or a Power User can grant permissions from the Permissions Management view in the CCS Console.

The following table lists which role has what permission for the various dashboard tasks and panel tasks:

Table 39-2 Roles with dashboard tasks

Task	CCS Administrator	Power User	CCS User
Create a dashboard.	Yes	Yes	Yes
Create a panel.	Yes	Yes	Yes
Edit any dashboard.	Yes	No	No
Edit the dashboards that they own.	Yes	Yes	Yes
Edit any panel.	Yes	No	No
Edit a panel that they own.	Yes	Yes	Yes
Publish any dashboard.	Yes	No	No
Publish a panel that they own.	Yes	Yes	No

See “Creating a dashboard” on page 973.

See “Creating a panel” on page 984.

Working with dashboards

You can do the following with dashboards:

- Create a dashboard.
  See “Creating a dashboard” on page 973.
- Edit a dashboard.
  See “Editing a dashboard” on page 977.
- Change the setting of the dashboard refresh interval.
  See “Setting a dashboard refresh interval ” on page 974.
- Add a panel to a dashboard.
  See “Adding a panel to a dashboard” on page 974.
- Publish a dashboard.
  See “Publishing a dashboard” on page 975.
- Emailing a dashboard URL.
  See “Emailing a dashboard URL” on page 978.

- Print a dashboard.
  See "Printing a dashboard" on page 978.
- Delete a dashboard.
  See "Deleting a dashboard" on page 979.

About the Dashboards page

The **Dashboards** page is the main page for dashboards. You can access the **Dashboards** page from the following places:

- From the CCS Web Console in the top navigation bar select **Dashboards**.
- From the CCS Web Console under the Quick Tasks panel click the **View Dashboards**.

The Dashboard page has the following four sections:

Table 39-3 Sections of the Dashboard page

Section	Description
Sidebar	From the sidebar you can select either the Dashboard tab or the Panel tab.
Information area	A descriptive text about the Dashboards and the Panels for you to read.
Three panes	These comprise of the Last Viewed Dashboard, Quick Tasks, and References.

From the Dashboard sidebar you can choose dashboards from the different filters. You can use the filter dropdown to narrow the number of dashboards you view. The filters are the following:

Table 39-4 Filters for the Dashboard sidebar

Filter Name	Description
All	Use this filter to view all the dashboards in their different categories.
My Private	Use this filter to view all the dashboards you create and are not published.
My Published	Use this filter to view all the dashboards you create and publish.

Table 39-4 Filters for the Dashboard sidebar *(continued)*

Filter Name	Description
All Published	Use this filter to view all user published dashboards and the predefined dashboards.
Search Dashboard	Use the search bar to find a specific dashboard.

From the Dashboard Taskbar you can do the following:

Table 39-5 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Import	You click this to launch the Import Panel dialog page.

From the three panes at the bottom of the Dashboards page you can do the following:

Table 39-6 Three panes on the Dashboard page

Name of the pane	Description
Last Viewed Dashboard	You can view the name of the most recent dashboard.
Quick Tasks	You can choose from the list some of the most common tasks.
References	You can choose from a list of Help topics.

You can change the default Dashboard page by taking the following steps:

1. Check **Do not show this page again**. The Default Dashboard dropdown will appear.
2. From the **Default Dashboard** dropdown select the dashboard you want as the default.
3. Click **Apply** to set the page as the default dashboard.

See “Creating a dashboard” on page 973.

See “Roles and permissions” on page 969.

Creating a dashboard

The following are some important points when creating a dashboard:

- You create a dashboard in the Web Console.
- The created dashboard must have a unique name.
- The created dashboard is listed under the category you select while creating the dashboard.
- The new dashboard in the list has the Private icon next to it.
- A dashboard contains at least one panel.
- The dashboard can have a mix of Published Panels and Private Panels.
- You can modify the dashboard's layout to emphasize the results.
- You can choose to **Preview Panel** to view the dashboard results.
- A CCS Admin or the dashboard creator can access a private dashboard.
- Publish the private dashboard to let other users view the content. Other users must have the appropriate permissions to view the information.

To create a dashboard

1. In the **Web console** > **Dashboards** > click the **Create a new Dashboard** icon in the Dashboard header.
2. In the **Create Dashboard** page enter a unique name in the Name field.
3. Select a category from the **Category** dropdown.

   You can add a new category by clicking the **Add Category** icon. Enter the new category name and click **Create**. Click **Cancel** to close the Add Category popup.
4. From the sidebar, select a panel from the Published Panels, Private Panels, or Recent Panels categories. Drag and drop the panel in the dashboard layout.
5. You can move and resize the panel in the dashboard
6. To remove a panel from the dashboard click the **Remove** icon on the panel.
7. Repeat step 4 until you have selected all of the panels for the dashboard.
8. Review the layout of the dashboard. Use **Preview Panel** to see real time information in the panels.
9. Click **Save**. Click **Cancel** if you do not want to create the dashboard.

See “Editing a dashboard” on page 977.

See “Publishing a dashboard” on page 975.

See “Creating a panel” on page 984.

See “Difference between drilldown and drill through” on page 976.

Adding a panel to a dashboard

You can add panels to a user-defined dashboard. You can add private and published panels to a dashboard.

To add a panel to a dashboard

1 In the **Web Console** > **Dashboards** > **Dashboards** tab > select a user-defined dashboard.

2 Click the **Edit the dashboard** icon on the Dashboard header.

3 Select a panel from the sidebar and then drag it onto the dashboard layout.

4 Click **Save** when you have finished.

See “Creating a dashboard” on page 973.

See “Editing a dashboard” on page 977.

See “Roles and permissions” on page 969.

Setting a dashboard refresh interval

You do not see any changes that are made to the dashboard in real time. In order to view any updates to the dashboard you need to refresh the dashboard.

The following are some important points when you change the dashboards refresh interval:

- The interval is measured in minutes.
- You can change the interval for the current dashboard or set the interval for all your dashboards.
- You must use an integer.

To set the dashboard refresh interval

1 Open the Web Console home page using the following URL:

```
http://<servername>/CCS_Web
```

2 In the **Web Console** > **Dashboards** > **Dashboards** view, select a dashboard.

3 From the dashboard header click the **Refresh** icon on the far right/

4 In the **Set Dashboard Refresh Interval** dialog box, set the interval in minutes.

5 Click **Use this refresh interval for all of Dashboards**, if necessary.

6 Click **Apply**. Click **Cancel** if you do not want to set the interval.

See "Creating a dashboard" on page 973.

Publishing a dashboard

Publishing a dashboard allows other users to view your dashboard. In order to publish your dashboard you must either be the CCS Admin or dashboard creator.

Some points to consider before publishing your dashboard:

- It should contain at least one published panel.
- It should contain only published panels.

If you choose to publish a dashboard containing private panels then you can publish the panels along with the dashboard. If you choose not to publish the panels, then you cannot publish the dashboard.

To publish a dashboard

1 In **Web Console** > **Dashboards** > **Dashboards** sidebar > select the **My Private** filter in the sidebar.

2 Select the dashboard and then click the **Publish the Dashboard** icon in the Dashboards header.

3 If there are any private panels in the dashboard then Publish Dashboard message box will list which panels are unpublished.

4 In the **Publish Dashboard** confirmation message, click **Yes**.

5 In the **Publish Dashboard** information message, click **OK**.

See "Creating a dashboard" on page 973.

See "Editing a dashboard" on page 977.

See "Creating a panel" on page 984.

See "Difference between drilldown and drill through" on page 976.

See "Publishing a panel" on page 997.

Applying filters to a dashboard

Dashboard filters are the combination of all the filters of the panels in the dashboard. The filters refine the information displayed in the panel of the dashboard.

For example, you can apply a filter for the following:

- To show the information in a specific time range.
- To display the information from only one location.
- To display the information from a specific division of the organization.

To apply filters to a dashboard

1. Open the Web Console home page using the following URL:

   ```
   http://<servername>/CCS_Web
   ```

2. In **Web Console** > **Dashboards** > **Dashboards** sidebar > select a dashboard.
3. Click the **Filter** icon at the far right of the dashboard header.
4. In **Select Filters - <browser name>** dialog box, select an available filter.
5. Click **Apply**.

See "Applying filters to a panel in a dashboard" on page 1002.

See "About panel options" on page 986.

Difference between drilldown and drill through

The drilldown provides information across various categories in a given hierarchy. The drill through provides advanced details on a category from the context of the drilldown.

The drilldown lets you view more information about a particular element of a chart in a panel. You can select a different dimension to view the particular element. The different dimension lets you view more information contributing to the overall generic information

In the previous dashboard infrastructure you can only drilldown one level. Now you can easily define the panels that provide n-level drilldown in a given hierarchy. You can link one panel to the other as well.

For example, a summary panel may present therisk experienced by an organization due to all the Security Objectives defined by its CISO. The CISO can drilldown to the Risk Objective with highest risk and see the various categories contributing to the risk score of the Risk Objective. From there the CISO can drilldown further by clicking on the category that has the highest risk. This way the CISO can continue to drilldown in the controls hierarchy, from Risk Category > Controls Objective > Controls Statement > Checks or Vulnerability or Questionnaire or Extended tests. Similarly the CISO can choose to drilldown in the asset hierarchy instead of controls hierarchy. For example, show the risk at enterprise then at BU then at BU1 the sub-divisions of BU1, then at specific assets in that sub division.

A drill through lets you view the information in a grid at any point and at any level. The grid lets you view the advanced details that contribute in creating the chart on the top level.

For example, if you are currently at the Controls Objective level in the drilldown and you can drill through to a more detailed information page to view the details for the Control Objective that you clicked upon.

See "About panels" on page 251.

Editing a dashboard

In the Web Console you can edit a dashboard that you have created.

Note: You cannot edit a predefined dashboard. In order for you to edit a predefined dashboard you make a copy and then edit the copy.

Some important points before editing a dashboard:

- You can edit a published dashboard or panel you created.
- The CCS Administrator or dashboard creator can edit a private dashboard.

The following list shows what you can edit in a dashboard:

- Change the name of the dashboard.
- Change the category of the dashboard.
- You can add a new category by clicking the Add Category icon.
- Drag a panel from the sidebar.
- Change the layout.
- Click the red "X" in the panel header to remove a panel.

To edit a dashboard

1. In the **Web Console** > **Dashboards** > **Dashboards** sidebar > select a dashboard
2. Click the **Edit the Dashboard** icon in the Dashboard header.
3. In the **Edit Dashboard** page make the changes.
4. Review the layout of the dashboard. Click **Preview Panel** to see real time information in the panels.

5 Click **Save** and continue editing the dashboard. In the Save Dashboard message, click **OK**.

6 Click **Close** when you finish editing the dashboard. Modifications made to the dashboard are not saved if you close the Edit Dashboard page. Click **Cancel** if you do not want to edit the dashboard.

See “Creating a dashboard” on page 973.

See “Publishing a dashboard” on page 975.

See “Deleting a dashboard” on page 979.

See “Creating a panel” on page 984.

See “Publishing a panel” on page 997.

See “Deleting a panel” on page 1001.

Printing a dashboard

With the appropriate permissions, you can print either a dashboard. You can select a dashboard or print the home page.

To print a dashboard

1 Open the Web Console home page using the following URL:

```
http://<servername>/CCS_Web
```

2 In **Web Console** > **Dashboards** > select the **Dashboards** tab in the sidebar

3 You can select a dashboard from the All, My Private, My Published, or All Published filter.

4 Click **Print** in the Web console header section.

See “Creating a dashboard” on page 973.

See “Creating a panel” on page 984.

See “Roles and permissions” on page 969.

Emailing a dashboard URL

You can email the dashboard URL to another user. When you select a dashboard for email, your email editor opens a blank email with the dashboard URL in the body of the email. The recipient can see any assets that they have permissions for.

To email a dashboard URL

1. Open the Web Console home page using the following URL:

   `http://<servername>/CCS_Web`

2. In the **Web Console** > **Dashboards** > **Dashboards** sidebar > select the dashboard.
3. From the dashboard header click the **Email Dashboard** icon.
4. Use the email editor to complete the message.

See "Creating a panel" on page 984.

See "Creating a dashboard" on page 973.

See "Publishing a panel" on page 997.

Deleting a dashboard

You can delete any private or published dashboard that you have created. When you delete the dashboard the panels within the dashboard remain available. You cannot retrieve a deleted dashboard.

To delete a dashboard

1. In the **Web Console** > **Dashboards** > **Dashboards** sidebar > select a dashboard.
2. 3. Click the Delete the **Dashboard** icon in the Dashboard header.
3. In the **Delete Dashboard** message box, click **Yes**.

See "Creating a dashboard" on page 973.

See "Editing a dashboard" on page 977.

See "Creating a panel" on page 984.

See "Deleting a panel" on page 1001.

Predefined dashboards

The following predefined dashboards are displayed in the **Dashboards** > **Dashboards** sidebar, in the **Published** tab.

The predefined dashboards are comprised of following predefined panels:

The **Compliance Administration - Assets** dashboard has the following panels:

- **Average Compliance Score for Standard**
- **Top 10 Failed Checks by Standard**
- **Average Asset Compliance by Asset Group**

- **Data Collection Coverage Rate**
- **Top 10 Assets with Highest Risk Score by Standard**

The **Compliance Administration - Standards** dashboards has the following panels:

- **Average Compliance Score for Standard**
- **Compliance Trends by Standards**
- **Active Exceptions for Standards**
- **Top 10 Failed Checks by Standard**
- **Check Status for Standards**

The **Compliance Analysis - Mandates** dashboard has the following panels:

- **Control Status for Mandates**
- **Control Status by Assets for Mandates**
- **Top 10 Failed Control Statements for Mandates**
- **Control Status Trends for Mandates**

The **Compliance Analysis - Policies** dashboard has the following panels:

- **Control Status for Policies**
- **Top 10 Failed Controls Statements for Policies**
- **Active Exceptions for Policy Controls**
- **Control Status Trends for Policies**
- **Top 10 Assets with Highest Risk Score by Policy**

The **IT Operations** dashboard has the following panels:

- **Average Compliance Score for Standard**
- **Top 10 Failed Checks by Standard**
- **Check Status Trends for Standards**
- **Top 10 Assets with Highest Risk Score by Standard**
- **Data Collection Coverage Rate**

The **Compliance Administration – SCAP Benchmark Profile** dashboard has the following panels:

- **Compliance Score for SCAP Profile (Benchmark)**
- **Rule Status by Assets for SCAP Profile (Benchmark)**
- **Top 10 Risk Scores by Assets for SCAP Profile (Benchmark)**

The **Compliance Analysis – HIPAA Mandate** dashboard has the following panels:

- **Compliance Score for HIPAA Mandate**
- **Control Status Trends for HIPAA Mandate**
- **Mapped Policies to HIPAA Mandate**
- **Mapped vs Unmapped Control Statements in HIPAA Mandate**
- **Top 10 Failed Control Statements for HIPAA Mandate**

The **Compliance Analysis – ISO Mandate** dashboard has the following panels:

- **Compliance Score for ISO Mandate**
- **Control Status Trends for ISO Mandate**
- **Mapped Policies to ISO Mandate**
- **Mapped vs Unmapped Control Statements in ISO Mandate**
- **Top 10 Failed Control Statements for ISO Mandate**

The **Compliance Analysis – NERC Mandate** dashboard has the following panels:

- **Compliance Score for NERC Mandate**
- **Control Status Trends for NERC Mandate**
- **Mapped Policies to NERC Mandate**
- **Mapped vs Unmapped Control Statements in NERC Mandate**
- **Top 10 Failed Control Statements for NERC Mandate**

The **Compliance Analysis – PCI Mandate** dashboard has the following panels:

- **Compliance Score for PCI Mandate**
- **Control Status Trends for PCI Mandate**
- **Mapped Policies to PCI Mandate**
- **Mapped vs Unmapped Control Statements in PCI Mandate**
- **Top 10 Failed Control Statements for PCI Mandate**

The **Compliance Analysis – SOX Mandate** dashboard has the following panels:

- **Compliance Score for SOX Mandate**
- **Control Status Trends for SOX Mandate**
- **Mapped Policies to SOX Mandate**
- **Mapped vs Unmapped Control Statements in SOX Mandate**
- **Top 10 Failed Control Statements for SOX Mandate**

The **Risk - Home** dashboard has the following panels:

- Top 5 Risk Objectives with Maximum Risk
- Risk Objectives Heatmap
- Top 5 Control Categories at Highest Risk
- Top 10 Asset Containers with Maximum Risk
- Alerts and Notifications

See "Predefined panels" on page 1003.

Working with panels

You can do the following with dashboards:

- Create a panel.
  See "Creating a panel" on page 984.
- Edit a panel.
  See "Editing a panel" on page 999.
- Add a panel to a dashboard.
  See "Adding a panel to a dashboard" on page 974.
- Publish a panel.
  See "Publishing a panel" on page 997.
- Apply filters to a panel in a dashboard.
  See "Applying filters to a panel in a dashboard" on page 1002.
- Maximizing a panel in a dashboard.
  See "Maximizing a panel in a dashboard" on page 1002.
- Viewing properties of a panel.
  See "Viewing properties of a panel" on page 998.
- Extracting a panel to Excel.
  See "Extracting a panel to Excel" on page 1001.
- Delete a dashboard.
  See "Deleting a dashboard" on page 979.
- Delete a panel.
  See "Deleting a panel" on page 1001.

About the Panels page

The Panel page is the main page for panels. You can access the panel page from the following places:

- From the CCS Web Console under the Quick Tasks pane click **View Panels**.
- From the Dashboards page under the Quick Tasks pane click **View Panels**.

The Dashboard page has the following three sections:

Table 39-7 Sections of the Panel page

Section	Description
Sidebar	From the sidebar you can select either the Dashboard tab or the Panel tab.
Information area	A descriptive text about the Dashboards and the Panels for you to read.
Three panes	These comprise of the Last Viewed Dashboard, Quick Tasks, and References.

From the Panels sidebar you can choose panels from the different filters. You can use the filter dropdown to narrow the number of panels you view. The filters are the following:

Table 39-8 Filters for the Panels sidebar

Filter Name	Description
All	Use this filter to view all the panels in their different categories.
My Private	Use this filter to view all the panels you create.
My Published	Use this filter to view your published panels.
All Published	Use this filter to view all the user published panels and the predefined panels.
Search Panel	Use the search bar to find a specific panel.

From the Dashboard Taskbar you can do the following:

Table 39-9 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Import	You click this to launch the Import Panel dialog page.

From the three panes at the bottom of the Dashboards page you can do the following:

Table 39-10 Three panes on the Panels page

Name of the pane	Description
Last Viewed Dashboard	You can view the name of the most recent dashboard.
Quick Tasks	You can choose from the list some of the most common tasks.
References	You can choose from a list of Help topics.

See “Roles and permissions” on page 969.

See “Creating a panel” on page 984.

See “Publishing a panel” on page 997.

See “Deleting a panel” on page 1001.

Creating a panel

The following are some important points when creating a panel:

- You create a panel in the Web Console.
- The created panel should have a unique name.
- The created panel is listed under the category you select while creating the panel.
- The new panel in the list has the Private icon next to it.
- Only the CCS Admin or the panel creator can view a private panel.

- Publish the private panel to let other users to view the content. Other users must have the appropriate permissions to view the information.
- You can select to link a drilldown panel.
  For more information on drilldown and drill through:
  See “Difference between drilldown and drill through” on page 976.

Note: Linking a drilldown panel is applicable to the Risk panels.

When creating a trend panel, you must select for **Dimension (X-axis)** on of the following:

- Trend by Week
- Trend by Month
- Trend by Quarter
- Trend by Year

If you do not select a date, the drilldown grid will fail to load when you select the **Grid** tab. When the dimension is set to a date, the **Grid** tab is disabled.

To create a panel

1. In the **Web Console** > **Dashboards** > **Panels** page > select the **Create a Panel** icon in the **Panels** header.
2. Select the appropriate options on the General, Display, Grid, and Actions tab. Fill in the mandatory fields.

   For more information on what the options are on the tabs:
3. If the type of panel supports this option, you should select the **Display** tab and configure the display.
4. If the type of panel supports this option, you should select the **Grid** tab and configure the drill through page.
5. If the type of panel supports this option, you should select the **Actions** tab and configure the drill through options.
6. Click **OK**. Click **Apply** save your selections and continue creating the panel. Click **Cancel** if you do not want to create the panel.

Note: If you have created a new standard, asset, or policy, you should run the **Reporting Database Synchronization** job in the Control Compliance Suite CCS Console. The job is in the **Monitor** > **Jobs** view. The data may not display correctly if the job has not been run.

See “Editing a dashboard” on page 977.

See “Roles and permissions” on page 969.

See “Publishing a panel” on page 997.

See “Deleting a panel” on page 1001.

About panel options

When you create as panel you need to configure the various options under the General, Display, Grid, and Actions tab. The first tab you configure the options is the General tab. Depending on the choices you make in the General tab the other tabs will be enabled.

In order to use the Display, Grid, and Actions tabs, you must do the following under the General tab:

1. Select an option under the **Area of interest**.
2. Select an option under the **Measure (Y axis)**.
3. Select an option under the **Dimension (X axis)**.

From the Summary display type, under the General tab, if you choose either the Text or Tabular options then the Display and Actions tabs are disabled.

The following tables describe the tabs available when you create a panel.

Table 39-11 General options

Name	Description	Required
Area of interest	Area of interest is grouping data by domain. For example: Standard Compliance Management	Yes
Summary display type	Select from the following options: ■ Chart ■ Text ■ Tabular	No
Measure (Y axis)	An attribute for which the performance is measured. The value should be an number. For example: Average Asset Risk Score	Yes

Table 39-11 General options *(continued)*

Name	Description	Required
Show measure as	The selection lets you choose which type of aggregation operation is best for your dashboard. For more information, see Table 39-12	No
Dimension (X axis)	The criteria on which the attribute is measured against. For example: Asset Name You can select more than one dimension. If you have more than one dimension, see **Axis label**. When creating a trend panel, you must select date as a dimension. If you do not select a date, errors may occur when you select the **Grid Properties** tab. When the dimension is set to a date, the **Grid Properties** tab and the drill through selections are disabled. The dimension selection that is selected determines the default chart type. For more information, see About chart types	Yes
Axis label	If you select more than one dimension, you can select which of the dimension to use for the axis label. This dimension title is used in the panel.	No
Show top [X] matching results (sorted high to low, by the selected measure)	If you only want a specific number of rows in the result to display in the panel.	No
Panel name	Name of the panel is generated from the **Measure** and **Dimension** selections. You can edit the name.	Yes
Panel Category	You can select under which category the new panel is listed. The default category for new panels is Private.	No
Add Category	You can add a new category by clicking the **Add Category** icon. Enter the new category name and click **Create**. Click **Cancel** to close the Add Category popup.	No

Table 39-11 General options *(continued)*

Name	Description	Required
Filters	A filter that you specify to restrict the scope of the data in the result. You can select multiple attributes. Attributes are evaluated by using an "And" operator. If you select two or more attributes, the value for those attributes changes to the default value, which is "All". For more information, see Table 39-14	No

The type of **Measure** selection determines the available **Show measure as** aggregation options. The following are the available selections:

Table 39-12 Available Show measure as selections

Type of Measure	Default value	Alternate values
Measure is an integer.	**Sum**	The alternate selections are the following: ■ **Average** ■ **Count** ■ **Distinct count** ■ **Maximum** ■ **Minimum**
Measure is a string.	**Count**	**Distinct count**
Measure is a date.	**Count**	The alternate selections are the following: ■ **Distinct count** ■ **Maximum** ■ **Minimum**

After you have made the selections in the **General Properties** tab and selected a chart, you see the chart in the **Display Properties** tab. You can choose an alternate chart type, based on the **General Properties** tab selections.

A chart type description is available.

See “About chart types” on page 993.

Table 39-13 Chart types based on dimension selection

General properties selections	Default chart type	Alternate chart types
Dimension is a date	Area	Line
Dimension is a date	Line	Area
One dimension that is not a date and Top [X] matching results.	Bar	Column
More than one dimension and the dimensions are either strings and integers and Top [X] matching results.	Stacked bar	The alternate chart type can be any of the following: ■ Stacked column ■ Bar ■ Column
One dimension that is not a date and Top [X] matching results.	Column	Bar
One dimension is not a date	Pie	The alternate chart type can be any of the following: ■ Bar ■ Column
More than one dimension and the dimensions are either strings or integers	Stacked column	The alternate chart type can be any of the following: ■ Stacked bar ■ Bar ■ Column
More than one measure and the measures are either strings or integers	Pareto	No alternate chart type
Select in Summary display type the Tabular option.	Tabular	No alternate chart type
Only one dimension	Alert	No alternate chart type
More than one dimension and the dimensions have the same set of values	HeatMap	No alternate chart type

Table 39-13 Chart types based on dimension selection *(continued)*

General properties selections	Default chart type	Alternate chart types
One dimension and measure	Gauge	No alternate chart type

Dashboard filters refine the types of data that you display in your dashboard. Filters help you find and focus on specific information. For example, you can create a filter to show the data from one particular time period to another time period. You can create a filter to display data from only one location or division of the organization. In the panel options, you can create filters in the **Subject** section.

In the **Subject** section, you can add a filter to the selected data. You select an **Attribute**, an **Operator**, and the **Values**. The type of attribute determines the operators. The selection of the operators determines the values. The default value is "All". The available values are based on the attribute and the operator selections.

Table 39-14 Available Filters

Type of attribute	Operators
String	You can choose from the following: ■ Contains ■ Is equal to ■ Does not contain ■ Is not equal to ■ Does not start with ■ Starts with
Date	You can choose from the following: ■ Is last ■ Older than

Table 39-14 Available Filters *(continued)*

Type of attribute	Operators
Integer	You can choose from the following: - Is between - Is equal to - Is greater than or equal to - Is greater than - Is less than or equal to - Is less than - Is maximum of - Is not between - Is not equal to

You can preview the chart. You can customize the chart panel. You can select an alternate chart type or change the axis titles.

Table 39-15 Display options

Name	Description	Required
Preview Panel	The **General properties** selections determine the chart. The default chart type is selected.	No
Selected Chart Type	The **General properties** selections determine the chart type. For more information, see About chart types	No
X axis title	The title that is displayed in the panel for the X axis	Yes
Y axis title	The title that is displayed in the panel for the Y axis	Yes
X axis Label Orientation Angle (-90 to 90)	The orientation of the X label can be set from -90 to 90 degrees	No

You can preview the grid. You can customize the grid panel. You can group the columns, decide if other columns are displayed, and decide if a column is used in the post filter in the panel. You cannot remove the columns that are already selected in the **General Properties** tab.

You can select columns to be used as a filter in the **General Properties** tab > Subject or the **Grid Properties** tab.

You can apply a filter on the columns that you set as **Use as filter** when you create a panel or edit a panel. After you have applied the filters, the filters are listed beneath the panel header. If you do not see the listing, click the arrow icon on the far right on the panel.

Table 39-16 Grid options

Name	Description	Required
Update preview	The **General properties** selections determine the grid. The columns and the sort order in the preview are displayed in the resulting panel.	No
Column names	Drag a column name to the header area to group by that column.	No
Show in grid	Select columns to be added to the grid panel.	No
Use as filter	Select columns to use as a post filter in the panel.	No

The Actions tab allows for the multilevel drilldown and allow for remediation.

Note: The Action tabe is available when the **Area of Interest** under the **Geneal properties** is set to a Risk Management KPI.

Table 39-17 Actions options

Name	Description	Required
Drilldowm Options	You can select the Enable Multi Level Drilldown. You can set the panel to default.	No
Select panels for orientation/drilldown	You can select a panel from the Panel column. The selected panel will be part of the drilldown.	No
Allow Remediation	You can check this to allow for remediation on the panel.	No

The Drilldown Options allows for the created panel to enable the multi level drilldown and be set as the default panel in the drilldown.

Table 39-18 Drilldown Options

Option	Description
Enable Multi Level Drilldown	This allows for multi level drilldown from the created panel.
Set to default	This allows for the created panel to be the default panel. If this is checked then the Is Default column under the Select panels for orientation/drilldown is disabled.

The Select panels for orientation/drilldown allows you to select panels for orientation and drilldown.

Table 39-19 Select panels for orientation/drilldown

Column Names	Description
Drilldown Display Name	You can type in a name for the panel. By default, drilldown display name is the panel selected in the Panel dropdown list.
Panel	You can select a panel from the dropdown list.
Is Default	You select the panel to be the default panel in the drilldown.
+/-	You can add or remove a panel from the drilldown.

See "Creating a panel" on page 984.

See "Roles and permissions" on page 969.

About chart types

Control Compliance Suite supports many kinds of charts to help you display your information in a meaningful way for your audience. You can easily select the type of chart that you want to use when you create a panel.

The chart types are as the following:

Table 39-20 Chart type descriptions

Name	Description	Number of Y values per point	Number of series
Pie	Displays how the proportions of the data that is displayed as pie-shaped pieces, contribute to the data as a whole.	One	One
Doughnut	Similar to the pie chart, except that the chart has a hole in the center.	One	One
Column	Shows a sequence of columns that compare values across categories.	One	One or more
Stacked column	Displays multiple series of data as stacked columns. The stacked column chart is useful when you measure multiple series as a proportion against time.	One	One or more Multiple series are stacked.
Cylinder	A column chart that uses cylinder-shape items to display data. The chart type does not display any additional data, but the shape may display your data better visually.	One	One or more
Stacked cylinder	Displays multiple series of data as stacked cylinder-shaped items.	One	Two or more
Bar	Displays the comparisons among individual items. Categories are organized horizontally while the values that are measured are displayed vertically. This organization may add emphasis to comparing values and less emphasis on time.	One	One or more
Stacked bar	Displays multiple series of data as stacked bars.	One	One or more Multiple series are stacked.
Line	Displays the trends in data with the passing of time.	One	One or more
Spline	Similar to a line chart that plots a fitted curve through each data point in a series.	One	One or more

Table 39-20 Chart type descriptions *(continued)*

Name	Description	Number of Y values per point	Number of series
Area	Displays the degree of change over time. The chart also displays the relationship of the parts to a whole.	One	One or more
Spline area	An area chart that plots a fitted curve through each data point in a series.	One	One or more
Gauge	This chart displays gauge chart For example, Y-axis is Risk Score and the X-axis is a Risk Objective. The gauge shows the what is the value of the Risk Score for a selected Risk Objective.	One or Two (“Actual” and “Target”). “Target” is optional.	One
Pareto	The chart contains both bars and a line graph, where individual values are represented in descending order by bars, and the cumulative total is represented by the line.	Two (“Actual” and “Target”).	One
Heatmap	The chart displays a graphical representation of data where the values taken by a variable in a two-dimensional table are represented as colors.	One	Two
Bubble	The chart displays each plotted entity as defined in terms of three distinct numeric parameters.	Not yet supported	Not yet supported
Alert	The chart displays a list of the alerts and notifications.	NA	NA

The 2D charts can have one of the following options:

Table 39-21 Options for the 2D charts

Name	Options
Pie	Concave
Doughnut	Concave
Pie	Convex
Doughnut	Convex

Table 39-21 Options for the 2D charts *(continued)*

Name	Options
Pie	Default
Doughnut	Default
Column	Emboss
Stacked Column	Emboss
Column	Default
Stacked Column	Default
Bar	Emboss
Stacked Bar	Emboss
Bar	Default
Stacked Bar	Default
Gauge	Default
Pareto	Default
Heatmap	Default
Bubble	Default
Alert	Default

The 3D charts can have one of the following options:

Table 39-22 Options for the 3D charts

Name	Options
Column	Emboss
Stacked Column	Emboss
Column	Default
Stacked Column	Default
Bar	Emboss
Stacked Bar	Emboss

Table 39-22 Options for the 3D charts *(continued)*

Name	Options
Bar	Default
Stacked Bar	Default
Gauge	Default
Pareto	Default
Heatmap	Default
Bubble	Default
Alert	Default

See "About panel options" on page 986.

Publishing a panel

Publishing a panel allows other users to view your panel. In order to publish your panel you must either be the CCS Admin or a the panel creator.

To publish a panel

1 To the **Web Console** home page using the following URL address:

```
http://servername/ccs_web
```

2 In **Web Console** > **Dashboards** > **Panels** sidebar > select the panel.

3 Select a panel and then click **Publish a Panel** in the Dashboard header.

4 In the **Publish Dashboard** confirmation message, click **Yes**.

5 In the **Publish Dashboard** information message, click **OK**.

See "Difference between drilldown and drill through" on page 976.

See "Creating a panel" on page 984.

See "Editing a dashboard" on page 977.

See "Deleting a panel" on page 1001.

Unpublishing a panel

A published panel can be unpublished to make it unavailable to other users. Unpublishing a panel can be done by either a CCS Administrator or the panel creator. Unpublishing a panel has the following effects:

- The panel moves from the My Published filter to the My Private filter.
- The icon next tot he panel in the sidebar changes from the Public icon to the Private icon.
- Only a CCS Admin or the panel creator can view the contents.

Note: You cannot unpublish predefined panels.

To unpublish a panel

1. In **Web Console** > **Dashboards** > **Panels** sidebar > select a panel in the **Panels** > **Published** sidebar.
2. Click **Unpublish the panel** in the **Panels** sidebar header section.
3. In the **Unpublish Panel** confirmation message, click **Yes**.
4. In the **Unpublish Panel** information message, click **OK**.

See “Roles and permissions” on page 969.

See “Publishing a panel” on page 997.

Viewing properties of a panel

Each panel has a Properties icon in the Panel header. You can click on the **Properties** icon to open the Panel Properties page.

The Properties page displays the following information:

- Panel title
- Who created the panel and when the panel was created
- General properties selections
- Display properties selections
- Grid properties selections

To view a panel summary

1. Open the Web Console home page using the following URL:

   ```
   http://<servername>/CCS_Web
   ```

2. In **Web Console** > **Dashboards** > **Panel** sidebar > select a panel.

   You can also select a panel from a dashboard.

3. Click the **Properties** icon at the top right of the panel header.
4. Once you are done reviewing the panel property information click **Close** at the bottom of the browser window.

See "Applying filters to a panel in a dashboard" on page 1002.

See "Maximizing a panel in a dashboard" on page 1002.

See "Creating a panel" on page 984.

Editing a panel

In the Web Console you edit a panel that you have created.

Note: You cannot edit a predefined panel. In order for you to edit a predefined panel you make a copy and then edit the copy.

Some important points before editing a panel:

- You can edit a published panel or a panel you have created.
- The CCS Administrator or panel creator can edit a private panel.

The following list shows what you can edit in a panel:

- You can change the name of the panel.
- You can change the category of the panel.
- You can change the panel options.
- You can change the measure or dimension.
- You can add additional dimensions.
- If the panel contains two dimensions you can remove the second dimension.
- You can change the **Summary display type** of the panel.
- You can change the chart type.

When editing a trend panel, you must select for **Dimension (X-axis)** on of the following:

- Trend by Week
- Trend by Month
- Trend by Quarter
- Trend by Year

If you do not select a date, the drill through grid will fail to load when you select the **Grid** tab. When the dimension is set to a date, the **Grid** tab is disabled.

To edit a panel

1. In the **Web Console** > **Dashboards** > **Panels** sidebar > select a panel.
2. Click **Edit the Panel** icon in the Panel header.
3. In the **Edit Panel** page make the changes.
4. Click **OK** to save and close the Edit Panel page. Click **Apply** to save your modifications and continue editing the panel. Click **Cancel** if you do not want to edit the panel.

See "Creating a panel" on page 984.

See "Publishing a panel" on page 997.

See "Deleting a panel" on page 1001.

See "About chart types" on page 993.

Copying a panel

You can make a copy of any panel. The copied panel is added under the My Private filter of the Panels sidebar.

The copied panel has the following text at the beginning of the panel name:

```
Copy of <panel name>
```

If you make a copy of the same panel then the following is added to the beginning of the name:

```
Copy (X) of <panel name>
```

The (X) is the number of times that the panel has been copied.

To copy a panel

1. In **Web Console** > **Dashboards** > **Panels** sidebar > select a panel.
2. Click **Copy the panel**.
3. In the **Copy Panel** message, click **Yes**.
4. In the **Copy Panel** confirmation message, click **OK**.

See "Editing a panel" on page 999.

Extracting a panel to Excel

If the panel supports it, you can extract the drill through information from a dashboard to an Excel file. Panels that display trends do not support a drill through page.

See "Editing a panel" on page 999.

See "Publishing a dashboard" on page 975.

See "Adding a panel to a dashboard" on page 974.

To extract a panel to Excel

1. Open the Web Console home page using the following URL:

   ```
   http://<servername>/CCS_Web
   ```

2. In the **Web Console** > **Dashboards** > **Panels** sidebar > select a panel in the sidebar.

   You can select a panel in either the **Published** tab or the **Private** tab.

3. Click anywhere on the panel to open the drill through page.
4. Click **Export to Excel**.
5. Choose to open the file, save the file, or cancel the export

Deleting a panel

You can delete any private or published panel that you have created. You cannot retrieve a deleted panel.

If the deleted panel is part of a dashboard, you must remove the panel from the dashboard. If the panel is not removed from the dashboard then you see the following:

- The panel's title is changed "Untitled".
- The contents of the panel is replaced with a message stating that the panel has been deleted.

To delete a panel

1. In **Web Console** > **Dashboards** > **Panels** sidebar > select the panel.
2. Click **Delete the Panel** icon in the Panel header.
3. In the **Delete Panel** message box, click **Yes**.

See "Creating a dashboard" on page 973.

See "Editing a dashboard" on page 977.

See “Deleting a dashboard” on page 979.

See “Creating a panel” on page 984.

Applying filters to a panel in a dashboard

Panel filters refine the types of data that you display in your panel. Filters help you find and focus on specific information. For example, you can apply a filter to show the data from on particular time period to another time period. You can apply a filter to display data from only one location or division of the organization.

After you have applied a filter, the filter is listed beneath the panel header. If you do not see the listing, click the arrow icon on the far right on the panel.

To apply filters to a panel

1. To the **Web Console** home page using the following URL address:

   `http://`*`servername`*`/ccs_web`

2. In **Web Console** > **Dashboards** > **Dashboards** view, select a dashboard.
3. Select a panel and then click the **Filter** icon at the far right of the panel header.
4. In **Select Filters - Webpage Dialog** dialog box, select an available filter.
5. Click **Apply**.
6. Click **Close**.

See “Creating a panel” on page 984.

See “Roles and permissions” on page 969.

See “Editing a dashboard” on page 977.

Maximizing a panel in a dashboard

You can maximize any panel in a dashboard to better view the information in the panel.

Some important points when you maximize a panel in a dashboard:

- The panel temporarily expands to fill the dashboard.
- Other panels in the dashboard are hidden while the selected panel is maximized.
- Upon restoring the panel to the design size the other panels will be seen in the dashboard.

To resize a panel in a dashboard

1. To the **Web Console** home page using the following URL address:

   `http://`*`servername`*`/ccs_web`

2. In **Web Console** > **Dashboards** > **Dashboards** sidebar > select a dashboard.
3. Select a panel and then click the **Maximize** icon on the panel header.
4. Click the **Restore** icon on the panel header to restore the panel to the design size.

See "Applying filters to a panel in a dashboard" on page 1002.

See "Viewing properties of a panel" on page 998.

See "Creating a panel" on page 984.

Predefined panels

The Panel sidebar displays the following predefined panels:

Active Exceptions:

- Active Exceptions for Policies
  See "Active Exceptions for Policies" on page 1546.
- Active Exceptions for Policy Controls
  See "Active Exceptions for Policy Controls" on page 1548.
- Active Exceptions for Standards
  See "Active Exceptions for Standards" on page 1551.

Asset:

- Data Collection Coverage
  See "Data Collection Coverage" on page 1553.

Compliance Management:

- Assets Compliance by Assets Group
  See "Asset Compliance by Asset Group" on page 1556.
- Check Status by Assets for Standards
  See "Check Status by Assets for Standards" on page 1559.
- Check Status for Standards
  See "Check Status for Standards" on page 1561.
- Compliance Score for Standard
  See "Compliance Score for Standard" on page 1564.
- Top 10 Assets with Highest Risk Score by Standard

See "Top 10 Assets with Highest Risk Score by Standard" on page 1567.

- Top 10 Failed Checks by Standard
  See "Top 10 Failed Checks by Standard" on page 1569.
- Top 10 Passed Checks by Standard
  See "Top 10 Passed Checks by Standard" on page 1572.

Data Loss Prevention:

- Response to Data Loss Prevention Incidents
  See "Response to Data Loss Prevention Incidents" on page 1575.
- Top 10 Data Loss Prevention Incidents by Protocol
  See "Top 10 Data Loss Prevention Incidents by Protocol" on page 1577.
- Top 10 Data Loss Prevention Incidents by User
  See "Top 10 Data Loss Prevention Incidents by User" on page 1580.

HIPAA Mandate:

- Compliance Score for HIPAA Mandate
  See "Compliance Score for HIPAA Mandate" on page 1581.
- Control Status Trends for HIPAA Mandate
  See "Control Status Trends for HIPAA Mandate" on page 1585.
- Mapped Policies to HIPAA Mandate
  See "Mapped Policies to HIPAA Mandate" on page 1588.
- Coverage of Control Statements in HIPAA Mandate
  See "Coverage of Control Statements in HIPAA Mandate" on page 1590.
- Top 10 Failed Control Statements for HIPAA Mandate
  See "Top 10 Failed Control Statements for HIPAA Mandate" on page 1592.

ISO Mandate:

- Compliance Score for ISO Mandate
  See "Compliance Score for ISO Mandate" on page 1595.
- Control Status Trends for ISO Mandate
  See "Control Status Trends for ISO Mandate" on page 1599.
- Mapped Policies to ISO Mandate
  See "Mapped Policies to ISO Mandate" on page 1602.
- Coverage of Control Statements in ISO Mandate
  See "Coverage of Control Statements in ISO Mandate" on page 1604.
- Top 10 Failed Control Statements for ISO Mandate
  See "Top 10 Failed Control Statements for ISO Mandate" on page 1606.

NERC Mandate:

- Compliance Score for NERC Mandate
  See "Compliance Score for NERC Mandate" on page 1609.
- Control Status Trends for NERC Mandate
  See "Control Status Trends for NERC Mandate" on page 1613.
- Mapped Policies to NERC Mandate
  See "Mapped Policies to NERC Mandate" on page 1615.
- Coverage of Control Statements in NERC Mandate
  See "Coverage of Control Statements in NERC Mandate" on page 1617.
- Top 10 Failed Control Statements for NERC Mandate
  See "Top 10 Failed Control Statements for NERC Mandate" on page 1619.

PCI Mandate:

- Compliance Score for PCI Mandate
- Control Status Trends for PCI Mandate
  See "Control Status Trends for PCI Mandate" on page 1626.
- Mapped Policies to PCI Mandate
  See "Mapped Policies to PCI Mandate" on page 1629.
- Coverage of Control Statements in PCI Mandate
  See "Coverage of Control Statements in PCI Mandate" on page 1631.
- Top 10 Failed Control Statements for PCI Mandate
  See "Top 10 Failed Control Statements for PCI Mandate" on page 1633.

Policy Management:

- Breakdown of Policies by Status
  See "Breakdown of Policies by Status" on page 1636.
- Control Status by Assets for Mandates
  See "Control Status by Assets for Mandates" on page 1639.
- Control Status by Assets for Policies
  See "Control Status by Assets for Policies" on page 1641.
- Control Status for Mandates
  See "Control Status for Mandates" on page 1644.
- Control Status for Policies
  See "Control Status for Policies" on page 1647.
- Control Status for Policy
  See "Control Status for Policy" on page 1650.

- Top 10 Assets with Highest Risk Score by Policy
  See “Top 10 Assets with Highest Risk Score by Policy” on page 1652.
- Top 10 Failed Control Statements for Mandates
  See “Top 10 Failed Control Statements for Mandates” on page 1655.
- Top 10 Failed Control Statements for Policies
  See “Top 10 Failed Control Statements for Policies” on page 1658.
- User Acceptance of Policies
  See “User Acceptance of Policies” on page 1661.

Risk Management

- Alerts and Notifications
  See “Alerts and Notifications” on page 1706.
- Overall Risk - Security Objective
  See “Overall Risk - Security Objective” on page 1714.
- Security Objectives Heatmap
  See “Security Objectives Heatmap” on page 1715.
- Top 10 Asset Groups with Maximum Risk
  See “Top 10 Asset Groups with Maximum Risk” on page 1717.
- Top 10 Assets with Highest Risk Score
  See “Top 10 Assets with Highest Risk Score” on page 1719.
- Top 5 Business Unit Types at Highest Risk
- Top 5 Business Units at Highest Risk
  See “Top 5 Business Units at Highest Risk” on page 1721.
- Top 5 Control Categories at Highest Risk
  See “Top 5 Control Categories at Highest Risk” on page 1723.
- Top 5 Security Objectives with Maximum Risk
  See “Top 5 Security Objectives with Maximum Risk” on page 1727.

SCAP:

- Compliance Score for SCAP Profile (Benchmark)
  See “Compliance Score for SCAP Profile (Benchmark)” on page 1663.
- Rule Status by Assets for SCAP Profile (Benchmark)
  See “Rule Status by Assets for SCAP Profile (Benchmark)” on page 1666.
- Top 10 Assets By Risk Score for SCAP Profile (Benchmark)
  See “Top 10 Assets By Risk Score for SCAP Profile (Benchmark)” on page 1669.

SOX Mandate:

- Compliance Score for SOX Mandate
  See "Compliance Score for SOX Mandate" on page 1672.
- Control Status Trends for SOX Mandate
  See "Control Status Trends for SOX Mandate" on page 1677.
- Mapped Policies to SOX Mandate
  See "Mapped Policies to SOX Mandate" on page 1680.
- Coverage of Control Statements in SOX Mandate
  See "Coverage of Control Statements in SOX Mandate" on page 1682.
- Top 10 Failed Control Statements for SOX Mandate
  See "Top 10 Failed Control Statements for SOX Mandate" on page 1684.

Trends:

- Monthly Status Trend of Checks
  See "Monthly Status Trend of Checks" on page 1687.
- Compliance Trends by Standards
  See "Compliance Trends by Standards" on page 1689.
- Control Status Trends for Mandates
  See "Control Status Trends for Mandates" on page 1691.
- Control Status Trends for Policies
  See "Control Status Trends for Policies" on page 1693.
- Overall Failure Trend of Checks
  See "Overall Failure Trend of Checks" on page 1696.

Vulnerability Assessment:

- Aggregated Risk Score for CCS VM Sites
  See "Aggregated Risk Score for CCS VM Sites" on page 1697.
- Top 10 Most Common Network Vulnerabilities
  See "Top 10 Most Common Network Vulnerabilities" on page 1699.
- Vulnerabilities by CVSS Score Range
  See "Vulnerabilities by CVSS Score Range" on page 1701.
- Vulnerabilities by Severity
  See "Vulnerabilities by Severity" on page 1703.

Chapter 40

Managing custom content

This chapter includes the following topics:

About the Content view

The Content view let you create and manage custom content in the Control Compliance Suite. It also lets you map your policies to control statements and control statements to checks, questions, and third-party controls.

You can access the Content view from **Manage > Content**.

You can use the view to start the Symantec Controls Studio. You can click **Controls Studio** to open the Symantec Controls Studio.

Creating custom content

The **Symantec Controls Studio** lets you create your own custom content. 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.
- Review the Symantec-provided control statements to find any that are applicable.
- Create any needed custom control statements.

- Map the subsections of your custom regulations or frameworks to your custom control statements or to the Symantec-created control statements.
- Map control statements to questions, standards, extended controls, or any combination.
- Create new policies in the Control Compliance Suite (CCS), then while the policies are in the **Draft** state map the policies to control statements.

You use the Symantec Controls Studio to create and modify custom content. You can also use it to map user-created checks, extended controls, and questions to the included control statements. You click **Manage > Content > Controls Studio** to open the Controls Studio.

See "About custom content" on page 220.

Creating a custom mandate or section

A mandate is a regulation or framework that you must comply with. The Symantec Controls Studio lets you create the custom mandates that fit your specific needs. You can also map custom mandates to control statements in the Controls 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 Controls 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 "About custom content" on page 220.

See "About mandates" on page 222.

See "Modifying the details of a custom mandate or section" on page 1011.

See "Mapping mandates to control statements" on page 1015.

Modifying the details of a custom mandate or section

After you have created a mandate or section, you can make changes to it in the Symantec Controls Studio. You can change any of the mandate attributes or section attributes. You can also add new sections to the mandate or section.

You also use the mandates workspace to map statements to the custom mandates.

To modify a mandate or section

1 In the navigation bar in the lower left corner of the **Symantec Controls 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**.

See "About custom content" on page 220.

See "Creating custom content" on page 1009.

See "About mandates" on page 222.

See "Mapping mandates to control statements" on page 1015.

Creating custom control statements

Custom control statements let you define how you meet the requirements of the custom mandates you create.

You can create control statements from start or you can create by copying from an existing custom or predefined statements. When you copy control statements the mappings to checks, questions, and extended controls of the control statement are copied too. The mappings to policies and mandates are not copied.

To create a custom control statement from start

1. In the navigation bar in the lower left corner of the **Symantec Controls Studio** window, click **Control 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**.

To create a custom control statement from an existing statement

1. In the navigation bar in the lower left corner of the **Symantec Controls Studio** window, click **Control Statements**.
2. In the Statements area, right-click a control statement, then click **Copy**.
3. Click **Paste** to create a copy of the selected control statement.
4. In the **Heading** box of the **Details** pane, modify the name of the statement.
5. In the **Body** box of the **Details** pane, modify the control statement content.
6. Select a status for the control statement from the Status options.
7. Click **Save**.

See “About control statements” on page 224.

See “Mapping mandates to control statements” on page 1015. See “Mapping policies to control statements” on page 1017.

See “Mapping checks to control statements” on page 1019.

See “Mapping questions to control statements” on page 1021.

See “Viewing the control statements mapped to a regulation, framework, or policy ” on page 1024.

Creating Control Categories

Symantec Controls Studio lets you create multiple control categories. You can group related controls under a control category.

To create a control category

1. Navigate to **Manage > Content > Controls Studio**.
2. Right-click on **Controls Framework** and select **New Control Category**.
3. In the details pane provide the following information:

Heading	A descriptive heading for the control category.
Body	The body text that comprises the control category.
Rationale	Provide more information to describe the purpose of the control category.
Author	Displays the name of the user who created the control category. This field cannot be edited.

4. Click **Save**.

Deleting Control Categories

You can delete a control category from Controls Framework if the control category is not mapped to any control. You must delete the control to delete the control category.

To delete a control category

1. Navigate to **Manage > Content > Controls Studio > Controls Framework**
2. Right-click the control category you want to delete and select **Delete**.

   You can also click **Delete** from the task bar.
3. Click **Yes** to confirm delete.

   A control category cannot be deleted if it contains any control.
4. A Details window opens if the control category contains a control. Click **Details** to view the control statements that are mapped to that control.

Creating Controls

Symantec Controls Studio lets you create multiple controls within a control category. You can map the relevant control statements to these controls.

To create a control

1. Navigate to **Manage > Content > Controls Studio > Controls Framework**.
2. Right-click on a control category and click **New Control**.
3. In the details pane provide the following information:

Heading	A descriptive heading for the control .
Body	The body text that comprises the control .
Rationale	Provide more information to describe the purpose of the control .
Author	Displays the name of the user who created the control . This field cannot be edited.

4. Click **Save**.

Moving Controls

Symantec Controls Studio lets you move a control from one control category to another control category. All the control statements that are mapped to that control are moved along with the control to the new location.

A control can be moved only if the control statements that are mapped to that control are not mapped to any policy or mandate. The control statement must be unmapped from the policy or mandate manually before the control is moved.

To move a control

1. Navigate to **Manage > Content > Controls Studio > Controls Framework**
2. From the control categories select the control that you want to move.
3. Right-click the control and select **Move**.
4. From the drop-down list select the destination control category you want to move the control to.
5. Click **Ok**.

Deleting Controls

You can delete a control from Controls Framework if that control is not mapped to any control statement. You must unmap the control statements to delete the control.

To delete a control

1. Navigate to **Manage > Content > Controls Studio > Controls Framework**
2. From the control categories select the control that you want to delete.
3. Right-click the control and select **Delete**.

   You can also click **Delete** from the task bar.
4. Click **Yes** to confirm delete.

   A control can be deleted only if it not mapped to any control statement.
5. A Details window opens if the control is mapped to control statements. Click **Details** to view the mapped control statements.

Mapping Control Statements to Controls

Symantec Controls Studio lets you map multiple control statements to a single control.

To map one or more control statements to a single control

1. Navigate to **Manage > Content > Controls Studio > Controls Framework**.
2. From the control categories select the control that you want to map the control statements to.
3. Click **Statement Mappings**.
4. Locate the statement that you want to map to the control 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 control.
   - Click the statement and drag it to the Mapped Statements table.
5. Click **Save**.

Mapping mandates to control statements

The Symantec Controls 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.

Note: You must always map the control stataments to a section in the mandate and not to root of the mandate.

You can use the **Mandates** view to map one or more control statements to a single mandate. You can also use the **Control Statements** view to 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 Controls 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 Controls 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 Controls Studio** window, click **Control 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 Controls 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 Controls Studio** window, click **Control 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 Controls 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 custom content” on page 220.

See “About mandates” on page 222.

See “About control statements” on page 224.

See “Creating custom content” on page 1009.

See “Viewing the control statements mapped to a regulation, framework, or policy ” on page 1024.

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.

You can use the **Policies** view to map one or more control statements to a single policy. You can also use the **Control Statements** view to map a single control statement to one or more policies.

To map one or more control statements to a policy

1 In the navigation bar in the lower left corner of the **Symantec Controls 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 policy 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 policy.
   - 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 Controls 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 policy 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 policy.
   - Click the statement and drag the statement to the Available Statements table.
4. Click **Save**.

To map one or more policies to a single control statement

1. In the navigation bar in the lower left corner of the **Symantec Controls Studio** window, click **Control Statements**.
2. Click the control statement that you want to map one or more extended controls to.
3. Click **Policy Mappings**.
4. Click **All Policies** to display the list of policies.
5. Select a policy 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 policy to the **Mapped Policies** area.

To remove one or more policies from a single control statement

1. In the navigation bar in the lower left corner of the **Symantec Controls Studio** window, click **Control Statements**.
2. Click the control statement that you want to remove one or more policies from.

3 Click **Policy Mappings**.

4 In the **Mapped** area, select a policy to remove, and do one of the following:

- Click the remove icon with the red X symbol.
- Drag the check from the **Mapped** area to the **All Policies** area.

See "Creating custom content" on page 1009.

See "Creating custom control statements" on page 1011.

See "Mapping mandates to control statements" on page 1015.

See "Mapping checks to control statements" on page 1019.

See "Mapping questions to control statements" on page 1021.

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.

You can use the **Standards** view to map one or more control statements to a single check. You can also use the **Control Statements** view to map a single control statement to one or more checks.

If a standard contains one or more copied checks, you can clone the control statements that are mapped to the checks.

To map a single control statement to one or more checks

1 In the navigation bar in the lower left corner of the **Symantec Controls Studio** window, click **Control 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 Controls 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 Controls Studio** window, click **Control 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 Controls 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 Controls 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 Controls 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.

To clone the control statements that are mapped to a copied check

1. In the navigation bar in the lower left corner of the **Symantec Controls Studio** window, click **Standards**.
2. Right-click the group, standard, or check that includes copied checks.
3. Click **Clone Mappings**.
4. In the dialog box, click **Ok**.

See “Creating custom content” on page 1009.

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.

You can use the **Questions** view to map one or more control statements to a single question. You can also use the **Control Statements** view to map a single control statement to one or more questions.

Before you map questions to control statements, you must connect the Controls Studio to the Response Assessment module Server.

To connect the Controls Studio to the Response Assessment module Server

1. In the navigation bar in the lower left corner of the **Symantec Controls Studio** window, click **Response Assessment Evidence**.
2. Right-click the **Response Assessment Evidence** area on the left of the **Controls Studio** dialog, then click **Connect**.
3. In the **Select a Response Assessment module Server** dialog, enter the name or IP address of the Response Assessment module server in the **Server** field. You can also select the server name from the drop-down list.
4. Enter the port to connect to the server in the **Port**. The default port is 1977.
5. Click **OK** to connect to the server.

To map one or more questions to a single control statement

1. In the navigation bar in the lower left corner of the **Symantec Controls Studio** window, click **Control 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 Controls 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 question to the Mapped Questions area.

To remove one of more questions from single control statement

1. In the navigation bar in the lower left corner of the **Symantec Controls Studio** window, click **Control 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 Controls 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 Controls Studio** window, click **Response Assessment Evidence**.
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 Controls Studio** window, click **Response Assessment Evidence**.
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 “Creating custom content” on page 1009.

Performing policy analysis

You use the **Symantec Controls Studio** to map the mandates with which you must comply to control statements. You also map the policies you create to the control statements. Policy analysis lets you view these mappings graphically to ensure that your policies completely cover the mandates.

Both policies and mandates are mapped to control statements. Policy analysis helps you view the control statements that are mapped to the mandates you must follow. You can then analyze those control statements and locate the control statements that are not mapped to a policy. This analysis helps you to ensure that your policies correctly implement the mandates with which you must comply.

When you find gaps in coverage, you can create additional policies and map them to the control statements.

When you perform policy analysis, you do the following:

- Map control statements to the mandates with which you must comply.
- Map control statements to your policies.
- Use the analysis view to view the links between the mandates and the control statements.
- Simultaneously view the links between the policies and the control statements.
- Locate any control statements that you mapped to mandates that are not also mapped to policies.
- Repeat as necessary until all of the control statements are mapped to both mandates and policies.

See "About custom content" on page 220.

See "Creating custom content" on page 1009.

See "About the Analysis view" on page 1023.

See "Viewing the control statements mapped to a regulation, framework, or policy " on page 1024.

See "Performing a gap analysis" on page 1026.

About the Analysis view

The Analysis view lets you map policies and policy templates to regulations and best-practice frameworks. The Analysis view also lets you see the existing gaps in compliance between currently defined policies and the security regulations.

After you have analyzed the existing relationships, you can use the other views in the Symantec Controls Studio to map control statements to required regulations and frameworks.

You can drag any regulation, framework, or policy from the tree view into the Analysis pane. You can drag multiple items into the view to examine their shared control statements.

In the **Analysis** view, 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 “About custom content” on page 220.

See “Performing policy analysis” on page 1023.

See “Performing a gap analysis” on page 1026.

See “Viewing the control statements mapped to a regulation, framework, or policy ” on page 1024.

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, policies, or risks. 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, policies, and risks one at a time or in groups. Use the controls studio to map your frameworks and regulations to the control statements and map the control statements in turn to your policies or risks. 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 or risks. Through their mutual maps to shared control statements, every framework or regulation will be linked to one or more policies or risks.

To view the control statements that are mapped to a regulation, framework, policy, or risk

1. In the **Symantec Controls Studio** window, on the navigation bar, click **Analysis**.
2. In the tree view, drag and drop any regulation, framework, policy, or risks 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 > Security Objectives** to display the risks that are mapped to the control statement.
   - Right-click a control statement, and then click **Expand > All** to display all regulations, frameworks, policies, and risks linked to the control statement.
   - Right-click any object and click **Remove** to remove it from the **Analysis** view.
4. If desired, return to 3 and add an additional regulation, framework, or policy.

   You must add a security objective from the CCS Web console.

See “About custom content” on page 220.

See “Creating custom content” on page 1009.

See “Performing policy analysis” on page 1023.

See “About the Analysis view” on page 1023.

See “Performing a gap analysis” on page 1026.

Performing a gap analysis

Gap analysis helps you to review your enterprise mandates, policies, and risks. The analysis view lets you see how the mandates relate to the policies and risks that you have mapped to those mandates. Gap analysis helps you to locate areas where you need to create additional policies to close any existing gaps in your policy coverage.

To perform a gap analysis on mandates and policies

1. In the **Symantec Controls 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 Controls Studio to map these Statements to the policy.

You can perform gap analysis on risk objectives. You can create risk objectives using Risk Management on the CCS Web Console.

To perform a gap analysis on security objectives

1. In the **Symantec Controls Studio** window, click **Analysis**.
2. In the tree view, expand the Security Objectives node.
3. Locate the required security objective and drag it to the map area.

   You can create security objectives in the Risk Management on the CCS Web Console.
4. 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.
5. You can see the control statements that are not mapped to the security objective. Use the Controls Studio to map these statements to a risk objective.

   Click **Clear** to clear the map view.

See “About custom content” on page 220.

See “Creating custom content” on page 1009.

See “Performing policy analysis” on page 1023.

See “About the Analysis view” on page 1023.

See “Viewing the control statements mapped to a regulation, framework, or policy ” on page 1024.

Viewing the Control Statement Dashboard

The Control Statement Dashboard displays details of active and inactive control statements. The dashboard give a graphical view of the control statements that are mapped to Policies, Mandates, and Risks.

The dashboard also displays the following panels:

- **Percentage Distribution of Control Statements**
  This panel displays the percentage of active and inactive control statements. A control statement that is not mapped to any policy, mandate or risk is considered inactive.
  Click on the pie diagram to view details of the control statements.
- **Distribution of Active Control Statements**
  This panel displays the number of control statements mapped to policies, mandates, or risks.
- **Percentage Distribution of Active Control Statements**
  This panel displays the percentage of control statements mapped to policies, mandates, or risks.

To view the Control Statement Dashboard

1. Navigate to **Manage > Content > Controls Studio > Controls Framework**
2. Do one of the following:
   - Right-click either a control category or a control and select **Control Statements Dashboard**.
   - In the navigation bar of the tree view click **Control Statements Dashboard**.

In the **Control Statements Dashboard**. you can view the following information:

Table 40-1 Control Statements Dashboard details

Field	Description
Count of control statements	The following counts are displayed: ■ Active Control Statements ■ Inactive Control Statement ■ Total Statements

Table 40-1 Control Statements Dashboard details *(continued)*

Field	Description
Panels	The following panels are displayed: ■ Percentage Distribution of Control Statements ■ Distribution of Active Control Statements ■ Percentage Distribution of Active Control Statements
View Mode	lets you choose the format in which you want to view the details: ■ Grid View ■ Tree View
Control Statements details view	Displays the details of Active and Inactive Control Statements. The following details are displayed: ■ Control Category ■ Control ■ Control Statement ■ Mapping The statement mapping is displayed if the control statement is active. You can click on the mapping icon to view the details of the policy, mandate, or risks the control statement is mapped to.

Chapter 41

Monitoring jobs

This chapter includes the following topics:

- About secondary job filters
- About job information display
- Managing jobs
- Managing job runs
- Viewing jobs information in the details pane

About the Jobs view

The **Jobs** view is used to view all jobs that are created in Control Compliance Suite.

You can access the **Jobs** view from **Monitor** > **Jobs**.

You need the following permissions to navigate to the **Jobs** view.

- Manage Jobs
- View all Jobs

The **Jobs** view displays the following three panes:

Table pane	The table pane displays the list of jobs. Expand a job to 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 details pane displays the job details.
Filters	The filters pane is used to filter jobs. When you set the filters and click the Update icon, the table pane lists the jobs.

The taskbar of the Jobs view is divided into the following major tasks:

Common tasks	■ Run CCS Standards evaluation ■ Run collection-evaluation-reporting ■ Import assets ■ Import entitlements ■ Set up data collection ■ Run baseline job ■ Run SCAP evaluation ■ Run SCAP OVAL evaluation

Job tasks	■ Run job now ■ Refresh selected job ■ Delete job ■ Edit job ■ Schedule job ■ Configure desktop notification
Job run tasks	■ Cancel job ■ Delete job run

You can search for a job through the Jobs view.

About Global metrics and trend computation job

The Global metrics and trend computation job is a system job. This job is run to compute metrics for Standards, Policies, and the Risk objectives modules to be able to view compliance and risk data in Reports, Panels, and Dynamic dashboards.

The Global metrics and trend computation job computes metrics for Standards, Policies, and the Risk objectives modules at a specified frequency.

You can configure the Global metrics and trend computation job to follow a schedule to either run it immediately or at a specified date and time. You can configure the 'Notification' setting to notify the user about its success or failure.

The Global metrics and trend computation job now replaces the Policy and mandates metrics computation job and is provided with the following modifications:

- The computation of Global metrics for the Standards module is now a part of this job. Earlier, it was a part of Evaluation jobs.
- The computation of metrics for Risk objectives module is a new part of this job.
- Computation of trend matrices is now a part of this job. Earlier, trend matrices were computed as part of Reporting database synchronization job.

See “ About job types” on page 227.

See “Managing jobs” on page 1041.

About Queries job

The queries job is executed to collect data about the managed objects in your network. The queries collect the data for the parameters that you configure. You can execute custom or predefined queries for data collection.

You can configure the queries job to follow a schedule to either run it immediately or at a specified date and time. You can configure the 'Notification' setting to notify the user about its success or failure.

See "About queries" on page 144.

See "Configuring queries" on page 355.

See "Managing jobs" on page 1041.

See " About job types" on page 227.

About Automatic updates installation job

The Automatic updates installation job is a system job. The Automatic updates installation job automatically installs the CCS updates on the CCS components after the updates are downloaded on the CCS staging area.

You must ensure that no other jobs are in execution when you schedule the Automatic updates installation job. If any job is in the executing state after the Automatic updates installation job starts, then the executing job is aborted. After the Automatic updates installation job starts, you cannot cancel it.

You can configure the Automatic updates installation job to follow a schedule to either run it immediately or at a specified date and time. You can also configure the 'Notification' setting to notify the user about its success or failure.

See "Updating Control Compliance Suite" on page 420.

See "Managing jobs" on page 1041.

See " About job types" on page 227.

About Asset import job

The Asset import job is a user-defined job that is run to import a specific set of assets.

The Asset import job can import various types of assets from various platforms. Data for the selected asset type is imported using either a CSV data collector or ODBC data collector or a manual asset source. For data collection, the Asset import job needs to be executed first, to know whether there are any updates or additions to the assets.

The Asset import job is run to import new assets as well as update the imported assets, if required.

You can configure the Asset import job to follow a schedule to either run it immediately or at a specified date and time. You can configure the 'Notification' setting to notify the user about its success or failure. On successful completion of the Asset Import job, it generates a summary report of the number of imported assets.

See "Importing asset-specific and common fields using the default data collector" on page 458.

See "Importing asset-specific and common fields using the CSV data collector" on page 461.

See "Importing asset-specific and common fields using the ODBC data collector" on page 470.

See "Managing jobs" on page 1041.

See " About job types" on page 227.

About Automatic entitlements import job

The Automatic entitlement import job is run 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. You can configure the Automatic Entitlement Import job to follow a schedule to run at a specified time on daily basis.

To execute the Automatic entitlements import job, you must configure the system-wide entitlements settings.

See "Configuring the entitlements settings" on page 347.

See "Working with entitlements import" on page 623.

See "Configuring the automatic entitlements import" on page 626.

See "Managing jobs" on page 1041.

See " About job types" on page 227.

About Baseline job

The Baseline job is executed for the following purposes:

- To mark the job or an asset as a baseline
- To compare the records with the previous baselines

The Baseline job supports the following types of baselines to compare the assets:

- Asset-based baseline
  The baseline job lets you collect the data for an asset and use that data as a baseline to compare with other assets.
- Job-based baseline
  The baseline job lets you collect the entire result data of the baseline job and use that data to compare with other assets.

When you execute this job, the records in the newer dataset are compared against records in the older data set. You can execute the Baseline job only for those assets whose data collection and evaluation is completed.

You can configure the Baseline job to follow a schedule to either run it immediately or at a specified date and time. You can configure the ‘Notification’ setting to notify the user about its success or failure.

See “About baseline” on page 212.

See “Managing jobs” on page 1041.

See “ About job types” on page 227.

About Entitlement import job

You manually create the Entitlement import job to import entitlements of the control points that await the entitlements import. You run this job to import entitlements 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.

To configure the Entitlement import job, you must configure the system-wide entitlements settings. Only the entitlement administrator can perform the task of entitlement import.

The Entitlement import job can be configured to follow a schedule to either run it immediately or at a specified date and time. You can configure the ‘Notification’ setting to notify the user about its success or failure.

See “Working with entitlements import” on page 623.

See “Configuring the entitlements settings” on page 347.

See “Managing jobs” on page 1041.

See “ About job types” on page 227.

About External data integration job

To create an External data integration job, you must first add an external system to CCS and create a data connection. Every such external data connection creates an External data integration job. You run this job to integrate data from an external application to Control Compliance Suite. This data from an external application is represented as a data schema in Control Compliance Suite.

The External data integration job can import data using a new data schema or an existing data schema . This job integrates data from the following pre-defined systems with CCS:

- Symantec Data Loss Prevention incident data
- Symantec Response Assessment data
- Symantec CCS Vulnerability Manager data

However, a user may integrate any other system as well.

You can configure the External data integration job to follow a schedule to run immediately or at a specified date and time. You can also configure the ‘Notification’ setting to notify the user about its success or failure.

See “About External Data Integration” on page 210.

See “Configuring data systems” on page 761.

See “Configuring data connections” on page 773.

See “Managing jobs” on page 1041.

See “ About job types” on page 227.

About Import assets and agents job

The Import assets and agents job is a system job. The Import assets and agents job is executed to import the agents that are registered with the CCS Manager and the assets associated with these agents. In order to import the agent, it needs to be registered with the CCS Manager which is done with the help of agent registration utility.

The Import assets and agents job provides an option to import assets either from registered ESM agents or from ESM Data Collector. You can import assets and agents using ESM Data Collector only if you have pre-configured ESM Managers.

If you do not choose to use ESM Data Collector, the import job by default uses the registered agents to import assets.

You can configure the Import assets and agents job to follow a Schedule to either run it immediately or at a specified date and time. You can also configure the 'Notification' setting to notify the user about its success or failure. On successful completion of the job, a summary report is generated that specifies the number of imported agents and associated assets.

See "Importing assets and agents " on page 556.

See "Managing jobs" on page 1041.

See " About job types" on page 227.

About Remediation verification job

The Remediation verification job is a system-job. This job is executed to verify the remediation status for assets that you have set for remediation in the evaluation job, as they are non-compliant with the CCS compliance criteria.

The Remediation verification job appears only if you enable the closed-loop verification. The closed-loop verification feature of Control Compliance Suite lets you reevaluate the remediated assets for compliance. The closed-loop verification feature is available only for the ServiceDesk remediation action.

You must configure the remediation settings to create ServiceDesk tickets and to send email notifications for asset remediation.

You cannot modify, schedule or delete the Remediation verification job.

See "About automatic remediation" on page 534.

See "About manual remediation" on page 535.

See "About closed-loop verification" on page 535.

See "Managing jobs" on page 1041.

See " About job types" on page 227.

About Report data purge job

The Report data purge job is executed to purge historical and summary data from the reporting database. To execute the Report data purge job, you must specify the global and individual purge settings.

You can configure the Report data purge job to follow a schedule to either run it immediately or at a specified date and time. You can also configure the 'Notification' setting to notify the user about its success or failure.

See "About the purge settings" on page 343.

See "About data purging in the reporting database" on page 346.

See "Configuring the purge job schedule" on page 346.

See "Managing jobs" on page 1041.

See " About job types" on page 227.

About Report data synchronization job

The Report data synchronization job synchronizes data from different applications such as Standards, Assets, Policies and so on from production database to reporting database. The Report data synchronization job operates in the following modes:

- Automatic
  The Automatic mode lets you configure the execution of this job on completion of selected jobs.
- Scheduled
  The Scheduled mode lets you schedule the job to start immediately or at a specific date and time.

You must execute the Report data synchronization job before you schedule a report for generation. Only administrators can run the Report data synchronization job. You can configure the 'Notification' setting to notify the user about its success or failure.

See "About data synchronization" on page 947.

See "Selecting the CCS Manager to synchronize the reporting database" on page 342.

See "Synchronizing the reporting database" on page 342.

See "Managing jobs" on page 1041.

See " About job types" on page 227.

About Report generation job

The Report generation job is a user-defined job that is run to generate reports using data from the reporting database. To generate reports, the data in the production database must be synchronized with the reporting database using the Report data synchronization job. However, the Report generation job generates a blank report in case the data in the production database is not synchronized with the reporting database. Hence, you must execute the Report Synchronization job first in order to run the Report generation job.

The Report generation job generates the following types of reports:

- Asset reports
- Standard reports
- Entitlements reports
- Policy reports
- Audit reports

CCS provides predefined report templates to generate reports. You can customize some of the report templates based on your requirement.

You can configure the Report generation job to add or remove viewers for the generated reports. You can also configure the job to send an email of job completion information to selected users when the report is ready. Further, you can also export the reports in various formats.

You can schedule the generation of reports from the appropriate templates either immediately or at a specified date and time. You can also configure the 'Notification' setting to notify the user about its success or failure.

See "Working with reports " on page 956.

See "Editing a report generation job" on page 966.

See "Managing jobs" on page 1041.

See " About job types" on page 227.

About SCAP evaluation job

The SCAP evaluation job collects data from assets and evaluates them against the SCAP content. You create the SCAP evaluation job to evaluate the assets against the SCAP benchmarks by selecting a profile. Before you evaluate, you must import the SCAP benchmarks into CCS. The CCS Manager performs the task of data collection and evaluation of SCAP content.

You can configure the SCAP evaluation job to follow a schedule to either run it immediately or at a specified date and time. You can configure the 'Notification' setting to notify the user about its success or failure.

See "Evaluating assets against the SCAP benchmarks" on page 750.

See "Status details for SCAP evaluation jobs" on page 1053.

See “Managing jobs” on page 1041.

See “ About job types” on page 227.

About SCAP OVAL evaluation job

The SCAP OVAL evaluation job is executed to evaluate assets against the OVAL definitions. Before you evaluate, you must import the OVAL definitions into CCS.

You can configure the SCAP OVAL evaluation job to follow a schedule to either run it immediately or at a specified date and time. You can configure the ‘Notification’ setting to notify the user about its success or failure.

See “Evaluating assets against OVAL definitions” on page 752.

See “Managing jobs” on page 1041.

See “ About job types” on page 227.

About Tiered dashboard update job

You execute a Tiered dashboard update job to edit or update the created Tiered dashboards. A Tiered dashboard is a hierarchical representation of roll-up data, where roll-up data is a summary of the evaluation results of the standard's checks and the bv-control query results. A hierarchy refers to the creation of sections and nodes which are scopes that represent either a geographical location or a business unit.

Before you run the Tiered dashboard update job, you must synchronize the data in the Reporting database by running the Reporting database synchronization job.

You can configure the Tiered dashboard update job to follow a schedule to either run it immediately or at a specified date and time. You can also configure the ‘Notification’ setting to notify the user about its success or failure.

See “Managing jobs” on page 1041.

See “ About job types” on page 227.

About job filters

The **Filters** pane in **Jobs view** displays the primary filters. Use these filters to determine the display of the required jobs. If you select no job type, then the pane displays all job types.

Control Compliance Suite provides the following default primary filters to filter jobs:

Job type

Lets you filter the jobs according to the type of the job.

The following types of jobs can be filtered:

- **Asset import**
- **Baseline job**
- **Entitlement import**
- **Automatic entitlements import**
- **Evidence collection**
- **Report generation**
- **Report data synchronization**
- **Report data purge**
- **Tiered dashboard update**
- **Evaluation**
- **Data collection**
- **Collection-Evaluation-Reporting**
- **Remediation verification**
- **Policy metrics calculation**
- **SCAP evaluation**
- **SCAP OVAL evaluation**
- **External data integration**
- **Automatic Updates Installation Job**

Last run date

Lets you filter the jobs according to the last completed job run date or time.

You can select one of the following options:

- **All**
- **Before**
- **After**
- **Between**

Select a filter and click the **Update** icon to view the filtered jobs in the table pane.

Click the **Select all** icon in the **Filters** pane to simultaneously select all job types. Click **Deselect all** to uncheck all check boxes for job types.

After you use the primary filters for the jobs you want displayed, use the secondary filters to refine the jobs display.

See “About jobs” on page 226.

See “ About job types” on page 227.

About secondary job filters

Jobs view of Control Compliance Suite provides the **View jobs** field with the following options for secondary job filters:

All jobs	Displays the jobs that you have created, the jobs that you can view, and the system jobs that you can view
My jobs	Displays the jobs that you have created
System jobs	Displays the system jobs that you can view **Note:** The **View jobs** field displays the **System jobs** option only if the job type that you selected in the **Filters** pane contains system jobs. The jobs display for all filters is restricted to those jobs that you can view.

About job information display

You can manage the display of jobs in the jobs table of **Jobs view**.

Use the following options to manage the display of job information:

- Use **Column Chooser** to select the columns for inclusion in the jobs table.
  Click the **Column Chooser** icon, and check the header boxes of the columns that you want included in the jobs table.
  Column Chooser displays the following column headers for Job details: Creator, Duration, End date, Next run date, Start date, Status, Status details, and Type.
  Column Chooser displays the following column headers for Job run details: Duration, End date, Status, and Status details.
- Isolate the information in one table column for viewing.
  Drag the table header of a column above the jobs table. This action isolates the job information in one column of the jobs table for better viewing.
- On **Settings**, set the number of jobs and job runs that the table pane displays.

Managing jobs

You can perform the following operations in the **Jobs** view:

- Create jobs
  See “Creating jobs” on page 1046.

- Edit a job
  See “Editing a job” on page 1042.
- Run a job now
  See “Running a job now” on page 1044.
- Schedule a job
  See “Scheduling jobs” on page 1043.
- Delete a job
  See “Deleting jobs” on page 1043.
- Refresh the jobs view
  See “Refreshing the jobs view” on page 1045.
- Search for a job
  See “Searching for a job” on page 1045.

Editing a job

To edit a job, right-click a job and use the Edit job option from the menu. You can also use the taskbar and the **Tasks** menu to edit jobs.

You can only edit one job at a time. Every job type has unique edit options. Only user-defined jobs are editable.

The following users can edit jobs:

- Users who have created the jobs
- CCS administrators

To edit jobs

1. Click **Monitor** > **Jobs**, and select the job in the Jobs view.
2. Right-click the job and click **Edit job**.
3. In the wizard of the respective job, complete the steps on the wizard screens. The job is edited.

See “About jobs” on page 226.

See “Scheduling jobs” on page 1043.

See “Deleting jobs” on page 1043.

See “Running a job now” on page 1044.

See “Canceling a job run” on page 1057.

See “Searching for a job” on page 1045.

See “Refreshing the jobs view” on page 1045.

See “Deleting a job run” on page 1058.

See “Creating jobs” on page 1046.

Scheduling jobs

You have the following options to schedule a job:

- Right-click a job and use the Schedule job option on the menu.
- Use the taskbar and the **Tasks** menu.

You can only schedule one job at a time.

To schedule a job

1. Click **Monitor** > **Jobs**, and select the job.
2. Right-click the job, and click **Schedule job.**
3. In the **Schedule** dialog box, select either or both of the following:
   - If you want a one-time run of the job, check **Run now**.
   - If you want recurrent runs of the job, select **Run periodically** and enter the relevant information.
4. In the **Run Periodically Options** box, if you want to run the job only one time, select **Run once**. If you want recurrent runs after intervals, enter the number of days in the **Run every _ days** field.
5. Click **OK**.

See “About jobs” on page 226.

See “Editing a job” on page 1042.

See “Deleting jobs” on page 1043.

See “Running a job now” on page 1044.

See “Canceling a job run” on page 1057.

See “Searching for a job” on page 1045.

See “Refreshing the jobs view” on page 1045.

See “Deleting a job run” on page 1058.

See “Creating jobs” on page 1046.

Deleting jobs

To delete a job, right-click the job and select the Delete job option from the menu. You can also use the taskbar and the **Tasks** menu to delete jobs.

You can delete multiple jobs. However, you can only delete user-defined jobs.

To delete a job

1. Click **Monitor** > **Jobs**, and select the job.
2. Right-click the job and click **Delete job**. In the confirmation message, click **Yes** and the job is deleted.

See "About jobs" on page 226.

See "Editing a job" on page 1042.

See "Scheduling jobs" on page 1043.

See "Running a job now" on page 1044.

See "Canceling a job run" on page 1057.

See "Searching for a job" on page 1045.

See "Refreshing the jobs view" on page 1045.

See "Deleting a job run" on page 1058.

See "Creating jobs" on page 1046.

Running a job now

You can right-click a job and use the option to run jobs from the menu to run the job. You can also use the taskbar and the **Tasks** menu to run jobs.

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 226.

See "Editing a job" on page 1042.

See "Scheduling jobs" on page 1043.

See "Deleting jobs" on page 1043.

See "Canceling a job run" on page 1057.

See "Searching for a job" on page 1045.

See "Refreshing the jobs view" on page 1045.

See "Deleting a job run" on page 1058.

See “Creating jobs” on page 1046.

Searching for a job

Use the **Search** option to search for a job. You can also use any of the columns to search for jobs. For example, type Failed to see the job runs with the Failed status.

You can also use the Filters pane to filter jobs. Control Compliance Suite performs a search only on the records available on the user interface.

To search for a job

1. Click **Monitor** > **Jobs**, and type the name of the job in the **Search** box available in the table pane.
2. Click the **Search** icon. The table pane provides the search results.

See “About jobs” on page 226.

See “Editing a job” on page 1042.

See “Scheduling jobs” on page 1043.

See “Deleting jobs” on page 1043.

See “Running a job now” on page 1044.

See “Canceling a job run” on page 1057.

See “Refreshing the jobs view” on page 1045.

See “Deleting a job run” on page 1058.

See “Creating jobs” on page 1046.

Refreshing the jobs view

You can refresh the Jobs view or the selected jobs.

To see the current status of a job or a job run, you can refresh the job.

To refresh a specific job

1. Select the job that you want to refresh.
2. Do one of the following:
   - On the **Tasks** menu, on **Job tasks**, click **Refresh selected job**.
   - Right-click the selected job and click **Refresh selected job**.
   - On the taskbar, click **Refresh selected job**.

See “About jobs” on page 226.

See “Editing a job” on page 1042.

See "Scheduling jobs" on page 1043.

See "Deleting jobs" on page 1043.

See "Running a job now" on page 1044.

See "Canceling a job run" on page 1057.

See "Searching for a job" on page 1045.

See "Deleting a job run" on page 1058.

See "Creating jobs" on page 1046.

Creating jobs

You can create some jobs from the Jobs view. Right-click and select an option in the table pane. You can also use the **Common Tasks** tab to create jobs.

You can create the following jobs from the Jobs view:

- Baseline job
- Evaluation job
- Data collection job
- Entitlements import job
- Import assets job

To create a job from the Jobs view

1. Click **Monitor** > **Jobs**, right-click in the empty grid in the table pane and select the job that you want to create.

   The application launches the wizard that is associated with the respective job.

2. Complete the steps in the wizard to create the job.

See "About jobs" on page 226.

See "Editing a job" on page 1042.

See "Scheduling jobs" on page 1043.

See "Deleting jobs" on page 1043.

See "Running a job now" on page 1044.

See "Canceling a job run" on page 1057.

See "Searching for a job" on page 1045.

See "Deleting a job run" on page 1058.

See "Refreshing the jobs view" on page 1045.

Setting the number of jobs and job runs in the jobs table

Configure the number of jobs and job runs to manage the display of jobs and job runs in the jobs table of **Jobs view**.

To set the number of jobs and job runs that is displayed in the jobs table

1. Click **Settings > General**.
2. In the left pane, expand **Application Customization**, and click **Job Count**.
3. On the **Job Count** page, enter values for the **Number of Jobs** and **Number of Job Runs** fields.

   The values you enter set the limits for the number of jobs and job runs that the jobs table of **Jobs view** displays.

About job results in Jobs view

Control Compliance Suite provides you the option to view generated reports, data collection, and evaluation details for some jobs. To use the option, right-click the job and click the option to view results for the job.

Use the **View Report** option for Report generation jobs to view the generated reports.

Use the **Data Collection Details** option to view data collection details for the following jobs:

- Data collection
- Collection-Evaluation-Reporting

Use the **Evaluation Details** option to view evaluation details for the following jobs:

- Evaluation
- Collection-Evaluation-Reporting
- SCAP evaluation
- SCAP OVAL evaluation

Viewing a generated report from Jobs view

Control Compliance Suite provides you the option to view reports from **Jobs view**. Alternatively, click **Reporting > My Reports** to view reports.

The option to view job results is only available for some types of jobs. The **View Report** option is available for the Report generation jobs whose runs have been completed, even with errors.

Control Compliance Suite disables the **View Report** option in the following instances:

- For the Report generation jobs that display a status other than Completed
- For users who do not have the requisite permissions

To view a generated report from Jobs view

1. In the jobs table of Jobs view, select a Report generation job.
2. Right-click the job, and click **View Report** to view the generated report in the Crystal Report Viewer.

Viewing data collection details from Jobs view

Control Compliance Suite provides you the option to view data collection details for the following jobs from **Jobs view**:

- Data collection
- Collection-Evaluation-Reporting

The option is only available for the jobs whose status indicates Completed. You can view the details if you have the necessary permissions.

The **Data Collection Details** page displays the information that pertains to multiple standards. The page displays the asset type in addition to the category of the asset.

Alternatively, click **Manage > Assets** to view the data collection information in the details pane of **Asset System view**.

To view Data Collection Details from Jobs view

1. In the jobs table of **Jobs view**, select a Data collection job or Collection-Evaluation-Reporting job.
2. Right-click the job, and click **Data Collection Details** to see the **Data Collection Details** page.

Viewing evaluation details from Jobs view

Control Compliance Suite provides you the option to view the details of evaluation job runs from **Jobs view**.

The option is only available for the jobs whose status indicates Completed. You can view the details if you have the necessary permissions.

Jobs view provides you the option to view evaluation details for the following jobs:

- Evaluation
- Collection-Evaluation-Reporting
- SCAP evaluation
- SCAP OVAL evaluation

You can also access evaluation results from the following views:

- **Evaluation Results view**: Click **Monitor > Evaluation Results** to view evaluation information.
- **Standards view**: Select a standard and run an evaluation job to view evaluation information in the details pane.
- **Asset System view**: Select an asset and run an evaluation job to view evaluation information in the details pane.

To view Evaluation Result Details from Jobs view

1. In the jobs table of **Jobs view**, select the job.
2. Right-click the job, and click **Evaluation Details** to see the **Evaluation Result Details** page.

About job desktop notifications

If you have enabled desktop notification for jobs, Control Compliance Suite displays **CCS Job Notification** on your desktop when your job is Started, Completed, Aborted, or Failed. Your desktop displays these notifications for a fleeting period.

CCS Job Notification displays the **Job** and **Status** fields that indicate the type and the status of the job.

Click on the notification for the system to display **Jobs view**.

You can configure or disable job desktop notifications in the following ways:

- In **Jobs view**, on **Job tasks**, click **Configure desktop notification.**
- Click the **Options** icon on the desktop notification, **CCS Job Notification**.

Configuring job desktop notifications

Configure job desktop notification to receive notifications about the status of the jobs that you can view.

In addition to the given procedure, you can click the **Options** icon on the desktop notification, **CCS Job Notification**, to access the **Job Desktop Notification** box and configure notifications.

Note: Ensure that you open the application server TCP port through a firewall for communication from the Application server to the Control Compliance Suite console. If the port is not open, you receive no notification. The job notification feature uses the same port as the Application server for real-time notifications.

To configure job notifications

1. In **Jobs view**, on **Job tasks**, click **Configure desktop notification**.
2. In the **Job Desktop Notification** box, check **Enable job notification** to activate notifications.
3. Do one of the following:

- To receive notifications for the jobs that you have created, click **Show notification for my jobs**.
- To receive notifications for all jobs that you can view, click **Show notification for all jobs**.

About monitoring jobs

Control Compliance Suite provides you the ability to monitor a job when you initiate it. The jobs table displays the job run that you initiated at the level that follows the job row. If you initiate multiple job runs, the jobs table displays the runs in multiple rows that follow the job row.

Jobs view provides you the following options to monitor your jobs:

- Refresh a job and view its status.
- View the status of a job in the **Status column** of the jobs table in **Jobs view**.
- View the details of a status for a job in the **Status details** column of the jobs table in **Jobs view**.

About job status

To help you monitor your jobs, Control Compliance Suite displays the status of jobs. The **Status** column of the jobs table in **Jobs view** provides the statuses of jobs.

The **Status** column displays the following statuses for jobs:

Job status	Description
Executing	The job run is in progress.
Completed	The job run is complete and results are available. Results are unavailable for the jobs that are completed with errors.
Failed	The job run encountered issues.
Aborted	The user has canceled the job run.
Awaiting manual review	Only asset import jobs display this status. The status indicates that the job needs user intervention. The user right-clicks **Review records**, and performs the actions that ensure job completion.

Status details for Report generation jobs

Monitor job progress by means of the status available for jobs in the **Status** column of the jobs table in **Jobs view**. The information in the **Status details** column of the table supplements the information in the **Status** column. The column adds precise information about the stages in the progress of the job.

The **Status details** column displays details about the Scope resolution, Preprocessing, Report generation, Post-processing, User notification, and Permission stamping stages of report generation.

Table 41-1 Status details: Report generation jobs

Job stage	Status details	What the details mean
Scope resolution	**Resolving trustee information**	Derives trustee information for report processing
	Resolving policy information	Derives policy information for report processing
	Resolving standards information	Derives standards information for report processing
	Resolving asset information	Derives pertinent asset information for report processing

Table 41-1 Status details: Report generation jobs *(continued)*

Job stage	Status details	What the details mean
Preprocessing	**Preparing data for report**	Prepares the data from many sources for the report
Report generation	**Generating report**	Undertakes the job of generating the report
Post-processing	**Removing provisional data**	Removes the data that was created during report generation
User notification	**Sending email notification**	Intimates the user who wants the report as an email attachment
Permission stamping	**Assigning view permissions for report**	Determines the permissions that are required to view the generated report

Note: To update the status details for a Report generation job, right-click the job and click **Refresh selected job**.

Status details for Evaluation jobs

Control Compliance Suite supplements the status information of an Evaluation job with details about the status. The **Status details** column of the jobs table in **Jobs view** provides details of the Initialization, Processing, and Post-processing stages in the progress of Evaluation jobs.

Table 41-2 Status details: Evaluation jobs

Job stage	Status details	What the details mean
Initialization	**Resolving assets**	Creates a list of assets for the DPS to route the evaluation job to the DPS Evaluator
	Resolving standards	Gets the latest version of the standards for the DPS
Processing	**Evaluating x assets for y standards. Results expected: z**	Indicates the number of assets from the total asset count for which evaluation is in progress

Table 41-2 Status details: Evaluation jobs *(continued)*

Job stage	Status details	What the details mean
	Evaluation results received: x/y	Indicates the number of assets from the total asset count that has been evaluated
Post-processing	**Processing results: x/y**	Uploads the evaluation results to the application server
	Storing results: x/y	Stores the evaluation results in the production database

Note: To update the status details for an Evaluation job, right-click the job and click **Refresh selected job**.

Status details for SCAP evaluation jobs

Control Compliance Suite supplements the status information of an SCAP evaluation job with details about the status. The **Status details** column of the jobs table in **Jobs view** provides details of the Initialization, Processing, and Post-processing stages in the progress of SCAP evaluation jobs.

Table 41-3 Status details: SCAP evaluation jobs

Job stage	Status details	What the details mean
Initialization	**Resolving assets**	Creates a list of assets for the DPS to route the evaluation job to the DPS Evaluator
	Resolving SCAP profile	Gets the SCAP profile from the production database for the DPS
Processing	**Evaluating x/y assets**	Indicates the number of assets from the total asset count for which evaluation is in progress
	Assets evaluated: x/y	Indicates the number of assets from the total asset count that has been evaluated

Table 41-3 Status details: SCAP evaluation jobs *(continued)*

Job stage	Status details	What the details mean
Post-processing	**Storing results: x/y**	Stores the SCAP evaluation results in the production database

Note: To update the status details for an SCAP evaluation job, right-click the job and click **Refresh selected job**.

Status details for SCAP OVAL evaluation jobs

Control Compliance Suite supplements the status information of an SCAP OVAL evaluation job with details about the status. **Status details** of the jobs table in **Jobs view** provides details of the Initialization, Processing, and Post-processing stages in the progress of SCAP OVAL evaluation jobs.

Table 41-4 Status details: SCAP OVAL evaluation jobs

Job stage	Status details	What the details mean
Initialization	**Resolving assets**	Creates a list of assets for the DPS to route the evaluation job to the DPS Evaluator
	Resolving OVAL definition	Gets the SCAP OVAL definition from the production database for the DPS
Processing	**Evaluating x/y assets**	Indicates the number of assets from the total asset count for which evaluation is in progress
	Assets evaluated: x/y	Indicates the number of assets from the total asset count that has been evaluated
Post-processing	**Storing results: x/y**	Stores the SCAP OVAL evaluation results in the production database

Note: To update the status details for an SCAP OVAL evaluation job, right-click the job and click **Refresh selected job**.

Status details for Data collection jobs

Control Compliance Suite supplements the status information of a Data collection job with details about the status. **Status details** in the jobs table in **Jobs view** provides details for the Initialization, Processing, and Post-processing stages in the progress of Data collection jobs.

Table 41-5 Status details: Data collection jobs

Job stage	Status details	What the details mean
Initialization	**Resolving assets**	Creates a list of assets for the DPS to route the data collection job to a DPS Collector
	Resolving standards	Gets the latest version of the standards for the DPS
Processing	**Collecting data for x entities on y assets. Results expected: z**	Indicates the number of assets from the total asset count for which data collection is in progress
	Data collection results received : x/y	Indicates the number of assets from the total asset count for which data has been collected
Post-processing	**Processing results : x/y**	Uploads the data collection results to the application server
	Storing results : x/y	Stores the data collection results in the production database

Note: To update the status details for a Data collection job, right-click the job and click **Refresh selected job**.

Status details for Asset import jobs

Control Compliance Suite supplements the status information of an Asset import job with details about the status. **Status details** of the jobs table in **Jobs view** provides status details for the Processing, and Post-processing stages in the progress of Asset import jobs.

Table 41-6 Status details: Asset import jobs

Job stage	Status details	What the details mean
Processing	**Resolving x scopes for asset import**	Data collectors retrieve assets in the specified scopes (sites or list of assets) to send to the application server.
	Data collected for scopes: x/y	Indicates the number of scopes from the total count of scopes for which data has been collected.
Post-processing	**Processing results: x/y**	Indicates the number of assets from the total count of assets for which results are uploaded from the DPS to the application server for processing.

Note: To update the status details for an Asset import job, right-click the job and click **Refresh selected job**.

Status details for Collection-Evaluation-Reporting jobs

Control Compliance Suite supplements the status information of a Collection-Evaluation-Reporting job with details about the status. The jobs table in **Jobs view** provides details for the various stages in the progress of Collection-Evaluation-Reporting jobs.

Status details of the jobs table displays status details for the following stages of data collection in Collection-Evaluation-Reporting jobs: Initialization, Processing, and Post-processing.

Status details of the jobs table displays status details for the following stages of evaluation in Collection-Evaluation-Reporting jobs: Initialization, Processing, and Post-processing.

Status details of the jobs table displays details about the following stages for reporting in Collection-Evaluation-Reporting jobs: Scope resolution, Preprocessing, Report generation, Post-processing, User notification, and Permission stamping.

Note: To update the status details for a Collection-Evaluation-Reporting job, right-click the job and click **Refresh selected job**.

Managing job runs

You can perform the following operations on job runs:

- Cancel a job run
  See "Canceling a job run" on page 1057.
- Delete a job run
  See "Deleting a job run" on page 1058.

Canceling a job run

Right-click a job and select the cancel option from the menu to cancel the job run. You can also use the taskbar and the **Tasks** menu to cancel job runs.

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 the Executing state.

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 226.

See “Editing a job” on page 1042.

See “Scheduling jobs” on page 1043.

See “Deleting jobs” on page 1043.

See “Running a job now” on page 1044.

See “Searching for a job” on page 1045.

See “Refreshing the jobs view” on page 1045.

See “Deleting a job run” on page 1058.

See “Creating jobs” on page 1046.

Deleting a job run

Right-click a job run and use the Delete job run option to delete a job run. You can also use the taskbar and the **Tasks** menu to delete job runs. You can only delete the job runs that are in the Completed, Aborted, or Faulted statuses.

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 click **Delete job run**. The job run is deleted.

See “About jobs” on page 226.

See “Editing a job” on page 1042.

See “Scheduling jobs” on page 1043.

See “Deleting jobs” on page 1043.

See “Running a job now” on page 1044.

See “Canceling a job run” on page 1057.

See “Searching for a job” on page 1045.

See “Refreshing the jobs view” on page 1045.

See “Creating jobs” on page 1046.

Viewing jobs information in the details pane

You can view jobs information in the details pane of the Jobs view.

The details pane displays all information about the selected job or the job run under the following tabs:

- General tab
  See "Job details pane- General tab" on page 1059.
- Schedule tab
  See "Job details pane- Schedule tab" on page 1060.
- Job configuration tab
  See "Job details pane - Job configuration tab" on page 1061.
- Summary tab
  See "Job run details pane- Job run summary tab" on page 1060.
- Failures tab
  See "Job run details pane- Failures tab" on page 1060.
- Template tab
  See "Job details pane- Template tab" on page 1060.

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.

Job details pane- General tab

The **General** tab of the Job details pane provides general information about the selected job. The information in this tab is read-only.

The **General** tab provides 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

See "Scheduling jobs" on page 1043.

Job details pane- Schedule tab

The **Schedule** tab of the Job details pane provides information about the scheduling of the selected job. The information under this tab is read-only.

The **Schedule** tab provides the following details about jobs:

Run on	Displays the date and time for the job to run or displays the next job execution time
Recurring	Indicates whether the job is recurrent
Run every	Displays the interval between two scheduled runs

See "Scheduling jobs" on page 1043.

Job run details pane- Job run summary tab

The **Job run 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.

See "Scheduling jobs" on page 1043.

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.

You can launch a new window that displays the errors. The **Job Run error** window provides information about the data collector errors of the selected job run. The information in this window is read-only. You can export the grid to the desired location with the desired file format.

See "Scheduling jobs" on page 1043.

Job details pane- Template tab

The **Template** tab of the Job details pane specifies the template that is used for creating the report. The information in this tab is read-only.

The **Template** tab provides the following information about the report:

Report title	Displays the name of the report

Report type	Displays the type of the 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

See “Scheduling jobs” on page 1043.

Job details pane - Job configuration tab

This tab shows the configuration details of the job. The job type determines the nature of the data that the tab displays.

Monitoring evaluation results

This chapter includes the following topics:

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 1065.

See “Evaluation Results details pane - Evaluation Summary tab” on page 1065.

See “Evaluation Results details pane - Assets Evaluated tab” on page 1066.

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 And	Lists all the evaluation jobs that were run during a specific time period. 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.

Note: When you upgrade Control Compliance Suite to 10.5.1, you have to reapply the filter options to display or refine the evaluation job runs.

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 1065.
- Evaluation Summary
  See "Evaluation Results details pane - Evaluation Summary tab" on page 1065.
- Assets Evaluated
  See "Evaluation Results details pane - Assets Evaluated tab" on page 1066.

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.

See "About the Evaluation Results view" on page 1063.

See "Evaluation Results details pane - General tab" on page 1065.

See "Evaluation Results details pane - Evaluation Summary tab" on page 1065.

See "Evaluation Results details pane - Assets Evaluated tab" on page 1066.

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 displays the following for an evaluation job run of a standard:

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.

The **Evaluation Summary** tab displays the following for an SCAP evaluation job run:

Benchmark	Lists the SCAP benchmark that was evaluated in the evaluation job.
Profile	Lists the profiles of the SCAP benchmark that were evaluated in the evaluation job.
Risk Score	Lists the risk score of the assets that are evaluated against the profile.
Compliance Score	Lists the compliance score of the profile.

The **Evaluation Summary** tab displays the following for an SCAP OVAL evaluation job run:

OVAL file name	Lists the name of the standalone OVAL file that was evaluated in the evaluation job.

See “About the Evaluation Results view” on page 1063.

See “Evaluation Results details pane - General tab” on page 1065.

See “Evaluation Results details pane - Evaluation Summary tab” on page 1065.

See “Evaluation Results details pane - Assets Evaluated tab” on page 1066.

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.

See “About the Evaluation Results view” on page 1063.

See “Evaluation Results details pane - General tab” on page 1065.

See “Evaluation Results details pane - Evaluation Summary tab” on page 1065.

See “Evaluation Results details pane - Assets Evaluated tab” on page 1066.

Chapter 43

Managing routing rules

This chapter includes the following topics:

Creating a routing rule

You must first create a routing rule by specifying a condition and scope for the rule. This is the standard way of creating a routing rule.

To create a routing rule

1 In the **Manage Routing Rules – Settings** view, click **Create**.

2 In the **Specify a Rule Name and a Condition** panel, do the following and then click **Next**.

Rule name	Enter the name of the rule that you want to create.
Rule type	Select the type of rule that you want to create. The options available under **Condition** depend on the selection that you make in the **Rule type** drop-down list. See "Creating routing rules based on IP address range" on page 1069. See "Creating routing rules based on subnet " on page 1070. See "Creating routing rules based on expression " on page 1071. See "Creating routing rules based on asset group" on page 1073.

3 In the **Select a CCS Manager or a Site** panel, do the following:

- In the left-hand pane, select the scope that will perform the task.
  For example, CCS Manager.
  Based on your selection, all the sites or the CCS managers are displayed in the right-hand pane.
- In the right-hand pane, select the site or the CCS manager, and then click **Add**.

  Note: You can only add a CCS manager or a site as the scope.

- In the **Selected Items** pane, view the scope that you have selected.
  If you want to remove the selected scope, you can click **Remove**.

4 In the **Summary** panel, view the summary and then click **Finish**.

The routing rule is created and listed at the bottom of the **Routing Rules** grid of the **Manage Routing Rules – Settings** view.

See "Editing a routing rule" on page 1075.

See “Enabling and disabling a routing rule” on page 1078.

See “Prioritizing a routing rule” on page 1077.

See “Evaluating routing rules” on page 1078.

See “Deleting a routing rule” on page 1076.

See “Concepts in routing rules” on page 230.

Creating routing rules based on IP address range

This rule lets a CCS manager or a site perform a job related task on the assets that come under the IP address range that you specify in the rule.

To create a routing rule based on IP address range

1 In the **Specify a Rule Name and a Condition** panel, do the following:

- Enter the name of the rule that you want to create.
  For example, IP rule.
- Select **IP Address Range** as the rule type.
- Under **Condition**, enter the IP range in the **Start IP Address** and **End IP Address** text boxes, and then click **Next**.
  For example, do the following:
  Type **10.216.40.1** as the start IP address.
  Type **10.216.47.254** as the end IP address.

2 In the **Select a CCS Manager or a Site** panel, do the following:

- In the left-hand pane, select the scope that will perform the task.
  For example, CCS Manager.
- In the right-hand pane, select the site or the CCS manager and then click **Add**.
  For example, CCS Manager 1.

- In the **Selected Items** pane, view the scope that you have selected.

3 In the **Summary** panel, view the summary and then click **Finish**.

For example:

Name	IP rule
Type	IP Address Range
Condition	IP address is in range 10.216.40.1 to 10.216.47.254
Route to	CCS Manager 1

The routing rule is created and listed at the bottom of the **Routing Rules** table of the **Manage Routing Rules - Settings** view.

See "Routing rules based on IP address range" on page 230.

See "Creating a routing rule " on page 1067.

Creating routing rules based on subnet

This rule lets a CCS manager or site perform a job related task on the assets that have the subnet ID and subnet mask that you specify in the rule.

To create a routing rule based on subnet

1 In the **Specify a Rule Name and a Condition** panel, do the following:

- Enter the name of the rule that you want to create.
  For example, Subnet rule.
- Select **Subnet** as the rule type.
- Under **Condition**, enter the subnet ID and subnet mask in the respective text boxes, and then click **Next**.
  For example, do the following:
  Type **10.216.46.0** as the subnet ID.
  Type **255.255.255.0** as the subnet mask.

2 In the **Select a CCS Manager or a Site** panel, do the following:

- In the left-hand pane, select the scope that will perform the task.
  For example, Sites.
- In the right-hand pane, select the site or the CCS manager, and then click **Add**.
  For example, Boston.

- In the **Selected Items** pane, view the scope that you have selected.

3 In the **Summary** panel, view the summary and then click **Finish**.

For example:

Name	Subnet rule
Type	Subnet
Condition	IP in subnet 10.216.46.0 with subnet mask as 255.255.255.0.
Route to	All CCS Managers in 'Boston'.

The routing rule is created and listed at the bottom of the **Routing Rules** grid of the **Manage Routing Rules - Settings** view.

See "Routing rules based on subnet " on page 231.

See "Creating a routing rule " on page 1067.

Creating routing rules based on expression

This rule lets you create rules based on the host name, FQDN, and domain. The jobs for the assets that are found with the matching expressions are sent to the CCS manager or site that you specify in the rule.

To create a routing rule based on expression

1 In the **Specify a Rule Name and a Condition** panel, do the following:

- Enter the name of the rule that you want to create.
  For example, Expression rule.
- Select **Expression** as the rule type.
- Under **Condition**, do the following and then click **Next**.
  - From the **Field** drop-down list, select one of the following:
    - Domain name
    - FQDN
    - Host name
- From the **Operator** drop-down list, select an operator to route jobs for the assets.
  For example:

Field	Operator
Domain name	is
FQDN	ends with
Host name	matches

- Based on the selection that you make in the **Field** drop-down, in the **Value** text box, type value.
  For example:

Field	Operator	Value
Domain name	is	MEDICAL
FQDN	ends with	CARDIAC-DEPT. MEDICAL.COM
Host name	matches	File Server on Win2k3

2 In the **Select a CCS Manager or a Site** panel, do the following:

- In the left-hand pane, select the scope that will perform the task.
  For example, Sites.
- In the right-hand pane, select the site or the CCS manager, and then click **Add**.
  For example, Medico.

- In the **Selected Items** pane, view the scope that you have selected.

3 In the **Summary** panel, view the summary and then click **Finish**.

For example:

Name	Expression rule
Type	Expression
Condition	Domain name is MEDICAL AND FQDN ends with CARDIAC-DEPT.MEDICAL.COM and Host name matches File Server on Win2k3.
Route to	All CCS Managers in ‘Medico’.

Note: You can create multiple expressions. By default, all expressions that are mentioned in the condition must be fulfilled.

The routing rule is created and listed at the bottom of the **Routing Rules** grid of the **Manage Routing Rules - Settings** view.

See “Routing rules based on expression” on page 231.

See “Creating a routing rule ” on page 1067.

Creating routing rules based on asset group

Use the asset group-based routing rules for a CCS manager or site to perform a job for the assets based on the asset group that you specify in the rule.

To create routing rule based on an asset group

1 In the **Specify a Rule Name and a Condition** panel, do the following:

- Enter the name of the rule that you want to create.
  For example, Asset group rule.
- Select **Asset Group** as the rule type.
- Under **Condition**, select the asset group , and then click **Next**.
  For example, Oracle Servers.

2 In the **Select a CCS Manager or a Site** panel, do the following:

- In the left-hand pane, select the scope that will perform the task.
  For example, Sites.

- In the right-hand pane, select the site or the CCS manager, and then click **Add**.
  For example, Oracle group.
- In the **Selected Items** pane, view the scope that you have selected.

3 In the **Summary** panel, view the summary and then click **Finish**.

For example:

Name	Asset group rule
Type	Asset Group
Condition	Oracle Servers
Route to	All CCS Managers in ‘Oracle group’.

The routing rule is created and listed at the bottom of the **Routing Rules** grid of the **Manage Routing Rules - Settings** view.

See “Routing rules based on asset groups” on page 233.

See “Creating a routing rule ” on page 1067.

Creating routing rules based on active directory site

This rule lets you create routing rules based on the subnet that are found for the sites in your Active Directory.

To create routing rules based on active directory

1 On the **Tasks** menu, on **Routing Rules** Tasks , click **Configure Active Directory Site Routing**.

2 In the **Configure Active Directory Site Routing** dialog box, do the following:

- Under **Domain\Domain controller** group box, in the **Name** field, enter the domain controller name, and click **Connect**.
  For example: mydc.mydomain.com

  Note: The information on the sites and subnets for the domain is cached on the Application Server. Next time, when you launch the **Configure Active Directory Site Routing** dialog box, you can select the domain controller from the **Name** field and CCS automatically displays the sites and subnet information of the selected domain.

- In the **Specify Credentials for <name of the domain controller>** dialog box, do the following, and then click **OK**:
  - Enter the user name for the domain controller.
    For example: mydomain\administrator
  - Enter the password for the domain controller.
    For example: password
    All the subnets that are present in the active directory site are displayed in the **Subnets** grid that comes under **Routing**.
- In the **Subnets** grid, do one of the following:
  - Select the active directory subnet rule that you want to use to create a subnet based routing rule and click **Create Routing Rule** .
  - Right-click the active directory rule and select **Create Routing Rule**.
- In the **Select a CCS Manager or a Site** dialog box, do the following:
  - In the left-hand pane, select the scope that will perform jobs on your assets.
    For example, Sites.
  - In the right-hand pane, select the site or the CCS manager, and then click **Add**.
    For example, TestSite.
  - Click **OK**.
    The routing rule is created and displayed in the **Subnets** grid.

3 Click **OK** to exit the **Configure Active Directory Site Routing** dialog box.

To view the routing rule, go to **Routing Tasks** > **Manage Routing Rules**. The routing rule is created and listed at the bottom of the **Routing Rules** grid of the **Manage Routing Rules – Settings** view.

See “Routing rules based on active directory site” on page 234.

Editing a routing rule

You can edit a user-defined routing rule from the **Edit** submenu.

Note: You cannot edit a system-defined routing rule.

To edit a routing rule

1 Do one of the following:

- In the **Manage Routing Rules – Settings** view, select the rule that you want to edit, and then click **Edit** submenu.
- Right-click the rule and select **Edit**.

2 In the **Specify a Rule Name and a Condition** panel of the **Create or Edit Routing Rule** wizard, you can edit the following fields:

- Name
- Condition
- Scope (CCS manager or site)

Note: You cannot change the rule type. This field cannot be edited.

3 Click **Finish**.

The routing rule is updated.

See "Enabling and disabling a routing rule" on page 1078.

See "Prioritizing a routing rule" on page 1077.

See "Evaluating routing rules" on page 1078.

See "Deleting a routing rule" on page 1076.

See "Creating a routing rule " on page 1067.

See "Concepts in routing rules" on page 230.

Deleting a routing rule

You can delete a user-defined routing rule from the **Delete** submenu.

Note: You cannot delete a system-defined routing rule.

To delete a routing rule

1 Do one of the following:

- In the **Manage Routing Rules – Settings** view, select the rule that you want to delete, and then click **Delete** submenu.
- Right-click the rule and select **Delete**.

2 In the **Delete Routing Rule** dialog box, click **Yes**.

The routing rule is deleted.

See “Enabling and disabling a routing rule” on page 1078.

See “Prioritizing a routing rule” on page 1077.

See “Evaluating routing rules” on page 1078.

See “Creating a routing rule ” on page 1067.

See “Editing a routing rule” on page 1075.

See “Concepts in routing rules” on page 230.

Prioritizing a routing rule

You can change the priority of a user-defined or a system-defined routing rule from the **Change Priority** submenu. The value sets the priority of the routing rule. The CCS manager that is in the load balancer role evaluates the rules based on the sequence of the evaluation order.

Priority is assigned numerically. The priority levels range from 1 being the highest priority and the count of the number of rules that you create being the lowerst priority. For example, if you create 5 routing rules, 1 is the highest priority and 5 is the lowest priority.

To prioritize a routing rule

1. Do one of the following:
   - In the **Manage Routing Rules – Settings** view, select the rule that you want to prioritize, and then click **Change Priority** submenu.
   - Right-click the rule and select **Change Priority**.
2. In the **Change Routing Rule Priority** dialog box, specify the new priority for the routing rule and click **OK**.

   Note: You can also use the arrow icons on the submenu to increase or decrease the priority of the routing rules. Select the rule that you want to increase in priority and then select **Increase Priority** arrow. Select the rule that you want to decrease in priority and then select **Decrease Priority** arrow.

   The priority of the selected routing rule is changed.

   Based on your input, the priority of all the rules change accordingly in the queue.

See “Enabling and disabling a routing rule” on page 1078.

See “Evaluating routing rules” on page 1078.

See “Creating a routing rule ” on page 1067.

See “Editing a routing rule” on page 1075.

See “Deleting a routing rule” on page 1076.

See “Concepts in routing rules” on page 230.

Enabling and disabling a routing rule

You can enable or disable a user-defined or a system-defined routing rule from the **Enable** submenu and **Disable** submenu.

To enable a routing rule

◆ Do one of the following:

- In the **Manage Routing Rules – Settings** view, select the rule that you want to enable, and then click **Enable** submenu.
- Right-click the rule and select **Enable**.
  The selected routing rule is enabled.

To disable a routing rule

◆ Do one of the following:

- In the **Manage Routing Rules – Settings** view, select the rule that you want to disable, and then click **Disable** submenu.
- Right-click the rule and select **Disable**.
  The selected routing rule is disabled.

See “Evaluating routing rules” on page 1078.

See “Exporting evaluation results” on page 1079.

See “Creating a routing rule ” on page 1067.

See “Editing a routing rule” on page 1075.

See “Prioritizing a routing rule” on page 1077.

See “Deleting a routing rule” on page 1076.

See “Concepts in routing rules” on page 230.

Evaluating routing rules

You can evaluate routing rules from the **Evaluate** submenu.

To evaluate routing rules

1. In the **Manage Routing Rules – Settings** view, click **Evaluate** tab.
2. In the **Select Assets** panel of the **Evaluate Routing Rules** wizard, do the following:
   - In the left-hand pane, click the **Asset System** folder.
     All the assets in the **Asset System** folder are displayed in the right-hand pane of the panel.
   - Select the assets whose routing plan you want to view and then click **Add**.
     If you want to add all assets, you can click **Add All**.
   - In the **Selected Items** pane, view the assets that you have selected.
     If you want to remove the selected assets, you can click **Remove**. If you want to remove all the assets, you can click **Remove All**.
3. In the **Evaluate Routing Rule – Settings** view, you can do the following:
   - View the route plan of the selected or all assets.
   - Reevaluate the route plan.
   - Close the **Evaluate Routing Rule – Settings** view.

See "Exporting evaluation results" on page 1079.

See "Routing rules evaluation " on page 236.

See "Concepts in routing rules" on page 230.

See "Creating a routing rule " on page 1067.

See "Editing a routing rule" on page 1075.

See "Enabling and disabling a routing rule" on page 1078.

See "Prioritizing a routing rule" on page 1077.

See "Deleting a routing rule" on page 1076.

Exporting evaluation results

You can export the evaluation results to the following formats:

- Excel
- Word
- PDF
- XML
- CSV

To export evaluation results

1. In the **Evaluate Routing Rule -Settings** dialog box, go to **File** menu > **Export to**.
2. Select the format to which you want to export the evaluation results.
3. In the **Export to** dialog box, type the file name by which the evlaution results must be saved and click **Save**.

See "Routing rules evaluation " on page 236.

See "Evaluating routing rules" on page 1078.

See "Concepts in routing rules" on page 230.

Scheduling a host IP cache update job

You can schedule this job by launching the **Schedule IP Cache Update** dialog box.

To schedule the host IP cache update job

1. Go to **System Topology** > **Routing Rules** > **Schedule IP Cache Update**.
2. On the **Schedule IP Cache Update** 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.
3. Click **OK**

   The host IP cache update job is created.

See "Host IP cache update job" on page 235.

See "About resolving IP addresses" on page 235.

Scheduling a host IP cache refresh job

You can schedule this job by launching the **Schedule IP Cache Refresh** dialog box.

To schedule the host IP cache refresh job

1. Go to **System Topology** > **Routing Rules** > **Schedule IP Cache Refresh**.
2. On the **Schedule IP Cache Update** 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.
3. Click **OK**.

   The host IP cache refresh job is created.

See "Host IP cache refresh job" on page 236.

See "About resolving IP addresses" on page 235.

Routing rules workflow

This section explains the end-to-end process of the routing rules.

You create the rules for routing and prioritize them in the following order:

Table 43-1 lists the routing rules and their priority.

Table 43-1 Routing rules and their priority

Routing rules	Priority
Route jobs for the assets that have subnet ID: 10.216.0.0 and subnet mask : 255.255.128.0 to Site A.	1
Route jobs for assets who are in the Medical domain to Site B.	2
Route jobs for the assets that fall within 10.216.40.1 - 10.216.47.254 to CCS Manager 1.	3

When the jobs for the assets reach the CCS manager that is in the load balancer role, the rules are evaluated based on their priority. The evaluation process is as follows:

- The jobs for the assets that have the subnet ID and subnet mask as specified in the rule are routed to Site A.
- The jobs for the assets that are in the Medical domain are routed to Site B.
- The jobs for the assets that belong to specified IP address range are routed to CCS Manager 1.

The jobs for the assets that cannot be routed are then routed to the fall back options such as network affinity and default site.

The fall back options work in the following sequence:

- The first fall back option is the network affinity. The assets on which the job is to be performed must be in the same or in the accessible subnet as that of the CCS manager.
  The jobs that cannot be routed to the network affinity are then routed to the default site.
- The second fall back option the default site. The default site must have a CCS manager in the collector role.
  If the default site does not have a CCS manager in the collector role, the jobs for the assets are not routed and are displayed in the **Failures** tab.

See "Concepts in routing rules" on page 230.

See "Scope in routing rules " on page 234.

See "Routing rules based on IP address range" on page 230.

See "Routing rules based on subnet " on page 231.

See "Routing rules based on expression" on page 231.

See "Routing rules based on asset groups" on page 233.

Chapter 44

Managing risks

This chapter includes the following topics:

- Treating risks - Remediation plan
- Treating risks - Exception plan
- Managing remediation plan and exception plan
- Configuring a default system for treating risks

About risk modeling

To effectively and consistently manage a relative concept like risk, you must start by defining what a risk is. Risk modeling is a process to identify and define security objectives to safeguard the assets in your organization. By using risk manager, you can model risks by performing the following tasks:

- Define a security objective by using predefined templates.
  You may also define a custom security objective by using a blank template.
- Associate critical assets with the security objective.
- Associate controls with the security objective.
  You may also optionally configure controls by assigning a weight percentage, defining compensating controls and compensation percentage.
  You may also optionally define monitoring parameters to monitor the risk score.
- Publish your security objective.

See “Risk modeling - Overview tab” on page 1084.

See “Risk modeling - Assets tab” on page 1085.

See “Risk modeling - Controls tab” on page 1086.

See “Risk modeling - Configure Controls tab” on page 1087.

See “Risk modeling - Monitoring tab” on page 1088.

Risk modeling - Overview tab

Table 44-1 explains the fields available under the **Overview** tab to create a security objective.

Table 44-1 Risk modeling overview details

Fields	Description
Security objective	The name of the security objective. This field is mandatory.
Description	The description that you may want to provide for the security objective.
Owner	The author of the security objective. The author can add a different owner for the security objective.
Created By	The name of the user who is logged in to create the security objective.
Stakeholders	The CCS users who can view the security objective in addition to the owner and the author.
Published Date	The date and time when the security objective is published. This field appears only if the security objective is published.
Status	The current status of the security objective. The status can either be Draft, Published, or Unpublished.
Creation Date	The date when the security objective is created. The locale system date is captured.

See "Defining a security objective - blank template" on page 1091.

See "Defining a security objective - predefined template" on page 1090.

See "Risk modeling - Assets tab" on page 1085.

See "Risk modeling - Controls tab" on page 1086.

See "Risk modeling - Configure Controls tab" on page 1087.

See "Risk modeling - Monitoring tab" on page 1088.

Risk modeling - Assets tab

The **Assets** tab on the **Risk Modeling** page lets you associate critical assets with the security objective.

Click **Add** or **Remove** to associate or disassociate assets with the security objective, respectively.

After you associate assets to the security objective, the **Risk Modeling** page displays the asset system in a tree view in the left pane and the available assets in the right pane. The right pane displays the name of the asset, the type of the asset, and the path where the asset is located.

Note: Associating assets with a security objective is mandatory.

See "Associating assets with security objective" on page 1093.

See "Risk modeling - Overview tab" on page 1084.

See "Risk modeling - Controls tab" on page 1086.

See "Risk modeling - Configure Controls tab" on page 1087.

See "Risk modeling - Monitoring tab" on page 1088.

Risk modeling - Controls tab

The **Controls** tab on the **Risk Modeling** page lets you associate control statements and controls with the security objective.

Click **Add** or **Remove** to associate or disassociate controls with the security objective, respectively. After you associate controls to the security objective, the control statements and controls are displayed in a tree view.

Click **Add from Template** to select and associate controls from the installed security objective templates. CCS provides a rich set of the following predefined security objective templates:

- User identification and authentication
- Media protection
- Training and awareness
- Information confidentiality and integrity
- Data loss protection
- Vulnerability assessment
- Human resources security
- Access control
- Network security
- Physical and environmental security

The controls from the Symantec Controls Studio are mapped to these templates.

Note: Associating controls with a security objective is mandatory.

If you associate controls with a security objective, you may also want to use the **Configure Controls** tab to define weights and compensating controls and the **Monitoring** tab to define parameters for monitoring the risk score.

See “Associating controls with security objective” on page 1093.

See “Risk modeling - Overview tab” on page 1084.

See “Risk modeling - Assets tab” on page 1085.

See “Risk modeling - Configure Controls tab” on page 1087.

See “Risk modeling - Monitoring tab” on page 1088.

Risk modeling - Configure Controls tab

After you associate controls with the security objective you may want to configure the controls with advanced parameters, for a realistic risk score. The **Configure Controls** tab lets you configure the associated controls.

Under the **Configure Controls** tab, the **Controls Weights and Compensating Controls** section is displayed.

Table 44-2 lists the fields that are displayed under the **Configure Controls** tab.

Table 44-2 Configuration details

Fields	Description
Control	The name of the control that evaluates the associated assets .
Weight %	The weight in percentage that you can assign to an individual control. As you type the weight percentage for each control, the total weight percentage gets calculated and displayed under the **Weight %** column.
In the column adjoining the **Weight%** column, you can click **Add Compensating Control (+)** icon to add compensating controls and a compensation percentage for the compensating control. You can click the **Remove Compensating Control (-)** icon and remove the associated compensating control.	
Compensating Control	The name of the control that compensates the risk of the primary control.

Table 44-2 Configuration details *(continued)*

Fields	Description
Compensation %	The percentage value by which the compensating control compensates the primary control.

Note: Configuring controls is not mandatory.

If you are viewing a published security objective, you can click **Unpublish** to unpublish the security objective.

If you are viewing a saved security objective that is in draft status, you can click **Save** to save or click **Publish** to publish the security objective.

Note: Make sure to fill in the mandatory details under the **Assets** tab and the **Controls** tab before you publish the security objective.

See "Configuring controls for security objective" on page 1095.

See "Risk modeling - Overview tab" on page 1084.

See "Risk modeling - Assets tab" on page 1085.

See "Risk modeling - Controls tab" on page 1086.

See "Risk modeling - Monitoring tab" on page 1088.

Risk modeling - Monitoring tab

The **Monitoring** tab on the **Risk Modeling** lets you set parameters for monitoring the risk score.

Table 44-3 lists the fields that are displayed under the **Monitoring** tab.

Table 44-3 Monitoring details

Fields	Description
Likelihood	The likelihood of the risk occurring.
Impact	The effect if the risk occurs.

Table 44-3 Monitoring details *(continued)*

Fields	Description
Impact Area	Type an impact area. The impact area that you enter is saved and displayed in a drop-down list, the next time you view the **Monitoring** tab. **Note:** This information you enter is specific to your credentials and can be viewed only under the **Monitoring** tab.
Monitoring and Notification	
Threshold	The lower and upper limit of the risk. This field is mandatory.
Target Risk	The target risk value is the risk level that you set for a specific security objective. This field is mandatory. This value is shown in the risk panels. Alerts can be enabled if the actual risk level exceeds the specified target risk value beyond the specified target date.
By	The date when the security objective should be reviewed. The security objective is valid until this date.
Show when	The risk manager displays alerts and notifications in the **Alerts and Notifications** panel under the **Risk - Home** dashboard if you check the following scenarios: ■ Risk score exceeds the lower threshold. ■ Risk score exceeds the upper threshold. ■ Risk score exceeds the target risk level.

Note: Adding monitoring details is not mandatory.

If you are viewing a published security objective, you can click **Unpublish** to unpublish the security objective.

If you are viewing a saved security objective that is in draft status, you can click **Save** to save or click **Publish** to publish the security objective.

Note: Make sure to fill in the mandatory details under the **Overview**, **Assets**, and **Controls** tab before you publish the security objective.

See “Defining monitoring parameters for security objective” on page 1095.

See “Risk modeling - Overview tab” on page 1084.

See “Risk modeling - Assets tab” on page 1085.

See “Risk modeling - Controls tab” on page 1086.

See “Risk modeling - Configure Controls tab” on page 1087.

Defining a security objective - predefined template

You can define a security objective from a list of predefined templates that are made available with risk manager.

To define a security objective from a template

1. Go to the Web console home page using the following URL:

   ```
   http://<server_name>/ccs_web
   ```

2. In the Web console, click **Risk Management**.

   The default risk management page is displayed.

3. Click **Risk Modeling**.

   The **Risk Modeling** page is displayed that lets you to view, edit, define, publish, unpublish, and delete security objectives.

4. On the **Risk Modeling** page, click **New**.

   The **Select Security Objective Template** dialog box is displayed.

   Note: You can choose to show or hide the **Select Security Objective Template** dialog box by setting your Web console preferences under **Preferences** on the CCS Web console.

5 Select a predefined template from the list of available templates in the left pane and click **Create**.

The **Security Objectives** panel collapses and the selected security objective template is displayed with the five tabs **Overview**, **Assets**, **Controls**, **Configure Controls**, and **Monitoring**.

The details of the security objective are predefined in the template. You may add, verify, or edit the predefined information under each tab.

6 Click **Save** to save any changes that you make to the security objective.

Click **Publish** to publish the security objective.

Note: Make sure that the mandatory details under the **Overview**, **Assets**, and **Controls** tabs are filled in before you publish the security objective.

See "Associating assets with security objective" on page 1093.

See "Associating controls with security objective" on page 1093.

See "Configuring controls for security objective" on page 1095.

See "Defining monitoring parameters for security objective" on page 1095.

See "Defining a security objective - blank template" on page 1091.

Defining a security objective - blank template

You can opt to not use the predefined template that is made available with risk manager and define a custom security objective from a blank template.

To define a custom security objective

1 Go to the Web console home page using the following URL:

```
http://<server_name>/ccs_web
```

2 In the Web console, click **Risk Management**.

The default risk management page is displayed.

3 Click **Risk Modeling**.

The **Risk Modeling** page is displayed that lets you view, edit, define, publish, unpublish, and delete security objectives.

4 On the **Risk Modeling** page, click **New**.

The **Select Security Objective Template** dialog box is displayed.

Note: You can choose to show or hide the **Select Security Objective Template** dialog box by setting your Web console preferences under **Preferences** on the CCS Web console.

---

5 Select **Blank Template** and click **Create**.

The **Security Objectives** panel collapses and the **Type New Security Objective Details** panel is displayed with the five tabs **Overview**, **Assets**, **Controls**, **Configure Controls**, and **Monitoring**.

6 Under the **Overview** tab, in the **Security Objective** text box, type a unique name for the security objective.

This field is mandatory.

7 In the **Description** text box, type a description for the security objective.

8 Click **Add** to add multiple owners for the security objective.

The currently logged in user is displayed as the owner in the **Owner** field.

Note: Owner can be different than the creator of the security objective.

---

9 In the **Stakeholders** field, click **Add** to add stakeholders for the security objective.

Stakeholders are CCS users who can view the security objective.

10 Verify the information that is displayed under the **Created By**, **Status**, and **Creation Date** fields.

11 Click **Save** to save the security objective or **Publish** to publish the security objective.

Note: Make sure that the mandatory details under the **Overview**, **Assets**, and **Controls** are filled up before you publish the security objective.

See “Associating assets with security objective” on page 1093.

See “Associating controls with security objective” on page 1093.

See “Configuring controls for security objective” on page 1095.

See “Defining monitoring parameters for security objective” on page 1095.

Associating assets with security objective

Risk is asset-centric therefore, you must associate assets with the security objective before you publish the security objective.

Note: Asset details are not predefined in a security objective template.

To associate assets with a security objective

1. Click the **Assets** tab on the **Risk Modeling** page.
2. Click **Add** to add assets.

   The **Add Assets** page is displayed.
3. In the left pane, expand the **Asset System** tree view and select the asset systems that you want to associate with the security objective.
4. Click **Add Assets** to add the selected assets.

   Under the **Assets** tab, the selected asset systems are displayed in the left pane and the available assets are displayed in the right pane.

   You can select asset systems from the left pane under the **Assets** tab and click **Remove** to exclude the assets from the security objective.
5. Click **Save** to save the security objective or click **Publish** to publish the security objective.

   Note: Make sure that the mandatory details under the **Overview**, **Assets**, and **Controls** are filled up before you publish the security objective.

You may also want to associate controls and configure controls with your security objective.

See “Associating controls with security objective” on page 1093.

See “Configuring controls for security objective” on page 1095.

See “Defining monitoring parameters for security objective” on page 1095.

Associating controls with security objective

Symantec Controls Studio is made available with a variety of security controls, when you install CCS. If you define a security objective by using a template, the relevant mapped controls are made available under the **Controls** tab. You may edit or add to this list.

Note: Associating controls with a security objective is not mandatory. If no controls are added then all the failed tests on those assets are also considered for risk scoring.

To associate controls with a security objective

1. Click the **Controls** tab on the **Risk Modeling** page.
2. Click **Add** to select and add the controls.

   The **Add Controls and Statements** page is displayed. The control categories are displayed in a tree view.

   To search controls, do the following:

   - From the **Type** drop-down list, select **All**, **Control Categories**, **Controls**, or **Control Statements**.
   - Type the name of the control in the text box and click **Go**.
3. Expand the control categories and the controls and select the controls and control statements that you want to associate with the security objective.
4. Click **Add Controls** to add the selected controls.

   You can select the controls in the tree view and click **Remove** to exclude the controls from the security objective.
5. If you want to add controls from security objective template, click **Add from Template**.

   The **Select Security Objective Template** dialog box is displayed. Select the desired template and click **Add** to add the controls.

   The predefined templates made available with CCS installation have the relevant set of controls from the Symantec Controls Studio mapped to the security objective template. You can add to the list if you want to.
6. Click **Save** to save the security objective or click **Publish** to publish the security objective.

   Note: Make sure that you have filled in the mandatory details under the **Overview**, **Assets**, and **Controls** tab before you publish the security objective.

You may also optionally want to configure the associated controls by assigning weights and defining compensating controls and compensation percentage.

See “Associating assets with security objective” on page 1093.

See “Configuring controls for security objective” on page 1095.

Configuring controls for security objective

After you associate controls with a security objective, you can assign weights to the controls and define compensating controls and a compensation percentage.

To configure controls

1 Under the **Configure Controls** tab, in the**Controls Weight and Compensating Controls** section, verify the listed controls.

The controls that you associated with the security objective under the **Controls** tab are listed. By default, equal weight is assigned to the controls under the **Weight%** column.

2 Double-click the cell under the **Weight %** column to edit the values.

The total weight is calculated and displayed under the **Weight%** column. The total of the values under the **Weight %** column is limited to 100.

3 Under the column adjoining the **Weight%** column, click the **Add Compensating Control (+)** icon to define compensating controls.

A child grid is displayed below the control. In the child grid, do the following:

- Click the cell under the **Compensating control** column and select the compensating control from the drop-down list.

  Note: Ensure that a primary control does not appear as a compensating control and vice versa, simultaneously.

- Double-click the cell under the **Compensation%** column and type the compensation percentage.

See “Associating assets with security objective” on page 1093.

See “Associating controls with security objective” on page 1093.

See “Defining monitoring parameters for security objective” on page 1095.

Defining monitoring parameters for security objective

The **Monitoring** tab lets you define parameters for monitoring the risk score.

Note: Associating monitoring parameters is not mandatory.

To associate compensating controls

1. On the **Risk Modeling** page, under the panel that displays the details of a new or existing security objective, click the **Monitoring** tab.
2. Move the **Likelihood** slider and select the likelihood of the risk to occur.

   You can select the likelihood as Low, Medium, or High.
3. Move the **Impact** slider and select the effect of the risk.

   You can select the impact as Low, Medium, or High.
4. Type an impact area in the **Impact Area** drop-down list.

   The value that you enter is specific to your login credentials and cannot be viewed by all the user. The values are available under a drop-down list the next time to log in.
5. Under the **Monitoring and Notifications** group box, do the following:
   - Move the **Threshold** slider from left to right to set the minimum threshold limit.
     The minimum threshold limit must be greater than 0. This is a mandatory field.
   - Move the **Threshold** slider from right to left to set the maximum threshold limit.
     The maximum threshold limit must be less than 10. This is a mandatory field.
   - Move the **Target Risk** slider to set the risk level.
     The target risk must be greater than 0 and less than 10.
   - Select a date from the **By** calendar picker.
     The target date has to be a date later than the current date.
   - In the **Show when** group box, check all or any of the following options:
     - Risk score exceeds the lower threshold
     - Risk score exceeds the upper threshold
     - Risk score exceeds the target risk level

Depending on the options that you check, risk manager sends out the alert to the **Alerts and Notifications** panel under **Dashboards > Risk - Home**.

6 Click **Save** to save the security objective or click **Publish** to publish the security objective.

Note: Make sure that you fill in the mandatory details under the **Overview**, **Assets**, and **Controls** tab before you publish the security objective.

See "Associating assets with security objective" on page 1093.

See "Associating controls with security objective" on page 1093.

See "Configuring controls for security objective" on page 1095.

Managing security objectives

You can perform the following tasks to manage your security objectives:

- View the security objective details.
- Unpublish a security objective.
- Delete a security objective.
- Edit a security objective.
- Publish a security objective.

To manage a security objective

1 Go to the Web console home page using the following URL:

```
http://<server_name>/ccs_web
```

2 In the Web console, under **Risk Management**, click **Risk Modeling**.

The risk modeling page is displayed, which lists the existing security objectives in a grid under the **Security objectives** panel.

3 In the **Action** column, click the appropriate icon to perform the following actions:

- View the security objective details.
  The security objective is displayed in a view mode.
- Unpublish a security objective.
  You can withdraw only a published security objective by unpublishing. The risk trends for a particular security objective may get impacted if you unpublish a security objective. Risk manager prompts you to retain a copy

of the published security. Click **OK** to retain a copy or the security objective that you want to unpublish or click **Cancel** to proceed with the unpublish without retaining a copy.

Note: The risk trend of the security objective may be affected if you opt to unpublish a security objective. If a remediation has been initiated for a published security objective, the security objective cannot be unpublished.

- Delete a security objective.
  You can delete a security objective that you have created. A deleted security objective cannot be retrieved. If you delete a security objective, the historical data that is associated with the security objective does not get deleted.
- Edit a security objective.
  The security objective that you select is displayed in an edit mode in a panel under the **Security objectives** panel.
  You can make changes to the details in the **Overview**, **Assets**, **Controls**, **Configure Controls**, and **Monitoring** tabs.
- Publish a security objective.
  You must publish the security objectives for CCS to derive the risk score. Only when the security objectives are published you can view the risk by creating charts and create action plans to treat risks.

4 Click **Save** to save the changes or click **Publish** to publish the security objective..

Note: You can save a security objective and edit it later. A saved security objective is not published. Make sure that the mandatory details under the **Overview**, **Assets**, and **Controls** tab are filled before you publish the security objective.

After you publish a security objective, run the Global Metrics and Trend Computation Job from the Windows console for risk analysis.

See “About risk modeling” on page 1084.

See “About Global metrics and trend computation job” on page 1031.

Publishing a security objective

You must publish the security objectives for CCS to derive the risk score. Only when the security objectives are published you can view the risk by creating charts and create action plans to treat risks.

Note: Make sure that the mandatory details under the **Overview**, **Controls**, and **Assets** tab are filled in before you publish the security objective.

To publish a security objective

1. Go to the Web console home page by using the following URL:

   ```
   http://<server_name>/ccs_web
   ```

2. In the Web console, click **Risk Management**.

   The risk modeling page is displayed, which lists the existing security objectives in a grid under the **Security objectives** panel.

3. You can publish the security objective in the following two ways:

   - Click **Publish Security Objective** in the **Actions** column.
   - Click **Edit Security Objective Details** to open the security objective in an edit mode and click **Publish**.

   Note: The status of the security objective is displayed as **Draft** when it is saved. The status changes to **Published** after the security objective published.

After you publish a security objective, run the Global Metrics and Trend Computation Job from the Windows console for risk analysis.

See “About risk modeling” on page 1084.

See “Managing security objectives” on page 1097.

See “About Global metrics and trend computation job” on page 1031.

About monitoring risks

CCS introduces the risk dashboards in the existing dashboards platform. Risk dashboards use the risk data that CCS collects, analyzes, and calculates and lets you present the risk posture of your business. With risk dashboards you have the ability to define and view the risk posture of your business, the way you want.

Risk dashboards help you monitor your complex business facets in a snapshot and draw an executive summary for taking strategic business decisions.

Risk dashboards consist of a predefined risk dashboard and predefined risk panels for monitoring risks. These panels provide a snapshot of the current risk to your business based on the security objective that you define and the risk calculation logic of the risk manager that calculates the risk score.

You can also analyze the risk scores and define an action plan from the risk panels.

See "Predefined dashboards" on page 979.

See "Predefined panels" on page 1003.

See "About risk treatment" on page 1102.

Using the risk dashboard

To access the risk dashboards, go to the CCS Web Console home page `http://<server_name>/CCS_Web` and click **Dashboards**. The dashboards home page is displayed. You can perform the following tasks by using the Web console:

- View risk and compliance by using the predefined dashboards and panels.
- Create and edit custom dashboards.
- Create, edit, and publish custom panels.
- Unpublish custom panels.
- Add panels to a dashboard.
- Import a panel.
- Email a dashboard URL.

See "About Dynamic Dashboards" on page 249.

Analyzing and prioritizing risks

The **Analyze Risk** page lets you view the details of a risk that is attached to a security objective and define an action plan. You can analyze the current risk score, target risk score, and projected risk score. Based on your analysis, you can decide on creating an exception plan or a remediation plan for the risk elements that make up the security objective.

To analyze and prioritize risks

1 Go to the Web console home page by using the following URL:

```
http://<server_name>/ccs_web
```

2 In the Web console, click **Dashboards**.

The default dashboards page is displayed.

3 Select the category **Risk** under the **Dashboards** tab in the left panel.

4 Click **Risk – Home**.

The risk dashboards and panels are displayed.

5 In the risk panel, click **Orientation Options** in the panel title or right-click the chart and select **Create Action Plan**.

The remediate option gets selected. The message **No options available** is displayed, if there are no orientation options configured for the panel.

Note: The remediation option is available on a right-click or under the orientation options only if you have opted to enable remediation at the time of creating the panel.

6 Click the chart of the risk element that you want to treat.

The **Analyze Risk** page is displayed. The **Security objective Details** pane displays the name and the owner of the security objective along with a graphical representation of the current risk score and the target risk score. A grid is displayed below the **Security objective Details** pane that explains the details of the risk.

7 Based on your analysis, you can select the assets that you want to treat.

Note: Check the assets that you want to remediate and click the **Click here to recalculate the projected risk** icon to preview the projected risk score for the selected risk elements, before creating a remediation plan.

After analyzing the assets at risk, perform the following actions:

- To add assets to an existing remediation or exception plan, click **Add to Plan**. The **Select Remediation Plan** dialog box is displayed. Select a remediation or an exception plan from the available plans and click **OK**.
- To create a remediation plan, check the assets at risk that you want to remediate and click **Create Remediation Plan**.

- To create an exception plan, check the assets at risk that you want to accept and click **Create Exception Plan**.

See "Treating risks - Remediation plan" on page 1103.

See "Treating risks - Exception plan" on page 1105.

About risk treatment

Risk manager lets you define a plan to treat risks, while you view them, by using the risk dashboards.

By using the risk dashboards you can do the following:

- Analyze the published security objectives.
- Select and prioritize risks based on the risk score.
  You can either accept the risk or opt for remediation.
- Create and submit an action plan to treat the risks.
  Integrate with an existing setup of Symantec Workflow or Symantec ServiceDesk to treat risks. You can also opt for email, if you do not want to use Symantec Workflow or Symantec ServiceDesk .

Following are the two types of action plans that you can create to treat risks by using risk manager:

- **Remediation plan**
  Risks that you want to treat become part of the remediation plan. A remediation plan has a completion date, an assignee, and remediation steps.
  Symantec Workflow, Symantec ServiceDesk , and Email can be used for submitting a remediation plan.
- **Exception plan**
  Risks that you do not want to treat become a part of an exception plan because the risk is accepted. Risks for exception that are part of the exception plan require an approval and a valid reason.
  Symantec Workflow and Email can be used as a remediation system for submitting an exception plan.

When do you accept risks?

- When we do not know about the risk.
- When the risk is insignificant.
- When the benefit is high compared to the risk. That is when it is worth accepting the risk.

Risks that do not meet the criteria for acceptance must be remediated.

See “Risk treatment - Workflow” on page 248.

Treating risks - Remediation plan

You can create an action plan while viewing the risk panels under the **Risk - Home** dashboard.

To create a remediation plan

1 Go to the Web console home page by using the following URL:

```
http://<server_name>/ccs_web
```

2 Click **Dashboards**.

The default dashboards page is displayed.

3 Under the **Dashboards** tab in the left-hand pane, expand the category **Risk** and click **Risk - Home**.

The predefined risk panels under the risk dashboard are displayed.

4 In the panel, at any level in the drill-down, do one of the following:

- Click **Orientation Options** and select **Create Action Plan**. Click the chart of risk element that you want to define an action.
- In the panel, right-click the element that you want to treat and select **Create Action Plan**.

The **Analyze Risk** page is displayed.

5 Check the assets for which you want to create a remediation plan and click **Create Remediation Plan**.

The **Create Remediation Plan** page is displayed.

6 In the **Plan Name** field, type a unique name for the plan.

This field is mandatory.

7 In the **Description** field, type a description for the remediation plan.

8 In the **Assigned To** field, type the name of the user to whom the remediation plan is assigned.

9 Select a completion date for the security objective from the **Complete By** date picker.

This date must be later than the current date.

10 In the **Recommended Action** field, type a recommended remediation action.

Note: Risk manager displays the values in the fields **Security objective**, **Asset Group**, **Initiated By**, **Current Risk Score**, and **Projected Risk Score**.

Click the name of the security objective to view the end-to-end details such as overview, directly scoped assets, and controls.

11 Under the **Risks for Remediation** tab, enter the following information:

- In the **Recommended Action** column, type a recommended action to be taken for remediation.
- Check the **Include Task List** check box, to ensure that the remediation steps are also included with the plan.
- Select a date from the **Complete By** drop-down.
  This is the completion date for the individual risk item.

  Note: This date must be earlier to the completion date of the security objective.

- In the **Assigned To** column, type the name of the user to whom you want to assign the remediation plan.

You can expand the row to view the tests that are mapped to the controls and their source systems. You can click on the test to view the remedy steps.

12 Select the system to submit the remediation plan from the **Submit Via** drop-down list. You can select either Email, Symantec Workflow, or Symantec ServiceDesk .

If you select Symantec Workflow, the **Select Workflow** drop-down list is displayed with a list of available workflows. Select the desired workflow for remediation.

Note: The system that you select overrides the default system that you may have selected under Settings > Risk Remediation.

---

13 Click **Save** to save the remediation plan.

You can click **Replan** to reset the values that you entered.

14 If you have selected the default remediation system as Symantec Workflow or Symantec ServiceDesk , click **Submit** to submit the remediation plan.

If you have selected the default system as email, click **Next** to proceed to the **Email Preview** page. Preview the email contents and click **Submit** to send the email.

See "Configuring a default system for treating risks" on page 1108.

See "Risk treatment - Workflow" on page 248.

See "About risk treatment" on page 1102.

See "Treating risks - Exception plan" on page 1105.

See "Managing remediation plan and exception plan" on page 1107.

Treating risks - Exception plan

You can create an exception plan for risks that you opt to accept.

To create an exception plan

1 Go to the Web console home page by using the following URL:

```
http://<server_name>/ccs_web
```

2 Click **Dashboards**.

The default dashboards page is displayed.

3 Under the **Dashboards** tab in the left-hand pane, expand the category **Risk** and click **Risk - Home**.

The predefined risk panels under the risk dashboard are displayed.

4 In the panel, at any level in the drill-down, do one of the following:

- Click **Orientation Options** and select **Create Action Plan**. Click the chart of the risk element that you want to treat.
- In the panel, right-click the risk element that you want to treat and select **Create Action Plan**.

The **Analyze Risk** page is displayed.

5 Check the assets for which you want to create an exception plan and click **Create Exception Plan**.

The **Create Exception Plan** page is displayed.

6 In the **Plan Name** field, type a unique name for the plan.

This field is mandatory.

7 In the **Description** field, type a description for the remediation plan.

8 In the **Assigned To** field, type the name of the user to whom the remediation plan is assigned.

9 Select a completion date for the security objective from the **Complete By** drop-down.

This date must be later than the current date.

10 In the **Recommended Action** field, type a recommended remediation action.

Note: Risk manager displays the values in the fields **Security Objective**, **Asset Group**, **Initiated By**, **Current Risk Score**, and **Projected Risk Score**.

Click the name of the security objective to view the end-to-end details such as overview, directly scoped assets, and controls.

11 Under the **Risks for Exception** tab, enter the following information:

- In the **Approver** column, type the name of the user who is authorized to approve the risk acceptance.
- In the **Effective Till** column, select a date until which the risk can be accepted.
- In the **Reason** column, type a reason for accepting the risk.
- In the **Approve By Date** column, select a date by which the approver must approve the accepted risks.

Expand the row to view the tests that are mapped to the control statement and their source systems. Click on the test to view the remedy steps.

12 Select the system to submit the exception plan from the **Submit Via** drop-down list. You can select either Email, Symantec Workflow, or Symantec ServiceDesk .

If you select Symantec Workflow, the **Select Workflow** drop-down list is displayed with a list of available workflows. Select the desired workflow for submitting the exception.

Note: The system that you select overrides the default system that you may have selected under Settings > Risk Remediation.

13 Click **Save** to save the remediation plan.

You can click **Replan** to reset the values that you entered.

14 If you have selected the default system as Symantec Workflow or Symantec ServiceDesk , click **Submit** to submit the exception plan.

If you have selected the default system as email, click **Next** to proceed to the **Email Preview** page. Preview the email contents and click **Submit** to send the email.

Note: Risks for exception cannot be submitted by using Symantec ServiceDesk .

See "Configuring a default system for treating risks" on page 1108.

See "Risk treatment - Workflow" on page 248.

See "About risk treatment" on page 1102.

See "Treating risks - Remediation plan" on page 1103.

See "Managing remediation plan and exception plan" on page 1107.

Managing remediation plan and exception plan

You can manage your remediation plans and exception plans by performing the following tasks:

- Viewing remediation and exception plans.
- Editing remediation and exception plans.

  Note: You can edit only the remediation plan or exception plan that is submitted or in-progress. The remediation or an exception plan that is completed cannot be edited.

- Deleting remediation and exception plans.

  Note: You can delete only the remediation or an exception plan that is in a draft or an error status.

To manage a remediation or an exception plan

1 Go to the Web console home page by using the following URL:

```
http://<server_name>/ccs_web
```

2 Click **Risk Management**.

The default risk management page or the risk modeling page is displayed, based on your preferences.

3 Click **Action Plans**.

The **Action Plans** page is displayed.

4 In the grid, under the **Action** column, click the appropriate icon to perform the following actions:

- View or edit remediation plan
The remediation plan is displayed in an edit mode.
- View or edit exception plan
The exception plan is displayed in an edit mode.
- Delete remediation plan
- Delete exception plan
- View remediation plan
The remediation plan is displayed in view mode.
- View exception plan
The exception plan is displayed in view mode.

5 Click **Save** to save the changes.

The updated plan is displayed on the **Action Plans** page.

Click **Cancel** to go to the **Action Plans** page without saving.

If you are submitting the action plan by using email, click **Next** to preview the email. If you are submitting the action plan by using Symantec Workflow or Symantec ServiceDesk , click **Submit** to submit the plan.

See “Treating risks - Remediation plan” on page 1103.

See “Treating risks - Exception plan” on page 1105.

Configuring a default system for treating risks

You can configure Symantec Workflow, Symantec ServiceDesk , or email as the default system for treating risks. The remediation system that you set as default is used by risk manager to submit the remediation plan.

To configure a default system for treating risks

1. On the CCS Web console, go to Settings > Risk Remediation.

   The **Risk Remediation System Settings** page is displayed.

2. Under the **External Remediation System** option, select one of the following:

   - Email
   - Symantec Workflow
   - Symantec ServiceDesk

3. Click **Ok** to save the setting.

Note: Configure Symantec Workflow with CCS before you use it as a default system for treating risks. See "Configuring Symantec Workflow with CCS" on page 363.

Data collection after upgrading to CCS 11.0

This appendix includes the following topics:

Data collection using the Information Server

After you upgrade to CCS 11.0, you can use your RMS Console and Information Server deployment to collect data from computers in your enterprise network. The CCS Manager in the role of a data collector collects data from the RMS data collectors.

In CCS 11.0, you can use RMS data collectors for the following platforms :

- Windows
- UNIX
- SQL
- Oracle
- Exchange
- NDS
- Netware

You must configure the RSM data collectors for data collection.

See " Configuring the Windows data collector" on page 1112.

See " Configuring the UNIX data collector" on page 1113.

See “ Configuring the SQL data collector” on page 1113.

See “ Configuring the Oracle data collector” on page 1114.

See “ Configuring the Exchange data collector” on page 1115.

See “ Configuring the NDS data collector” on page 1115.

See “ Configuring the NetWare data collector” on page 1116.

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 CCS Manager 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 CCS Manager 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 data collectors for raw data based data collection” on page 327.

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 CCS Manager component and click **Edit Settings**.
3. In the **Edit Settings** dialog box, under Data Collector, click **Windows - Information Server**.
4. In the Windows - Information Server panel, enter the required information.
5. Click **Save**.

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 CCS Manager 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 CCS Manager computer, you must configure this data collector for an Information Server.

See " Configuring data collectors for raw data based data collection" on page 327.

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 CCS Manager component and click **Edit Settings**.
3. In the **Edit Settings** dialog box, click **UNIX - Information Server**.
4. On the UNIX - Information Server panel, enter the required information.
5. Click **Save**.

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 CCS Manager Collector. The collector then returns the collected data to the Control Compliance SuiteGo to Settings > Map View > Right-click the site > Edit settings. 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 Control Compliance Suite uses the SQL data collector to collect data from the Information Server. Before you use the SQL data collector on the CCS Manager 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 data collectors for raw data based data collection" on page 327.

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 CCS Manager component and click **Edit Settings**.

3 In the **Edit Settings** dialog box, click **SQL - Information Server**.

4 On the SQL - Information Server panel, enter the required information.

5 Click **Save**.

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 CCS Manager 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 CCS Manager 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 data collectors for raw data based data collection" on page 327.

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 CCS Manager component and click **Edit Settings**.

3 In the **Edit Settings** dialog box, click **Oracle - Information Server**.

4 On the Oracle - Information Server panel, enter the required information.

5 Click **Save**.

Configuring the Exchange data collector

The Control Compliance Suite can use Symantec RMS to retrieve data from your enterprise network. RMS passes the collected data to the CCS Manager Collector. The collector then returns the collected data to the Control Compliance Suite infrastructure for further processing. RMS uses the bv-Control for Microsoft Exchange snap-in module to collect data from the Exchange server.

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

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

See " Configuring data collectors for raw data based data collection" on page 327.

To configure the Exchange 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 CCS Manager component and click **Edit Settings**.

3 In the **Edit settings** dialog box, click **Exchange - Information Server**.

4 On the Exchange - Information Server panel, enter the required information.

5 Click **Save**.

Configuring the NDS data collector

The Control Compliance Suite can use Symantec RMS to retrieve data from your enterprise network. RMS passes the collected data to the CCS Manager collector. The collector then returns the collected data to the Control Compliance Suite infrastructure for further processing. RMS uses the bv-Control for NDS eDirectory snap-in module to collect data from the server.

You can configure a CCS Manager as an NDS data collector to collect data from the NDS eDirectory snap-in module.

See “ Configuring data collectors for raw data based data collection” on page 327.

To configure the NDS 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 CCS Manager component and click **Edit Settings**.
3. In the **Edit Settings** dialog box, click **NDS - Information Server**.
4. On the NDS - Information Server panel, enter the required information.
5. Click **Save**.

Configuring the NetWare data collector

The Control Compliance Suite can use Symantec RMS to retrieve data from your enterprise network. RMS passes the collected data to the CCS Manager collector. The collector then returns the collected data to the Control Compliance Suite infrastructure for further processing. RMS uses the bv-Control for NetWare snap-in module to collect data from the server.

You can configure a CCS Manager as a NetWare data collector to collect data from the NetWare snap-in module.

See “ Configuring data collectors for raw data based data collection” on page 327.

To configure the NetWare 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 CCS Manager component and click **Edit Settings**.
3. In the **Edit Settings** dialog box, click **NetWare - Information Server**.
4. On the NetWare - Information Server panel, enter the required information.
5. Click **Save**.

Data collection using ESM data collectors

In the CCS 11.0 installation, you can configure the ESM data collector to collect data from the enterprise network.

You must configure the ESM data collector before you use the ESM data collector on a computer where CCS Manager 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 data collectors for raw data based data collection” on page 327.

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 CCS Manager component and click **Edit Settings**.
3. In the **Edit Settings** dialog box, click **Data Collector Sites > 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.
6. Click **Save**.

See “Configuring the ESM manager settings” on page 1118.

See “Configuring the ESM general settings ” on page 1123.

Configuring the ESM components

You must configure the ESM data collector before you use the ESM data collector on the CCS Manager 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 CCS Manager 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 CCS Manager is installed and then click **Edit Settings**.
3. In the **Edit Settings** dialog box, do one of the following:
   - Click **Data Collector > ESM**
   - Click **Data Collector Sites > ESM**

See “Configuring the ESM manager settings” on page 1118.

See “Configuring the ESM general settings ” on page 1123.

See “Configuring an ESM manager for custom messages” on page 1119.

See “Collecting suppressed ESM messages ” on page 1120.

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

1. In the **Edit Settings** dialog box, click **Data Collector Sites - ESM** option on the left pane.
2. On the right pane, provide the required information to configure an ESM manager.

Adding, modifying, or removing an ESM manager

You must configure a data collector as the ESM Manager before you start ESM data collection from the ESM infrastructure. In the ESM infrastructure, the ESM manager collects data from the individual computers on which the ESM agents are installed. You can configure a data collector by adding an ESM manager through the **ESM Manager Credentials** dialog box. The ESM manager can also be modified or removed for the configured data collector.

To add or modify an ESM manager

1. On the **Data Collector > ESM** panel of the **Edit Settings** dialog box, click **Add** or **Modify**.
2. In the ESM Manager Credentials dialog box, in the Manager details section, provide the required information.

Note: You can add upto 5 ESM managers to a CCS Manager.

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 1118.

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 CCS Manager and click **Edit Settings**.
2. In the **Edit Settings** dialog box, select **Data Collector Sites - ESM** .

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 1118.

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 CCS Manager and click **Edit Settings**.
2. In the **Edit Settings** dialog box, select **Data Collector Sites - ESM** .
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 1118.

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.

The Symantec.CSM.ESM.Integration.dll.config file contains parameters like MaximumPolicyRunMessageCount and UseESMManagerForFormattingMessages. The .config file is located in the following location:

<Install_Directory>\CCS\Reporting and Analytics\CCS Manager\Data Collectors\ESM

You can use the MaximumPolicyRunMessageCount parameter to configure the number of messages that you want ESM data collector to fetch for each policy run. The default value for this parameter is 3000.

You can use the UseESMManagerForFormattingMessages parameter to configure either CCS Manager or ESM Manager to format the messages returned by ESM Agents by specifying a value True or False. The default value is True as ESM Manager formats the messages returned by ESM Agents by default.

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 CCS Manager 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.

See “Configuring CCS ESM policy run options” on page 1122.

Configuring CCS ESM policy run options

The ESM data collector collects policy run data 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.

To configure policy run options

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

2 In the **Edit Settings** dialog box, select **Data Collector Sites - ESM** .

3 On the right pane of the dialog box, click **Configure policy run options**.

4 In the **ESM Policy Configuration** dialog box, click **Add** to add a policy configuration.

5 In the **Configure policy** dialog box, type the ESM policy name in the **Policy name** text box and provide the required information.

You can use the **Configure Policy** dialog box to add, modify, or remove an ESM policy.

6 In the **ESM Policy Configuration** dialog box, select the policy that you want to modify and then click **Modify**.

7 In the **ESM Policy Configuration** dialog box, select the policy that you want to delete and then click **Remove**.

You cannot delete a predefined policy.

8 Click **Yes** on the message prompt that appears to confirm the deletion of the ESM policy.

See "Configuring the ESM manager settings" on page 1118.

Configuring the ESM general settings

The **Edit Settings** dialog box lets you configure the functional settings of the ESM data collector component.

To configure the ESM general settings

1 In the **Edit Settings** dialog box, click **Data Collector - ESM**.

2 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 1124.
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 1125.

See "Configuring the ESM manager settings" on page 1118.

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 1118.

See "Configuring the ESM general settings " on page 1123.

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	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. The default value is 300 seconds.

See “Configuring the ESM manager settings” on page 1118.

See “Configuring the ESM general settings ” on page 1123.

Appendix B

Using the PowerShell cmdlets

This appendix includes the following topics:

- Create-EvaluationJob
- Create-DataCollectionEvaluationJob
- Get-ChecksFromSection
- Get-SectionsFromSection
- Get-DataCollectionJob
- Get-LastDataCollection
- Get-EvaluationJob
- Get-EvaluationJobForStandard
- Initialize-CollectionJobDetails
- Initialize-EvaluationJobDetails
- Initialize-CollectionEvaluationJobDetails
- Create-TagCategory
- Create-Tag
- Search-Tags
- Add-Tags
- Remove-Tags
- Get-TaggedObjects
- Search-Jobs
- Execute-Job
- Request-Exception
- Get-AllExceptions
- Get-ExceptionByTitle
- Set-ExceptionState
- Update-Exception
- Terminate-Exception
- Initialize-ExceptionDetails
- Initialize-IncrementalSchedule

- Initialize-Schedule
- Initialize-EmailNotification
- Initialize-Notification
- Add-Associations
- Remove-Associations

Get-Sites

`Get-Sites` – Returns the list of sites based on the search criteria.

Synopsis

The Get-Sites cmdlet returns a list of sites that matches the specified search criteria.

Syntax

```
Get-Sites -AppServerNameAndPort <String> [-BindingType
<String>] [-Name <String>] [-PipingEnabled [<Boolean>]]
[<CommonParameters>]
```

Authorization requirements

You must have the following CCS tasks to use the cmdlet:

- View Assets

Note: You do not require permissions on any folders to use the cmdlet.

Description

The Get-Site cmdlet returns a site or all sites in the CCS system based on the specified search options.

Parameters

The following table describes the parameters that the cmdlet requires:

Table B-1 Get-Sites - parameters

Switch Name	Switch Type	Data Type	Supports pipeline input? (Yes/No)	Description
AppServerNameAndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServerNameAndPort="<AppServerName/IP> : <Port Number Corresponding To Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-1 Get-Sites - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports pipeline input? (Yes/No)	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$Binding Type="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-1 Get-Sites - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports pipeline input? (Yes/No)	Description
Name	Optional	Name	No	The name of the site. If you do not specify any value for the parameter, then the cmdlet returns all the sites that are available in the system.
PipingEnabled	Optional	Boolean	No	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

Inputs

You cannot pipe objects to the cmdlet.

Outputs

The Get-Sites cmdlet returns a site or a list of sites as an output.

Notes

You can set AppServerNameAndPort variable only once and reuse it till the session is closed.

You can set BindingType variable only once and reuse it till the session is closed.

The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example 1

```
C:/PS>Get-Sites

Output:
Name                  Id            Type
----
Default Site 43b045f6-2998-4269-
             9455-5ff5c3520854      symc-csm-
                                    AssetSystem-Asset-
                                    Infra-Site
```

Description: Returns Name, Id, and Type of all the sites available in the CCS system.

Example 2

```
C:/PS>Get-Sites –Name “ABC”
Output:
Name          Id                    Type
----
ABC     43b045f6-2998-4269-
       9455-5ff5c3520854    symc-csm-AssetSystem-
                            Asset-Infra-Site
```

Description: Returns Name, Id, and Type of the specified sites in the CCS system.

Related Links

See Create-AssetImportJob on page 1143.

Search-AssetGroups

`Search-AssetGroups` – Finds an asset group or asset groups based on the search criteria.

Synopsis

The Search-AssetGroups cmdlet finds the asset groups based on the specified filters.

Syntax

```
Search-AssetGroups -AppServerNameAndPort <String>
[-BindingType <String>] [-ContainerPath <String>] [-Filter <String[]>]
[-SearchSubTree [<Boolean>]] [-ExcludePredefin
    eObjects [<Boolean>]] [-NumberOfObjectsToRetrieve <Int32>]
[-PipingEnabled [<Boolean>]] [<CommonParameters>]
```

Authorization requirements

You must have the following CCS tasks to use the cmdlet:

- View Assets

Note: You do not require permissions on any folders to use the cmdlet.

Description

The Search-AssetGroups cmdlet returns the specified asset group or a list of asset groups based on the search criteria. The Search-AssetGroups cmdlet returns both, the static and the dynamic the asset groups

Parameters

The following table describes the input parameters that the cmdlet requires:

Table B-2 Search-AssetGroups - parameters

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
AppServerNameAndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServerNameAndPort="<AppServer Name/IP> : <Port Number Corresponding To Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-2 Search-AssetGroups - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$Binding Type="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.
ContainerPath	Optional	String	No	The path of the folder that contains the asset group. The default value of the parameter is Null.

Table B-2 Search-AssetGroups - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
Filter	Optional	Scriptblock	No	The Scriptblock should contain one or more Expressions. You have to use { } brackets for the filter. **Note:** If you do not specify any value in the Filter parameter, the cmdlet returns all the asset groups.
SearchSubTree	Optional	Boolean	No	The default value for the parameter is True. True or False value that states if the sub-tree under the folder has to be searched for the asset group or not.
Exclude Predefined Objects	Optional	Boolean	No	The default value for the parameter is False. True or False value that states if the predefined objects should be excluded from the search criteria.

Table B-2 Search-AssetGroups - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
NumberOf Objects ToRetrieve	Optional	Integer	No	The maximum number of asset groups that the cmdlet must return. The default value for the parameter is Null.
PipingEnabled	Optional	Boolean	No	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

The Expression of the Filter contains the following information:

Table B-3 Expression

Switch name	Switch type	Data type	Description
FieldName	Mandatory	String	The name of the field.
ExpressionOperator	Mandatory	String	The ExpressionOperator contains the following members: ■ EqualTo ■ Contains ■ StartsWith ■ EndsWith
FieldValue	Mandatory	String	The value of the field.

Table B-3 Expression *(continued)*

Switch name	Switch type	Data type	Description
FieldType	Optional	String	The data type by which you want to compare the fields. The FieldDataType contains the following members: - String - DateTime - Boolean - Guid **Note:** If FieldType is not provided, then String type will be used by default.

Filter can have more than one expression.

You have to apply the following rules while using the filter expression:

- The expression should be inside " " double quotes.
- The expression consists of FieldName, ExpressionOperator, FieldValue ,and FieldType. Each of these parts is separated by , comma.
- The comma can be escaped using \ backslash.
- The expression can be inside ( ) parentheses.

To combine multiple filter expressions, you can use the following logical operators:

Table B-4 Logical Operators

Operator name	Description	Usage
-and	Logical AND is used to add expressions to the search.	For example, -Filter {(("objectGUID, equalto, c8f0de1a-a278-4c29-86a1 -47d5ab91cb16, Guid") -and (("displayname, startswith, domainname\machinename"))}

Table B-4 Logical Operators *(continued)*

Operator name	Description	Usage
-or	Logical OR is used to provide options to the search.	For example, -Filter {(("objectGUID, equalto, c8f0de1a-a278-4c29-86a1 -47d5ab91cb16, Guid") -or (("displayname, startswith, domainname\machinename"))}
!	Logical ! (bang) is used to negate the ExpressionOperator.	For example, -Filter {(("objectGUID, equalto, c8f0de1a-a278-4c29-86a1 -47d5ab91cb16, Guid") -and!("displayname, endswith, admin"))}

Inputs

You cannot pipe objects to the cmdlet.

Outputs

The Search-AssetGroups cmdlet returns the list of asset groups.

The Asset Group object contains the following information:

Table B-5 Asset Group object

Switch name	Data type	Description
Id	Guid	The unique identifier of the asset group.
Name	String	The display name of the asset group.
Description	String	The description of the asset group
Type	String	The type of the asset group such as static or dynamic.
ContainerPath	String	The path to the asset group folder.

Table B-5 Asset Group object *(continued)*

Switch name	Data type	Description
Owner	String	The name of the user who created the asset group.
ModifiedBy	String	The name of the user who last modified the asset group.

Notes

- You can set AppServerNameAndPort variable only once and reuse it till the session is closed.
- If you do not specify any filter for the cmdlet, the cmdlet returns all the asset groups.
  The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example 1

```
Search-AssetGroups -Filter {("displayname,startswith,win") -and
("displayname,contains,2003")} -NumberOfObjectsToRetrieve 1
```

Description: The Script block is written in the filter to search for specific Asset group

Example 2

```
Search-AssetGroups -Filter {("displayname,startswith,win")}
-ExcludePredefineObjects 1
```

Description: The Script block is written in the filter to search for specific Asset group

Related Links

See Add-AssetsToAssetGroup on page 1153.

Create-AssetImportJob

`Create-AssetImportJob` – Creates an asset import job and returns guid of the created Job.

Synopsis

The Create-AssetImportJob cmdlet creates an asset import job and returns the unique identifier of the newly created Job.

Syntax

```
Create-AssetImportJob -AppServerNameAndPort
<String> [-BindingType <String>]
-Name <String> [-Description <String>] -AssetType <String>
[-DataCollector <String>]
[-Assets <Asset[]>] [-Sites <SiteIdentifier[]>] -ReconciliationRules
<ReconciliationRule>
[-Schedule <ScheduleData>] [-SuccessNotification <NotificationData>]
[-FailureNotification <NotificationData>]
[-ScopeAssetType <String[]>] [-PipingEnabled [<Boolean>]]
[<CommonParameters>]
```

Authorization requirements

You must have the following CCS tasks to use the cmdlet:

- Manage Job

You must have the permissions on following folders to use the cmdlet:

- Asset System
- Reconciliation rules

Description

The Create-AssetImportJob cmdlet creates a job to import the assets into the asset system and returns guid of the created job based on the specified parameters.

Parameters

The following table describes the input parameters that the Create-AssetImportJob cmdlet requires:

Table B-6 Create-AssetImportJob - parameters

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
AppServerName AndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServer NameAndPort="< AppServer Name/IP> : <Port Number Corresponding To Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-6 Create-AssetImportJob - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$Binding Type="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.
Name	Mandatory	String	No	The name of the asset import job.
Description	Optional	String	No	The description of the asset import job.
AssetType	Mandatory	String	No	The type of the asset. For example, "Windows Machine" . Get the value for this parameter from the Output of the `Get-AllAssetTypes` cmdlet.

Table B-6 Create-AssetImportJob - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
DataCollector	Optional	String	No	The default value of the parameter is Null that uses the Default data collector for importing assets. You can specify the value as Default, CSV, or ODBC.
Assets	Mandatory	List<Asset>	Yes	Get the value for this parameter from the Output of the `Search-Assets` cmdlet.
Sites	Mandatory	String	No	The Site object list. Get the value for this parameter from the output of the `Get-Sites` cmdlet.
Reconciliation Rules	Mandatory	Reconciliation Rule	Yes	Get the value for this parameter from the Output of the `Initialize-ReconciliationRule` helper class.
Schedule	Optional	ScheduleData	Yes	Get the value for this parameter from the Output of the `Initialize-Schedule` helper class.

Table B-6 Create-AssetImportJob - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
Success Notification	Optional	NotificationData	Yes	Get the value for this parameter from the Output of the `Initialize-Email Notification` helper class.
Failure Notification	Optional	NotificationData	Yes	Get the value for this parameter from the Output of the `Initialize-Email Notification` cmdlet.
ScopeAssetType	Optional	String	Yes	The scope type. The default value of this parameter is Assets.
PipingEnabled	Optional	Boolean	Yes	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

The following table describes the output of the Initialize-Schedule cmdlet that is used as the input parameters for the Create-AssetImportJob cmdlet.

Table B-7 Schedule Object

Switch Name	Data Type	Description
RepeatDays	Integer	The number of days after which you want to re-run the job. The value for this field is considered only if you set True for RunEveryNDays.
RunEveryNDays	Boolean	The default value of this parameter is False. True if you want to run the job at a specified interval that is provided in the RepeatDays field. False if you do not want to run the job at a specified interval.
RunNow	Boolean	The default value of this parameter is False. True if you want to run the job immediately . False if you do not want to run the job immediately.
RunOnce	Boolean	The default value of this parameter is False. True if you want to run the job only once on the StartDate. False if you do not want to run the job only once on the StartDate.
RunPeriodically	Boolean	The default value of this parameter is False. True if you want to run the job periodically. If you set True for this field, you must set True for either of the following: ■ RunOnce ■ RunEveryNDays False if you do not want to run the job periodically.

Table B-7 Schedule Object *(continued)*

Switch Name	Data Type	Description
StartDate	DateTime	The date when the job run must begin. If you set True for RunNow, the job is run immediately. If you set True for RunPeriodically, one of the following options is possible: ■ You can set RunOnce. The job will be run only once on the start date, You can set RunEveryNDays. The job will be repeated after every <RepeatDays> starting from specified StartDate.

The following table describes the output of the Initialize-AssetNotificationData cmdlet that is used as the input parameters for the Create-AssetImportJob cmdlet.

Table B-8 Notification Object

Switch name	Data type	Description
ToEmailAddress	String	The email address to which the notification must be sent.
FromEmailAddress	String	The email address from which the notification must be sent.
Subject	String	The subject of the email notification.
Body	String	The detailed message.

The following table describes the Asset object that is default value of ScopeAssetType parameter for the Create-AssetImportJob cmdlet.

The Asset object contains the following information:

Table B-9 Asset object

Switch name	Data type	Description
ID	Guid	The unique identifier of the asset in the system.

Table B-9 Asset object *(continued)*

Switch name	Data type	Description
Type	AssetType	The asset type.
DisplayName	String	The display name of the asset.
Path	String	The full path of the asset.
Attributes	Attributes	The attributes of the object.

Inputs

You can pipe output of Search-Assets, Initialize-Emailnotification, Initialize-Schedule, or Get-Sites to Create-AssetImportJob.

Outputs

The Create-AssetImportJob cmdlet returns Guid of the created Job as an output.

Notes

You can set AppServerNameAndPort variable only once and reuse it till the session is closed.

You can set BindingType variable only once and reuse it till the session is closed.

The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example 1

```
C:/PS> $jobName = "Asset Import Job 1 "
C:/PS> $dataCollector = "Default" # Default/CSV/ODBC

#Assets
C:/PS> $Assets = Search-Assets -AssetType
"Windows Machine" -Filter {("displayname,startswith,win")}
-NumberOfObjectsToRetrieve 5
C:/PS> $Sites = get-sites
#ReconcialiationRules
C:/PS> $ReconcialiationRules = @()
C:/PS> $ReconcialiationRule = Initialize-ReconciliationRule
```

```
-Name "Add asset to the Asset System"
-Path "Reconciliation Rules\Pre-defined Rules"
C:/PS> $ReconcialiationRules += $ReconcialiationRule

#Schedule Data
C:/PS> $ScheduleData = Initialize-Schedule -RepeatDays 7
-RunEveryNDays $FALSE -RunNow $TRUE -RunOnce $True
-RunPeriodically $TRUE   -StartDate <(get-date).AddMinutes(10))

#SuccessNotification
C:/PS> $SuccessNotification = Initialize-EmailNotification
-FromAddress "user1 @symantec.com" -ToAddress "user2@symantec.com"
-Subject "Success Notification Message"  -Body "Test Body"

#FailureNotification
C:/PS> $FailureNotification = Initialize-EmailNotification
-FromAddress "user1@symantec.com" -ToAddress "user2@symantec.com"
-Subject "Failure Notification Message"  -Body "Test Body"

C:/PS> Create-AssetImportJob  -Name $jobName -Description
"Test Job Description" -DataCollector $dataCollector
-AssetType "symc-csm-AssetSystem-Asset-Wnt-Machine" -Assets
$Assets -Sites $Sites -ReconciliationRules $ReconcialiationRules
-Schedule $ScheduleData  -SuccessNotification $SuccessNotification
-FailureNotification  $FailureNotification

Output
3748c44b-342c-4431-b6c4-778be6e71d20
```

Example 2

```
C:/PS> $jobName = "Asset Import Job2 "
C:/PS> $dataCollector = "Default" # Default/CSV/ODBC

#ReconcialiationRules
C:/PS> $ReconcialiationRules = @()
$ReconcialiationRule = Initialize-ReconciliationRule
-Name "Add asset to the Asset System"
-Path "Reconciliation Rules\Pre-defined Rules"
$ReconcialiationRules += $ReconcialiationRule

#Schedule Data
C:/PS> $ScheduleData = Initialize-AssetScheduleData
```

```
-RepeatDays 7 -RunEveryNDays $FALSE -RunNow $TRUE
-RunOnce $True -RunPeriodically $TRUE -StartDate <(get-date).AddMinutes(10)))
#SuccessNotification
C:/PS> $SuccessNotification = Initialize-EmailNotification
-FromAddress "user1@symantec.com"
-ToAddress "user2@symantec.com" -Subject
"Success Notification Message"  -Body "Test Body"

#FailureNotification
C:/PS> $FailureNotification =
Initialize-EmailNotification -FromAddress "user1@symantec.com"
-ToAddress "user2@symantec.com" -Subject
"Failure Notification Message"  -Body "Test Body"

C:/PS> Search-Assets -Filter {("displayname,startswith,e2e")}
-AssetType "symc-csm-AssetSystem-Asset-Wnt-Machine"
-PipingEnabled $True |   Create-AssetImportJob
-Name $jobName -Description "Test Job Description"
-DataCollector $dataCollector -AssetType
"symc-csm-AssetSystem-Asset-Wnt-Machine"
-ReconciliationRules $ReconcialiationRules
-Schedule $ScheduleData  -SuccessNotification
$SuccessNotification
-FailureNotification  $FailureNotification
Output
4748c44b-342c-4431-b6c4-778be6e71d20
```

Description: It shows how the output of the Search-Assets can be piped to Create-AssetImportJob and its execution.

Related Links

See Initialize-ReconciliationRule on page 1202.

See Initialize-Schedule on page 1453.

See Initialize-EmailNotification on page 1459.

See Search-Assets on page 1190.

See Get-AllAssetTypes on page 1164.

Add-AssetsToAssetGroup

`Add-AssetsToAssetGroup` – Adds the asset to the specified static asset group.

Synopsis

The Add-AssetToAssetGroup cmdlet adds the assets to the specified static asset group.

Syntax

```
Add-AssetsToAssetGroup -AppServerNameAndPort <String>
[-BindingType <String>] -Id <Guid>
-Assets <Asset[]> [-PipingEnabled [<Boolean>]]
[<CommonParameters>]
```

Authorization requirements

You must have the following CCS tasks to use the cmdlet:

- View Assets
- Manage Assets and Asset Groups

You must have the permissions on following folders to use the cmdlet:

- Asset System

Description

You can add the assets to the specified asset group using Add-AssetsToAssetGroup cmdlet. You cannot add assets to a dynamic asset group. You can add assets to the asset group only from the folder that contains the asset group.

Parameters

The following table describes the parameters that the Add-AssetToAssetGroup cmdlet requires:

Table B-10 Add-AssetsToAssetGroup - parameters

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
AppServerName AndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServer NameAndPort ="< AppServer Name/IP> : <Port Number Corresponding To Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-10 Add-AssetsToAssetGroup - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$Binding Type="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.
Id	Mandatory	Id	No	The id of an asset group.
Assets	Mandatory	Assets	Yes	The list of Asset objects.

Table B-10 Add-AssetsToAssetGroup - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
PipingEnabled	Optional	Boolean	Yes	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

Each Asset object contains the following information:

Table B-11 Asset object

Switch name	Data type	Description
Id	Guid	The unique identifier of the asset in the system.
Type	AssetType	The asset type.
DisplayName	String	The display name of the asset.
Path	String	The full path of the asset.
Attributes	Attributes	The attributes of the object.

Inputs

You can pipe the output of Search-Assets to Add-AssetsToAssetGroup

Outputs

The Add-AssetsToAssetGroup cmdlet does not return any output. As a result of the successful execution of the cmdlet, the assets are added to the asset group.

Notes

You can set AppServerNameAndPort variable only once and reuse it till the session is closed.

You can set BindingType variable only once and reuse it till the session is closed.

The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example 1

```
C:\PS> $Assets = Search-Assets -Filter
{("displayname,startswith,Win")}
-SearchsubTree $True -AssetType "symc-csm-AssetSystem-Asset-Wnt-Machine"
PS C:\ > Search-AssetGroups -ExcludePredefineObjects $TRUE
PS C:\ > Add-AssetsToAssetGroup -Id " fd5db668-8957-4da5-96b2-a02a2a46161e
" -Assets $Assets

Output:
Id            : fd5db668-8957-4da5-96b2-a02a2a46161e
Name          : test
Description   : test
Type          : Static
ContainerPath : Asset System
Owner         : DOMAINNAME\Administrator
ModifiedBy    : DOMAINNAME \Administrator
ExtensionData : System.Runtime.Serialization.ExtensionDataObject
```

Description: The ID of the AssetGroup is retrieved using the Add-AssetsToAssetGroup cmdlet. The assets to be added to the Asset group are assigned to variable $Assets and used as the input to the Add-AssetsToAssetGroup.

Example 2

```
C:\PS> Search-Assets -Filter {("displayname,startswith,Name")}
-SearchsubTree $True
-AssetType "symc-csm-AssetSystem-Asset-Wnt-Machine" -PipingEnabled $true |
Add-AssetsToAssetGroup
-Id "be2d252b fd5db668-8957-4da5-96b2-a02a2a46161e "
```

Description: The ID of the AssetGroup is retrieved using the Add-AssetsToAssetGroup cmdlet. The assets to be added to the Asset group are retrieved using the Search-Assets cmdlet and piped it to the Add-AssetsToAssetGroup.

Related Links

See Search-Assets on page 1190.

Remove-Assets

`Remove-Assets` – Removes the specified assets from the asset system.

Synopsis

The Remove-Assets cmdlet removes the specified assets from the asset system.

Syntax

```
Remove-Assets -AppServerNameAndPort <String>
[-BindingType <String>] -Assets <Asset[]>
[-PipingEnabled [<Boolean>]] [<CommonParameters>]
```

Authorization requirements

You must have the following CCS tasks to use the cmdlet:

- View Assets
- Manage Assets and Asset Groups

You must have the permissions on following folders to use the cmdlet:

- Asset System

Description

The Remove-Assets cmdlet removes the specified asset. It also deletes associated asset data either from the SQL store or from the CCS directory.

Parameters

The following table describes the input parameters that the Remove-Assets cmdlet requires:

Table B-12 Remove-Assets - parameters

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
AppServerName AndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServer NameAndPort="< AppServer Name/IP> : <Port Number Corresponding To Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-12 Remove-Assets - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$Binding Type="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.
Assets	Mandatory	List< Asset>	Yes	Get the value for this parameter from the Output of the `Search- Assets` cmdlet.
PipingEnabled	Optional	Boolean	Yes	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

The following table describes the output of the Search-Assets cmdlet that is used as the input parameters for the Remove-Assets cmdlet.

Table B-13 Asset Object

Switch Name	Data Type	Description
Id	Guid	The unique identifier of the asset in the system.
Type	AssetType	The asset type.
DisplayName	String	The display name of the asset.
Path	String	The full path of the asset.
Attributes	Attributes	The attributes of the object.

Inputs

You can pipe output of Search-Assets to Remove-Assets.

Outputs

The Remove-Assets cmdlet does not return any value as an output. As a result of the successful execution of the cmdlet, the assets are removed from the CCS system.

Notes

You can set AppServerNameAndPort variable only once and reuse it till the session is closed.

You can set BindingType variable only once and reuse it till the session is closed.

The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example 1

```
C:/PS> $assets= Search-Assets  -AssetType "Windows Machine"
-NumberOfObjectsToRetrieve 5
C:/PS>Remove-Assets  - Assets $assets

Output:
Assets deleted successfully.
```

Description: The assets with specified criteria gets removed from the system.

Example 2

```
C:/PS> Search-Assets  -Filter {("displayname,startswith,Win")}
-SearchsubTree $True
-AssetType "symc-csm-AssetSystem-Asset-Wnt-Machine"  |
Remove-Assets

Output:
Assets deleted successfully.
```

Description: The assets with specified criteria gets removed from the system.

Related Links

See Search-Assets on page 1190.

Get-AllAssetTypes

`Get-AllAssetTypes` – Returns the list of all the asset types in the asset system.

Synopsis

The Get-AllAssetTypes cmdlet returns all the asset types that the CCS system supports.

Syntax

```
Get-AllAssetTypes -AppServerNameAndPort <String>
[-BindingType <String>] [-PipingEnabled [<Boolean>]] [<CommonParameters>]
```

Authorization requirements

You must have the following CCS tasks to use the cmdlet:

- View Assets

Note: You do not require permissions on any folders to use the cmdlet.

Description

Returns all the asset types in the CCS system.

Parameters

The following table describes the parameters that the Get-AllAssetTypes cmdlet requires:

Table B-14 Get-AllAssetTypes - parameters

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
AppServerNameAndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServerNameAndPort="< AppServer Name/IP> : <Port Number Corresponding To Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-14 Get-AllAssetTypes - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$Binding Type="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.
PipingEnabled	Optional	Boolean	No	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

Inputs

You cannot pipe objects to the cmdlet.

Outputs

The Get-AllAssetTypes cmdlet returns the list of all the asset types in the CCS system.

The Asset Type object contains the following information:

Table B-15 Asset Type object

Filed name	Data type	Description
DisplayName	String	The display name of the asset type.
Name	String	The asset type name.
Description	String	The description of the asset type.

Notes

You can set AppServerNameAndPort variable only once and reuse it till the session is closed.

You can set BindingType variable only once and reuse it till the session is closed.

The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example 1

```
C:/PS>Get-AllAssetTypes
```

Description: Returns all the asset types available in the CCS system.

Related Links

See Search-Assets on page 1190.

Get-AttributesOnFilter

`Get-AttributesOnFilter` – Returns the attributes of the specified asset type that match the search criteria.

Synopsis

The Get-AttributesOnFilter cmdlet returns the ArrayOfAssetAttributeMetaData object based on the given parameters..

Syntax

```
Get-AttributesOnFilter -AppServerNameAndPort <String>
[-BindingType <String>] -AssetType <String> [-AttributeType <Int32>]
[-PipingEnabled [<Boolean>]] [<CommonParameters>]
```

Authorization requirements

You must have the following CCS tasks to use the cmdlet:

- View Assets

Note: You do not require permissions on any folders to use the cmdlet.

Description

The Get-AttributesOnFilter cmdlet returns the ArrayOfAssetAttributeMetaData object based on the given parameters.

Parameters

The following table describes the parameters that the cmdlet requires:

Table B-16 Get-AttributesOnFilter - parameters

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
AppServerNameAndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServerNameAndPort="<AppServer Name/IP> : <Port Number Corresponding To Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-16 Get-AttributesOnFilter - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$Binding Type="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.
AssetType	Mandatory	String	No	A valid asset type.

Table B-16 Get-AttributesOnFilter - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
AttributeType	Mandatory	Integer	No	The parameter requires an integer value that is derived from the AttributeType data contract. Use the following values to create a filter criteria to get the attributes of specific types. ■ All = 0 ■ Primary = 1 ■ Mandatory = 2 ■ Optional = 4 ■ Base = 8 ■ AssetSpecific = 16 ■ Predefined = 32, ■ Custom = 64
PipingEnabled	Optional	Boolean	No	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

Inputs

You cannot pipe objects to the cmdlet.

Outputs

The Get-AttributesOnFilter cmdlet returns the ArrayOfAssetAttributeMetaData object.

The Get-AttributesOnFilter cmdlet returns the following information in the output:

Table B-17 ArrayOfAssetAttributeMetaData - object

Switch Name	Data Type	Description
DisplayName	String	Display name of the field. For example: Domain/Workgroup Name
Name	String	Name of the field. For example: symc-csm-AssetSystem-Asset- Dbif-server-SQLServerDomainName
Description	String	Description of the field.
FieldTypes	FieldType	The FieldType data contact. Returns if the field is primary, mandatory, or optional.
Type	String	The data type of the field.
IsBaseAttribute	Boolean	Returns True if the field is a base attribute.
IsCaseSensitive	Boolean	Returns True if the field is case sensitive and False if the field is not case sensitive.
IsEditable	Boolean	Returns True if the field is editable and False if the field is not editable.
IsPredefined	Boolean	Returns True if the field is Predefined and False if the field is custom.
IsSingleValued	Boolean	Returns True if the field is single-valued and False if the field is multi-valued.
OptionalProperties	Optional Properties	Represents optional properties for field
OrdinalValues	OrdinalValues	Represents list of ordinal values for field.

Table B-17 ArrayOfAssetAttributeMetaData - object *(continued)*

Switch Name	Data Type	Description
Range	AssetAttributeRange	Represents the upper and the lower range of the fields.

Notes

You can set AppServerNameAndPort variable only once and reuse it till the session is closed.

You can set BindingType variable only once and reuse it till the session is closed.

The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example 1

```
C:/PS>Get-AttributesOnFilter -AssetType
"Windows Machine" -AttributeType 3  |
Format-  table  Name, Displayname
```

Description: Returns mandatory and primary [1+2] attributes of the asset type “Windows Machine” and displays in table format as Name and Display name.

Example 2

```
C:/PS>$Type=Get-AllAssetTypes
C:/PS>Get-AttributesOnfilter -AssetType
$Type[0].Display name
```

Description: Returns all Attributes of the asset type returned by the Get-AllAssetTypes cmdlet.

Related Links

See Get-AllAssetTypes on page 1164.

See Get-AssetDetails on page 1174.

See Update-Asset on page 1185.

Get-AssetDetails

`Get-AssetDetails` – Returns the detailed information of the specified asset.

Synopsis

The Get-AssetDetails cmdlet returns the Asset Object.

Syntax

```
 Get-AssetDetails -AppServerNameAndPort <String>
[-BindingType <String>] -Id <Guid> [-PipingEnabled [<Boolean>]]
[<CommonParameters>]
```

Authorization requirements

You must have the following CCS tasks to use this cmdlet:

- View Assets
- Manage Assets and Asset Groups

You must have the permissions on following folders to use this cmdlet:

- Asset System

Description

The Get-AssetDetails cmdlet returns the details of the specified asset as an Asset object.

Parameters

The following table describes the parameters that the cmdlet requires:

Table B-18 Get-AssetDetails - parameters

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
AppServerNameAndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServerNameAndPort="<AppServer Name/IP> : <Port Number Corresponding To Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-18 Get-AssetDetails - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$Binding Type="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.
Id	Mandatory	Guid	No	The unique identifier of the asset in the system.
PipingEnabled	Optional	Boolean	Yes	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

Inputs

You can pipe output of Search-Assets to Get-AssetDetails.

Outputs

The Get-AssetDetails cmdlet returns the Asset Object.

The Asset Object contains the following information:

Table B-19 Asset object

Switch name	Data type	Description
Id	Guid	The unique identifier of the asset in the system.
Name	String	The display name of the asset.
Type	AssetType	The asset type.
Path	String	The full path of the asset.
Attributes	Attributes	The attributes of the object.

Notes

You can set AppServerNameAndPort variable only once and reuse it till the session is closed.

You can set BindingType variable only once and reuse it till the session is closed.

The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example 1

```
C:/PS> Get-AssetDetails  -Id  bb152ef1-8fe0-4b41-bfb3-c2d1b323ea4b

Output:
Id              : bb152ef1-8fe0-4b41-bfb3-c2d1b323ea4b
Name            :SQL -database
Type            : Symantec.CSM.PS.Assets.RefAssetService.AssetType
Path            : Asset System
Attributes      : {symc-csm-AssetSystem-Asset-Dbif-database-domainNameField,
symc-csm-AssetSystem-Asset-Dbif-database-hostNameField,
symc-csm-AssetSystem-databasesName...}
ExtensionData : System.Runtime.Serialization.ExtensionDataObject
```

Description: Returns details of the asset when asset Id is passed on as the input.

Example 2

```
C:/PS> Search-Assets -NumberOfObjectsToRetrieve 2|Get-AssetDetails

Output:
Id             : bb152ef1-8fe0-4b41-bfb3-c2d1b323ea4b
Name           :SQL -database1
Type           : Symantec.CSM.PS.Assets.RefAssetService.AssetType
Path           : Asset System
Attributes     : {symc-csm-AssetSystem-Asset-Dbif-database-domainNameField,
symc-csm-AssetSystem-Asset-Dbif-database-hostNameField,
symc-csm-AssetSystem-databasesName...}
ExtensionData : System.Runtime.Serialization.ExtensionDataObject
Output:
Id             : bb152ef1-8fe0-4b21-bfb3-c2d1b323ea4b
Name           :SQL -database2
Type           : Symantec.CSM.PS.Assets.RefAssetService.AssetType
Path           : Asset System
Attributes     : {symc-csm-AssetSystem-Asset-Dbif-database-domainNameField,
 symc-csm-AssetSystem-Asset-Dbif-database-hostNameField,
symc-csm-AssetSystem-databasesName...}
ExtensionData : System.Runtime.Serialization.ExtensionDataObject
```

Description: The output of the Search-Assets cmdlet can be used as an input to Get-AssetDetails.

Related Links

- See Search-Assets on page 1190.
- See Update-Asset on page 1185.
- See Get-AttributesOnFilter on page 1168.

Get-Scores

`Get-Scores` – Returns the risk and compliance information of the specified asset.

Synopsis

The Get-Scores cmdlet returns the AssetScores object based on the given parameters.

Syntax

```
Get-Scores -AppServerNameAndPort <String>
[-BindingType <String>] -Assets <Asset[]> [-PipingEnabled
[<Boolean>]] [<CommonParameters>]
```

Authorization requirements

You must have the following CCS tasks to use this cmdlet:

- View Assets

You must have the permissions on following folders to use this cmdlet:

- Asset System

Description

The Get-Scores cmdlet returns the AssetScores object that comprises the consolidated risk score, the consolidated compliance score, and the risk rating of the specified asset.

Parameters

The following table describes the parameters that the cmdlet requires:

Table B-20 Get-Scores - parameters

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
AppServerNameAndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServerNameAndPort="<AppServerName/IP> : <Port Number Corresponding To Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-20 Get-Scores - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$Binding Type="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.
Assets	Mandatory	List<Asset>	Yes	The list of Asset objects for which you want to get the consolidated compliance scores and risk ratings. You can get the value of this parameter from the `Search-Assets` or `Get-Asset Details` cmdlet.

Table B-20 Get-Scores - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
PipingEnabled	Optional	Boolean	Yes	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

The Asset data type of the Assets field contains the following information:

Table B-21 Asset object

Switch name	Switch Type	Data type	Description
Id	Mandatory	Guid	The unique identifier of the asset in the system.
Type	Optional	AssetType	The asset type.
Name	Optional	String	The display name of the asset.
Path	Optional	String	The full path of the asset.
Attributes	Optional	Attributes	The attributes of the object.

Inputs

You can pipe output of Search-Assets to Get-Scores.

Outputs

The Get-Scores cmdlet returns the AssetScores object.

The AssetScores object contains the following information:

Table B-22 AssetScores object

Switch name	Data type	Description
Id	Guid	The ID of the asset.
Type	AssetType	The asset type.
Name	String	The display name of the asset.
Path	String	The full path of the asset.
RiskScore	Float	The consolidated risk score of the specified asset. This is the score that is calculated based on the weights specified for different providers for the risk property.
ComplianceScore	Float	The consolidated compliance score of the specified asset. This is the score that is calculated based on the weights specified for different providers for the compliance property.
MaxRiskScore	Float	The maximum risk score is the maximum value amongst the risk weight from all the providers for the specified asset. The maximum risk score is the Risk Rating for the asset.

Notes

You can set AppServerNameAndPort variable only once and reuse it till the session is closed.

You can set BindingType variable only once and reuse it till the session is closed.

The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example 1

```
C:/PS> $Assets = Search-Assets -Filter {("displayname,startswith,Win")}
-AssetType "symc-csm-AssetSystem-Asset-Wnt-Machine"
C:/PS> Get-Scores  -Assets $Assets
```

Description: The output of the Search-Assets is collected in variable. The $Assets given as the input to Get-Scores, which in turn returns the Id, Name, Path, Type ,RiskScore, ComplianceScore, and MaxRiskScore.

Example 2

```
C:/PS> Search-Assets –NumberOfObjectsToRetrieve 2 | Get-Scores
```

Description: The output of the Search-Assets can be directly piped to Get-Scores that returns Id, Name, Path, Type ,RiskScore, ComplianceScore, and MaxRiskScore.

Related Links

- See Search-Assets on page 1190.
- See Update-Asset on page 1185.
- See Get-AssetDetails on page 1174.

Update-Asset

`Update-Asset` – Updates the asset fields.

Synopsis

The Update-Asset cmdlet updates the asset fields

Syntax

```
Update-Asset -AppServerNameAndPort <String>
[-BindingType <String>] -Asset <Asset> [-PipingEnabled
[<Boolean>]] [<CommonParameters>]
```

Authorization requirements

You must have the following CCS tasks to use this cmdlet:

- View Assets
- Manage Assets and Asset Groups

You must have the permissions on following folders to use this cmdlet:

- Asset System

Description

The Update-Asset cmdlet updates the following fields of the specified asset or assets:

- Id
- Type
- DisplayName
- Path
- Attributes

Parameters

The following table describes the parameters that the Update-Asset cmdlet requires:

Table B-23 Update-Asset - parameters

Switch Name	Switch Type	Data Type	Supports piping input? Yes/No	Description
AppServerNameAndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServerNameAndPort="<AppServer Name/IP> : <Port Number Corresponding To Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-23 Update-Asset - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? Yes/No	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$Binding Type="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.
Asset	Mandatory	Asset	No	The Asset object which you want to update. You can get the value of this parameter from the `Search-Assets` cmdlet.
PipingEnabled	Optional	Boolean	Yes	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

The data type for the Asset field is an Asset object that contains the following information:

Table B-24 Asset object

Switch name	Data type	Description
Id	Guid	The unique identifier of the asset in the system.
Type	AssetType	The asset type.
Name	String	The display name of the asset.
Path	String	The full path of the asset.
Attributes	Attributes	The attributes of the object.

Inputs

You cannot pipe objects to the cmdlet.

Outputs

The Update-Asset cmdlet does not provide any output. The values of the fields of the specified assets are updated.

Notes

You can set AppServerNameAndPort variable only once and reuse it till the session is closed.

You can set BindingType variable only once and reuse it till the session is closed.

The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example

```
C:/PS> $asset=Get-AssetDetails -Id
"baf2bdeb-66ed-4a79-b424-b4e8ea67ea91"
 #Asset ID
#$asset.Attributes | ForEach-Object {
```

```
#
Write-Host $_.DisplayName
#
Write-Host $_.value
#                                    }
#Attribute[9] =
"symc-csm-AssetSystem-Asset-Wnt-Machine-HostNameDNS"
C:/PS> $asset.attributes[9].Value="Test Host Name 1"
#symc-csm-AssetSystem-Asset-AssetBase-Confidentiality=low
C:/PS> $asset.attributes[14].Value=1
#symc-csm-AssetSystem-Asset-AssetBase-Integrity=Medium
C:/PS> $asset.attributes[15].Value=2
#symc-csm-AssetSystem-Asset-AssetBase-Availability=High
C:/PS> $asset.attributes[16].Value=3
#Owner
C:/PS> $asset.attributes[20].Value="abc"
C:/PS> Update-Asset -Asset $asset

Output:
Returns message:
Asset updated Successfully.
```

Description: It demonstrates how the asset attribute values are retrieved from the Get-AssetDetails cmdlet. The changed values then passed on to the Update-Assets cmdlet.

Related Links

- See Search-Assets on page 1190.
- See Get-AssetDetails on page 1174.

Search-Assets

`Search-Assets` – Finds an asset or assets based on the search criteria.

Synopsis

The Search-Assets cmdlet finds an asset or assets that match the specified search criteria.

Syntax

```
Search-Assets -AppServerNameAndPort <String>
[-BindingType <String>] [-AssetType <String>]
[-ContainerPath <String>] [-Filter <String[]>]
[-SearchSubTree [<Boolean>]]
    [-ExcludePredefineObjects [<Boolean>]]
[-NumberOfObjectsToRetrieve <Int32>] [-PipingEnabled
[<Boolean>]] [<CommonParameters>]
```

Authorization requirements

You must have the following CCS tasks to use the cmdlet:

- View Assets

You must have the permissions on following folders to use the cmdlet:

- Asset System

Description

The Search-Assets cmdlet finds an asset or a list of assets that matches the specified filter.

Parameters

The following table describes the parameters that the cmdlet requires:

Table B-25 Search-Assets - parameters

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
AppServerNameAndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServerNameAndPort="<AppServerName/IP> : <Port Number CorrespondingTo Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-25 Search-Assets - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$Binding Type="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-25 Search-Assets - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
AssetType	Optional	AssetType	No	The type of an asset. For example, Windows Machine. Get the value of this parameter from the Get-AllAssetTypes cmdlet. You can use either Name or DisplayName of the asset type returned by the Get-AllAssetTypes cmdlet.
ContainerPath	Optional	ContainerPath	No	The path of the folder that contains the assets. The default value of the parameter is Null.

Table B-25 Search-Assets - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
Filter	Optional	Scriptblock	No	The Scriptblock should contain one or more Expressions. You have to use { } brackets for the filter. **Note:** If you do not specify any value in the Filter parameter, the cmdlet returns all the assets.
SearchSubTree	Optional	Boolean	No	The default value for the parameter is True. True or False value that states if the sub-tree under the folder has to be searched for the asset or not.

Table B-25 Search-Assets - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
Exclude Predefine Objects	Optional	Boolean	No	The default value for the parameter is False. True or False value that states if the predefined objects should be excluded from the search criteria.
NumberOf Objects ToRetrieve	Optional	Int	No	The maximum number of assets that the cmdlet must return. The default value for the parameter is Null.
PipingEnabled	Optional	Boolean	No	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

Table B-26 Expression

Switch name	Switch type	Data type	Description
FieldName	Mandatory	String	The name of the field.

Table B-26 Expression *(continued)*

Switch name	Switch type	Data type	Description
ExpressionOperator	Mandatory	String	The ExpressionOperator contains the following members: ■ EqualTo ■ Contains ■ StartsWith ■ EndsWith
FieldValue	Mandatory	String	The value of the field.
FieldType	Optional	String	The data type by which you want to compare the fields. The FieldDataType contains the following members: ■ String ■ DateTime ■ Boolean ■ Guid **Note:** If FieldType is not provided, then String type will be used by default.

Table B-27 Expression

Switch name	Switch type	Data type	Description
FieldName	Mandatory	String	The name of the field.

Table B-27 Expression *(continued)*

Switch name	Switch type	Data type	Description
ExpressionOperator	Mandatory	String	The ExpressionOperator contains the following members: ■ EqualTo ■ Contains ■ StartsWith ■ EndsWith
FieldValue	Mandatory	String	The value of the field.
FieldType	Optional	String	The data type by which you want to compare the fields. The FieldType contains the following members: ■ String ■ DateTime ■ Boolean ■ Guid **Note:** If FieldType is not provided, then String type will be used by default.

The Expression of the Filter contains the following information:

Table B-28 Expression

Switch name	Switch type	Data type	Description
FieldName	Mandatory	String	The name of the field.

Table B-28 Expression *(continued)*

Switch name	Switch type	Data type	Description
ExpressionOperator	Mandatory	String	The ExpressionOperator contains the following members: ■ EqualTo ■ Contains ■ StartsWith ■ EndsWith
FieldValue	Mandatory	String	The value of the field.
FieldType	Optional	String	The data type by which you want to compare the fields. The FieldType contains the following members: ■ String ■ DateTime ■ Boolean ■ Guid **Note:** If FieldType is not provided, then String type will be used by default.

Filter can have more than one expression.

You have to apply the following rules while using the filter expression:

- The expression should be inside " " double quotes.
- The expression consists of FieldName, ExpressionOperator, FieldValue ,and FieldType. Each of these parts is separated by , comma.
- The comma can be escaped using \ backslash.
- The expression can be inside ( ) parentheses.

To combine multiple filter expressions, you can use the following logical operators:

Table B-29 Logical Operators

Operator name	Description	Usage
-and	Logical AND is used to add expressions to the search.	For example, -Filter {(("objectGUID, equalto, c8f0de1a-a278-4c29-86a1 -47d5ab91cb16, Guid") -and (("displayname, startswith, domainname\machinename"))}
-or	Logical OR is used to provide options to the search.	For example, -Filter {(("objectGUID, equalto, c8f0de1a-a278-4c29-86a1 -47d5ab91cb16, Guid") -or (("displayname, startswith, domainname\machinename"))}
!	Logical ! (bang) is used to negate the ExpressionOperator.	For example, -Filter {(("objectGUID, equalto, c8f0de1a-a278-4c29-86a1 -47d5ab91cb16, Guid") -and!("displayname, endswith, admin"))}

Inputs

You cannot pipe objects to the cmdlet.

Outputs

The Search-Assets cmdlet returns the list of assets as an output.

Each Asset object contains the following information:

Table B-30 Asset object

Switch name	Data type	Description
Id	Guid	The unique identifier of the asset in the system.
Name	String	The display name of the asset.
Type	AssetType	The asset type.

Table B-30 Asset object *(continued)*

Switch name	Data type	Description
Path	String	The full path of the asset.
Attributes	Attributes	The attributes of the object.

Notes

- You can set AppServerNameAndPort variable only once and reuse it till the session is closed.
- You can set BindingType variable only once and reuse it till the session is closed.
- If the DisplayName attribute of the returned Asset object is found to be null, then you must use the DisplayName attribute from the Attributes collection of the returned Asset object to get the asset display name.
- The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example 1

```
C:\PS> Search-Assets -AssetType "Windows Machine" -Filter
{("displayname,startswith,Name")}
-NumberOfObjectsToRetrieve 15
```

Description: The Script block is written in filter to get the desired assets using the Search-Assets cmdlet.

Example 2

```
C:\PS> Search-AssetGroups -ExcludePredefineObjects $TRUE

Output:
Id            : fd5db668-8957-4da5-96b2-a02a2a46161e
Name          : test
Description   : test
Type          : Static
ContainerPath : Asset System
Owner         : DOMAINNAME\Administrator
ModifiedBy    : DOMAINNAME \Administrator
```

```
ExtensionData : System.Runtime.Serialization.ExtensionDataObject

C:\PS> Search-Assets -Filter {("displayname,startswith,Name")}
-NumberOfObjectsToRetrieve 10|Add-AssetsToAssetGroup
-Id fd5db668-8957-4da5-96b2-a02a2a46161e
```

Description: The ID of the AssetGroup is retrieved using the Add-AssetsToAssetGroup cmdlet. The Script block is written in filter to get the desired assets using the Search-Assets cmdlet. These assets are piped to Add-AssetsToAssetGroup and added to the given asset group using its ID.

Related Links

See Add-AssetsToAssetGroup on page 1153.

See Create-DataCollectionEvaluationJob on page 1247.

See Create-DataCollectionJob on page 1230.

Initialize-ReconciliationRule

`Initialize-ReconciliationRule` – Creates the ReconciliationRule object.

Synopsis

The Initialize-ReconciliationRule helper class returns a ReconciliationRule object.

Syntax

```
Initialize-ReconciliationRule -Name <String>
-Path <String> [<CommonParameters>]
```

Authorization requirements

- The Initialize-ReconciliationRule helper class does not require any authorization. Any CCS user can initialize the ReconciliationRule object.

Description

The Initialize-ReconciliationRule helper class returns a ReconciliationRule object.

Parameters

The following table describes the parameters that the Initialize-ReconciliationRule helper class requires:

Table B-31 Initialize-ReconciliationRule - parameters

Switch Name	Switch Type	Data Type	Support piping input? (Yes/No)	Description
Name	Mandatory	String	No	The name of the rule.
Path	Mandatory	String	No	The location of the rule.

Table B-31 Initialize-ReconciliationRule - parameters *(continued)*

Switch Name	Switch Type	Data Type	Support piping input? (Yes/No)	Description
PipingEnabled	Optional	Boolean	No	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

Inputs

You cannot pipe objects to the helper class.

Outputs

The Initialize-ReconciliationRule helper class initializes and returns the Reconciliation Rule object as an output.

The Reconciliation Rule object contains the following information:

Table B-32 Reconciliation Rule object

Switch name	Data type	Description
Name	String	The name of the rule.
Path	String	The location of the rule.

Notes

You can set AppServerNameAndPort common variable only once and reuse it till the session is closed.

You can set BindingType common variable only once and reuse it till the session is closed.

The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example 1

```
C:/PS> $ReconcialiationRules = @()
C:/PS> $ReconcialiationRule = Initialize-ReconciliationRule
-Name "Add asset to the Asset System" -Path
"Reconciliation Rules\Pre-defined Rules"
C:/PS> $ReconcialiationRules += $ReconcialiationRule

Output:
  Name                                       Path

 Add asset to the Asset System  Reconciliation Rules\
                                Pre-defined Rules
```

Description: Returns Reconciliation Rules which can be given as input to Create-AssetImportJob.

Example 2

```
C:/PS> $ReconcialiationRules = @()
C:/PS> $ReconcialiationRule = Initialize-ReconciliationRule
-Name "Add asset to the Asset System" -Path "Reconciliation
Rules\Pre-defined Rules"
C:/PS> $ReconcialiationRules += $ReconcialiationRule
C:/PS>  Create-AssetImportJob  -Name $jobName -Description
"Test Job Description" -DataCollector $dataCollector
-AssetType "symc-csm-AssetSystem-Asset-Wnt-Machine"
-Assets $Assets -Sites $Sites -ReconciliationRules
$ReconcialiationRules -Schedule $ScheduleData
-SuccessNotification $SuccessNotification -FailureNotification
$FailureNotification
```

Description: It shows how the $ReconcialiationRules created by Initialize-ReconciliationRule can be consumed by Create-AssetImportJob.

Related Links

- See Create-AssetImportJob on page 1143.

Search-Standards

`Search-Standards` – Finds a standard or standards based on the specified search criteria.

Synopsis

The Search-Standard cmdlet finds a standard or a list of standards that matches the specified filter.

Syntax

```
Search-Standards -AppServerNameAndPort <String>
[-BindingType <String>] [-ContainerPath <String>]
[-Filter <Scriptblock>] [-SearchSubree [<Boolean>]]
[-ExcludePredefineObjects [<Boolean>]]
[-NumberOfObjectsToRetrieve <Int32>] [-PipingEnabled
[<Boolean>]] [<CommonParameters>]
```

Authorization requirements

You must have the following CCS tasks to use the cmdlet:

- View Standards

You must have the permissions on the following folders to use the cmdlet:

- Standards

Description

The Search- Standard cmdlet finds a specific standard or a list of standards that matches the specified filter.

All parameters or switches are optional for this cmdlet except AppServerNameAndPort. If you do not specify any input parameters, the cmdlet returns all the standards.

Parameters

The following table describes the parameters that the cmdlet requires:

Table B-33 Search-Standards - parameters

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
AppServerNameAndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServerNameAndPort ="< AppServer Name/IP> : <Port Number Corresponding To Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-33 Search-Standards - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$Binding Type="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.
ContainerPath	Optional	ContainerPath	No	The path of the folder that contains the standard. The default value of the parameter is Null.

Table B-33 Search-Standards - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
Filter	Optional	Scriptblock	No	The Scriptblock should contain one or more Expressions. You have to use { } brackets for the filter. **Note:** If you do not specify any value in the Filter parameter, the cmdlet returns all the standards.
SearchSubTree	Optional	Boolean	No	The default value for the parameter is True. True or False value that states if the sub-tree under the folder has to be searched for the standard or not.

Table B-33 Search-Standards - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
Exclude PredefineObjects	Optional	Boolean	No	The default value for the parameter is False. True or False value that states if the predefined objects should be excluded from the search criteria.
NumberOfObjects ToRetrieve	Optional	Int	No	The maximum number of standards that the cmdlet must return. The default value of the parameter is Null.
PipingEnabled	Optional	Boolean	No	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

The Expression of the Filter contains the following information:

Table B-34 Expression

Switch name	Switch type	Data type	Description
FieldName	Mandatory	String	The name of the field.
ExpressionOperator	Mandatory	String	The ExpressionOperator contains the following members: ■ EqualTo ■ Contains ■ StartsWith ■ EndsWith
FieldValue	Mandatory	String	The value of the field.
FieldType	Optional	String	The data type by which you want to compare the fields. The FieldType contains the following members: ■ String ■ DateTime ■ Boolean ■ Guid **Note:** If FieldType is not provided, then String type will be used by default.

Filter can have more than one expression.

You have to apply the following rules while using the filter expression:

- The expression should be inside " " double quotes.
- The expression consists of FieldName, ExpressionOperator, FieldValue ,and FieldType. Each of these parts is separated by , comma.
- The comma can be escaped using \ backslash.

- The expression can be inside ( ) parentheses.

To combine multiple filter expressions, you can use the following logical operators:

Table B-35 Logical Operators

Operator name	Description	Usage
-and	Logical AND is used to add expressions to the search.	For example, -Filter {(("objectGUID, equalto, c8f0de1a-a278-4c29-86a1 -47d5ab91cb16, Guid") -and (("displayname, startswith, domainname\machinename"))}
-or	Logical OR is used to provide options to the search.	For example, -Filter {(("objectGUID, equalto, c8f0de1a-a278-4c29-86a1 -47d5ab91cb16, Guid") -or (("displayname, startswith, domainname\machinename"))}
!	Logical ! (bang) is used to negate the ExpressionOperator.	For example, -Filter {(("objectGUID, equalto, c8f0de1a-a278-4c29-86a1 -47d5ab91cb16, Guid") -and!("displayname, endswith, admin"))}

Inputs

You cannot pipe objects to the cmdlet.

Outputs

The Search-Standards cmdlet returns the list of standards as an output.

The Standard object contains the following information:

Table B-36 Standard object

Switch name	Data type	Description
Id	Guid	The unique identifier of the standard.
Name	String	The DisplayName of the standard.

Table B-36 Standard object *(continued)*

Switch name	Data type	Description
Version	String	The version of the standard.

Notes

- You can set AppServerNameAndPort common variable only once and reuse it till the session is closed.
- You can set BindingType common variable only once and reuse it till the session is closed.
- The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example 1

```
Search-standards  -Filter {("displayname,equalto,CIS*") -and
("displayname,contains,Security Benchmark")}
-SearchsubTree $True
```

Description: The Script block is written in filter to get the desired standards using the Search-Standard cmdlet.

Example 2

```
Search-standards  -Filter {("displayname,equalto,CIS*") -and
("displayname,contains,Security Benchmark")}
-SearchsubTree $True -ExcludePredefinedObjects $TRUE
```

Description: The Script block is written in filter to get the desired standards using the Search-Standard cmdlet.

Related Links

See Create-DataCollectionJob on page 1230.

See Create-DataCollectionEvaluationJob on page 1247.

Search-Checks

`Search-Checks` – Finds a check that matches the specified criteria.

Synopsis

The Search-Checks cmdlet retrieves the checks from the specified section.

Syntax

```
Search-Checks -AppServerNameAndPort <String>
[-BindingType <String>] [-ContainerPath <String>]
[-Filter <Scriptblock>]
[-SearchSubTree[<Boolean>]] [-ExcludePredefineObjects
[<Boolean>]] [-NumberOfObjectsToRetrieve <Int32>]
[-PipingEnabled [<Boolean>]] [<CommonParameters>]
```

Authorization requirements

You must have the following CCS tasks to use the cmdlet:

- View Standards

You must have the following permissions on folders to use the cmdlet:

- Standards

Description

The Search-Checks cmdlet returns the checks from the specified section.

Parameters

The following table describes the input parameters that the Search-Checks cmdlet requires:

Table B-37 Search-Checks - parameters

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
AppServerNameAndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServerNameAndPort ="< AppServer Name/IP> : <Port Number Corresponding To Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-37 Search-Checks - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$Binding Type="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.
ContainerPath	Optional	String	No	The full path of the folder that contains the object.

Table B-37 Search-Checks - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
Filter	Optional	Scriptblock	No	The Scriptblock should contain one or more Expressions. You have to use { } brackets for the filter. **Note:** If you do not specify any value in the Filter parameter, the cmdlet returns all the checks.
SearchSubtree	Optional	Boolean	No	True or False value that states if the sub-tree under the folder has to be searched for the check or not. The default value for this parameter is True.

Table B-37 Search-Checks - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
Exclude PredefinedObjects	Optional	Boolean	No	True or False value that states if the predefined objects should be excluded from the search criteria. The default value for this parameter is False.
NumberOf ObjectsToRetrieve	Optional	Int	No	The maximum number of checks that must be returned. The default value of this parameter is 0.
PipingEnabled	Optional	Boolean	Yes	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

The Expression of the Filter contains the following information:

Table B-38 Expression

Switch name	Switch type	Data type	Description
FieldName	Mandatory	String	The name of the field.
ExpressionOperator	Mandatory	String	The ExpressionOperator contains the following members: ■ EqualTo ■ Contains ■ StartsWith ■ EndsWith
FieldValue	Mandatory	String	The value of the field.
FieldType	Optional	String	The data type by which you want to compare the fields. The FieldType contains the following members: ■ String ■ DateTime ■ Boolean ■ Guid **Note:** If FieldType is not provided, then String type will be used by default.

Filter can have more than one expression.

You have to apply the following rules while using the filter expression:

- The expression should be inside " " double quotes.
- The expression consists of FieldName, ExpressionOperator, FieldValue ,and FieldType. Each of these parts is separated by , comma.
- The comma can be escaped using \ backslash.

- The expression can be inside ( ) parentheses.

To combine multiple filter expressions, you can use the following logical operators:

Table B-39 Logical Operators

Operator name	Description	Usage
-and	Logical AND is used to add expressions to the search.	For example, -Filter {(("objectGUID, equalto, c8f0de1a-a278-4c29-86a1 -47d5ab91cb16, Guid") -and (("displayname, startswith, domainname\machinename"))}
-or	Logical OR is used to provide options to the search.	For example, -Filter {(("objectGUID, equalto, c8f0de1a-a278-4c29-86a1 -47d5ab91cb16, Guid") -or (("displayname, startswith, domainname\machinename"))}
!	Logical ! (bang) is used to negate the ExpressionOperator.	For example, -Filter {(("objectGUID, equalto, c8f0de1a-a278-4c29-86a1 -47d5ab91cb16, Guid") -and!("displayname, endswith, admin"))}

Inputs

You cannot pipe objects to the cmdlet

Outputs

The Search-Checks cmdlet returns the Check object. It returns the list of checks that match the search criteria.

The Check object contains the following information:

Table B-40 Search-Checks- output

Switch name	Data type	Description
Id	Guid	The unique ID of the check.
Name	String	The display name of the standard.

Table B-40 Search-Checks- output *(continued)*

Switch name	Data type	Description
Version	String	The version of the check.
StandardID	Guid	The ID of the standard to which the check belongs.

Notes

- You can set AppServerNameAndPort variable only once and reuse it till the session is closed.
- You can set BindingType variable only once and reuse it till the session is closed.
- The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example

```
PS C:\> Search-Checks  -Filter {("displayname,startswith,data*")
-or ("displayname,equalto,*Security*")}
 -SearchsubTree $True -Numberofobjectstoretrieve 5 -ContainerPath
"\Standards\Predefined"

Output:
Version       : 1.0.0
StandardID    : ec1b6f2c-0f3f-468a-ab21-9670946f589a
Id            : e25f77a0-f439-409f-8cfe-0c243b8bcefa
Name          : Database Audit Specification enabled to audit
required database level Audit Action groups
ExtensionData : System.Runtime.Serialization.ExtensionDataObject

Version       : 1.0.0
StandardID    : 38c99bcb-739e-4dde-8ec1-e3cdd4dbd0a5
Id            : 7a5281fb-0331-4dcc-810c-8ad87487a2ab
Name          : Database Audit Specification enabled to audit
required database level Audit Action groups
ExtensionData : System.Runtime.Serialization.ExtensionDataObject

Version       : 1.0.0
```

```
StandardID    : 38c99bcb-739e-4dde-8ec1-e3cdd4dbd0a5
Id            : bc5bfbd3-b72d-4a68-89c5-4c97dc48fac3
Name          : Database Audit Specification enabled to audit
required database level Audit Action groups
ExtensionData : System.Runtime.Serialization.ExtensionDataObject

Version       : 1.0.0
StandardID    : 38c99bcb-739e-4dde-8ec1-e3cdd4dbd0a5
Id            : 7406b115-9a83-41c0-9f59-8667341aa51a
Name          : Database Audit Specification enabled to audit

required database level Audit Action groups
ExtensionData : System.Runtime.Serialization.ExtensionDataObject

Version       : 1.0.0
StandardID    : 38c99bcb-739e-4dde-8ec1-e3cdd4dbd0a5
Id            : e1182780-edeb-4bc6-bbc2-6e894ec00c61
Name          : Database Audit Specification enabled to audit
required database level Audit Action groups
ExtensionData : System.Runtime.Serialization.ExtensionDataObject
```

Description: This example shows how written proper script-blocks in filter can be used to retrieve desired checks from given container location.

Related Links

See Create-DataCollectionEvaluationJob on page 1247.

See Create-DataCollectionJob on page 1230.

See Create-EvaluationJob on page 1239.

Get-SectionsFromStandard

`Get-SectionsFromStandard` – Finds sections in the specified standard.

Synopsis

The Get-SectionsFromStandard cmdlet gets the sections from the specified standard.

Syntax

```
Get-SectionsFromStandard -AppServerNameAndPort <String>
[-BindingType <String>] [-Id <Guid>] [-Filter <String[]>]
 [-SearchSubTree [<Boolean>]] [-ExcludePredefineObjects
[<Boolean>]] [-NumberOfObjectsToRetrieve <Int32>]
[-PipingEnabled [<Boolean>]] [<CommonParameters>]
```

Authorization requirements

You must have the following CCS tasks to use this cmdlet:

- View Standards

Description

The Get-SectionsFromStandard cmdlet returns the sections from the specified standard.

Parameters

The following table describes the input parameters that the Get-SectionsFromStandard cmdlet requires:

Table B-41 Get-SectionsFromStandard - parameters

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
AppServerNameAndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServerNameAndPort="<AppServerName/IP> :<Port Number Corresponding To Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-41 Get-SectionsFromStandard - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$BindingType="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.
Id	Mandatory	Guid	Yes	The unique identifier of the Standard.

Table B-41 Get-SectionsFromStandard - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
Filter	Optional	Scriptblock	No	The Scriptblock should contain one or more Expressions. You have to use { } brackets for the filter. **Note:** If you do not specify any value in the Filter parameter, the cmdlet returns all the sections.
SearchSubtree	Optional	Boolean	No	True or False value that states if the sub-tree under the folder has to be searched for the check or not. The default value for this parameter is True.

Table B-41 Get-SectionsFromStandard - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
Exclude PredefinedObjects	Optional	Boolean	No	True or False value that states if the predefined objects should be excluded from the search criteria. The default value for this parameter is False.
NumberOf ObjectsTo Retrieve	Optionalretrieve	Int	No	The maximum number of checks that must be returned.
PipingEnabled	Optional	Boolean	Yes	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

The Expression of the Filter contains the following information:

Table B-42 Expression

Switch name	Switch type	Data type	Description
FieldName	Mandatory	String	The name of the field.

Table B-42 Expression *(continued)*

Switch name	Switch type	Data type	Description
ExpressionOperator	Mandatory	String	The ExpressionOperator contains the following members: ■ EqualTo ■ Contains ■ StartsWith ■ EndsWith
FieldValue	Mandatory	String	The value of the field.
FieldType	Optional	String	The data type by which you want to compare the fields. The FieldType contains the following members: ■ String ■ DateTime ■ Boolean ■ Guid **Note:** If FieldType is not provided, then String type will be used by default.

Filter can have more than one expression.

You have to apply the following rules while using the filter expression:

- The expression should be inside " " double quotes.
- The expression consists of FieldName, ExpressionOperator, FieldValue ,and FieldType. Each of these parts is separated by , comma.
- The comma can be escaped using \ backslash.
- The expression can be inside ( ) parentheses.

To combine multiple filter expressions, you can use the following logical operators:

Table B-43 Logical Operators

Operator name	Description	Usage
-and	Logical AND is used to add expressions to the search.	For example, -Filter {(("objectGUID, equalto, c8f0de1a-a278-4c29-86a1 -47d5ab91cb16, Guid") -and (("displayname, startswith, domainname\machinename"))}
-or	Logical OR is used to provide options to the search.	For example, -Filter {(("objectGUID, equalto, c8f0de1a-a278-4c29-86a1 -47d5ab91cb16, Guid") -or (("displayname, startswith, domainname\machinename"))}
!	Logical ! (bang) is used to negate the ExpressionOperator.	For example, -Filter {(("objectGUID, equalto, c8f0de1a-a278-4c29-86a1 -47d5ab91cb16, Guid") -and!("displayname, endswith, admin"))}

Inputs

You can pipe output of Search-Standards to Get-SectionsFromStandard.

Outputs

The Get-SectionsFromStandard cmdlet returns the Section object. It returns the list of sections that match the search criteria.

The Section object contains the following information:

Table B-44 Get-SectionsFromStandard- output

Switch name	Data type	Description
Id	Guid	The unique ID of the section.
Name	String	The display name of the section
Version	String	The version of the section.

Table B-44 Get-SectionsFromStandard- output *(continued)*

Switch name	Data type	Description
StandardID	Guid	The ID of the standard to which the section belongs.

Notes

- You can set AppServerNameAndPort variable only once and reuse it till the session is closed.
- You can set BindingType variable only once and reuse it till the session is closed.
- The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Examples

```
C:\PS> Search-Standards -Filter{("displayname,startswith,PCI DSS v1.2
 - CIS Windows Server 2003 Legacy)}| Get- SectionsFromStandard
```

Description: You can search the desired standard using the Search-Standards cmdlet and piping its output to Get-SectionsFromStandard.

Example 2

```
C:\PS> Get-SectionsFromStandard -Id
dbcabf6b-af5a-4111-beaa-da1e5c44e8fd
```

Description: You can use the Id of the standard as an input to Get-SectionsFromStandard.

Related Links

- See Search-Standards on page 1205.
- See Get-SectionsFromSection on page 1268.

Create-DataCollectionJob

`Create-DataCollectionJob` – Creates the data collection job.

Synopsis

The Create-DataCollectionJob cmdlet creates a data collection job and returns the unique identifier of the newly created data collection job.

Syntax

```
Create-DataCollectionJob -AppServerNameAndPort <String>
[-BindingType <String>]
-JobDetails <JobDetails>
-Assets <Asset[]> -Standards <Standard[]> [-Schedule
<IncrementalScheduleData>]
[-SuccessNotification <NotificationData>]
[-FailureNotification <NotificationData>] [-PipingEnabled
[<Boolean>]] [<CommonParameters>]
```

Authorization requirements

You must have the following CCS tasks to use the cmdlet:

- Manage Jobs
- Collect Data
- View Assets
- View Standards

You must have the permission on the following folders to use the cmdlet:

- Asset System
- Standards

Description

The Create-DataCollectionJob cmdlet creates a data collection job based on the parameters.

Parameters

The following table describes the parameters that the cmdlet requires:

Table B-45 Create-DataCollectionJob - parameters

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
AppServerNameAndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServerNameAndPort ="<AppServerName/IP> :<Port Number Corresponding To Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-45 Create-DataCollectionJob - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$Binding Type="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-45 Create-DataCollectionJob - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
JobDetails	Mandatory	JobDetails	Yes	It contains basic details about collection job such as JobName, description. You get the value for this parameter from the Output of the helper class `Initialize-Collection JobDetails`.
Assets	Mandatory	Assets	Yes	Get the value for this parameter from the Output of the `Search-Assets` cmdlet .
Standards	Mandatory	Standards GUID	Yes	Get the value of this parameter from the Output of the `Search-Standards` cmdlet. The `Search-Standard` cmdlet returns the standards GUID as an output.

Table B-45 Create-DataCollectionJob - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
Schedule	Optional	Schedule	Yes	Get the value for this parameter from the Output of the helper class `Initialize-IncrementalSchedule`.
Success Notification	Optional	NotificationData	Yes	Get the value of this parameter from the helper class `Initialize-EmailNotification`. **Note:** When you set the value as null or do not specify a value for the Subject and the Body fields in NotificationData data contract, the default values are set automatically. The default values are the ones that appear in the CCS Console when you create a new Data Collection or Evaluation job.

Table B-45 Create-DataCollectionJob - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
Failure Notification	Optional	NotificationData	Yes	Get the value of this parameter from the helper class `Initialize-EmailNotification`. **Note:** When you set the value as null or do not specify a value for the Subject and the Body fields in NotificationData data contract, the default values are set automatically. The default values are the ones that appear in the CCS Console when you create a new Data Collection or Evaluation job.
PipingEnabled	Optional	Boolean	Yes	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

Inputs

You can pipe the output of Search-Assets or Search-Standards to Create-DataCollectionJob.

Outputs

The Create-DataCollectionJob cmdlet returns the Guid of the newly created data collection job as an output.

Notes

You can set AppServerNameAndPort variable only once and reuse it till the session is closed.

You can set BindingType variable only once and reuse it till the session is closed.

The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example 1

```
C:\PS>$AppServerNameAndPort="localhost:1431" # <ServerName:Port>
C:\PS>$jobName = "DataCollectionJob1"
C:\PS>$JobDetails = Initialize-CollectionJobDetails -Name $jobName
-Description "Test Job Description" -DataCollectionCriteria 1

C:\PS>$Standards=Search-standards  -Filter {("displayname,equalto,CIS*")
-and ("displayname,contains,Security Benchmark")}
-SearchsubTree $True

C:\PS>$IncrementalScheduleData = Initialize-IncrementalSchedule
-SubScheduleRepeatDays 0 -SubScheduleRepeatPeriodDays 0
-RepeatDays 7 -RunEveryNDays $FALSE -RunNow $TRUE -RunOnce $True
-RunPeriodically $TRUE -StartDate
((get-date).AddSeconds(5) -f "yyyy-MM-dd HH:mm:ss")

C:\PS>$SuccessNotification = Initialize-EmailNotification -FromAddress
"username@domain.com"  -ToAddress "username@domain.com"
-Subject "Success Notification Message" -Body "Test Body"

C:\PS>$FailureNotification = Initialize-EmailNotification -FromAddress
"username@domain.com"
```

```
-ToAddress "username@domain.com"  -Subject "Failure Notification Message"
-Body "Test Body"
C:\PS>Search-Assets -Filter {("displayname,startswith,Win")}
-SearchsubTree
$True -AssetType
"symc-csm-AssetSystem-Asset-Wnt-Machine" -PipingEnabled $True |
Create-DataCollectionJob -JobDetails $JobDetails
-Schedule $IncrementalScheduleData -Standards $Standards
-SuccessNotification $SuccessNotification
-FailureNotification  $FailureNotification
```

Description: All the input details for creation of the data-collection job are created such as Job-Name, Job-Details, Standards Scope, Suceess Notification, Failure Notification, and Incremental Schedule that are assigned to variables. These variables are passed on as the input while creating the job. The Assets to be used as scope are piped as the input to the Create-DataCollectionJob cmdlet.

Example 2

```
C:\PS>$AppServerNameAndPort="localhost:1431" # <ServerName:Port>
C:\PS>$jobName = "DataCollectionJob1"
C:\PS>$Assets  = Search-Assets -Filter {("displayname,startswith,Win")}
-SearchsubTree $True
-AssetType "symc-csm-AssetSystem-Asset-Wnt-Machine"
C:\PS>$JobDetails = Initialize-CollectionJobDetails -Name $jobName
-Description
"Test Job Description"
-DataCollectionCriteria 1
C:\PS>$IncrementalScheduleData = Initialize-IncrementalSchedule
-SubScheduleRepeatDays 0
-SubScheduleRepeatPeriodDays 0 -RepeatDays 7 -RunEveryNDays $FALSE
-RunNow $TRUE -RunOnce $True
-RunPeriodically $TRUE -StartDate ((get-date).AddSeconds(5) –f
"yyyy-MM-dd HH:mm:ss")
C:\PS>$SuccessNotification = Initialize-EmailNotification -FromAddress
"username@domain.com"
-ToAddress "username@domain.com" -Subject "Success Notification Message" -B
"Test Body"
C:\PS>$FailureNotification = Initialize-EmailNotification -FromAddress
"username@domain.com"
-ToAddress "username@domain.com"  -Subject "Failure Notification Message"
-Body "Test Body"
C:\PS>Search-standards  -Filter {("displayname,equalto,CIS*") -and
("displayname,contains,Security Benchmark")}
-SearchsubTree $True -PipingEnabled $True | Create-DataCollectionJob
-JobDetails $JobDetails -Assets $Assets
-Schedule $IncrementalScheduleData -SuccessNotification $SuccessNotification
-FailureNotification  $FailureNotification
```

Description: All the input details for creation of the data-collection job are created such as Job-Name, Job-Details, Standards Scope, Success Notification, Failure Notification, and Incremental Schedule that are assigned to variables. These variables are passed on as the input while creating the job. The Standards to be used as scope are piped as the input to the Create-DataCollectionJob cmdlet.

Related Links

- See Initialize-CollectionJobDetails on page 1300.
- See Initialize-EmailNotification on page 1459.
- See Initialize-IncrementalSchedule on page 1447.
- See Search-Assets on page 1190.
- See Search-Standards on page 1205.

Create-EvaluationJob

`Create-EvaluationJob` – Returns the Guid of the evaluation job that is newly created.

Synopsis

The Create-EvaluationJob cmdlet returns the unique identifier of the evaluation job that is created newly.

Syntax

```
Create-EvaluationJob -AppServerNameAndPort <String>
[-BindingType <String>] -JobDetails <JobDetails> -Assets <Asset[]>
-Standards <Standard[]> [-Schedule <IncrementalScheduleData>]
[-SuccessNotification <NotificationData>] [-FailureNotification
<NotificationData>] [-PipingEnabled [<Boolean>]] [<CommonParameters>]
```

Authorization requirements

You must have the following CCS tasks to use the cmdlet:

- Manage Jobs
- Collect Data
- View Assets
- View Standards

You must have the permission on the following folders to use the cmdlet:

- Asset System
- Standards

Description

Creates a new Evaluation Job based on the given parameters.

Parameters

The following table describes the parameters that the cmdlet requires:

Table B-46 Create-EvaluationJob - parameters

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
AppServerName AndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServer NameAndPort="< AppServer Name/IP> : <Port Number Corresponding To Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-46 Create-EvaluationJob - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$Binding Type="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.
JobDetails	Mandatory	JobDetails	Yes	Get the value for this parameter from the Output of the `Initialize-Evaluation JobDetails` cmdlet.

Table B-46 Create-EvaluationJob - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
Assets	Mandatory	Asset	Yes	Get the value for this parameter from the Output of the `Search-Assets` cmdlet. The AssetResolutionInfo object contains the Asset ID and the Asset Type.
Standards	Mandatory	Standard	Yes	Get the value of this parameter from the Output of the `Search-Standards` cmdlet. The Search-Standards cmdlet returns the Standard object as an output.
Schedule	Optional	Schedule	Yes	Get the value for this parameter from the Output of the `Initialize-IncrementalSchedule` cmdlet.

Table B-46 Create-EvaluationJob - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
Success Notification	Optional	Success Notification	Yes	Get the value of this parameter from the `Initialize -EmailNotification` cmdlet **Note:** The parameter is mandatory if the value of the ShouldSend Notification in the EvaluationJobDetails object is set to True.
Failure Notification	Optional	Failure Notification	Yes	Get the value of this parameter from the `Initialize -EmailNotification` cmdlet **Note:** The parameter is mandatory if the value of the ShouldSend Notification in the EvaluationJobDetails object is set to True.
PipingEnabled	Optional	Boolean	Yes	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

The Standard object contains the following information:

Table B-47 Standard object

Switch name	Data type	Description
Id	Guid	The unique identifier of the standard.
Name	String	The Display Name of the standard.
Version	String	The version of the standard.

Inputs

You can pipe the output of Search-Assets or Search-Standards to Create-EvaluationJob.

Outputs

The Create-EvaluationJob cmdlet returns the Guid of the newly created evaluation job.

Notes

You can set AppServerNameAndPort variable only once and reuse it till the session is closed.

You can set BindingType variable only once and reuse it till the session is closed.

The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example 1

```
C:\PS>$AppServerNameAndPort="localhost:1431" #  <ServerName:Port>

C:\PS>$jobName = "EvaluationJob"

C:\PS>$JobDetails = Initialize-EvaluationJobDetails -Name $jobName
-Description "Test Job Description"

C:\PS>$Assets = Search-Assets -Filter {("displayname,startswith,Win")}
-SearchsubTree $True -AssetType "symc-csm-AssetSystem-Asset-Wnt-Machine"
-Numberofobjectstoretrieve 5
```

```
C:\PS>$Standards=Search-standards  -Filter {("displayname,equalto,CIS*")
-and ("displayname,contains,Security Benchmark")} -SearchsubTree $True
-Numberofobjectstoretrieve 2

C:\PS>$ScheduleData = Initialize-Schedule -RepeatDays 7 -RunEveryNDays
$FALSE -RunNow $TRUE -RunOnce $True -RunPeriodically $TRUE -StartDate
((get-date).AddSeconds(60) -f "yyyy-MM-dd HH:mm:ss")

C:\PS>$SuccessNotification = Initialize-EmailNotification -FromAddress
"username@domain.com" -ToAddress "username@domain.com" -Subject "Success
Notification Message" -Body "Test Body"

C:\PS>$FailureNotification = Initialize-EmailNotification -FromAddress
"username@domain.com" -ToAddress "username@domain.com"  -Subject
"Failure Notification Message" -Body "Test Body"

C:\PS>Create-EvaluationJob -JobDetails $JobDetails -Assets $Assets
-Schedule $ScheduleData -Standards $Standards -SuccessNotification
$SuccessNotification -FailureNotification  $FailureNotification
```

Description: All the input details for creation of a evaluation job are created such as Job-Name, Job-Details, Assets Scope, Standards Scope, Suceess Notification, Failure Notification, and Schedule that are assigned to variables. These variables are passed on as the input while creating the job.

Example 2

```
C:\PS>$AppServerNameAndPort="localhost:1431" # <ServerName:Port>

C:\PS>$jobName = "EvaluationJob"

C:\PS>$JobDetails = Initialize-EvaluationJobDetails -Name $jobName
-Description "Test Job Description"

C:\PS>$Assets = Search-Assets -Filter {("displayname,startswith,Win")}

 -SearchsubTree $True -AssetType "symc-csm-AssetSystem-Asset-Wnt-Machine"
-Numberofobjectstoretrieve 5

C:\PS>$ScheduleData = Initialize-Schedule -RepeatDays 7 -RunEveryNDays
$FALSE -RunNow $TRUE -RunOnce $True -RunPeriodically $TRUE -StartDate
((get-date).AddSeconds(60) -f "yyyy-MM-dd HH:mm:ss")
```

```
C:\PS>$SuccessNotification = Initialize-EmailNotification -FromAddress
"username@domain.com" -ToAddress "username@domain.com" -Subject
"Success Notification Message" -Body "Test Body"

C:\PS>$FailureNotification = Initialize-EmailNotification -FromAddress
"username@domain.com" -ToAddress "username@domain.com"  -Subject
"Failure Notification Message" -Body "Test Body"

C:\PS> Search-standards  -Filter {("displayname,equalto,CIS*") -and
("displayname,contains,Security Benchmark")} -SearchsubTree $True
-Numberofobjectstoretrieve 2 -PipingEnabled $TRUE |  Create-EvaluationJob
-JobDetails $JobDetails -Assets $Assets -Schedule $ScheduleData
-SuccessNotification $SuccessNotification -FailureNotification
$FailureNotification
```

Description: All the input details for creation of a evaluation job are created such as Job-Name, Job-Details, Assets Scope, Standards Scope, Suceess Notification, Failure Notification, and Schedule that are assigned to variables. These variables are passed on as the input while creating the job. The standards to be used as scope are piped as the input to Create-Evaluation Job.

Related Links

See Initialize-Schedule on page 1453.

See Initialize-EmailNotification on page 1459.

See Search-Assets on page 1190.

See Search-Standards on page 1205.

Create-DataCollectionEvaluationJob

`Create-DataCollectionEvaluationJob` – Creates a new data collection evaluation job.

Synopsis

The Create-DataCollectionEvaluationJob cmdlet creates a new collection-evaluation job and returns the unique identifier of the newly created collection-evaluation job.

Syntax

```
Create-DataCollectionEvaluationJob -AppServerNameAndPort
<String> [-BindingType <String>] -JobDetails
<CollectionEvaluationJobDetails>
-Assets <Asset[]> -Standards <Standard[]> [-Schedule
<IncrementalScheduleData>] [-SuccessNotification <NotificationData>]
[-FailureNotification <NotificationData>] [-PipingEnabled
[<Boolean>]] [<CommonParameters>]
```

Authorization requirements

You must have the following CCS tasks to use the cmdlet:

- Manage Jobs
- Collect Data
- View Assets
- View Standards

You must have the permission on the following folders to use the cmdlet:

- Asset System
- Standards

Description

The Create-DataCollectionEvaluationJob cmdlet creates a new collection-evaluation job for given parameters.

Parameters

The following table describes the input parameters that the Create-DataCollectionEvaluationJob cmdlet requires:

Table B-48 Create-DataCollectionEvaluationJob - parameters

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
AppServerName AndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServer NameAndPort="< AppServer Name/IP> : <Port Number Corresponding To Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-48 Create-DataCollectionEvaluationJob - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$Binding Type="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.
JobDetails	Mandatory	JobDetails	Yes	Get the value for this parameter from the Output of the `Initialize -Collection Evaluation JobDetails` cmdlet.
Assets	Mandatory	List<Asset>	Yes	Get the value for this parameter from the Output of the `Search- Assets` cmdlet.

Table B-48 Create-DataCollectionEvaluationJob - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
Standards	Mandatory	Standard	Yes	Get the value for this parameter from the Output of the `Search-Standards` cmdlet.
Schedule	Optional	Schedule	Yes	Get the value for this parameter from the Output of the `Initialize-IncrementalSchedule` cmdlet.
Success Notification	Optional	Notification	Yes	Get the value for this parameter from the Output of the `Initialize-EmailNotification` cmdlet. **Note:** This parameter is mandatory if the value for the ShouldSend SuccessNotification field is set to True in the NotificationData object.

Table B-48 Create-DataCollectionEvaluationJob - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
Failure Notification	Optional	Notification	Yes	Get the value for this parameter from the Output of the `Initialize-Email Notification` cmdlet. **Note:** This parameter is mandatory if the value for the ShouldSend FailureNotification field is set to True in the Collection Evaluation JobDetails object.
PipingEnabled	Optional	Boolean	Yes	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

The CollectionEvaluationJobDetails object is required data type for one of the parameters for the Create-DataCollectionEvaluationJob cmdlet. You can get the CollectionEvaluationJobDetails object as an output of the `Initialize-CollectionEvaluationJobDetails` cmdlet.

The CollectionEvaluationJobDetails object contanis the following information:

Table B-49 CollectionEvaluationJobDetails object

Switch Name	Switch Type	Data Type	Description
JobName	Mandatory	String	The name of the Collection Evaluation job

Table B-49 CollectionEvaluationJobDetails object *(continued)*

Switch Name	Switch Type	Data Type	Description
JobDescription	Optional	String	The description of the Collection Evaluation job
DataCollection Criteria	Optional	Int	The default value for the parameter is 0. **Note:** The maximum value for Data Collection criteria is 100. If you specify value more than 100 then data collection criteria defaults to 100.
ShouldSend FailureNotification	Optional	Boolean	The default value of the parameter is False. True if you want to send the notification of the job failure False if you do not want to send the notification of the job failure
ShouldSend SuccessNotification	Optional	Boolean	The default value of the parameter is False. True if you want to send the notification of the job success False if you do not want to send the notification of the job success
EvaluationResult Viewers	Optional	Strings	The list of users who can view the evaluation result.

The Asset object is required data type for one of the parameters for the Create-DataCollectionEvaluationJob cmdlet. You can get the Asset object as an output of the `Search-Assets` cmdlet.

The Asset object contains the following information:

Table B-50 Asset object

Switch Name	Switch Type	Data Type	Description
Id	Mandatory	Guid	The unique identifier of the asset in the system.
Type	Optional	AssetType	The asset type.
DisplayName	Optional	String	The display name of the asset.
Path	Optional	String	The full path of the asset.
Attributes	Optional	Attributes	The attributes of the object.

The ScheduleData object is required data type for one of the parameters for the Create-DataCollectionEvaluationJob cmdlet. You can get the ScheduleData object as an output of the `Initialize-Schedule` cmdlet.

Table B-51 Schedule object

Switch Name	Switch Type	Data Type	Description
SubSchedule RepeatDays	Optional	Integer	The number of days after which the sub-schedule must be repeated.
SubSchedule Repeat PeriodDays	Optional	Integer	The end day for the sub-schedule to stop the job execution. The job stops running on this day.
RepeatDays	Optional	Integer	The number of days after which you want to repeat the job. The value for this field is considered only if you set True for RunEveryNDays.

Table B-51 Schedule object *(continued)*

Switch Name	Switch Type	Data Type	Description
RunEveryNDays	Optional	Boolean	True if you want to run the job at a specified interval that is provided in the RepeatDays field. False if you do not want to run the job at a specified interval.
RunNow	Optional	Boolean	The default value of this parameter is False. True if you want to run the job immediately at the StartDate. False if you do not want to run the job immediately at the start date.
RunOnce	Optional	Boolean	The default value of this parameter is False. True if you want to run the job only once on the StartDate. False if you do not want to run the job once on the StartDate.
RunPeriodically	Optional	Boolean	The default value of this parameter is False. True if you want to run the job periodically. If you set True for this field, you must set True for either of the following: ■ RunOnce ■ RunEveryNDays False if you do not want to run the job periodically.

Table B-51 Schedule object *(continued)*

Switch Name	Switch Type	Data Type	Description
StartDate	Optional	DateTime	The date when the job run must begin. If you set True for RunNow, thejob is run immediately at the start date. If you set True for RunPeriodically, one of the following options is possible: ■ You can set RunOnce. The job will be run only once on the start date, You can set RunEveryNDays. The job will be repeated after every <RepeatDays>.

The Standard object is a required data type for one of the parameters for the Create-CollectionEvaluationJob cmdlet. You can get the Standard object from the `Search-Standards` cmdlet.

The Standard object contains the following information:

Table B-52 Standard object

Switch Name	Switch Type	Data Type	Description
ID	Mandatory	Guid	The unique identifier of the standard.
DisplayName	Optional	String	The display name of the standard.
Version	Optional	String	The version of the standard.

The NotificationData object is a required data type for one of the parameters for the Create-CollectionEvaluationJob cmdlet. You can get the Notification object from the `Initialize-Notification` cmdlet.

Table B-53 Notification Object

Switch name	Switch Type	Data type	Description
ToEmailAddress	Optional	String	The email address to which the notification must be sent.
FromEmailAddress	Optional	String	The email address from which the notification must be sent.
Subject	Mandatory	String	The subject of the email notification.
Body	Mandatory	String	The detailed message.

Inputs

You can pipe output of Search-Assets and Search-Standards to Create-DataCollectionEvaluationJob.

Outputs

The Create-DataCollectionEvaluationJob cmdlet returns the Guid of the newly created data collection evaluation job as an output.

Notes

You can set AppServerNameAndPort variable only once and reuse it till the session is closed.

You can set BindingType variable only once and reuse it till the session is closed.

The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Examples

```
C:\PS>$AppServerNameAndPort="localhost:1431" # <ServerName:Port>
C:\PS>$jobName = "CollectionEvaluationJob"
C:\PS>$JobDetails = Initialize-CollectionEvaluationJobDetails
```

```
-Name $jobName -Description "Test Job Description"
-DataCollectionCriteria 1
C:\PS>$Assets = Search-Assets -Filter {("displayname,startswith,e2e")}
-SearchsubTree $True -AssetType "symc-csm-AssetSystem-Asset-Wnt-Machine"

-Numberofobjectstoretrieve 5
C:\PS>$Standards=Search-standards  -Filter {("displayname,equalto,CIS*")
-and ("displayname,contains,Security Benchmark")} -SearchsubTree $True
C:\PS>$ScheduleData = Initialize-IncrementalSchedule -RepeatDays 7
-RunEveryNDays $FALSE -RunNow $TRUE -RunOnce $True -RunPeriodically
$TRUE -StartDate "2010-10-10 1:20:20"
C:\PS>$SuccessNotification = Initialize-EmailNotification -FromAddress
"username@domain.com" -ToAddress "username@domain.com" -Subject "Success
Notification Message" -Body "Test Body"
C:\PS>$FailureNotification = Initialize-EmailNotification -FromAddress
"username@domain.com" -ToAddress "username@domain.com"  -Subject
"Failure Notification Message" -Body "Test Body"
C:\PS>Create-DataCollectionEvaluationJob -JobDetails $JobDetails -Assets
$Assets -Schedule $ScheduleData -Standards $Standards -SuccessNotification
$SuccessNotification -FailureNotification  $FailureNotification
```

Description: All the input details for creation of the collection-evaluation job are created such as Job-Name, Job-Details, Standards Scope, Assets-scope, Suceess Notification, Failure Notification, and Incremental Schedule-Data that are assigned to variables. These variables are passed on as the input while creating the job.

Example 2

```
C:\PS>$AppServerNameAndPort="localhost:1431" # <ServerName:Port>
C:\PS>$jobName = "CollectionEvaluationJob"
C:\PS>$JobDetails = Initialize-CollectionEvaluationJobDetails -Name $jobNam
-Description "Test Job Description" -DataCollectionCriteria 1
C:\PS>$Standards=Search-standards  -Filter {("displayname,equalto,CIS*") -a
("displayname,contains,Security Benchmark")} -SearchsubTree $True
C:\PS>$ScheduleData = Initialize-IncrementalSchedule -RepeatDays 7
-RunEveryNDays $FALSE -RunNow $TRUE -RunOnce $True -RunPeriodically $TRUE
-StartDate "2010-10-10 1:20:20"
C:\PS>$SuccessNotification = Initialize-EmailNotification -FromAddress
"username@domain.com" -ToAddress "username@domain.com" -Subject
"Success Notification Message" -Body "Test Body"
C:\PS>$FailureNotification = Initialize-EmailNotification -FromAddress
"username@domain.com" -ToAddress "username@domain.com"  -Subject
"Failure Notification Message" -Body "Test Body"
```

```
C:\PS>= Search-Assets -Filter {("displayname,startswith,e2e")}
-SearchsubTree $True -AssetType "symc-csm-AssetSystem-Asset-Wnt-Machine"
-Numberofobjectstoretrieve 5 | Create-DataCollectionEvaluationJob
-JobDetails $JobDetails -Assets $Assets -Schedule $ScheduleData -Standards
$Standards -SuccessNotification $SuccessNotification -FailureNotification
$FailureNotification
```

Description: All the input details for creation of the collection-evaluation job are created such as Job-Name Job-Details, Standards Scope, Assets-scope, Suceess Notification, Failure Notification, and Incremental Schedule-Data that are assigned to variables. These variables are passed on as the input while creating the job. The assets to be used as the scope to be piped as the input to the Create-DataCollectionEvaluationJob cmdlet.

Related Links

See Initialize-CollectionEvaluationJobDetails on page 1307.

See Search-Assets on page 1190.

See Search-Standards on page 1205.

Get-ChecksFromSection

`Get-ChecksFromSection` – Gets the checks from the specified section.

Synopsis

The Get-ChecksFromSection cmdlet retrieves the checks from the specified section.

Syntax

```
Get-ChecksFromSection -AppServerNameAndPort <String>
[-BindingType <String>] -Id <Guid> [-Filter <String[]>]
[-SearchSubTree [<Boolean>]] [-ExcludePredefineObjects [<Boolean>]]
 [-NumberOfObjectsToRetrieve <Int32>] [-PipingEnabled [<Boolean>]]
 [<CommonParameters>]
```

Authorization requirements

You must have the following CCS tasks to use the cmdlet:

- View Standards

You must have the permissions on following folders to use the cmdlet:

- Standards

Description

The Get-ChecksFromSection cmdlet returns the checks from the specified section.

Parameters

The following table describes the input parameters that the Get-ChecksFromSection cmdlet requires:

Table B-54 Get-ChecksFromSection - parameters

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
AppServerNameAndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServerNameAndPort ="<AppServerName/IP> :<Port Number Corresponding To Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-54 Get-ChecksFromSection - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$Binding Type="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.
Id	Mandatory	Guid	Yes	The unique identifier of the section.

Table B-54 Get-ChecksFromSection - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
Filter	Optional	Scriptblock	No	The Scriptblock should contain one or more Expressions. You have to use { } brackets for the filter. **Note:** If you do not specify any value in the Filter parameter, the cmdlet returns all the checks.
SearchSubtree	Optional	Boolean	No	True or False value that states if the sub-tree under the folder has to be searched for the check or not. The default value for this parameter is True.

Table B-54 Get-ChecksFromSection - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
Exclude PredefinedObjects	Optional	Boolean	No	True or False value that states if the predefined objects should be excluded from the search criteria. The default value for this parameter is False.
NumberOf ObjectsTo Retrieve	Optional	Int	No	The maximum number of checks that must be returned.
PipingEnabled	Optional	Boolean	Yes	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

The Expression of the Filter contains the following information:

Table B-55 Expression

Switch name	Switch type	Data type	Description
FieldName	Mandatory	String	The name of the field.

Table B-55 Expression *(continued)*

Switch name	Switch type	Data type	Description
ExpressionOperator	Mandatory	String	The ExpressionOperator contains the following members: ■ EqualTo ■ Contains ■ StartsWith ■ EndsWith
FieldValue	Mandatory	String	The value of the field.
FieldType	Optional	String	The data type by which you want to compare the fields. The FieldType contains the following members: ■ String ■ DateTime ■ Boolean ■ Guid **Note:** If FieldType is not provided, then String type will be used by default.

Filter can have more than one expression.

You have to apply the following rules while using the filter expression:

- The expression should be inside " " double quotes.
- The expression consists of FieldName, ExpressionOperator, FieldValue ,and FieldType. Each of these parts is separated by , comma.
- The comma can be escaped using \ backslash.
- The expression can be inside ( ) parentheses.

To combine multiple filter expressions, you can use the following logical operators:

Table B-56 Logical Operators

Operator name	Description	Usage
-and	Logical AND is used to add expressions to the search.	For example, -Filter {(("objectGUID, equalto, c8f0de1a-a278-4c29-86a1 -47d5ab91cb16, Guid") -and (("displayname, startswith, domainname\machinename"))}
-or	Logical OR is used to provide options to the search.	For example, -Filter {(("objectGUID, equalto, c8f0de1a-a278-4c29-86a1 -47d5ab91cb16, Guid") -or (("displayname, startswith, domainname\machinename"))}
!	Logical ! (bang) is used to negate the ExpressionOperator.	For example, -Filter {(("objectGUID, equalto, c8f0de1a-a278-4c29-86a1 -47d5ab91cb16, Guid") -and!("displayname, endswith, admin"))}

Inputs

You can pipe output of Get-SectionsFromStandard to Get-ChecksFromSection.

Outputs

The Get-ChecksFromSection cmdlet returns the Check object. It returns the list of checks that matches the search criteria.

The Check object contains the following information:

Table B-57 Get-ChecksFromSection- output

Switch name	Data type	Description
Id	Guid	The unique ID of the check.
Name	String	The display name of the check.
Version	String	The version of the check.

Table B-57 Get-ChecksFromSection- output *(continued)*

Switch name	Data type	Description
SectionID	Guid	The ID of the section to which the check belongs.

Notes

- You can set AppServerNameAndPort variable only once and reuse it till the session is closed.
- You can set BindingType variable only once and reuse it till the session is closed.
- The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example 1

```
PS C:\> Get-SectionsFromStandard -Id dbcabf6b-af5a-4111-beaa-da1e5c44e8fd
-Filter{("displayname,endswith,Operations")} -SearchSubTree $TRUE
-ExcludePredefineObjects $FALSE -NumberOfObjectsToRetrieve 10 |
Get-ChecksFromSection

Output:
StandardID    : dbcabf6b-af5a-4111-beaa-da1e5c44e8fd
Version       : 1.0.0
Id            : 8a177ecf-7edb-43ea-88d5-eee13c914665
Name          : 3.5.8 SQL Server service is not running as Local System
ExtensionData : System.Runtime.Serialization.ExtensionDataObject
```

Description: You can pipe the output of Get-SectionsFromStandard to Get-ChecksFromSection to get desired checks.

Example 2

```
PS C:\> Get-SectionsFromStandard -Id dbcabf6b-af5a-4111-beaa-da1e5c44e8fd
-Filter{("displayname,endswith,Operations")} -SearchSubTree $TRUE
-ExcludePredefineObjects $FALSE -NumberOfObjectsToRetrieve 10 |
Get-SectionsFromSection -Filter{("displayname,endswith,Devices")} |
 Get-ChecksFromSection

Output:
StandardID    : dbcabf6b-af5a-4111-beaa-da1e5c44e8fd
Version       : 1.0.0
Id            : 8a177ecf-7edb-43ea-88d5-eee13c914665
Name          : 3.5.8 SQL Server service is not running as Local System
ExtensionData : System.Runtime.Serialization.ExtensionDataObject
```

Description: You can pipe the output of Get-SectionsFromStandard to Get-ChecksFromSection to get the desired sub-sections. Then pipe this output to Get-ChecksFromSection to get the desired checks.

Related Links

- See Get-SectionsFromStandard on page 1222.

Get-SectionsFromSection

`Get-SectionsFromSection` – Gets the sections from the specified section.

Synopsis

The Get-SectionsFromSection cmdlet retrieves the sections from the specified section.

Syntax

```
Get-SectionsFromSection -AppServerNameAndPort <String>
 [-BindingType <String>] -Id <Guid> [-Filter <String[]>]
[-SearchSubTree [<Boolean>]] [-ExcludePredefineObjects [<Boolean>]]
[-NumberOfObjectsToRetrieve <Int32>] [-PipingEnabled [<Boolean>]]
 [<CommonParameter s>]
```

Authorization requirements

You must have the following CCS tasks to use the cmdlet:

- View Standards

You must have the following permissions on folders to use the cmdlet:

- Standards

Description

The Get-SectionsFromSection cmdlet returns the sections from the specified section.

Parameters

The following table describes the input parameters that the Get-SectionsFromSection cmdlet requires:

Table B-58 Get-SectionsFromSection - parameters

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
AppServerNameAndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServerNameAndPort="< AppServer Name/IP> : <Port Number Corresponding To Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-58 Get-SectionsFromSection - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$Binding Type="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.
Id	Mandatory	Guid	Yes	The unique identifier of the section.

Table B-58 Get-SectionsFromSection - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
Filter	Optional	Scriptblock	No	The Scriptblock should contain one or more Expressions. You have to use { } brackets for the filter. **Note:** If you do not specify any value in the Filter parameter, the cmdlet returns all the sections.
SearchSubtree	Optional	Boolean	No	True or False value that states if the sub-tree under the folder has to be searched for the section or not. The default value for this parameter is True.

Table B-58 Get-SectionsFromSection - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
Exclude PredefinedObjects	Optional	Boolean	No	True or False value that states if the predefined objects should be excluded from the search criteria. The default value for this parameter is False.
NumberOf ObjectsTo Retrieve	Optional	Int	No	The maximum number of sections that must be returned.
PipingEnabled	Optional	Boolean	Yes	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

The Expression of the Filter contains the following information:

Table B-59 Expression

Switch name	Switch type	Data type	Description
FieldName	Mandatory	String	The name of the field.

Table B-59 Expression *(continued)*

Switch name	Switch type	Data type	Description
ExpressionOperator	Mandatory	String	The ExpressionOperator contains the following members: ■ EqualTo ■ Contains ■ StartsWith ■ EndsWith
FieldValue	Mandatory	String	The value of the field.
FieldType	Optional	String	The data type by which you want to compare the fields. The FieldType contains the following members: ■ String ■ DateTime ■ Boolean ■ Guid **Note:** If FieldType is not provided, then String type will be used by default.

Filter can have more than one expression.

You have to apply the following rules while using the filter expression:

- The expression should be inside " " double quotes.
- The expression consists of FieldName, ExpressionOperator, FieldValue ,and FieldType. Each of these parts is separated by , comma.
- The comma can be escaped using \ backslash.
- The expression can be inside ( ) parentheses.

To combine multiple filter expressions, you can use the following logical operators:

Table B-60 Logical Operators

Operator name	Description	Usage
-and	Logical AND is used to add expressions to the search.	For example, -Filter {(("objectGUID, equalto, c8f0de1a-a278-4c29-86a1 -47d5ab91cb16, Guid") -and (("displayname, startswith, domainname\machinename"))}
-or	Logical OR is used to provide options to the search.	For example, -Filter {(("objectGUID, equalto, c8f0de1a-a278-4c29-86a1 -47d5ab91cb16, Guid") -or (("displayname, startswith, domainname\machinename"))}
!	Logical ! (bang) is used to negate the ExpressionOperator.	For example, -Filter {(("objectGUID, equalto, c8f0de1a-a278-4c29-86a1 -47d5ab91cb16, Guid") -and!("displayname, endswith, admin"))}

Inputs

You can pipe output of Get-SectionsFromStandard to Get-SectionFromSection.

Outputs

The Get-SectionsFromSection cmdlet returns the Section object. It returns the list of sections that match the search criteria.

The Section object contains the following information:

Table B-61 Get-SectionsFromSection- output

Switch name	Data type	Description
ID	Guid	The unique ID of the section.
Name	String	The display name of the section
Version	String	The version of the section.

Table B-61 Get-SectionsFromSection- output *(continued)*

Switch name	Data type	Description
StandardID	Guid	The ID of the standard to which the section belongs.

Notes

- You can set AppServerNameAndPort variable only once and reuse it till the session is closed.
- You can set BindingType variable only once and reuse it till the session is closed.
- The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example

```
C:\PS> Get-SectionsFromStandard -Id dbcabf6b-af5a-4111-beaa-da1e5c44e8fd
 -Filter{("displayname,endswith,Operations")} -SearchSubTree $TRUE
-ExcludePredefineObjects $FALSE -NumberOfObjectsToRetrieve 10 |
Get-SectionsFromSection

Output:
Version       : 1.0.0
StandardID    : dbcabf6b-af5a-4111-beaa-da1e5c44e8fd
Id            : f75fb20d-b8fa-4230-9c17-cbe1072b342d
Name          : DS13 - Manage Operations
ExtensionData : System.Runtime.Serialization.ExtensionDataObject
Version       : 1.0.0
StandardID    : dbcabf6b-af5a-4111-beaa-da1e5c44e8fd
Id            : 298ec372-9b74-456f-b6a3-172a709d1a3c
Name          : DS13.4 - Sensitive Documents and Output Devices
ExtensionData : System.Runtime.Serialization.ExtensionDataObject
```

Description: You can get the desired section using the Get-SectionsFromStandard cmdlet and then pipe that out-put to Get-SectionsFromSection to get the sub-sections.

Related Links

- See Get-SectionsFromStandard on page 1222.

Get-DataCollectionJob

`Get-DataCollectionJob` – Returns the data collection job for the given parameters.

Synopsis

The Get-DataCollectionJob cmdlet returns the data collection job parameters for the given Guid.

Syntax

```
Get-DataCollectionJob -AppServerNameAndPort <String>
[-BindingType <String>] -Id <Guid> [-PipingEnabled [<Boolean>]] [<CommonPar
    ters>]
```

Authorization requirements

You must have the following CCS tasks to use the Get-DataCollectionJob cmdlet:

- View Assets
- View Standards
- View Jobs

You must have the permissions on the following folders to use the Get-DataCollectionJob cmdlet:

- Asset System
- Standards

Description

The Get-DataCollectionJob cmdlet returns the CollectionJobParams object for the given Guid.

Parameters

Table B-62 Get-DataCollectionJob - parameters

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
AppServerNameAndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServerNameAndPort ="<AppServer Name/IP> : <Port Number Corresponding To Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-62 Get-DataCollectionJob - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$Binding Type="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.
Guid	Mandatory	Guid	Yes	The unique identifier of the data collection job.

Table B-62 Get-DataCollectionJob - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
PipingEnabled	Optional	Boolean	Yes	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

Inputs

You can pipe output of Search-Jobs to Get-DataCollectionJob.

Outputs

The cmdlet returns the formatted string which contains collection job parameter details.

Notes

You can set AppServerNameAndPort variable only once and reuse it till the session is closed

You can set BindingType variable only once and reuse it till the session is closed.

The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example 1

```
PS C:\> Search-Jobs -Name DC | Get-DataCollectionJob

Output:
Name: dc
Description:
Data Collection criteria: 0
```

```
Should send Success Notification: False
Should send Failure Notification: False
Incremental Schedule:
---------------------------------------------------------------------------
Run Now: False
Run Periodically: False
Start Date: 9/29/2010 12:41:36 AM
Run Once: False
Run Every N Days: False
Repeat Days Interval: 1
SubSchedule Repeat Days: 0
SubSchedule Repeat Period Days: 0

Success Email Notification details:
---------------------------------------------------------------------------
From Address:
To Address:
Subject:
Body:

Failure Email Notification details:
---------------------------------------------------------------------------
From Address:
To Address:
Subject:
Body:
```

Description: The Search-Jobs cmdlet is used to search the desired data-collection job and the output is piped to Get-DataCollectionJob.

Related Links

See Search-Jobs on page 1351.

Get-LastDataCollection

`Get-LastDataCollection` – Returns the date and time of the last data collection job that is executed for the given asset Guid.

Synopsis

The Get-LastDataCollection cmdlet returns the date and time of the last data collection job that is executed for the given asset Guid.

Syntax

```
 Get-LastDataCollection [-AppServerNameAndPort <String>]
[-BindingType <String>] [-Asset <Asset>] [-PipingEnabled [<Boolean>]]
[<CommonParameters>]
```

Authorization requirements

You must have the following CCS tasks to use the cmdlet:

- View All Jobs
- View Assets

Description

The Get-LastDataCollection cmdlet returns the date and time of the last data collection job that is executed for the given asset Guid. .

Parameters

The following table describes the input parameters that the Get-LastDataCollection cmdlet requires:

Table B-63 Get-LastDataCollection - parameters

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
AppServerName AndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServer NameAndPort ="< AppServer Name/IP> : <Port Number Corresponding To Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-63 Get-LastDataCollection - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$BindingType="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-63 Get-LastDataCollection - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
Asset	Mandatory	List<Asset>	Yes	The Asset object. You can get the value of this parameter from the `Search-Assets` cmdlet.
PipingEnabled	Optional	Boolean	Yes	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

The Asset object contains the following information:

Table B-64 Asset object

Switch name	Switch type	Data type	Description
Id	Mandatory	Guid	The unique identifier of the asset in the system.
Type	Optional	AssetType	The asset type.
Name	Optional	String	The display name of the asset.
Path	Optional	String	The full path of the asset.
Attributes	Optional	Attributes	The attributes of the object.

Inputs

You can pipe output of Search-Assets to Get-LastDataCollection.

Outputs

The GetLastDataCollection cmdlet returns the LastCollectionDateInfo object.

The LastDataCollectionInfo object contains the following information

Table B-65 LastDataCollectionInfo - object

Switch name	Data type	Description
Id	Guid	The unique identifier of the asset.
Name	String	The display name of the asset.
LastCollectionDate	DateTime	The last data collection date for given asset.
JobID	Guid	The job ID of the data collection job.

Notes

- You can set AppServerNameAndPort variable only once and reuse it till the session is closed.
- You can set BindingType variable only once and reuse it till the session is closed.
- The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Examples

```
PS C:\> Search-Assets -NumberOfObjectsToRetrieve 10 |
Get-LastDataCollection

Output:
Id                                  Name
--                                  ----
```

```
5f8aea29-16f0-4be2-addb-a4... MACHINE1
09f05e4b-f179-4e45-a6fa-d4... MACHINE2
                          ..
  LastCollectionDate            JobID
9/29/2010 12:41:41 AM         2207af5c-cb71-41e0-b41d-ba..
9/29/2010 12:41:41 AM         2207af5c-cb71-41e0-b41d-ba
```

Description: All the assets for which you want to get the last data collection information, you can search them using Search-Assets cmdlet and pipe it to Get-LastDataCollection

Related Links

- See Search-Assets on page 1190.

Get-EvaluationJob

`Get-EvaluationJob` – Returns the evaluation job for the given parameters.

Synopsis

The Get-EvaluationJob cmdlet returns the evaluation job parameters for the given job ID.

Syntax

```
 Get-EvaluationJob -AppServerNameAndPort <String>
[-BindingType <String>] -Id <Guid>
[-PipingEnabled [<Boolean>]] [<CommonParameters>]
```

Authorization requirements

You must have the following CCS tasks to use the cmdlet:

- View All Jobs
- View Assets
- View Standards

You must have the permission on the following folders to use the cmdlet:

- Asset System
- Standards

Description

The Get-EvaluationJob cmdlet returns the EvaluationJobParams object for the given job Guid.

Parameters

The following table describes the input parameters that the Get-EvaluationJob cmdlet requires:

Table B-66 Get-EvaluationJob - parameters

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
AppServerName AndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServer NameAndPort="< AppServer Name/IP> : <Port Number Corresponding To Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-66 Get-EvaluationJob - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$Binding Type="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.
Id	Mandatory	Id	Yes	The unique identifier of the job in the system.
PipingEnabled	Optional	Boolean	Yes	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

Inputs

You can pipe output of Search-Jobs to Get-EvaluationJob.

Outputs

The cmdlet returns the formatted string which contains Evaluation Job Parameters details.

Notes

You can set AppServerNameAndPort variable only once and reuse it till the session is closed.

You can set BindingType variable only once and reuse it till the session is closed.

The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example 1

```
C:\PS > Documents and Settings\Administrator.E2EDOM.000>
Search-Jobs -Type EVALUATION_JOB -Name EvaluationJob|
Get-EvaluationJob

Output
Name: EvaluationJob
Description: Test Job Description
Results Synchronization required: True
Should send Success Notification: True
Should send Failure Notification: True

Schedule:
-------------------------------------------------------
Run Now: False
Run Periodically: False
Start Date: 9/28/2010 3:15:34 AM
Run Once: False
Run Every N Days: False
Repeat Days Interval: 1

Result Viewers:
-------------------------------------------------------

Success Email Notification details:
-------------------------------------------------------
```

```
From Address: username@domain.com
To Address: username@domain.com
Subject: Success Notification Message
Body: Test Body

Failure Email Notification details:
-------------------------------------------------------
From Address: username@domain.com
To Address: username@domain.com
Subject: Failure Notification Message
Body: Test Body
```

Description: The desired evaluation job is searched using the Search-Jobs cmdlet and its output is piped to Get-EvaluationJob cmdlet.

Example 2

```
C:\PS > Documents and Settings\Administrator.E2EDOM.000>
Search-Jobs -Type EVALUATION_JOB -Name EvaluationJob

Output:
Id            : 5fcbb0e0-c288-45ed-8848-484d7ed22590
Name          : EvaluationJob
Type          : EVALUATION_JOB
CreationTime  : 9/26/2010 11:52:31 AM
ModifiedTime  : 9/26/2010 11:52:32 AM
LastRunDate   : 9/26/2010 11:52:34 AM
LastRunStatus : Faulted
Get-EvaluationJob -Id 5fcbb0e0-c288-45ed-8848-484d7ed22590
Name: EvaluationJob
Description: Test Job Description
Results Synchronization required: True
Should send Success Notification: True
Should send Failure Notification: True

Schedule:
--------------------------------------------------------------------
Run Now: False
Run Periodically: False
Start Date: 9/28/2010 3:28:16 AM
Run Once: False
Run Every N Days: False
```

```
Repeat Days Interval: 1
Result Viewers:
--------------------------------------------------------------------

Success Email Notification details:
--------------------------------------------------------------------
From Address: username@domain.com
To Address: username@domain.com
Subject: Success Notification Message
Body: Test Body
Failure Email Notification details:
--------------------------------------------------------------------
From Address: username@domain.com
To Address: username@domain.com
Subject: Failure Notification Message
Body: Test Body
```

Description: The desired evaluation job is searched using the Search-Jobs cmdlet. The Id of returned job is used as the input for the Get-EvaluationJob cmdlet.

Related Links

See Search-Jobs on page 1351.

Get-EvaluationJobForStandard

`Get-EvaluationJobForStandard` – Returns the list of evaluation and collection-evaluation jobs specific to the given standard.

Synopsis

The Get-EvaluationJobForStandard cmdlet returns the JobDetails object for the given Standard.

Syntax

```
Get-EvaluationJobsForStandard -AppServerNameAndPort
<String> [-BindingType <String>] -Id <Guid>
[-PipingEnabled [<Boolean>]] [<CommonParameters>]
```

Authorization requirements

Description

The Get-EvaluationJobForStandard cmdlet returns the JobDetails object for the specified standard.

Parameters

The following table describes the input parameters that the Get-EvaluationJobForStandard cmdlet requires:

Table B-67 Get-EvaluationJobForStandard - parameters

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
AppServerName AndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServerNameAndPort="<AppServerName/IP> : <Port Number Corresponding To Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-67 Get-EvaluationJobForStandard - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$Binding Type="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.
Id	Mandatory	Guid	Yes	The unique identifier of the standard for which you want to get the list of evaluation and collection-evaluation jobs. You can get the value of this parameter from the `Search-Standard` cmdlet.

Table B-67 Get-EvaluationJobForStandard - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
PipingEnabled	Optional	Boolean	Yes	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

Inputs

You can pipe output of Search-Standards to Get-EvaluationJobForStandard.

Outputs

The Get-EvaluationJobForStandard cmdlet returns the list of JobDetails objects for the given standard.

The JobDetails object contains the following information:

Table B-68 JobDetails object

Switch name	Data type	Description
Id	Guid	The unique identifier of the job.
Name	String	The name of the job.
Type	JobType	The valid job types.
CreationTime	DateTime	The creation time of the job.
ModifiedTime	DateTime	The time when the job was updated.
LastRunDate	DateTime	The date and time of the last job run.
LastRunStatus	String	The status of the last job run.

Notes

You can set AppServerNameAndPort variable only once and reuse it till the session is closed.

You can set BindingType variable only once and reuse it till the session is closed.

The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example 1

```
C:\PS > Search-Standards -Filter{("displayname,equalto,PCI
DSS v1.2 - CIS Windows Server 2003
Legacy Security Settings for Domain Member Servers v2.0")}
| Get-EvaluationJobsForStandard

Output:
Id             : 5fcbb0e0-c288-45ed-8848-484d7ed22590
Name           : EvaluationJob
Type           : EVALUATION_JOB
CreationTime   : 9/26/2010 11:52:31 AM
ModifiedTime   : 9/26/2010 11:52:32 AM
LastRunDate    : 9/26/2010 11:52:34 AM
LastRunStatus  : Faulted
```

Description: The Standard for which the Evaluation jobs need to find out, is searched using the Search-Standard cmdlet and its output is piped to Get-EvaluationJobsForStandard.

Example 2

```
C:\PS > Search-Standards -Filter{("displayname,equalto,PCI
DSS v1.2 - CIS Windows Server 2003
Legacy Security Settings for Domain Member Servers v2.0")}|
select Id
Id --c7020ff8-8ed8-4531-bdd0-82a02fc08c8a
PS C:\> Get-EvaluationJobsForStandard -Id
c7020ff8-8ed8-4531-bdd0-82a02fc08c8a

Output:
```

```
Id            : 5fcbb0e0-c288-45ed-8848-484d7ed22590
Name          : EvaluationJob
Type          : EVALUATION_JOB
CreationTime  : 9/26/2010 11:52:31 AM
ModifiedTime  : 9/26/2010 11:52:32 AM
LastRunDate   : 9/26/2010 11:52:34 AM
LastRunStatus : Faulted
```

Description: The Standard for which the Evaluation jobs need to find out, is searched using the Search-Standard cmdlet. The returned Id is used as the input to Get-EvaluationJobsForStandard.

Related Links

See Search-Standards on page 1205.

Initialize-CollectionJobDetails

`Initialize-CollectionJobDetails` – Creates the CollectionJobDetails object.

Synopsis

The Initialize-CollectionJobDetails helper class creates and returns the CollectionJobDetails object for the given parameters.

Syntax

```
Initialize-CollectionJobDetails -Name <String> [-Description <String>]
[-DataCollectionCriteria <Int32>] [<CommonParameters>]
```

Authorization requirements

All CCS users can run the Initialize-CollectionJobDetails helper class.

Description

The Initialize-CollectionJobDetails helper class creates and returns CollectionJobDetails object for the given parameters.

Parameters

The following table describes the parameters that the Initialize-CollectionJobDetails helper class requires:

Table B-69 Initialize-CollectionJobDetails - parameters

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
Name	Mandatory	String	No	The name of the Collection job
Description	Optional	String	No	The description of the Collection job

Table B-69 Initialize-CollectionJobDetails - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
DataCollection Criteria	Optional	Integer	No	The default value for the parameter is 0. Collect if data is { } days old or missing. **Note:** The maximum value for Data Collection criteria is 100. If you specify value more than 100 then data collection criteria defaults to 100.
PipingEnabled	Optional	Boolean	No	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

Inputs

You cannot pipe objects to the cmdlet.

Outputs

The Initialize-CollectionJobDetails helper class returns the CollectionJobDetails object.

The CollectionJobDetails object contains the following information:

Table B-70 CollectionJobDetails object

Switch name	Data type	Description
JobName	String	The name of the Collection job
JobDescription	String	The description of the Collection job
DataCollectionCriteria	Integer	The default value for the parameter is 0.

Notes

You can set AppServerNameAndPort variable only once and reuse it till the session is closed.

You can set BindingType variable only once and reuse it till the session is closed.

The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example

```
C:\PS> Initialize-CollectionJobDetails -Name “DataCollectionJob1”
-Description "Test Job Description" -DataCollectionCriteria 1
```

Description: The input values such as Job name, Job description, and Data-collection criteria are provided to create Initialize-CollectionJobDetails.

Related Links

- See Create-DataCollectionJob on page 1230.
- See Initialize-CollectionJobDetails on page 1300.
- See Initialize-EmailNotification on page 1459.
- See Initialize-IncrementalSchedule on page 1447.
- See Search-Assets on page 1190.
- See Search-Standards on page 1205.

Initialize-EvaluationJobDetails

`Initialize-EvaluationJobDetails` – Creates and returns the EvaluationJobDetails object.

Synopsis

The Initialize-EvaluationJobDetails helper class creates and returns EvaluationJobDetails object for the given parameters.

Syntax

```
Initialize-EvaluationJobDetails -Name <String> [-Description <String>]
[-ResultViewers [<String[]>]]
[-ShouldSynchronizeResults <Boolean>] [<CommonParameters>]
```

Authorization requirements

All CCS users can run the Initialize-EvaluationJobDetails helper class.

Description

The Initialize-EvaluationJobDetails helper class creates and returns EvaluationJobDetails object for the given parameters.

Parameters

The following table describes the parameters that the helper class requires:

Table B-71 Initialize-EvaluationJobDetails - parameters

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
Name	Mandatory	String	No	The name of the evaluation job
Description	Optional	String	No	The description of the evaluation job

Table B-71 Initialize-EvaluationJobDetails - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
Data Collection Criteria	Optional	Integer	No	The default value for the parameter is 0. **Note:** The maximum value for Data Collection criteria is 100. If you specify value more than 100 then data collection criteria defaults to 100.
ResultViewers	Optional	String	No	The list of users who can view the evaluation results.
Should Synchronise Results	Optional	Boolean	No	True if you want to synchronize the evaluation results to the reporting database. False if you do not want to synchronize the evaluation results to the reporting database.
PipingEnabled	Optional	Boolean	No	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

Inputs

You cannot pipe objects to the helper class.

Outputs

The helper class returns the EvaluationJobDetails object.

The EvaluationJobDetails object contains the following information:

Table B-72 EvaluationJobDetails object

Switch name	Data type	Description
JobName	String	The name of the evaluation job
JobDescription	String	The description of the evaluation job
DataCollectionCriteria	Integer	The default value for the parameter is 0. **Note:** The maximum value for Data Collection criteria is 100. If you specify value more than 100 then data collection criteria defaults to 100.
EvaluationResultViewers	String	The list of users who can view the evaluation results.

Notes

You can set AppServerNameAndPort variable only once and reuse it till the session is closed.

You can set BindingType variable only once and reuse it till the session is closed.

The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example 1

```
Initialize-EvaluationJobDetails -Name “EvaluationJob”
-Description "Test Job Description"
```

Description: The mandatory input values such as Job name and Job description are provided to create Initialize-EvaluationJobDetails.

Example 2

```
Initialize-EvaluationJobDetails -Name “EvaluationJob”
-Description "Test Job Description"
-ResultViewers “Administrator” -ShouldSynchronizeResults $TRUE
```

Description: The input values such as Job name, Job description, Result Viewers Names and Synch resultsare provided to create Initialize-EvaluationJobDetails.

Related Links

- See Create-EvaluationJob on page 1239.
- See Initialize-Schedule on page 1453.

Initialize-CollectionEvaluationJobDetails

`Initialize-CollectionEvaluationJobDetails` – Creates and returns the CollectionEvaluationJobDetails object for the given parameters.

Synopsis

The Initialize-CollectionEvaluationJobDetails helper class creates and returns CollectionEvaluationJobDetails object for the given parameter.

Syntax

```
Initialize-CollectionEvaluationJobDetails -Name <String>
[-Description <String>] [-DataCollectionCriteria <Int32>]
[-ResultViewers [<String[]>]] [-ShouldSynchronizeResults
[<Boolean>]] [<CommonParameters>]
```

Authorization requirements

The helper class does not require any authorization. Any CCS user can initialize the CollectionEvaluationJobDetails object.

Description

The Initialize-CollectionEvaluationJobDetails helper class creates and returns CollectionEvaluationJobDetails object based on the specified parameters. The output of this helper class is used as an input parameter for the Create-CollectionEvaluationJob cmdlet.

Parameters

The following table describes the input parameters that the Initialize-CollectionEvaluationJobDetails helper class requires:

Table B-73 Initialize-CollectionEvaluationJobDetails - parameters

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
Name	Mandatory	String	No	The name of the collection evaluation job.
Description	Optional	String	No	The description of the collection evaluation job.
DataCollection Criteria	Optional	Integer	No	The default value for the parameter is 0. Collect if data is { } days old or missing. **Note:** The maximum value for Data Collection criteria is 100. If you specify value more than 100 then data collection criteria defaults to 100.
ResultViewers	Optional	String	No	The list of users who can view the evaluation result.
Should Synchronise Results	Optional	Boolean	No	True if you want to synchronize the evaluation results to the reporting database. False if you do not want to synchronize the evaluation results to the reporting database.

Table B-73 Initialize-CollectionEvaluationJobDetails - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
PipingEnabled	Optional	Boolean	No	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

Inputs

You cannot pipe objects to the helper class.

Outputs

The Initialize-CollectionEvaluationJobDetails helper class returns the CollectionEvaluationJobDetails object.

The CollectionEvaluationJobDetails object contains the following information:

Table B-74 CollectionEvaluationJobDetails object

Switch name	Data type	Description
JobName	String	The name of the collection evaluation job.
JobDescription	String	The description of the collection evaluation job.
DataCollectionCriteria	Integer	The default value for the parameter is 0.
EvaluationResultViewers	String	The list of users who can view the evaluation result.

Notes

You can set AppServerNameAndPort variable only once and reuse it till the session is closed.

You can set BindingType variable only once and reuse it till the session is closed.

The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example 1

```
C:\PS>Initialize-CollectionEvaluationJobDetails
-Name “JobName” -Description "Test Job Description"
-DataCollectionCriteria 1
```

Description: All mandatory input values are provided to the Initialize-CollectionEvaluationJobDetails cmdlet.

Example 2

```
C:\PS>Initialize-CollectionEvaluationJobDetails
-Name “JobName” -Description "Test Job Description"
-DataCollectionCriteria 1 –ResultViewers “Administrator”
–ShouldSynchronizeResults $TRUE
```

Description: All mandatory input values are provided to the Initialize-CollectionEvaluationJobDetails cmdlet.

Related Links

- See Create-DataCollectionEvaluationJob on page 1247.

Create-TagCategory

`Create-TagCategory` – Creates a new tag category

Synopsis

The Create-TagCategory cmdlet creates a new tag category.

Syntax

```
Create-TagCategory -AppServerNameAndPort <String>
[-BindingType <String>] -Name <String> [-Description <String>]
[-PipingEnabled [<Boolean>]] [<CommonParameters>]
```

Authorization requirements

You must have the following CCS tasks to use the cmdlet:

- Manage Tags

Description

The Create-TagCategory cmdlet creates a new tag category.

Parameters

The following table describes the parameters that the cmdlet requires:

Table B-75 Create-TagCategory - parameters

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
AppServerName AndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServer NameAndPort="< AppServer Name/IP> : <Port Number Corresponding To Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-75 Create-TagCategory - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$Binding Type="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.
Name	Mandatory	String	No	The name of the new tag category that you want to create.
Description	Optional	String	No	The description for the new tag category.
PipingEnabled	Optional	Boolean	No	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

Inputs

You cannot pipe objects to the cmdlet.

Outputs

The Create-TagCategory does not return any value as an output. A new tag category with the specified name is created at the end of the successful execution of the cmdlet.

Notes

You can set AppServerNameAndPort variable only once and reuse it till the session is closed.

You can set BindingType variable only once and reuse it till the session is closed.

The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Control Compliance Suite does not support the following special characters in the name of the tag category:

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

Example 1

```
C:/PS> Create-TagCategory  -Name "Tag Catagory1" -Description
 "Test Description"
```

Output: Returns message: Tag Category Created Successfully.

Description: Creates Tag category named "Tag Catagory1" and description "Test Description".

Example 2

```
C:/PS> Create-TagCategory  -Name "Tag Catagory2"
```

Output: Returns message: Tag Category Created Successfully

Description: Creates Tag category named "Tag Catagory2" .Description field is optional.

Related Links

- See Create-Tag on page 1316.

Create-Tag

`Create-Tag` – Creates a new tag.

Synopsis

The Create-Tag cmdlet creates a new tag.

Syntax

```
Create-Tag -AppServerNameAndPort <String>
[-BindingType <String>] -Name <String> [-Description <String>]
-Category <String> [-PipingEnabled [<Boolean>]]
[<CommonParameters>]
```

Authorization requirements

You must have the following CCS tasks to use the cmdlet:

- Manage Tags

Description

The Create-Tag cmdlet creates a new tag with the specified name under the specified tag category.

Parameters

The following table describes the parameters that the cmdlet requires:

Table B-76 Create-Tag - parameters

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
AppServerNameAndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServerNameAndPort="<AppServer Name/IP> : <Port Number Corresponding To Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-76 Create-Tag - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$Binding Type="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.
Name	Mandatory	String	No	The name for the new tag.
Description	Optional	String	No	The description for the new tag.
Category	Mandatory	String	No	The name of the tag category under which you want to create a new tag.

Table B-76 Create-Tag - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
PipingEnabled	Optional	Boolean	No	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

Inputs

You cannot pipe objects to the cmdlet.

Outputs

The Create-Tag cmdlet returns a Tag object as an output.

The Tag object contains the following information:

Table B-77 Tag object

Switch name	Data type	Description
Id	Guid	The Id of the tag.
Name	String	The display name of the tag.
Description	String	The description of the tag.
Category	String	The tag category to which the tag belongs.
Owner	String	The owner of the tag.

Notes

You can set AppServerNameAndPort variable only once and reuse it till the session is closed.

You can set BindingType variable only once and reuse it till the session is closed.

The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Control Compliance Suite does not support the following special characters in the name of the tag:

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

Example 1

```
C:/PS> Create-Tag  -Name "Tag1"  -Description "Test tag"
-Category "Tag Catagory1"
```

```
Output:
Id            : eccb4d32-4a8d-4d0c-8f2b-67ea04032f76
Name          : Tag1
Description   : Test tag
Category      : Tag Catagory1
Owner         : Domain\user
ExtensionData : System.Runtime.Serialization.ExtensionDataObject
```

Description: Creates tag named, Tag1 under tag category, Tag Category1.

Example 2

```
C:/PS> Create-Tag  -Name  "Tag2"
-Category "Tag Catagory2"
```

```
Output:
Id            : eccb4d32-4a8d-4d0c-8f2b-67ea04032f76
Name          : Tag2
Description   :
Category      : Tag Catagory2
Owner         : Domain\user
ExtensionData : System.Runtime.Serialization.ExtensionDataObject
```

Description: Creates tag named, Tag2 under tag category, Tag Category2 The step is optional.

Related Links

- See Get-TaggedObjects on page 1339.
- See Add-Tags on page 1327.
- See Create-TagCategory on page 1311.
- See Create-Tag on page 1316.
- See Search-Assets on page 1190.
- See Search-Standards on page 1205.

Search-Tags

`Search-Tags` – Finds a tag or tags based on the specified criteria.

Synopsis

The Search-Tags cmdlet finds a tag or tags based on the specified parameters.

Syntax

```
Search-Tags -AppServerNameAndPort <String>
[-BindingType <String>] [-Name <String>] [-Category <String>]
[-PipingEnabled [<Boolean> ]]
[<CommonParameters>]
```

Authorization requirements

You must have the following CCS tasks to use the cmdlet:

- Manage Tags

Description

The Search-Tags cmdlet finds a tag or tags based on the specified parameters.

Parameters

The following table describes the parameters that the cmdlet requires:

Table B-78 Search-Tags - parameters

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
AppServerNameAndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServerNameAndPort="<AppServer Name/IP> : <Port Number Corresponding To Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-78 Search-Tags - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$Binding Type="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.
Name	Optional	String	No	The name for the new tag.
Category	Optional	String	No	The name of the tag category under which you want to create a new tag.
PipingEnabled	Optional	Boolean	No	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

Inputs

You cannot pipe objects to the cmdlet.

Outputs

The Search-Tag cmdlet returns a Tag object list as an output.

The Tag object contains the following information:

Table B-79 Tag object

Switch name	Data type	Description
Id	Guid	The Id of the tag.
Name	String	The display name of the tag.
Description	String	The description of the tag.
Category	String	The tag category to which the tag belongs.
Owner	String	The owner of the tag.

Notes

You can set AppServerNameAndPort variable only once and reuse it till the session is closed.

You can set BindingType variable only once and reuse it till the session is closed.

The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example 1

```
C:\PS> Search-Tags

Output:
Id            : 8d3c4f13-e341-43ba-b3f8-f53be1a0bb58
Name          : tag1
Description   :
Category      : TC-1
Owner         :Domain\User
ExtensionData : System.Runtime.Serialization.ExtensionDataObject
```

```
Id            : 867ff11a-769f-4b9b-8eb7-1fd9b6973504
Name          : tag2
Description   :
Category      : TC-1
Owner         : Domain\User
ExtensionData : System.Runtime.Serialization.ExtensionDataObject
```

Description: Returns all Tags available in the system.

Example 2

```
C:\PS> Search-Tags  -Name “Tag1” –Category  “TC-1”

Output:
Id            : 8d3c4f13-e341-43ba-b3f8-f53be1a0bb58
Name          : tag1
Description   :
Category      : TC-1
Owner         :Domain\User
ExtensionData : System.Runtime.Serialization.ExtensionDataObject
```

Description: Returns tag with name “Tag1” under category “TC-1”.

Related Links

- See Create-Tag on page 1316.
- See Create-TagCategory on page 1311.

Add-Tags

`Add-Tags` – Adds tags to the specified objects. The existing tags are overwritten if you set the Overwrite parameter to True. Else, the specified tags are added and the existing tags remain unaffected.

Synopsis

The Add-Tags cmdlet Adds tags to the specified objects.

Syntax

```
Add-Tags -AppServerNameAndPort <String>
[-BindingType <String>] -Tags <Tag[]> -ObjectType <String>
-ObjectIDs <Guid[]> [-Overwrite [<Boolean>]]
[-PipingEnabled [<Boolean>]] [<CommonParameters>]
```

Authorization requirements

You must have the following CCS tasks to use the cmdlet:

- Manage Assets & Assets Group
- Manage Standards
- Manage Policies
- Exception Approver
- Exception Requester

You must have the permissions on the following folders to use the cmdlet:

- Asset System
- Standards
- Policies

Description

The Add-Tags cmdlet adds tags to the objects for the given parameters. The previous tags of the objects remain unaffected.

Parameters

The following table describes the parameters that the Add-Tag cmdlet requires:

Table B-80 Add-Tags - parameters

Switch Name	Switch Type	Data Type	Supports piping input? Yes/No	Description
AppServerNameAndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServerNameAndPort="<AppServer Name/IP> : <Port Number Corresponding To Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-80 Add-Tags - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? Yes/No	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$Binding Type="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.
Tags	Mandatory	Tag	Yes	The tag object list. You can get the value of this parameter from the `Search-Tags` or `Create-Tag` cmdlets if piping is enabled for this field.
ObjectType	Mandatory	String	No	The type of the business object to which you want to add tags.

Table B-80 Add-Tags - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? Yes/No	Description
ObjectGuids	Mandatory	Guid	No	The IDs of the business objects to which you want to add the tags. You can get the value of this parameter from the `Search-Assets` or `Search-Standards` cmdlets if piping is enabled for this field.
Overwrite	Optional	Boolean	No	The default value for this parameter is False. If you specify the value as True, then the new tag overwrites the old tag of the business object..
PipingEnabled	Optional	Boolean	Yes	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

The Tag data type for the Tag field contains the following information:

Table B-81 Tag object

Switch name	Switch type	Data type	Description
ID	Mandatory	Guid	The ID of the tag.

Table B-81 Tag object *(continued)*

Switch name	Switch type	Data type	Description
DisplayName	Optional	String	The display name of the tag.
Description	Optional	String	The description of the tag.
TagCategory	Optional	String	The tag category to which the tag belongs.
Owner	Optional	String	The owner of the tag.

Inputs

You can pipe output of Search-Tags to Add-Tags.

Outputs

If tags get added successfully, the Add-Tags cmdlet returns the message 'Tag added successfully' .

Notes

You can set AppServerNameAndPort variable only once and reuse it till the session is closed.

You can set BindingType variable only once and reuse it till the session is closed.

The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example 1

```
C:\PS>$Tags = Search-Tags -Category "Default"
C:\PS>$AssetsGuid= @()
C:\PS>$Assets = Search-Assets -Filter
{("displayname,startswith,U")} -SearchsubTree $True
-AssetType "Windows Machine"
C:\PS>foreach($asset in $Assets)
```

```
>{
>  $AssetsGuid += $asset.ID
>}
C:\PS>Add-Tags -Tags $Tags -ObjectType "Windows Machine"
-ObjectGuids $AssetsGuid

Output:
Tag added successfully.
```

Description: Tags are retrived from the Search-Tags cmdlet and assets to be tagged are retrieved from the Search -Assets cmdlet. The array of Asset Ids formed from assets and passed on as ObjectGuids to Add-Tags.

Example 2

```
C:\PS>Search-Tags |Add-Tags -ObjectType "windows machine"
-ObjectGuids  900cbd47-8c7b-47b5-9940-9640903b2a69
-Overwrite 1

Output:
Tag added successfully.
```

Description: The tags are retrieved from Search-Tags cmdlet and are added to the specified windows machines. The existing tags of the objects get overwritten.

Related Links

See Create-Tag on page 1316.

See Search-Tags on page 1322.

See Search-Assets on page 1190.

See Search-Standards on page 1205.

See Get-AllExceptions on page 1392.

Remove-Tags

`Remove-Tags` – Removes the specified tags that are applied to the specified objects.

Synopsis

The Remove-Tags cmdlet removes the specified tags that are applied to the specified object.

Syntax

```
Remove-Tags -AppServerNameAndPort <String>
[-BindingType <String>] -Tags <Tag[]> -ObjectType <String>
-ObjectIDs <Guid[]> [-PipingEnabled [<Boolean>]]
[<CommonParameters>]
```

Authorization requirements

You must have the following CCS tasks to use the cmdlet:

- Manage Assets & Assets Group
- Manage Standards
- Manage Policies
- Exception Approver
- Exception Requester

You must have the permissions on the following folders to use the cmdlet:

- Asset System
- Standards
- Policies

Description

The Remove-Tags cmdlet removes tags of the objects for the given parameters.

Parameters

The following table describes the parameters that the Remove-Tag cmdlet requires:

Table B-82 Remove-Tags - parameters

Switch Name	Switch Type	Data Type	Supports piping input? Yes/No	Description
AppServerNameAndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServerNameAndPort="<AppServer Name/IP> : <Port Number Corresponding To Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-82 Remove-Tags - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? Yes/No	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$Binding Type="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.
Tags	Mandatory	Tag	Yes	The tag object list. You can get the value of this parameter from the `Search-Tags` or `Create-Tag` cmdlets if piping is enabled for this field.
ObjectType	Mandatory	String	No	The type of the business object from which you want to remove tags.

Table B-82 Remove-Tags - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? Yes/No	Description
ObjectGuids	Mandatory	Guid	No	The IDs of the business objects from which you want to remove tags. You can get the value of this parameter from the `Search-Assets`, `Search-Standards`, `Get-AllExceptions`, and `Get-ExceptionByTitle` cmdlets if piping is enabled for this field.
PipingEnabled	Optional	Boolean	-	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

The Tag data type for the Tag field contains the following information:

Table B-83 Tag object

Switch name	Switch type	Data type	Description
ID	Mandatory	Guid	The ID of the tag.
DisplayName	Optional	String	The display name of the tag.
Description	Optional	String	The description of the tag.

Table B-83 Tag object *(continued)*

Switch name	Switch type	Data type	Description
TagCategory	Optional	String	The tag category to which the tag belongs.
Owner	Optional	String	The owner of the tag.

Inputs

You can pipe output of Search-Tags to Remove-Tags.

Outputs

If tags get removed successfully, the Remove-Tags cmdlet returns the message, 'Tag removed successfully'.

Notes

You can set AppServerNameAndPort variable only once and reuse it till the session is closed.

You can set BindingType variable only once and reuse it till the session is closed.

The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example 1

```
C:\PS>$Tags = Search-Tags -Category "Default"
C:\PS>$AssetsGuid= @()
C:\PS>$Assets = Search-Assets -Filter
{("displayname,startswith,U")} -SearchsubTree $True
-AssetType "Windows Machine"
C:\PS>foreach($asset in $Assets)
>{
>  $AssetsGuid += $asset.ID
>}
C:\PS>Remove-Tags -Tags $Tags -ObjectType "Windows Machine"
-ObjectGuids $AssetsGuid
```

```
Output:
Tag removed successfully
```

Description: Tags are retrived from the Search-Tags cmdlet and assets are retrieved from the Search -Assets cmdlet. Array of Asset Ids formed from the assets and passed on as ObjectGuids to Remove-Tags.

Example 2

```
C:\PS>Search-Tags |Remove-Tags -ObjectType
"windows machine" -ObjectGuids  900cbd47-8c7b-47b5-9940-9640903b2a69
```

```
Output:
Tag removed successfully.
```

Description: Tags returned by search-Tags get removed from specified windows machines.

Related Links

- See Get-TaggedObjects on page 1339.
- See Add-Tags on page 1327.
- See Create-TagCategory on page 1311.
- See Create-Tag on page 1316.
- See Search-Assets on page 1190.
- See Search-Standards on page 1205.

Get-TaggedObjects

`Get-TaggedObjects` – Retrieves the tagged objects matching the criteria specified in the given parameters.

Synopsis

The Get-TaggedObjects cmdlet retrieves the tagged business objects.

Syntax

```
Get-TaggedObjects -AppServerNameAndPort <String>
[-BindingType <String>] -Tags <Tag[]>
-ObjectType <String> -ResultType <String> [-ContainerPath <String>]
[-Filter <String[]>]
[-SearchSubTree [<Boolean>]] [-ExcludePredefinedObjects [<Boolean>]]
[-NumberOfObjectsToRetrieve <Int32>] [-PipingEnabled [<Boolean>]]
[<CommonParameters>]
```

Authorization requirements

You must have the following CCS tasks to use the Get-TaggedObjects cmdlet:

- View Assets
- View Standards
- Manage Policies

You must have the permissions on the following folders to use the Get-TaggedObjects cmdlet:

- Asset System
- Standards
- Policies

Description

The Get-TaggedObjects cmdlet retrieves the business objects in a folder that are tagged as specified in the given parameters.

Parameters

The following table describes the parameters that the Get-TaggedObjects cmdlet requires:

Table B-84 Get-TaggedObjects - parameters

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
AppServerNameAndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServerNameAndPort ="<AppServerName/IP> : <Port Number Corresponding To Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-84 Get-TaggedObjects - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$Binding Type="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.
Tags	Mandatory	Tag	Yes	The tag object list. Get the value of the parameter from the `Create-Tag` or `Search-Tags` cmdlets if piping is enabled for this field.

Table B-84 Get-TaggedObjects - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
ObjectType	Mandatory	String	No	The object types that must be searched for. You can search for the assets or standards. Get the value of the parameter from the `Search-Assets` or `Search-Standards` cmdlets if piping is enabled for this field.

Table B-84 Get-TaggedObjects - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
ResultType	Mandatory	Enum	No	The ResultType is an enum. The tags are returned on the basis of the selection between All or Any. If the ResultType is 'All,' then the business objects that are associated with all the specified tags are returned. If the ResultType is 'Any,' then the business objects that are associated with any of the specified tags are returned.
ContainerPath	Optional	String	No	The full path of the folder that contains the object.

Table B-84 Get-TaggedObjects - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
Filter	Optional	Scriptblock	No	The Scriptblock should contain one or more Expressions. You have to use { } brackets for the filter. **Note:** If you do not specify any value in the Filter parameter, the cmdlet returns all the objects.
SearchSubtree	Optional	Boolean	No	The default value for this parameter is True. True or False value that states if the sub-tree under the folder has to be searched for the check or not.

Table B-84 Get-TaggedObjects - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
Exclude PredefinedObjects	Optional	Boolean	No	The default value for this parameter is False. True or False value that states if the predefined objects should be excluded from the search criteria.
NumberOf ObjectsToRetrieve	Optional	Int	No	The default value for this parameter is 0. The maximum number of checks that must be returned.
PipingEnabled	Optional	Boolean	Yes	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

The Tag data type for the Tag field contains the following information:

Table B-85 Tag object

Switch name	Switch type	Data type	Description
Id	Mandatory	Guid	The ID of the tag.

Table B-85 Tag object *(continued)*

Switch name	Switch type	Data type	Description
Name	Optional	String	The display name of the tag.
Description	Optional	String	The description of the tag.
Category	Optional	String	The tag category to which the tag belongs.
Owner	Optional	String	The owner of the tag.

The Expression of the Filter contains the following information:

Table B-86 Expression

Switch name	Switch type	Data type	Description
FieldName	Mandatory	String	The name of the field.
ExpressionOperator	Mandatory	String	The ExpressionOperator contains the following members: ■ EqualTo ■ Contains ■ StartsWith ■ EndsWith
FieldValue	Mandatory	String	The value of the field.

Table B-86 Expression *(continued)*

Switch name	Switch type	Data type	Description
FieldType	Optional	String	The data type by which you want to compare the fields. The FieldType contains the following members: ■ String ■ DateTime ■ Boolean ■ Guid **Note:** If FieldType is not provided, then String type will be used by default.

Filter can have more than one expression.

You have to apply the following rules while using the filter expression:

- The expression should be inside " " double quotes.
- The expression consists of FieldName, ExpressionOperator, FieldValue ,and FieldType. Each of these parts is separated by , comma.
- The comma can be escaped using \ backslash.
- The expression can be inside ( ) parentheses.

To combine multiple filter expressions, you can use the following logical operators:

Table B-87 Logical Operators

Operator name	Description	Usage
-and	Logical AND is used to add expressions to the search.	For example, -Filter {(("objectGUID, equalto, c8f0de1a-a278-4c29-86a1 -47d5ab91cb16, Guid") -and (("displayname, startswith, domainname\machinename"))}

Table B-87 Logical Operators *(continued)*

Operator name	Description	Usage
-or	Logical OR is used to provide options to the search.	For example, -Filter {(("objectGUID, equalto, c8f0de1a-a278-4c29-86a1 -47d5ab91cb16, Guid") -or (("displayname, startswith, domainname\machinename"))}
!	Logical ! (bang) is used to negate the ExpressionOperator.	For example, -Filter {(("objectGUID, equalto, c8f0de1a-a278-4c29-86a1 -47d5ab91cb16, Guid") -and!("displayname, endswith, admin"))}

Inputs

You can pipe output of Search-Tags or Search-Assets to Get-TaggedObjects.

Outputs

The Get-TaggedObjects cmdlet returns the BusinessObjectData object.

The following table describes the fields in the BusinessObjectData object:

Table B-88 BusinessObjectData object

Switch name	Data type	Description
Id	Guid	The ID of the business object.
Name	String	The name of the business object.
ObjectType	String	The type of the business object.

Notes

- You can set AppServerNameAndPort variable only once and reuse it till the session is closed.
- You can set BindingType variable only once and reuse it till the session is closed.

- The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example 1

```
C:\PS>$tag=Search-Tags
C:\PS>Get-TaggedObjects  -Tags $tag -ObjectType
"windows machine" -ResultType any

Output:
Id          900cbd47-8c7b-47b5-9940-96
Name           E2EDOM\ISS-J74
ObjectType                symc-csm-AssetSystem-Asset..
ExtensionData            System.Runtime.Serializati..
            No objects found for given search Criteria
```

Description: Returns windows machines objects that are tagged with the tags obtained from the Search-Tags cmdlet. The cmdlet returns the following message for the tags that are not used for any objects:

No object found for given search criteria.

Example 2

```
C:\PS> search-tags |Get-TaggedObjects
-Filter{("displayname,startswith,U") -and
("displayname,endswith,1") }
-ObjectType "windows machine" -ResultType any

Output:
Id          900cbd47-8c7b-47b5-9940-96
Name           E2EDOM\ISS-J74
ObjectType                symc-csm-AssetSystem-Asset..
ExtensionData            System.Runtime.Serializati..
            No objects found for given search Criteria
```

Description: Returns windows machines objects that are tagged with the tags obtained from the Search-Tags cmdlet. The cmdlet returns the following message for the tags that are not used for any objects:

No object found for given search criteria.

Related Links

- See Get-TaggedObjects on page 1339.
- See Add-Tags on page 1327.
- See Create-TagCategory on page 1311.
- See Create-Tag on page 1316.
- See Search-Assets on page 1190.
- See Search-Standards on page 1205.

Search-Jobs

`Search-Jobs` – Retrieves the list of jobs based on the given parameters.

Synopsis

The Search-Jobs cmdlet retrieves the JobDetails object based on the given parameters.

Syntax

```
Search-Jobs [-AppServerNameAndPort <String>]
[-BindingType <String>]
[-Name <String>] [-Type <String>] [-PipingEnabled
[<Boolean>]] [<CommonParameters>]
```

Authorization requirements

You must have the following CCS tasks to use the cmdlet:

- View Jobs

Description

The Search-Jobs cmdlet retrieves the JobDetails object based on the given parameters.

Parameters

The following table describes the input parameters that the Search-Jobs cmdlet requires:

Table B-89 Search-Jobs - parameters

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
AppServerNameAndPort	Mandatory	String	No	

Table B-89 Search-Jobs - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
				The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServerNameAndPort="<AppServerName/IP>: <Port Number Corresponding To Binding Type Set>"` Once specified, you need not specify the value again for every

Table B-89 Search-Jobs - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
				cmdlet in that session.

Table B-89 Search-Jobs - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
Binding Type	Optional	String	No	

Table B-89 Search-Jobs - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
				A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$BindingType="<NETTCP or HTTP or HTTPS>"` Once specified, you need not specify the value again for every

Table B-89 Search-Jobs - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
				cmdlet in that session.
Name	Optional	String	No	The name of the job that you want to retrieve.
Type	Optional	String	No	The type of job that you want to search for. The valid job types.
PipingEnabled	Optional	Boolean	Yes	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

Inputs

You cannot pipe objects to the cmdlet

Outputs

The Search-Jobs cmdlet returns the JobDetails object as an output

The JobDetails object contains the following information:

Table B-90 Search-Jobs output

Switch name	Data type	Description
Id	Guid	The unique identifier of the job.
Name	String	The name of the job.
Type	JobType	The type of the job.
CreationTime	DateTime	The creation time of the job.
ModifiedTime	DateTime	The time when the job was updated.
LastRunDate	DateTime	The date and time of the last job run.
LastRunStatus	String	The status of the last job run.

Notes

- You can set AppServerNameAndPort variable only once and reuse it till the session is closed.
- You can set BindingType variable only once and reuse it till the session is closed.
- The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example 1

```
C:/PS> Search-Jobss -Name dc

Output:
Id              : 6fc3c3e8-3ed3-43b8-a8e7-9e136fb964ce
Name            : dc
Type            : DATA_COLLECTION
```

```
CreationTime  : 9/29/2010 12:41:10 AM
ModifiedTime  : 9/29/2010 12:41:10 AM
LastRunDate   : 9/29/2010 12:46:17 AM
LastRunStatus : Completed
```

Description: Providing the name of the Job returns all the details of the required job.

Example 2

```
C:/PS> Search-Jobss -Type EVALUATION_JOB

Output:
Id            : 5fcbb0e0-c288-45ed-8848-484d7ed22590
Name          : EvaluationJob
Type          : EVALUATION_JOB
CreationTime  : 9/26/2010 11:52:31 AM
ModifiedTime  : 9/26/2010 11:52:32 AM
LastRunDate   : 9/26/2010 11:52:34 AM
LastRunStatus : Faulted
```

Description: Providing the type of the Job as the input returns all the jobs of that job type.

Related Links

See Get-DataCollectionJob on page 1277.

See Get-EvaluationJob on page 1288.

See Execute-Job on page 1360.

Execute-Job

`Execute-Job` – Executes the specified job.

Synopsys

Executes the specified job and returns the ExecuteJobInfo object.

Syntax

```
Execute-Job -AppServerNameAndPort <String>
[-BindingType <String>] -Name <String> [-PipingEnabled
[<Boolean>]] [<CommonParameters>]
```

Authorization requirements

You must have the following CCS tasks to use the cmdlet:

- View All Jobs
- Manage Jobs

Description

The Execute-Job cmdlet executes the specified job. The cmdlet executes the job immediately and returns the ExecuteJobInfo object. This does not schedule the job for later execution.

Parameters

The Execute-Job cmdlet requires the following input parameters:

Table B-91 Execute-Job - input parameters

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
AppServerNameAndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServerNameAndPort="<AppServerName/IP> : <Port Number Corresponding To Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-91 Execute-Job - input parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$Binding Type="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.
Name	Mandatory	Name	Yes	A valid name for the job.

Table B-91 Execute-Job - input parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
PipingEnabled	Optional	Boolean	Yes	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

Inputs

You can pipe output of Search-Jobs to Execute-Job.

Output

The Execute-Job cmdlet returns the ExecuteJobInfo object.

The Execute-Job cmdlet returns the following information in the output:

Table B-92 ExecuteJobInfo - object

Switch Name	Data Type	Description
Id	Guid	The id of the job
StartTime	DateTime	The time when the job started.
Status	Enum	The status code of the job. For example, Executing, Pending
WorkFlowInstanceID	Guid	The ID of workflow instance associated with Job.
Exception	ExceptionDetails	The details of the unhandled exception for the job.

Notes

You can set AppServerNameAndPort variable only once and reuse it till the session is closed.

You can set BindingType variable only once and reuse it till the session is closed.

The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example 1

```
Execute-Job -Name "EvaluationJob1"
Output:
Id                 : fcb53be6-7eed-4b7d-9677-0e8c69285636
StartTime          : 9/28/2010 4:06:08 PM
Status             : Executing
WorkflowInstanceID : 9fbb1a12-f0e9-4ed4-9acc-03dbc1ca56e8
Exception          :
```

Description: The Job name is passed on as the input to Execute-Job.

Example 2

```
Search-Job -Name "Evaluation_Job2”| Execute-Job
Output:
Id                 : fcb53be6-7eed-4b7d-9677-0e8c69285636
StartTime          : 9/28/2010 5:06:08 PM
Status             : Executing
WorkflowInstanceID : 9fbb1a12-f0e9-4ed4-9acc-03dbc1ca56e8
Exception          :
```

Description: The output of the Search-Job is piped to Execute-Job.

Related Links

See Search-Jobs on page 1351.

Request-Exception

`Request-Exception` – Creates an exception for the given associations.

Synopsis

The Request-Exception cmdlet returns the ExceptionReturnData object based on the given parameters.

Syntax

```
Request-Exception -AppServerNameAndPort <String>
[-BindingType <String>] -ExceptionDetails <ExceptionBasicDetail>
-AssetsForAssociation <Asset[]> -ToAssociation <Guid[]>
[-RequestedNotification
<Notification>] [-StateChangeNotification <Notification>]
[-PreExpirationNotification <Notification>] [-PipingEnabled
[<Boolean>]] [<CommonParameters>]
```

Authorization requirements

You must have the following CCS tasks to use the cmdlet:

- View Assets
- View Standards
- View Exceptions

You must have the permissions on the following CCS folders to use the cmdlet:

- Asset System
- Standards

Description

The Request-Exception cmdlet returns the ExceptionReturnData object based on the given parameters.

Parameters

The following table describes the input parameters that the Request-Exception cmdlet requires:

Table B-93 Request-Exception- parameters

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
AppServerNameAndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServerNameAndPort ="< AppServer Name/IP> : <Port Number Corresponding To Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-93 Request-Exception- parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$Binding Type="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.
ExceptionDetails	Mandatory	ExceptionDetails	Yes	Get the value of this parameter from the Initialize-ExceptionDetails helper class.

Table B-93 Request-Exception- parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
ToAssociation	Mandatory	Guid	Yes	You must specify the IDs of the assets as input parameters. **Note:** If the count of the IDs in the `To Association` parameter is zero, the cmdlet throws an Exception ManagementError after resolution. If the count of the IDs that are specified by the user do not match with the resolved asset count, the exception system creates an exception, with Partially Failed status. The cmdlet returns the list of `Unresolved ToAssociation` IDs.

Table B-93 Request-Exception- parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
AssetsFor Association	Mandatory	Asset	Yes	You must specify the IDs of the assets as input parameters. **Note:** If the count of the IDs in the `Assets ForAssociation` parameter is zero, the cmdlet throws an Exception ManagementError after resolution. If the count of the IDs that are specified by the user do not match with the resolved check count, the exception system creates an exception, with Partially Failed status. The cmdlet returns the list of `Unresolved ForAssociation` IDs.

Table B-93 Request-Exception- parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
Requested Notification	Optional	Notification	No	

Table B-93 Request-Exception- parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
				If you specify the customized notification data for exceptions, the Subject should not be null or empty. If the subject is empty, the default subject and body are used to send notification. If you do not specify the notification data at all, the default subject and body are used to send notification. The default subject is: Exception requested #Title The default body contains: The details of the exception are as follows: Title: #Title#. Effective date: #StartDate# Expiration date:

Table B-93 Request-Exception- parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
				#EndDate#. Current State: #CurrentState# Comments: #Comments#.

Table B-93 Request-Exception- parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
StateChange Notification	Optional	Notification	No	

Table B-93 Request-Exception- parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
				If you specify the customized notification data for state change, the Subject should not be null or empty. If the subject is empty, the default subject and body are used to send notification. If you do not specify the state change notification data at all, the default subject and body are used to send notification. The default subject is: State of the exception : #Title# is changed. The default body contains: The state of the exception has changed. The details of the exception are as follows:

Table B-93 Request-Exception- parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
				Title: #Title#. Effective date: #StartDate#. Expiration date: #EndDate#. Previous State#PreviousState# Current State: #CurrentState# Comments: #Comments#.

Table B-93 Request-Exception- parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
PreExpiration Notification	Optional	Notification	No	

Table B-93 Request-Exception- parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
				If you specify the customized notification data the Subject should not be null or empty. If the subject is empty, the default subject and body are used to send notification. If you do not specify the notification data at all, the default subject and body are used to send notification. The default subject is: Pre expiry notification for exception: #Title# The default body contains: The details of the exception are as follows: Title: #Title# Effective date: #StartDate# Expiration date:

Table B-93 Request-Exception- parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
				#EndDate# Current State: #CurrentState#
PipingEnabled	Optional	Boolean	Yes	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

The ExceptionDetails object contains the following information:

Table B-94 ExceptionDetails object

Switch name	Switch type	Data type	Description
Id	Mandatory	Guid	The ID is assigned to the exception after creation and is returned in the return object. This parameter is ignored after the creation of an exception.
Title	Optional	String	The title of the exception that you want to view. Maximum length allowed is 256 characters. After creation, you cannot edit the exception title.

Table B-94 ExceptionDetails object *(continued)*

Switch name	Switch type	Data type	Description
Description	Optional	String	Maximum length allowed is 1024 characters.
Type **Note:** When you create an exception of the type “Entitlement,” you must only provide inputs for the ForAssociation. If you specify ToAssociation instead of ForAssociation, the cmdlet throws an exception and if you specify both the parameters, then the cmdlet ignores the ToAssociation field.	Optional	ExceptionType (Enum)	You must specify the type of exception that is based on the module for which the exception is created. The Exception Type can be one of the following: ■ Standard ■ Entitlement ■ Policy

Table B-94 ExceptionDetails object *(continued)*

Switch name	Switch type	Data type	Description
State	Optional	ExceptionStates	ExceptionStates is an Enum that represents the state of an exception which can be one of the following: ■ Requested ■ Approved ■ Request Clarification ■ In Review ■ Deny ■ Approval overdue ■ Expired The parameter is ignored when you create an exception, but the exception state is always set to "Requested."

Table B-94 ExceptionDetails object *(continued)*

Switch name	Switch type	Data type	Description
ToAssociation Info	Optional	List <ToAssociation>	You must specify the IDs of the assets as input parameters. **Note:** If the counts of the IDs in the `ToAssociation` parameter is zero, the cmdlet throws an Exception ManagementError after resolution. If the counts of the IDs that are specified by the user do not match with the resolved asset count, the exception system creates an exception, with Partially Failed status. The cmdlet returns the list of `Unresolved ToAssociation` IDs.

Table B-94 ExceptionDetails object *(continued)*

Switch name	Switch type	Data type	Description
ForAssociationInfo	Optional	List<ForAssociation>	You must specify the IDs of the assets as input parameters. **Note:** If the counts of the IDs in the `ForAssociation` parameter is zero, the cmdlet throws an Exception ManagementError after resolution. If the counts of the IDs that are specified by the user do not match with the resolved check count, the exception system creates an exception, with Partially Failed status. The cmdlet returns the list of `Unresolved ForAssociation` IDs.
StartDate	Optional	DateTime	You must specify the start date that is greater than or equal to today's date. The cmdlet uses the date and the time is always set to 12 am for the specified date. **Note:** The DateTime format should always be universal and not local.

Table B-94 ExceptionDetails object *(continued)*

Switch name	Switch type	Data type	Description
EndDate	Optional	DateTime	You must specify the end date that is greater than or equal to the start date. The cmdlet uses the date and the time is always set to 11.59.59 pm for the specified date. **Note:** The DateTime format should always be universal and not local.
Requestor EmailID	Optional	String	The notification email for exception creation or failure is not sent if no email ID is specified.
Requestor GroupName	Optional	String	The Windows Group Users who have requested to create the exception.
RequesterSam AccountName	Optional	String	If not specified then Clients Windows identity will be used to Exception Requester and submitter.

Table B-94 ExceptionDetails object *(continued)*

Switch name	Switch type	Data type	Description
Requested NotificationData	Optional	Notification	If you specify the customized notification data for exceptions, the Subject should not be null or empty. If the subject is empty, the default subject and body are used to send notification. If you do not specify the notification data at all, the default subject and body are used to send notification. The default subject is: Exception requested #Title The default body contains: The details of the exception are as follows: Title: #Title#. Effective date: #StartDate# Expiration date: #EndDate#. Current State: #CurrentState# Comments: #Comments#.

Table B-94 ExceptionDetails object *(continued)*

Switch name	Switch type	Data type	Description
PreExpiration NotificationData	Optional	Notification	If you specify the customized notification data the Subject should not be null or empty. If the subject is empty, the default subject and body are used to send notification. If you do not specify the notification data at all, the default subject and body are used to send notification. The default subject is: Pre expiry notification for exception : #Title# The default body contains: The details of the exception are as follows: Title: #Title# Effective date: #StartDate# Expiration date: #EndDate# Current State: #CurrentState#

Table B-94 ExceptionDetails object *(continued)*

Switch name	Switch type	Data type	Description
StateChange NotificationData	Optional	Notification	

Table B-94 ExceptionDetails object *(continued)*

Switch name	Switch type	Data type	Description
			If you specify the customized notification data for state change, the Subject should not be null or empty. If the subject is empty, the default subject and body are used to send notification. If you do not specify the state change notification data at all, the default subject and body are used to send notification. The default subject is: State of the exception: #Title# is changed. The default body contains: The state of the exception has changed. The details of the exception are as follows: Title: #Title#. Effective date: #StartDate#. Expiration date: #EndDate#. Previous State:#PreviousState# Current State:

Table B-94 ExceptionDetails object *(continued)*

Switch name	Switch type	Data type	Description
			#CurrentState# Comments: #Comments#.

Table B-95 Notification Object

Switch name	Switch type	Data type	Description
ToEmailAddress	Optional	String	The email address to which the notification must be sent.
FromEmailAddress	Optional	String	The email address from which the notification must be sent.
Subject	Mandatory	String	The subject of the email notification.
Body	Mandatory	String	The detailed message.

Inputs

You can pipe output of Search-Assets to Request-Exception.

Outputs

The Request-Exception cmdlet returns the ExceptionReturnData object as an output.

The ExceptionReturnData object contains the following information

Table B-96 ExceptionReturnData object

Switch name	Data type	Description
Id	Guid	The title of the exception that you want to update.

Table B-96 ExceptionReturnData object *(continued)*

Switch name	Data type	Description
Status	OperationStatus (Enum)	The OperationStatus is an Enum that represents the status of the exception operation which can be one of the following: ■ Failed ■ Partially Failed ■ Passed
FailedAssociationForIds	List<Guid>	The unique IDs of all the assets for which the exception creation has failed.
FailedAssociationToIds	List<Guid>	The unique IDs of all the checks or policies for which the exception creation has failed.
Reason	String	The reason of failure of the operation status.

Notes

- You can set AppServerNameAndPort variable only once and reuse it till the session is closed.
- You can set BindingType variable only once and reuse it till the session is closed.
- The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example

```
PS C:\> $AppServerNameAndPort="localhost:1431" #
<ServerName:Port>

PS C:\> $Title = "Exception Created on  " +
(get-date -format g) | foreach {$_ -replace "/", "_"} |
 foreach {$_ -replace " ", "_"}

PS C:\> $ExceptionDetails = Initialize-ExceptionDetails
-Title "TITLE1" -Description "Test Description" -StartDate
"10/29/2010 12:41:41" -EndDate "12/29/2010 12:41:41"
-RequesterEmailID "abd@abc.com" -State "Requested" -Type
"Standards" -RequesterSamAccountName "ABCD" -RequesterGroupName
"ABCDEF"
PS C:\> $CheckGuids = @()
$Checks= Search-Checks  -Filter {("displayname,startswith,file")}
-SearchsubTree $True
foreach($Check in $Checks)
{
    $CheckGuids += $Check.ID
}

PS C:\> $RequestedNotification = Initialize-Notification -Subject
"Subject: RequestedNotification"  -Body "Test Exception Message Body"

PS C:\> $StateChangeNotification = Initialize-Notification -Subject
"Subject: StateChangeNotification"  -Body "Test Exception Message Body"

PS C:\> $PreExpirationNotification = Initialize-Notification
-Subject "Subject: PreExpirationNotification"  -Body "Test
Exception Message Body"

PS C:\> Search-Assets -Filter {("displayname,startswith,Win")}
-SearchsubTree $True -AssetType "symc-csm-AssetSystem-Asset-Wnt-Machine"
 -PipingEnabled $true  | Request-Exception -ExceptionDetails
$ExceptionDetails  -ToAssociation $CheckGuids -RequestedNotification
$RequestedNotification -StateChangeNotification $StateChangeNotification
-PreExpirationNotification $PreExpirationNotification
```

Description: You can use the helper class to initialize input for the exception. The scope of the exception is created using Search- Checks that is created as GUID list and passed on as the scope. The assets are directly searched and piped as the input to the Request-Exception cmdlet.

Related Links

See Search-Assets on page 1190.

See Search-Checks on page 1213.

See Initialize-ExceptionDetails on page 1437.

See Initialize-Notification on page 1462.

Get-AllExceptions

`Get-AllExceptions` – Returns all the exceptions that exist in the CCS system.

Synopsis

The Get-AllExceptions cmdlet returns the ExceptionInfo object based on the given parameters.

Syntax

```
Get-AllExceptions -AppServerNameAndPort <String>
[-BindingType <String>] [-PipingEnabled [<Boolean>]]
[<CommonParameters>]
```

Authorization requirements

All CCS users can read and view the exceptions in the exception store.

Description

The Get-AllExceptions cmdlet returns the ExceptionInfo object based on the given parameters.

Parameters

The following table describes the input parameters that the Get-AllExceptions cmdlet requires:

Table B-97 Get-AllExceptions - parameters

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
AppServerName AndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServer NameAndPort ="< AppServer Name/IP> : <Port Number Corresponding To Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-97 Get-AllExceptions - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$BindingType="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-97 Get-AllExceptions - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
Id	Mandatory	Guid	No	The unique ID that is internally assigned to an exception when the exception is created.
Title	Mandatory	String	No	The title of the exception.
State	Mandatory	ExceptionStates (Enum)	No	ExceptionStates is an Enum that represents the state of an exception which can be one of the following: ■ Requested ■ Approved ■ Request Clarification ■ Deny ■ InReview ■ Approval OverDue ■ Expired The parameter is ignored when you create an exception, but the exception state is always set to "Requested."

Table B-97 Get-AllExceptions - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
PipingEnabled	Optional	Boolean	Yes	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

Inputs

You cannot pipe objects to the cmdlet.

Outputs

The Get-AllExceptions cmdlet returns the ExceptionInfo object as an output

The ExceptionInfo object contains the following information:

Table B-98 ExceptionInfo object

Switch name	Data type	Description
Id	Guid	The title of the exception that you want to create. Maximum length allowed is 256 characters. After creation, you cannot edit the exception title.
Title	String	The title of the exception.

Table B-98 ExceptionInfo object *(continued)*

Switch name	Data type	Description
State	ExceptionStates (Enum)	ExceptionStates is an Enum that represents the state of an exception which can be one of the following: ■ Requested ■ Approved ■ RequestClarification ■ Deny ■ InReview ■ ApprovalOverDue ■ Expired The parameter is ignored when you create an exception, but the exception state is always set to "Requested."

Notes

- You can set AppServerNameAndPort variable only once and reuse it till the session is closed.
- You can set BindingType variable only once and reuse it till the session is closed.
- The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example

```
C:\PS>Get-AllExceptions
```

The cmdlet does not take any mandatory inputs. All exceptions and their details are returned.

Related Links

See Terminate-Exception on page 1431.

See Update-Exception on page 1416.

See Set-ExceptionState on page 1410.

Get-ExceptionByTitle

`Get-ExceptionByTitle` – Retrieves the ExceptionDetails object for the given parameters.

Synopsis

The Get-ExceptionByTitle cmdlet returns the ExceptionDetails object based on the given parameters.

Syntax

```
Get-ExceptionByTitle -AppServerNameAndPort <String>
[-BindingType <String>] -Title <String> [-PipingEnabled [<Boolean>]]
[<CommonParameters>]
```

Authorization requirements

Any CCS user can read or view the exception. Any CCS user can use the GetExceptionByTitle cmdlet to get the exception details.

Description

The Get-ExceptionByTitle cmdlet retrieves the ExceptionDetails object based on the given parameters.

Parameters

The following table describes the input parameters that the Get-ExceptionByTitle cmdlet requires:

Table B-99 Get-ExceptionByTitle - parameters

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
AppServerNameAndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServerNameAndPort="<AppServerName/IP> : <Port Number Corresponding To Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-99 Get-ExceptionByTitle - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$Binding Type="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.
Title	Mandatory	String	No	You must provide the name of the exception for which you want to view the details.

Table B-99 Get-ExceptionByTitle - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
PipingEnabled	Optional	Boolean	Yes	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

Inputs

You cannot pipe objects to the cmdlet.

Outputs

The Get-ExceptionByTitle cmdlet returns the ExceptionDetails object as an output

The ExceptionDetails object contains the following information:

Table B-100 ExceptionDetails object

Switch name	Data type	Description
Id	Guid	The ID is assigned to the exception after creation and is returned in the return object. This parameter is ignored after the creation of an exception.
Title	String	The title of the exception that you want to view. Maximum length allowed is 256 characters. After creation, you cannot edit the exception title.

Table B-100 ExceptionDetails object *(continued)*

Switch name	Data type	Description
Description	String	Maximum length allowed is 1024 characters.
Type **Note:** When you create an exception of the type “Entitlement,” you must only provide inputs for the ForAssociation. If you specify ToAssociation instead of ForAssociation, the cmdlet throws an exception and if you specify both the parameters, then the cmdlet ignores the ToAssociation field.	ExceptionType (Enum)	You must specify the type of exception that is based on the module for which the exception is created. The Exception Type can be one of the following: ■ Standard ■ Entitlement ■ Policy
State	ExceptionStates	ExceptionStates is an Enum that represents the state of an exception which can be one of the following: ■ Requested ■ Approved ■ Request Clarification ■ In Review ■ Deny ■ Approval overdue ■ Expired The parameter is ignored when you create an exception, but the exception state is always set to "Requested."

Table B-100 ExceptionDetails object *(continued)*

Switch name	Data type	Description
ToAssociationInfo	List <ToAssociation>	You must specify the IDs of the assets as input parameters. **Note:** If the counts of the IDs in the `ToAssociation` parameter is zero, the cmdlet throws an ExceptionManagementError after resolution. If the counts of the IDs that are specified by the user do not match with the resolved asset count, the exception system creates an exception, with Partially Failed status. The cmdlet returns the list of `UnresolvedTo Association` IDs.
ForAssociationInfo	List<ForAssociation>	You must specify the IDs of the assets as input parameters. **Note:** If the counts of the IDs in the `ForAssociation` parameter is zero, the cmdlet throws an ExceptionManagementError after resolution. If the counts of the IDs that are specified by the user do not match with the resolved check count, the exception system creates an exception, with Partially Failed status. The cmdlet returns the list of `Unresolved ForAssociation` IDs.

Table B-100 ExceptionDetails object *(continued)*

Switch name	Data type	Description
StartDate	DateTime	You must specify the start date that is greater than or equal to today's date. The cmdlet uses the date and the time is always set to 12 am for the specified date. **Note:** The DateTime format should always be universal and not local.
EndDate	DateTime	You must specify the end date that is greater than or equal to the start date. The cmdlet uses the date and the time is always set to 11.59.59 pm for the specified date. **Note:** The DateTime format should always be universal and not local.
RequestorEmailID	String	The notification email for exception creation or failure is not sent if no email ID is specified.
RequestorGroupName	String	The Windows Group Users who have requested to find the exception.
RequesterSamAccountName	String	If not specified then Clients Windows identity will be used to Exception Requester and submitter.

Table B-100 ExceptionDetails object *(continued)*

Switch name	Data type	Description
RequestedNotificationData	Notification	If you specify the customized notification data for exceptions, the Subject should not be null or empty. If the subject is empty, the default subject and body are used to send notification. If you do not specify the notification data at all, the default subject and body are used to send notification. The default subject is: Exception requested #Title The default body contains: The details of the exception are as follows: Title: #Title#. Effective date: #StartDate# Expiration date: #EndDate#. Current State: #CurrentState# Comments: #Comments#.

Table B-100 ExceptionDetails object *(continued)*

Switch name	Data type	Description
PreExpirationNotificationData	Notification	If you specify the customized notification data the Subject should not be null or empty. If the subject is empty, the default subject and body are used to send notification. If you do not specify the notification data at all, the default subject and body are used to send notification. The default subject is: Pre expiry notification for exception : #Title# The default body contains: The details of the exception are as follows: Title: #Title# Effective date: #StartDate# Expiration date: #EndDate# Current State: #CurrentState#

Table B-100 ExceptionDetails object *(continued)*

Switch name	Data type	Description
StateChangeNotificationData	Notification	If you specify the customized notification data for state change, the Subject should not be null or empty. If the subject is empty, the default subject and body are used to send notification. If you do not specify the state change notification data at all, the default subject and body are used to send notification. The default subject is: State of the exception: #Title# is changed. The default body contains: The state of the exception has changed. The details of the exception are as follows: Title: #Title#. Effective date: #StartDate#. Expiration date: #EndDate#. Previous State:#PreviousState# Current State: #CurrentState# Comments: #Comments#.

Notes

- You can set AppServerNameAndPort variable only once and reuse it till the session is closed.
- You can set BindingType variable only once and reuse it till the session is closed.

- The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example

```
Get-ExceptionByTitle -Title "Exception_Created_on_8_23_2010_10:40_AM"
```

Description: You can provide the name of the title to get all the details of the exception.

Related Links

See Terminate-Exception on page 1431.

See Update-Exception on page 1416.

See Set-ExceptionState on page 1410.

Set-ExceptionState

`Set-ExceptionState` – Changes the state of an exception as specified.

Synopsis

The Set-ExceptionState cmdlet returns the message string based on the given parameters.

Syntax

```
Set-ExceptionState [-AppServerNameAndPort <String>]
[-Binding Type <String>] [-ExceptionId <Guid>] [-ExceptionState
<String>] [-Comments <String>] [-PipingEnabled [<Boolean>]]
[<CommonParameters>]
```

Authorization requirements

All CCS users can read and view the exceptions in the exception store.

Description

The Set-ExceptionState cmdlet changes the state of an exception as specified. You cannot set the Expired state for an exception with the cmdlet. You must use the Terminate-Exception cmdlet to set the state of an exception to Expired.

Parameters

The following table describes the input parameters that the Set-ExceptionState cmdlet requires:

Table B-101 Set-ExceptionState - parameters

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
AppServerNameAndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServerNameAndPort="<AppServerName/IP> : <Port Number Corresponding To Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-101 Set-ExceptionState - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$BindingType="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-101 Set-ExceptionState - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
Id	Mandatory	Guid	Yes	The unique ID that is internally assigned to an exception when the exception is created.
State	Mandatory	ExceptionState (Enum)	No	ExceptionStates is an Enum that represents the state of an exception which can be one of the following: ■ Requested ■ Approved ■ Request Clarification ■ Deny ■ InReview ■ Approval OverDue ■ Expired The parameter is ignored when you create an exception, but the exception state is always set to "Requested."

Table B-101 Set-ExceptionState - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
Comments	Mandatory	String	No	The comments provided by the user.
PipingEnabled	Optional	Boolean	Yes	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

Inputs

You can pipe the output of Get-ExceptionByTitle to Set-ExceptionState.

Outputs

The Set-ExceptionState cmdlet sets the exception state as required on its successful execution.

Notes

- You can set AppServerNameAndPort variable only once and reuse it till the session is closed.
- You can set BindingType variable only once and reuse it till the session is closed.
- The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example 1

```
C:\PS> Get-ExceptionByTitle -title "excp1" | Set-ExceptionState
-State "Deny" -Comments "ASJJDAJSJD"

Output:
Set-ExceptionState : Successfully completed the current operation.
Failed to send Email notification. Contact CCS administrator or
specify the sender's Email address in the `From Email Address'
in the General Settings from the CCS Console.
```

Description: You can get the desired exception using Get-ExceptionByTitle to pipe that to the Set-ExceptionState. The state and the comments of the exception are given as the inputs.

Example 2

```
C:\PS> Get-AllExceptions | Set-ExceptionState -State "Deny"
-Comments "ASJJDAJSJD"

Output:
Exception state set successfully for given exception ID
Exception state set successfully for given exception ID
Exception state set successfully for given exception ID
Exception state set successfully for given exception ID
Exception state set successfully for given exception ID
Exception state set successfully for given exception ID
Exception state set successfully for given exception ID
```

Description: All the exceptions can be retrieved using Get-Allexceptions to be piped them to Set-ExceptionState. Thereby you can set the state for all the exceptions.

Related Links

- See Get-AllExceptions on page 1392.
- See Get-ExceptionByTitle on page 1399.

Update-Exception

`Update-Exception` – Finds and updates the specified exceptions that exist in the CCS system.

Synopsis

The Update-Exception cmdlet returns the ExceptionReturnData object based on the given parameters.

Syntax

```
Update-Exception -AppServerNameAndPort <String>
[-BindingType <String>] -ExceptionDetails <ExceptionDetails>
-Comments <String> [-PipingEnabled [<Boolean>]]
[<CommonParameters>]
```

Authorization requirements

All CCS users can view and update the exceptions in the exception store.

Description

The Update-Exception cmdlet returns the ExceptionReturnData object based on the given parameters.

It updates the specified exception; however you cannot update an expired exception.

You cannot update the following fields of an exception:

- Title
- Requester SAM Account Name
- Exception ID
- Exception Type
- State

Parameters

The following table describes the input parameters that the Update-Exception cmdlet requires:

Table B-102 Update-Exception - parameters

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
AppServerNameAndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServerNameAndPort ="< AppServer Name/IP> : <Port Number Corresponding To Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-102 Update-Exception - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$Binding Type="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.
ExceptionDetails	Mandatory	ExceptionDetails	Yes	Get the value of this parameter from the Get-Exception ByTitle cmdlet.

Table B-102 Update-Exception - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
Comments	Mandatory	String	No	The comments provided by the user.
PipingEnabled	Optional	Boolean	Yes	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

The ExceptionDetails object contains the following information:

Table B-103 ExceptionDetails object

Switch name	Switch type	Data type	Description
Id	Mandatory	Guid	The ID is assigned to the exception after creation and is returned in the return object. This parameter is ignored after the creation of an exception.
Title	Optional	String	The title of the exception that you want to view. Maximum length allowed is 256 characters. After creation, you cannot edit the exception title.

Table B-103 ExceptionDetails object *(continued)*

Switch name	Switch type	Data type	Description
Description	Optional	String	Maximum length allowed is 1024 characters.
Type **Note:** When you create an exception of the type "Entitlement," you must only provide inputs for the ForAssociation. If you specify ToAssociation instead of ForAssociation, the cmdlet throws an exception and if you specify both the parameters, then the cmdlet ignores the ToAssociation field.	Optional	ExceptionType (Enum)	You must specify the type of exception that is based on the module for which the exception is created. The Exception Type can be one of the following: ■ Standard ■ Entitlement ■ Policy

Table B-103 ExceptionDetails object *(continued)*

Switch name	Switch type	Data type	Description
State	Optional	ExceptionStates	ExceptionStates is an Enum that represents the state of an exception which can be one of the following: ■ Requested ■ Approved ■ Request Clarification ■ In Review ■ Deny ■ Approval overdue ■ Expired The parameter is ignored when you create an exception, but the exception state is always set to "Requested."

Table B-103 ExceptionDetails object *(continued)*

Switch name	Switch type	Data type	Description
ToAssociationInfo	Optional	List <ToAssociation>	You must specify the IDs of the assets as input parameters. **Note:** If the counts of the IDs in the `ToAssociation` parameter is zero, the cmdlet throws an Exception ManagementError after resolution. If the counts of the IDs that are specified by the user do not match with the resolved asset count, the exception system creates an exception, with Partially Failed status. The cmdlet returns the list of `Unresolved ToAssociation` IDs.

Table B-103 ExceptionDetails object *(continued)*

Switch name	Switch type	Data type	Description
ForAssociationInfo	Optional	List<ForAssociation>	You must specify the IDs of the assets as input parameters. **Note:** If the counts of the IDs in the `ForAssociation` parameter is zero, the cmdlet throws an Exception ManagementError after resolution. If the counts of the IDs that are specified by the user do not match with the resolved check count, the exception system creates an exception, with Partially Failed status. The cmdlet returns the list of `Unresolved ForAssociation` IDs.
StartDate	Optional	DateTime	You must specify the start date that is greater than or equal to today's date. The cmdlet uses the date and the time is always set to 12 am for the specified date. **Note:** The DateTime format should always be universal and not local.

Table B-103 ExceptionDetails object *(continued)*

Switch name	Switch type	Data type	Description
EndDate	Optional	DateTime	You must specify the end date that is greater than or equal to the start date. The cmdlet uses the date and the time is always set to 11.59.59 pm for the specified date. **Note:** The DateTime format should always be universal and not local.
RequestorEmailID	Optional	String	The notification email for exception creation or failure is not sent if no email ID is specified.
RequestorGroupName	Optional	String	The Windows Group Users who have requested to update the exception.
Requester SamAccountName	Optional	String	If not specified then Clients Windows identity will be used to Exception Requester and submitter.

Table B-103 ExceptionDetails object *(continued)*

Switch name	Switch type	Data type	Description
Requested NotificationData	Optional	Notification	If you specify the customized notification data for exceptions, the Subject should not be null or empty. If the subject is empty, the default subject and body are used to send notification. If you do not specify the notification data at all, the default subject and body are used to send notification. The default subject is: Exception requested #Title The default body contains: The details of the exception are as follows: Title: #Title#. Effective date: #StartDate# Expiration date: #EndDate#. Current State: #CurrentState# Comments: #Comments#.

Table B-103 ExceptionDetails object *(continued)*

Switch name	Switch type	Data type	Description
PreExpiration NotificationData	Optional	Notification	If you specify the customized notification data the Subject should not be null or empty. If the subject is empty, the default subject and body are used to send notification. If you do not specify the notification data at all, the default subject and body are used to send notification. The default subject is: Pre expiry notification for exception : #Title# The default body contains: The details of the exception are as follows: Title: #Title# Effective date: #StartDate# Expiration date: #EndDate# Current State: #CurrentState#

Table B-103 ExceptionDetails object *(continued)*

Switch name	Switch type	Data type	Description
StateChange NotificationData	Optional	Notification	

Table B-103 ExceptionDetails object *(continued)*

Switch name	Switch type	Data type	Description
			If you specify the customized notification data for state change, the Subject should not be null or empty. If the subject is empty, the default subject and body are used to send notification. If you do not specify the state change notification data at all, the default subject and body are used to send notification. The default subject is: State of the exception: #Title# is changed. The default body contains: The state of the exception has changed. The details of the exception are as follows: Title: #Title#. Effective date: #StartDate#. Expiration date: #EndDate#. Previous State:#PreviousState# Current State:

Table B-103 ExceptionDetails object *(continued)*

Switch name	Switch type	Data type	Description
			#CurrentState# Comments: #Comments#.

Inputs

You cannot pipe objects to the cmdlet.

Outputs

The Update-Exception cmdlet returns the ExceptionReturnData object as an output

The ExceptionReturnData object contains the following information:

Table B-104 ExceptionReturnData object

Switch name	Data type	Description
Id	Guid	The title of the exception that you want to update.
Status	OperationStatus (Enum)	The OperationStatus is an Enum that represents the status of the exception operation which can be one of the following: ■ Failed ■ Partially Failed ■ Passed
Failed AssociationForIds	List<Guid>	The unique IDs of all the assets for which the exception creation has failed.
FailedAssociationToIds	List<Guid>	The unique IDs of all the checks or policies for which the exception creation has failed.
Reason	String	The reason of failure of operation.

Notes

- You can set AppServerNameAndPort variable only once and reuse it till the session is closed.
- You can set BindingType variable only once and reuse it till the session is closed.
- The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example

```
C:\PS>$ExceptionDetail =  Get-ExceptionByTitle -Title
"Exception_Created_on_8_24_2010_2:39_PM"
C:\PS>$ExceptionDetail.RequestorEmailID  = "abcd@abcd.com"
C:\PS>$ExceptionDetail.StartDate = "10/29/2010 12:41:41"
C:\PS>$ExceptionDetail.EndDate = "12/29/2010 12:41:41"
C:\PS>update-Exception -ExceptionDetails $ExceptionDetail
-Comments "Test Comments"
```

Description: You can get the exception that needs to be updated using the Get-ExceptionByTitle cmdlet. Depending on the requirement you can update the start-date, the end-date, or the requestor-email and pass the objects to the Update-Exception cmdlet with the comments.

Related Links

See Get-ExceptionByTitle on page 1399.

Terminate-Exception

`Terminate-Exception` – Terminates the specified exception before its end date.

Synopsis

The Terminate-Exception cmdlet removes the specified exception.

Syntax

```
Terminate-Exception -AppServerNameAndPort <String>
[-BindingType <String>] -Id <Guid> [-PipingEnabled [<Boolean>]]
[<CommonParameters>]
```

Authorization requirements

All CCS users can view and delete the exceptions in the exception store.

Description

The specified exceptions are removed on successful excecution of the Terminate-Exception cmdlet.

Parameters

The following table describes the input parameters that the Terminate-Exception cmdlet requires:

Table B-105 Terminate-Exception - parameters

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
AppServerNameAndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServerNameAndPort="<AppServer Name/IP> :<Port Number Corresponding To Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-105 Terminate-Exception - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$Binding Type="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-105 Terminate-Exception - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
Id	Mandatory	Guid	Yes	The unique ID that is internally assigned to an exception when the exception is created.
PipingEnabled	Optional	Boolean	Yes	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

Inputs

You can pipe output of Get-ExceptionByTitle or Get-AllExceptions to Terminate-Exception.

Outputs

The Terminate-Exception cmdlet does not give any output. The specified exceptions are removed on successful execution of the cmdlet.

Notes

- You can set AppServerNameAndPort variable only once and reuse it till the session is closed.
- You can set BindingType variable only once and reuse it till the session is closed.
- The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example 1

```
 C:\PS> Get-ExceptionByTitle -Title excp1 |
Terminate-Exception

Output:
Terminate-Exception : Successfully completed
the current operation.
```

Description: The exception that needs to be terminated passed on to the Terminate-Exception cmdlet.

Example 2

```
 C:\PS> Get-AllExceptions | Terminate-Exception

Output:
Terminate-Exception : The exception has already expired.
Exception terminated successfully
Exception terminated successfully
Exception terminated successfully
Exception terminated successfully
Exception terminated successfully
Exception terminated successfully
Exception terminated successfully
```

Description: All the exceptions can be retrieved using the Get-AllExceptions cmdlet and piped to the Terminate-Exception cmdlet.

Example 3

```
 C:\PS> Get-AllExceptions | select id, title

Output:

Id                                 Title
--
a42e6dcc-a3af-4921-
b975-b3ce0f246c6d               Exception_Created_
                                on5__9_29_2010_5:45_AM
```

Description: The ID of the exception that needs to be terminated is given to the Terminate-Exception cmdlet as an input.

Related Links

- See Get-AllExceptions on page 1392.
- See Get-ExceptionByTitle on page 1399.

Initialize-ExceptionDetails

`Initialize-ExceptionDetails` – Creates and returns the ExceptionDetails object for the given parameters.

Synopsis

The Initialize-ExceptionDetails helper class returns the ExceptionDetails object based on the given parameters.

Syntax

```
Initialize-ExceptionDetails -AppServerNameAndPort
<String> [-BindingType <String>] -Title <String>
[-Description <String>] -StartDate <DateTime> -EndDate <DateTime>
[-RequesterEmailID <String>] [-RequesterSamAccountName <String>]
[-RequesterGroupName <String>] -State <String> -Type <String>
[-PipingEnabled [<Boolean>]] [<CommonParameters>]
```

Authorization requirements

All CCS users can read and view the exceptions in the exception store.

Description

The Initialize-ExceptionDetails helper class retrieves the ExceptionDetails object based on the given parameters.

Parameters

The following table describes the input parameters that the Initialize-ExceptionDetails helper class requires:

Table B-106 Initialize-ExceptionDetails - parameters

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
Title	Mandatory	String	No	The title of the exception that you want to create. Maximum length allowed is 256 characters. After creation, you cannot edit the exception title.
Description	Optional	String	No	Maximum length allowed is 1024 characters.

Table B-106 Initialize-ExceptionDetails - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
StartDate	Mandatory	DateTime	No	You must specify the start date that is greater than or equal to today's date. The cmdlet uses the date and the time is always set to 12 am for the specified date. **Note:** The DateTime format should always be universal and not local.

Table B-106 Initialize-ExceptionDetails - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
EndDate	Mandatory	DateTime	No	You must specify the end date that is greater than or equal to the start date. The cmdlet uses the date and the time is always set to 11.59.59 pm for the specified date. **Note:** The DateTime format should always be universal and not local.
Requester EmailID	Optional	String	No	The notification email for exception creation or failure is not sent if no email ID is specified.

Table B-106 Initialize-ExceptionDetails - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
RequesterSam AccountName	Optional	String	No	If not specified then Clients Windows identity will be used to Exception Requester and submitter.
Requester GroupName	Optional	String	No	The Windows group containing users who have requested to create exception.

Table B-106 Initialize-ExceptionDetails - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
State	Mandatory	State (Enum)	No	ExceptionStates is an Enum that represents the state of an exception which can be one of the following: ■ Requested ■ Approved ■ Request Clarification ■ Deny ■ InReview ■ Approval OverDue ■ Expired The parameter is ignored when you create an exception, but the exception state is always set to "Requested."

Table B-106 Initialize-ExceptionDetails - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
Type	Mandatory	ExceptionType (Enum)	No	You must specify the type of exception that is based on the module for which the exception is created. The Exception Type can be one of the following: ■ Standard ■ Entitlement ■ Policy
PipingEnabled	Optional	Boolean	No	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

Inputs

You cannot pipe objects to the helper class.

Outputs

The Initialize-ExceptionDetails helper class returns the ExceptionDetails object as an output

The ExceptionDetails object contains the following information:

Table B-107 ExceptionDetails object

Switch name	Data type	Description
Title	String	The title of the exception that you want to create. Maximum length allowed is 256 characters. After creation, you cannot edit the exception title.
Description	String	Maximum length allowed is 1024 characters.
Type **Note:** When you create an exception of the type "Entitlement," you must only provide inputs for the ForAssociation. If you specify ToAssociation instead of ForAssociation, the cmdlet throws an exception and if you specify both the parameters, then the cmdlet ignores the ToAssociation Switch.	ExceptionType (Enum)	The Exception Type can be one of the following: ■ Standard ■ Entitlement ■ Policy

Table B-107 ExceptionDetails object *(continued)*

Switch name	Data type	Description
State	ExceptionStates	ExceptionStates is an Enum that represents the state of an exception which can be one of the following: ■ Requested ■ Approved ■ Request Clarification ■ In Review ■ Deny ■ Approval Overdue ■ Expired The parameter is ignored when you create an exception, but the exception state is always set to "Requested."
StartDate	DateTime	The cmdlet uses the date and the time is always set to 12 am for the specified date. **Note:** The DateTime format should always be universal and not local.
EndDate	DateTime	The cmdlet uses the date and the time is always set to 11.59.59 pm for the specified date. **Note:** The DateTime format should always be universal and not local.
Requestor EmailID	String	The notification email for exception creation or failure is not sent if no email ID is specified.

Table B-107 ExceptionDetails object *(continued)*

Switch name	Data type	Description
RequesterSam AccountName	String	If not specified then Clients Windows identity will be used to Exception Requester and submitter.
Requester GroupName	String	The Windows group containing users who have requested to create exception.

Notes

- You can set AppServerNameAndPort variable only once and reuse it till the session is closed.
- You can set BindingType variable only once and reuse it till the session is closed.
- The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example

```
Initialize-ExceptionDetails -Title "TITLE1" -Description "Test Description"
-StartDate "10/29/2010 12:41:41" -EndDate "12/29/2010 12:41:41"
-RequesterEmailID "abd@abc.com"
-State "Requested" -Type "Standards" -RequesterSamAccountName "ABCD"
 -RequesterGroupName "ABCDEF"
```

Description: The helper class takes the title name, description, start-date, end-date, email id, state, and requestor details. In turn that forms as the input to the main Request-Exception cmdlet.

Related Links

See Request-Exception on page 1365.

Initialize-IncrementalSchedule

`Initialize-IncrementalSchedule` – Creates and returns the Schedule object.

Synopsis

The Initialize-IncrementalSchedule helper class creates and returns the Schedule object based on the given parameters.

Syntax

```
 Initialize-IncrementalSchedule
[-RunNow [<Boolean>]] [-RunPeriodically [<Boolean>]]
[-StartDate <DateTime>] [-RunOnce [<Boolean>]] [-RunEveryNDays
[<Boolean>]] [-RepeatDays <Int32>]
[-SubScheduleRepeatDays <Int32>] [-SubScheduleRepeatPeriodDays
<Int32>] [<CommonParameters>]
```

Authorization requirements

The Initialize-IncrementalSchedule helper class does not require any authorization. Any CCS user can initialize the Schedule object.

Description

The Initialize-IncrementalSchedule helper class creates and returns the Schedule object based on the given parameters.

Parameters

The following table describes the parameters that the Initialize-IncrementalSchedule helper class requires:

Table B-108 Initialize-IncrementalSchedule - parameters

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
SubSchedule RepeatDays	Optional	Integer	No	The number of days after which the sub-schedule must be repeated.

Table B-108 Initialize-IncrementalSchedule - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
SubSchedule Repeat PeriodDays	Optional	Integer	No	The end day for the sub-schedule to stop the job execution. The job stops running on this day.
RepeatDays	Optional	Integer	No	The number of days after which the main schedule must be repeated.
RunEveryNDays	Optional	Boolean	No	The default value of this parameter is False. True if you want to run the job on every specified days
RunNow	Optional	Boolean	No	The default value of this parameter is False. True if you want to run the job immediately after its creation. False if you do not want to run the job immediately but wants to specify a schedule for the job.
RunOnce	Optional	Boolean	No	The default value of this parameter is False. True if you want to run the job only once.

Table B-108 Initialize-IncrementalSchedule - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
RunPeriodically	Optional	Boolean	No	The default value of this parameter is False. True if you want to run the job periodically. You can specify the values for the sub-schedule parameters if you set the value for this parameter as True.
StartDate	Optional	DateTime	No	The date and time when the job schedule must start.
PipingEnabled	Optional	Boolean	No	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

Inputs

You cannot pipe objects to the helper class.

Outputs

The Initialize-IncrementalSchedule helper class returns the ScheduleData object.

The ScheduleData object contains the following information.

Table B-109 CollectionEvaluationScheduleData Object

Switch Name	Data Type	Description
SubScheduleRepeatDays	Integer	The number of days after which the sub-schedule must be repeated.
SubScheduleRepeat PeriodDays	Integer	The end day for the sub-schedule to stop the job execution. The job stops running on this day.
RepeatDays	Integer	The number of days after which you want to re-run the job. The value for this field is considered only if you set True for RunEveryNDays.
RunEveryNDays	Boolean	True if you want to run the job at a specified interval that is provided in the RepeatDays field. False if you do not want to run the job at a specified interval.
RunNow	Boolean	The default value of this parameter is False. True if you want to run the job immediately. False if you do not want to run the job immediately.
RunOnce	Boolean	The default value of this parameter is False. True if you want to run the job only once on the StartDate. False if you do not want to run the job only once on the StartDate.

Table B-109 CollectionEvaluationScheduleData Object *(continued)*

Switch Name	Data Type	Description
RunPeriodically	Boolean	The default value of this parameter is False. True if you want to run the job periodically. If you set True for this field, you must set True for either of the following: ■ RunOnce ■ RunEveryNDays False if you do not want to run the job periodically.
StartDate	DateTime	The date when the job run must begin. If you set True for RunNow, thejob is run immediately. If you set True for RunPeriodically, one of the following options is possible: ■ You can set RunOnce. The job will be run only once on the start date, You can set RunEveryNDays. The job will be repeated after every <RepeatDays> starting from specified StartDate.

Notes

You can set AppServerNameAndPort variable only once and reuse it till the session is closed.

You can set BindingType variable only once and reuse it till the session is closed.

The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example 1

```
PS C:\>Initialize-IncrementalSchedule -SubScheduleRepeatDays 0
-SubScheduleRepeatPeriodDays 0 -RepeatDays 7
```

```
-RunEveryNDays $FALSE -RunNow $TRUE -RunOnce $True
-RunPeriodically $TRUE -StartDate “11/26/2010 11:52:31 AM”

Output:
SubScheduleRepeatDays       : 0
SubScheduleRepeatPeriodDays : 0
RunNow                      : True
RunPeriodically             : True
StartDate                   : 11/26/2010 11:52:31 AM
RunOnce                     : True
RunEveryNDays               : False
RepeatDays                  : 7
```

Description: The Schedule with no sub-schedule is created by adding the appropriate values for RepeatDays, RunNow, and RunPeriodically.

Example 2

```
PS C:\> Initialize-IncrementalSchedule -SubScheduleRepeatDays 7
-SubScheduleRepeatPeriodDays 8 -RepeatDays 10 -RunEveryN
Days $TRUE -RunNow $FALSE -RunOnce $FALSE -RunPeriodically
$TRUE -StartDate "11/26/2010 11:52:31 AM"

Output:
SubScheduleRepeatDays       : 7
SubScheduleRepeatPeriodDays : 8
RunNow                      : False
RunPeriodically             : True
StartDate                   : 11/26/2010 11:52:31 AM
RunOnce                     : False
RunEveryNDays               : True
RepeatDays                  : 10
```

Description: The Schedule and sub-schedule is created by adding the appropriate values for RepeatDays, RunNow, RunPeriodically, Sub-scheduleRepeatDays, and Period for subschedule repeat.

Related Links

See Create-DataCollectionJob on page 1230.

See Create-DataCollectionEvaluationJob on page 1247.

Initialize-Schedule

`Initialize-Schedule` – Creates and returns the Schedule object.

Synopsis

The Initialize-Schedule helper class creates and returns the Schedule object based on the given parameters.

Syntax

```
Initialize-Schedule [-RunNow [<Boolean>]]
[-RunPeriodically [<Boolean>]] [-StartDate <DateTime>]
[-RunOnce [<Boolean>]] [-RunEveryN
    Days [<Boolean>]] [-RepeatDays <Int32>]
 [<CommonParameters>]
```

Authorization requirements

The helper class does not require any authorization. Any CCS user can initialize the Schedule object.

Description

The Initialize-Schedule helper class creates and returns Schedule object for the given parameter.

Parameters

The following table describes the parameters that the helper class requires:

Table B-110 Initialize-Schedule - parameters

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
RunNow	Optional	Boolean	No	The default value of this parameter is False. True if you want to run the job immediately after its creation. False if you do not want to run the job immediately but wants to specify a schedule for the job.
RunPeriodically	Optional	Boolean	No	The default value of this parameter is False. True if you want to run the job periodically. You can specify the values for the sub-schedule parameters if you set the value for this parameter as True.
StartDate	Optional	DateTime	No	The date and time when the job schedule must start.
RunOnce	Optional	Boolean	No	The default value of this parameter is False. True if you want to run the job only once.

Table B-110 Initialize-Schedule - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
RunEveryNDays	Optional	Boolean	No	The default value of this parameter is False. True if you want to run the job on every specified days.
RepeatDays	Optional	Integer	No	The number of days after which the main schedule must be repeated.
PipingEnabled	Optional	Boolean	No	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

Inputs

You cannot pipe objects to the helper class.

Outputs

The Initialize-Schedule helper class returns the Schedule object.

The Schedule object contains the following information.

Table B-111 Schedule Object

Switch Name	Data Type	Description
RepeatDays	Integer	The number of days after which you want to re-run the job. The value for this Switch is considered only if you set True for RunEveryNDays.

Table B-111 Schedule Object *(continued)*

Switch Name	Data Type	Description
RunEveryNDays	Boolean	The default value of this parameter is False. True if you want to run the job at a specified interval that is provided in the RepeatDays Switch. False if you do not want to run the job at a specified interval.
RunNow	Boolean	The default value of this parameter is False. True if you want to run the job immediately . False if you do not want to run the job immediately.
RunOnce	Boolean	The default value of this parameter is False. True if you want to run the job only once on the StartDate. False if you do not want to run the job only once on the StartDate.
RunPeriodically	Boolean	The default value of this parameter is False. True if you want to run the job periodically. If you set True for this Switch, you must set True for either of the following: ■ RunOnce ■ RunEveryNDays False if you do not want to run the job periodically.

Table B-111 Schedule Object *(continued)*

Switch Name	Data Type	Description
StartDate	DateTime	The date when the job run must begin. If you set True for RunNow, the job is run immediately. If you set True for RunPeriodically, one of the following options is possible: ■ You can set RunOnce. The job will be run only once on the start date, You can set RunEveryNDays. The job will be repeated after every <RepeatDays> starting from specified StartDate.

Notes

You can set AppServerNameAndPort variable only once and reuse it till the session is closed.

You can set BindingType variable only once and reuse it till the session is closed.

The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example 1

```
Initialize-Schedule -RepeatDays 7 -RunEveryNDays $FALSE
-RunNow $TRUE -RunOnce $True -RunPeriodically $TRUE
-StartDate “2010-10-10 1:20:20”
```

Description: The Schedule is created with all required inputs.

Example 2

```
Initialize-Schedule -RepeatDays 7 -RunEveryNDays $FALSE
-RunNow $TRUE
```

Description: The Schedule is created with some inputs.

Related Links

- See Create-EvaluationJob on page 1239.

Initialize-EmailNotification

`Initialize-EmailNotification` – Creates and returns the Notification object.

Synopsis

The Initialize-EmailNotification helper class creates and returns Notification object for the given parameter.

Syntax

```
Initialize-EmailNotification -FromAddress <String>
 -ToAddress <String> [-Subject <String>] [-Body <String>]
[<CommonParameters>]
```

Authorization requirements

The Initialize-EmailNotification helper class does not require any authorization. Any CCS user can initialize the Notification object.

Description

The Initialize-EmailNotification helper class creates and returns Notification object for given parameter.

Parameters

The following table describes the parameters that the Initialize-EmailNotification helper class requires:

Table B-112 Initialize-EmailNotification - parameters

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
From EmailAddress	Mandatory	String	No	A valid Email address from which the notification Email must be sent.

Table B-112 Initialize-EmailNotification - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? (Yes/No)	Description
To EmailAddress	Mandatory	String	No	A valid Email address to which the notification must be sent
Subject	Mandatory	String	No	The subject of the Email.
Body	Mandatory	String	No	The body of the Email.
PipingEnabled	Optional	Boolean	No	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

Inputs

You cannot pipe objects to the helper class.

Outputs

The Initialize-EmailNotification helper class returns the AssetNotificationData object.

The Notification object contains the following information:

Table B-113 Notification Object

Switch name	Data type	Description
FromEmailAddress	String	The email address from which the notification must be sent.
ToEmailAddress	String	The email address to which the notification must be sent.

Table B-113 Notification Object *(continued)*

Switch name	Data type	Description
Subject	String	The subject of the email notification.
Body	String	The detailed message.

Notes

You can set AppServerNameAndPort variable only once and reuse it till the session is closed.

You can set BindingType variable only once and reuse it till the session is closed.

The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example

```
Initialize-EmailNotification -FromAddress "username@domain.com"
-ToAddress "username@domain.com"
-Subject "Success Notification Message" -Body "Test Body"

Output:
FromAddress : username@domain.com
ToAddress   : username@domain.com
Subject     : Success Notification Message
Body        : Test Body
```

Description: From email address, To email address, Subject, and Body of the email are given as the inputs to Initialize-EmailNotification.

Related Links

None

Initialize-Notification

`Initialize-Notification` – Creates and returns Notification object for the given parameters.

Synopsis

The Initialize-Notification helper class returns the Notification object based on the given parameters.

Syntax

```
Initialize-Notification -Subject <String> -Body <String>
[-Notify [<Boolean>]]
[-PipingEnabled [<Boolean>]] [<CommonParameters>]
```

Authorization requirements

All CCS users can run the Initialize-Notification helper class.

Description

The Initialize-Notification helper class creates and returns Notification object for the given parameters.

Parameters

The following table describes the input parameters that the Initialize-Notification helper class requires:

Table B-114 Initialize-Notification - parameters

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
Subject	Mandatory	String	No	The subject of the email notification.

Table B-114 Initialize-Notification - parameters *(continued)*

Switch name	Switch type	Data type	Supports piping input? (Yes/No)	Description
Body	Mandatory	String	No	The detailed message.
Notify	Optional	Boolean	No	The default value of this parameter is False.
PipingEnabled	Optional	Boolean	No	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

Inputs

You cannot pipe objects to the helper class.

Outputs

The Initialize-Notification helper class returns the Notification object as an output.

The Notification object contains the following information

Table B-115 Notification Object

Switch name	Data type	Description
ToEmailAddress	String	The email address to which the notification must be sent.
FromEmailAddress	String	The email address from which the notification must be sent.
Subject	String	The subject of the email notification.

Table B-115 Notification Object *(continued)*

Switch name	Data type	Description
Body	String	The detailed message.

Notes

- You can set AppServerNameAndPort variable only once and reuse it till the session is closed.
- You can set BindingType variable only once and reuse it till the session is closed.
- The ExtensionData property should be ignored, if present in the output. It is a WCF specific property that is required for making the data contract forward-compatible and for versioning process.

Example

```
C:\PS>Initialize-Notification -Subject "Subject:
StateChangeNotification"  -Body "Test Exception Message Body"
```

Description: The subject and the body of notification are given as the inputs to this helper class.

Related Links

See Request-Exception on page 1365.

Add-Associations

`Add-Associations` – Adds associations with the Business Assets.

Synopsis

The Add-Associations cmdlet associate assets with the business asset.

Syntax

```
Add-Associations -AppServerNameAndPort <String> [-BindingType <String>] -Bu
[-PipingEnabled [<Boolean>]] [<CommonParameters>]
```

Authorization requirements

You must have the following CCS tasks to use the cmdlet:

- View Assets
- Manage Assets and Asset Groups

You must have the permissions on the following folders to use the cmdlet:

- Asset System
- Business Assets

Description

You can associate assets with the specified business asset.

Parameters

The following table describes the parameters that the Add-Associations cmdlet requires:

Table B-116 Add-Associations - parameters

Switch Name	Switch Type	Data Type	Supports piping input? Yes/No	Description
AppServerNameAndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServerNameAndPort="<AppServerName/IP> : <Port Number Corresponding To Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-116 Add-Associations - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? Yes/No	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$Binding Type="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.
BusinessAsset	Mandatory	Asset	Yes	It is a business asset. You can get the value of this parameter from the `Search-Assets` cmdlet if piping is enabled for this field.
Associations	Mandatory	Asset	Yes	A list of assets for associations with business asset.

Table B-116 Add-Associations - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? Yes/No	Description
PipingEnabled	Optional	Boolean	Yes	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

Inputs

You can pipe output of Search-Assets to the Add-Associations cmdlet.

Outputs

The Add-Associations cmdlet did not return any output. As a result of the successful execution of the cmdlet, the assets are associated with the business asset.

Notes

You can set AppServerNameAndPort variable only once and reuse it till the session is closed.

You can set BindingType variable only once and reuse it till the session is closed.

This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer, and OutVariable. For more information, type, **get-help about_commonparameters** on the PowerShell CLI.

Example 1

```
C:\PS > $businessAsset = Search-Assets -AssetType "Business Asset"
         -NumberOfObjectsToRetrieve 1
C:\PS > $WindowsAsset = Search-Assets -Filter {("displayname,startswith,Win
        -SearchsubTree $True -AssetType "Windows Machine" -NumberOfObjectsT
C:\PS > Add-Associations -BusinessAsset $businessAsset -Associations $Windo
```

```
Output:
Associations formed.
```

Description: The business asset and associations are retrieved from Search-Assets using proper filters and are assigned to variable $businessAsset and $WindowsAsset. These variables are used as inputs to the Add-Associations cmdlet.

Example 2

```
C:\PS > $businessAsset = Search-Assets -AssetType "Business Asset"
        -NumberOfObjectsToRetrieve 1
C:\PS > Search-Assets -Filter {("displayname,startswith,Win")} -SearchsubTr
        -AssetType "Windows Machine" -NumberOfObjectsToRetrieve 5 |
        Add-Associations -BusinessAsset $businessAsset
```

```
Output:
Associations formed.
```

Description: Associations are formed using piping. The output of Search-Assets is piped to Add-Associations cmdlet.

Related Links

See Search-Assets on page 1190.

Remove-Associations

`Remove-Associations` – Removes the business asset associations.

Synopsis

The Remove-Associations cmdlet removes the business asset associations.

Syntax

```
Remove-Associations -AppServerNameAndPort <String> [-BindingType <String>] -Bus
[-PipingEnabled [<Boolean>]] [<CommonParameters>]
```

Authorization requirements

You must have the following CCS tasks to use the cmdlet:

- View Assets
- Manage Assets and Asset Groups

You must have the permissions on the following folders to use the cmdlet:

- Asset System
- Business Assets

Description

You can remove business asset associations.

Parameters

The following table describes the parameters that the Remove-Associations cmdlet requires:

Table B-117 Remove-Associations - parameters

Switch Name	Switch Type	Data Type	Supports piping input? Yes/No	Description
AppServerName AndPort	Mandatory	String	No	The name of the application server and the port matching the binding type. The value for the parameter can be specified from the PowerShell variable as: `$AppServer NameAndPort="< AppServer Name/IP> : <Port Number Corresponding To Binding Type Set>"` Once specified , you need not specify the value again for every cmdlet in that session.

Table B-117 Remove-Associations - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? Yes/No	Description
Binding Type	Optional	String	No	A valid binding type. The default binding type is NETTCP. You can specify binding types such as HTTP, HTTPS, NETTCP. The value for the parameter can be specified from the PowerShell variable as: `$Binding Type="<NETTCP or HTTP or HTTPS>"` Once specified , you need not specify the value again for every cmdlet in that session.
BusinessAsset	Mandatory	Asset	Yes	It is a business asset. You can get the value of this parameter from the `Search-Assets` cmdlet if piping is enabled for this field.
Associations	Mandatory	Asset	Yes	A list of assets for associations with business asset.

Table B-117 Remove-Associations - parameters *(continued)*

Switch Name	Switch Type	Data Type	Supports piping input? Yes/No	Description
PipingEnabled	Optional	Boolean	Yes	The default value of this parameter is False. Set to True if output of the cmdlet required as piping inputs.

Inputs

You can pipe output of Search-Assets to the Remove-Associations cmdlet.

Outputs

The Remove-Associations cmdlet did not return any output. As a result of the successful execution of the cmdlet, the associations are removed from the business asset.

Notes

You can set AppServerNameAndPort variable only once and reuse it till the session is closed.

You can set BindingType variable only once and reuse it till the session is closed.

This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer, and OutVariable. For more information, type, **get-help about_commonparameters** on the PowerShell CLI.

Example 1

```
C:\PS > $businessAsset = Search-Assets -AssetType "Business Asset"
       -NumberOfObjectsToRetrieve 1
C:\PS > $WindowsAsset = Search-Assets -Filter {("displayname,startswith
       -SearchsubTree $True -AssetType "Windows Machine" -NumberOfObjec
C:\PS > Remove-Associations -BusinessAsset $businessAsset -Associations
```

```
Output:
Associations removed.
```

Description: The business asset and associations are retrieved from Search-Assets using proper filters and are assigned to variable $businessAsset and $WindowsAsset. These variables are used as inputs to the Remove-Associations cmdlet.

Example 2

```
    C:\PS > $businessAsset = Search-Assets -AssetType "Business Asset" -NumberC
    C:\PS > Search-Assets -Filter {("displayname,startswith,Win")} -SearchsubTr
            Remove-Associations -BusinessAsset $businessAsset
```

```
Output:
Associations removed.
```

Description: Associations are removed using piping. The output of Search-Assets is piped to Remove-Associations cmdlet.

Related Links

See Search-Assets on page 1190.

Appendix C

Reporting database

This appendix includes the following topics:

- About the Unified Data Model
- Mapping 9.0.1 tables to 10.0 views
- About the CCS Data Migration utility

About the Unified Data Model

The Control Compliance Suite Reporting database was redesigned for version 10.0. The new design is named the Unified Data Model (UDM). The UDM provides the following attributes to the database:

Extensibility — The database can accept data from the Control Compliance Suite modules and third-party applications with a minimal change. Additions to the data or updates to the data do not affect the existing data. The reports and the dashboards function in the same way.

Scalability — The model is planned and implemented to handle metrical and dimensional data for assets and users within a huge enterprise environment. The model generates reports in a timely manner.

Versatility — The model allows for customizations with a low degree of difficulty.

See “Mapping 9.0.1 tables to 10.0 views” on page 1481.

About the asset-based views

The asset-based views are generated from the data in the reporting database. The following table lists the asset-based views and their descriptions:

Table C-1 Asset-based views

View name	Description
`vAsset`	The common asset information for all asset types.
`vAssetAttributeLookup`	All asset data in a lookup format including common assets and attributes.
`vAssetResults`	Asset-based results. An example is aggregated compliance scores.
`vAssetResultsLookup`	The same data as the `vAssetResults`, but in a lookup format.
`vAssetRollup`	Asset-based rollup metrics. An example is exception counts.
`vAssetFolder`	Asset folders.
`vAssetFolderMembership`	Asset folder membership.
`vAssetGroup`	Asset groups.
`vAssetGroupMembership`	Asset group membership.
`vAssetSummary`	Summarizes the current version combining results and rollup information.

See “Mapping 9.0.1 tables to 10.0 views” on page 1481.

About the standards-based views

The standard-based views are generated from the reporting database. The following table lists the standards-based views and their descriptions:

Table C-2 Standards-based views

View name	Description
`vStandard`	Standards.
`vStandardChecks`	Checks on standards.
`vStandardChecksRollup`	Rollup metrics by check that are not associated to a specific asset.
`vStandardCheckResults`	Raw check results.

Table C-2 Standards-based views *(continued)*

View name	Description
vStandardCheckResultsWithEvidence	Raw check results including text and XML evidence.
vStandardResults	Standard aggregate and count results.
vStandardRollup	Standard metrics. An example is exception counts.
vStandardSections	Standard sections.
vStandardSummary	Current standard values that combine results and rollup information.
vStandardTags	Tags associated to standards.

See "Mapping 9.0.1 tables to 10.0 views" on page 1481.

About the asset-to-standard views

The following table lists the asset-to-standard results views and their descriptions:

Table C-3 Asset-to-standard views

View name	Description
vComplianceAssetSummary	A compliance-based view that combines assets, standards, asset results, and standard results.
vComplianceAssetSummaryLookup	The same data as the vComplianceAssetSummary but in a lookup format.

See "Mapping 9.0.1 tables to 10.0 views" on page 1481.

About the entitlement-based views

The entitlements in Control Compliance Suite facilitate the ability to monitor access rights within the organization. The Entitlements view in the console lets you efficiently gather the permissions data from the various platforms.

The following table lists the entitlement-based views and their descriptions:

Table C-4 Entitlement-based views

View name	Description
`vEntitlementControlPoint`	Entitlement control point is a version of the asset under control.
`vEntitlementReviewCycle`	A specific review cycle and the state of the review.
`vEntitlementReviewCyclePlan`	The plan that is used for the review cycle.
`vEntitlementFrequency`	The frequency that is used for the review cycle. For example, the frequency can be a weekly review or a monthly review.
`vEntitlementControlPointTrusteeMembership`	Maps a control point to a specific trustee.
`vEntitlementTrustee`	Trustee.
`vEntitlementTrusteeFlat`	A flatten view of the trustee information. The view is used in reporting.
`vEntitlementTrusteePermissionLookup`	Tracks changed permissions for a trustee
`vEntitlementTrusteeLookup`	Trustee information. For example, the read permissions for a trustee.
`vEntitlementWorkflowTrail`	Participants can provide comments during the review cycle and stores the different states of a control point in a review cycle.

See “Mapping 9.0.1 tables to 10.0 views” on page 1481.

About the policy-based views

The policy features of Control Compliance Suite let you manage, publish, and track your policies across an organization. You can also collect evidence of due care of the policy compliance. Policies include the control statements that are mapped to regulations and frameworks. The ability to map lets you discover any gaps in the current policies and lets you comply with the regulation requirements for your organization.

The following table lists the policy views and their descriptions:

Table C-5 Policy-based views

View name	Description
`vPolicy`	Policy data
`vPolicyRollup`	Policy rollup metrics
`vPolicyCategory`	Policy categories
`vPolicyClarification`	Policy clarifications
`vPolicyComment`	Policy comments
`vPolicyContentLevel`	Content level for a policy
`vPolicyContentNote`	Content notes
`vPolicyContentToStatement`	Content to statement mapping
`vPolicyControlStatement`	Control statements
`vPolicyStatementToCheck`	Control statements to check mapping
`vPolicyStatementToEvidence`	Control statement to third-party evidence mapping
`vPolicyStatementToQuestion`	Control statement to questions mapping
`vPolicyToStatement`	Policy to control statement mapping
`vPolicyToTarget`	Policy to associated groups, folders, and assets
`vPolicyUserRespones`	Policy user responses
`vPolicyTags`	Tags that are associated with the policies
`vPolicyContent`	Content
`vFrameworkName`	Content framework name
`vRegulationName`	Regulation Name lookup

See "Mapping 9.0.1 tables to 10.0 views" on page 1481.

About the user views

The views contain user specific information. The following table lists the user views and their descriptions:

Table C-6 User views

View name	Description
vUser	Users that are configured from the user management.
vUserSubject	Native explicit read permissions for objects. The objects can be asset folders.
vUserTest	Native explicit read permissions for objects. The objects can be policy or standards.
vUserAsset	Resolved users to assets. The dashboard systems use the view and the view is based on the last logon to the Web console.
vUserStandard	Resolved users to standards. The dashboard systems use the view and the view is based on the last logon to the Web console.
vUserPolicy	Resolved users to policies. The dashboard systems use the view and view is based on the last logon to the Web console.

See "Mapping 9.0.1 tables to 10.0 views" on page 1481.

About the exception views

The following table lists the exception views and their descriptions:

Table C-7 Exception views

View name	Description
vException	Exception information
vExceptionIdentity	Users that are mapped to an exception
vExceptionMembership	A map of the exceptions to the objects that they apply
vExceptionTags	Tags that are associated to exceptions

See "Mapping 9.0.1 tables to 10.0 views" on page 1481.

About the tag views

The following table lists the tag views and their descriptions::

Table C-8 Tag views

View name	Description
`vTag`	Tag definitions
`vReportTags`	Labels for the reports the international tables

See "Mapping 9.0.1 tables to 10.0 views" on page 1481.

About the third-party views

The following table lists the third-party views and their descriptions:

Table C-9 Third-party views and descriptions

View name	Description
`vThirdPartyProviders`	All of the third-party providers that are registered in the evidence system
`vThirdPartyControls`	All of the third-party controls that are registered in the evidence system and the controls that are mapped to content
`vThirdPartyEvidence`	Provider imported evidence
`vThirdPartyEvidenceLookup`	Provider imported flattened custom XML evidence that is flattened

See "Mapping 9.0.1 tables to 10.0 views" on page 1481.

Mapping 9.0.1 tables to 10.0 views

The version 10.0 database uses views to display customer information. A view is a virtual table that is an abstract data structure.

This data structure has the following advantages:

- Views can display a subset of a table's data.
- Views can join and simplify multiple tables into one virtual table.
- Views can display aggregated data easily.

- Views can hide the complexity of the underlying database.
- Views can provide another level of security because you can add permissions to views.

Table C-10 displays the result of migrating 9.0.1 tables to 10.0 views. A column may have multiple listings for either the tables or the views because the data in the tables are equivalent.

Table C-10 Mapping 9.0.1 tables to 10.0 views

9.0.1 table	10.0 view
Asset	vAsset
Asset_Detail	vAssetAttributesLookup
BO_AssetToTags	vAssetTags
Checks	vStandardChecks
EM_ReviewCycle_FACT	vEntitlementWorkflowTrail
EM_ControlPoint_Fact	vControlPoint
EM_ControlPoint_Fact	vControlPointSnapshot
EM_Entitlement_FACT	vEntitylementTrusteeLookup, vEntitylementTrusteeFlat
EM_EntitlementChange_FACT	vEntitylementTrusteePermissionLookup
EM_Entitlement_FACT	vEntitylementTrustee
EM_FrequencySettings	vEntitlementReviewFrequency
EM_ReviewCycle	vEntitlementReviewCycle
EM_ReviewCycleSettings	vEntitlementReviewCyclePlan
CM_WorkflowTrail_Entry(where Type is control point)	vEntitlementWorkflowTrail
TP_Fact_Table	vThirdPartyEvidence, vThirdPartyEvidenceLookup
PM_StatementCustomEvidenceProvider	vThirdPartyControls, vThirdPartyProviders

Table C-10 Mapping 9.0.1 tables to 10.0 views *(continued)*

9.0.1 table	10.0 view
EX_AssociationFor	vExceptionStandardCheckMapping
EX_AssociationTo	vExceptionStandardCheckMapping
EX_Exceptions	vException
EX_ExceptionAssociationFor	vExceptionMembership
EX_ExceptionAssociationTo	vExceptionMembership
EX_Identity	vExceptionIdentity
PM_Clarification	vPolicyClarification
PM_Comment	vPolicyComment
PM_Content	vPolicyContent
PM_Content	vPolicyContent
PM_ContentStatement	vPolicyContentToStatement
PM_ContentStatementLevel	HierarchyRelationship
PM_Level	vPolicyContentLevel
PM_MergedStatement	N/A
PM_Note	vPolicyContentNote
PM_Policy	vPolicy
PM_PolicyStatement	vPolicyToStatement
PM_PolicyTargetAssetCollection	vPolicyToResolvedAsset
PM_Statement	vPolicyControlStatement
PM_StatementCheck	vPolicyStatementToCheck
PM_StatementEntitlement	N/A
PM_StatementQuestion	vPolicyStatementToQuestion
PM_UserResponse	vPolicyUserResponse

Table C-10 Mapping 9.0.1 tables to 10.0 views *(continued)*

9.0.1 table	10.0 view

`Asset_Std_Summ,`
`Asset_Std_Summ_Archive`
	`vComplianceAssetSummary,`
	`vComplianceAssetSummaryLookup`

`Asset_Summary,`
`Asset_Summary_Archive`
	`vAssetResults,`
	`vAssetResultsLookup`

`Fact_Table,`
`Fact_Table_Archive`
	`vStandardCheckResults,`
	`vStandardCheckResultsLookup`

`EvalChecksToEvidence,`
`EvalChecksToEvidence_Archive`
	`vStandardCheckResultsWithEvidence`

`Standards_Summary,`
`Standards_Summary_Archive`
	`vStandardSummary`

`Sections`	`vStandardSections`
`Evaluation_Jobs`	`N/A`
`Standards`	`vStandard`
`BO_Tags`	`vTag`
`CM_UserMgmt_SecurityPrincipals`	`vUser`

About the CCS Data Migration utility

During the upgrade process of a CCS installation to CCS 11.0, you must migrate the data of the various CCS modules. Use the CCS Data Migration utility to migrate the data of the applications such as, Extended Evidence Sources, Reports, Dashboard, Assets, and Policies. The CCS Data Migration utility is an executable, MigrationUtility.exe and is located in the <Install Directory>\Application Server directory of the product.

You are prompted to run the CCS Data Migration utility after the upgrade process, or you can choose to run the utility at a later stage.

The CCS Data Migration utility extracts the SQL connection details from the Application Server and shuts down the Application Server Service. After the migration is complete, the Application Server Service is automatically restarted.

The CCS Data Migration utility lets you migrate data of the following applications:

- Evidence Management
- Reports and Dashboards data
- Asset data
- Policies

Note: In case of an upgrade, you will not be able to use the CCS application until you have migrated the data of the previous CCS installation.

Prerequisites for running the CCS Data Migration Utility

You must ensure the following before running the CCS Data Migration utility:

- Take a backup of the Production (CSM_DB), Reporting (CSM_Reports), and Evidence (CSM_EvidenceDB) databases.
- Ensure that no jobs are running when you run the CCS Data Migration Utility.
- Ensure that you run the CCS Data Migration Utility in a user context with Application Server credentials.
  See "Configuring the application server credentials" on page 307.
- Set the value of the Index creation memory (in KB) to 0 for the SQL server. The Index creation memory setting can be done through the Memory page of the SQL Server Properties dialog box.
  See "Setting the value of Index Creation Memory" on page 1485.
- Configure and activate the SQL Server Service Broker for successful migration of the Reporting database, CSM_Reports.
  See "Configuring the SQL Server Service Broker" on page 1486.
- Change tempdb and Auto Growth settings on the production database and the reporting database server.
  See "Changing the settings of tempdb" on page 1486.

Setting the value of Index Creation Memory

To set the value of Index Creation Memory

1. In the SQL Server Management Studio, right-click the SQL server node.
2. Click **Properties**, and click the **Memory** tab.
3. In other memory options, set Index creation memory to 0.
4. Click **OK**.

Configuring the SQL Server Service Broker

By default, CCS configures the SQL Server Service Broker. If you have configured the SQL Server Service Broker for any specific scenario, then you must execute the stored procedure, spManageUDMSQLBroker.

The scenarios for which the configuration of the SQL Server Service Broker can change are as follows:

- The reporting database is installed or upgraded by a user who is not in the role of a dbo.
- The reporting database is recovered from the back-up.
- The user credentials that are configured to access or synchronize the reporting database have changed.

You must execute the stored procedure, spManageUDMSQLBroker to activate and configure the SQL Server Service Broker for the specific user context. You must execute the stored procedure in the user context that has the privileges to run the database synchronization process.

To enable SQL broker

1. In the SQL Server Management Studio, expand **Databases**.
2. Right-click **CSM_Reports**, and click **New Query**.
3. Run the following command:

```
exec dbo.spManageUDMSQLBroker 1, <Reporting user name>,CSM_Reports
```

See "Prerequisites for running the CCS Data Migration Utility" on page 1485.

Changing the settings of tempdb

Before running the CCS Data Migration Utility, you must change the initial size of tempdb on the reporting database (CSM_Reports) server. You can avoid memory related errors while running the reporting synchronization job under peak load condition, by changing these settings.

Symantec recommends the following settings for the initial size of tempdb for deployments of different scales:

Small scale deployment	1 GB Autogrowth should be set at 10% of tempdb
Medium and large scale deployment	5 GB Autogrowth should be set at 10% of tempdb

Very large scale deployment	20 GB Autogrowth should be set at 10% of tempdb

For more information about the tempdb settings, refer to *Temp DB recommendations in the Planning and Deployment Guide*.

To change the settings of tempdb

1. Connect to the SQL database.
2. Expand Databases > System Databases > tempdb.
3. Right click tempdb and select Properties.
4. Click Files. Set the Initial size of tempdb to 1024 MB. The default value for Auto Growth is 10% and it is the recommended value.

Running the CCS Data Migration utility

To run the CCS Data Migration Utility

1. Navigate to the <Install Directory>\Application Server.

   By default, the <Install Directory> is C:\Program Files\Symantec\CCS folder.

2. Double-click **MigrationUtility.exe**.

   In the **Migrate Application Data** dialog box, by default, all the applications are checked.

   Note: You must not uncheck the option, **Reports and Dashboards data** in the utility.

3. Click **Migrate** to start the database migration process.

   The Evidence Management, Reports and Dashboards data, Asset data, and Policies are migrated by the utility. You can view the progress of the migration in the Status pane.

   The status pane also shows the status of post migration operations. For the Reports and Dashboards data, the post migration operation includes triggering of the synchronization job for the reporting database. You can track the status of the synchronization job through the jobs workspace.

4. After migration is complete, click **Finish**.

   In case of an error, click **View Errors** to view the error details.

See “About the CCS Data Migration utility” on page 1484.

Appendix D

Troubleshooting

This appendix includes the following topics:

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

- Control Compliance Suite configuration
- Asset import
- Data collection
- Control Compliance Suite Console and Web Portal
- Symantec ESM

Deployment and upgrade troubleshooting

The following possible problems can occur when you deploy the Control Compliance Suite.

- Failed Directory Server Installation
  See "Failed Directory Server Installation - Troubleshooting" on page 1491.
- Certificate does not match specified computer during deployment
  See "Certificate does not match a specified computer during deployment - Troubleshooting" on page 1491.
- Application Server Installation Wizard rejects Directory Server credentials
  See " Application Server installation wizard rejects the Directory Server credentials - Troubleshooting" on page 1492.
- Application Server, Directory Server, or CCS Manager fail to start
  See "Application Server, Directory Server, or CCS Manager fail to start - Troubleshooting" on page 1492.
- When you install with Remote Desktop Connection, installation logs are deleted when the user logs off
  See "Installation logs are deleted when the user logs off after using Remote Desktop Connection to install - Troubleshooting" on page 1493.
- During the installation, an error message indicates that the state of the secure channel cannot be verified
  See "State of the secure channel cannot be verified during installation - Troubleshooting" on page 1494.
- When you install the Control Compliance Suite Console, an error message appears indicating that the Web server cannot be located.
  See "Unable to contact the Web server when installing the Control Compliance Suite Console - Troubleshooting" on page 1494.
- When you install the Control Compliance Suite components on a virtual machine, an error warns that your screen does not meet the minimum required size.

See "Warning appears about the minimum required screen resolution - Troubleshooting" on page 1494.

- Error occurs when upgrading RMS Console and Information Server
- Migration fails if Numeric_Round_Abort is set on SQL the server

Failed Directory Server Installation - Troubleshooting

When you deploy the Control Compliance Suite (CCS), the CCS directory may fail to correctly install. If this error occurs, one of the following may be the cause:

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 CCS.
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.

Certificate does not match a specified computer during deployment - Troubleshooting

When you deploy the Control Compliance Suite (CCS), the certificate may not match the specified computer. If this error occurs, one of the following may be the cause:

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 installation wizard rejects the Directory Server credentials - Troubleshooting

When you deploy the Control Compliance Suite (CCS), the Application Server installation wizard may not accept the Directory Server credentials you supply. If this error occurs, one of the following may be the cause:

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.

Application Server, Directory Server, or CCS Manager fail to start - Troubleshooting

When you deploy the Control Compliance Suite (CCS), the Application Server, the CCS directory, or a CCS Manager instance may fail to start correctly. If this error occurs, the following may be the cause:

Host computer does not have Internet connectivity or connection to the VeriSign Web server is blocked.	Try any of the following solutions: ■ Provide access to the VeriSign Web server the first time the service starts. ■ Disable certificate checking for all components on the host. ■ Manually download the Certificate Revocation List from VeriSign and install it on the host. ■ In .NET Framework 3.5 there is a configuration option that allows bypassing the Authenticode verification by adding the following entry in the app.config file: `<configuration> <runtime> <generatePublisherEvidence enabled="false"/> </runtime> </configuration>` For example, in a distributed setup, the Directory Support Service (DSS) is installed but after installation, the DSS, and Encryption Management Services do not start. To start the services, you can edit the `Symantec.CSM.DSS.Service.exe.config` file and `Symantec.CSM.EncryptionManagement.Service.exe.config` file and add the following lines: `<configuration> <runtime> <generatePublisherEvidence enabled="false"/> </runtime> </configuration>`

Installation logs are deleted when the user logs off after using Remote Desktop Connection to install - Troubleshooting

If you use Windows Remote Desktop Connection to install the Control Compliance Suite (CCS) components, the installation logs are deleted when you log off the computer.

Installation 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.

To retain these logs, you must manually copy the log file to another folder after the installation is complete but before logging out.

State of the secure channel cannot be verified during installation - Troubleshooting

When you deploy the Control Compliance Suite (CCS), an error message may appear that indicates that the state of the secure channel cannot be verified. If this error message appears, it indicates that the computer has lost its secure channel with the domain.

To correct the issue, you must rejoin the computer to the domain.

SSPI context cannot be generated during installation - Troubleshooting

When you deploy the Control Compliance Suite (CCS), an error message may appear that indicates that the SSPI context cannot be generated. The error message indicates that the computer that hosts the Microsoft SQL Server has lost its secure channel with the domain.

To correct the issue, you must rejoin the computer to the domain. You can then install CCS.

Unable to contact the Web server when installing the Control Compliance Suite Console - Troubleshooting

When you install the Control Compliance Suite (CCS) Console an error message may indicate that the installer is unable to contact the Web server . If this message appears, you should use the IP address of the Web server instead of the server name.

Warning appears about the minimum required screen resolution - Troubleshooting

When you install the Control Compliance Suite (CCS) components on a virtual machine, a warning may appear that the screen resolution is below the minimum required if the virtual machine is minimized. If this error appears, repeat the installation with the virtual machine unminimized.

Configuration troubleshooting

Table D-1 lists possible configuration problems and their associated causes and resolutions.

Table D-1 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.
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.

User is unable to start the Certificate Management Console - Troubleshooting

When you deploy the Control Compliance Suite (CCS), the Application Server, the CCS directory, or a CCS Manager instance may fail to start correctly. If this error occurs, the following may be the cause:

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 CCS Administrator.

Synchronization jobs fail to complete after migration - Troubleshooting

If you use the Control Compliance Suite (CCS) Migration Utility, then start the CCS Console and start a Global Synchronization job, the synchronization jobs may fail to complete.

This error occurs because the synchronization job requires additional SQL Server permissions.

You should use the SQL Manager to assign the `EXECUTE` permission on the `sp_upgradestats` object to the database owner (`dbo`) of the `CSM_Reports` reporting database.

Asset import troubleshooting

The following table lists possible asset import problems and their associated causes and resolutions.

Asset imports fail to complete - Troubleshooting

When you perform an Asset import, the import job may fail to complete correctly. If this error occurs, one of the following may be the cause:

Asset imports fail to complete.	Verify that the asset system is properly configured. See "About assets" on page 61. Verify that the reconciliation rules are correctly configured. See "Creating reconciliation rules without manual review" on page 437.
Not all expected assets are imported.	Verify that the scope of the Asset Import job is valid for the given asset type. See "About scopes in asset import" on page 481.
Not all assets of a given type are collected.	Verify that the data collector for the given asset type is properly configured.
The error message "**An Error occurred in Data Query activity: Unable to retrieve list of Assets from ADAM: No Assets were resolved from the directory, either due to insufficient permissions or an invalid job definition**" appears during asset import job processing.	Verify that the Application Server service account is trusted for delegation. Verify that the Service Principal Names are properly registered.

Asset import jobs from a single site run slowly - Troubleshooting

When you perform an Asset import, the import jobs from a single site may run more slowly than jobs from other sites. If a slow import happens, the following may be the cause:

One of the CCS Managers in a Collector role that retrieves data from the site has failed.	Correct the fault that prevents the CCS Manager from operating properly. Temporarily unregister the CCS Manager, then register it again when repair is complete. Temporarily move the CCS Manager to a site with no assets.

See “ Unregistering a CCS Manager ” on page 314.

Asset import jobs fail and report an exception - Troubleshooting

When you perform an Asset import, the Asset import job may fail with the following exception:

```
An error occurred in the data query activity. Unable to retrieve the
list of assets from ADAM. No assets were resolved from the directory,
either due to insufficient permissions or invalid job definition.
```

This error indicates that the asset types that you selected in the “Limit Asset Import Scope” dialog box do not match. The selected types should match the asset types that are contained in the asset folder or asset group that is used for asset import.

To correct the error, you should limit the asset import scope. You should include only the asset types that are contained in the asset folder or the asset group that is used for asset import.

For example, consider the following case:

- You import Windows machines.
- You use the “All Windows Machines” asset group.
- The scope does not contain any domains, only Windows machines.
- The scope that you select in the **Limit Asset Import Scope** dialog box contains only domains.

In this case, the asset import fails to resolve the assets unless you select “Machines” in the “Limit Asset Import Scope” dialog box.

See “About scopes in asset import” on page 481.

Deleted ODBC data locations appear in the CCS Manager settings - Troubleshooting

When a user creates an ODBC data location and imports assets from the ODBC data location, then deletes the ODBC data location, the location may still appear in the CCS Manager settings.

If another user uses the data location, Asset Import jobs will fail, since the location no longer exists.

The user who created the ODBC data location or a Control Compliance Suite (CCS) Administrator should use the DPS Settings dialog to manually delete the platform and data location.

Data collection troubleshooting

The following table lists possible data collection problems and their associated causes and resolutions.

Data collection jobs fail to run - Troubleshooting

When you run a data collection job, the data collection job may fail to run properly at the scheduled time. If this error occurs, one of the following may be the cause:

Scheduled data collection jobs fail to run at the scheduled time.	Verify that the scheduling user password is properly updated in user management.
Data collection jobs fail to run.	Verify that the Application Server credentials are correct.
Data collection jobs fail to run.	Verify that the Application Server and Directory Server credentials are both Local Administrators.
All jobs fail to run.	Verify that the Production database host works properly.
Jobs fail to run, and the error “Dispatcher.SimpleDispatch” appears.	Verify that the Symantec.CSM.DSS SPN is associated with only one account.
Jobs fail to run.	Verify that the SPNs have been created properly. Also verify that the Service Name portion of the SPN for the Directory Service matches what is specified in the AppServerService.exe.config file.

Data collection jobs from a single site run slowly - Troubleshooting

When you run data collection jobs, you may find that all data collection jobs from a single site run slowly.

One possible cause of this error is that one of the CCS Manager Collectors that retrieve data from the site has failed. If this error occurs, you must correct the fault that prevents the DPS from operating correctly.

While you repair the error, you should remove the DPS from the site. If the failed DPS is associated with the site, the DPS Load Balancers continue to assign jobs to the DPS Collector. Until the DPS Collector is unable to retrieve the data and times out, the DPS Load Balancer does not reassign the job to another DPS Collector.

To remove the DPS Collector, you can do one of the following:

- Temporarily unregister the DPS, then register it again when repair is complete.
- Temporarily move the DPS to a site with no assets.

Exception appears during data collection for Oracle assets - Troubleshooting

When you run a data collection job, a `System.OutOfMemory` exception may appear when you collect data from Oracle assets.

This error appears because data that the Control Compliance Suite (CCS) collects from Oracle Assets uses chained data queries. These queries are very memory-intensive.

To avoid this error, you should limit Oracle queries to 1000 assets per job.

Data collection jobs fail with the error - Troubleshooting`Login failed for user`

When a data collection job runs, it may fail, and the error message `Login failed for user` may appear. If this error occurs, one of the following may be the cause:

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.
The Account that is used for the CCS Manager is not a domain account.	Use a domain account for the CCS Manager .

Data collection jobs fail with an exception - Troubleshooting

When you run data collection jobs, a data collection job may fail, and the following error message may appear:

```
An error occured in the evaluation activity.
Unable to retrieve the list of assets from ADAM.
No assets were resolved from the directory, either due to
insufficient permissions or invalid job definition.
```

If this error appears, it means that the standard that is associate with the asset group does not contain a target type that matches the assets in the asset group or the asset folder.

To correct the error, you should use the asset groups that contains the assets of the target type that the standard contains.

Consider the following example:

You run a data collection job with the standard that contains only “IIS Web Sites” target types. You use “All Windows Machines” asset group as to run the data collection. In this case, the data collection job fails unless you select an asset group that contains IIS Web Sites.

“Computer Unreachable” errors appear for Windows computers that do not have Internet Information Services installed - Troubleshooting

A data collection job can include both computers with the Microsoft Internet Information Services (IIS) Manager installed and computers without IIS installed. If you run a standard against that data collection job that includes IIS checks, the error “Computer Unreachable” appears for computers in the scope that do not have IIS installed.

Since the computer does not include IIS, the Control Compliance Suite (CCS) is unable to determine if the computer is reachable and that it does not collect data for non-IIS checks.

You should restructure your data collection job to separate out assets with IIS installed from the ones without IIS installed and recollect the data for the respective standards and assets.

Console and Web Console troubleshooting

The following errors can occur when using the Control Compliance Suite (CCS) Console and Web Console:

- The user cannot open or launch the help topics from the Topics section of SymHelp.
- When installing the Control Compliance Suite Console, an error message appears indicating that the Web Server cannot be located.

  See "Unable to contact the Web server when installing the Control Compliance Suite Console - Troubleshooting" on page 1494.
- The user cannot start the Control Compliance Suite Console
- The Web Console is unable to connect to the Response Assessment module
- The Web Console does not correctly display Response Assessment module pages
- Configuration changes do not appear
- The correct time does not appear on reports
- Reports may cause a system slowdown or reports may fail
- HTTP Error 401.1 - Unauthorized: Access is denied when you open the Web Console
- Blank reports may appear
- Error viewing dashboard on Web Console
- Custom asset type does not appear in the console
- Message "The Server is not operational" appears in the console
- Message "The Server is not operational" appears in the console
- -1 value is displayed in a chart for an asset risk score
- Message "Error in reading policy data" appears
- Dashboard panel data is incorrect
- Expected data is not displayed in the policy panels
- Launching the Control Compliance Suite Console is slow
- Message "Login failed for user <username>" appears
- Delay in permission changes in the Web Console
- Web Console does not start after upgrading to version 10.0
- Drill down dashboards do not work unless the settings for Internet Explorer are modified

User cannot start the Control Compliance Suite Console - Troubleshooting

If a user is unable to start the Control Compliance Suite (CCS) Console, one of the following may be the cause:

The user cannot locate the CCS Console installer.	The installer is hosted on the Application Server in the \\Application Server Name\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.
The console is unable to successfully start.	Verify that the Application Server service account is trusted for delegation. Verify that the Service Principal Names are properly registered.

Unable to launch help topics from the Topics section of the SymHelp console - Troubleshooting

When you try to launch a topic from the Topics section of the SymHelp console, the topic may not launch or may not display the contents.

This may occur if the Active Scripting is not enabled in your browser.

Enable Active Scripting in the browser. Refer to the following link to enable Active Scripting.

http://support.microsoft.com/gp/howtoscript

The Web Console is unable to connect to the Response Assessment module - Troubleshooting

The Web Console may be able to connect to the Response Assessment module. If this occurs, one of the following may be the cause:

Web Console is not configured to connect to the Response Assessment module.	Configure the Web Console to connect to the Response Assessment module. **Note:** You configure the Web Console to connect to the Response Assessment Module when you install the Web Console.

All jobs fail to run.	Verify that the Production database host works properly.

The Web Console does not correctly display Response Assessment module pages - Troubleshooting

The Web Console may not correctly display Response Assessment module pages.

One possible cause for this is that the Internet Explorer Enhanced Security Components are installed and cookies are blocked on the Web Console Internet Information Services (IIS) Manager.

For the Response Assessment module to function correctly, you must allow the Web Console IIS Manager to set cookies.

The configuration changes do not appear - Troubleshooting

The Control Compliance Suite (CCS) supports multiple simultaneous users. In certain circumstances, a user can make changes that adversely affect another user. If multiple users simultaneously make changes to the same configuration settings, only the changes made by the first user take effect.

If this happens, 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 - Troubleshooting

When you run a report job, the correct time may not appear on generated reports if the time or locale setting was changed on the Application Server host.

To correct this error, you should do the following:

- Restart the Application Server service
- Restart the Control Compliance Suite (CCS) Console
- Run the **Reporting Database Synchronization** job

Reports cause a system slowdown or reports fail - Troubleshooting

When a user runs a report job, the reports may cause a system slowdown or reports may fail completely.

This error may be caused when the complexity of the report exceeds the limits of the report engine the Control Compliance Suite (CCS) uses.

If it occurs, the only solution is to reduce the complexity of the report.

`HTTP Error 401.1 - Unauthorized: Access is denied` appears when you open the Web Console - Troubleshooting

The error `HTTP Error 401.1 - Unauthorized: Access is denied` may appear when you connect to the Web Console.

If this error occurs, the Service Principal Names (SPNs) used by the Web Console may be misconfigured.

To correct the error, you should properly configure the Service Principal Names (SPNs).

See http://support.microsoft.com/kb/871179

Blank reports appear - Troubleshooting

When you run a report, the report contents may not appear. The report appears to be blank.

This error occurs because the **Reporting Database Synchronization** job must run before you can run a report.

You should 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.

Error appears while viewing a dashboard on the Web Console - Troubleshooting

The error **System.DirectoryServices.DirectoryServicesCOMException** may appear when you open a dashboard panel in the Web Console.

This error can occur because you have the Service Principal Names (SPNs) set incorrectly on the Control Compliance Suite (CCS) Application Server.

You should use the `<install directory>\Application server\CCSSPNUtil.exe` utility to verify that the SPNs are set correctly for the Application Server, and that there are no duplicate SPNs set.

Cannot create a custom asset type - Troubleshooting

If you use the **Add new asset type** wizard to create a custom asset type, the custom entity schema may not appear in the wizard. The failure occurs because Control Compliance Suite (CCS) Console is unable to successfully transfer the custom entity schema XML files from the Application Server.

This error can occur if the Application Server has not completed loading the custom entity schema. This error only occurs immediately after the Application Server starts and the service has not completed loading. The error does not appear if you use the Console on the same computer that hosts the Application Server. It does appear if you use the Console on another computer.

You should close the CCS Console and wait until the Application Server completes its startup sequence. The startup sequence takes less than 5 minutes to complete. When the Application Server startup is complete, restart the CCS Console, and the custom entity schema information appears. You can use the **Add new asset type** wizard to create a custom asset type with the custom schema.

Message “The server is not operational” appears in the console - Troubleshooting

When the user performs an action in the Control Compliance Suite(CCS) Console, the error message “The server is not operational” can appear.

This message appears because the CCS components are unable to contact the CCS Directory Server or the CCS Directory Server is busy.

The CCS Administrator can correct the issue. The CCS Administrator should do the following:

- Check the socket connection state on the CCS Directory Server host.
- Change the timeouts for the CCS Directory Server.
- Change the maximum number of socket connections for the CCS Directory Server.

To check the socket connection state on the CCS Directory Server host, you use the `NETSTAT` command from the command line. If one of the sockets is in a waiting state, the command output should be similar to the following:

```
TCP    <CCS_Directory_Server_Name>:<Port> TIME_WAIT
```

You should use the Registry Editor to change the value of `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCPIP\Parameters\TCPTimedWaitDelay` to 35 seconds. If the key is not present, please add it to the registry as REG_DWORD type keys.

You should also use the Registry Editor to change the value of `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCPIP\Parameters\MaxUserPort` to 65530. This change increases the number of available socket connections on the CCS Directory Server. If the key is not present, please add it to the registry as REG_DWORD type keys.

Once you have completed these changes, you should restart the CCS Directory Server and retry the action in the CCS Console.

Message “Login failed for user *<user name>*” appears in the Web Console - Troubleshooting

When you log on to the Control Compliance Suite (CCS) Web Console, the error message “Login failed for user *<user name>*” may appear. This error appears if the SQL credentials used for the production database or the reporting database change.

If this error occurs, the CCS Administrator should use the Internet Information Services (IIS) Manager to recycle the `CCS_WebAppPool` service on the CCS Web Console server.

-1 value is displayed in a chart for an asset risk score - Troubleshooting

If you select asset risk score as the **Measure** for a panel, you may see a -1 score in the chart for certain assets.

The -1 score is generated in the following conditions:

- An evaluated asset that does not have any data collected on the checks
- An asset with 100% compliance

You can correct the score by adding the following **Subject** settings:

Attribute	Asset risk score
Operator	is not equal to
Values	-1

Error message appears while navigating to the Policies page in the Web Console - Troubleshooting

When you navigate to the Policies page in the Web console, the error message "Error in reading policy data" may appear for any of the following reasons:

- SPNs are not configured correctly
- IIS 7 computer is not set for delegation
- HTTP SPN is set on IIS 7 computer that is already configured to be trusted for delegation.

HTTP SPN is not required on IIS 7 computers as the IIS 7 computers are configured for Kerberos authentication. However, you must set HTTP SPN on IIS 7 in the following cases:

- IIS 7 is used with Kernel Mode Authentication disabled
- IIS 7 is used with Kernel Mode Authentication enabled and the useAppPoolCredentials attribute set to TRUE.

If you have installed the CCS Directory Server and the CCS Application Server on separate computers, you must configure the IIS Server (CCS Application Server) and the Directory Support Service for constrained delegation. For more information on configuring constrained delegation, see the *Symantec Control Compliance Suite Installation Guide*.

You must set HTTP SPN on Windows Server 2008 computers where the IIS Host Header and the CCS Application Server name are not same.

Dashboard panel data is incorrect - Troubleshooting

You have created a standard, asset, or policy or you have imported a standard, asset, or policy. You have run the evaluation job. You create a dashboard panel, but the data is not displayed or the data is incorrect.

You must run the **Reporting Database Synchronization** job in the Control Compliance Suite CCS Console. The job is in the **Monitor** > **Jobs** view. The data may not display correctly if the job has not been run.

Expected data is not displayed in the policy panels - Troubleshooting

You have created a policy, mapped users, and published the policy. You open a policy panel in **Web Console** > **Dashboards** > **Panels** and you do not see the expected data.

Verify that the following jobs have run:

- **Policy and Mandates Metrics Computation**
- **Reporting Database Synchronization**
- Daily policies

These jobs are scheduled to run once a day. You can manually start the **Policy and Mandates Metrics Computation** job and the **Reporting Database Synchronization** job. The jobs are located in **Monitor** > **Jobs** view of the CCS Console.

The daily policies job updates the following information:

- "Not read' audience

- Expiring policies per date
- Maintaining the review or approve by dates
- Mappings in synch with check deletions
- Detecting expired policy asset exceptions

You can start the policies job by resetting the start time. You can set the time in **Settings** > **General** > **Policies** > **Run the daily policies job at**. If you change the time, the job starts at that time until it is changed.

Launching the Control Compliance Suite Console is slow - Troubleshooting

Launching the CCS console can be slow on a Windows 2003 or 2008 server with no Internet connectivity.

Do the following steps to improve the performance:

- Open the Internet Explorer browser on the computer that experiences the performance issue.
- Go to Internet Option and select the Advanced tab.
- Uncheck the box "check for publisher's revocation list”.

Once the changes are made, the CCS console opens quickly.

Error message appears on the Control Compliance Suite console or in the logs of DPS - Troubleshooting

When you connect to the reporting database in a user context that has insufficient rights on the reporting database, an error message “Login failed for user <username>” appears on the Control Compliance Suite console or in the logs of the DPS in a reporting role:

To correct this issue, you must do the following

- Check if you can connect to the SQL Server from the Application Server and DPS using the same user context
- Verify whether the user context used to connect to the reporting database (CSM_Reports) is having the role of db_owner. Else change the user context or add the user context to the role of db_owner in the reporting database.

Delay in permission changes in the Web Console - Troubleshooting

When a user's permissions change in an Active Directory group, the user must do the following:

- Wait the default time before the change is disseminated through the system.
- Log off and logon to retrieve the new permissions.

A user sees the permission change in the Web Console dashboards after a default 60-minute delay .

You can add this setting to the web.config file to change the default delay time:

```
<add key="DynamicDashboard:GroupMembershipUpdateTimeSpan" value="2"/>
```

The value is measured in minutes. You must use a whole number.

Web Console does not start after upgrading to version 10.0 - Troubleshooting

If the Web console does not start after you upgrade to version 10.0 and if the error message `System.Runtime.InteropServices.COMException (0x8007203A): The server is not operational` appears in the Web console logs on the CCS Web server computer, then do the following:

The Control Compliance Suite (CCS) Administrator should use the Internet Information Services (IIS) Manager to recycle the CCS_WebAppPool service on the CCS Web Console server.

On a remote computer, CCS console does not launch from the desktop shortcut -Troubleshooting

The issue and the workaround are as follows:

On the remote computer, the CCS console does not launch using the desktop shortcut	The workaround for the issue is as follows: ■ Uninstall the CCS Console ■ Uninstall all the versions of .NET framework ■ Install .NET Framework 3.5 SP1 ■ Launch the CCS Console remotely using the following URL: http://<Machine name or FQDN name of Application Server>/CCS_Web/Downloads/GetConsole.aspx ■ Double-click the shortcut for the CCS Console that is created on the desktop.

The error, Unable to load configuration file is displayed during CCS console launch from a remote computer - Troubleshooting

During launch of the CCS console from the remote computer, the following error can occur:

```
Unable to launch the console

Details:Error occurred while downloading application configuration
file
```

As a workaround for this issue you can do the following:

- Verify whether the Application Server Service is running
- Ensure that the SPN settings are correct
  For more details about the SPN settings, refer to the topic, Configuring Service Principal Names of the *CCS Installation Guide*.

Drill down dashboards do not work unless the settings for Internet Explorer are modified - Troubleshooting

In dynamic dashboards, the drill down does not work unless the settings for Internet Explorer are changed.

This may occur if the Active Scripting is not enabled in your browser.

Enable Active Scripting in the browser. Refer to the following link to enable Active Scripting.

http://support.microsoft.com/gp/howtoscript

Policy Module troubleshooting

The following errors can occur when you use the Policy Module:

Cannot assign a reviewer or approver for a policy.

See "Cannot assign a reviewer or approver for a policy - Troubleshooting" on page 1511.

Cannot assign a reviewer or approver for a policy - Troubleshooting

When you create a new policy, if no user has been explicitly assigned the Policy Reviewer or Policy Approver role, you cannot assign a reviewer or approver to the policy.

By default no user has been assigned to the Policy Reviewer role or the Policy Approver role. Earlier versions of the Control Compliance Suite (CCS) automatically assigned any users that you assigned to the CCS Administrator role were also assigned to the Policy Reviewer and Policy Approver roles automatically. This automatic assignment no longer occurs.

You must manually assign one or more users to the Policy Reviewer and Policy Approver roles, then assign the users to the policies you create.

Reports troubleshooting

The following errors can occur during report generation:

- Failed report generation job for an Entitlements Management report

  See "Failed report generation job for an Entitlements Management report - Troubleshooting" on page 1511.
- Performance slowdown in execution of report generation jobs

  See "Performance slowdown in execution of report generation jobs - Troubleshooting" on page 1512.
- Server memory error in a reporting database synchronization job

  See "Server memory error in a reporting database synchronization job - Troubleshooting" on page 1513.

Failed report generation job for an Entitlements Management report - Troubleshooting

When you launch a report generation job for an Entitlements Management report, where data owner is included in the filter, the reporting job fails with the error

“An error occurred in ReportDashboardActivity: There are no DPS Load Balancers available for job execution".

To resolve this issue, you must do the following:

1. Launch the Edit wizard for the EM report generation job.
2. Save the job without making any changes.
3. Execute the job.

   The EM report generation job runs successfully without any error.

Performance slowdown in execution of report generation jobs - Troubleshooting

While you run the report generation jobs, it is possible that the performance degrades over a period of time . The performance degradation happens when the report generation jobs fail or are cancelled during previous runs. The temporary data that is generated in the report generation job staging tables is not cleaned up when the report generation jobs fail or are cancelled. This results in performance degradation due to accumulation of data in the temporary staging tables.

Use the CleanStagingTables utility to clean the data in the temporary staging tables. The CleanStagingTables utility is located in the <install dir>\ CCS\Reporting and Analytics\Application Server.

Prerequisites to run the CleanStagingTables utility - Troubleshooting

The prerequisites to run the CleanStagingTables utility are as follows:

- The Application Server service must be running.
- No reporting jobs must be running.

See “Performance slowdown in execution of report generation jobs - Troubleshooting” on page 1512.

Running the CleanStagingTables utility - Troubleshooting

To run the CleanStagingTables utility

1. Navigate to <install dir>\ CCS\Reporting and Analytics\Application Server.
2. Double click the CleanStagingTables utility.
3. The following message is displayed on the console: Ensure no report jobs are running. All the staging tables will be cleaned up. Do you want to continue (Y/N?)

   If you enter N, the utility stops and exits.

   If you enter Y, the console displays the progress of the utility.

   The utility exits after the cleanup of staging tables is complete.

See "Prerequisites to run the CleanStagingTables utility - Troubleshooting" on page 1512.

See "Performance slowdown in execution of report generation jobs - Troubleshooting" on page 1512.

Server memory error in a reporting database synchronization job - Troubleshooting

When the error "XML document could not be created because server memory is very low" appears in a reporting database synchronization job, you must change the settings of the tempdb on the production database (CSM_DB) and the reporting database (CSM_Reports).

To change the settings of tempdb:

1. Connect to SQL database.
2. Expand Databases > System Databases > tempdb.
3. Right click tempdb and select **Properties**.
4. Click **Files**. Set the initial size of tempdb to 1024 MB. The default value for Autogrowth is 10% and it is the recommended value.

If the error still persists, then restart the SQL server on the production database (CSM_DB) and the reporting database (CSM_Reports).

SCAP Content troubleshooting

The following error occurs when you import SCAP content:

- A time-out error occurs during SCAP content import

Improper display of SCAP Content view during first time launch of CCS console - Troubleshooting

In certain scenarios, after installation of CCS, when you navigate to **Manage > SCAP Content** view of the console for the first time, the view is displayed improperly. The **SCAP Content** view displays only the details pane while the table pane of the view is hidden. You must drag the details pane section downwards and reduce it to view the table pane section.

The cause of the issue and the workaround are as follows:

This happens if you uninstall the Control Compliance Suite and reinstall it again on the same computer.	You must delete the contents of the Preferences folder after you uninstall CCS. The Preferences folder is present at the following location on your local computer: %USERPROFILE%\Local Settings\Application Data\Symantec\CCS\Preferences

For the dashboard panel, Compliance score for SCAP profile (benchmark), if the profile and benchmark names are same but are of different versions, then a single bar is displayed - Troubleshooting

The predefined dashboard panel, Compliance score for SCAP profile (benchmark) displays single bar for profiles and benchmarks of same name but different benchmark versions.

The impacts of this issue and the workaround are as follows:

Following are the impacts of this issue: ■ For different benchmark versions, if profile name and benchmark name are same, then the dashboard panel, Compliance score for SCAP profile(benchmark) displays aggregate compliance score for benchmarks with same name but different version. ■ You cannot view the compliance score for a profile of a benchmark against a benchmark version. ■ You cannot compare compliance scores for different benchmark versions for the predefined dashboard panel.	Do the following to resolve the issue: ■ Copy and edit the predefined dashboard panel, Compliance score for SCAP profile (benchmark). ■ In the **Subject-attributes**, select, **benchmark version is equal to** and provide the benchmark version for which you want to see compliance scores.

Incorrect calculation of aggregate risk score for profiles in custom dashboard panels - Troubleshooting

Create a custom panel with asset risk score as, measure, and profile:benchmark as, dimension. Consider assets with risk score, NA to calculate the aggregate risk score for the profile: benchmark. If you evaluate assets against profiles for which risk score is not applicable, then CCS still incorrectly considers those assets to calculate the aggregate risk score.

The method to resolve the issue is as follows:

Create a custom panel with SCAP asset risk score as, measure and profile: benchmark as, dimension. In the **Subject-attributes** select, **SCAP Asset Risk Score is greater than 0**.

Export of evaluation results to OVAL thin fails for OVAL definition files of more than 15 MB size - Troubleshooting

The issue and the workaround are as follows:

When you import OVAL definition file that exceeds 15 MB and you try to export the evaluation results into OVAL thin for more than 3 assets, then export fails.	The asset batch size for exporting the evaluation results is configurable in the AppserverService.exe.config file that is located at the following path: <installation directory>\Symantec\CCS\Reporting and Analytics\Application Server In the AppserverService.exe.config file, the default value for the asset batch size is 5. <add key="SCAPResultExportBatchSize" value="5”/> If the export of evaluation results fails for some number of assets, then reduce the asset batch size in the AppserverService.exe.config file and try exporting the results. For example, if the export fails for more than 3 assets, then set the asset batch size to 3 or any number less than 3 in the AppserverService.exe.config file. <add key="SCAPResultExportBatchSize" value="3" />

Time-out error occurs during SCAP content import - Troubleshooting

Sometimes a time-out error occurs during import of the following SCAP objects:

- FDCC benchmarks
- CCE
- CVE
- Standalone OVAL

The cause for the error and the method to resolve are as follows:

By default, CCS sets a time-out period of 10 minutes to import the SCAP objects.	The time-out setting can be configured through the configuration file, Symconsole.exe.config that is located in, %temp% directory. The %temp% directory of the computer refers to the installation path of the files that are installed to launch the CCS console on a remote computer. For the following element in the Symconsole.exe.config file, edit the value of the sendTimeout attribute: <binding name="netTcpWinConfig" closeTimeout="00:01:00" openTimeout="00:01:00" receiveTimeout="00:10:00" sendTimeout="00:10:00"... </binding> Re-launch the CCS console after you modify the value.

Appendix E

Dynamic Dashboards - Predefined dashboards and panels

This appendix includes the following topics:

- Data Collection Coverage
- Asset Compliance by Asset Group
- Check Status by Assets for Standards
- Check Status for Standards
- Compliance Score for Standard
- Top 10 Assets with Highest Risk Score by Standard
- Top 10 Failed Checks by Standard
- Top 10 Passed Checks by Standard
- Response to Data Loss Prevention Incidents
- Top 10 Data Loss Prevention Incidents by Protocol
- Top 10 Data Loss Prevention Incidents by User
- Compliance Score for HIPAA Mandate
- Control Status Trends for HIPAA Mandate
- Mapped Policies to HIPAA Mandate
- Coverage of Control Statements in HIPAA Mandate
- Top 10 Failed Control Statements for HIPAA Mandate
- Compliance Score for ISO Mandate
- Control Status Trends for ISO Mandate
- Mapped Policies to ISO Mandate
- Coverage of Control Statements in ISO Mandate
- Top 10 Failed Control Statements for ISO Mandate
- Compliance Score for NERC Mandate
- Control Status Trends for NERC Mandate
- Mapped Policies to NERC Mandate
- Coverage of Control Statements in NERC Mandate
- Top 10 Failed Control Statements for NERC Mandate
- Compliance Score for PCI Mandate

- Control Status Trends for PCI Mandate
- Mapped Policies to PCI Mandate
- Coverage of Control Statements in PCI Mandate
- Top 10 Failed Control Statements for PCI Mandate
- Breakdown of Policies by Status
- Control Status by Assets for Mandates
- Control Status by Assets for Policies
- Control Status for Mandates
- Control Status for Policies
- Control Status for Policy
- Top 10 Assets with Highest Risk Score by Policy
- Top 10 Failed Control Statements for Mandates
- Top 10 Failed Control Statements for Policies
- User Acceptance of Policies
- Compliance Score for SCAP Profile (Benchmark)
- Rule Status by Assets for SCAP Profile (Benchmark)
- Top 10 Assets By Risk Score for SCAP Profile (Benchmark)
- Compliance Score for SOX Mandate
- Control Status Trends for SOX Mandate
- Mapped Policies to SOX Mandate
- Coverage of Control Statements in SOX Mandate
- Top 10 Failed Control Statements for SOX Mandate
- Monthly Status Trend of Checks
- Compliance Trends by Standards
- Control Status Trends for Mandates
- Control Status Trends for Policies
- Overall Failure Trend of Checks

- Aggregated Risk Score for CCS VM Sites
- Top 10 Most Common Network Vulnerabilities
- Vulnerabilities by CVSS Score Range
- Vulnerabilities by Severity
- Alerts and Notifications
- Asset Group Yearly Trend
- Control Category Yearly Trend
- My Security Objectives
- Risk by Action Status
- Security Objective Yearly Trend
- Overall Risk - Security Objective
- Security Objectives Heatmap
- Top 10 Asset Groups with Maximum Risk
- Top 10 Assets with Highest Risk Score
- Top 5 Business Units at Highest Risk
- Top 5 Control Categories at Highest Risk
- Top 5 Security Objectives with Highest Base Risk (with Provider Weight)
- Top 5 Security Objectives with Maximum Risk

Compliance Administration - Assets

The **Compliance Administration - Assets** dashboard displays six panels. These panels display the compliance information in regards to the various assets in the system.

The dashboard displays the following panels:

Table E-1 Panels within the Compliance Administration - Assets Dashboard

Panel Name	Description
Compliance Score for Standard	The panel displays an average compliance score for a standard.

Table E-1 Panels within the Compliance Administration - Assets Dashboard *(continued)*

Panel Name	Description
Top 10 Risk Score by Asset for SCAP Profile (Benchmark)	The panel displays, in descending order, the 10 assets with the highest risk score as determined by the SCAP Profile.
Top 10 Failed Checks by Standard	The panel displays, in descending order, the 10 checks failing against maximum number of assets.
Asset Compliance by Asset Group	The panel displays the asset compliance score for asset groups.
Data Collection Coverage	The panel displays the data collection coverage for all assets in the CCS asset system.
Top 10 Assets with Highest Risk Score by Standard	The panel displays, in descending order, the 10 assets with the highest risk score as determined by standard provider.

From the Dashboard Taskbar you can do the following:

Table E-2 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the dashboard. This is active for custom created dashboard.
Copy	You can copy the dashboard.
Delete	You can delete the dashboard. This is active for custom created dashboard.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the dashboard. This is active for custom created dashboard.

Table E-2 Dashboard Taskbar *(continued)*

Option Name	Description
Unpublish	You can unpublish the dashboard. This is active for custom created dashboard.
Email Dashboard	You can email the dashboard.

The following options are available at the top of the dashboard:

Table E-3 General options on the Dashboard

Options	Descriptions
Open in a new window	Lets you open the dashboard in a new window.
Filter	Lets you open a webpage dialog to set filter conditions for the dashboard.
Set Dashboard Refresh Interval	Lets you set the refresh interval for the dashboard. By default the refresh interval is set to 120 minutes. You can check **Use this refresh interval for all my dashboards** to apply the refresh interval to all other dashboards.
Hide Taskbar	Lets you collaspe and expand the dashboard taskbar.

The following options are available at the top of each panel in the dashboard:

Table E-4 General options on each Panel

Options	Descriptions
Maximize	Lets you maximize the panel in the dashboard area.
Filter	Lets you open a webpage dialog to set filter conditions for the selected panel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Compliance Administration – SCAP benchmark Profile

The **Compliance Administration – SCAP benchmark Profile** dashboard displays three panels. These panels display the compliance information in regards to the SCAP benchmark profile.

The dashboard displays the following panels:

Table E-5 Panels within the Compliance Administration – SCAP benchmark Profile Dashboard

Panel Name	Description
Top 10 Risk Score by Asset for SCAP Profile (Benchmark)	The panel displays, in descending order, the 10 assets with the highest risk score as determined by SCAP Profile.
Compliance Score for SCAP Profile (Benchmark)	The panel displays an average compliance score for SCAP Profile.
Rule Status by Assets for SCAP Profile (Benchmark)	The panel displays the rule count with respective rule result name per asset for a SCAP Profile.

From the Dashboard Taskbar you can do the following:

Table E-6 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the dashboard. This is active for custom created dashboard.
Copy	You can copy the dashboard.
Delete	You can delete the dashboard. This is active for custom created dashboard.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the dashboard. This is active for custom created dashboard.

Table E-6 Dashboard Taskbar *(continued)*

Option Name	Description
Unpublish	You can unpublish the dashboard. This is active for custom created dashboard.
Email Dashboard	You can email the dashboard.

The following options are available at the top of the dashboard:

Table E-7 General options on the Dashboard

Options	Descriptions
Open in a new window	Lets you open the dashboard in a new window.
Filter	Lets you open a webpage dialog to set filter conditions for the dashboard.
Set Dashboard Refresh Interval	Lets you set the refresh interval for the dashboard. By default the refresh interval is set to 120 minutes. You can check **Use this refresh interval for all my dashboards** to apply the refresh interval to all other dashboards.
Hide Taskbar	Lets you collaspe and expand the dashboard taskbar.

The following options are available at the top of each panel in the dashboard:

Table E-8 General options on each Panel

Options	Descriptions
Maximize	Lets you maximize the panel in the dashboard area.
Filter	Lets you open a webpage dialog to set filter conditions for the selected panel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Compliance Administration – Standards

The **Compliance Administration – Standards** dashboard displays five panels. These panels display the compliance information in regards to the various assets in the system.

The dashboard displays the following panels:

Table E-9 Panels within the Compliance Administration – Standards Dashboard

Panel Name	Description
Compliance Score for Standard	The panel displays an average compliance score for a standard.
Compliance Trends by Standard	The panel displays compliance scores for standards.
Active Exceptions for Standards	The panel represents the number of approved check exceptions versus the standards the check exceptions are associated with.
Top 10 Failed Checks by Standard	The panel displays, in descending order, the 10 checks failing against maximum number of assets.
Check Status for Standards	The panel represents the count of asset with asset result name per check in a standard.

From the Dashboard Taskbar you can do the following:

Table E-10 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the dashboard. This is active for custom created dashboard.
Copy	You can copy the dashboard.

Table E-10 Dashboard Taskbar *(continued)*

Option Name	Description
Delete	You can delete the dashboard. This is active for custom created dashboard.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the dashboard. This is active for custom created dashboard.
Unpublish	You can unpublish the dashboard. This is active for custom created dashboard.
Email Dashboard	You can email the dashboard.

The following options are available at the top of the dashboard:

Table E-11 General options on the Dashboard

Options	Descriptions
Open in a new window	Lets you open the dashboard in a new window.
Filter	Lets you open a webpage dialog to set filter conditions for the dashboard.
Set Dashboard Refresh Interval	Lets you set the refresh interval for the dashboard. By default the refresh interval is set to 120 minutes. You can check **Use this refresh interval for all my dashboards** to apply the refresh interval to all other dashboards.
Hide Taskbar	Lets you collaspe and expand the dashboard taskbar.

The following options are available at the top of each panel in the dashboard:

Table E-12 General options on each Panel

Options	Descriptions
Maximize	Lets you maximize the panel in the dashboard area.

Table E-12 General options on each Panel *(continued)*

Options	Descriptions
Filter	Lets you open a webpage dialog to set filter conditions for the selected panel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Compliance Analysis – HIPAA Mandate

The **Compliance Analysis – HIPAA Mandate** dashboard displays five panels. The Health Insurance Portability and Accountability Act (HIPAA) panels display the compliance information in regards to the mandates of various assets in the system.

The dashboard displays the following panels:

Table E-13 Panels within the Compliance Analysis – HIPAA Mandate Dashboard

Panel Name	Description
Control Status Trends for HIPAA Mandate	The panel displays a control count for all available control result status for the controls mapped to control statement.
Compliance Score for HIPAA Mandate	The panel displays the percentage of average of control status evaluated against assets.
Top 10 Failed Control Statements for HIPAA Mandate	The panel displays, in descending order, the top 10 failed control statements that are mapped to a single mandate.
Coverage of HIPAA Mandate	The panel displays the percentage of mapped and unmapped control statements to the mandate.
Mapped Policies to HIPAA Mandate	The panel displays the total number of control statements mapped to the policies and the mandate.

From the Dashboard Taskbar you can do the following:

Table E-14 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the dashboard. This is active for custom created dashboard.
Copy	You can copy the dashboard.
Delete	You can delete the dashboard. This is active for custom created dashboard.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the dashboard. This is active for custom created dashboard.
Unpublish	You can unpublish the dashboard. This is active for custom created dashboard.
Email Dashboard	You can email the dashboard.

The following options are available at the top of the dashboard:

Table E-15 General options on the Dashboard

Options	Descriptions
Open in a new window	Lets you open the dashboard in a new window.
Filter	Lets you open a webpage dialog to set filter conditions for the dashboard.
Set Dashboard Refresh Interval	Lets you set the refresh interval for the dashboard. By default the refresh interval is set to 120 minutes. You can check **Use this refresh interval for all my dashboards** to apply the refresh interval to all other dashboards.
Hide Taskbar	Lets you collaspe and expand the dashboard taskbar.

The following options are available at the top of each panel in the dashboard:

Table E-16 General options on each Panel

Options	Descriptions
Maximize	Lets you maximize the panel in the dashboard area.
Filter	Lets you open a webpage dialog to set filter conditions for the selected panel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Compliance Analysis – ISO Mandate

The **Compliance Analysis – ISO Mandate** dashboard displays five panels. The International Organization for Standardization (ISO) panels display the compliance information in regards to the mandates of various assets in the system.

Note: The supported versions of ISO Mandate for predefined **Compliance Analysis - ISO Mandate** dashboard and its panels are as follows:

- ISO/IEC 27001:2005
- ISO/IEC 27002:2005

The dashboard displays the following panels:

Table E-17 Panels within the Compliance Analysis – ISO Mandate Dashboard

Panel Name	Description
Control Status Trends for ISO Mandate	The panel displays a control count for all available control result status for the controls mapped to control statement.
Compliance Score for ISO Mandate	The panel displays the percentage of average of control status evaluated against assets.
Top 10 Failed Control Statements for ISO Mandate	The panel displays, in descending order, the top 10 failed control statements that are mapped to a single mandate.

Table E-17 Panels within the Compliance Analysis – ISO Mandate Dashboard *(continued)*

Panel Name	Description
Coverage of Control Statements in ISO Mandate	The panel displays the percentage of mapped and unmapped control statements to the mandate.
Mapped Policies to ISO Mandate	The panel displays the total number of control statements mapped to the policies and the mandate.

From the Dashboard Taskbar you can do the following:

Table E-18 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the dashboard. This is active for custom created dashboard.
Copy	You can copy the dashboard.
Delete	You can delete the dashboard. This is active for custom created dashboard.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the dashboard. This is active for custom created dashboard.
Unpublish	You can unpublish the dashboard. This is active for custom created dashboard.
Email Dashboard	You can email the dashboard.

The following options are available at the top of the dashboard:

Table E-19 General options on the Dashboard

Options	Descriptions
Open in a new window	Lets you open the dashboard in a new window.
Filter	Lets you open a webpage dialog to set filter conditions for the dashboard.
Set Dashboard Refresh Interval	Lets you set the refresh interval for the dashboard. By default the refresh interval is set to 120 minutes. You can check **Use this refresh interval for all my dashboards** to apply the refresh interval to all other dashboards.
Hide Taskbar	Lets you collaspe and expand the dashboard taskbar.

The following options are available at the top of each panel in the dashboard:

Table E-20 General options on each Panel

Options	Descriptions
Maximize	Lets you maximize the panel in the dashboard area.
Filter	Lets you open a webpage dialog to set filter conditions for the selected panel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Compliance Analysis – Mandates

The **Compliance Analysis – Mandates** dashboard displays four panels. These panels display the compliance information in regards to the mandates of various assets in the system.

The dashboard displays the following panels:

Table E-21 Panels within the Compliance Analysis – Mandates Dashboard

Panel Name	Description
Control Status for Mandates	The panel displays the asset count with respective control mapped to mandates.
Control Status by Assets for Mandates	The panel displays the count of controls with respective control result name mapped to mandates.
Top 10 Failed Control Statements for Mandates	The panel displays, in descending order, the top 10 failed control statements that are mapped to single or to multiple mandates.
Control Status Trends for Mandates	The panel displays a control count for all available control result status for all the controls mapped to control statement.

From the Dashboard Taskbar you can do the following:

Table E-22 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the dashboard. This is active for custom created dashboard.
Copy	You can copy the dashboard.
Delete	You can delete the dashboard. This is active for custom created dashboard.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the dashboard. This is active for custom created dashboard.
Unpublish	You can unpublish the dashboard. This is active for custom created dashboard.
Email Dashboard	You can email the dashboard.

The following options are available at the top of the dashboard:

Table E-23 General options on the Dashboard

Options	Descriptions
Open in a new window	Lets you open the dashboard in a new window.
Filter	Lets you open a webpage dialog to set filter conditions for the dashboard.
Set Dashboard Refresh Interval	Lets you set the refresh interval for the dashboard. By default the refresh interval is set to 120 minutes. You can check **Use this refresh interval for all my dashboards** to apply the refresh interval to all other dashboards.
Hide Taskbar	Lets you collaspe and expand the dashboard taskbar.

The following options are available at the top of each panel in the dashboard:

Table E-24 General options on each Panel

Options	Descriptions
Maximize	Lets you maximize the panel in the dashboard area.
Filter	Lets you open a webpage dialog to set filter conditions for the selected panel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Compliance Analysis – NERC Mandate

The **Compliance Analysis – NERC Mandate** dashboard displays five panels. The North American Electric Reliability Corporation (NERC) panels display the compliance information in regards to the mandates of various assets in the system.

The dashboard displays the following panels:

Table E-25 Panels within the Compliance Analysis – NERC Mandate Dashboard

Panel Name	Description
Control Status Trends for NERC Mandate	The panel displays a control count for all available control result status for the controls mapped to control statement.
Compliance Score for NERC Mandate	The panel displays the percentage of average of control status evaluated against assets.
Top 10 Failed Control Statements for NERC Mandate	The panel displays, in descending order, the top 10 failed control statements that are mapped to a single mandate.
Coverage of Control Statements in NERC Mandate	The panel displays the percentage of mapped and unmapped control statements to the mandate.
Mapped Policies to NERC Mandate	The panel displays the total number of control statements mapped to the policies and the mandate.

From the Dashboard Taskbar you can do the following:

Table E-26 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the dashboard. This is active for custom created dashboard.
Copy	You can copy the dashboard.
Delete	You can delete the dashboard. This is active for custom created dashboard.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the dashboard. This is active for custom created dashboard.

Table E-26 Dashboard Taskbar *(continued)*

Option Name	Description
Unpublish	You can unpublish the dashboard. This is active for custom created dashboard.
Email Dashboard	You can email the dashboard.

The following options are available at the top of the dashboard:

Table E-27 General options on the Dashboard

Options	Descriptions
Open in a new window	Lets you open the dashboard in a new window.
Filter	Lets you open a webpage dialog to set filter conditions for the dashboard.
Set Dashboard Refresh Interval	Lets you set the refresh interval for the dashboard. By default the refresh interval is set to 120 minutes. You can check **Use this refresh interval for all my dashboards** to apply the refresh interval to all other dashboards.
Hide Taskbar	Lets you collaspe and expand the dashboard taskbar.

The following options are available at the top of each panel in the dashboard:

Table E-28 General options on each Panel

Options	Descriptions
Maximize	Lets you maximize the panel in the dashboard area.
Filter	Lets you open a webpage dialog to set filter conditions for the selected panel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Compliance Analysis – PCI Mandate

The **Compliance Analysis – PCI Mandate** dashboard displays five panels. The Payment Card Industry (PCI) panels display the compliance information in regards to the mandates of various assets in the system.

Note: The supported versions of PCI Mandate for predefined **Compliance Analysis - PCI Mandate** dashboard and its panels are as follows:

- PCI DSS v1.2

The dashboard displays the following panels:

Table E-29 Panels within the Compliance Analysis – PCI Mandate Dashboard

Panel Name	Description
Control Status Trends for PCI Mandate	The panel displays a control count for all available control result status for all the controls mapped to control statement.
Compliance Score for PCI Mandate	The panel displays the percentage of average of control status evaluated against assets.
Top 10 Failed Control Statements for PCI Mandate	The panel displays, in descending order, the top 10 failed control statements that are mapped to a single mandate.
Coverage of Control Statements in PCI Mandate	The panel displays the percentage of mapped and unmapped control statements to the mandate.
Mapped Policies to PCI Mandate	The panel displays the total number of control statements mapped to the policies and the mandate.

From the Dashboard Taskbar you can do the following:

Table E-30 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.

Table E-30 Dashboard Taskbar *(continued)*

Option Name	Description
Edit	You can edit the dashboard. This is active for custom created dashboard.
Copy	You can copy the dashboard.
Delete	You can delete the dashboard. This is active for custom created dashboard.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the dashboard. This is active for custom created dashboard.
Unpublish	You can unpublish the dashboard. This is active for custom created dashboard.
Email Dashboard	You can email the dashboard.

The following options are available at the top of the dashboard:

Table E-31 General options on the Dashboard

Options	Descriptions
Open in a new window	Lets you open the dashboard in a new window.
Filter	Lets you open a webpage dialog to set filter conditions for the dashboard.
Set Dashboard Refresh Interval	Lets you set the refresh interval for the dashboard. By default the refresh interval is set to 120 minutes. You can check **Use this refresh interval for all my dashboards** to apply the refresh interval to all other dashboards.
Hide Taskbar	Lets you collaspe and expand the dashboard taskbar.

The following options are available at the top of each panel in the dashboard:

Table E-32 General options on each Panel

Options	Descriptions
Maximize	Lets you maximize the panel in the dashboard area.
Filter	Lets you open a webpage dialog to set filter conditions for the selected panel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Compliance Analysis – Policies

The **Compliance Analysis – Policies** dashboard displays five panels. These panels display the compliance information in regards to the policies of various assets in the system.

The dashboard displays the following panels:

Table E-33 Panels within the Compliance Analysis – Policies Dashboard

Panel Name	Description
Control Status for Policies	The panel displays the asset count with respective control mapped to policies.
Top 10 Failed Control Statements for Policies	The panel displays, in descending order, the 10 failed control statements that are mapped to single or to multiple policies.
Control Status Trends for Policies	The panel displays a control count for all available control result status for all the controls mapped to control statement.
Active Exceptions for Policy Controls	The panel displays the number of approved check exceptions for controls mapped to policies through control statements.
Top 10 Assets with Highest Risk Score by Policy	The panel displays, in descending order, the 10 assets with the highest risk score as scoped by policy application.

From the Dashboard Taskbar you can do the following:

Table E-34 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the dashboard. This is active for custom created dashboard.
Copy	You can copy the dashboard.
Delete	You can delete the dashboard. This is active for custom created dashboard.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the dashboard. This is active for custom created dashboard.
Unpublish	You can unpublish the dashboard. This is active for custom created dashboard.
Email Dashboard	You can email the dashboard.

The following options are available at the top of the dashboard:

Table E-35 General options on the Dashboard

Options	Descriptions
Open in a new window	Lets you open the dashboard in a new window.
Filter	Lets you open a webpage dialog to set filter conditions for the dashboard.
Set Dashboard Refresh Interval	Lets you set the refresh interval for the dashboard. By default the refresh interval is set to 120 minutes. You can check **Use this refresh interval for all my dashboards** to apply the refresh interval to all other dashboards.
Hide Taskbar	Lets you collaspe and expand the dashboard taskbar.

The following options are available at the top of each panel in the dashboard:

Table E-36 General options on each Panel

Options	Descriptions
Maximize	Lets you maximize the panel in the dashboard area.
Filter	Lets you open a webpage dialog to set filter conditions for the selected panel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Compliance Analysis – SOX Mandate

The **Compliance Analysis – SOX Mandate** dashboard displays five panels. The Sarbanes Oxley (SOX) panels display the compliance information in regards to the mandates of various assets in the system.

The dashboard displays the following panels:

Table E-37 Panels within the Compliance Analysis – SOX Mandate Dashboard

Panel Name	Description
Control Status Trends for SOX Mandate	The panel displays a control count for all available control result status for all the controls mapped to control statement.
Compliance Score for SOX Mandate	The panel displays the percentage of average of control status evaluated against assets.
Top 10 Failed Control Statements for SOX Mandate	The panel displays, in descending order, the top 10 failed control statements that are mapped to a single mandate.
Coverage of Control Statements in SOX Mandate	The panel displays the percentage of mapped and unmapped control statements to the mandate.
Mapped Policies to SOX Mandate	The panel displays the total number of control statements mapped to the policies and the mandate.

From the Dashboard Taskbar you can do the following:

Table E-38 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the dashboard. This is active for custom created dashboard.
Copy	You can copy the dashboard.
Delete	You can delete the dashboard. This is active for custom created dashboard.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the dashboard. This is active for custom created dashboard.
Unpublish	You can unpublish the dashboard. This is active for custom created dashboard.
Email Dashboard	You can email the dashboard.

The following options are available at the top of the dashboard:

Table E-39 General options on the Dashboard

Options	Descriptions
Open in a new window	Lets you open the dashboard in a new window.
Filter	Lets you open a webpage dialog to set filter conditions for the dashboard.
Set Dashboard Refresh Interval	Lets you set the refresh interval for the dashboard. By default the refresh interval is set to 120 minutes. You can check **Use this refresh interval for all my dashboards** to apply the refresh interval to all other dashboards.
Hide Taskbar	Lets you collaspe and expand the dashboard taskbar.

The following options are available at the top of each panel in the dashboard:

Table E-40 General options on each Panel

Options	Descriptions
Maximize	Lets you maximize the panel in the dashboard area.
Filter	Lets you open a webpage dialog to set filter conditions for the selected panel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

IT Operations

The **IT Operations** dashboard displays five panels. These panels display the check status information in regards to the various assets in the system.

The dashboard displays the following panels:

Table E-41 Panels within the IT Operations Dashboard

Panel Name	Description
Compliance Score for Standard	The panel displays an average compliance score for a standard.
Top 10 Failed Checks by Standard	The panel displays, in descending order, the 10 checks failing against maximum number of assets.
Top 10 Assets with Highest Risk Score by Standard	The panel displays, in descending order, the 10 assets with the highest risk score as determined by standard provider.
Monthly Status Trend of Checks	The panel displays a check status count for all evaluated standards.
Data Collection Coverage	The panel displays the data collection coverage for all assets in the CCS asset system.

From the Dashboard Taskbar you can do the following:

Table E-42 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the dashboard. This is active for custom created dashboard.
Copy	You can copy the dashboard.
Delete	You can delete the dashboard. This is active for custom created dashboard.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the dashboard. This is active for custom created dashboard.
Unpublish	You can unpublish the dashboard. This is active for custom created dashboard.
Email Dashboard	You can email the dashboard.

The following options are available at the top of the dashboard:

Table E-43 General options on the Dashboard

Options	Descriptions
Open in a new window	Lets you open the dashboard in a new window.
Filter	Lets you open a webpage dialog to set filter conditions for the dashboard.
Set Dashboard Refresh Interval	Lets you set the refresh interval for the dashboard. By default the refresh interval is set to 120 minutes. You can check **Use this refresh interval for all my dashboards** to apply the refresh interval to all other dashboards.
Hide Taskbar	Lets you collaspe and expand the dashboard taskbar.

The following options are available at the top of each panel in the dashboard:

Table E-44 General options on each Panel

Options	Descriptions
Maximize	Lets you maximize the panel in the dashboard area.
Filter	Lets you open a webpage dialog to set filter conditions for the selected panel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Risk - Home

The **Risk - Home** dashboard displays five panels. These panels display the risk information in regards to the various assets in the system.

The dashboard displays the following panels:

Table E-45 Panels within the Compliance Administration - Assets Dashboard

Panel Name	Description
Top 5 Risk Objectives with Maximum Risk	The panel displays the top 5 risk objectives with the maximum risk score.
Risk Objectives Heatmap	The panel displays.
Top 5 Control Categories at Highest Risk	The panel displays the top 5 control categories with the highest risk score.
Top 10 Asset Containers with Maximum Risk	The panel displays the top 10 asset containers with the maximum risk score.
Alerts and Notifications	The panel displays the alerts and notifications.

From the Dashboard Taskbar you can do the following:

Table E-46 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.

Table E-46 Dashboard Taskbar *(continued)*

Option Name	Description
New Panel	You click this to launch the create panel page.
Edit	You can edit the dashboard. This is active for custom created dashboard.
Copy	You can copy the dashboard.
Delete	You can delete the dashboard. This is active for custom created dashboard.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the dashboard. This is active for custom created dashboard.
Unpublish	You can unpublish the dashboard. This is active for custom created dashboard.
Email Dashboard	You can email the dashboard.

The following options are available at the top of the dashboard:

Table E-47 General options on the Dashboard

Options	Descriptions
Open in a new window	Lets you open the dashboard in a new window.
Filter	Lets you open a webpage dialog to set filter conditions for the dashboard.
Set Dashboard Refresh Interval	Lets you set the refresh interval for the dashboard. By default the refresh interval is set to 120 minutes. You can check **Use this refresh interval for all my dashboards** to apply the refresh interval to all other dashboards.
Hide Taskbar	Lets you collaspe and expand the dashboard taskbar.

The following options are available at the top of each panel in the dashboard:

Table E-48 General options on each Panel

Options	Descriptions
Maximize	Lets you maximize the panel in the dashboard area.
Filter	Lets you open a webpage dialog to set filter conditions for the selected panel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Active Exceptions for Policies

The **Active Exception for Policies** panel displays the number of approved check exceptions for the policies. The panel displays a 2D-column chart.

Policy Exception is the area of interest for this panel.

The panel displays the following information:

Table E-49 Components for the Active Exceptions for Policies Panel

Components	Description
Dimension (X axis)	Policy Name
Measure (Y axis)	Count of Exceptions
Chart style	2D-column chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the number of exceptions for a selected policy:

```
User has requested and approved exception for Policy1 from Win32
console.
```

```
User has requested and approved exception for Policy1 from web
console.
```

Therefore, the panel displays a bar for Policy1 with exception count as 2.

You can click one of the bars to drill down and view a table for detailed information.

The table displays the following columns:

Table E-50 Active Exceptions for Policies

Column Name	Description
Policy Name	Displays the name of the policy. The Policy Name opens a page with detailed information on the policy.
Policy Author	Displays the name of the author of the policy.
Requestor Name	Displays the name of the check exception requestor.
Exception Expiration Date	Displays the date when the exception expires.
Exception Approval Date	Displays the date of approval of the check exception.
Policy Tag Name	Displays the name of the policy tag.

From the Dashboard Taskbar you can do the following:

Table E-51 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-52 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-column chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Active Exceptions for Policy Controls

The **Active Exception for Policy Controls** panel displays the number of approved check exceptions for controls mapped to policies through control statements. The panel displays a 2D-bar chart.

Policy Control Exception is the area of interest for this panel.

The panel displays the following information:

Table E-53 Components for the Active Exceptions for Policy Controls Panel

Components	Description
Dimension (X axis)	Control Statement
Measure (Y axis)	Count of Control Exceptions
Chart style	2D-bar chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the number of exceptions for selected policy controls:

```
Controls C1, C2, and C3 are mapped to the Control Statement CS01.
```

```
Policy P1 is mapped to these controls through CS01.
Policy P1 is scoped to assets A1 and A2.

User requested and approved exception for Controls C1 against asset
A1.
```

Therefore, the panel displays a bar for CS01 with exception count as 1.

Note: To view all the details about the policies in the drill through table, ensure that you have the view permissions on the entities in the panel.

You can click one of the bars to drill down and view a table for detailed information.

The table displays the following columns:

Table E-54 Active Exceptions for Policy Controls

Column Name	Description
Exception Name	Displays the name of the exception. The Exception Name opens a page with detailed information on the exception.
Control Name	Displays the name of the control to which the exception is made to. The Control Name opens a page with detailed information on the control.
Control Statement	Displays the name of the control statement. The Control Statement opens a page with detailed information on the control statement.
Policy Name	Displays the name of the policy. The Policy Name opens a page with detailed information on the policy.
Control Type	Displays the type of control.
Requestor Name	Displays the name of the requestor for the check exception.
Exception Approval Date	Displays the date of approval of the check exception.
Exception Expiration Date	Displays the date when the check exception expires.

From the Dashboard Taskbar you can do the following:

Table E-55 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-56 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-bar chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Active Exceptions for Standards

The **Active Exception for Standards** panel displays the number of approved check exceptions versus the standards the check exceptions are associated with. The panel displays a 2D-bar chart.

Standard Compliance Management is the area of interest for this panel.

The panel displays the following information:

Table E-57 Components for the Active Exceptions for Standards Panel

Components	Description
Dimension (X axis)	Standard Name
Measure (Y axis)	Exception Check Count
Chart style	2D-bar chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the number of exceptions for selected standards:

`Standard1 has five checks Check1, Check2, Check3, Check4, and Check5.`

`Standard2 has three checks Check11, Check12, and Check13.`

`User requested and approved exception for Check1, Check2, and Check3 from Standard1 against Asset1.`

`User requested and approved exception for Check11 from Standard2 against asset Asset1.`

Therefore, the panel displays the following exception check count as:

`Standard1 -3 (exception check count).`

`Standrad2- 1 (exception check count).`

You can click one of the bars to drill down and view a table for detailed information.

The table displays the following columns:

Table E-58 Active Exceptions for Standards

Column Name	Description
Exception Name	Displays the name of the exception. The Exception Name opens a page with detailed information on the exception.
Standard Name	Displays the name of the standard for which the check is associated with. The Standard Name opens a page with detailed information on the standard.
Check Name	Displays the name of the check on which an active exception is applied. The Check Name opens a page with detailed information on the check.
Exception Requestor E-mail Address	Displays the email address of the requestor for the check exception.
Exception Effective Date	Displays the date when the check exception is applied.
Exception Expiration Date	Displays the date when the check exception has expired.

From the Dashboard Taskbar you can do the following:

Table E-59 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.

Table E-59 Dashboard Taskbar *(continued)*

Option Name	Description
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-60 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-bar chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Data Collection Coverage

The **Data Collection Coverage** panel displays the data collection coverage for all assets in CCS asset system. The panel displays a 3D-pie chart.

The pie chart displays information about the number of assets from which data has been collected and not collected.

Asset Collection Coverage is the area of interest for this panel.

The panel displays the following information:

Table E-61 Components for the Data Collection Coverage Panel

Components	Description
Dimension (X axis)	None
Measure (Y axis)	Collected / Not Collected

Table E-61 Components for the Data Collection Coverage Panel *(continued)*

Components	Description
Chart style	3D-pie chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the data collection coverage of assets in the CCS asset system:

```
Data collection is done for 20 assets against any CCS standards.

100 assets are imported in CCS asset system.

Data collection is not done for 80 assets against any CCS standards.
```

The panel displays the results of the assets count as follows:

```
Collected = 20

Not Collected = 80
```

Therefore, the collection of data is from 20 assets out of the 100 assets that are imported in CCS asset system.

You can click on the pie chart to drill down and view a table for detailed information.

The table displays the following columns:

Table E-62 Data Collection Coverage

Column Name	Description
Asset Folder Name	Displays the name of the folder that the asset belongs to.
Asset Group Name	Displays the name of the group that the asset belongs to. The Asset Group Name opens a page with detailed information on the selected asset group.
Asset Group Type	Displays the type of the asset group. For example, static or dynamic.
Asset Location	Displays the location of the asset.
Asset Name	Displays the name of the asset. The Asset Name opens a page with detailed information on the selected asset.

Table E-62 Data Collection Coverage *(continued)*

Column Name	Description
Asset Owner	Displays the name of the owner of the asset.
Asset Tag Name	Displays the name of the asset tag.
Asset Type	Displays the type of the asset. For example, Windows Machine, UNIX Machine , and so forth.
Collection Date	Displays the date of the data collection on an asset.

From the Dashboard Taskbar you can do the following:

Table E-63 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-64 General options

Options	Descriptions
Back to chart	Lets you return to the 3D-pie chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Asset Compliance by Asset Group

The **Asset Compliance by Asset Group** panel displays the asset compliance score for asset groups. The panel displays a 2D-column chart.

Standard Compliance Management is the area of interest for this panel.

Each bar represents an asset group. An asset group contains a number of assets that are evaluated against a standard.

The panel displays the following information:

Table E-65 Components for the Asset Compliance by Asset Group Panel

Components	Description
Dimension (X axis)	Asset Group Name
Measure (Y axis)	Average Asset Compliance (%)
Chart style	2D-column chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the average asset compliance score:

```
Asset group, AG1 contains three assets: Asset1, Asset2, and Asset3.
```

```
Asset1 is evaluated against the standard, Standard1. The compliance
score is 50%.
```

```
Asset2 is evaluated against the standard, Standard2. The compliance
score is 75%.
```

```
Asset3 is evaluated against the standard, Standard2. The compliance
score is 100%.
```

The following formula displays the average compliance score for AG1.

```
= (Asset1 compliance score + Asset2 compliance score + Asset3
compliance score) / 3
```

```
= (50+75+100) /3
```

```
= 75%
```

Therefore, the average asset compliance score for Asset group, AG1 is 75%.

You can click one of the bars to drill down and view a table for detailed information.

The table displays the following columns:

Table E-66 Asset Compliance by Asset Group

Column Name	Description
Results Summary	Displays the compliance score for an asset that has been evaluated against a standard. The Results Summary opens a page with detailed information on the checks evaluated.
Asset Name	Displays the name of the asset. The Asset Name opens a page with detailed information on the asset.
Standard Name	Displays the name of the standard. The Standard Name opens a page with detailed information on the standard.
Asset Type	Displays the type of the asset. For example, Windows Machine, UNIX Machine, and so forth.
Asset Location	Displays the location of the asset.
Asset Owner	Displays the name of the owner of the asset.
Asset Group	Displays the name of the group that the asset is in. The Asset Group opens a page with detailed information on the asset group.

From the Dashboard Taskbar you can do the following:

Table E-67 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-68 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-column chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Check Status by Assets for Standards

The **Check Status by Assets for Standards** panel represents the count of checks with respective check result name per asset for a standard. The panel displays a 3D-pie chart.

Standard Compliance Management is the area of interest for this panel.

The panel displays the following information:

Table E-69 Components for the Check Status by Assets for Standards Panel

Components	Description
Dimension (X axis)	Results Name
Measure (Y axis)	Result Summary (Sum of all checks with same check result name)
Chart style	3D-pie chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the check status of a standard against assets:

```
Standard, Standard1 has 5 checks, Check1, Check2, Check3, Check4,
and Check5.
```

```
Standard1 is evaluated against assets, Asset1, Asset2 and Asset3.
```

Table E-70 Standard1 is evaluated against assets

Asset/Check	Check1	Check2	Check3	Check4	Check5
Asset1	Pass	Fail	Pass	NA	Unknown
Asset2	Fail	Fail	Error	Pass	NA
Asset3	Fail	Pass	Fail	Fail	Unknown

Therefore, the results of the check status for the assets against the Standard1 are the following:

```
Pass = 4, Fail = 6, Error = 1, Unknown = 2, and Not Applicable = 2.
```

You can click pie chart to drill down and view a table for detailed information.

The table displays the following columns:

Table E-71 Check Status by Assets for Standards

Column Name	Description
Asset Name	Displays the name of the asset. The Asset Name opens a page with detailed information on the asset.
Results Name	Displays the result of the check status. For example, Standard asset check pass, fail, and so forth.
Results Summary	Displays the check count with respective check result name. The Results Summary opens a page with detailed information on the check status.
Standard Asset Risk Score	Displays the risk score of the asset based on certain standards.
Standard Name	Displays the name of the standard. The Standard Name opens a page with detailed information on the standard.
Asset Type	Displays the type of the asset. For example, Windows Machine, Unix Machine, and so forth.
Asset Location	Displays the location of the asset.
Asset Owner	Displays the name of the owner of the asset.
Standard Asset Compliance Pass	Displays the compliance pass value.

From the Dashboard Taskbar you can do the following:

Table E-72 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.

Table E-72 Dashboard Taskbar *(continued)*

Option Name	Description
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-73 General options

Options	Descriptions
Back to chart	Lets you return to the 3D-pie chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Check Status for Standards

The **Check Status for Standards** panel displays the count of asset with asset result name per check in a standard. The panel displays a 2D-stacked column chart.

Standard Compliance Management is the area of interest for this panel.

Each bar represents a standard and an asset count with their respective asset result name.

The panel displays the following information:

Table E-74 Components for the Check Status for Standard Panel

Components	Description
Dimension (X axis)	Standard name
Measure (Y axis)	Count of Checks per Asset
Chart style	2D-stacked column chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the check status of a standard against assets:

```
Standard, Standard1 has 3 checks, Check1, Check2, and Check3.
```

```
Standard1 is evaluated against assets, Asset1, Asset2, Asset3, Asset4,
and Asset5.
```

Table E-75 Standard1 is evaluated against assets

Check/Asset	Asset1	Asset2	Asset3	Asset4	Asset5
Check1	Pass	Fail	Pass	NA	Unknown
Check2	Fail	Fail	Error	Pass	NA
Check3	Fail	Pass	Fail	Fail	Unknown

You can click one of the bars to drill down and view for detailed information.

The table displays the following columns:

Table E-76 Check Status for Standards

Column Name	Description
Results Name	Displays the result of the check status. For example, asset check pass, fail, and so forth.
Results Summary	Displays the asset count with respective asset result name. The Results Summary opens a page with detailed information on the asset.
Standard Name	Displays the name of the standard. The Standard Name opens a page with detailed information on the standard.

Table E-76 Check Status for Standards *(continued)*

Column Name	Description
Check Name	Displays the name of the check. The Check Name opens a page with detailed information on the check.
Check Type	Displays the type of the check. For example, technical.

From the Dashboard Taskbar you can do the following:

Table E-77 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-78 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-stacked column chart in the first panel.

Table E-78 General options *(continued)*

Options	Descriptions
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Compliance Score for Standard

The **Compliance Score for Standard** panel displays an average compliance score for a standard. The panel displays a 2D-stacked column chart.

Standard Compliance Management is the area of interest for this panel.

Each bar represents an average compliance score of all assets that are evaluated against a standard.

The panel displays the following information:

Table E-79 Components for the Compliance Score for Standard Panel

Components	Description
Dimension (X axis)	Standard Name
Measure (Y axis)	Average Compliance Score (%)
Chart style	2D-stacked column chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the average asset compliance score for a standard:

```
Standard, Standard1 is evaluated against assets, Asset1, Asset2 and
Asset3.

Compliance score for Asset1 evaluated against Standard1 = 50%.

Compliance score for Asset2 evaluated against Standard1 = 75%.

Compliance score for Asset3 evaluated against Standard1 = 0%.
```

The following formula displays the average compliance score for Standard1.

```
= (Asset1 compliance score + Asset2 Compliance score + Asset3
Compliance score ) / 3

= (50+75+0) / 3

= 41.67%
```

Therefore, the average asset compliance score for Standard1 is 41.67 %.

You can click one of the bars to drill down and view a table for detailed information.

The table displays the following columns:

Table E-80 Compliance Score for Standard

Column Name	Description
Results Name	Displays the result of the compliance score. For example, Standard asset compliance pass, fail, and so forth.
Results Summary	Displays the Standard asset compliance score. The Results Summary opens a page with detailed information on the compliance score.
Standard Asset Risk Score	Displays the risk score of the asset against the certain standard.
Standard Name	Displays the name of the standard. The Standard Name opens a page with detailed information on the standard.
Asset Name	Displays the name of the asset. The Asset Name opens a page with detailed information on the asset.
Asset Type	Displays the type of the asset. For example, Windows Machine, UNIX Machine, and so forth.
Asset Location	Displays the location of the asset.
Asset Owner	Displays the name of the owner of the asset.

From the Dashboard Taskbar you can do the following:

Table E-81 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-82 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-stacked column chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Top 10 Assets with Highest Risk Score by Standard

The **Top 10 Assets with Highest Risk Score by Standard** panel displays, in descending order, the 10 assets with the highest risk score as determined by standard provider. The panel displays a 2D-bar chart.

Standard Compliance Management is the area of interest for this panel.

The panel displays the following information:

Table E-83 Components for the Top 10 Assets with Highest Risk Score by Standard Panel

Components	Description
Dimension (X axis)	Asset Name
Measure (Y axis)	Average Asset Risk Score
Chart style	2D-bar chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the assets with the highest risk score:

```
Asset, Asset1 is evaluated against standard, Std1, Std2 and Std3.

Asset, Asset2 is evaluated against standard, Std1, and Std2.

Asset, Asset3 is evaluated against standard Std3.
```

The following table displays the assets and their risk scores against each standard:

Table E-84 Asset's risk score against each standard

Asset/Check	Standard1	Standard2	Standard3
Asset1	7.5	NA	9.2
Asset2	6.2	4.5	-
Asset3	-	-	NA

Any asset with a risk score of NA is not part of the calculation for average risk score.

```
Asset1 risk score = (7.5 + 9.2)/2 = 8.4

Asset2 risk score = (6.2 + 4.5)/2 = 5.4

Asset3 risk score = NA
```

Therefore, the panel displays Asset1 = 8.4 and Asset2 = 5.4 risk score in descending order.

You can click one of the bars to drill down and view a table for detailed information.

The table displays the following columns:

Table E-85 Top 10 Assets with Highest Risk Score by Standard

Column Name	Description
Asset Name	Displays the name of the asset. The Asset Name opens a page with detailed information on the asset.
Results Summary	Displays the asset risk score. The Results Summary opens a page with detailed information on the asset risk score.
Standard Name	Displays the name of the standard. The Standard Name opens a page with detailed information on the standard.
Asset Type	Displays the type of the asset. For example, Windows Machine, UNIX Machine, and so forth.
Asset Location	Displays the location of the asset.
Asset Owner	Displays the name of the owner of the asset.

From the Dashboard Taskbar you can do the following:

Table E-86 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.

Table E-86 Dashboard Taskbar *(continued)*

Option Name	Description
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-87 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-bar chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Top 10 Failed Checks by Standard

The **Top 10 Failed Checks by Standard** panel displays, in descending order, the 10 checks failing against maximum number of assets. The panel displays a 2D-bar chart.

Standard Compliance Management is the area of interest for this panel.

The panel displays the following information:

Table E-88 Components for the Top 10 Failed Checks by Standard Panel

Components	Description
Dimension (X axis)	Check Name

Table E-88 Components for the Top 10 Failed Checks by Standard Panel *(continued)*

Components	Description
Measure (Y axis)	Count of Failed Assets
Chart style	2D-bar chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the assets with failed check score:

```
Standard, Standard1 has 3 checks, Check1, Check2, and Check3.
```

```
These are evaluated against 5 assets, Asset1, Asset2, Asset3, Asset4,
and Asset5.
```

The following table displays the evaluation results of the checks against assets:

Table E-89 Evaluation of Standard1 against the assets

Check/Asset	Asset1	Asset2	Asset3	Asset4	Asset5
Check1	Pass	Fail	Pass	Fail	Fail
Check2	Fail	Fail	Pass	Pass	Pass
Check3	Fail	Pass	Fail	Fail	Fail

The results of the table are:

```
Check3 = 4 (Failed against 4 asset)
```

```
Check1 = 3 (Failed against 3 asset)
```

```
Check2 = 2 (Failed against 2 asset)
```

Therefore, the panel displays Check3 = 4, Check1 = 3, and Check2 = 2 failed check scores in descending order.

You can click one of the bars to drill down and view a table for detailed information.

The table displays the following columns:

Table E-90 Top 10 Failed Checks by Standard

Column Name	Description
Check Name	Displays the failed check name. The Check Name pens a page with detailed information on the check.
Results Summary	Displays the asset count with respective failed checks. The Results Summary opens a page with detailed information on the asset.
Standard Name	Displays the name of the standard. The Standard Name opens a page with detailed information on the standard.
Check Author	Displays the name of the author of the check.
Check Risk Impact - Access Complexity	Displays the access complexity value of the check.
Check Risk Impact - Access Vector	Displays the access vector value of the check.
Check Risk Impact - Availability	Displays the availability value of the check.
Check Risk Impact - Confidentiality	Displays the confidentiality value of the check.
Check Risk Impact - Integrity	Displays the integrity value of the check.
Check Type	Displays the type of the check. For example, technical.

From the Dashboard Taskbar you can do the following:

Table E-91 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.

Table E-91 Dashboard Taskbar *(continued)*

Option Name	Description
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-92 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-bar chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Top 10 Passed Checks by Standard

The **Top 10 Passed Checks by Standard** panel displays, in descending order, the 10 checks passing against maximum number of assets. The panel displays a 2D-bar chart.

Standard Compliance Management is the area of interest for this panel.

The panel displays the following information:

Table E-93 Components for the Top 10 Passed Checks by Standard Panel

Components	Description
Dimension (X axis)	Check Name
Measure (Y axis)	Count of Passed Assets
Chart style	2D-bar chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the assets with passed check score:

```
Standard, Standard1 has 3 checks, Check1, Check2, and Check3.
```

```
These are evaluated against 5 assets, Asset1, Asset2, Asset3, Asset4,
and Asset5.
```

The following table displays the evaluation results of the checks against assets:

Table E-94 Evaluation of Standard1 against the assets

Check/Asset	Asset1	Asset2	Asset3	Asset4	Asset5
Check1	Pass	Fail	Pass	Fail	Fail
Check2	Fail	Fail	Pass	Pass	Pass
Check3	Fail	Pass	Fail	Fail	Fail

The results of the table are:

```
Check2 = 3 (Passed against 3 asset)
```

```
Check1 = 2 (Passed against 2 asset)
```

```
Check3 = 1 (Passed against 1 asset)
```

Therefore, the panel displays Check2 = 3, Check1 = 2, and Check3 = 1 passed check scores in descending order.

You can click one of the bars to drill down and view a table for detailed information.

The table displays the following columns:

Table E-95 Top 10 Failed Passed by Standard

Column Name	Description
Results Summary	Displays the asset count with respective failed checks. The Results Summary opens a page with detailed information on the asset.
Check Name	Displays the passed check name. The Check Name opens a page with detailed information on the check.
Standard Name	Displays the name of the standard. The Standard Name opens a page with detailed information on the standard.
Check Author	Displays the name of the author of the check.
Check Risk Impact - Access Complexity	Displays the Access Complexity value of the check.
Check Risk Impact - Access Vector	Displays the Access Vector value of the check.
Check Risk Impact - Availability	Displays the Availability value of the check.
Check Risk Impact - Confidentiality	Displays the Confidentiality value of the check.
Check Risk Impact - Integrity	Displays the Integrity value of the check.
Check Type	Displays the type of the check.

From the Dashboard Taskbar you can do the following:

Table E-96 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.

Table E-96 Dashboard Taskbar *(continued)*

Option Name	Description
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-97 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-bar chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Response to Data Loss Prevention Incidents

The **Response to Data Loss Prevention Incidents** panel displays incidents grouped by blocked status. The panel displays a 3D-pie chart.

Symantec Data Loss Prevention Incidents is the area of interest for the panel.

The panel displays the following information:

Table E-98 Components of the Response to Data Loss Prevention Incidents Panel

Components	Description
Dimension (X axis)	Blocked Status
Measure (Y axis)	Blocked Status ID (Count)
Chart style	3D-pie chart
Properties	The Properties button on the title bar opens the Panel Properties

You can click on a segment of the pie chart to drill down and view a table for detailed information.

The table displays the following columns:

Table E-99 Response to Data Loss Prevention Incidents

Column name	Description
Incident ID	Displays the unique ID of the Symantec Data Loss Prevention incident.
Message Type	Displays the type of Symantec Data Loss Prevention component that generated the incident.
Blocked Status	Displays the string value that indicates if the message was blocked.
Policy Name	Displays the policy name that was violated.
Detection Date	Displays the date and time the Symantec Data Loss Prevention incident was detected.
Status	Displays the status of the incident.
Severity	Displays the severity of the incident.

From the Dashboard Taskbar you can do the following:

Table E-100 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.

Table E-100 Dashboard Taskbar *(continued)*

Option Name	Description
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The following options are available at the top of the drill through page:

Table E-101 General options

Options	Descriptions
Back to chart	Lets you return to the 3D-pie chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Top 10 Data Loss Prevention Incidents by Protocol

The **Top 10 Data Loss Prevention Incidents by Protocol** panel displays the top 10 protocols categorized by the incident count. The panel displays a 2D-bar chart.

Symantec Data Loss Prevention Incidents is the area of interest for the panel.

The panel displays the following information:

Table E-102 Components of the Top 10 Data Loss Prevention Incidents by Protocol Panel

Components	Description
Dimension (X axis)	Message Type
Measure (Y axis)	Message Type ID (Count)
Chart style	2D-bar chart
Properties	The Properties button on the title bar opens the Panel Properties

You can click one of the bars to drill down and view a table for detailed information.

The table displays the following columns:

Table E-103 Top 10 Data Loss Prevention Incidents by Protocol

Column name	Description
Incident ID	Displays the unique ID of the Symantec Data Loss Prevention incident.
Message Type	Displays the type of Symantec Data Loss Prevention component that generated the incident.
Policy Name	Displays the policy name.
Detection Date	Displays the date and time of the Symantec Data Loss Prevention incident was detected.
Status	Displays the status of the incident.
Originator IP	Displays the IP address of the sender of the network message.
Recipient IP	Displays the IP address of the intended recipient of the network message.
Severity	Displays the severity of the incident.

From the Dashboard Taskbar you can do the following:

Table E-104 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The following options are available at the top of the drill through page:

Table E-105 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-bar chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Top 10 Data Loss Prevention Incidents by User

The **Top 10 Data Loss Prevention Incidents by User** panel displays the top 10 users categorized by the incident count. The panel displays a 2D-bar chart.

Symantec Data Loss Prevention Incidents is the area of interest for the panel.

The panel displays the following information:

Table E-106 Components of the Top 10 Data Loss Prevention Incidents by User Panel

Components	Description
Dimension (X axis)	User Name
Measure (Y axis)	User ID (Count)
Chart style	2D-bar chart
Properties	The Properties button on the title bar opens the Panel Properties

You can click one of the bars to drill down and view a table for detailed information.

The table displays the following columns:

Table E-107 Top 10 Data Loss Prevention Incidents by User

Column name	Description
Incident ID	Displays the unique ID of the Symantec Data Loss Prevention incident.
Message Type	Displays the type of Symantec Data Loss Prevention component that generated the incident.
User Name	Displays the name of the endpoint user. (For example, MYDOMAIN\bsmith)
Policy Name	Displays the policy name.
Blocked Status	Displays the string value that indicates if the message was blocked.
Detection Date	Displays the date and time of the Symantec Data Loss Prevention incident was detected.
Status	Displays the status of the incident.

Table E-107 Top 10 Data Loss Prevention Incidents by User *(continued)*

Column name	Description
Severity	Displays the severity of the incident.
Application Name	Displays the name of the application that caused the incident.
Application Path	Displays the path of the application that caused the incident.

The following options are available at the top of the drill through page:

Table E-108 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-bar chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Compliance Score for HIPAA Mandate

The **Compliance Score for HIPAA Mandate** panel displays the percentage of average of control status evaluated against assets. This panel displays a 2D-pie chart about the Health Insurance Portability and Accountability Act (HIPAA) mandate.

Mandate and Policy Compliance Management is the area of interest for this panel.

The panel displays the following information:

Table E-109 Components for the Compliance Score for HIPAA Mandate Panel

Components	Description
Chart style	2D-pie chart

Table E-109 Components for the Compliance Score for HIPAA Mandate Panel *(continued)*

Components	Description
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the compliance score for the HIPAA mandate:

```
Standard1 has Controls, Control1, Control2, and Control3.
```

```
Control1, Control2, and Control3 are mapped to Mandate through Control
Statement1.
```

```
Control1, Control2, and Control3 are evaluated against Asset1, Asset2
and Asset3.
```

Table E-110 Evaluation results for controls evaluated against assets

Control/Asset	Asset1	Asset2	Asset3
Control1	Fail	Fail	Fail
Control2	Unknown	Fail	Fail
Control3	Pass	Pass	Pass

The result status for Asset1 - Pass = 1, Fail = 1, Unknown = 1, and Error = 0.

The result status for Asset2 - Pass = 1, Fail = 2, Unknown = 0, and Error = 0.

The result status for Asset3 - Pass = 1, Fail = 2, Unknown = 0, and Error = 0.

The following formula calculates the percentage for each result status per asset:

```
Asset1 Pass = (P count / (P count + F count + U count + E count)) x
100%
```

```
Asset1 Pass = (1 / (1 + 1 + 1 + 0)) x 100%
```

```
Asset1 Pass = 33.33%
```

```
Asset1 Fail = (F count / (P count + F count + U count + E count)) x
100%
```

```
Asset1 Fail = (1 / (1 + 1 + 1 + 0)) x 100%
```

```
Asset1 Fail = 33.33%
```

Asset1 Unknown = (U count / (P count + F count + U count + E count)) x 100%

Asset1 Unknown = (1 / (1 + 1 + 1 + 0)) x 100%

Asset1 Unknown = 33.33%

The following is the compliance score percentage for Asset1:

Pass = 33.33%, Fail = 33.33%, Unknown = 33.33%.

Similar calculations are done for Asset2 and Asset3.

The following is the compliance score percentage for Asset2:

Pass = 33.33%, Fail = 66.67%, Unknown = 0%.

The following is the compliance score percentage for Asset3:

Pass = 33.33%, Fail = 66.67%, Unknown = 0%.

The following formula calculates the average compliance score percentage of the mandate:

Average Mandate percent Result Status = (sum of all asset result status) / (Count of total assets)

Average Mandate percent Pass = (Asset1 Pass + Asset2 Pass + Asset2 Pass) / 3

Average Mandate percent Pass = (33.33% + 33.33% + 33.33%) / 3

Average Mandate percent Pass = 33.33%

Average Mandate percent Fail = (Asset1 Fail + Asset2 Fail + Asset2 Fail) / 3

Average Mandate percent Fail = (33.33% + 66.67% + 66.67%) / 3

Average Mandate percent Fail = 55.56%

Average Mandate percent Unknown = (Asset1 Unknown + Asset2 Unknown + Asset2 Unknown) / 3

Average Mandate percent Unknown = (33.33% + 0 + 0) / 3

Average Mandate percent Unknown = 11.11%

Therefore, the panels displays the average Mandate percent Result Status as follows:

Pass = 33.33%, Fail = 55.56%, and Unknown = 11.11%.

The panel does not reflect the result status for the controls which do not have instances.

You can click on the pie to drill down and view a table for detailed information.

The table displays the following columns:

Table E-111 Compliance Score for HIPAA Mandate

Column Name	Description
Mandate Asset Compliance	Displays the individual compliance for that result type. The Mandate Asset Compliance opens a page with detailed information on the control that are evaluated per asset.
Asset Compliance Score	Displays the consolidated compliance score of the asset.
Mandate Name	Displays the name of the mandate. The Mandate Name opens a page with detailed information on the mandate.
Asset Name	Displays the name of the asset. The Asset Name opens a page with detailed information on the asset.
Asset Type	Displays the type of the asset. For example, Windows Machine, UNIX Machine, and so forth.
Asset Owner	Displays the name of the owner of the asset.
Asset Location	Displays the location of the asset.
Compliance Result Name	Displays the result of the compliance score. For example, Mandate asset compliance pass, fail, and so forth.

From the Dashboard Taskbar you can do the following:

Table E-112 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.

Table E-112 Dashboard Taskbar *(continued)*

Option Name	Description
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-113 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-pie chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Control Status Trends for HIPAA Mandate

The **Control Status Trends for HIPAA Mandate** panel displays a control count for all available control result status for all the controls mapped to control statement. The Health Insurance Portability and Accountability Act (HIPAA) trend is based on the control count against the assets mapped to the HIPAA mandate. This is done at the end of every month. The panel displays a 2D-line chart.

Mandate and Policy Compliance Management is the area of interest for this panel.

The panel displays the following information:

Table E-114 Components for the Control Status Trends for HIPAA Mandate Panel

Components	Description
Dimension (X axis)	Trends by End of Month
Measure (Y axis)	Instances
Chart style	2D-line chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the control status trend for HIPAA mandate:

`The Control statement1 is mapped to 5 controls, Control1, Control2, Control3, Control4, and Control5.`

`Mandate mapped to Control statement1.`

The following table displays the January 2011 evaluation of Mandate against the assets, Asset1, Asset2, and Asset3:

Table E-115 January 2011 Control evaluation details

Asset/Control	Control1	Control2	Control3	Control4	Control5
Asset1	Pass	Fail	Pass	NA	Unknown
Asset2	Fail	Fail	Error	Pass	NA
Asset3	Fail	Pass	Fail	Fail	Unknown

For January 2011 the panel shows following control count for each control result status:

`Pass = 4, Fail = 6, Error = 1, Unknown = 2, Not Applicable = 2.`

`The Control statement2 is mapped to 5 controls, Control1, Control2, Control3, Control4, and Control5.`

`Mandate mapped to Control statement2.`

The following table displays the February 2011 evaluation of Mandate against the assets, Asset1, Asset2, and Asset3:

Table E-116 February 2011 Control evaluation details

Asset/Control	Control1	Control2	Control3	Control4	Control5
Asset1	Fail	Fail	Pass	Unknown	NA
Asset2	Fail	Unknown	Pass	Pass	Fail
Asset3	Pass	Error	Fail	NA	Fail

For February 2011 the panel shows following control count for each control result status:

```
Pass = 4, Fail = 6, Error = 1, Unknown = 2, Not Applicable = 2
```

Therefore, at the end of February 2011 the trend panel displays the following control count result based on control count for Mandate as:

```
Pass = 4, Fail = 6, Error = 1, Unknown = 2, Not Applicable = 2
```

From the Dashboard Taskbar you can do the following:

Table E-117 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

Mapped Policies to HIPAA Mandate

The **Mapped Policies to HIPAA Mandate** panel displays the total number of control statements mapped to the policies and the mandate. This panel displays a 2D-bar chart about the Health Insurance Portability and Accountability Act (HIPAA) mandate.

Mandate and Policy Compliance Management is the area of interest for this panel.

The panel displays the following information:

Table E-118 Components for the Mapped Policies to HIPAA Mandate Panel

Components	Description
Dimension (X axis)	Policy Name
Measure (Y axis)	Count of Mapped Control
Chart style	2D-bar chart
Properties	The Properties button on the title bar opens the Panel Properties
Orientation Options	Lets you drill down to another chart panel.

The following is an example to determine the number of mapped policies to the HIPAA mandate:

`Control statements, Control statement1 is mapped to policy P1.`

`Control statements, Control statement2 is mapped to policy P1 and P2.`

`Control statements, Control statement3 is mapped to policy P1 and P2.`

`Control statement1, Control statement2, and Control statement3 are mapped to Mandate.`

`The total number of control statements mapped to P1 = 3.`

`The total number of control statements mapped to P2 = 2.`

Therefore, the panel displays the count of control statements for each policy as a separate bar.

You can click the bar to drill down and view a table for detailed information.

The table displays the following columns:

Table E-119 Mapped Policies to HIPAA Mandate

Column Name	Description
Policy Name	Displays the name of the policy. The Policy Name opens a page with detailed information on the selected policy.
Control Statement Name	Displays the name of the control statement. The Control Statement Name opens a page with detailed information on the selected control statement.
Mandate Name	Displays the name of the mandate. The Mandate Name opens a page with detailed information on the selected mandate.

From the Dashboard Taskbar you can do the following:

Table E-120 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-121 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-bar chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Coverage of Control Statements in HIPAA Mandate

The **Coverage of Control Statements in HIPAA Mandate** panel displays the percentage of mapped and unmapped control statements to the mandate. This panel displays a 2D-pie chart about the Health Insurance Portability and Accountability Act (HIPAA) mandate.

Mandate and Policy Compliance Management is the area of interest for this panel.

The panel displays the following information:

Table E-122 Components for the Coverage of Control Statements in HIPAA Mandate Panel

Components	Description
Chart style	2D-pie chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the percentage of mapped and unmapped control statements in HIPAA mandate:

```
Controls, Control1, Control2, and Control3 are mapped to Mandate
through Control Statement1.

Control Statement2 and Control Statement3 are mapped to Mandate, but
do not have mapped controls.

The total number of mapped control statements to Mandate is 1.
The total number of unmapped control statements to Mandate is 2.
```

Therefore, the panel displays the percentage of the total mapped controls statements and the total unmapped controls statements.

You can click the pie to drill down and view a table for detailed information.

The table displays the following columns:

Table E-123 Coverage of Control Statements in HIPAA Mandate

Column Name	Description
Control Statement Count	Displays the count of the control statement.
Mandate Name	Displays the name of the mandate. The Mandate Name opens a page with detailed information on the selected mandate.
Mapped Unmapped Type	Displays whether control statement is mapped or unmapped.

From the Dashboard Taskbar you can do the following:

Table E-124 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-125 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-pie chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Top 10 Failed Control Statements for HIPAA Mandate

The **Top 10 Failed Control Statements for HIPAA Mandate** panel displays, in descending order, the top 10 failed control statements that are mapped to a single mandate. This panel displays a 2D-bar chart about the Health Insurance Portability and Accountability Act (HIPAA) mandate.

Mandate and Policy Compliance Management is the area of interest for this panel.

The panel displays the following information:

Table E-126 Components for the Top 10 Failed Control Statements for HIPAA Mandate Panel

Components	Description
Dimension (X axis)	Control Statement
Measure (Y axis)	Count of Controls
Chart style	2D-bar chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine which control statements have failed controls mapped to it:

```
Controls C1, C2, and C3 are mapped to Control statement1 which is
mapped to Mandate1.
```

```
Controls C4, C5, and C6 are mapped to Control statement2 which is
mapped to Mandate2.
```

Controls have the following result for assets:

Table E-127 Control Statement1

Asset/Control	C1	C2	C3
Asset1	Fail	Fail	Pass
Asset2	Fail	Unknown	Pass

The result for Control statement1 is three failed control counts.

Control statement2 has the following result for assets:

Table E-128 Control Statement2

Asset/Control	C4	C5	C6
Asset3	Pass	Error	Pass
Asset4	Fail	Unknown	Pass

The result for Control statement2 is one failed control counts.

Therefore, the panel displays the top 10 failed control statements in descending order with respect to failed control count.

You can click one of the bars to drill down and view a table for detailed information.

The table displays the following columns:

Table E-129 Top 10 Failed Control Statements for HIPAA Mandate

Column Name	Description
Control Statement	Displays the failed control statement. The Control Statement opens a page with detailed information on the control statement.
Mandate Name	Displays the name of the mandate. The Mandate Name opens a page with detailed information on the mandate.

Table E-129 Top 10 Failed Control Statements for HIPAA Mandate *(continued)*

Column Name	Description
Control Name	Displays the name of control. The Control Name opens a page with detailed information on the control.
Control Type	Displays the type of control. For example, checks RAM question, Third-party control, SCAP rule, and so forth.
Evaluation Date	Displays the date and time of the evaluation.

From the Dashboard Taskbar you can do the following:

Table E-130 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-131 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-column chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Compliance Score for ISO Mandate

The **Compliance Score for ISO Mandate** panel displays the percentage of average of control status evaluated against assets. This panel displays a 2D-pie chart about the International Organization for Standardization (ISO) mandate.

Mandate and Policy Compliance Management is the area of interest for this panel.

Note: The supported versions of ISO Mandate for predefined **Compliance Analysis - ISO Mandate** dashboard and its panels are as follows:

- ISO/IEC 27001:2005
- ISO/IEC 27002:2005

The panel displays the following information:

Table E-132 Components for the Compliance Score for ISO Mandate Panel

Components	Description
Chart style	2D-pie chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the compliance score for the ISO mandate:

```
Standard1 has Controls, Control1, Control2, and Control3.
```

```
Control1, Control2, and Control3 are mapped to Mandate through Control
Statement1.
```

```
Control1, Control2, and Control3 are evaluated against Asset1, Asset2
and Asset3.
```

Table E-133 Evaluation results for controls evaluated against assets

Control/Asset	Asset1	Asset2	Asset3
Control1	Fail	Fail	Fail
Control2	Unknown	Fail	Fail
Control3	Pass	Pass	Pass

The result status for Asset1 - Pass = 1, Fail = 1, Unknown = 1, and Error = 0.

The result status for Asset2 - Pass = 1, Fail = 2, Unknown = 0, and Error = 0.

The result status for Asset3 - Pass = 1, Fail = 2, Unknown = 0, and Error = 0.

The following formula calculates the percentage for each result status per asset:

```
Asset1 Pass = (P count / (P count + F count + U count + E count)) x
100%
```

```
Asset1 Pass = (1 / (1 + 1 + 1 + 0)) x 100%
```

```
Asset1 Pass = 33.33%
```

```
Asset1 Fail = (F count / (P count + F count + U count + E count)) x
100%
```

```
Asset1 Fail = (1 / (1 + 1 + 1 + 0)) x 100%
```

```
Asset1 Fail = 33.33%
```

```
Asset1 Unknown = (U count / (P count + F count + U count + E count))
x 100%
```

```
Asset1 Unknown = (1 / (1 + 1 + 1 + 0)) x 100%
```

```
Asset1 Unknown = 33.33%
```

The following is the compliance score percentage for Asset1:

```
Pass = 33.33%, Fail = 33.33%, Unknown = 33.33%.
```

Similar calculations are done for Asset2 and Asset3.

The following is the compliance score percentage for Asset2:

```
Pass = 33.33%, Fail = 66.67%, Unknown = 0%.
```

The following is the compliance score percentage for Asset3:

`Pass = 33.33%, Fail = 66.67%, Unknown = 0%.`

The following formula calculates the average compliance score percentage of the mandate:

```
Average Mandate percent Result Status = (sum of all asset result
status) / (Count of total assets)

Average Mandate percent Pass = (Asset1 Pass + Asset2 Pass + Asset2
Pass) / 3

Average Mandate percent Pass = (33.33% + 33.33% + 33.33%) / 3

Average Mandate percent Pass = 33.33%

Average Mandate percent Fail = (Asset1 Fail + Asset2 Fail + Asset2
Fail) / 3

Average Mandate percent Fail = (33.33% + 66.67% + 66.67%) / 3

Average Mandate percent Fail = 55.56%

Average Mandate percent Unknown = (Asset1 Unknown + Asset2 Unknown
+ Asset2 Unknown) / 3

Average Mandate percent Unknown = (33.33% + 0 + 0) / 3

Average Mandate percent Unknown = 11.11%
```

Therefore, the panels displays the average Mandate percent Result Status as follows:

`Pass = 33.33%, Fail = 55.56%, and Unknown = 11.11%.`

The panel does not reflect the result status for the controls which do not have instances.

You can click on the pie to drill down and view a table for detailed information.

The table displays the following columns:

Table E-134 Compliance Score for ISO Mandate

Column Name	Description
Mandate Asset Compliance	Displays the individual compliance for that result type. The Mandate Asset Compliance opens a page with detailed information on the control that are evaluated per asset.

Table E-134 Compliance Score for ISO Mandate *(continued)*

Column Name	Description
Asset Compliance Score	Displays the consolidated compliance score of the asset.
Mandate Name	Displays the name of the mandate. The Mandate Name opens a page with detailed information on the mandate.
Asset Name	Displays the name of the asset. The Asset Name opens a page with detailed information on the asset.
Asset Type	Displays the type of the asset. For example, Windows Machine, UNIX Machine, and so forth.
Asset Owner	Displays the name of the owner of the asset.
Asset Location	Displays the location of the asset.
Compliance Result Name	Displays the result of the compliance score. For example, Mandate asset compliance pass, fail, and so forth.

From the Dashboard Taskbar you can do the following:

Table E-135 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.

Table E-135 Dashboard Taskbar *(continued)*

Option Name	Description
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-136 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-pie chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Control Status Trends for ISO Mandate

The **Control Status Trends for ISO Mandates** panel displays a control count for all available control result status for all the controls mapped to control statement. The International Organization for Standardization (ISO) trend is based on the control count against assets mapped to the ISO mandate. This is done at the end of every month. The panel displays a 2D-line chart.

Mandate and Policy Compliance Management is the area of interest for this panel.

Note: The supported versions of ISO Mandate for predefined **Compliance Analysis - ISO Mandate** dashboard and its panels are as follows:

- ISO/IEC 27001:2005
- ISO/IEC 27002:2005

The panel displays the following information:

Table E-137 Components for the Control Status Trends for ISO Mandate Panel

Components	Description
Dimension (X axis)	Trends by End of Month
Measure (Y axis)	Instances
Chart style	2D-line chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the control status trend for ISO mandate:

```
The Control statement1 is mapped to 5 controls, Control1, Control2,
Control3, Control4, and Control5.
```

```
Mandate mapped to Control statement1.
```

The following table displays the January 2011 evaluation of Mandate against the assets, Asset1, Asset2, and Asset3:

Table E-138 January 2011 Control evaluation details

Asset/Control	Control1	Control2	Control3	Control4	Control5
Asset1	Pass	Fail	Pass	NA	Unknown
Asset2	Fail	Fail	Error	Pass	NA
Asset3	Fail	Pass	Fail	Fail	Unknown

For January 2011 the panel shows following control count for each control result status:

```
Pass = 4, Fail = 6, Error = 1, Unknown = 2, Not Applicable = 2.
```

```
The Control statement2 is mapped to 5 controls, Control1, Control2,
Control3, Control4, and Control5.
```

```
Mandate mapped to Control statement2.
```

The following table displays the February 2011 evaluation of Mandate against the assets, Asset1, Asset2, and Asset3:

Table E-139 February 2011 Control evaluation details

Asset/Control	Control1	Control2	Control3	Control4	Control5
Asset1	Fail	Fail	Pass	Unknown	NA
Asset2	Fail	Unknown	Pass	Pass	Fail
Asset3	Pass	Error	Fail	NA	Fail

For February 2011 the panel shows following control count for each control result status:

```
Pass = 4, Fail = 6, Error = 1, Unknown = 2, Not Applicable = 2
```

Therefore, at the end of February 2011 the trend panel displays the following control count result based on control count for Mandate as:

```
Pass = 4, Fail = 6, Error = 1, Unknown = 2, Not Applicable = 2
```

From the Dashboard Taskbar you can do the following:

Table E-140 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

Mapped Policies to ISO Mandate

The **Mapped Policies to ISO Mandate** panel displays the total number of control statements mapped to the policies and the mandate. This panel displays a 2D-bar chart about the International Organization for Standardization (ISO) mandate.

Mandate and Policy Compliance Management is the area of interest for this panel.

Note: The supported versions of ISO Mandate for predefined **Compliance Analysis - ISO Mandate** dashboard and its panels are as follows:

- ISO/IEC 27001:2005
- ISO/IEC 27002:2005

The panel displays the following information:

Table E-141 Components for the Mapped Policies to ISO Mandate Panel

Components	Description
Dimension (X axis)	Policy Name
Measure (Y axis)	Count of Mapped Control
Chart style	2D-bar chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the number of mapped policies to the ISO mandate:

```
Control statements, Control statement1 is mapped to policy P1.

Control statements, Control statement2 is mapped to policy P1 and
P2.

Control statements, Control statement3 is mapped to policy P1 and
P2.

Control statement1, Control statement2, and Control statement3 are
mapped to Mandate.

The total number of control statements mapped to P1 = 3.

The total number of control statements mapped to P2 = 2.
```

Therefore, the panel displays the count of control statements for each policy as a separate bar.

You can click the bar to drill down and view a table for detailed information.

The table displays the following columns:

Table E-142 Mapped Policies to ISO Mandate

Column Name	Description
Policy Name	Displays the name of the policy. The Policy Name opens a page with detailed information on the selected policy.
Control Statement Name	Displays the name of the control statement. The Control Statement Name opens a page with detailed information on the selected control statement.
Mandate Name	Displays the name of the mandate. The Mandate Name opens a page with detailed information on the selected mandate.

From the Dashboard Taskbar you can do the following:

Table E-143 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-144 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-bar chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Coverage of Control Statements in ISO Mandate

The **Coverage of Control Statements in ISO Mandate** panel displays the percentage of mapped and unmapped control statements to the mandate. This panel displays a 2D-pie chart about the International Organization for Standardization (ISO) mandate.

Mandate and Policy Compliance Management is the area of interest for this panel.

Note: The supported versions of ISO Mandate for predefined **Compliance Analysis - ISO Mandate** dashboard and its panels are as follows:

- ISO/IEC 27001:2005
- ISO/IEC 27002:2005

The panel displays the following information:

Table E-145 Components for the Coverage of Control Statements in ISO Mandate Panel

Components	Description
Chart style	2D-pie chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the percentage of mapped and unmapped control statements in ISO mandate:

```
Controls, Control1, Control2, and Control3 are mapped to Mandate
through Control Statement1.

Control Statement2 and Control Statement3 do not have mapped controls.

The total number of mapped control statements to Mandate is 1.

The total number of unmapped control statements to Mandate is 2.
```

Therefore, the panel displays the percentage of the total mapped controls statements and the total unmapped controls statements.

You can click the pie to drill down and view a table for detailed information.

The table displays the following columns:

Table E-146 Coverage of Control Statements in ISO Mandate

Column Name	Description
Control Statement Count	Displays the count of the control statement.
Mandate Name	Displays the name of the mandate. The Mandate Name opens a page with detailed information on the selected mandate.
Mapped Unmapped Type	Displays whether control statement is mapped or unmapped.

From the Dashboard Taskbar you can do the following:

Table E-147 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.

Table E-147 Dashboard Taskbar *(continued)*

Option Name	Description
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-148 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-pie chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Top 10 Failed Control Statements for ISO Mandate

The **Top 10 Failed Control Statements for ISO Mandate** panel displays, in descending order, the top 10 failed control statements that are mapped to a single mandate. This panel displays a 2D-bar chart about the International Organization for Standardization (ISO) mandate.

Mandate and Policy Compliance Management is the area of interest for this panel.

Note: The supported versions of ISO Mandate for predefined **Compliance Analysis - ISO Mandate** dashboard and its panels are as follows:

- ISO/IEC 27001:2005

- ISO/IEC 27002:2005

The panel displays the following information:

Table E-149 Components for the Top 10 Failed Control Statements for ISO Mandate Panel

Components	Description
Dimension (X axis)	Control Statement
Measure (Y axis)	Count of Controls
Chart style	2D-bar chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine which control statements have failed controls mapped to it:

```
Controls C1, C2, and C3 are mapped to Control statement1 which is
mapped to Mandate1.
```

```
Controls C4, C5, and C6 are mapped to Control statement2 which is
mapped to Mandate2.
```

Controls have the following result for assets:

Table E-150 Control Statement1

Asset/Control	C1	C2	C3
Asset1	Fail	Fail	Pass
Asset2	Fail	Unknown	Pass

The result for Control statement1 is three failed control counts.

Control statement2 has the following result for assets:

Table E-151 Control Statement2

Asset/Control	C4	C5	C6
Asset3	Pass	Error	Pass
Asset4	Fail	Unknown	Pass

The result for Control statement2 is one failed control counts.

Therefore, the panel displays the top 10 failed control statements in descending order with respect to failed control count.

You can click one of the bars to drill down and view a table for detailed information.

The table displays the following columns:

Table E-152 Top 10 Failed Control Statements for ISO Mandate

Column Name	Description
Control Statement	Displays the failed control statement. The Control Statement opens a page with detailed information on the control statement.
Mandate Name	Displays the name of the mandate. The Mandate Name opens a page with detailed information on the mandate.
Control Name	Displays the name of control. The Control Name opens a page with detailed information on the control.
Control Type	Displays the type of control. For example, checks RAM question, Third-party control, SCAP rule, and so forth.
Evaluation Date	Displays the date and time of the evaluation.

From the Dashboard Taskbar you can do the following:

Table E-153 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.

Table E-153 Dashboard Taskbar *(continued)*

Option Name	Description
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-154 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-column chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Compliance Score for NERC Mandate

The **Compliance Score for NERC Mandate** panel displays the percentage of average of control status evaluated against assets. This panel displays a 2D-pie chart about the North American Electric Reliability Corporation (NERC) mandate.

Mandate and Policy Compliance Management is the area of interest for this panel.

The panel displays the following information:

Table E-155 Components for the Compliance Score for NERC Mandate Panel

Components	Description
Chart style	2D-pie chart

Table E-155 Components for the Compliance Score for NERC Mandate Panel *(continued)*

Components	Description
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the compliance score for the NERC mandate:

```
Standard1 has Controls, Control1, Control2, and Control3.
```

```
Control1, Control2, and Control3 are mapped to Mandate through Control
Statement1.
```

```
Control1, Control2, and Control3 are evaluated against Asset1, Asset2
and Asset3.
```

Table E-156 Evaluation results for controls evaluated against assets

Control/Asset	Asset1	Asset2	Asset3
Control1	Fail	Fail	Fail
Control2	Unknown	Fail	Fail
Control3	Pass	Pass	Pass

The result status for Asset1 - Pass = 1, Fail = 1, Unknown = 1, and Error = 0.

The result status for Asset2 - Pass = 1, Fail = 2, Unknown = 0, and Error = 0.

The result status for Asset3 - Pass = 1, Fail = 2, Unknown = 0, and Error = 0.

The following formula calculates the percentage for each result status per asset:

```
Asset1 Pass = (P count / (P count + F count + U count + E count)) x
100%
```

```
Asset1 Pass = (1 / (1 + 1 + 1 + 0)) x 100%
```

```
Asset1 Pass = 33.33%
```

```
Asset1 Fail = (F count / (P count + F count + U count + E count)) x
100%
```

```
Asset1 Fail = (1 / (1 + 1 + 1 + 0)) x 100%
```

```
Asset1 Fail = 33.33%
```

Asset1 Unknown = (U count / (P count + F count + U count + E count)) x 100%

Asset1 Unknown = (1 / (1 + 1 + 1 + 0)) x 100%

Asset1 Unknown = 33.33%

The following is the compliance score percentage for Asset1:

Pass = 33.33%, Fail = 33.33%, Unknown = 33.33%.

Similar calculations are done for Asset2 and Asset3.

The following is the compliance score percentage for Asset2:

Pass = 33.33%, Fail = 66.67%, Unknown = 0%.

The following is the compliance score percentage for Asset3:

Pass = 33.33%, Fail = 66.67%, Unknown = 0%.

The following formula calculates the average compliance score percentage of the mandate:

Average Mandate percent Result Status = (sum of all asset result status) / (Count of total assets)

Average Mandate percent Pass = (Asset1 Pass + Asset2 Pass + Asset2 Pass) / 3

Average Mandate percent Pass = (33.33% + 33.33% + 33.33%) / 3

Average Mandate percent Pass = 33.33%

Average Mandate percent Fail = (Asset1 Fail + Asset2 Fail + Asset2 Fail) / 3

Average Mandate percent Fail = (33.33% + 66.67% + 66.67%) / 3

Average Mandate percent Fail = 55.56%

Average Mandate percent Unknown = (Asset1 Unknown + Asset2 Unknown + Asset2 Unknown) / 3

Average Mandate percent Unknown = (33.33% + 0 + 0) / 3

Average Mandate percent Unknown = 11.11%

Therefore, the panels displays the average Mandate percent Result Status as follows:

Pass = 33.33%, Fail = 55.56%, and Unknown = 11.11%.

The panel does not reflect the result status for the controls which do not have instances.

You can click on the pie to drill down and view a table for detailed information.

The table displays the following columns:

Table E-157 Compliance Score for NERC Mandate

Column Name	Description
Mandate Asset Compliance	Displays the individual compliance for that result type. The Mandate Asset Compliance opens a page with detailed information on the control that are evaluated per asset.
Asset Compliance Score	Displays the consolidated compliance score of the asset.
Mandate Name	Displays the name of the mandate. The Mandate Name opens a page with detailed information on the mandate.
Asset Name	Displays the name of the asset. The Asset Name opens a page with detailed information on the asset.
Asset Type	Displays the type of the asset. For example, Windows Machine, UNIX Machine, and so forth.
Asset Owner	Displays the name of the owner of the asset.
Asset Location	Displays the location of the asset.
Compliance Result Name	Displays the result of the compliance score. For example, Mandate asset compliance pass, fail, and so forth.

From the Dashboard Taskbar you can do the following:

Table E-158 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.

Table E-158 Dashboard Taskbar *(continued)*

Option Name	Description
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-159 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-pie chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Control Status Trends for NERC Mandate

The **Control Status Trends for NERC Mandates** panel displays a control count for all available control result status for all the controls mapped to control statement. The North American Electric Reliability Corporation (NERC) trend is based on the control count against assets mapped to the NERC mandate. This is done at the end of every month. The panel displays a 2D-line chart.

Mandate and Policy Compliance Management is the area of interest for this panel.

The panel displays the following information:

Table E-160 Components for the Control Status Trends for NERC Mandate Panel

Components	Description
Dimension (X axis)	Trends by End of Month
Measure (Y axis)	Instances
Chart style	2D-line chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the control status trend for NERC mandate:

```
The Control statement1 is mapped to 5 controls, Control1, Control2,
Control3, Control4, and Control5.
```

```
Mandate mapped to Control statement1.
```

The following table displays the January 2011 evaluation of Mandate against the assets, Asset1, Asset2, and Asset3:

Table E-161 January 2011 Control evaluation details

Asset/Control	Control1	Control2	Control3	Control4	Control5
Asset1	Pass	Fail	Pass	NA	Unknown
Asset2	Fail	Fail	Error	Pass	NA
Asset3	Fail	Pass	Fail	Fail	Unknown

For January 2011 the panel shows following control count for each control result status:

```
Pass = 4, Fail = 6, Error = 1, Unknown = 2, Not Applicable = 2.
```

```
The Control statement2 is mapped to 5 controls, Control1, Control2,
Control3, Control4, and Control5.
```

```
Mandate mapped to Control statement2.
```

The following table displays the February 2011 evaluation of Mandate against the assets, Asset1, Asset2, and Asset3:

Table E-162 February 2011 Control evaluation details

Asset/Control	Control1	Control2	Control3	Control4	Control5
Asset1	Fail	Fail	Pass	Unknown	NA
Asset2	Fail	Unknown	Pass	Pass	Fail
Asset3	Pass	Error	Fail	NA	Fail

For February 2011 the panel shows following control count for each control result status:

```
Pass = 4, Fail = 6, Error = 1, Unknown = 2, Not Applicable = 2
```

Therefore, at the end of February 2011 the trend panel displays the following control count result based on control count for Mandate as:

```
Pass = 4, Fail = 6, Error = 1, Unknown = 2, Not Applicable = 2
```

Mapped Policies to NERC Mandate

The **Mapped Policies to NERC Mandate** panel displays the total number of control statements mapped to the policies and the mandate. This panel displays a 2D-bar chart about the North American Electric Reliability Corporation (NERC) mandate.

Mandate and Policy Compliance Management is the area of interest for this panel.

The panel displays the following information:

Table E-163 Components for the Mapped Policies to NERC Mandate Panel

Components	Description
Dimension (X axis)	Policy Name
Measure (Y axis)	Count of Mapped Control
Chart style	2D-bar chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the number of mapped policies to the NERC mandate:

```
Control statements, Control statement1 is mapped to policy P1.
```

```
Control statements, Control statement2 is mapped to policy P1 and
P2.
```

```
Control statements, Control statement3 is mapped to policy P1 and
P2.

Control statement1, Control statement2, and Control statement3 are
mapped to Mandate.

The total number of control statements mapped to P1 = 3.

The total number of control statements mapped to P2 = 2.
```

Therefore, the panel displays the count of control statements for each policy as a separate bar.

You can click the bar to drill down and view a table for detailed information.

The table displays the following columns:

Table E-164 Mapped Policies to NERC Mandate

Column Name	Description
Policy Name	Displays the name of the policy. The Policy Name opens a page with detailed information on the selected policy.
Control Statement Name	Displays the name of the control statement. The Control Statement Name opens a page with detailed information on the selected control statement.
Mandate Name	Displays the name of the mandate. The Mandate Name opens a page with detailed information on the selected mandate.

From the Dashboard Taskbar you can do the following:

Table E-165 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.

Table E-165 Dashboard Taskbar *(continued)*

Option Name	Description
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-166 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-bar chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Coverage of Control Statements in NERC Mandate

The **Coverage of Control Statements in NERC Mandate** panel displays the percentage of mapped and unmapped control statements to the mandate. This panel displays a 2D-pie chart about the North American Electric Reliability Corporation (NERC) mandate.

Mandate and Policy Compliance Management is the area of interest for this panel.

The panel displays the following information:

Table E-167 Components for the Coverage of Control Statements in NERC Mandate Panel

Components	Description
Chart style	2D-pie chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the percentage of mapped and unmapped control statements in NERC mandate:

```
Controls, Control1, Control2, and Control3 are mapped to MANDATE
through Control Statement1.
```

```
Control Statement2 and Control Statement3 do not have mapped controls.
```

```
The total number of mapped control statements to Mandate is 1.
```

```
The total number of unmapped control statements to Mandate is 2.
```

Therefore, the panel displays the percentage of the total mapped controls statements and the total unmapped controls statements.

You can click the pie to drill down and view a table for detailed information.

The table displays the following columns:

Table E-168 Coverage of Control Statements in NERC Mandate

Column Name	Description
Control Statement Count	Displays the count of the control statement.
Mandate Name	Displays the name of the mandate. The Mandate Name opens a page with detailed information on the selected mandate.
Mapped Unmapped Type	Displays whether control statement is mapped or unmapped.

From the Dashboard Taskbar you can do the following:

Table E-169 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.

Table E-169 Dashboard Taskbar *(continued)*

Option Name	Description
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-170 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-pie chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Top 10 Failed Control Statements for NERC Mandate

The **Top 10 Failed Control Statements for NERC Mandates** panel displays, in descending order, the top 10 failed control statements that are mapped to a single mandate. This panel displays a 2D-bar chart about the North American Electric Reliability Corporation (NERC) mandate.

Mandate and Policy Compliance Management is the area of interest for this panel.

The panel displays the following information:

Table E-171 Components for the Top 10 Failed Control Statements for NERC Mandate Panel

Components	Description
Dimension (X axis)	Control Statement
Measure (Y axis)	Count of Controls
Chart style	2D-bar chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine which control statements have failed controls mapped to it

```
Controls C1, C2, and C3 are mapped to Control statement1 which is
mapped to Mandate1.
```

```
Controls C4, C5, and C6 are mapped to Control statement2 which is
mapped to Mandate2.
```

Controls have the following result for assets:

Table E-172 Control Statement1

Asset/Control	C1	C2	C3
Asset1	Fail	Fail	Pass
Asset2	Fail	Unknown	Pass

The result for Control statement1 is three failed control counts.

Control statement2 has the following result for assets:

Table E-173 Control Statement2

Asset/Control	C4	C5	C6
Asset3	Pass	Error	Pass
Asset4	Fail	Unknown	Pass

The result for Control statement2 is one failed control counts.

Therefore, the panel displays the top 10 failed control statements in descending order with respect to failed control count.

You can click one of the bars to drill down and view a table for detailed information.

The table displays the following columns:

Table E-174 Top 10 Failed Control Statements for NERC Mandate

Column Name	Description
Control Statement	Displays the failed control statement. The Control Statement opens a page with detailed information on the control statement.
Mandate Name	Displays the name of the mandate. The Mandate Name opens a page with detailed information on the mandate.
Control Name	Displays the name of control. The Control Name opens a page with detailed information on the control.
Control Type	Displays the type of control. For example, checks RAM question, Third-party control, SCAP rule, and so forth.
Evaluation Date	Displays the date and time of the evaluation.

From the Dashboard Taskbar you can do the following:

Table E-175 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.

Table E-175 Dashboard Taskbar *(continued)*

Option Name	Description
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-176 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-column chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Compliance Score for PCI Mandate

The **Compliance Score for PCI Mandate** panel displays the percentage of average of control status evaluated against assets. This panel displays a 2D-pie chart about the Payment Card Industry (PCI) mandate.

Mandate and Policy Compliance Management is the area of interest for this panel.

Note: The supported versions of PCI Mandate for predefined **Compliance Analysis - PCI Mandate** dashboard and its panels are as follows:

- PCI DSS v1.2

The panel displays the following information:

Table E-177 Components for the Compliance Score for PCI Mandate Panel

Components	Description
Chart style	2D-pie chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the compliance score for the PCI mandate:

`Standard1 has Controls, Control1, Control2, and Control3.`

`Control1, Control2, and Control3 are mapped to Mandate through Control Statement1.`

`Control1, Control2, and Control3 are evaluated against Asset1, Asset2 and Asset3.`

Table E-178 Evaluation results for controls evaluated against assets

Control/Asset	Asset1	Asset2	Asset3
Control1	Fail	Fail	Fail
Control2	Unknown	Fail	Fail
Control3	Pass	Pass	Pass

The result status for Asset1 - Pass = 1, Fail = 1, Unknown = 1, and Error = 0.

The result status for Asset2 - Pass = 1, Fail = 2, Unknown = 0, and Error = 0.

The result status for Asset3 - Pass = 1, Fail = 2, Unknown = 0, and Error = 0.

The following formula calculates the percentage for each result status per asset:

`Asset1 Pass = (P count / (P count + F count + U count + E count)) x 100%`

`Asset1 Pass = (1 / (1 + 1 + 1 + 0)) x 100%`

`Asset1 Pass = 33.33%`

`Asset1 Fail = (F count / (P count + F count + U count + E count)) x 100%`

`Asset1 Fail = (1 / (1 + 1 + 1 + 0)) x 100%`

`Asset1 Fail = 33.33%`

```
Asset1 Unknown = (U count / (P count + F count + U count + E count))
x 100%
```

```
Asset1 Unknown = (1 / (1 + 1 + 1 + 0)) x 100%
```

```
Asset1 Unknown = 33.33%
```

The following is the compliance score percentage for Asset1:

```
Pass = 33.33%, Fail = 33.33%, Unknown = 33.33%.
```

Similar calculations are done for Asset2 and Asset3.

The following is the compliance score percentage for Asset2:

```
Pass = 33.33%, Fail = 66.67%, Unknown = 0%.
```

The following is the compliance score percentage for Asset3:

```
Pass = 33.33%, Fail = 66.67%, Unknown = 0%.
```

The following formula calculates the average compliance score percentage of the mandate:

```
Average Mandate percent Result Status = (sum of all asset result
status) / (Count of total assets)
```

```
Average Mandate percent Pass = (Asset1 Pass + Asset2 Pass + Asset2
Pass) / 3
```

```
Average Mandate percent Pass = (33.33% + 33.33% + 33.33%) / 3
```

```
Average Mandate percent Pass = 33.33%
```

```
Average Mandate percent Fail = (Asset1 Fail + Asset2 Fail + Asset2
Fail) / 3
```

```
Average Mandate percent Fail = (33.33% + 66.67% + 66.67%) / 3
```

```
Average Mandate percent Fail = 55.56%
```

```
Average Mandate percent Unknown = (Asset1 Unknown + Asset2 Unknown
+ Asset2 Unknown) / 3
```

```
Average Mandate percent Unknown = (33.33% + 0 + 0) / 3
```

```
Average Mandate percent Unknown = 11.11%
```

Therefore, the panels displays the average Mandate percent Result Status as follows:

```
Pass = 33.33%, Fail = 55.56%, and Unknown = 11.11%.
```

The panel does not reflect the result status for the controls which do not have instances.

You can click on the pie to drill down and view a table for detailed information.

The table displays the following columns:

Table E-179 Compliance Score for PCI Mandate

Column Name	Description
Mandate Asset Compliance	Displays the individual compliance for that result type. The Mandate Asset Compliance opens a page with detailed information on the control that are evaluated per asset.
Asset Compliance Score	Displays the consolidated compliance score of the asset.
Mandate Name	Displays the name of the mandate. The Mandate Name opens a page with detailed information on the mandate.
Asset Name	Displays the name of the asset. The Asset Name opens a page with detailed information on the asset.
Asset Type	Displays the type of the asset. For example, Windows Machine, UNIX Machine, and so forth.
Asset Owner	Displays the name of the owner of the asset.
Asset Location	Displays the location of the asset.
Compliance Result Name	Displays the result of the compliance score. For example, Mandate asset compliance pass, fail, and so forth.

From the Dashboard Taskbar you can do the following:

Table E-180 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.

Table E-180 Dashboard Taskbar *(continued)*

Option Name	Description
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-181 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-pie chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Control Status Trends for PCI Mandate

The **Control Status Trends for PCI Mandates** panel displays a control count for all available control result status for all the controls mapped to control statement. The Payment Card Industry (PCI) trend is based on the control count against assets mapped to the PCI mandate at the end of every month. The panel displays a 2D-line chart.

Mandate and Policy Compliance Management is the area of interest for this panel.

Note: The supported versions of PCI Mandate for predefined **Compliance Analysis - PCI Mandate** dashboard and its panels are as follows:

- PCI DSS v1.2

The panel displays the following information:

Table E-182 Components for the Control Status Trends for PCI Mandate Panel

Components	Description
Dimension (X axis)	Trends by End of Month
Measure (Y axis)	Instances
Chart style	2D-line chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the control status trend for PCI mandate:

```
The Control statement1 is mapped to 5 controls, Control1, Control2,
Control3, Control4, and Control5.
```

```
Mandate mapped to Control statement1.
```

The following table displays the January 2011 evaluation of Mandate against the assets, Asset1, Asset2, and Asset3:

Table E-183 January 2011 Control evaluation details

Asset/Control	Control1	Control2	Control3	Control4	Control5
Asset1	Pass	Fail	Pass	NA	Unknown
Asset2	Fail	Fail	Error	Pass	NA
Asset3	Fail	Pass	Fail	Fail	Unknown

For January 2011 the panel shows following control count for each control result status:

```
Pass = 4, Fail = 6, Error = 1, Unknown = 2, Not Applicable = 2.
```

```
The Control statement2 is mapped to 5 controls, Control1, Control2,
Control3, Control4, and Control5.
```

```
Mandate mapped to Control statement2.
```

The following table displays the February 2011 evaluation of Mandate against the assets, Asset1, Asset2, and Asset3:

Table E-184 February 2011 Control evaluation details

Asset/Control	Control1	Control2	Control3	Control4	Control5
Asset1	Fail	Fail	Pass	Unknown	NA
Asset2	Fail	Unknown	Pass	Pass	Fail
Asset3	Pass	Error	Fail	NA	Fail

For February 2011 the panel shows following control count for each control result status:

```
Pass = 4, Fail = 6, Error = 1, Unknown = 2, Not Applicable = 2
```

Therefore, at the end of February 2011 the trend panel displays the following control count result based on control count for Mandate as:

```
Pass = 4, Fail = 6, Error = 1, Unknown = 2, Not Applicable = 2
```

From the Dashboard Taskbar you can do the following:

Table E-185 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

Mapped Policies to PCI Mandate

The **Mapped Policies to PCI Mandate** panel displays the total number of control statements mapped to the policies and the mandate. This panel displays a 2D-bar chart about the Payment Card Industry (PCI) mandate.

Mandate and Policy Compliance Management is the area of interest for this panel.

Note: The supported version of the PCI Mandate that generate the PM Metrics is as follows:

- PCI DSS v1.2

The panel displays the following information:

Table E-186 Components for the Mapped Policies to PCI Mandate Panel

Components	Description
Dimension (X axis)	Policy Name
Measure (Y axis)	Count of Mapped Control
Chart style	2D-bar chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the number of mapped policies to the PCI mandate:

```
Control statements, Control statement1 is mapped to policy P1.

Control statements, Control statement2 is mapped to policy P1 and
P2.

Control statements, Control statement3 is mapped to policy P1 and
P2.

Control statement1, Control statement2, and Control statement3 are
mapped to Mandate.

The total number of control statements mapped to P1 = 3.

The total number of control statements mapped to P2 = 2.
```

Therefore, the panel displays the count of control statements for each policy as a separate bar.

You can click the bar to drill down and view a table for detailed information.

The table displays the following columns:

Table E-187 Mapped Policies to PCI Mandate

Column Name	Description
Policy Name	Displays the name of the policy. The Policy Name opens a page with detailed information on the selected policy.
Control Statement Name	Displays the name of the control statement. The Control Statement Name opens a page with detailed information on the selected control statement.
Mandate Name	Displays the name of the mandate. The Mandate Name opens a page with detailed information on the selected mandate.

From the Dashboard Taskbar you can do the following:

Table E-188 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-189 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-bar chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Coverage of Control Statements in PCI Mandate

The **Coverage of Control Statements in PCI Mandate** panel displays the percentage of mapped and unmapped control statements to the mandate. This panel displays a 2D-pie chart about the Payment Card Industry (PCI) mandate.

Mandate and Policy Compliance Management is the area of interest for this panel.

Note: The supported versions of PCI Mandate for predefined **Compliance Analysis - PCI Mandate** dashboard and its panels are as follows:

- PCI DSS v1.2

The panel displays the following information:

Table E-190 Components for the Coverage of Control Statements in PCI Mandate Panel

Components	Description
Chart style	2D-pie chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the percentage of mapped and unmapped control statements in PCI mandate:

```
Controls, Control1, Control2, and Control3 are mapped to Mandate
through Control Statement1.
```

```
Control Statement2 and Control Statement3 do not have mapped controls.

The total number of mapped control statements to Mandate is 1.

The total number of unmapped control statements to Mandate is 2.
```

Therefore, the panel displays the percentage of the total mapped controls statements and the total unmapped controls statements.

You can click the pie to drill down and view a table for detailed information.

The table displays the following columns:

Table E-191 Coverage of Control Statements in PCI Mandate

Column Name	Description
Control Statement Count	Displays the count of the control statement.
Mandate Name	Displays the name of the mandate. The Mandate Name opens a page with detailed information on the selected mandate.
Mapped Unmapped Type	Displays whether control statement is mapped or unmapped.

From the Dashboard Taskbar you can do the following:

Table E-192 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.

Table E-192 Dashboard Taskbar *(continued)*

Option Name	Description
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-193 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-pie chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Top 10 Failed Control Statements for PCI Mandate

The **Top 10 Failed Control Statements for PCI Mandate** panel displays, in descending order, the 10 failed control statements that are mapped to a single mandate. This panel displays a 2D-bar chart about the Payment Card Industry (PCI) mandate.

Mandate and Policy Compliance Management is the area of interest for this panel.

Note: The supported versions of PCI Mandate for predefined **Compliance Analysis - PCI Mandate** dashboard and its panels are as follows:

- PCI DSS v1.2

The panel displays the following information:

Table E-194 Components for the Top 10 Failed Control Statements for PCI Mandate Panel

Components	Description
Dimension (X axis)	Control Statement
Measure (Y axis)	Count of Controls
Chart style	2D-bar chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine which control statements have failed controls mapped to it:

```
Controls C1, C2, and C3 are mapped to Control statement1 which is
mapped to Mandate1.
```

```
Controls C4, C5, and C6 are mapped to Control statement2 which is
mapped to Mandate2.
```

Controls have the following result for assets:

Table E-195 Control Statement1

Asset/Control	C1	C2	C3
Asset1	Fail	Fail	Pass
Asset2	Fail	Unknown	Pass

The result for Control statement1 is three failed control counts.

Control statement2 has the following result for assets:

Table E-196 Control Statement2

Asset/Control	C4	C5	C6
Asset3	Pass	Error	Pass
Asset4	Fail	Unknown	Pass

The result for Control statement2 is one failed control counts.

Therefore, the panel displays the top 10 failed control statements in descending order with respect to failed control count.

You can click one of the bars to drill down and view a table for detailed information.

The table displays the following columns:

Table E-197 Top 10 Failed Control Statements for PCI Mandate

Column Name	Description
Control Statement	Displays the failed control statement. The Control Statement opens a page with detailed information on the control statement.
Mandate Name	Displays the name of the mandate. The Mandate Name opens a page with detailed information on the mandate.
Control Name	Displays the name of control. The Control Name opens a page with detailed information on the control.
Control Type	Displays the type of control. For example, checks RAM question, Third-party control, SCAP rule, and so forth.
Evaluation Date	Displays the date and time of the evaluation.

From the Dashboard Taskbar you can do the following:

Table E-198 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.

Table E-198 Dashboard Taskbar *(continued)*

Option Name	Description
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-199 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-column chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Breakdown of Policies by Status

The **Breakdown of Policies by Status** panel displays the breakdown of all the available policies that are categorized as per the policy status. The panel displays a Column Type chart.

Policy is the area of interest for this panel.

Each bar represents the number of policies in each status.

The panel displays the following information:

Table E-200 Components of the Breakdown of Policies by Status panel

Components	Description
Dimension (X axis)	Policy Status
Measure (Y axis)	Count of Policies
Chart style	Column Type chart

Table E-200 Components of the Breakdown of Policies by Status panel *(continued)*

Components	Description
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the breakdown of the policies by status.

```
Policies P1, P2, P3, P4, and P5 are available in CCS system.
```

The table displays the status of the policies in the CCS system.

Table E-201 Breakdown of policies as per status

Policies	P1	P2	P3	P4	P5
Status	Draft	In Review	Pending Approval	Approved	Published

Therefore, the panel displays the separate bars for individual policy status and the policy count for each status as follows:

```
Draft = 1, In Review = 1, Pending Approval = 1, Approved = 1,
Published = 1.
```

You can click one of the bars to drill down and view a table for detailed information.

The table displays the following columns:

Table E-202 Breakdown of Policies by Status

Column name	Description
Policy Name	Displays the name of the policy. The Policy Name opens a page with detailed information on the policy.
Policy Status	Displays the status of the policy.
Policy Author	Displays the author of the policy.
Policy Review-by Date	Displays the date by which the policy has to be reviewed.
Policy Creation Date	Displays the date the policy was created.
Policy Expiration Date	Displays the date the policy expires.
Policy Publication Date	Displays the date the policy was published.

Table E-202 Breakdown of Policies by Status *(continued)*

Column name	Description
Policy Tag name	Displays the tag name of the policy.

From the Dashboard Taskbar you can do the following:

Table E-203 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options that are available at the top of the drill through page:

Table E-204 General options

Options	Descriptions
Back to chart	Lets you return to the Column Type chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.

Table E-204 General options *(continued)*

Options	Descriptions
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Control Status by Assets for Mandates

The **Control Status by Assets for Mandates** panel displays the count of controls with respective control result name mapped to mandates. The panel displays a 3D-pie chart.

Mandate Asset Compliance is the area of interest for this panel.

The panel displays the following information:

Table E-205 Components for the Control Status by Assets for Mandates Panel

Components	Description
Dimension (X axis)	Result Name
Measure (Y axis)	Control Status Count for Asset
Chart style	3D-pie chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the control count by the assets that are mapped to a mandate through a control statement:

```
Controls Control1, Control2, Control3 are mapped to Mandate1 through
Control Statement1.
```

```
All mapped controls have following evidence against Asset1 and Asset2.
```

Table E-206 Assets of Mandate1 is evaluated against controls

Asset/Check	Control1	Control2	Control3
Asset1	Fail	Fail	Pass
Asset2	Fail	Unknown	Pass
Asset3	Pass	NA	Fail

Therefore, the panel displays the control status by asset data with separate sections for control result name and respective control count as follows:

```
Pass = 3, Fail = 4, Unknown = 1, Not Applicable = 1.
```

You can click part of the pie to drill down and view a table for detailed information.

The table displays the following columns:

Table E-207 Control Status by Assets for Mandates

Column Name	Description
Result Name	Displays the name of the result. For example, pass, fail, and so forth.
Control Status Count for Asset	Displays the control count for an asset for the selected result name. The Control Status Count for Asset opens a page with detailed information on the controls.
Mandate Name	Displays the name of the mandate. The Mandate Name opens a page with detailed information on the mandate.
Asset Name	Displays the name of the asset. The Asset Name opens a page with detailed information on the selected asset.
Asset Type	Displays the type of the asset. For example, Windows Machine, UNIX Machine, and so forth.
Asset Compliance Pass Score	Displays the compliance pass score of the asset.
Asset Location	Displays the location of the asset.
Asset Owner	Displays the name of the owner of the asset.
Asset Risk Score	Displays the risk score of the asset.

From the Dashboard Taskbar you can do the following:

Table E-208 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.

Table E-208 Dashboard Taskbar *(continued)*

Option Name	Description
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-209 General options

Options	Descriptions
Back to chart	Lets you return to the 3D-pie chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Control Status by Assets for Policies

The **Control Status by Assets for Policies** panel displays the count of controls with respective control result name mapped to policies. The panel displays a 3D-pie chart.

Policy Asset Compliance is the area of interest for this panel.

The panel displays the following information:

Table E-210 Components for the Control Status by Assets for Policies Panel

Components	Description
Dimension (X axis)	Result Name
Measure (Y axis)	Control Status Count for Asset
Chart style	3D-pie chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the control count by the assets that are scoped to the policies:

```
Policy, P1 is scoped to assets, Asset1, Asset2, and Asset3.
```

```
Controls, Control1, Control2, and Control3 are mapped to P1 through
control statement1.
```

```
All mapped controls have following evidence against Asset1 and Asset2.
```

Table E-211 Assets of P1 is evaluated against controls

Asset/Control	Control1	Control2	Control3
Asset1	Fail	Fail	Pass
Asset2	Fail	Unknown	Pass
Asset3	Pass	NA	Fail

Therefore, the panel displays the control status by asset data with separate sections for control result name and respective control count as follows:

```
Pass = 3, Fail = 4, Unknown = 1, Not Applicable = 1.
```

You can click part of the pie to drill down and view a table for detailed information.

The table displays the following columns:

Table E-212 Control Status by Assets for Policies

Column Name	Description
Policy Name	Displays the name of the policy. The Policy Name opens a page with detailed information on the policy.
Result Name	Displays the name of the result. For example, pass, fail, and so forth.
Control Status Count for Asset	Displays the control count for an asset for the selected result name. The Control Status Count for Asset opens a page with detailed information on the controls.
Asset Name	Displays the name of the asset. The Asset Name opens a page with detailed information on the selected asset.
Asset Type	Displays the type of the asset. For example, Windows Machine, UNIX Machine and so forth.
Asset Owner	Displays the name of the owner of the asset.
Asset Location	Displays the location of the asset.
Asset Compliance Pass Score	Displays the compliance pass score of the asset.
Asset Risk Score	Displays the risk score of the asset.
Policy Tag name	Displays the tag name of the policy.

From the Dashboard Taskbar you can do the following:

Table E-213 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.

Table E-213 Dashboard Taskbar *(continued)*

Option Name	Description
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-214 General options

Options	Descriptions
Back to chart	Lets you return to the 3D-pie chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Control Status for Mandates

The **Control Status for Mandates** panel displays the asset count with respective control mapped to mandates. The panel displays a 2D-stacked column chart.

Mandate Control Compliance is the area of interest for this panel.

The panel displays the following information:

Table E-215 Components for the Control Status for Mandates Panel

Components	Description
Dimension (X axis)	Mandate Name
Measure (Y axis)	Asset Count for Control Status
Chart style	2D-stacked column chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the asset count for control status that are mapped to a mandate through a control statement:

```
Controls, Control1, Control2, and Control3 are mapped to Mandate1
through Control Statement1.
```

```
All mapped controls have following evidence against Asset1, Asset2,
and Asset3.
```

Table E-216 Controls of P1 is evaluated against assets

Asset/Check	Control1	Control2	Control3
Asset1	Fail	Fail	Pass
Asset2	Fail	Unknown	Pass
Asset3	Pass	NA	Fail

Therefore, the panel displays the asset count data for Mandate1 with separate sections for each asset result name as follows:

```
Pass = 3, Fail = 4, Not Applicable = 1, Unknown = 1.
```

You can click part of the column to drill down and view a table for detailed information.

The table displays the following columns:

Table E-217 Control Status by Assets for Mandates

Column Name	Description
Asset Count for Control Status	Displays the control count for an asset for the selected result name. The Control status count for asset opens a page with detailed information on the controls.

Table E-217 Control Status by Assets for Mandates *(continued)*

Column Name	Description
Result Name	Displays the name of the result. For example, pass, fail, and so forth.
Mandate Name	Displays the name of the mandate. The Mandate Name opens a page with detailed information on the selected mandate.
Control Name	Displays the name of the control. The Control Name opens a page with detailed information on the selected control.
Control Type	Displays the type of the control. For example, standard check, Third-party control, RAM question, and so forth.

From the Dashboard Taskbar you can do the following:

Table E-218 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-219 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-stacked column chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Control Status for Policies

The **Control Status for Policies** panel displays the asset count with respective control mapped to policies. The panel displays a 2D-stacked column chart.

Policy Control Compliance is the area of interest for this panel.

The panel displays the following information:

Table E-220 Components for the Control Status for Policies Panel

Components	Description
Dimension (X axis)	Policy Name
Measure (Y axis)	Asset count for control status
Chart style	2D-stacked column chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the asset count for the control status which are scoped to the policies:

`Policy, P1 is scoped to assets, Asset1, Asset2, and Asset3.`

`Controls, Control1, Control2, and Control3 are mapped to P1 through Control Statement1.`

`All mapped controls have following evidence against Asset1 and Asset2.`

Table E-221 Controls of P1 is evaluated against assets

Asset/Control	Control1	Control2	Control3
Asset1	Fail	Fail	Pass
Asset2	Fail	Unknown	Pass
Asset3	Pass	NA	Fail

Therefore, the panel displays the asset count data for P1 with separate sections for each asset result name as follows:

```
Pass = 3, Fail = 4, Not Applicable = 1, Unknown = 1.
```

You can click part of the column to drill down and view for detailed information.

The table displays the following columns:

Table E-222 Control Status for Policies

Column Name	Description
Result Name	Displays the name of the result. For example, control asset pass, fail, and so forth.
Asset Count for Control Status	Displays the asset count for an asset for the selected result name. The Asset Count for Control Status opens a page with detailed information on the assets.
Policy Name	Displays the name of the policy. The Policy Name opens a page with detailed information on the policy.
Control Name	Displays the name of the control. The Control Name opens a page with detailed information on the control.
Control Type	Displays the type of the control. For example, standard check, Third-party control, RAM question, and so forth.
Policy Tag Name	Displays the tag name of the policy.

From the Dashboard Taskbar you can do the following:

Table E-223 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-224 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-stacked column chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Control Status for Policy

The **Control Status for Policy** panel displays the asset count with respective control mapped to policies. The panel displays a 3D-pie chart.

Policy Control Compliance is the area of interest for this panel.

The panel displays the following information:

Table E-225 Components for the Control Status for Policy Panel

Components	Description
Dimension (X axis)	Result Name
Measure (Y axis)	Asset count for control status
Chart style	3D-pie chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the asset count for the control status which are scoped to the policies:

```
Policy, P1 is scoped to assets, Asset1, Asset2, and Asset3.
```

```
Controls, Control1, Control2, and Control3 are mapped to P1 through
Control Statement1.
```

```
All mapped controls have following evidence against Asset1 and Asset2.
```

Table E-226 Controls of P1 is evaluated against assets

Asset/Control	Control1	Control2	Control3
Asset1	Fail	Fail	Pass
Asset2	Fail	Unknown	Pass
Asset3	Pass	NA	Fail

Therefore the panel displays the asset count data for P1 with separate sections for each asset result name as follows:

```
Pass = 3, Fail = 4, Not Applicable = 1, Unknown = 1.
```

You can click part of the column to drill down and view a table for detailed information.

The table displays the following columns:

Table E-227 Control Status for Policy

Column Name	Description
Policy Name	Displays the name of the policy. The Policy Name opens a page with detailed information on the policy.
Result Name	Displays the name of the result. For example, control asset pass, fail, and so forth.
Asset count for control status	Displays the asset count for an asset for the selected result name. The Asset count for control status opens a page with detailed information on the assets.
Control Name	Displays the name of the control. The Control Name opens a page with detailed information on the control.
Control type	Displays the type of the control. For example, standard check, Third-party control, RAM question, and so forth.
Policy Tag name	Displays the tag name of the policy.

From the Dashboard Taskbar you can do the following:

Table E-228 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.

Table E-228 Dashboard Taskbar *(continued)*

Option Name	Description
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-229 General options

Options	Descriptions
Back to chart	Lets you return to the 3D-pie chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Top 10 Assets with Highest Risk Score by Policy

The **Top 10 Assets with Highest Risk Score by Policy** panel displays, in descending order, the 10 assets with the highest risk score as scoped by policy application. The panel displays a 2D-bar chart.

Policy Asset Compliance is the area of interest for this panel.

The panel displays the following information:

Table E-230 Components for the Top 10 Assets with Highest Risk Score by Policy Panel

Components	Description
Dimension (X axis)	Asset Name
Measure (Y axis)	Asset Risk Score

Table E-230 Components for the Top 10 Assets with Highest Risk Score by Policy Panel *(continued)*

Components	Description
Chart style	2D-bar chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the assets with the highest risk score:

```
Policy P1 is scoped to Asset Group1 contains Asset1 with risk score
7.2.
```

```
Policy P2 is scoped to Asset Group2 contains Asset2 with risk score
9.1.
```

```
Policy P3 is scoped to Asset Container1 contains Asset3 with risk
score NA.
```

Therefore the panel displays Asset2 and Asset1 with risk score in descending order.

Note: To view all the details about the policies in the drill through table, ensure that you have the view permissions on the entities in the panel.

You can click one of the bars to drill down and view a table for detailed information.

The table displays the following columns:

Table E-231 TOP 10 Assets with Highest Risk Score by Policy

Column Name	Description
Asset Name	Displays the name of the asset. The Asset Name opens a page with detailed information on the asset.
Asset Risk Score	Displays the risk score of the asset.
Policy Name	Displays the name of the policy. The Policy Name opens a page with detailed information on the policy.
Asset Group Name	Displays the name of the asset group. The Asset Group Name opens a page with detailed information on the asset group.

Table E-231 TOP 10 Assets with Highest Risk Score by Policy *(continued)*

Column Name	Description
Asset Type	Displays the type of the asset. For example, Windows Machine, UNIX machine , and so forth.
Asset Location	Displays the location of the asset.
Asset Owner	Displays the name of the owner of the asset.
Asset Tag Name	Displays the name of the asset tag.
Asset Compliance Pass Score	Displays the compliance pass score of the asset.
Evaluation Date	Displays the date and time of the evaluation.
Result Name	Displays the name of the result. For example, Policy Asset Pass, Fail, and so forth.

From the Dashboard Taskbar you can do the following:

Table E-232 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-233 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-bar chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Top 10 Failed Control Statements for Mandates

The **Top 10 Failed Control Statements for Mandates** panel displays, in descending order, the 10 failed control statements that are mapped to single or to multiple mandates. The panel displays a 2D-bar chart.

Mandate Control Compliance is the area of interest for this panel.

The panel displays the following information:

Table E-234 Components for the Top 10 Failed Control Statements for Mandates Panel

Components	Description
Dimension (X axis)	Control Statement
Measure (Y axis)	Count of Controls
Chart style	2D-bar chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine which controls have failed:

```
Controls C1, C2, and C3 are mapped to Control statement1 which is
mapped to Mandate1.
```

```
Controls C4, C5, and C6 are mapped to Control statement2 which is
mapped to Mandate2.
```

Control statement1 has the following result for assets:

Table E-235 Control Statement1

Asset/Control	C1	C2	C3
Asset1	Fail	Fail	Pass
Asset2	Fail	Unknown	Pass

The result for Control statement1 is three failed control counts.

Control statement2 has the following result for assets:

Table E-236 Control Statement2

Asset/Control	C4	C5	C6
Asset3	Pass	Error	Pass
Asset4	Fail	Unknown	Pass

The result for Control statement2 is one failed control counts.

Therefore, the panel displays the top 10 failed control statements in descending order with respect to failed control count.

You can click one of the bars to drill down and view a table for detailed information.

The table displays the following columns:

Table E-237 Top 10 Failed Control Statements for Policies

Column Name	Description
Control Statement	Displays the failed control statement. The Control Statement opens a page with detailed information on the control statement.
Mandate Name	Displays the name of the mandate. The Mandate Name opens a page with detailed information on the mandate.
Control Name	Displays the name of control. The Control Name opens a page with detailed information on the control.

Table E-237 Top 10 Failed Control Statements for Policies *(continued)*

Column Name	Description
Control Type	Displays the type of control. For example, checks RAM question, Third-party control, SCAP, and so forth.
Evaluation Date	Displays the date and time of the evaluation.

From the Dashboard Taskbar you can do the following:

Table E-238 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-239 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-column chart in the first panel.

Table E-239 General options *(continued)*

Options	Descriptions
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Top 10 Failed Control Statements for Policies

The **Top 10 Failed Control Statements for Policies** panel displays, in descending order, the 10 failed control statements that are mapped to single or to multiple policies. The panel displays a 2D-bar chart.

Policy Control Compliance is the area of interest for this panel.

The panel displays the following information:

Table E-240 Components for the Top 10 Failed Control Statements for Policies Panel

Components	Description
Dimension (X axis)	Control Statement
Measure (Y axis)	Count of Controls
Chart style	2D-bar chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine which controls have failed:

```
Controls C1, C2, and C3 are mapped to Control statement1 which is
mapped to Policy1.
```

```
Controls C4, C5, and C6 are mapped to Control statement2 which is
mapped to Policy2.
```

```
Policy1 is scoped to Asset1 and Asset2.
```

```
Policy2 is scoped to Asset3 and Asset4.
```

Control statement1 has the following result for scoped assets of policies:

Table E-241 Control Statement1

Asset/Control	C1	C2	C3
Asset1	Fail	Fail	Pass
Asset2	Fail	Unknown	Pass

The result for Control statement1 is three failed control counts.

Control statement2 has the following result for scoped assets of policies:

Table E-242 Control Statement2

Asset/Control	C4	C5	C6
Asset3	Pass	Error	Pass
Asset4	Fail	Unknown	Pass

The result for Control statement2 is one failed control counts.

Therefore, the panel displays the top 10 failed control statements in descending order with respect to failed control count.

Note: To view all the details about the policies in the drill through table, ensure that you have the view permissions on the entities in the panel.

You can click one of the bars to drill down and view a table for detailed information.

The table displays the following columns:

Table E-243 Top 10 Failed Control Statements for Policies

Column Name	Description
Policy Name	Displays the name of the policy. The Policy Name opens a page with detailed information on the policy.
Control Statement	Displays the failed control statement. The Control Statement opens a page with detailed information on the control statement.
Control Name	Displays the name of control. The Control Name opens a page with detailed information on the control.

Table E-243 Top 10 Failed Control Statements for Policies *(continued)*

Column Name	Description
Control Type	Displays the type of control. For example, checks RAM question, Third-party control, SCAP rule, and so forth.
Evaluation Date	Displays the date and time of the evaluation.

From the Dashboard Taskbar you can do the following:

Table E-244 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-245 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-bar chart in the first panel.

Table E-245 General options *(continued)*

Options	Descriptions
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

User Acceptance of Policies

The **User Acceptance of Policies** panel displays the user responses of published policies. The panel displays a 2D-stacked column chart.

Policy User Acceptance is the area of interest for this panel.

The panel displays the following information:

Table E-246 Components for the User Acceptance of Policies Panel

Components	Description
Dimension (X axis)	User Acceptance/Policy Name
Measure (Y axis)	Policy User Response Count
Chart style	2D-stacked column chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the user's response for certain policies:

```
Policy1, Policy2, and Policy3 are published policies.

The user responds to these policies from the web console.

Policy1 = Accepted.

Policy2 = Declined.

Policy3 = Read but did not accept it or declined it.
```

Therefore, the panel displays a separate bar per policy with the appropriate user response.

You can click one of the bars to drill down and view a table for detailed information.

The table displays the following columns:

Table E-247 User Acceptance of Policies

Column Name	Description
User Acceptance	Displays the acceptance of the policy by the user. For example, Accepted , Declined , Read , or Unread.
Policy Name	Displays the name of the policy. The Policy Name opens a page with detailed information on the policy.
Policy Author	Displays the name of the author of the policy.
Policy User	Displays the name of the user of the policy
Policy User Response Date	Displays the response date of the policy by the user.

From the Dashboard Taskbar you can do the following:

Table E-248 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.

Table E-248 Dashboard Taskbar *(continued)*

Option Name	Description
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-249 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-stacked column chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Compliance Score for SCAP Profile (Benchmark)

The **Compliance Score for SCAP Profile (Benchmark)** panel displays an average compliance score for SCAP Profile. The panel displays a 2D-stacked column chart.

SCAP Benchmark Compliance is the area of interest for this panel.

The panel displays the following information:

Table E-250 Components for the Compliance Score for SCAP Profile (Benchmark) Panel

Components	Description
Dimension (X axis)	Profile: SCAP Benchmark
Measure (Y axis)	Average Compliance Score (%)
Chart style	2D-stacked column chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the compliance score for SCAP profile:

```
SCAP Profile Profile1 is evaluated against assets Asset1, Asset2,
and Asset3.
```

The following is the compliance score for each asset:

```
Compliance score for Asset1 evaluated against Profile1 = 50%.

Compliance score for Asset2 evaluated against Profile1 = 75%.

Compliance score for Asset3 evaluated against Profile1 = 0%.
```

The following formula displays the average compliance score for Profile1.

```
= (Asset1 compliance score + Asset2 compliance score + Asset3
compliance score) / 3

= (50+75+0) /3

= 41.67%
```

Therefore, the average asset compliance score for SCAP Profile Profile1 is 41.67%.

You can click one of the bars to drill down and view a table for detailed information.

The table displays the following columns:

Table E-251 Compliance Score for SCAP Profile (Benchmark)

Column Name	Description
SCAP Asset Compliance Score	Displays the compliance score of the SCAP asset. The SCAP Asset Compliance Score opens a page with detailed information on the rule.
SCAP Asset Risk Score	Displays the risk score of the SCAP asset.
Asset Name	Displays the name of the asset. The Asset Name opens a page with detailed information on the asset.
Profile Name	Displays the name of the profile. The Profile Name opens a page with detailed information on the profile.
Benchmark Name	Displays the name of the benchmark.
Asset Type	Displays the type of the asset. For example, Windows Machine, UNIX Machine, and so forth.

Table E-251 Compliance Score for SCAP Profile (Benchmark) *(continued)*

Column Name	Description
Asset Location	Displays the location of the asset.
Asset Owner	Displays the name of the owner of the asset.
Profile: Benchmark Name	Displays the benchmark name of the profile.

From the Dashboard Taskbar you can do the following:

Table E-252 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-253 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-stacked column chart in the first panel.

Table E-253 General options *(continued)*

Options	Descriptions
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Rule Status by Assets for SCAP Profile (Benchmark)

The **Rule Status by Assets for SCAP Profile (Benchmark)** panel displays the rule count with respective rule result name per asset for a SCAP Profile. The panel displays a 3D-pie chart.

SCAP Benchmark Compliance is the area of interest for this panel.

The panel displays the following information:

Table E-254 Components for the Rule Status by Assets for SCAP Profile (Benchmark) Panel

Components	Description
Chart style	3D-pie chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the rule count by asset for a SCAP Profile:

```
SCAP Profile Profile1 has 5 rules Rule1, Rule2, Rule3, Rule4, and
Rule5.
```

```
Profile1 is evaluated against assets Asset1, Asset2, and Asset3.
```

The following is the evaluation result:

Table E-255 Rule counts for each Rule result name

Asset/Rule	Rule1	Rule2	Rule3	Rule4	Rule5
Asset1	Pass	Fail	Pass	NA	Unknown

Table E-255 Rule counts for each Rule result name *(continued)*

Asset/Rule	Rule1	Rule2	Rule3	Rule4	Rule5
Asset2	Informational	Not Selected	Error	Fixed	NA
Asset3	Fail	Pass	Not Checked	Fail	Unknown

Therefore, the panel displays the following Rule status by asset data with separate section for Rule result name and respective Rule count:

```
Pass = 3, Fail = 3, Error = 1, Unknown = 2, Not Applicable = 2, Not
Selected = 1, Not checked = 1, Fixed = 1, Informational = 1
```

You can click one of the bars to drill down and view a table for detailed information.

The table displays the following columns:

Table E-256 Rule Status by Assets for SCAP Profile (Benchmark)

Column Name	Description
Rule Count	Displays the rule count with respective rule result name. The Rule Count opens a page with detailed information on the rules evaluated.
Rule Status	Displays the status of the rule. For example, pass, fail, and so forth.
Profile Name	Displays the name of the profile. The Profile Name opens a page with detailed information on the profile.
Benchmark Name	Displays the name of the benchmark.
Asset Name	Displays the name of the asset. The Asset Name opens a page with detailed information on the asset.
SCAP Asset Compliance Score	Displays the compliance score of the SCAP asset. The SCAP Asset Compliance Score opens a page with detailed information on the rule.
SCAP Asset Risk Score	Displays the risk score of the SCAP asset.
Asset Type	Displays the type of the asset. For example, Windows Machine, UNIX Machine, and so forth.

Table E-256 Rule Status by Assets for SCAP Profile (Benchmark) *(continued)*

Column Name	Description
Asset Location	Displays the location of the asset.
Asset Owner	Displays the name of the owner of the asset.

From the Dashboard Taskbar you can do the following:

Table E-257 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-258 General options

Options	Descriptions
Back to chart	Lets you return to the 3D-pie chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.

Table E-258 General options *(continued)*

Options	Descriptions
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Top 10 Assets By Risk Score for SCAP Profile (Benchmark)

The **Top 10 Assets By Risk Score For SCAP Profile (Benchmark)** panel displays, in descending order, the 10 assets with the highest risk score as determined by SCAP Profile. The panel displays a 2D-bar chart.

SCAP Benchmark Compliance is the area of interest for this panel.

The panel displays the following information:

Table E-259 Components for the Top 10 Assets By Risk Score For SCAP Profile (Benchmark) Panel

Components	Description
Dimension (X axis)	Asset Name
Measure (Y axis)	Average Asset Risk Score
Chart style	2D-bar chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the rule count by asset for a SCAP Profile:

```
Asset, Asset1 is evaluated against SCAP Profiles, Profile1, Profile2,
and Profile3.
```

```
Asset, Asset2 is evaluated against SCAP Profiles, Profile1 and
Profile2.
```

```
Asset, Asset3 is evaluated against SCAP Profiles, Profile3
```

The following is the risk score contributed by different SCAP Profile:

Table E-260 Risk score contributed by different SCAP Profile

Asset/SCAP Profile	Profile1	Profile2	Profile3
Asset1	7.5	NA	9.2
Asset2	6.2	4.5	-
Asset3	-	-	NA

Any asset with a risk score of NA is not part of the calculation for average risk score.

```
Asset1 risk score = (7.5 + 9.2)/2 = 8.4
```

```
Asset2 risk score = (6.2 + 4.5)/2 = 5.4
```

```
Asset3 risk score = NA
```

Therefore, the panel displays Asset1 = 8.4 and Asset2 = 5.4 risk score in descending order.

You can click one of the bars to drill down and view a table for detailed information.

The table displays the following columns:

Table E-261 Top 10 Assets By Risk Score For SCAP Profile (Benchmark)

Column Name	Description
SCAP Asset Risk Score	Displays the risk score of the SCAP asset. The SCAP Asset Risk Score opens a page with detailed information on the rule evaluated.
Asset Name	Displays the name of the asset. The Asset Name opens a page with detailed information on the asset.
SCAP Asset Compliance Score	Displays the compliance score of the SCAP asset.
Profile Name	Displays the name of the profile. The Profile Name opens a page with detailed information on the profile.
Benchmark Name	Displays the name of the benchmark.
Asset Type	Displays the type of the asset. For example, Windows Machine, UNIX Machine, and so forth.
Asset Location	Displays the location of the asset.

Table E-261 Top 10 Assets By Risk Score For SCAP Profile (Benchmark) *(continued)*

Column Name	Description
Asset Owner	Displays the name of the owner of the asset.

From the Dashboard Taskbar you can do the following:

Table E-262 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-263 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-bar chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.

Table E-263 General options *(continued)*

Options	Descriptions
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Compliance Score for SOX Mandate

The **Compliance Score for SOX Mandate** panel displays the percentage of average of control status evaluated against assets. This panel displays a 2D-stacked column chart about the Sarbanes-Oxley (SOX) mandate.

Standard Compliance Management is the area of interest for this panel.

The panel displays the following information:

Table E-264 Components for the Compliance Score for SOX Mandate Panel

Components	Description
Chart style	2D-pie chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the compliance score for the SOX mandate:

```
Standard1 has Controls, Control1, Control2, and Control3.
```

```
Controls, Control1, Control2, and Control3 are mapped to Mandate
through Control Statement1.
```

```
Control1, Control2, and Control3 are evaluated against assets, Asset1,
Asset2 and Asset3.
```

Table E-265 Evaluation results for controls evaluated against assets

Control/Asset	Asset1	Asset2	Asset3
Control1	Fail	Fail	Fail
Control2	Unknown	Fail	Fail

Table E-265 Evaluation results for controls evaluated against assets *(continued)*

Control/Asset	Asset1	Asset2	Asset3
Control3	Pass	Pass	Pass

The result status for Asset1 - Pass = 1, Fail = 1, Unknown = 1, and Error = 0.

The result status for Asset2 - Pass = 1, Fail = 2, Unknown = 0, and Error = 0.

The result status for Asset3 - Pass = 1, Fail = 2, Unknown = 0, and Error = 0.

The following formula calculates the percentage for each result status per asset:

```
Asset1 Pass = (P count / (P count + F count + U count + E count)) x
100%
```

```
Asset1 Pass = (1 / (1 + 1 + 1 + 0)) x 100%
```

```
Asset1 Pass = 33.33%
```

```
Asset1 Fail = (F count / (P count + F count + U count + E count)) x
100%
```

```
Asset1 Fail = (1 / (1 + 1 + 1 + 0)) x 100%
```

```
Asset1 Fail = 33.33%
```

```
Asset1 Unknown = (U count / (P count + F count + U count + E count))
x 100%
```

```
Asset1 Unknown = (1 / (1 + 1 + 1 + 0)) x 100%
```

```
Asset1 Unknown = 33.33%
```

The following is the compliance score percentage for Asset1:

```
Pass = 33.33%, Fail = 33.33%, Unknown = 33.33%.
```

Similar calculations are done for Asset2 and Asset3.

The following is the compliance score percentage for Asset2:

```
Pass = 33.33%, Fail = 66.67%, Unknown = 0%.
```

The following is the compliance score percentage for Asset3:

```
Pass = 33.33%, Fail = 66.67%, Unknown = 0%.
```

The following formula calculates the average compliance score percentage of the mandate:

```
Average Mandate percent Result Status = (sum of all asset result
status) / (Count of total assets)
```

```
Average Mandate percent Pass = (Asset1 Pass + Asset2 Pass + Asset2
Pass) / 3

Average Mandate percent Pass = (33.33% + 33.33% + 33.33%) / 3

Average Mandate percent Pass = 33.33%

Average Mandate percent Fail = (Asset1 Fail + Asset2 Fail + Asset2
Fail) / 3

Average Mandate percent Fail = (33.33% + 66.67% + 66.67%) / 3

Average Mandate percent Fail = 55.56%

Average Mandate percent Unknown = (Asset1 Unknown + Asset2 Unknown
+ Asset2 Unknown) / 3

Average Mandate percent Unknown = (33.33% + 0 + 0) / 3

Average Mandate percent Unknown = 11.11%
```

Therefore, the panels displays the average Mandate percent Result Status as follows:

```
Pass = 33.33%, Fail = 55.56%, and Unknown = 11.11%.
```

The panel does not reflect the result status for the controls which do not have instances.

You can click on the pie to drill down and view a table for detailed information.

The table displays the following columns:

Table E-266 Compliance Score for SOX Mandate

Column Name	Description
Mandate Asset Compliance	Displays the individual compliance for that result type. The Mandate Asset Compliance opens a page with detailed information on the control that are evaluated per asset.
Asset Compliance Score	Displays the consolidated compliance score of the asset.
Mandate Name	Displays the name of the mandate. The Mandate Name opens a page with detailed information on the mandate.
Asset Name	Displays the name of the asset. The Asset Name opens a page with detailed information on the asset.

Table E-266 Compliance Score for SOX Mandate *(continued)*

Column Name	Description
Asset Type	Displays the type of the asset. For example, Windows Machine, UNIX Machine, and so forth.
Asset Owner	Displays the name of the owner of the asset.
Asset Location	Displays the location of the asset.
Compliance Result Name	Displays the result of the compliance score. For example, Mandate asset compliance pass, fail, and so forth.

From the Dashboard Taskbar you can do the following:

Table E-267 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

From the Dashboard Taskbar you can do the following:

Table E-268 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

From the Dashboard Taskbar you can do the following:

Table E-269 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.

Table E-269 Dashboard Taskbar *(continued)*

Option Name	Description
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-270 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-stacked column chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Control Status Trends for SOX Mandate

The **Control Status Trends for SOX Mandate** panel displays a control count for all available control result status for all the controls mapped to control statement. The Sarbanes Oxley (SOX) trend is based on the control count against assets mapped to the SOX mandate at the end of every month. The panel displays a 2D-line chart.

Mandate and Policy Compliance Management is the area of interest for this panel.

The panel displays the following information:

Table E-271 Components for the Control Status Trends for SOX Mandate Panel

Components	Description
Dimension (X axis)	Trends by End of Month

Table E-271 Components for the Control Status Trends for SOX Mandate Panel *(continued)*

Components	Description
Measure (Y axis)	Instances
Chart style	2D-line chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the control status trend for SOX mandate:

```
The Control statement1 is mapped to 5 controls, Control1, Control2,
Control3, Control4, and Control5.
```

```
SOXMandate1 mapped to Control statement1.
```

The following table displays the January 2011 evaluation of Mandate against the assets, Asset1, Asset2, and Asset3:

Table E-272 January 2011 Control evaluation details

Asset/Control	Control1	Control2	Control3	Control4	Control5
Asset1	Pass	Fail	Pass	NA	Unknown
Asset2	Fail	Fail	Error	Pass	NA
Asset3	Fail	Pass	Fail	Fail	Unknown

For January 2011 the panel shows following control count for each control result status:

```
Pass = 4, Fail = 6, Error = 1, Unknown = 2, Not Applicable = 2.
```

```
The Control statement2 is mapped to 5 controls, Control1, Control2,
Control3, Control4, and Control5.
```

```
Mandate mapped to Control statement2.
```

The following table displays the February 2011 evaluation of Mandate against the assets, Asset1, Asset2, and Asset3:

Table E-273 February 2011 Control evaluation details

Asset/Control	Control1	Control2	Control3	Control4	Control5
Asset1	Fail	Fail	Pass	Unknown	NA

Table E-273 February 2011 Control evaluation details *(continued)*

Asset/Control	Control1	Control2	Control3	Control4	Control5
Asset2	Fail	Unknown	Pass	Pass	Fail
Asset3	Pass	Error	Fail	NA	Fail

For February 2011 the panel shows following control count for each control result status:

```
Pass = 4, Fail = 6, Error = 1, Unknown = 2, Not Applicable = 2
```

Therefore, at the end of February 2011 the trend panel displays the following control count result based on control count for Mandate as:

```
Pass = 4, Fail = 6, Error = 1, Unknown = 2, Not Applicable = 2
```

From the Dashboard Taskbar you can do the following:

Table E-274 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

Mapped Policies to SOX Mandate

The **Mapped Policies to SOX Mandate** panel displays the total number of control statements mapped to the policies and the mandate. This panel displays a 2D-bar chart about the Sarbanes-Oxley (SOX) mandate.

Mandate and Policy Compliance Management is the area of interest for this panel.

The panel displays the following information:

Table E-275 Components for the Mapped Policies to SOX Mandate Panel

Components	Description
Dimension (X axis)	Policy Name
Measure (Y axis)	Count of Mapped Control
Chart style	2D-bar chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the number of mapped policies to the SOX mandate:

```
Control statements, Control statement1 is mapped to policy P1.

Control statements, Control statement2 is mapped to policy P1 and
P2.

Control statements, Control statement3 is mapped to policy P1 and
P2.

Control statement1, Control statement2, and Control statement3 are
mapped to Mandate.

The total number of control statements mapped to P1 = 3.

The total number of control statements mapped to P2 = 2.
```

Therefore, the panel displays the count of control statements for each policy as a separate bar.

You can click the bar to drill down and view a table for detailed information.

The table displays the following columns:

Table E-276 Mapped Policies to SOX Mandate

Column Name	Description
Policy Name	Displays the name of the policy. The Policy Name opens a page with detailed information on the selected policy.
Control Statement Name	Displays the name of the control statement. The Control Statement Name opens a page with detailed information on the selected control statement.
Mandate Name	Displays the name of the mandate. The Mandate Name opens a page with detailed information on the selected mandate.

From the Dashboard Taskbar you can do the following:

Table E-277 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-278 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-bar chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Coverage of Control Statements in SOX Mandate

The **Coverage of Control Statements in SOX Mandate** panel displays the percentage of mapped and unmapped control statements to the mandate. This panel displays a 2D-pie chart about the Sarbanes Oxley (SOX) mandate.

Mandate and Policy Compliance Management is the area of interest for this panel.

The panel displays the following information:

Table E-279 Components for the Coverage of Control Statements in SOX Mandate Panel

Components	Description
Chart style	2D-pie chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the percentage of mapped and unmapped control statements in SOX mandate:

```
Controls, Control1, Control2, and Control3 are mapped to Mandate
through Control Statement1.

Control Statement2 and Control Statement3 do not have mapped controls.

The total number of mapped control statements to Mandate is 1.

The total number of unmapped control statements to Mandate is 2.
```

Therefore, the panel displays the percentage of the total mapped controls statements and the total unmapped controls statements.

You can click the pie to drill down and view a table for detailed information.

The table displays the following columns:

Table E-280 Coverage of Control Statements in SOX Mandate

Column Name	Description
Control Statement Count	Displays the count of the control statement.
Mandate Name	Displays the name of the mandate. The Mandate Name opens a page with detailed information on the selected mandate.
Mapped Unmapped Type	Displays whether control statement is mapped or unmapped.

From the Dashboard Taskbar you can do the following:

Table E-281 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-282 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-pie chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Top 10 Failed Control Statements for SOX Mandate

The **Top 10 Failed Control Statements for SOX Mandate** panel displays, in descending order, the 10 failed control statements that are mapped to a single mandate. This panel displays a 2D-bar chart about the Sarbanes Oxley (SOX) mandate.

Mandate and Policy Compliance Management is the area of interest for this panel.

The panel displays the following information:

Table E-283 Components for the Top 10 Failed Control Statements for SOX Mandate Panel

Components	Description
Dimension (X axis)	Control Statement
Measure (Y axis)	Count of Controls
Chart style	2D-bar chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine which controls have statements have failed controls mapped to it:

```
Controls C1, C2, and C3 are mapped to Control statement1 which is
mapped to Mandate1.
```

```
Controls C4, C5, and C6 are mapped to Control statement2 which is
mapped to Mandate2.
```

Controls have the following result for assets:

Table E-284 Control Statement1

Asset/Control	C1	C2	C3
Asset1	Fail	Fail	Pass
Asset2	Fail	Unknown	Pass

The result for Control statement1 is three failed control counts.

Control statement2 has the following result for assets:

Table E-285 Control Statement2

Asset/Control	C4	C5	C6
Asset3	Pass	Error	Pass
Asset4	Fail	Unknown	Pass

The result for Control statement2 is one failed control counts.

Therefore, the panel displays the top 10 failed control statements in descending order with respect to failed control count.

You can click one of the bars to drill down and view a table for detailed information.

The table displays the following columns:

Table E-286 Top 10 Failed Control Statements for SOX Mandate

Column Name	Description
Control Statement	Displays the failed control statement. The Control Statement opens a page with detailed information on the control statement.
Mandate Name	Displays the name of the mandate. The Mandate Name opens a page with detailed information on the mandate.

Table E-286 Top 10 Failed Control Statements for SOX Mandate *(continued)*

Column Name	Description
Control Name	Displays the name of control. The Control Name opens a page with detailed information on the control.
Control Type	Displays the type of control. For example, checks RAM question, Third-party control, SCAP rule, and so forth.
Evaluation Date	Displays the date and time of the evaluation.

From the Dashboard Taskbar you can do the following:

Table E-287 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-288 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-column chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Monthly Status Trend of Checks

The **Check Status Trends for Standards** panel displays a check status count for all evaluated standards. This trend is based on the check count against all evaluated standard at the end of every month. The panel displays a 2D-line chart.

Standard Compliance Management is the area of interest for this panel.

The panel displays the following information:

Table E-289 Components for the Check Status Trends for Standards Panel

Components	Description
Dimension (X axis)	Trends by End of Month
Measure (Y axis)	Count of Checks
Chart style	2D-line chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the check status trend for standards:

```
The standard, Standard1 has 5 checks, Check1, Check2, Check3, Check4,
and Check5.
```

The following table displays the January 2011 evaluation of Standard1 against the assets, Asset1, Asset2, and Asset3:

Table E-290 January 2011 evaluation of Standard1

Asset/Check	Check1	Check2	Check3	Check4	Check5
Asset1	Pass	Fail	Pass	NA	Unknown
Asset2	Fail	Fail	Error	Pass	NA
Asset3	Fail	Pass	Fail	Fail	Unknown

```
The trend panel displays the results:
```

```
Pass = 4, Fail = 6, Error = 1, Unknown = 2, Not Applicable = 2
```

```
The standard, Standard2 has 5 checks, Check1, Check2, Check3, Check4,
and Check5.
```

The following table displays the February 2011 evaluation of Standard2 against the assets, Asset1, Asset2, and Asset3:

Table E-291 February 2011 evaluation of Standard2

Asset/Check	Check1	Check2	Check3	Check4	Check5
Asset1	Fail	Fail	Pass	Unknown	NA
Asset2	Fail	Unknown	Pass	Pass	Fail
Asset3	Pass	Error	Fail	NA	Fail

```
The trend panel displays the results:
```

```
Pass = 4, Fail = 6, Error = 1, Unknown = 2, Not Applicable = 2
```

Therefore, at the end of February 2011 the final check status result is:

```
Pass = 8, Fail = 12, Error = 2, Unknown = 4, Not Applicable = 4
```

From the Dashboard Taskbar you can do the following:

Table E-292 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.

Table E-292 Dashboard Taskbar *(continued)*

Option Name	Description
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

Compliance Trends by Standards

The **Compliance Trends by Standards** panel displays the compliance scores for standards. This trend is based on the compliance score against all evaluated standards at the end of every month. The panel displays a 2D-line chart.

Standard Compliance Management is the area of interest for this panel.

The panel displays the following information:

Table E-293 Components for the Compliance Trends by Standards Panel

Components	Description
Dimension (X axis)	Trend By End of Month
Measure (Y axis)	Compliance Score (%)
Chart style	2D-line chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the compliance score trend for evaluated standards:

The table displays the compliance score for January 2011:

Table E-294 January 2011 compliance score

Asset/Standard	Standard1	Standard2	Standard3
Asset1	50	33.33	70
Asset2	75	100	50
Asset3	25	50	75

For January 2011 the average compliance score for each standard is as follows:

```
Standard1 = (50+75+25)/3 = 50%
```

```
Standard2 = (33.33+100+50)/3 = 61.11%
```

```
Standard3 = (70+50+75)/3 = 65%
```

The table displays the compliance score for February 2011:

Table E-295 February 2011 compliance score

Asset/Standard	Standard1	Standard2	Standard3
Asset1	50	33.33	95
Asset2	90	90	50
Asset3	40	75	50
Asset4	50	50	50

For February 2011 the average compliance score for each standard is as follows:

```
Standard1 = (50+90+40+50)/4 = 57.5%
```

```
Standard2 = (33.33+90+75+50)/4 = 53.75%
```

```
Standard3 = (95+50+50+50)/4 = 61.25%
```

The trend panel displays the compliance score for each evaluated standard at end of each month.

From the Dashboard Taskbar you can do the following:

Table E-296 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.

Table E-296 Dashboard Taskbar *(continued)*

Option Name	Description
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

Control Status Trends for Mandates

The **Control Status Trends for Mandates** panel displays a control count for all available control result status for all the controls mapped to control statement. This trend is based on the control count against assets mapped to mandates at the end of every month. The panel displays a 2D-line chart.

Mandate and Policy Compliance Management is the area of interest for this panel.

The panel displays the following information:

Table E-297 Components for the Control Status Trends for Mandates Panel

Components	Description
Dimension (X axis)	Trends by End of Month
Measure (Y axis)	Instances
Chart style	2D-line chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the control status trend for mandates:

`The Control statement1 is mapped to 5 controls, Control1, Control2, Control3, Control4, and Control5.`

`Mandate1 mapped to Control statement1.`

The following table displays the January 2011 evaluation of Mandate1 against the assets, Asset1, Asset2, and Asset3:

Table E-298 January 2011 Control evaluation details

Asset/Control	Control1	Control2	Control3	Control4	Control5
Asset1	Pass	Fail	Pass	NA	Unknown
Asset2	Fail	Fail	Error	Pass	NA
Asset3	Fail	Pass	Fail	Fail	Unknown

For January 2011 the panel shows following control count for each control result status:

`Pass = 4, Fail = 6, Error = 1, Unknown = 2, Not Applicable = 2.`

`The Control statement2 is mapped to 5 controls, Control1, Control2, Control3, Control4, and Control5.`

`Mandate2 mapped to Control statement2.`

The following table displays the February 2011 evaluation of Mandate2 against the assets, Asset1, Asset2, and Asset3:

Table E-299 February 2011 Control evaluation details

Asset/Control	Control1	Control2	Control3	Control4	Control5
Asset1	Fail	Fail	Pass	Unknown	NA
Asset2	Fail	Unknown	Pass	Pass	Fail
Asset3	Pass	Error	Fail	NA	Fail

For February 2011 the panel shows following control count for each control result status:

`Pass = 4, Fail = 6, Error = 1, Unknown = 2, Not Applicable = 2`

Therefore, at the end of February 2011 the trend panel displays the following control count result based on control count for Mandate2 as:

`Pass = 4, Fail = 6, Error = 1, Unknown = 2, Not Applicable = 2`

From the Dashboard Taskbar you can do the following:

Table E-300 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

Control Status Trends for Policies

The **Control Status Trends for Policies** panel displays a control count for all available control result status for all the controls mapped to control statement. This trend is based on the control count against all available control result status at the end of every month. The panel displays a 2D-line chart.

Mandate and Policy Compliance Management is the area of interest for this panel.

The panel displays the following information:

Table E-301 Components for the Control Status Trends for Policies Panel

Components	Description
Dimension (X axis)	Trends by End of Month
Measure (Y axis)	Instances
Chart style	2D-line chart

Table E-301 Components for the Control Status Trends for Policies Panel *(continued)*

Components	Description
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the control status trend for policies:

`The Control statement1 is mapped to 5 controls, Control1, Control2, Control3, Control4, and Control5.`

`Policy1 is scoped to Asset1, Asset2, and Asset3 and mapped to Control statement1.`

The following table displays the January 2011 evaluation of Policy1 against the assets, Asset1, Asset2, and Asset3:

Table E-302 January 2011 Control evaluation details

Asset/Control	Control1	Control2	Control3	Control4	Control5
Asset1	Pass	Fail	Pass	NA	Unknown
Asset2	Fail	Fail	Error	Pass	NA
Asset3	Fail	Pass	Fail	Fail	Unknown

For January 2011 the panel shows following control count for each control result status:

`Pass = 4, Fail = 6, Error = 1, Unknown = 2, Not Applicable = 2.`

`The Control statement2 is mapped to 5 controls, Control1, Control2, Control3, Control4, and Control5.`

`Policy2 is scoped to Asset1, Asset2, and Asset3 and mapped to Control statement2.`

The following table displays the February 2011 evaluation of Policy2 against the assets, Asset1, Asset2, and Asset3:

Table E-303 February 2011 Control evaluation details

Asset/Control	Control1	Control2	Control3	Control4	Control5
Asset1	Fail	Fail	Pass	Unknown	NA
Asset2	Fail	Unknown	Pass	Pass	Fail

Table E-303 February 2011 Control evaluation details *(continued)*

Asset/Control	Control1	Control2	Control3	Control4	Control5
Asset3	Pass	Error	Fail	NA	Fail

For February 2011 the panel shows following control count for each control result status:

```
Pass = 4, Fail = 6, Error = 1, Unknown = 2, Not Applicable = 2
```

Therefore, at the end of February 2011 the trend panel displays the following control count result based on control count for Policy2 as:

```
Pass = 4, Fail = 6, Error = 1, Unknown = 2, Not Applicable = 2
```

From the Dashboard Taskbar you can do the following:

Table E-304 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

Overall Failure Trend of Checks

The **Failure Trends for Assets** panel displays a failure trend for assets. This trend is based on the count of failed checks against assets at the end of every month. The panel displays a 2D-line chart.

The panel displays the following information:

Table E-305 Components for the Failure Trends for Assets Panel

Components	Description
Dimension (X axis)	Trends by End of Month
Measure (Y axis)	Number of Failed Checks for Asset
Chart style	2D-line chart
Properties	The Properties button on the title bar opens the Panel Properties

The following is an example to determine the failure trend for assets:

```
The standard, Standard1 has 5 checks, Check1, Check2, Check3, Check4,
and Check5.
```

The following table displays the January 2011 evaluation of Standard1 against the assets, Asset1, Asset2, and Asset3:

Table E-306 January 2011 evaluation of Standard1

Asset/Check	Check1	Check2	Check3	Check4	Check5
Asset1	Pass	Fail	Pass	NA	Unknown
Asset2	Fail	Fail	Error	Pass	NA
Asset3	Fail	Pass	Fail	Fail	Fail

```
The evaluation of failed check result for assets in January 2011 =
7.
```

The following table displays the February 2011 evaluation of Standard1 against the assets, Asset1, Asset2, and Asset3:

Table E-307 February 2011 evaluation of Standard1

Asset/Check	Check1	Check2	Check3	Check4	Check5
Asset1	Pass	Fail	Pass	NA	Unknown

Table E-307 February 2011 evaluation of Standard1 *(continued)*

Asset/Check	Check1	Check2	Check3	Check4	Check5
Asset2	Fail	Pass	Error	Pass	NA
Asset3	Fail	Pass	Pass	Pass	Pass

```
The evaluation of failed check result for assets in February 2011 =
3.
```

The trend panel displays the following data:

```
Failed checks against assets at end of January = 7.
```

```
Failed checks against assets at end of February = 10.
```

From the Dashboard Taskbar you can do the following:

Table E-308 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

Aggregated Risk Score for CCS VM Sites

The **Aggregated Risk Score for CCS VM Sites** panel displays aggregated risk score for CCS Vulnerability Manager sites. The panel displays a 2D-bar chart.

Symantec CCS Vulnerability Manager is the area of interest for this panel.

The panel displays the following information:

Table E-309 Components for the Aggregated Risk Score for CCS VM Sites Panel

Components	Description
Dimension (X axis)	CCS VM Site Name
Measure (Y axis)	Sum of Device Risk Score
Chart style	2D-bar chart
Properties	The Properties button on the title bar opens the Panel Properties

You can click the bar to drill down and view a table for detailed information.

The table displays the following columns:

Table E-310 Aggregated Risk Score for CCS VM Sites

Column Name	Description
Device IP Address	Displays the IP address of the device.
Device Host Name	Displays the host name of the device.
Device Risk Score	Displays the aggregated risk score of the device.
CCS VM Site Name	Displays the name of the CCS Vulnerability Manager site.
CCS VM Site Description	Displays the description of the CCS Vulnerability Manager site.

From the Dashboard Taskbar you can do the following:

Table E-311 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.

Table E-311 Dashboard Taskbar *(continued)*

Option Name	Description
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-312 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-bar chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Top 10 Most Common Network Vulnerabilities

The **Top 10 Most Common Network Vulnerabilities** panel displays the top 10 most common network vulnerabilities. The panel displays a 2D-bar chart.

Symantec CCS Vulnerability Manager is the area of interest for this panel.

The panel displays the following information:

Table E-313 Components for the Top 10 Most Common Network Vulnerabilities Panel

Components	Description
Dimension (X axis)	Vulnerability Name
Measure (Y axis)	Top 10 Count of Device IP Address
Chart style	2D-bar chart
Properties	The Properties button on the title bar opens the Panel Properties

You can click the bar to drill down and view a table for detailed information.

The table displays the following columns:

Table E-314 Top 10 Most Common Network Vulnerabilities

Column Name	Description
Device IP Address	Displays the IP address of the device.
Device Host Name	Displays the host name of the device.
Vulnerability Name	Displays the name of the network vulnerability. The Vulnerability Name opens a page with detailed information on the selected vulnerability.

From the Dashboard Taskbar you can do the following:

Table E-315 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.

Table E-315 Dashboard Taskbar *(continued)*

Option Name	Description
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-316 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-bar chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Vulnerabilities by CVSS Score Range

The **Vulnerabilities by CVSS Score Range** panel displays the vulnerabilities by CVSS score range. The panel displays a 2D-bar chart.

Symantec CCS Vulnerability Manager is the area of interest for this panel.

The panel displays the following information:

Table E-317 Components for the Vulnerabilities by CVSS Score Range Panel

Components	Description
Dimension (X axis)	Vulnerability CVSS Score Range
Measure (Y axis)	Count of Vulnerabilities Name

Table E-317 Components for the Vulnerabilities by CVSS Score Range Panel *(continued)*

Components	Description
Chart style	2D-bar chart
Properties	The Properties button on the title bar opens the Panel Properties

You can click the bar to drill down and view a table for detailed information.

The table displays the following columns:

Table E-318 Vulnerabilities by CVSS Score Range

Column Name	Description
Device IP Address	Displays the IP address of the device.
Device Host Name	Displays the host name of the device.
Vulnerability Name	Displays the name of the network vulnerability. The Vulnerability Name opens a page with detailed information on the selected vulnerability.
Vulnerability CVSS Score	Displays the CVSS score of the vulnerability.
Vulnerability CVSS Vector	Displays the CVSS vector of the vulnerability.
Vulnerability Severity	Displays the severity of the vulnerability.
Vulnerability Published Date	Displays the date on which the vulnerability is published.
Vulnerability Score Range	Displays the CVSS score range of the vulnerability.

From the Dashboard Taskbar you can do the following:

Table E-319 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.

Table E-319 Dashboard Taskbar *(continued)*

Option Name	Description
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-320 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-bar chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Vulnerabilities by Severity

The **Vulnerabilities by Severity** panel displays the vulnerabilities by severity. The panel displays a 2D-pie chart.

Symantec CCS Vulnerability Manager is the area of interest for this panel.

The panel displays the following information:

Table E-321 Components for the Vulnerabilities by Severity Panel

Components	Description
Dimension (X axis)	Vulnerability Severity
Measure (Y axis)	Count of Vulnerability Name
Chart style	2D-pie chart
Properties	The Properties button on the title bar opens the Panel Properties

You can click on the pie to drill down and view a table for detailed information.

The table displays the following columns:

Table E-322 Vulnerabilities by Severity

Column Name	Description
Device IP Address	Displays the IP address of the device.
Device Host Name	Displays the host name of the device.
Vulnerability Name	Displays the name of the network vulnerability. The Vulnerability Name opens a page with detailed information on the selected vulnerability.
Vulnerability CVSS Score	Displays the CVSS score of the vulnerability.
Vulnerability CVSS Vector	Displays the CVSS vector of the vulnerability.
Vulnerability Severity	Displays the severity of the vulnerability.
Vulnerability Published Date	Displays the date on which the vulnerability is published.

From the Dashboard Taskbar you can do the following:

Table E-323 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-324 General options

Options	Descriptions
Back to chart	Lets you return to the 2D-pie chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel.

Alerts and Notifications

The **Alerts and Notifications** panel displays alerts for the risk objectives present in the system. The system generates the alerts using the Risk Analytics engine which is part of the centralized metrics calculation job.

Risk Management is the area of interest for this panel.

The panel displays the following information:

Table E-325 Components for the Alerts and Notifications Panel

Components	Description
Dimension (X axis)	Alert
Measure (Y axis)	Risk Objective Name (Count)
Chart style	Alert Chart
Properties	The Properties button on the title bar opens the Panel Properties

Risk manager monitors the risk score and displays appropriate alerts and notifications under the Alerts and Notifications panel. The Alerts will be ranked by severity with the most severe alert at the top.

From the Dashboard Taskbar you can do the following:

Table E-326 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.

Table E-326 Dashboard Taskbar *(continued)*

Option Name	Description
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-327 General options

Options	Descriptions
Properties	Lets you open the Panel Properties.

Asset Group Yearly Trend

The **Asset Group Yearly Trend** panel displays yearly trend of the risk score for an asset group.

Risk Management is the area of interest for this panel.

The panel displays the following information:

Table E-328 Components for the Asset Group Yearly Trend Panel

Components	Description
Dimension (X axis)	Year
Measure (Y axis)	Risk Score
Chart style	2D Line Chart
Properties	The Properties button on the title bar opens the Panel Properties

From the Dashboard Taskbar you can do the following:

Table E-329 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-330 General options

Options	Descriptions
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you select the option to view the quarterly trend.

Control Category Yearly Trend

The **Control Category Yearly Trend** panel displays yearly trend of the risk score for a control category.

Risk Management is the area of interest for this panel.

The panel displays the following information:

Table E-331 Components for the Control Category Yearly Trend Panel

Components	Description
Dimension (X axis)	Year
Measure (Y axis)	Risk Score
Chart style	2D Line Chart
Properties	The Properties button on the title bar opens the Panel Properties

From the Dashboard Taskbar you can do the following:

Table E-332 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-333 General options

Options	Descriptions
Properties	Lets you open the Panel Properties.

Table E-333 General options *(continued)*

Options	Descriptions
Orientation Options	Lets you select the option to view the quarterly trend.

My Security Objectives

The **My Security Objectives** panel displays the risk score of the security objectives.

Risk Management is the area of interest for this panel.

The panel displays the following information:

Table E-334 Components for the My Security Objectives Panel

Components	Description
Dimension (X axis)	Not applicapble
Measure (Y axis)	Not applicapble
Chart style	Tabular
Properties	The Properties button on the title bar opens the Panel Properties

The table displays the following columns:

Table E-335 My Security Objectives

Column Name	Description
Risk Score	Displays the risk score of the asset for which the check is associated with.
My Role	Displays your role status.
Security Objective	Displays the name of the security objective.
Security Objective Creator	Displays the name of the creator of the security objective.
Security Objective Owner	Displays the name of the owner of the security objective.
Target Date	Displays the target date of the security objective.

Table E-335 My Security Objectives *(continued)*

Column Name	Description
Target Risk	Displays the target risk of the security objective.

From the Dashboard Taskbar you can do the following:

Table E-336 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-337 General options

Options	Descriptions
Properties	Lets you open the Panel Properties.

Risk by Action Status

The **Risk by Action Status** panel displays the risk by action status.

Risk Management is the area of interest for this panel.

The panel displays the following information:

Table E-338 Components for the Risk by Action Status Panel

Components	Description
Dimension (X axis)	Not applicapble
Measure (Y axis)	Not applicapble
Chart style	2D Concave Doughnut Chart
Properties	The Properties button on the title bar opens the Panel Properties

From the Dashboard Taskbar you can do the following:

Table E-339 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-340 General options

Options	Descriptions
Properties	Lets you open the Panel Properties.

Security Objective Yearly Trend

The **Security Objective Yearly Trend** panel displays yearly trend of the risk score for a security objective.

Risk Management is the area of interest for this panel.

The panel displays the following information:

Table E-341 Components for the Security Objective Yearly Trend Panel

Components	Description
Dimension (X axis)	Year
Measure (Y axis)	Risk Score
Chart style	2D Line Chart
Properties	The Properties button on the title bar opens the Panel Properties

From the Dashboard Taskbar you can do the following:

Table E-342 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.

Table E-342 Dashboard Taskbar *(continued)*

Option Name	Description
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-343 General options

Options	Descriptions
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you select the option to view the quarterly trend.

Overall Risk - Security Objective

The **Overall Risk - Security Objective** panel displays the average risk score of the security objectives. The panel displays a gauge chart of a security objective name and what is the current overall risk score.

Risk Management is the area of interest for this panel.

The panel displays the following information:

Table E-344 Components for the Overall Risk - Security Objective Panel

Components	Description
Dimension (X axis)	Security Objective Name
Measure (Y axis)	Risk Score (Average)
Chart style	Gauge Chart
Properties	The Properties button on the title bar opens the Panel Properties

From the Dashboard Taskbar you can do the following:

Table E-345 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available page with the Overall Risk – Security Objective panel:

Table E-346 General options

Options	Descriptions
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you select the option to view the details or create an action plan.

Security Objectives Heatmap

The **Security Objectives Heatmap** panel displays the count of security objectives by impact and likelihood values. The panel displays a HeatMap chart of the security objective likelihood and what is the current risk objective impact. A cell in the Heatmap displays the count of security objectives for corresponding values of Impact and Likelihood.

Risk Management is the area of interest for this panel.

The panel displays the following information:

Table E-347 Components for the Security Objectives Heatmap Panel

Components	Description
Dimension (X axis)	Risk Objective Likelihood
Measure (Y axis)	Risk Objective Name (Count)
Chart style	HeatMap Chart
Properties	The Properties button on the title bar opens the Panel Properties

You can click one of the bars to drill down and view a table for detailed information.

The table displays the following columns:

Table E-348 Security Objectives Heatmap

Column Name	Description
Security Objective	Displays the name of the security objective.
Impact	Displays the impact of the security objective.
Likelihood	Displays the likelihood of the security objective.
Target Risk	Displays the target risk of the security objective.
Target Date	Displays the target date of the security objective.
Security Objective Description	Displays the description of the security objective.
Security Objective Owner	Displays the owner of the security objective.

From the Dashboard Taskbar you can do the following:

Table E-349 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.

Table E-349 Dashboard Taskbar *(continued)*

Option Name	Description
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-350 General options

Options	Descriptions
Back to chart	Lets you return to the HeatMap chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.

Top 10 Asset Groups with Maximum Risk

The **Top 10 Asset Groups with Maximum Risk** panel displays top 10 assets groups with the maximum risk. The panel displays a 2D column chart of the risk score of each asset group in the chart.

Risk Management is the area of interest for this panel.

The panel displays the following information:

Table E-351 Components for the Top 10 Asset Groups with Maximum Risk Panel

Components	Description
Dimension (X axis)	Asset Group Name
Measure (Y axis)	Risk Score (Average)
Chart style	2D Column Chart
Properties	The Properties button on the title bar opens the Panel Properties

The table displays the following columns:

Table E-352 Top 10 Asset Groups with Maximum Risk

Column Name	Description
Risk Score	Displays the risk score of the asset for which the check is associated with.
Control Statement Name	Displays the name of the control statement.
Asset Name	Displays the name of the asset.
Asset Display Path	Displays the location path of the asset.
Asset Type	Displays the type of the asset.
Asset Group	Displays the name of the asset group.
Asset Group Type	Displays the type of the asset group.

From the Dashboard Taskbar you can do the following:

Table E-353 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.

Table E-353 Dashboard Taskbar *(continued)*

Option Name	Description
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-354 General options

Options	Descriptions
Back to chart	Lets you return to the 2D column chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel or create an action plan.

Top 10 Assets with Highest Risk Score

The **Top 10 Assets with Highest Risk Score** panel displays the top 10 network assets with the highest risk score. The panel displays a 2D column chart of the risk score of each asset in the chart.

Risk Management is the area of interest for this panel.

The panel displays the following information:

Table E-355 Components for the Top 10 Assets with Highest Risk Score Panel

Components	Description
Dimension (X axis)	Asset Name
Measure (Y axis)	Risk Score (Average)
Chart style	2D Column Chart
Properties	The Properties button on the title bar opens the Panel Properties

You can click one of the bars to drill down and view a table for detailed information.

The table displays the following columns:

Table E-356 Top 10 Assets with Highest Risk Score

Column Name	Description
Risk Score	Displays the risk score of the asset for which the check is associated with.
Control Statement Name	Displays the name of the control statement.
Asset Name	Displays the name of the asset.
Asset Display Path	Displays the location path of the asset.
Asset Type	Displays the type of the asset.

From the Dashboard Taskbar you can do the following:

Table E-357 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.

Table E-357 Dashboard Taskbar *(continued)*

Option Name	Description
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-358 General options

Options	Descriptions
Back to chart	Lets you return to the 2D column chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel or create an action plan.

Top 5 Business Units at Highest Risk

The **Top 5 Business Units at Highest Risk** panel displays the top 5 business units that are at the highest risk. The panel displays a 3D column chart of the risk score of each business asset in the chart.

Risk Management is the area of interest for this panel.

The panel displays the following information:

Table E-359 Components for the Top 5 Business Units at Highest Risk Panel

Components	Description
Dimension (X axis)	Business Asset Name

Table E-359 Components for the Top 5 Business Units at Highest Risk Panel *(continued)*

Components	Description
Measure (Y axis)	Risk Score (Average)
Chart style	3D Column Chart
Properties	The Properties button on the title bar opens the Panel Properties

You can click one of the bars to drill down and view a table for detailed information.

The table displays the following columns:

Table E-360 Top 5 Business Units at Highest Risk

Column Name	Description
Risk Score	Displays the risk score of the business asset for which the check is associated with.
Business Asset	Displays the name of the business asset.
Asset Display Path	Displays the location path of the asset.
Asset Group	Displays the name of the asset group.
Asset Name	Displays the name of the asset.
Asset Type	Displays the type of the asset.
Control Statement Name	Displays the name of the control statement.
Asset Group Type	Displays the type of the asset group.

From the Dashboard Taskbar you can do the following:

Table E-361 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.

Table E-361 Dashboard Taskbar *(continued)*

Option Name	Description
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-362 General options

Options	Descriptions
Back to chart	Lets you return to the 3D column chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel or create an action plan.

Top 5 Control Categories at Highest Risk

The **Top 5 Control Categories at Highest Risk** panel displays the top 5 control categories that are at the highest risk. The panel displays a 2D column chart of the risk score of each control category in the chart.

Risk Management is the area of interest for this panel.

The panel displays the following information:

Table E-363 Components for the Top 5 Control Categories at Highest Risk Panel

Components	Description
Dimension (X axis)	Control Category Name
Measure (Y axis)	Risk Score (Average)
Chart style	2D Column Chart
Properties	The Properties button on the title bar opens the Panel Properties

You can click one of the bars to drill down and view a table for detailed information.

The table displays the following columns:

Table E-364 Top 5 Control Categories at Highest Risk

Column Name	Description
Risk Score	Displays the risk score of the asset for which the check is associated with.
Control Statement Name	Displays the name of the control statement.
Asset Name	Displays the name of the asset.
Asset Display Path	Displays the location path of the asset.
Asset Type	Displays the type of the asset.
Control Category Name	Displays the name of the control category.

From the Dashboard Taskbar you can do the following:

Table E-365 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.

Table E-365 Dashboard Taskbar *(continued)*

Option Name	Description
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-366 General options

Options	Descriptions
Back to chart	Lets you return to the 2D column chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel or create an action plan.

Top 5 Security Objectives with Highest Base Risk (with Provider Weight)

The **Top 5 Security Objectives with Highest Base Risk (with Provider Weight)** panel displays the top 5 security objectives with the highest base risk. The panel displays a 2D Column chart of the risk score of each security objective in the chart.

Risk Management is the area of interest for this panel.

The panel displays the following information:

Table E-367 Components for the Top 5 Security Objectives with Highest Base Risk (with Provider Weight)

Components	Description
Dimension (X axis)	Security Objective
Measure (Y axis)	Weighted Base Risk Score (Average)
Chart style	2D Column Chart
Properties	The Properties button on the title bar opens the Panel Properties

You can click one of the bars to drill down and view a table for detailed information.

The table displays the following columns:

Table E-368 Top 5 Security Objectives with Highest Base Risk (with Provider Weight)

Column Name	Description
Weighted Base Risk Score	Displays weighted base risk score of the asset.
Security Objective	Displays the name of the security objective.
Asset Name	Displays the name of the asset.
Asset Type	Displays the type of the asset.

From the Dashboard Taskbar you can do the following:

Table E-369 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.
Copy	You can copy the panel.

Table E-369 Dashboard Taskbar *(continued)*

Option Name	Description
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-370 General options

Options	Descriptions
Back to chart	Lets you return to the 2D Column chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel or create an action plan.

Top 5 Security Objectives with Maximum Risk

The **Top 5 Security Objectives with Maximum Risk** panel displays the top 5 security objectives with the highest risk score. The panel displays a Pareto chart of the risk score of each security objective in the chart.

Risk Management is the area of interest for this panel.

The panel displays the following information:

Table E-371 Components for the Top 5 Security Objectives with Maximum Risk Panel

Components	Description
Dimension (X axis)	Security Objective Name
Measure (Y axis)	Risk Score (Average)
Chart style	Pareto Chart
Properties	The Properties button on the title bar opens the Panel Properties

You can click one of the bars to drill down and view a table for detailed information.

The table displays the following columns:

Table E-372 Top 5 Security Objectives with Maximum Risk

Column Name	Description
Risk Score	Displays the risk score of the asset for which the check is associated with.
Security Objective	Displays the name of the security objective.
Security Objective Owner	Displays the owner of the security objective.
Target Date	Displays the target date of the security objective.
Target Risk	Displays the target risk of the security objective.

From the Dashboard Taskbar you can do the following:

Table E-373 Dashboard Taskbar

Option Name	Description
New Dashboard	You click this to launch the Create Dashboard page.
New Panel	You click this to launch the create panel page.
Edit	You can edit the panel. This is active for custom created panel.

Table E-373 Dashboard Taskbar *(continued)*

Option Name	Description
Copy	You can copy the panel.
Delete	You can delete the panel. This is active for custom created panel.
Import	You click this to launch the Import Panel dialog page.
Publish	You can publish the panel. This is active for custom created panel.
Unpublish	You can unpublish the panel. This is active for custom created panel.

The table displays the following options available at the top of the drill through page:

Table E-374 General options

Options	Descriptions
Back to chart	Lets you return to the Pareto chart in the first panel.
Page Size	Lets you select the number of rows that the table displays. The default value is 25.
Export to Excel	Lets you export the information in the table to Microsoft Excel.
Properties	Lets you open the Panel Properties.
Orientation Options	Lets you drill down to another chart panel or create an action plan.

Appendix F

Migration utilities

This appendix includes the following topics:

- About the Symantec 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 F-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

Table F-1 ESM and CCS content mapping *(continued)*

ESM	CCS
ESM check description	CCS check description
ESM message, message string ID, or message numeric ID	CCS check expression
ESM check CIA value	CCS check CIA value

Note: Only the compliance-related checks include the CIA value. If an ESM check does not pertain to compliance, then the CIA value for the corresponding CCS check displays as “Undefined”.

If an ESM policy contains both the application module checks and the operating system module checks, then the CCS standard for the policy is considered for the application module checks only.

About packaging and deployment

A Web package by the name Symantec_Control_Compliance_Suite_ESM_SU_42_Migration_Utility_11_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
Symantec™ ESM Policy to CCS Standard Migration Utility User Guide	Documentation

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
- Microsoft Windows 7

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. **Note:** Unlike the earlier versions of the migration utility that only required a policy xml as an input, the current version also requires a template folder containing the template files that are included in the ESM policy. The Policy tool when run with the export option for the specified ESM policy, creates the template folder under the parent folder that contains the policy xml.
`-m`	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. See "About the message IDs in ESM Policy to CCS Standard Migration Utility" on page 725.

`-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`

This parameter is optional. If you specify this option, then the migration utility does not migrate the ESM suppressions to CCS Standard.

See "About ESM suppressions migration" on page 725.

`-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 724.

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 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
Windows 2003	205336
Windows 2008	248336
Windows Vista	228336
Windows XP	200336
Windows 7	258336

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

If you specify the message expression type as 'Numeric' by using the -m switch for a policy that contains application modules, then the migration of all the application module checks is done by using the message expression as 'String'. The migration utility changes the message expression type to 'String' only for the application module checks. The database module checks are migrated by using the message expression type as 'Numeric'. If the ESM policy that you want to migrate contains application module checks, then the migration tool displays the following warning:

“The ESM policy contains at least one application module. The message expression type 'String' will be used to migrate the application module checks”.

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
  - Tru64
- 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 725.
- The utility sets CIA attributes to default values.
- The utility migrates only the enabled ESM checks from the ESM policy.

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 Compliance Suite Web Console A Web-based user interface for creating policy awareness and managing dynamic dashboards.

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.

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.

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