Symantec™ Control Compliance Suite Planning and Deployment Guide

Version: 11.1

Symantec™ Control Compliance Suite Planning and Deployment Guide

Documentation version: 11.1

Legal Notice

passwords, security logs, server logs, which is stored on Your system only and is not transmitted to Symantec. Please contact Your network administrator for further details.

Telemetry Option; Non-Personal Information. The Licensed Software contains a telemetry feature which may collect non-personal information. Such non-personal information may include, without limitation, machine configuration, SQL server details, license status, and system performance and will not be correlated with any personal information. Unless You affirmatively opt-out of this feature, telemetry will be automatically enabled to transmit such non-personal information to Symantec so we can better understand the usability and supportability of the product.

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, DVDs, 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

Contents

Chapter 1

Understanding CCS

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. 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.

See "How to achieve your business objective with CCS" on page 14.

The CCS Suite is the host infrastructure in CCS. You must deploy the CCS Suite to use any of the CCS capabilities.

See “CCS architecture” on page 19.

You can use CCS to collect data using the following methods:

- Raw-data based content using agent-less or agent-based methods
- Message based content using agent-based method
- Security assessment data from external data systems

See “About the CCS deployment” on page 34.

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 CCS Assessment Manager for assessment.

For details about external data systems, See “External data systems architecture” on page 113.

How to achieve your business objective with CCS

You can use CCS to meet different business objectives such as:

- Plan for internal and external audits
- Assess technical controls
- Evaluate exposure to external threats
- Assess procedural controls
- Assess data controls
- Report on IT risk and compliance posture

The following table helps you understand how CCS helps you achieve your business objective and the CCS modules you must deploy to meet that objective.

Note: The CCS Suite comprises of the CCS Application Server and the CCS Manager.

You must plan your CCS deployment based on your business objective.

Table 1-1 How to achieve your business objective with CCS

Business objective to achieve	How CCS helps achieve the objective	CCS components to be deployed?
Plan for internal and external audits	Policy Manager ■ CCS hosts more than 150 customizable sample policies and templates. ■ The policies are mapped to technical and procedural controls, that let you measure a given a control and use the results across multiple mandates. ■ You can also import your own data from the existing data collection solution to use the CCS Policy Manager	CCS Suite AND CCS Agent OR External Data System See "About the CCS deployment" on page 34. For an example scenario and procedures to plan for internal and external audits, see the *Symantec Control Compliance Suite Quick Start Guide for Policy Compliance*.
Assess technical controls	Standards Manager ■ CCS provides a capacity to assess the security compliance of the assets against a set of standards. ■ You can use predefined standards or can create custom standards to evaluate your assets. ■ You can also import your own data from the existing data collection solution to use the CCS Policy Manager	CCS Suite AND CCS Agent OR External Data System See "About the CCS deployment" on page 34. For an example scenario and procedures for assessing technical controls, see the *Symantec Control Compliance Suite Quick Start Guide for security compliance*.

Table 1-1 How to achieve your business objective with CCS *(continued)*

Business objective to achieve	How CCS helps achieve the objective	CCS components to be deployed?
Evaluate exposure to external threats	External Data Integration ■ CCS provides a capability to integrate with external data systems. CCS also supports Vulnerability Manager as a pre-integrated external data systems. ■ You can use the Vulnerability Manager to prevent threats to critical assets by quickly identifying vulnerabilities in your most sensitive servers, Web-based applications, operating systems, and databases.	CCS Suite AND Symantec CCS Vulnerability Manager See "About the CCS deployment" on page 34. For an example scenario and procedures to assess the external data, see the *Symantec Control Compliance Suite Quick Start Guide for External Data Integration*.
Assess procedural controls	External Data Integration ■ CCS provides a capability to integrate with external data systems. CCS also supports CCS Assessment Manager (AM) as a pre-integrated external data systems. ■ You can use AM for procedural controls with its built-in content and mandates.	CCS Suite AND Symantec CCS Assessment Manager See "About the CCS deployment" on page 34. For an example scenario and procedures to assess the external data, see the *Symantec Control Compliance Suite Quick Start Guide for External Data Integration*.

Table 1-1 How to achieve your business objective with CCS *(continued)*

Business objective to achieve	How CCS helps achieve the objective	CCS components to be deployed?
Assess data controls	External Data Integration ■ CCS provides a capability to integrate with external data systems. CCS also supports Data Loss Prevention (DLP) as a pre-integrated external data systems. ■ You can use DLP to scans your network, endpoints, and servers to check the loss of sensitive data	CCS Suite AND Symantec Data Loss Prevention See "About the CCS deployment" on page 34. For an example scenario and procedures to assess the external data, see the *Symantec Control Compliance Suite Quick Start Guide for External Data Integration*.

Table 1-1 How to achieve your business objective with CCS *(continued)*

Business objective to achieve	How CCS helps achieve the objective	CCS components to be deployed?
Assess IT risk	Risk Manager ■ CCS enables you to Transform IT risk into business-relevant risk metrics that can be shared with key stakeholders to drive awareness, accountability, and action. ■ You can visualize current risk exposure and analyze historical trends to illustrate how your IT risk and compliance program systematically reduces risks to the business over time. ■ You can prioritize remediation efforts based on business risk rather than technical severity. ■ You can work with key business stakeholders to make consistent plans for better security practices within their business and monitor progress against these plans on an ongoing basis.	CCS Suite AND CCS Agent OR External Data System See "About the CCS deployment" on page 34. For an example scenario and procedures to assess the IT risk, see the *Symantec Control Compliance Suite Quick Start Guide for Risk Compliance*.
Report on IT risk and compliance posture	Reports and Dynamic Dashboards ■ CCS supports various predefined reports and dynamic Dashboards to present a snapshot of the compliance posture of your system.	CCS Suite See "About the CCS deployment" on page 34.

Note: For more information on the CCS ISS APIs including Web APIs, Controls Studio APIs, and Workflows refer to *Symantec Control Compliance Suite API Referenece Guide*. For details on the CCS PowerShell cmdlets, refer to SymHelp, which is installed with the product.

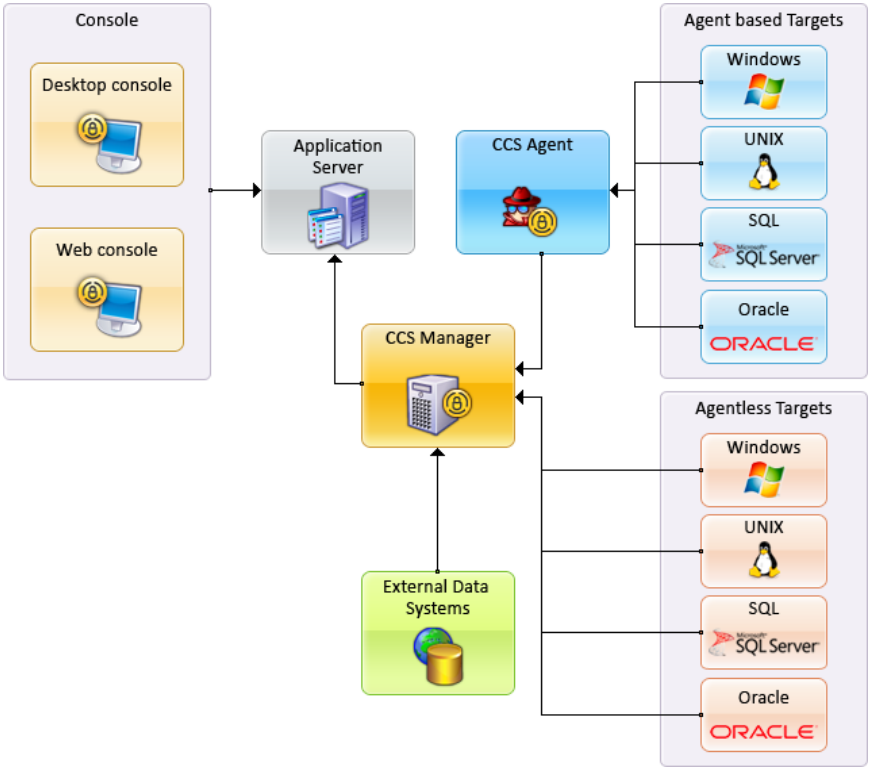
See "About the CCS deployment" on page 34.

CCS architecture

CCS consists of a number of components that work together. The components collect, store, and analyze data from the network, then transmit that data to clients in a usable form. In some instances, a single computer can serve in more than one role. Other roles require a dedicated server.

See Figure 1-1 on page 19. illustrates how the CCS components work together.

Figure 1-1 CCS Infrastructure Architecture Diagram



See “Components of CCS” on page 20.

See “About raw-data collection” on page 98.

See “About message based data collection” on page 100.

Components of CCS

The various components of CCS can be described as follows:

Table 1-2 Components of CCS

Component	Description
Application Server	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 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. See “CCS Application Server” on page 22.
CCS Manager	CCS Manager performs up to five different duties in CCS. Each of these duties is called a role. A single instance of the CCS Manager can provide more than one role simultaneously. Normally, a CCS deployment includes many servers that each hosts a CCS Manager installation. When a deployment contains multiple CCS Manager installations, each CCS Manager performs a single role. See “CCS Manager” on page 22.

Table 1-2 Components of CCS *(continued)*

Component	Description
CCS Agent	The CCS Agent resides on the computers in your network. The CCS Agent collects data about the target computer and forwards the data to the CCS Manager. The CCS Agent can: ■ Collect and interpret data about the security of the computer. The resulting data is forwarded to the CCS Manager . ■ Collect data about the security of the computer and forward the data to the CCS Manager. See "CCS Agent" on page 28.
Databases	CCS hosts the production and reporting databases. See "Databases" on page 28.
CCS Console	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. See "CCS Console" on page 30.
Web Console	CCS Web Console lets users access a subset of the CCS functionality using a web browser. See "CCS Web Console" on page 30.
Policy Central	Policy Central is intended for the policy audience. Policy Central allows the policy audience to respond to the published policies, request exceptions and clarifications if necessary. It also provides searching and filtering capabilities for the policies based on their review status. In addition the policy audience can download the policy document for reference or copy the policy link for distribution. See "Policy Central" on page 31.

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.

See “CCS architecture” on page 19.

See “CCS Web Console” on page 30.

CCS Manager

The CCS Manager performs up to five different duties in CCS. Each of these duties is called a role. A single instance of the CCS Manager can provide more than one role simultaneously. Normally, a CCS deployment includes many servers that each hosts a CCS Manager installation. When a deployment contains multiple CCS Manager installations, each CCS Manager performs a single role.

You can install the CCS Manager and the CCS Application Server on a single computer. For a scale-out deployment, you can install the CCS Application Server on one computer and keep adding one more CCS Managers as per your sizing

requirements. Installing more than one CCS Manager is conducive for load sharing and provides better scalability.

If you have more than one CCS Manager in your deployment, while applying SCU updates on the CCS Managers, ensure that all CCS Managers have the same version of SCU applied.

Note: You must deploy the CCS Manager in an Active Directory domain, although you can deploy the CCS Manager in a Windows workgroup when required. You can deploy only a CCS Manager in data collector role, in the Windows workgroup.

If you install the CCS Manager along with the CCS Application Server, using the CCS Suite installer, by default, that CCS Manager is registered in the System Topology in the CCS Console and all roles are assigned to that CCS Manager.

The CCS Manager contains the Data Processing Service and the ESM Manager Service.

In the **Services** control panel, the CCS Manager services are listed as Symantec Data Processing Service and Symantec ESM Manager.

The CCS Manager performs the following roles:

- Load Balancer
  See "About the CCS Manager Load Balancer" on page 24.
- Collector
  See "About the CCS Manager Collector" on page 25.
- Evaluator
  See "About the CCS Manager Evaluator" on page 27.
- Reporter
  See "About the CCS Manager Reporter" on page 27.
- External Data Connector
  See "About the CCS Manager External Data Connector" on page 28.

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

The CCS Manager performs the following functions for the agent:

- 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 LiveUpdate of the registered agents.
  The App Server creates granular LiveUpdate 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.

When you install a CCS Manager, you must have local administrator-equivalent privileges.

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

Ensure that there is a domain trust relationship between different domains in the following cases:

- If the CCS Manager in the evaluator or reporting role, and the Production database, Reporting database or the ADAM database are located in different domains.
- If the CCS Manager in the data collector role, and the target computers for Windows data collection on Oracle platform are located in different domains. You must have a one way trust from the CCS Manager domain to the target computer domain. CCS Manager must be able to login to the target computer.

See "User Privileges for deploying the CCS components" on page 55.

See "CCS architecture" on page 19.

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 25.

See "About the CCS Manager Evaluator" on page 27.

See "About the CCS Manager Reporter" on page 27.

See "About the CCS Manager External Data Connector" on page 28.

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.

See “CCS architecture” on page 19.

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
- VMware 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.

Note: CCS 11.1 does not support NDS and NetWare data collectors. In case you have upgraded from previous versions of CCS to 11.0 and then to 11.1, CCS collects data from NDS or NetWare platforms and functions in the same manner as in the previous versions of CCS 11.0.

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

See “CCS architecture” on page 19.

See “About the CCS Manager Load Balancer” on page 24.

See “About the CCS Manager Evaluator” on page 27.

See “About the CCS Manager Reporter” on page 27.

See “About the CCS Manager External Data Connector” on page 28.

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 “CCS architecture” on page 19.

See “About the CCS Manager Load Balancer” on page 24.

See “About the CCS Manager Collector” on page 25.

See “About the CCS Manager Reporter” on page 27.

See “About the CCS Manager External Data Connector” on page 28.

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 “CCS architecture” on page 19.

See “About the CCS Manager Load Balancer” on page 24.

See “About the CCS Manager Collector” on page 25.

See “About the CCS Manager Evaluator” on page 27.

See “About the CCS Manager External Data Connector” on page 28.

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 “About the CCS Manager Load Balancer” on page 24.

See “About the CCS Manager Collector” on page 25.

See “About the CCS Manager Evaluator” on page 27.

See “About the CCS Manager Reporter” on page 27.

CCS Agent

The CCS Agent resides on the computers in your network. The CCS Agent collects data about the target computer and forwards the data to the CCS Manager. The CCS Agent can:

- Collect data about the security of the computer and forward the data to the CCS Manager.
- Collect and interpret data about the security of the computer. The resulting data is forwarded to the CCS Manager.

The CCS agent can perform raw data-based as well as message-based data collection to assess security compliance. You can install the CCS Agent on Windows / UNIX computers.

In the **Services** control panel, the CCS Agent service is listed as Symantec ESM Agent.

Databases

CCS hosts the following types of databases:

- Production
  See “Production database” on page 29.
- Reporting
  See “Reporting database” on page 29.

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. If you use the Symantec CCS Assessment Manager with CCS, the CCS AM data is also stored in the production database.

The production database requires Microsoft SQL Server 2008, Microsoft SQL Server 2012, or Microsoft SQL Server 2014. 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.

See "Components of CCS" on page 20.

See "Reporting database" on page 29.

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 2008, Microsoft SQL Server 2012, or Microsoft SQL Server 2014. 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.

The reporting database, CSM_Reports contains two filegroups. All reporting data other than evidence data is stored in the default CSM_Reports filegroup. Evidence data is stored in a separate filegroup FG_EvidenceStorage_<yyyymmdd>.

The evidence filegroup Autogrowth settings are set at 512 MB with unrestricted file growth. You can change the Autogrowth settings according to your current filegroup size and growth rate.

By default, the reporting database recovery model is set to Simple. You can change the recovery model according to your recovery requirements.

See "Components of CCS" on page 20.

See "Production database" on page 29.

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.

For trust requirements for CCS Console, See "Network Ports" on page 41.

See "CCS architecture" on page 19.

See "CCS Web Console" on page 30.

CCS Web Console

CCS Web Console lets users access a subset of the CCS functionality using a web browser.

For a list of browsers supported by the CCS Web Console, See "Software requirements" on page 48.

In the Web console, users can do the following:

- 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.
- Enter your password to map the CCS and the SPC user profiles from the Credentials panel.

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

The computer that hosts the CCS Application Server also hosts the CCS Web Console server, and uses Windows NTLM authentication.

For trust requirements for CCS Web Console, See "Network Ports" on page 41.

On CCS Web Console Home page under Quick Tasks, **Go to Policy Central** link is available to navigate to policy central portal.

Policy Central lets you perform the following tasks:

- Accept or decline policies.
- Request policy exceptions.
- Request policy clarifications.

See "Policy Central" on page 31.

See "Launching the CCS Web Console and the Policy Central" on page 216.

Policy Central

Policy Central is a single portal to access your organizational policies and to manage policy attestations.

Policy Central is opened when you click the **Launch Policy Central** link on the CCS Home page.

For a list of browsers supported by the Policy Central, See "Software requirements" on page 48.

The **Policy Central** provides the following:

- Ability to download the policy document for reference or copy the policy link for distribution.
- Ability to view the policies organized in hierarchical structure and perform various operations like accept, decline, request exceptions and clarifications.
- Capability to look into policy document as well as policy names using the Search feature.
- Filter to locate the policy for the policy audience.
- Consolidated view of exceptions, clarifications, and historical events for the policy audience.

Policy Central comprises following two main sections:

- **Policies**
  You can click **Policies** section to view policies.

Note: After upgrading from CCS v11.0 to 2013-2 Product Update if you want to attach policy document to the published policies, for which no content is displayed in the Policy Central, unpublish such policies first and then re-publish them. However on re-publishing these policies, the actions history (accepted, declined, Comments, and so on) related to the policies would be lost.

- **Exceptions and Clarifications**
  You can click **Exceptions and Clarification** section to view exceptions, clarifications, and information on policy actions.

In the **Policy Central**, the policy audience can perform the following actions:

- Review the policy details and its related resources
- Search and Filter the policies
- Copy the policy URL
- Download policy documents
- Accept the policy
- Decline the policy
- Request clarification
- Request exception
- View exceptions and clarifications of the selected policy

Note: Administrator has the capability to control the operations performed on a policy by the policy audience so if some policy operations are not available, either the policy is read only or the Administrator has configured specific operations for the selected policies.

For information on configuring the Policy Central, see the *Configuring the Policy Central Settings* section in the *Symantec Control Compliance Suite User Guide*.

See "Launching the CCS Web Console and the Policy Central" on page 216.

Chapter 2

Planning for CCS deployment

This chapter includes the following topics:

- About FIPS compliance
- About external data integration
- About installing the CCS PowerShell snap-ins
- About internationalization and localization

About the CCS deployment

You can identify the deployment based on the following factors:

- Data collection solution that you use- raw-data based content, message based content or content from external data system
  See "Deployment based on the data collection solution" on page 34.
- Size of your organization- Small, medium, large
  See "Deployment based on the size" on page 35.
- Type of installation - first-time installation or upgrade from previous version
  See "Deployment based on the type of installation" on page 36.

Note: For example, you can choose a raw-data based data collection for a first-time installation of CCS for a large-sized organization.

Deployment based on the data collection solution

You must collect asset data from your enterprise network to achieve your business objectives using CCS. Following are the ways in which you can collect asset data from your enterprise network. You can decide the deployment based on the data collection solution that you choose to collect data for the assets.

The different solutions available for data collection are listed in the table below.

Table 2-1 Deployment based on the data collection solution

Use case	Description
Raw-data based	Raw-data based collection lets you collect asset data from your enterprise network. The collected data is then evaluated against a standard in CCS. You can collect raw-data using the agent-less method or the agent-based method. See "About raw-data collection" on page 98.

Table 2-1 Deployment based on the data collection solution *(continued)*

Use case	Description
Message based	Message based collection lets you collect and interpret asset data from your enterprise network before sending the data to CCS. The CCS Agent installed on each computer in the enterprise network performs the actual task of data collection and interpretation. The CCS Agent interprets the data against the standards or policies and presents the data to CCS in the form of messages. See "About message based data collection" on page 100.
External data integration	External data integration lets you seamlessly import data from an application that is external to CCS and represent the data in CCS as a data schema. The collected data is then evaluated against a standard in CCS. See "About external data integration" on page 112.

See "Deployment based on the size" on page 35.

See "Deployment based on the type of installation" on page 36.

Deployment based on the size

You can deploy the various components of CCS based on the size of your organization. The size of the organization is considered in terms of the number of assets in the organization on which the data collection, evaluation, and report generation tasks are performed

The different deployment scales are as follows:

- Deployment to monitor up to 1000 assets monthly
  See "Sizing requirements to monitor up to 1000 assets monthly" on page 73.
- Deployment to monitor up to 5000 assets monthly
  See "Sizing requirements to monitor up to 5000 assets monthly" on page 75.
- Deployment to monitor up to 10000 assets monthly
  See "Sizing requirements to monitor up to 10000 assets monthly" on page 77.
- Deployment to monitor up to 30000 assets monthly
  See "Sizing requirements to monitor up to 30000 assets monthly" on page 79.

- Deployment to monitor up to 100000 assets monthly
  See “Sizing requirements to monitor up to 100000 assets monthly” on page 81.

See “Deployment based on the data collection solution” on page 34.

See “Deployment based on the type of installation” on page 36.

Deployment based on the type of installation

After you review the data collection based deployment and the size of your organization, you can deploy CCS based on the type of installation.

Use the following table to identify your deployment based on the type of installation:

Table 2-2 Deployment based on the type of installation

Type of installation	Deployment model
First-time deployment	You can decide about the first-time deployment based on which operating system platforms you need to collect data from. For example, if you need to perform raw data collection only on Windows, SQL, Oracle, Cisco, or UNIX, you need to deploy only the CCS components. But, if you need to collect raw-data from VMware or Exchange you require additional RMS components. Similarly, if you need to collect message based data from platforms other than those directly supported by CCS components, you need to deploy additional ESM components. In this case the deployment becomes a hybrid deployment involving both CCS and RMS or CCS and ESM components. For information about raw data collection and respective components required: See “About raw-data collection” on page 98. For information about message based data collection and respective components required: See “About message based data collection” on page 100.
Upgrade	Upgrade to CCS 11.1 from the previous CCS deployment

See “Deployment based on the data collection solution” on page 34.

Hardware and operating system requirements

You must ensure that the computers that host the CCS infrastructure components meet the minimum requirements. These requirements are for a minimum system, and are sufficient only to run the components and experiment with a limited test environment. Before you plan your CCS deployment, review the component recommendations individually.

For a minimum system in a lab setting, you can install all components on one or two servers. If you do so, CCS performance diminishes. Any production CCS deployment should plan for separate servers for separate roles.

You can perform a fresh installation of the CCS Application Server version 11.1 only on a computer running a 64 bit operating system. However, you can upgrade an existing CCS Application Server installed on a computer running a 32 bit operating system, to CCS Application Server version 11.1. You can perform a standalone installation of the CCS Manager on computers running 32 bit or 64 bit operating systems.

CCS 11.1 supports upgrade from previous installations of CCS on computers running 32 bit or 64 bit operating systems.

In addition to these minimum requirements, each component has recommendations to ensure optimal performance. Some recommendations vary with the size of the deployment. In particular, multiple SQL Servers are normally used to host the databases.

These server requirements do not take into account the needs of the data collector deployments that collect data from the network.

The domain where you install the Application Server must be a Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, or a Windows Server 2012 R2 domain.

The functional level of the domain can be any of the following:

- Windows Server 2012
- Windows Server 2008 or later

If you install multiple CCS server components on a single host computer, the minimum disk space requirements are cumulative.

You can decide the model for deploying the various components of CCS based on the size of your organization. The size of the organization is considered in terms of the number of assets in the organization on which the data collection, evaluation, and report generation tasks are performed.

See "Deployment sizing" on page 72.

Note: Ensure that the computer on which you are installing the CCS Application Server does not have a hostname with non-ASCII characters. Also ensure that while performing data collection from target computers, the target computers do not contain hostnames with non-ASCII characters.

The following table contains the minimum requirements for each component.

Table 2-3 CCS server requirements

Component name	Hardware requirements	Required operating system	Software requirements
Application Server and Web Console server	■ Minimum memory: 4 GB ■ Minimum processor: 2.8 GHz ■ Minimum hard disk space: 20 GB	■ Windows Server 2008 SP2 x64 Enterprise or Standard edition ■ Windows Server 2008 R2 x64 Enterprise or Standard edition ■ Windows Server 2012 x64 Enterprise or Standard edition ■ Windows Server 2012 R2 x64 Enterprise or Standard edition **Note:** You can perform a fresh installation of the CCS Application Server version 11.1 only on a computer running a 64 bit operating system. However, you can upgrade an existing CCS Application Server installed on a computer running a 32 bit operating system, to CCS Application Server version 11.1.	■ Microsoft visual C++ 2010 redistributable framework. ■ Microsoft .NET 4.0 framework. ■ Microsoft .NET Framework 3.5 SP1. ■ ADAM SP1 / ADLDS. ■ Microsoft Core XML Service(MSXML) 6.0. ■ Symantec LiveUpdate Client ■ Internet Information Services (IIS) 6.0, 7.0 or 7.5. Static Content and Windows Authentication required for IIS 7.0 and above. If the computer that hosts the CCS Web Console server uses Windows Server 2008 or Windows Server 2012 the computer must have the **Windows Authentication** role added. For more information, See "Software requirements" on page 48.

Table 2-3 CCS server requirements *(continued)*

Component name	Hardware requirements	Required operating system	Software requirements
Production database or Reporting database	■ Minimum memory: 4 GB ■ Minimum processor: 2.8 GHz ■ Minimum hard disk space: 50 GB	■ Windows Server 2008 Enterprise or Standard edition ■ Windows Server 2008 x64 Enterprise or Standard edition ■ Windows Server 2008 SP2 Enterprise or Standard edition ■ Windows Server 2008 SP2 x64 Enterprise or Standard edition ■ Windows Server 2008 R2 x64 Enterprise or Standard edition ■ Windows Server 2012 x64 Enterprise or Standard edition ■ Windows Server 2012 R2 x64 Enterprise or Standard edition	■ Microsoft SQL Server 2008 SP1, SP2 ■ Microsoft SQL Server 2008 R2 ■ Microsoft SQL Server 2012 ■ Microsoft SQL Server 2014 CCS supports 32 bit and 64 bit versions of the SQL Server. These requirements are for a standalone database server. For more information, See "Software requirements" on page 48.
CCS Manager	■ Minimum memory: 2 GB ■ Minimum processor: 2.8 GHz ■ Minimum hard disk space: 20 GB	■ Windows Server 2008 Enterprise or Standard edition ■ Windows Server 2008 x64 Enterprise or Standard edition ■ Windows Server 2008 SP2 Enterprise or Standard edition ■ Windows Server 2008 SP2 x64 Enterprise or Standard edition ■ Windows Server 2008 R2 x64 Enterprise or Standard edition ■ Windows Server 2012 x64 Enterprise or Standard edition ■ Windows Server 2012 R2 x64 Enterprise or Standard edition **Note:** Windows Server 2003 is supported only if you are upgrading from an earlier version of CCS. Ensure that the computer on which you install the CCS Manager has the latest Windows Service Pack along with the latest updates. **Note:** CCS 11.1 does not support CCS Manager installation on the Windows Core operating system.	■ Microsoft visual C++ 2010 redistributable framework. ■ Microsoft .NET 4.0 framework. ■ Crystal Reports 2010 for CCS Manager in a reporting role. ■ SQL DMO 8.05.1054. ■ Oracle Instance Client 12.1 for collecting data from Oracle. ■ Microsoft Access Database Engine 2010. ■ Internet Information Services (IIS) 6.0, 7.0 or 7.5. Static Content and Windows Authentication required for IIS 7.0 and above. For more information, See "Software requirements" on page 48.

Table 2-3 CCS server requirements *(continued)*

Component name	Hardware requirements	Required operating system	Software requirements
CCS Agent	■ Minimum memory: 1 GB ■ Minimum processor: 1.33 GHz ■ Minimum hard disk space: 2 GB ■ Swap space: 1 GB	See "Supported target computers and databases for data collection" on page 48.	See "Software requirements" on page 48.
CCS Console	■ Minimum memory: 2 GB ■ Minimum processor: 2.8 GHz ■ Minimum hard disk space: 20 GB **Note:** The hardware requirements would differ if you are installing and launching the CCS Console as a standalone component on a separate computer.	■ Windows Vista Business or Enterprise ■ Windows Vista Business or Enterprise SP1 ■ Windows Vista Business or Enterprise SP2 ■ Windows Vista Business or Enterprise x64 ■ Windows Vista Business or Enterprise SP1 x64 ■ Windows Vista Business or Enterprise SP2 x64 ■ Windows 7 ■ Windows 7 x64 ■ Windows Server 2008 Enterprise or Standard edition ■ Windows Server 2008 x64 Enterprise or Standard edition ■ Windows Server 2008 SP2 Enterprise or Standard edition ■ Windows Server 2008 SP2 x64 Enterprise or Standard edition ■ Windows Server 2008 R2 x64 Enterprise or Standard edition ■ Windows Server 2012 x64 Enterprise or Standard edition ■ Windows Server 2012 R2 x64 Enterprise or Standard edition	■ Microsoft visual C++ 2010 redistributable framework. ■ Microsoft .NET 4.0 redistributable framework. See "Software requirements" on page 48.

If .NET is not installed, the Control Compliance Suite installer prompts you to install it.

Before you install the CCS components, you should run Windows Update to ensure that the latest Windows security updates are installed.

The computers that host the following components must be in the same LAN segment:

- CCS Application Server
- CCS Manager Load Balancer
- CCS Manager Evaluator
- CCS Manager Reporter
- CCS Production database
- CCS Reporting database

Microsoft Office and the Microsoft Office Primary Interop Assembly are required to import Microsoft Word documents as policies. You can use Microsoft Office XP, Microsoft Office 2003, or Microsoft Office 2007.

Note: Symantec recommends a minimum screen resolution of 800 x 600 for successful installation of the CCS components.

Network Ports

The Control Compliance Suite (CCS) 11.1 components use your existing TCP/IP network to communicate with each other. Based on your network configuration and on the location of your components, the communications may need to pass through a firewall. When the communications need to pass through a firewall, you must configure the firewall ports to allow components to access each other. You can configure the ports that each component uses if you choose.

Firewalls are often located between the CCS components and the Application Server. In addition, firewalls are found between the Application Server and the CCS Manager Load Balancers or Collectors.

The following table lists the ports used by CCS components to communicate with each other, and ports used by CCS for agent-less and agent-based data collection from target computers

Table 2-4 Ports used by CCS components

Component name	Requires to communicate with	Ports	Description
CCS Application Server	Symantec Directory Support Service	12467	Required by the Application Server to communicate with the Symantec Directory Support Service.
	Symantec Encryption Management Service	12468	Required by the Application Server to communicate with the Symantec Encryption Management Service
	LDAP	3890	Required by the CCS Console to connect to the Symantec ADAM/ADLDS instance.
	SSL	6360	Required by the Application Server for Secured Communication with the Directory Service.
	Integration services	12431 1431 / 80	Required by the Integration Services APIs.
	CCS Manager	5600 / 3993	Required by the Application Server to communicate with the CCS Manager.
	Microsoft SQL Server (Production database or reporting database)	1433	Required by the Application Server to communicate with the databases.
	CCS Assessment Manager (AM)	1977	Required by the Application Server to communicate with the CCS Assessment Manager (AM).
	Integration Services	12431	Required by the Integration Services.

Table 2-4 Ports used by CCS components *(continued)*

Component name	Requires to communicate with	Ports	Description
	Integration with AM	12432	Required by the Integration Services APIs for integration with the CCS Assessment Manager (AM).
CCS Console	Symantec Directory Support Service	12467	Required by the CCS Console to communicate with the Symantec Directory Support Service.
	Symantec Encryption Management Service	12468	Required by the CCS Console to communicate with the Symantec Encryption Management Service
	LDAP	3890	Required by the Application Server to connect to the Symantec ADAM/ADLDS instance.
	SSL	6360	Required by the CCS Console for Secured Communication with the Directory Service.
	Symantec Application Server Service	1431	Required by the CCS Console to communicate with the Application Server.

Table 2-4 Ports used by CCS components *(continued)*

Component name	Requires to communicate with	Ports	Description
CCS Manager	CCS Windows Agent	5601	Required by the CCS Manager to communicate with the CCS Agent.
	CCS UNIX Agent	5600	Required by the CCS Manager to communicate with the CCS Agent.
	CCS Agent-RMS UNIX Agent	1236	Required to upgrade the CCS RMS UNIX Agent.
	All CCS Agents	5599	Required to upgrade the CCS Agent. This port is also used while restarting the CCS Agent.
	RMS Information Server	3027 135 137 139	Required by the CCS Manager to communicate with the RMS Information Server.
	Microsoft SQL Server (Production database or reporting database)	1433	Required by the CCS Manager to communicate with the databases.
	Domain Controller for Collection/Target Domain CCS Windows Agentless Target	135 / 137 / 138 / 139 / 445 / 389	Need for cache building
	CCS Unix Agentless Target	22	Required to connect to Server target for data collection.
	CCS SQL Agentless Target (Default)	1433	
		1521	

Table 2-4 Ports used by CCS components *(continued)*

Component name	Requires to communicate with	Ports	Description
	CCS Oracle Agentless Target (Default)		
	CCS Cisco Agentless Target	22	
CCS Agent	CCS Manager	5600 / 3993 Default port is 5600.	If you have upgraded a Data Processing Service to CCS Manager, the CCS Manager continues to use the Data Processing Service port. If you are upgrading an ESM Manager to CCS Manager, the CCS Manager continues to use the ESM Manager port. **Note:** Do not use port 5601 for the CCS Manager. Port 5601 is required for the CCS Agent.
CCS Web Console	CCS Application Server	80 443	Required by the CCS Web Console to communicate with the Application Server.

Note: MS SQL connections are SSL encrypted only when the connections are configured for SSL encryption.

If the CCS infrastructure components must traverse a firewall to contact the Domain Controller, you must open additional ports for Windows authentication.

Table 2-5 Additional ports that must be open

Port	Protocol	Used by
123	TCP/UDP	Windows Time Service (W32Time)

Table 2-5 Additional ports that must be open *(continued)*

Port	Protocol	Used by
137 /138 /139	UDP	NetBIOS
389	TCP UDP	LDAP
636	TCP	LDAP SSL
88	TCP UDP	Kerberos
53	TCP UDP	DNS
135	TCP	RPC-EPMAP
137	UDP	NETBIOS Name Service
139	TCP	Netbios - ssn
145	UDP	UAAC Protocol
445	NP - TCP NP - UDP	SAM / LSA
3268	UDP	LDAP GC
3269	TCP	LDAP GC SSL
12467	TCP	CCS Directory Server
12468	TCP	CCS Encryption Management Service
1433	OLEDB SSL (TCP)	Microsoft SQL Server **Note:** MS SQL connections SSL encrypted only when configured.

For more information about the additional ports, see http://technet.microsoft.com/en-us/library/dd772723%28ws.10%29.aspx.

Note: You must use a port in the range from 1024 to 65535 for all other Control Compliance Suite 11.1 components.

Trust and delegation requirements:

- CCS requires Kerberos authentication to be enabled in your network environment.
- If the CCS Application Server and CCS Directory Server are on different computers you must configure delegation in order to impersonate the appropriate user.
  See "About delegation in Control Compliance Suite" on page 248.
- If the CCS Application Server and the CCS Console are in different forests, configure a forest level trust between the two forests.

Note: CCS Web Console works in a non trusted environment if the CCS Application Server and the CCS Directory Server are installed on a single computer.

The following ports must be open on the target computers to discover networks and assets.

Table 2-6 Ports used for network and asset discovery

Port	Protocol
1,2,3	UDP
21	TCP/FTP
22	TCP/SSH
23	TCP/Telnet
25	TCP/SMTP
80	TCP/HTTP
135	TCP
137	UDP - used by the NETBIOS Name Service
161	SNMP
443	TCP/HTTPS
445	TCP/SMB

Supported target computers and databases for data collection

CCS 11.1 supports raw-data or message based data collection from various operating system platforms and databases. For agent-based data collection you must install and configure the appropriate application modules on the CCS Agents

For information on supported target computers and databases for data collection, see the following link:

http://www.symantec.com/security_response/securityupdates/list.jsp?fid=ccs&pvid=sm

Software requirements

You must install/configure the following prerequisites before installing the CCS components:

Table 2-7 Prerequisites required to install CCS

Prerequisite	Description
SQL Server	The following versions of SQL Server are supported: ■ Microsoft SQL Server 2008 SP1, SP2 (supported for both 32-bit and 64-bit computers) ■ Microsoft SQL Server 2008 R2 (supported for both 32-bit and 64-bit computers) ■ Microsoft SQL Server 2012 (supported for both 32-bit and 64-bit computers) ■ Microsoft SQL Server 2014 (supported for both 32-bit and 64-bit computers) **Note:** Microsoft SQL Server 2005 is supported only if you are upgrading from an earlier version of CCS. You must manually install the software or use an existing installation. CCS creates a production database and a reporting database to store the compliance data. Depending on the scale of the deployment, you might require one or more Microsoft SQL Server installations. It is recommended that the Application Server should be configured to use the SSL connections for the Microsoft SQL Server instances that host the CCS databases. If you use SSL connections, you must ensure that you configure them before you install CCS. Refer to the Microsoft SQL Server documentation (http://support.microsoft.com/kb/316898) for information about configuring SSL connections. These requirements are for a standalone database server.

Table 2-7 Prerequisites required to install CCS *(continued)*

Prerequisite	Description
Microsoft .Net Framework 3.5 SP1	To install .Net 3.5 SP1 on Windows Server 2008, in the **Prerequisites** panel of the CCS Setup, expand Microsoft .Net Framework 3.5 SP1 and check **Install**. To install .Net 3.5 SP1 on Windows Server 2008 R2, in the Windows Server 2008 Server Manager, go to **Features > Add new Feature**. Select **.Net Framework 3.5.1 features** and click **Next** to complete the installation.
Oracle Instant Client 12.1	If you are collecting data from the Oracle platform, you require the Oracle Instant Client 12.1 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. To install the Oracle Instant Client 12.1, locate the Oracle Instant Client version 12.1 files on the Oracle product support website and download the Instant Client Package - Basic package. Unzip the contents of the package to a directory at a known location, and add the directory path to the PATH environment variable at system level. Oracle Instant Client 12.1 is not installed by default while installing CCS. You can install Oracle Instant Client 12.1 before or after you install CCS. See "Installing the Oracle Instant Client for data collection on Oracle" on page 182.
Internet connection for CCS service	CCS services require access to certificate revocation list (CRL) published by verisign at location http://crl.verisign.com in order to validate the digital signatures of the assembly. This ensures security by verifying that the certificates with which the assemblies are signed are not in the revocation list. Symantec recommends that you enable the Internet connection on the computers where the CCS Application Server or CCS Console is installed. CCS Manager does not require internet access.
Java Runtime Environment (JRE) 1.7_03 or later	If you are upgrading the ESM Console and ESM Utilities to version 11.1, you require JRE 1.7_03 or later to run the ESM Console and ESM Utilities.

Table 2-8 Prerequisites required to use the CCS Web Console and the Policy Central

Configuration	Description
Browsers	Symantec has verified the functioning of the CCS Web Console and the Policy Central on the following versions of specified Web browsers: ■ Internet Explorer version 11.0 The following patches need to be applied in case you are using IE 10 or IE 11: ■ Internet Explorer version 10.0 http://support.microsoft.com/kb/2600217 ■ Internet Explorer version 11.0 http://support.microsoft.com/kb/2836939 ■ Mozilla Firefox version 30.0 (only on Windows) ■ Google Chrome version 35.0 (only on Windows) ■ Safari version 7.0 (only on the Macintosh) Perform the following browser specific configurations on the computer from which you are accessing the CCS Web Console or the Policy Central. If you are using the Internet Explorer browser: ■ Add the FQDN of the CCS Application Server to Trusted sites. ■ Enable the Windows Integrated Authentication. ■ Logon automatically with the current username and password or logon automatically only in the intranet zone. ■ Enable the Active Scripting setting for JavaScript execution ■ Go to **Tools > Compatibility View Settings** and uncheck the option **Display intranet sites in Compatibility View**. If you are using the Mozilla Firefox browser: ■ Open Firefox, and in the address bar, type `about:config`. ■ In the Search bar, type `network.negotiate` to filter the list. ■ Double-click `network.negotiate-auth.delegation-uris`, and add the FQDN of the CCS Application Server in the dialog box. ■ Double-click `network.negotiate-auth.trusted-uris`, and add the FQDN of the CCS Application Server in the dialog box. If you are using the Google Chrome browser: ■ In the Settings, click Show Advanced Settings.... and under Network, click **Change proxy settings...**. Add the FQDN of the CCS Application Server to Local Intranet.
Screen resolution	Symantec recommends a screen resolution with an aspect ratio of 1280 x 1024 to view the CCS Web Console.

Table 2-8 Prerequisites required to use the CCS Web Console and the Policy Central *(continued)*

Configuration	Description
Internet Information Service (IIS)	For the CCS Application Server installed on Windows Server 2008 or Windows Server 2012, ensure that you use Windows Authentication and Static Content. If there is no Windows authentication on the server, then you can add it through the **Add Role Services** dialog box for Web Server (IIS), in Server Manager. CCS Web Console works using both HTTP or HTTPS protocol. If you want to use HTTPS protocol, ensure that you have enabled HTTPS protocol on the computer on which CCS Web Console is installed. If not, then refer to the support website for Microsoft to install HTTPS. You require the following MIME types for the CCS Web Console: .js .css .htm .html .exe .deploy

Table 2-8 Prerequisites required to use the CCS Web Console and the Policy Central *(continued)*

Configuration	Description
Service Principal Name (SPN)	You must setup Service Principal Names' (SPN) after installing CCS 11.1 or upgrading to CCS 11.1. CCS 11.1 provides a batch file containing the SPN setup script. The SPN script file contains the set SPN commands to set the required SPNs for the CCS components. Provide the script file to the domain administrator to create the Service Principal Names. You can export the batch file from the CCS Suite installer after installing the Application Server, or by using the VerifyDelegation utility located inside the <Install_Directory>\Application Server folder Set up an SPN with the NetBIOS name and the fully qualified domain name (FQDN) of the domain user account in whose context the application pool executes. SPN can be set up from the Application Server or the DC. Execute the following commands on the CCS Application Server where IIS 6 or IIS 7 is used. For IIS 7, you must execute these commands only 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. By default, the Kernel Mode Authentication is enabled. ■ `SetSpn.exe -a http/Application_Server_computer's_NetBIOS_name DomainName\UserName` ■ `SetSpn.exe -a http/Application_Server_computer's_FQDN DomainName\UserName` The setspn is a command-line utility. **Note:** You can associate an SPN with a single user account. Do the following on the Windows Server computers to enable delegation for the Application Server's service account.: ■ In the user properties, go to the **Delegation** tab, and select the option **Trust this Computer for delegation to any service (Kerberos only)**.

Table 2-8 Prerequisites required to use the CCS Web Console and the Policy Central *(continued)*

Configuration	Description
ASP.NET v4.0.30319	Perform respective tasks to install the application on the CCS Application Server that is installed on Windows Server 2008 or Windows Server 2012. ■ Windows Server 2008 The command to install the application is as follows: `%systemroot%\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe -I -enable` ■ Windows Server 2012 To set up the Server Roles to install the application on the CCS Application Server, See "Configuring Server Roles to install the prerequisites manually on the CCS Application Server " on page 155.
ASP.NET v4.0.30319 Web Service Extensions	On the CCS Application Server computer, in the IIS Manager, you must set the value as Allowed for the ASP.NET v4.0.30319 Web Service Extensions. If ASP.NET v4.0.30319 is not present on the computer, the CCS setup installs the ASP.NET v4.0.30319. You can perform this procedure once the CCS setup installs the prerequisites and displays the **Welcome** panel. To set the value on Windows Server 2008 and Windows Server 2012, in the Internet Information Services (IIS) Manager, in the **Connections** Pane, click the server node in the tree. On the server home page, under IIS, double-click **ISAPI and CGI Restrictions**. Right-click **ASP.NET v4.0.30319** and click **Allow**. To set the value on Windows Server 2003, in the Internet Information Services (IIS) Manager, in the left Pane, click the server node in the tree, and then click Web Service Extensions. On the Web Service Extensions page, select**ASP.NET v4.0.30319** and click **Allow**.
HTTP Activation for .NET Framework 4.5	To launch Policy Central on a Windows 2012 computer, HTTP must be activated for .NET Framework 4.5. In the Server Manager, under Roles and Features, navigate to ASP under Webserver(IIS) > Web Server > Application Development and select **HTTP Activation** under WCF Services.
Full-Text Search on SQL Server	Policy Central uses the Full-Text Search feature of the SQL Server to search in policy documents.

The CCS setup installs the following prerequisites automatically during the UI based installation:

Note: You must install all prerequisites manually if you are performing a silent installation of the CCS components. CCS setup does not install any prerequisites automatically during the silent installation.

Table 2-9 Prerequisites installed automatically during CCS installation

Configuration	Description
Microsoft .NET 4.0 framework	Installs automatically.
Microsoft Visual C++ 2010 redistributable framework	Installs automatically.
Microsoft installer 4.5	Installs automatically.
Microsoft Access Database Engine 2010	Installs automatically.
SQL Database Management Objects (SQL-DMO) 8.05.1054	Installs automatically. CCS supports only version 8.05.1054 of the SQL-DMO for data collection. You must have the correct SQL DMO version on the CCS Manager computers for agent-less data collection and CCS Agent computers for agent-based data collection. If the SQL-DMO version is other than version 8.05.1054, you may experience problems in data collection. For example, the Members field in the server login datastore may show value as “UNKNOWN”. The SQL DMO version 8.05.1054 files for 32 bit and 64 bit operating systems are located in the `Redist` folder of the product media. The filenames are `SQLServer2005_BC` and `SqlServer2005_BC_x64`.
Crystal Reports 2010	Installs automatically during the CCS Suite installation. You must install Crystal Reports 2010 on the CCS Manager computer that is configured with the Reporter role. To install Crystal Reports 2010 manually, in the **Prerequisites** panel of the CCS Setup, expand Crystal Reports and check **Install**. You can also install Crystal Reports 2010 using the CrystalReportsDotNet.MSI file from the <installation directory>/Symantec/CCS/Reporting and Analytics/WebPortal/Console/Redist folder of the CCS Application Server or you can install CrystalReportsDotNet.MSI from the Redist folder of the product media

Table 2-9 Prerequisites installed automatically during CCS installation *(continued)*

Configuration	Description
Crystal Reports 2010 hot fix	Installs automatically during the CCS Suite installation. If the hot fix fails to install automatically, you must install the hot fix manually. For example, while installing CCS on Windows Server x64, incase of hot fix installation failure, the **Warning** panel of the CCS Setup displays the following error message: `Access to the path C:\Program Files (x86)\SAP BusinessObjects\Crystal Reports for .NET Framework 4.0\Common\SAP BusinessObjects Enterprise XI 4.0\win64_x64.` To install the hot fix manually on Windows Server x64, extract the `secSSOwin64_x64` file located in the `Redist` folder of the product media, to the location C:\Program Files (x86)\SAP BusinessObjects\Crystal Reports for .NET Framework 4.0\Common\SAP BusinessObjects Enterprise XI 4.0\win64_x64\. Extract the `secSSOwin32_x86` file located in the `Redist` folder of the product media, to the location C:\Program Files (x86)\SAP BusinessObjects\Crystal Reports for .NET Framework 4.0\Common\SAP BusinessObjects Enterprise XI 4.0\win32_x86\ To install the hot fix manually on Windows Server x86, extract the `secSSOwin32_x86` file located in the `Redist` folder of the product media, to the location C:\Program Files (x86)\SAP BusinessObjects\Crystal Reports for .NET Framework 4.0\Common\SAP BusinessObjects Enterprise XI 4.0\win32_x86\
ADAM SP1 instance	Installs automatically.
Symantec LiveUpdate Client	Installs automatically.
Symantec Help	Installs automatically.

User Privileges for deploying the CCS components

The CCS infrastructure supports multiple deployments of the product components. Every component such as the CCS Application Server, the CCS Manager and the CCS Agent comprises of the services that are a part of the deploying component. To install the components successfully, you require specific permissions and privileges. Besides, you must also configure the user accounts with specific privileges to run the services that are a part of the components. The user in which context the product component is installed need not necessarily be a regular user of the component. Sometimes, the user might need to have higher permissions and privileges than the regular user.

Table 2-10 Lists the user privileges to deploy the CCS components

Deployment task	Description	User privileges required
Install CCS Application Server	The following components are installed for the CCS Application Server: ■ Application Server ■ CCS Console ■ CCS Web Console ■ Databases	You must have all the following user privileges to install the component: ■ Domain user ■ Local administrator The users in whose context the Directory Service and the Application Server Service are run on the computer must have the following user privileges: ■ Domain user Refer to the User privileges on SQL server if no existing databases are used topic for more information. See Table 2-12 on page 62. Refer to the User privileges on SQL server for using existing databases topic for more information. See Table 2-13 on page 62.
Install CCS Manager	Installs the CCS Manager.	You must have all the following user privileges to install the component: ■ Local or domain user ■ Local administrator
Install CCS Agent	Installs the CCS Agent	You must have all the following user privileges to install the component: ■ Local or domain user ■ Local administrator

Table 2-10 Lists the user privileges to deploy the CCS components *(continued)*

Deployment task	Description	User privileges required
Install CCS Content	Installs additional CCS content	You must have all the following user privileges to install additional CCS content: ■ CCS administrator ■ Local administrator
Configure Service Principal Name (SPN) configuration	Sets the required SPNs for the CCS components.	You must have the following user privileges to set the SPNs: ■ Domain administrator
Create certificates	Creates certificates for installing standalone CCS Managers	You must have the following user privileges to create certificates: ■ CCS administrator ■ Local administrator
Add / Upgrade CCS components	Adds / upgrades components to an existing CCS installation	You must have all the following user privileges to add / upgrade the CCS components: ■ CCS administrator ■ Local administrator ■ Domain user
Repair CCS components	Repairs an existing CCS installation	You must have all the following user privileges to repair the CCS components: ■ CCS administrator ■ Local administrator If you are not the Application Server Service account user and you are using Windows authentication, for repairing the CCS Application Server you require the following user privileges on the SQL Server ■ db_owner, and Control permission through the securables option.

Table 2-10 Lists the user privileges to deploy the CCS components *(continued)*

Deployment task	Description	User privileges required
Uninstall CCS Components	Uninstalls all or specific CCS components	You must have all the following user privileges to uninstall the CCS components: ■ CCS administrator ■ Local administrator **Note:** CCS Administrator privileges not required if you are uninstalling all CCS components. If you are not the Application Server Service account user and you are using Windows authentication, for uninstalling the CCS Application Server you require the following user privileges on the SQL Server ■ sysadmin
Upgrade CCS Application Server and CCS Directory Server	Upgrades the CCS Application Server and CCS Directory Server from an earlier version to CCS 11.1.	You must have all the following user privileges to upgrade the CCS Application Server and CCS Directory Server from an earlier version to CCS 11.1: ■ CCS administrator ■ Local administrator ■ Domain user For privileges required on the SQL Server, See "User privileges for SQL server and CCS databases" on page 60.

Table 2-11 Lists the user privileges for the CCS services

CCS service	CCS service name	User privileges required
Directory Service	Symantec Directory Support Service	You must have the following user privileges for the service: ■ Domain user **Note:** The user must have the Local administrator privileges.
Encryption Management Service	Symantec Encryption Management Service	You must have the following user privileges for the service: ■ Domain user **Note:** The user must have the Local administrator privileges.
Application Server Service	Symantec Application Server Service	You must have all the following user privileges for the service: ■ Domain user **Note:** The user must have the Local administrator privileges. You require db_owner rights if you are using Windows authentication to connect to the SQL Server for creating the CCS databases. Refer to the User privileges on SQL server if no existing databases are used topic for more information. See Table 2-12 on page 62. Refer to the User privileges on SQL server for using existing databases topic for more information. See Table 2-13 on page 62.

Table 2-11 Lists the user privileges for the CCS services *(continued)*

CCS service	CCS service name	User privileges required
CCS Manager in the reporting role	Symantec Data Processing Service for the reporting role	You must have all the following user privileges for the service: ■ db_owner on CSM_Reports database ■ Logon locally for the service account of the Application Server on the CCS Manager computer
CCS Manager in the data evaluator	Symantec Data Processing Service for the data evaluation	You must have all the following user privileges for the service: ■ Logon locally for the service account of the Application Server on the CCS Manager computer
CCS Manager in other roles	Symantec Data Processing Service for roles of a load balancer or data collector	No additional permission are required.
CCS Manager in the external data connector role	Symantec Data Processing Service for the role of an external data connector	You must have all the following user privileges for the service: ■ db_owner on CSM_Reports database ■ Logon locally for the service account of the Application Server on the CCS Manager computer
CCS Agent	Symantec CCS Agent	You must have the following user privileges for the service: ■ Local administrator

User privileges for SQL server and CCS databases

The CCS infrastructure uses two SQL Server databases CSM_DB and CSM_Reports. These databases are known as production database and reporting

database respectively. These databases are created during the installation of the CCS Application Server. The SQL Server instance can be located on the same computer as the CCS Application Server or on a separate computer. The databases are case sensitive and hence you must ensure that you have the correct database names.

If you use the Windows authentication mode, then the credentials of the user who installs the CCS Application Server is used to connect to the SQL Server. The credentials of the user in whose context the Application Server Service is installed are used in the post-installation.

Note: If you use the Windows authentication mode for accessing the CCS database, the SQL Server service account must be a NETWORK SERVICE account or a domain user account. If the SQL Server service account is other than a NETWORK SERVICE account or a domain user account, you must set the Service Principal Name (SPN) on the SQL Server service account for authentication of the CCS Application Server service account

---

If you use the SQL authentication mode, then the credentials of the SQL user is used to connect to the SQL Server during the CCS Application Server installation.

The user privileges on the SQL server varies for the CCS Application Server component installation based on whether you use an existing database or not. You can create the two databases prior to installing the product components.

See “Installing the CCS Suite” on page 140.

These user privileges also depend whether the SQL server is in the Windows authentication mode or the SQL authentication mode.

The user privileges on the SQL server when no existing databases are created for the Application Server component installation are as follows:

Table 2-12 User privileges on SQL server if no existing databases are used

User context	Privileges for Windows authentication mode	Privileges for SQL authentication mode
Install user	You must have sysadmin rights on the SQL server during the installation. After the successful installation of the component, you can change the database rights to db_owner.	The SQL account specified during installation must have sysadmin rights. After the successful installation of the component, you can change the database rights to db_owner.
Application Server Service user	You must have db_owner rights on the SQL server during the installation.	You do not require specific privileges if you are using SQL authentication.

Table 2-13 User privileges on SQL server for using the existing databases

User context	Privileges for Windows authentication mode	Privileges for SQL authentication mode
Install user	When the user context for the installation of the Application Server component and Application Server Service are same. Do the following: ■ Create the empty databases for CSM_DB and CSM_Reports. ■ Assign the db_owner rights to the user in whose context the component is installed.	Do the following: ■ Create the empty databases for CSM_DB and CSM_Reports. ■ Specify a user who has the db_owner rights.

Table 2-13 User privileges on SQL server for using the existing databases *(continued)*

User context	Privileges for Windows authentication mode	Privileges for SQL authentication mode
Application Server Service user	When the user context for the installation of the Application Server component and Application Server Service are different Do the following: ■ Create the empty databases for CSM_DB and CSM_Reports. ■ Assign the db_owner rights to both users. You must add the user in whose context the service is executed to the user in whose context the component is installed. You also must assign the following permissions to the added user through the securables option: ■ Control	Do the following: ■ Create the empty databases for CSM_DB and CSM_Reports. ■ Specify a user who has the db_owner rights.

Note: If you have installed CCS databases on SQL Server 2012 and use Windows authentication, NT ATHORITY\SYSTEM must have db_owner permissions on CSM_DB and CSM_Reports databases.

Configuring credentials for asset import and data collection

You can configure credentials for various platforms to achieve the following:

- Asset Import
- Data Collection

Note: You must configure Windows Domain Cache credentials, if your asset is a part of Windows domain. For Windows Domain Cache credentials, domain name should be net bios name of the domain, else cache will not be built and data collection will not proceed.

See "Frequently asked questions about Windows domain cache credentials" on page 67.

The credentials required for asset import are as follows:

Table 2-14 Credentials required for asset import

Asset type	Scoped to	Credentials required
Windows assets Windows File, Windows Directory, Windows Share, Windows Group, IIS Virtual Directory, IIS Web Sites	Windows Machine	You must configure Windows common or Windows asset credentials first. Next, configure Windows Domain Cache credentials.
SQL Server	Windows Machine	You must configure Windows Domain Cache credentials first. Next, configure SQL common credentials. **Note:** User associated with specified credential should be able to login to SQL Server in Windows Authentication mode.
SQL Database	Windows Machine	You must configure Windows Domain Cache credentials. Next, configure SQL common and SQL asset credentials.
Oracle Configured Database	Windows Machine	You must configure Windows common or Windows asset credentials.
Oracle Configured Database	UNIX Machine	You must configure UNIX common or UNIX asset credentials. The following both credentials are required for UNIX platform: ■ Connection credentials ■ Data Collection credentials

Table 2-14 Credentials required for asset import *(continued)*

Asset type	Scoped to	Credentials required
UNIX File, UNIX Group	UNIX Machine	You must configure UNIX common or UNIX asset credentials. The following both credentials are required for UNIX platform: ■ Connection credentials ■ Data Collection credentials
Cisco Routers	Cisco IOS Router	You must configure Cisco common or Cisco asset credentials.

The credentials required for data collection are as follows:

Table 2-15 Credentials required for data collection

Platform type	Credentials required
Windows	You must configure Windows common or Windows asset credentials first. Next, configure Windows Domain Cache credentials.
SQL Server	You must configure Windows common or Windows asset and Windows Domain Cache credentials first. Next, configure SQL common or SQL asset credentials. **Note:** For reporting on SQL servers, you may also require Windows platform credentials as applicable. For instance, if you want to report on SQL server file permissions, you will require Windows platform credentials.
Oracle Database on Windows	You must configure Windows common, or Windows asset and Windows Domain Cache credentials first. Next, configure Oracle common or Oracle asset credentials. **Note:** For reporting on Oracle Databases, you may also require Windows platform credentials as applicable. For instance, if you want to report on Oracle file permissions, you will require Windows platform credentials.

Table 2-15 Credentials required for data collection *(continued)*

Platform type	Credentials required
Oracle Database on UNIX	You must configure UNIX common or UNIX asset credentials. The following both credentials are required for UNIX platform: ■ Connection credentials ■ Data Collection credentials **Note:** For reporting on Oracle Databases, you may also require UNIX platform credentials as applicable. For instance, if you want to report on Oracle file permissions, you will require UNIX platform credentials.
UNIX	You must configure UNIX common or UNIX asset credentials. The following both credentials are required for UNIX platform: ■ Connection credentials ■ Data Collection credentials
Cisco Routers	You must configure Cisco common or Cisco asset credentials.

Note: For the data collection job, the CCS Application Server passes on the credentials to the CCS Manager in an encrypted form. Encryption is done using the particular CCS Manager's certificate. Therefore, if the data collection job is sent to any other CCS Manager than the one for which the encryption is done using the certificate, the job will not get executed because the credentials will not get decrypted. The CCS Manager then performs data collection for that job, without storing the credentials locally.

For agent-less asset import and data collection mode, you can manage credentials centrally.

For agent-based asset import and data collection mode, you can manage credentials locally on the agents.

CCS requires certain minimum privileges in order to query target computers for data collection.

Privileges for Windows

To query targets on Windows, CCS requires local administrator privileges on target computers for some Windows APIs which are built into the product.

For information on minimum required privileges to query Windows targets, see http://www.symantec.com/docs/HOWTO83950

Privileges for SQL

To query targets on SQL, CCS requires the following kinds of privileges:

- Privileges to import SQL server assets into CCS
- Common privileges to query all data sources
- Privileges to collect data from specific data sources

For information on minimum required privileges to query an SQL Server database, see http://www.symantec.com/docs/HOWTO83942

Privileges for Oracle

To query targets on Oracle, CCS requires the following kinds of privileges:

- Privileges for database-related queries
- Privileges for platform-specific queries
- Privileges on views to query database-related data sources

Though CCS requires only minimum privileges for data collection, in some cases you may require to query targets using higher privileges. The Sudo functionality permits you to execute a command on the target computer, as a super user, or another user. For agent-less raw data collection on Oracle UNIX targets, you can use the Oracle sudo (superuser do) functionality to run queries in the context of a super user.

For information on minimum required privileges to query an Oracle database, see http://www.symantec.com/docs/HOWTO83943

Privileges for UNIX

To query or perform data collection on UNIX computers, ensure that root has sufficient privileges to access the home directory of the data collection user. This privilege is independent of the user profile existing on the NFS mount or the local computer.

Frequently asked questions about Windows domain cache credentials

This section provides functional information on Windows domain cache credentials which lets you address all your queries on using Windows domain cache credentials.

Table 2-16 Windows Domain Cache Credentials - FAQ

Query	Resolution
What is domain cache and why is domain cache required?	Domain cache is a Microsoft Access database file which contains information about users, groups, computers, and miscellaneous objects that are required during data collection. This cache is required to optimize data collection job and does not affect the domain controller for data per job.
Was the domain cache built-in legacy RMS system?	Yes. The Windows domain cache was built-in RMS as well and was built on the Master Query Engine.
What are contents of domain cache?	Cache contains users, groups, computer information, and miscellaneous objects that are required during data collection.
Is the entire Active Directory replicated into the Windows cache?	The data, which CCS requires during data collection, is cached. Entire Active Directory is not cached. The cache also gets updated if there is any change in AD for the data which is cached.
Where do you provide domain cache credentials in CCS Reporting & Analytics?	You can provide Windows domain cache credentials by navigating to the **Settings** menu. Go to **Credentials** view > **Add Common Credentials** tab and Select **Windows Domain Cache** as the **Platform type**.
For parent-child domain, do we need to specify credential for each domain or only for the parent domain?	Cache is built per domain. Hence, we need to provide credentials per domain.
Where is the cache stored?	The cache is stored on the CCSM in the folder at <InstallDir> /DPS/ Control/ Windows/ Cache.
How is this Windows domain cache secured?	Windows domain cache is a password-protected Microsoft Access database file.
How does CCS use the Windows domain cache credential to build the domain cache?	Domain cache is built internally during data collection. Using the domain cache credentials, CCS Manager (CCSM) connects to the domain controller (AD) and fetches the required information to build and update the cache.
Which data sources refer to data from the Windows domain cache?	Any entity or any data source that fetches data from the host Windows computer refers to Windows domain cache. Thus, all Windows platform entities or data source refer to cache. SQL and Oracle entities, or data sources, which need to fetch data from the host Windows computers, also refer to Windows domain cache.

Table 2-16 Windows Domain Cache Credentials - FAQ *(continued)*

Query	Resolution
What is the format of credentials which need to be provided for Windows domain cache credentials?	Domain name field : Value should be in NetBIOS format for the domain name. Username field: domain name\username Or username@domain name fqdn Password field: <password>
What are the minimum privileges that are required for the account to create domain cache?	At present the requirement is confined to Windows domain user credentials. The minimum privileges that are required for the account to create domain cache are available with latest Security Content Updates.
Do I need to restart CCSM service after providing domain cache credentials?	Symantec recommends that you restart CCSM service after you reset credentials.
Do we need to provide Windows domain cache credentials even if we perform data collection using RMS?	Credentials in CCS R&A are required only during data collection through new simplified architecture by the way of CCSM.
What protocol does CCS use to build the domain cache? Any firewall port needs to be opened between the domain controller and the CCS server?	Cache is built using MS RPC protocol and needs RPC ports open. The mechanism is same as what CCS needs for Windows data collection.
Is the cache created or required in agent-based mode of data collection?	Cache is required for both agent based and agent less mode of data collection. The cache is always created and updated on the CCSM. This cache is pushed to the agent when the agent has an outdated copy of the cache.
Is the entire cache pushed to the agent based during data collection?	The entire cache is pushed to the agent up to the cache size threshold limit. If the cache size has crossed the threshold limit, then only cache difference (delta) is sent to the agent. The cache threshold limit can be managed using Windows platform settings page by navigating to **Settings** > **System Topology** > **Map View** > **Common Tasks** > **Configure Platform Settings** > **Windows**.

Table 2-16 Windows Domain Cache Credentials - FAQ *(continued)*

Query	Resolution
Can Windows domain cache building be optional?	No.
Is there a separate job to create the domain cache?	CCS does not provide a separate job to create the domain cache. The domain cache is created during data collection if the cache file is not present on the CCSM.
Is there a separate job to update the domain cache?	CCS does not provide a separate job to update the domain cache. The domain cache is updated during data collection if the cache on the CCSM is out of date.
What is the refresh interval for domain cache?	Refresh interval is the period between two subsequent cache refreshes. By default, the cache refresh interval is 72 hrs. The refresh interval can be managed updating the cache refresh interval using Windows platform for a particular site using platform settings page by navigating to **Settings** > **System Topology** > **Grid View** > **Common Tasks** > **Configure Platform Settings** > **Windows**.

How to specify the cache build failure retry interval?	Cache build failure retry interval is the period between two subsequent retries to refresh the cache, if a cache refresh fails. Specifying an appropriate cache build retry interval ensures that jobs do not remain in executing state for a long time if cache building fails.
	The default cache build failure retry interval is 30 minutes.
	To specify a custom cache build retry interval, add the following information in the ConfigurationSettings.xml file located at <CCS_install_directory>\DPS\control\Windows.
	`<PlatformSetting>`
	`<Key>CacheFailureRetryInterval</Key>`
	`<Value><![CDATA[30]]></Value>`
	`</PlatformSetting>`

What is the lowest value that can be set for domain cache refresh interval?	You can set the lowest value for domain cache refresh interval to 5 hrs.
Why do we need the setting, Last logon interval?	Last Logon Interval is required for updating the user last logon field in the cache file.

Table 2-16 Windows Domain Cache Credentials - FAQ *(continued)*

Query	Resolution
Is the Windows domain cache built for workgroup computer assets?	Windows domain cache is required only for domain member server targets or assets. Since workgroup assets do not belong to a domain, Windows cache is not built for workgroup computer assets.
Why does the Data collection job show an error for not able to build the cache nevertheless the data collection job completes successfully?	These warning messages are shown for trusted domain for which the cache cannot be built. It is optional and hence the data collection job gets successfully completed. Symantec recommends that you provide domain cache credentials for the trusted domains also so that the cache for the same can be built and the data collection results can be accurate.
What if the cache file gets deleted accidentally?	Restart the CCSM service on the computer where the cache was stored. Next run of data collection job builds the cache again.
What if Windows domain cache is unable to build on workgroup CCSM?	CCSM manager requires minimum one-way trust between the CCSM and the domain for which it creates the cache. Hence, CCSM cannot build cache for a not trusted domain or if CCSM is on a workgroup.
Is the cache synchronized between all CCSM?	The CCSM, that gets the data collection job automatically, refreshes the cache for itself and no synchronization is required between CCSM.
Why do we need domain cache for trusted domains?	If you have domains having a trust relationship between each other, and users of either domains are members of groups in either domain, for example, for trusted domains A and B, domain A users are member of a group in domain B and vice versa. In order to perform data collection on assets in a domain whose users are members of the other domain, the trusted domains are required to be cached. For CCS to build the domain cache for the trusted domain, you need to configure the cache credentials for that trusted domain.

Table 2-16 Windows Domain Cache Credentials - FAQ *(continued)*

Query	Resolution

How to specify a particular domain controller to be used for cache building?	To specify a domain controller, add the following information in the ConfigurationSettings.xml file located at <CCS_install_directory>\DPS\control\Windows.
	
	`<PlatformSetting>`
	`<Key>DCForCacheToUse</Key>`
	`<Value><![CDATA[DomainName:DomainControllerName;`
	`Domain1:DomianController1]]></Value>`
	`</PlatformSetting>`
	
	You must specify only one domain controller for a domain. You can provide either the hostname, IP Address or FQDN of the domain controller. Ensure that the domain controller you provide is getting resolved from the CCS Manager computer.
	
	If the domain controller specified in the ConfigurationSettings.xml file is not reachable, then CCS uses any other available domain controller on the network , to build or refresh the cache.

Performance and scalability

This section includes the following topics:

- See “Deployment sizing” on page 72.
- See “Database recommendations” on page 83.
- See “Recommendations for data evaluation” on page 89.
- See “Modifying the CCS Manager configuration settings for collecting raw-data using agent-less method” on page 89.
- See “Modifying the CCS Manager configuration settings for message based data collection” on page 92.
- See “Modifying the CCS Manager page file size” on page 94.
- See “ Virtualization” on page 96.

Deployment sizing

CCS provides flexible way to scale the operations. Organizations can deploy CCS infrastructure based on the expected load, utilization and availability requirements.

As business needs evolve, the environment can adapt and scale to meet the new demands. This section on deployment guide provides detailed information for designing and configuring a CCS for various loads. This guide can be scaled up for larger deployments by increasing the number of servers and storage needed. Please note that all the below recommendations are predominantly applicable to windows Targets environment.

- Deployment to monitor up to 1000 assets monthly
  See "Sizing requirements to monitor up to 1000 assets monthly" on page 73.
- Deployment to monitor up to 5000 assets monthly
  See "Sizing requirements to monitor up to 5000 assets monthly" on page 75.
- Deployment to monitor up to 10000 assets monthly
  See "Sizing requirements to monitor up to 10000 assets monthly" on page 77.
- Deployment to monitor up to 30000 assets monthly
  See "Sizing requirements to monitor up to 30000 assets monthly" on page 79.
- Deployment to monitor up to 100000 assets monthly
  See "Sizing requirements to monitor up to 100000 assets monthly" on page 81.

Sizing requirements to monitor up to 1000 assets monthly

This section recommends the hardware, software, and job sizing requirements that are required for CCS to monitor up to 1000 assets monthly.

Table 2-17 Requirements and recommendations

Requirements	Recommendations
Hardware	Following are the hardware recommendations: ■ 1 server to host the CCS Application Server, and CCS Manager in all roles except the Collector role. ■ 1 SQL server to host production database and reporting database. ■ In case of agent-less data collection, 1 server to host the CCS Manager in Collector role. ■ In case of agent-based raw-data collection, 1 server to host the CCS Manager in Collector role. ■ In case of message based data collection, 1 server to host the CCS Manager in Collector role. For information on Hardware configurations for CCS servers, See Table 2-18 on page 74.

Table 2-17 Requirements and recommendations *(continued)*

Requirements	Recommendations
Software	Following are the software recommendations: ■ 64-bit operating system should be deployed on the servers. Recommended operating system is Windows Server 2008 R2 with latest service pack and latest windows updates. ■ The SQL server hosting the production and reporting database should be of 64-bit.
Job sizing	Following is the job sizing recommendation: ■ Data collection job can be scoped to maximum 500 assets. ■ Data evaluation job can be scoped to maximum 500 assets. Ensure the following: ■ Evaluation job does not overlap with other jobs as evaluation is processor intensive operation. Else include a separate CCS Manager with Data Evaluation role. ■ Any Sync job such as Report data synchronization job or evaluation sync job does not overlap with the Reporting data purge job. This is required to avoid slow performance of the system as both are database-intensive operations.

Table 2-18 Hardware configurations for CCS servers

CCS Component	Memory	Processor	Disk
Server hosting CCS Application server, and CCS Manager in evaluator, reporting, and load balancer role	4 GB	Dual Proc 3GHz	140 GB
SQL server hosting production and reporting database	4 GB	Dual Proc 3GHz	See "Disk sizing for Production database" on page 84. See "Disk sizing for Reporting database" on page 85.
CCS Manager for agent-less data collection	8 GB	Quad Proc, Quad core (16 logical processors), 3GHz	140 GB

Table 2-18 Hardware configurations for CCS servers *(continued)*

CCS Component	Memory	Processor	Disk
CCS Manager for agent-based data collection (raw-data or message based data)	4 GB	Dual Proc 3GHz	140 GB

See "Sizing requirements to monitor up to 5000 assets monthly" on page 75.

See "Sizing requirements to monitor up to 10000 assets monthly" on page 77.

See "Sizing requirements to monitor up to 30000 assets monthly" on page 79.

See "Sizing requirements to monitor up to 100000 assets monthly" on page 81.

Sizing requirements to monitor up to 5000 assets monthly

This section recommends the hardware, software, and job sizing requirements that are required for CCS to monitor up to 5000 assets monthly.

Table 2-19 Requirements and recommendations

Requirements	Recommendations

Hardware	Following are the hardware recommendations:
	■ 1 server to host the CCS Application Server, and CCS Manager in all roles except the Collector role.
	■ 1 SQL server to host production database and reporting database.
	■ In case of agent-less data collection, 1 server to host the CCS Manager in Collector role.
	■ In case of agent-based data collection:
	  ■ For raw-data collection, 1 server to host the CCS Manager in Collector role.
	  ■ For message based data collection, 2 servers to host CCS Managers in Collector role. Symantec recommends to deploy 1 CCS Manager or every 4000 agents.
	For information on Hardware configurations for CCS servers, See Table 2-20 on page 76.

Table 2-19 Requirements and recommendations *(continued)*

Requirements	Recommendations
Software	Following are the software recommendations: ■ 64-bit operating system should be deployed on the servers. Recommended operating system is Windows Server 2008 R2 with latest service pack and latest windows updates. ■ The SQL server hosting the production and reporting database should be of 64-bit.
Job sizing	Following are the job sizing recommendations: ■ Data collection job can be scoped to maximum 1000 assets. ■ Data evaluation job can be scoped to maximum 1000 assets. Ensure the following: ■ Evaluation job does not overlap with other jobs as evaluation is processor intensive operation. Else include a separate CCS Manager with Data Evaluation role. ■ Any Sync job such as Report data synchronization job or evaluation sync job does not overlap with the Reporting data purge job. This is required to avoid slow performance of the system as both are database intensive operations.

Table 2-20 Hardware configurations for CCS servers

CCS Component	Memory	Processor	Disk
Server hosting Application server, and CCS Manager in load balancer, evaluator, and reporting role	4 GB	Dual Proc 3GHz	140 GB
SQL server hosting production and reporting database	4 GB	Dual proc 3GHz	See "Disk sizing for Production database" on page 84. See "Disk sizing for Reporting database" on page 85.
CCS Manager for agent-less data collection	8 GB	Quad Proc, Quad core (16 logical processors), 3GHz	140 GB

Table 2-20 Hardware configurations for CCS servers *(continued)*

CCS Component	Memory	Processor	Disk
CCS Manager for agent-based raw-data collection	8 GB	Quad Proc, Quad core (16 logical processors), 3GHz	140GB
CCS Manager for agent-based message based data collection	4 GB	Dual Proc 3GHz	140 GB

See "Sizing requirements to monitor up to 1000 assets monthly" on page 73.

See "Sizing requirements to monitor up to 10000 assets monthly" on page 77.

See "Sizing requirements to monitor up to 30000 assets monthly" on page 79.

See "Sizing requirements to monitor up to 100000 assets monthly" on page 81.

Sizing requirements to monitor up to 10000 assets monthly

This section recommends the hardware, software, and job sizing requirements that are required for CCS to monitor up to 10000 assets monthly.

Table 2-21 Requirements and recommendations

Requirements	Recommendations

Hardware	Following are the hardware recommendations:
	■ 1 server to host the CCS Application Server.
	■ 1 server to host the CCS Manager with load balancer, evaluator, and reporting role.
	■ 1 SQL server to host production database.
	■ 1 SQL server to host reporting database.
	■ In case of agent-less data collection, 1 server to host the CCS Manager in Collector role.
	■ In case of agent-based data collection:
	  ■ For raw-data collection, 2 servers to host CCS Managers in Collector role.
	  ■ For message based data collection, 3 servers to host CCS Managers in Collector role. Symantec recommends to deploy 1 CCS Manager or every 4000 agents.
	For information on Hardware configurations for CCS servers, See Table 2-22 on page 78.

Table 2-21 Requirements and recommendations *(continued)*

Requirements	Recommendations
Software	Following are the software recommendations: ■ 64-bit operating system should be deployed on the servers. Recommended operating system is Windows Server 2008 R2 with latest service pack and latest windows updates. ■ The SQL server hosting the production and reporting database should be of 64-bit.
Job sizing	Following are the job sizing recommendations: ■ Data collection job can be scoped to maximum 2000 assets. ■ Data evaluation job can be scoped to maximum 2000 assets. Ensure that any Sync job such as Report data synchronization job or evaluation sync job does not overlap with the Reporting data purge job. This is required to avoid slow performance of the system as both are database intensive operations.

Table 2-22 Hardware configurations for CCS servers

CCS Component	Memory	Processor	Disk
Server hosting Application server	8 GB	Quad Proc, Quad core (16 logical processors), 3GHz	140 GB
CCS Manager in load balancer, evaluator, and reporting role	8 GB	Quad Proc, Quad core (16 logical processors), 3GHz	140 GB
SQL server hosting production database	8 GB	Quad Proc, Quad core (16 logical processors), 3GHz	See "Disk sizing for Production database" on page 84.
SQL server hosting reporting database	8 GB	Quad Proc, Quad core (16 logical processors), 3GHz	See "Disk sizing for Reporting database" on page 85.
CCS Manager for agent-less data collection	8 GB	Quad Proc, Quad core (16 logical processors), 3GHz	140 GB

Table 2-22 Hardware configurations for CCS servers *(continued)*

CCS Component	Memory	Processor	Disk
CCS Manager for agent-based raw-data collection	8 GB	Quad Proc, Quad core (16 logical processors), 3GHz	140 GB
CCS Manager for agent-based message based data collection	4 GB	Dual Proc 3GHz	140 GB

See "Sizing requirements to monitor up to 1000 assets monthly" on page 73.

See "Sizing requirements to monitor up to 5000 assets monthly" on page 75.

See "Sizing requirements to monitor up to 30000 assets monthly" on page 79.

See "Sizing requirements to monitor up to 100000 assets monthly" on page 81.

Sizing requirements to monitor up to 30000 assets monthly

This section recommends the hardware, software, and job sizing requirements that are required for CCS to monitor up to 30000 assets monthly.

Table 2-23 Requirements and recommendations

Requirements	Recommendations

Hardware	Following are the hardware recommendations:
	■ 1 server to host the CCS Application Server.
	■ Separate servers to host the CCS Manager in each role: load balancer, evaluator, and reporting role.
	■ 1 SQL server to host production database.
	■ 1 SQL server to host reporting database.
	■ In case of agent-less data collection, 3 servers to host the CCS Manager in Collector role.
	■ In case of agent-based data collection:
	  ■ For raw-data collection, 5 servers to host CCS Managers in Collector role.
	  ■ For message based data collection, 8 servers to host CCS Managers in Collector role. Symantec recommends to deploy 1 CCS Manager or every 4000 agents.
	For information on Hardware configurations for CCS servers, See Table 2-24 on page 80.

Table 2-23 Requirements and recommendations *(continued)*

Requirements	Recommendations
Software	Following are the software recommendations: ■ 64-bit operating system should be deployed on the servers. Recommended operating system is Windows Server 2008 R2 with latest service pack and latest windows updates. ■ The SQL server hosting the production and reporting database should be of 64-bit.
Job sizing	Following are the job sizing recommendations: ■ Data collection job can be scoped to maximum 2000 assets. ■ Data evaluation job can be scoped to maximum 5000 assets. Ensure that any Sync job such as Report data synchronization job or evaluation sync job does not overlap with the Reporting data purge job. This is required to avoid slow performance of the system as both are database intensive operations.

Table 2-24 Hardware configurations for CCS servers

CCS Component	Memory	Processor	Disk
Server hosting Application server	8 GB	Quad Proc, Quad core (16 logical processors), 3GHz	140 GB
CCS Manager in load balancer role	8 GB	Quad Proc, Quad core (16 logical processors), 3GHz	140 GB
CCS Manager in evaluator role	8 GB	Quad Proc, Quad core (16 logical processors), 3GHz	140 GB
CCS Manager in reporting role	8 GB	Quad Proc, Quad core (16 logical processors), 3GHz	140 GB
SQL server hosting production database	8 GB	Quad Proc, Quad core (16 logical processors), 3GHz	See "Disk sizing for Production database" on page 84.

Table 2-24 Hardware configurations for CCS servers *(continued)*

CCS Component	Memory	Processor	Disk
SQL server hosting reporting database	8 GB	Quad Proc, Quad core (16 logical processors), 3GHz	See "Disk sizing for Reporting database" on page 85.
CCS Manager for agent-less data collection	8 GB	Quad Proc, Quad core (16 logical processors), 3GHz	140 GB
CCS Manager for agent-based raw-data collection	8 GB	Quad Proc, Quad core (16 logical processors), 3GHz	140 GB
CCS Manager for agent-based message based data collection	4 GB	Dual Proc 3GHz	140 GB

See "Sizing requirements to monitor up to 1000 assets monthly" on page 73.

See "Sizing requirements to monitor up to 5000 assets monthly" on page 75.

See "Sizing requirements to monitor up to 10000 assets monthly" on page 77.

See "Sizing requirements to monitor up to 100000 assets monthly" on page 81.

Sizing requirements to monitor up to 100000 assets monthly

This section recommends the hardware, software, and job sizing requirements that are required for CCS to monitor up to 100000 assets monthly.

Table 2-25 Requirements and recommendations

Requirements	Recommendations

Hardware	Following are the hardware recommendations:
	■ 1 server to host the CCS Application Server.
	■ 4 servers to host the CCS Manager in the load balancer role.
	■ 10 servers to host the CCS Manager in the evaluator role.
	■ 1 server to host the CCS Manager in the reporting role.
	■ 1 SQL server to host production database.
	■ 1 SQL server to host reporting database.
	■ In case of agent-less data collection, 10 servers to host the CCS Manager in Collector role.
	■ In case of agent-based data collection:
	  ■ For raw-data collection, 17 servers to host CCS Managers in Collector role.
	  ■ For message based data collection, 25 servers to host CCS Managers in Collector role. Symantec recommends to deploy 1 CCS Manager or every 4000 agents.
	For information on Hardware configurations for CCS servers, See Table 2-24 on page 80.

Software	Following are the software recommendations: ■ 64-bit operating system should be deployed on the servers. Recommended operating system is Windows Server 2008 R2 with latest service pack and latest windows updates. ■ The SQL server hosting the production and reporting database should be of 64-bit.
Job sizing	Following are the job sizing recommendations: ■ Data collection job can be scoped to maximum 2000 assets. ■ Data evaluation job can be scoped to maximum 5000 assets. Ensure that any Sync job such as Report data synchronization job or evaluation sync job does not overlap with the Reporting data purge job. This is required to avoid slow performance of the system as both are database intensive operations.

Table 2-26 Hardware configurations for CCS servers

CCS Component	Memory	Processor	Disk
Server hosting Application server	8 GB	Quad Proc, Quad core (16 logical processors), 3GHz	140 GB

Table 2-26 Hardware configurations for CCS servers *(continued)*

CCS Component	Memory	Processor	Disk
CCS Manager in load balancer role	8 GB	Quad Proc, Quad core (16 logical processors), 3GHz	300 GB
CCS Manager in evaluator role	8 GB	Quad Proc, Quad core (16 logical processors), 3GHz	140 GB
CCS Manager in reporting role	8 GB	Quad Proc, Quad core (16 logical processors), 3GHz	140 GB
SQL server hosting production database	16 GB	Quad Proc, Quad core (16 logical processors), 3GHz	See "Disk sizing for Production database" on page 84.
SQL server hosting reporting database	16 GB	Quad Proc, Quad core (16 logical processors), 3GHz	See "Disk sizing for Reporting database" on page 85.
CCS Manager for agent-less data collection	8 GB	Quad Proc, Quad core (16 logical processors), 3GHz	140 GB
CCS Manager for agent-based raw-data collection	8 GB	Quad Proc, Quad core (16 logical processors), 3GHz	140 GB
CCS Manager for agent-based message based data collection	4 GB	Dual Proc 3GHz	140 GB

See "Sizing requirements to monitor up to 1000 assets monthly" on page 73.

See "Sizing requirements to monitor up to 5000 assets monthly" on page 75.

See "Sizing requirements to monitor up to 10000 assets monthly" on page 77.

See "Sizing requirements to monitor up to 30000 assets monthly" on page 79.

Database recommendations

A SQL server hosts the production and reporting databases. The database performance depends on the configuration and settings of the SQL server.

Review the following for recommendations related to databases:

- Disk sizing for production database
  See "Disk sizing for Production database" on page 84.
- Disk sizing for reporting database
  See "Disk sizing for Reporting database" on page 85.
- Recommendations for Reporting database deployment
  See "Recommendations for Reporting database deployment" on page 84.
- Recommendations for SQL server
  See "Recommendations for the SQL server" on page 87.
- Recommendations for Temp DB
  See "Recommendations for Temp DB" on page 88.
- Performance tuning
  See "Performance tuning" on page 89.

Recommendations for Reporting database deployment

The reporting database server deployment has the following recommendations:

- Symantec recommends to have the reporting database on 64 bit Windows Server and 64 bit SQL Server.
- If you have a single disk and disk controller, reporting database operations such as reporting sync, report purge or archival consume disk input/output (I/O), which can potentially affect the performance. If you have multiple high performance disks with separate disk controllers. SQL Server spawns one writer thread for each physical disk. This improves the performance of I/O operations.
- Symantec recommends to have multiple high performance disks with separate disk controllers to store the SQL data, SQL Log, and Temp DB components. All the disks should be high-speed: 15,000 RPM drives.

See "Recommendations for Temp DB" on page 88.

Disk sizing for Production database

The disk size that a SQL server computer hosting production database requires, depends on the following variables:

- Number of assets in the system
- Number of standards in the system
- Frequency of evaluation of a standard against number of assets
- Evaluation results

- Production database purge criteria

To determine disk requirements for SQL server computer hosting production database, the following guidelines should be followed:

No. of assets*No. of checks*constant 2 * No. of iterations =Size in KB

The following table gives the disk sizing for the Production database

Table 2-27 Disk sizing for the Production database

No. of Assets	Approx. production db size after one scan for 350 checks (GB)	Approx. increase in production db size for 10 scans (GB)
1000	1	15
5000	5	60
10000	10	120
30000	20	250
100000	70	750

Note: Considering that purge criteria for production database is set at 10 scans by default, the disk space requirement for storing evaluation results should not exceed the figures mentioned in the above table.

The above disk sizing requirements are estimated for Windows assets. For other platforms the disk size may vary due to increase in evidence size as well as type of evidence (positive / negative).

See "Disk sizing for Reporting database" on page 85.

Disk sizing for Reporting database

The disk size that a SQL server computer hosting reporting database requires, depends on the following variables:

- Number of assets in the system
- Number of standards in the system
- Frequency of evaluation of a standard against number of assets
- Evaluation results

To determine disk requirements for SQL server computer hosting reporting database, the following guidelines should be followed:

No. of assets*No. of checks*constant 3.5 * No. of iterations =Size in KB

The disk requirements for SQL server computer hosting reporting database depends on the frequency of scans.

Table 2-28 Disk sizing for the Reporting database considering weekly scan

No. of Assets	Approx. reporting db size after one scan for 350 checks (GB)	Approx. increase in a month for reporting db size assuming Weekly scan(GB)	Approx. Disk space needed for 1 year of usage. (GB)
1000	2	8	100
5000	6	24	300
10000	12	50	600
30000	36	150	1800
100000	120	500	6000

Table 2-29 Disk sizing for the Reporting database considering monthly scan

No. of Assets	Approx. reporting db size after one scan for 350 checks (GB)	Approx. increase in a month for reporting db size assuming Weekly scan(GB)	Approx. Disk space needed for 1 year of usage. (GB)
1000	2	2	25
5000	6	6	80
10000	12	12	150
30000	36	36	450
100000	120	120	1500

Table 2-30 Disk sizing for the Reporting database considering quarterly scan

No. of Assets	Approx. reporting db size after one scan for 350 checks (GB)	Approx. increase in a month for reporting db size assuming Weekly scan(GB)	Approx. Disk space needed for 1 year of usage. (GB)
1000	2	1	8

Table 2-30 Disk sizing for the Reporting database considering quarterly scan *(continued)*

No. of Assets	Approx. reporting db size after one scan for 350 checks (GB)	Approx. increase in a month for reporting db size assuming Weekly scan(GB)	Approx. Disk space needed for 1 year of usage. (GB)
5000	6	2	24
10000	12	4	50
30000	36	13	150
100000	120	40	500

Note: The above database size recommendations are for one year. For 3 years of usage, disk space can be increased linearly. Reporting database purge criteria is 3 years, by default.

Note: The above disk sizing requirements are estimated for Windows assets. For other platforms the disk size may vary due to increase in evidence size as well as type of evidence (positive / negative).

See "Disk sizing for Production database" on page 84.

See "Recommendations for Reporting database deployment" on page 84.

Recommendations for the SQL server

A SQL server hosts the production and reporting databases. Correct SQL server configuration and correct settings on the computer that hosts the SQL server helps to improve the CCS performance.

The recommended settings are as follows:

- Ensure that the SQL server is configured to use 75% of available physical memory (RAM). Perform the settings through the Memory tab of the SQL server properties dialog box.
- Ensure that the page file size on the computer that hosts the SQL server is set to the value, system managed size and not to any specific value. To set the value in the System Properties dialog box, click the advanced tab and then click Performance. In the Performance Options dialog box click Settings and select

the advanced tab. In the Virtual memory option, click Change and select, System managed size.

- Ensure that the computer that hosts the SQL server has the latest updates. If not, then you must install the service packs along with the cumulative update package (if any) on the computer that hosts the SQL server. For example, If you have SQL 2008, then you should deploy Service Pack 2 on it.

See "Recommendations for Reporting database deployment" on page 84.

Recommendations for Temp DB

The tempdb recommendations are as follows:

- The size and physical placement of the tempdb database can affect the performance of a system.
- Set the file growth increment to a reasonable size to avoid the tempdb database files from growing by a too small value. If the file growth is too small, compared to the amount of data that is being written to TempDb, TempDb may have to constantly expand. This can affect performance.
- Pre-allocate space for all TempDb files by setting the file size to a value large enough to accommodate the typical workload in the environment. This prevents TempDb from expanding too frequently, which can affect performance.
- Symantec recommends that you change the initial size of Tempdb on the reporting database (CSM_Reports) server to avoid memory related errors, while running the reporting synchronization job under peak load conditions. Set Auto growth to 10% of the initial size of Tempdb.
  Symantec recommends the following settings for the initial size of tempdb on the reporting database server for deployments of different scales:

Small scale deployment	1 GB Auto growth should be set to 10% of Tempdb
Medium and large-scale deployment	5 GB Auto growth should be set to 10% of Tempdb
Very-large scale deployment	20 GB Auto growth should be set to 10% of Tempdb

- Put the TempDb database on a disk with speed of 15,000 RPM.

- Put the TempDb database on disks which are separate from the CCS reporting database.

Performance tuning

For optimum performance of CCS, you must configure the following:

- The SQL server that hosts the production, and reporting databases.
- The computer that hosts the SQL server.

See "Recommendations for the SQL server" on page 87.

Your deployment of CCS, stores a large amount of data in the databases. Over a period of time, heavy use of the product causes index fragmentation in the CCS databases. This affects the performance of the tasks that are dependent on the databases. It is necessary to plan and perform database maintenance tasks, to optimize the performance of the databases.

For information on performing maintenance tasks on the databases, See "Database maintenance" on page 305.

CCS databases also include detailed evidence data of the Standards module and external data providers. This data is stored in separate filegroups. You can perform certain tasks on the database to optimize the database performance and storage management, such as moving the filegroups to different disks or compressing the filegroups.

For information on performing maintenance tasks on evidence data, See "Database maintenance for evidence data" on page 310.

Recommendations for data evaluation

Following are the recommendations for data evaluation:

- If you have more than 5000 assets, Symantec recommends to deploy a separate CCS Manager in evaluator role.
- Symantec recommends to deploy an additional CCS Manager in evaluator role, for every 10000 assets.
- Deployment of every additional CCS Manager of same configuration in evaluator role, increases the performance of data evaluation by 30 %.

Modifying the CCS Manager configuration settings for collecting raw-data using agent-less method

You can change the CCS Manager configuration settings to optimize data collection for agent-less raw-data in the following scenarios:

- If you are using a high configuration or a low configuration computer for CCS Manager, and you want to optimize data collection accordingly.
- If your CCS Manager co-exists with other CCS components, or other 3rd party components on a single computer, for example, CCS Manager + CCS Application Server, and you want to optimize the use of system resources during data collection, by the CCS Manager

To modify the CCS Manager configuration settings for agent-less raw-data collection

1 Open the CCS Manager configuration file from the following location:

<Install Directory>\Symantec\CCS\Reporting and Analytics\DPS\Symantec.CSM.DPS.exe.config

2 You can update the following keys in the <appSettings> section of the configuration file. The following table contains the default, minimum, and maximum values of the keys.

Table 2-31 CCS Manager configuration settings for agent-less raw-data collection

Key	Value	Description
<add key="WPM_MaximumJobsPerWorkerProcess" value="" />	■ Default: 10 ■ Minimum: 1 ■ Maximum: 20	The number of concurrent jobs that are assigned to any single worker process. If your CCS Manager computer has low physical memory, you can set the value of WPM_MaximumJobsPerWorkerProcess to 4 or 5.

Table 2-31 CCS Manager configuration settings for agent-less raw-data collection *(continued)*

Key	Value	Description
<add key="WPM_ActiveWorkerProcessesLimit" value="" />	■ Default: 7 ■ Minimum on 64 bit computer: 4 Minimum on 32 bit computer: 2 ■ Maximum: No limit.	The number of active worker processes. The Worker Process Manager (WPM) starts up to the specified number of worker processes while jobs are awaiting to be processed. Out of the 4 minimum active worker processes running on a 64 bit computer, 2 processes are 32 bit and 2 processes are 64 bit. Maximum value depends on configuration of the computer. If you are using a low-configuration computer or if you are collecting data from less number of assets you can set the value of WPM_ActiveWorkerProcessesLimit between 3 to 5.
<add key="WPM_WorkerProcessesThresholdLimit" value="" />	■ Default: 12 ■ Minimum: 4 ■ Maximum: No limit.	The number of concurrent worker processes, which includes active and obsolete processes. Maximum value depends on configuration of the computer. You can set the maximum value of WPM_WorkerProcessesThresholdLimit to 80 % or 100% more than the WPM_ActiveWorkerProcessesLimit" value.
<add key="MaxConnectionsPerAsset" value="" />	■ Default: 5 ■ Minimum: 1 ■ Maximum: 10	The number of parallel queries made to an asset from a single job, for data collection.
<add key="WPM_MinimumWorkerProcesses" value="" />	■ Default: 2 ■ Minimum: 2	Governs the minimum number of worker processes for a 64 bit computer.

Table 2-31 CCS Manager configuration settings for agent-less raw-data collection *(continued)*

Key	Value	Description
<add key="WPM_x86MinimumWorkerProcesses" value="" />	■ Default: 2 ■ Minimum: 2	Governs the minimum number of worker processes for a 32 bit computer.

Note: WPM_ActiveWorkerProcessesLimit and WPM_WorkerProcessesThresholdLimit are interdependent. The value of WPM_WorkerProcessesThresholdLimit must be greater than WPM_ActiveWorkerProcessesLimit. There must be a significant difference between the two values. If there is no significant difference, the performance is compromised, as large number of worker processes process less number of jobs, and the overall throughput is reduced

Modifying the CCS Manager configuration settings for message based data collection

You can change the CCS Manager configuration settings to optimize data collection for message based data in the following scenarios:

- If you are using a high configuration or a low configuration computer for CCS Manager, and you want to optimize data collection accordingly.
- If your CCS Manager co-exists with other CCS components, or other 3rd party components on a single computer, for example, CCS Manager + CCS Application Server, and you want to optimize the use of system resources during data collection, by the CCS Manager

To modify the CCS Manager configuration settings for message based data collection

1. Open the CCS Manager configuration file from the following location:

   <Install Directory>\Symantec\CCS\Reporting and Analytics\DPS\Symantec.CSM.DPS.exe.config

2. You can update the following keys in the <appSettings> section of the configuration file. The following table contains the recommended values for message based data collection.

Table 2-32 CCS Manager configuration settings for message based data collection

Key	Value	Description
<add key="WPM_MaximumJobsPerWorkerProcess" value="" />	■ Default: 10 ■ Recommended for message based data: 1	The number of concurrent jobs that are assigned to any single worker process.
<add key="WPM_ActiveWorkerProcessesLimit" value="" />	■ Default: 7 ■ Recommended for message based data: 3	The number of active worker processes. The Worker Process Manager (WPM) starts up to the specified number of worker processes while jobs are awaiting to be processed. Configure the CCS Manager to have at least 2 active worker processes running in 32 bit mode at any given point of time. If the CCS Manager is installed on a 32 bit operating system, set the value to 2. If the CCS Manager is installed on a 64 bit operating system, set the value to 3. **Note:** For each additional ESM Manager configured for the CCS Manager, increase the number of active worker processes by 1.
<add key="WPM_WorkerProcessesThresholdLimit" value="" />	■ Default: 12 ■ Recommended for message based data: 5	The number of concurrent worker processes, which includes active and obsolete processes. Configure the CCS Manager to create maximum 4 worker processes running in 32 bit mode. If the CCS Manager is installed on a 32 bit operating system, set the value to 4. If the CCS Manager is installed on a 64 bit operating system, set the value to 5. **Note:** Any change to active worker process limit must be reflected in the worker process threshold limit. For example, if you increase the value of WPM_ActiveWorkerProcessesLimit by 2, you must increase the value of WPM_WorkerProcessesThresholdLimit by 2.

Table 2-32 CCS Manager configuration settings for message based data collection *(continued)*

Key	Value	Description
<add key="WPM_CumulativeJobLimit" value="" />	■ Default: 100 ■ Recommended for message based data: 10	The number of jobs processed, after which a worker process is recycled.
<add key="WPM_MinimumWorkerProcesses" value="" />	■ Default: 2 ■ Minimum: 2	Governs the minimum number of worker processes for a 64 bit computer.
<add key="WPM_x86MinimumWorkerProcesses" value="" />	■ Default: 2 ■ Minimum: 2	Governs the minimum number of worker processes for a 32 bit computer.

Note: WPM_ActiveWorkerProcessesLimit and WPM_WorkerProcessesThresholdLimit are interdependent. The value of WPM_WorkerProcessesThresholdLimit must be greater than WPM_ActiveWorkerProcessesLimit. There must be a significant difference between the two values. If there is no significant difference, the performance is compromised, as large number of worker processes process less number of jobs, and the overall throughput is reduced

For data collection, using a CCS Manager with multiple roles such as collector, evaluation or reporting may affect the data collection performance. For message based data collection, Symantec recommends that you install a CCS Manager only with the Collector role.

Modifying the CCS Manager page file size

To improve the CCS Manager memory usage during high loads, Symantec recommends to increase the page file size of the computer that hosts the CCS Manager.

To modify the CCS Manager page file size

1 In the Control Panel, double-click the System icon.

2 Performing this step only if you are modifying the page file size on Windows Server 2008.

Click **Change settings**.

3. In the System Properties dialog box, click the **Advanced** tab.
4. Under Performance, click **Settings**.
5. In the Performance Options dialog box, click the **Advanced** tab, and under Virtual memory, click **Change**.
6. In the Virtual Memory dialog box, select a drive to store the paging file, and click **Custom size**.
7. If you have configured the CCS Manager to synchronize the reporting database, set the Initial size (MB) to 40960 MB, and Maximum size (MB) to 51200 MB.

   If your CCS Manager is in the load balancer, evaluator or external data collector role, set the Initial size (MB) to 12288 MB, and Maximum size (MB) to 20480 MB.
8. Click **Set** and then click **OK**.
9. Restart the CCS Manager computer.

Recommendations for Policy Central

The Policy Central on the Web Console is used by policy audience to respond to the published policies, request exceptions and clarifications. For efficient performance of the Policy Central when a large number of concurrent users are performing tasks simultaneously, Symantec recommends the following configuration changes:

On the CCS Application Server, in the folder CCS\Reporting and Analytics\CCS.Portal, edit the `web.config` file to set the value of `maxConcurrentCalls` to the maximum number of users performing tasks on the Policy Central. Increasing the value may affect the response time of each call.

The default value of `maxConcurrentCalls` is 250.

This is a global service throttling setting for the following Policy Central services, controlled with the behavior name ThrottlingServiceBehavior:

```
<services>
<service name="Symantec.CSM.PolicyCentral.Services.PolicyCentral"
 behaviorConfiguration="ThrottlingServiceBehavior"></service>
<service name="Symantec.CSM.PolicyCentral.Services.ClarificationsService"
 behaviorConfiguration="ThrottlingServiceBehavior"></service>
<service name="Symantec.CSM.PolicyCentral.Services.ExceptionsService"
 behaviorConfiguration="ThrottlingServiceBehavior"></service>
<service name="Symantec.CSM.PolicyCentral.Services.SearchService"
 behaviorConfiguration="ThrottlingServiceBehavior"></service>
<service name="Symantec.CSM.PolicyCentral.Services.UserResponseService"
```

```
 behaviorConfiguration="ThrottlingServiceBehavior"></service>
</services>
```

Each of the services listed above perform specific policy related tasks, such as request exceptions, clarifications and so on.

Depending on the number of users performing each of the tasks, for efficient load balancing, you can configure separate respective values for `maxConcurrentCalls` for each service.

To specify a separate `maxConcurrentCalls` value for each setting, create multiple instances of the following tags specific to a behavior:

```
<behavior name="ThrottlingServiceBehavior>
<serviceMetadata httpGetEnabled="true"/>
<serviceDebug includeExceptionDetailInFaults="false"/>
<!-- Specify throttling behavior -->
<serviceThrottling maxConcurrentCalls="250" maxConcurrentInstances="100" />
</behavior>
```

For each instance, you can change the behavior name `ThrottlingServiceBehavior` to refer to specific throttling behavior such as `ClarificationsServiceBehavior` and refer the name in the service tag as follows:

```
<service name="Symantec.CSM.PolicyCentral.Services.ClarificationsService"
 behaviorConfiguration="ClarificationsServiceBehavior">
```

Note: Policy Central may display errors if the number of users performing tasks exceed the value specified for `maxConcurrentCalls`.

Virtualization

Although CCS recommends dedicated hardware for optimal performance, certain components of the application can be run successfully within virtualized environments. For ease of management, you can use virtualized servers to host CCS servers. A virtualized server can host any CCS server role. Certain server roles lend themselves naturally to a virtualized host. When you create a virtualized server to host CCS components, ensure that the computer that hosts the virtual servers meets certain recommendations. You should also ensure that the individual virtual servers meet the recommendations appropriate to the role.

A virtualized server can successfully host the following server roles:

- Application Server in a very small deployment (Less than 1000 assets in a system)

- CCS Manager Load Balancer
- CCS Manager Evaluator
- CCS Manager Reporter

A virtualized server should generally not host the following server roles:

- Production database
- Reporting database
- CCS Manager Collector

CCS does not recommend running Microsoft SQL Server in a virtualized environment; the memory and I/O demands of a SQL database are such that the physical to virtual translation penalty for each transaction accumulate to a substantial increase in response times. You can use a virtualized server to host any role, but for highest performance you should use a physical server for the following server roles:

- Production database
- Reporting database
- CCS Manager Collector

When you create a virtual machine to host a CCS Manager for agent-less data collection, the virtual machine must have access to at least 8 GB of memory. It should also have 16 logical processors. For agent-based raw-data or message based data collection, CCS Manager should have at least 4GB of memory and 8 logical processors. Also for the Virtual machines used for CCS components, user should assign reserved memory and CPU. When you create the virtual machine, you should immediately install the VMware Tools. The network adapter type for the virtual machine should be set to Flexible.

The virtual server host has the following specifications:

- 8-way 3.0 GHz or faster processors
- 32 GB or more memory
- 600 GB or greater, 15000 RPM hard disk
- Gigabit network interface

As permanent storage resources are typically shared across VMs, there is a much greater potential to encounter disk and/or I/O contention issues as compared to a physical server. Dedicated spindles or a SAN are recommended to lessen the likelihood of this contention.

About raw-data collection

You must collect asset data from your enterprise network in order to achieve your business objectives using CCS. Raw-data based collection lets you collect asset data from your enterprise network. The collected data is then evaluated against a standard in CCS. You can collect raw-data using the agent-less method or the agent-based method.

The agent-less method allows you to collect asset data without installing any components on the computers in your network. Using the agent-less method, you can collect asset data for the following platforms:

- Windows
- UNIX
- Oracle
- Microsoft SQL Server
- Cisco

The agent-based method allows you to collect asset data using agents installed on the computers in your network. A CCS Agent collects asset data from the host computer and sends the data to the CCS Infrastructure in order to process the data to meet your business objectives. Using the agent-based method, you can collect asset data for the following platforms:

- Windows
- UNIX
- Oracle
- Microsoft SQL Server

You can deploy the RMS Information Server and BV-Controls to collect data from the following platforms:

- Exchange
- VMware

For information on installing and configuring RMS Information Server and BV-Controls, see the *Symantec Control Compliance Suite Installation Guide version 10.5*.

If you are using agents to collect raw-data from your network, you can also collect message based data using the agents.

See “About message based data collection” on page 100.

The following tables lists the components that you must install in order to collect asset data from your enterprise network.

Note: The CCS Suite comprises of the CCS Application Server and the CCS Manager.

Table 2-33 Components required to deploy a raw-data based collection solution

Deployment method	Description	Components required
Agent-less	Use the CCS Manager to collect data from the network. CCS Manager sends the data to the CCS infrastructure in order to process the data.	CCS Suite
Agent-based	Use the CCS Agents to collect data from host computers. CCS Agents send the data to the CCS Manager. CCS Manager sends the data to the CCS infrastructure in order to process the data.	CCS Suite CCS Agent
RMS Information Server	For platforms such as Exchange or VMware, use the RMS Information Server to collect data from the network. RMS Information Server sends the data to the CCS Manager. CCS Manager sends the data to the CCS infrastructure in order to process the data.	CCS Suite RMS Information Server RMS BV-Control snap-in modules for Exchange or VMware.

Review the following to plan for a raw-data based collection solution.

- Components of CCS
  See "Components of CCS" on page 20.
- CCS hardware requirements
  See "Hardware and operating system requirements" on page 37.
- CCS software requirements
  See "Software requirements" on page 48.
- User privileges for installing the CCS components

See “User Privileges for deploying the CCS components” on page 55.

- Performance and scalability
  See “Deployment sizing” on page 72.
  See “About using sites” on page 105.
  See “Database recommendations” on page 83.
  See “ Virtualization” on page 96.

About message based data collection

You must collect asset data from your enterprise network in order to achieve your business objectives using CCS. Message based collection lets you collect and interpret asset data from your enterprise network before sending the data to CCS. The CCS Agent installed on each computer in the enterprise network performs the actual task of data collection and interpretation. The CCS Agent interprets the data against the standards or policies and presents the data to CCS in the form of messages. You can plan a message based collection solution to collect asset data for the following platforms:

- Windows
- UNIX
- Oracle
- Microsoft SQL Server
- DB2
- Sybase
- VMware

To perform data collection, you must install and configure the application modules for the respective platforms on the CCS Agents

---

Note: If you want to collect message based data, install the ESM Console to initiate policy runs for message based data collection. For information on installing the ESM Console, see the *Symantec Enterprise Security Manager Installation Guide*.

The following tables lists the components that you must install in order to collect asset data from your enterprise network.

Note: The CCS Suite comprises of the CCS Application Server and the CCS Manager.

Table 2-34 Components required to deploy a message based collection solution

Deployment method	Description	Components required
CCS Agent	Use the CCS Agents to collect data from host computers. CCS Agents collect and interpret the data before sending the data to the CCS Manager. CCS Manager sends the data to the CCS infrastructure in order to process the data.	CCS Suite CCS Agent ESM Console If you want to collect message based data, install the ESM Console to initiate policy runs for message based data collection.

Review the following to plan for a message based collection solution.

- Components of CCS
  See "Components of CCS" on page 20.
- CCS hardware requirements
  See "Hardware and operating system requirements" on page 37.
- CCS software requirements
  See "Software requirements" on page 48.
- User privileges for installing the CCS components
  See "User Privileges for deploying the CCS components" on page 55.
- Performance and scalability
  See "Deployment sizing" on page 72.
  See "About using sites" on page 105.
  See "Database recommendations" on page 83.
  See " Virtualization" on page 96.

About collecting data from assets located on the cloud

CCS can collect data from assets located on the cloud. Following are the considerations for collecting asset data from the cloud.

Infrastructure considerations

- You can collect asset data using both agent-less and agent-based methods. The CCS Application Server must be located in your premises, but you can place the CCS Manager either in your premises or on the cloud.
- For agent-less data collection:

- If both the CCS Manager and the target computers are on the cloud, you can collect asset data from Windows, UNIX and SQL platforms.
- If the CCS Manager is in your premises and the target computers are on the cloud, you can collect asset data only from the UNIX platform.

Environment Settings

- If the CCS Manager is on the cloud, the CCS Application Server must contain host entries with IP addresses of both the external and internal names of the CCS Manager.
- If the CCS Manager is in your premises, the CCS Manager must contain host entries with IP addresses of both the external and internal names of the target computers
- The target computers must contain host entries with IP addresses of both the external and internal names of the CCS Manager.

CCS Settings

- While generating a certificate for the CCS Manager located on the cloud, in the **Create Certificates** dialog box of the Certificate Management Console, the **NetBIOS Name** must be the internal name of the CCS Manager and the **FQDN** must be the external name of the CCS Manager.
  See "Creating a certificate for installing a standalone CCS Manager" on page 167.
- For data collection from Windows platform, if the CCS Manager and the target computers are located in different workgroups, the CCS Manager must be configured to use pass-through authentication to collect asset data from the target computers.
- You can use the following methods in CCS to import assets from the cloud:
  - CSV import using the CSV data collector
  - ODBC import using the ODBC data collector
  - Add assets manually. You can use the Add Assets task to add assets without performing an asset import.
  - Import agent-based assets using the Import assets and agents job.
- For importing cloud based assets, provide the following platform specific information:.

  For Windows asset:

  - **Domain / Workgroup Name**: External name of the target computer.
  - **Machine Name**: Internal name (NetBIOS name) of the target computer.

  For UNIX asset:

- **Machine Name**: External name of the target computer.
- **IP Address**: External IP address of the target computer.

For SQL Server asset:

- **Domain / Workgroup Name**: External name of the target computer.
- **Server Name (Instance)**: Internal name of the target computer.
- **Host Name (Node)**: Internal name of the target computer.

Internal IP address is a private IP address used on your local network to communicate within that network. External IP address is a public IP address which is accessible outside of your network, such as on the Internet.

Internal name is a computer name used on your local network to communicate within that network. External name is a public DNS name which is accessible outside of your network, such as on the Internet.

For more information on importing assets into CCS, see the *Asset management* section in the *Symantec Control Compliance Suite User Guide*.

For firewall and port information, See "Network Ports" on page 41.

Note: Perimeter security products or external facing firewalls might block the connection between CCS - and the CCS components or assets deployed on the cloud. You must open the firewall ports for allowing successful TCP/IP handshake between the components and the data collection to proceed.

CCS Upgrade Paths

The upgrade to the latest release version of the Control Compliance Suite (CCS) lets you access the new and updated features and functionality of the product.

CCS 11.1 supports direct upgrade only from CCS 11.0.

For upgrading ESM deployments, CCS 11.1 supports direct upgrade from ESM 11.0. Upgrade the ESM Console to ESM Console 11.1. ESM console is required to initiate policy runs for message based data collection.

If you are using CCS 10.5.1 or earlier versions of CCS, you need to upgrade to CCS 11.0 first and then upgrade to CCS 11.1.

The following table gives the various upgrade paths that are supported.

Table 2-35 Supported upgrade paths

Supported upgrade path	Description
CCS 11.0 to CCS 11.1	Upgrade CCS 11.0 to CCS 11.1.
CCS 10.5.1 to CCS 11.1	Use the following sequence to upgrade: **1** Upgrade CCS 10.5.1 to CCS 11.0. **2** Upgrade CCS 11.0 to CCS 11.1.
ESM 11.0 to CCS 11.1	Upgrade ESM 11.0 to CCS 11.1.
ESM 10.0 to ESM 11.1	Use the following sequence to upgrade: **1** Upgrade ESM 10.0 to ESM 11.0 **2** Upgrade ESM 11.0 to ESM 11.1

Upgrading CCS Agent

You can upgrade CCS Agent 10.5.1 to CCS Agent 11.1, and CCS Agent 11.0 to CCS Agent 11.1.

CCS 11.1 supports upgrading ESM Agent 10.0 to CCS Agent 11.1, CCS Agent 11.0 to CCS Agent 11.1, and CCS Manager 11.0 to CCS Manager 11.1. You cannot upgrade ESM Manager 10.0 to CCS Manager 11.1.

You can replace the BV-Control for UNIX Agents with the CCS Agents. In your existing deployment, if you are collecting data from UNIX computers using the BV-Control for UNIX Agents, you can replace those agents with the CCS Agents.

It is recommended that until you complete the upgrade and perform data collection from the new deployment for the first time, you should maintain a co-existence of the existing components with the new components of CCS 11.1. Later, once you are sure that you are able to collect data from the new components, you can remove the existing components.

After you upgrade the components, you must configure routing rules and credentials for data collection.

Routing rules let you determine the entire route plan for data collection. With routing rules, you can now control the distribution of data collection jobs for assets based on IP range, Subnet, Expressions or Asset groups. While planning for the upgrade, consider how you want to plan the data collection. If you are performing a phased migration, consider which sites or assets you want to upgrade depending on how you will be configuring the routing rules to perform data collection on those assets.

Credentials allow CCS to gain access to and perform asset import or data collection from target computers in your network. The credentials can be used either for assets

or to centrally store user name and password for WINDOWS, UNIX, SQL, Oracle users and use them in platform configuration. CCS lets you manage common credentials and asset credentials at a central location.

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.

See "What sites can do for you" on page 105.

See "About planning sites" on page 106.

See "About upgrading to routing rules" on page 106.

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.

See “About using sites” on page 105.

See “About planning sites” on page 106.

See “About upgrading to routing rules” on page 106.

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.

See “About using sites” on page 105.

See “What sites can do for you” on page 105.

See “About upgrading to routing rules” on page 106.

About upgrading to routing rules

Routing rules let you define a particular site or a CCS Manager to perform the jobs that are related to your assets or your agents.

For fresh installation of CCS, you can create new routing rules for assets based on IP range, Subnet, Expressions or Asset groups. If no rules are created or if the jobs

cannot be routed through a routing rule that is created, jobs are first routed to network affinity. Jobs are routed to network affinity if the assets are in the same or in the accessible subnet as that of the CCS Manager. If they are not, then the jobs are routed to the default site where a CCS Manager must be present in the collector role.

In case of upgrade, CCS creates a site specific routing rule to route CCS jobs based on your existing sites, through RMS. The site specific routing rule is used by default. To route jobs through the CCS Manager, you must create new routing rules as stated in the *Platform specific configurations for data collection using CCS Manager* section in the *Symantec™ Control Compliance Suite Quick Start Guide for RMS upgrade*.

To know more about routing rules, refer to *Concepts in routing rules* in the CCS SymHelp.

About job hopping

Job hopping allows you to collect data from assets across networks that have restricted communication between each other. For example, restricted communication between the network that contains the CCS Manager Load Balancer, and the network that contains the assets.

Suppose you want to collect data from assets located in four network zones A, B, C and D. Each network zone allows only one way connectivity to the other zone. For example, the connectivity between the above mentioned network zones is A > B > C > D, zone A is not directly connected to zone C and D. Zone A contains the installation of the CCS core components, such as the CCS Application Server, CCS Console and a CCS Manager with Load Balancer role. Zones B, C and D each contain a CCS Manager that is collecting data from assets located in the respective zones. As there is only a one way connectivity between the zones, the CCS Application Server located in zone A cannot collect data directly from assets located in zones C and D.

In such a network scenario, you can collect data from zones C and D by configuring an appropriate job hopping plan. A job hopping plan sends requests for and collects data, by forwarding the request to an immediately accessible zone. For example, a request for collecting data from assets in zone D, will be forwarded from zone A to zone B, then from zone B to zone C, and finally from zone C to zone D. Collected data from an asset in zone D is sent back in the same sequence in which the request was sent.

You can configure job hopping using the Manage Job Hopping Plan panel.

From the above example, if you want to collect data from zone D, you must create a job hopping plan which forwards the data collection request through each CCS

Manager located in the respective zones. In this scenario the job hopping plan that is required is as follows:

Zone A CCS Manager Load Balancer > Zone B CCS Manager Data Collector > Zone C CCS Manager Data Collector > Zone D CCS Manager Data Collector

The job hopping plan will forward the data collection request using the above mentioned route and send the data back through the same route.

Note: The job hopping plan is required to collect data from zones other than the zone which contains the CCS Application Server and the CCS Manager Load Balancer. Therefore, in the job hopping plan, you cannot add a CCS Manager Data Collector which is installed on a computer that hosts the CCS Application Server, CCS Directory server or CCS Manager Load Balancer.

For more information on how a job hopping plan works, see http://www.symantec.com/docs/HOWTO83961.

About FIPS compliance

The following CCS components are Federal Information Processing Standard-compliant:

CCS Suite	CCS is a collection of the following components: ■ CCS console ■ CCS Application Server ■ CCS Manager All the components are collectively responsible for content and job management, data collection, data processing and analysis, and report generation.
CCS Agent	The CCS Agent resides on the computers in your network. The CCS Agent collects data about the target computer and forwards the data to the CCS Manager.

Prerequisites for FIPS compliance

To work in a Federal Information Processing Standard (FIPS) compliant environment, ensure that you perform the following configurations:

- Configure the computers that hosts the CCS Application Server and the CCS Manager.

  To configure the environment in the FIPS enabled mode, navigate to the computers that host the above services local security setting and enable the option **System cryptography: use FIPS compliant algorithms for encryption, hashing, and signing**.

  Note: In a scale-out setup of CCS, ensure that all the CCS components are either in a complete FIPS compliance mode or a complete non-FIPS compliance mode. For example, if the Application Server is enabled for FIPS mode then all other CCS components like CCS Manager and database servers must also be enabled for FIPS compliance mode. CCS console on a remote computer and CCS Web Console are independent from the FIPS settings and can work in non-FIPS enabled environment, even when the CCS setup is in FIPS enabled environment

  ---

- Apply the Microsoft hot fix, http://support.microsoft.com/kb/981119

  This hot fix is required for proper function of the CCS Web Console when the CCS Application Server is deployed on the Windows Server 2008 R2 computer which is configured in a FIPS compliance enabled environment.

- Apply the Microsoft hot fix, http://support.microsoft.com/kb/977069

  This hot fix is required for the CCS jobs to function properly on the CCS Application Server that is deployed on the Windows Server 2003 or Windows Server 2008 computers which is configured in a FIPS compliance enabled environment

About mandatory configuration for Federal Information Processing Standard compliance

Following are the mandatory configurations for CCS to function in a Federal Information Processing Standard (FIPS)-compliant environment:

- You must set the **FIPS enabled** flag through the Local/Group security policy on the server that hosts the following CCS components:
  - CCS Application Server
  - CCS Manager
- You must configure the Integration Bridges and all the protocols under the Bridge Manager to use Basic256 or higher cipher suite.
- The CCS Web Console requires the Microsoft hot fix 981119 to function correctly when the application server is installed on a Windows 2008 R2 platform in a

FIPS-enabled environment. The Microsoft hot fix 981119 corrects an issue with ASP.Net in a FIPS-enabled environment on Windows 2008 R2 platforms.

For more information, visit the following link:

http://support.microsoft.com/kb/981119

- The CCS Application Server jobs require the Microsoft hot fix 977069 to function correctly on a Windows 2003/2008 server in a FIPS-enabled environment. The Microsoft hot fix 977069 corrects an issue with Windows Workflow run-time in a FIPS-enabled environment.

  For more information, visit the following link:

  http://support.microsoft.com/kb/977069

About the modules that handle sensitive information and their Federal Information Processing Standard-compliance status

CCS is based on Microsoft .Net Framework and internally uses Federal Information Processing Standard (FIPS)-compliant algorithms and technology.

To ensure FIPS 140-2 compliance, Symantec uses the following algorithms and technology in the specified CCS modules:

Table 2-36 Algorithms and technology used for FIPS compliance in CCS

Name	Description
WCF channel encryption	Symantec uses WCF message security with AES256 and SHA1 (default setup) for all communications to and from the application server.
Certificate Management	The Certificate Management module generates the certificates and uses FIPS-enabled OpenSSL that complies to the security policy of OpenSSL FIPS module. For more information about the security policy of OpenSSL FIPS module, visit the following link: http://www.openssl.org/docs/fips/SecurityPolicy-2.0.pdf The Certificate Management module ensures that OpenSSL is always initialized in the FIPS mode if the **FIPS Enabled** flag is configured for the operating system. Certificate generation uses RSA 2048 or later and SHA1 or later algorithms.

Table 2-36 Algorithms and technology used for FIPS compliance in CCS *(continued)*

Name	Description
Secure Storage	The Secure Storage module stores sensitive information such as user credentials and database connection strings. CCS uses the FIPS-certified crypto provider that is available in .Net framework 4.0 (AesCryptoServiceProvider) to secure the sensitive information that is stored in secure storage. For more details on FIPS-compliance claim of AesCryptoServiceProvider, visit the following link: http://blogs.msdn.com/b/winsdk/archive/2009/11/04/Is-rijndaelmanaged-class-fips-complaint.aspx
Symantec Licensing	The Symantec Licensing module, which is shared across various Symantec products, uses RSA's BSAFE Crypto library v1.5.1 that is FIPS 140-1 certified. For more details on FIPS security policy, visit the following link: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp163.pdf

Symantec has ensured that all cryptographic algorithms that are used in CCS are approved as per FIPS 140-2 guidelines.

For more details on FIPS 140-2 approved algorithms, visit the following link:

http://csrc.nist.gov/groups/STM/cavp/index.html

Apart from the mentioned CCS modules, the product has been fully tested in FIPS-enabled environment, which is done by enabling FIPS Enabled flag through Group/Local security policy. Symantec has ensured that the third party components do not violate any of FIPS 140-2 guidelines. Since CCS Reporting and Analytics is a .Net application, Symantec has relied on the **FIPS Enabled** flag of Windows Local/Global security policy for FIPS compliance.

For more details on effects of enabling FIPS key on .Net applications, visit the following link:

http://support.microsoft.com/kb/811833/en-us

About external data integration

External data integration lets you seamlessly assimilate data from an application that is external to CCS and represent the same by leveraging the CCS Dashboards and reports

You can import external data by using any of the following preconfigured data systems:

- Symantec CCS Vulnerability Manager
- Symantec Data Loss Prevention
- Symantec CCS Assessment Manager

You can also integrate with any third-party application and use the following data connectors to import the required data:

Table 2-37 Data connectors for importing external data

Data connectors	Description
ODBC data connector	The ODBC connector lets you import data from an external system that stores data in the databases that support ODBC drivers.
CSV data connector	The CSV connector lets you import data from an external system that stores data in .csv files.
Web Services connector	The Web Services connector lets you import data from an external system that stores data .xml files and can export the data by using APIs.

Before you integrate an external data system and import data by using the ODBC, CSV, or the Web Services connector, you must do the following:

- Identify the Asset, Assessment, and Status attributes in the external data.
- Identify the schema that you want to use to process the imported data.
- Correlate the asset and the status data fields to CCS.
- Configure reconciliation rules to add the imported assets to the CCS system.
- Configure asset risk aggregation.

See “Preparing for external data integration” on page 113.

External data systems architecture

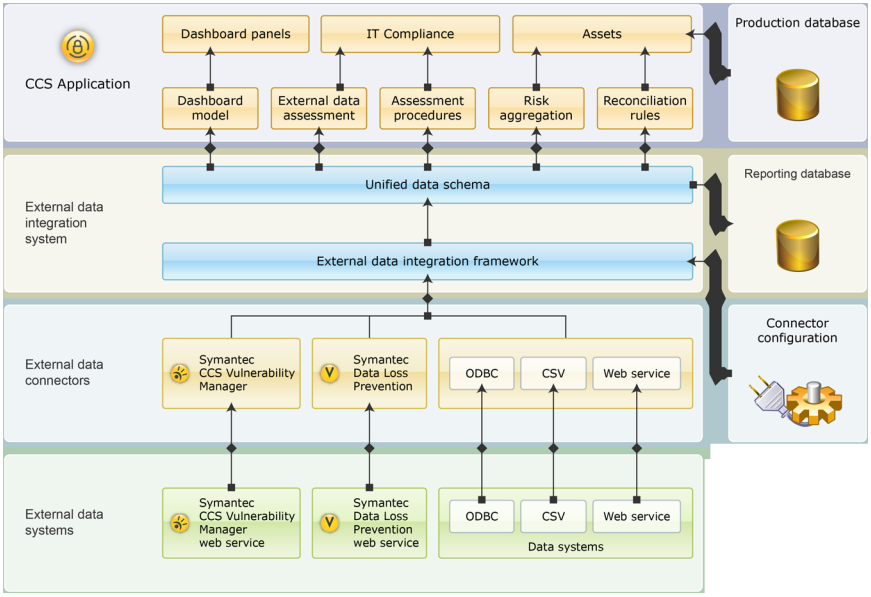
CCS lets you assimilate data from an external data system into CCS using the ODBC, CSV or Web services connectors.

CCS provides pre-integrated solutions for:

- Vulnerability assessment - Symantec CCS Vulnerability Manager
- CCS AM assessment - Symantec CCS Assessment Manager
- Data loss prevention incidents - Symantec Data Loss Prevention

The following table illustrates how the external data systems work together with the various CCS modules.

Figure 2-1 External data systems architecture



Preparing for external data integration

You can integrate with any third-party application and use the ODBC, CSV, or the Web services connectors to import the required data into CCS.

Before you import external data, you must do the following:

- Identify the following attributes in the external data:

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.

CCS consumes and represents data only in terms of the Asset-Assessment-Status attributes. Hence, before you import external data into CCS, you must map the external data fields to the Asset-Assessment-Status attributes in the CCS schema. You can map the external data fields to the CCS schema from the **External Data Integration** view.

- Correlate the external system data to CCS.
  By means of correlation, you basically establish an association between the imported data and the existing CCS assets. Without correlation, you cannot leverage the CCS infrastructure to represent the external data in CCS Dashboards and reports. You can correlate the external data fields and the CCS asset fields from the **External Data Integration** view.
- Configure asset risk aggregation.
  For risk score calculation, you either use CCS to calculate the risk scores based on the CVSS parameters or use the risk scores that are defined the imported data. You can specify the risk score parameters from the **External Data Integration** view.

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.
- 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.

- 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.
- Correlate data with CCS:
  Data correlation lets you establish an association between the data fields in the imported data and the CCS data.
- Reconcile assets:
  You can use the reconciliation rules to add new assets, update existing asset fields and update the data schema.

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:

Table 2-38 Attributes of the data schema

Attributes	Description
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
- CCS AM 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.

You must have appropriate permissions to integrate external data.See "Permissions required for External Data Integration" on page 117.

Business objectives for external data integration

You can plan the external data integration based on the following business objectives:

- Do you want to import external data and view the data in CCS Dashboards without correlating to the CCS assets?
  See "Scenario 1: Import external data and view the data in CCS Dashboards without CCS asset correlation" on page 118.
- Do you want to import external data and view the data in CCS Dashboards in correlation with the CCS assets?
  See "Scenario 2: Import external data and view the data in CCS Dashboards in correlation with the CCS assets" on page 120.
- Do you want to import external data and use it for policy compliance?
  See "Scenario 3: Import external data and use it for policy compliance" on page 123.
- Do you want to import external data and use it for contributing to the CCS asset Risk Score?
  See "Scenario 4: Import external data and use it for contributing to the CCS asset risk score" on page 126.

See "How to achieve your business objectives with external data integration" on page 127.

Prerequisites for external data integration

There are no specific system requirements for external data integration. Refer to the hardware and operating system requirements for CCS components.

See "Hardware and operating system requirements" on page 37.

Permissions required for External Data Integration

You must have the following permissions to perform external data integration:

Table 2-39 Permissions for CCS

Tasks	Permissions required
Configuring data systems and data connections.	■ Manage Evidence Definitions ■ Manage Jobs ■ Manage Configuration Settings ■ View Configuration Settings
Asset Correlation	■ Manage Asset Reconciliation Rules ■ View Assets ■ View Asset Reconciliation Rules
Policy compliance	■ View Policies ■ Manage Controls Studio
Reports	■ View Reports ■ View Report templates ■ Generate reports
Viewing and creating Dashboards	■ View all Dashboards, Reports and Job Results ■ 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 2-40 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

Table 2-40 Permissions for external data connections *(continued)*

Tasks	Permissions required
Web Service	■ Appropriate permission based on the binding type used for Web Service. For example, Basic HTTP, WSHTTP, or Basic HTTP(SSL).

Scenario 1: Import external data and view the data in CCS Dashboards without CCS asset correlation

You can import the external data and view the data by using the CCS Dashboards. For the basic Dashboard and panel creation using imported data, you do not have to correlate the external data to the CCS assets.

In such a scenario, you may want to plan the external data integration as follows:

- Identify the source of external data.
  - Do you want to integrate an external system that stores data in .csv files? If yes, then use the CSV connector to import the data into CCS.
  - Do you want to integrate an external system that stores data in databases that support ODBC drivers? If yes, then use the ODBC connector to import the data into CCS.
  - Do you want to integrate an external system that exports data by using APIs? If yes, then use the Web services connector to import the data into CCS.
- Identify the schema that you want to use to process the imported data.
  You can use the existing CCS schema or create new schema to process the imported data. You must map the data fields in the imported data to the CCS schema or the new schema that you create. The association of the data fields to CCS schema ensures that the external data is ready to be consumed by CCS.
- Once the data is imported into CCS, you can generate reports and Dashboards based on the imported data.

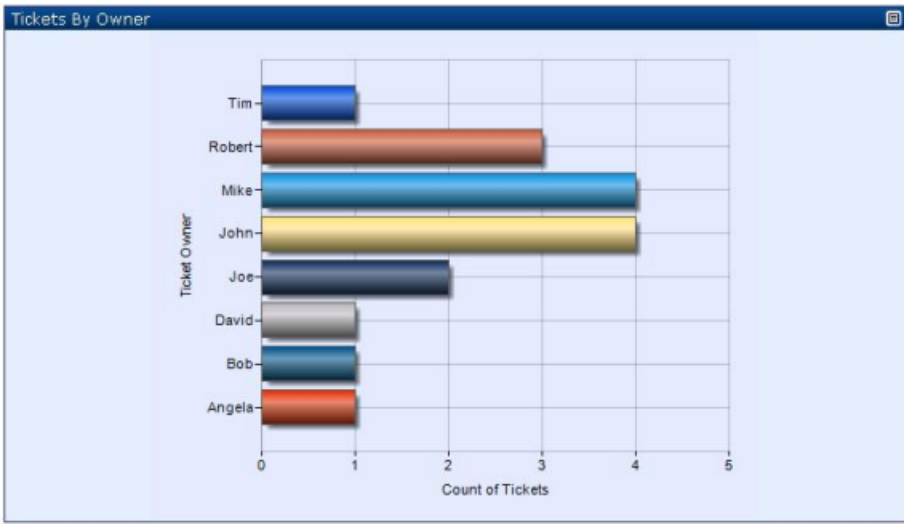
Example of viewing the data in CCS Dashboards without CCS asset correlation

The Asset and Status table shows an example of viewing the data in CCS Dashboards without CCS asset correlation.

Table 2-41 Asset and Status

Asset	Status		
Ticket ID	Ticket Owner	Ticket Owner Email	Ticket Abstract
ID:200125	John	John@galaxy.com	Install IE8
ID:200126	Tim	Tim@galaxy.com	Upgrade Hardware: CCS AM
ID:200127	Robert	Robert@galaxy.com	Install new version of Office
ID:200128	Robert	Robert@galaxy.com	Upgrade OS
ID:200129	Mike	Mike@galaxy.com	Install Office 2007
ID:200130	John	John@galaxy.com	Machine restarts several times
ID:200131	Joe	Joe@galaxy.com	Upgrade Hardware: CCS AM
ID:200132	David	David@galaxy.com	Hardware Failure: Hard Disk
ID:200134	Angela	Angela@galaxy.com	Software Installation:VPN
ID:200135	Bob	Bob@galaxy.com	Machine Configuration- Setup Email Account
ID:200136	John	John@galaxy.com	Install IE8
ID:200138	Robert	Robert@galaxy.com	Upgrade OS
ID:200139	Joe	Joe@galaxy.com	Install Windows Patch
ID:200140	Mike	Mike@galaxy.com	Install Office 2007
ID:200141	John	John@galaxy.com	Install IE8
ID:200142	Mike	Mike@galaxy.com	Install Office 2007
ID:200143	Mike	Mike@galaxy.com	Install Excel 2007

Figure 2-2 Panel - Tickets By Owner



Scenario 2: Import external data and view the data in CCS Dashboards in correlation with the CCS assets

You can import the external data and view the data by using the CCS Dashboards in correlation with the CCS assets. By means of correlation, you basically establish an association between the external assets and the existing CCS assets. For example, if you import data on patch assessment, you can associate the reported patch to an asset and then try to correlate to the CCS assets.

In such a scenario, you may want to plan the external data integration as follows:

- Identify the source of external data.
  - Do you want to import the data using an ODBC connection?
  - Do you want to import the data using a CSV connection?
  - Do you want to create a custom Web services connector for importing data into CCS?
- Identify the schema that you want to use to process the imported data.
  You can use the existing CCS schema or create new schema to process the imported data. You must map the data fields in the imported data to the CCS schema or the new schema that you create. The association of the data fields to CCS schema ensures that the external data is ready to be consumed by CCS.
- Once you have identified the data to be imported, you must specify the Asset-Assessment-Status fields.

For more information on the external data integration, refer to the About external data integration section in the *Symantec™ Control Compliance Suite 10.5.1 User Guide*.

- Once the data is imported into CCS after you establish a correlation, you can generate reports and Dashboards in correlation with the CCS assets.

Example of panel showing external data in correlation with the CCS assets

This section gives an example of CCS Dashboards in correlation with the CCS assets.

The following table shows the external data field mapping of Asset, Assessment, and Status.

Table 2-42 Asset, Assessment, and Status

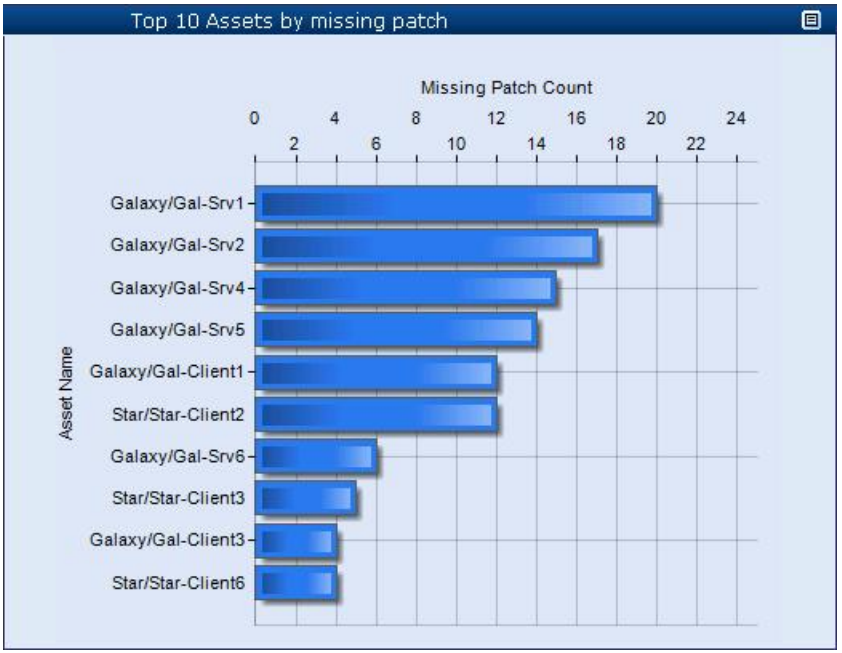
Asset			Assessment		Status
Domain	Machine Name	Operating System	Patch Name	Patch Product Name	Patch Status
Galaxy	Galaxy\Gal-Srv1	Windows Server 2003	WindowsServer2003-SP2-KB941202-x64-ENU.exe	Windows Server 2003, Enterprise Edition	Missing
Galaxy	Galaxy\Gal-Srv1	Windows Server 2003	WindowsServer2003-SP2-KB933729-x64-ENU.exe	Windows Server 2003, Enterprise Edition	Installed
Galaxy	Galaxy\Gal-Srv1	Windows Server 2003	msxml6-KB933579-enu-x86.exe	MSXML 6.0	Missing
Galaxy	Galaxy\Gal-Srv2	Windows Server 2008 R2 Enterprise	office2007-kb936514-fullfile-x86-glb.EXE	Excel 2007	Missing
Galaxy	Galaxy\Gal-Srv2	Windows Server 2008 R2 Enterprise	publisher2007-kb936646-fullfile-x86-glb.exe	Publisher 2007	Missing

Table 2-42 Asset, Assessment, and Status *(continued)*

Asset			Assessment		Status
Galaxy	Galaxy\Gal-Srv2	Windows Server 2003	WindowsServer2003-SP2-KB936782-x64-ENU.exe	Windows Server 2003, Enterprise Edition	Effectively Installed
Galaxy	Galaxy\Gal-Client1	Windows XP Professional	WindowsXP-SP2-KB893756-x86-ENU.exe	Windows XP Professional	Missing
Star	Star\Star-Client1	Windows XP Professional	office2003-kb873378-fullfile-enu.exe	Office 2003	Installed
Star	Star\Star-Client1	Windows XP Professional	WindowsMedia9-KB917734-x86-ENU.exe	Windows Media Player 9.0	Effectively Installed
Star	Star\Star-Client1	Windows XP Professional	WindowsXP-SP2-KB893756-x86-ENU.exe	Windows XP Professional	Missing
Star	Star\Star-Client2	Windows XP Professional	office2003-kb873378-fullfile-enu.exe	Office 2003	Missing

Note: The columns are grouped based on the field mapping of Asset, Assessment, and Status.

Figure 2-3 Panel showing external data in correlation with CCS assets



Scenario 3: Import external data and use it for policy compliance

You can import the external data and use the data for policy compliance calculation in correlation with the CCS assets. By means of correlation, you basically establish an association between the external assets and the existing CCS assets. For example, if you import data on patch assessment, you can associate the reported patch to an asset and then try to correlate to the CCS assets.

In such a scenario, you may want to plan the external data integration as follows:

- Identify the source of external data.
  - Do you want to import the data using an ODBC connection?
  - Do you want to import the data using a CSV connection?
  - Do you want to create a custom Web services connector for importing data into CCS?
- Identify the schema that you want to use to process the imported data.
  You can use the existing CCS schema or create new schema to process the imported data. You must map the data fields in the imported data to the CCS

schema or the new schema that you create. The association of the data fields to CCS schema ensures that the external data is ready to be consumed by CCS.

- Once you have identified the data to be imported, you must specify the Asset-Assessment-Status fields.
  For more information on the external data integration, refer to the About external data integration section in the *Symantec™ Control Compliance Suite 10.5.1 User Guide*.
- Once the data is imported into CCS in correlation with the CCS assets, you can use the imported data to evaluate policy compliance.
  In order to consume the external data for compliance evaluation, you must do the following:
  - Map the imported data with CCS policies or regulations through control statement mapping.
  - Map the imported data fields to the CCS result attributes such as Pass, Fail, Unknown, or N/A.

  For more information on the compliance score, refer to the Policy compliance in correlation with CCS assets section in the *Symantec™ Control Compliance Suite 10.5.1 User Guide*.

Example of policy compliance using external data

This section gives an example of the policy compliance with CCS asset correlation.

The following table shows the external data field mapping of Asset, Assessment, and Status.

Table 2-43 Asset, Assessment, and Status

Asset			Assessment		Status
Domain	Machine Name	Operating System	Patch Name	Patch Product Name	Patch Status
Galaxy	Galaxy\Gal-Srv1	Windows Server 2003	WindowsServer2003-SP2-KB941202-x64-ENU.exe	Windows Server 2003, Enterprise Edition	Missing

Table 2-43 Asset, Assessment, and Status *(continued)*

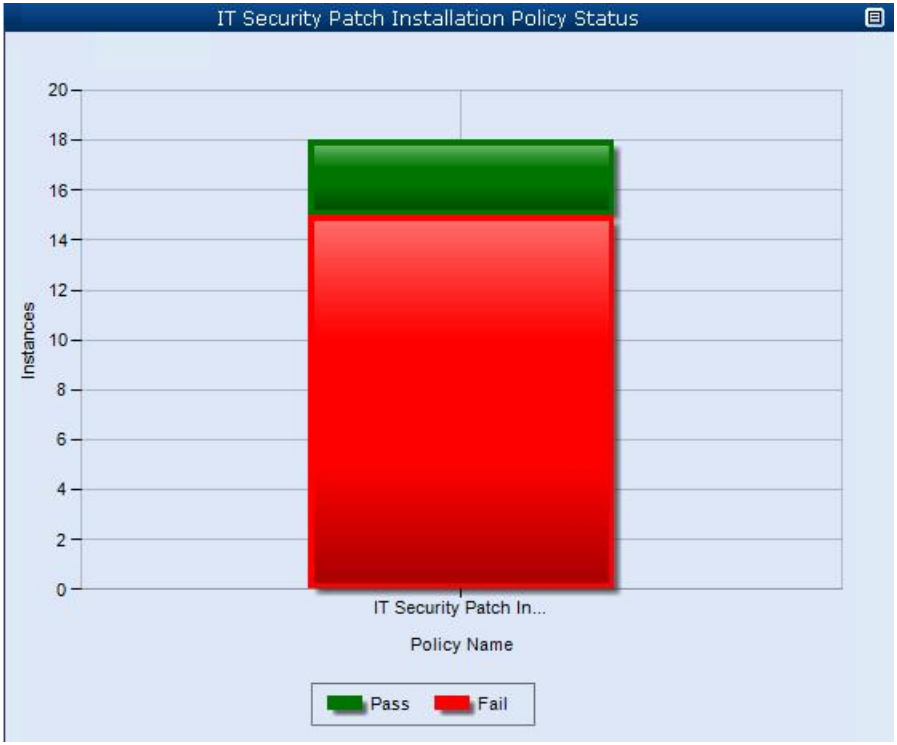
Asset			Assessment		Status
Galaxy	Galaxy\Gal-Srv1	Windows Server 2003	WindowsServer2003-SP2-KB933729-x64-ENU.exe	Windows Server 2003, Enterprise Edition	Installed
Galaxy	Galaxy\Gal-Srv1	Windows Server 2003	msxml6-KB933579-enu-x86.exe	MSXML 6.0	Missing
Galaxy	Galaxy\Gal-Srv2	Windows Server 2008 R2 Enterprise	office2007-kb936514-fullfile-x86-glb.EXE	Excel 2007	Missing
Galaxy	Galaxy\Gal-Srv2	Windows Server 2008 R2 Enterprise	publisher2007-kb936646-fullfile-x86-glb.exe	Publisher 2007	Missing
Galaxy	Galaxy\Gal-Srv2	Windows Server 2003	WindowsServer2003-SP2-KB936782-x64-ENU.exe	Windows Server 2003, Enterprise Edition	Effectively Installed
Galaxy	Galaxy\Gal-Client1	Windows XP Professional	WindowsXP-SP2-KB893756-x86-ENU.exe	Windows XP Professional	Missing
Star	Star\Star-Client1	Windows XP Professional	office2003-kb873378-fullfile-enu.exe	Office 2003	Installed
Star	Star\Star-Client1	Windows XP Professional	WindowsMedia9-KB917734-x86-ENU.exe	Windows Media Player 9.0	Effectively Installed
Star	Star\Star-Client1	Windows XP Professional	WindowsXP-SP2-KB893756-x86-ENU.exe	Windows XP Professional	Missing
Star	Star\Star-Client2	Windows XP Professional	office2003-kb873378-fullfile-enu.exe	Office 2003	Missing

Note: The columns are group based on the field mapping of Asset, Assessment, and Status.

You can create an assessment procedure to check if an asset has all the required patches installed, which can be mapped to a policy through a control statement.

Once the data is imported into CCS after you establish a correlation, you can generate reports and Dashboards in correlation with the CCS assets.

Figure 2-4 Example using external data for policy compliance



Scenario 4: Import external data and use it for contributing to the CCS asset risk score

You can import external data and use it for contributing to the CCS asset risk score by using the CVSS algorithm or custom risk score field.

In such a scenario, you may want to plan the external data integration as follows:

- Identify the source of external data
  - Do you want to import the data using an ODBC connection?
  - Do you want to import the data using a CSV connection?

- Do you want to create a custom Web services connector for importing data into CCS?

- Identify the schema that you want to use to process the imported data.
  You can use the existing CCS schema or create new schema to process the imported data. You must map the data fields in the imported data to the CCS schema or the new schema that you create. The association of the data fields to CCS schema ensures that the external data is ready to be consumed by CCS.
- Once you have identified the data to be imported, you must specify the Asset-Assessment-Status fields.
  For more information on the external data integration, refer to the About external data integration section in the *Symantec™ Control Compliance Suite 10.5.1 User Guide*.
- Once the data is imported into CCS after you establish a correlation, you can generate reports and Dashboards in correlation with the CCS assets.
  For more information on the external data integration, refer to the About external data integration section in the *Symantec™ Control Compliance Suite 10.5.1 User Guide*.
- Specify the parameters for risk aggregation for the imported data in correlation with the CCS assets. You can specify the values for risk score aggregation from **Manage** > **External Data Integration** > **Set Asset Risk Aggregation**.
  For more information on the risk score aggregation, refer to the Contributing to the CCS asset Risk Score section in the *Symantec™ Control Compliance Suite 10.5.1 User Guide*.

How to achieve your business objectives with external data integration

After you have identified the business objectives for external data integration, you need to perform certain tasks to meet those objectives.

To elaborate on the required actions, let us take the example of the use-case scenarios to elaborate on the implementation of the external data integration.

Table 2-44 External data integration model based on your business objective

Scenario	Description	What you need to do
Import external data and view the data in CCS Dashboards without correlating to the CCS assets See "Scenario 1: Import external data and view the data in CCS Dashboards without CCS asset correlation" on page 118.	You can import the external data and view the data by using the CCS Dashboards. For the basic Dashboard and panel creation using imported data, you do not need to correlate the external data to the CCS assets.	To meet this business goal, you need to do the following: ■ Identify the asset and the status fields for the external data and map the data field to the existing CCS data schema or custom data schema. ■ Identify the Key Performance Indicators (KPIs) that you want to use to monitor the data and subsequently to create the panels.

Import external data and view the data in CCS Dashboards in correlation with the CCS assets.
 	
See "Scenario 2: Import external data and view the data in CCS Dashboards in correlation with the CCS assets" on page 120.
	You can import the external data and view the data by using the CCS Dashboards in correlation with the CCS assets. By means of correlation, you basically establish an association between the external assets and the existing CCS assets.	To meet this business goal, you need to do the following:
		■ Identify the key fields for the following attributes in the external data:
		  ■ Asset
		  ■ Status
		■ Once you have identified the mentioned fields, you must map the fields to the existing CCS data schema or a custom data schema.
		■ Identify and map the fields that you want to use to correlate the data to the assets.
		■ Identify the asset-based KPIs that you want to use to monitor the data and subsequently to create the panels.

Table 2-44 External data integration model based on your business objective *(continued)*

Scenario	Description	What you need to do

Import external data and use it for policy compliance
 	
See "Scenario 3: Import external data and use it for policy compliance" on page 123.
	You can import the external data and use the data for policy compliance calculation in correlation with the CCS assets. By means of correlation, you basically establish an association between the external assets and the existing CCS assets.	To meet this business goal, you need to do the following:
		■ Identify the key fields for the following attributes in the external data:
		  ■ Asset
		  ■ Assessment
		  ■ Status
		■ Map the identified data fields in the external data to the existing CCS data schema or a custom data schema.
		■ Identify the possible result values in the external data and map the values to the CCS result attributes.
		■ Based on the mandates that you want to comply to, decide if the existing assessments are sufficient or you need to create new assessment procedures.
		■ Based on the mandates that you want to comply to, decide if the existing control statements are sufficient or you need to create new ones.

Table 2-44 External data integration model based on your business objective *(continued)*

Scenario	Description	What you need to do

Import external data and use it for contributing to the CCS asset risk score
 	
See "Scenario 4: Import external data and use it for contributing to the CCS asset risk score" on page 126.
	You can import the external data and use the data for risk score calculation in correlation with the CCS assets. You can use the imported data to correlate with the CCS assets and then calculate the risk score of the assets based on CVSS attributes and the risk score that is defined in the external data.	To meet this business goal, you need to do the following:
		■ Identify the key fields for the following attributes in the external data:
		  ■ Asset
		  ■ Assessment
		  ■ Status
		■ Once you have identified the mentioned fields, you must map the fields to the existing CCS data schema or a custom data schema.
		■ Identify and map the fields in the external data that you want to correlate to the assets.
		■ Identify and map the result fields in the external data that you want to correlate to the CCS result attributes.
		■ Decide if you want to use CVSS attributes to calculate the risk score or you want to use the existing risk score of the external data.
		■ Specify a value for the weight to be used in the risk score calculation.
		■ Decide if you want to use the risk score in the external data to calculate the asset risk aggregation in CCS.

Planning for the Symantec CCS Vulnerability Manager integration

CCS VM integration lets you seamlessly assimilate the vulnerability assessment data from Symantec CCS Vulnerability Manager into CCS. It lets you represent the imported data by leveraging the CCS Dashboards and reports.

Before you integrate the Symantec CCS Vulnerability Manager and import data into CCS, you must do the following:

- Create a data connection to Symantec CCS Vulnerability Manager
- Configure reconciliation rules to add the imported assets to the CCS system.
- Set asset risk aggregation.

Note: The Symantec CCS Vulnerability Manager data connection uses the CCS Vulnerability Manager Web service reporting API to connect to the Symantec CCS Vulnerability Manager server.

See "Prerequisites for the Symantec CCS Vulnerability Manager connection" on page 131.

See "Permissions required for the Symantec CCS Vulnerability Manager connection" on page 131.

Prerequisites for the Symantec CCS Vulnerability Manager connection

Before you add the Symantec CCS Vulnerability Manager data connection, you must do the following:

- Install and configure Symantec CCS Vulnerability Manager v10.0.
- Install and configure CCS.

Note: You must select the External Data Connector Service role while registering a new CCS Manager after CCS installation.

Permissions required for the Symantec CCS Vulnerability Manager connection

The user account that is used for data connection must have the following permissions in CCS Vulnerability Manager:

- View sites
- View asset groups

- Import sites
- Import asset groups
- Manage reports

See "Permissions required for External Data Integration" on page 117.

Planning for the Symantec Data Loss Prevention integration

The Symantec Data Loss Prevention integration lets you seamlessly import incident data from Symantec Data Loss Prevention(DLP) into CCS. It allows you to represent the imported data in Dashboards and reports by leveraging the CCS features.

Before you import the incident data in CCS using the pre-integrated DLP data system, you must do the following:

- Create a data connection to Symantec Data Loss Prevention.
- Configure reconciliation rules to add the imported incident data to the CCS data system.
- Map the Symantec DLP statuses to CCS statuses.

See "Requirements for the Symantec Data Loss Prevention Incidents connection" on page 132.

See "Permissions required for the Symantec Data Loss Prevention Incidents connection" on page 132.

Requirements for the Symantec Data Loss Prevention Incidents connection

Before you add the Data Loss Prevention data connection, you must do the following:

- Install and configure the Symantec Data Loss Prevention any version from 10.0 to 11.6.0.19033.
- Install and configure CCS.

Note: You must select the External Data Connector Service role while registering a new CCS Manager after CCS installation.

Permissions required for the Symantec Data Loss Prevention Incidents connection

The user account that you configure for the Symantec Data Loss Prevention Incidents connection must have the Reporting API Web Service access permission on Symantec Data Loss Prevention.

See "Permissions required for External Data Integration" on page 117.

Planning for the Symantec CCS Assessment Manager integration

AM integration lets you seamlessly assimilate the assessment data from Symantec CCS Assessment Manager (AM) into CCS. It lets you represents the imported data by leveraging the CCS Dashboards and reports.

Before you integrate the Symantec CCS Assessment Manager and import data by using ODBC data connector, you must create a data connection to Symantec CCS Assessment Manager.

See "Requirements for the AM connection" on page 133.

See "Permissions required for the Symantec CCS Assessment Manager connection" on page 133.

Requirements for the AM connection

Before you add the Symantec CCS Assessment Manager data connection, you must do the following:

- Install and configure the Symantec CCS Assessment Manager v11.1.
- Install and configure CCS.

Note: You must select the External Data Connector Service role while registering a new CCS Manager after CCS installation.

Permissions required for the Symantec CCS Assessment Manager connection

The user account that is used for data connection must have the view permissions to Symantec CCS Assessment Manager database view, RAM.CCS Evidence.

See "Permissions required for External Data Integration" on page 117.

About installing the CCS PowerShell snap-ins

The CCS PowerShell snap-ins extend the functionality of the Windows PowerShell for the CCS users. You can integrate the CCS PowerShell snap-ins within your business processes to achieve the various functionalities in CCS. For example, assets management, standards management. You can install the CCS PowerShell snap-ins on a computer other than the CCS Application Server. You can run the CCS PowerShell cmdlets on the command-line interface (CLI) with a minimal scripting knowledge.

The CCS already provides the flexibility to the third-party clients to integrate the core functionality of CCS within their own business processes. To serve the purpose, all the application modules in the CCS expose their core functionality to the third-party clients through a set of APIs. In addition, the CCS 11.1 provides the CCS PowerShell snap-ins to automate the CCS tasks. For instance, creating a collection-evaluation job for a specific asset is possible through CLI without navigating to the CCS Console.

Prerequisites for installing CCS PowerShell snap-ins

The prerequisites of the CCS PowerShell snap-ins installation are as follows:

Table 2-45 CCS PowerShell snap-ins installation requirements

Component name	Required operating system	Other requirements
CCS PowerShell snap-ins	Windows XP Professional SP2 and above Windows Vista SP1 and above Windows 7 Windows Server 2008 Windows Server 2012 Windows Server 2012 R2	Administrator or equivalent user privileges Microsoft .Net Framework 3.5 SP1 Microsoft Windows PowerShell 2.0 **Note:** To view the instructions to download and install Windows PowerShell 2.0, you can visit the following URL: http://support.microsoft.com/kb/968929

Installing CCS PowerShell snap-ins

Before installing CCS PowerShell snap-ins, you must ensure that your computer meets the recommended system requirements.

Note: The CCS PowerShell snap-ins are registered internally on Windows PowerShell during snap-ins installation and are unregistered during snap-ins uninstallation.

See "Prerequisites for installing CCS PowerShell snap-ins" on page 134.

To install CCS PowerShell snap-ins

1. Insert the CCS product disc into the computer drive.

   Navigate to the InstallSet\Tools\CCS PowerShell Snap-ins folder of the media structure.

2. Click **CCS PowerShell Snap-ins.exe**.

3. In the **Welcome** panel of the **Symantec Control Compliance Suite PowerShell Snap-ins Setup** Installation Wizard, click **Next**.

4. In the **End-User License Agreement** panel, read the license agreement and select **I accept the terms in the License Agreement** to accept the terms of the end-user license agreement. Click **Next** to continue.

5. In the **Destination Folder** panel, click **Next** to install the CCS PowerShell snap-ins to the default folder or click **Browse** to choose another folder.

6. In the **Ready to install Symantec CCS PowerShell Snap-ins** panel, click **Install** to begin the installation.

   The Installing **Symantec CCS PowerShell Snap-ins** panel indicates the progress of the installation.

7. In the **Finish** panel, click **Finish** to exit the wizard.

Adding CCS PowerShell snap-ins

After installing CCS PowerShell snap-ins, you must ensure that CCS PowerShell snap-ins are added to Windows PowerShell for the particular session.

See "Installing CCS PowerShell snap-ins" on page 134.

To add CCS PowerShell snap-ins

1. Open the Windows PowerShell command-line interface.

2. To get a list of snap-ins that are registered on your computer, execute the command `Get-PSSnapin -reg;.`

   The list of all the registered snap-ins along with CCS snap-ins is displayed.

3. Execute the following CCS PowerShell snap-in commands:

   - `Add-PSSnapin Symantec.CSM.PS.Standards.SnapIn`
   - `Add-PSSnapin Symantec.CSM.PS.Assets.SnapIn`
   - `Add-PSSnapin Symantec.CSM.PS.Tags.SnapIn`
   - `Add-PSSnapin Symantec.CSM.PS.JobManager.SnapIn`
   - `Add-PSSnapin Symantec.CSM.PS.Shared.SnapIn`

- `Add-PSSnapin Symantec.CSM.PS.Exceptions.SnapIn`

4 Specify the values for AppserverNameAndPort values and Binding Type that are set for the current session.

For instance,

- $AppServerNameAndPort = <appservername: port>
- $BindingType = nettcp

You can start using the CCS PowerShell cmdlets.

Note: The Remove-PSSnapin cmdlet removes a Windows PowerShell snap-in from the current session. You can use it to remove snap-ins that you have added to Windows PowerShell.

About internationalization and localization

In CCS 11.1, internationalization (I18N) and localization (L10N) support is provided to the following features:

Table 2-46 Internationalization and localization support

Support	Features
Internationalization	All
Localization	The following features are localized: ■ Installer ■ Regulatory Content ■ Standards Content ■ Reporting and Dynamic Dashboards ■ Risk management ■ Policy Publishing and Workflows **Note:** Localization for the legacy ESM components such as ESM Console, ESM Utilities and so on is still supported in Japanese. However, if the base release of CCS 11.1 is in a different language other than Japanese then the language of ESM Console and Manager is English.

Table 2-46 Internationalization and localization support *(continued)*

Support	Features
Multi-lingual support	The following features have multi-lingual support: ■ Risk Manager ■ Dynamic Dashboards ■ Policy Publishing and Workflows Multilingual User Interface (MUI) lets you select your preferred display language. For example, in case of Web application, you can change the browser language settings to German and view the CCS Web portal in German language, provided, you have German language pack installed on the computer. You may change the browser language to French, and see the UI in French language once the page is reloaded, if the French language pack is installed on that computer.

Note: Controls Studio and Certificate Management, Policy Manager in Windows Console, and CCS Agent and CCS Agent Registration utility are not localized. These components are in English language. Although, CCS Console is not localized, the language-specific formatting such as date and time formats and localized data input is supported on the Console.

The base release of CCS 11.1 is in the United States English language (en-us) however CCS is also available in the following languages:

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

In non-English installation, the language of the base language determines the language of the installer.

See "About installation and configuration in locale setups" on page 138.

About installation and configuration in locale setups

You can install CCS in the supported languages also known as the base language of installation. All CCS Components are registered in the same base language. During installation and configuration, a language parameter is added to the Active Directory Application Mode (ADAM), which is then used by the CCS Application Server to update the CCS managers and all other components with this parameter. In addition, you can install multiple language packs on the same computer to view CCS Web portal in that language.

You cannot install the following on a computer that contains extended ASCII characters in the host name and an operating system other than English:

- Application Server
- CCS agent
- Windows and UNIX asset type

Note: Upgrade is not supported for CCS L10N.

Product documentation

CCS 11.1 product documentation is localized in the following languages:

- French
- German
- Japanese
- Korean
- Simplified Chinese
- Spanish

See “About internationalization and localization” on page 136.

Chapter 3

Deploying CCS

This chapter includes the following topics:

CCS Suite deployment sequence

CCS deployment involves installation and configuration of multiple components. For proper deployment of CCS, these installation and configuration related tasks must be performed in a certain sequence.

The following tasks must be performed for deploying CCS:

- Install and configure the CCS components
- Configure credentials for asset import and data collection
- Import assets into CCS
- Configure routing rules to route CCS jobs based on your network environment
- Check the health status of all CCS components

For an example scenario and detailed procedure on deploying CCS for the first time, see the *Symantec™ Control Compliance Suite Quick Start Guide for fresh installation*.

Collecting data from other platforms

If you want to collect raw-data from VMware or Exchange platforms, install and configure the RMS Information Server and BV-Controls for the respective platforms. For information on installing and configuring RMS Information Server and BV-Controls, see the *Symantec Control Compliance Suite Installation Guide version 10.5*.

Perform the following additional steps:

- Configure the CCS Manager for data collection from VMware or Exchange platforms. See the *Configuring data collectors* section in the *Symantec™ Control Compliance Suite User Guide*.
- Install CCS content for VMware and Exchange.
  See "Installing the CCS Content" on page 219.

Installing the CCS Suite

You can install the CCS Manager and the CCS Application Server on a single computer. For a scale-out deployment, you can install the CCS Application Server on one computer and keep adding one more CCS Managers on other computers as per your sizing requirements. Installing more than one CCS Manager is conducive for load sharing and provides better scalability.

If you install the CCS Manager along with the CCS Application Server, using the CCS Suite installer, by default, that CCS Manager is registered in the System Topology in the CCS Console and all roles are assigned to that CCS Manager.

Note: You can install a CCS Application Server and CCS Agent on a single computer, but you cannot install a CCS Manager and a CCS Agent on a single computer. Therefore, you cannot install a CCS Manager along with the CCS Application Server on a computer that contains a CCS Agent.

Control Compliance Suite makes available a set of predefined Technical Standards, Frameworks and Regulations. The CCS Suite installer installs content for the following Technical Standards and Regulations by default:

CCS Suite installer installs content for the following Technical Standards by default:

- CIS Benchmark v1.1.2 for Red Hat Enterprise Linux 6.x
- CIS Oracle Database Server 11g Security Benchmark v1.0.1
- CIS Security Configuration Benchmark For Microsoft Windows Server 2012 v1.0.0
- Security Essentials for Microsoft SQL Server 2012

CCS Suite installer installs content for the following Regulations by default:

- COBIT 5th Edition
- PCI DSS v3.0
- IT Control Objectives for Sarbanes-Oxley 2nd Edition
- HIPAA HHS 45 CFR Part 164 Subpart C

You can install more content using the CCS Content installer. See "Installing the CCS Content" on page 219.

See the following sections before installing the CCS Suite:

See "Hardware and operating system requirements" on page 37.

See "Network Ports" on page 41.

See "Software requirements" on page 48.

See "User Privileges for deploying the CCS components" on page 55.

See "User privileges for SQL server and CCS databases" on page 60.

The CCS Suite installs the following components:

- CCS Application Server
- CCS Manager

Do the following to install the CCS components:

- Launch the Installation Wizard
  See "To launch the Installation Wizard" on page 142.
- Install the CCS Suite
  See "To install the CCS Suite" on page 142.
- Provide details to install components and databases
  See "To provide details for installing the components and databases" on page 144.

Note: The installer places a copy of the installation files in the media cache folder. On the Windows Server 2003 computers, the media cache is in the folder, C:\Documents and Settings\All Users\Application Data\Symantec\CSM-RA\MediaCache.On the Windows Server 2008 and Windows Server 2012 computers, the media cache is in the folder, C:\ProgramData\Symantec\CSM-RA\MediaCache. These files require approximately 1.2 GB disk space.

To launch the Installation Wizard

1. Insert the **Symantec Control Compliance Suite 11.1** product disc into the drive on your computer and double-click **Setup.exe**.

   In the security warning dialog box, click **Run**.
2. In the DemoShield, click **CCS Suite**.
3. On the splash screen, click **Install CCS Suite**. The Setup file is located inside the CCS_Reporting folder of the product media.

   Setup prepares the CCS Suite installation wizard and prompts to install any prerequisites, if required. During the prerequisite installation, if the computer prompts you to restart, restart the computer and launch the setup again.

   See "Software requirements" on page 48.

To install the CCS Suite

1. In the **Welcome** panel of the launched Symantec Control Compliance Suite 11.1 installation wizard, read and accept the license agreement, and then click **Next**.

   The Product Improvement Program is enabled by default. The Product Improvement Program does not collect any personally identifiable data and the participation is optional. If you do not want to share the data with Symantec, then you must opt-out of the program. To opt-out of the product improvement program, uncheck **I agree to participate in the Product Improvement Program by sharing the installation and product usage information with**

Symantec. To opt-out of the product improvement program later, on the CCS Console, go to **Settings > General > Product Improvement Program** and uncheck **Share installation and product usage information with Symantec**. For more information about the product improvement program, See "Product Improvement Program" on page 156.

2 In the **Components** panel, by default the CCS Manager is selected. You can install both CCS Application Server and CCS Manager, on a single computer. Uncheck **CCS Manager** if you do not want to install CCS Manager on this computer. To install a standalone CCS Manager for a scale-out deployment, See "Installing a standalone CCS Manager for a scale out deployment of CCS" on page 169.

3 Click **Next**.

4 In the **Licensing** panel, click **Add Licenses** to add licenses for the components that require mandatory licenses to install. You can add more licenses later using the CCS Console.The CCS Core license is required to install the CCS Application Server and the CCS Maintenance license is required to install the default CCS Content during the CCS installation.

See "About licensing of the product components" on page 158.

5 Click **Next**.

6 In the **Prerequisites** panel, review the prerequisites that are required for the installation. Install any prerequisite application that is required to be installed. Click **Check again** to verify whether the installation is successful.

See "Software requirements" on page 48.

7 Click **Next**.

8 In the **Installation Folder** panel, review the installation path for product installation.

Click browse (**...**) to specify a different installation path to install the product.

You can change the default location of the Installation files cache folder where the setup files that are cached during installation. Click browse (**...**) to select a different location to store the setup files.

Click **Refresh disk space information** to verify the available disk space on the computer.

9 Click **Next**. If you have specified a different installation path, and the installer folder does not exist, the installer prompts you to create the installation folder.

To provide details for installing the components and databases

1. In the launched **Symantec Control Compliance Suite 11.1** installation wizard, perform steps 1 to 9
2. In the **CCS Application Server - Root Certificate** panel, enter the required values for the fields to create the root certificate and then click **Next**.

   The root certificate is required for secure communication between CCS Application Server and CCS Manager. The root certificate is created on the CCS Application Server and contains the details that are used to create certificates for the CCS Manager. You must generate certificates for all CCS Manager installations. The root certificate is created using the CCS Installation Wizard during the installation of the product.

   The certificates that are deployed on the CCS Managers are created using the **Certificate Management Console**. The **Certificate Management Console** is installed on the CCS Application Server computer.

   See "Creating a certificate for installing a standalone CCS Manager" on page 167.

   The fields for the **CCS Application Server - Root Certificate** panel and their description is as follows:

Organization	The name of your organization.
Expiration term (years)	The expiration time period of the root certificate. The expiration time period of the root certificate must be more than 10 years.
Password (Min. 8 char.)	The password to authenticate the certificate.
Re-type password	Re-enter the password that you have typed.

Signature Algorithm	The Secure Hash Algorithm (SHA) that is required to create the certificates that use the cryptographic hash functions. The following hash functions are used in CCS: ■ sha1RSA ■ sha256RSA ■ sha384RSA ■ sha512RSA **Note:** On the Windows Server 2003 computers, the sha256RSA or higher encryption algorithm appears in the drop-down list only if the computer is configured with sha256RSA or higher encryption capability.
Key Size	The key that is associated with a signature algorithm. The key sizes are, 2048, 3072, and 4096.

Note: Ensure that computers having the CCS Application Server and CCS Managers support the Signature Algorithm and Key Size.

3 In the **CCS Application Server - Directory Service Configuration** panel, enter the required values for the fields and then click **Next**.

The fields for the **CCS Application Server - Directory Service Configuration** panel and their description is as follows:

User name	Enter the user name in whose context the Directory Service is run on the computer. The user must be a domain user. Or click browse (**...**) to select the user name.
Password	Enter the password that authenticates the specified user account.
Use the same user account for Application Server	Check this option if you want to reuse the same user account for configuring the CCS Application Server.
Directory Service port	Enter the port number of the computer that hosts the CCS Application Server on which the Directory Service runs. By default, the port in which the Directory Service runs is, 12467.
Encryption Management Service port	Enter the port number of the computer that hosts the CCS Application Server on which the Encryption Management Service runs. By default, the port in which the Encryption Management Service runs is, 12468.
LDAP port	Enter the LDAP port number of the computer that hosts the CCS Application Server. By default, the Directory Service uses the port 3890 to communicate with the CCS Application Server.
SSL port	Enter the SSL port number of the computer that hosts the CCS Application Server. By default, the Directory Service uses the SSL port 6360 to communicate with the CCS Application Server.
Data Files	Click browse (**...**) to change the location where you want to store the data files, which contain the Directory information.

When you install the CCS Application Server on a domain controller or on any other computer on which the Active Directory is installed, the default port numbers for LDAP is 3890 and for SSL is 6360.

4 In the **CCS Application Server - Encryption Management Service Pass Phrase** panel, enter the pass phrase that is used to generate the symmetric keys and click **Next**.

The Encryption Management Service uses the symmetric keys generated by the pass phrase to encrypt and decrypt configuration information, including passwords and connection details.

The pass phrase must be minimum 8 characters long.

Note: You require this pass phrase later to change the service user account, and to make changes to the installation.

See "About the pass phrase" on page 159.

5 In the **Application Server - Service Configuration** panel, enter the required values in the text boxes and click **Next**.

The fields of the **Application Server - Service Configuration** panel and their descriptions are as follows:

User name	Enter the user name in whose context the Application Server Service is run on the computer. The user must be a domain user. Or click browse (**...**) to select the user name. You can reuse the Directory Service user account This field is available only if you uncheck **Use the same user account for Application Server** in the **CCS Application Server - Directory Service Configuration** panel.
Password	Enter the password that authenticates the specified user account.
Application server port	Enter the port number of the computer on which the Application Server Service runs. The Application Server Service runs on the computer on which the Application Server is installed. By default, the port number is, 1431.
Application server integration service port	Enter the port number of the computer on which the Application Server Integration Services run. The Application Server Integration Services is required for the Integration Services APIs and runs on the Application Server computer. By default, the service runs in the HTTPS port, whose number is, 12431. You can also configure the Integration Services to run in the TCP port or the HTTP port. The default HTTP port is 80 and the default TCP port is 1431.

IIS site for Web Console	Select the IIS site that launches the CCS Web Console. The IIS site is required because the Application Server and the Web Console are installed on the same computer. By default, you can use the Default website, which is configured for the IIS Manager that is installed on the Application Server computer. Alternatively, you can specify a custom website to launch the CCS Web Console. Symantec recommends to use an IIS site that accepts only HTTPS connections. If you use SSL connections, you must configure them before you install CCS. For information about configuring SSL connections, see the Microsoft SQL Server documentation at the following location: http://support.microsoft.com/kb/316898
IIS site for Symantec Help	Select the IIS site that launches the Symantec Help. The IIS site is required because the Application Server and the Symantec Help are installed on the same computer. The IIS site is also used to launch the Symantec Help on the remote computer. By default, you can use the Default website, which is configured for the IIS Manager that is installed on the Application Server computer. Alternatively, you can specify a custom website to launch the Symantec Help.
Target path for Symantec Help	Specify the location for the Symantec Help installation. You can accept the default location, or type a path, or click browse (**...**) to select a new location. You require minimum 30 MB disk space for Symantec Help installation.

Click **Yes** in the SSL recommendation dialog box to proceed with the installation.

To know the special characters that are supported to create the user account for CCS.

See “About using special characters in credentials” on page 159.

6 In the **Application Server - Production Database** panel, enter the required values in the text boxes and click **Next**.

The SQL server is used to create the production database on the Application Server computer that stores data, which is queried by the data collectors. The production database must be configured to use the Windows authentication.

By default, the setup creates a production database, CSM_DB on the computer. If the user account that you specify to log in to the SQL Server, does not have the required privileges to create the database, the setup will not create the database. In this case, you must create the CSM_DB database, and then run the CCS Suite installer.

See "Recommendations for manual creation of databases" on page 159.

See "User privileges for SQL server and CCS databases" on page 60.

The fields of the **Application Server - Production Database** panel and their descriptions are as follows:

SQL Server	Enter the computer name that hosts the SQL server. `SQL\Instancename,port` For example, `CCSSQL\Instance1`. Or click browse (**...**) to locate the SQL Server. Computer names must 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
Use SSL	By default, this option is checked. You must have the required SSL certificate for establishing secured communication. If you use SSL connections, you must configure them before you install CCS. Refer to the Microsoft SQL Server documentation, http://support.microsoft.com/kb/316898 for information about configuring SSL connections.
Use Windows NT Integrated Security	Select this option if you have the SQL server installed in the Windows NT Authentication user context.

Use a SQL user name and password	Select this option if you have the SQL server installed in the SQL Authentication user context. You must specify the authentication details of the user in the respective text boxes.
Use the same configuration for the reporting database	Check this option if you want to replicate the same configuration for the Reporting Server. By default, this option is checked, which does not invoke the panel, Application Server - Reporting Database on clicking Next. You can uncheck this option to invoke the panel in step 7. If you check this option, the setup creates a reporting database, CSM_Reports on the computer. If the user account that you specify to log in to the SQL Server, does not have the required privileges to create the database, the setup will not create the database. In this case, you must create the CSM_Reports database, and then run the CCS Suite installer.

7 The **Application Server - Reporting Database** panel is available only if you have unchecked **Use the same configuration for the reporting database** in step 6

In the **Application Server - Reporting Database** panel, enter the requisite values in the text boxes and click **Next**.

The SQL server information is used to create the reporting database for the Reporting Server. The reporting database is used to store the reports that are generated for the evaluated data. You can choose either Windows or SQL authentication modes to connect to the SQL server.

By default, the setup creates a reporting database, CSM_Reports on the computer. If the user account that you specify to log in to the SQL Server, does not have the required privileges to create the database, the setup will not create the database. In this case, you must create the CSM_Reports database, and then run the CCS Suite installer.

See "Recommendations for manual creation of databases" on page 159.

See "User privileges for SQL server and CCS databases" on page 60.

The fields of the **Application Server - Reporting Database** panel and their descriptions are as follows:

SQL Server

Enter the computer name that hosts the SQL server.

`SQL\Instancename,port`

For example, `CCSSQL\Instance1`.

Or click browse (**...**) to locate the SQL Server.

Computer names must 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

Use SSL

By default, this option is checked.

You must have the required SSL certificate for establishing secured communication.

If you use SSL connections, you must configure them before you install CCS.

Refer to the Microsoft SQL Server documentation, http://support.microsoft.com/kb/316898 for information about configuring SSL connections.

Use Windows NT Integrated Security	Select this option if you have the SQL server installed in the Windows NT Authentication user context.
Use a SQL user name and password	Select this option if you have the SQL server installed in the SQL Authentication user context. You must specify the authentication details of the user in the respective text boxes.

8 In the **CCS Application Server - Pass Phrase** panel, enter the pass phrase that is used to generate the symmetric keys and then click **Next**.

The Application Server Service uses the symmetric keys generated by the pass phrase to encrypt and decrypt configuration information, including passwords and connection details.

The pass phrase must be minimum 8 characters long.

Note: You require this pass phrase later to change the service user account, and to make changes to the installation.

---

9 The **CCS Manager - Service Configuration** panel is available on if you are installing the CCS Application Server and CCS Manager on a single computer and you have checked **CCS Manager** in the **Components** panel.

In the **CCS Manager - Service Configuration** panel, enter a port for the CCS Manager and then click **Next**.

CCS components use this port to communicate with the CCS Manager. The default port is 5600.

10 In the **Summary** panel, review the installation details and click **Install**.

You can click the link, **Export Summary** to export the configuration details of all the components that are installed on the computer. The details appear in a browser, after you specify the location to export the summary.

11 The **Install** panel indicates the progress of the component installation. After the installation finishes, the **Result** panel appears.

If the installation is completed with warnings, a **Warning** panel displays warning messages or a **Result** panel displays critical errors, perform the remediation steps displayed in the **Detail** window to complete the installation.

You can click the link, **Log Files** to view the CCS installation log files. The log files are in .csv format. You can use the Log Viewer in the <Install_Directory>\Application Server to view the log files. The LogViewer helps you to easily identify warnings and errors using the color codes. Warnings are highlighted in yellow color and errors are highlighted in red color.

12 In the **Result** panel, review the installation result and then click **Next**.

You can click the link, **Log Files** to view the CCS installation log files. The log files are in .csv format. You can use the LogViewer in the <Install_Directory>\Application Server to view the log files. The LogViewer helps you to easily identify warnings and errors using the color codes. Warnings are highlighted in yellow color and errors are highlighted in red color.

13 The **Next Steps** panel displays the additional steps that you must perform to complete the CCS deployment. Perform the next steps and then click **Finish**.

You can click the link, **Save the next steps** to save the next steps for future reference. The details appear in a browser, after you specify the location to save the next steps.

You can check options to launch the CCS console or view the release notes.

You can click the link, **Log Files** to view the CCS installation log files. The log files are in .csv format. You can use the LogViewer in the <Install_Directory>\Application Server to view the log files. The LogViewer helps you to easily identify warnings and errors using the color codes. Warnings are highlighted in yellow color and errors are highlighted in red color.

See “Configuring Service Principal Names” on page 161.

See “Creating a certificate for installing a standalone CCS Manager” on page 167.

See “Installing a standalone CCS Manager for a scale out deployment of CCS” on page 169.

See “Installing the CCS Content” on page 219.

See “Installing the CCS Suite in silent mode” on page 223.

See “CCS Suite deployment sequence ” on page 140.

See “Repairing or reinstalling the CCS Suite” on page 291.

See "Uninstalling the CCS Suite" on page 295.

Configuring Server Roles to install the prerequisites manually on the CCS Application Server

The following prerequisites are required to be installed manually on CCS Application Server that is installed on Windows Server 2008 and Windows Server 2012:

- ASP.NET v4.0.30319
- IIS Static Content
- IIS Windows Authentication

On Windows Server 2008 and Windows Server 2012, you can install these prerequisites on either 32-bit or 64-bit computers by configuring the Server roles.

To configure Server Roles for Windows Server 2008

1. Start the Server Manager.
2. Click **Add Roles**.
3. Click **Web Server IIS**.
4. Click **Next**.
5. Under **Common HTTP Features**, select **Static Content**.
6. Under **Application Development**, select **ASP.NET** and **ASP**.
7. Under **Security**, select **Windows Authentication**.
8. Click Install.

To configure Server Roles for Windows Server 2012

1. Start the Server Manager.
2. Click **Add Roles and Features**.
3. Under **Installation** type, select **Role based or feature based installation**.
4. Click **Web Server IIS**.
5. Click **Next**.
6. Under **Common HTTP Features**, select **Static Content**.
7. Under **Application Development**, select **ASP.NET 3.5**, **ASP.NET 4.5**, and **ASP**.
8. Under **Security**, select **Windows Authentication**.
9. Click **Install**.

To set the value on Windows Server 2008 and Windows Server 2012, in the Internet Information Services (IIS) Manager, in the **Connections Pane**, click the server node in the tree. On the server home page, under **IIS**, double-click **ISAPI and CGI Restrictions**. Right-click **ASP.NET v4.0.30319** and click **Allow**.

See "Software requirements" on page 48.

Product Improvement Program

The Product Improvement Program has been devised to capture the installation and the product usage information about the CCS instances in your environment. The Product Improvement Program collects information about how the Symantec customers use the product and the issues that they encounter. Symantec leverages the data to analyze the features that the customers use the most or the areas that may require improvement. The sole focus of the program is on enhancement of the product to better meet the needs of the customers. The Product Improvement Program does not collect any personally identifiable data and the end user's participation is optional. The data collection is done as a part of the Health and Status job and the data is stored in the production database. Symantec can access the data only if you consent to participate in the Product Improvement Program.

Note: The Product Improvement Program is enabled by default. If you do not want to share the data with Symantec, then you must disable the option to opt-out of the program.

In Control Compliance Suite, the areas that the Product Improvement Program covers are as follows:

- The installed product version and the installation ID.
- Whether the installation is a fresh installation or an upgrade.
- The deployment scenario - whether the product is installed in a distributed environment or all the components are installed in one computer
- The configuration of the computers on which CCS is installed.
- The installation timestamp.
- The installed modules.
- The details of the processor of the computers on which CCS is installed.
- The success or the failure status of the installations.
  In case of a failed installation, the program captures the error details.
  In case of upgrades, the program captures the previous version of MSI.
- The errors that the end-users encounter.

- The number of CCS Managers and their roles.
- The type and the number of agent-based and agent-less assets.
- The total number of job runs till date.
- The total number of job runs per week.
- The sizes of the production and reporting databases.
- The SQL server details and if SSL is configured.
- The license and the certificate details.
- The number of licenses that are used.
- The certificate algorithm and the certificate renewal year in case of a fresh CCS installation.
- Whether or not the environment is FIPS-enabled
- If the integration services have been enabled.
- The culture information that is specific to internationalization
- If the NTLM option is enabled.

To learn about Symantec's privacy policy, refer to the following URL:

http://www.symantec.com/privacy

See "Disabling the Product Improvement Program" on page 157.

Disabling the Product Improvement Program

The Product Improvement Program is enabled by default. If you do not want to share the data with Symantec, then do one of the following to opt-out of the program:

- Disable the Product Improvement Program during installation.
- Disable the Product Improvement Program from General settings.

To disable the Product Improvement Program during installation

- On the **Welcome** panel of the CCS installer, uncheck **I agree to participate in the Product Improvement Program by sharing the installation and product usage information with Symantec**.

  Later, if you want to participate in the program, go to General settings and check **Share installation and product usage information with Symantec**.

To disable the Product Improvement Program from General settings

- On the CCS console, go to **Settings** > **General** > **Product Improvement Program** and uncheck **Share installation and product usage information with Symantec**.

See "Product Improvement Program" on page 156.

About licensing of the product components

CCS categorizes the features that require mandatory licenses during installation and the features that can be licensed in the post-installation of the product.

CCS contains a core license that is required for installing the CCS Application Server components including the Directory Service. The core license is a mandatory license and must be provided during the installation of CCS.

The CCS Maintenance license is required to install the default CCS Content during CCS installation. For optional CCS features you can provide a license though the CCS Console later.

Base license is required to activate a product feature. For example, activating Policy Manager to use CCS for policy compliance.

Note: Licenses for CCS Policy Manager and CCS Risk Manager are not metered per user. Hence total license count for these features is displayed as Unlimited.

The features are licensed with the Symantec Enterprise License Service (ELS), which constitute the .slf files. The licenses can be provided either through the Installation Wizard during installation of the product or in the post-installation of the product. Once the licenses are provided to CCS, the licenses are stored at the location %programdata%\Symantec Shared\Licenses.

For fresh installation, new CCS 11.1 licenses are provided.

If you are upgrading from CCS 11.0 you can continue using the existing 11.0 licenses till they are valid. Once the CCS 11.0 licences expire, new CCS 11.1 licenses will be provided.

Contact Symantec Technical Support for assistance on renewal or procurement of licenses.

For more information about licenses, see the *Licenses* section is the *Symantec™Control Compliance Suite User Guide*

See "Installing the CCS Suite" on page 140.

See "Installing a standalone CCS Manager for a scale out deployment of CCS" on page 169.

About the pass phrase

CCS uses pass phrases to generate symmetric key. The Encryption Management Service and the Application Server use these keys in turn to encrypt and decrypt configuration information, including passwords and connection details. The person who installs CCS creates the pass phrases.

You enter the pass phrase when you install the Application Server and the Encryption Management Service. The Encryption Management Service and the Application Server should use unique pass phrases. The pass phrases you choose should be complex passwords. These passwords must be difficult to guess.

You require the pass phrase to perform the following actions:

- Change the service user account.
- Uninstall from a different user context.
- Install an upgraded version.

If the pass phrase is lost, you can use the **Configure Service Account** tool to reset it. If you reset the pass phrase, you must re-enter all of the credentials that the Application Server and the Encryption Management Service use.

See "Installing the CCS Suite" on page 140.

Recommendations for manual creation of databases

If you are creating the CCS databases manually in SQL Server, following are the recommendations for creating the databases.

In the Microsoft SQL Server Management Studio, New Database window:

- In the **Database name** field, ensure that you specify the correct database names: CSM_DB for Production Database, and CSM_Reports for the Reporting Database.
- In the **Database files** section:
  - In the **Filegroup** column, ensure that you create databases under the PRIMARY file group.
  - In the **File Name** column, do not specify any file name.

See "Installing the CCS Suite" on page 140.

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

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 (>)

See “Installing the CCS Suite” on page 140.

About Service Principal Names

A Service Principal Name (SPN) is an attribute of a user or a computer in the Active Directory environment. SPNs are used to support mutual authentication between a client application and a service using Kerberos without transmitting sensitive authentication data to the service. When a user application connects to a remote service, the user application requests a service ticket from the domain controller (DC). The DC identifies the Kerberos service that is to be used. The Kerberos authentication service searches through the Active Directory to find a matching SPN and issues an appropriate service ticket. Every computer in an Active Directory

environment possess at least one SPN. Services such as IIS and SQL Server require SPNs to support Kerberos authentication.

The CCS Application Server and Directory Service require SPNs for successful configuration and functioning. If the SPNs are not configured, the CCS Console and the CCS Web Console sessions cannot authenticate and hence results in CCS operation failure. You must ensure that you plan the user accounts and the service accounts for the Application Server and the Directory Service before you configure the SPNs.

CCS 11.1 provides a batch file containing the Service Principal Names' (SPN) setup script. The SPN script file contains the set SPN commands to set the required SPNs for the CCS components. Provide the script file to the domain administrator to create the Service Principal Names. You can export the batch file during the CCS Suite installation or by using the VerifyDelegation utility located inside the <Install_Directory>\Application Server folder.

See “User Privileges for deploying the CCS components” on page 55.

The CCS Web Console that uses the Microsoft Internet Information Services also requires a valid SPN. Usually, the IIS SPN is created automatically during the IIS installation. However, in cloned systems the SPNs are not created automatically. Hence, it is important to create and validate the SPNs before installing CCS.

See “Configuring Service Principal Names” on page 161.

See “CCS Suite deployment sequence ” on page 140.

Configuring Service Principal Names

CCS 11.1 provides a batch file containing the Service Principal Names' (SPN) setup script. The SPN script file contains the set SPN commands to set the required SPNs for the CCS components. Provide the script file to the domain administrator to create the Service Principal Names. You can export the batch file during the CCS Suite installation or by using the VerifyDelegation utility located inside the <Install_Directory>/Application Server folder.

If you want to set the SPNs manually, perform the following procedure to set the SPNs.

Create SPNs for the Application Server Service and the Directory Service (DSS). The CCS SPNs are associated with the service accounts that are used by CCS. In a default Active Directory environment, only the domain administrators and the account operators have sufficient rights to create, modify, or delete SPNs.

See “About Service Principal Names” on page 160.

To configure an SPN

1. Identify the user accounts that you want to use as the service account for the Application Server and the Directory Server.
2. Set up an SPN with the NetBIOS name and the fully qualified domain name (FQDN) of the domain user account in whose context the application pool executes. SPN can be set up from the Application Server or the DC. You must associate an SPN to a single user account.

   Execute the following commands to set up an SPN:

   - SetSpn -A Symantec.CSM.AppServer/**appserver_machine DomainName/appserver_account**
   - SetSpn -A Symantec.CSM.AppServer/**appserver_machine.fqdn DomainName/appserver_account**
   - SetSpn -A Symantec.CSM.DSS/**dss_machine DomainName/dss_account**
   - SetSpn -A Symantec.CSM.DSS/**dss_machine.fqdn DomainName/dss_account**
     Where,
     - appserver_machine: The NetBios name of the computer where the Application Server is installed.
     - DomainName/appserver_account: The domain name of Application Server service account.
     - dss_machine: The NetBios name of the computer where the Directory Service is installed.
     - DomainName/dss_account: The domain name of Directory Service account.
     - dss_machine.fqdn: The fully qualified domain name of the Directory Service computer.

   Further, execute the following commands on the computers where IIS 6 or IIS 7 is used. For IIS 7, you must execute these commands only 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.

   By default, the Kernel Mode Authentication is enabled.

   - SetSpn.exe -A http/**IIS_computer's_NetBIOS_name DomainName/UserName**

- SetSpn.exe -A http/**IIS_computer's_FQDN DomainName/UserName**
  Where,
  - IIS_computer's_NetBIOS_name: The NetBIOS name of the IIS computer.
  - IIS_computer's_FQDN: The fully qualified domain name of the IIS computer.
  - DomainName/UserName: The domain name of Application Server service account.

You must set HTTP SPN on Windows Server 2008 computers where the IIS Host Header and the CCS Application Server name are not same.

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 “About certificate encryption” on page 164.

See “Creating a certificate for installing a standalone CCS Manager” on page 167.

See “Installing a standalone CCS Manager for a scale out deployment of CCS” on page 169.

See “CCS Suite deployment sequence ” on page 140.

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 hot fix. 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 2008/2012 systems may have passwords up to 255 characters.

Table 3-1 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.

See “About creating certificates” on page 163.

See “Creating a certificate for installing a standalone CCS Manager” on page 167.

See “Installing a standalone CCS Manager for a scale out deployment of CCS” on page 169.

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 3-2 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 3-3

Table 3-3 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 standalone CCS Managers. For standalone 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

See “Installing a standalone CCS Manager for a scale out deployment of CCS” on page 169.

Creating certificates for the CCS Suite components

The CCS Application Server and the CCS Manager exchange certificates for secured communication. You must create the certificates based on the service type that you install.

See “Creating a certificate for installing a standalone CCS Manager” on page 167.

The root certificate is created during the installation of the CCS Application Server. 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. For standalone CCS Managers, certificates must be created manually using the **Certificate Management Console**. The CCS Manager certificate is unbound until the CCS Manager is registered in **System Topology** in the CCS Console.

While installing standalone CCS Managers, you can either pull these certificates from the CCS Application Server computer or place them manually on the computers on which the CCS Managers are installed.

See "About the Certificate Management Console" on page 164.

Certificates are encrypted and use the Secure Hash Algorithm (SHA) set of cryptographic hash functions.

See "About certificate encryption" on page 164.

See "Installing a standalone CCS Manager for a scale out deployment of CCS" on page 169.

Creating a certificate for installing a standalone CCS Manager

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 3-4 Certificate options

Name	Description	Default value
Service Type	The available **Service Type** names are the following: ■ CCS Manager ■ Application Server ■ Application Server (SSL Only) ■ Encryption Management Service	**CCS Manager**

Table 3-4 Certificate options *(continued)*

Name	Description	Default value
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 See "About certificate encryption" on page 164.	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 See "About certificate encryption" on page 164.	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.
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

You require the Certificate Management Console (CMC) for creating certificates for CCS. The Certificate Management Console is installed while installing the CCS Application Server.

Perform the following procedure before creating a certificate:

See "Installing the CCS Suite" on page 140.

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 3-4
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 the Certificate Management Console" on page 164.

See "About certificate encryption" on page 164.

See "About creating certificates" on page 163.

See "Installing a standalone CCS Manager for a scale out deployment of CCS" on page 169.

See "Installing a standalone CCS Manager for scale-out deployment in silent mode" on page 228.

See "CCS Suite deployment sequence " on page 140.

Installing a standalone CCS Manager for a scale out deployment of CCS

CCS Manager is the interface to the programs that do the actual work of collecting data from the network. Your Control Compliance Suite (CCS) deployment can

include multiple CCS Managers. Based on network affinity and load, CCS automatically detects the appropriate CCS manager to execute a specific job.

The installation of the CCS Manager instance is of paramount importance for collecting data and reporting to the Control Compliance Suite infrastructure. The CCS Manager also plays roles of a load balancer and data evaluator. The CCS Manager's data collector role is to collect data from the data collection infrastructures including data collection from Agents, CSV files, or ODBC databases.

The collected data is stored in a SQL database where it can be further evaluated and reported against the standards. The reporter generates reports of the collected data and displays them in the console. The load balancer routes the data collection and the data evaluation jobs evenly to the configured data collectors and data evaluators respectively.

You can install the CCS Manager and the CCS Application Server on a single computer. See "Installing the CCS Suite" on page 140.

You can add the CCS Manager to an existing installation of the CCS Application Server. See "Adding or upgrading CCS components" on page 286.

The CCS Manager also installs the CCS Agent on the computer.

Note: You cannot install a CCS Manager on a computer that has a standalone CCS Agent installed, because the CCS Manager installation also contains the installation of CCS Agent.

See the following sections before installing the CCS Manager:

See "Hardware and operating system requirements" on page 37.

See "Network Ports" on page 41.

See "Software requirements" on page 48.

Perform the following procedures before installing a standalone CCS Manager:

Install the CCS Application Server. See "Installing the CCS Suite" on page 140.

Create a certificate for the CCS Manager using the Certificate Management Console. The Certificate Management Console is installed along with the installation of the CCS Application Server. See "Creating a certificate for installing a standalone CCS Manager" on page 167.

Do the following to install the CCS Manager:

- Launch the Installation Wizard.
  See "To launch the Installation Wizard" on page 171.
- Install the CCS Manager.

See "To install the CCS Manager" on page 171.

To launch the Installation Wizard

1 Insert the **Symantec Control Compliance Suite 11.1** product disc into the drive on your computer and double-click **Setup.exe**.

In the security warning dialog box, click **Run**.

2 In the DemoShield, click **CCS Manager**.

On the splash screen, click **Install CCS Manager**. The Setup file is located inside the CCS_Manager folder of the product media.

Setup prepares the CCS Manager installation wizard and prompts to install any prerequisites, if required. During the prerequisite installation, if the computer prompts you to restart, restart the computer and launch the setup again.

See "Software requirements" on page 48.

To install the CCS Manager

1 In the **Welcome** panel of the launched Symantec Control Compliance Suite 11.1 installation wizard, read and accept the license agreement, and then click **Next**.

The Product Improvement Program is enabled by default. The Product Improvement Program does not collect any personally identifiable data and the participation is optional. If you do not want to share the data with Symantec, then you must opt-out of the program. To opt-out of the product improvement program, uncheck **I agree to participate in the Product Improvement Program by sharing the installation information with Symantec**. For more information about the product improvement program, See "Product Improvement Program" on page 156.

2 In the **Prerequisites** panel, review the prerequisites that are required for the installation. Install any prerequisite application that is required to be installed. Click **Check again** to verify whether the installation is successful.

You must install Crystal Reports 2010 manually on the CCS Manager computer that is configured with the role of a reporter. To install Crystal Reports 2010 during the CCS Manager installation, expand Crystal Reports and check **Install**. You can also install Crystal Reports 2010 using the CrystalReportsDotNet.MSI file from the <installation directory>/Symantec/CCS/Reporting and Analytics/WebPortal/Console/Redist folder of the CCS Application Server or you can install CrystalReportsDotNet.MSI from the CCS_Reporting\Redist folder of the product media.

See "Software requirements" on page 48.

3 Click **Next**.

4 In the **Installation Folder** panel, review the installation path for product installation.

Click browse (**...**) to specify a different installation path to install the product.

You can change the default location of the Installation files cache folder where the setup files that are cached during installation. Click browse (**...**) to select a different location to store the setup files.

Click **Refresh disk space information** to verify the available disk space on the computer.

5 Click **Next**. If you have specified a different installation path, and the installer folder does not exist, the installer prompts you to create the installation folder.

6 In the **CCS Manager - Service Configuration** panel, enter a port for the CCS Manager. CCS components use this port to communicate with the CCS Manager.

You must import the security certificate that is used by the CCS Manager to communicate with the CCS Application Server securely.

The certificate which is to be deployed on the CCS Manager is created using the **Certificate Management Console**. The **Certificate Management Console** is installed on the CCS Application Server computer. You can either pull the certificate from the CCS Application Server computer or place it manually on the computer on which you are installing the CCS Manager.

Browse for the Security Certificate file location and enter the password.

7 In the **Summary** panel, review the installation details and click **Install**.

You can click the link, **Export Summary** to export the configuration details of the CCS Manager that is installed on the computer. The details appear in a browser, after you specify the location to export the summary.

8 The **Install** panel indicates the progress of the component installation. After the installation finishes, the **Result** panel appears.

If the installation is completed with warnings, a **Warning** panel displays warning messages or a **Result** panel displays critical errors, perform the remediation steps displayed in the **Detail** window to complete the installation.

You can click the link, **Log Files** to view the CCS Manager installation log files. The log files are in .csv format. You can use the LogViewer in the <Install_Directory>\Application Server to view the log files. The LogViewer helps you to easily identify warnings and errors using the color codes. Warnings are highlighted in yellow color and errors are highlighted in red color.

9 In the **Result** panel, review the installation result and then click **Next**.

You can click the link, **Log Files** to view the CCS Manager installation log files. The log files are in .csv format. You can use the LogViewer in the <Install_Directory>\Application Server to view the log files. The LogViewer helps you to easily identify warnings and errors using the color codes. Warnings are highlighted in yellow color and errors are highlighted in red color.

10 The **Next Steps** panel displays the additional steps that you must perform to complete the CCS deployment. Perform the next steps and then click **Finish**.

You can click the link, **Save the next steps** to save the next steps for future reference. The details appear in a browser, after you specify the location to save the next steps.

You can click the link, **Log Files** to view the CCS Manager installation log files. The log files are in .csv format. You can use the LogViewer in the <Install_Directory>\Application Server to view the log files. The LogViewer helps you to easily identify warnings and errors using the color codes. Warnings are highlighted in yellow color and errors are highlighted in red color.

You can check the option to view the release notes.

See “Registering the CCS Manager” on page 173.

See “Configuring basic CCS Manager settings” on page 175.

See “Configuring advanced CCS Manager settings ” on page 177.

See “Assigning a role to a CCS Manager” on page 179.

See “Configuring CCS Manager data collectors” on page 180.

See “Creating a lightweight package for remote installation of CCS Manager ” on page 183.

See “Installing a standalone CCS Manager for scale-out deployment in silent mode” on page 228.

See “CCS Suite deployment sequence ” on page 140.

See “Repairing or reinstalling a standalone CCS Manager” on page 292.

See “Uninstalling a standalone CCS Manager” on page 297.

Registering the CCS Manager

Before the CCS Application Server can use a newly installed CCS Manager, you must register the CCS Manager with the CCS Application Server. When you register a CCS Manager, the Directory Service 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.

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

If you install the CCS Manager along with the CCS Application Server, using the CCS Suite installer, by default, that CCS Manager is registered in the System Topology in the CCS Console and all roles are assigned to that CCS Manager.

For standalone CCS Manager installations, you must register the CCS Managers and assign appropriate roles to the CCS Managers, through the CCS Console.

Perform the following procedure before registering the CCS Manager:

Install the CCS Manager. You can install the CCS Manager along with the CCS Application Server on a single computer, See "Installing the CCS Suite" on page 140.

You can add a CCS Manager to an existing installation of the CCS Application Server, See "Adding or upgrading CCS components" on page 286.

You can install a standalone CCS Manager. See "Installing a standalone CCS Manager for a scale out deployment of CCS" on page 169.

To register the 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. In the **System Topology > Map View** or **System Topology > Grid View**, click **Infrastructure Tasks > Register CCS Manager**.
5. In the **CCS Manager Selection** panel, select one or more CCS Manager hosts to register and click **Next**.

   The **CCS Manager Selection** panel displays the unregistered CCS Manager hosts in your network.

   Note: You must first install a CCS Manager in your network for that CCS Manager to show up in the **CCS Manager Selection** panel.

6 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 **OK**.

7 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.

Expand **Advanced Options** to change the port the CCS Manager uses to communicate with the CCS Application Server. The default port is 5600. Click **Next**.

8 If you selected the Data Collection Service role, in the **Data Collector Selection** panel, select the data collectors that the CCS Manager should use, then click **Next**.

9 If you selected the Reporting Service role, 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**.

10 In the **Summary** panel, review the CCS Manager settings and click **Finish**.

11 In the **Finished** panel, click **Close**.

Click **Change advanced settings for the new CCS Manager** to configure the advanced settings for the CCS Manager which you registered.

12 Click **Register another CCS Manager** to register one more CCS Manager in your network.

See “Configuring basic CCS Manager settings” on page 175.

See “Configuring advanced CCS Manager settings ” on page 177.

See “Installing a standalone CCS Manager for a scale out deployment of CCS” on page 169.

See “CCS Suite deployment sequence ” on page 140.

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.

Perform the following procedure before configuring the basic CCS Manager settings:

Install the CCS Manager. You can install the CCS Manager along with the CCS Application Server on a single computer, See "Installing the CCS Suite" on page 140.

You can add a CCS Manager to an existing installation of the CCS Application Server, See "Adding or upgrading CCS components" on page 286.

You can install a standalone CCS Manager. See "Installing a standalone CCS Manager for a scale out deployment of CCS" on page 169.

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.

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.

Perform the following procedure before configuring the advanced CCS Manager settings:

Install the CCS Manager. You can install the CCS Manager along with the CCS Application Server on a single computer, See "Installing the CCS Suite" on page 140.

You can add a CCS Manager to an existing installation of the CCS Application Server, See "Adding or upgrading CCS components" on page 286.

You can install a standalone CCS Manager. See "Installing a standalone CCS Manager for a scale out deployment of CCS" on page 169.

To configure the advanced 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 **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.

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

Perform the following procedure before assigning a role to a CCS Manager:

Install the CCS Manager. You can install the CCS Manager along with the CCS Application Server on a single computer, See "Installing the CCS Suite" on page 140.

You can add a CCS Manager to an existing installation of the CCS Application Server, See "Adding or upgrading CCS components" on page 286.

You can install a standalone CCS Manager. See "Installing a standalone CCS Manager for a scale out deployment of CCS" on page 169.

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.

See "CCS Suite deployment sequence " on page 140.

Configuring CCS Manager data collectors

The role of a data collector is to collect data from the enterprise network. The Control Compliance Suite can collect data from any data collection infrastructure including data collection from Agents, CSV files, or ODBC databases. The data collection is triggered through the data collection jobs. The collected data is evaluated for the standards by the data evaluator. The data evaluation jobs trigger the data evaluation of the collected data. The load balancer routes the data collection and the data evaluation jobs evenly to the configured data collectors and the data evaluators respectively.

In Control Compliance Suite 11.1 , you can perform raw-data based and message based data collection on various platforms using CCS Manager. You can configure CCS Manager or CCS Agent installed on the computers within the enterprise, to collect data.

Based on the data collection model you choose, you must complete configuration steps before actually performing data collection.

Table 3-5 provides the information related to platforms supported for different types of data collection.

Table 3-5 Platforms supported for data collection

Platform	Raw-data collection	Message based data collection
Windows	Yes	Yes
UNIX	Yes	Yes
SQL	Yes	Yes
Oracle	Yes	Yes
VMware	Yes	Yes
Sybase	No	Yes
DB2	No	Yes
Cisco	Yes	No

Note: CCS 11.1 does not support NDS, NetWare, and Exchange data collectors. In case you have upgraded from previous versions of CCS to 11.0 and then to 11.1, CCS collects data from NDS, NetWare, or Exchange platforms and functions in the same manner as in the previous versions of CCS 11.0. Message based data collection is not supported for these platforms.

Perform the following procedure before configuring CCS Manager data collectors:

Install the CCS Manager. You can install the CCS Manager along with the CCS Application Server on a single computer, See "Installing the CCS Suite" on page 140.

You can add a CCS Manager to an existing installation of the CCS Application Server, See "Adding or upgrading CCS components" on page 286.

You can install a standalone CCS Manager. See "Installing a standalone CCS Manager for a scale out deployment of CCS" on page 169.

To configure CCS Manager data collectors

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, select the data collectors to enable on the CCS Manager.

8 Click **Save** to save the changes.

For information on configuring the data collectors, see the *Symantec Control Compliance Suite User Guide*.

Installing the Oracle Instant Client for data collection on Oracle

If you are collecting data on the Oracle platform, you require the Oracle Instant Client 12.1 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:

```
Exception occurred The 'Symantec CCS Oracle Database' data-collection
module could not be initialized
```

To install Oracle Instant Client 12.1

1 Locate the **Oracle Instant Client version 12.1** 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 recommends 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.

Creating a lightweight package for remote installation of CCS Manager

You can create a light weight package of the CCS Manager setup files to install standalone CCS Managers on other computers. The lightweight package contains only the files necessary for installing CCS Managers on specific platforms, thereby reducing the size of the setup package that needs to be copied to the target computer for installing the CCS Manager. You can create lightweight packages for each platform that you want to install the CCS Managers on. CCS 11.1 provides a batch file which creates the lightweight package from the CCS 11.1 product media.

The lightweight package contains the following files from the product media:

- Entire contents of the CCS_Manager\DPS folder
- Entire contents of the CCS_Manager\ESMManager folder
- Entire contents of the CCS_Manager\ThirdPartyConnectors folder
- Entire contents of the SU\DC folder
- Security Update files from the SU folder
  The Security Update files are of the Windows platform which is specified in the batch file.
- AccessDatabaseEngine from the Redist folder
- SQLServer2005_BC from the Redist folder
  The SQL Server backward compatibility files are of the platform (32 bit or 64 bit) which is specified in the batch file.

The batch file for creating the lightweight package is located in the `Tools` folder of the product media. Copy the batch file to the local computer, and then edit the batch file to provide the following inputs to create the lightweight package for the specific platform:

- INSTALLSETPATH
  Specify the location of the CCS 11.1 product media.
- DESTINATIONPATH
  Specify the location to create the lightweight package.
- WINPLATFORM
  Specify the Windows platform for the Security Update for message based content.
- WINDOWS
  Specify whether the Windows platform is 32 bit or 64 bit.

Once the lightweight package is created, double-click the Setup file located inside the CCS_Manager folder of the lightweight package to install the CCS Manager.

Configuring IPv4 and IPV6 sockets for communication

You can configure the CCS Manager or CCS Agent service to listen on IPV4 socket, IPV6 socket or dual stack (IPV4 and IPV6) in your setup. The operating system can be one of the following:

- Windows 2003
- Windows 2008
- Windows 2012

Following are the sockets that the CCS Manager service or CCS Agent service listens on for various types of installation :

Table 3-6 IPV4 and IPV6 settings

Installation on Operating system	IPV4	IPV6	Dual
Manager + Agent on Windows 2003	0	1	0
Manager + Agent on Windows 2008	0	1	2
Agent only installation on any platform	0	2	0

0 = CCS service listens on pure IPV4 socket.

1 = CCS service listens on pure IPV6 socket.

2 = CCS service listens on both IPV4 and IPV6 sockets.

You can set the IPV6_SERVER flag in the tcp_port.dat file, to listen on a particular port.

The tcp_port.dat file is located in the <Installdir>\config\ folder.

See “Setting the IPV6_SERVER flag” on page 184.

Setting the IPV6_SERVER flag

The IPV6_SERVER flag controls the socket that the CCS Manager service or CCS Agent service listens on. The setting can be as follows:

- IPV6_SERVER=1

The CCS Manager or Agent service listens on IPV6 port.

- IPV6_SERVER=0
  The CCS Manager or Agent service listens on IPV4 port.

Note: On Solaris SPARC version 5.10 or higher, by default an IPV6 socket receives both IPV4 and IPV6 traffic.

See "Configuring IPv4 and IPV6 sockets for communication" on page 184.

Installing the CCS Agent on Windows

The CCS Agent collects data from target computers and forwards the data to the CCS Manager.

Note: To install an Agent with the latest updates, use the setup files for Agent installation available on the Symantec website.

See the following sections before installing the CCS Manager:

See "Hardware and operating system requirements" on page 37.

See "Network Ports" on page 41.

See "Supported target computers and databases for data collection" on page 48.

See "Software requirements" on page 48.

Perform the following procedure before installing the CCS Agent:

Install the CCS Manager. You require a CCS Manager for the CCS Agent to register to. However, you cannot install a CCS Agent on a computer that contains a CCS Manager.

Do one of the following:

- Install the CCS Manager along with the CCS Application Server on a single computer, See "Installing the CCS Suite" on page 140.
- Add a CCS Manager to an existing installation of the CCS Application Server, See "Adding or upgrading CCS components" on page 286.
- Install a standalone CCS Manager. See "Installing a standalone CCS Manager for a scale out deployment of CCS" on page 169.

Note: You cannot install a standalone CCS Agent on a computer that contains a CCS Manager, because the CCS Manager installation also contains the installation of CCS Agent.

Do the following to install the CCS Agent:

- Launch the Installation Wizard.
  See "To launch the Installation Wizard" on page 186.
- Install the CCS Agent.
  See "To install the CCS Agent" on page 187.

To launch the Installation Wizard

1. Insert the **Symantec Control Compliance Suite 11.1** product disc into the drive on your computer and double-click **Setup.exe**.

   In the security warning dialog box, click **Run**.

2. In the DemoShield, click **CCS Agent**.

   On the splash screen, click **Install CCS Agent**.

   See "Software requirements" on page 48.

3. The Setup files for installing CCS Agents on various platforms are located inside the CCS_Agent folder of the product media.

   If you want to install the application modules while installing the CCS Agent, you must copy the CCS_Agent\win folder on the local computer. Then create a folder "AppModules" at the level of the SU folder, and copy the platform specific application module from the CCS_Agent\MBC\AppModules folder to the local computer in the following folder structure:

   \\....AppModules\<Application module name>\<Platform folder>\<appmoduleinstaller.exe>

   For example, to install application modules for Oracle, create a folder structure as follows:

   \\....AppModules\Oracle\w3s-ix86\esmoracletpi.exe

   The installer installs this application module while installing the agent.

4. In the CCS_Agent\win folder, double-click **Setup.exe**.

   Setup prepares the CCS Agent installer.

To install the CCS Agent

1. In the **Welcome** panel of the launched Symantec Control Compliance Suite 11.1 Agent Setup wizard, click **Next**.
2. In the **License Agreement** panel, read and accept the license agreement and then click **Next**.
3. In the **Destination Folder** panel, review the installation folder path for product installation and click **Next**.

   Click**Change** to specify a different installation path to install the product.
4. In the **Install Security Update** panel, review the folder path to look for security updates and click **Next**.

   The setup detects the required security updates.

   Click**Browse** to specify a different folder path for security updates.

   If you are installing the application module during the agent installation, the setup detects the application module you have copied to the local computer in step 3
5. In the **Ready to Install the Program** panel, click **Install**.

   You can review or change the installation settings before proceeding with the installation.
6. The progress bar indicates the progress of the installation. After the installation finishes, the **Setup Wizard Completed** panel appears.
7. In the **Setup Wizard Completed** panel, click **Finish**

   You can check **Launch Agent Configuration Utility** to register the CCS Agent to the CCS Manager, enable LiveUpdate and enable Integrated Command Engine.

See “Registering the CCS Agent” on page 188.

See “Configuring LiveUpdate for a CCS Agent” on page 190.

See “Configuring the Integrated Command Engine for a CCS Agent” on page 191.

See “Installing the CCS Agent on UNIX” on page 192.

See “Configuring CCS Agents for message based data collection ” on page 203.

See “Installing and registering a CCS Agent on Windows in silent mode” on page 231.

See “CCS Suite deployment sequence ” on page 140.

Registering the CCS Agent

Registration of a CCS Agent with a CCS Manager establishes secured communications between the agent and manager. Each agent can register to one manager or multiple managers. You can register an agent to a manager during or after the installation.

During an agent registration, the following information about the agent computer is fetched:

- The name of the agent
- The IP addresses of the agent computer
- The FQDN of the agent computer
- The host name of the agent computer
- The operating system on which the agent is installed
- OS details of the agent computer
- The ESM version that is installed on the agent
- The port that the agent uses to communicate with the manager
- The proxy agent of the agent computer
- Whether LiveUpdate is enabled for the agent

Note: The agent name must not contain more than 61 characters. Agent registration fails if the agent name contains more than 61 characters.

Your user account must have the following permissions to be able to register an agent to a specific manager:

- Register agent right in Advanced manager permissions
- Modify access right on “All Agents” domain
- Create domain right if “<OS> Agents” domain is not present
- Modify permission on all policies if the manager is not locked for any Security Update. If the manager is locked for a Security Update, then this permission is not required

CCS Agents can only register with the CCS Managers that use the same communication port.

You must re-register the agents if you change the IP address of a CCS Manager. When you register an agent to a manager, a key is generated and is stored in the manager database. The registration key is used to establish communication between

the manager and its agent. If you change the IP address of the manager, the registration key becomes invalid. When you re-register the agent, a new registration key is generated, which is used for re-establishing the communication between the manager and its agent.

Note: If an agent is registered to multiple managers, then you must use the same format for the agent name to register the agent to the other managers. For example, if you use the IP address to register an agent, then use the IP address to register the agent to other managers.

Note: The CCS Manager must have a valid license to register CCS Agents.

Perform the following procedure before registering the CCS Agent:

Install the CCS Agent. See "Installing the CCS Agent on Windows" on page 185.

To register a CCS Agent

1. Log on as administrator or use a role that is equivalent to an administrator.
2. You can register the Agent by launching the Agent Configuration Utility from the CCS Agent Installer or by clicking **Start > All Programs > Symantec Corporation > Symantec Control Compliance Suite > Agent Configuration**.
3. In the **Configure CCS Agent** dialog box, in the left pane, click **Registration**.
4. In the **Agent Information** section, click the appropriate option for the agent name. The **FQDN** (Fully Qualified Domain Name) option is selected by default.
5. In the **Manager Information** section of the CCS Agent Registration panel, do the following:
   - In the **Manager Name** text box, type the name of the CCS Manager.
   - In the **Port** text box, type the port number for the CCS Manager. Computers that run Symantec managers and agents must use the same communication port to register the agents.
   - Perform this step if you are registering the agent for message based data collection. You must first enable the CCS Application Server and CCS Manager for message based data collection.
     See "Enabling message based data collection" on page 205.
     Check **Message Based Content Registration**, if you are registering the agent for message based data collection.
   - Perform this step if you are registering the agent for message based data collection. You must first enable the CCS Application Server and CCS Manager for message based data collection.

See "Enabling message based data collection" on page 205.

In the **Username** text box, type ESM.

- Perform this step if you are registering the agent for message based data collection.

  In the **Password** text box, type the ESM password which you have set while enabling the CCS Manager for message based data collection.

6 Check **Verify Manager to Agent communication** if you want to verify the manager to agent communication before registering the agent.

7 Click **Register** to register the agent with the manager.

To register the agent to more than one manager, perform steps 5 to 7 for each manager.

8 Click **Close**.

See "Configuring LiveUpdate for a CCS Agent" on page 190.

See "Configuring the Integrated Command Engine for a CCS Agent" on page 191.

See "Installing and registering a CCS Agent on Windows in silent mode" on page 231.

See "Changing the LiveUpdate setting for an agent" on page 201.

See "CCS Suite deployment sequence " on page 140.

Configuring LiveUpdate for a CCS Agent

CCS uses LiveUpdate to distribute CCS Agent upgrades and install security updates. You can specify the CCS Managers that are permitted to perform LiveUpdate on the agent. You must enable LiveUpdate on the local agent and on the CCS Console.

To change the LiveUpdate configuration on the local agent

1 Log on as administrator to the computer on which the agent is installed. Alternatively, use a role that is equivalent to an administrator.

2 You can change LiveUpdate configuration for a CCS Agent by launching the Agent Configuration Utility from the CCS Agent Installer or by clicking **Start > All Programs > Symantec Corporation > Symantec Control Compliance Suite > Agent Configuration**.

3 In the **Configure CCS Agent** dialog box, in the left pane, click **LiveUpdate**.

4 In the LiveUpdate settings panel, do one of the following:

- Click **Disable LiveUpdate on this agent** to disable LiveUpdate on the agent.
- Click **Enable LiveUpdate on this agent from all registered managers** to enable LiveUpdate from all managers to which the agent is registered.

- Click **Enable LiveUpdate on this agent from the selected registered managers**, and then in the Available Managers list, select the managers that are allowed to perform LiveUpdate. Use the right-arrow to move the managers into the Selected Managers list.

5 Click **Close**.

Note: If a manager is connected to multiple consoles, do not apply LiveUpdate simultaneously on that manager from the consoles that the manager is connected to.

Configuring the Integrated Command Engine for a CCS Agent

If you are using the CCS Agent for message based data collection, use the Integrated Command Engine (ICE) scripts to enable the CCS Manager to execute custom scripts on the agent.

To configure the Integrated Command Engine

1 Log on as administrator or use a role that is equivalent to an administrator.

2 You can configure the Integrated Command Engine by launching the Agent Configuration Utility from the CCS Agent Installer or by clicking **Start > All Programs > Symantec Corporation > Symantec Control Compliance Suite > Agent Configuration**.

3 In the **Configure CCS Agent** dialog box, in the left pane, click **ICE Settings**.

4 Check **Enable Integrated Command Engine** and then click **Apply**.

5 Click **Close**.

Changing a CCS Agent port

CCS Agent uses specific ports, which you can change.

To change a CCS Agent port

1. On the Windows taskbar, click **Start > Programs > Administrative Tools > Services**, and stop the Symantec ESM Agent service.
2. In the tcp_port.dat file, enter the port number.

   Following are the field names for the agents that are installed on various operating systems:

Type of CCS Agent	Field name for port number
UNIX agent	PORT_AGENT_UNIX
VMS agent	PORT_AGENT_VMS
Netware agent	PORT_AGENT_NETWARE
Windows NT agent	PORT_AGENT_NT

3. Start the Symantec ESM Agent service.
4. Reregister the agent with the manager.

   See “Registering the CCS Agent” on page 188.

Installing the CCS Agent on UNIX

You can install CCS Agents on UNIX computers. For the installation process, you run the installation program and register the CCS Agents with the CCS Managers.

Symantec distributes software on a disc. To install this software, at least one computer with a UNIX operating system must have access to a disc drive.

Symantec provides the software files in a compress-format tar file for the computers that have UNIX operating systems. The software disc contains installation files for each operating system that is supported for installing CCS Agents on UNIX.

The disc contains the following installation files:

- esmsetup
- esm.tgz
- app
- su
- esmuppd
- license.txt

- cs.tbl

The util folder in the disc contains the following installation file:

- gzip

The esmsetup is the installation program. The esm.tgz is the compressed tar file that contains the program files. The gzip is the GNU uncompress utility. The app folder should contain esm.tpi, which is the installer for application modules. The su folder contains the esm.tpk, which is the installer for Security Updates for message based data collection and ccs.tpk, which is the installer for Security Updates for raw-data based collection.

Ensure that the host name of the computer is present in the /etc/hosts file before installing the agent.

Note: You cannot install a standalone CCS Agent on a computer that contains a CCS Manager, because the CCS Manager installation also contains the installation of CCS Agent.

Perform the following procedure before installing the CCS Agent:

Install the CCS Manager. You require a CCS Manager for the CCS Agent to register to. However, you cannot install a CCS Agent on a computer that contains a CCS Manager.

Do one of the following:

- Install the CCS Manager along with the CCS Application Server on a single computer, See “Installing the CCS Suite” on page 140.
- Add a CCS Manager to an existing installation of the CCS Application Server, See “Adding or upgrading CCS components” on page 286.
- Install a standalone CCS Manager. See “Installing a standalone CCS Manager for a scale out deployment of CCS” on page 169.

If you want to install the application modules while installing the CCS Agent, you must copy the CCS_Agent/<platform> folder on the local computer. Then create a folder “AppModules” at the level of the SU folder, and copy the platform specific application module from the CCS_Agent/MBC/AppModules folder to the local computer in the following folder structure:

<platform folder>/esm1110/AppModules/<appmoduleinstaller.tpi>

For example, to install application modules for Oracle on Linux, create a folder structure as follows:

#/linux/intel/esm1110/AppModules/esmora.tpi

The installer installs this application module while installing the agent.

The installation process is as follows:

- Mount the disc drive.
- Perform the installation.

To mount the disc drive

1. Use su or log in to root on a computer with a UNIX operating system that has access to a disc drive.
2. Type the appropriate command to mount the disc drive to device /dvdrom.

To start the installer

1. Use su or log in to root on the computer with a UNIX operating system that you use to install the CCS Agent software.
2. Mount the disc to /dvdrom .
3. Type `./esmsetup` to run the installer from the product disc.

   You can also run the installer from the /tmp directory if you use gzip to extract the file from the product disc. If you have copied the CCS Agent setup to the local computer for installing the application module during the agent installation, run the installer from the CCS Agent setup that is copied on the local computer.
4. Type **2** to perform a CCS Agent installation.
5. Type **A** if you agree to the terms of the license agreement.
6. Do one of the following:
   - Type the name of the directory where you want to install the CCS Agent files.

     Do not choose the root folder. The installer creates the directory if the directory does not already exist. The installer creates a /esm symbolic link that points to the directory.
   - Type **df** to list the partitions that have sufficient disk space to install the CCS Agent.
7. Do one of the following:
   - Type the name of the product disc drive that contains the distribution media.
   - Type the full path of the tar or tgz file on a disk.
   - Type the special device file name of the tape drive that contains the installation tape.
8. Type the name of the CCS Manager to which the Agent must be registered.
9. Type **y** if you want to register the Agent for message based data collection.

10 Type the port number of the CCS Manager.

11 Perform this step if you are registering the agent for message based data collection. You must first enable the CCS Application Server and CCS Manager for message based data collection.

See "Enabling message based data collection" on page 205.

Type **ESM**.

12 Perform this step if you are registering the agent for message based data collection.

Type the ESM password which you have set while enabling the CCS Manager for message based data collection.

13 Type the name of the computer you are installing agent on. The CCS Manager uses the name to search for the IP address of the agent computer. This name can have up to 61 characters.

14 Type **y** to verify the manager to agent communication.

15 Type **y** if you want to register this agent with one more CCS Manager.

Perform steps 8 to 14 to register the agent with one more manager.

Type **n** if you do not want to register the agent with more CCS Managers.

16 Type **y** if you want to copy the ICE module scripts to the agent.

17 Do one of the following:

- Type **1** to disable LiveUpdate on the agent.
- Type **2** to enable all managers that register the agent to update the agent.
- Type **3** to select the managers that can update the agent.

18 Type **y** if you want to specify a preferred IP address of the computer you are installing the agent on. The CCS Manager uses the IP address you specified while connecting to the Asset.

19 Type the preferred IPv4 address that the CCS Manager uses to connect with the asset.

20 Type the complete path to locate the TPK to be installed on the CCS Agent. The file name is esm.tpk. The esm.tpk is the installer for Security Updates for message based data collection.

Note: The path for esm.tpk or ccs.tpk must include the file name of the tpk file. For example, to specify the location of the esm.tpk file for Solaris SPARC, ensure that the path includes the file name as shown below:

```
Installset\CCS_Agent\unix\sun\solaris\sparc\esm1110\su\esm.tpk
```

21 Type the complete path to locate the CCS TPK to be installed on the CCS Agent. The file name is ccs.tpk. The ccs.tpk is the installer for Security Updates for raw-data based collection.

Setup installs the CCS Agent. If you are installing the application module during the agent installation, the setup detects and installs the application module you have copied to the local computer.

See "Installing the manager and the agent by using the advanced installation option" on page 196.

See "Installing and registering a CCS Agent on UNIX in silent mode" on page 235.

See "Configuring CCS Agents for message based data collection " on page 203.

See "Installing the CCS Agent on Windows" on page 185.

See "CCS Suite deployment sequence " on page 140.

Installing the manager and the agent by using the advanced installation option

You can use the advanced installation option to install the ESM manager and the agent on UNIX platforms. The advanced installation procedure consists of various phases. The successful installation of an ESM component depends on the successful completion of all the selected phases, based on the component that you select.

During agent installation if you want to install an application module, then you must manually create a folder structure. The installer identifies the folder and installs the application module from it.

To create an application module folder

- Create a folder “AppModules” at the level of the SU folder and a structure within that folder as follows:

  #/<platform folder>/esm1110/AppModules/<appmoduleinstaller.tpi>

  For example, create an application module folder structure for oracle as follows:

  #/linux/intel/esm1110/AppModules/esmora.tpi

To install the agent by using the advanced installation option

1. Use su or log on to root on the computer with a UNIX operating system that you use to install the Symantec ESM software.
2. Copy the disc to the /dvdrom directory.
3. Type `./esmsetup` to run the Symantec ESM installer from the product disc.

   You can also run the Symantec ESM installer from the /tmp directory if you use gzip to extract the file from the product disc.

To select the advanced installation option

1. Type a **3** to select the advanced installation option and then type a **y** to continue with the installation.
2. Type the values for the respective installation phases that you want to execute.

   Note: A new phase has been added to the existing ones, “Phase 15” - titled Execute the rename_agent_binary fix for the installed manager. This phase must be selected by the user when upgrading from ESM Manager version 6.5.3 or earlier.

3. Type an **A** if you agree to the terms of the Symantec License Agreement.
4. Press Enter to continue with the advanced installation. By pressing Enter, you acknowledge that you have successfully completed the installation of the previous phases.
5. Do one of the following:
   - Type a **1** to perform an ESM agent installation.
   - Type a **2** to perform an ESM manager installation.
     The manager installation includes the agent installation too.

     Note: You get the option to choose the manager installation only if the manager is supported on the current operating system.

To install an agent by using the advanced installation option

1. After you choose to install the agent, press Enter to see the disk space requirements and the available space on your local computer.
2. Type the location where you want to install the agent. If you want to check the available disc space on your local computer, then type a **?**.
3. Specify the special device file name of the tape drive that contains the installation tape. You may also enter the full path of the tar/tgz file that is located on the disc.
4. Press Enter.
5. Enter the manager name to which you want to register the agent.
6. Enter the port number that the agent should use to contact the manager.
7. Enter the user name who owns the ESM files and then press Enter.
8. Enter the password for the user account that you specified and then press Enter.
9. Enter the IP address, Hostname, or FQDN of the agent that you want to register to the specified manager.
10. Type **y** to verify Manager to Agent communication.
11. Do one of the following:
    - If you want to register the agent to multiple agents, then type a **y**, and then repeat the steps 1 to 10.
    - Type an **n** to continue with the installation and registration of the agent.
12. Type a **y** if you want to copy the ICE module scripts to the agent.

    The setup continues to install the ESM agent.

To install a manager by using the advanced installation option

1. After you choose to install the manager, press Enter to see the disk space requirements and the available space on your local computer.
2. Type the location where you want to install the agent. If you want to check the available disc space on your local computer, then type a **?**.
3. Press Enter.
4. Enter the user account that has the superuser permissions on the ESM files.
5. Enter the group ownership for the ESM files and then press Enter.

6 Specify the special device file name of the tape drive that contains the installation tape and then press Enter.

You may also enter the full path of the tar/tgz file that is located on the disc.

7 Enter the password for the ESM superuser account and then press Enter.

8 Re-type the superuser password to authenticate the user account credentials.

9 Enter the IP address, Hostname, or FQDN of the agent that you want to register to the specified manager.

10 Press Enter.

11 Type **y** to verify Manager to Agent communication.

To specify the LiveUpdate option

1 Do one of the following to choose the LiveUpdate option:

- Type a **1** to disable LiveUpdate.
- Type a **2** to enable Liveupdate.
- Type a **3** to specify the manager that is allowed to perform LiveUpdate on the agent.

2 If you typed a **3**, then type a y to enable the manager to perform LiveUpdate on the agent.

3 Type **n** if you do not want to deploy the Manager TPK during upgrade (y/n)? [y]

4 Select **y** if you want to copy the agent remote upgrade packages to the ESM Manager (y/n)? [n]

Note: If you select 'y', the existing agent remote upgrade packages on the manager will be overwritten.The setup should find the agent remote upgrade packages for each operating system in a separate directory at the specified location. For example: If Remote Upgrade package for Linux (lnx-x86 folder) is present in /RU/Agent, then the path will be /RU/agent/. Specify the source directory for the agent remote upgrade packages as follows: /ccs_builds/RU_pkg .

---

5 Enter the complete path of the TPK to be installed: [//<platform>/esm1110/su/esm.tpk]

6 Enter the complete path of the CCS TPK to be installed:
[//<platform>/esm1110/su/ccs.tpk]

7 Type a **y** if you want to copy the ICE module scripts to the agent.

The setup continues to install the ESM manager and the agent.

Registering the CCS Agent on UNIX

When you register a CCS Agent with a manager you establish a secured communication between the agent and manager. You can register up to 4000 agents to one CCS Manager during or after the CCS Agent installation. You can register one agent to as many managers as you want.

Do not use more than one agent name to register a CCS Agent to a manager. You can register an CCS Agent to multiple CCS Managers during or after the installation. However, for the registration to succeed, each CCS Manager must be in the connected state.

The manager must be running to register the agent. If the manager is not running, you restart the manager and use the Register agent option in the installer to register the agent.

CCS Agents can only register with the managers that use the same communication protocol.

Perform the following procedure before registering the CCS Agent:

Install the CCS Agent. See “Installing the CCS Agent on UNIX” on page 192.

To register a CCS Agent on UNIX

1 Use su or log in to root on the agent computer.

2 Type `./esmsetup` to run the installer from the product disc.

You can also run the installer from the /tmp directory if you use gzip to extract the file from the product disc.

3 Type `4` to select the post-installation configuration options.

4 Type `4` to register the CCS Agent with a CCS Manager.

5 Type the name of the CCS Manager to which the Agent must be registered.

6 Type **y** if you want to register the Agent for message based data collection.

7 Type the port number of the CCS Manager.

8 Perform this step if you are registering the agent for message based data collection. You must first enable the CCS Application Server and CCS Manager for message based data collection.

See "Enabling message based data collection" on page 205.

Type **ESM**.

9 Perform this step if you are registering the agent for message based data collection.

Type the ESM password which you have set while enabling the CCS Manager for message based data collection.

10 Type the name of the computer that is to install the agent. The CCS Manager uses the name to search for the IP address of the agent computer. This name can have up to 61 characters.

11 Type **y** to verify the manager to agent communication.

12 Type **y** if you want to register this agent with one more CCS Manager.

Perform steps 8 to 8 to register the agent with one more manager.

Type **n** if you do not want to register the agent with more CCS Managers.

13 Type **y** if you want to specify a preferred IP address of the computer you are installing the agent on. The CCS Manager uses the IP address you specified while connecting to the Asset.

14 Type the preferred IPv4 address that the CCS Manager uses to contact to the asset.

See "Changing the LiveUpdate setting for an agent" on page 201.

See "CCS Suite deployment sequence " on page 140.

Changing the LiveUpdate setting for an agent

You can specify whether or not the agent can be updated. You can also specify which managers can update the agent. You must change the setting on the local agent computer as well as from the Symantec ESM console.

Note: If a manager is connected to multiple consoles, do not apply LiveUpdate simultaneously on that manager from the different consoles where the manager is connected.

To change the LiveUpdate setting for an agent

1. Use su or log in to root on the agent computer.
2. Navigate to the <installdir> and run the Symantec ESM installer.
3. Type **4** to select the post-installation options.
4. Type **6** at the Symantec ESM installation phases prompt.
5. At the LiveUpdate prompt, do one of the following:
   - Type **1** to disable LiveUpdate on the agent.
   - Type **2** to enable the managers that register the agent to run LiveUpdate on the agent.
   - Type **3** to select the managers that can run LiveUpdate on the agent.

Installing the SQL Server content on CCS Agents for raw-data collection on SQL Server

You must install the SQL Server content for raw-data collection on SQL Server through the CCS Agents.

The SQL Server content installation file `ccsmssqltpi.exe` is located in the CCS_Agent\RBC\AppModules\MSSQL\winx folder of the product media.

Perform the following procedure before installing the SQL Server content:

Install the CCS Agent. See "Installing the CCS Agent on Windows" on page 185.

To install the SQL Server content on the CCS Agent

1. Run the `ccsmssqltpi.exe` file located in the CCS_Agent\win\AppModules\MSSQL\winx folder of the product media.
2. Choose one of the following options:

Option 1	To display the contents of the package.
Option 2	To install the module.

3. The **Do you wish to register the agent to the manager: [no]?** message appears. Do one of the following:
   - Type **Y** to register the agent to the manager. Perform steps 4 to 8.
   - Type **N**, if you do not want to register the agent to the manager. Skip to step 11.

4 Enter the CCS Manager that the agent is registered to.

Usually, it is the name or the IP of the computer that the manager is installed on.

5 The **Enter the network protocol that you use to connect to the CCS manager:** message appears. Do one of the following:

- Type **1**, if you use the IPX protocol.
- Type **2**, if you use the TCP protocol.

6 Enter the port that is used to contact the CCS Manager. The default port is 5600.

7 Enter the name of the computer the agent is installed on. The CCS Manager uses the name to search for the IP address of the agent computer. This name can have up to 61 characters.

8 The **Is this information correct?** message appears. Do one of the following:

- Type **Y**, the program continues with the installation.
- Type **N**, the setup prompts to re-enter the details of the new manager.

When you type **Y** the program installs the content on the agent computer.

When the installation completes, you are prompted to exit.

See "Configuring CCS Manager data collectors" on page 180.

See "CCS Suite deployment sequence " on page 140.

Configuring CCS Agents for message based data collection

If you are using the CCS Agent for message based data collection, you must install the application modules and security content on **CCS Managers** and **CCS Agents**. You must first install the platform specific application modules and security content on the CCS Agents and then import the security content to the respective CCS Manager using the importcontent utility. The security content consists of the security module(.m) files, property files, template files, word files and report content (UpdatePackage.rdl) files for security updates as well as application modules. A new folder named, **Content** is created on the CCS Manager that contains platform-specific data, which the importcontent utility imports.

See "Supported target computers and databases for data collection" on page 48.

To configure the CCS Agents for message based data collection

If you want to use predefined CCS message based content for evaluating Windows and UNIX assets, only perform steps 1, 4 and 6.

1 Enable CCS for message based data collection.

See "Enabling message based data collection" on page 205.

2 Install the platform specific application modules and security content on CCS Agent.

See "Installing the application modules on CCS Agent on Windows" on page 207.

See "Installing the application modules on CCS Agent on UNIX" on page 209.

See "Installing the application modules on CCS Agent on Windows in silent mode" on page 238.

See "Installing the application modules on CCS Agent on UNIX in silent mode" on page 239.

3 Install the security content on the CCS Manager.

See "Installing the security content on CCS Manager" on page 211.

- If you want to import security content on CCS Manager during the installation of the security content, you can modify the importcontent.conf file, to include or exclude platforms that are available to the CCS Manager when using the importcontent utility.
  See "Modifying the importcontent.conf file" on page 212.
- If you want to import security content on CCS Manager during the installation of the security content, you must run the importcontent utility.
  See "Importing security content on CCS Manager using the importcontent utility" on page 212.

4 For Windows and UNIX platforms, ensure that corresponding standards of the predefined CCS message based content are installed on the CCS Application Server, corresponding policies are installed on the CCS Manager and content is installed on the CCS Agent. You can use the CCS Content installer to install content on the CCS Application Server and CCS Manager. For CCS Agent, you can install content during the agent installation. For the list of predefined msg based content shipped with CCS 11.1, See "Predefined CCS message based content for Windows and UNIX" on page 215.

   For other platforms such as SQL, Oracle, DB2, Sybase, or VMware, or for creating custom policies for Windows and UNIX, you must create the policies using the ESM Console, and then run the ESM Policy to CCS Standard Migration Utility, to map the ESM policies to CCS standards. See the *About the Symantec ESM Policy to CCS Standard Migration Utility* section in the *Symantec Control Compliance Suite User Guide*.

5 Configure the application modules on CCS Agent for data collection

   For information on configuring the application modules, refer to the specific application module documentation located inside the ESM Components\Documentation folder of the product media.

6 Run the Import assets and agents job to create agent-based assets. See the *Importing assets and agents* section in the *Symantec Control Compliance Suite User Guide*.

See "CCS Suite deployment sequence " on page 140.

Enabling message based data collection

You must enable message based data collection in CCS before registering a CCS Agent for message based data collection. You must perform the following steps to enable message based data collection in CCS.

Perform the following procedures before enabling message based data collection:

Install the CCS Application Server. See "Installing the CCS Suite" on page 140.

Install the CCS Manager. You can install the CCS Manager along with the CCS Application Server on a single computer, See "Installing the CCS Suite" on page 140.

You can add a CCS Manager to an existing installation of the CCS Application Server, See "Adding or upgrading CCS components" on page 286.

You can install a standalone CCS Manager. See "Installing a standalone CCS Manager for a scale out deployment of CCS" on page 169.

To enable message based data collection

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 **Settings > General**.
5. In the **General** view, on the left panel, click **Application Configuration > Standards**.
6. On the right panel, under CCS Standard Settings, check **Enable message based content**.
7. Go to the **System Topology > Grid View** or **System Topology > Map View**.
8. Right-click the CCS Manager to be configured for message based data collection, and click **Edit Settings**.
9. In the **Edit Settings** dialog box, in the left pane, under **Symantec CCS Manager**, click **Basic**.
10. On the **CCS Manager - Basic** panel, in the Configure Message Based Content section, enter the ESM password.

    You need to provide the ESM password while registering a CCS Agent for message based data collection.
11. Confirm the ESM password, and then click **Apply**
12. Click **Save** to save the changes.

See “Installing the application modules on CCS Agent on Windows” on page 207.

See “Installing the application modules on CCS Agent on UNIX” on page 209.

See “Installing the application modules on CCS Agent on Windows in silent mode” on page 238.

See “Installing the application modules on CCS Agent on UNIX in silent mode” on page 239.

See “Importing security content on CCS Manager using the importcontent utility” on page 212.

See “CCS Suite deployment sequence ” on page 140.

Installing the application modules on CCS Agent on Windows

Symantec recommends that if you are deploying content for the first time, run the platform specific content installer to install the content. Platform specific content installers and related documentation is located in the CCS_Agent\MBC\AppModules folder of the product media. For the consecutive releases, perform a LiveUpdate to get the latest security content.

For example if you want to install content for the Oracle platform on Windows 2003 32 bit operating system, run the **esmoracletpi.exe** installer located inside the CCS_Agent\MBC\AppModules\Oracle\w3s-ix86 folder of the product media.

The installation program extracts and installs configuration (.m) files, template files, word files, .properties files, and report content files (RDL).

Perform the following procedure before installing the application modules on CCS Agent on Windows:

Install the CCS Agent. See “Installing the CCS Agent on Windows” on page 185.

To install the security content on the CCS Agents

1. Run **esmoracletpi.exe** file.
2. Choose one of the following options:

Option 1	To display the contents of the package.
Option 2	To install the module.

3. The **Do you wish to register the agent to the manager: [no]?** message appears. Do one of the following:
   - Type **Y** to register the agent to the manager. Perform steps 4 to 8.
   - Type **N**, if you do not want to register the agent to the manager. Skip to step 11.
4. Enter the CCS Manager that the agent is registered to.

   Usually, it is the name or the IP of the computer that the manager is installed on.
5. Enter the ESM access name (logon name) for the manager.
6. Enter the ESM password that is used to log on to the CCS manager.

7 The **Enter the network protocol that you use to connect to the ESM manager:** message appears. Do one of the following:

- Type **1**, if you use the IPX protocol.
- Type **2**, if you use the TCP protocol.

8 Enter the port that is used to contact the CCS Manager. The default port is 5600.

9 Enter the name of the computer the agent is installed on. The CCS Manager uses the name to search for the IP address of the agent computer. This name can have up to 61 characters.

10 The **Is this information correct?** message appears. Do one of the following:

- Type **Y**, the program continues with the installation.
- Type **N**, the setup prompts to re-enter the details of the new manager.

When you type **Y** the program extracts the configuration (.m) files, template files, word files, .properties files, and report content files (RDL) on the CCS Agent.

11 The **Do you want to continue and add configuration records to enable the ESM security checking for the Oracle server?** message appears. Do one of the following:

- Type a **Y**, to provide the Oracle connection information. Perform step 4.
- Type an **N**, to end the installation without adding the security checks.

Note: Prompts for connecting to the database differ according to which application module you are installing. For example, the prompts for connecting to the Oracle server are different from those for connecting to the SQL Server. Refer to the specific application module documentation located inside the ESM Components\Documentation folder of the product media.

---

12 Specify the Oracle connection options. Do one of the following:

- Type **A**, to connect using the SYSTEM account.
- Type **B**, to connect using the "/as sysdba" method.

Provide the user account credentials. When the installation completes, you are prompted to exit.

After you install the application modules, you must configure the application modules for data collection. For information on configuring the application modules, refer to

the specific application module documentation located inside the ESM Components\Documentation folder of the product media.

See "Importing security content on CCS Manager using the importcontent utility" on page 212.

Installing the application modules on CCS Agent on UNIX

Symantec recommends that if you are deploying content for the first time, run the platform specific content installer to install the content. Platform specific content installers and related documentation is located in the CCS_Agent\MBC\AppModules folder of the product media. For the consecutive releases, perform a LiveUpdate to get the latest security content.

For example if you want to install content for the Oracle platform on solaris-sparc, run the **esmora.tpi** installer located inside the CCS_Agent\MBC\AppModules\Oracle\solaris-sparc folder of the product media.

The installation program extracts and installs configuration (.m) files, template files, word files, .properties files, and report content files (RDL).

Perform the following procedure before installing the application modules on CCS Agent on UNIX:

Install the CCS Agent. See "Installing the CCS Agent on UNIX" on page 192.

To install the security content on the CCS Agents

1. Run **esmora.tpi** file using the command `./esmora.tpi`.
2. Choose one of the following options:

Option 1	To display the contents of the package.
Option 2	To install the module.

3. The **Do you wish to register the agent to the manager: [no]?** message appears. Do one of the following:
   - Type **Y** to register the agent to the manager. Perform steps 4 to 9.
   - Type **N**, if you do not want to register the agent to the manager. Skip to step 10.
4. Enter the CCS Manager that the agent is registered to.

   Usually, it is the name or the IP of the computer that the manager is installed on.
5. Enter the ESM access name (logon name) for the manager.

6 Enter the ESM password that is used to log on to the CCS manager.

7 Enter the port that is used to contact the CCS Manager. The default port is 5600.

8 Enter the name of the computer the agent is installed on. The CCS Manager uses the name to search for the IP address of the agent computer. This name can have up to 61 characters.

9 The **Is this information correct?** message appears. Do one of the following:

- Type **Y**, the program continues with the installation.
- Type **N**, the setup prompts to re-enter the details of the new manager.

When you type **Y** the program extracts the configuration (.m) files, template files, word files, .properties files, and report content files (RDL) on the CCS Agent.

10 The **Do you want to continue and add configuration records to enable the ESM security checking for the Oracle server?** message appears. Do one of the following:

- Type a **Y**, to provide the Oracle connection information. Perform step 4.
- Type an **N**, to end the installation without adding the security checks.

Note: Prompts for connecting to the database differ according to which application module you are installing. For example, the prompts for connecting to the Oracle server are different from those for connecting to the SQL Server. Refer to the specific application module documentation located inside the ESM Components\Documentation folder of the product media.

---

11 Specify the Oracle connection options. Do one of the following:

- Type **A**, to connect using the SYSTEM account.
- Type **B**, to connect using the "/as sysdba" method.

Provide the user account credentials. When the installation completes, you are prompted to exit.

After you install the application modules, you must configure the application modules for data collection. For information on configuring the application modules, refer to the specific application module documentation located inside the ESM Components\Documentation folder of the product media.

See “Importing security content on CCS Manager using the importcontent utility” on page 212.

Installing the security content on CCS Manager

You must install the security content on CCS Manager for message based data collection. The security content consists of the security module (.m) files, template files, word files, .properties files, and report content files (RDL). A new folder named, Content is created on the CCS Manager that contains platform-specific data.

For example if you want to install content for the Oracle platform, run the **esmoraclecontenttpi.exe** installer located inside the ESM Components\ManagerContent\AppModules\Oracle\win-ix86 folder of the product media.

Perform the following procedure before installing the security content on the CCS Manager:

Install the CCS Manager. You can install the CCS Manager along with the CCS Application Server on a single computer, See "Installing the CCS Suite" on page 140.

You can add a CCS Manager to an existing installation of the CCS Application Server, See "Adding or upgrading CCS components" on page 286.

You can install a standalone CCS Manager. See "Installing a standalone CCS Manager for a scale out deployment of CCS" on page 169.

To install the security content on the CCS Manager

1. Run **esmoraclecontenttpi.exe** file.
2. Choose one of the following options:

Option 1	To display the contents of the package.
Option 2	To install the module.

3. The **Do you want to import the templates or the .m files? [no]** message appears. Do one of the following:
   - Type **Y** to import the templates or the .m files.
     The program displays a message to include or exclude the platforms that you want to import. See "Modifying the importcontent.conf file" on page 212.
   - Type **N**, if you do not want to import the templates or the .m files.
     You can skip this step if you want to import the content later. You can import the content by running the importcontent utility. See "Importing security content on CCS Manager using the importcontent utility" on page 212.
4. Enter the CCS Manager that the agent is registered to.

   Usually, it is the name or the IP of the computer that the manager is installed on.

5 Enter the ESM access name (logon name) for the manager.

6 Enter the ESM password that is used to log on to the CCS manager.

7 Enter the port that is used to contact the CCS Manager. The default port is 5600.

8 The **Is this information correct?** message appears. Do one of the following:

- Type **Y**, the program continues with the installation.
- Type **N**, the setup prompts to re-enter the details of the new manager.

When you type **Y** the program extracts the configuration (.m) files, template files, word files, .properties files, and report content files (RDL) on the CCS Agent.

9 The **Do you want to import the report content file <UpdatePackage.rdl>? [yes]** message appears. Do one of the following:

- Type a **Y** to import the report content file.
- Type an **N**, if you do not want to import the report content file.

When the installation completes, you are prompted to exit.

Modifying the importcontent.conf file

The platforms that you specify in the importcontent.conf file are the platforms that are available to the CCS Manager when using the importcontent utility. The importcontent utility only imports the platforms on the CCS manager that are not prefixed with a hash (#).

To modify the importcontent.conf file

1 Go to <install_directory>\Symantec\Reporting and Analytics\ESM\config\importcontent.conf.

2 Add a # before the platform that you want to exclude.

3 Save the file.

4 Go back to esmoraclecontenttpi.exe installer and press <return> to continue with the installation process.

See “Installing the security content on CCS Manager” on page 211.

Importing security content on CCS Manager using the importcontent utility

Importcontent utility is a command line utility, used to import the application modules and security content information to the specified CCS Manager. The utility displays

the content version on the GUI or on the CLI. The utility is located in the bin folder of the installation directory, along with other ESM Manager binaries in platform-specific folders.

For example, <install_directory>\Symantec\CCS\Reporting and Analytics\ESM\bin\w8s-ix86\importcontent.exe.

You can use the importcontent utility on Windows and UNIX platforms. The utility provides the option of importing security module (.m) files, property (.properties) files, template files, word (.wrd) files, and report content (UpdatePackage.rdl) files for the application modules. You can use the -f option to force import content related information at a later stage.

Pre-requisites for using the importcontent utility:

- You must be in the role of ESM administrator.
- You must have CCS Manager installed on the computer on which you are running the importcontent utility.
- You must be in the role of an administrator of the computer to run the importcontent utility.

Perform the following procedure before importing security content on CCS Manager using the importcontent utility:

Install the CCS Manager. You can install the CCS Manager along with the CCS Application Server on a single computer, See “Installing the CCS Suite” on page 140.

You can add a CCS Manager to an existing installation of the CCS Application Server, See “Adding or upgrading CCS components” on page 286.

You can install a standalone CCS Manager. See “Installing a standalone CCS Manager for a scale out deployment of CCS” on page 169.

Install the application modules on the CCS Agent. See “Installing the application modules on CCS Agent on Windows” on page 207.

See “Installing the application modules on CCS Agent on UNIX” on page 209.

To use the importcontent utility

1. At the Windows command prompt, navigate to the platform-specific bin folder, where the importcontent utility is located.
2. Type the following command:

   ```
   importcontent [-RLrnvfW] [-m manager] [-U user] [-P password] [-p
   port] [-L app_module_name1, app_module_name2,...] [-a |
   module_config_file1 [module_config_file2... ]]
   ```

   The switch options that can be used with the importcontent utility are listed below.

Table 3-7 Switch options for the importcontent utility

Switch	Description
-m	Manager name - the local manager name is used by default.
-U	User name - the ESM user name is used by default.
-P	Password - the ESM user account password.
-p	TCP port number to connect to the CCS Manager - the port number is 5600 by default.
-L	Import application module, Security Update contents (SU) or language pack. For example: ■ To import an application module, use `-L app_module_name`. ■ To import an SU, use `-L su`. ■ To import a language pack, use `-L langpack`.
-a	Import and register all security module (.m) files with the manager.
-R	Import property files (.properties).
-T	Import all templates.
-r	Import report content file (UpdatePackage.rdl).
-W	Import word files.
-n	Synchronize policies.
-f	Force the import of security module information.
-h	Write C include file for security module compilation. **Note:** -h, and -M options can be used only with the -a option.
-M	Write VMS macro file for security module compilation. **Note:** -h, and -M options can be used only with the -a option.
-v	Set verbose mode, log each action as it is performed.
-F	Log the program finish.

See "Examples of using the importcontent utility" on page 215.

Examples of using the importcontent utility

The following examples are provided for using the importcontent utility:

- To access the help menu for the importcontent utility, type the following command:

  ```
  importcontent
  ```

- To import Oracle Application modules type the following command:

  ```
  importcontent -L oracle -U <user1> -P <pwd123> -m <managerXYZ>
  ```

  Note: The utility requires the application module names to be similar to the folder names created in the <install dir>\ content directory.

- To import templates for Oracle, type the following command:

  ```
  importcontent -T -L oracle -U <user1> -P <pwd123> -m <managerXYZ>
  ```

- To synchronize policies, type the following command:

  ```
  importcontent -nv -U <user1> -P <pwd123> -m <managerXYZ> -U <user1>
  -P <pwd123>
  ```

- To register specific .m files with the manager, type the following command:

  ```
  importcontent -U <user1> -P <pwd123> -m <managerXYZ>
  C:\Symantec\ESM\account.m D:\ESM\acctinfo.m E:\abc.m xyz.m
  ```

See "Importing security content on CCS Manager using the importcontent utility" on page 212.

Predefined CCS message based content for Windows and UNIX

CCS 11.1 provides the following predefined message based content with ESM policies mapped to CCS standards. For platforms such as SQL, Oracle, DB2, Sybase, or VMware, or for creating custom policies for Windows and UNIX, you must create the policies using the ESM Console, and then run the ESM Policy to CCS Standard Migration Utility, to map the ESM policies to CCS standards. See the *About the Symantec ESM Policy to CCS Standard Migration Utility* section in the *Symantec Control Compliance Suite User Guide*.

Table 3-8 Predefined message based content with ESM policies mapped to CCS standards

ESM policy	CCS standard
HPUX_11i_CIS.exe	CIS Security Benchmark for HP-UX v1.5.0
RHEL_5_CIS.exe	CIS Benchmark for Red Hat Enterprise Linux 5.0-5.1 v1.1.2
Solaris10_SecurityEssentials.exe	CIS Security Benchmark for Sun Solaris 10 V4.0
Solaris_SOA_Change_Notification.exe	Change Notifications for UNIX
Windows_2003_SecurityEssentials.exe	CIS Legacy Security Settings Benchmark for Windows 2003 Domain Controller v2.0 CIS Windows Server 2003 Legacy Security Settings for Domain Member Servers v2.0
Windows_2003_SOA_Change_Notification.exe	Change Notifications for Windows
Windows_2008_CIS.exe	CIS Security Benchmark for Windows 2008 Domain Controller v1.0.0 CIS Security Benchmark for Windows 2008 Domain Member Servers v1.0.0

See "Configuring CCS Agents for message based data collection " on page 203.

Launching the CCS Web Console and the Policy Central

The CCS Web Console and the Policy Central are installed along with the installation of the CCS Application Server. Symantec recommends a screen resolution with an aspect ratio of 1024 x 768 to access the CCS Web Console or the Policy Central.

For a list of prerequisites required by the CCS Web Console and the Policy Central, including a list of supported web browsers, See "Software requirements" on page 48.

Perform the following procedure before launching the CCS Web Console or the Policy Central:

Install the CCS Application Server. See "Installing the CCS Suite" on page 140.

You can launch the CCS Web Console or the Policy Central on a FIPS enabled computer or a non-FIPS enabled computer.

Note: In a FIPS enabled environment if the Web server is configured to use only SSL connection, then the CCS Web Console or the Policy Central fails to launch on a remote computer .

To launch the CCS Web Console or the Policy Central from the CCS Console, you can use the respective links provided on the CCS Console homepage.

To launch the CCS Web Console or the Policy Central

- Open a web browser on the computer on which you want to launch the CCS Web Console or the Policy Central, and type the following URL:

  For the CCS Web Console:

  http://<Computer name or FQDN name of the Application Server>/CCS_Web

  For the Policy Central

  http://<Computer name or FQDN name of the Application Server>/CCS_Portal

To launch the CCS Web Console or the Policy Central on a FIPS enabled computer

1. Open a web browser on the computer on which you want to launch the CCS Web Console or the Policy Central.
2. Configure the web browser to use TLS 1.0.
3. Type the following URL to launch the CCS Web Console or the Policy Central:

   For the CCS Web Console:

   http://<Computer name or FQDN name of the Application Server>/CCS_Web

   For the Policy Central

   http://<Computer name or FQDN name of the Application Server>/CCS_Portal

For information on configuring the Policy Central, see the *Configuring the Policy Central Settings* section in the Symantec Control Compliance Suite User Guide.

Installing and launching the CCS Console

The CCS Console is installed on the computer on which the CCS Application Server is installed. You can either launch the CCS Console on the computer on which the CCS Application Server is installed or launch it on a remote computer. After you install the CCS Application Server, a shortcut of the CCS Console is created on the computer desktop. The CCS Console can also be launched on a remote computer through a browser that is supported by CCS.

You must know the prerequisites before you launch the CCS Console.

See “Software requirements” on page 48.

Perform the following procedure before installing and launching the CCS Console:

Install the CCS Application Server. See “Installing the CCS Suite” on page 140.

You must ensure that at any given point of time the CCS Console connects to only a single CCS Application Server.

Note: After upgrade from the previous release versions to CCS 11.1, any shortcut of the CCS modules that you created earlier are removed. The CCS modules are, Reporting, Assets, Standards, or so on. You can create shortcut of the CCS Console only on your computer desktop.

To launch the CCS Console on the CCS Application Server computer

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 on a remote computer

1 On the remote computer, open a web browser and type the following URL to launch the CCS Web Console:

http://<Computer name or FQDN name of Application Server>/CCS_Web/Downloads/GetConsole.aspx

For a list of browsers supported by the CCS Web Console, see See "Software requirements" on page 48.

If your website is SSL enabled you may encounter a certificate warning in the browser address bar. To resolve the certificate error, click Certificate Error to view the certificate. In the Certificate window, from the General tab, use the server name mentioned in the **Issued to** field in place of <Computer name or FQDN name of Application Server> in the above URL.

2 You must ensure that the software, Microsoft .NET Framework 4.0 is installed on the computer that launches the CCS Console. To check whether the software is installed or not, click on the link, **Check if .NET Framework 4.0 is installed**. If the software is not installed, then click on the link, **Install .NET Framework 4.0** for the appropriate platform to install it.

3 Click on the link, **Install Symantec Control Compliance Suite Console** to download and install the CCS Console.

Note: If you are using Mozilla Firefox or Google Chrome, you must install the following plugins on the respective browsers before you can download and install the CCS Console.

Plugin for Mozilla Firefox version 20.0

Plugin for Mozilla Google Chrome version 26.0

See "CCS Suite deployment sequence " on page 140.

Installing the CCS Content

Control Compliance Suite makes available a set of predefined Technical Standards, Frameworks and Regulations. When you install CCS for the first time, by default, the CCS Suite installer installs content for the following Technical Standards and Regulations.

CCS Suite installer installs content for the following Technical Standards by default:

- CIS Benchmark v1.1.2 for Red Hat Enterprise Linux 6.x
- CIS Oracle Database Server 11g Security Benchmark v1.0.1

- CIS Security Configuration Benchmark For Microsoft Windows Server 2012 v1.0.0
- Security Essentials for Microsoft SQL Server 2012

CCS Suite installer installs content for the following Regulations by default:

- COBIT 5th Edition
- PCI DSS v3.0
- IT Control Objectives for Sarbanes-Oxley 2nd Edition
- HIPAA HHS 45 CFR Part 164 Subpart C

You can install more content using the CCS Content installer. The CCS Maintenance license is required to install the CCS Content.

Perform the following procedure before installing the CCS Content:

Install the CCS Application Server. See "Installing the CCS Suite" on page 140.

Do the following to install the CCS Content:

- Launch the Installation Wizard.
  See "To launch the Installation Wizard" on page 220.
- Install the CCS Content.
  See "To install the CCS Content" on page 221.

Note: Symantec Control Compliance Suite 11.1 installation wizard displays the message-based content for Windows and UNIX platforms only if message-based data collection is enabled.

To enable message-based data collection, See "Enabling message based data collection" on page 205.

To launch the Installation Wizard

1 Insert the **Symantec Control Compliance Suite 11.1** product disc into the drive on your computer and click **Setup.exe**.

  In the security warning dialog box, click **Run**.

2 In the DemoShield, click **CCS Suite**.

  On the splash screen, click **Install CCS Content**. The Setup file is located inside the CCS_Content folder of the product media.

  Setup prepares the CCS Content installation wizard.

  See "Software requirements" on page 48.

To install the CCS Content

1. In the **Welcome** panel of the launched Symantec Control Compliance Suite 11.1 installation wizard, click **Next**.
2. In the **Add Components** panel, check the Technical Standards, Frameworks and Regulations which you require for the appropriate platform, and then click **Next**.

   You can select individual standards or select a platform name to select all standards for the particular platform.

   Message-based content for Windows and UNIX platforms appears only if message-based data collection is enabled.
3. In the **Installation Folder** panel, review the installation path for product installation.

   Click browse (**...**) to specify a different installation path to install the product.

   Click **Refresh disk space information** to verify the available disk space on the computer.
4. Click **Next**. If you have specified a different installation path, and the installer folder does not exist, the installer prompts you to create the installation folder.
5. In the **Summary** panel, review the installation details and then click **Install**.
6. The **Installation Progress** panel indicates the progress of the component installation. After the installation finishes, the **Finish** panel appears.
7. In the **Finish** panel, review the installation result and then click **Finish**.

   You can click the link, **Log Files** to view the CCS Content installation log files. The log files are in .csv format. You can use the LogViewer in the <Install_Directory>\Application Server to view the log files. The LogViewer helps you to easily identify warnings and errors using the color codes. Warnings are highlighted in yellow color and errors are highlighted in red color.

   You can check the option to view the release notes.

See “Installing CCS content in silent mode” on page 229.

See “Installing the SQL Server content on CCS Agents for raw-data collection on SQL Server” on page 202.

See “Configuring CCS Agents for message based data collection ” on page 203.

See “CCS Suite deployment sequence ” on page 140.

Installing the CCS components in silent mode

The silent installation mode in CCS is about installation of the CCS components on different computers in your network without navigating through the Installation Wizard. You must ensure that all computers on which the CCS components are to be installed in the silent mode belong to the same network. The main requisite for the silent installation is the `SilentInstallLauncher.exe` file and the response file.

In the silent mode of installation, no user interface is displayed. To install a CCS component in the silent mode you must run the `SilentInstallLauncher.exe` and provide the locations of the setup file and response file. The `SilentInstallLauncher.exe` triggers the silent installation of the setup and helps you to track the success or failure of the installation. The `SilentInstallLauncher.exe` displays return codes to help ascertain the status of the installation. If the return code is 0, that means the installation is successful.

See "About silent installation return codes" on page 241.

The response file is an XML file, which contains the inputs of the components that are to be installed. The response file is not specific to any operating system.

The CCS 11.1 product media contains response files for the following types of installations:

- Installing all CCS components on a single computer. This installs the CCS Application Server and CCS Manager on a single computer.
- Installing a standalone CCS Application Server.
- Installing a standalone CCS Manager.
- Installing the CCS Content.

The `SilentInstallLauncher.exe` file and the response files are located in the Documentation\Utilities\Silent Install folder of the product media.

The Documentation\Utilities\Silent Install folder of the product media also contains a batch file that you can use to run the silent installation commands. The file name is `Silent Install.bat`. Before running the batch file, you must edit the batch file to provide the location of the setup and response files for the particular installation.

Note: You must ensure that the computers on which the silent installation is triggered contain all the prerequisites, which you must install manually. CCS setup does not install any prerequisites automatically during the silent installation. See "Software requirements" on page 48.

See "Installing the CCS Suite in silent mode" on page 223.

See “Installing a standalone CCS Application Server in silent mode” on page 225.

See “Installing a standalone CCS Manager for scale-out deployment in silent mode” on page 228.

See “Installing CCS content in silent mode” on page 229.

See “About silent installation return codes” on page 241.

See “CCS Suite deployment sequence ” on page 140.

Installing the CCS Suite in silent mode

Perform the following procedure to install the CCS Suite in the silent mode. The CCS Suite consists of the CCS Application Server and the CCS Manager.

Read the end-user license agreement eula.txt located in the product media before proceeding with the installation.

All inputs required in the response file are case-sensitive. Ensure that you use the correct case for each value. For example, where "True" is required, enter "True" and not "true".

Note: You can install a CCS Application Server and CCS Agent on a single computer, but you cannot install a CCS Manager and a CCS Agent on a single computer. Therefore, you cannot install a CCS Manager along with the CCS Application Server on a computer that contains a CCS Agent.

See the following sections before installing the CCS Suite:

See “Hardware and operating system requirements” on page 37.

See “Network Ports” on page 41.

See “Software requirements” on page 48.

See “User Privileges for deploying the CCS components” on page 55.

See “User privileges for SQL server and CCS databases” on page 60.

To install the CCS Suite in silent mode

You can install the CCS Application Server and CCS Manager on a single computer.

1 You require the `CCS_Suite` response file to install the CCS components. The response file is located in the Documentation\Utilities\Silent Install folder of the product media. Copy the response file to the local computer, and then edit the response file to provide user inputs required during the installation.

For example, in the response file, provide the path of license file at `<License File="<path>"/>`

Where, `<path>` is the path of the license file, for example, `c:\Temp\2109884.sif`

The user inputs required in the response file correspond to the user inputs required during UI based installation. For detailed explanation of each input refer to the field description tables in the UI based installation section.

See "Installing the CCS Suite" on page 140.

Note: Do not set the value of `Use existing database` to `True`. Silent installation does not support using existing databases. To use existing databases, perform the installation using the UI based installer.

The CCS Core license is required to install the CCS Application Server and the CCS Maintenance license is required to install the default CCS Content during the CCS installation.

2 On the command prompt, navigate the location of the `SilentInstallLauncher.exe` file.

The `SilentInstallLauncher.exe` file is located in the Documentation\Utilities\Silent Install folder of the product media.

3 Run the following command to install all CCS components on a single computer:

```
SilentInstallLauncher.exe /SetupPath="SetupExePath"
/ResponseFile="ResponseFilePath"
/CertInfo.Password="CertInfopassword"
/MgmtServices.Password="MgmtServicespassword"
/EncryptMgmtService_PassPhrase.Password="EncryptMgmtServicepassword"
/AppServerService_PassPhrase.Password="AppServerServicepassword"
/AppServer.Password="AppServerpassword"
```

If you are using SQL authentication to connect to the SQL server, add the following switches to the above mentioned command.

- If the Product database and reporting database have the same configuration, or if you are configuring only the Production database on the CCS Suite computer, you must add the following switch:

```
/AppServerDB.Password="SQLpassword"
```

If the Product database and reporting database have different configuration, you must add the following switch:

```
/ReportingServerDB.Password="SQLpassword"
```

Where:

- `SetupExePath` is the location of the CCS setup file. The Setup file is located inside the CCS_Reporting folder of the product media.
- `ResponseFilePath` is the location of the response file for installing the CCS components. Provide the location of the response file you edited in Step 1.
- `CertInfopassword` is the password of the root certificate.
- `MgmtServicespassword` is the password of the Directory Service. The Directory Service user must be a domain user.
- `EncryptMgmtServicepassword` is the password required to generate the Encryption Management Service symmetric keys. You require this pass phrase later to change the service user account, and to make changes to the installation.
- `AppServerServicepassword` is the password required to generate the Application Server Service symmetric keys. You require this pass phrase later to change the service user account, and to make changes to the installation.
- `AppServerpassword` is the password of the CCS Application Server. The CCS Application Server user must be a domain user.
- `SQLpassword` is the SQL server user account password. The password is required if you are using SQL authentication to connect to the SQL server.

See "About silent installation return codes" on page 241.

Installing a standalone CCS Application Server in silent mode

Perform the following procedure to install the CCS Application Server in the silent mode.

Read the end-user license agreement eula.txt located in the product media before proceeding with the installation.

All inputs required in the response file are case-sensitive. Ensure that you use the correct case for each value. For example, where "True" is required, enter "True" and not "true".

Note: You cannot install the CCS Application Server on a computer that has a CCS Agent.

See the following sections before installing the CCS Application Server:

See "Hardware and operating system requirements" on page 37.

See "Network Ports" on page 41.

See "Software requirements" on page 48.

See "User Privileges for deploying the CCS components" on page 55.

See "User privileges for SQL server and CCS databases" on page 60.

To install the CCS Application Server in silent mode

1 You require the `CCS_Suite_WithoutCCSManager` response file to install the CCS components. The response file is located in the Documentation\Utilities\Silent Install folder of the product media. Copy the response file to the local computer, and then edit the response file to provide user inputs required during the installation.

For example, in the response file, provide the path of license file at `<License File="<path>"/>`

Where, `<path>` is the path of the license file, for example, `c:\Temp\2109884.sif`

The user inputs required in the response file correspond to the user inputs required during UI based installation. For detailed explanation of each input refer to the field description tables in the UI based installation section.

See "Installing the CCS Suite" on page 140.

Note: Do not set the value of `Use existing database` to `True`. Silent installation does not support using existing databases. To use existing databases, perform the installation using the UI based installer.

The CCS Core license is required to install the CCS Application Server and the CCS Maintenance license is required to install the default CCS Content during the CCS installation.

2 On the command prompt, navigate the location of the `SilentInstallLauncher.exe` file.

The `SilentInstallLauncher.exe` file is located in the Documentation\Utilities\Silent Install folder of the product media.

3 Run the following command to install the CCS Application Server:

```
SilentInstallLauncher.exe /SetupPath="SetupExePath"
/ResponseFile="ResponseFilePath"
/CertInfo.Password="CertInfopassword"
/MgmtServices.Password="MgmtServicespassword"
/EncryptMgmtService_PassPhrase.Password="EncryptMgmtServicepassword"
/AppServerService_PassPhrase.Password="AppServerServicepassword"
/AppServer.Password="AppServerpassword"
```

If you are using SQL authentication to connect to the SQL server, add the following switches to the above mentioned command.

- If the Product database and reporting database have the same configuration, or if you are configuring only the Production database on the CCS Suite computer, you must add the following switch:

  ```
  /AppServerDB.Password="SQLpassword"
  ```

  If the Product database and reporting database have different configuration, you must add the following switch:

  ```
  /ReportingServerDB.Password="SQLpassword"
  ```

Where:

- `SetupExePath` is the location of the CCS setup file. The Setup file is located inside the CCS_Reporting folder of the product media.
- `ResponseFilePath` is the location of the response file for installing the CCS Application Server. Provide the location of the response file you edited in Step 1.
- `CertInfopassword` is the password of the root certificate.
- `MgmtServicespassword` is the password of the Directory Service. The Directory Service user must be a domain user.
- `EncryptMgmtServicepassword` is the password required to generate the Encryption Management Service symmetric keys. You require this pass phrase later to change the service user account, and to make changes to the installation.
- `AppServerServicepassword` is the password required to generate the Application Server Service symmetric keys. You require this pass phrase later to change the service user account, and to make changes to the installation.
- `AppServerpassword` is the password of the CCS Application Server. The CCS Application Server user must be a domain user.
- `SQLpassword` is the SQL server user account password. The password is required if you are using SQL authentication to connect to the SQL server.

See “About silent installation return codes” on page 241.

Installing a standalone CCS Manager for scale-out deployment in silent mode

Perform the following procedure to install the CCS Manager in the silent mode.

Read the end-user license agreement eula.txt located in the product media before proceeding with the installation.

All inputs required in the response file are case-sensitive. Ensure that you use the correct case for each value. For example, where "True" is required, enter "True" and not "true".

See the following sections before installing the CCS Manager:

See “Hardware and operating system requirements” on page 37.

See “Network Ports” on page 41.

See “Software requirements” on page 48.

Note: You cannot install a CCS Manager on a computer that has a standalone CCS Agent installed, because the CCS Manager installation also contains the installation of CCS Agent.

Perform the following procedures before installing a standalone CCS Manager:

Install the CCS Application Server. See “Installing the CCS Suite” on page 140.

See “Installing the CCS Suite in silent mode” on page 223.

See “Installing a standalone CCS Application Server in silent mode” on page 225.

Create a certificate for the CCS Manager using the Certificate Management Console. The Certificate Management Console is installed along with the installation of the CCS Application Server. See “Creating a certificate for installing a standalone CCS Manager” on page 167.

To install the CCS Manager in silent mode

You can perform a standalone installation of the CCS Manager.

1 You require the `CCSManager` response file to install the CCS Manager. The response file is located in the Documentation\Utilities\Silent Install folder of the product media. Copy the response file to the local computer, and then edit the response file to provide user inputs required during the installation.

For example, in the response file, provide the folder location to install the CCS Manager at `<Property Name="Target path" Value="<path>"/>`

Where, `<path>` is the folder location to install the CCS Manager, for example, `c:\Program Files (x86)\Symantec\CCS\Reporting and Analytics`

Provide the following user inputs required to install the CCS Manager:

- Server port number
  Specify the port for the CCS Manager. The default CCS Manager port number is 5600. CCS components use this port to communicate with the CCS Manager.
- Data Processing Service
  Specify the location of the CCS Manager certificate. You must import the security certificate that is used by the CCS Manager to communicate with the CCS Application Server securely. The certificate which is to be deployed on the CCS Manager is created using the **Certificate Management Console**. The **Certificate Management Console** is installed on the CCS Application Server computer. You can either pull the certificate from the CCS Application Server computer or place it manually on the computer on which you are installing the CCS Manager.

2 On the command prompt, navigate the location of the `SilentInstallLauncher.exe` file.

The `SilentInstallLauncher.exe` file is located in the Documentation\Utilities\Silent Install folder of the product media.

3 Run the following command to install the CCS Manager:

```
SilentInstallLauncher.exe /SetupPath="SetupExePath"
/ResponseFile="ResponseFilePath"
/DPSCert.Password="DPSCertpassword"
```

Where:

- `SetupExePath` is the location of the CCS Manager setup file. The Setup file is located inside the CCS_Manager folder of the product media.
- `ResponseFilePath` is the location of the response file for installing the CCS Manager. Provide the location of the response file you edited in Step 1.
- `DPSCertpassword` is the password of the CCS Manager certificate that is imported while installing the CCS Manager.

See “About silent installation return codes” on page 241.

Installing CCS content in silent mode

Perform the following procedure to install additional CCS content in the silent mode.

Read the end-user license agreement eula.txt located in the product media before proceeding with the installation.

All inputs required in the response file are case-sensitive. Ensure that you use the correct case for each value. For example, where "True" is required, enter "True" and not "true".

Perform the following procedures before installing the CCS Content:

Install the CCS Application Server. See “Installing the CCS Suite” on page 140.

See “Installing the CCS Suite in silent mode” on page 223.

See “Installing a standalone CCS Application Server in silent mode” on page 225.

To install additional CCS content in silent mode

When you install CCS for the first time, by default, the CCS Suite installer installs content for some Technical Standards and Regulations.

To see the list of default content

See “Installing the CCS Content” on page 219.

You can install more content using the CCS Content installer.

1. You require the `CCSContent` response file to install the CCS content. The response file is located in the Documentation\Utilities\Silent Install folder of the product media. Copy the response file to the local computer, and then edit the response file to provide user inputs for content to be installed during the installation. To install content for a Technical Standard, Framework or Regulation, change the value to "true". Changing the value to "false" does not install the content for that Technical Standard, Framework or Regulation.

   For example, to install Standard Content, in the response file, provide the value for Enabled as "True" in `<Feature Name="Standard Content" Enabled="True"/>`. If you provide "False", Standard Content will not be installed.

   The CCS Maintenance license is required to install the CCS Content.

2. On the command prompt, navigate the location of the `SilentInstallLauncher.exe` file.

   The `SilentInstallLauncher.exe` file is located in the Documentation\Utilities\Silent Install folder of the product media.

3. Run the following command to install additional CCS content:

   ```
   SilentInstallLauncher.exe /SetupPath="SetupExePath"
   /ResponseFile="ResponseFilePath"
   ```

   Where:

- `SetupExePath` is the location of the CCS Content setup file. The Setup file is located inside the CCS_Content folder of the product media.
- `ResponseFilePath` is the location of the response file for installing the CCS Content. Provide the location of the response file you edited in Step 1.

See "About silent installation return codes" on page 241.

Installing and registering a CCS Agent on Windows in silent mode

When you install a CCS Agent, the installer prompts for necessary information such as the type of installation or the name of a directory. If you use the same settings to install the CCS Agent on a large number of computers, you can avoid the prompts by performing silent installations. The silent installation feature lets you install CCS Agents and register the agents to CCS Managers.

Note: To install an Agent with the latest updates, use the setup files for Agent installation available on the Symantec website.

If the silent installation fails for any reason, check the SymantecESMAgentInstall.log file at the Temp folder for the error logs. If the silent registration fails for any reason, check the SymantecESMAgentReg.log file at the following location for the error logs:

#\Symantec\CCS\Reporting and Analytics\ESM\system\<name of the computer where you have installed the agent>

Note: The GPGV.exe, which is a third-party application licensed by GNU GPL, is installed when you perform a silent or an interactive installation of Symantec ESM. The GPGV.exe installs in the same location where you install Symantec ESM. Symantec ESM internally uses the GPGV.exe for security verification.

See the following sections before installing the CCS Agent:

See "Hardware and operating system requirements" on page 37.

See "Network Ports" on page 41.

See "Supported target computers and databases for data collection" on page 48.

See "Software requirements" on page 48.

Note: You cannot install a standalone CCS Agent on a computer that contains a CCS Manager, because the CCS Manager installation also contains the installation of CCS Agent.

Perform the following procedure before installing the CCS Agent:

Install the CCS Manager. You require a CCS Manager for the CCS Agent to register to. However, you cannot install a CCS Agent on a computer that contains a CCS Manager.

Do one of the following:

- Install the CCS Manager along with the CCS Application Server on a single computer, See “Installing the CCS Suite” on page 140.
  See “Installing the CCS Suite in silent mode” on page 223.
- Add a CCS Manager to an existing installation of the CCS Application Server, See “Adding or upgrading CCS components” on page 286.
- Install a standalone CCS Manager. See “Installing a standalone CCS Manager for a scale out deployment of CCS” on page 169.
  See “Installing a standalone CCS Manager for scale-out deployment in silent mode” on page 228.

To silently install an agent

1. Log on as administrator to the computer on which you want to install the CCS Agent. Alternatively, use a role that is equivalent to an administrator.
2. Copy the CCS_Agent\win folder from the product media to a network installation folder or to a local folder.
3. Copy the `AgentSilentInstallSample.bat` file from the CCS_Agent\win\examples folder of the product media. Save the `AgentSilentInstallSample.bat` file in the CCS_Agent\win folder that you copied to a local folder. You must save the `AgentSilentInstallSample.bat` file at the location where the Setup.exe is present for installing the agent.

   For security purpose, you can use an encrypted password to install the CCS Agent. For information on creating an encrypted password see To create an encrypted password.
4. Right-click the `AgentSilentInstallSample.bat` file, and select **Edit**.
5. Specify the parameters of <COMMANDLINE>.

   See Table 3-9 on page 234.

To silently register an agent

1. Log on as administrator to the computer on which you want to install the CCS Agent. Alternatively, use a role that is equivalent to an administrator.
2. Copy the CCS_Agent\win folder from the product disc to a network installation folder or to a local folder.

3 Copy the `AgentRegSilentInstallSample.bat` file from the CCS_Agent\win\examples folder of the product media. Save the `AgentRegSilentInstallSample.bat` file in the CCS_Agent\win folder that you copied to a local folder. You must save the `AgentRegSilentInstallSample.bat` file at the location where the `Setup.exe` is present for installing the agent.

   For security purpose, you can use an encrypted password to register the CCS Agent. For information on creating an encrypted password see To create an encrypted password.

4 Right-click the `AgentRegSilentInstallSample.bat` file, and then click **Edit**.

5 Specify the parameters of <COMMANDLINE>.

   See Table 3-9 on page 234.

To create an encrypted password

You can install and register an agent using an encrypted password for security purpose. Perform the following steps to create an encrypted password.

1 Copy the CCS_Agent\win folder from the product disc to a network installation folder or to a local folder.

2 On the command line, go to the CCS_Agent\win\util folder and run the `EncryptionTool.bat` file. Provide the password as a argument followed by an `e`.

   For example, `EncryptionTool.bat <Password> e`

   Where, <Password> is your password that you want to encrypt.

3 The encrypted password is displayed in a text file.

   For example, `encrypted password is : <%%C%%1D%%F%%F%%3C%%4D%%4E%%4F>`

4 Copy the encrypted password including the opening and closing brackets and paste it in quotes "" into the `AgentSilentInstallSample.bat` and `AgentRegSilentInstallSample.bat` files in place of `esm4now`.

   For example, in the `AgentSilentInstallSample.bat` file you must copy the password at the following location:

   ```
   AGENTCONFIG=\"-m [{dev-imr50-2,esm,esm4now,1,default,5600,1}]
   ```

   Replace `esm4now` with the following encrypted password

   ```
   AGENTCONFIG=\"-m
   [{dev-imr50-2,esm,"<%%C%%1D%%F%%F%%3C%%4D%%4E%%4F>",1,default,5600,1}]
   ```

Table 3-9 contains the information on the silent installation options and their descriptions.

Example command to install and register a CCS Agent on Windows in silent mode:

```
setup.exe /s /v"/qn /l*v \"%TEMP%\SymantecCCSAgentInstall.log\"
INSTALLDIR=\"C:\Program Files\Symantec\Enterprise Security Manager\"
AGENTCONFIG=\"-m [{dev-imr50-2,esm,esm4now,1,default,5600,1}] -i
enable -e [dev-imr50-2]\"
```

Table 3-9 Command-line options

Option	Description
/s	Install CCS agent in silent mode.
/v "<COMMAND LINE>"	Parameters to pass to the CCS Agent installer.
/qn	Run the CCS Agent installer without the GUI (Graphical User Interface).
/l*v<LOGFILE>	Use a verbose log and write the output to the specified log file. Log on to www.microsoft.com for more log options.
INSTALLDIR=<DIRECTORY>	Specify the directory where you need to install the agent
AGENTCONFIG	Specify the attributes of managers to whom the agent needs to be registered. Each manager specification includes the following information: ■ Manager name ■ Logon password ■ Agent name type ■ Agent name ■ Port number for the manager to listen on For security purpose, you can use an encrypted password to install the CCS Agent. For information on creating an encrypted password see To create an encrypted password. The agent name type can be a 1 (long), a 2 (short), or a 3 (user-defined). The agent name is ignored during installation unless you specify the agent name type as a 3. REGAGENTLIST is ignored if you specify the SELECTION as a 2.
-e	Enable LiveUpdate on the agent from all managers on which the agent is registered.
-e [m1,m2,m3..]	Enable LiveUpdate on the agent from specific managers.

Table 3-9 Command-line options *(continued)*

Option	Description
-d	Disable LiveUpdate on the agent from all managers on which the agent is registered.
-d [m1,m2,m3..]	Disable LiveUpdate on the agent from specific managers.
-i enable	Enable the ICE scripts. This option lets you copy the ICE scripts from a manager to an agent.
-i disable	Disable the ICE scripts.
SULOCATION=<SU package folder>	Lets you specify the custom location of the SU package. **Note:** The installer installs the su package from the default location, if custom location is not specified.

Installing and registering a CCS Agent on UNIX in silent mode

When you install a CCS Agent, the installer prompts for necessary information such as the type of installation or the name of a directory. If you use the same settings to install the CCS Agent on a large number of computers, you can avoid the prompts by performing silent installations. The silent installation feature lets you install CCS Agents and register the agents to CCS Managers.

Ensure that the host name of the computer is present in the /etc/hosts file before installing the agent.

See the following sections before installing the CCS Agent:

See “Hardware and operating system requirements” on page 37.

See “Network Ports” on page 41.

See “Supported target computers and databases for data collection” on page 48.

See “Software requirements” on page 48.

Note: You cannot install a standalone CCS Agent on a computer that contains a CCS Manager, because the CCS Manager installation also contains the installation of CCS Agent.

Perform the following procedure before installing the CCS Agent:

Install the CCS Manager. You require a CCS Manager for the CCS Agent to register to. However, you cannot install a CCS Agent on a computer that contains a CCS Manager.

Do one of the following:

- Install the CCS Manager along with the CCS Application Server on a single computer, See "Installing the CCS Suite" on page 140.
  See "Installing the CCS Suite in silent mode" on page 223.
- Add a CCS Manager to an existing installation of the CCS Application Server, See "Adding or upgrading CCS components" on page 286.
- Install a standalone CCS Manager. See "Installing a standalone CCS Manager for a scale out deployment of CCS" on page 169.
  See "Installing a standalone CCS Manager for scale-out deployment in silent mode" on page 228.

The following table contains the information on the silent installation options and their descriptions.

Example command to install and register a CCS Agent on UNIX:

```
./esmsetup -Q -ibcmaEXx -p 1,2,3,4,5,6,7,8,9,10,11,12,13,14 -d
<directory> -u <user> -g <group> -t <Path of esm.tgz> -M <Manager
IP> -O <port> -U <username> -W <password> -N <Agent_IP/Name> -B
<LiveUpdateMgr> -R <remote upgrade package path> -K <ESM tpk path>
-C <CCS tpk path> -S <CCS Manager tpk path> -I <Asset IPv4 address>
```

Table 3-10 Command-line options

Option	Description
-m	Install CCS Manager with the CCS Agent.
-a	Install only the CCS Agent.
-c	NFS installation.
-b	Enable LiveUpdate from all managers.
-i	Enable ICE scripts to be copied to the agent. This option lets you copy the ICE scripts from a manager to an agent.
-x	Disable ICE scripts to be copied to the agent.
-Q	Print File Version Stamp information.
-E	Verify Manager to Agent communication.

Table 3-10 Command-line options *(continued)*

Option	Description
-R <remote upgrade package path>	Copy remote upgrade packages to manager from the specified path. This command is applicable only for Manager + Agent installation. For example, if the Remote Upgrade package for Linux (lnx-x86 folder) is present in the folder /RU/Agent, then specify the path /RU/agent/.
-K <ESM tpk path>	Specify the complete path for esm.tpk. The path must include the file name of the tpk file. For example, to specify the location of the esm.tpk file for Solaris SPARC, ensure that the path includes the file name as shown below: `Installset\CCS_Agent\unix\sun\solaris\sparc\esm1110\su\esm.tpk`
-C <CCS tpk path>	Specify the complete path for ccs.tpk. The path must include the file name of the tpk file. For example, to specify the location of the ccs.tpk file for Solaris SPARC, ensure that the path includes the file name as shown below: `\Installset\CCS_Reporting\DCContent\AgentContent\Unix\Solaris\sparc\ccs.tpk`
-S <CCS Manager tpk path>	Specify the complete path for the CCS Manager tpk. This command is applicable only for Manager + Agent installation.
-X	Uninstall the BV-Control for UNIX agent existing on the computer.
-I <Asset IPv4 address>	Specify a preferred IPv4 address that the CCS Manager uses to connect with the asset.

Specify `-U <username>` and `-W <password>` only if you are registering the agent for message based data collection. You must first enable the CCS Application Server and CCS Manager for message based data collection.

See "Enabling message based data collection" on page 205.

If the silent installation or registration fails for any reason, the respective errors are displayed on the screen.

Installing the application modules on CCS Agent on Windows in silent mode

You can silently install the application modules. Following table lists the common options for installing the application modules.

Options for connecting to the database differ according to which application module you are installing. For example, the options for connecting to the Oracle server are different from those for connecting to the SQL Server. Refer to the specific application module documentation located inside the ESM Components\Documentation folder of the product media.

Table 3-11 Options to silently install the application modules

Option	Description
-d	Display the description and contents of this tune-up package.
-I	Install the tune-up installation package on your computer.
-U	Specify the ESM access record name
-P	Specify the ESM access record password.
-p	Specify the TCP Port to connect to the CCS Manager. - the port number is 5600 by default.
-m	Specify the ESM manager name.
-t	Connect to the ESM manager by using TCP.
-x	Connect to the ESM manager by using IPX.
-g	Specify the ESM agent name to use for registration.
-K	Do not prompt for and do the re-registration of the agents.
-h	Display help on the usage of options that can be used for silent installation.
-e	Does not execute the before and after executables (installation without configuration.)

For example if you want to install content for the Oracle platform on Windows, from the Security Response Web site, you must download the **esmoracletpi.exe** installer.

To install content for SQL Server download the **esmmssqltpi.exe** installer. For other platforms, download the platform specific content installer from the Security Response Web site.

Perform the following procedure before installing the application modules on CCS Agent on Windows:

Install the CCS Agent. See "Installing the CCS Agent on Windows" on page 185.

See "Installing and registering a CCS Agent on Windows in silent mode" on page 231.

To install the application modules for Oracle silently:

- Copy the **esmoracletpi.exe** to a folder on your computer and at the command prompt, type cd <path> to open the directory.
- Type the following at the command prompt:

  ```
  esmoracletpi.exe {-it} {-m} {-U} {-p} {-P} {-g} {-e}
  ```

  This command only installs the application modules for Oracle. To configure the Oracle connection, run `esmorasetup` from the \esm\bin\<platform> directory.

  Options for connecting to the database differ according to which application module you are installing. For example, the options for connecting to the Oracle server are different from those for connecting to the SQL Server. Refer to the specific application module documentation located inside the ESM Components\Documentation folder of the product media.

After you install the application modules, you must configure the application modules for data collection. For information on configuring the application modules, refer to the specific application module documentation located inside the ESM Components\Documentation folder of the product media.

Installing the application modules on CCS Agent on UNIX in silent mode

You can silently install the application modules. Following table lists the common options for installing the application modules.

Options for connecting to the database differ according to which application module you are installing. For example, the options for connecting to the Oracle server are different from those for connecting to the SQL Server. Refer to the specific application module documentation located inside the ESM Components\Documentation folder of the product media.

Table 3-12 Options to silently install the application modules

Option	Description
-d	Display the description and contents of this tune-up package.
-I	Install the tune-up installation package on your computer.

Table 3-12 Options to silently install the application modules *(continued)*

Option	Description
-U	Specify the ESM access record name
-P	Specify the ESM access record password.
-p	Specify the TCP Port to connect to the CCS Manager. - the port number is 5600 by default.
-m	Specify the ESM manager name.
-t	Connect to the ESM manager by using TCP.
-x	Connect to the ESM manager by using IPX.
-g	Specify the ESM agent name to use for registration.
-K	Do not prompt for and do the re-registration of the agents.
-h	Display help on the usage of options that can be used for silent installation.
-e	Does not execute the before and after executables (installation without configuration.)

For example if you want to install content for the Oracle platform on UNIX, from the Security Response Web site, you must download the **esmora.tpi** installer.

For other platforms, download the platform specific content installer from the Security Response Web site.

Perform the following procedure before installing the application modules on CCS Agent on UNIX:

Install the CCS Agent. See "Installing the CCS Agent on UNIX" on page 192.

See "Installing and registering a CCS Agent on UNIX in silent mode" on page 235.

To install the application modules for Oracle silently:

- Copy the **esmora.tpi** to a folder on your computer and at the command prompt, type cd <path> to open the directory.
- Type the following at the command prompt:

  `./esmoracletpi.exe {-it} {-m} {-U} {-p} {-P} {-g} {-e}`

  This command only installs the application modules for Oracle. To configure the Oracle connection, run `esmorasetup` from the \esm\bin\<platform> directory.

  Options for connecting to the database differ according to which application module you are installing. For example, the options for connecting to the Oracle

server are different from those for connecting to the SQL Server. Refer to the specific application module documentation located inside the ESM Components\Documentation folder of the product media.

After you install the application modules, you must configure the application modules for data collection. For information on configuring the application modules, refer to the specific application module documentation located inside the ESM Components\Documentation folder of the product media.

About silent installation return codes

In the silent mode of installation, no user interface is displayed. To install a CCS component in the silent mode you must run the `SilentInstallLauncher.exe` and provide the locations of the setup file and response file. The `SilentInstallLauncher.exe` triggers the silent installation of the CCS Setup and helps you to track the success or failure of the installation. The `SilentInstallLauncher.exe` file is located in the Documentation\Utilities\Silent Install folder of the product media.

The `SilentInstallLauncher.exe` displays the following return codes to help ascertain the status of the installation. If the return code is 0, that means the installation is successful.

Note: The return codes mentioned in the following table are not applicable for installation / upgrade of the CCS Agent in silent mode and installation of application modules on the CCS Agent in silent mode.

Table 3-13 Return codes of Silent installation

Return code	Failure description
-1	Failure in Setup.exe. Failure can occur during the detection of the required operating system, pre-requisites, disk space, digital signatures or so on.
-2	Failure during setup initialization. Failure can occur during validation of the required operating system, pre-requisites, disk space, digital signatures or so on.
-3	Invalid user input or validation failure for SQL Server.
-4	Invalid user input or validation failure for Certificate.
-5	Invalid user input for User Account.

Table 3-13 Return codes of Silent installation *(continued)*

Return code	Failure description
-6	Invalid user input for Port.
-7	Failure while getting the cached properties in case of distributed deployment of CCS components.
-8	Failure while copying the Redist components.
-15	Failure due to setup launched in maintenance mode. You cannot add, repair or uninstall CCS components in silent mode. Use the UI based installer for adding, repairing or uninstalling CCS components.
-16	Failure due to detection of non domain user or local administrator. You require a domain user and a local administrator to install the CCS components.
2	SymCert failure.
3	Directory Support Service failure.
4	Encryption Management Service failure.
5	Management Services failure.
8	Data Collector failure.
9	CCS Application Server failure.
10	Data Collector content failure.
11	Standards Management content failure.
12	Regulation content failure.
13	Symantec Help failure.
14	CCS Web Console failure.
Return codes specific to CCS Manager installation	
-9	Invalid user input for CCS Manager.
-10	Invalid user input for CCS Manager Port.
-11	Invalid user input for ESM superuser password.
-12	Invalid user input for Remote Update (RU) packages location.
-13	Invalid user input for CCS Manager certificate location.

Table 3-13 Return codes of Silent installation *(continued)*

Return code	Failure description
6	Data Processing Service failure.
7	ESM Manager failure.

See "Installing the CCS components in silent mode" on page 222.

See "Upgrading the CCS components in the silent mode" on page 277.

Deploying external data systems

CCS supports some pre-integrated data systems like:

- Symantec Data Loss Prevention
  See "Integrating Symantec Data Loss Prevention with CCS" on page 243.
- Symantec CCS Vulnerability Manager
  See "Integrating Symantec CCS Vulnerability Manager with CCS" on page 244.
- CCS Assessment Manager
- See "Integrating Symantec CCS Assessment Manager with CCS" on page 244.

You must deploy the CCS Application Server in order to import and process external data.

It is not necessary to perform any specific deployment tasks for the pre-integrated data systems.

Integrating Symantec Data Loss Prevention with CCS

Symantec Data Loss Prevention (DLP) is a pre-integrated data system in CCS. Since it is a pre-integrated data system you are not required to do any deployment tasks.

You can import the incident data from Symantec Data Loss Prevention (DLP) to CCS by using any of the following options:

- Create a data connection by using the pre-integrated Symantec DLP data system.
  For more information refer to the Working with Symantec Data Loss Prevention Integration topic in the *Symantec™ Control Compliance Suite 10.5.1 User Guide*
- Create a new data system using the CCS Data Loss Prevention data schema that is available in CCS.
  For more information refer to the Adding an external data system topic in the *Symantec™ Control Compliance Suite 10.5.1 User Guide*

See "Planning for the Symantec Data Loss Prevention integration" on page 132.

Integrating Symantec CCS Vulnerability Manager with CCS

Symantec CCS Vulnerability Manager is a pre-integrated system in CCS. Since it is a pre-integrated data system you are not required to do any deployment tasks.

You can import the vulnerability assessment data from CCS Vulnerability Manager to CCS using any of the following options:

- Create a data connection using the pre-integrated Symantec CCS Vulnerability Manager system.
  For details, refer to the topic, Adding a data connection to Symantec CCS Vulnerability Manager in the *Symantec™ Control Compliance Suite 10.5.1 User Guide*.
- Create a new data system using the vulnerability assessment data schema that is available in CCS.
  For details, refer to the topic, Adding an external data system topic in the *Symantec™ Control Compliance Suite 10.5.1 User Guide*.

See "Planning for the Symantec CCS Vulnerability Manager integration" on page 131.

Integrating Symantec CCS Assessment Manager with CCS

Symantec CCS Assessment Manager (AM) is a pre-integrated system in CCS. Since it is a pre-integrated data system you are not required to do any deployment tasks.

You can import the assessment data from AM to CCS by using any of the following options:

- Add the ODBC data location and create a data connection by using the pre-integrated Symantec CCS Assessment Manager system.
  For details, refer to the topics, Adding an external data system and Adding a data connection for external data import in the *Symantec™ Control Compliance Suite 10.5.1 User Guide*.
- Create a new data system by using the Symantec CCS Assessment Manager data schema that is available in CCS.
  For details, refer to the topic, Adding an external data system in the *Symantec™ Control Compliance Suite 10.5.1 User Guide*.

See "Planning for the Symantec CCS Assessment Manager integration" on page 133.

Maintaining and Updating CCS using LiveUpdate

The installed CCS components that are updated with the latest content and system patches must be updated periodically. Symantec releases system patches and updates for the CCS components, which are downloaded using the LiveUpdate mechanism.

LiveUpdate (LU) is a core Symantec technology that is used to simplify the maintenance and update of Symantec software post 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 LU client. The LU server returns a list of appropriate updates.

CCS uses the Windows LiveUpdate Client that is installed on the computer on which the CCS Application Server and CCS Manager are installed.

It is recommended that the LU Client uses the LiveUpdate Administrator (LUA) for downloading the patches. You can install the LUA on the same LU Client computer or on any computer where Internet access is available. The LiveUpdate Administrator (LUA) is equipped with a distribution mechanism to distribute the updates to a distribution area. The LU Client is responsible for picking up the updates from the distribution area for the components that are installed on the LU component. The administrator must decide whether the content or the system updates are required for the installed components and configure the LUA appropriately.

The following two types of updates are available for the CCS components:

- Quarterly content updates
- System patches and service pack updates

The process of downloading the updates involve the following:

- All packages are automatically downloaded, distributed, and are installed manually. Optionally, some organizations can use third-party applications such as Altiris and SMS, and so on instead of using LiveUpdate.
- The packages can be downloaded using the LiveUpdate Administrator and are repackaged for manual distribution. Other distribution methods such as direct download from the website are available as per Symantec policies.
- All computers are installed with LiveUpdate Client (LU) and are configured with a host file pointing to the LUA distribution area.

For information on using LiveUpdate, see the *Updating Control Compliance Suite using LiveUpdate* section in the *Symantec™ Control Compliance Suite User Guide*.

Chapter 4

Upgrading CCS

This chapter includes the following topics:

About upgrading the CCS Reporting and Analytics components

Upgrade to the latest release version of the Control Compliance Suite (CCS) lets you access the new and updated features and functionality of the product. The infrastructure also performs database migration of the product after the upgrade operation completes.

The CCS 11.1 is a full release upgrade for all the components of CCS. The new architecture in CCS 11.1 provides simplified deployment, out of the box support for raw-data based and message based data collection using agent-less and agent-based methods, and new risk management functionality

CCS 11.1 contains the following component level changes:

- CCS 11.1 calls the CCS Reporting and Analytics as the CCS Suite. The CCS Suite comprises of the CCS Application Server and the CCS Manager.
- Ensure that there is a domain trust relationship between different domains in the following cases:
  - If the CCS Manager in the evaluator or reporting role, and the Production database, Reporting database or the ADAM database are located in different domains.
  - If the CCS Manager in the data collector role, and the target computers for Windows data collection on Oracle platform are located in different domains. You must have a one way trust from the CCS Manager domain to the target computer domain. CCS Manager must be able to login to the target computer.

  CCS Manager uses the port 5600. If you have upgraded a Data Processing Service to CCS Manager, the CCS Manager continues to use the Data Processing Service port. If you are upgrading an ESM Manager to CCS Manager, the CCS Manager continues to use the ESM Manager port.
- CCS 11.1 segregates component installation from content installation, and provides a separate installer to install CCS content. The CCS Content consists of a set of predefined Technical Standards, Frameworks and Regulations.

CCS 11.1 integrates the Directory Server components in the CCS Application Server. As a result the concept of distributed installation is now replaced with the concept of scale-out installation, wherein you only need to install the CCS Application Server on one computer and keep adding one more CCS Managers as per your sizing requirements.

If your existing CCS deployment contains standalone installations of the Directory Server and Data Processing Service, CCS 11.1 provides separate installers to:

- upgrade the Directory Server.

- upgrade the Data Processing Service to CCS Manager.

See "Upgrading the reporting and analytics components" on page 251.

About delegation in Control Compliance Suite

Control Compliance Suite (CCS) uses Microsoft Active Directory Lightweight Directory Services (ADLDS) to store assets, policies, and jobs data. Access control within CCS is enforced by ADLDS. When a user views assets, collects data, evaluates assets, or runs reports, the user identity is used by ADLDS to validate the access rights. During interactive console sessions, the user's identity is established interactively by the CCS Console or the CCS Web Console. The Application Server Service impersonates the user that scheduled the jobs to enforce access control during the non-interactive sessions. This is useful when CCS jobs are executed during the non-interactive sessions.

In CCS, user impersonation is supported in two ways. In the first method, you must provide user credentials to CCS to schedule jobs. These credentials are stored in CCS using secure storage. The CCS architecture ensures that once a password is stored, only the Application Server can recover the password. When necessary, the Application Server Service can retrieve the password and authenticate to Kerberos directly as the user. Whenever you change the password, you must launch the CCS console and re-enter the new password. Until this is done, any job that you schedule fails to run.

In the second method, you do not require to provide user credentials to CCS to schedule jobs, but you can use an Active Directory feature called delegation. Delegation lets the CCS Application Server Service and the Directory Support Service to directly impersonate the appropriate user, and access network resources securely without any knowledge of the user credentials. To configure the CCS Application for delegation, in the Basic settings of the Application Server, select **Use controlled delegation of security rights** as the authentication type. In a default Active Directory environment, only the domain administrator has sufficient rights to configure delegation.

Note: You must configure delegation only if your existing deployment contains a standalone installation of the Directory Server.

Delegation is of two types:

- Constrained delegation:
  Constrained delegation lets a trusted account present the delegated credentials to selected CCS services. Constrained delegation is more secure because it limits the scope of impersonation for the Application Server Service and the

DSS. You can configure the service accounts for the Application Server Service and the Directory Support Service to operate with constrained delegation in the distributed setup mode. Constrained delegation is available in Windows Server 2003 functional level or higher.

See "Configuring constrained delegation for CCS" on page 249.

- Unconstrained delegation:

  Unconstrained delegation lets a trusted account present the delegated credentials to any service. In unconstrained delegation, the scope of impersonation is not limited to any particular CCS services. The Application Server Service can access all services after impersonating the user. Thus there is a risk that any application on the Application Server could potentially abuse impersonation capabilities. You can configure the service accounts for the Application Server Service and the Directory Support Service to operate with unconstrained delegation in distributed and single setup modes. Unconstrained delegation is available in Windows 2000 functional level or higher.

  See "Configuring unconstrained delegation for CCS" on page 250.

Note: Use of constrained delegation is a security best practice and is the recommended configuration for CCS. However, the CCS infrastructure supports either constrained or unconstrained delegation.

Configuring constrained delegation for CCS

Configuration of Constrained delegation requires a Service Principal Name (SPN) for the Symantec CCS ADLDS instance which is created during the installation of the Directory Server. Ensure that the Constrained delegation is configured after installation of the Directory Server.

You need to configure constrained delegation only if your deployment contains a standalone installation of the Directory Server.

See "About delegation in Control Compliance Suite" on page 248.

To configure a service account for constrained delegation

1. Open the properties for the Application Server's service account and make the following changes on the **Delegation** tab:
   - Select **Trust this user for delegation to specified services only**. By default the user is set to **Do not trust this user for delegation**.
   - Select **Use any authentication protocol**.
   - Under Services to which this account can provide delegated credentials do the following:

- Click **Add** and type in the name of the computer where DSS is installed. From the list of services, select the service, LDAP that has the same port number as the port where the ADAM instance is running and click **OK**.
- Click **Add** and type the name of the service account for which the DSS service is running. You can view the custom SPN that was created for the DSS before installation. Select the service and click **OK**.
- Click **Expand** to verify that both the short names and long names are present.

2 On the Application Server computer, open the Local Security Policy editor.

Navigate to **Under Local Policies > User Rights Assignment** and grant the privilege, **Act as part of the operating system** to the Application Server.

Note: If you use the constrained delegation and choose not to store passwords with CCS, then you need to give the service user the **Act as part of the operating system** privilege. This privilege is required by S4U to impersonate an account. If you choose to store the password with CCS, then this privilege is not required.

---

3 After the product is installed, configure delegation for the Application Server in the following manner:

- In the CCS Console, go to **Settings > System Topology > Map View** or go to **Settings > System Topology > Grid View**.
- Select the Application Server component, and right-click on **Edit Settings**.
- In the **Edit Settings** dialog box, select the **Application Server > Basic** option in the left pane.
- For the **Authentication type** option, select **Use controlled delegation of security rights** in the right pane.
- Click **Save**.

4 Restart the DSS and the Application Server computer so that the delegation settings can take effect.

See "Configuring unconstrained delegation for CCS" on page 250.

Configuring unconstrained delegation for CCS

You need to configure unconstrained delegation only if your deployment contains a standalone installation of the Directory Server.

See "About delegation in Control Compliance Suite" on page 248.

To configure a service account with unconstrained delegation

1. Identify the user accounts that you want to use as the service accounts for DSS and Application Server.
2. Enable delegation for the Application Server's service account. By default, the user is set to **Do not trust this user for delegation**.

   To enable a service account, in the user properties, go to the **Delegation** tab and select the option, **Trust this user for delegation to any service (Kerberos only)**.
3. After the product is installed, configure delegation for the Application Server in the following manner:
   - In the CCS Console, go to **Settings > System Topology > Map View** or go to **Settings > System Topology > Grid View**.
   - Select the Application Server component, and right-click on **Edit Settings**.
   - In the **Edit Settings** dialog box, select the **Application Server > Basic** option in the left pane.
   - For the **Authentication type** option, select **Use controlled delegation of security rights** in the right pane.
   - Click **Save**.
4. Restart the DSS and the Application Server computer so that the delegation settings can take effect.

See "Configuring constrained delegation for CCS" on page 249.

Upgrading the reporting and analytics components

You can upgrade the reporting and analytics components from CCS Suite 11.0 to CCS Suite 11.1. If your existing CCS version is 10.5.1, you must first upgrade to 11.0, before upgrading to CCS 11.1.

To upgrade, you must ensure that the user in whose context the components and services are installed and upgraded, have the sysadmin privileges on the SQL server. After upgrade, you can later change the user privileges to db_owner.

While upgrading to CCS 11.1, the setup upgrades the following Technical Standards and Regulations by default.

CCS Suite installer upgrades content for the following Technical Standards by default:

- CIS Benchmark v1.1.2 for Red Hat Enterprise Linux 6.x

- CIS Oracle Database Server 11g Security Benchmark v1.0.1
- CIS Security Configuration Benchmark For Microsoft Windows Server 2012 v1.0.0
- Security Essentials for Microsoft SQL Server 2012

CCS Suite installer upgrades content for the following Regulations by default:

- COBIT 5th Edition
- PCI DSS v3.0
- IT Control Objectives for Sarbanes-Oxley 2nd Edition
- HIPAA HHS 45 CFR Part 164 Subpart C

You can install or upgrade more content using the CCS Content installer.

See "Upgrading the CCS Content" on page 275.

The upgrade of the reporting and analytics components can be performed for the following installation modes:

- Single setup mode of installation
  See "Upgrading the components of a single setup mode of installation" on page 253.
- Distributed setup mode of installation
  CCS 11.1 integrates the Directory Server components in the CCS Application Server. As a result the concept of distributed installation is now replaced with the concept of scale-out installation, wherein you only need to install the CCS Application Server on one computer and keep adding one more CCS Managers as per your sizing requirements. However, for deployments containing standalone installation of the CCS Directory Server, CCS 11.1 provides a setup to upgrade such Directory Server to version 11.1.
  In the distributed setup mode of installation, you must upgrade the components in the following order:
  - CCS Directory Server
    Upgrade the CCS Directory Server to CCS Suite 11.1 Directory Server
    See "Upgrading a standalone CCS Directory Server" on page 256.
  - CCS Application Server
    See "Upgrading a standalone CCS Application Server" on page 259.
  - CCS Manager
    See "Upgrading a stand-alone CCS Manager" on page 264.

Note: To reduce any risk of installation failure during upgrade to the CCS 11.1, you must install the Microsoft patch, http://support.microsoft.com/kb/958655.

The installer places a copy of the installation files in the media cache folder. On the Windows Server 2003 computers, the media cache is in the folder, C:\Documents and Settings\All Users\Application Data\Symantec\CSM-RA\MediaCache.On the Windows Server 2008/2012 computers, the media cache is in the folder, C:\ProgramData\Symantec\CSM-RA\MediaCache. These files require approximately 1.2 GB.

Upgrading the components of a single setup mode of installation

You can upgrade the reporting and analytics components of CCS that are installed in a single setup mode to CCS Suite 11.1.

To upgrade the components, ensure that you have a minimum of 7-GB disk space in the computer. The disk space that is required to migrate the databases depends on the SQL server settings of the computer and the amount of data that you want to migrate.

You can upgrade the reporting and analytics components from CCS 11.0 to CCS Suite 11.1. If your existing CCS version is 10.5.1, you must first upgrade to 11.0, before upgrading to CCS 11.1.

You can perform this procedure to upgrade a standalone installation of the CCS Application Server to CCS Suite 11.1

Do the following to upgrade the CCS components:

- Launch the Installation Wizard
  The installation wizard detects a previous installation of CCS installed on the computer, and prompts you to upgrade.
  See "To launch the Installation Wizard" on page 253.
- Upgrade the CCS Suite
  See "To upgrade the components in a single setup mode" on page 254.

To launch the Installation Wizard

1. Insert the **Symantec Control Compliance Suite 11.1** product disc into the drive on your computer and double-click **Setup.exe**.

   In the security warning dialog box, click **Run**.
2. In the DemoShield, click **CCS Suite**.
3. On the splash screen, click **Install CCS Suite**. The Setup file is located inside the CCS_Reporting folder of the product media.

Setup prepares the CCS Suite installation wizard and prompts to install any prerequisites, if required. During the prerequisite installation, if the computer prompts you to restart, restart the computer and launch the setup again.

See "Software requirements" on page 48.

To upgrade the components in a single setup mode

1. In the **Welcome** panel of the launched Symantec Control Compliance Suite 11.1 installation wizard, read and accept the license agreement, and then click **Next**.

   The Product Improvement Program is enabled by default. The Product Improvement Program does not collect any personally identifiable data and the participation is optional. If you do not want to share the data with Symantec, then you must opt-out of the program. To opt-out of the product improvement program, uncheck **I agree to participate in the Product Improvement Program by sharing the installation and product usage information with Symantec**. To opt-out of the product improvement program later, on the CCS Console, go to **Settings > General > Product Improvement Program** and uncheck **Share installation and product usage information with Symantec**. For more information about the product improvement program, See "Product Improvement Program" on page 156.

2. In the **Upgrade** panel review the components that are being upgraded, and then click **Next**.

3. The **Add Components** panel displays the components that you can add to the CCS deployment during the upgrade. If your existing deployment does not contain a CCS Manager, you can check **CCS Manager** to install the CCS Manager on the computer. You can install both CCS Application Server and CCS Manager, on a single computer.

4. In the **Licensing** panel of the wizard, review the existing licenses or click **Add Licenses** to add licenses for the components that require mandatory licenses to install. You can add more licenses later using the CCS Console. The CCS Core license is required to install the CCS Application Server and the CCS Maintenance license is required to install the default CCS Content during the CCS installation.

   See "About licensing of the product components" on page 158.

5. Click **Next**.

6 In the **Prerequisites** panel, review the prerequisites that are required for the upgrade. Install any prerequisite application that is required to be installed. Click **Check again** to verify whether the installation is successful. CCS 11.1 requires Crystal Reports 2010 and ASP.NET v4.0.30319.

See "Software requirements" on page 48.

7 Click **Next**.

8 In the **Installation Folder** panel, review the installation path for product installation.

You can change the default location of the Installation files cache folder where the setup files that are cached during the upgrade. Click browse (**...**) to select a different location to store the setup files.

Click **Refresh disk space information** to verify the available disk space on the computer.

9 Click **Next**.

10 Perform this step if you are installing the CCS Manager during the upgrade.

In the **CCS Manager - Service Configuration** panel, enter a port for the CCS Manager. CCS components use this port to communicate with the CCS Manager.

You must import the security certificate that is used by the CCS Manager to communicate with the CCS Application Server securely.

The certificate which is to be deployed on the CCS Manager is created using the **Certificate Management Console**. The **Certificate Management Console** is installed on the CCS Application Server computer. You can either pull the certificate from the CCS Application Server computer or place it manually on the computer on which you are installing the CCS Manager.

Browse for the Security Certificate file location and enter the password.

11 In the **Summary** panel, review the installation details and click **Install**.

12 The **Install** panel indicates the progress of the component installation. After the installation finishes, the **Result** panel appears.

If the upgrade is completed with warnings, a **Warning** panel displays warning messages or a **Result** panel displays critical errors, perform the remediation steps displayed in the **Detail** window to complete the installation.

You can click the link, **Log Files** to view the installation log files. The log files are in .csv format. You can use the LogViewer in the <Install_Directory>\Application Server to view the log files. The LogViewer helps you to easily identify warnings and errors using the color codes. Warnings are highlighted in yellow color and errors are highlighted in red color.

13 In the **Result** panel, review the installation result and then click **Next**.

You can click the link, **Log Files** to view the installation log files. The log files are in .csv format. You can use the LogViewer in the <Install_Directory>\Application Server to view the log files. The LogViewer helps you to easily identify warnings and errors using the color codes. Warnings are highlighted in yellow color and errors are highlighted in red color.

14 The **Next Steps** panel displays the additional steps that you must perform to complete the CCS deployment. Perform the next steps and then click **Finish**.

You can click the link, **Save the next steps** to save the next steps for future reference. The details appear in a browser, after you specify the location to save the next steps.

You can check the option to view the release notes.

You can click the link, **Log Files** to view the installation log files. The log files are in .csv format. You can use the LogViewer in the <Install_Directory>\Application Server to view the log files. The LogViewer helps you to easily identify warnings and errors using the color codes. Warnings are highlighted in yellow color and errors are highlighted in red color.

See "Upgrading the CCS Content" on page 275.

Upgrading a standalone CCS Directory Server

If your deployment contains a standalone installation of the CCS Directory Server, you can upgrade to CCS Directory Server version 11.1.

Ensure that the following conditions are satisfied before you upgrade the CCS Directory Server:

- No CCS jobs are executing on the computer
- No instances of CCS are executing on the remote computers that are connected to the same CCS Application Server to which the Directory Server is connected.

Do the following to upgrade the CCS Directory Server:

- Launch the Installation Wizard
  The installation wizard detects a previous installation of the CCS Directory Server installed on the computer, and prompts you to upgrade.
  See "To launch the Installation Wizard" on page 257.
- Upgrade the CCS Directory Server
  See "To upgrade the CCS Directory Server" on page 257.

To launch the Installation Wizard

1. Insert the **Symantec Control Compliance Suite 11.1** product disc into the drive on your computer and double-click **Setup.exe**.

   In the security warning dialog box, click **Run**.

2. In the DemoShield, click **CCS Suite**.

3. On the splash screen, click **Upgrade to CCS 11.1 Directory Server**. The Setup file is located inside the CCS_DSS folder of the product media.

   Setup prepares the CCS Suite installation wizard and prompts to install any prerequisites, if required. During the prerequisite installation, if the computer prompts you to restart, restart the computer and launch the setup again.

   See "Software requirements" on page 48.

To upgrade the CCS Directory Server

1. In the **Welcome** panel of the launched Symantec Control Compliance Suite 11.1 installation wizard, read and accept the license agreement, and then click **Next**.

   The Product Improvement Program is enabled by default. The Product Improvement Program does not collect any personally identifiable data and the participation is optional. If you do not want to share the data with Symantec, then you must opt-out of the program. To opt-out of the product improvement program, uncheck **I agree to participate in the Product Improvement Program by sharing the installation information with Symantec**. For more information about the product improvement program, See "Product Improvement Program" on page 156.

2. In the **Upgrade** panel review the comments that are being upgraded, and then click **Next**.

3. Setup prompts you to install any updates, if required. Click **Yes** to continue.

4. The **Add Components** panel displays the components that you can add to the CCS deployment during the upgrade. If your existing deployment does not contain a CCS Manager, you can check **CCS Manager** to install the CCS Manager on the computer.

5. In the **Licensing** panel of the wizard, review the existing licenses or click **Add Licenses** to add licenses for the components that require mandatory licenses to install. You can add more licenses later using the CCS Console.

6. In the **Prerequisites** panel, review the prerequisites that are required for the upgrade. Install any prerequisite application that is required to be installed. Click **Check again** to verify whether the installation is successful.

   See "Software requirements" on page 48.

7 Click **Next**.

8 In the **Installation Folder** panel, review the installation path for product installation.

You can change the default location of the Installation files cache folder where the setup files that are cached during the upgrade. Click browse (**...**) to select a different location to store the setup files.

Click **Refresh disk space information** to verify the available disk space on the computer.

9 Click **Next**.

10 Perform this step if you are installing the CCS Manager during the upgrade.

In the **CCS Manager - Service Configuration** panel, enter a port for the CCS Manager. CCS components use this port to communicate with the CCS Manager.

You must import the security certificate that is used by the CCS Manager to communicate with the CCS Application Server securely.

The certificate which is to be deployed on the CCS Manager is created using the **Certificate Management Console**. The **Certificate Management Console** is installed on the CCS Application Server computer. You can either pull the certificate from the CCS Application Server computer or place it manually on the computer on which you are installing the CCS Manager.

Browse for the Security Certificate file location and enter the password.

11 In the **Summary** panel, review the installation details and click **Install**.

12 The **Install** panel indicates the progress of the component installation. After the installation finishes, the **Result** panel appears.

If the upgrade is completed with warnings, a **Warning** panel displays warning messages or a **Result** panel displays critical errors, perform the remediation steps displayed in the **Detail** window to complete the installation.

You can click the link, **Log Files** to view the installation log files. The log files are in .csv format. You can use the LogViewer in the <Install_Directory>\Application Server to view the log files. The LogViewer helps you to easily identify warnings and errors using the color codes. Warnings are highlighted in yellow color and errors are highlighted in red color.

13 In the **Result** panel, review the installation result and then click **Next**.

You can click the link, **Log Files** to view the installation log files. The log files are in .csv format. You can use the LogViewer in the <Install_Directory>\Application Server to view the log files. The LogViewer helps you to easily identify warnings and errors using the color codes. Warnings are highlighted in yellow color and errors are highlighted in red color.

14 The **Next Steps** panel displays the additional steps that you must perform to complete the CCS deployment. Perform the next steps and then click **Finish**.

You can click the link, **Save the next steps** to save the next steps for future reference. The details appear in a browser, after you specify the location to save the next steps.

You can check the option to view the release notes.

You can click the link, **Log Files** to view the installation log files. The log files are in .csv format. You can use the LogViewer in the <Install_Directory>\Application Server to view the log files. The LogViewer helps you to easily identify warnings and errors using the color codes. Warnings are highlighted in yellow color and errors are highlighted in red color.

See "Upgrading a standalone CCS Application Server" on page 259.

See "Upgrading a stand-alone CCS Manager" on page 264.

Upgrading a standalone CCS Application Server

After you upgrade the CCS Directory Server, upgrade the CCS Application Server to CCS 11.1. The default Technical Standards and Regulations are also upgraded during the upgrade. You can install or upgrade more content using the CCS Content installer.

See "Upgrading the CCS Content" on page 275.

Ensure that the following conditions are satisfied before you upgrade the CCS Application Server:

- No CCS jobs are executing on the computer
- No instances of CCS are executing on the remote computers that are connected to the same CCS Application Server to which the Directory Server is connected.
- The CCS Directory Server is upgraded to version 11.1.
  See "Upgrading a standalone CCS Directory Server" on page 256.

Do the following to upgrade the CCS Application Server:

- Launch the Installation Wizard

The installation wizard detects a previous installation of the CCS Application Server installed on the computer, and prompts you to upgrade.
See "To launch the Installation Wizard" on page 260.

- Upgrade the CCS Application Server
See "To upgrade the CCS Application Server" on page 260.

To launch the Installation Wizard

1. Insert the **Symantec Control Compliance Suite 11.1** product disc into the drive on your computer and double-click **Setup.exe**.

   In the security warning dialog box, click **Run**.
2. In the DemoShield, click **CCS Suite**.
3. On the splash screen, click **Install CCS Suite**. The Setup file is located inside the CCS_Reporting folder of the product media.

   Setup prepares the CCS Suite installation wizard and prompts to install any prerequisites, if required. During the prerequisite installation, if the computer prompts you to restart, restart the computer and launch the setup again.

   See "Software requirements" on page 48.

To upgrade the CCS Application Server

1. In the **Welcome** panel of the launched Symantec Control Compliance Suite 11.1 installation wizard, read and accept the license agreement, and then click **Next**.

   The Product Improvement Program is enabled by default. The Product Improvement Program does not collect any personally identifiable data and the participation is optional. If you do not want to share the data with Symantec, then you must opt-out of the program. To opt-out of the product improvement program, uncheck **I agree to participate in the Product Improvement Program by sharing the installation and product usage information with Symantec**. To opt-out of the product improvement program later, on the CCS Console, go to **Settings > General > Product Improvement Program** and uncheck **Share installation and product usage information with Symantec**. For more information about the product improvement program, See "Product Improvement Program" on page 156.
2. In the **Upgrade** panel review the comments that are being upgraded, and then click **Next**.
3. Setup prompts you to install any PCU updates, if required. Click **Yes** to continue.

4 The **Add Components** panel displays the components that you can add to the CCS deployment during the upgrade. If your existing deployment does not contain a CS Manager, you can check **CCS Manager** to install the CCS Manager on the computer. You can install both CCS Application Server and CCS Manager, on a single computer.

5 In the **Licensing** panel of the wizard, review the existing licenses or click **Add Licenses** to add licenses for the components that require mandatory licenses to install. You can add more licenses later using the CCS Console. The CCS Core license is required to install the CCS Application Server and the CCS Maintenance license is required to install the default CCS Content during the CCS installation.

See "About licensing of the product components" on page 158.

6 In the **Prerequisites** panel, review the prerequisites that are required for the upgrade. Install any prerequisite application that is required to be installed. Click **Check again** to verify whether the installation is successful.

See "Software requirements" on page 48.

7 Click **Next**.

8 In the **Installation Folder** panel, review the installation path for product installation.

You can change the default location of the Installation files cache folder where the setup files that are cached during the upgrade. Click browse (**...**) to select a different location to store the setup files.

Click **Refresh disk space information** to verify the available disk space on the computer.

9 Click **Next**.

10 In the **Symantec Help - Site Information** panel, select the IIS site that launches the Symantec Help and specify the target path for the Symantec Help installation.

The IIS site is required because the Application Server and the Symantec Help are installed on the same computer. The IIS site is also used to launch the Symantec Help on the remote computer.

By default, you can use the Default website, which is configured for the IIS Manager that is installed on the Application Server computer. Alternatively, you can specify a custom website to launch the Symantec Help.

Click browse (**...**) to specify a different target path for the Symantec Help installation.

11 Perform this step if you are installing the CCS Manager during the upgrade.

In the **CCS Manager - Service Configuration** panel, enter a port for the CCS Manager. CCS components use this port to communicate with the CCS Manager.

You must import the security certificate that is used by the CCS Manager to communicate with the CCS Application Server securely.

The certificate which is to be deployed on the CCS Manager is created using the **Certificate Management Console**. The **Certificate Management Console** is installed on the CCS Application Server computer. You can either pull the certificate from the CCS Application Server computer or place it manually on the computer on which you are installing the CCS Manager.

Browse for the Security Certificate file location and enter the password.

12 In the **Summary** panel, review the installation details and click **Install**.

13 The **Install** panel indicates the progress of the component installation. After the installation finishes, the **Result** panel appears.

If the upgrade is completed with warnings, a **Warning** panel displays warning messages or a **Result** panel displays critical errors, perform the remediation steps displayed in the **Detail** window to complete the installation.

You can click the link, **Log Files** to view the installation log files. The log files are in .csv format. You can use the LogViewer in the <Install_Directory>\Application Server to view the log files. The LogViewer helps you to easily identify warnings and errors using the color codes. Warnings are highlighted in yellow color and errors are highlighted in red color.

14 In the **Result** panel, review the installation result and then click **Next**.

You can click the link, **Log Files** to view the installation log files. The log files are in .csv format. You can use the LogViewer in the <Install_Directory>\Application Server to view the log files. The LogViewer helps you to easily identify warnings and errors using the color codes. Warnings are highlighted in yellow color and errors are highlighted in red color.

15 The **Next Steps** panel displays the additional steps that you must perform to complete the CCS deployment. Perform the next steps and then click **Finish**.

You can click the link, **Save the next steps** to save the next steps for future reference. The details appear in a browser, after you specify the location to save the next steps.

You can check the option to view the release notes.

You can click the link, **Log Files** to view the installation log files. The log files are in .csv format. You can use the LogViewer in the <Install_Directory>\Application Server to view the log files. The LogViewer helps you to easily identify warnings and errors using the color codes. Warnings are highlighted in yellow color and errors are highlighted in red color.

See "Upgrading a stand-alone CCS Manager" on page 264.

Upgrading the CCS Application Server without the pass phrase

When you upgrade the CCS Application Server to CCS 11.1, the installer prompts you to enter the pass phrase the Application Server uses. If you do not know this pass phrase, you can still upgrade the Application Server. However, you must run the standalone utility, called `PrepForUpgade`, on the Application Server before you start upgrade.

The standalone utility is included on the CCS product disc. The `PrepForUpgade` utility is stored in the `Tools\PrepForUpgrade` directory on the product disc.

The utility must run with the user privileges of the Application Server service account. To do so, you normally use the `Run As` option for the command prompt. You can also log in using the service account credentials and run the tool.

Preparing the Application Server for upgrade without the pass phrase

1 Close the CCS Suite 11.1 Installation Wizard and log out of the Application Server host.

2 Click **Start > All Programs > Accessories**, then right-click **Command Prompt**.

Click **Run as**.

3 In the **Run As** dialog, click **The following user** and enter the CCS Application Server service account credentials. Click **OK**.

4 At the command prompt, navigate to the Tools\PrepForUpgrade directory on the product media.

5 At the command prompt, type the following:

```
Symantec.CSM.Tools.Security.PrepForUpgrade.exe [<AppServer Directory>]
```

Then press return.

6 The utility will prepare the Application Server for the upgrade. When the utility is complete, the message `Preparations for upgrade complete` appears.

7 At the command prompt, type `Exit` and press return to close the command prompt window.

8 Use the CCS Suite 11.1 Installation Wizard to upgrade the Application Server.

See "Upgrading a standalone CCS Application Server" on page 259.

Upgrading a stand-alone CCS Manager

You can upgrade your standalone installations of the CCS Manager.

Do the following to upgrade the CCS Manager:

- Launch the Installation Wizard
  The installation wizard detects a previous installation of the CCS Manager installed on the computer, and prompts you to upgrade.
  See "To launch the Installation Wizard" on page 264.
- Upgrade the CCS Manager
  See "To upgrade the CCS Manager" on page 265.

To launch the Installation Wizard

1 Insert the **Symantec Control Compliance Suite 11.1** product disc into the drive on your computer and double-click **Setup.exe**.

In the security warning dialog box, click **Run**.

2 In the DemoShield, click **CCS Manager**.

3 On the splash screen, click **Install CCS Manager**. The Setup file is located inside the CCS_Manager folder of the product media.

Setup prepares the CCS Manager installation wizard and prompts to install any prerequisites, if required. During the prerequisite installation, if the computer prompts you to restart, restart the computer and launch the setup again.

See "Software requirements" on page 48.

To upgrade the CCS Manager

1. In the **Welcome** panel of the launched Symantec Control Compliance Suite 11.1 installation wizard, read and accept the license agreement, and then click **Next**.

   The Product Improvement Program is enabled by default. The Product Improvement Program does not collect any personally identifiable data and the participation is optional. If you do not want to share the data with Symantec, then you must opt-out of the program. To opt-out of the product improvement program, uncheck **I agree to participate in the Product Improvement Program by sharing the installation information with Symantec**. For more information about the product improvement program, See "Product Improvement Program" on page 156.

2. In the **Upgrade** panel review the comments that are being upgraded, and then click **Next**.

3. In the **Prerequisites** panel, review the prerequisites that are required for the upgrade. Install any prerequisite application that is required to be installed. Click **Check again** to verify whether the installation is successful.

   See "Software requirements" on page 48.

4. Click **Next**.

5. In the **Installation Folder** panel, review the installation path for product installation.

   Click **Refresh disk space information** to verify the available disk space on the computer.

6. Click **Next**.

7. In the **Summary** panel, review the installation details and click **Install**.

8. The **Installation Progress** panel indicates the progress of the component installation. After the installation finishes, the **Result** panel appears.

   If the upgrade is completed with warnings, a **Warning** panel displays warning messages or a **Result** panel displays critical errors, perform the remediation steps displayed in the **Detail** window to complete the installation.

   You can click the link, **Log Files** to view the installation log files. The log files are in .csv format. You can use the LogViewer in the <Install_Directory>\Application Server to view the log files. The LogViewer helps you to easily identify warnings and errors using the color codes. Warnings are highlighted in yellow color and errors are highlighted in red color.

9 In the **Result** panel, review the installation result and then click **Next**.

You can click the link, **Log Files** to view the installation log files. The log files are in .csv format. You can use the LogViewer in the <Install_Directory>\Application Server to view the log files. The LogViewer helps you to easily identify warnings and errors using the color codes. Warnings are highlighted in yellow color and errors are highlighted in red color.

10 The **Next Steps** panel displays the additional steps that you must perform to complete the CCS deployment. Perform the next steps and then click **Finish**.

You can click the link, **Save the next steps** to save the next steps for future reference. The details appear in a browser, after you specify the location to save the next steps.

You can check the option to view the release notes.

You can click the link, **Log Files** to view the installation log files. The log files are in .csv format. You can use the LogViewer in the <Install_Directory>\Application Server to view the log files. The LogViewer helps you to easily identify warnings and errors using the color codes. Warnings are highlighted in yellow color and errors are highlighted in red color.

See "Registering the CCS Manager" on page 173.

Upgrading Oracle Instant Client to 12.1

When you install or upgrade to CCS 11.1, you must also upgrade Oracle Instant Client to 12.1 for data-collection of Oracle-configured databases. To know how to install the Oracle Instant Client for data collection of Oracle-configured databases, refer to the *Symantec™ Control Compliance Suite 11.1 User Guide*

You can download the Oracle Instant Client (version 12.1) for Microsoft Windows (32-bit) from the Oracle website at http://www.oracle.com

You can upgrade Oracle Instant Client to 12.1 by any of the following ways:

- Upgrading without changing the PATH variable
- Updating the PATH variable
- Updating the PATH variable without deleting the 10.2 Instant Client

Upgrading without changing the PATH variable

You can upgrade Oracle Instant Client without changing the PATH variable on your operating system. For example, the following is the PATH variable on your operating system:

PATH=%..%;C:\oracle_instantclient(where **C:\ oracle_instantclient** is the path of the Oracle Instant Client 10.2 folder)

To upgrade Oracle Instant Client without changing the PATH variable

1. Back up (optional) the **oracle_instantclient** folder on your machine and delete all the existing binaries from the **oracle_instantclient** folder.
2. Copy the Oracle Instant Client 12.1 binaries in the **oracle_instantclient** folder.
3. Restart CCS Manager and DPS services.

   The upgrade process is complete.

   In this case, the PATH variable will remain unchanged, but the **C:\ oracle_instantclient** directory will contain all the required binaries of the upgraded Oracle Instant Client 12.1 version.

Updating the PATH variable

You can upgrade Oracle Instant Client by updating the PATH variable on your operating system. For example, the following is the PATH variable on your operating system:

PATH=%..%;C:\instantclient_10_2(where **C:\instantclient_10_2** is the path of Oracle Instant Client 10.2 folder)

To upgrade Oracle Instant Client by updating the PATH variable

1. In the **Environment Variables** dialog box, in the **System variables** section, update the Oracle Instant Client folder name in the existing PATH variable. (Change it from **instantclient_10_2** to **instantclient_12_1** in the given example.)
2. Back up (optional) the **instantclient_10_2** folder on your machine, and then delete this folder.
3. Restart CCS Manager and DPS services.

   The upgrade process is complete.

   In this case, the PATH variable will be updated to the following:

   PATH=%..%;C:\instantclient_12.1

Updating the PATH variable without deleting the 10.2 Instant Client

You can upgrade Oracle Instant Client by updating the PATH variable on your operating system and also without deleting the earlier Instant Client. For example, the following is the PATH variable on your operating system:

PATH=%..%;C:\instantclient_10_2(where **C:\instantclient_10_2** is the path of Oracle Instant Client 10.2 folder)

To update the PATH variable without deleting the 10.2 instant client

1. In the **Environment Variables** dialog box, in the **System variables** section, update the Oracle Instant Client folder name in the existing PATH variable. (Change it from **instantclient_10_2** to **instantclient_12_1** in the given example.)
2. Restart the DPS machine.

   In this case, the PATH variable will be updated to the following:

   PATH=%..%;C:\instantclient_12.1

Note: This method requires the DPS machine restart.

Upgrading the ESM Utilities

You can upgrade the ESM Utilities after upgrading the CCS Managers.

Perform the following procedure before upgrading the ESM Utilities:

Do the following to upgrade the ESM Utilities:

- Launch the Installation Wizard
  See "To launch the Installation Wizard" on page 268.
- Upgrade the ESM Utilities
  See "To upgrade the ESM Utilities" on page 268.

To launch the Installation Wizard

1. Insert the **Symantec Control Compliance Suite 11.1** product disc into the drive on your computer.
2. Go to ESM Components\Utilities and run the setup.exe.

   In the security warning dialog box, click **Run**.

   Setup prepares the ESM utilities installer.

To upgrade the ESM Utilities

1. In the **Welcome** panel of the launched Symantec Control Compliance Suite 11.1 ESM Utilities Setup wizard, click **Next**.
2. In the **License Agreement** panel, read and accept the license agreement and then click **Next**.

3 In the **Destination Folder** panel, review the installation folder path for installing the ESM Utilities and click **Next**.

ClickChange to specify a different installation path to install the ESM Utilities.

4 In the **Install Security Update** panel, review the folder path to look for security updates and click **Next**.

The setup detects the required security updates.

ClickBrowse to specify a different folder path for security updates.

5 In the **Ready to Install the Program** panel, click **Install**.

You can review or change the installation settings before proceeding with the upgrade.

6 The progress bar indicates the progress of the upgrade. After the upgrade finishes, the **InstallShield Wizard Completed** panel appears.

7 In the **InstallShield Wizard Completed** panel, click **Finish**.

Upgrading the ESM Agent (previous to version 11.0) to CCS Agent on Windows manually

You can upgrade your ESM Agents to CCS Agents.

Note: To upgrade an ESM Agent to the latest CCS Agent, use the setup files for Agent installation available on the Symantec website.

Do the following to upgrade the ESM Manager:

- Launch the Installation Wizard
  The installation wizard detects a previous installation of the ESM Agent installed on the computer, and prompts you to upgrade.
  See "To launch the Installation Wizard" on page 270.
- Upgrade the ESM Agent
  See "To upgrade the ESM Agent" on page 270.

To launch the Installation Wizard

1. Insert the **Symantec Control Compliance Suite 11.1** product disc into the drive on your computer and double-click **Setup.exe**.

   In the security warning dialog box, click **Run**.

2. In the DemoShield, click **CCS Agent**.

   On the splash screen, click **Install CCS Agent**.

   See "Software requirements" on page 48.

3. The Setup files for various platforms are located inside the CCS_Agent folder of the product media.

   Open the Windows folder and double-click **Setup.exe**.

   Setup prepares the CCS Agent installer.

To upgrade the ESM Agent

1. In the **Welcome** panel of the launched Symantec Control Compliance Suite 11.1 Agent Setup wizard, click **Next**.
2. In the **License Agreement** panel, read and accept the license agreement and then click **Next**.
3. In the **Destination Folder** panel, review the installation folder path for product installation and click **Next**.

   Click**Change** to specify a different installation path to install the product.

4. In the **Install Security Update** panel, review the folder path to look for security updates and click **Next**.

   The setup detects the required security updates.

   Click**Browse** to specify a different folder path for security updates.

5. In the **Ready to Install the Program** panel, click **Install**.

   You can review or change the installation settings before proceeding with the upgrade.

6. The progress bar indicates the progress of the upgrade. After the upgrade finishes, the **Setup Wizard Completed** panel appears.
7. In the **Setup Wizard Completed** panel, click **Finish**.

   You can check **Launch Agent Configuration Utility** to register the CCS Agent to the CCS Manager, enable LiveUpdate and enable Integrated Command Engine.

Upgrading the ESM Agent (previous to version 11.0) to CCS Agent on UNIX manually

The procedure to upgrade the ESM Agent to CCS Agent is the same as the procedure to install the CCS Agent.

Upgrading the ESM agent (previous to version 11.0) by using Agent Product Update

You can use the **Agent Product Update** job task to conveniently upgrade the ESM agent software on Windows or UNIX computers. This job can upgrade a single agent or all of the agents in a manager domain.

To upgrade ESM agents

1. While upgrading, copy the RemoteUpdate packages on the CCS Manager in the <Install Directory>ESM\Update\Agent folder. Additionally, for SU 4200 or lower, the LU_4201 and PrepRU packages are required. For SU 4201 or above, only PrepRU package is required. The packages are located inside the `ESM Components` folder of the product media.
2. Upgrade the ESM Console to the latest version.
3. On the ESM Console, copy the LU_4201 package in the <Install Directory>\ESM Enterprise Console\liveupdate\granularlu folder.
4. Enable LiveUpdate on the ESM Agent.
5. On the ESM Console, run LiveUpdate to push LU_4201.
6. Perform steps 3 to 5 to push the PrepRU package to the ESM Agent.
7. On the ESM Console, ensure that **Asset Information** and **Prepare RU** policies are listed under the Policies node.
8. Click **Asset Information > Agent Information** policy, right-click the agent platform , select **Properties** and then check **Asset Information**.
9. On the CCS Console, go to **Agent Management Tasks > Import Agents below v11.0**, to import the ESM agents into CCS.
10. On the CCS Console, go to **Manage > Asset System > Agents**.
11. In the table pane, select an agent which you want to upgrade.
12. Right-click the agent and select **Agent Product Update**.

    The **Create or Edit Agent Product Update Job** wizard appears.

13 In the **Select agent product update type** panel, select **Upgrade Agent**, and then click **Next**.

In the subsequent panels, provide relevant information to run the Job.

14 Go to **Agent Tasks > Show Upgrade Status**, to view the agent upgrade status.

15 Once the job 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.

You can download SU 4201 or later content using the ESM Console. ESM Console requires the CCS maintenance license if you have installed the ESM Console update provided with the CCS 11.0 Product Update 2013-2. If you have not installed the ESM Console update, you can continue to use the LiveUpdate license to download SU content from the ESM Console."

You can get the ESM Console update located inside the ESM Components folder of the product media.

See "Upgrading the BV-Control for UNIX agent to CCS Agent by using Agent Product Update " on page 273.

Upgrading the BV-Control for UNIX agent to CCS Agent manually

The procedure to upgrade the BV-Control for UNIX agent to CCS Agent is the same as the procedure to install the CCS Agent on UNIX.

After you accept the license agreement in step 5 in Installing the CCS Agent on UNIX, the installer detects a previous installation of the BV-Control for UNIX agent on the computer and prompts you to uninstall the agent.

If you type **y** to uninstall the agent, the BV-Control for UNIX agent is uninstalled before installing the CCS Agent. The CCS Agent uses the same port which was used by the BV-Control for UNIX agent.

If you type **n**, the CCS Agent is installed along with the BV-Control for UNIX agent. The BV-Control for UNIX agent and the CCS Agent co-exist on the same computer. The CCS Agent uses the default port 5600.

To continue installing the CCS Agent, continue from step 6 in Installing the CCS Agent on UNIX.

Upgrading the BV-Control for UNIX agent to CCS Agent by using Agent Product Update

You can use the **Agent Product Update** job to conveniently upgrade the imported BV-Control for UNIX agents to CCS Agents.

Before you upgrade the registered BV-Control for UNIX agents, to the version 11.1, you must perform the following steps in the given order:

- On the RMS Information Server, open the registry editor and go to `HKEY_LOCAL_MACHINE\SOFTWARE\Bindview\BV-Control for Unix` and set the value of the key `MaxThreads` to `10`.
- 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.
- Expand **UNIX Enterprise** and click **All Servers**.
- In the right pane, select all agent computers.
- Right-click the agent computers and click **Update Rapid Fire**.
- In the **Select Rapid Fire Package** dialog, select the **RapidFire file RF10575.rf**, and then click **Update**.
- On the CCS Console, go to **Agent Management Tasks > Import Agents below v11.0**, to import the BV-Control for UNIX 10.5.1 agents into CCS.
- Before upgrading the BV-Control for UNIX agents, copy the RapidFire file `RF11100.rf` to the <install_directory>\Symantec\RMS\Control\UNIX\rf folder. Do not change the file name. The `RF11100.rf` file is located inside the `BV-ControlUpgrade` folder of the product media.

Your BV-Control for UNIX agents are now ready for upgrade to CCS 11.1.

The job automatically performs a backup and restore of the agent configuration files.

Ensure that the hostname of the agent computer is present in the /etc/hosts file before upgrading the agent.

To upgrade the BV-Control agents for UNIX

1. Go to **Manage** > **Asset System** > **Agents**.
2. In the table pane, select an agent which you want to upgrade.
3. Right-click the agent and select **Agent Product Update** .

   The **Create or Edit Agent Product Update Job** wizard appears.
4. In the **Select agent product update type** panel, select **Upgrade Agent**, and click **Next**.
5. In the subsequent panels, provide relevant information to run the Job.

   In the **Specify CCS Manager and Agent Settings**panel of the wizard, check **Do not remove existing agent**. It is recommended that until you complete the upgrade and Perform data collection from the new deployment for the first time, you should maintain a co-existence of the BV-control for UNIX Agents and the CCS Agents.
6. Import assets and agents to get the upgraded agents into CCS.

Note: You must apply RF 10575 to the BV-Control Agent 10.50.33, which is released with PCU 2012-1. However, you need not apply RF 10575 to the BV-Control Agent 10.50.34, which was released with PCU 2012-2 and is available with the agent.

See "Upgrading the ESM agent (previous to version 11.0) by using Agent Product Update " on page 271.

Upgrading CCS 11.0 agents to CCS 11.1 manually

The procedure to upgrade the CCS 11.0 Windows or UNIX agents to CCS 11.1 manually is same as the upgrading the ESM Agent (previous to version 11.0) to CCS Agent on Windows or UNIX manually.

Upgrading CCS 11.0 agents to CCS 11.1 by using Agent Product Update

You can use the Agent Product Update job with **Patch agent** option to conveniently upgrade the CCS 11.0 agent software on Windows or UNIX computers to CCS 11.1 agents.

To upgrade CCS 11.0 agents to CCS 11.1 by using Agent Product Update

1. On the CCS Console, go to **Agent Management Tasks** > **Import registered agents** to import the CCS 11.0 agents into CCS.
2. Go to **Manage** > **Asset System** > **Agents**.
3. In the **Table** pane, select the agent that you want to upgrade.
4. Right-click the agent and click **Agent Product Update**.
5. In the **Create or Edit Agent Product Update Job** wizard, in the **Select agent product update type** panel, select **Upgrade Agent**, and then click **Next**.
6. Select **Patch Agent** option.
7. In the subsequent panels, provide relevant information to run the Job.
8. Go to **Agent Tasks** > **Show Upgrade Status** to view the agent upgrade status.
9. After the job 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.

Upgrading the CCS Content

Control Compliance Suite makes available a set of predefined Technical Standards, Frameworks and Regulations. When you upgrade the CCS Reporting and Analysis components, the CCS Suite installer updates content for the following Technical Standards and Regulations.

CCS Suite installer installs content for the following Technical Standards by default:

- CIS Benchmark v1.1.2 for Red Hat Enterprise Linux 6.x
- CIS Oracle Database Server 11g Security Benchmark v1.0.1
- CIS Security Configuration Benchmark For Microsoft Windows Server 2012 v1.0.0
- Security Essentials for Microsoft SQL Server 2012

CCS Suite installer installs content for the following Regulations by default:

- COBIT 5th Edition
- PCI DSS v3.0
- IT Control Objectives for Sarbanes-Oxley 2nd Edition
- HIPAA HHS 45 CFR Part 164 Subpart C

You can upgrade more content using the CCS Content installer. The CCS Maintenance license is required to install additional CCS Content.

Perform the following procedure before upgrading the CCS Content:

Upgrade the CCS Application Server. See "Upgrading the components of a single setup mode of installation" on page 253.

See "Upgrading a standalone CCS Application Server" on page 259.

Do the following to upgrade the CCS Content:

- Launch the Installation Wizard.
  See "To launch the Installation Wizard" on page 220.
- Upgrade the CCS Content.
  See "To install the CCS Content" on page 221.

To launch the Installation Wizard

1. Insert the **Symantec Control Compliance Suite 11.1** product disc into the drive on your computer and click **Setup.exe**.

   In the security warning dialog box, click **Run**.
2. In the DemoShield, click **CCS Suite**.

   On the splash screen, click **Install CCS Content**. The Setup file is located inside the CCS_Content folder of the product media.

   Setup prepares the CCS Content installation wizard.

   See "Software requirements" on page 48.

To upgrade the CCS Content

1. In the **Welcome** panel of the launched Symantec Control Compliance Suite 11.1 installation wizard, click **Next**.
2. In the **Upgrade** panel, review the Technical Standards, Frameworks and Regulations that are being upgraded, and then click **Next**.
3. The **Add Components** panel lets you install additional content

   Check the Technical Standards, Frameworks and Regulations which you require for the appropriate platform, and then click **Next**.

   You can select individual standards or select a platform name to select all standards for the particular platform.
4. In the **Licensing** panel, review the existing licenses or click **Add Licenses** to add licenses for the components that require mandatory licenses to install. The CCS Maintenance license is required to install CCS Content.

5 In the **Installation Folder** panel, review the installation path for product installation.

Click **Refresh disk space information** to verify the available disk space on the computer.

6 Click **Next**.

7 In the **Summary** panel, review the installation details and then click **Install**.

8 The **Installation Progress** panel indicates the progress of the content installation. After the installation finishes, the **Finish** panel appears.

9 In the **Finish** panel, review the installation result and then click **Finish**.

You can click the link, **Log Files** to view the CCS Content installation log files. The log files are in .csv format. You can use the LogViewer in the <Install_Directory>\Application Server to view the log files. The LogViewer helps you to easily identify warnings and errors using the color codes. Warnings are highlighted in yellow color and errors are highlighted in red color.

You can check the option to view the release notes.

See "Installing CCS content in silent mode" on page 229.

See "Installing the SQL Server content on CCS Agents for raw-data collection on SQL Server" on page 202.

See "Configuring CCS Agents for message based data collection " on page 203.

See "CCS Suite deployment sequence " on page 140.

Upgrading the CCS components in the silent mode

The silent upgrade mode in CCS is about upgrade of the CCS components on different computers in your network without navigating through the Installation Wizard. The main requisite for the silent upgrade is the `SilentInstallLauncher.exe` file and the response file.

In the silent mode of upgrade, no user interface is displayed. To upgrade a CCS component in the silent mode you must run the `SilentInstallLauncher.exe` and provide the locations of the setup file and response file. The `SilentInstallLauncher.exe` triggers the silent installation of the setup and helps you to track the success or failure of the upgrade. The `SilentInstallLauncher.exe` displays return codes to help ascertain the status of the installation. If the return code is 0, that means the installation is successful.

See "About silent installation return codes" on page 241.

The response file is an XML file, which contains the inputs of the components that are to be upgraded. The response file is not specific to any operating system.

The CCS 11.1 product media contains response files for the following types of upgrades:

- Upgrade all CCS components on a single computer. This upgrades the CCS Application Server and CCS Manager installed on a single computer.
- Upgrading a standalone CCS Directory Server. If the CCS Manager is installed along with the CCS Directory Server on the same computer, while upgrading the CCS Directory Server, you can upgrade the CCS Manager.
- Upgrading a standalone CCS Application Server.
- Upgrading the Directory Processing Service to CCS Manager.
- Upgrading the CCS content.

The `SilentInstallLauncher.exe` file and the response files are located in the Documentation\Utilities\Silent Install folder of the product media.

The Documentation\Utilities\Silent Install folder of the product media also contains a batch file that you can use to run the silent upgrade commands. The file name is `Silent Install.bat`. Before running the batch file, you must edit the batch file to provide the location of the setup and response files for the particular upgrade.

Note: You must ensure that the computers on which the silent installation is triggered contain all the prerequisites, which you must install manually. CCS setup does not install any prerequisites automatically during the silent installation. See “Software requirements” on page 48.

See “Upgrading all CCS components in silent mode” on page 278.

See “Upgrading a standalone CCS Directory Server in silent mode” on page 280.

See “Upgrading a standalone CCS Application Server in silent mode” on page 282.

See “Upgrading the CCS Manager in silent mode” on page 283.

See “Adding or upgrading CCS content in silent mode” on page 289.

See “About silent installation return codes” on page 241.

See “CCS Suite deployment sequence ” on page 140.

Upgrading all CCS components in silent mode

Perform the following procedure to upgrade all CCS components in the silent mode.

Read the end-user license agreement eula.txt located in the product media before proceeding with the upgrade.

All inputs required in the response file are case-sensitive. Ensure that you use the correct case for each value. For example, where "True" is required, enter "True" and not "true".

To upgrade all CCS components in silent mode

You can upgrade all CCS components installed on a single computer.

1 You require the `CCS_Suite_Upgrade` response file to upgrade the CCS components. The response file is located in the Documentation\Utilities\Silent Install folder of the product media. Copy the response file to the local computer, and then edit the response file to provide user inputs required during the upgrade.

For example, in the response file, provide the path of license file at `<License File="<path>"/>`

Where, `<path>` is the path of the license file, for example, `c:\Temp\2109884.sif`

The user inputs required in the response file correspond to the user inputs required during UI based installation. For detailed explanation of each input refer to the field description tables in the UI based installation section.

See "Upgrading the components of a single setup mode of installation" on page 253.

The CCS Core license is required to upgrade the CCS Application Server and the CCS Maintenance license is required to upgrade the default CCS Content during the CCS upgrade.

2 On the command prompt, navigate the location of the `SilentInstallLauncher.exe` file.

The `SilentInstallLauncher.exe` file is located in the Documentation\Utilities\Silent Install folder of the product media.

3 Run the following command to upgrade all CCS components installed on a single computer:

```
SilentInstallLauncher.exe /SetupPath="SetupExePath"
/ResponseFile="ResponseFilePath"
```

Where:

- `SetupExePath` is the location of the CCS setup file. The Setup file is located inside the CCS_Reporting folder of the product media.

- `ResponseFilePath` is the location of the response file for upgrading the CCS components. Provide the location of the response file you edited in Step 1.

See "About silent installation return codes" on page 241.

Upgrading a standalone CCS Directory Server in silent mode

Perform the following procedure to upgrade the CCS Directory Server in the silent mode. If the CCS Manager is installed along with the CCS Directory Server on the same computer, while upgrading the CCS Directory Server, you can upgrade the CCS Manager.

Read the end-user license agreement eula.txt located in the product media before proceeding with the upgrade.

All inputs required in the response file are case-sensitive. Ensure that you use the correct case for each value. For example, where "True" is required, enter "True" and not "true".

To upgrade the CCS Directory Server in silent mode

You can upgrade a standalone CCS Directory Server.

1 You require the `CCS_DSS_Upgrade` response file to upgrade the CCS Directory Server. If the CCS Manager is installed along with the CCS Directory Server on the same computer, you can use the same response file to upgrade the CCS Manager, while upgrading the CCS Directory Server. The response file is located in the Documentation\Utilities\Silent Install folder of the product media. Copy the response file to the local computer, and then edit the response file to provide user inputs required during the upgrade.

   For example, in the response file, provide the path of license file at `<License File="<path>"/>`

   Where, `<path>` is the path of the license file, for example, `c:\Temp\2109884.sif`

   The user inputs required in the response file correspond to the user inputs required during UI based installation. For detailed explanation of each input refer to the field description tables in the UI based installation section.

   See "Upgrading a standalone CCS Directory Server" on page 256.

   The CCS Core license is required to upgrade the CCS Directory Server.

   CCS Manager upgrade does not require a response file.

2 On the command prompt, navigate the location of the `SilentInstallLauncher.exe` file.

   The `SilentInstallLauncher.exe` file is located in the Documentation\Utilities\Silent Install folder of the product media.

3 Run the following command to upgrade the CCS Directory Server. You can use the same command if you want to upgrade the CCS Manager, while upgrading the CCS Directory Server.

   ```
   SilentInstallLauncher.exe /SetupPath="SetupExePath"
   /ResponseFile="ResponseFilePath"
   ```

   Where:

   - `SetupExePath` is the location of the CCS Directory Server setup file. The Setup file is located inside the CCS_DSS folder of the product media.
   - `ResponseFilePath` is the location of the response file for upgrading the CCS components. Provide the location of the response file you edited in Step 1.
   - `SuperUserPassword` is the ESM superuser password.
   - `DPSCertpassword` is the password of the CCS Manager certificate that is imported while installing the CCS Manager.

See "About silent installation return codes" on page 241.

Upgrading a standalone CCS Application Server in silent mode

Perform the following procedure to upgrade the CCS Application Server in the silent mode.

Read the end-user license agreement eula.txt located in the product media before proceeding with the upgrade.

All inputs required in the response file are case-sensitive. Ensure that you use the correct case for each value. For example, where "True" is required, enter "True" and not "true".

Perform the following procedures before upgrading a standalone CCS Application Server:

Upgrade the CCS Directory Server. See “Upgrading a standalone CCS Directory Server” on page 256.

See “Upgrading a standalone CCS Directory Server in silent mode” on page 280.

To upgrade the CCS Application Server in silent mode

You can upgrade the CCS Application Server after upgrading the CCS Directory Server.

1. You require the `CCS_Suite_WithoutCCSManager` response file to upgrade the Application Server. The response file is located in the Documentation\Utilities\Silent Install folder of the product media. Copy the response file to the local computer, and then edit the response file to provide user inputs required during the upgrade.

   For example, in the response file, provide the path of license file at `<License File="<path>"/>`

   Where, `<path>` is the path of the license file, for example, `c:\Temp\2109884.sif`

   The user inputs required in the response file correspond to the user inputs required during UI based installation. For detailed explanation of each input refer to the field description tables in the UI based installation section.

   See "Upgrading a standalone CCS Application Server" on page 259.

   The CCS Core license is required to upgrade the CCS Application Server and the CCS Maintenance license is required to upgrade the default CCS Content during the CCS upgrade.

2. On the command prompt, navigate the location of the `SilentInstallLauncher.exe` file.

   The `SilentInstallLauncher.exe` file is located in the Documentation\Utilities\Silent Install folder of the product media.

3. Run the following command to upgrade the Application Server:

   ```
   SilentInstallLauncher.exe /SetupPath="SetupExePath"
   /ResponseFile="ResponseFilePath"
   ```

   Where:

   - `SetupExePath` is the location of the CCS setup file. The Setup file is located inside the CCS_Reporting folder of the product media.
   - `ResponseFilePath` is the location of the response file for upgrading the CCS Application Server. Provide the location of the response file you edited in Step 1.

See "About silent installation return codes" on page 241.

Upgrading the CCS Manager in silent mode

Perform the following procedure to upgrade the CCS Manager in the silent mode.

Read the end-user license agreement eula.txt located in the product media before proceeding with the upgrade.

Note: CS Manager upgrade does not require a response file.

To upgrade the CCS Manager in silent mode

You can upgrade a standalone CCS Manager.

1 On the command prompt, navigate the location of the `SilentInstallLauncher.exe` file.

The `SilentInstallLauncher.exe` file is located in the Documentation\Utilities\Silent Install folder of the product media.

2 Run the following command to upgrade the CCS Manager:

```
SilentInstallLauncher.exe /SetupPath="SetupExePath"
```

Where:

- `SetupExePath` is the location of the CCS Manager setup file. The Setup file is located inside the CCS_Manager folder of the product media.

See "About silent installation return codes" on page 241.

Upgrading the ESM Agent to CCS Agent on Windows in silent mode

The procedure to upgrade the ESM Agent to CCS Agent in silent mode is the same as the procedure to install the CCS Agent in silent mode.

See "Installing and registering a CCS Agent on Windows in silent mode" on page 231.

Upgrading the ESM Agent to CCS Agent on UNIX in silent mode

The procedure to upgrade the ESM Agent to CCS Agent on UNIX in silent mode is the same as the procedure to install the CCS Agent on UNIX in silent mode.

See "Installing and registering a CCS Agent on UNIX in silent mode" on page 235.

Upgrading the BV-Control for UNIX agent to CCS Agent in silent mode

The procedure to upgrade the BV-Control for UNIX agent to CCS Agent in silent mode is the same as the procedure to install the CCS Agent on UNIX in silent mode.

If you want to uninstall the BV-Control for UNIX agent before installing the CCS Agent, add `-x` at the end of the command which is used to install and register a CCS Agent on UNIX. The BV-Control for UNIX agent is uninstalled before installing the CCS Agent. The CCS Agent uses the same port which was used by the BV-Control for UNIX agent.

Use the same command that is used to install the CCS Agent on UNIX, to install the CCS Agent along with the BV-Control for UNIX agent. The BV-Control for UNIX agent and the CCS Agent co-exist on the same computer. The CCS Agent uses the default port.

See “Installing and registering a CCS Agent on UNIX in silent mode” on page 235.

Upgrading CCS content in silent mode

The procedure to upgrade the CCS content in silent mode is the same as the procedure to install the CCS content in silent mode.

See “Installing CCS content in silent mode” on page 229.

Chapter 5

Modifying or repairing CCS components

This chapter includes the following topics:

Adding or upgrading CCS components

You can add a new component or upgrade an existing component of the product. You can add a new component only if the component is not already installed on the computer. You can upgrade a component by applying the component update packages that are released in the post release of CCS.

You can perform the addition or upgrade of a component through the **Maintenance** panel of the **Symantec Control Compliance Suite 11.1 Installation Wizard**.

If you are adding a CCS Manager to an existing installation of the CCS Application Server, perform the following procedure before adding the CCS Manager:

- Create a certificate for the CCS Manager using the Certificate Management Console. The Certificate Management Console is installed along with the installation of the CCS Application Server. See "Creating a certificate for installing a standalone CCS Manager" on page 167.

Do the following to add or upgrade the CCS components:

- Launch the Installation Wizard Maintenance panel
  The installation wizard detects a previous installation of CCS installed on the computer, and displays the **Maintenance** panel.
  See "To launch the Installation Wizard Maintenance panel" on page 287.
- Add or upgrade the CCS components
  See "To add or upgrade a CCS component" on page 287.

To launch the Installation Wizard Maintenance panel

1. Insert the **Symantec Control Compliance Suite 11.1** product disc into the drive on your computer and double-click **Setup.exe**.

   In the security warning dialog box, click **Run**.
2. In the DemoShield, click **CCS Suite**.
3. On the splash screen, click **Install CCS Suite**. The Setup file is located inside the CCS_Reporting folder of the product media.

   Setup prepares the CCS Suite installation wizard.

   See "Software requirements" on page 48.

To add or upgrade a CCS component

1. In the **Maintenance** panel of the launched Symantec Control Compliance Suite 11.1 installation wizard, select **Add/Upgrade**, and then click **Next**.
2. The **Add Components** panel lists the component that is not installed on your computer. The next panel that appears is dependent on the component you select. If this computer does not contain a CCS Manager installation, you can check **CCS Manager** to install the CCS Manager on the computer.

   You can add / upgrade CCS content. Check the Technical Standards, Frameworks and Regulations which you require for the appropriate platform.

   You can select individual standards or select a platform name to select all standards for the particular platform.

   Perform the following steps to install the CCS Manager.
3. In the **Add Components** panel, check **CCS Manager** to install the CCS Manager on the computer and click **Next**.
4. In the **Prerequisites** panel, review the prerequisites that are required for the installation. Install any prerequisite application that is required to be installed. Click **Check again** to verify whether the installation is successful.

   See "Software requirements" on page 48.
5. Click **Next**.

6 In the **Installation Folder** panel, review the installation path for product installation and click **Next**.

If the setup is unable to detect a valid installation source, specify a valid installation source location in the **Installation source location** field. If you are accessing the installation source from a network share, and you do not have direct access to the share, but you are using other user's credentials, ensure that the credentials of the user who has access to the share are cached. The credentials can be cached by checking **Remember my password** in the connection window that is displayed while logging on to the network share for the first time. If you are using Windows net use command to connect to the share, you can specify the **savecred** switch to cache the credentials.

Click **Refresh disk space information** to verify the available disk space on the computer.

7 In the **CCS Manager - Service Configuration** panel, enter a port for the CCS Manager. CCS components use this port to communicate with the CCS Manager.

You must import the security certificate that is used by the CCS Manager to communicate with the CCS Application Server securely.

The certificate which is to be deployed on the CCS Manager is created using the **Certificate Management Console**. The **Certificate Management Console** is installed on the CCS Application Server computer. You can either pull the certificate from the CCS Application Server computer or place it manually on the computer on which you are installing the CCS Manager.

Browse for the Security Certificate file location and enter the password.

8 In the **Summary** panel, review the installation details and click **Install**.

You can click the link, **Export Summary** to export the configuration details of all the components that are installed on the computer. The details appear in a browser, after you specify the location to export the summary.

9 The **Install** panel indicates the progress of the component installation. After the installation finishes, the **Result** panel appears.

If the installation is completed with warnings, a **Warning** panel displays warning messages or a **Result** panel displays critical errors, perform the remediation steps displayed in the **Detail** window to complete the installation.

You can click the link, **Log Files** to view the CCS Manager installation log files. The log files are in .csv format. You can use the LogViewer in the <Install_Directory>\Application Server to view the log files. The LogViewer helps you to easily identify warnings and errors using the color codes. Warnings are highlighted in yellow color and errors are highlighted in red color.

10 In the **Result** panel, review the installation result and then click **Next**.

You can click the link, **Log Files** to view the CCS Manager installation log files. The log files are in .csv format. You can use the LogViewer in the <Install_Directory>\Application Server to view the log files. The LogViewer helps you to easily identify warnings and errors using the color codes. Warnings are highlighted in yellow color and errors are highlighted in red color.

11 The **Next Steps** panel displays the additional steps that you must perform to complete the CCS deployment. Perform the next steps and then click **Finish**.

You can click the link, **Save the next steps** to save the next steps for future reference. The details appear in a browser, after you specify the location to save the next steps.

You can click the link, **Log Files** to view the CCS Manager installation log files. The log files are in .csv format. You can use the LogViewer in the <Install_Directory>\Application Server to view the log files. The LogViewer helps you to easily identify warnings and errors using the color codes. Warnings are highlighted in yellow color and errors are highlighted in red color.

You can check the option to view the release notes.

See "Registering the CCS Manager" on page 173.

Adding or upgrading CCS content in silent mode

Perform the following procedure to add or upgrade CCS content in the silent mode.

Read the end-user license agreement eula.txt located in the product media before proceeding with the upgrade.

All inputs required in the response file are case-sensitive. Ensure that you use the correct case for each value. For example, where "True" is required, enter "True" and not "true".

To add or upgrade CCS content in silent mode

While upgrading to CCS 11.1, the setup upgrades some Technical Standards and Regulations by default.

To see the list of content which is upgraded by default

See "Installing the CCS Content" on page 219.

You can install or upgrade more content using the CCS Content installer.

1. You require the `CCSContent_Upgrade.xml` response file to install / upgrade the CCS content. The response file is located in the Documentation\Utilities\Silent Install folder of the product media. Copy the response file to the local computer, and then edit the response file to provide user inputs for content to be installed during the installation. To install content for a Technical Standard, Framework or Regulation, change the value to "true". Changing the value to "false" does not install the content for that Technical Standard, Framework or Regulation.

   For example, to install Standard Content, in the response file, provide the value for Enabled as "True" in `<Feature Name="Standard Content" Enabled="True"/>`. If you provide "False", Standard Content will not be installed.

   The CCS Maintenance license is required to install / upgrade the CCS Content.

2. On the command prompt, navigate the location of the `SilentInstallLauncher.exe` file.

   The `SilentInstallLauncher.exe` file is located in the Documentation\Utilities\Silent Install folder of the product media.

3. Run the following command to add or upgrade CCS content:

   ```
   SilentInstallLauncher.exe /SetupPath="SetupExePath"
   /ResponseFile="ResponseFilePath"
   ```

   Where:

   - `SetupExePath` is the location of the CCS Content setup file. The Setup file is located inside the CCS_Content folder of the product media.
   - `ResponseFilePath` is the location of the response file for installing the CCS Content. Provide the location of the response file you edited in Step 1.

See "About silent installation return codes" on page 241.

Upgrading a standalone CCS Manager

You can upgrade the CCS Manager by applying the component update packages that are released in the post release of CCS.

You can perform the upgrade of the CCS Manager through the **Maintenance** panel of the **Symantec Control Compliance Suite 11.1 Installation Wizard**.

Do the following to upgrade the CCS Manager:

- Launch the Installation Wizard Maintenance panel
  The installation wizard detects a previous installation of CCS Manager installed on the computer, and displays the **Maintenance** panel.

See "To launch the Installation Wizard Maintenance panel" on page 291.

- Upgrade the CCS Manager
  See "Upgrade the CCS Manager" on page 291.

To launch the Installation Wizard Maintenance panel

1. Insert the **Symantec Control Compliance Suite 11.1** product disc into the drive on your computer and double-click **Setup.exe**.

   In the security warning dialog box, click **Run**.
2. In the DemoShield, click **CCS Manager**.
3. On the splash screen, click **Install CCS Manager**. The Setup file is located inside the CCS_Manager folder of the product media.

   Setup prepares the CCS Suite installation wizard.

   See "Software requirements" on page 48.

Upgrade the CCS Manager

1. In the **Maintenance** panel of the launched Symantec Control Compliance Suite 11.1 installation wizard, select **Add/Upgrade**, and then click **Next**.
2. In the **Installation Folder** panel, review the installation path for product installation and click **Next**.

   Click **Refresh disk space information** to verify the available disk space on the computer.
3. In the **Summary** panel, review the components to upgrade and click **Install**.
4. When the upgrade is complete, the **Finish** panel lists the results of the upgrade. Click **Finish** to close the Installation Wizard.

Repairing or reinstalling the CCS Suite

You can repair or reinstall the product components that are already installed on the computer. The requirement to repair the component can arise if the component was not installed properly during the first installation. You can repair or reinstall the product using the product disc, or through the **Add/Remove Programs** or **Programs and Features** window of the computer.

The repair or reinstallation of a component is performed through the **Maintenance** panel of the **Symantec Control Compliance Suite 11.1 Installation Wizard**.

Do the following to repair or reinstall the CCS components:

- Launch the Installation Wizard Maintenance panel

The installation wizard detects a previous installation of CCS installed on the computer, and displays the **Maintenance** panel.

See "To launch the Installation Wizard Maintenance panel" on page 292.

- Repair or reinstall the CCS components

See "To repair or reinstall CCS components" on page 292.

To launch the Installation Wizard Maintenance panel

1. Insert the **Symantec Control Compliance Suite 11.1** product disc into the drive on your computer and double-click **Setup.exe**.

   In the security warning dialog box, click **Run**.
2. In the DemoShield, click **CCS Suite**.
3. On the splash screen, click **Install CCS Suite**. The Setup file is located inside the CCS_Reporting folder of the product media.

   Setup prepares the CCS Suite installation wizard.

   See "Software requirements" on page 48.

To repair or reinstall CCS components

1. In the **Maintenance** panel of the launched Symantec Control Compliance Suite 11.1 installation wizard, select **Repair/Reinstall**, and then click **Next**.
2. In the **Summary** panel, review the components to repair and click **Install**.
3. When the repair is complete, the **Finish** panel lists the results of the repair. Click **Finish** to close the Installation Wizard.

Repairing or reinstalling a standalone CCS Manager

You can repair or reinstall the CCS Manager that is already installed on the computer. The requirement to repair the component can arise if the component was not installed properly during the first installation. You can repair or reinstall the CCS Manager using the product disc, or through the **Add/Remove Programs** or **Programs and Features** window of the computer.

The repair or reinstallation of the CCS Manager is performed through the **Maintenance** panel of the **Symantec Control Compliance Suite 11.1 Installation Wizard**.

Do the following to repair or reinstall the CCS Manager:

- Launch the Installation Wizard Maintenance panel

  The installation wizard detects a previous installation of the CCS Manager installed on the computer, and displays the **Maintenance** panel.

  See "To launch the Installation Wizard Maintenance panel" on page 293.

- Repair or reinstall the CCS Manager
  See "To repair or reinstall the CCS Manager" on page 293.

To launch the Installation Wizard Maintenance panel

1. Insert the **Symantec Control Compliance Suite 11.1** product disc into the drive on your computer and double-click **Setup.exe**.

   In the security warning dialog box, click **Run**.
2. In the DemoShield, click **CCS Manager**.
3. On the splash screen, click **Install CCS Manager**. The Setup file is located inside the CCS_Manager folder of the product media.

   Setup prepares the CCS Suite installation wizard.

   See "Software requirements" on page 48.

To repair or reinstall the CCS Manager

1. In the **Maintenance** panel of the launched Symantec Control Compliance Suite 11.1 installation wizard, select **Repair/Reinstall**, and then click **Next**.
2. In the **Summary** panel, review the components to repair and click **Install**.
3. When the repair is complete, the **Finish** panel lists the results of the repair. Click **Finish** to close the Installation Wizard.

Repairing the CCS Agent

You can repair a CCS Agent using the product disc.

Note: If you are using an updated version of the CCS Agent, ensure that you use that CCS Agent setup for repair.

To repair the CCS Agent

1. Insert the **Symantec Control Compliance Suite 11.1** product disc into the drive on your computer and double-click the CCS_Agent folder.
2. The Setup files for installing CCS Agents on various platforms are located inside the CCS_Agent folder of the product media.

   Open the Windows folder and double-click **Setup.exe**.

   Setup prepares the CCS Agent installer.
3. In the **Program Maintenance** panel of the launched Symantec Control Compliance Suite 11.1 Agent installation, click **Repair** to repair the CCS Agent installation.

4 Click **Next**.

5 In the **Ready to Repair the Program** panel, click **Install**.

6 The progress bar indicates the progress of the installation. After the installation finishes, the **Setup Wizard Completed** panel appears.

7 In the **Setup Wizard Completed** panel, click **Finish**

Chapter 6

Uninstalling CCS components

This chapter includes the following topics:

Uninstalling the CCS Suite

You can uninstall all the components that are installed on a single computer as part of the single setup mode. You can uninstall the product using the product disc, or through the **Add/Remove Programs** or **Programs and Features** window of the computer.

The uninstallation of all the components can be performed through the **Maintenance** panel of the **Symantec Control Compliance Suite 11.1 Installation Wizard**

Do the following to uninstall CCS components:

- Launch the Installation Wizard Maintenance panel
  The installation wizard detects a previous installation of CCS installed on the computer, and displays the **Maintenance** panel.
  See "To launch the Installation Wizard Maintenance panel" on page 296.
- Uninstall CCS components

  Do one of the following:

  - Uninstall all CCS components

This uninstalls both the CCS Application Server and the CCS Manager.
See "To uninstall all CCS components" on page 296.

- Uninstall the CCS Manager
  This lets you uninstall the CCS Manager, when the CCS Manager is installed along with the CCS Application Server on a single computer.
  See "To uninstall the CCS Manager" on page 297.

To launch the Installation Wizard Maintenance panel

1. Insert the **Symantec Control Compliance Suite 11.1** product disc into the drive on your computer and double-click **Setup.exe**.

   In the security warning dialog box, click **Run**.
2. In the DemoShield, click **CCS Suite**.
3. On the splash screen, click **Install CCS Suite**. The Setup file is located inside the CCS_Reporting folder of the product media.

   Setup prepares the CCS Suite installation wizard.

To uninstall all CCS components

1. In the **Maintenance** panel of the launched Symantec Control Compliance Suite 11.1 installation wizard, select **Uninstall**.
2. Under the **Uninstall** option, select **All**.
3. Click **Next**.
4. In the **Directory Server- Remove ADAM instance** panel, select either of the following options and click **Next**.
   - Remove the ADAM instance that Control Compliance Suite uses.
   - Do not remove the ADAM instance that Control Compliance Suite uses.
5. In the **Application Server - Delete Stored Data** panel, select the databases that are to be removed and click **Next**.

   The databases that can be removed are Production database and Reporting database.

Note: If you remove the production database, then all the Technical Standards Pack (TSP) that are stored in ADAM are also removed. The TSPs are removed from ADAM, even if you select the option, Do not remove the ADAM instance that Control Compliance Suite uses in the previous panel.

---

6 In the **Summary** panel, review the components that are to be uninstalled and click **Uninstall**.

7 When the uninstallation is complete, the **Finish** panel lists the results of the uninstallation. Click **Finish** to close the Installation Wizard.

To uninstall the CCS Manager

1 In the **Maintenance** panel of the launched Symantec Control Compliance Suite 11.1 installation wizard, select **Uninstall**.

2 Under the **Uninstall** option, select **Select Components**.

3 Click **Next**.

4 In the **Remove Components** panel, select **CCS Manager** and click **Next**.

5 In the **Summary** panel, review the components that are to be uninstalled and click **Uninstall**.

6 When the uninstallation is complete, the **Finish** panel lists the results of the uninstallation. Click **Finish** to close the Installation Wizard.

Uninstalling a standalone CCS Manager

You can uninstall a standalone CCS Manager using the product disc, or through the **Add/Remove Programs** or **Programs and Features** window of the computer.

The uninstallation of the CCS Manager can be performed through the **Maintenance** panel of the **Symantec Control Compliance Suite 11.1 Installation Wizard**

Do the following to uninstall CCS components:

- Launch the Installation Wizard Maintenance panel
  The installation wizard detects a previous installation of the CCS Manager installed on the computer, and displays the **Maintenance** panel.
  See "To launch the Installation Wizard Maintenance panel" on page 298.
- Uninstall the CCS Manager
  See "To uninstall the CCS Manager" on page 298.

To launch the Installation Wizard Maintenance panel

1. Insert the **Symantec Control Compliance Suite 11.1** product disc into the drive on your computer and double-click **Setup.exe**.

   In the security warning dialog box, click **Run**.
2. In the DemoShield, click **CCS Manager**.
3. On the splash screen, click **Install CCS Manager**. The Setup file is located inside the CCS_Manager folder of the product media.

   Setup prepares the CCS Suite installation wizard.

   See "Software requirements" on page 48.

To uninstall the CCS Manager

1. In the **Maintenance** panel of the launched Symantec Control Compliance Suite 11.1 installation wizard, select **Uninstall**.
2. Under the **Uninstall** option, select **All**.
3. Click **Next**.
4. In the **Summary** panel, review the components that are to be uninstalled and click **Uninstall**.
5. When the uninstallation is complete, the **Finish** panel lists the results of the uninstallation. Click **Finish** to close the Installation Wizard.

Uninstalling the CCS Agent on Windows

You can uninstall a CCS Agent using the product disc, or through the control panel of the computer. **Add/Remove Programs** or **Programs and Features** window of the computer.

Note: If you are using an updated version of the CCS Agent, ensure that you use that CCS Agent setup to uninstall.

To uninstall the CCS Agent using the product disc

1. Insert the **Symantec Control Compliance Suite 11.1** product disc into the drive on your computer and double-click the CCS_Agent folder.
2. The Setup files for installing CCS Agents on various platforms are located inside the CCS_Agent folder of the product media.

   Open the Windows folder and double-click **Setup.exe**.

   Setup prepares the CCS Agent installer.

3 In the **Program Maintenance** panel of the launched Symantec Control Compliance Suite 11.1 Agent installation, click **Remove** to remove the CCS Agent installation.

4 Click **Next**.

5 In the **Remove the Program** panel, click **Remove**.

6 The progress bar indicates the progress of the uninstallation. After the uninstallation finishes, the **Setup Wizard Completed** panel appears.

7 In the **Setup Wizard Completed** panel, click **Finish**

To uninstall the CCS Agent through the control panel

1 In the control panel of the computer, open the **Add/Remove Programs** or **Programs and Features** window.

2 Double-click **Symantec Control Compliance Suite 11.1 - Agent**

3 Click **Yes** on the message that appears.

4 The progress bar indicates the progress of the uninstallation and the uninstallation finishes.

Uninstalling the CCS Agent on UNIX

On the computers that have a UNIX operating system, the esmdeinstall program removes everything under the /esm directory.

Before you uninstall the CCS Agent, make sure that you not using the /esm directory or any of its subdirectories. If you use the /esm directory or subdirectory, the esmdeinstall program reports an error message and does not remove the directory.

To uninstall the CCS Agent on UNIX

1 At the command prompt, type `/esm/esmdeinstall`.

2 Type `Yes` to remove the CCS Agent.

Appendix A

Altiris integration

This appendix includes the following topics:

About Altiris integration

Review the following information to plan for the deployment of Altiris integration:

- CCS Asset Export Task architecture
  See "CCS Asset Export Task architecture" on page 301.
- CCS Asset Export Task requirements
  See "Prerequisites for installing the CCS Asset Export Task" on page 302.
- CCS Asset Export Task recommendations
  See "CCS Asset Export Task recommendations" on page 303.

About importing assets from Altiris

CCS provides the CCS Asset Export Task solution to import certain types of assets from the Altiris Configuration Management Database (CMDB) to the CCS database. Windows and UNIX are the predefined asset types that are supported.

The CCS Asset Export Task solution must be installed on the Altiris Notification Server before you can export the assets.

See "Installing Asset Export Task on Altiris Notification Server" on page 303.

When you install the CCS Asset Export Task solution, it becomes part of the Altiris Symantec Management Console. Most of the functionality appears in the **Manage > Jobs and Tasks > Notification Server** option.

The **Altiris Symantec Management Console** is a Web-based user interface that is the primary tool for interacting with Notification Server and installed solutions.

The CCS Asset Export Task solution does the following:

- Exports assets from the Altiris CMDB to a CSV file.
- Runs an asset import job on CCS. The asset import job imports assets from the CSV file to the CCS asset system. The assets are imported using a CSV data collector.

If any resource is deleted from the Altiris CMDB, the corresponding asset is not deleted from the CCS asset system.

CCS Asset Export Task architecture

The CCS Asset Export Task plugs in to the Altiris Notification Server to export asset data CSV files. The CCS CSV importer can import the exported asset data files. When the export is complete, the Asset Export Task automatically starts asset import job. The CCS reconciliation rules manage the imported assets.

When you install the Asset Import Task, it appears in the **Manage > Jobs and Tasks > Notification Server** option in the Symantec Altiris Management Console.

See "About using Altiris Symantec Management Console with CCS" on page 301.

See "What the CCS Asset Export Task can do for you" on page 301.

See "How the Asset Export Task works" on page 302.

About using Altiris Symantec Management Console with CCS

The CCS Asset Export Task lets you export assets from the Altiris Configuration Management Database (CMDB). When you export these assets, you can use the Altiris Symantec Management Console with CCS. When you link the products, you can link compliance management and remediation together.

See "What the CCS Asset Export Task can do for you" on page 301.

See "CCS Asset Export Task architecture" on page 301.

See "How the Asset Export Task works" on page 302.

What the CCS Asset Export Task can do for you

The CCS Export Task lets you use CCS with an existing Symantec Altiris Management Console deployment. The task lets you link the notification tools and remediation tools in the Altiris Management Console with compliance tools in CCS. You can then automatically open Altiris ServiceDesk tickets based on compliance criteria you specify. If you choose, the assets can automatically be reevaluated for compliance when the ticket is closed.

See "CCS Asset Export Task architecture" on page 301.

See "How the Asset Export Task works" on page 302.

How the Asset Export Task works

The CCS Asset Export Task lets you export certain types of resources from the Altiris Configuration Management Database (CMDB) to a CSV file. The CCS CSV data collector automatically imports the intermediate CSV file. When you import the file, the assets it includes are processed according to the reconciliation rules in effect.

Note: If an asset is deleted from the Altiris CMDB, it is not deleted from the CCS asset system automatically.

See "About using Altiris Symantec Management Console with CCS" on page 301.

See "What the CCS Asset Export Task can do for you" on page 301.

See "CCS Asset Export Task architecture" on page 301.

Prerequisites for installing the CCS Asset Export Task

The CCS Asset Export Task installs as a part of the Symantec Altiris Management Console on the Altiris Notification Server. It is used to connect the Altiris Notification Server to CCS. The CCS Asset Export Task does not have additional requirements beyond those for the Altiris Notification Server and those for CCS. Each of these products has minimum requirements for hardware and software. Symantec recommends that you do not install the CCS Asset Export Task component on any computers that do not meet these requirements.

Before you install the CCS Asset Export Task, you must do the following:

- Install and configure the Altiris Notification Server 7.0.
- Install and configure the Symantec Install Manager.
- Configure the CSV Data Collector to import the assets CSV file.
- Create asset import jobs for Windows and UNIX asset types.

See "CCS Asset Export Task architecture" on page 301.

See "How the Asset Export Task works" on page 302.

See "CCS Asset Export Task recommendations" on page 303.

CCS Asset Export Task recommendations

You must specify credentials for a location on the network that is accessible to both CCS and the Altiris Notification Server. The Asset Export Task stores the exported files in the specified location and CCS imports the files from the same location.

See "CCS Asset Export Task architecture" on page 301.

See "Prerequisites for installing the CCS Asset Export Task" on page 302.

Planning the Asset Export Task deployment

Your deployment of the CCS Asset Export Task should take place as part of your overall deployment of CCS. Before you deploy the Asset Export Task, you should have a complete, configured CCS and Altiris Notification Server. You should only deploy the CCS Asset Export Task when you are comfortable with the performance and operations of the other components.

Deployment of the CCS Asset Export Task must be carefully coordinated between the CCS administrator and the Altiris administrator. Both administrators have tasks to perform. Since those tasks must be performed in sequence, coordination between them is essential.

In particular, the CCS administrator must be able to provide the URL of the CCS Web Services host.

Installing the Asset Export Task

You use the Symantec Install Manager to download the CCS Asset Export Task. After it is installed, you can install and configure the Asset Export Task.

Installing Asset Export Task on Altiris Notification Server

You use Symantec Installation Manager to install the CCS Asset Export Task solution.

You must install the solution on Altiris Notification Server 7.0.

To install the CCS Asset Export Task

1. Start Symantec Installation Manager.
2. On the **Installed Products** page, click **Install new products**.
3. On the **Install New Products** page, check **CCSAssetExport**, and then click **Review selected products**.
4. On the **Selected Products and Features** page, verify that you selected the correct product, and then click **Next**.

5 On the **End User License Agreement** page, check **I accept the terms in the license agreements**, and then click **Next**.

6 On the **Contact Information** page, type the required information, and then click **Next**.

7 On the **Computers to Manage** page, click **Begin install** to begin the installation.

8 On the **Installation Complete** page, click **Finish**.

You can now launch the Symantec Management Console to access the CCS Asset Export Task solution.

See "About importing assets from Altiris" on page 300.

Appendix B

Maintenance

This appendix includes the following topics:

Database maintenance

In normal operations, your deployment of CCS stores large amounts of data in the databases. Over time, these normal operations require you to perform maintenance on the databases outside of CCS. Regular database maintenance is required for the following reasons:

- Over time, heavy use of CCS can cause index fragmentation in CCS databases which can negatively affect performance of the activities that depend on the databases.
- Performance of Reporting sync job, Report generation jobs and dynamic Dashboards can become slow.

Symantec recommends to execute database maintenance plan if the index fragmentation in CCS databases goes above 90%. You can check index fragmentation levels of CCS databases in the Health and Status Details.

The Product Health and Status area on the CCS Console homepage, displays a notification when the CCS database plan is pending. The Database maintenance is pending notification appears if the index fragmentation in CCS databases goes above 90% and when the alert notification is due as per the number of days specified in the Health and Status Notifications configuration. To setup Health and Status notifications, on the CCS Console, go to **Settings > General > System Configuration > Health and Status Notification**.

Clicking the Database maintenance is pending link allows you to run the database maintenance plan or view the database maintenance plan. You can run the maintenance plan directly to perform the Rebuild Index and Update Statistics maintenance tasks. You can view a help topic on the database maintenance plan which provides information about performing the database maintenance tasks using Microsoft SQL Server. While the database maintenance is running, the Database Maintenance Status dialog box appears and the alert link changes to Database maintenance in progress. CCS cannot run any other jobs until the database maintenance is complete.

Symantec recommends running the Database maintenance plan at a time when database utilization by CCS is at its lowest. Ideally this maintenance plan should be executed by scheduling CCS downtime to make sure CCS does not hit the database during the time SQL is running maintenance plan.

Before performing the database maintenance plan, you must run the SQL script for archiving the historical results data.

See "SQL script for archival of historical results data" on page 310.

To create a basic database maintenance plan for production and reporting database

1. Ensure SQL Agent service is up and running.
2. Launch SQL Management Studio from **All Programs** > **SQL Microsoft SQL Server**
3. Expand **Management** node.
4. Right click **Maintenance Plans** and select **Maintenance Plan Wizard**.
5. Click **Next** in the first panel.
6. Specify a name for the maintenance plan.

   Retain the default option and if required specify a schedule. The database maintenance plan can be created once and then scheduled to run periodically.
7. Click **Next** and select the maintenance tasks to be executed.
8. Select **Rebuild Index** and **Update Statistics**. Additionally, you can select **Shrink Database** or **Back Up Database** tasks as per your requirement.
9. Click **Next** to launch the sequence confirmation page.

   Make sure **Rebuild Index** is run before **Update Statistics**. If selected in step 8, the **Shrink Database** or **Back Up Database** must be run after **Update Statistics**.
10. Click **Next**. This allows for definition of rebuild index task.
11. From databases, select the CCS databases CSM_DB and CSM_Reports.

12 Under Advanced options, check **Keep index online while reindexing** only when SQL server is low on memory resources. If you choose this option, then the indexes may take longer time to rebuild. The **Keep index online while reindexing** option is available only in Enterprise editions and Symantec recommends not to check that option.

13 Click **Next** to define update statistics.

14 From databases, select the CCS databases CSM_DB and CSM_Reports.

15 Retain the default options **All existing statistics** and **Full Scan**.

16 Click **Next** and select the appropriate reporting options.

17 Click **Next** and then click **Finish** to complete the creation of the maintenance plan.

18 Click **Close** on the Maintenance Pan Wizard Progress panel.

19 To execute the maintenance plan, right click **Maintenance Plan**, and select **Execute**.

After you execute the database maintenance plan, you must run the alter index views script. When you execute a database maintenance plan, it sets the parameter STATISTICS_NORECOMPUTE =ON for indexes, which disables automatic statistics updating. You must enable automatic statistics updating by executing the SQL script to alter index views.

See "SQL script to alter index views" on page 307.

In cases where there are large number of controls that are added to the controls hierarchy, run the database maintenance plan to avoid a degrade in the performance of the Global Metrics and Trend Computation job. For information on Global Metrics and Trend Computation job, see the *Symantec™ Control Compliance Suite User Guide*.

SQL script to alter index views

When you execute a database maintenance plan, it sets the parameter STATISTICS_NORECOMPUTE =ON for indexes, which disables automatic statistics updating. You must enable automatic statistics updating by executing the following SQL script :

```
USE [CSM_Reports]

GO

ALTER INDEX [uci_ivMandateID] ON [Dashboard].[ivMandateID] REBUILD
WITH ( PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, ALLOW_ROW_LOCKS
```

```
= ON, ALLOW_PAGE_LOCKS = ON, SORT_IN_TEMPDB = OFF, IGNORE_DUP_KEY =
OFF, ONLINE = OFF )

GO

USE [CSM_Reports]

GO

ALTER INDEX [uci_ivStatementName] ON [Dashboard].[ivStatementName]
REBUILD WITH ( PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF,
ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON, SORT_IN_TEMPDB = OFF,
IGNORE_DUP_KEY = OFF, ONLINE = OFF )

GO

USE [CSM_Reports]

GO

ALTER INDEX [uci_ivAssetName_AssetName_AssetType_AssetID_AssetVersion]
ON [dbo].[ivAssetName] REBUILD WITH ( PAD_INDEX = ON,
STATISTICS_NORECOMPUTE = OFF, ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS
= ON, SORT_IN_TEMPDB = OFF, IGNORE_DUP_KEY = OFF, ONLINE = OFF )

GO

USE [CSM_Reports]

GO

ALTER INDEX [unci_ivAssetName_AID_AV_Name] ON [dbo].[ivAssetName]
REBUILD WITH ( PAD_INDEX = ON, STATISTICS_NORECOMPUTE = OFF,
ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON, SORT_IN_TEMPDB = OFF,
IGNORE_DUP_KEY = OFF, ONLINE = OFF )

GO

USE [CSM_Reports]
```

GO

```
ALTER INDEX [uci_ivMandateState_MandateID_MandateVersion] ON
[dbo].[ivMandateState] REBUILD WITH ( PAD_INDEX = OFF,
STATISTICS_NORECOMPUTE = OFF, ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS
= ON, SORT_IN_TEMPDB = OFF, IGNORE_DUP_KEY = OFF, ONLINE = OFF )

GO

USE [CSM_Reports]

GO
```

```
ALTER INDEX
[uci_ivSubjectName_SubjectName_SubjectType_SubjectID_SubjectVersion]
ON [dbo].[ivSubjectName] REBUILD WITH ( PAD_INDEX = ON,
STATISTICS_NORECOMPUTE = OFF, ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS
= ON, SORT_IN_TEMPDB = OFF, IGNORE_DUP_KEY = OFF, ONLINE = OFF )

GO

USE [CSM_Reports]
GO

ALTER INDEX [uci_ivTestName_TestName_TestID_TestVersion] ON
[dbo].[ivTestName] REBUILD WITH ( PAD_INDEX = ON,
STATISTICS_NORECOMPUTE = OFF, ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS
= ON, SORT_IN_TEMPDB = OFF, IGNORE_DUP_KEY = OFF, ONLINE = OFF )

GO

USE [CSM_Reports]
GO

ALTER INDEX [unci_ivTestName_TID_TV_TN] ON [dbo].[ivTestName] REBUILD
WITH ( PAD_INDEX = ON, STATISTICS_NORECOMPUTE = OFF, ALLOW_ROW_LOCKS
= ON, ALLOW_PAGE_LOCKS = ON, SORT_IN_TEMPDB = OFF, IGNORE_DUP_KEY =
OFF, ONLINE = OFF )

GO

USE [CSM_Reports]
GO

ALTER INDEX [uci_vUserAsset_UID_AID_AV] ON [dbo].[vUserAsset] REBUILD
WITH ( PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, ALLOW_ROW_LOCKS
= ON, ALLOW_PAGE_LOCKS = ON, SORT_IN_TEMPDB = OFF, IGNORE_DUP_KEY =
OFF, ONLINE = OFF )

GO

USE [CSM_Reports]
GO

ALTER INDEX [unci_ivTestName_TID_TV_TN] ON [dbo].[ivTestName] REBUILD
WITH ( PAD_INDEX = ON, STATISTICS_NORECOMPUTE = OFF, ALLOW_ROW_LOCKS
= ON, ALLOW_PAGE_LOCKS = ON, SORT_IN_TEMPDB = OFF, IGNORE_DUP_KEY =
OFF, ONLINE = OFF )

GO
```

```
USE [CSM_Reports]
```

GO

```
ALTER INDEX [uci_vUserAsset_UID_AID_AV] ON [dbo].[vUserAsset] REBUILD
WITH ( PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, ALLOW_ROW_LOCKS
= ON, ALLOW_PAGE_LOCKS = ON, SORT_IN_TEMPDB = OFF, IGNORE_DUP_KEY =
OFF, ONLINE = OFF )
```

See "SQL script for archival of historical results data" on page 310.

SQL script for archival of historical results data

After you execute the database maintenance plan on the reporting database, you must run the following SQL script on the reporting database CSM_Reports for archival of historical results data:

```
USE [CSM_Reports]

GO

EXEC [dbo].[symc_ArchiveSTRTables]

GO
```

See "SQL script to alter index views" on page 307.

SQL script for deletion of third party evidence data

After you upgrade to CCS 11.1, as part of the database maintenance plan, you must run the following SQL script on the reporting database CSM_Reports for deletion of third party evidence data:

```
USE [CSM_Reports]

GO

EXEC [dbo].[spDeleteExtendedEvidenceData]

GO
```

See "SQL script to alter index views" on page 307.

Database maintenance for evidence data

In Control Compliance Suite, the Standards module generates results after running checks for a compliance policy. The results include detailed evidence data which describes the reason why a check has passed or failed. You can use the evidence data for remediation, to demonstrate compliance to auditors, or in litigation.

In CCS 11.1, the evidence data of Standards module and external data providers is stored directly in the reporting database CSM_Reports. The data is stored in the evidence file group for 90 days from the installation of the product, and a new evidence file group gets created after every 90 days

The details of the evidence data that is stored in the reporting database, is as follows:

File name	CSM_Reports_EvidenceStorage_<yyyymmdd>.ndf
Filegroup Name	FG_EvidenceStorage_<yyyymmdd>
Evidence Storage Table Name for one quarter	dbo.EvidenceStorage_<yyyymmdd>
Default Filegroup Path	By default the secondary filegroup .ndf file is created in the same directory where primary filegroup CSM_reports.mdf file resides.

Note: The existing evidence data remains in the primary filegroup, CSM_reports.

You can perform certain tasks to optimize database performance and storage management.

To optimize database performance:

- Move filegroups to different disks
  See "Moving filegroups to different locations" on page 312.
- Compress evidence storage filegroup
  You can compress the filegroups to save on storage space. Depending on the SQL Server edition you use, you can either use the page compression or NTFS compression.
  See "Compressing the evidence storage filegroup for enterprise edition of SQL Server " on page 312.
  See "Compressing the evidence storage filegroup for non-enterprise edition of SQL server" on page 314.
- Backup and restore of evidence storage data
  See "Backup and restore of evidence data" on page 314.
- Purge evidence data from reporting database
  See "Purging of evidence data" on page 314.

Moving filegroups to different locations

Evidence data consumes a major part of the database. If there is low disk space on the primary filegroups drive, then Symantec recommends that the filegroups be moved to different disks, in order to improve the database performance and storage management.

You must be in the role of db_owner on CSM_Reports database and must have the Alter permission on the database.

To move filegroups to different disks

1 Run the following query:

```
ALTER DATABASE CSM_Reports

MODIFY FILE

(

NAME = CSM_Reports_EvidenceStorage_<yyyymmdd>,

FILENAME = N'newpath\CSM_Reports_EvidenceStorage_<yyyymmdd>.ndf'

);
```

For example

```
ALTER DATABASE CSM_Reports

MODIFY FILE

(

NAME = CSM_Reports_EvidenceStorage_20110820,

FILENAME = N'C:\CSM_Reports_EvidenceStorage_20110820.ndf'

);
```

2 Take the database offline by running the command:

```
ALTER DATABASE CSM_Reports SET OFFLINE WITH ROLLBACK IMMEDIATE
```

Note: In case you an unable to take the database offline, restart the SQL server.

Compressing the evidence storage filegroup for enterprise edition of SQL Server

If you are using the Microsoft SQL Server 2008, Microsoft SQL Server 2012, or Microsoft SQL Server 2014 Enterprise Edition, then to save on storage space,

Symantec recommends that you use the page compression feature to compress the old filegroups

After compressing the database, you can further reduce the size of the database by shrinking the individual files or the database. This way you can release unallocated space.

Note: In case you are using SQL Server 2008 edition then you must install the latest service pack of SQL Server 2008.

You must be in the role of db_owner on CSM_Reports database and must have the Alter permission on the database.

To compress the older filegroups

1. In the CSM_Reports database, navigate to the evidence storage table. Right-click the table and click Storage > Manage compression.
2. On the Select Compression Type, select **Page**, and click **Next**.
3. On the **Select an output option** dialog box, select **Run immediately** , and click **Finish**.
4. You can use the Shrink database option to shrink all the files in a database. Navigate to the CSM_Reports database.
5. Right-click CSM_Reports database, and click **Tasks > Shrink > Files**.
6. Enter the size to which you want the file to be shrunk.

   Note: Before compressing the evidence data file `CSM_Reports_EvidenceStorage_<yyyymmdd>.ndf`, ensure that the available free disk space is greater than or equal to 1.5 times of the existing ndf file size.

Note: Microsoft has reported an issue in SQL Server 2008 Enterprise Edition in the page compression feature when used with the Shrink database option.

Refer to the following knowledge base article for a resolution of the reported issue:

http://support.microsoft.com/kb/963658

Compressing the evidence storage filegroup for non-enterprise edition of SQL server

For SQL Server standard edition, when there is low disk space due to large amount of evidence data, you can perform filegroup based NTFS compression on older filegroups till the retention period for it is over

You must be a db_owner on CSM_Reports database and must have ALTER permission on the database. You must be a local administrator to perform NTFS compression on the filegroup.

To perform filegroup based NTFS compression

1. Navigate to **CSM_Reports > Properties > Filegroups**.
2. Click the Options tab and mark the filegroup as read-only.
3. Right-click **CSM_Reports**, click **Tasks**, and click **Take offline**.
4. At the command prompt, type the following command:

   ```
   COMPACT /C <ndf filename>
   ```

5. Bring the database online by clicking **Take online** on **Tasks**.

Backup and restore of evidence data

You can use multiple backup options to take backup of evidence storage tables.

The different type of backups are as follows:

- Full database backup
- Backup of .ndf files
- Filegroup-based backup

Refer to the following link for more details:

http://technet.microsoft.com/en-us/library/ms186865.aspx

Purging of evidence data

Evidence data purging is based on reporting database purge settings for historical results. The option **Purge historical results from reporting database after N days** from the Reports tab, under Purge settings is used for purging of evidence data. The evidence table and filegroup are deleted after the purge period is over. The default retention period for evidence purge is three years (1095 days).

If there are issues with deleting filegroups during purge operations, then evidence data purge is required to be a part of the database maintenance plan. During the

normal purge operations, there can be errors because some files are in use. If you identify any orphan filegroups, you can delete them manually.

To delete a filegroup manually

1 Run the query:

```
(select PartitionName as TableName,Filegroup from
EvidencePartitionInfo where State = 2)
```

2 Manually delete the table and filegroup that is returned from the query in step 1. Delete the filegroup and table in one of the following ways:

- Navigate to the evidence storage table and right-click and select **Delete**.
- Navigate to CSM_Reports->Properties->Filegroup and click **Remove** and **OK**.

Disaster recovery and migration

This section contains procedures for disaster recovery and data migration for Symantec Control Compliance Suite release 11.1. Restoration of a component prevents data loss and eliminates the need to perform reconfiguration tasks in the CCS Console.

Migration includes restoring CCS components and then migrating CCS components from one computer to another computer with existing data.

As part of your disaster recovery procedures, you must backup the following CCS components at regular intervals in case you need to recover from a component failure in the future:

- The CCS ADAM and SQL Databases.
  See "Backing up the CCS ADAM and SQL databases" on page 324.
- If you are using ESM for data collection, backup the ESM components.
  See "Backing up the ESM components" on page 328.

You can restore the following CCS components in case of a failure.

- The CCS ADAM and SQL Databases, and the CCS configuration files.
  See "Restoring the CCS ADAM and SQL databases" on page 325.
- If you are using ESM for data collection, restore the ESM components.
  See "Restoring the ESM components" on page 328.

This document provides disaster recovery and migration procedures for the following scenarios:

You can consolidate the CCS components or migrate to other platforms or computers in the following scenarios:

- You have upgraded to 11.1 with CCS Directory Server and CCS Application Server on two separate computers and you want to consolidate the CCS Directory Server and CCS Application Server components on a single computer. This will reduce your hardware requirements from using two separate computers to host the Directory Sever and Application Server to using one single computer to host both the Directory Server and Application Server components.
  - You have upgraded to 11.1 with components installed are on a 32 bit operating system and you want to migrate to a 64 bit operating system.
  - You have upgraded to 11.1 and you want to migrate your CCS setup from a physical computer to a virtual computer.

  See "Consolidating the CCS Directory Server and CCS Application Server on a single computer and migrating to other platforms" on page 319.
- You have installed / upgraded to 11.1 and you want to migrate your existing CCS 11.1 setup to a new computer.
  See "Migrating CCS 11.1 installation to a new computer" on page 319.
- You have installed / upgraded to 11.1 and you want to migrate your existing CCS 11.1 setup to a new domain.
  See "Migrating CCS 11.1 installation to a new domain" on page 320.
- You have installed / upgraded to 11.1 and you want to change the domain of an existing CCS 11.1 installation.
  See "Changing the domain of an existing CCS 11.1 installation" on page 320.

For supported operating systems and databases, See "Supported operating systems and databases for migration" on page 316.

Supported operating systems and databases for migration

The following table lists the operating systems supported for migration.

Table B-1 Operating systems supported for migration

Current operating system	Operating system you can migrate to
Windows Server 2003 32 bit	Windows Server 2008 32 bit / 64 bit / R2
Windows Server 2003 64 bit	Windows Server 2008 64 bit / R2
Windows Server 2008 32 bit	Windows Server 2008 32 bit / 64 bit / R2
Windows Server 2008 64 bit	Windows Server 2008 64 bit / R2

Note: CCS does not support migration of CCS installed on Windows Server 2008 64 bit operating system to Windows Server 2003 32 bit or Windows Server 2008 32 bit operating system. CCS also does not support migration of CCS installed on Windows Server 2008 R2 operating system to Windows Server 2008 64 bit operating system.

The following table lists the Microsoft SQL Server versions supported for migration.

Table B-2 SQL Server versions supported for migration

Current SQL Server version	SQL Server version you can migrate to
SQL Server 2005 32 bit	SQL Server 2005 64 bit SQL Server 2008 64 bit / R2
SQL Server 2005 64 bit	SQL Server 2005 64 bit SQL Server 2008 64 bit / R2
SQL Server 2008 32 bit	SQL Server 2008 64 bit / R2
SQL Server 2008 64 bit	SQL Server 2008 64 bit / R2

Disaster Recovery and Migration scenarios

This section provides disaster recovery and migration procedures for the following scenarios:

- You are upgrading from CCS 10.5.1 to CCS 11.1 and the upgrade fails. You can recover the CCS 10.5.1 setup provided you are taking regular backups of existing CCS 10.5.1.
  See "Recovering CCS 10.5.1 in case of disaster while upgrading to CCS 11.1" on page 318.
- You can consolidate the CCS components or migrate to other platforms or computers in the following scenarios:
  - You have upgraded to 11.1 with CCS Directory Server and CCS Application Server on two separate computers and you want to consolidate the CCS Directory Server and CCS Application Server components on a single computer. This will reduce your hardware requirements from using two separate computers to host the Directory Sever and Application Server to using one single computer to host both the Directory Server and Application Server components.
  - You have upgraded to 11.1 with components installed are on a 32 bit operating system and you want to migrate to a 64 bit operating system.

- You have upgraded to 11.1 and you want to migrate to a new computer and collect data from platforms only supported by CCS 10.5.1, such as NDS and NetWare.
- You have upgraded to 11.1 and you want to migrate your CCS setup from a physical computer to a virtual computer.

See "Consolidating the CCS Directory Server and CCS Application Server on a single computer and migrating to other platforms" on page 319.

- You have installed / upgraded to 11.1 and you want to migrate your existing CCS 11.1 setup to a new computer.
  See "Migrating CCS 11.1 installation to a new computer" on page 319.
- You have installed / upgraded to 11.1 and you want to migrate your existing CCS 11.1 setup to a new domain.
  See "Migrating CCS 11.1 installation to a new domain" on page 320.
- You have installed / upgraded to 11.1 and you want to change the domain of an existing CCS 11.1 installation.
  See "Changing the domain of an existing CCS 11.1 installation" on page 320.

Recovering CCS 10.5.1 in case of disaster while upgrading to CCS 11.1

You can recover CCS 10.5.1 in case of a disaster while upgrading to CCS 11.1. Perform the following procedure to recover CCS in case of a disaster while upgrading CCS 10.5.1 to CCS 11.1.

It is assumed that you are performing a regular backup of the CCS ADAM and SQL databases, and the ESM components, if you are using ESM for data collection.

See "Backing up the CCS ADAM and SQL databases" on page 324.

See "Backing up the ESM components" on page 328.

To recover CCS 10.5.1 from a disaster while upgrading to CCS 11.1

1. Install CCS 10.5.1 on a new computer. See "Creating a new CCS setup" on page 323.

   For information on installing CCS 10.5.1, see the *Symantec Control Compliance 10.5 Installation Guide*.
2. Restore the Application Server my restoring the CCS ADAM and SQL databases. See "Restoring the CCS ADAM and SQL databases" on page 325.
3. If you are using an ESM Manager and ESM Agent to collect asset data from your network, restore the ESM components. See "Restoring the ESM components" on page 328.

Consolidating the CCS Directory Server and CCS Application Server on a single computer and migrating to other platforms

You can use the migration procedure given in the section in case of the following scenarios:

- You have upgraded to 11.1 with CCS Directory Server and CCS Application Server on two separate computers and you want to consolidate the CCS Directory Server and CCS Application Server components on a single computer. This will reduce your hardware requirements from using two separate computers to host the Directory Sever and Application Server to using one single computer to host both the Directory Server and Application Server components.
- You have upgraded to 11.1 with components installed are on a 32 bit operating system and you want to migrate to a 64 bit operating system.
- You have upgraded to 11.1 and you want to migrate to a new computer and collect data from platforms only supported by CCS 10.5.1, such as NDS and NetWare.
- You have upgraded to 11.1 and you want to migrate your CCS setup from a physical computer to a virtual computer.

It is assumed that after upgrading to CCS 11.1 you are performing a regular backup of the CCS ADAM and SQL databases. See "Backing up the CCS ADAM and SQL databases" on page 324.

To consolidating the CCS Directory Server and CCS Application Server and migrate to other platforms

1. Install CCS 10.5.1 on a new computer. See "Creating a new CCS setup" on page 323.

   For information on installing CCS 10.5.1, see the *Symantec Control Compliance 10.5 Installation Guide*.
2. Upgrade CCS 10.5.1 to CCS 11.1.
3. Restore the Application Server my restoring the CCS ADAM and SQL databases. See "Restoring the CCS ADAM and SQL databases" on page 325.

Migrating CCS 11.1 installation to a new computer

You can migrate your existing CCS 11.1 setup to a new computer.

Perform the following procedure to migrate your existing CCS 11.1 setup to a new computer.

It is assumed that you are performing a regular backup of the CCS ADAM and SQL databases, and the ESM components, if you are using ESM for data collection.

See “Backing up the CCS ADAM and SQL databases” on page 324.

See “Backing up the ESM components” on page 328.

To migrate your existing CCS 11.1 setup to a new computer

1. Install CCS 11.1 on a new computer. See “Creating a new CCS setup” on page 323.
2. Restore the Application Server my restoring the CCS ADAM and SQL databases. See “Restoring the CCS ADAM and SQL databases” on page 325.
3. If you are using an ESM Manager and ESM Agent to collect asset data from your network, restore the ESM components. See “Restoring the ESM components” on page 328.

Migrating CCS 11.1 installation to a new domain

You can migrate your existing CCS 11.1 setup to a new domain.

Perform the following procedure to migrate your existing CCS 11.1 setup to a new computer.

To migrate your existing CCS 11.1 setup to a new computer

Let us assume that you want to migrate CCS 11.1 from domain A to domain B.

1. Install CCS 11.1 on a new computer in domain B. See “Creating a new CCS setup” on page 323.
2. Ensure domain A and domain B have trust relationship.
3. Add the Application Server service account of your existing CCS 11.1 setup in domain A, to the CCS setup in domain B. You can add the user account through the CCS console of the CCS setup in domain B. For information on adding a user account, see the *Symantec Control Compliance Suite User Guide*.
4. Backup the CCS ADAM and SQL databases of the CCS setup in domain A. See “Backing up the CCS ADAM and SQL databases” on page 324.
5. Restore the CCS ADAM and SQL databases to the CCS setup in domain B. See “Restoring the CCS ADAM and SQL databases” on page 325.

Changing the domain of an existing CCS 11.1 installation

You can change the domain of the existing CCS 11.1 installation.

Perform the following procedure to change the domain of the existing CCS 11.1 installation.

It is assumed that you are performing a regular backup of the CCS ADAM and SQL databases.

See "Backing up the CCS ADAM and SQL databases" on page 324.

To change the domain of the existing CCS 11.1 installation

Let us assume that you want to change the domain of an existing CCS 11.1 installation from domain A to domain B.

1. Install CCS 11.1 on a computer in domain A. See "Creating a new CCS setup" on page 323.
2. Ensure domain A and domain B have trust relationship.
3. Create a new Application Server service account in domain B.
4. Add the newly created Application Server service account to the following groups in your existing CCS 11.1 setup in domain A:
   - Local Administrator on your local computer
   - SQL Server with Sysadmin server role.
   - CCS Administrator role in the CCS Console
5. Run the Symantec.CSM.ConfigureServiceAccount.exe located at <install_directory>/CCS/Reporting and Analytics/Application Server/ to set the service accounts and database connections to domain B. Set the Application Server service credentials first by specifying the database locations. Then re-run Symantec.CSM.ConfigureServiceAccount.exe to set the Encryption Management Server service credentials.
6. In the Microsoft Management Console (MMC), change the account context of all CCS Services to the new Application Server service account in domain B.
7. Change the domain of the CCS computer from domain A to domain B.
8. Login to CCS using the domain B Application Server service account.
9. Change the FQDN values of following configuration files to new values. For example, for domain A to domain B, change Host_Name.A.Com to Host_Name.B.Com.

   Directory Support Service:

   - ...\Symantec\CCS\Reporting and Analytics\Directory Support Service\Symantec.CSM.DSS.Service.exe.Config

     ```
     Value = <add key="AdamHost" value="Host_Name.B.Com:3890" />
     ```

   - ...\Symantec\CCS\Reporting and Analytics\EncryptionManagementService\Symantec.CSM.EncryptionManagement.Service.exe.Config

     ```
     Value = <add key="AdamHost" value="Host_Name.B.Com:3890" />
     ```

Application Server:

- ...\Symantec\CCS\Reporting and Analytics\Application Server\AppserverService.exe.Config

  ```
  Value = <add key="AppServerAdam" value="Host_Name.B.Com:3890"
  />
  ```

Click Once Console:

- ...\Symantec\CCS\Reporting and Analytics\Application Server\AppserverService.exe.Config

  ```
  Value = <add key="ADAMServer" value="Host_Name.B.Com" />
  ```

Web Console:

- In the IIS Manager, change all CCS Application pool user context to the new Application Server service account in domain B.

Registry Keys:

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Symantec\CCS\Installs\ADAM for PCU upgrade

  ```
  Value = MachineName
  ```

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Symantec\Symhelp

  ```
  Value = SymhelpUrl
  ```

10 On the command prompt, run the following command to export the CCS configuration using the CCSUtil.exe located at <install_directory>/CCS/Reporting and Analytics/Directory Support Service/:

```
CCSUtil.Exe export /configfile=alloriginal.xml /save
/server=DSS_Server_Name:3890
```

In the exported file, change Host_Name.A.Com to Host_Name.B.Com.

Run the following command to import the CCS configuration using the CCSUtil.exe:

```
CCSUtil.Exe import /configfile=alloriginal.xml /save
/server=DSS_Server_Name:3890
```

11 Restart all CCS Services.

12 Install and launch the CCS Console.

Backing up and restoring CCS components

As part of your disaster recovery procedures, you must backup the following CCS components at regular intervals in case you need to recover from a component failure in the future:

- The CCS ADAM and SQL Databases.
  See “Backing up the CCS ADAM and SQL databases” on page 324.
- CCS System General Settings.
  See “Backing up CCS System General Settings” on page 325.
- If you are using ESM for data collection, backup the ESM components.
  See “Backing up the ESM components” on page 328.

You can restore the following CCS components in case of a failure.

- The CCS ADAM and SQL Databases, and the CCS configuration files.
  See “Restoring the CCS ADAM and SQL databases” on page 325.
- CCS System General Settings.
  See “Restoring CCS System General Settings” on page 328.
- If you are using ESM for data collection, restore the ESM components.
  See “Restoring the ESM components” on page 328.

Information required for restoring a CCS setup

As part of your disaster recovery procedures, you must note down the following information about your existing CCS setup. In case of a disaster, you require this information to create a new CCS setup which is similar to your existing CCS setup.

As part of your backup strategy, record the following information:

- Root Certificate Signature Algorithm and Key Size
- Root certificate password
- Encryption Management Service Pass Phrase
- CCS Application Server Pass Phrase
- The service account the Directory Service uses
- The service account the Application Server uses

Creating a new CCS setup

In case of a disaster, you may require to create a new CCS setup and then restore the backed up databases to the new setup. Perform the following procedure to create a new CCS setup. While creating a new CCS setup, you must provide the same information for the following items as was used in your existing setup.

- Root Certificate Signature Algorithm and Key Size
- Root certificate password
- Encryption Management Service Pass Phrase

- CCS Application Server Pass Phrase
- The service account the Directory Service uses
- The service account the Application Server uses

See "Disaster Recovery and Migration scenarios" on page 317.

To create a new CCS setup

1. Install the CCS Suite using the same configuration information as was used in your existing CCS setup. The CCS Suite contains the CCS Application Server.
2. On the command prompt, run the following command to export the CCS configuration using the `CCSUtil.exe` located at <install_directory>/CCS/Reporting and Analytics/Directory Support Service/.

   ```
   CCSUtil.exe export /configfile=alloriginal.xml /save
   /server=DSS_Server_Name:3890
   ```

Backing up the CCS ADAM and SQL databases

You must backup the CCS ADAM and SQL databases at regular intervals in case you need to recover from an Application Server failure in the future. Perform the following procedure to back up the CCS ADAM and SQL databases.

To back up the CCS ADAM and SQL databases

If you are using CCS 11.1 perform the following procedure on the CCS Application Server. If you are using any previous CCS version, perform the following procedure on the CCS Directory Server.

1. Stop all the Symantec CCS services.
2. Create a folder to copy the ADAM database backup files. For example, C:\ADAM_backup
3. On the command prompt, go to C:\windows\ADAM\
4. Run the `DsdbUtil.exe` file.
5. At the `dsdbutil.exe:` prompt, type **files**
6. At the `file maintenance:` prompt, type **compact to <foldername>**, where **foldername** is the folder you created to copy the ADAM database.

   For example, **compact to C:\ADAM_backup**

   The ADAM database is backed up and the file `adamntds.dit` is created in the you created to copy the ADAM database.

7 Using the SQL Server Management Studio, take the CCS SQL Server databases offline.

8 Backup the following SQL Server database files and restart all the Symantec CCS services.

Table B-3 CCS SQL databases that you must backup

Database	SQL Server Name	Filenames
Production database	CSM_DB	`CSM_DB.mdf` `CSM_DB.ldf`
Reporting database	CSM_Reports	`CSM_Reports.mdf` `CSM_Reports.ldf`
Evidence database **Note:** Backup the evidence database only if you want to restore databases prior to CCS 10.5.1.	CSM_EvidenceDB	`CSM_EvidenceDB.mdf` `CSM_EvidenceDB.ldf`

Backing up CCS System General Settings

In case of any failure, you can restore the CCS System General Settings from the backup.

To back up the CCS System General Settings

1 Close all CCS Consoles and stop the Symantec Application Server Service.

2 On the command prompt, run the following command to export the CCS System General Settings using the `CCSUtil.exe` located at <install_directory>/CCS/Reporting and Analytics/Directory Support Service/.

```
ccsutil.exe /Export /GeneralSettings /Server=DSS_Server_Name:3890
/ConfigFile=GSConfiginfo.xml /Save
```

3 The GSConfig.xml is created in the working directory. Copy the file to the location where the other CCS Backup files are saved.

4 Start the Symantec Application Server Service.

Restoring the CCS ADAM and SQL databases

You can restore the CCS ADAM and SQL databases on the new setup that you have created for restoring CCS. Perform the following procedure to restore the CCS ADAM and SQL databases on the new CCS setup.

See the following section before restoring the CCS ADAM and SQL databases:

See "Backing up the CCS ADAM and SQL databases" on page 324.

To restore the CCS ADAM and SQL databases on the new CCS setup

If you are using CCS 11.1 perform the following procedure on the CCS Application Server. If you are using any previous CCS version, perform the following procedure on the CCS Directory Server.

1. Stop all CCS services.
2. Relocate the existing ADAM database and copy the ADAM database backup file `adamntds.dit` at the location C:\Program Files\Microsoft ADAM\SymantecCCS\data\.
3. Relocate the old log files at the location C:\Program Files\Microsoft ADAM\SymantecCCS\logs\

   The relocated database files can be used to restore the new system to a new state if the disaster recovery procedure fails.
4. Start SymantecCCS Service.

Note: On a Windows Server 2008 computer, you may get the following error while starting the SymantecCCS service:

```
Windows could not start the SymantecCCS service on local computer.
0xc0000001; 0xc0000001
```

If you encounter such error, remove the following registry entry and restart the SymantecCCS service.

```
HKLM\System\CurrentControlSet\Services\ADAM_SymantecCCS\Parameters\DSA
Database Epoch
```

Note: If the SymantecCCS service fails to start after deleting the log files in step 3, go to C:\windows\ADAM\ and run the `DsdbUtil.exe` file to perform the integrity check.

At the `dsdbutil.exe:` prompt, type **files** and

At the `file maintenance:` prompt, type **Integrity**.

---

5 On the command prompt, run the following command to import the CCS configuration using the `CCSUtil.exe` located at <install_directory>/CCS/Reporting and Analytics/Directory Support Service/.

```
CCSUtil.exe import /configfile=alloriginal.xml /save
/server=DSS_Server_Name:3890
```

6 Run the `Symantec.CSM.ConfigureServiceAccount.exe` located at <install_directory>/CCS/Reporting and Analytics/Application Server/ to set the service accounts and database connections.

7 On the SQL Server Management Studio, detach the CCS SQL Server databases.

8 Relocate the existing CCS databases and copy the backed up SQL Server databases.

The relocated database files can be used to restore the new system to a new state if the disaster recovery procedure fails.

9 Attach the backed up SQL Server databases in the SQL Server Management Studio.

10 Activate SQL Broker.

Note: Evaluation synchronization and default global synchronization fails if you do not activate the SQL Broker.

Run the following command on the SQL Server to check the SQL Broker status: `select is_broker_enabled from sys.databases where name = 'CSM_Reports'`.

Run the following command to activate the SQL Broker: `exec spManageUDMSQLBroker 1, 'dbo', 'CSM_Reports', 1`.

If you have moved the database to another computer, run the following command to set the authorization to CSM_Reports database: `ALTER AUTHORIZATION ON DATABASE::CSM_Reports TO sa ALTER DATABASE CSM_Reports SET ENABLE_BROKER with rollback immediate`.

---

11 Restart all the remaining CCS services.

12 Launch the CCS Console.

13 Go to **Settings > Secure Configuration** and verify the CCS Application Server credentials and database connections.

14 Verify that migrated asset structure, assets, collections, evaluations and reports are displayed in the CCS Console.

15 Verify that all user defined jobs are functional.

Restoring CCS System General Settings

You can restore the CCS System General Settings on the new setup that you have created for restoring CCS. Perform the following procedure to restore the System General Settings on the new CCS setup.

To restore the CCS System General Settings

1 Close all the CCS Consoles and stop the Symantec Application Server Service

2 On the command prompt, run the following command to register the CCS System General Settings using the `CCSUtil.exe` located at <install_directory>/CCS/Reporting and Analytics/Directory Support Service/.

```
CCSUtil.exe Register /File=GSConfiginfo.xml /save /Force=True
```

3 Start the Symantec Application Server Service.

Backing up the ESM components

If you are using an ESM Manager and ESM Agent to collect asset data from your network, you can backup and restore the ESM Manager and Agent. You must backup the ESM components at regular intervals in case you need to recover the components from a failure in the future. Perform the following procedure to back up the ESM components.

To back up the ESM components

1 Export all agents list in 9.0 format from the ESM Manager, using the **Export Agent List** option in the ESM Console.

2 On the CCS Manager, stop the following ESM services.

- Enterprise Security Manager
- Enterprise Security Agent

3 Back up the <install_directory>/CCS/Reporting and Analytics/ESM folder.

Restoring the ESM components

If you are using an ESM Manager and ESM Agent to collect asset data from your network, you can backup and restore the ESM Manager and Agent. Perform the following procedure to restore the ESM components.

See the following section before restoring the ESM components:

See "Backing up the ESM components" on page 328.

To restore the ESM components

1. Install the CCS Manager.
2. On the CCS Manager, stop the following ESM services.
   - Enterprise Security Manager
   - Enterprise Security Agent
3. Restore the ESM folder that you have backed up. Ensure that you do not overwrite the files: `agent.dat`, `agtcert.dat` and `agtdesc.dat`.

   Note: If you have changed the computer name while installing the new CCS Manager, rename the folder of the host located at <install_directory>/CCS/Reporting and Analytics/ESM/system/ to match the computer name of the new CCS Manager.

4. Start the following services.
   - Enterprise Security Manager
   - Enterprise Security Agent
5. On the ESM Console, use the Agent Recovery Registration option to import the agent list that you exported during the ESM components backup.
6. If you are collecting raw-data using the agent based method, you must re-register all CCS Agents to establish communication with the CCS Managers.
7. If you are collecting message based data, you must the update the new CCS Manager name and IP address in the agent.agent table in production database CSM_DB.

   You can use the following SQL script to update the agent.agent table:

```
UPDATE agent.agent

SET managerName = 'New_Manager_Name', managerfqdn = '
New_Manager_Name.Domain.Com', ManagerIPAddresses = '
New_Manager_IP address'

WHERE managerName = ' Old_Manager_Name ' OR managerfqdn =
'Old_Manager_Name.Domain.Com' OR ManagerIPAddresses = '
Old_Manager_IP address ';
```

Appendix C

Troubleshooting

This appendix includes the following topics:

Deployment troubleshooting

CCS 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

The following table lists possible deployment problems and their associated causes and resolutions.

Table C-1 Deployment troubleshooting

Problem	Cause	Resolution
Installer displays the `Copying CR 2010 LA fix file` warning	The Crystal Reports 2010 hot fix is installed automatically during the CCS installation. If the hot fix fails to install automatically, the following warning message is displayed in the **Warning** panel of the CCS installer. `Copying CR 2010 LA fix file.`	To install the hot fix manually on Windows Server x64, extract the `secSSOwin64_x64` file located in the `Redist` folder of the product media, to the location C:\Program Files (x86)\SAP BusinessObjects\Crystal Reports for .NET Framework 4.0\Common\SAP BusinessObjects Enterprise XI 4.0\win64_x64\. Extract the `secSSOwin32_x86` file located in the `Redist` folder of the product media, to the location C:\Program Files (x86)\SAP BusinessObjects\Crystal Reports for .NET Framework 4.0\Common\SAP BusinessObjects Enterprise XI 4.0\win32_x86\. To install the hot fix manually on Windows Server x86, extract the `secSSOwin32_x86` file located in the `Redist` folder of the product media, to the location C:\Program Files (x86)\SAP BusinessObjects\Crystal Reports for .NET Framework 4.0\Common\SAP BusinessObjects Enterprise XI 4.0\win32_x86\.
Installer displays the `Create Connector tables in the production database` warning during upgrade	If you are upgrading to CCS 11.1 from a previous version of CCS and the installer displays critical errors. When you rectify the errors and you relaunch the installer to upgrade again, the **Warning** panel of the CCS installer displays the following warning messages `Create Connector tables in the production database`	Ignore the warning message.

Table C-1 Deployment troubleshooting *(continued)*

Problem	Cause	Resolution
Installer does not launch the Migration utility after upgrade	If you are upgrading from CCS 10.0 to CCS 11.1 and the installer displays critical errors. When you rectify the errors and you relaunch the installer to upgrade again, the installer does not launch the Migration utility after upgrade.	Migrate the CCS databases using the `MigrationUtility.exe` located in the <installation directory>/Symantec/CCS/Reporting and Analytics folder of the installed product.
Installer displays critical errors during fresh installation	Installer displays critical errors while installing CCS for the first time.	Uninstall the product, rectify the errors and then reinstall the product by performing the following steps: ■ Launch the CCS setup. ■ The installation wizard detects a previous installation of CCS installed on the computer, and displays the **Maintenance** panel. Use the **Uninstall** option to uninstall the product. ■ Rectify the errors. ■ Relaunch the setup to install the product again.
Failed Application Server Installation	The domain account credentials that are used for the component are not valid.	Supply valid credentials.
	The `c:\Windows` folder does not allow software to be installed.	Specify a different location to install the product.
	The `C:\Program Files` folder on the Application Server host is compressed.	Uncompress the `C:\Program Files` folder on the Application Server host. Reinstall the Application Server instance.
Certificate does not match specified computer	The ping utility has different results for the target computer when run from the Application 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.

Table C-1 Deployment troubleshooting *(continued)*

Problem	Cause	Resolution
Application Server or CCS manager fail to start	Host computer does not have Internet connectivity or connection to the VeriSign Web server is blocked.	Provide access to the VeriSign Web server the first time the service starts. You can also disable certificate checking for all components on the host. Finally, you can manually download the Certificate Revocation List from VeriSign and install it on the host.
Unable to start 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 Application Server.
	The Certificate Management Console fails to start.	Verify that the user is an administrator of the Application Server. Verify that the user is a CCS Administrator.
Synchronization jobs fail to complete after migration	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.