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 website 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 Introducing Symantec Data Center Security: Server Advanced ................................................................. 11
   About Symantec Data Center Security: Server Advanced .......... 11
      How Symantec Data Center Security: Server Advanced works ........................................................................ 13
   About Symantec Data Center Security: Server Advanced features ..................................................................... 14
   About the DCS:SA infrastructure ..................................................... 16
   About building DCS:SA testbed ....................................................... 23
   About database scalability .............................................................. 24

Chapter 2 Planning the Installation for DCS:SA .......................................................... 27
   About installation of DCS:SA .......................................................... 27
   System requirements for DCS:SA .................................................... 28
      Software requirements ............................................................ 28
      Operating system requirements ................................................. 29
      Hardware requirements ........................................................... 30
   About using firewalls with DCS:SA ................................................... 31
   Disabling Windows XP firewalls .................................................... 33
      Disabling Internet Connection Firewall ........................................ 33
      Disabling Windows Firewall ...................................................... 33
   About name resolution .................................................................. 34
   About IP routing ........................................................................... 34
   About intrusion prevention .......................................................... 34
   About simple failover .................................................................... 35
      How simple failover works ........................................................ 35
      About the fail back interval ...................................................... 36
   About the management server list for an agent ................................ 37
   Specifying the management server list for an agent .................... 37
   Installation log files ....................................................................... 40
   About server telemetry ................................................................. 41
   What to do after installation .......................................................... 41
## Chapter 3 Planning the Installation for DCS:S

- About installing DCS:S ................................................................. 124
- How DCS:S works ...................................................................... 43
- System requirements for DCS:S .................................................. 44
- Setting up the VMware environment ........................................ 45

## Chapter 4 Planning the Deployment Architecture and Rollout

- About network architecture and policy distribution .................. 47
- Planning for enterprise deployment .......................................... 48
- About scaling ........................................................................... 51
- Key database server installation considerations ....................... 52
- Agent installation considerations for key features .................. 52
  - About enabling intrusion prevention .................................... 53
  - About enabling the real-time file integrity monitoring feature in intrusion detection ........................................................ 55
  - About creating agent registration groups ............................... 56
- About automating agent installations ........................................ 56
- Best practice for agent installation .......................................... 56
- About development, test, and production instances ................... 57
- About the incremental rollout of agent installations and policy deployment ................................................................. 58

## Chapter 5 Installing DCS:SA

- Installing Symantec Data Center Security: Server Advanced components on Windows ................................................. 60
- About the Windows installation ................................................ 60
- About installing a database linked to a SQL Server instance ..... 62
- Configuring the temp environment variable ............................ 63
- Installing the management server .......................................... 64
- Installing and configuring the Java console ............................ 78
- Installing a Windows agent ....................................................... 82
- Silent installation of agent ....................................................... 90
- Uninstalling DCS:SA ................................................................. 97
- Temporarily disabling Windows agents ................................ 100
- Reinstalling Windows agents .................................................. 101

- Installing Symantec Data Center Security: Server Advanced components on UNIX ......................................................... 102
- About installing UNIX agents ................................................ 102
- Installing an agent in verbose mode ....................................... 107
- Installing an agent in silent mode .......................................... 108
Uninstalling agents using package commands ........................................ 113
Disabling and enabling UNIX agents ...................................................... 114
Monitoring and restarting UNIX agents ................................................ 121
Troubleshooting agent issues ............................................................... 122
Integrating with data center orchestration tools .................................. 122

Chapter 6 Installing DCS:S ................................................................. 124

About installing DCS:S ....................................................................... 124
About installing a database linked to a SQL Server instance .................. 125
About Unified Management Console .................................................. 126
Deploying the Unified Management Console (UMC) ............................ 126
Installing the management server ....................................................... 129
Deploying Operations Director virtual appliance on VMware infrastructure ....................................................... 131
Installing the UMC root certificate on a browser .................................. 132
Enabling CORS .................................................................................. 136
Creating new certificates for DCS:S .................................................... 137
Deploying a Security Virtual Appliance ................................................. 139
Registering Data Center Protection Service with VMware NSX Manager ................................................................................. 140
Deploying Datacenter Protection Service ............................................. 141
Upgrading Datacenter Protection Service .......................................... 142
Uploading and registering the Security Virtual Appliance ................. 143
Unregistering the Security Virtual Appliance with NSX ..................... 143

Chapter 7 Registering DCS:S and Operations Director with UMC ............ 146

Registering DCS:S and Operations Director with UMC ....................... 146
Registering DCS:S with UMC ............................................................... 148
Registering Operations Director with UMC .......................................... 150
Operations Director fails to register with UMC ................................... 151

Chapter 8 Configuring a Data Center Security Product with UMC ........... 153

Using Unified Management Console .................................................. 154
Configuring an Active Directory ......................................................... 155
About User Management ..................................................................... 157
Assigning roles to users and user groups ............................................ 158
Configuring components required for Operations Director ............... 160
Configuring DCS:S and UMC with FQDN .......................................... 161
About the Home Page in the DCS:S view ......................................... 161
Introducing Symantec Data Center Security: Server Advanced

This chapter includes the following topics:

- About Symantec Data Center Security: Server Advanced
- About the DCS:SA infrastructure
- About building DCS:SA testbed
- About database scalability

About Symantec Data Center Security: Server Advanced

Symantec Data Center Security: Server Advanced (DCS:SA) provides a policy-based approach to endpoint security and compliance. The intrusion prevention and detection features of DCS:SA operate across a broad range of platforms and applications. It provides:

- A policy-based host security agent for monitoring and protection.
- Proactive attack prevention using the least privilege containment approach.
- A centralized management environment for enterprise systems that contain Windows, UNIX, and Linux computers.
Table 1-1  DCS:SA capabilities

<table>
<thead>
<tr>
<th>Security and protection</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>■ Real-time proactive enforcement</td>
<td>■ Real-time monitoring and auditing</td>
</tr>
<tr>
<td>■ Intrusion and malware prevention</td>
<td>■ Host intrusion detection</td>
</tr>
<tr>
<td>■ System hardening</td>
<td>■ File integrity monitoring</td>
</tr>
<tr>
<td>■ Application control</td>
<td>■ Configuration monitoring</td>
</tr>
<tr>
<td>■ Privileged user access control</td>
<td>■ Tracking and monitoring of user access</td>
</tr>
<tr>
<td>■ Vulnerability and patch mitigation</td>
<td>■ Logging and event reporting</td>
</tr>
<tr>
<td>■ Does not use signatures or require continual updates to content</td>
<td></td>
</tr>
</tbody>
</table>

The major features of DCS:SA are as follows:

■ Intrusion detection facility for compliance auditing
  ■ Real-time file integrity monitoring
  ■ Granular change detection of registry values, file contents, and attributes
  ■ Operating system and application log monitoring
  ■ Local event correlation and smart response actions

■ Intrusion Prevention facility for malware prevention and system lockdown
  ■ Sandbox containment of operating system and application processes by an in-kernel reference monitor
  ■ Granular access control of network, file systems, registry, process-to-process memory access, system calls, and application and child process launches
  ■ Privileged user and program behavior

■ Anti-malware security
DCS:SA Security Virtual Appliance (SVA) provides agentless anti-malware security services for the virtualized network through integration with the VMware Network and Security Virtualization (NSX) platform. SVA provides two types of policies: Antivirus policies, and configuration policies.

■ Comprehensive out-of-the-box policies for complete system monitoring and protection of physical and virtual systems

■ Security orchestration using Operations Director. Operations Director is intended to:
  ■ Automate security provisioning workflow.
  ■ Provide application-centric security service.
  ■ Seamlessly integrate with VMware NSX.
- Provide out-of-box security product integration.
- Centralized management environment for administering agents, policies, and events
- Integration with Security Information and Event Management (SIEM) and other security tools, as well as enterprise infrastructure components such as Active Directory, SMTP, and SNMP
- Broad platform support across Windows, Linux, UNIX and virtual environments for critical servers, workstations, laptops, and standalone systems

The major benefits of DCS:SA are as follows:

- Reduces emergency patching and minimizes patch-related downtime and IT expenses through proactive protection that does not require continuous updates.
- Reduces incidents and remediation costs with continuous security. Once the agent has a policy, it enforces the policy even when the computer is not connected to the corporate network. And even if a computer is unable to obtain the latest patches in a timely fashion, DCS:SA continues to block attacks so that the computer is always protected.
- Provides visibility and control over the security posture of business-critical enterprise assets.
- Uses predefined compliance and hardening policies to provide efficient security management, reporting, alerting, and auditing of activities. Also provides compensating controls for compliance failures.

How Symantec Data Center Security: Server Advanced works

Symantec Data Center Security: Server Advanced controls and monitors what programs and users can do to computers. Agent software at the endpoints controls and monitors behavior based on policy.

The DCS:SA policy library contains prevention and detection policies that you can use and customize to protect your network and endpoints, as follows:

- A prevention policy is a collection of rules that governs how processes and users access resources.
  For example, prevention policies can contain a list of files and registry keys that no program or user can access. Prevention policies can contain a list of UDP and TCP ports that permit and deny traffic. Prevention policies can deny access to startup folders. Prevention policies define the actions to take when unacceptable behavior occurs.
- A detection policy is a collection of rules that are configured to detect specific events. An agent can enforce one or more detection policies simultaneously.
For example, detection policies can be configured to generate events when files and registry keys are deleted; when known, vulnerable CGI scripts are run on Microsoft Internet Information Server (IIS); when USB devices are inserted and removed from computers; and when network shares are created and deleted.

You use the Java console to manage agent policies, and customize how agents communicate with the management server.

Agents report events to the management server for storage and are viewed in the Java console. Agent log rules control the events that are logged for that agent. Logged data includes event date and time, event type, importance rating, and any prevention action performed.

DCS:SA includes queries and reports with charts, graphs, and tables that provide detailed and aggregated summary data about events, agents, and policies. You can also create your own queries and reports.

Transport Layer Security using X.509 certificates secures communication between the Java console and the management server, and between the agent and the management server.

About Symantec Data Center Security: Server Advanced features

Key features of Symantec Data Center Security: Server Advanced are as follows:

- **Computer security**: Offers a flexible computer security solution that includes the following features:
  - Day-zero protection: stop malicious exploitation of systems and applications; prevent introduction and spread of malicious code
  - Hardened systems: lock down OS, applications, and databases; prevent unauthorized executables from being introduced or run
  - Integrated firewall blocks inbound and outbound TCP/UDP traffic; administrator can block traffic per port, per protocol, per IP address or range
  - Maintain compliance by enforcing security policies on clients and servers
  - Buffer overflow protection
Out-of-the-box security policies offer the following features:

- Intrusion prevention
  - Proactive security against day-zero attacks
  - Protection against buffer over-flow and memory-based attacks
  - Out-of-the-box operating system hardening
  - External device protection
  - Administrative privilege de-escalation

- Intrusion detection
  - Sophisticated policy-based auditing and monitoring
  - Log consolidation for easy search, archival, and retrieval
  - Advanced event analysis and response capabilities
  - File and registry protection and monitoring

- Policies configured with easy enable/disable style options
- Includes application policies for popular Microsoft® interactive applications

Java console

Java console that lets administrators create and deploy policies, manage users and roles, view alerts, and run reports.

Features include the following:

- Configure agent properties to determine how agents communicate with the management server and which events agents send to the management server
- Customize policy options to increase or decrease restrictions enforced by a policy
- Import and export custom and third-party policies

Agent

Agents enforce policy on the endpoint. Features include the following:

- Control behavior by detecting and preventing specific actions that an application or user might take
- Configure polling interval, real-time notification, log consolidation, log rotation
- Apply policies to agents and groups agents
- Load policies without reboot

Management server

Provides secure communication to and from agents and the Java console.

Features include the following:

- Agents automatically register with the management server during installation
- Sends configuration changes to agents
- Real-time and bulk logging of agent events
Platform support

Symantec Data Center Security: Server Advanced offers broad platform support for the following operating systems:

- Ubuntu
- Microsoft Windows
- Sun™ Solaris™
- Red Hat® Enterprise Linux
- CentOS Linux
- Oracle Linux
- SUSE® Enterprise Linux
- IBM® AIX®
- Hewlett-Packard® HP-UX®

See the Symantec Data Center Security: Server Advanced Platform and Feature Matrix to determine the specific operating system versions supported and the specific agent features for each operating system version.

About the DCS:SA infrastructure

DCS:SA includes the following components:

- The Java console and the server components
- The agent components that provide intrusion prevention and detection on physical or virtual computers
- The Security Virtual Appliance (SVA) that provides agentless anti-malware protection for VMware guest VMs running Windows

The management server and the Java console run on Windows operating systems. The agents run on Windows and UNIX operating systems. The SVA is deployed into VMWare NSX by using the DCS:SA Java console.

The management components of DCS:SA can be installed on one system or in a distributed model. Agents are generally deployed to every supported host to be monitored and protected, including the management server, the Java console, and the SQL server database. Remote monitoring can extend file integrity monitoring and log monitoring functionality to systems where no native agent exists. For example, such systems include mainframe zLinux, AS 400, VAX, or VMS systems. The DCS:SA Java console is available in both a Web browser or as a standalone thick client.

The following diagram displays the DCS:SA environment setup:
Figure 1-1 DCS:SA environment setup

Introducing Symantec Data Center Security: Server Advanced

About the DCS:SA infrastructure
### Table 1-2

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Virtual Appliance (SVA)</td>
<td>The SVA provides agentless anti-malware security services for VMware guest virtual machines. The SVA is deployed as the Datacenter Protection Service from the vSphere web client, after registering the service with the NSX Manager. DCS:SA SVA’s reputation based exoneration capabilities minimizes the convictions of false positives. For information on deploying and using the SVA see the <em>Symantec Data Center Security: Server Advanced Implementation Guide Integration with VMware NSX</em>. The SVA is a closed system that should not require access under normal use by users. If you are encountering a problem with the SVA, contact Symantec Technical Support for guidance and instructions on the appropriate next steps.</td>
</tr>
<tr>
<td>DCS:SA agent for behavior control</td>
<td>The DCS:SA agent for behavior control provides the following capabilities: - Intercepts the system calls to enforce prevention policies - Contains multiple detection sensors for monitoring system change events and log files - Contains the tools for configuration and diagnostic support - Downloads the policies and settings from the management server and uploads events and status information to the management server - Natively supports a wide variety of Windows, UNIX and Linux servers and workstations - Supported on VMware guest systems for detection and prevention with any of the operating systems that are natively supported - Can be used to remotely monitor another host without a native agent, but note that only detection features are available in this mode See the <em>Symantec Data Center Security: Server Advanced Platform and Feature Matrix</em> for more information on the supported operating systems, and agent features supported on each operating system.</td>
</tr>
</tbody>
</table>
### Table 1-2  Key components of DCS:SA (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| Management server| The management server is based on Tomcat Application Server software. The management server provides the following capabilities:  
■ Secure communications with agent and console  
■ Bulk event file storage management for efficient archival storage of all logged events  
■ Store policies in a central location and provides an integrated, scalable, flexible, agent, and policy management infrastructure.  
■ Alert processing (SMTP, SNMP, file), data purging, and other management functions  
■ Coordinate policy distribution, and manages agent event logging and reporting.  
The management server supports high availability and scalability. |
| Java console     | The Java console provides the following capabilities:  
■ Policy, agent, and event management  
■ Real-time event monitoring from the dashboard  
■ Flexible hierarchy and agent grouping support  
■ Event Wizard for quick policy adjustment  
■ Querying, reporting, alerting  
■ User and role management  
■ Auditing console actions and server events  
The Java console is a rich client user interface which is also available in a Web browser version |
### Key components of DCS:SA (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operations Director</td>
<td>Operations Director lets you:</td>
</tr>
</tbody>
</table>
|                                    | **Automate security provisioning workflow**  
  Security provisioning workflow gets triggered directly from vCenter upon creation of new virtual application. Operations Director also automates the collaboration between the virtual infrastructure administrator and security administrator to reduce security provisioning time to minutes.                                                                                                                                       |
|                                    | **Provide application-centric security service**  
  Instantly assesses application security requirements during vApp/VM provisioning by using security tags. An intelligent rule engine identifies the appropriate security policies. Operations Director also provides out-of-box tags and security policy mapping.                                                                                                     |
|                                    | **Seamlessly integrate with VMware NSX**  
  Leverages NSX platform and NSX compatible security services to create application specific security groups and policies.                                                                                                                                                                                                                           |
|                                    | **Provide out-of-box security product integration**  
  Applies antimalware controls by using Symantec Data Center Security: Server, server hardening controls by using Symantec Data Center Security: Server Advanced, and automates application firewall rules by using Palo Alto Networks Next Generation Firewall.                                                                                                                                  |
| Unified Management Console         | The Unified Management Console (UMC) is an appliance that provides a web-based console to register, configure, and manage various features and products in Symantec Data Center Security: Server.                                                                                                                                                           |
| Database                           | The database provides the following capabilities:                                                                                                                                                                                                                                                                                           |
|                                    | **Accessible through JDBC/ODBC**  
  Stores the policies, agent information, and real-time actionable events  
  Lets you configure encrypted communications between the database and the management server                                                                                                                                                                                                                       |
| Predefined Detection and Prevention policies | The predefined Detection and Prevention policies provide the following capabilities:                                                                                                                                                                                                                                                             |
|                                    | **Best practice policy content for operating system protection of Windows, Linux, and UNIX.**  
  **Common use case templates for creating customer-specific rules**  
  **Easy policy configuration interface**  
  **Flexible administration of the policies that are applied to agents**                                                                                                                                       |
**Table 1-2** Key components of DCS:SA *(continued)*

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Predefined Anti-malware policies</td>
<td>DCS:SA SVA provides out-of-the-box anti-malware policies to protect your virtual environment against malware. SVA provides three types of policies as follows:</td>
</tr>
<tr>
<td></td>
<td>■ Network security policies are used for specifying settings to monitor Network traffic. You can configure these policies to detect, log, and block the network threats.</td>
</tr>
<tr>
<td></td>
<td>■ Antivirus policies are the policies that provide basic level and advanced level protection from malware. For example, antivirus policies can be configured to provide protection to the guest virtual machines from malicious virus attacks.</td>
</tr>
<tr>
<td></td>
<td>■ Configuration policies are predefined configuration settings that are applicable to the SVA. For example, configuration policies define the behavior of a SVA and can generate events if any changes are made to the configuration settings of a SVA and its services, and when the settings of scheduled scans and LiveUpdate server are changed.</td>
</tr>
</tbody>
</table>

Key points to remember about the ports and the communication flow in DCS:SA are as follows:

- DCS:SA requires very few ports.
- All ports are configurable.
- Agents can communicate readily within a network address translation environment. A network address translation environment initiates connections to the management server to transmit events and download policy updates or configuration updates.
When you deploy DCS:SA in your environment, you must ensure that the proper communications and connectivity are available for the following components:

- Console to server
- Server to database
- Agents to server
- Security Virtual Appliance (SVA) to server

Agents continue to monitor and enforce security even if network outages occur between the agents and the server environment. In fact, you can also configure the agent to operate in a standalone or an unmanaged mode.

If network outage occurs between the SVA and the NSX Manager, SVA uses the default policies to continue monitoring and enforcing anti-malware security on the guest virtual machines.

You can deploy DCS:SA components on physical systems and in virtualized environments. A virtualized ecosystem such as the one supported by VMware has many parts. Its parts include management infrastructure, virtual guest machines, and hypervisors that span a variety of operating systems. To protect this heterogeneous environment, DCS:SA relies on specific policies and enforcement agents that are appropriate to each component to be secured. The components include ESX, ESXi, and vCenter.

For more information about DCS:SA, refer to the Symantec™ Data Center Security: Server Advanced Overview Guide.
About building DCS:SA testbed

You can quickly set up a demonstration environment that contains all of the DCS:SA components on one computer. These components include the management server, the database, the Java console, the agent, and the SVA. Such environments are useful early on to gain hands-on experience and a deeper understanding of the product features and capabilities. Although the built-in database is limited to 4GB and typically should not be used for more than 500 agents, you can still exercise most major capabilities of the solution. You can deploy all components in one virtual machine on a low end server with a two-processor Xeon, 4GB memory, and 10GB free disk space. You can also use workstation virtual machines to deploy a small number of agents.

Note: High availability and scalability tests require dedicated systems for DCS:SA, and should not be conducted in the demonstration environment.

Table 1-3 Quick installation overview for an evaluation environment

<table>
<thead>
<tr>
<th>Deployment scenario</th>
<th>Tasks to perform</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCS:S (integrating SVA with NSX)</td>
<td>Deploy the DCS:S server, database, and console for security virtual appliance.</td>
</tr>
<tr>
<td>1</td>
<td>Deploy UMC</td>
</tr>
<tr>
<td>2</td>
<td>Install management server</td>
</tr>
<tr>
<td>3</td>
<td>Install console</td>
</tr>
<tr>
<td>4</td>
<td>Configure DCS:S with VMware and NSX</td>
</tr>
<tr>
<td>5</td>
<td>Deploy SVA and register with UMC</td>
</tr>
<tr>
<td>6</td>
<td>Deploy OD and register with UMC</td>
</tr>
<tr>
<td>DCS:SA (prevention and detection capabilities)</td>
<td>Deploy UMC</td>
</tr>
<tr>
<td>1</td>
<td>Note: If you want to use RESTful APIs, deploy UMC and register DCS:SA with UMC</td>
</tr>
<tr>
<td></td>
<td>See &quot;Integrating with data center orchestration tools &quot; on page 122.</td>
</tr>
<tr>
<td>2</td>
<td>Install management server</td>
</tr>
<tr>
<td>3</td>
<td>Install console</td>
</tr>
<tr>
<td>4</td>
<td>Install agent</td>
</tr>
</tbody>
</table>
**About database scalability**

The database size that you require primarily depends on how many events you want to store in the database. All of the other components combined together, such as agent data, policies, queries, and so on, consume less than 100 MB at initial installation of DCS:SA. The required space is not likely to grow to more than 1 GB. Thus, the remaining database size is based on the events stored in the database, which varies greatly depending on the use case and number of servers. It is possible to plan a rough database size by multiplying number of events you plan to generate time 4K. In order to maximize performance and minimize storage used, you must utilize the Bulk Logging and Event Purging features.

**Bulk Logging**

DCS:SA has the ability for "bulk-event" compressed file storage. This allows a customer to collect many more events for regulatory or forensic analysis purposes than is desired to be transmitted, stored and viewed in the console. By configuring log filtering rules, you decide which events are “actionable” or worthy of real-time transmission to the server vs those events that can be delivered on a periodic basis via a compressed CSV file to the server. DCS:SA keeps a track of the event files so that you can find and load the CSV files when necessary to perform in-depth analysis. These event files take up far less storage and can also act as an archival store. A 1 MB bulk event file holds about 80,000 events. Thus, 10 GB of file system storage can hold nearly a billion events.
The bulk log transfer feature helps you reduce the amount of events being sent to the database that could otherwise overwhelm it. In any large environment where you have several thousand agents deployed, you must configure your Transmit Action accordingly. The events that are based on policies that could be a high risk to your environment should be set to real-time where the events that are less important and generate a lot more noise should be set to bulk log transfer. In other words, send up only actionable events in real-time and use efficient bulk logging mechanism for capturing or recording voluminous events for audit, forensic, or regulatory retention purposes.

You can control the transmission of events by using any of the following:

- **Real-time logging rules**: Lets you determine which events you wish to send to server in real-time mode.
- **Real-time logging batch size**: Lets you determine how many events get sent in a single connection to the server.
- **Bulk Logging/Event File Rotation**: Lets you specify if and when compressed event files get sent to server. Rotation of agent log files based on time or size. Typical 100MB event file is compressed down to about 5MB in size. A checksum and event file catalog message is transmitted to server in real-time. This "bulk file" mechanism can dramatically reduce network load while still providing capture of extensive, fine-grained detailed event data.

**Event Purging**

For those events that are transmitted and stored in the database, you can configure the purge setting to remove events that exceed a specified age range (such as 90 days). This purge method keeps the database from growing without bounds. By default, DCS:SA does not purge any old events from the database. Purging events is critical to keeping the database healthy. You should monitor your daily event flow into the database and the number of events being purged and be sure that the database is staying at roughly a steady state.

To compare the daily inflow and purge counts, do the following:

- Run the “Event Counts by Day” query for the last month to see the event inflow rate.
- If you enable event purging, it happens daily and generates a Server Management event with the number of events actually purged.
Alternatively, you can monitor the total events in the database on a regular basis using the Event Summary report. If the total number of events stays fairly level, then your purging is able to keep up with the event inflow.
This chapter includes the following topics:

- About installation of DCS:SA
- System requirements for DCS:SA
- About using firewalls with DCS:SA
- Disabling Windows XP firewalls
- About name resolution
- About IP routing
- About intrusion prevention
- About simple failover
- Installation log files
- About server telemetry
- What to do after installation

About installation of DCS:SA

To install Symantec Data Center Security: Server Advanced you must install the following components:

- Unified Management Console
  See “Deploying the Unified Management Console (UMC)” on page 126.
- Management Server
You can install the Java console and management server on the same computer or on separate computers. All computers must run a supported operating system. The management server and the Java console are supported on Windows operating system.

Additionally, you must also install the following and get it up and running:

- Set up the VMware environment.
- Register the Datacenter Protection Service with the NSX Manager.
- Deploy the protection service.

## System requirements for DCS:SA

System requirements fall into the following categories:

- See “Software requirements” on page 28.
- See “Operating system requirements” on page 29.
- See “Hardware requirements” on page 30.

### Software requirements

Install the following software before you install or upgrade to the DCS:SA 6.5 management server:

- Windows Installer 2.0 or higher
  
  This is required for installing or upgrading the DCS:SA Management Server on supported Windows operating systems.

- Microsoft SQL Server 2005 or later for the DCS:SA database.

If you want to install the management server along with the SQL Server Express, you must install the following additional prerequisite software:

- NET Framework 4.0 or 4.5.1
- PowerShell 2.0
- For Windows 2008, SP2 or later is required.
- For Windows 2008 R2, SP1 or later is required.
Browser requirements for the DCS:SA Java console

The DCS:SA Java console supports the following browsers:

- Internet Explorer 8
- Internet Explorer 9
- Mozilla Firefox 24

Operating system requirements

This section lists the DCS:SA operating system requirements for the management server, the Java console, and the agent.

The DCS:SA operating system requirements for the management server, the Java console, and the agent are available in the DCS:SA Platform Feature Matrix. The platform support matrix also provides information about the agent features supported on each operating system.

Solaris packages

The agent installation checks for the presence of Solaris system packages.

The following core system packages are required for computers running Solaris 9.0, Solaris 10.0, and Solaris 11.0 operating systems:

- SUNWcar Core Architecture, (Root)
- SUNWkvm Core Architecture, (Kvm)
- SUNWcsr Core Solaris, (Root)
- SUNWcsu Core Solaris, (Usr)
- SUNWcsd Core Solaris Devices
- SUNWcsl Core Solaris Libraries
- SUNWloc System Localization

The following extended system packages are required for computers running Solaris 10.0 operating systems:

- SUNWxcu4, XCU4 Utilities
  Utilities conforming to XCU4 specifications (XPG4 utilities)
- SUNWesu Extended System Utilities
- SUNWuiu8 Iconv modules for UTF-8 Locale
**VMware support**

The DCS:SA Agent is supported on any VMWare guest VM as long as that guest VM is running an OS which supports the Agent as listed in the Symantec Data Center Security: Server Advanced Platform and Feature Matrix. This is true for any version of any VMWare virtualization product.

SVA supports the following VMware® software for agentless monitoring of the guest virtual machines:

- VMware ESXi v5.5U2
- NSX Manager v6.1.2
- vCenter v5.5U2

SVA supports the following Windows versions on VMware guest operating systems:

- Windows Server 2012 (x64)
- Windows Server 2008
- Windows Server 2008 R2
- Windows 8 (32 bit / 64 bit)
- Windows 7 (32 bit / 64 bit)
- Windows XP Professional SP3 x86

**Hardware requirements**

Hardware support includes x86, EM64T, and AMD64. VMware must also support this hardware.

The following table lists the recommended hardware for the DCS:SA components.

<table>
<thead>
<tr>
<th>Table 2-1</th>
<th>Recommended hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component</td>
<td>Hardware</td>
</tr>
<tr>
<td>Security Virtual Appliance</td>
<td>35 GB free datastore space</td>
</tr>
<tr>
<td></td>
<td>2 GB RAM</td>
</tr>
<tr>
<td></td>
<td>4 CPUs</td>
</tr>
<tr>
<td>Java console</td>
<td>150 MB free disk space</td>
</tr>
<tr>
<td></td>
<td>512 MB RAM</td>
</tr>
<tr>
<td></td>
<td>Pentium III 1.2 GHz</td>
</tr>
</tbody>
</table>
Table 2-1  Recommended hardware (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management server</td>
<td>1 GB free disk space (all platforms and databases)</td>
</tr>
<tr>
<td></td>
<td>2 GB RAM</td>
</tr>
<tr>
<td></td>
<td>Pentium III 1.2 GHz</td>
</tr>
<tr>
<td></td>
<td>EM64T</td>
</tr>
<tr>
<td></td>
<td>AMD™64</td>
</tr>
<tr>
<td>Agent</td>
<td>100 MB free disk space (all platforms)</td>
</tr>
<tr>
<td></td>
<td>256 MB RAM</td>
</tr>
<tr>
<td></td>
<td>Sun SPARC™ 450 MHz</td>
</tr>
<tr>
<td></td>
<td>Sun SPARC32, SPARC64</td>
</tr>
<tr>
<td></td>
<td>HP-UX 11i V3 on Itanium2</td>
</tr>
<tr>
<td></td>
<td>IBM PowerPC® (CHRP) 450 MHz</td>
</tr>
<tr>
<td></td>
<td>x86</td>
</tr>
<tr>
<td></td>
<td>EM64T</td>
</tr>
<tr>
<td></td>
<td>AMD™64</td>
</tr>
</tbody>
</table>

See the Symantec Data Center Security: Server Advanced Platform and Feature Matrix for information on supported operating systems, and agent features supported on each operating system.

About using firewalls with DCS:SA

To use DCS:SA with a firewall, you need to configure the firewall to support communications by opening ports, or by specifying trusted services.

**Note:** All ports are default settings that you can change during installation.

You should note the following about using firewalls with DCS:SA:

- The management server uses UDP port 1434 to query the MS SQL Server system and find the port used by the DCS:SA instance. Once the MS SQL Server system returns the port for the DCS:SA instance, the management server then connects to the instance using that port. Thus, your firewall must allow
traffic from the management server to the MS SQL Server system on UDP port 1434 and on the TCP port used by the DCS:SA instance. You can get more information about MS SQL Server’s use of ports at http://support.microsoft.com/default.aspx?scid=kb;EN-US;823938.

- The bulk log transfer feature of the DCS:SA agent is implemented by the bulklogger.exe. If you have a host-based firewall that allows specific programs to access the Internet, you must allow bulklogger.exe as well as SISIPSService.exe to access the Internet. The bulklogger.exe program uses the same ports as SISIPSService.exe. If you do not use the bulk log transfer feature, bulklogger.exe will not run.

The following table lists the services that you can permit to send and receive traffic through your firewalls.

**Table 2-2 Components, services, and traffic**

<table>
<thead>
<tr>
<th>Component</th>
<th>Service</th>
<th>Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Java console</td>
<td>Console.exe</td>
<td>Communicates with the management server using remote TCP ports 4443, 8006, and 8081.</td>
</tr>
<tr>
<td>Management server</td>
<td>SISManager.exe</td>
<td>Communicates with the Java console by using local TCP ports 4443, 8006, and 8081. Communicates with the agents using local TCP port 443. Communicates with remote production SQL servers using the remote TCP port that the SQL server uses for the server instance.</td>
</tr>
<tr>
<td>Agent</td>
<td>SISIPSService.exe sisipsdaemonbulklogger.exe</td>
<td>Communicates with the management server using local TCP port 2222, and remote TCP port 443.</td>
</tr>
</tbody>
</table>

See “Disabling Windows XP firewalls” on page 33.
See “Disabling Internet Connection Firewall” on page 33.
See “Disabling Windows Firewall” on page 33.
Disabling Windows XP firewalls

Windows XP and Windows 2003 Server contain firewalls that are enabled by default. If these firewalls are enabled, you might not be able to establish network communications between the Java console, management server, and agents.

Disabling Internet Connection Firewall

Windows XP with Service Pack 1 includes a firewall called Internet Connection Firewall that can interfere with network communications. If any of your computers run Windows XP, you can disable the Windows XP firewall before or after you install DCS:SA components.

To disable Internet Connection Firewall

1. On the Windows XP taskbar, click Start > Control Panel.
2. In the Control Panel window, double-click Network Connections.
3. In the Network Connections window, right-click the active connection, and then click Properties.
4. On the Advanced tab, under Internet Connection Firewall, uncheck Protect my computer and network by limiting or preventing access to this computer from the Internet.

Disabling Windows Firewall

Windows XP with Service Pack 2 and Windows 2003 Server include a firewall called Windows Firewall that can interfere with network communications. If any of your computers run Windows XP with Service Pack 2 or Windows Server 2003, you can disable Windows Firewall before or after you install DCS:SA components.

To disable Windows Firewall

1. On the Windows XP taskbar, click Start > Control Panel.
2. In Control Panel, double-click Network Connections.
3. In the Network Connections window, right-click the active connection, and then click Properties.
4. On the Advanced tab, under Internet Connection Firewall, click Settings.
5. In the Windows Firewall window, on the General tab, uncheck On (recommended).
About name resolution

To verify proper name resolution for the management server, use a utility, such as `nslookup`, to look up the host name for the management server. If you cannot resolve the host name of the management server, you will need to modify the DNS database or the host file that the client uses to look up host names.

About IP routing

As bastion hosts, firewalls traditionally incorporate some form of network address translation (NAT) between the two networks that the firewall bridges. For example, the management server may be on an internal network while the Agents are in a DMZ network, with a firewall between the two networks. Typically, the internal network IP addresses are hidden from the DMZ network, and are not routable from the DMZ network.

To allow the agents in the DMZ network to communicate with the management server on the internal network, use a DMZ IP address to represent the management server. Then, configure the firewall or router to forward requests for this IP address and port to the real, internal IP address of the management server. Open the agent port only if the agents are in a DMZ. Finally, configure the name database on the DMZ network to return the DMZ IP address for the management server instead of the internal IP address.

About intrusion prevention

The DCS:SA agent installation kit includes an enable intrusion prevention option. When the enable intrusion prevention option is selected, the prevention features of DCS:SA are enabled for the agent. The IPS drivers are loaded on the agent computer, and the agent accepts prevention policies from the Java console.

When the enable intrusion prevention option is not selected, the prevention features of DCS:SA are completely disabled for the agent. The IPS drivers are not loaded on the agent computer, and the agent does not accept prevention policies from the Java console.

Symantec strongly recommends that you enable the intrusion prevention option when installing agents. Changing this option after installation (to disable or re-enable it) requires logging on to the agent computer, running the Agent Config Tool, and rebooting the agent computer.

If you are only interested in the detection features of DCS:SA, Symantec recommends that you select the enable intrusion prevention option during agent installation, and use the Null prevention policy to avoid any blocking. If you later
decide to use the prevention features of DCS:SA, then you simply apply one of the prevention policies that are included with the product. Applying a policy requires no logging onto the agent computer, no running the agent config tool, no rebooting the agent computer.

By default, the enable intrusion prevention option is selected during DCS:SA agent installation.

DCS:SA supports intrusion prevention on computers that run Windows, Solaris, AIX, and Linux operating systems.

**About simple failover**

DCS:SA includes simple failover. Should the primary management server fail, simple failover lets agents automatically switch to the next management server in an ordered list of alternate servers.

Simple failover enables you to deploy a set of front-end Tomcat servers without reconfiguring your IT infrastructure. The ordered list of management server host names or IP addresses is maintained by the DCS:SA agent configuration.

Another use for simple failover is static load balancing. With static load balancing, you manually assign a set of agents to each Tomcat server. Each agent can fail to a different Tomcat server if its primary server becomes inaccessible.

**Note:** All DCS:SA agents support the native DCS:SA simple failover feature, but the DCS:SA SVA does not support it. For SVA failover, you must change the Management Server host address which was specified while registering the Symantec Datacenter Protection Service to VMware NSX Manager.

See "How simple failover works" on page 35.

**How simple failover works**

Simple failover works as follows:

- When the IPS Service starts up, it uses the first server in the ordered list of management servers. The first server in the ordered list is considered the primary management server; the remaining servers are alternate servers. The IPS Service uses server #1 as long as communication with the server is successful.

- At startup, the IPS Service always uses the first server in the ordered list of management servers, regardless of which server was in use when the IPS Service was shut down.
When the ordered list of management servers changes, the IPS Service immediately attempts to connect to the first server in the new list.

When communication with a server fails, the IPS Service uses the next server in the ordered list of management servers. When communication with the last server fails, the IPS Service uses the first server in the list. The IPS Service loops through the ordered list of management servers indefinitely.

When the IPS Service switches to a new management server, it logs the action.

Once the IPS Service fails away from the first server in the ordered list, it periodically checks if server #1 is back, based on the fail back interval. See “About the fail back interval” on page 36.

When the fail back interval expires, the IPS Service checks if server #1 is available. If server #1 is available, the IPS Service starts using it immediately. If server #1 is not available, the IPS Service continues to use the current alternate server; the IPS Service does not traverse the entire ordered list of management servers.

Simple failover with static load balancing works as described in the following example:

- Suppose you have two Tomcat servers pointing to a single database, and two agents.
- You initially configure Agent1 with a management server list of Tomcat1, Tomcat2. You initially configure Agent2 with a management server list of Tomcat2, Tomcat1.
- After installation completes, Agent1 should be talking to Tomcat1, and Agent2 should be talking to Tomcat2.
- Take Tomcat1 off the network.
- Agent1 should fail talking to Tomcat1 and switch to Tomcat2. Now both agents are talking to Tomcat2.
- Put Tomcat1 back on the network.
- Wait longer than the fail back interval.
- Agent1 should fail back to Tomcat1. Agent2 continues to use Tomcat2. Everything is back to the initial state; both agents should be communicating successfully with their original Tomcat servers.

### About the fail back interval

Once an agent fails away from the first server in an ordered list, the agent periodically checks if the first server is back. The agent uses a fail back interval to determine
when to perform this server check. By default, the agent performs the server check every 60 minutes.

For example, suppose you configured three management servers. The primary server #1 and alternate server #2 have failed; alternate server #3 is working. When the fail back interval expires, the agent checks if server #1 is available. If server #1 is available, the agent immediately starts using server #1. If server #1 is not available, the agent continues to use server #3; it does not recheck the ordered list of servers. The agent resets the fail back interval, so it can perform future server checks.

About the management server list for an agent

To use simple failover for an agent, you must provide the list of primary and alternate management servers using one of the following methods:

- If you are installing DCS:SA for the first time, you can provide the list of primary and alternate management servers during agent installation.
- If you are upgrading to DCS:SA, you can provide the list of primary and alternate management servers using the SDCSS_Agent_Diagnostics detection policy or the agent config tool.

The primary and alternate management server hostnames or IP addresses configured for a single agent must be Tomcat servers that talk to a single DCS:SA database. Using multiple databases will result in unexpected agent behavior.

The primary and alternate management servers must use the same server certificate and agent port.

See “Specifying the management server list for an agent” on page 37.

Specifying the management server list for an agent

This section explains how to specify the primary management server and optional alternate management servers for an agent.

See “About simple failover” on page 35.

You can use the following:

- SDCSS_Agent_Diagnostics detection policy
- Agent config tool

Using the SDCSS_Agent_Diagnostics detection policy

A version of the SDCSS_Agent_Diagnostics detection policy is available for Windows and UNIX agents.
See the *DCS:SA Detection Policy Reference Guide* for information about the SDCSS_Agent_Diagnostics policy.

**To use the SDCSS_Agent_Diagnostics detection policy**

1. Log on to the Java console as an administrator.
2. In the Java console, on the Policies page, in the Symantec folder, edit the SDCSS_Agent_Diagnostics policy.
3. Enable **Modify the management server list used by the agent**, and then click **Specify a comma-separated list of servers**.
4. In the Value box, type the primary management server, followed by any optional alternate management servers.

   You must specify the primary management server as the first server, followed by any optional alternate servers. Specify the IP address or fully qualified host name of each server in the list. All the servers in the list must use the same server certificate and agent port.
5. Click **OK** to save the policy changes.
6. Apply the policy to the agent.

   The policy modifies the management server list immediately after the policy is applied to the agent.
7. In the Java console, monitor the events on the **Monitors** page to determine if the management server list was modified.
8. Clear the policy from the agent.

**Using the agent config tool**

You use the agent config tool to do the following:

- After upgrading to SCSP agent 5.1.1 or higher, add alternate management servers to an agent's configuration
- Change the primary management server or alternate management servers that an agent uses
- Change the fail back interval that an agent uses
- Display the current management server list and fail back interval that an agent uses
- Test the connection information for a management server

The agent config tool is located in the following directories on an agent computer:

- On Windows, sisipsconfig.exe is located in the agent/ips/bin directory.
On UNIX-based operating systems, the sisipsconfig tool is named sisipsconfig.sh. It is located in the agent/ips directory.

The following table lists the management server-related agent config tool commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-host</td>
<td>Windows: sisipsconfig -host primary[,alternate1,alternate2,...] UNIX: sisipsconfig.sh –host primary[,alternate1,alternate2,...]</td>
<td>Set the IP address or fully qualified host name of the primary management server and the optional alternate management servers the agent uses. The list of management servers must comprise the primary management server, which is always the first server in the list. The remaining optional servers in the list are considered alternate servers. You may specify any number of optional alternate management servers. The management server list that you specify replaces the current management server list that the agent uses. You cannot reorder or edit an existing management server list. The management server host names or IP addresses that are configured for a single agent must be Tomcat servers that talk to a single DCS:SA database. Using multiple databases can result in unexpected agent behavior. The management servers must use the same server certificate and agent port.</td>
</tr>
<tr>
<td>-failbackinterval</td>
<td>Windows: sisipsconfig -failbackinterval num_mins UNIX: sisipsconfig.sh -failbackinterval num_mins num_mins = number of minutes Default: 60 minutes</td>
<td>Set the fail back interval, in minutes, for the agent to try to communicate with the primary management server. Once an agent fails away from the first (primary) server in the management server list, the agent periodically checks if the first server is back. The agent uses a fail back interval to determine when to perform this server check.</td>
</tr>
</tbody>
</table>
Table 2-3  Agent config tool commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-view</td>
<td>Windows: sisipsconfig -view UNIX: sisipsconfig.sh -view</td>
<td>Display all values that are configurable through the agent config tool. The configurable values include the management server list and failback interval.</td>
</tr>
<tr>
<td>-test</td>
<td>To test first server in list (default):</td>
<td>Test the connection information for a server in the management server list.</td>
</tr>
<tr>
<td></td>
<td>■ Windows: sisipsconfig -t</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ UNIX: sisipsconfig.sh -t</td>
<td></td>
</tr>
<tr>
<td></td>
<td>To test the nth server in list:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Windows: sisipsconfig -t n</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ UNIX: sisipsconfig.sh -t n</td>
<td></td>
</tr>
</tbody>
</table>

To specify the management server list for an agent

1. At a command prompt, locate the folder that contains the agent config tool, and then navigate to that directory.

2. Type `sisipsconfig` `-host` (Windows) or `sisipsconfig.sh` `-host` (UNIX), followed by a comma-separated list of server host names or IP addresses, and then press Enter.

Installation log files

DCS:SA uses log files to record events and messages related to agent and management server installation. The log files have information required for troubleshooting installation problems if they occur.

Table 2-4  Installation log files

<table>
<thead>
<tr>
<th>File name</th>
<th>Operating System</th>
<th>Default location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server \SISManagerSetup.log</td>
<td>Windows</td>
<td>On 32-bit operating system: C:\Program Files\Symantec\Data Center Security Server\</td>
</tr>
<tr>
<td>Console \SISConsoleSetup.log</td>
<td></td>
<td>On 64-bit operating system: C:\Program Files (x86)\Symantec\Data Center Security Server\</td>
</tr>
<tr>
<td>Agent \SISAgentSetup.log</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 2-4  Installation log files (continued)

<table>
<thead>
<tr>
<th>File name</th>
<th>Operating System</th>
<th>Default location</th>
</tr>
</thead>
<tbody>
<tr>
<td>/var/log/sdcsslog/agent_install.log</td>
<td>UNIX</td>
<td>-</td>
</tr>
</tbody>
</table>

See the *DCS:SA Administrator's Guide* for more information on log files.

**About server telemetry**

The Management Server Telemetry feature allows you to optionally collect and send anonymous Customer Agent deployment statistics to the Symantec Backend Telemetry Server. This periodic data collection and submission is seamless to the end user and does not require any administrative interaction. As part of the telemetry data, DCS:SA sends statistics such as agent counts, event counts, and DCS:SA Server settings. The Server Telemetry is an opt-in or opt-out feature for the DCS:SA Management Server. By default, Server Telemetry is enabled with DCS:SA Server fresh install and upgrade from a previous version. When this feature is enabled, you can optionally enter the **Customer Name** in the provided text box. The customer name that is entered in this text box is submitted to Symantec as part of telemetry data submission.

**To disable the Server Telemetry feature from the Java console**

1. Click **Admin > Settings > System Settings**.
2. In the **Data Collection** page, uncheck the check box to stop Telemetry data collection and submission.

**What to do after installation**

You can begin enforcing the DCS:SA policies on agents immediately after agent installation and registration with the management server.

Symantec recommends that you first apply a policy to a few agents, and then verify that the agent computers are functioning properly with the applied policy.

See the *DCS:SA Administrator's Guide* for information about applying policies to agents.

See “About the incremental rollout of agent installations and policy deployment” on page 58.
Planning the Installation for DCS:S

This chapter includes the following topics:

- About installing DCS:S
- How DCS:S works
- System requirements for DCS:S
- Setting up the VMware environment

About installing DCS:S

To install DCS:S, you must install the following components:

- Unified Management Console
  See “Deploying the Unified Management Console (UMC)” on page 126.
- Management Server
  See “Installing the management server” on page 129.
- Security Virtual Appliance
  See “Deploying a Security Virtual Appliance” on page 139.

You can install the Java console and management server on the same computer or on separate computers. All computers must run a supported operating system. The management server and the Java console are supported on Windows operating system.

Additionally, you must also complete the following tasks:

- Set up the VMware environment.
- Register DCS:S with UMC
Configure NSX Manager to register the Datacenter Protection Service with the NSX Manager.

Deploy the protection service.

How DCS:S works

DCS:S provides a mechanism to secure guest virtual machines against malware attack. The DCS:S policy page displays policies that are published, unpublished, and modified. The unpublished policies are editable and can be applied to guest virtual machines only when they are published.

The three types of policies are as follows:

- **Antivirus policies**
  Antivirus policies provide basic level and advanced level protection from malware. For example, antivirus policies can be configured to provide protection to the guest virtual machines from malicious virus attacks.

- **Network security policies**
  Network Security policies are used for specifying settings to monitor Network traffic. This policy can be applied on Windows GVMs only.

- **SVA configuration policies**
  SVA configuration policies are predefined configuration settings that are applicable to Security Virtual Appliances. This policy can be applied on Windows GVMs only.
  For example, configuration policies define the behavior of a SVA and can generate events if any changes are made to the configuration settings of a SVA and its services, and when the settings of scheduled scans and LiveUpdate server are changed.

The following diagram illustrates a high-level work flow of DCS:S.
You use the Unified Management Console to monitor the Datacenter protection status. After you register the Datacenter Protection Service with VMware, you can view the security groups, run scans on a guest virtual machine or on a security group, view the command status, run LiveUpdate on a SVA, view alerts and notifications that are received from the SVA, and the overall health of the datacenter.

DCS:SA also allows you to create queries and reports with charts, graphs, and tables that provide detailed and aggregated summary data about Security Virtual Appliances, events, agents, and policies appears in DCS:SA. On the basis of command result, the guest virtual machines receive a tag to specify its state. You can decide upon the preventive measure to adopt in case a threat is detected.

System requirements for DCS:S

Ensure that you meet the appropriate system requirements for the management server, the Java console, and Security Virtual Appliance.

VMware support

Symantec Data Center Security: Server supports the following VMware® software:

- NSX v6.1.2
- VMware ESXi v5.5 update 2
vCenter v5.5 update 2

The following Windows versions are supported on VMware guest operating systems:

- Microsoft Windows Server 2012 (64-bit) with latest Service Pack
- Microsoft Windows Server 2008 R2 (64-bit) with latest Service Pack
- Microsoft Windows 2008 (32-bit or 64-bit) with latest Service Pack
- Microsoft Windows 8 or 8.1 (32-bit or 64-bit) with latest Service Pack
- Microsoft Windows 7 (32-bit or 64-bit) with latest Service Pack
- Microsoft Windows Vista (32-bit or 64-bit)

Hardware requirements

Table 3-1 lists the recommended hardware for DCS:S.

<table>
<thead>
<tr>
<th>Component</th>
<th>Hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Java console</td>
<td>150 MB free disk space</td>
</tr>
<tr>
<td></td>
<td>512 MB RAM</td>
</tr>
<tr>
<td></td>
<td>Pentium III 1.2 GHz</td>
</tr>
<tr>
<td>Management server</td>
<td>1 GB free disk space (all platforms and databases)</td>
</tr>
<tr>
<td></td>
<td>2 GB RAM</td>
</tr>
<tr>
<td></td>
<td>Pentium III 1.2 GHz</td>
</tr>
<tr>
<td>Security Virtual Appliance</td>
<td>35 GB free datastore space</td>
</tr>
<tr>
<td></td>
<td>4 GB RAM</td>
</tr>
<tr>
<td></td>
<td>4 CPUs</td>
</tr>
</tbody>
</table>

For more information on installation requirements, refer to Symantec Data Center Security: Server Advanced Planning and Deployment Guide at: www.symantec.com/business/support/index?page=content&id=DOC8101

Setting up the VMware environment

To deploy the Symantec Datacenter Security Service for VMware NSX, which is Virtual Machine Threat Protection, you must set up the VMware environment by installing and configuring the following VMware components:
- Deploy vCenter 5.5 update 2 appliance.
- Deploy NSX Manager v6.1.2.
- Register vCenter with NSX Manager.
- Create a data center.
- Create a cluster and add ESXi hosts to the cluster.
- Create a distributed switch and add ESXi hosts to the distributed switch.
- Install host preparation.
- Deploy Guest Introspection service.

For more details on setting up the VMware environment, refer to the VMware guide at: http://pubs.vmware.com
Planning the Deployment Architecture and Rollout

This chapter includes the following topics:

- About network architecture and policy distribution
- Planning for enterprise deployment
- About scaling
- Key database server installation considerations
- Agent installation considerations for key features
- About automating agent installations
- Best practice for agent installation
- About development, test, and production instances
- About the incremental rollout of agent installations and policy deployment

About network architecture and policy distribution

When you install DCS:SA for the first time for testing purposes, you do not need to consider network architecture and policy distribution. You can install a management server and a Java console, along with a few agents and an SVA for malware protection on virtual machines, and become familiar with DCS:SA operations. When you are ready to roll out policies to your production environment, you can roll out different policies that are based on computing needs, and prevention and detection levels.
The DCS:SA prevention policies protect against inappropriate modification of system resources. The policies confine each process on a computer to its normal behavior. Programs that are identified as critical to system operation are given specific behavior controls; generic behavior controls provide compatibility for other services and applications.

The DCS:SA detection policies monitor events and syslogs, and report anomalous behavior. Detection policies define which system events or user-defined criteria are selected, which criteria are ignored, and what actions are performed after select and ignore criteria are met.

Areas where computing needs and prevention and detection levels might differ include the following:

- Local workstations
- Remote annex workstations
- Computers that run production databases
- Computers that are located in demilitarized zones (DMZ) such as Web servers, mail proxy servers, public DNS servers
- Virtualized environment

Prevention policies pushed to local and remote workstations would most likely be less restrictive than prevention policies pushed to production databases and DMZ servers.

Detection policies pushed to local workstations, production databases, and DMZ servers would also differ. Detection policies pushed to production databases and DMZ servers are more likely to offer more signatures than policies pushed to workstations.

You can distribute different policies to different computers by creating agent groups with the Java console and then associating the agents with one or more groups during agent installation. You first create the groups by using the Java console, set the different policies for the groups, and then associate the agents with the groups during installation. It is not necessary, however, to associate an agent with a group during installation. You can perform this operation after installation.

See “About the DCS:SA infrastructure” on page 16.

Planning for enterprise deployment

While installation of a small demonstration environment can be completed within an hour, enterprise deployments require careful planning. You first need to gain a deeper understanding of the product and how it best integrates with your organization’s overall security and compliance strategy.
Most development or test environments deploy at least a two-node management environment setup. One node hosts the DCS:SA management server. The other node hosts the MS SQL Server instance that is needed for the DCS:SA database. The following diagram illustrates a simple setup.

**Figure 4-1** Simple system setup

With appropriate hardware and configuration settings, this scenario can support 10,000 deployed agents. The DCS:SA Management Server node, which is itself stateless, does not require excessive system resources and uses little disk I/O. It can also operate efficiently as a Guest Virtual Machine (GVM). Thus, configuring multiple Management Server systems on virtual machines provides for simple failover and easy setup.

A best practice is to install a DCS:SA agent on each computer that hosts a management component. This setup lets you monitor and secure the systems from tampering. For example, in this two-node scenario, you should deploy a DCS:SA Windows agent to protect the Management Server. You should deploy a second agent on the computer where the DCS:SA SQL Server database resides. You should deploy appropriate protection and detection policies to these agents to activate enforcement.

DCS:SA’s J2EE application server and Microsoft SQL Server management components support high availability scenarios using common enterprise techniques. Many users add an additional DCS:SA Management Server node to provide high availability. With the proper configuration, when one DCS:SA Management Server fails, the remaining node can still service agent communications and console activities. The following diagram shows this configuration.
Figure 4-2  DCS:SA high availability

For details, see the following section about specifying alternate management servers.
See “About the management server list for an agent” on page 37.

To further enhance the high availability scenario, some users choose to add a fourth system to avoid database system outages. Several SQL Server high availability techniques are available. For example, you can configure an active/passive SQL Server database cluster or use a SQL Server log shipping approach for near-real time database redundancy.

See the various documents on Microsoft's Web site for information about MS SQL high availability scenarios. For example:

High Availability Solutions Overview

High Availability Solutions (SQL Server)

See the VMware product documentation on the VMware's Web site for information about High Availability on VMware.

See “About the DCS:SA infrastructure” on page 16.
See “System requirements for DCS:SA” on page 28.
About scaling

For a configuration that supports a large number of agents, such as 20,000 to 100,000 endpoints, you should add more front-end DCS:SA management servers. You need the additional Management Servers to handle agent communications. As a general rule, you can have 10,000 agents per system.

For these larger environments, you must configure the agent communication settings appropriately. The most notable setting is the agent polling check-in interval, which by default is five minutes. A setting of five minutes is appropriate for evaluation purposes, but not for large-scale deployments. You need to set it to a larger time interval, such as 30 minutes to 60 minutes for most agents. In the production environments that have few policy or configuration changes, agents do not need to check so frequently for changes. Most agents do not need to listen for notification changes from the DCS:SA Management Server. If the agents do not need to listen, then you can disable the default listening port, which is 2222 on most agents.

Some examples of polling and listening configurations are as follows:

- System whose policy and configuration settings are relatively stable and that are typical with respect to your DCS:SA deployment. Such systems should have a relatively longer polling interval, such as 30-60 minutes. They should not listen for policy and configuration change notifications. This scenario should be for a majority of agents in your deployment.

- System whose policy and configuration settings change significantly more often than your typical agents. This scenario can represent a small set of the systems that you use as the initial phase of rolling out policy or configuration changes. Therefore these systems have more frequent changes due to policy tuning. Or, this scenario can represent the high risk systems, such as in the DMZ, for which you want a fast reaction time to policy changes. These agents should have a shorter polling interval, 5-15 minutes, for example. They should not listen for policy and configuration change notifications. This scenario should represent a small percentage of your deployment to avoid putting a constant, heavy load on the management servers.

- System whose policy and configuration settings are relatively stable, but need a fast reaction time to infrequent policy or configuration changes. These systems can have a long polling interval, 30-60 minutes, for example. These systems should listen for policy and configuration change notifications and therefore you should maintain the default listening port, 2222. This scenario represents an alternative for high risk systems, such as in the DMZ, and for internal systems with unusually sensitive applications or data. This scenario should represent a small percentage of your deployment to avoid putting a heavy load on the management servers when you do change a policy or configuration.
The DCS:SA SVA supports up to 200 guest VMs on a single ESX host. If more than 200 guest VMs are seen on a single ESX host, the SVA will only protect 200 of them and the remaining guest VMs are unprotected. The DCS:SA Java console highlights oversubscribed SVAs, i.e. SVAs with more than 200 guest VMs as well as the total number of unprotected guests. You must monitor these counts in the console and rebalance the guest VMs on your ESX hosts if these situations occur on a regular basis. If you have more than one ESX host in a cluster then you can balance the oversubscribed guest VMs of one ESX host with the unused threshold limit of another ESX host.

Key database server installation considerations

A key question during the initial server installation is whether or not you should configure the DCS:SA database to “Enable Unicode storage.” This option is enabled by default and is designed to work with all agents and policies that require double-byte character support. Examples of these languages are Japanese, Chinese, Korean, and other multi-byte languages.

The advantage of enabling unicode storage is that it allows DCS:SA to support data from international operating systems. The disadvantage is that it affects system sizing and performance. Unicode storage consumes two bytes of data space for every character in the strings that are stored in the database. Two bytes are used even when the source data is itself in a single-byte format, such as ASCII data. DCS:SA stores strings such as Syslog and Windows event log messages, path names, and policy names. As a result, non-Unicode customers can experience increased database disk space usage and subsequent increased processing and backup. Many customers have only single-byte language requirements and do not need to use Unicode storage. You should choose to enable or disable this setting based on your understanding of your organization’s deployment requirements.

Note: It is difficult to convert a Unicode database to a non-Unicode database at a later stage. You can experience a data loss of 2-byte character data when it is constrained to a 1-byte format.

Agent installation considerations for key features

Agent installation configures the appropriate networking for the environment. The agent installation configuration includes which DCS:SA Management Servers to communicate with, what ports to use, and how often to poll for changes. The initial DCS:SA installation also determines whether key product features are enabled or not. The key agent feature installation considerations are discussed in greater detail in each section, as follows:
About enabling intrusion prevention

The intrusion prevention capability is enabled by default during agent installation on all DCS:SA agents that support it.

See the Symantec Data Center Security: Server Advanced Platform and Feature Matrix for more information on the supported operating systems, and agent features supported on each operating system.

Symantec recommends that you have intrusion prevention enabled. The prevention enforcement engine consists of the kernel mode drivers. When intrusion prevention is enabled, it is loaded on the agent computer on the next restart. Immediately after installation, the intrusion prevention engine is configured to run with a Null policy. A Null policy contains no prevention rules and hence does not block any actions on the system. So, while the kernel driver intercepts all resource access operations by the operating system, it essentially operates in pass-through mode.

The key advantage of enabling the intrusion prevention feature with a Null policy is that the appropriate kernel drivers are loaded. Thus, the agent is ready to accept other prevention policies when you decide to deploy them. This configuration avoids any disruption to the normal operation of the critical server, since it does not require a restart to deploy the policy. If you plan to deploy prevention policies on an agent, you must leave the intrusion prevention feature enabled so that the agent can accept a prevention policy.

The slight disadvantage of leaving this setting enabled is its effect on performance. The drivers continue to intercept every resource request even when there is no benefit. This setting results in unnecessary overhead if the only requirement for the system is for file integrity monitoring or log monitoring. Symantec recommends that you deploy the agents in a lab or a quality assurance pre-production environment before you deploy the agent on production systems. Deploying the agents on a pre-production environment that closely represents the configuration and load of your production systems is the best way to understand the performance or throughput impact on a specific server that may have high number of processes, disk I/O activity, or network activity.

The intrusion prevention deployment by default also requires a system restart for the driver to load initially and observe all process launches from startup. Some
production systems have very long periods of time before they can be stopped and restarted. You may prefer to deploy only detection features to avoid having to restart.

If you choose to continue with intrusion prevention enabled, it is best practice to restart the system immediately after installation activities have completed. Restarting immediately provides the best chance to discover any adverse system effects so that you can take action quickly. For example, you can disable the intrusion prevention capability until the underlying issue is corrected. Deferring a system restart after installation activities is a significant risk, since a system restart may not occur for a long time following the installation. Operational staff may erroneously attribute the issues that are seen during a later restart to factors unrelated to the earlier DCS:SA installation. This mistake can in turn increase the time to resolution and overall costs. Thus, a best practice is to do at least one if not both of the following tasks:

- Restart immediately when you install or upgrade the agent with intrusion prevention enabled.
- Perform thorough testing up front to be sure there are no issues on production systems.

You can use the DCS:SA console to visually determine the status of agents needing to be restarted. A blue triangle icon in the Asset display indicates that the prevention driver is due to be enabled at the next system restart. In addition, you can modify and run the Agent Detail query to see the status of agents pending restarts.

For more information about queries, see the DCS:SA Administrator's Guide.

**Note:** At the time of installation, you can selectively decide which agents should have intrusion prevention enabled.

For example you may initially roll out the prevention feature to a subset of the systems, such as a DMZ or particularly valuable system. You can then increase the prevention usage over time. If you disable intrusion prevention and want to enable it in the future, you must run the sisipsconfig.exe tool with the -I option and restart the computer. The -I option toggles the intrusion prevention service feature on and off. The sisipsconfig.exe tool is located in the \Agent\IPS\bin directory.

For information about the sisipsconfig.exe tool, you can see the following sources:

 Disable Intrusion Prevention [IPS] for Solaris|AIX|Linux|Windows

Symantec recommends that all policy tuning be conducted on representative systems in a test or pre-production environment. This will help identify and correct any Symantec or customer-defined policy rules that inadvertently block resources required for the normal functioning of applications or operating system services.
About enabling the real-time file integrity monitoring feature in intrusion detection

During agent installation, the real-time file integrity monitoring capability is enabled by default on all DCS:SA agents that support the feature. Symantec recommends that you enable the real-time file integrity monitoring capability. When this feature is enabled, the detection engine loads kernel mode drivers on the agent to aid in file monitoring activities. When real-time file integrity monitoring capability is enabled as part of intrusion detection, the driver functions are observational only. However, Symantec still recommends a phased rollout on representative systems, to ensure that the operating system or business critical applications operate as expected.

The use of the drivers in the real-time file integrity monitoring feature has the following key advantages:

- The richness of the file integrity monitoring event data for local file systems. Data such as real time logging and the user and process that are involved in the file integrity events are logged.
- The flexibility in determining which changes are valid and which are invalid by adding exceptions for trusted installers or users performing the changes.

You can disable the real-time file integrity monitoring feature at the initial installation, if desired or necessary. The detection engine then does not load the real-time file integrity monitoring kernel mode drivers. It automatically uses polling-based file integrity monitoring instead. The file monitoring polling interval is defined in the policy or in the global default settings.

If you disable real-time file integrity monitoring and want to enable it in the future, you must run the sisipsconfig.exe tool with the -rtfim option. The sisipsconfig.exe tool is located in the \Agent\IPS\bin directory. The -rtfim option toggles the real-time file integrity monitoring feature on and off. On some operating systems, you may also need to restart the agent to load the real-time file integrity monitoring kernel mode drivers.

The Windows and UNIX detection policies are pre-configured to monitor critical operating system files in real-time. You can select additional files or de-select the files that are selected by default by configuring the General Settings of a detection policy. When you apply the configured policy on an agent and any of the files that you want to monitor is accessed by a user or a process, a real-time detection event is generated.

For information about the sisipsconfig.exe tool, see the following sources:


How to disable File Integrity Monitoring (FIM) driver in DCS:SA for Windows and AIX
### About creating agent registration groups

You can distribute different policies and configuration settings to different computers by creating agent groups in the Java console. First create the groups by using the Java console, set the different policies for the groups, and then associate the agents with the groups during installation. When the agent first registers with the DCS:SA Management Server, it is placed into the groups that were specified during the agent installation. It immediately takes on the policies and settings that were defined for those groups.

The specification of group settings is optional during installation. If you leave the group settings empty, the agents register to the topmost node in the group hierarchy. Later, you must manually move agents into appropriate groups in the console. However, this method can be tedious for a large number of agents. If your deployment numbers grow into the thousands, it is very beneficial to plan in advance. You should know how you want to manage policy deployments. Typically, you should determine how you want to group and organize your agents and specify your group settings during agent installation.

### About automating agent installations

For larger organizations, you can automate the agent installation process effectively with provisioning tools, scripts, and other mechanisms. The agent installation kits all support silent, unattended installation. However, it is very important that you fully understand the types of computers that you install the agent on. You should understand their hardware specifications and software specifications, as well as other possible software that might conflict with the installation process.

The agent's operating system requirements are detailed in the [Symantec Data Center Security: Server Advanced Platform and Feature Matrix](#). Use DCS:SA only with supported hardware and operating systems. Using the product with unsupported equipment and operating systems may result in unexpected behavior.

Once you decide on your installation choices, encode these choices in your automated deployment scripts. You can begin enforcing the DCS:SA policies on agents immediately after agent installation and registration with the management server.

### Best practice for agent installation

As a best practice, Symantec recommends that you use DCS:SA's full protection and monitoring features unless you have no immediate need to use the underlying
features. Users who focus only on intrusion detection for the foreseeable future should disable the intrusion prevention features. Similarly, users who focus only on intrusion prevention should disable the real-time file integrity monitoring feature. Regulatory needs or a need for increased visibility into file integrity monitoring events should drive use of real-time file integrity monitoring by intrusion detection users.

Some users may be under pressure to broadly and quickly deploy only the file integrity monitoring and log monitoring features. They may not have time to perform adequate internal quality assurance testing. In this scenario, it would be safest to disable intrusion prevention and real-time file integrity monitoring and look into re-enabling those features when time permits.

**About development, test, and production instances**

You need to consider how your organization intends to enforce code promotion and change management practices in regard to your development, test, and production deployments. You should treat DCS:SA like any other enterprise application in the following aspects:

- Source code version control
- Change processes related to policy or configuration changes
- Separation of duties

Some organizations have distinctly separate development, test, pre-production, and production environments for DCS:SA. Policy changes are made first in the development environment and then promoted to the test environment. Eventually, they are promoted to the production environment. In classic source code provisioning, policies are exported from the DCS:SA console and checked into a source control system. Then, in each phase of the code promotion cycle, the policy is retrieved from source control and imported into the DCS:SA console. It is deployed from the console to its scope of systems. Eventually, the policy is verified and then imported into the production DCS:SA console and deployed to operational production systems.

Some customers have combined their development environment and test environment into one DCS:SA environment, while the production environment remains separate. Under some circumstances, users manage all classes of system from one central console. Symantec generally does not recommend a single control console across types of system. This can and has led to abuses and inadvertent situations where production systems are mistakenly used for test bed activities. Such mistakes can lead to errors in the policy rules or the configuration settings that affect production systems.
In all environments, you should grant only the access rights that any one individual requires. You can use the user roles in the DCS:SA console to control who has access to specific agents or you can use access rights to agent groups. In addition, explicit user roles can limit access to basic functionality in the console. These predefined roles include Administrators, Authors, Managers, and Guests. By default, the built-in Administrator's role has complete, unrestricted access to all available DCS:SA features and tasks and agents. The Guest's role has only read access to the console. Because you need at least one role with unrestricted access, Symantec recommends that you do not modify the built-in Administrator's role.

For more information about default roles and defining custom roles, read the chapter titled "Using the Admin page," in the DCS:SA Administrator's Guide.

About the incremental rollout of agent installations and policy deployment

In any software deployment, you should first deploy the software to a representative sample of systems and validate it before you deploy it more broadly. In many organizations, installation or operations teams deploy DCS:SA agents, while security or compliance functions maintain the detection policies and prevention policies. Plan the agent installation and deployment activities in phases to account for the differences in the workload and activities on production systems. By planning the agent installation and deployment activities in phases, you can proactively address any issues that you encounter.

Symantec recommends that you first deploy agents configured with the appropriate policies on a small number of representative systems, to ensure that the systems and any business applications operate properly. Then, from the DCS:SA console, deploy policies to a representative pool of agents. Verify that the systems and business functions operate properly with the appropriate security policies applied.

See the DCS:SA Administrator's Guide for information about applying policies to agents.

Incremental rollout is especially valuable for blocks of like systems such as a dozen domain controllers or many similar database, Web servers, or cluster members. Symantec considers it a best practice to deploy to a small subset of like systems first, say one to three agents, to validate that critical business applications function as desired. Incremental rollouts provide the opportunity to manage each checkpoint and not have to troubleshoot both installation issues and policy issues at the same time.

Incremental testing and incremental deployment are especially valuable for the small set of extreme systems that are found in some environments. These extreme systems exhibit high end scaling that is out of proportion in comparison to the rest
of the enterprise. Such systems are candidates for additional scrutiny and testing before production deployment. Examples of extreme systems include the following:

- Systems that have more than 1,000 concurrent processes where most other systems may have less than 100 processes.
- Systems that monitor changes on 500,000 files where most other systems generally have less than 10,000 files to monitor.
- Domain controllers, database servers, or other application servers that handle an order of magnitude more requests than typical systems.
- Systems that are near the limit of CPU or memory usage before DCS:SA is installed.
- A clustered environment
Installing DCS:SA

This chapter includes the following topics:

- Installing Symantec Data Center Security: Server Advanced components on Windows
- Installing Symantec Data Center Security: Server Advanced components on UNIX
- Integrating with data center orchestration tools

Installing Symantec Data Center Security: Server Advanced components on Windows

Refer to the following sections for installing the DCS:SA components on Windows:

- See “About the Windows installation” on page 60.
- See “Installing the management server” on page 64.
- See “Installing and configuring the Java console” on page 78.
- See “Installing a Windows agent” on page 82.

About the Windows installation

If this is a first-time installation, you should install, configure, and test DCS:SA components in a test environment.

You should install the DCS:SA in the order listed:

- Management server
- Java console
- Agent
You can install the Java console and management server on the same computer or on separate computers. You can install agents on any computer. All computers must run a supported operating system.

The management server and Java console are supported on Windows operating systems.

Symantec recommends that you install the agent on the manager and apply the Windows whitelisting strategy to enable self-protection capabilities.

---

**Note:** The installation directory names for the Java console and management server must contain printable ASCII characters only. Multi-byte, double-byte, hi-ASCII and non-printable ASCII characters are not supported.

---

**About port mapping**

When you install the DCS:SA components, you must specify ports through which the components communicate. In a few instances, these ports must match.

The following table shows the DCS:SA ports that must have matching numbers.

**Table 5-1**  Port mapping

<table>
<thead>
<tr>
<th>Management server</th>
<th>Java console</th>
<th>Agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Port</td>
<td></td>
<td>Agent Port</td>
</tr>
<tr>
<td>Console Port</td>
<td>Port</td>
<td></td>
</tr>
<tr>
<td>Web server</td>
<td>Admin Port</td>
<td></td>
</tr>
</tbody>
</table>

**Bypassing prerequisite checks**

The Windows installation kit lets you bypass some of the prerequisite checks for agent and management server installation. You can use this feature if you know the installation kit is incorrectly failing a prerequisite.

When you use the bypass prerequisite checks feature, the installation kit displays all errors and warnings about prerequisite check failures. However, instead of terminating the installation, you may choose to continue.

When you run the installation kit in interactive mode, you are asked if you want to continue. When you run the installation kit in silent mode, the prerequisite failure is logged and the installation continues.

To enable the bypass prerequisite checks feature, do the following:
(Agent only) For silent installs, set the ENABLE_BYPASS_CHECKS variable to a nonzero value.

For interactive installs, the presence of the file scsp-check-bypass.txt, either in the installer directory or %temp% folder will confirm the bypass enabling.

The Windows installation kit does not remove the scsp-check-bypass.txt file upon successful installation.

You can bypass the following checks when installing the DCS:SA agent:

- Agent install disk space checks that are performed apart from Windows Installer (MSI) engine
- Service user account (allow domain users or local users even though the installer can not confirm the required rights and privileges)
- Existence of AppFire 4.5

You can bypass the following checks when installing the DCS:SA management server:

- Existence of AppFire 4.5
- Disk space checks
- User privilege and rights check for service user account
- Microsoft Data Access (MDAC) version

About installing a database linked to a SQL Server instance

The DCS:SA installation lets you install an SQL Server 2012 Express evaluation database locally. The installation also lets you install an evaluation or production database linked to an instance of SQL Server locally or remotely. All installations allocate 100 MB space for the database. SQL Server automatically allocates more space when it is required.

If you choose to install a database linked to an instance of SQL Server, Symantec recommends that you first install a new instance of SQL Server that conforms to the installation requirements. You can install a database on an older, existing instance, but the instance must be configured properly or your database installation will fail. For example, if the authentication configuration is not set to Mixed Mode, your installation will fail.

About SQL Server installation requirements

You can install the SQL Server on the same machine that you plan to install DCS:SA management server, or on a different machine.
The DCS:SA Management Server supports Microsoft SQL Server 2012 and all newer versions. This includes all "editions", e.g. Express, Standard, etc., and includes all service packs.

The following information applies to the SQL Server software.

When you install the instance of SQL Server, do the following:

- Do not accept the default instance name. Use SCSP (the default when you install DCS:SA management server), or some other name. Type the same name when installing DCS:SA management server.
  A database named scspdb, the default, will be created in this instance when you install DCS:SA management server.
- Set authentication configuration to Mixed Mode (Windows authentication and SQL Server authentication).
- Set the sa password when you set Mixed Mode authentication. You will type this password when you install DCS:SA management server.

After you install the instance of SQL Server, you must do the following:

- Select to authenticate using SQL Server credentials.
- Register the instance.
  Registering the instance also starts the instance.

When you register the instance of SQL Server, you must do the following:

- Set the authentication mode to SQL Server authentication.
- Configure the connection option to log on automatically through SQL authentication with the sa account, and type the sa password.
- If registration fails due to authentication failure, display the properties available from the server messages dialog box, and type the sa password again.

After you register the instance, you must do the following:

- Use the networking utility to verify that NamedPipes and TCP/IP are enabled protocols. If they are not enabled, enable them.

You are then ready to install DCS:SA management server.

Configuring the temp environment variable

The installation packages unpack installation files into the directory that is specified by the TEMP environment variable. The volume that contains this directory must have at least 200 MB of available disk space. If this volume does not have the required disk space, you must change your TEMP environment variable or your installation will fail.
Note: After successful installation of the management server and Java console, SISManagerSetup.log and SISConsoleSetup.log appear in the \Server and \Console directories respectively. If installation is cancelled or unsuccessful, then the log files appear in the directory specified by the TEMP environment variable.

To configure the temp environment variable

1. At a command prompt, type **set**, and then press **Enter**.
2. Write down the value that appears for TEMP.
3. Check the disk space for the volume that is specified for TEMP.
4. If the volume does not contain enough disk space, in a command prompt, type the following command to change the volume and directory:

   ```
   set temp=<volume>.\<directory path>
   ```

5. Press **Enter**.

Installing the management server

The management server coordinates events from agents, and provides database access to the DCS:SA Java console. The management server secures communication with other components by using SSL to encrypt the communication channel.

You must log on to an Administrator account to install the management server.

About installation types and settings

When installing the management server, you can install the following installation types:

- Evaluation installation that runs SQL Server 2012 Express on the local system
  You can install an evaluation installation of SQL Server 2012 Express. The CD installs the server and database automatically.

- Evaluation installation that uses existing MS SQL instance
  You can install an evaluation installation on SQL Server. The SQL Server instance must exist and be running before you perform the installation. The SQL Server can be local or remote.

- Production installation with Tomcat and database schema
  You can install a production installation that installs Tomcat and creates the database schema. This option installs on SQL Server. The SQL Server instance must exist and be running before you perform the installation. The SQL Server can be local or remote.
- Tomcat component only
  You can install a production installation that only installs the Tomcat component, and points to a remote database. This option requires that you provide the file paths to the following files from an installed management server:
  - server.xml
  - server-cert.ssl
  - server-console-cert.ssl
  - cacerts
  - agent-cert.ssl

**Warning:** The management server installation makes network connections to populate both the evaluation and production databases. For local installations, these connections are internal. Quite often, host-based firewalls either block these connections or display messages that prompt you to decide whether to allow the connections. In both situations, the connections time out and the database is not set up correctly.

Before starting the management server installation, do one of the following:
- Permit all programs to initiate connections on port 1433 or your site-specific SQL Server port. Several programs connect to the database during the installation process.
- Disable all host-based firewalls on the management server computer and on the database server if it is on a remote computer. You can enable the firewalls after installation completes.

**Installing the DCS:SA management server into a database instance previously used for SCSP**

If you install DCS:SA management server into an existing SQL Server (or SQL Server 2012 Express) instance that contained a previous SCSP server database, you must clean the previous SCSP database and user accounts from the instance.

Once you have cleaned up the database from the previous installation, you can install the new management server. If you fail to clean up the database from the previous installation, you get a Database Population Failed error during the new installation.
To clean up the previous database using the SQL Server Enterprise Manager

1. Drop the SCSP database.

2. Select the Security folder of the instance, click **Logins**, select the SCSP user accounts, and then right-click **Delete**.

   You must delete the following accounts:
   - scsp_ops
   - scsp_guest
   - scsp_plugin
   - scspdba

**Management server installation settings and options**

Installation prompts you to enter a series of values consisting of port numbers, user names, passwords, and so forth. Each database that you can install uses different default settings and options for the management server and database. Also, some settings for evaluation installation are hard-coded, while the same settings for production are variables that you can change. For example, the database name scspdb is hard-coded for evaluation installation, but is a variable that you can change for production installation.

The following table describes the management server installation settings and options.

**Table 5-2** Management server installation settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default/options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation type</td>
<td>Evaluation Installation, Install SQL Server 2012 Express on the local system</td>
<td>Select the type of installation. If you install a database on SQL Server, the instance must be running.</td>
</tr>
<tr>
<td></td>
<td>You have the following options: Evaluation installation:</td>
<td>The Install Tomcat Component Only option requires that you provide the file path to the following files from an installed management server:</td>
</tr>
<tr>
<td></td>
<td>- Install SQL Server 2012 Express on the local system</td>
<td>- server.xml</td>
</tr>
<tr>
<td></td>
<td>- Use an existing MS SQL instance</td>
<td>- server-cert.ssl</td>
</tr>
<tr>
<td></td>
<td>Production installation:</td>
<td>- server-console-cert.ssl</td>
</tr>
<tr>
<td></td>
<td>- Install Tomcat and create the database schema</td>
<td>- cacerts</td>
</tr>
<tr>
<td></td>
<td>- Install Tomcat Component ONLY</td>
<td>- agent-cert.ssl</td>
</tr>
</tbody>
</table>

### Table 5-2  
Management server installation settings *(continued)*

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default/options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Folder</td>
<td>C:\Program Files\Symantec\Data Center Security Server\Server</td>
<td>The directory location for the management server.</td>
</tr>
</tbody>
</table>
| Agent port                    | 443                                                 | The port that is used to communicate with the agent.  
If you install on a computer that runs a Web server, you must either stop the Web server from running permanently, or enter a different port number.  
This number maps to the Agent Port number that is used when installing the agent.  
See “About the installation settings and options” on page 83.  
See “About port mapping” on page 61. |
| Console port                  | 4443                                                | The port that is used to communicate with the Java console.  
This number maps to the Port number that is used when configuring the Java console.  
See “Configuring the Java console” on page 79.  
See “About port mapping” on page 61. |
| Web server shutdown port      | 8006                                                | The port that is used to shut down the management server. |
Table 5-2  Management server installation settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default/options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web server administration port</td>
<td>8081</td>
<td>The port that is used to administer the management server. This number maps to the Admin Port number that is used when configuring the Java console. See “Configuring the Java console” on page 79. See “About port mapping” on page 61.</td>
</tr>
<tr>
<td>SQL Server 2012 Express Install Path</td>
<td></td>
<td>The directory in which to install the SQL Server 2012 Express server. You have the following options: SQL Eval: NA, SQL Prod: NA.</td>
</tr>
<tr>
<td>SQL Server 2012 Express Data Path</td>
<td></td>
<td>The directory in which to install the SQL Server 2012 Express database. You have the following options: SQL Eval: NA, SQL Prod: NA.</td>
</tr>
</tbody>
</table>
### Table 5-2  Management server installation settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default/options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service user name</td>
<td>LocalSystem</td>
<td>The account that is used to start the management server services. For a SQL Production installation, you can specify a different account that exists on the computer. This account must have administrator privileges. Enter the account using <code>&lt;domain&gt;\&lt;username&gt;</code> format.</td>
</tr>
<tr>
<td></td>
<td>You have the following options:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ SQL Eval: hard-coded</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ SQL Prod: variable</td>
<td></td>
</tr>
<tr>
<td>Host name</td>
<td>Current host IP address</td>
<td>The IP address or fully qualified host name of the computer on which you install the SQL database.</td>
</tr>
<tr>
<td></td>
<td>You have the following options:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ SQL Eval: variable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ SQL Prod: variable</td>
<td></td>
</tr>
<tr>
<td>Database Instance</td>
<td>SCSP</td>
<td>The name of the SQL Server instance. The instance must be running.</td>
</tr>
<tr>
<td></td>
<td>You have the following options:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ SQL Eval: variable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ SQL Prod: variable</td>
<td></td>
</tr>
<tr>
<td>sa Username</td>
<td>sa</td>
<td>The user name for the SQL Server built-in <code>sa</code> account. You can accept the default and proceed with the normal installation, or you can specify the password for a privileged user account.</td>
</tr>
<tr>
<td></td>
<td>You have the following options:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ SQL Eval: variable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ SQL Prod: variable</td>
<td></td>
</tr>
<tr>
<td>Setting</td>
<td>Default/options</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>sa password</td>
<td>none</td>
<td>The password that is associated with the database sa account. The password must conform to the following password policy:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Must not contain the account name of the user.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Must be at least eight characters long. The maximum length is 128 characters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Must contain characters from three of the following four categories:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Latin uppercase letters (A through Z)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Latin lowercase letters (a through z)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Base 10 digits (0 through 9)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Must contain at least one of the following non-alphanumeric characters:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Exclamation mark (!)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Dollar sign ($)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Number sign (#)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Percent sign (%)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you install a SQL database, you must type the same sa password that is used on the SQL Server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You have the following options:</td>
</tr>
<tr>
<td></td>
<td>SQL Eval: Must match existing password</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SQL Prod: Must match existing password</td>
<td></td>
</tr>
<tr>
<td>Database name</td>
<td>SCSPDB</td>
<td>The name of the SQL Server instance.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you install to a production database, the instance name must exist.</td>
</tr>
<tr>
<td>Enable Unicode Storage</td>
<td>enabled</td>
<td>This option is used by production installation, install Tomcat and create the database schema. The option is for use with international operating systems.</td>
</tr>
</tbody>
</table>
### Table 5-2 Management server installation settings *(continued)*

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default/options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDCSS Database Owner user name</td>
<td>scspdba</td>
<td>The name of the account that is used to administer the database.</td>
</tr>
<tr>
<td></td>
<td>You have the following options:</td>
<td>The installation creates this account and password.</td>
</tr>
<tr>
<td></td>
<td>■ SQL Eval: hard-coded</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ SQL Prod: variable</td>
<td></td>
</tr>
<tr>
<td>SDCSS Database Owner user password</td>
<td>none</td>
<td>The password that is associated with the database owner user account, which is used for installations and upgrades.</td>
</tr>
<tr>
<td></td>
<td>You have the following options:</td>
<td>The password must conform to the following password policy:</td>
</tr>
<tr>
<td></td>
<td>■ SQL Eval: hard-coded to the sa password that you type</td>
<td>■ Must not contain the account name of the user.</td>
</tr>
<tr>
<td></td>
<td>■ SQL Prod: variable</td>
<td>■ Must be at least eight characters long. The maximum length is 128 characters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Must contain characters from three of the following four categories:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Latin uppercase letters (A through Z)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Latin lowercase letters (a through z)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Base 10 digits (0 through 9)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Must contain at least one of the following non-alphanumeric characters:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Exclamation mark (!)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Dollar sign ($)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Number sign (#)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Percent sign (%)</td>
</tr>
<tr>
<td>SDCSS Database Guest user name</td>
<td>scspdba</td>
<td>The name of the account that is used to access the database with read-only guest privileges.</td>
</tr>
<tr>
<td></td>
<td>You have the following options:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ SQL Eval: NA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ SQL Prod: variable</td>
<td></td>
</tr>
<tr>
<td>Setting</td>
<td>Default/options</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SDCSS Database Guest user password</td>
<td>none</td>
<td>The password that is associated with the database guest user account.</td>
</tr>
<tr>
<td></td>
<td>You have the following options:</td>
<td>The password must conform to the following password policy:</td>
</tr>
<tr>
<td></td>
<td>■ SQLEval: NA</td>
<td>■ Must not contain the account name of the user.</td>
</tr>
<tr>
<td></td>
<td>■ SQL Prod: variable</td>
<td>■ Must be at least eight characters long. The maximum length is 128 characters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Must contain characters from three of the following four categories:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Latin uppercase letters (A through Z)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Latin lowercase letters (a through z)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Base 10 digits (0 through 9)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Must contain at least one of the following non-alphanumeric characters:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Exclamation mark (!)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Dollar sign ($)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Number sign (#)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Percent sign (%)</td>
</tr>
</tbody>
</table>

**Installing evaluation installation that runs SQL Server 2012 Express on the local system**

The evaluation installation option installs a management server that runs a local SQL Server 2012 Express evaluation database.

Before performing the installation, you should note the following:

- The management server installation installs the server and database automatically.
- During the management server installation, you must create and enter a password that will be associated with the database sa account.
To install evaluation installation that runs SQL Server 2012 Express on the local system

1. Insert and display the installation CD, and then double-click `server.exe`.
2. In the **Welcome** panel, click **Next**.
3. In the **License Agreement** panel, select **I accept the terms in the license agreement**, and then click **Next**.
4. In the **Installation Type** panel, click **Evaluation Installation**, click **Install SQL Server 2012 Express on the Local System**, and then click **Next**.
5. In the **Destination Folder** panel, change the folder if necessary, and then click **Next**.
   
The directory name must contain printable ASCII characters only. Multi-byte, double-byte, hi-ASCII, and non-printable ASCII characters are not supported.
6. In the **Server Configuration** panel, accept or type new port values, and then click **Next**.
   
   If you enter port numbers that are in use, error messages appear until you enter port numbers that are not in use.
7. In the **Database Selection** panel, in the Password and Confirm Password boxes, type the password that will be associated with the database sa account, type the password again to confirm, and then click **Next**.
   
   The directory name must contain printable ASCII characters only. Multi-byte, double-byte, hi-ASCII, and non-printable ASCII characters are not supported.
8. In the **Ready to Install the Program** panel, click **Install**.
9. When the **InstallShield Wizard Completed** panel appears, click **Finish**.

**Installing evaluation installation using existing MS SQL instance**

This evaluation installation option installs the management server with a local or remote evaluation database on SQL Server.

Before performing the installation, you should note the following:

- Your SQL Server instance must exist and be running before you start the installation.
- The sa account must already exist and you must provide the accurate password for the sa account during the management server installation.
To install evaluation installation that uses existing MS SQL instance

1. Insert and display the installation CD, and then double-click `server.exe`.
2. In the **Welcome** panel, click **Next**.
3. In the **License Agreement** panel, select **I accept the terms in the license agreement**, and then click **Next**.
4. In the **Installation Type** panel, click **Evaluation Installation**, then click **Use an Existing MS SQL Instance**, and then click **Next**.
5. In the **Destination Folder** panel, change the folder if necessary, and then click **Next**.

   The directory name must contain printable ASCII characters only. Multi-byte, double-byte, hi-ASCII, and non-printable ASCII characters are not supported.
6. In the **Server Configuration** panel, accept or type new port values, and then click **Next**.

   If you enter port numbers that are in use, error messages appear until you enter port numbers that are not in use.
7. In the **Database Selection** panel, specify the database parameters, and then click **Next**.

   | Host Name | Type the IP address or fully qualified domain name of the SQL Server. |
   | Database Instance | Type the name of the existing SQL Server instance on which you want to install the database. |
   | sa Privileged User | Accept or change the sa user name. |
   | Password | Type the same password that is used on the SQL Server, type the password again to confirm. |
8. In the **Ready to Install the Program** panel, click **Install**.
9. When the **InstallShield Wizard Completed** panel appears, click **Finish**.

**Installing production installation with Tomcat and database schema**

The production installation option installs Tomcat and creates the database schema. The option installs the management server with a local or remote production database on SQL Server.

Before performing the installation, you should note the following:
Your SQL Server instance must exist and be running before you start the installation.

The sa account must already exist and you must provide the accurate password for the sa account during the management server installation.

All other accounts (owner, guest, and internal accounts) must not exist in the instance. The management server installation creates these accounts and aborts if it cannot create them.

The database name that you enter into the management server installation must not exist in the instance. The management server installation creates these accounts and aborts if it cannot create them.

To install production installation with Tomcat and database schema

1. Insert and display the installation CD, and then double-click server.exe.
2. In the Welcome panel, click Next.
3. In the License Agreement panel, select I accept the terms in the license agreement, and then click Next.
4. In the Installation Type panel, click Production Installation, click Install Tomcat component ONLY, and then click Next.
5. In the Destination Folder panel, change the folder if necessary, and then click Next.
   
   The directory name must contain printable ASCII characters only. Multi-byte, double-byte, hi-ASCII, and non-printable ASCII characters are not supported.
6. In the Server Configuration panel, accept or type new port values, and then click Next.
   
   If you enter port numbers that are in use, error messages appear until you enter port numbers that are not in use.
7. In the Service User Configuration panel, do one of the following:
   
   Click Use Local System Account, and then click Next.
   
   Click Use an alternate Account, type a user name in the Username box using <domain>\<username> format, type the same password in the Password and Confirm Password boxes, and then click Next.
8 In the **Database Selection** panel, specify the database parameters, and then click **Next**.

- **Host Name**: Type the IP address or fully qualified domain name of the SQL Server.
- **Database Instance**: Type the name of the existing SQL Server instance on which you want to install the database.
- **sa Privileged User**: Accept or change the sa user name.
- **Password**
- **Confirm Password**: Type the same password that is used on the SQL Server, type the password again to confirm.

9 In the **Database Configuration** panel, specify the database parameters, and then click **Next**.

- **Database Name**: Type the name of the database to install.
- **Enable Unicode Storage**: The option is for use with international operating systems.
- **SDCSS Database Owner**: Under SDCSS Database Owner, do the following:
  - In the User name box, type the name of the SDCSS Database Owner.
  - In the Password and Confirm Password boxes, type the password that is associated with the SDCSS Database Owner, and then type the password again to confirm.
- **SDCSS Database Guest User**: To create an SDCSS database guest user, do the following under SDCSS Database Guest User:
  - Select **Create a Guest User**.
  - In the User name box, type the guest User name.
  - In the Password and Confirm Password boxes, type the password that is associated with the SDCSS Database Guest User, and then type the password again to confirm.

10 In the **Ready to Install the Program** panel, click **Install**.

11 When the **InstallShield Wizard Completed** panel appears, click **Finish**.

**Installing Tomcat component only**

The production installation option installs only Tomcat component. You can use this option to point multiple Tomcat servers to a single management server database.
on a dedicated system. The Tomcat only option is useful if you want to create a set of identical Tomcat servers for load balancing or failover.

The Tomcat only option requires that you provide the file path to the following files from an installed management server:

- server.xml
- server-cert.ssl
- server-console-cert.ssl
- cacerts
- agent-cert.ssl

By default, these files are located in the following management server installation directory:

```
C:\Program Files\Symantec\Data Center Security Server\Server
```

You should do the following changes in the server.xml as mentioned below:

- If the primary server is installed on 32-bit operating system and the secondary server is installed on 64-bit operating system or vice-versa, then you should modify the keystore File path for server-cert.ssl file in server.xml on Tomcat-only server.

  On 32-bit operating system, the keystore File path is `C:\Program Files\Symantec\Data Center Security Server\Server\server-cert.ssl` and on 64-bit operating system, the keystore File path is `C:\Program Files(x86)\Symantec\Data Center Security Server\Server\server-cert.ssl`.

- If either of the original management server or the tomcat-only server are installed in a non-standard location, you must also modify the keystore location in the server.xml file to refer the correct location on the tomcat-only server.

- The URL for resources Database-Console and Database-Agent cannot contain localhost or 127.0.0.1 in the server.xml file on Tomcat-only server. You must use the IP address or the host name of the primary server.

---

**Note:** If the management server database is on a Tomcat system instead of a dedicated system, you must specify the real IP (not localhost) for the initial installation.

---

**To install Tomcat component only**

1. Insert and display the installation CD, and then double-click `server.exe`.
2. In the **Welcome** panel, click **Next**.
3 In the License Agreement panel, select I accept the terms in the license agreement, and then click Next.

4 In the Installation Type panel, click Production Installation, click Install Tomcat component ONLY, and then click Next.

5 In the Installation Type panel, specify the file paths to server.xml, server-cert.ssl, server-console-cert.ssl, cacerts, and agent-cert.ssl from an installed management server, and then click Next.

6 In the Destination Folder panel, change the folder if necessary, and then click Next.

   The directory name must contain printable ASCII characters only. Multi-byte, double-byte, hi-ASCII, and non-printable ASCII characters are not supported.

7 In the Service User Configuration panel, do one of the following:

   Click Use Local System Account, and then click Next.

   Click Use an alternate Account, type a user name in the Username box using <domain>|<username> format, type the same password in the Password boxes, and then click Next.

8 In the Ready to Install the Program panel, click Install.

9 When the InstallShield Wizard Completed panel appears, click Finish.

Installing and configuring the Java console

After installation, you must configure the Java console before you can use it.

You must log on to an Administrator account to install the Java console.

Installing the Java console

By default the Java console is installed in the following directory:

C:\Program Files\Symantec\Data Center Security Server\Console

The Java console installation does not prompt you to enter port numbers or server names. You enter this information after installation.

To install the Java console

1 On the installation CD, double-click console.exe.

2 In the Initial installation panel, click Next.

3 In the License Agreement panel, select I accept the terms in the license agreement, and then click Next.
4 In the **Destination Folder** panel, change the folder if necessary, and then click **Next**.

The installation directory name must contain printable ASCII characters only. Multi-byte, double-byte, hi-ASCII, and non-printable ASCII characters are not supported.

5 In the **Ready to Install the Program** panel, click **Install**.

6 When the **InstallShield Wizard Completed** panel appears, click **Finish**.

**Configuring the Java console**

Configuration prompts you to enter a series of values consisting of port numbers, passwords, and a server name. In a few instances, the port numbers must match the port numbers that were specified during the management server installation.

The following table describes the Java console configuration settings and options.

<table>
<thead>
<tr>
<th>Table 5-3</th>
<th>The Java console configuration settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting</td>
<td>Default</td>
</tr>
<tr>
<td>Server name</td>
<td>Localhost Server</td>
</tr>
<tr>
<td>Host</td>
<td>local host</td>
</tr>
</tbody>
</table>
Table 5-3  The Java console configuration settings *(continued)*

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
</table>
| Port      | 4443    | The Console Port number that was used during management server installation.  
See “Management server installation settings and options” on page 66.  
See “About port mapping” on page 61. |
| Admin port| 8081    | The Web server Administration Port number that was used during management server installation.  
See “Management server installation settings and options” on page 66.  
See “About port mapping” on page 61. |
Table 5-3  The Java console configuration settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
</table>
| Use encrypted communications     | Enabled | Check **Use encrypted communications** to use Secure Sockets Layer (SSL) X.509 certificate-based channel encryption for DCS:SA.  
                                |         | SSL X.509 certificate-based channel encryption secures communication between the Java console and the management server, and between the agent and the management server.  
                                |         | If you feel that your system provides adequate firewall security and you do not want to use SSL X.509 certificate-based channel encryption for DCS:SA, uncheck **Use encrypted communications**. After you uncheck **Use encrypted communications**, you must edit the server.xml file, found on the management server, in the `<Server_Install_Root>/tomcat/conf` directory.  
                                |         | Refer to the DCS:SA Administrator's Guide for instructions on editing the server.xml.  |
| Password                         | none    | The password that is associated with the symadmin user name, which you create the first time you start the Java console.  |
To configure the Java console

1. Click **Start > Programs > Symantec Data Center Security Server > Management Console**.

2. In the **Login** window, click the green plus sign icon.

3. In the **New Server Configuration** panel, replace New Server with the name that you want to use to identify your server.

4. In the **New Server Configuration** panel, specify the server configuration parameters, and then click **OK**.

5. In the **Login** window, type symadmin in the **Username** box, select the new server that you added, and then click **Login**.

6. In the **Verify Server Certificate** panel, select **Always accept this certificate**, and then click **OK**.

7. In the **Set Password** panel, in the **Password** and **Confirm Password** boxes, type the password to associate with the symadmin user name, type the password again to confirm.

---

**Installing a Windows agent**

The DCS:SA agent enforces policy on the endpoints. Each agent enforces rules that are expressed in policies, thereby controlling and monitoring application (process) and user behavior.

You must log on to an Administrator account to install a Windows agent.

---

**Note:** Windows agents must be restarted after installation or upgrade.

---

**About the SSL certificate file**

The Windows agent installation requires access to a copy of the SSL certificate file that was created during management server installation. The certificate file is named Agent-cert.ssl, and is located in the management server installation directory. The default management server installation directory is as follows:

C:\Program Files\Symantec\Data Center Security Server\Server

To place the certificate on a computer that does not run the management server, do the following:

- On the management server that will be used to manage the agent, locate the server installation directory and copy Agent-cert.ssl to removable media. Optionally, you can copy the file from mapped network drives or network shares.
On the computer on which the agent will be installed, create a directory and then copy Agent-cert.ssl into the directory. The directory path name cannot contain spaces.

About the installation settings and options
Installation prompts you to enter a series of Windows agent values consisting of port numbers, management server name, and so forth.

Note: The agent does not support IP aliases. If your network card is bound to more than one IP address, the agent uses the first IP address on the network card.

The following table describes the Windows agent installation settings and options.

Table 5-4 Windows agent installation settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation Directory</td>
<td>C:\Program Files\Symantec\Data Center Security Server\Agent</td>
<td>The installation directory for the agent.</td>
</tr>
<tr>
<td>Logs File Directory</td>
<td>C:\Program Files\Symantec\Data Center Security Server\Agent</td>
<td>The installation directory prefix for the &lt;prefix dir&gt;/sdcsslog subdirectory. The installation creates an sdcsslog folder under the folder that you specify. The directory name will remain scsplog if you are upgrading an existing SCSP agent to an DCS:SA agent.</td>
</tr>
<tr>
<td>Agent Name</td>
<td>Host name of agent computer</td>
<td>The agent name. After installation, you can change the agent name by using the Java console.</td>
</tr>
<tr>
<td>Polling Interval</td>
<td>300 seconds</td>
<td>The interval that the agent uses to poll the management server for policy and configuration updates.</td>
</tr>
<tr>
<td>Setting</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable Intrusion Prevention</td>
<td>Enabled</td>
<td>Indicates whether to enable intrusion prevention. When enabled, the prevention features of DCS:SA are enabled for the agent. The IPS drivers are loaded on the agent computer, and the agent accepts prevention policies from the Java console. If you disable intrusion prevention and want to enable it in the future, you must run the sisipsconfig.exe tool in the \Agent\IPS\bin directory with the –ipsstate on option, and restart the computer. To disable intrusion prevention, use –ipsstate off option. Symantec strongly recommends that you enable intrusion prevention.</td>
</tr>
</tbody>
</table>
Table 5-4  Windows agent installation settings *(continued)*

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Real-time Notification</td>
<td>Enabled</td>
<td>Indicates whether to enable real-time notification.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In addition to the polling interval, agents can also use real-time notification to obtain configuration changes. With real-time notification, the management server sends a real-time notification message to an agent as configuration changes occur. Upon receiving the notification, the agent queries the management server for the changes. When real-time notification is disabled, the management server does not send any messages to the agent and relies on the polling interval to update the agent.</td>
</tr>
<tr>
<td>Notification port</td>
<td>2222</td>
<td>The port that is used to receive real-time notifications from the management server. You can change this port after installation by using the Java console to change the agent properties.</td>
</tr>
<tr>
<td>Primary Management Server</td>
<td>localhost</td>
<td>The IP address or fully qualified host name of the management server that will manage the agent.</td>
</tr>
<tr>
<td>Setting</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Agent Port</td>
<td>443</td>
<td>The Agent Port number that was used during management server installation. Refer to the SymHelp for more information about Management server installation settings and options and About port mapping. See “Management server installation settings and options” on page 66. See “About port mapping” on page 61.</td>
</tr>
<tr>
<td>Alternate Management Servers</td>
<td>none</td>
<td>An ordered list of optional alternate management servers used for failover. For each alternate management server, specify the IP address or fully qualified host name. Specify the servers in a comma-separated list. Refer to the SymHelp for more information regarding About simple failover. See “About simple failover” on page 35.</td>
</tr>
<tr>
<td>Setting</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Management Server Certificate</td>
<td>none</td>
<td>The directory location of the SSL certificate file, Agent-cert.ssl. The installation requires access to a copy of the SSL certificate file that was created during management server installation. The file is located in the management server installation directory. All primary and alternate management servers must use the same certificate file. Refer to the SymHelp for more information regarding <em>About the SSL certificate file</em>. See “<em>About the SSL certificate file</em>” on page 82.</td>
</tr>
<tr>
<td>Common Configuration Group</td>
<td>none</td>
<td>The name of an existing common configuration group for this agent to join. An agent is placed in the default common configuration group (named Common Configuration), unless you specify another configuration group that already exists in the Java console. After installation, you can change the group assignment by using the Java console.</td>
</tr>
</tbody>
</table>
Table 5-4  Windows agent installation settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
</table>
| Prevention Configuration Group| none    | The name of an existing prevention configuration group for this agent to join.  
An agent is placed in the default prevention configuration group (named Configuration), unless you specify another configuration group that already exists in the Java console.  
After installation, you can change the group assignment by using the Java console. |
| Prevention Policy Group      | none    | The name of an existing prevention policy group for this agent to join.  
An agent is placed in the default prevention policy group (named Policy), unless you specify another policy group that already exists in the Java console.  
After installation, you can change the group assignment by using the Java console. |
| Detection Configuration Group| none    | The name of an existing detection configuration group for this agent to join.  
An agent is placed in the default detection configuration group (named Configuration), unless you specify another configuration group that already exists in the Java console.  
After installation, you can change the group assignment by using the Java console. |
Table 5-4  Windows agent installation settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection Policy Group</td>
<td>Windows</td>
<td>The name of an existing detection policy group for this agent to join. You can specify multiple groups using commas between the group names.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You may optionally include the name of an existing detection policy domain in the group path/name. You may include the domain name with or without the group name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>An agent is placed in the default Policy/Windows detection policy group, unless you specify another policy group that already exists in the Java console.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>After installation, you can change the group assignment by using the Java console.</td>
</tr>
</tbody>
</table>

Installing the Windows agent software

The installation CD contains the following executable for installing the agent software:

agent.exe Use agent.exe to install the agent software on computers that run supported Windows operating systems.

To install the Windows agent software

1. On the installation CD, double-click **agent.exe**.
2. In the **Welcome** panel, click **Next**.
3. In the **License Agreement** panel, select **I accept the terms in the license agreement**, and then click **Next**.
4. In the **Destination Folder** panel, change the folders if necessary, and then click **Next**.
5 In the **Agent Configuration** panel, accept or change the default settings, and then click **Next**.

Ensure that **Enable Intrusion Prevention** is checked.

6 In the **Management Server Configuration** panel, in the Primary Management Server box, type the fully qualified host name or IP address of the primary server that is used to manage this agent.

If you changed the Agent Port setting during management server installation, in the Agent Port box, type a port number that matches.

7 (Optional) In the **Management Server Configuration** panel, in the Alternate Management Servers box, type the fully qualified host name or IP address of the alternate servers that are used for failover for this agent.

Type the servers in a comma-separated list.

8 In the **Management Server Configuration** panel, accept the directory for the SSL certificate Agent-cert.ssl, or click **Browse** to browse to and locate Agent-cert.ssl.

Access to a copy of the SSL certificate Agent-cert.ssl is required to connect to the management server. All primary and alternate management servers must use the same certificate.

9 In the **Management Server Configuration** panel, click **Next**.

10 (Optional) In the **Agent Group Configuration** panel, in the group boxes, type the group names that you created with the Java console.

You may add multiple detection policy group names separated with commas. You may include the name of an existing detection policy domain in the group path/name.

11 In the **Agent Group Configuration** panel, click **Next**.

12 In the **Service User Configuration** panel, accept the default LocalSystem account, and then click **Next**.

13 In the **Ready to Install the Program** panel, confirm the installation parameters, and then click **Install**.

14 When the installation completes, click **Finish**.

A message displays if the intrusion prevention driver requires a restart.

---

**Silent installation of agent**

You must log on with administrator privileges to install a Windows agent.
You can perform a silent installation of Windows agent by using the agent.exe executable and InstallShield and Windows Installer commands. The following command structure shows the sequencing:

```
agent.exe <InstallShield commands> "<Windows Installer commands> <installation properties>
```

The following examples show a command string:

```
agent.exe /s /v"MANAGEMENT_SERVER=192.168.1.103
SSL_CERT_FILE=c:\Agent-cert.ssl
-l*v+! %temp%\SISAgentSetup.log /qn"
```

You create command strings by using the following:

- InstallShield commands
- Microsoft Windows Installer commands
- Installation properties

**Note:** Copying and pasting command lines into the command window can result in silent installation failure. If you copy and paste command lines into the command window, make sure that there are no line breaks or spaces in between command lines.

### Displaying InstallShield commands

For a list of InstallShield commands, you can display Help for the agent installation command. The important commands are /s, which suppresses the initialization dialog, and /v, which specifies that the values that follow are Windows Installer commands.

**Note:** You must enclose the command string that follows /v in quotations.

**To display InstallShield commands**

1. Insert the installation CD into your computer.
2. Display a command prompt, and navigate to the agent installation directory.
3. Type and run the following command:

   ```
   agent.exe ?
   ```
Microsoft Windows Installer commands

Refer to the Microsoft documentation for information about standard Microsoft Windows Installer commands and additional logging levels.

The following table describes the optional basic commands that are used for installations.

Table 5-5 Optional Installer commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/qn</td>
<td>none</td>
<td>Install silently</td>
</tr>
<tr>
<td>-l*v+! &lt;log filename&gt;</td>
<td>none</td>
<td>Log all events except for the v argument (*), create a verbose log file (v), append to the existing log file (+), flush each line to the log (!), to a file named &lt;log filename&gt; that either exists or is created. If the path includes spaces, use quotation marks.</td>
</tr>
<tr>
<td>INSTALLDIR=&lt;path&gt;</td>
<td>C:\Program Files\Symantec\Data Center Security Server\Agent</td>
<td>Designate a custom path on the target computer where &lt;path&gt; is the specified target directory. If the path includes spaces, use quotation marks. Escape the internal quotation marks, as in the following example: agent.exe /s /v&quot;INSTALLDIR=&quot;E:\Program Files...Symantec\System Critical Protection\Agent&quot; -l*v+! c:\agent-install.log /qn&quot;</td>
</tr>
</tbody>
</table>
Table 5-5  Optional Installer commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
</table>
| REBOOT=<val> | Based on operating system | Whether or not to restart a computer after installation, where <val> is a valid argument. If REBOOT=<val> is not specified in the command line, the computer will not reboot. Valid arguments are as follows:  
  - Force (prompts for restart)  
  - Suppress (prevents most restarts)  
  - ReallySuppress (prevents all restarts as part of the installation process) |

Installation properties

The following table describes the Windows agent installation settings and options.

Table 5-6  Windows agent installation settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MANAGEMENT_SERVER=&lt;val&gt;</td>
<td>localhost</td>
<td>The IP address or fully qualified host name of the management server that will manage the agent. Required</td>
</tr>
<tr>
<td>ALT_MANAGEMENT_SERVERS=&lt;server1, server2,...&gt;</td>
<td>none</td>
<td>An ordered list of alternate management servers for failover. For each alternate management server, specify the IP address or fully qualified host name. Specify the servers in a comma-separated list. Optional See “About simple failover” on page 35.</td>
</tr>
<tr>
<td>PROTOCOL=&lt;val&gt;</td>
<td>https</td>
<td>Select https or http communications.</td>
</tr>
</tbody>
</table>
Table 5-6  Windows agent installation settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL_CERT_FILE=&lt;val&gt;</td>
<td>none</td>
<td>The directory location of the SSL certificate file, Agent-cert.ssl. Example: C:\Agent\Agent-cert.ssl See “About the SSL certificate file” on page 82. Optional</td>
</tr>
<tr>
<td>ENABLE_BYPASS_CHECKS</td>
<td>none</td>
<td>Indicates whether to enable the bypass prerequisite checks feature. To enable, set the variable to a nonzero value. Optional</td>
</tr>
<tr>
<td>NOTIFICATION_ENABLE=&lt;val&gt;</td>
<td>True</td>
<td>Indicates whether to enable notification, where &lt;val&gt; is a valid argument (True, False). Optional</td>
</tr>
<tr>
<td>AGENT_NAME=&lt;name&gt;</td>
<td>Host name of agent computer</td>
<td>The agent name. After installation, you can modify the agent name by using the Java console. Optional</td>
</tr>
<tr>
<td>AGENT_PORT=&lt;val&gt;</td>
<td>443</td>
<td>The Agent Port number that is used during management server installation. See “Management server installation settings and options” on page 66. See “About port mapping” on page 61. Optional</td>
</tr>
<tr>
<td>LOG_DIR=&lt;val&gt;</td>
<td>C:\Program Files\Symantec\Data Center Security Server\Agent</td>
<td>The installation directory prefix for the &lt;prefix dir&gt;/sdcsslog subdirectory. Optional The directory name will remain scsplog if you are upgrading an existing SCSP agent to an DCS:SA agent.</td>
</tr>
<tr>
<td>POLLING_INTERVAL=&lt;val&gt;</td>
<td>300 seconds</td>
<td>The interval that the agent uses to poll the management server for policy and configuration updates. Optional</td>
</tr>
</tbody>
</table>
### Table 5-6  Windows agent installation settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPS_ENABLE=&lt;val&gt;</td>
<td>True</td>
<td>The switch for enabling or disabling intrusion prevention, where &lt;val&gt; is a valid argument (True, False). Optional When enabled, the prevention features of DCS:SA are enabled for the agent. The IPS drivers are loaded on the agent computer, and the agent accepts prevention policies from the Java console. If you disable intrusion prevention and want to enable it in the future, you must run the sisipsconfig.exe tool in the \Agent\IPS\bin directory with the -ipsstate on option, and restart the computer. Symantec strongly recommends that you enable intrusion prevention. When you upgrade DCS:SA with IPS enabled, IPS continues to be enabled. You must manually disable IPS by using the following command: sisipsconfig.exe -ipsstate off</td>
</tr>
<tr>
<td>NOTIFICATION_PORT=&lt;val&gt;</td>
<td>2222</td>
<td>The port that is used to receive broadcast alerts from the management server, where &lt;val&gt; is a valid port number. This property is only used when NOTIFICATION_ENABLE is True. Optional</td>
</tr>
<tr>
<td>COMMON_CONFIG_GROUP=&lt;val&gt;</td>
<td>Common Configuration</td>
<td>The name of an existing common configuration group for this agent to join. An agent is placed in the default common configuration group, unless you specify another configuration group that already exists in the Java console. After installation, you can change the group assignment by using the Java console. Optional</td>
</tr>
<tr>
<td>Setting</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| IPS_CONFIG_GROUP=<val>      | Configuration | The name of an existing prevention configuration group for this agent to join.  
                               |                        | An agent is placed in the default prevention configuration group, unless you specify another configuration group that already exists in the Java console.  
                               |                        | After installation, you can change the group assignment by using the Java console.  
                               |                        | Optional |
| IPS_POLICY_GROUP=<val>     | Policy | The name of an existing prevention policy group for this agent to join.  
                               |                        | An agent is placed in the default prevention policy group, unless you specify another policy group that already exists in the Java console.  
                               |                        | After installation, you can change the group assignment by using the Java console.  
                               |                        | Optional |
| IDS_CONFIG_GROUP=<val>     | Configuration | The name of an existing detection configuration group for this agent to join.  
                               |                        | An agent is placed in the default detection configuration group, unless you specify another configuration group that already exists in the Java console.  
                               |                        | After installation, you can change the group assignment by using the Java console.  
                               |                        | Optional |
Table 5-6  Windows agent installation settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDS_POLICY_GROUP=&lt;val&gt;</td>
<td>Windows</td>
<td>The name of an existing detection policy group for this agent to join. You can specify multiple groups using commas between the group names.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can optionally include the name of an existing detection policy domain in the group path/name. You can include the domain name with or without the group name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>An agent is placed in the default Windows detection policy group in the default Policy domain, unless you specify another domain/policy group that already exists in the Java console.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>After installation, you can change the group assignment by using the Java console.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Optional</td>
</tr>
<tr>
<td>SERVICE_USER=&lt;val&gt;</td>
<td></td>
<td>SERVICE_USER is the account that registers services for the agent. If you change the default of LocalSystem, use the format &lt;domain&gt;&lt;user name&gt;.</td>
</tr>
<tr>
<td>SERVICE_PW=&lt;val&gt;</td>
<td>LocalSystem</td>
<td>SERVICE_PW is the password for SERVICE_USER.</td>
</tr>
<tr>
<td>SERVICE_CONFPW=&lt;val&gt;</td>
<td>none</td>
<td>SERVICE_CONFPW is the confirmation of the password for SERVICE_USER.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: If you use any of these properties, you must use all three properties.</td>
</tr>
</tbody>
</table>

Uninstalling DCS:SA

To uninstall DCS:SA, you need to uninstall each component separately. You can uninstall the components in any order. If the agent runs on a computer that also runs the management server or Java console, disable policy prevention on the agent by setting the Null policy or by using the policy override tool.

Uninstalling an agent using Add or Remove Programs

Agent uninstallation uses the Windows Add or Remove Programs utility.

If the agent enforces policy prevention, it prevents you from removing agent-related files, the management server, and Java console. If a service user account was created during installation, the account is not removed during uninstallation.

Use one of the following methods to disable policy prevention on the agent:
Start the Java console, and set the policy for the target agent to the Null prevention policy (sym_win_null_sbp).

If the policy on the computer that runs the agent is not Null and permits policy override, use the policy override tool to disable policy prevention. Refer to the Symantec Data Center Security: Server Advanced Agent Guide.

To uninstall an agent

1. Disable policy prevention on the agent computer.
2. On the computer that runs the agent, click Start > Settings > Control Panel > Add/Remove Programs.
3. Click Symantec Data Center Security Server Agent, and then click Remove.
4. Follow and complete the prompts until uninstallation completes.
5. Restart the agent computer.

Silent uninstallation of an agent

You can perform a silent uninstallation of an agent by using the agent.exe executable and InstallShield and Windows Installer commands.

The following command structure shows the sequencing:

MsiExec.exe /{<PRODUCT CODE>} /qn /l*v!+ <UNINSTLL LOG FILE>

The <PRODUCT CODE> is the DCS:SA uninstall string necessary for MsiExec.exe. It is in the following directory:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall

For Windows 2008 64-bit system, the <PRODUCT CODE> is in the following directory:

HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

Browse the list of IDs. Locate the DCS:SA agent application by looking at the properties in the right pane. Note the UninstallString string, and copy and modify it. For example:

MsiExec.exe /{3D24482F-98BD-48DD-AA62-8B24BFDE7329} /qn /l*v!+ C:\SISAgentUninstall.log

The system restart is suppressed after the uninstallation.

See “Silent installation of agent” on page 90.

Uninstalling the Java console

Java console uninstallation uses the Windows Add or Remove Programs utility.
If the computer that runs the Java console also runs the agent, use one of the following methods to disable policy prevention on the agent:

- Start the Java console, and set the policy for the target agent to the Null prevention policy (sym_win_null_sbp).
- If the policy on the computer that runs the agent is not Null and permits policy override, use the policy override tool to disable policy prevention. Refer to the *DCS:SA Policy Override Guide*.

To uninstall the Java console and database

1. Disable policy prevention on the agent computer.
2. Click *Start > Settings > Control Panel > Add/Remove Programs*.
3. Click *Symantec Data Center Security Server Console*, and then click *Remove*.
4. Follow and complete the prompts until uninstallation completes.

**Uninstalling the management server and database**

Management server uninstallation uses the Windows Add or Remove Programs utility.

If the computer that runs the management server also runs the agent, disable policy prevention on the agent. The management server may also use SQL Server database to store data.

Use one of the following methods to disable policy prevention on the agent:

- Start the Java console, and set the policy for the target agent to the Null prevention policy (sym_win_null_sbp).
- If the policy on the computer that runs the agent is not Null and permits policy override, use the policy override tool to disable policy prevention. Refer to the *DCS:SA Policy Override Guide*.

To uninstall the management server and database

1. Disable policy prevention on the agent computer.
2. Click *Start > Settings > Control Panel > Add/Remove Programs*.
3. Click *Symantec Data Center Security Server Manager*, and then click *Remove*.
4. Follow and complete the prompts until uninstallation completes.
5 (Optional) Do one of the following:

    If you installed the evaluation database, click *Microsoft SQL Server 2012 Express*, and then click *Remove*.

    If you installed the evaluation or production database on SQL Server, drop the database that you created during installation, which is scspdb by default.

6 Follow and complete the prompts until uninstallation completes.

7 Delete the C:\Program Files\Symantec\Data Center Security Server\Server directory.

8 Delete the file in C:\Program Files\Common Files\Symantec Shared\SDCSS directory.

9 Restart the computer.

Temporarily disabling Windows agents

You can temporarily disable DCS:SA Windows agents.

**Temporarily disabling Windows 2000, Windows Server 2003, or Windows XP Professional agents**

To temporarily disable agents that run on Windows 2000, Windows Server 2003, or Windows XP Professional, you must boot the agent computer in safe mode and then reset the prevention policy to the built-in Null policy.

---

**Warning:** You should perform these procedures only in emergency situations.

To temporarily disable Windows 2000, Windows 2003, or Windows XP agents

1 Boot the agent computer in safe mode.

   Refer to your Microsoft Windows documentation for instructions on booting in safe mode.

2 Reset the prevention policy to the built-in Null policy.

Resetting the prevention policy to the built-in Null policy

Run the sisipsconfig.exe tool with the -r option to reset the prevention policy to the built-in Null policy. On Windows, sisipsconfig.exe is located the following directory:

---

**Note:** To run the agent config tool (sisipsconfig.exe), you must have administrative privilege.
To reset the prevention policy

1. On the agent computer, open a command prompt.
2. At a command prompt, type the following command, and then press Enter:

   ```
   sisipsconfig -r
   ------------------------------
   
   Agent Configuration Tool version 5.0.0.240
   ------------------------------
   
   The agent will now use the built-in policy
   ```
   c:\>

3. Reboot the agent computer, and then start the Java console.

   In the Java console, on the Assets page, the agent is marked with an
   exclamation point (!) to indicate a policy error. When you select the agent, the
   following message appears in the Details pane, on the Policies tab:

   ```
   ! Policy Errors:
   ** Policy error has occurred at 17-Nov-2005 05:55:56 EST
   Driver is using the built-in policy and not the assigned policy.
   ```

4. In the Java console, apply the desired policy to the agent, and then give
   appropriate permissions to the desired programs.

Reinstalling Windows agents

You can perform an unattended reinstall of Windows agents by using the agent.exe
executable and InstallShield and Windows Installer commands. Reinstalling a
Windows agent is useful if an agent becomes corrupted. Reinstalling a Windows
agent is equivalent to uninstalling an agent and then installing the same version of
that agent.

The following examples show a command string:

   ```
   agent.exe /s /v"/qn /l*v!+ %temp%\SISAgentSetup.log"
   ```

See “Silent installation of agent” on page 90.

See “Unattended Windows agent migration” on page 180.
Installing Symantec Data Center Security: Server Advanced components on UNIX

Refer to the following sections before installing the DCS:SA agents:

- See “About installing UNIX agents” on page 102.
- See “Installing an agent in verbose mode” on page 107.
- See “Installing an agent in silent mode” on page 108.
- See “About the incremental rollout of agent installations and policy deployment” on page 58.

About installing UNIX agents

Installation prompts you to enter a series of values.

Please note the following UNIX agent installation requirements:

- UNIX agents do not support IP aliases. If your network card is bound to more than one IP address, the agent uses the first IP address on the network card.
- You must install UNIX agents as root. UNIX agents require root privileges to run.
- Directory path names cannot contain spaces.
- If you transfer UNIX agent installation .bin files from a Windows computer to a UNIX computer using FTP or some other file transport method, you must use binary transfer mode. Otherwise the installation files will be corrupted.
- If you are installing a Solaris, Linux, HP-UX, or AIX agent on a system that supports non-English character sets, the destination directory that you choose for the agent must contain only ASCII characters. If you include any non-ASCII characters in the path, the installation will fail.

The following table describes the agent installation settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation Directory</td>
<td>/opt/Symantec</td>
<td>The Installation directory prefix for the &lt;prefix dir&gt;/sdcssagent subdirectory. The directory path name cannot contain spaces.</td>
</tr>
<tr>
<td>Logs File Directory</td>
<td>/var/log</td>
<td>The installation directory prefix for the &lt;prefix dir&gt;/sdcsslog subdirectory.</td>
</tr>
<tr>
<td>Setting</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>----------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable Real-time File Integrity Monitoring</td>
<td>/opt/Symantec/sdcssagent/IDS/driver</td>
<td>Enables real-time event logging on the agent.</td>
</tr>
<tr>
<td>Protocol</td>
<td>https</td>
<td>Select https or http communications.</td>
</tr>
<tr>
<td>Primary Management Server</td>
<td>127.0.0.1</td>
<td>The IP address or fully qualified host name of the primary management server that will manage the agent.</td>
</tr>
</tbody>
</table>
| Alternate Management Servers        | none                                         | A comma-separated list of alternate management servers. For each alternate management server, specify the IP address or fully qualified host name. Optional  
                                          | See “About simple failover” on page 35.                                                                                                     |
| Management Server Certificate       | /tmp/agent-cert.ssl                           | The directory location of the SSL certificate file, agent-cert.ssl, obtained from the DCS:SA management server installation directory.  
                                          | You must copy this file from the management server to the specified location before starting the installation.  
                                          | The directory path name cannot contain spaces.                                                                                               
                                          | All primary and alternate management servers must use the same certificate file. Required                                                                 |
| Agent Name                          | Host name of agent computer                  | The name of the agent computer. After installation, you can change the agent name through the Java console.                                 |
| Agent Locale                        | POSIX®                                       | DCS:SA agent locale setting.                                                                                                                |
| Agent Port                          | 443                                          | The Agent Port number that was used during management server installation. See “Management server installation settings and options” on page 66. |

Table 5-7 UNIX agent installation settings (continued)
### Table 5-7 UNIX agent installation settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Polling Interval</td>
<td>300 seconds</td>
<td>The interval that the agent uses to poll the management server for policy and configuration updates.</td>
</tr>
<tr>
<td>Notification Port</td>
<td>2222</td>
<td>The port that is used to receive alerts from the management server. You can also change this port after installation by using the Java console to change the properties of the agent.</td>
</tr>
<tr>
<td>Agent Notifications</td>
<td>Enable</td>
<td>When enabled, the agent listens on the Notification port to alerts from the management server. The alerts instruct the agent to immediately update to a new policy or configuration. This feature requires an unblocked notification port.</td>
</tr>
<tr>
<td>Util Service Port</td>
<td>2323</td>
<td>This installation setting supports the policy override tool for Solaris and Linux. You use the policy override tool to override prevention policy enforcement. You can change this value during installation.</td>
</tr>
<tr>
<td>Enable IPS Feature</td>
<td>Enable</td>
<td>When enabled, prevention is enabled on the agent.</td>
</tr>
<tr>
<td>Common Config Group</td>
<td>none</td>
<td>The name of an existing common configuration group for this agent to join. You use common configuration groups to apply communication and event logging parameters to agents. An agent is placed in the default common configuration group, unless you specify another configuration group that already exists in the Java console. After installation, you can change the group assignment by using the Java console.</td>
</tr>
</tbody>
</table>
### Table 5-7  UNIX agent installation settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevention Config Group</td>
<td>none</td>
<td>The name of an existing prevention configuration group for this agent to join. You use prevention configuration groups to apply log rules to agents. An agent is placed in the default prevention configuration group, unless you specify another configuration group that already exists in the Java console. After installation, you can change the group assignment by using the Java console.</td>
</tr>
<tr>
<td>Prevention Policy Group</td>
<td>none</td>
<td>The name of an existing prevention policy group for this agent to join. You use prevention policy groups to apply prevention policies to agents. An agent is placed in the default prevention policy group, unless you specify another policy group that already exists in the Java console. After installation, you can change the group assignment by using the Java console.</td>
</tr>
<tr>
<td>Detection Configuration Group</td>
<td>none</td>
<td>The name of an existing detection configuration group for this agent to join. You use detection configuration groups to apply detection parameters and log rules to agents. An agent is placed in the default detection configuration group, unless you specify another configuration group that already exists in the Java console. After installation, you can change the group assignment by using the Java console.</td>
</tr>
</tbody>
</table>
Table 5-7  UNIX agent installation settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
</table>
| Detection Policy Group       | One of the following:       | The name of an existing detection policy group for this agent to join. You can specify multiple groups by using commas between the group names.  
You can optionally include the name of an existing detection policy domain in the group path/name. You can include the domain name with or without the group name.  
An agent is placed in one of the default OS-specific detection policy groups in the default Policy domain, unless you specify another domain/policy group that already exists in the Java console.  
After installation, you can change the group assignment by using the Java console. |

**Bypassing prerequisite checks**

The UNIX installation kit lets you bypass some of the prerequisite checks for agent installation. You can use this feature if you know the installation kit is incorrectly failing a prerequisite.

To enable the bypass prerequisite checks feature, run touch as superuser:

touch /etc/scsp-check-bypass

You can use the bypass prerequisite checks feature to bypass the following prerequisite checks:

- Verify that the installation kit is being run by the root user
- Perform OS platform and version checks
- Perform package dependencies checks
- Perform file system/disk space usage checks

When the bypass prerequisite checks feature is used, the installation kit displays all errors and warnings about prerequisite check failures. However, instead of terminating the installation, you may choose to continue.
When you run the installation kit in interactive mode, you are asked if you want to continue. When you run the installation kit in silent mode, the prerequisite failure is logged and the installation continues.

The installation kit removes the /etc/scsp-check-bypass file upon a successful installation. Thus, creating the file enables the feature for one installation only.

**Warning:** Use of the bypass prerequisite checks feature does not guarantee that the installation will be successful if a non-recoverable error is bypassed. Please use this feature with caution.

### Installing an agent in verbose mode

Ports that are used for communications between an agent and the management server must be available on the agent computer and must match the values used during management server installation. The default settings are 443 and 2222.

After agent installation, you should assign a prevention policy and one or more detection policies to the agent by using the Java console.

Refer to the *DCS:SA Administrator's Guide* for information on assigning policies.

Before you install an agent, you need to place the SSL certificate on the computer that is targeted for installation. The certificate file is on the management server in the \Symantec\Data Center Security Server\Server directory. The file is named agent-cert.ssl.

To place the certificate on the computer that is targeted for installation, do the following:

- On the management server that will be used to manage the agent, locate the file named agent-cert.ssl in the \Server directory.
- On the computer on which the agent will be installed, create a directory and then copy the file agent-cert.ssl into the directory using FTP in binary mode or some other protocol.

The directory path name cannot contain spaces.

**To install an agent in verbose mode**

1. Open a Terminal window and become superuser.
2. Insert the installation CD and if necessary, mount the volume.
3. Type and run the following command:

   `cd /mnt/cdrom`
4 The product media provides agent installation files for various flavors of UNIX (32 bit or 64 bit). Run the following command to install the agent:

`./<file-name>

Where `<file-name>` is the file name of the agent installer for the specific flavor of UNIX.

For example, type the following command to install the agent on Red Hat Enterprise Linux 5.0:

`./agent-linux-rhel5.bin`

5 Agree to the license agreement, and then follow the onscreen prompts until the installation completes.

6 On Solaris, Linux or AIX computers, restart the computer if prevention was enabled.

Installing an agent in silent mode

You can use the silent installation for UNIX installations.

**Note:** The required options for silent installation are `-silent`, `-server`, and `-cert`.

The following table describes the settings that are used with the installation commands.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-help</code></td>
<td>none</td>
<td>You can run the installer with the <code>–help</code> switch to get a list of all the switches.</td>
</tr>
<tr>
<td><code>-rtfim</code></td>
<td></td>
<td>Install Real-time File Integrity Monitoring.</td>
</tr>
<tr>
<td><code>-version</code></td>
<td>none</td>
<td>Displays the installation package version information. Installation does not occur.</td>
</tr>
<tr>
<td><code>-silent</code></td>
<td>Interactive</td>
<td>Installs silently without user prompts. Uses default settings if they are not set by installation options. Required</td>
</tr>
</tbody>
</table>

Installing DCS:SA

Installing Symantec Data Center Security: Server Advanced components on UNIX
## Table 5-8 UNIX agent installation settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-allowreboot</td>
<td>No reboot</td>
<td>Initiates an automatic restart after installation completes, if intrusion prevention is enabled after installation. Applies to IPS agents.</td>
</tr>
<tr>
<td>-altroot</td>
<td>none</td>
<td>Used with Solaris Jumpstart.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In a Jumpstart environment, the system where the install takes place is booted from a temporary OS instance. The alternate root is necessary to ensure that files get installed in the correct place, relative to real OS instance, and not the temporarily booted instance.</td>
</tr>
<tr>
<td>-server=&lt;addr&gt;</td>
<td>127.0.0.1</td>
<td>The management server IP address or fully qualified host name. Required</td>
</tr>
<tr>
<td>-altservers=</td>
<td>none</td>
<td>A comma-separated list of alternate management servers. For each alternate management server, specify the IP address or fully qualified host name.</td>
</tr>
<tr>
<td>&lt;server1,server2,...&gt;</td>
<td></td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “About simple failover” on page 35.</td>
</tr>
<tr>
<td>-prefix=&lt;dir&gt;</td>
<td>/opt/Symantec</td>
<td>The installation directory prefix for the &lt;prefix dir&gt;/sdcssagent subdirectory. The directory path name cannot contain spaces.</td>
</tr>
<tr>
<td>-logdir=&lt;dir&gt;</td>
<td>/var/log/sdcsslog</td>
<td>The installation directory prefix for the &lt;prefix dir&gt;/sdcsslog subdirectory. If the directory does not exist, it is created.</td>
</tr>
<tr>
<td>-protocol=&lt;protocol&gt;</td>
<td>https</td>
<td>Select https or http communications.</td>
</tr>
</tbody>
</table>
Table 5-8 UNIX agent installation settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-cert=&lt;file&gt;</code></td>
<td>/tmp/agent-cert.ssl</td>
<td>The directory location of the SSL certificate file, <code>agent-cert.ssl</code>, obtained from the DCS:SA management server installation directory. You must copy this file from the management server to the specified location before starting the installation. The directory path name cannot contain spaces. All primary and alternate management servers must use the same certificate file. Required</td>
</tr>
<tr>
<td><code>-agentname=&lt;name&gt;</code></td>
<td>Host name of agent computer</td>
<td>The name of the agent computer. After installation, you can change the agent name through the Java console.</td>
</tr>
<tr>
<td><code>-locale=&lt;locale setting&gt;</code></td>
<td>POSIX</td>
<td>DCS:SA agent locale setting.</td>
</tr>
<tr>
<td><code>-comCfgGrp=&lt;group&gt;</code></td>
<td>none</td>
<td>The name of an existing common configuration group for this agent to join. The group must exist and appear in the Java console.</td>
</tr>
<tr>
<td><code>-ipsCfgGrp=&lt;group&gt;</code></td>
<td>none</td>
<td>The name of an existing prevention configuration group for this agent to join. The group must exist and appear in the Java console. Applies to IPS agents.</td>
</tr>
<tr>
<td><code>-ipsPolGrp=&lt;group&gt;</code></td>
<td>none</td>
<td>The name of an existing prevention policy group for this agent to join. The group must exist and appear in the Java console. Applies to IPS agents.</td>
</tr>
<tr>
<td><code>-idsCfgGrp=&lt;group&gt;</code></td>
<td>none</td>
<td>The name of an existing detection configuration group for this agent to join. The group must exist and appear in the Java console.</td>
</tr>
</tbody>
</table>
Table 5-8  UNIX agent installation settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-idsPolGrp=&lt;group&gt;</td>
<td>OS-specific group</td>
<td>The name of an existing detection policy group for this agent to join. You can specify multiple groups by using commas between the group names. You can optionally include the name of an existing detection policy domain in the group path/name. You can include the domain name with or without the group name. An agent is placed in one of the default OS-specific detection policy groups in the default Policy domain, unless you specify another domain/policy group that already exists in the Java console. After installation, you can change the group assignment by using the Java console.</td>
</tr>
<tr>
<td>-agentport=&lt;port&gt;</td>
<td>443</td>
<td>The Agent Port number that was used during management server installation. See &quot;Management server installation settings and options&quot; on page 66.</td>
</tr>
<tr>
<td>-notifyport=&lt;port&gt;</td>
<td>2222</td>
<td>The notification port that is used to receive broadcast alerts from the management server. You can also change this port after installation by using the Java console to change the properties of the agent.</td>
</tr>
<tr>
<td>-notify=&lt;0</td>
<td>1&gt;</td>
<td>1 (Enable)</td>
</tr>
<tr>
<td>-poll=&lt;sec&gt;</td>
<td>300</td>
<td>The polling interval, in seconds, that the agent uses to poll the management server for policy updates.</td>
</tr>
<tr>
<td>-svcport=&lt;port&gt;</td>
<td>2323</td>
<td>This installation setting supports the policy override tool for Solaris and Linux agents. The policy override tool overrides prevention policy enforcement. Use this switch to change the port value during silent install.</td>
</tr>
<tr>
<td>Setting</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>-disableips</td>
<td>Enable</td>
<td>Indicates whether to enable intrusion prevention for Solaris or Linux agents. When enabled, the prevention features of DCS:SA are enabled for the agent. The IPS drivers are loaded on the agent computer, and the agent accepts prevention policies from the Java console. To disable intrusion prevention, include the -disableips installation option in the command string. If you disable intrusion prevention and want to enable it in the future, you must run the sisipsconfig.sh tool in the /sdcssagent/IPS directory with the -I option, and restart the computer. The -I option toggles the intrusion prevention service on and off. Symantec strongly recommends that you enable intrusion prevention.</td>
</tr>
</tbody>
</table>

Use the -silent option and other options to perform a silent installation.

The following command string shows an example of a silent installation:

```
./agent-aix.bin -silent -prefix=/opt/Symantec -server=192.168.1.1 -cert=/var/tmp/agent-cert.ssl -agentport=443
```
To install an agent in silent mode

1. Follow the procedures and steps that are used to install an agent in verbose mode, up to and including mounting the installation CD drive.

   See "Installing an agent in verbose mode" on page 107.

2. Type and run the following command after replacing <file-name> with the filename of the agent installer for the specific flavor of UNIX:
   
   ```
   ./<file-name> -silent <additional options>
   ```

   For example, to install the agent on Red Hat Enterprise Linux 5.0 in silent mode:
   
   ```
   ./agent-linux-rhel5.bin -silent <additional options>
   ```

3. If you did not specify the -allowreboot option, restart the computer if intrusion prevention is enabled on Solaris, AIX, or Linux.

   If the agent fails to install correctly, review the /var/log/sdcsslog/agent_install.log file.

Uninstalling agents using package commands

You can uninstall the agents by using native operating system package commands. The package name for the agent is SYMCsdcss.

When the uninstaller completes, it reports an uninstall status.

To uninstall agents using package commands

1. (Solaris/Linux) Start the Java console, and set the policy for the agent to uninstall to the Null policy.

   The agent prevents you from installing and removing agent-related files if it is enforcing a restrictive prevention policy.

   If the Solaris or Linux agent is not communicating with the Java console, disable the agent, and then continue with the uninstall.

   See “Disabling and enabling Solaris agents” on page 115.

   See “Disabling and enabling Linux agents” on page 116.

2. Open a Terminal window on the computer that runs the agent to uninstall, and become superuser.
3 On Solaris, type and run the following command:

```
pkgrm SYMCsdcss
```

On Solaris, run the following command to restart the computer:

```
init 6
```

4 On Linux, type and run the following command:

```
rpm -e SYMCsdcss
```

On Linux, run the following command to restart the computer:

```
init 6
```

5 On AIX, type and run the following command:

```
rpm -e SYMCsdcss
```

On AIX, if the installation completes successfully, run the following command to restart the computer:

```
shutdown -Fr now
```

6 On HP-UX, type and run the following command:

```
swremove SYMCsdcss
```

7 (Solaris, and Linux) If the uninstall completes successfully, run the following command to restart the computer:

```
init 6
```

8 On AIX, if the uninstall completes successfully, run the following command to restart the computer:

```
shutdown -Fr
```

Computers running HP-UX does not require restart. If you have enabled IPS or File Integrity Monitoring (FIM), you must restart the system.

Disabling and enabling UNIX agents

You can temporarily and permanently disable UNIX agents. If you permanently disable an agent, the agent daemons stop immediately and disable startup upon restart. It does not disable the agent daemons. Upon restart, the agent daemons continue to load and enforce the currently-applied policies.
Disabling and enabling Solaris agents
This section describes how to disable and enable Solaris agents.

Temporarily disabling the IPS driver
If you have performance issues with Solaris agents, you may need to temporarily disable the intrusion prevention driver. You should do this only if there are serious performance issues that you suspect are being caused by the IPS driver, or if you have applied a prevention policy that is not allowing you to access the system in any way.

After you disable the driver, apply the Null prevention policy or a prevention policy in which prevention was disabled. Reboot the system.

Warning: You should perform these procedures only in emergency situations.

To temporarily disable the IPS driver
1. Interrupt the boot cycle with a Stop-a or break sequence.
2. At the ok prompt, type and run the following command:
   ```
   boot -as
   ```
   You must include the s switch in the boot command to boot into single-user mode. If you omit the s switch, then once the system boots into multi-user mode, it will enable the DCS:SA driver.
3. When the boot sequence asks for the location of your /etc/system file, type one of the following:
   ```
   /etc/system-pre-sisips
   /dev/null
   ```

Permanently disabling Solaris agents
If you have performance issues with Solaris agents, you may need to permanently disable them.

The following procedure disables an agent, not the driver. The driver will still be running.

Warning: You should perform these procedures only in emergency situations.
To permanently disable Solaris agents

1. Open a Terminal window and become superuser.
2. Type and run the following commands:
   ```
   /etc/init.d/sisipsagent stop
   /etc/init.d/sisidsagent stop
   ```
3. Type and run the following commands to rename the agent scripts, which temporarily break any symbolic links in the rc#.d startup scripts:
   ```
   mv /etc/init.d/sisipsagent /etc/init.d/sisipsagentOFF
   mv /etc/init.d/sisidsagent /etc/init.d/sisidsagentOFF
   ```

Enabling a disabled Solaris agent

You can enable a Solaris agent that was previously disabled.

To enable a disabled Solaris agent

1. Open a Terminal window and become superuser.
2. Type and run the following commands, which rename the sisipsagent scripts:
   ```
   mv /etc/init.d/sisipsagentOFF /etc/init.d/sisipsagent
   mv /etc/init.d/sisidsagentOFF /etc/init.d/sisidsagent
   ```
3. Type and run the following command to restart the computer:
   ```
   init 6
   ```

Disabling and enabling Linux agents

This section describes how to disable and enable Linux agents.

Temporarily disabling the IPS driver

If you have performance issues with Linux agents, you may need to temporarily disable the intrusion prevention driver. You should do this only if there are serious performance issues that you suspect are being caused by the IPS driver, or if you have applied a prevention policy that is not allowing you to access the system in any way.

After you disable the driver, apply the Null prevention policy or a prevention policy in which prevention was disabled. Reboot the system.
Warning: You should perform these procedures only in emergency situations.

To temporarily disable the IPS driver

- During the boot cycle, add the string SISIPSNULL to the boot options. The agent and kernel mode driver do not load, and the policy is not enforced.

Permanently disabling Linux agents

If you have performance issues with Linux agents, you may need to permanently disable them.

The following procedure disables an agent, not the driver. The driver will still be running.

Warning: You should perform these procedures only in emergency situations.

To permanently disable Linux agents

1. Open a Terminal window and become superuser.
2. Type and run the following commands:
   
   ```
   /etc/init.d/sisipsagent stop
   /etc/init.d/sisidsagent stop
   ```
3. Type and run the following commands to rename the agent scripts, which temporarily break any symbolic links in the rc#.d startup scripts:
   
   ```
   mv /etc/init.d/sisipsagent /etc/init.d/sisipsagentOFF
   mv /etc/init.d/sisidsagent /etc/init.d/sisidsagentOFF
   ```

Enabling a disabled Linux agent

You can enable a Linux agent that was previously disabled.
To enable a disabled Linux agent
1. Open a Terminal window and become superuser.
2. Type and run the following commands, which rename the sisipsgent scripts:
   ```
   mv /etc/init.d/sisipsagentOFF /etc/init.d/sisipsagent
   mv /etc/init.d/sisidsagentOFF /etc/init.d/sisidsagent
   ```
3. Type and run the following command to restart the computer:
   ```
   init 6
   ```

Disabling and enabling HP-UX agents
This section describes how to disable and enable HP-UX agents.

Temporarily disabling HP-UX agents

Warning: You should perform these procedures only in emergency situations.

To temporarily disable HP-UX agents
1. Open a Terminal window and become superuser.
2. Type and run the following commands:
   ```
   /sbin/init.d/sisipsagent stop
   /sbin/init.d/sisidsagent stop
   ```

Permanently disabling HP-UX agents
If you have performance issues with HP-UX agents, you may need to permanently disable them.

Warning: You should perform these procedures only in emergency situations.
To permanently disable HP-UX agents
1. Open a Terminal window and become superuser.
2. Type and run the following commands:
   
   ```
   /sbin/init.d/sisipsagent stop
   /sbin/init.d/sisidsagent stop
   ```
3. Type and run the following commands to rename the agent scripts, which temporarily break any symbolic links in the rc#.d startup scripts:
   
   ```
   mv /sbin/init.d/sisipsagent /sbin/init.d/sisipsagentOFF
   mv /sbin/init.d/sisidsagent /sbin/init.d/sisidsagentOFF
   ```

Enabling a disabled HP-UX agent
You can enable a HP-UX agent that was previously disabled.

To enable a permanently disabled HP-UX agent
1. Open a Terminal window and become superuser.
2. Type and run the following commands, which rename the sisipsgent scripts:
   
   ```
   mv /sbin/init.d/sisipsagentOFF /sbin/init.d/sisipsagent
   mv /sbin/init.d/sisidsagentOFF /sbin/init.d/sisidsagent
   ```
3. Type and run the following commands to start the agents:
   
   ```
   /sbin/init.d/sisipsagent start
   /sbin/init.d/sisidsagent start
   ```

Disabling and enabling AIX agents
This section describes how to disable and enable AIX agents.

Temporarily disabling AIX agents

---

Warning: You should perform these procedures only in emergency situations.
To temporarily disable AIX agents

1. Open a Terminal window and become superuser.
2. Type and run the following commands:
   
   /etc/rc.sisipsagent stop

   /etc/rc.sisidsagent stop

Permanently disabling AIX agents

If you have performance issues with AIX agents, you may need to permanently disable them.

Warning: You should perform these procedures only in emergency situations.

To permanently disable AIX agents

1. Open a Terminal window and become superuser.
2. Type and run the following commands:
   
   /etc/rc.sisipsagent stop

   /etc/rc.sisidsagent stop

3. Comment the agent startup commands from the /etc/inittab file by adding a colon (:) at the front of the rcsisipsagent and rcsisidsagent lines.
   
   This causes the agents to not start at the next reboot.

Enabling a disabled AIX agent

You can enable an AIX agent that was previously disabled.
To enable a permanently disabled AIX agent

1. Open a Terminal window and become superuser.
2. Uncomment the agent startup commands from the /etc/inittab file by removing the colon (:) at the front of the rcsisipsagent and rcsisidsagent lines.
   This causes the agents to start at the next reboot. The lines should look like the following:
   
   rcsisipsagent:23456789:wait:/etc/rc.sisipsagent start >/dev/console 2>&1  
   rcsisidsagent:23456789:wait:/etc/rc.sisidsagent start >/dev/console 2>&1

3. Type and run the following commands to restart the agents:
   
   /sbin/init.d//sisipsagent start  
   /sbin/init.d//sisidsagent start

Monitoring and restarting UNIX agents

The Health Check feature monitors and restarts UNIX agents in the event of an unexpected termination. This feature is available through the use of a crontab entry, which calls the daemon startup scripts at regular intervals with a health_check parameter.

For example, to monitor the UNIX agents every hour, add the following lines to the crontab file:

0 * * * * /etc/init.d/sisipsagent health_check  
0 * * * * /etc/init.d/sisidsagent health_check  
0 * * * * /etc/init.d/sisipsutil health_check (Solaris and Linux Only)

Use the appropriate crontab file for the UNIX platform:

- **AIX**
  
  Crontab: /var/spool/cron/crontabroot  
  Scripts: /etc/rc.sisidsagent, /etc/rc.sisipsagent

- **HP-UX**
  
  Crontab: /var/spool/cron/crontab.root  
  Scripts: /sbin/init.d/sisidsagent, /sbin/init.d/sisipsagent

- **Linux**
  
  Crontab: /var/spool/cron/tabs/root  
  Scripts: /etc/init.d/sisidsagent, /etc/init.d/sisipsagent, /etc/init.d/sisipsutil

- **Solaris**
Crontab: /var/spool/cron/crontabs/root
Scripts: /etc/init.d/sisidsagent, /etc/init.d/sisipsagent, /etc/init.d/sisipsutil

**Note:** The scripts keep the last five core files generated in the agent's respective home directory (/opt/Symantec/sdcssagent/IDS/bin and /opt/Symantec/sdcssagent/IPS). To change this setting, modify the MAX_CORES=5 value in the scripts.

Troubleshooting agent issues

**ISSUE:** An NFS server that does not respond on an agent computer causes the agent installation to hang.

**SOLUTION:** Press Ctrl+C to exit the installation, and then run df -k. If this causes the agent computer to hang, and you are sure that a mounted share is causing the problem, forcefully unmount the share that is not responding by typing and running the following command:

```
umount -f <mount-point>
```

Integrating with data center orchestration tools

RESTful APIs provide support for additional platforms and integration.

To access the RESTful APIs, you must perform the following tasks:

- Generate UMC token
  
  See [To generate UMC token](#)

- Access RESTful APIs
  
  See [To access RESTful APIs](#)

122 Installing DCS:SA

Integrating with data center orchestration tools
To generate UMC token

1. Make a post request to the following URL with the Json request:

   POST https://<UMC server IP>:8443/umcservices/rest/v1.0/auth/token

   Json request: { "username":"dcsadmin", "password":"password" }

   The password for dcsadmin is the one specified while deploying UMC. In case of an AD user, the username is domain alias name\username and the password is the configured AD password for that user.

   A token is generated.

2. Pass the token that is generated in step 1 to all the subsequent requests.

   Pass token header:

   Content-Type: application/json
   Authorization: bearer UMC token

To access RESTful APIs

1. Enter the following URL in your browser:

   https://<DCSserver-IP:PortNumber>/sis-ui/api/

   Enter the IP address and the port number of the Management Server, in the Server and Port fields.

2. In the Data Center Security: Server API documentation page, click Details. API information is displayed.
Installing DCS:S

This chapter includes the following topics:

- About installing DCS:S
- About installing a database linked to a SQL Server instance
- About Unified Management Console
- Deploying the Unified Management Console (UMC)
- Installing the management server
- Deploying Operations Director virtual appliance on VMware infrastructure
- Installing the UMC root certificate on a browser
- Enabling CORS
- Creating new certificates for DCS:S
- Deploying a Security Virtual Appliance
- Registering Data Center Protection Service with VMware NSX Manager
- Deploying Datacenter Protection Service
- Upgrading Datacenter Protection Service
- Uploading and registering the Security Virtual Appliance
- Unregistering the Security Virtual Appliance with NSX

About installing DCS:S

To install DCS:S, you must install the following components:
- Unified Management Console
  See “Deploying the Unified Management Console (UMC)” on page 126.

- Management Server
  See “Installing the Management Server” on page 129.

- Security Virtual Appliance
  See “Deploying a Security Virtual Appliance” on page 139.

You can install the Java console and management server on the same computer or on separate computers. All computers must run a supported operating system. The management server and the Java console are supported on Windows operating system.

Additionally, you must also complete the following tasks:

- Set up the VMware environment.
- Register DCS:S with UMC
- Configure NSX Manager to register the Datacenter Protection Service with the NSX Manager.
- Deploy the protection service.

### About installing a database linked to a SQL Server instance

You can locally install an SQL Server 2012 Express evaluation database. Besides, you can locally or remotely install an evaluation database or production database that is linked to an instance of SQL Server. All installations allocate 100 MB of storage for the database. SQL Server automatically allocates more space when it is needed. To install a database linked to an instance of SQL Server, Symantec recommends that you first install a new instance of SQL Server that conforms to the installation requirements.

You can install a database on an older, existing instance, but the instance must be configured properly or your database installation fails. For example, if the authentication configuration is not set to Mixed Mode, your installation fails.


See “About installing DCS:S” on page 124.
About Unified Management Console

The Unified Management Console (UMC) is a console appliance that provides a web-based console for NSX virtual data center protection and orchestration. The console is used to register and configure various features and products in Symantec Data Center Security: Server Advanced (DCS:SA).

UMC provides unification of the common tasks across DCS:S, DCS:SA, and Operations Director.

A UMC administrator has the required rights and permissions to configure and set up the DCS:SA products.


Deploying the Unified Management Console (UMC)

The Unified Management Console (UMC) is an appliance that provides a web-based console for NSX virtual data center protection and orchestration. UMC must be deployed on the VMware virtual infrastructure.

You can deploy the UMC OVA by using either the VMware vSphere Client or the VMware vSphere web portal.

Deploying the UMC OVA involves the following tasks:

- Locate the UMC OVA
- Deploy the UMC OVA
- Launch the UMC web-portal

Locate the UMC OVA

To locate the UMC OVA

- Navigate to the location of the UMC OVA on the installation disc.

Deploy the UMC OVA

To deploy the UMC appliance using VMware vSphere Client

1. In the VMware vSphere Client, navigate to File > Deploy OVF Template...
2. Provide a link to the location for the OVA file of the UMC appliance, and click Next.
3. On the OVF Template Details pane, verify the details of the OVA and click Next.
4. Click Accept on the End User License Agreement pane and then click Next.
5 In the **Name and Location** pane, provide a name for the appliance and specify the location for the deployment and click **Next**.

6 From the **Host / Cluster** pane, select the host of cluster on which you want to deploy the appliance and click **Next**.

7 From **Storage** pane, select location for the storage of the virtual machine files and click **Next**.

8 Select a **Disk Format** to store the virtual disks and click **Next**.

9 In the **Properties** pane, provide information for the following fields in the **Networking Properties** section:
   - Host name
   - IP address
   - Subnet mask
   - Domain Name Server
   - Default Gateway

A static IP is recommended over DHCP. In case you leave the field blank then the dynamic IP is taken through DHCP.

10 In the **Properties** pane, set a password for the default dcsadmin user in the **Credential management** section.

   This dcsadmin user is used as an appliance service user to perform appliance maintenance operations.

11 In the **Ready to Complete** pane, review your selection and click **Finish** to complete the setup.

   Select the **Power on after deployment** option to power on the appliance after deployment.

---

**Note:** IP address for any of the following must be specified in the IPv4 format: Appliance IP, DHCP IP, DNS IP, GATEWAY IP, etc.
To deploy the UMC appliance by using VMware vSphere web portal

1. Launch the VMware vSphere web client and on the home page select the vCenter option from the left navigation.

2. Click on VMs and Templates and from Actions menu select Deploy OVA Template.

   **Note:** The plug-in for client integration of vSphere web client must be installed to enable OVA functionality. The plugin must be allowed to run on the browser.

3. Provide the location for the OVA file of the UMC appliance, and click Next.

4. On the OVF Template Details pane, verify the details of the OVA and then click Next.

5. Click Accept on the Accept EULAs pane and click Next.

6. In the Select name and folder pane, provide a name for the appliance and specify the location for the deployment and click Next.

7. From the Select a resource pane, select the host of cluster on which you want to deploy the appliance and click Next.

8. From Select storage pane, select location and disk format for the storage of the virtual machine files and click Next.

9. On the Setup networks pane, select the network and click Next.

10. In the Customize template pane, provide information for the following fields in the Networking Properties section:

    - Host name
    - IP address
    - Subnet mask
    - Domain Name Server
    - Default Gateway

   If you leave the IP address field blank, the system takes a dynamic IP address through DHCP. However, it is recommended to use a static IP address. Enter the IP address in IPv4 format.
11 In the Properties pane, set a password for the dcsadmin user in the Credential management section.

This dcsadmin user is used as an appliance service user to perform appliance maintenance operations. This user ID and password is also required to log in to the UMC web portal for the first time.

12 In the Ready to Complete pane, review your selection and click Finish to complete the setup.

Select the Power on after deployment option to power on the appliance after deployment.

Launch the UMC web-portal

To launch the UMC web-portal

1 In a web browser, enter the URL in the following format:

   https://<UMCserverhostname>:8443/webportal/

2 Log in to UMC.

   To log in, the username is dcsadmin and the password is the one you had specified for the user dcsadmin while deploying the UMC appliance.

See “Installing the UMC root certificate on a browser” on page 132.

See “Configuring an Active Directory” on page 155.

See “Registering DCS:S with UMC” on page 148.

See “Registering Operations Director with UMC” on page 150.

Installing the management server

The management server coordinates events from Symantec Security Virtual Appliances, and provides database access to the Symantec Data Center Security: Server Advanced Java console. The management server secures communication with other components by using SSL to encrypt the communication channel. You must log on with administrator privileges to install the management server.

About installation types and settings

You can have the following type of installations for management server:

- Evaluation installation that runs SQL Server 2012 Express on the local system
  You can have an evaluation installation of SQL Server 2012 Express. The CD installs the server and database automatically.

- Evaluation installation that uses existing SQL instance
You can have an evaluation installation on SQL Server. Before you perform the installation, ensure that you have a running instance of SQL Server. The SQL Server instance can be local or remote.

- **Production installation with Tomcat and database schema**
  You can have a production installation that installs Tomcat and creates the database schema. This option installs on SQL Server. Before you perform the installation, ensure that you have a running instance of SQL Server. The SQL Server instance can be local or remote.

- **Tomcat component only**
  You can have a production installation that only installs the Tomcat component, and points to a remote database. This option requires that you provide the file paths to a server.xml, server-cert.ssl, server-console-cert.ssl and ca-cert.ssl file from an installed management server.

Before starting the management server installation, do one of the following:

- Allow all programs to initiate connections on port 1433 or your site-specific SQL Server port. Several programs connect to the database during the installation process.

- Disable all host-based firewalls on the management server computer and on the database server if it is on a remote computer. You can enable the firewalls after installation completes. After enabling firewall, you must set up a rule to allow connection on port 1433.

**Management server installation settings and options**

Installation prompts you to enter a series of values consisting of port numbers, user names, passwords, and so on. Each database that you install uses different default settings and options for the management server and database. Also, some settings for evaluation installation are hard-coded, while the same settings for production can be changed using variables. For example, the database name scspdb is hard-coded for evaluation installation, but is a variable that you can change for production database.

For more information on management server installation settings and options, refer to *Symantec Data Center Security: Server Advanced Planning and Deployment Guide* at: www.symantec.com/business/support/index?page=content&id=DOC8101

See “About installation of DCS:SA” on page 27.
Deploying Operations Director virtual appliance on VMware infrastructure

Operations Director appliance must be imported and deployed in the VMware virtual infrastructure.

Before you import and deploy Operations Director appliance, make sure that the UMC appliance is deployed in your virtual infrastructure. See “Deploying the Unified Management Console (UMC)” on page 126.

Operations Director appliance can be deployed using either the VMware vSphere Client or the VMware vSphere web portal. UMC is the console framework that hosts the pages of the Operations Director appliance. Therefore, Operations Director cannot work independent of UMC.

To deploy the Operations Director appliance using VMware vSphere client

1. In the VMware vSphere client, navigate to File > Deploy OVF Template...
2. Provide a link to the location for the OVA file of the Operations Director appliance, and click Next.
3. On the OVF Template Details pane verify the details of the OVA. Click Next.
4. In the Name and Location pane provide a name for the appliance and specify the location for the deployment. Click Next.
5. From Storage pane select location for the storage of the virtual machine files. Click Next
6. Select a Disk Format to store the virtual disks and click Next.
7. For details that you must provide in the Properties pane,
8. In the Ready to Complete pane, review your selection and click Finish to complete the setup.
   Select the Power on after deployment option to power on the appliance after deployment.

To deploy the Operations Director appliance using VMware vSphere web portal

1. Launch the VMware vSphere web client and on the home page select the vCenter option from the left navigation.
2. Click on VMs and Templates and from Actions menu select Deploy OVA Template.

Note: The plug-in for client integration of vSphere web client must be installed to enable OVA functionality. The plug-in must be allowed to run on the browser.
3 Provide a link to the location for the OVA file of the Operations Director appliance, and click **Next**.

4 On the **OVF Template Details** pane verify the details of the OVA. Click **Next**.

5 In the **Name and Location** pane provide a name for the appliance and specify the location for the deployment. Click **Next**.

6 From **Storage** pane select location for the storage of the virtual machine files. Click **Next**.

7 Select a **Disk Format** to store the virtual disks and click **Next**.

8 For details that you must provide in the **Properties** pane,

9 In the **Ready to Complete** pane, review your selection and click **Finish** to complete the setup.

Select the **Power on after deployment** option to power on the appliance after deployment.

---

**Installing the UMC root certificate on a browser**

After you install UMC, you must install the UMC root certificate on the browser you use. To install the root certificate, you must be logged on to the computer as an Administrator. In Windows Vista and later, you must start the browser with Administrator privileges (right-click on the browser icon and click **Run as administrator**; for Windows 8, search for the program name in the Metro start screen, right-click on the program name and click on **Advanced**, and then click **Run as administrator**.)

You need to perform this procedure only once on the computers from where UMC Web Portal will be accessed, except for Chrome. However, you will need to repeat these steps if a new certificate is installed or regenerated.

To install the certificate, perform the following steps, depending on your browser:

- **Internet Explorer**
- **Chrome**
- **Firefox**

For information on the supported browser versions, refer to *Symantec Data Center Security: Server Advanced Platform and Feature Matrix* document at: [www.symantec.com/docs/DOC7980](http://www.symantec.com/docs/DOC7980)
Internet Explorer

To install the UMC root certificate on Internet Explorer

1 Start Internet Explorer with Administrator privileges, and in the address box, type the following URL where hostname is the IP address or computer name of the server where Unified Management Console is installed:

https://<umcserverhostname>:8443/webportal

If you are using the computer name, then ensure that the computer name is added in your hosts file.

2 On the certificate alert screen ("There is a problem with this website's security certificate"), click Continue to this website (not recommended).

3 In the address bar, click the red Certificate Error alert.

4 In the Security Alert dialog box, click View Certificates.

5 In the Certificate Path properties under Certification Path tab, select UMC Root CA and click on View Certificate.

   Another Certificate properties window opens.

6 Under Details tab, click Copy to File.

   The Certificate Export Wizard opens.

7 Under Select the format you want to use: section, select Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B) and Include all certificates in the certification path if possible, and click Next.

8 In the File to Export screen, enter the file name.

9 Click Finish to save the certificate.

10 In the Internet Explorer, navigate to Tools > Internet Options > Content tab, and click Certificates.

11 In the Certificates properties, go to Trusted Root Certification Authorities, and click Import.

12 Follow the wizard and select the file that you just saved.

13 Click Next, and then click Finish.

   The Certificate Import Wizard dialog shows that the certificate import was successful.
14 Click **OK**.
   If you do not see the certificate import success message, then your certificate is not imported.

15 Clear the cache, and restart the browser.
   You should be able to log in to UMC URL https://<umcserverhostname>:8443/webportal.

**Chrome**

*To install the UMC root certificate on Chrome*

1 Type the UMC URL https://<umcserverhostname>:8443/webportal.
   If you are using the computer name, then ensure that the computer name is added in your `hosts` file.

   The privacy error **Your connection is not private** is displayed on the page. "https" appears with a strikethrough and the lock icon adjacent to "https" is also crossed.

2 Click the lock icon to display the site information.

3 In the **Connection** tab, click **Certificate information**.

4 Click **Certification Path** tab, and select **UMC Root CA** and click on **View Certificate**.
   Another **Certificate** properties window opens.

5 Under **Details** tab, click **Copy to File**.

   The **Certificate Export Wizard** opens.

6 Under **Select the format you want to use:** section, select **Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)** and include all certificates in the certification path if possible, and click **Next**.

7 In the **File to Export** screen, enter the file name, and click **Next**.

8 Click **Finish** to save the certificate.

   A message appears that the message was successful.

9 In Chrome, on the top right corner, navigate to **Settings > Show advanced settings... > HTTPS/SSL**, and click **Manage certificates**.

10 Click **Trusted Root Certification Authorities** tab, and click **Import**.

11 Follow the wizard and select the file that you just saved, and click **Next** multiple times. A **Security Warning** window appears for confirmation.
12 Click Yes.

The Certificate Import Wizard dialog shows that the certificate import was successful.

13 Click OK.

14 Clear the cache, and restart the browser.

Now you can log in to UMC URL https://<umcserv hostname>:8443/webportal.

---

**Note:** Chrome process continues to run in the background even after the browser is closed. At times, you may have to close the browser processes and then re-launch the UMC Web Portal.

---

**Note:** If you are using Chrome, you must accept the DCS:S certificate in every browser session of UMC.

---

**Firefox**

To install the UMC root certificate on Firefox

1 Type the UMC URL https://<umcserv hostname>:8443/webportal.
   If you are using the computer name, then ensure that the computer name is added in your hosts file.
   
   The privacy error **This Connection is Untrusted** is displayed on the page.

2 Expand I Understand the Risks section and click Add Exception...

3 In the Add Security Exception window, under Certificate Status section, click View to view the Certificate Viewer window.

4 Click the Details tab, and from the Certificate Hierarchy section, select UMC Root CA.

5 Click Export..., and save the certificate at a desired location.
   
   Cancel the Add Security Exception operation once the certificate is saved.

6 In the Firefox browser, from the top right corner navigate to Open Menu and click Options.

7 Go to the Advanced tab > Certificates tab, and click View Certificates.

8 From the Certificate Manager window, go to the Authorities tab and click Import.
9 Select the file that you just saved. Select the Trust this CA to identify websites options and click OK.

10 Clear the cache, and restart the browser.

You can now log in to UMC URL https://<umcservhostname>:8443/webportal.

After adding UMC CA certificate in a browser trust store, the address bar turns green while accessing the UMC URL.

---

**Note:** Make sure that the date and time on the UMC Appliance, Operations Director appliance, and DCS:S machines as well as the machines from where UMC web portal is being accessed are in sync.

To access DCS:S workspace in UMC you need to accept the DCS:S certificate in same browser session of UMC.

If DCS:S is registered with UMC by using IP address, then execute the following URL on the browser:

`https://<DCS:S IP>:4443/sis-ui/api/`

If DCS:S is registered with UMC by using host name then execute the following URL on the browser:

`https://<DCS:S host name>:4443/sis-ui/api/`

To access the DCS:S data, you must enable Cross-Origin Resource Sharing (CORS).

---

**Enabling CORS**

To access the DCS: Server data, you must enable Cross-Origin Resource Sharing (CORS).

Before you enable CORS, you must accept the certificate of DCS: Server by executing the following url on a browser.

`https://<DCSServerIP:DCSServerPortNumber>/sis-ui/api/`

To enable CORS in Internet Explorer

1 Open Internet Explorer, and navigate to **Tools > Internet Options**.
2 In the Internet Options window, click **Security tab > Custom Level**.
3 In the Security Settings - Internet Zone window, under **Miscellaneous > Access data sources across domains**, select **Enable**.
4 Close the browser and launch it again.
To enable CORS in Firefox

1. Open Firefox, and on the address bar, type `about:config`.
2. Click on `I'll be careful, I promise!`.
4. Right-click and select `Toggle` to change the value from `true` to `false`.
5. Close the browser and launch it again.

**Note:** In Chrome, cross scripting is handled automatically.

Creating new certificates for DCS:S

The SCSP 5.2.4 requires 2048-bit certificate, and SCSP 5.2.9 will be generating key using SHA256 hash. In order to be compatible with SCSP 5.2.4 agents, you must upgrade to 2048-bit certificate.

Support for 2048-bit keys was introduced in OpenSSL 0.9.7, and certificates of this type will therefore work with SCSP 5.2.4 and later. However, since SCSP 5.2.9, the keys will be generated with a SHA256 hash. This is not supported until OpenSSL 0.9.8. They will therefore not work on versions of SCSP prior to 5.2.6 in which OpenSSL 0.9.8n was introduced. In order to create 2048-bit certificates on an SCSP 5.2.9 server to be compatible with SCSP 5.2.4 agents, you would need to add the following switch to the command lines:

```
-sigalg SHA1withRSA
```

To create new encryption keys (certs) for the DCS:S

1. Copy the original cert files to a safe location.
   These files are located at:
   ```
   %programfiles%\Symantec\Data Center Security Server\server
   agent-cert.ssl
   server-cert.ssl
   ui-cert.ssl
   ```

2. Save a copy of server.xml available at:
   ```
   %programfiles%\Symantec\Data Center Security Server\server\tomcat\conf.
   ```
   Record the value for keystorepass. It is an alphanumeric string of 40 characters.
   The Common Name (CN) should be the Hostname of the server if that hostname is DNS resolvable otherwise you can use the servers IP address.
3 Record the host name of the DCS:S. This will be used to fill in the CN parameter.

4 Locate the following third-party tools found in the DCS:S installation folder:
   keytool.exe, located in:
   %programfiles%\Symantec\Data Center Security Server\server\jre\bin

5 openssl.exe is located in:
   %programfiles%\Symantec\Data Center Security Server\Server\tools

To generate a new 2048-bit RSA key for agent-manager communication

1 Using a command line interface, access the keytool utility by navigating to:
   %programfiles%\Symantec\Data Center Security Server\server\jre\bin
   Copy server-cert.ssl to this location.

2 Using the command line interface, enter the following command:
   keytool.exe -delete -keystore server-cert.ssl -alias sss -storepass
   [40 character alpha-numeric string found in server.xml]

3 Using the command line, enter the following command:
   keytool.exe -genkey -keystore server-cert.ssl -alias sss -keyalg RSA -sigalg SHA1withRSA -keysize 2048 -storepass
   [40 character alpha-numeric string found in server.xml] -keypass
   [40 character alpha-numeric string found in server.xml] -dname "CN=[DCS server hostname/ipaddress]"

4 Using the command line interface, enter the following command:
   keytool.exe -export -v -keystore server-cert.ssl -alias sss -rfc -storetype PKCS12 -file agent-cert.ssl -storepass
   [40 character alpha-numeric string found in server.xml]

Replacing Existing Certificates with new 2048-bit Certificates for DCS:S

1 Stop the DCS:S management service.

2 Replace the original server-cert.ssl located at:
   %programfiles%\Symantec\Data Center Security Server\server, with the new certificates created in keytool
Replacing Existing Certificates with new 2048-bit Certificates for Agents on Primary DCS:S

1. Copy the newly created agent-cert.ssl to: 
   "%programfiles%\Symantec\Data Center Security Server\server"

2. Update Agent to use new agent-cert.ssl with this command (forces use of new agent-cert.ssl file): 
   sisipsconfig -c agent-cert.ssl

3. Test connection from command prompt: 
   sisipsconfig –t

   **Note:** On Windows systems, sisipsconfig works from: 
   "%programfiles%\Symantec\Data Center Security Server\agent"

   **Note:** On UNIX systems, sisipsconfig works from /opt/Symantec/scsparser/ips

Deploying a Security Virtual Appliance

After you have successfully installed the management server, you must perform the following activities to register the SVA with UMC, and protect guest VMs:

- Register the Datacenter Protection Service with NSX Manager.
Deploy the Datacenter Protection Service.
Create a security group and associate Guest VMs to the group.
Create DCS:S policies and publish.
Assign published policies to a security group.
Upload and register the Security Virtual Appliance with UMC.

Note: SVA can be accessed using Web console only.

Note: The DCS:S Security Virtual Appliance supports up to 200 guest virtual machines on a single ESX host. If more than 200 guest virtual machines are seen on a single ESX host, the security virtual appliance protects only 200 of them, and the remaining guest virtual machines are unprotected.

For more information on installation requirements, refer to Symantec Data Center Security: Server Advanced Planning and Deployment Guide at: www.symantec.com/business/support/index?page=landing&key=63068
See “About installing DCS:S” on page 124.
See “Uploading and registering the Security Virtual Appliance” on page 143.
See “Registering Data Center Protection Service with VMware NSX Manager” on page 140.
See “Deploying Datacenter Protection Service” on page 141.

Registering Data Center Protection Service with VMware NSX Manager

After you import the security virtual appliance, you must register the Datacenter Protection Service with VMware NSX Manager. The Management Server encrypts and stores all the registration information in the database including the vCenter and NSX Manager information as Datacenter Protection Service entities.

To register Datacenter Protection Service with VMware NSX Manager

1 In the Java console, click the Assets tab.
2 On the Assets page, click the Malware Protection tab.
3 In the Register Symantec Data Center Protection Service to VMware NSX Manager panel, you are prompted to provide the following information.
DCP server details, such as the IP address, user name, and password of the vCenter.

- NSX Manager details, such as the IP address, user name, and password.
- IP address or fully qualified domain name (FQDN) of the Service Manager Host.
  By using FQDN, we can migrate service manager to a different computer without interrupting the deployment of the Datacenter Protection Service.

4. Click Register to complete service registration.

See "Deploying a Security Virtual Appliance" on page 139.

Deploying Datacenter Protection Service

You can deploy the Datacenter Protection Service from vSphere Web Client only after successful registration of the service with NSX Manager.

You must ensure that VMware Endpoint Service is successfully deployed and the service status is running.

To deploy the datacenter protection service

1. Log in to vSphere Web Client, and click the Home tab.
2. On the right pane under Inventories, click Networking & Security.
3. On the left pane under the Networking & Security tree, click Installation.
4. On the right pane, click the Service Deployments tab, and then click the green plus sign to deploy the protection service. The Deploy Network & Security Services wizard is launched.
5 In the **Deploy Network & Security Services** page, respond to each prompt and click **Next** to go to the next page.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select services &amp; schedule</td>
<td>Select <a href="#">Symantec Datacenter security server for VMware NSX</a>. Specify the schedule for deployment.</td>
</tr>
<tr>
<td>Select cluster</td>
<td>Select one or more clusters on which to deploy the service.</td>
</tr>
<tr>
<td>Select storage</td>
<td>Assign a data store to each cluster for service management.</td>
</tr>
<tr>
<td></td>
<td>Select iSCASI if more than one ESX hosts are present in one cluster.</td>
</tr>
<tr>
<td>Configure management network</td>
<td>Assign a network group and IP assignment mode (DHCP or IP pool).</td>
</tr>
<tr>
<td>Ready to Complete</td>
<td>Verify your deployment options.</td>
</tr>
</tbody>
</table>

6 Click **Finish** to complete the deployment.

See “**Deploying a Security Virtual Appliance**” on page 139.

---

### Upgrading Datacenter Protection Service

After you update your SVA, an upgrade alarm is raised on the vSphere Web Client. You can complete the update process from the vSphere Web Client. You can upgrade the Datacenter Protection Service by updating to a later version of the OVA file.

**To upgrade the protection service**

1 Log in to vSphere Web Client, and click the **Home** tab.
2 On the right pane under **Inventories**, click **Networking & Security**.
3 On the left pane under the **Networking & Security** tree, click **Installation**
4 On the right pane, click the **Service Deployments** tab, and then click the service you want to upgrade.
   The installation status informs that an upgrade is available.
5 Click the green down-arrow sign to initiate the upgrade.
6 In the **Confirm Upgrade** dialog, click **OK** to complete the upgrade process.
Uploading and registering the Security Virtual Appliance

Follow this procedure to upload and register your new SVA OVA file or upgrade your existing SVA. You can update your SVA to another version, which can be a later version, older version, or the same version. Ensure that the OVA file of the version that you want to update to is stored in your local drive.

To update the SVA

1. Navigate to Settings > Integration > Security Virtual Appliance in UMC.
2. Click Edit icon in the Actions column against the entry for Symantec Data Center Security Service for VMware NSX.
3. In the Upload and Register New SVA dialog, click Browse to navigate and select the SVA file that you want to register with UMC.
4. Click Upload.
5. Click Yes in the Confirm Operation dialog to proceed with the update.

See “Upgrading Datacenter Protection Service” on page 142.

Unregistering the Security Virtual Appliance with NSX

To unregister the SVA with NSX, perform the following steps:

- Delete security policies and security groups.
- Undeploy the SVA by deleting the Datacenter Protection Service.
- Unregister the Datacenter Protection Service.
- Unregister the SVA with NSX.

Note: Deleting an SVA without deleting security policies and security groups will result in firewall synchronization error.

To delete the protection service

1. Log in to vSphere Web Client, and click the Home tab.
2. On the right pane under Inventories, click Networking & Security.
3. On the left pane under the Networking & Security tree, click Installation.
4 On the right pane, click the **Service Deployments** tab.

5 Select the service that you want to delete, and then click the red cross sign.

6 In the **Confirm Delete** dialog, click **OK** to complete the delete process.

Ensure the policies that are bound on the security group no longer use the Symantec Antimalware Service before you proceed with unregistering the protection service.

**Note:** You cannot delete a service definition when its service manager does not exist.

---

**To unregister SVA with NSX**

1 Navigate to **Settings > Integration** in UMC.

2 In the **Security Virtual Appliance** section, click **X** icon.

3 Click **OK** in the **Confirm unregistration of appliance** dialog to delete the OVA file.

**Note:** If the datacenter protection service is not registered with the NSX Manager, the **Delete** option is disabled.

---

**Unregistering and re-registering SVA with NSX when FIPS mode is ON**

If you want to unregister and re-register SVA with NSX when the FIPS mode is ON, then you must first turn the FIPS mode OFF from the DCS Server, and then unregister SVA with NSX. After you re-register SVA with NSX, then you must turn the FIPS mode ON.

**To unregister and re-register SVA with NSX when FIPS mode is ON**

1 Open the command prompt, and navigate to the following location:

   ```
   C:\Program Files (x86)\Symantec\Data Center Security Server\Server\tools
   ```

2 In the command prompt window, execute the following command:

   ```
   ConfigFIPS.vbs -d
   ```

   The FIPS mode turns OFF.

3 Unregister the SVA with NSX.

4 Re-register the SVA with NSX.
5 After successful registration of SVA, open the command prompt, and navigate to the following location:

C:\Program Files (x86)\Symantec\Data Center Security Server\Server\tools

6 In the Command prompt window, execute the following command:

ConfigFIPS.vbs enable

See “Deploying a Security Virtual Appliance” on page 139.
Registering DCS:S and Operations Director with UMC

This chapter includes the following topics:

- Registering DCS:S and Operations Director with UMC
- Registering DCS:S with UMC
- Registering Operations Director with UMC

Registering DCS:S and Operations Director with UMC

Symantec Data Center Security: Server (DCS:S) or Operations Director (OD) must be registered with UMC after deployment.

DCS:S or Operations Director users must initiate a registration request to register with UMC. Any user of the configured Active Directory can trigger a product registration request. The registration request is displayed in pending approval state if the request is initiated by a user other than the UMC administrator. Only a UMC administrator can approve or deny a registration request.

If the registration request is initiated by a UMC Administrator, then the request is auto-approved by UMC.

Only one instance of a product can be registered at a time.
To approve a registration request

1. Log on to UMC as a UMC Administrator.
2. Navigate to **Settings > Product Setup** on the console.
   
   Registration requests that are received from products are displayed on the page.

3. The name of the user who has initiated the request for registration is displayed along with the product details for the following fields:
   
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP or Host name</td>
<td>IP address or host name of the product.</td>
</tr>
<tr>
<td>Port</td>
<td>Port that is used by the product.</td>
</tr>
<tr>
<td>Version</td>
<td>Version of the product.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the approval request.</td>
</tr>
</tbody>
</table>

4. Click **Approve** to approve the registration request.

5. Once the request is successfully approved, the value of the Status field changes from Pending Approval to **Configured**.

   **Note:** In case of auto-approval, you must refresh the browser to view the newly registered product. If you have already logged into the UMC console, then you must log out and login again after auto-approval to get the privileges for the newly registered product.

To deny a registration request

1. Navigate to **Settings > Product Setup**.

2. Click **Deny** for the product that has a Pending Approval status.

Unregistering a product

You can unregister a product from the **Product Setup** workspace. In case you want to re-register a product, you must unregister the product first and then register it again.

To unregister a product

1. Log on to UMC as a UMC Administrator.

2. Navigate to **Settings > Product Setup** on the console.

   All the registered products are displayed.
3 Click **Unregister** corresponding to the product that you want to unregister.

4 In the **Confirm Unregistration** window click **OK** to unregister the product.

Select **Retain user role mappings** in case you want to reuse the existing settings for the user account.

See “Registering DCS:S with UMC” on page 148.

### Registering DCS:S with UMC

You can access DCS:S from UMC only. To use the DCS:S, you must first register the DCS:S with UMC.

After successful registration of DCS:S, UMC receives a registration request from DCS:S. This request can either be approved or denied by the UMC administrator. If the registration request is initiated by a user having the UMC Administrator role, then the request is auto-approved by UMC.

To register DCS:S with UMC

1 Open command prompt on the computer on which you installed the Management Server.

2 Using the command prompt, navigate to **C:\Program Files (x86)\Symantec\Data Center Security Server\Server\tools** folder.

3 Type **registerProduct.bat**, and click **Enter**.
4 During the batch file execution, you are prompted to enter the following:

<table>
<thead>
<tr>
<th>Input</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter IP address or hostname of the UMC</td>
<td>Enter IP address or hostname of the UMC.</td>
</tr>
<tr>
<td>Enter umcadmin username</td>
<td>Enter dcsadmin or the username that is created for an admin user in UMC.</td>
</tr>
<tr>
<td>Enter umcadmin password</td>
<td>If you are registering DCS:S with UMC as a DCS:S admin, then enter the same password provided at the time of deploying UMC. If you are registering DCS:S with UMC as an admin user created in UMC, then enter the password of that user.</td>
</tr>
<tr>
<td>Type &quot;ok&quot; to register</td>
<td>Type OK.</td>
</tr>
</tbody>
</table>

**Note:** The Username and Password for UMC must be provided on the command line of the Registration Utility, and cannot be provided in the properties file.

5 After successful registration, a registration request is sent to the UMC administrator.

**Approving a registration request**

**To approve a registration request**

1 Log on to UMC, and navigate to **Settings > Product Setup** on the console. Registration request that is received from DCS:S is displayed on the **Product Setup** page.

2 The name of the user who has initiated the request for registration is displayed along with the product details for the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP or Host name</td>
<td>IP address or host name of the product.</td>
</tr>
<tr>
<td>Port</td>
<td>Port that is used by the product.</td>
</tr>
<tr>
<td>Version</td>
<td>Version of the product.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the approval request.</td>
</tr>
</tbody>
</table>
Click **Approve** to approve the registration request. Only a user with the UMC Administrator role can approve a registration request.

4. Once the request is successfully approved, the value of the Status field changes from Pending Approval to **Configured**.

---

**Note:** In case of auto-approval, any user who is logged in as UMC Administrator must refresh the browser to view the newly registered product. If a user is already logged into the UMC console, then to get the privileges for the newly registered product, the user must log out and login again after auto-approval.

If DCS:S is registered with UMC using the IP address, then execute the following URL on a browser:

https://<DCS:S IP>:4443/sis-ui/api/

If DCS:S is registered with UMC by using the host name, then execute the following URL on the browser:

https://<DCS:S host name>:4443/sis-ui/api/

---

**Note:** If DCS:S is registered with UMC using the IP instead of host name, then you must accept the DCS:S certificate in every browser session of UMC to view DCS:S related data.

---

### Denying a registration request

Only a UMC administrator can deny a product registration request. When a product registration request comes to UMC, the UMC administrator must verify the authenticity of the registration request. The administrator can then either approve or deny the request.

**To deny a registration request**

1. Navigate to **Settings > Product Setup**.
2. Click **Deny** that has a Pending Approval status.

---

### Registering Operations Director with UMC

Operations Director gets registered with UMC when you deploy the Operations Director appliance in vCenter. While deploying Operations Director, specify the following fields in the **Properties** pane to register Operations Director with UMC:
■ Under **Networking Properties**, provide the **Host name**, **IP Address**, **Subnet Mask**, **Domain Name Server**, and **Default Gateway**.
In the **IP address** field, specify a static IP.
If you leave the IP address, subnet mask, domain name server, and default gateway fields blank then the dynamic IP is taken through DHCP.

■ Under **Symantec Data Center Security Unified Management Console (UMC) Configuration**, provide the following information:
In the **UMC host name / IP address** field, enter the host name or the IP address of the UMC server.
In the **UMC user name** field, enter the user name using which you want to connect to the UMC server.
In the **UMC password** field, enter the password associated with the above user name.

■ Under **Credential Management**, provide a password that the server administrator will use when performing any appliance maintenance operations.

See “Deploying Operations Director virtual appliance on VMware infrastructure” on page 131.

**Operations Director fails to register with UMC**
If Operations Director fails to register with UMC during deployment, you must manually register Operations Director with UMC using the Operations Director registration tool.

**To execute Operations Director registration with UMC manually**
1. Connect to UMC using SSH.
2. Go to the location:
   
   `cd /usr/local/Symantec/so/
   ` 
3. Enter the command:
   
   ```
   java -cp "./lib/odregistration-6.5.0.1252.jar:./lib/*" 
   com.symantec.dcsc.common.odregistration.ODRegistration
   <umc_ipaddress> <umc_port> <umc_user> <umc_password>
   <od_ipaddress/od_hostname> <od_port>
   ```

   **Example:**
   
   ```
   java -cp "./lib/odregistration-6.5.0.1252.jar:./lib/*" 
   com.symantec.dcsc.common.odregistration.ODRegistration
   xx.xxx.xxx.xx 8443 testumcadmin testpassword xx.xxx.xxx.xxx 8443
   ```
Note: If `<umc_user>` is a domain user, the credentials must be either within double quotation " " with or without domain name or separated by a double backward slash.

For example:

"<domain name>\umcadmin"

or

"umcadmin"

or

<domain name>\\umcadmin

The port number is 8443 for HTTPS communication.

If you are providing UMC host name/Operations Director host name while registration, make sure the DNS server is configured correctly to resolve the host name. If DNS server is not configured, provide UMC IP address/Operations Director IP address instead of the host name for Operations Director registration tool to work correctly.

Refer to log file at `/var/log/Symantec/DCSC/od/odregistration.log`. 
Configuring a Data Center Security Product with UMC

This chapter includes the following topics:

- Using Unified Management Console
- Configuring an Active Directory
- About User Management
- Assigning roles to users and user groups
- Configuring components required for Operations Director
- Configuring DCS:S and UMC with FQDN
- About the Home Page in the DCS:S view
- About the Operations Director Home Page
- About alerts and notification
- About LiveUpdate Server Settings
- About Log Management
- Configuring VMware vCenter Server with UMC
- Configuring VMware NSX Server with UMC
- Uploading and Registering SVA with NSX using UMC
- Deploying a trusted CA certificate
- About importing licenses in DCS:S
Using Unified Management Console

Unified Management Console helps you configure and set up the various features and products in DCS.

Using the Unified Management Console, you can do the following:

**Home page**
- You can view the following from the Home page:
  - Provide step by step guidance to configure DCS:S.
  - View direct links to related workspaces and product help for respective step.

**Monitor page**
- You can do the following from the Monitor page:
  - Facilitates download of UMC and Operations Director logs directly from the console.
<table>
<thead>
<tr>
<th>Settings page</th>
<th>You can do the following from the Settings page:</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Management</td>
<td>■ Search users and groups in the configured Active Directory and assign them roles in DCS:S.</td>
</tr>
<tr>
<td>Product Setup</td>
<td>■ Approve or deny registration requests received from various features and products. Unregister products or features that are already registered.</td>
</tr>
<tr>
<td>Integration</td>
<td>■ Configure the Active Directory</td>
</tr>
<tr>
<td></td>
<td>■ Configure VMware vCenter server settings.</td>
</tr>
<tr>
<td></td>
<td>■ Configure VMware NSX server settings.</td>
</tr>
<tr>
<td></td>
<td>■ Configure Security Virtual Appliance.</td>
</tr>
<tr>
<td></td>
<td>■ Configure Alerts and Notifications.</td>
</tr>
<tr>
<td></td>
<td>■ Configure Orchestrated Security Products</td>
</tr>
<tr>
<td>LiveUpdate</td>
<td>■ Configure the LiveUpdate server settings.</td>
</tr>
<tr>
<td></td>
<td>■ Configure the Proxy server settings.</td>
</tr>
<tr>
<td>Licenses</td>
<td>■ Import licenses for the products registered with UMC.</td>
</tr>
<tr>
<td></td>
<td>■ Configure data collection for Telemetry.</td>
</tr>
</tbody>
</table>

See “About the Home Page in the DCS:S view” on page 161.

See “About the Operations Director Home Page” on page 162.

### Configuring an Active Directory

You can configure an Active Directory with UMC so that user authentication for UMC can be done using the configured Active Directory credentials. After the Active Directory is configured, you can assign roles to users and groups that are specific to DCS:SA.

The UMC Administrator role can use the Integration page in the Settings tab to configure the Active Directory.
Configuring an Active Directory

1. Navigate to **Settings > Integration**.

2. Click **Add** under the **Actions** column to configure an Active Directory.

   By default, an entry for an Active Directory is present. The state of this Active Directory stays Not Configured till the first Active Directory is configured.

3. In the Configure Active Directory window, provide the following information:

   - **Domain Name**: Provide fully qualified domain name of the Active Directory. For example: Abc.com
   - **Domain Name Alias**: Provide an alias for quick reference. The Domain Name Alias is used to log in to UMC web-portal using the following format: Domainnamealias\username
   - **LDAP path**: Provide a URL for the LDAP server. For example: ldap://XXX.XXX.XXX.XXX:389/ or in case of secured LDAP server use: ldaps://XXX.XXX.XXX.XXX:636
   - **User Name**: Provide user name of the Active Directory user. The user must have:
     - Read access to the Active Directory.
     - The User Principal Name (UPN) attribute configured.
   - **Password**: Provide password of the Active Directory user.

4. If you are configuring secured LDAP then, select the **Use SSL** option.

   **Note**: Using SSL will only work with LDAPS. To use LDAPS, SSL must be enabled in the Active Directory.

5. Click **Test Connection** to validate the connection to the Active Directory domain.

6. Click **Add** to configure the Active Directory.

   The Active Directory is displayed in the list and the status is changed to **Configured**.

Editing the configuration of an existing Active Directory

You can edit the parameters of an Active Directory that is already configured in UMC.
To edit the configuration of an existing Active Directory

1. Navigate to Settings > Integration.

2. From the displayed list select the Active Directory that you want to edit and click the Edit icon in the Action column.

3. In the Configure Active Directory window, make the required changes and click Save to save the changes.

If an AD user is disabled, locked, or if the user password expires, then the user cannot log on to UMC. User must reconfigure that user account in AD to log on to UMC.

About User Management

A user with the UMC Administrator role can assign predefined roles to Active Directory users or user groups for various products and features in DCS. A user or a user group can have multiple roles assigned for multiple products or features. If the credentials of a UMC user gets expired in the Active Directory, the user must be reconfigured in UMC.

To log into UMC web portal for the first time the default dcsadmin user must be used along with password specified during the appliance deployment. The default dcsadmin user is deleted after the UMC Administrator role is assigned to the first active directory user or group. The default dcsadmin user is then signed out and cannot sign in again.

The following predefined roles can be assigned to Active Directory users or groups:

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified Management Console Administrator</td>
<td>This role gives the user complete access to Data Center Security.</td>
</tr>
<tr>
<td>Operations Director Administrator</td>
<td>This role allows the user to administrate Operations Director.</td>
</tr>
<tr>
<td>DCS Server Administrator</td>
<td>This role allows the user to administrate DCS Server.</td>
</tr>
<tr>
<td>DCS Server Operator</td>
<td>This role allows the user to perform day to day operations in the DCS Server.</td>
</tr>
<tr>
<td>DCS Server Viewer</td>
<td>This role allows the user to view all DCS Server content.</td>
</tr>
</tbody>
</table>
To assign predefined roles to Active Directory users and user groups for a specific product, the product must be registered and approved and the AD must be configured with UMC.

Only the UMC administrator can assign or edit any role to any users across all the products that are registered in UMC.

**Note:** A logged in user cannot edit the current role assigned to the user, however the user can add additional roles.

See “Configuring an Active Directory” on page 155.

# Assigning roles to users and user groups

As a UMC Administrator you can Assign, Edit or Delete roles for a user or groups from the User Management workspace.

**Note:** Ensure that the first AD user that is added in UMC administrator role is not disabled, locked or the user password does not expire. If that happens then the user cannot log into the UMC webportal because the default dcsadmin user gets deleted after assigning the UMC administrator role to first AD user or group.

# Assigning roles to users or user groups

You can assign role to a user or a group or edit roles of an existing user or group.

**To assign a role to a user or a group**

1. Navigate to **Setting > User Management** in UMC.
2. Select **Users** or **Groups** in the left pane.
3. Click the Add (+) icon to assign a role.
4 In the **Assign User to Role** or **Assign Group to Role** dialog and provide the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Active Directory</strong></td>
<td>Select the Active Directory of the user.</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>Start typing the name of user or group. This field is an auto-suggest field and names start loading as you type.</td>
</tr>
<tr>
<td><strong>Feature</strong></td>
<td>Select the feature or product for which you want to add the role.</td>
</tr>
<tr>
<td><strong>Role</strong></td>
<td>Select the role you want to assign the user or group. You can assign more than one role to a user or group.</td>
</tr>
</tbody>
</table>

5 Click (+) below the Role field to add another set of Feature and Role. You can assign roles from multiple features or products to a user or a group.

6 Click **Assign** to assign the selected roles.

**Editing roles of a user or a user group**

You can edit the roles that are assigned to a user or a user group.

**To edit a role of a user or a user group**

1 Navigate to **Setting > User Management** in UMC.

2 Select **Users** or **Groups** in the left pane.

3 Select a user or a user group from the list. Click the **Edit** icon to edit the roles that are assigned to the user or a user group.

4 In the **Edit User Role** dialog the Active Directory and Name field are pre-filled and appear non-editable.

5 Edit the Features and Roles and click **Save**.

When you select a user from the list, all the groups which the user belongs to which are configured in UMC and all the roles which are assigned to the user are displayed at the bottom of the page.

When you select a group from the list, all the users which belong to the group that are added in UMC and all the roles which are assigned to the group are displayed at the bottom of the page.
Viewing Roles in DCS

You can view the details of the roles that are assigned to users and user groups of various features and products.

To view roles in DCS

1. Navigate to Setting > User Management in UMC.
2. Select Roles in the left pane.
3. Select a role from the displayed list of roles.

In the details pane all the users and user groups that are assigned the selected role are displayed.

Configuring components required for Operations Director

Refer the Installer Help for Setting up Operations Director that involves:

- Importing and deploying Operations Director virtual appliance on VMware infrastructure.
- Registering Operations Director with UMC.

After the Operations Director appliance has been imported and registered with the UMC, here are the next steps that you must complete.

Configure the orchestrated security products

Once the security products are configured, security policies and services get synchronized with Operations Director. The capabilities and library of security policies get integrated with Operations Director's software-defined security (SDS) services. This is managed from the Settings > Integration page of UMC.

Prerequisite for Symantec Data Center Security plug-in

You must register Operations Director with UMC while deploying the Operations Director appliance and also configure vCenter server from the Settings > Integration page of UMC. This ensures that the Symantec Data Center Security plug-in gets deployed to the vCenter.

If vCenter server is already configured and if you register Operations Director with UMC later, go to the Settings > Integration page of UMC to verify the vCenter server configuration.
Configuring DCS:S and UMC with FQDN

If you want to have multiple DCS: Server setup, then you must configure DCS:S and UMC with FQDN. In this setup, all the DCS: Server’s point to a single database.

You can now register or un-register SVA with NSX from any of the DCS: Server.

To install and configure DCS and UMC with FQDN

1. Update DNS configuration to associate IP address of DCS: Server #1 FQDN to its own IP.
2. Register DCS server #1 with UMC using FQDN.
3. Register DCS server #1 with NSX using FQDN.
4. Click **Upload and Register New SVA** to register SVA.
5. Install Tomcat component only on DCS: Server #2.

   After few minutes, the SVA files on DCS: Server #1 are replicated to the file server on DCS: Server #2.
6. Update DNS configuration to associate DCS: Server #2 IP also to the FQDN used for DCS: Server #1.

   You can now register or un-register SVA with NSX from any of the DCS: Server.

About the Home Page in the DCS:S view

After you install UMC and register DCS:S with UMC, you can access the DCS:S pages from the UMC console. The Home page in the **Server** view provides the malware protection and threat detection status, and displays whether the AV and GNTP definitions of DCS:S are up-to-date or not. The **SVAs** pane displays the number of Security Virtual Appliances that are online along with other details.

- **SVAs**
- **Network Threats Detected**
- **Viruses Detected**
- **Top 10 GVMs with network threats remediated**
- **Top 10 GVMs with virus threats remediated**
- **Global Threatcon**
About the Operations Director Home Page

Operations Director is available only after you register Operations Director appliance with UMC. After you log in to DCS:SA UMC console, on the top right select Operations Director in the drop-down to navigate to the Operations Director home page.

Operations Director home page serves as a dashboard that gives an insight into your virtual data center security posture.

The filter buttons in the **Key Security Provisioning Metrics** area display the count of:

- Policy provisioning errors.
- New applications that are pending approval for security provisioning.
- Notifications that pending an approval by the server administrator.
- Exceptions requested that need attention.

Clicking on any of the filter buttons will take you to the respective page and the filter will be applied while displayed the data. For example, if you click the filter button **13 New App Pending approval**, you will be navigated to the Monitor > Notifications page and only the notifications about 13 new applications that are pending approval will be displayed. You can clear or change the filters on the Notifications page.

The **Current Data Center Security Status** donut chart shows the applications that are at risk and that are secured.

The granular details of the count of applications are shown in the **Security Provisioning Status** donut chart. The granular details include:

- Pending Approval
- Waiting
- Provisioned
- In Progress
- Exception Requested
- Failed

Clicking any region in the donut chart takes you to the respective page and the filter will be applied while displaying the data. For example, if you click **Exception Requested** in the Security Provisioning Status donut chart, you will be navigated to the Assets > VMs page and the associated virtual machines will be displayed. You can clear or change the filters on the VMs page.
The **Overall Security Requirements by Tags** area chart displays the tags that are in use. The area chart acts as a filter. Clicking a specific tag in the area chart takes you to the **Tag Details** page. For example, if you click **PCI-DSS**, you will be navigated to the tag details page where you can view the tag description, security mappings, mandates, security controls, and questions associated to the tag.

**Note:** The home page only displays a real-time snapshot. You cannot perform any tasks from this page.

### About alerts and notification

Alerts and notifications for products registered with UMC can be set up by configuring the SNMP and SMTP server setting. Only the users who have the UMC Administrator role can configure SNMP and SMTP settings. You can configure settings for multiple SNMP server. However, you can configure only one setting for SMTP server. The SNMP and SMTP settings are shared by all the products that are registered with UMC.

### Configuring settings for Alerts and Notifications

You can configure settings for alerts and notifications from the Integration workspace.

#### To configure the SNMP settings

1. Navigate to **Settings > Integration** in UMC.
2. In the SNMP row, of the **Alerts and Notification** section, click the **Edit** icon.
3. In the **Add SNMP** dialog, provide the following information:

   - **Host name/IP Address**
     - Provide the host name or IP address of the SNMP server.
   - **Port**
     - Provide the port that is used by the SNMP server.
4. Click **Save**.
5. Once the settings are saved the status changes to **Configured**.

   You can add settings for multiple SNMP servers.

#### To configure SMTP settings

1. Navigate to **Settings > Integration > Alerts and Notification** in UMC.
2. In the SMTP row, click the **Edit** icon.
3 In the **Configure SMTP** dialog, provide the following information:

- **Host name/IP Address**: Provide the host name or IP address of the SMTP server.
- **Port**: Provide the port that is used by the SMTP server.
- **From Address**: Provide email address to configure notification mail sender's name.

4 Click **Save**.

5 Once the settings are saved the status changes to **Configured**.

---

**Note:** Only one SMTP server can be configured.

---

### Editing the SNMP settings

You can edit the existing SNMP settings.

**To edit the SNMP settings**

1. Navigate to **Settings > Integration > Alerts and Notification** in UMC.
2. In the SNMP row, click the **Edit** icon.
3. In the **Edit SNMP** dialog, edit the relevant values and click **Save**:

### Deleting the SNMP settings

You can delete the settings of an SNMP server.

**To delete the SNMP settings**

1. Navigate to **Settings > Integration > Alerts and Notification** in UMC.
2. In the SNMP row, click the **Delete** icon.
3. In the **Confirm SNMP Delete** dialog, click **OK**:

**Note:** There will always be at least one SNMP server entry present. The last entry cannot be deleted.
About LiveUpdate Server Settings

You can configure the liveupdate server settings to enable the download of updates for the product. By default the Symantec LiveUpdate server is configured in UMC.

In case you plan to use a Proxy Server in your environment, then you must configure the proxy server settings before you configure the LiveUpdate settings.

You can choose edit the default LiveUpdate server settings or add a new Live Update server. You can configure maximum five LiveUpdate servers.
To add a LiveUpdate Server

1. Navigate to Settings > LiveUpdate > LiveUpdate Server Settings in UMC and click Add.

2. In the Add LiveUpdate Server dialog, provide the following values:

   - **Host Name/IP Address**: Provide the host name or IP address of the LiveUpdate server. If you provide a host name, ensure that DNS is in place and its accessible from UMC.
   - **Path**: Provide the path to the location of the LiveUpdate files. This is an optional field.
   - **User Name**: Provide the user name of the LiveUpdate server user. This is an optional field.
   - **Password**: Provide the password of the LiveUpdate server user. This field is mandatory if case you provide the LiveUpdate server user name.
   - **Protocol**: Provide the protocol that you want to use for the LiveUpdate server. By default the value of this field is set to HTTP.
   - **Port**: Provide a port number for the LiveUpdate server.
   - **Bypass Proxy**: Select Yes to bypass the proxy server. In case you want to use the proxy server must be configured before configuring the LiveUpdate server.

3. Click Save.
To edit LiveUpdate server settings
1. Navigate to Settings > LiveUpdate > LiveUpdate Server Settings in UMC.
2. Click Edit icon in the Actions column against the entry for LiveUpdate server you want to edit.
3. In the Edit LiveUpdate Settings dialog, make the required changes and click Save.

Deleting a LiveUpdate Server
You can delete a LiveUpdate server from the LiveUpdate workspace. Product configuration requires at least one LU server to be configured. Hence, the last LU setting cannot be deleted.

To delete LiveUpdate server settings
1. Navigate to Settings > LiveUpdate > LiveUpdate Server Settings in UMC.
2. Click Delete icon in the Actions column against the entry for LiveUpdate server that you want to delete.

About Proxy Server Settings
In case you want to use the proxy server then the Proxy server settings must be configured before you configure the LiveUpdate server settings.
To configure the Proxy Server settings

1. Navigate to Settings > LiveUpdate > Proxy Server Settings in UMC.

2. Provide the following values for the proxy server:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name/Address</td>
<td>Provide the host name or the IP address of the proxy server.</td>
</tr>
<tr>
<td>User Name</td>
<td>Provide the user name of the proxy server user.</td>
</tr>
<tr>
<td></td>
<td>This is an optional field.</td>
</tr>
<tr>
<td>Password</td>
<td>Provide the password of the proxy server user.</td>
</tr>
<tr>
<td></td>
<td>This field is mandatory in case you provide the user name for the proxy server.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Provide the protocol you want to use for the proxy server.</td>
</tr>
<tr>
<td></td>
<td>By default the value of this field is set to HTTP.</td>
</tr>
<tr>
<td>Port</td>
<td>Provide the port number for the proxy server.</td>
</tr>
</tbody>
</table>

3. Click Save.

You can reset the proxy server settings from the LiveUpdate workspace, if you have set the Bypass Proxy field to Yes for the LiveUpdate server in the LiveUpdate server settings. Once the proxy server settings are used by any of the Live update server then the Proxy server cannot be reset.

About Log Management

Unified Management Console (UMC) supports download of logs for Operations Director and UMC from this workspace. You can choose to download all log files together or separately from the Log Management workspace to a known location.

UMC facilitates download product logs directly from the Console. This helps you to share the logs easily with Support.
To download logs

1. Navigate to Monitor > Log Management in UMC.
2. From Download logs select the features or products for which you want to download the logs.
   You can select the Feature Name option to select all products and features in the list.
3. Click Download.
4. The log files are downloaded at the default download location of the browser. The download location may differ depending on the browser you choose to use.

Note: Download of log files does not succeed in case you are using an older version of the Internet Explorer 10 browser. Use Internet Explorer 10.0.9200.17183 and above to download log files successfully.

Configuring VMware vCenter Server with UMC

You can configure the VMware vCenter Server from the Integration workspace.

To configure the VMware vCenter Server

1. Navigate to Settings > Integration > VMware in UMC.
2. Click Edit icon in the Actions column against the entry for VMware vCenter Server.
3. In the Configure VMware vCenter Server dialog provide the following values:
   - IP Address: Provide the IP Address of the vCenter Server. If the vCenter is running on a port other than the default port number, then you must enter <IPAddress:PortNumber>.
     Note: You can connect to only a single instance of vCenter server. If the IP address of the configured vCenter server changes, you must edit the vCenter server configuration in UMC (Settings > Integration page) to update the new IP address.
   - User name: Provide a user name of the vCenter Server user.
   - Password: Provide the password for the vCenter Server user.
4 Select the **Accept vCenter Server SSL certificate** option.
You can click the vCenter SSL certificate link to read the content of the certificate.

5 Click **Save**.
The status changes to Configured after the vCenter Server is configured successfully.

---

**Note:** VMware NSX Server can only be configured after the vCenter Server configuration is successful.

---

**Configuring VMware NSX Server with UMC**

VMware NSX Server can only be configured after the vCenter Server configuration is successful.

**To configure the VMware NSX Server**

1. Navigate to **Settings > Integration > VMware** in UMC.
2. Click **Edit** icon in the **Actions** column against the entry for **VMware NSX Server**.
3. In the **Configure VMware NSX Server** dialog provide the following values:

   - **NSX Server IP Address**
     - Provide the host name or IP Address of the NSX Server.
     - If you specify the host name, ensure that the DNS is in place to resolve host name and is accessible from UMC.
     - If the DCS: Server is running on a port other than the default port number, then you must enter either `<HostName:PortNumber>` or `<IPAddress:PortNumber>`.
     - **Note:** You can connect to only a single instance of NSX server. If the IP address of the configured NSX server changes, you must edit the vCenter server configuration in UMC (**Settings > Integration** page) to update the new IP address.

   - **NSX User Name**
     - Provide a user name of the vCenter user.

   - **NSX Password**
     - Provide the password for the vCenter user.

   - **DCS Server Name**
     - Provide IP or host name of the DCS:S.
     - In case of host name, ensure that the host name is resolvable from UMC.
4 Select the **Accept NSX Server SSL certificate** option.

You can click the vCenter SSL certificate link to read the content of the certificate.

5 Click **Save**.

The status changes to **Configured** after the NSX Server is configured successfully.

---

**Note:** The Security Virtual Appliance can be configured after the NSX Server is configured successfully.

---

### Uploading and Registering SVA with NSX using UMC

You must first configure the vCenter and NSX Server to register SVA with NSX using UMC. SVA related settings appear in UMC, only after successful configuration of vCenter and NSX Server, and after successful registration of DCS:S with UMC. If the SVA settings do not appear on the Integration page after successful configuration of vCenter and NSX Server, then perform a page refresh for the settings to appear. Ensure that the OVA file is stored in your local drive.

To upload and register SVA with UMC

1 Navigate to **Settings > Integration > Security Virtual Appliance** in UMC.

2 Click **Edit** icon in the **Actions** column against the entry for **Symantec Data Center Security Service for VMware NSX**.

3 In the **Upload and Register New SVA** dialog, click **Browse** to navigate and select the SVA file that you want to register with UMC.

4 Click **Upload**.

The status changes to Configured after the SVA is successfully uploaded. The registration of SVA with NSX time depends on the network speed and availability.

---

**Note:** In case you have an SVA already registered with UMC, then the new SVA replaces the old SVA. All settings related to the previous SVA are also deleted.
Deploying a trusted CA certificate

In case you do not want to use the UMC root certificate, you can use a trusted CA certificate.

Note: The following steps are applicable for UMC and Operations Director.

To deploy a trusted CA certificate

1 Login to the UMC application as a dcsadmin, using the command prompt.

2 Generate a key for UMC certificate.

To generate a key for UMC certificate, following is the command syntax:

```bash
openssl genrsa -out <<Location of the key>>/<<name of the key>>.key 2048
```

Following is an example command:

```bash
openssl genrsa -out /usr/local/Symantec/umc/ssl/umcCA/keys/SymantecTestUnifiedMgmtConsole.key 2048
```

3 Generate the UMC CSR.

To generate the UMC CSR, following is the command syntax:

```bash
openssl req -sha256 -new -key <<Location of the key>>/<<name of the key>>.key -out <<Location of the CSR>>/<<Name of the CSR file>>.csr (Provide the remaining details on command prompt for Common Name, OU, Location, State, and Country.)
```

Following is an example command:

```bash
openssl req -sha256 -new -key /usr/local/Symantec/umc/ssl/umcCA/keys/SymantecTestUnifiedMgmtConsole.key -out /usr/local/Symantec/umc/ssl/umcCA/keys/SymantecTestUnifiedMgmtConsole.csr (The remaining details provided as 
"/cn=SymantecTestUnifiedMgmtConsole.com/O=Symantec Corp/OU=DCS/L=Mountain View/S= California/C=US")
```

4 Perform the following steps once you receive the certificate:

It is recommended to use the default location for certificate and key

For UMC:
/usr/local/Symantec/umc/ssl/umcCA/certs and /usr/local/Symantec/umc/ssl/umcCA/keys respectively.

For OD:
/usr/local/Symantec/so/certs

- Export all the relevant certificate (RootCA, Intermediate CA, and the issued certificate) to a Base64 format and copy it on the UMC appliance.

- Concatenate the intermediate certificate and the root certificate in one file. Following are the command syntax and example, respectively:
  ```bash
  cat "<<Location of Root CA>>/<<Name of the Root CA file>>.cer" "<<Location of Intermediate CA>>/<<Name of the Intermediate CA>>.cer" > "<<Location of concatenated certificate>>/TrustedCA-chain.cer"
  ```

  ```bash
  cat "/usr/local/Symantec/umc/ssl/umcCA/certs/VeriSign Class 3 Public Primary Certification Authority - G5B64.cer" "/usr/local/Symantec/umc/ssl/umcCA/certs/Symantec Class 3 Secure Server CA - G4B64.cer" > "/usr/local/Symantec/umc/ssl/umcCA/certs/TrustedCA-chain.cer"
  ```

- chmod 444

- "/usr/local/Symantec/umc/ssl/umcCA/certs/TrustedCA-chain.cer"

- Convert all the relevant certificate files to a .PEM format. Following are the command syntax and example, respectively:
  ```bash
  openssl x509 -in "<<Location of Issued certificate>>/<<Issued certificate name>>.cer" -out "<<Location of Issued certificate>>/<<Issued certificate name>>.pem" -outform PEM
  openssl x509 -in "<<Location of Intermediate certificate>>/<<Intermediate Certificate name>>.cer" -out "<<Location of Intermediate certificate>>/<<Intermediate Certificate name>>.pem" -outform PEM
  openssl x509 -in "<<Location of RootCA>>/<<Root Certificate name>>.cer" -out "<<Location of RootCA>>/<<Root Certificate name>>.pem" -outform PEM
  openssl x509 -in "<<Location of Concatenated certificate>>/TrustedCA-chain.cer" -out "<<Location of Concatenated certificate>>/TrustedCA-chain.pem" -outform PEM
  ```

- openssl x509 -in "/usr/local/Symantec/umc/ssl/umcCA/certs/UMC-WK-UMCB64.cer" -out "/usr/local/Symantec/umc/ssl/umcCA/certs/UMC-WK-UMC.pem"
-outform PEM openssl x509 -in
"/usr/local/Symantec/umc/ssl/umcCA/certs/Symantec Class 3 Secure Server CA - G4B64.cer" -out
"/usr/local/Symantec/umc/ssl/umcCA/certs/Symantec Class 3 Secure Server CA - G4.pem" -outform PEM openssl x509 -in
"/usr/local/Symantec/umc/ssl/umcCA/certs/VeriSign Class 3 Public Primary Certification Authority - G5B64.cer" -out
"/usr/local/Symantec/umc/ssl/umcCA/certs/VeriSign Class 3 Public Primary Certification Authority - G5.pem" -outform PEM openssl x509 -in
"/usr/local/Symantec/umc/ssl/umcCA/certs/TrustedCA-chain.cer" -out
"/usr/local/Symantec/umc/ssl/umcCA/certs/TrustedCA-chain.pem" -outform PEM

- Rename the key file to a .PEM format.
- Add intermediate CA and Root CA in the Java default keystore as there is a possibility that a entry for a CA might not be present. Following are the command syntax and example, respectively:
  - keytool -importcert -trustcacerts -alias <<Alias name of IntermediateCA>> -file "<<Location of Intermediate certificate file>>/<<Name of Intermediate Certificate>>.pem" -keystore "<<Location of Java keystore on UMC appliance>>" -storepass changeit -noprompt keytool -importcert -trustcacerts -alias <<Alias name of RootCA>> -file "<<Location of RootCA certificate file>>/<<Name of Root CA Certificate>>.pem" -keystore "<</usr/java/jre1.7.0_72/bin/keytool>>" -storepass changeit -noprompt

- Make relevant changes in Tomcat's configuration file (server.xml) located at '/opt/apache-tomcat-7.0.53/conf'.
Configuring a Data Center Security Product with UMC

Deploying a trusted CA certificate

Following is an example of xml configuration:

```xml
<Connector port="8443"
sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"
sslProtocol="TLS"
ciphers="TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_256_CBC_SHA"
maxThreads="150" minSpareThreads="5"
enableLookups="false" disableUploadTimeout="true"
maxKeepAliveRequests="1"
acceptCount="10" scheme="https" secure="true"
SSLEnabled="true"
clientAuth="false"
keystoreType="PKCS12"
SSLCertificateFile="<<Location of Issued certificate>>
/umcservercrt1.pem"
SSLCertificateKeyFile="<<Location of key>>
/umcservercrtkey1.pem"
SSLCertificateChainFile="<<Location of concatenated
certificate>>/umcCA1.pem"
SSLPassword="changeit"
URIEncoding="UTF-8"
useSendfile="false"
/>
```
To deploy a trusted CA certificate for DCS:S


2. keytool -certreq -keyalg RSA -keysize 2048 -alias tomcat -keystore "C:\For Trusted certs\server-cert.ssl" -storepass <same value as that of keypass> -storetype PKCS12 -keypass <same value as that of keypass> -file "C:\For Trusted certs\server-cert.csr"

3. Generate a CSR (Certificate Signing Request) to Trusted Certificate Issuing Authority for obtaining certificate.

4. Export the received certificate in Base64 format.

5. Concatenate the Root and Intermediate Certificate files into one file.
   e.g. type Verisign.cer Inter.cer > concat.cer

6. Convert the certificate from .p12 format to .pem.
   openssl pkcs12 -nokeys -in "Path to server-console-cert.ssl" -out "Path to server-console-cert.pem" -password pass:"keypass"

7. Convert the concatenated certificate file e.g. concat.cer to .pem format.
   openssl x509 -in "Path to concat.cer" -out "Path to concat.pem"

   openssl pkcs12 -export -out "Path to server-cert1.ssl"{from tomcat} -in -inkey "Path to server-cert.pem"{private key} -certfile "Path to concat.pem"{chained file} -name sss(alias name) -caname trustedWKCA -password pass:"Keypass"

Note: Customer needs to install OpenSSL

See "Installing the UMC root certificate on a browser" on page 132.
About importing licenses in DCS:S

You can import licenses for DCS:S that is registered with UMC from the Licenses workspace. Before you import the licenses the relevant license files must be downloaded from the following location:


To import licenses in DCS:S

1. Navigate to Settings > Licenses in UMC.
2. Click Import Licenses.
3. Browse to the location where the downloaded license file (.slf) is saved and choose the relevant file for import.

Once the license is imported, you can view the type of imported licence, the validity of the licenses and the available and consumed count of licenses.

If the count of consumed licenses is not visible then ensure that DCS:S is up and running.

About Telemetry in DCS:S

Data collection for telemetry is enabled by default. However, you can configure the telemetry settings and choose to opt out of data collection from your environment for telemetry.

To disallow data collection for telemetry

1. Navigate to Settings > Licenses in UMC.
2. Deselect Yes, I would like to help optimize Symantec's security solutions by submitting anonymous system and usage information to Symantec to enable the data collection.

Providing your Organization's name to be sent along the telemetry data is optional.

About secured communication with UMC

Unified Management Console (UMC) provides unification of common tasks across products that are part of the Symantec Data Center Security suite and are registered with UMC. The communication between UMC and the registered products happens over HTTPS protocol.
Summary of secured communication rules

UMC uses the following communication rules:

- AES-256 algorithm for protecting confidential data.
- RSA-2048 for digital signature.
Upgrading to DCS:SA 6.5

This chapter includes the following topics:

- About upgrading to DCS:SA v6.5

About upgrading to DCS:SA v6.5

You can upgrade SDCS:SA v6.x installations to DCS:SA v6.5. You can upgrade any SCSP 5.x component (server, console or agent) to DCS:SA v6.5.

Abbreviations and Terminology

The following abbreviations and terminology is used in this doc:

- Symantec Data Center Security: Server Advanced (DCS:SA)
- Symantec Critical System Protection (SCSP)
- Primary management server: The management server is based on Tomcat Application Server software. Provides secure communication to and from agents and the Java console.
- Tomcat-only server (Secondary management server)
- Console: Console that lets administrators create and deploy policies, manage users and roles, view alerts, and run reports.
- Agent: Agents enforce policy on the endpoint.
- Database - The database provides the following capabilities:
  - Accessible through JDBC/ODBC
  - Stores the policies, agent information, and real-time actionable events
  - Lets you configure encrypted
Upgrade recommendations and best practices for an upgrade

When you upgrade earlier versions of SDCS:SA, you must ensure the following:

- Use a user account having administrative privileges to upgrade the management server and the agent.
- The Java console version should be equal to the management server version.
- The management server version should be higher or equal to the agent version.

Management server upgrade

You can upgrade the following versions to the latest version:

- 5.2.x Server
- 6.0.x Server

During upgrade process, the installation kit automatically detects the older version and upgrades the software to the latest version.

Only the password of the server database owner account is required during an upgrade. The default account name is ‘scspdba’.

Providing scspdba password during management server upgrade

During a management server upgrade, you are asked for the password to the scspdba account. If you chose the Evaluation installation when you initially installed the management server, the scspdba password is the same as the sa account password that you specified during the installation. Enter that same password during the upgrade. If you chose the Production installation, you entered the password for this account (the Database Owner account) during the initial installation of the management server. Enter that same password during the upgrade.

If you do not remember the scspdba password, you should change it in the database using SQL Server tools. This account is used strictly for upgrading the software; it is not used operationally by the management server. So changing the password in the database is safe—there is no corresponding change needed for the management server.

If you changed the name of the database owner account during a Production installation, you should enter that account name during the upgrade as well. You should not use the sa account during the upgrade.

Unattended Windows agent migration

You can perform an unattended migration of Windows agents using the agent.exe executable and InstallShield and Windows Installer commands.
The following examples show a command string:

agent.exe /s /v"/qn /l*v!+ %temp%\SISAgentSetup.log"

See “Silent installation of agent” on page 90.

Recommendations for a server upgrade in case of large data in the database

Server upgrade may fail with a query timeout error if the database contains large number of events in the "CSPevents" table. To avoid an upgrade failure, Symantec recommends the following guidelines:

- Effective configuration of prevention and detection configs.
  Instead of transferring all the event types to server in real-time, you must transmit only those events that you want to monitor on a daily basis. Rest of the event types must be bulk-logged, which can be imported to the database in future for any investigation.

- Enable purge settings from console. By default, it is disabled during server installation.

- Configure maximum number of events to be purged from the sis-server.properties file. The default value is 0.1 million.
Disaster Recovery

This chapter includes the following topics:

- Disaster Recovery

Disaster Recovery

As part of your disaster recovery procedures, you must use cloning feature of VMware to take regular backups of the appliances to minimize data loss.

When a VM is cloned, the VM is not assigned an IP.

This is a known issue with VMware:

VMware Knowledge Base

The following procedure is applicable for both, UMC and OD.

Do the following for disaster recovery:

1. Log in to the appliance as an administrator using SSH.
   For UMC, you must log in as `dcsadmin`.
2. Run setup command as: `sudo usr/local/bin/setup`.
3. Go to Device Configuration and press Enter.
4. Rename the default device name from `eth0` to `eth1`.
5. Save the settings.
6. Enter the following commands to stop and start network services:
   - `sudo service network stop`
   - `sudo service network start`
In UMC the products that are registered before the cloning of the application need not be re-registered. Any information or data that is created after the last cloning of the appliance is lost in case of disaster.
Where to get more information

Product manuals for DCS:SA are available on the DCS:SA product media. Updates to the documentation are available from the Symantec Technical Support and Business Critical Services (BCS) Web sites.

The DCS:SA product manuals are as follows:

- Installation Guide Online Help
- DCS:SA Online Help
- Planning and Deployment Guide
- Overview Guide
- Administrator's Guide
- Prevention Policy Reference Guide
- Detection Policy Reference Guide
- Agent Guide
- Implementation Guide Integration with VMware NSX (for Security Virtual Appliance)
- Operations Director Reference Guide
- vSphere Support Guide
- Release Notes
- Platform and Feature Matrix
The following table lists additional information that is available from the Symantec Web sites.

<table>
<thead>
<tr>
<th>Type of information</th>
<th>Web address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Knowledge Base</td>
<td><a href="http://www.symantec.com/business/support/">http://www.symantec.com/business/support/</a></td>
</tr>
<tr>
<td>Releases and updates</td>
<td></td>
</tr>
<tr>
<td>Manuals and other documentation</td>
<td></td>
</tr>
<tr>
<td>Contact options</td>
<td></td>
</tr>
<tr>
<td>Virus and other threat information and updates</td>
<td><a href="http://securityresponse.symantec.com">http://securityresponse.symantec.com</a></td>
</tr>
</tbody>
</table>