Symantec™ Data Center Security Installation Guide

Version 6.5
Symantec™ Data Center Security Installation Guide

Documentation version: 1.2

Legal Notice

Copyright © 2015 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

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

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

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

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Symantec as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.
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             seema@symantec.com
North America and Latin America            supportsolutions@symantec.com
Chapter 5  Next Steps ........................................................................................................ 38
Unified Management Console ....................................................................................... 38
  About the Home Page in the DCS:S view ................................................................. 39
  About the Operations Director Home Page .............................................................. 42
Deploying a trusted CA certificate .............................................................................. 43
Deploying a Security Virtual Appliance ................................................................. 48
  Configuring VMware vCenter Server with UMC ..................................................... 49
  Configuring VMware NSX Server with UMC .......................................................... 50
  Uploading and Registering SVA with NSX using UMC ........................................... 51
  Deploying Datacenter Protection Service ................................................................. 52
Installing a Windows agent ....................................................................................... 53
  About the SSL certificate file .................................................................................... 53
  About the installation settings and options ............................................................... 53
  Installing the Windows agent software ................................................................. 60
  Silent installation of agent ....................................................................................... 61
Data Center Security Operations Director .............................................................. 68
Integrating with data center orchestration tools ...................................................... 69

Chapter 6  Troubleshooting ............................................................................................ 70
Operations Director fails to register with UMC ......................................................... 70
Manually removing UMC integration with vCenter and NSX server ......................... 71
Viewing registration status of Operations Director with UMC .............................. 72
Installing DCS: SA

This chapter includes the following topics:

- About the installation guide
- About Symantec Data Center Security: Server Advanced licenses

About the installation guide

The installation guide for Symantec Data Center Security: Server Advanced (DCS:SA) walks you through the installation and configuration of Symantec Data Center Security: Server Advanced features. Installation of the Symantec Data Center Security: Server Advanced features entail various deployment scenarios and the online Help guides you through the steps that are required to deploy various features.

<table>
<thead>
<tr>
<th>Table 1-1</th>
<th>Installation at a snapshot</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High-level steps</strong></td>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
| Select features | Symantec Data Center Security: Server Advanced  
| | Symantec Data Center Security: Server Operations Director |
| Review components | Data Center Security Unified Management Console (UMC)  
| | Data Center Security Management Server  
| | Data Center Security Server Advanced Console  
| | Data Center Security Operations Director (OD) |
Table 1-1  Installation at a snapshot (continued)

<table>
<thead>
<tr>
<th>High-level steps</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified Management Console</td>
<td>Deploy the management console appliance.</td>
</tr>
<tr>
<td>Symantec Data Center Security: Server Advanced</td>
<td>Deploy the management server appliance and register it with UMC.</td>
</tr>
<tr>
<td>Management Server</td>
<td></td>
</tr>
<tr>
<td>Operations Director</td>
<td>Deploy the Operations Director appliance and register it with UMC.</td>
</tr>
<tr>
<td>Next steps</td>
<td>After successfully installing the product, follow the online Help to get started with using the product.</td>
</tr>
</tbody>
</table>

Additional Information

- You may want to refer to the product installation online help to understand how to deploy the various components of Symantec Data Center Security.
- Documentation set for Symantec Data Center Security: Server Advanced is available at the support site.
- Documentation set for Symantec Data Center Security: Server is available at the support site.

Note: The online help is best viewed using the latest version of Google Chrome browser.

About Symantec Data Center Security: Server Advanced licenses

You can download the DCS:S and the DCS:SA licenses from the following location:


For Operations Director, there is no separate license. Operations Director requires either the Data Center Security or the Data Center Security Server Advanced license.
Setting up the Unified Management Console Appliance

This chapter includes the following topics:

- Deploying the Unified Management Console (UMC)
- Installing the UMC root certificate on a browser
- Enabling CORS
- Creating new certificates for DCS:S
- Registering DCS:S and Operations Director with UMC

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 14.
See “Registering DCS:S with UMC” on page 32.

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

**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://<umcservhostname>: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://<umcserverhostname>: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://<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 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://<umcservicename>: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**.
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!.
3 Search for security.fileuri.strict_origin_policy.
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`
   `%programfiles%\Symantec\Data Center Security Server\server\server-cert.ssl`
   `%programfiles%\Symantec\Data Center Security Server\server\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 keystreopass. 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 hostname 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`

3 Replace the original agent-cert.ssl located at:

   `%programfiles%\Symantec\Data Center Security Server\server, with the renamed agent-cert.ssl created by openssl`

4 Restart the SCSP management service.

---

Note: Assuming server.xml is not changed, and the new keystore, cert and keystore passwords match what is already in the server.xml, the new certificate will automatically be used with the console and you should be asked at next console login to accept the new certificate. If not asked, then remove the siscerts file from the console’s certificate store:

   `[INSTALLDIR]\Console\certs\siscerts` which is usually located at:

   `%programfiles%\Symantec\Data Center Security Server\Console\certs\siscerts`.

After this file is removed, start the console and you will then be asked to accept the new certificate you generated.
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/scspagent/ips

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:

- **IP address or host name of the product.**
- **Port**
- **Version**
- **Status**

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 Navigateto **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 32.
See "Registering Operations Director with UMC" on page 37.
Setting up DCS: SA Management Server

This chapter includes the following topics:

- Installing the management server
- About installing the Java console
- Configuring the management console
- About installing DCS: S

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 scapdb 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


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 11.
- Management Server
Java Console
- Security Virtual Appliance

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.

About installing the Java console

The management console provides an interface for users and administrators. You can manage SVA configuration policy and antivirus policies for a guest virtual machine, and perform administrative tasks such as creating user accounts, restricting the functions that users can access, and running reports.

The features and tasks that you can perform in the management console can be accessed by pages. You can access other pages in the console from any page that you are currently viewing without losing the state of each page. See the Symantec Data Center Security: Server Advanced Administrator's Guide for more information on using the pages in the management console.

You must log on with administrator privileges to install the management console. After you install the management console, you must configure the management console before you can use it.

Installing the management console

By default, the management console is installed in the following directory:
C:\Program Files (x86)\Symantec\Data Center Security Server\Console

Management console installation does not prompt you to enter port numbers or server names.

To install the management console

1. On the installation CD, double-click console.
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 name 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 management console

When you configure the management console, you are prompted 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.

Reports and Queries for Security Virtual Appliance can be generated only through thick console.

To configure the management console

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

   Note: Symantec Data Center Security: Server Advanced does not support Symantec Data Center Security Server web client.

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 User name box, leave the password field blank, select the new server that you added, and then click Login.

6 In the Set Password panel, in the Password and Confirm Password boxes, type the password to associate with the symadmin user name.
To start the management console

1. Click Start -> All Programs -> Symantec Data Center Security Server -> Management Console.
2. In the Login dialog, in the User name and Password boxes, type your user name and password.
3. In the Login dialog, in the Server box, select the management server.
4. Click Log On.

See “About installing DCS:S” on page 29.

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 11.
- Management Server
  See “Installing the management server” on page 30.
- Security Virtual Appliance

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.

For more information on SQL Server 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

See “About installing DCS:S” on page 29.

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.


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!**.
3 Search for `security.fileuri.strict_origin_policy`.
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 scriptinig is handled automatically.

---

**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**.
During the batch file execution, you are prompted to enter the following:

- **IP or hostname of the UMC**: Enter IP address or hostname of the UMC.
- **umcadmin username**: Enter `dcsadmin` or the username that is created for an admin user in UMC.
- **umcadmin password**: 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.

Type "ok" to register Type **OK**.

**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.

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:

   - **IP or Host name**: IP address or host name of the product.
   - **Port**: Port that is used by the product.
   - **Version**: Version of the product.
   - **Status**: Status of the approval request.
3 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.
Setting up Operations Director

This chapter includes the following topics:

- Deploying Operations Director virtual appliance on VMware infrastructure
- Registering Operations Director with UMC

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 11.

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, see “Registering Operations Director with UMC” on page 37.

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, see “Registering Operations Director with UMC” on page 37.

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.
Registering Operations Director with UMC

To register Operations Director with UMC

1 Follow the steps to import and deploy Operations Director as explained in *Importing and deploying Operations Director virtual appliance on VMware infrastructure*.

2 Registration details of Operations Director with UMC must be provided in the *Properties* pane.
   - 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 or leave it blank. In case 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 to connect to the UMC server.
     - In the **UMC password** field, enter the password to connect to the UMC server.
   - Under *Credential Management*, provide a password that the server administrator will use when performing any appliance maintenance operations.

3 Follow the remaining steps as explained in *Importing and deploying Operations Director virtual appliance on VMware infrastructure*.

---

**Note**: You can register only one Operations Director appliance with one Unified Management Console appliance.

See “Deploying Operations Director virtual appliance on VMware infrastructure” on page 35.
Next Steps

This chapter includes the following topics:

- Unified Management Console
- Deploying a trusted CA certificate
- Deploying a Security Virtual Appliance
- Installing a Windows agent
- Data Center Security Operations Director
- Integrating with data center orchestration tools

Unified Management Console

Unified Management Console helps you configure and set up the various features and products in DCS:SA.

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 products with UMC.
- View direct links to related workspaces and product help for respective step.

**Monitor page**

You can do the following from the **Monitor** page:

- Download log files for UMC and Operations Director.
**Settings page**

You can do the following from the Settings page:

**User Management**
- Assign roles to users and groups in the Active Directory.

**Product Setup**
- Approve or deny registration requests received from various features and products. Unregister products or features that are already registered.

**Integration**
- Configure the Active Directory
- Configure VMware vCenter server settings.
- Configure VMware NSX server settings.
- Configure Security Virtual Appliance.
- Configure Alerts and Notifications.
- Configure Orchestrated Security Products

**LiveUpdate**
- Configure the LiveUpdate server settings.
- Configure the Proxy server settings.

**Licenses**
- Import licenses for the products registered with UMC.
- Allow data collection for Telemetry.

See “About the Home Page in the DCS:S view” on page 39.
See “About the Operations Director Home Page” on page 42.

**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**
About the SVAs pane

The SVAs pane displays the overall health of the SVAs in your environment. You get a count of the overall SVAs along with the count of online SVAs, SVAs on which the integrity check is passed, SVAs on which different services are running, and SVAs on which the definitions are up-to-date.

About the Network Threats Detected pane

Displays the total network threats detected for a period of last 28 days.

About the Viruses Detected pane

About the Top 10 GVMs with network threats remediated pane

Displays the top 10 guest virtual machines having maximum network threats detected.

About the Top 10 GVMs with virus threats remediated pane

About the Global Threatcon pane

Overall global threat found. It is not related to Symantec Data Center Security: Server, it is related to the Global threat which is also seen in Symantec web page.

About the Datacenter Protection Status pane

The Datacenter Protection Status pane displays the number of Security Virtual Appliances which are online or offline, the number of Security Virtual Appliances on which the Antivirus Service (AVS) and Content Management Service (CMS) is enabled, and the number of SVAs that offer support to more than the subscribed number of guest virtual machines. You can also get a count of the Security Virtual Appliances with unprotected guest virtual machines where the number of subscribed guest virtual machines on that host have gone beyond the defined limit.

To navigate to the Datacenter Protection Status view, click Assets -> Malware Protection -> Datacenter Protection Status. The Datacenter Protection Status pane also displays whether the definitions content is up to date or out of date and also displays the following status details:

- Online-Offline status
- Services Status
You can also perform other tasks by clicking on the **Cancel All Scans**, **Run LiveUpdate**, or **Refresh** tabs that are available in this pane.

Click **Cancel All Scans** to cancel all scans, including scheduled scans which are currently running on all the SVAs.

Click **Run LiveUpdate** to download the latest content on all the SVAs using LiveUpdate.

Click **Refresh** to refresh the **Datacenter Protection Status** pane.

### Guest VMs Threshold view

The **Guest VMs Threshold** pane displays the details of the security groups and the associated guest virtual machines within a security group. You can also view the count of protected and unprotected guest virtual machines and the threat violations that has occurred in the last 24 hours.

### LiveUpdate Definitions view

The **LiveUpdate Definitions** pane has information about the AV definitions, Reputation settings, Reputation revocation list, and SymEFA signatures.

The **Activity Monitoring Data Collection** pane displays the details of guest virtual machines as per the search criteria.

You can initiate a scan for all the guest virtual machines in a security group by selecting a specific security group and right-clicking **Scan Now**. If you want, you can initiate a scan only on a particular guest virtual machine.

### Guest VM View

The **Guest VM View** pane displays the information of the security groups and the guest virtual machines that belong to the security groups. The information of guest virtual machines that do not belong to a security group are also available in this view.

To navigate to the **Guest VM View** pane, click **Assets - > Malware Protection - > Guest VM View**. The guest virtual machines that are in the Powered On state are displayed in this view. Those guest virtual machines that are in the powered off or suspended state are not listed in this view.
To view the information for the latest security groups and guest virtual machines from the VMware inventory, click the **Refresh** tab at the top of the pane. You can also select a security group or guest virtual machine, and right-click **Refresh**.

### 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**
**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:

   ```
   openssl genrsa -out <<Location of the key>>/<<name of the key>>.key 2048
   ```

   Following is an example command:

   ```
   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:

```
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:

```
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:

  - 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"

  - 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
- Convert all the relevant certificate files to a .PEM format. Following are the command syntax and example, respectively:

  - 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

- 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>>/IntermediateCA-chain.pem" -keystore "<<Location of Java default keystore>>/keystore.jks" -storepass <<Store password>> -alias <<Alias name of IntermediateCA>>

- Next Steps
Deploying a trusted CA certificate

Next Steps

```java
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 Root CA 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'.

```xml
<Connector port="8443" protocol="org.apache.coyote.http11.Http11AprProtocol" sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2" ss1Protocol="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>>/umcservерkey1.pem" SSLCertificateChainFile="<<Location of concatenated certificate>>/umcCA1.pem" SSLPassword="changeit" URIEncoding="UTF-8"
```
useSendfile="false"

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="/usr/local/Symantec/umc/ssl/umcCA
certs/umcservercrt1.pem"
    SSLCertificateKeyFile="/usr/local/Symantec/umc/ssl
umcCA/keys/umcserverkey1.pem"
    SSLCertificateChainFile="/usr/local/Symantec/umc/ssl
/umcCA/certs/umcCA1.pem"
    SSLPassword="changeit"
    URIEncoding="UTF-8"
    useSendfile="false"
/>
```

- Restart the Tomcat server.

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 -nocerts -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"
8 Create pkcs12 file comprising the Root, Intermediate and key file.
   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 Open SSL

See “Installing the UMC root certificate on a browser” on page 14.

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 29.

See “Deploying Datacenter Protection Service” on page 52.

### 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 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 <strong>Symantec Datacenter security server for VMware NSX</strong>. 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.

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>
<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>
</tbody>
</table>
| Logs File Directory | C:\Program Files\Symantec\Data Center Security Server\Agent          | The installation directory prefix for the <prefix dir>/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. |
| Agent Name         | Host name of agent computer                                             | The agent name.  
After installation, you can change the agent name by using the Java console.                  |
| Polling Interval   | 300 seconds                                                            | The interval that the agent uses to poll the management server for policy and configuration updates. |
Table 5-1  Windows agent installation settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>

Next Steps  Installing a Windows agent
<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. 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>
</tbody>
</table>
Table 5-1  Windows agent installation settings *(continued)*

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Port</td>
<td>443</td>
<td>The Agent Port number that was used during management server installation. Referto the <a href="#">SymHelp</a> for more information about Management server installation settings and options and About port mapping.</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 <a href="#">SymHelp</a> for more information regarding About simple failover.</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. All primary and alternate management servers must use the same certificate file. Refer to the SymHelp for more information regarding About the SSL certificate file. See “About the SSL certificate file” on page 53.</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>
<tr>
<td>Setting</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Prevention Configuration Group</td>
<td>none</td>
<td>The name of an existing prevention configuration group for this agent to join.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</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>Prevention Policy Group</td>
<td>none</td>
<td>The name of an existing prevention policy group for this agent to join.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</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>Detection Configuration Group</td>
<td>none</td>
<td>The name of an existing detection configuration group for this agent to join.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</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>
Table 5-1  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. 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. 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. 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 5-2**  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>-1*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:</td>
</tr>
</tbody>
</table>

agent.exe /s /v"INSTALLDIR=\"E:\Program Files\...Symantec\System Critical Protection\Agent\" -1*v+! c:\agent-install.log /qn"
### Table 5-2  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 5-3  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</td>
</tr>
<tr>
<td>PROTOCOL=&lt;val&gt;</td>
<td>https</td>
<td>Select https or http communications.</td>
</tr>
</tbody>
</table>
### 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 53. 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. 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>

Next Steps

Installing a Windows agent
### Table 5-3  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</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Symantec strongly recommends that you enable intrusion prevention.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When you upgrade DCS:SA with IPS enabled, IPS continues to be enabled. You must manually disable IPS by using the following command:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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>
<tr>
<td>IPS_CONFIG_GROUP=&lt;val&gt;</td>
<td>Configuration</td>
<td>The name of an existing prevention configuration group for this agent to join.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>An agent is placed in the default prevention configuration group, unless you specify another configuration 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>IPS_POLICY_GROUP=&lt;val&gt;</td>
<td>Policy</td>
<td>The name of an existing prevention policy group for this agent to join.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>An agent is placed in the default prevention 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>
<tr>
<td></td>
<td></td>
<td>Optional</td>
</tr>
<tr>
<td>IDS_CONFIG_GROUP=&lt;val&gt;</td>
<td>Configuration</td>
<td>The name of an existing detection configuration group for this agent to join.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>An agent is placed in the default detection configuration group, unless you specify another configuration 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>
</tbody>
</table>
Table 5-3  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>LocalSystem</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>none</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>

Data Center Security Operations Director

After Operations Director appliance has been imported and deployed in vCenter and registered with the Unified Management Console (UMC), Operations Director appliance is ready for use.

To start working with Operations Director

1 Log on to the console by using the following URL:
   https://<UMC_appliance_IP>:8443/webportal/#/

2 In the drop-down on the top right corner, select Operations Director.
   The Operations Director home page is displayed.

To understand the features and functionality of Operations Director, refer the Online Help or the Symantec Data Center Security Operations Director Reference Guide.
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

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.
Troubleshooting

This chapter includes the following topics:

- Operations Director fails to register with UMC
- Manually removing UMC integration with vCenter and NSX server
- Viewing registration status of Operations Director with UMC

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 the Operations Director appliance 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`.

---

**Manually removing UMC integration with vCenter and NSX server**

In a scenario where you need to redeploy your UMC appliance for any reason you have to manually modify vCenter to clear the Symantec services before you can redeploy a new UMC appliance and integrate with it.

**To manually remove UMC integration with vCenter and NSX:**

1. Log in to vSphere Web client.
2. Go to **Home > Networking & Security > Service Definitions**.
3. In the right panel select the **NSX Manager** from the drop-down list.
4. Double-click the service definition **Symantec Data Center Security Service for VMware NSX**.
5. Go to the **Related Objects** tab. This will take you to the **Service Instances** page.
6 Right-click and delete all Symantec Data Center Security related service instances.

7 Go back to the Symantec Data Center Security Service for VMware NSX and right-click and delete this service definition. This will remove the Symantec Data Center Security Service for VMware NSX from service definitions.

**Note:** If for some reason you need to redeploy the UMC appliance and you have not removed each of these items, you will not be able to register or the environment will not work properly if registration is successful.

### Viewing registration status of Operations Director with UMC

To check the registration status of Operations Director with UMC, log in to UMC ([https://<UMC appliance IP>:8443/webportal/#/](https://<UMC appliance IP>:8443/webportal/#/)) and go to the Settings > Product Setup page. **Table 6-1** explains the registration status of that of Operations Director with UMC.

<table>
<thead>
<tr>
<th>Status</th>
<th>Next Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configured</td>
<td>If Operations Director is successfully registered with UMC, you must complete the post installation steps. See “Installing the UMC root certificate on a browser” on page 14.</td>
</tr>
<tr>
<td>Not Configured</td>
<td>If Operations Director registration with UMC fails, register Operations Director manually with UMC. See “Registering Operations Director with UMC” on page 37.</td>
</tr>
<tr>
<td>Pending Approval</td>
<td>UMC administrator must now approve the pending registration request or deny it so that you can again register Operations Director with UMC.</td>
</tr>
<tr>
<td>Deny Progress</td>
<td>UMC administrator has denied the pending registration request and it in progress. Wait for some time and then again register Operations Director UMC.</td>
</tr>
<tr>
<td>Status</td>
<td>Next Steps</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Unregister Progress</td>
<td>UMC administrator has initiated a request to unregister Operations Director and it in progress. Wait for some time and then again register Operations Director with UMC.</td>
</tr>
<tr>
<td>Approval Progress</td>
<td>UMC administrator has approval Operations Director registration request and it in progress. Wait for some time and then again register Operations Director with UMC.</td>
</tr>
</tbody>
</table>