Symantec™ Data Center Security: Server Implementation Guide

Integration with VMware NSX

Version 6.5
Symantec™ Data Center Security: Server Implementation Guide

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

Documentation version: 1.3

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.

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.
Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com
Technical Support

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

Symantec’s support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec’s support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/

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

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

**Licensing and registration**

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

www.symantec.com/business/support/

**Customer service**

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

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

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

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

Technical Support ........................................................................................................... 4

Chapter 1 Introducing Data Center Security: Server .................. 11
About Symantec Data Center Security: Server Advanced ............... 11
How DCS:S works ................................................................................................. 12
Key features of DCS:S ...................................................................................... 13

Chapter 2 Planning the installation .......................................... 15
Installation prerequisites for DCS:S ................................................................. 15
System requirements for DCS:S ................................................................. 15
Setting up the VMware environment ...................................................... 16

Chapter 3 Installing Data Center Security: Server ................. 18
About installing DCS:S .................................................................................... 19
About installing a database linked to a SQL Server instance .......... 19
Deploying the Unified Management Console (UMC) ..................... 20
Installing the UMC root certificate on a browser ......................... 23
Installing the management server .......................................................... 27
Enabling CORS ............................................................................................. 28
Creating new certificates for DCS:S ....................................................... 29
Configuring an Active Directory .......................................................... 32
Registering DCS:S with UMC ................................................................. 34
Configuring an IP pool on NSX Manager ............................................ 36
Deploying a Security Virtual Appliance ........................................... 37
Configuring VMware vCenter Server with UMC ......................... 38
Configuring VMware NSX Server with UMC ................................. 39
Uploading and Registering SVA with NSX using UMC ............. 40
Deploying Datacenter Protection Service ........................................ 41
Upgrading Datacenter Protection Service ...................................... 42
Uploading and registering the Security Virtual Appliance .......... 42
Unregistering the Security Virtual Appliance with NSX .......... 43
Configuring DCS:S and UMC with FQDN ........................................ 44
Purging quarantined files ............................................................... 76
Establishing local quarantine file thresholds ....................................... 76
Automatically deleting quarantined files .......................................... 76
Rescanning quarantined files .......................................................... 77
Generating events upon quarantine ................................................. 77

Chapter 8 Scanning and tagging ......................................................... 79
About the types of scans ................................................................ 79
About excluding items from scans .................................................... 80
About tagging .............................................................................. 80
Tagging a guest virtual machine ...................................................... 81
Untagging a guest virtual machine ................................................... 81
Scanning a GVM or a security group ............................................... 82

Chapter 9 Viewing events ................................................................. 83
About events ............................................................................... 83
About the Malware Protection Events pane .................................... 83
About event severity levels ............................................................. 85
Exporting events .......................................................................... 86
Purging events ............................................................................. 86

Chapter 10 Reporting ....................................................................... 88
About the Symantec queries and reports ........................................... 88
  About the Symantec queries ..................................................... 88
  About the Symantec reports ..................................................... 90
Viewing the Reports page .............................................................. 90
Managing queries ......................................................................... 91
  Running a query .................................................................... 91
  Exporting query results to multiple file formats ......................... 92
  Creating a query .................................................................. 92
  Editing a query .................................................................. 100
Managing reports ........................................................................ 101
  Running a report .................................................................. 101
  Creating a report .................................................................. 102
  Editing a report .................................................................. 102
Publishing a query or report .......................................................... 104
  Exporting a published report ................................................... 105

Chapter 11 Managing alerts .............................................................. 106
About alerts .................................................................................. 106
  About email aggregation ......................................................... 107
About SNMP traps ................................................................. 107
About alert text files ............................................................ 108
About troubleshooting alert problems ................................. 108
About the Notifications pane ............................................... 108
Viewing the Alerts page ...................................................... 109
Configuring alert settings .................................................... 109
Creating an alert ............................................................... 110
  Creating an alert filter .................................................... 111
  Specifying an email address template ............................... 112
  Specifying an SNMP trap ............................................... 113
  Specifying an alert text file ............................................. 114
Creating an alert configuration ........................................... 115
Enabling or disabling an alert ............................................. 116
About copying alerts ......................................................... 117
  Creating copies of alert .................................................. 117
Importing an alert ............................................................ 117
Exporting an alert ............................................................ 118
Deleting an alert .............................................................. 118
Purging alerts ................................................................. 118
Introducing Data Center Security: Server

This chapter includes the following topics:

- About Symantec Data Center Security: Server Advanced
- How DCS:S works
- Key features of DCS:S

About Symantec Data Center Security: Server Advanced

Symantec Data Center Security product suite entails components that provide you solutions to achieve different business objectives.

Table 1-1 Components of Symantec Data Center Security product suite

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec Data Center Security: Server Advanced</td>
<td>Symantec Data Center Security: Server Advanced provides granular, policy-based controls via a low impact in-guest agent to monitor and protect heterogeneous physical and virtual server environments.</td>
</tr>
<tr>
<td>Symantec Data Center Security: Server</td>
<td>Symantec Data Center Security: Server delivers agentless malware protection for VMware® infrastructures via a security virtual appliance, and enables security policy orchestration and automated workflows for the software-defined data center (SDDC).</td>
</tr>
</tbody>
</table>
Table 1-1 | Components of Symantec Data Center Security product suite (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified Management Console (UMC)</td>
<td>The Unified Management Console (UMC) is a console appliance that provides a Web-based console for NSX virtual data center protection and orchestration. The console is used to register and configure various features and products in Symantec™ Data Center Security (DCS). The UMC Administrator is a super user and has all the rights and permissions that are required to configure and set up DCS.</td>
</tr>
<tr>
<td>Operations Director</td>
<td>Operations Director appliance runs the security orchestration engine that computes and applies security policies on applications.</td>
</tr>
</tbody>
</table>

Another key feature is the unprecedented focus for an enterprise product on usability and simplicity through a new management console which is built upon a fully instrumented set of RESTful APIs to enable security automation in an agile world.

**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 by using the latest version of Google Chrome browser.

See “How DCS:S works” on page 12.

**How DCS:S works**

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

The following diagram illustrates a high-level work flow of DCS:S.

**Figure 1-1** DCS:S work flow diagram

You use the Unified Management Console to monitor the Datacenter protection status. After you register the Datacenter Protection Service with VMware, you can view the security groups, run scans on a guest virtual machine or on a security group, view the command status, run LiveUpdate on a SVA, view alerts and notifications that are received from the SVA, and the overall health of the datacenter.

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


**Key features of DCS:S**

Key features of Symantec Data Center Security: Server are as follows:
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agentless antivirus and antimalware security for VMware guest virtual machines</td>
<td>Provides on-demand and on-access antivirus and antimalware security with the reputation-based capabilities that decrease the detection of false positives.</td>
</tr>
<tr>
<td>Schedule scans and virus updates without affecting performance</td>
<td>DCS:S has the capability to run on-demand or on-access scans, and update virus definitions without affecting the datacenter's operational performance.</td>
</tr>
<tr>
<td>Integration with VMware Network and Security Virtualization (NSX) platform</td>
<td>Provides the antivirus protection automatically to the newly added physical hosts and guests in the vCenter after the initial setup is performed.</td>
</tr>
<tr>
<td>Supports the quarantine of malware inside a GVM with options to manage quarantine folders</td>
<td>Configuring the antivirus policies to enable quarantine of infected files and send them to the quarantine folder.</td>
</tr>
<tr>
<td>Provides Network security</td>
<td>Provides network security on VMware ESX 5.5 platform.</td>
</tr>
</tbody>
</table>

Planning the installation

This chapter includes the following topics:

- Installation prerequisites for DCS:S
- System requirements for DCS:S
- Setting up the VMware environment

Installation prerequisites for DCS:S

Ensure that you meet all system requirements before you install DCS:S.
See “System requirements for DCS:S” on page 15.

Ensure that you set up the VMware environment before you install DCS:S.
See “Setting up the VMware environment” on page 16.

System requirements for DCS:S

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

VMware support

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

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

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

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

Hardware requirements

Table 2-1 lists the Console, Server, and SVA requirements. VMware must also support this hardware.

Table 2-1 lists the recommended hardware for DCS:S

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

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

Setting up the VMware environment

To deploy the Symantec Datacenter Security Service for VMware NSX, which is Virtual Machine Threat Protection, you must set up the VMware environment by installing and configuring the following VMware components:

- Deploy vCenter appliance.
- Deploy NSX Manager
- Register vCenter with NSX Manager.
- Create a data center.
- Create a cluster and add ESXi hosts to the cluster.
- Create a distributed switch and add ESXi hosts to the distributed switch.
- Install host preparation.
- Deploy Guest Introspection service.

For more details on setting up the VMware environment, refer to the VMware guide at: http://pubs.vmware.com
This chapter includes the following topics:

- About installing DCS:S
- About installing a database linked to a SQL Server instance
- Deploying the Unified Management Console (UMC)
- Installing the UMC root certificate on a browser
- Installing the management server
- Enabling CORS
- Creating new certificates for DCS:S
- Configuring an Active Directory
- Registering DCS:S with UMC
- Configuring an IP pool on NSX Manager
- Deploying a Security Virtual Appliance
- Configuring VMware vCenter Server with UMC
- Configuring VMware NSX Server with UMC
- Uploading and Registering SVA with NSX using UMC
- Deploying Datacenter Protection Service
- Upgrading Datacenter Protection Service
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 20.

- Management Server
  
  See “Installing the management server” on page 27.

- Security Virtual Appliance
  
  See “Deploying a Security Virtual Appliance” on page 37.

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 19.

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 23.

See “Configuring an Active Directory” on page 32.

See “Registering DCS:S with UMC” on page 34.

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://<umcserverhostname>:8443/webportal

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

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

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

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

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

   Another Certificate properties window opens.

6. Under Details tab, click Copy to File.

   The Certificate Export Wizard opens.

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

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

9. Click Finish to save the certificate.

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

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

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

13. Click Next, and then click Finish.

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

If you do not see the certificate import success message, then your certificate is not imported.

15 Clear the cache, and restart the browser.

You should be able to log in to UMC URL https://<umcserverhostname>:8443/webportal.

Chrome
To install the UMC root certificate on Chrome

1 Type the UMC URL https://<umcserverhostname>:8443/webportal.

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

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

2 Click the lock icon to display the site information.

3 In the Connection tab, click Certificate information.

4 Click Certification Path tab, and select UMC Root CA and click on View Certificate.

Another Certificate properties window opens.

5 Under Details tab, click Copy to File.

The Certificate Export Wizard opens.

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

7 In the File to Export screen, enter the filename, 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://<umcservhostname>: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://<umcservhostname>: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://<umcservenamehostname>: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:

```bash
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:

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

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

---

### Installing the management server

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

### About installation types and settings

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

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

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

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

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

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

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

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

**Management server installation settings and options**

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

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

**Enabling CORS**

To access the DCS: Server data, you must enable Cross-Origin Resource Sharing (CORS).
Before you enable CORS, you must accept the certificate of DCS: Server by executing the following URL on a browser.

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

To enable CORS in Internet Explorer

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

To enable CORS in Firefox

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

Note: In Chrome, cross scripting is handled automatically.

Creating new certificates for DCS:S

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

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

"-sigalg SHA1withRSA".
To create new encryption keys (certs) for the DCS:S

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

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

3. Record the host name of the DCS:S. This will be used to fill in the CN parameter.

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

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

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

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

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

```cmd
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:

```cmd
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

Configuring an Active Directory

You can configure an Active Directory with UMC so that user authentication for UMC can be done using the configured Active Directory credentials. After the Active Directory is configured, you can assign roles to users and groups that are specific to DCS:SA.

The UMC Administrator role can use the Integration page in the Settings tab to configure the Active Directory.

Configuring an Active Directory

1 Navigate to Settings > Integration.

2 Click Add under the Actions column to configure an Active Directory.
   By default, an entry for an Active Directory is present. The state of this Active Directory stays Not Configured till the first Active Directory is configured.

3 In the Configure Active Directory window, provide the following information:
   Domain Name: Provide fully qualified domain name of the Active Directory.
   For example: Abc.com
Domain Name Alias  Provide an alias for quick reference. The Domain Name Alias
is used to log in to UMC web-portal using the following format:
Domainnamealias\username

LDAP path  Provide a URL for the LDAP server.
For example: ldap://XXX.XXX.XXX.XXX:389/ or in case of
secured LDAP server use: ldaps://XXX.XXX.XXX.XXX:636

User Name  Provide user name of the Active Directory user.
The user must have:
  ■  Read access to the Active Directory.
  ■  The User Principal Name (UPN) attribute configured.

Password  Provide password of the Active Directory user.

4  If you are configuring secured LDAP then, select the **Use SSL** option.

---

**Note:** Using SSL will only work with LDAPS. To use LDAPS, SSL must be
enabled in the Active Directory.

5  Click **Test Connection** to validate the connection to the Active Directory
domain.

6  Click **Add** to configure the Active Directory.
The Active Directory is displayed in the list and the status is changed to
**Configured**.

**Editing the configuration of an existing Active Directory**

You can edit the parameters of an Active Directory that is already configured in
UMC.

**To edit the configuration of an existing Active Directory**

1  Navigate to **Settings > Integration**.

2  From the displayed list select the Active Directory that you want to edit and
click the **Edit** icon in the **Action** column.

3  In the **Configure Active Directory** window, make the required changes and
click **Save** to save the changes.

If an AD user is disabled, locked, or if the user password expires, then the user
cannot log on to UMC. User must reconfigure that user account in AD to log on to
UMC.
Registering DCS:S with UMC

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

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

To register DCS:S with UMC

1. Open command prompt on the computer on which you installed the Management Server.
2. Using the command prompt, navigate to `C:\Program Files (x86)\Symantec\Data Center Security Server\Server\tools` folder.
3. Type `registerProduct.bat`, and click Enter.
4. During the batch file execution, you are prompted to enter the following:
   - 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.

5. After successful registration, a registration request is sent to the UMC administrator.
Note: UMC registration with DCS:S fails if you have upgraded from an earlier version of the product to DCS:S v6.5 as the root directory does not change after the upgrade. You must change the default root directory to C:\Program Files (x86)\Symantec\Data Center Security Server\Server\tools to register DCS:S with UMC after an upgrade.

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.

---

**Configuring an IP pool on NSX Manager**

Before you deploy Security Virtual Appliance (SVA), Symantec recommends that you configure an IP pool on the NSX Manager. You can then use IPs from the IP pool while deploying the SVA.
To configure an IP pool on NSX Manager

1. Log in to vSphere Web Client, and click the **Home** tab.
2. Under **Inventories**, click **Networking and Security**.
3. On the left pane, under the **Networking and Security** tree, click **Networking and Security Inventory**.
4. Click **NSX Manager** and the IP displayed for NSX Manager.
5. On the right pane, click the **Manage** tab and then the **Grouping Objects** tab.
6. Click **IP Pools** and then click the green + icon to add an IP pool.
   
   Enter the following details:
   
   ■ Name
   ■ Gateway
   ■ Prefix Length
   ■ Primary DNS
   ■ Static IP pool
7. Click **OK**.

**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 19.

See “Uploading and registering the Security Virtual Appliance” on page 42.

See “Deploying Datacenter Protection Service” on page 41.

**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 &lt;IPAddress:PortNumber&gt;.
     - **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 Symantec Datacenter security server for VMware NSX.</td>
</tr>
<tr>
<td></td>
<td>Specify the schedule for deployment.</td>
</tr>
<tr>
<td>Select cluster</td>
<td>Select one or more clusters on which to deploy the service.</td>
</tr>
<tr>
<td>Select storage</td>
<td>Assign a data store to each cluster for service management.</td>
</tr>
<tr>
<td></td>
<td>Select iSCASI if more than one ESX hosts are present in one cluster.</td>
</tr>
<tr>
<td>Configure management network</td>
<td>Assign a network group and IP assignment mode (DHCP or IP pool).</td>
</tr>
<tr>
<td>Ready to Complete</td>
<td>Verify your deployment options.</td>
</tr>
</tbody>
</table>

6. Click Finish to complete the deployment.

See “Deploying a Security Virtual Appliance” on page 37.
Upgrading Datacenter Protection Service

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

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

See “Uploading and registering the Security Virtual Appliance” on page 42.

Uploading and registering the Security Virtual Appliance

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

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

See “Upgrading Datacenter Protection Service” on page 42.
Unregistering the Security Virtual Appliance with NSX

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

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

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

To delete the protection service

1. Log in to vSphere Web Client, and click the Home tab.
2. On the right pane under Inventories, click Networking & Security.
3. On the left pane under the Networking & Security tree, click Installation.
4. On the right pane, click the Service Deployments tab.
5. Select the service that you want to delete, and then click the red cross sign.
6. In the Confirm Delete dialog, click OK to complete the delete process.

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

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

To unregister SVA with NSX

1. Navigate to Settings > Integration in UMC.
2. In the Security Virtual Appliance section, click X icon.
3. Click OK in the Confirm unregistration of appliance dialog to delete the OVA file.

**Note:** If the datacenter protection service is not registered with the NSX Manager, the Delete option is disabled.
Unregistering and re-registering SVA with NSX when FIPS mode is ON

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

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

1. Open the command prompt, and navigate to the following location:
   C:\Program Files (x86)\Symantec\Data Center Security Server\Server\tools
2. In the command prompt window, execute the following command:
   ConfigFIPS.vbs -d
   The FIPS mode turns OFF.
3. Unregister the SVA with NSX.
4. Re-register the SVA with NSX.
5. After successful registration of SVA, open the command prompt, and navigate to the following location:
   C:\Program Files (x86)\Symantec\Data Center Security Server\Server\tools
6. In the Command prompt window, execute the following command:
   ConfigFIPS.vbs enable
See “Deploying a Security Virtual Appliance” on page 37.

Configuring DCS:S and UMC with FQDN

If you want to have multiple DCS: Server setup, then you must configure DCS:S and UMC with FQDN. In this setup, all the DCS: Server’s point to a single database.

You can now register or un-register SVA with NSX from any of the DCS: Server.

To Install and configure DCS:S and UMC with FQDN

1. Update DNS configuration to associate IP address of DCS: Server # 1 FQDN to its own IP.
2. Register DCS: Server #1 with UMC using FQDN.
3. Register DCS: Server #1 with NSX using FQDN.
4. Click Upload and Register New SVA to register SVA.
5 Install Tomcat component only on DCS: Server #2.

After few minutes, the SVA files on DCS: Server #1 are replicated to the file server on DCS: Server #2.

6 Update DNS configuration to associate DCS: Server #2 IP also to the FQDN used for DCS: Server #1.

You can now register or un-register SVA with NSX from any of the DCS: Server.
Using the Unified Management Console

This chapter includes the following topics:

- About Unified Management Console
- About User Management
- Assigning roles to users and user groups
- Role-based access control and user rights
- Accessing DCS: Server from UMC
- About the Home Page in the DCS:S view
- About the Malware Protection settings

About Unified Management Console

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

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

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

A user with the UMC Administrator role can assign predefined roles to Active Directory users or user groups for various products and features in DCS. A user or a user group can have multiple roles assigned for multiple products or features. If the credentials of a UMC user gets expired in the Active Directory, the user must be reconfigured in UMC.

To log into UMC web portal for the first time the default dcsadmin user must be used along with password specified during the appliance deployment. The default dcsadmin user is deleted after the UMC Administrator role is assigned to the first active directory user or group. The default dcsadmin user is then signed out and cannot sign in again.

The following predefined roles can be assigned to Active Directory users or groups:

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified Management Console Administrator</td>
<td>This role gives the user complete access to Data Center Security.</td>
</tr>
<tr>
<td>Operations Director Administrator</td>
<td>This role allows the user to administrate Operations Director.</td>
</tr>
<tr>
<td>DCS Server Administrator</td>
<td>This role allows the user to administrate DCS Server.</td>
</tr>
<tr>
<td>DCS Server Operator</td>
<td>This role allows the user to perform day to day operations in the DCS Server.</td>
</tr>
<tr>
<td>DCS Server Viewer</td>
<td>This role allows the user to view all DCS Server content.</td>
</tr>
</tbody>
</table>

To assign predefined roles to Active Directory users and user groups for a specific product, the product must be registered and approved and the AD must be configured with UMC.

Only the UMC administrator can assign or edit any role to any users across all the products that are registered in UMC.

Note: A logged in user cannot edit the current role assigned to the user, however the user can add additional roles.

See “Configuring an Active Directory” on page 32.
Assigning roles to users and user groups

As a UMC Administrator you can Assign, Edit or Delete roles for a user or groups from the User Management workspace.

---

**Note**: Ensure that the first AD user that is added in UMC administrator role is not disabled, locked or the user password does not expire. If that happens then the user cannot log into the UMC webportal because the default dcsadmin user gets deleted after assigning the UMC administrator role to first AD user or group.

---

Assigning roles to users or user groups

You can assign role to a user or a group or edit roles of an existing user or group.

**To assign a role to a user or a group**

1. Navigate to **Setting > User Management** in UMC.
2. Select **Users** or **Groups** in the left pane.
3. Click the Add (+) icon to assign a role.
4. In the **Assign User to Role** or **Assign Group to Role** dialog and provide the following information:

   - **Active Directory**: Select the Active Directory of the user.
   - **Name**: Start typing the name of user or group. This field is an auto-suggest field and names start loading as you type.
   - **Feature**: Select the feature or product for which you want to add the role.
   - **Role**: Select the role you want to assign the user or group.
     - You can assign more than one role to a user or group.

5. Click (+) below the Role field to add another set of Feature and Role.
   - You can assign roles from multiple features or products to a user or a group.
6. Click **Assign** to assign the selected roles.

**Editing roles of a user or a user group**

You can edit the roles that are assigned to a user or a user group.
To edit a role of a user or a user group

1. Navigate to Setting > User Management in UMC.
2. Select Users or Groups in the left pane.
3. Select a user or a user group from the list. Click the Edit icon to edit the roles that are assigned to the user or a user group.
4. In the Edit User Role dialog the Active Directory and Name field are pre-filled and appear non-editable.
5. Edit the Features and Roles and click Save.

When you select a user from the list, all the groups which the user belongs to which are configured in UMC and all the roles which are assigned to the user are displayed at the bottom of the page.

When you select a group from the list, all the users which belong to the group that are added in UMC and all the roles which are assigned to the group are displayed at the bottom of the page.

Viewing Roles in DCS

You can view the details of the roles that are assigned to users and user groups of various features and products.

To view roles in DCS

1. Navigate to Setting > User Management in UMC.
2. Select Roles in the left pane.
3. Select a role from the displayed list of roles.

In the details pane all the users and user groups that are assigned the selected role are displayed.

Role-based access control and user rights

DCS:S implements role-based access control to regulate user access to the various capabilities of the product. As a user, your account is associated to a particular role, which in turn is mapped to the tasks that you can perform.

DCS:S includes the following roles:

- Administrator
- Operator
- Viewer
When you log in to the console, you have access only to those options that you have the rights to perform.

Administrator has access to every task. The options on the User Management page are available only to an Administrator. A Viewer's role is restricted to read-only access to most of the actions on the console.

The following table lists the tasks that a DCS: S user with different roles can perform from the various views of the web console:

<table>
<thead>
<tr>
<th>Task</th>
<th>Administrator</th>
<th>Operator</th>
<th>Viewer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a tag</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>View an agent</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Edit an agent</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Move an agent</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Edit agent properties</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>View agent properties</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Edit an alert</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Import an alert</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>View an alert</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>View configuration properties</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Edit configuration properties</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>View configuration</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Generate Diagnostic Package</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Add a domain</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Rename a domain</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Delete a domain</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Edit an event</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>View an event</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Group application data</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Edit a group</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Move a group</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Task</td>
<td>Administrator</td>
<td>Operator</td>
<td>Viewer</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------</td>
<td>----------</td>
<td>--------</td>
</tr>
<tr>
<td>Edit group properties</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>View group properties</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Run Live update</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>View a monitor</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Edit a monitor</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Import a monitor</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>View a notification</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Edit a notification</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Register NSX server</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Manage OVA</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Apply a policy</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Edit a policy</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Edit a policy folder</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Move a policy folder</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>View policy folder properties</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Edit policy folder properties</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Import a policy</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Move a policy</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>View policy properties</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Edit policy properties</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Publish a policy</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>View a policy</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Remove tag</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>View scan details</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Edit a scan</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Cancel a scan</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
## Accessing DCS: Server from UMC

You can access DCS: Server from Unified Management Console only.

**To access DCS: Server**

1. Log in to UMC using the following URL format.
   
   `https://<UMC appliance IP>:8443/webportal/#/`


## About the Home Page in the DCS:S view

After you install UMC and register DCS:S with UMC, you can access the DCS:S pages from the UMC console. The Home page in the Server view provides the malware protection and threat detection status, and displays whether the AV and GNTP definitions of DCS:S are up-to-date or not. The SVAs pane displays the number of Security Virtual Appliances that are online along with other details.

- SVAs
- Network Threats Detected
- Viruses Detected
- Top 10 GVMs with network threats remediated
- Top 10 GVMs with virus threats remediated
- Global Threatcon
About the 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

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

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

Displays the top 10 guest virtual machines having malware virus detected.

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 Malware Protection settings

The Malware Protection settings control the maintenance of security virtual appliances, and manage the commands that are run on the security virtual appliance.

You can navigate to the Malware Protection pane by navigating to Settings > System > Malware Protection.

When a security virtual appliance is detected as offline for the last 30 days, the virtual appliance gets deleted.

You can configure the Malware Protection settings to delete the commands when the commands stop responding after a specific period of time.

Commands older than the age that you specify are purged.

The Malware Protection settings are as follows:
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Delete SVA which are offline since last [n] days. (1-90)</strong></td>
<td>You can configure to delete the security virtual appliances that are detected as offline. The default value is 30 days.</td>
</tr>
<tr>
<td><strong>Cancel/Fail commands with no progress for [n] hours. (1-72)</strong></td>
<td>Select this check box to cancel the command that is not making any progress. You can specify the time in hours since when there has been no progress. The default value is four hours.</td>
</tr>
<tr>
<td><strong>Purge commands older than [n] days. (1-9999)</strong></td>
<td>Select this check box to purge old commands, and then type the age of the command, in days. The default value is seven days.</td>
</tr>
</tbody>
</table>

See “About the Home Page in the DCS:S view” on page 52.
Managing Policies

This chapter includes the following topics:

- About policies for agentless protection
- Creating policies for agentless protection
- Creating an AV policy for Windows GVMs
- Editing an AV policy for Windows GVMs
- Creating an SVA configuration policy
- Editing SVA configuration policies for agentless protection
- Publishing a policy
- Viewing a published policy
- Unpublishing a policy

About policies for agentless protection

Symantec Data Center Security: Server uses the antivirus policies, configuration policies, and guest network protection policies to let you protect your virtual environment. You can create multiple instances of Antivirus, Network Security, and SVA configuration policies, edit the policy settings, and publish them to protect your virtual environment.

In the left pane, you can see the different types of policy categories.

In the right pane, you can see the different policies. You can add, edit, copy, delete, import, export, publish, and unpublish a policy. You can make changes to the configuration settings of a policy without affecting the system behavior. To reflect the changes in the policy, you must publish the policy again.
You can edit published and unpublished policies. In the right pane, all the policy details such as policy name, revision, policy type, last modified date, and status are displayed.

- Blue flag indicates the total number of policies available based on the category selected.
- Red flag indicates the policy is not published.
- Green flag indicates the policy is published.
- Purple flag indicates the policy is modified, and need to be published again.

The configuration policy has the configuration settings that are applicable to the security virtual appliances. The antivirus policy consists of the configuration settings on how protection can be provided to the guest virtual machines. The network protection policy has the configuration settings to block the threats at network level.

The filters that are available to view the policies are:

- All Agentless Protection policies
- AV Protection policies
- SVA Configuration policies
- Guest Network Protection policies

About predefined policies

DCS:S offers three predefined policies — two antivirus policies, one network security policy, and one configuration policy. The antivirus policies consist of the configuration settings on how protection can be provided to the guest virtual machines. The configuration policy has the configuration settings that are applicable to the security virtual appliances. At any point in time, only one SVA configuration policy and one Network security policy can be published for all the security virtual appliances.

**AV Policy – Scan On Apply**

The **AV Policy – Scan On Apply** scans the guest virtual machines within a security group for virus and threats as per the configured settings in the policy. When an antivirus policy is bound with the NSX security policies, and then applied to a security group, and the **AV Policy – Scan On Apply** is applied, all the guest virtual machines within the security group are scanned as per the configured settings. The configuration settings for this policy that are available by default are:

- On-access threat protection
- Reputation lookups
- Delete threat on detection
Add security tags to the guest virtual machines on threat detection

Scan guest virtual machines when the policy is applied

Remove tag after clean and successful completion of scan

**AV Policy – Scan On Access**

Whenever a file or folder is accessed on a guest virtual machine, all the settings that were configured for the **AV Policy – Scan On Access** comes into effect. The default options available are on-access threat protection, reputation lookups, and add security tags to the guest virtual machines. The delete threat on detection and scan the guest virtual machines when the policy applied options are not available by default.

While configuring the AV Policy – Scan On Access settings, if you do not enable the Delete Threat option, multiple events are generated each time the same threat is detected. The events are not suppressed, and you can view them in the web console by grouping the related events together.

**Network Security Policy**

Network Security policies are used for specifying settings to monitor Network traffic. If the block option is checked, it detects, logs, and blocks the network threat. If the block option is unchecked, then it detects and logs the Network threat. This policy can be applied on Windows GVMs only.

You can define the traffic to be monitored by selecting from the following options:

- All endpoints (servers and desktops)
- All server
- Only Microsoft Exchange Server
- All desktops

**SVA Config Base Policy**

The **SVA Config Base Policy** defines the communication settings and external server settings of the security virtual appliance. Only one predefined **SVA Config Base Policy** gets published after the security virtual appliance is registered. This policy cannot be unpublished, but can be replaced with a new instance of the **SVA Config Base Policy**. This policy can be applied on Windows GVMs only.

**About antivirus policies**

Antivirus policy contains the configuration settings for security services provided by Symantec Anti-malware Service. The service configuration can be configured for Symantec Anti-malware Service in VMware security policy. Based on the
configuration settings, a security policy is applied to a security group, and protection is provided by the security virtual appliance.

All the guest virtual machines in the security group are protected using the configurations as per the applied antivirus policy.

You can create the antivirus policy from the DCS: Server web console, publish the policy on the NSX Manager, configure the antivirus policy as service configuration for VMware security policy, and then apply the VMware security policy to the security group for the antivirus policy to take effect.

Creating policies for agentless protection

You must create a policy that is based on a policy template from the policy pack. You can also create a policy that you customized using the DCS: Server web console before you publish it.

You can create antivirus policies, configuration base policies, and network protection policies from the web console.

The Add New Policy page lets you create a policy.

To add a policy

1. Click Manage > Policies in UMC.
3. In the Add New Policy page, do the following:
   - In the Name text box, enter a name for the policy that you create.
   - In the Description text box, enter a description for your policy.
   - From the Select Policy Template drop-down list, select one of the following template.
     - Network Security Policy
     - SVA Config Base Policy
     - AV Policy – Scan On Apply
     - AV Policy – Scan On Access
   - Enter all other relevant details.
4. Click Save.

You are prompted to complete a change request that describes the policy modifications.
Copying a policy

You can copy an existing policy. The copy is saved in the same folder as the original policy. The copy name is prefixed with Copy of followed by the original policy name. For example:

Copy of AV Policy - Scan On Apply

To copy a policy

1. Click Manage > Policies in UMC.
2. On the Policies page, select a policy, and click the Copy icon.

See “About policies for agentless protection” on page 55.

Creating an AV policy for Windows GVMs

You can create an AV policy for Windows GVMs that is based on a policy template. The Add New Policy page lets you create a new AV policy for Windows GVMs. You can select AV Policy Windows - Scan On Access or AV Policy Windows - Scan On Apply from the Policy Template.

To create an AV policy for Windows GVMs

1. Click Manage > Policies in UMC
2. On the Policies page, click the Add icon.
   The Add New Policy page appears.
3. Enter the following details under the General section:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the antivirus policy.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the antivirus policy. This is optional.</td>
</tr>
<tr>
<td>Select Policy Template</td>
<td>Select one of the following template from the list of policy templates.</td>
</tr>
<tr>
<td></td>
<td>■ AV Policy Windows - Scan On Access</td>
</tr>
<tr>
<td></td>
<td>■ AV Policy Windows - Scan On Apply</td>
</tr>
</tbody>
</table>

When you select a Windows policy, additional details associated with the Windows policy appear.

4. Enter the information in the following sections, and click Save.

   ■ General
## On-Access Settings

## On-Demand Scan Settings

### General section

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reputation Lookups</strong></td>
<td>Check this check box to consider verifying the file reputation during scans.</td>
</tr>
<tr>
<td><strong>Add security tag to guest VM</strong></td>
<td>Check this check box to add a tag to the guest virtual machine based on threat detection and its severity.</td>
</tr>
<tr>
<td><strong>Deny access</strong></td>
<td>Check this check box to deny access to the file that contains malicious content.</td>
</tr>
<tr>
<td><strong>Delete threat</strong></td>
<td>Check this check box to delete the file that contains malicious content. If the malicious file cannot be deleted, the file is truncated to remove the threat.</td>
</tr>
<tr>
<td><strong>Quarantine file</strong></td>
<td>Check this check box to move the quarantine files to the default location.</td>
</tr>
<tr>
<td><strong>Scan Exclusions — Extensions</strong></td>
<td>Add file extensions to the exclusions list to exempt them from scanning.</td>
</tr>
<tr>
<td><strong>Scan Exclusions — Folders</strong></td>
<td>Add folder paths to the exclusions list to exempt them from scanning. Optionally, subfolders can be included in or excluded from the exclusions list. By default, all network folders and subfolders are excluded from scanning.</td>
</tr>
<tr>
<td><strong>Scan Exclusions — Files</strong></td>
<td>Add files to the exclusions list to exempt them from scanning.</td>
</tr>
</tbody>
</table>

### On-Access Settings section

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>On-Access Threat Protection</strong></td>
<td>Check this check box to protect a file or folder from threat every time it is being accessed.</td>
</tr>
</tbody>
</table>
On-Access scan caching: Select this check box to cache a file every time it is being accessed.

Use the update sequence number (USN): Select this check box to use the update sequence number to cache while scanning.

On-Demand Scan Settings section

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Guest VM when the policy is applied</td>
<td>Check this check box to scan a guest virtual machine whenever the policy is applied.</td>
</tr>
<tr>
<td>Remove the security tag from Guest VM after clean completion of scan</td>
<td>Check this check box to remove the security tag from a guest virtual machine after a scan is complete when no threats are discovered, or identified threats are removed.</td>
</tr>
<tr>
<td>Scan Path Settings</td>
<td>Select Scan Entire System or Scan Targeted Paths to configure scan path settings for on-demand scans.</td>
</tr>
<tr>
<td>Scan Entire System</td>
<td>Scan the entire system.</td>
</tr>
<tr>
<td></td>
<td>You can optionally check the Include Shadow Copy Volumes check box to enable scan of the shadow copy volumes.</td>
</tr>
<tr>
<td></td>
<td>By default, the shadow copy volumes are not scanned.</td>
</tr>
<tr>
<td>Scan Targeted Paths</td>
<td>Scan only the selected file paths and folders that are added to the scan file paths list or scan folder paths list.</td>
</tr>
<tr>
<td>On-Demand scan caching</td>
<td>Select this check box to cache the scanned files, so that the cached files can be quickly accessed at a later time, when needed.</td>
</tr>
</tbody>
</table>

Editing an AV policy for Windows GVMs

You can modify the general settings, on-access scan settings, on-demand scan settings, and exclude folders and files from scanning by editing the AV policy for Windows GVM as required.
To edit an AV policy for Windows GVM

1. Click **Manage > Policies** in UMC.
2. In the left pane, under **All Agentless Protection**, expand **AV Protection**, and select **Windows**.
3. In the right pane, click on the policy name that you want to modify.
4. In the **Edit Policy** page, edit the values for the settings that you want to modify in any of the following sections:
   - **General**
   - **On-Access Settings**
   - **On-Demand Scan Settings**
5. Click **Save** to save the changes.

You are prompted to complete a change request that describes the policy modifications.

Creating an SVA configuration policy

The SVA configuration policy is a collection of predefined configuration settings that is applicable for all the registered security virtual appliances. At any given point in time, only a single instance of the SVA configuration policy can be published to all the security virtual appliances. You can modify the general communication settings, scan settings, and LiveUpdate schedule settings of the SVA configuration policy as required.

To create an SVA configuration base policy

1. Click **Manage > Policies** in UMC.
2. On the Policies page, click the **Add (+)** icon. The **Add New Policy** page appears.
3. Enter the following details under the **General** section:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the antivirus policy.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the antivirus policy. This is optional.</td>
</tr>
</tbody>
</table>

**Select Policy Template**

Select **SVA Config Base Policy**.

When you select the SVA Config Base Policy, additional details associated with the policy appear.

4. Enter the information in the following sections, and click **Save**.

- **General**
- **Communication**
- **Scan Settings**
- **Whitelisted Files**
- **LiveUpdate Schedule**
- **LiveUpdate Server Settings**
- **Proxy Server Settings**

### General section

<table>
<thead>
<tr>
<th>Field name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the SVA configuration policy.</td>
</tr>
<tr>
<td>Description (optional)</td>
<td>Description of the SVA configuration policy, and this is optional.</td>
</tr>
<tr>
<td>Policy Type</td>
<td>Type of the policy.</td>
</tr>
</tbody>
</table>

### Communication section

<table>
<thead>
<tr>
<th>Field name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polling Interval</td>
<td>The frequency in minutes and seconds when the security virtual appliance polls the management server for configuration changes. The default value is 5 minutes.</td>
</tr>
</tbody>
</table>
Connection Timeout

The TCP connection timeout is configured for the security virtual appliance to connect with the management server.

The default value is 30 seconds.

Notification Port

The port that is used to receive notification from the management server when a configuration update is available. The security virtual appliance then fetches the update immediately.

The default real-time notification port is 2222.

NTP Server

The Network Time Protocol server can be configured by providing the server details.

Scan Settings section

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum concurrent scheduled scans per ESX host</td>
<td>Schedule the maximum number of scans for guest virtual machines that can run concurrently on an ESX host in the available scan window.</td>
</tr>
</tbody>
</table>

The default number of concurrent scans is two.
Schedule scan time interval

Check this check box to enable scheduled scans for guest virtual machines.

The default scan interval is seven days.

Set the minimum interval in days between two scans for a guest virtual machine by selecting any of the following:

- **Allow anytime**
- **Schedule**

By selecting **Schedule**, you can configure the hourly time slots when a security virtual appliance can run the scheduled scans on the guest virtual machines. You can also decide specific hourly slots when you do not want to run any scans.

Select the day and time as required to schedule scans. The blue square indicates the hourly slot when a scheduled scan can run, and the white square indicates the hourly slot when a scheduled scan cannot run. By default, scans are scheduled to run on weekdays from 12:00 midnight to 6:00 A.M., and 7:00 P.M. to 12:00 midnight. On weekends, scans are scheduled to run for 24 hours.

---

**Whitelisted Files section**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Whitelisted Files</td>
<td>Add file hashes to the Whitelisted Files list to prevent them from scanning. Click <strong>Add (+)</strong> icon to add more files.</td>
</tr>
</tbody>
</table>

**LiveUpdate Schedule**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduled update</td>
<td>Check this check box to enable the LiveUpdate server to run the updates at scheduled intervals.</td>
</tr>
<tr>
<td>Every 15 mins.</td>
<td>Schedule to run the updates every 15 minutes.</td>
</tr>
<tr>
<td>Hourly</td>
<td>Set the hour you want the updates to run.</td>
</tr>
</tbody>
</table>

The default is four hours.
Daily
Set the time of day you want the updates to run.

Weekly
Set the day of the week and time of day you want the updates to run.

LiveUpdate Server Settings and Proxy Server Settings

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LiveUpdate Server Settings</td>
<td>Use the default Symantec LiveUpdate server settings provided.</td>
</tr>
<tr>
<td>Proxy Server Settings</td>
<td>Click Setup Proxy Server or the already configured proxy server to open the Proxy Server setting. The Proxy Server setting opens in either a new tab or in an already opened UMC tab. Add or edit the proxy server settings, and save the settings. Open the SVA config policy again and save the policy.</td>
</tr>
</tbody>
</table>

Editing SVA configuration policies for agentless protection

You can edit a SVA configuration policy to adjust the policy options.

For editing a policy, select the configuration base policy that you want to edit. You are prompted to complete a change request that describes the policy modifications.

Policy modifications are saved in your policy and take effect only when you publish them.

To edit a SVA configuration base policy

1. Navigate to Manage > Policies in UMC.
2. In the left pane, expand All Agentless Protection, and select the SVA Configuration.
3. In the right pane, click on the policy that you want to modify.
4. In the Edit Policy - SVA Config Base Policy page, edit the values for the settings that you want to modify in any of the following sections:
   - General
   - Communication
Publishing a policy

For a newly created or edited policy to be applied to a security group, it must be published.

To publish a policy
1. Click Manage > Policies in UMC.
2. On the Policies page, select the newly created or edited policy.
   The state of a policy appears in the Status column.
3. Select a policy that you want to publish, and click Publish.
   For the published policy to take effect, you may want to go to the VMware Web Client and apply the published policy to the security groups.

Viewing a published policy

You can view the configured settings of all the published policies in the Policies page.

To view a published policy
1. Navigate to Manage > Policies.
2. On the Policies page, click Published flag.
   List of published policies appear.

Unpublishing a policy

You can unpublish a previously published policy from the Published Policies taskpad.
To unpublish a policy

1. Navigate to Manage > Policies.

2. On the Policies page, click Published flag.
   
   List of published policies appear.

3. From the list of published policies, select the policy that you want to unpublish, and click Unpublish flag.
Protecting your network

This chapter includes the following topics:

- Introducing network-based intrusion prevention system
- Installing network virtualization components
- About Network Security policy
- Creating and editing Network Security policies

Introducing network-based intrusion prevention system

Network-based Intrusion Prevention Systems (NIPS) are the network security appliances or applications that monitor the network traffic comprising network segments or devices, and analyze the network and the protocol activities for any suspicious activities. The main functions of intrusion prevention systems are to protect the network from threats such as identify malicious or suspicious activities, log information about these activities, attempt to block or stop them, and report them.

When a threat is detected at the application layer or protocol, Symantec's network security service logs the information of the threat and appropriate action is taken as per the policy that is applied. Details of all the detected threats as well as the blocked threats are displayed on the Unified Management Console.

Guest Network Security monitors network traffic through integration with NSX 6.1.2. NSX communicates to SVA when to begin monitoring network traffic as well as when to stop monitoring network traffic. Administrators should use best practices when establishing security groups and applying network threat protection policies to those security groups for appropriate protection.
The SVA limits the maximum number of protected TCP flows to be 1000. TCP flows established after this limit is hit are not protected. Once the number of TCP connections drops below 1000, new TCP flows are then protected. The SVA expunges stale TCP flows; flows will be expunged if the last packet for that flow was observed between an hour and two hours ago. A new TCP flow can start being scanned only at the completion of a three way handshake, not later.

The SVA limits UDP protected flows as follows:

- Maximum UDP flows per virtual NIC is 300.
- Maximum number of UDP flows per SVA is 6000.
- Stale UDP flows are expunged on a 5 second interval.

This means that expunging this flow, new UDP traffic on this flow is then seen as a new flow by the SVA.

In order to self protect the SVA, network security service may be restarted when the SVA limits are reached.

**Working of NIPS in DCS:S**

By integrating with VMWare’s NSX Manager, Symantec Data Center Security: Server gains access to network traffic from or to the guest virtual machines within the security group. The working of NIPS is as follows:

- NetX service monitors all the inbound or outbound traffic that flows to and from the guest virtual machines within the network and across different networks.
- NSX Manager monitors and redirects the network data to SVA.
- NetX service that is running on the SVA reassembles and scans the network packets using signature-based detection.
- If any threat is detected, policy-defined action is taken.

**Installing network virtualization components**

After you register vCenter with the NSX Manager, you can install network virtualization components on the vSphere hosts. You must complete the host preparation under installation section of NSX.

**To install the host preparation**

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 **Host Preparation** tab.

5 From the table, select the cluster where you want to install the components, and click **Install**.

After the network components are installed, expand the cluster and verify that all the hosts in the cluster are in the **Ready** state under the Installation Status column, the component version is displayed, and firewall is enabled.

### About Network Security policy

The Network Security policy is the pre-defined policy that protects your network from suspicious activities. You can create the Network Security policy from DCS:S by selecting the policy template from the policy pack.

You can configure the General settings and the Network Security policy settings as required.

NSX v6.1.2 may start sending network traffic to the SVA before NSX v6.1.2 provides network security policy information for that network traffic. Until the policy information is received by SVA, the network traffic is not protected. Administrators must follow VMware best practices for configuration of security groups and virtual machine management to minimize this delay.

The definitions are required in order to get the full functional behavior of Antivirus services and Network Protection services. For getting the definitions, you must update the LiveUpdate Server settings using Administrator privileges.

### Creating and editing Network Security policies

You can create the Network Security policy from the DCS:S by selecting the policy template from the policy pack.

**To add a network security policy**

1 Click **Manage > Policies** in UMC.

2 Expand **All Agentless Protection** in the left pane and select Guest Network Protection.

3 In the right pane, click **Add**.

4 In the **Add New Policy** page, do the following:
   
   ■ In the **Name** text box, enter a name for the policy that you create.
   
   ■ In the **Description** text box, enter a description for your policy.
From the **Select Policy Template** drop-down list, select the policy pack that you want to use as the baseline for the new policy.

5. In the **Guest Network Threat Policy Settings** page, select one of the following to apply network security policy settings to it:

- **All endpoints (servers and desktops)**
- **All servers**
- **Only Microsoft exchange server**
- **All desktops**

6. Click **Save**.
   
   You are prompted to complete a change request that describes the policy modifications.

**To edit a guest network protection policy**

1. Click **Manage > Policies** in UMC.

2. In the left pane, under **All Agentless Protection**, select **Guest Network Protection**.

3. In the right pane, click on a policy that you want to modify.

4. In the **Edit Policy** page, edit the values for the settings that you want to modify.

5. Click **Save**.

   You are prompted to complete a change request that describes the policy modifications.
Quarantining files

This chapter includes the following topics:

- About quarantining files
- About the SVA Extension driver
- Installing the SVA Extension driver
- Uninstalling the SVA Extension driver
- How to quarantine a file
- Purging quarantined files
- Establishing local quarantine file thresholds
- Automatically deleting quarantined files
- Rescanning quarantined files
- Generating events upon quarantine

About quarantining files

Upon detection of a threat, DCS:S lets you send infected files to a local quarantine folder. You can configure the quarantine option in the antivirus policies and send infected files to the local quarantine folder.

When an infected file is quarantined, the virus or risk cannot infect other files on your guest virtual machines or other guest virtual machines in the datacenter. However, the quarantine action does not clean the risk. The risk stays on your guest virtual machine until the file is cleared of the risk, and is tagged after a successful rescan. To make the infected file inert, the file is altered by adding a header and footer, and encrypting it.
When the SVA downloads the latest virus definitions, the files in the quarantine folder can be rescanned. If the latest definitions find a file to be clean, the clean file is restored to its original location.

If you want to quarantine infected files, you must install VMware Tools with the EPSec driver. You must enable the quarantine option while configuring the antivirus policies for Windows GVMs, and then install the SVA Extension on the Windows guest virtual machine where you want to perform quarantine. A quarantine folder is then created on the guest virtual machine, and the infected files are moved to that folder.

**About the SVA Extension driver**

To quarantine an infected file, perform the following steps and install the SVA Extension driver on the Windows guest virtual machines. When a threat is detected on the guest virtual machines, only the actions configured in the policy come into effect.

- Enable EPSEC communication channels between the AV engine and the guest virtual machine during the installation of VMware Tools with the EPSec driver.
- Enable the Quarantine files option while configuring the general settings of the Basic Antivirus policy.
- Ensure that you install Symantec Virtual Extension driver on all the guest virtual machines within the security group. See Installing the SVA Extension driver on page 74.

The virtual agent, toaster, and SymEFA components get installed during the driver installation. A quarantine folder is created where the infected files are placed. To access the quarantine folder, you must have administrative rights. The default path of the quarantine folder is created on the drive where windows is installed.

For example, if windows is installed on drive C, the default path is:

```
C:\ProgramData\Symantec\VirtualAgent\Quarantine
```

**Installing the SVA Extension driver**

To enable the quarantine of detected threat, you must install SVA Extension driver on Windows guest virtual machine.
To install SVA Extension driver

1. On the installation CD, double-click SVAExtension.exe
2. Or type the following parameter at the command line:
   
   msiexec /i SVA_Extension.exe /l*v install.log

   The log files are stored at the same location as the installer.

Uninstalling the SVA Extension driver

You can uninstall the SVA Extension driver and its components from Windows guest virtual machine by using command line parameters or by removing it from Control Panel.

To uninstall SVA Extension driver

1. On the Windows guest virtual machine that runs the services, click Start > Settings > Control Panel > Add/Remove Programs.
2. Click Symantec Virtual Extension, and then click Remove.
3. Follow and complete the prompts until uninstallation completes.

Or, you can type the following parameter at the command line for uninstalling the services:

   msiexec /x SVA_Extension.exe /l*v uninstall.log

How to quarantine a file

While configuring the general settings for antivirus policies for Windows GVMs, you can define any one of the following actions to be performed when a threat is detected:

- Deny Access
- Delete Threat
- Quarantine File

To enable quarantining files, navigate to Manage > Policies, and click on Add icon or edit an existing Antivirus policy. In Add New Policy or Edit Policy page, under General Settings > Threat Detection Actions, check the Quarantine file option to ensure the infected files that are detected during scans and are moved to the quarantine folder.

For example, when On-Access Threat Protection is enabled, and if the accessed file is infected, it is moved to the quarantine folder. On the other hand, when a scan
is scheduled on a specific folder, path, or entire system, or an on-demand scan is running, all the infected files are moved to the quarantine folder.

### Purging quarantined files

You can prevent the buildup of files in the quarantine folder. You can specify the duration up to when a file must be retained in the local quarantine folder. You can also configure how you want to respond when the threshold is met.

For example, if you have configured to purge files older than a specific number of days, and if the threshold is met, the oldest file from the quarantine folder is purged first.

The default purge interval is 30 days. You can retain the files in the quarantine folder for a maximum of 90 days.

### Establishing local quarantine file thresholds

There is a limit to the number of files that can be moved to the quarantine folder. Similarly, there is a limit to the file size and the folder size too.

The maximum number of files that you can store in the quarantine folder is 1000. The maximum file size is 100MB, and the maximum size of the quarantine folder is 500 MB. Depending on the AV Policy settings, when any one of the thresholds is met, no more infected files are moved to the quarantine folder. If AV Policy setting is with Purge enabled, then it will delete old file and allow new file to be quarantined.

These settings prevent the buildup of files in the quarantine folder.

### Automatically deleting quarantined files

By default, the files in the quarantine folder are retained for 30 days. You can customize an antivirus policy to automatically remove files from the quarantine folder after retaining them for a specified number of days.

**To configure automatic deletion of quarantine files**

1. Navigate to **Manage > Policies**.
2. On the **Policies** page, click on an antivirus policy.
3. In the **Edit Policy - AV Policy - Scan On Access** page, under **Threat Detection Actions**, check **Quarantine file**.

The deleted files are stored in the default location specified against the **Quarantine file** option.
Rescanning quarantined files

You can configure to rescan all the files in the quarantined folder by enabling the Enable On-Access Threat Protection and Rescan quarantined files when On-Demand scan runs options. The Rescan quarantined files when On-Demand scan runs option appears after you select Quarantine file option.

Rescan happens when these options are enabled and the on-demand scan is running. The quarantined files are compared against the latest definitions. If they are found to be clean, these files are restored to the original location.

To configure rescan of quarantined files

1. Navigate to Manage > Policies.
2. On the Policies page, click on an antivirus policy.
3. In the Edit Policy page, under the General section, under Threat Detection Actions, enable the Quarantine File option.
4. Check Re-scan quarantined files when On-Demand scan runs if you want to re-scan the quarantined files.

Note: You can re-scan a quarantined file only if the on-demand scan is running.

Generating events upon quarantine

You can configure the antivirus policy to quarantine the infected files upon detection. For all the threats that are detected, a corresponding File quarantine event is generated. The remediation is to move the infected file to the quarantine folder.

You can view the event that is generated after a file is quarantined in the Malware Protection Events pane under the Monitors tab.

File quarantine event: Contains information of the detected threat, time when the file was created, and the remediation offered.

Note: The rescan option is available only on the File quarantine event.

Some of the Event types generated upon quarantine are as follows:

- Server Status
- Agent Status
- Endpoint Malware Threat Detection
- Endpoint Malware Quarantine Status
- Content Update Status
Scanning and tagging

This chapter includes the following topics:

- About the types of scans
- About excluding items from scans
- About tagging
- Tagging a guest virtual machine
- Untagging a guest virtual machine
- Scanning a GVM or a security group

About the types of scans

DCS:S offers the on-access and on-demand scans to provide protection against different types of viruses, threats, and risks. The on-demand feature provides Scan now and Schedule scan options. You can scan a virtual machine for which Yes appears under Protected column.

On-demand scans are the scans that you start manually. This scan includes the scans that are triggered as a result of scan commands and antivirus policy change on guest virtual machines. You can trigger an on-demand scan on a security group or an individual guest virtual machine. To initiate a manual scan, navigate to Manage > NSX Security Groups > Security Groups, and select a security group and select the guest virtual machines that you want to scan, and select the any of the following options from the Scan drop-down.

- Default Scan
- Scan Entire System
- Scan Targeted Paths
You can start a queue of new on-demand scan as soon as you cancel an existing on-demand scan. The request to cancel a scan is processed immediately, and the new scan begins successfully.

You can plan to run scheduled scans on the guest virtual machines by defining the scan window when scheduled scans are permitted to run. By default, no active scheduled scans are enabled to run at a specific time. Scanning happens based on the eligibility of a guest virtual machine. The eligibility criteria is determined by the last scanned time and the configured scan time interval.

The security virtual appliance can concurrently schedule scans on multiple guest virtual machines as per the maximum number of concurrent scans that are configured in the SVA Config Base Policy. The default number of concurrent scans that can be scheduled is two and the maximum is 100. If a guest virtual machine is offline, no scan is scheduled on that guest virtual machine. You cannot perform two on-demand scans concurrently on a guest virtual machine. Additional requests to scan a guest virtual machine are queued, and then run after the previous scan request is completed.

**Note:** When a scan is completed, you may observe the count of files that are scanned is different from the total number of files on a guest virtual machine. The difference is observed if files are skipped from scan due to reasons such as permissions, opportunistic locking, low resources, sharing, and so on.

### About excluding items from scans

If you have scanned a guest virtual machine or security group and know that certain files are safe, you can exclude them from scanning. In some cases, exceptions can reduce scan time and increase system performance. Exceptions are the known files, file extensions, and folder paths that you want to exclude from a scan.

You can add files, file extensions, folders, and subfolders to the exclusions list. By default, all network folders and subfolders are excluded from scanning. If you do not want to exclude a network folder from scanning, remove \ from the Excluded Folders list under Scan Exclusions -> Folders. However, excluding network folders and subfolders from scanning is likely to affect system performance.

### About tagging

Tagging is a feature provided by VMware that enables you to distinguish clean guest virtual machines from other infected guest virtual machines. The guest virtual machines that have had a malicious attack can then be isolated or quarantined with outbound communication blocked. A cleanup action can be initiated to remove the
Tagging a guest virtual machine

Whenever a guest virtual machine is scanned, the policy that is associated with the security group to which the guest virtual machine belongs, takes effect. If a threat is detected and if the Add Security Tag to the Guest VM option is enabled while adding or editing a policy, the management server tags the guest virtual machine with a security service tag. The three different security service tags used are:

1. ANTI_VIRUS.VirusFound.threat=high
2. ANTI_VIRUS.VirusFound.threat=medium
3. ANTI_VIRUS.VirusFound.threat=low

If no threat is detected, an event with a Scan has completed successfully message is generated and you can view it in the Events page.

If a threat is detected, an event with a Threat Detected message is generated and you can view it in the Events page. Subsequently, another event with a message Successfully tagged VM, MOID: vm-xx, Tag ID: ANTI_VIRUS.VirusFound.threat=high is generated after the management server tags the infected guest virtual machine. vm-xx is themoid of the guest virtual machine that is under protection.

Note: A guest virtual machine that is not tagged by the management server, but is manually tagged from the vSphere Web client, can be untagged manually by selecting and right-clicking the Scan has completed successfully event, and then clicking Remove security tag from Guest VM in the Event Wizard.

Untagging a guest virtual machine

After a threat is detected and a guest virtual machine gets tagged, you can initiate an action to clean the infected guest virtual machine. You can choose to run a manual scan immediately or schedule a scan, and if the threat does not persist any longer, the management server untags the guest virtual machine. An event with the

Event: Scan completed successfully, removing all security tags, if available., MOID: vm-28, Tag ID: low, medium, high message is generated, and you can view it in the Events page.
If the AV policy is not configured to remove the tag, the tag continues to remain even after the scan is completed.

Scanning a GVM or a security group

You can scan your GVMs or a security group for any threat. When you scan a security group, all the GVMs in that security group are scanned.

To scan a GVM or a security group

1. Navigate to Manage > NSX Security Groups in UMC.
2. Do one of the following:
   - On the right pane, under Security Groups page, select a security group
   - On the left pane, under Security Groups, select a security group, and select a guest virtual machine associated to that group in the right pane.
3. Click Scan, and select one of the following options to run a manual scan on a targeted group or on a GVM:
   - **Default Scan** - Scans a GVM or all the GVMs under a security group, as defined in the policy template.
     If you select this option, Confirm Operation dialog appears. Click Yes to confirm the operation.
   - **Scan Entire System** - Scans the entire GVM or all the GVMs under a security group.
     If you select this option, Confirm Operation dialog appears. Click Yes to confirm the operation.
   - **Scan Targeted Paths** - Scans the targeted paths of a GVM or all the GVMs under a security group.
     If you select this option, Scan Targeted Paths window appears. Do the following:
     - In the File Paths field, enter the file path of a GVM or GVMs for which you want to scan.
       Optionally, click + icon to add more file paths.
     - In the Folder Paths field, enter the folder path of a GVM or GVMs for which you want to scan.
       Optionally, click + icon to add more folder paths.
     - Click Scan.
     A message appears indicating that the scan is triggered successfully.
Viewing events

This chapter includes the following topics:

- About events
- About the Malware Protection Events pane
- About event severity levels
- Exporting events
- Purging events

About events

Events are informative, notable, and critical activities that concern the DCS:SA agent and Symantec Data Center Security: Server. The agent logs events to the management server, and the Symantec Data Center Security: Server lets you view summaries and details of those events.

An agent's log rules determine which events are sent to the management server.

You can use the Home page in the Symantec Data Center Security: Server to obtain an overview of events that are being generated in your network.

You can use the DCS:SA agent event viewer to display recent events that were reported by a DCS:SA agent.


About the Malware Protection Events pane

A security virtual appliance’s malware protection policy generates events for on-demand scan, scheduled scan, threat detection, content updates, or antivirus
services. You can view the events generated for malware protection in the Malware Protection Events pane under the Monitors tab. The events pane on the right is sorted by the descending total number of malware protection events for a security virtual appliance, which causes the most recent events to be at the top of the list.

You can view the .csv file using a text editor or spreadsheet program. For troubleshooting purposes, you can view the additional event details that comprises information such as source machine, date, event type, severity, and description.

See the Symantec™ Data Center Security: Server Advanced Administrator’s Guide for more information about events and event categories in DCS:S.

Event types

Event types are as follows:

- Malware Protection
  - Threat Detected Events – Contains information about the detected threat.
  - Scan Status Events – Contains information about the status of a scan.
  - File Scan Timeout Events – Contains information about the File Scan Timeout.
  - SVA Over-subscribed Events – Contains information when the threshold of security virtual appliance for guest virtual machines is out-of-limit.
  - Guest VM Protection Events – Contains information about an unprotected guest virtual machine when the security virtual appliance has reached its threshold.

- Network Protection
  - Threat blocked events – Contains information about the blocked events.
  - Threat unblocked events – Contains information about the unblocked events.

- Management
  - Agent Status Events – Contains information about the status from the security virtual appliance such as the policy applied.
  - Content Revision (in use) Events – Contains information about the version of the LiveUpdate content when it is put to use by the security virtual appliance.
  - Content Update Status Events – Contains information if the LiveUpdate content download status is pass or fail.
  - SVA Integrity Check Status Events – Contains information if the security virtual appliance integrity check is pass or fail.
Root Access Events – Contains information about the root access on the security virtual appliance.

To view a malware protection event detail

1. Navigate to Monitor > Events in UMC.
2. In the left pane, select Malware Protection under All, for viewing events.
3. In the right pane, select the events that you want to view, and you can perform any of the following tasks:
   - To export events to a .csv file, select an event and click Export.
   - To add file hash to whitelisted files, select an event and click More > Add to whitelisted files, and provide the required information.
   - To add a security tag to a guest virtual machine, select an event and click More > Add security tag to guest VM. In the Add Security Tag to Guest VM dialog, you can define the severity of the tag you want to apply, and click Submit to modify the tag.
   - To view event details, select an event. The event details are displayed under the Details tab on the same page.

About event severity levels

Symantec Data Center Security: Server assigns a severity level to each event.

The event severity levels are as follows:

<table>
<thead>
<tr>
<th>Severity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Info</td>
<td>Events with a severity of Info contain information about normal system operation.</td>
</tr>
<tr>
<td>Notice</td>
<td>Events with a severity of Notice contain information about normal system operation.</td>
</tr>
<tr>
<td>Warning</td>
<td>Events with a severity of Warning indicate unexpected activity or problems that have already been handled by Symantec Data Center Security: Server. These Warning messages might indicate that a service or application on a target computer is functioning improperly with the applied policy. After investigating the policy violations, you can configure the policy and allow the service or application to access to the specific resources if necessary.</td>
</tr>
<tr>
<td>Major</td>
<td>Events with a severity of Major imply more impact than Warning and less impact than Critical.</td>
</tr>
</tbody>
</table>
Events with a severity of Critical indicate activity or problems that might require administrator intervention to correct.

### Exporting events

DCS:S offers the option to export events to a CSV file. You can view the comma-separated value (CSV) file by using a text editor or a spreadsheet program.

**To export events**

1. Navigate to Monitors > Events.
2. On the All Events page, select the events that you want to export, and then click the Export icon.

   To export multiple events, hold down the Shift or Ctrl key while you select the events. To export the current page or all pages, you need not select the events.
3. In the event-export dialog, specify the following information:

   - **Open with**
     Select this option if you want to open and view the contents of the file.
   - **Save File**
     Select this option if you want to save the file.
   - **Do this automatically for files like this from now on**
     Select this option if you want to set the earlier selection as a default option for exporting.

4. Click OK.

### Purging events

You can specify how long to retain real-time, profile, and analysis events in the DCS:S database.
To purge events

1. Click **Settings**.

2. In the **System** page, under the **Event Management** section, use the following options to configure the purge settings:

   - **Purge Real-Time Events older than** <number of> day(s) (1 to 999999)
     - Check to purge the real-time events from the database upon reaching the specified threshold.
     - The default value is 365 days.

   - **Purge Profile Events older than** <number of> day(s) (1 to 999999)
     - Check to purge the profile events from the database upon reaching the specified threshold.
     - The default value is 60 days.

   - **Purge Analysis Events older than** <number of> day(s) (1 to 999999)
     - Check to purge the analysis events from the database upon reaching the specified threshold.
     - The default value is 60 days.

---

**Note:** When a guest virtual machine is deleted from your VMware infrastructure, DCS:S deletes all information about that guest virtual machine including the command history for the guest virtual machine after you refresh the VMware Inventory.
Reporting

This chapter includes the following topics:

- About the Symantec queries and reports
- Viewing the Reports page
- Managing queries
- Managing reports
- Publishing a query or report

About the Symantec queries and reports

Symantec Data Center Security: Server includes over 75 predefined queries and reports that provide an overall view of your deployed environment, and prevention, detection, and management activity.

About the Symantec queries

The Symantec queries can help you identify groups with policies that provide no protection or only partial protection. The queries can help you identify agents that are disconnected from the network for a period of time or that are experiencing network connectivity issues.

The Symantec queries are grouped by the following categories:
### Agents
Agent queries provide information about the following:
- Agent details, such as host name, IP address, agent version, asset network path, and OS version
- Agent counts based on OS type and version
- Offline agents that are not communicating with the management server
- Agents with no prevention policies or with overridden policies
- Counts of registered agents for each network path
- Duplicate agents

### Events
Event queries provide information about agent, prevention, detection, and management events, including information about the following:
- Agent event counts for all agents
- Agent event counts by day, week, month
- Event counts grouped by disposition, event type, OS network
- Event severities
- Event types

### Homepage
Home page queries provide information about agent and event statistics for the console views, including information about the following:
- Agents with errors
- Agents that are offline
- Agents with configurations pending
- Agents with policies pending

### Policies
Policy queries provide information about policy attributes. Policy queries include a glossary of all process sets and operating systems.

### Security
Security queries provide information about the following:
- Audit detail records by date/time
- Audit detail records for failed logins
- Users, roles, last login dates

### Status
Status queries provide information about the following:
- Event statistics
- DCS:SA objects by name and type
- System statistics
- Workload

The Symantec queries are stored in the Symantec folder. The folder name includes the date that Symantec released the queries.

You can use the Symantec queries as the basis for custom query development.
To view a description of a Symantec query, select the query, and then right-click Properties.

## About the Symantec reports

The Symantec reports include the following samples, which illustrate how the report feature works:

- The Last Week Event Charts report displays statistics about the previous week’s events. The report uses the following Symantec event queries:
  - Event Counts By Day (weekly)
  - Top 10 Processes (weekly)
  - Top 10 Event Types (weekly)
  - Event Severities (weekly)

- The Recent Event Summary is a two-page report that summarizes the number of events and corresponding event types. Page one shows the data for the last month; page two shows the data for the last week.
  The report uses the following Symantec event queries:
  - Event Counts by Day (weekly, monthly)
  - Top 10 Event Types (weekly, monthly)

The Symantec reports are stored in the Symantec folder. The folder name includes the date that Symantec released the reports.

To view a description of a Symantec report, select the report, and then right-click Properties.

## Viewing the Reports page

You use the Reports page in the Symantec Data Center Security: Server java console to create and run Symantec Data Center Security: Server queries and reports.

You can do the following activities from the Reports page:

- Run the Symantec predefined queries and reports
- Create and run custom queries and reports
- Publish the results from queries and reports
- Import and export queries and reports
- Organize queries and reports in folders
To view the Reports page

1. In the Symantec Data Center Security: Server java console, click Reports.
2. Under the Reports tab, click Reports.
3. On the Reports page, in the Reports pane, double-click the Symantec folder to list the Symantec reports.
4. On the Reports page, double-click a folder to expand or collapse the panes on the Reports page.

To view the Queries page

1. In the Symantec Data Center Security: Server java console, click Reports.
2. Under the Reports tab, click Queries.
3. On the Queries page, in the Queries pane, click the Symantec folder to list the Symantec queries.

Managing queries

A query is a request for information from the Symantec Data Center Security: Server Advanced management server database.

Running a query

The results from running a query appear in a tab in the Report Results pane. Each time you run a query, another tab appears.

To run a query

1. In the Symantec Data Center Security: Server java console, click Reports.
2. Under the Report tab, click Queries.
3. On the Queries page, in the Queries pane, select a query, and then right-click Run Query.
4. If the query prompts for input parameters, specify the parameter values, and then click Run query.
5. (Optional) Publish the results from running the query.
   See “Publishing a query or report” on page 104.
6. When you no longer need the query results, in the Report Results pane, click the query tab, and then click the green X icon to close the query results.
   To recover the query results, rerun the query.
Exporting query results to multiple file formats

You can export query results to a CSV, HTML, or PDF file.

To export query results to multiple file formats

1. Run the query.
2. In the Report Results pane, click the query results tab to make it the active tab.
3. Click the Export Results icon.
4. In the Export To dialog box, specify the following information:

   - **Look In**: Select the location where you want to store the file.
   - **Export range**: Select the export range.
     - For tabular queries, specify the export range (All pages, Current page, Selected rows).
     - For queries with images, specify the export range (All pages, Current page).
   - **File Name**: Type the name of the file you want to export.
   - **Files of Type**: Select the file format such as CSV, HTML, or PDF.
     
     **Note**: You can export the query output with images to a JPEG, HTML, or PDF file.

5. Click Export.
6. For the HTML and PDF file formats, type Export Title in the Export dialog box.
   
   The export title appears on the top-left corner of the query file that you export.
7. Click OK.

Creating a query

You create a query using the New Query Wizard.

The New Query Wizard prompts you to specify the following:

- Query chart type, query name, and data source
- Output columns
- Optional filters
- Optional input parameters
You follow each wizard page by clicking Next. To change a query selection, click Back to return to a previous wizard page.

To create a query

1. In the Symantec Data Center Security: Server java console, click Reports.
2. Under the Reports tab, click Queries.
3. On the Queries page, in the Queries pane, select the folder in which you want to store the query, and then right-click New Query.
4. In the New Query Wizard dialog box, specify the chart type, query name, and data source, and then click Next.
   See “Selecting the general query parameters” on page 93.
5. In the New Query Wizard dialog box, select the output columns that you want to appear in the query, and then click Next.
   See “Selecting the query output columns” on page 94.
6. (Optional) In the New Query Wizard dialog box, add filters to expand or restrict the data source, and then click Next.
   See “Selecting the query filters” on page 96.
7. (Optional) In the New Query Wizard dialog box, create the query input parameters.
   See “Creating query input parameters” on page 97.
8. In the New Query Wizard dialog box, preview the results of the query, and then click Finish to save the query.
   The query is saved in the folder that you selected. The icon next to the query name indicates the chart type that the query uses to display the query results.
9. Run the query to verify that the query works as needed.

Selecting the general query parameters

General query parameters include the following:
Chart type

Select from the following query chart types:

- Table
- Line graph
- Area graph
- Stacked area graph
- Horizontal bar
- Vertical bar
- Horizontal stacked bar
- Vertical stacked bar
- Pie

The Preview feature illustrates each chart type.

Query Name

Type a name for the query.

Data Source

Select a data source.

When you run a query, the results are based on one of the following data sources:

- Assets (agents)
- Policies
- All real-time events
- Profile events
- Analysis events
- Console audit events
- Catalog files
- Assets and objects

Advanced Query

Select this check box if you prefer to build the query SQL statement yourself. The next page in the wizard prompts you to enter the SQL statement.

Only users who are assigned the Administrators role may select the Advanced Query box.

Fast Query Mode

Select this check box to build the query so that it runs in fast (no-lock) mode.

Fast mode does not guarantee consistent results.

Selecting the query output columns

You select the output columns that you want to appear in your query.

The query output columns are as follows:
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only get the top [100] results</td>
<td>This check box limits the total number of rows (records) that appear in a query. Select the check box, and then enter the number of rows. For example, suppose you create a query that displays all the events generated by an agent. The query could potentially yield thousands of events, but you only want to show the first 500 events. You would select the Only get the top [100] results check box, and then enter 500.</td>
</tr>
<tr>
<td>Distinct results</td>
<td>Select this check box to eliminate duplicate output rows.</td>
</tr>
<tr>
<td>Show [1000] results per page</td>
<td>Type the number of output rows that you want to display per page. Applies to queries that use the table chart type.</td>
</tr>
<tr>
<td>Column</td>
<td>Select a column that you want to appear in the query results.</td>
</tr>
<tr>
<td>Aggregate Function</td>
<td>Select the aggregate function. The aggregate function performs a calculation on a set of values and returns a single value shown as a column in the query results. Select one of the following options:</td>
</tr>
<tr>
<td></td>
<td>- Count–Returns the number of items in a group.</td>
</tr>
<tr>
<td></td>
<td>- Count Distinct–Returns the number of distinct items in a group.</td>
</tr>
<tr>
<td></td>
<td>- Sum–Returns the sum of all the values (or only the distinct values).</td>
</tr>
<tr>
<td></td>
<td>- Min–Returns the minimum value.</td>
</tr>
<tr>
<td></td>
<td>- Max–Returns the maximum value.</td>
</tr>
<tr>
<td></td>
<td>- Average–Returns the average of the values in a group.</td>
</tr>
<tr>
<td>Display Name</td>
<td>Type the column heading text. By default, Display Name uses the Column name.</td>
</tr>
<tr>
<td>Display Width</td>
<td>Type the column width.</td>
</tr>
<tr>
<td>Move Up</td>
<td>To order a selected column, click Move Up and Move Down until the column is in the desired order.</td>
</tr>
<tr>
<td>Move Down</td>
<td>To remove a selected column, click Remove.</td>
</tr>
<tr>
<td>Remove</td>
<td></td>
</tr>
<tr>
<td>Add</td>
<td>To add a column to the query results, specify the column options, and then click Add to add the column to the column list.</td>
</tr>
<tr>
<td>Update</td>
<td>To save changes to a selected column, click Update.</td>
</tr>
<tr>
<td>Add All</td>
<td>To include all columns in the query results, click Add All.</td>
</tr>
<tr>
<td>Column list</td>
<td>This pane lists all the columns that appear in the query results.</td>
</tr>
</tbody>
</table>
Selecting the query filters

You use query filters to expand or restrict the data source. Each filter rule comprises <field, operator, value>.

For each filter rule, you specify the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Select the field.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Examples of valid fields include event type, event date, event severity, event disposition, OS type, agent version, host name.</td>
</tr>
<tr>
<td>Required</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Operator</th>
<th>Select the operator for the field.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Examples of valid operators include equals, not equals, in, not in, contains, not contains, greater than, less than. Some operators support the use of wildcard characters in a value. Valid wildcard characters are asterisk (*), which represents zero or more consecutive characters, and question mark (?), which represents exactly one character.</td>
</tr>
<tr>
<td>Required</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Value</th>
<th>Specify the default value for the input parameter.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Valid values vary, depending on the field. Some fields are limited to a pre-defined list, while other fields allow free-form typing.</td>
</tr>
<tr>
<td>Optional</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group By</th>
<th>Select this check box to group the output columns.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optional</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Order By</th>
<th>Select this check box to sort an output column in ascending order or descending order.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optional</td>
<td></td>
</tr>
</tbody>
</table>

To select the query filters

1. In the **New Query Wizard** dialog box, on the Configure the Filters page, select <field, operator, value>.

2. (Optional) Select the **Group By** check box to group the output columns.

3. (Optional) Select the **Order By** check box to sort an output column in ascending order or descending order.

4. Click **Add**.

5. Repeat steps 1-4 to add additional filter rules.

6. To edit an existing filter rule, edit <field, operator, value>, and then click **Update**.
Creating query input parameters

You can build a basic query with input parameters. When run, the query prompts for the parameter values.

For each input parameter, you specify the following:

<table>
<thead>
<tr>
<th>Column</th>
<th>Select the input parameter. Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operator</td>
<td>Select the operator for the input parameter. Required</td>
</tr>
<tr>
<td>Default Value</td>
<td>Specify the default value for the input parameter. Optional</td>
</tr>
<tr>
<td>Require a non-empty value at runtime</td>
<td>Select this check box to force the query user to specify a value for the input parameter. Optional</td>
</tr>
<tr>
<td>Display Name</td>
<td>Specify a custom display name for the input parameter. The display name appears when the query is run. Optional</td>
</tr>
<tr>
<td>Description</td>
<td>Specify a description of the input parameter. The description appears when the query is run. The description helps the user understand how to use the input parameter. Optional</td>
</tr>
</tbody>
</table>

When building queries with input parameters, please note the following:

- Each input parameter comprises <column, operator> or <column, operator, default value>.
- Query users can save a specific instance of a query, which they can run repeatedly. If a query is refreshed (re-run) without being closed, the query uses the same input values.
- Query users can save a query with or without input parameters. When saving a query without input parameters, users must set fixed values for the input parameters.
Queries with input parameters can be included in reports, and imported and exported.

When a query with input parameters is published, the query user is prompted for values when the query is run. The query user is not prompted for the values when the published results are used.

The following instructions demonstrate how to create an input parameter to prompt for operating system. The default value is Windows, and users must select a value from a defined list. A non-empty value is required.

To create query input parameters

1. In the New Query Wizard dialog box, on the Configure the Parameters page, in the Column box, select OS Type.
2. In the New Query Wizard dialog box, on the Configure the Parameters page, in the Operator box, select Equals.
3. In the New Query Wizard dialog box, on the Configure the Parameters page, in the Default Value box, select Windows.
4. Select the check box to require a non-empty value at runtime.
5. In the Display Name box, type Operating System.
6. Click Add.
7. In the New Query Wizard dialog box, on the Configure the Parameters page, in the Column box, select OS Type.
8. In the New Query Wizard dialog box, on the Configure the Parameters page, in the Operator box, select In.
9. Select the check box to require a non-empty value at runtime.
10. In the Display Name box, type Operating System.
11. Click Add.

Creating a query to count the number of event types

The following query is provided as a tutorial in creating a query. The query counts the number events types. The query results are shown in a pie chart.

To create a query to count the number of event types

1. In the Symantec Data Center Security: Server java console, click Reports.
2. Under the Reports tab, click Queries.
3. On the Queries page, in the Queries pane, select the folder in which you want to store the query, and then right-click New Query.
4 In the **New Query Wizard** dialog box, select *Pie* as the chart type, type Event types for the query name, select **All Events** as the data source, and then click **Next**.

5 In the **New Query Wizard** dialog box, specify the query output for the event types, and then click **Add**.

<table>
<thead>
<tr>
<th>Column</th>
<th>Select Event Type.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregate Function</td>
<td>Select Max.</td>
</tr>
<tr>
<td>Display Name</td>
<td>Type Event Type.</td>
</tr>
<tr>
<td>Display Width</td>
<td>Type 10.</td>
</tr>
</tbody>
</table>

6 In the **New Query Wizard** dialog box, specify the query output for the event type counts, and then click **Add**.

<table>
<thead>
<tr>
<th>Column</th>
<th>Select Event Type.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregate Function</td>
<td>Select Count.</td>
</tr>
<tr>
<td>Display Name</td>
<td>Type Event Counts.</td>
</tr>
<tr>
<td>Display Width</td>
<td>Type 10.</td>
</tr>
</tbody>
</table>

7 Click **Next**.

8 In the **New Query Wizard** dialog box, group the event types, and then click **Add**.

<table>
<thead>
<tr>
<th>Column</th>
<th>Select Event Type.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group By</td>
<td>Select the Group By check box.</td>
</tr>
</tbody>
</table>

9 Click **Next**.

10 Preview the query, and then click **Finish** to save the query.

**Creating a query to display event types and event severities**

The following query is provided as a tutorial in creating a query. The query lists event types and event severities. The query results are shown in a table.
To create a query to display event types and event severities

1. In the Symantec Data Center Security: Server java console, click Reports.
2. Under the Reports tab, click Queries.
3. On the Queries page, in the Queries pane, select the folder in which to store the query, and then right-click New Query.
4. In the New Query Wizard dialog box, select Table as the chart type, type Event types and severity for the query name, select All Events as the data source, and then click Next.
5. Set up the event type column, and then click Add.
   - Distinct results: Select the Distinct results check box to eliminate duplicate output rows.
   - Column: Select Event Type.
   - Display Name: Type Event Type.
   - Display Width: Type 20.
6. Set up the event severity column, and then click Add.
   - Column: Select Event Severity.
   - Display Name: Type Event Severity.
   - Display Width: Type 20.
7. Click Next.
8. Click Next, to skip the filter.
9. Preview the query, and then click Finish to save the query.

Editing a query

After you create a query using the New Query Wizard, you can go back and edit the query using the same wizard.

To edit a query

1. In the Symantec Data Center Security: Server java console, click Reports.
2. Under the Reports tab, click Queries.
3. On the Reports page, in the Queries pane, select a query, and then right-click Edit Query.
4 In the **New Query Wizard** dialog box, modify the query using the New Query Wizard.

5 On the Reports page, in the Queries pane, select the query, and then right-click **Properties**.

6 In the query properties dialog, revise the revision number and query description, and then click **OK** to save your changes.

### Editing the Symantec queries

You can use the Symantec queries as the basis for custom query development. When editing a Symantec query, you should do the following:

- Make a copy of the Symantec query.
- Save the copy in your own folder.
- Edit the copy.

Some Symantec queries are edited using the New Query Wizard. Other Symantec queries can only be edited by modifying the SQL statement.

### Managing reports

A report comprises one or more queries that are configured as a group and viewed in a single display.

### Running a report

The results from running a report appear in a tab in the Report Results pane. Each time you run a report, another tab appears.

You use the report tool bar to save and print reports, adjust your view of a report, navigate the pages in a report, and add and delete report pages.

**To run a report**

1. In the **Symantec Data Center Security: Server** java console, click **Reports**.

2. Under the **Reports** tab, click **Reports**.

3. On the Reports page, in the Reports pane, select a report, and then right-click **Run Report**.

   The report results are shown in the Report Results pane.

4. When you no longer need the report results, in the **Report Results** pane, click the report tab, and then click **Close** to close the report results.

   To recover the report results, rerun the report.
Creating a report


You can customize a report's appearance by including a title, header and footer, and your company's logo.

Reports support a maximum graphic size of 150x100 pixels.

To create a report

1. In the Symantec Data Center Security: Server java console, click Reports.
2. Under the Reports tab, click Reports.
3. On the Reports page, in the Reports pane, select the folder in which you want to store the report, and then right-click New Report.
4. In the New Report Wizard dialog box, specify the report layout, name, and page size.
   - **Report Layout**: Select one of the following report layouts:
     - One Query—Each report page shows one query centered on the page.
     - Two Horizontal Queries—Each report page shows two queries placed side by side.
     - Two Vertical Queries—Each report page shows two queries placed one on top of the other.
     - Four Queries—Each report page shows two vertical columns, with two queries in each column.
   - **Report Name**: The name of the report.
   - **Page Size**: Select a page size:
     - Portrait—The report is created using a vertical page orientation.
     - Landscape—The report is created using a horizontal page orientation.

5. Click Finish.
6. Edit the report to insert queries and customize the report appearance.

Editing a report

You can edit a report by doing the following:

- Insert queries in the report
To edit a report

1 In the Symantec Data Center Security: Server java console, click Reports.
2 Under the Reports tab, click Reports.
3 In the Reports pane, select a report, and then right-click Edit Report.

The report is shown in the Report Results pane.

Use the following toolbar icons to adjust the report view and size, add and delete pages, save, and print:

- Actual Size, Fit Page, Fit Width, Zoom In, Zoom Out, Zoom Ratio
- First Page, Previous Page, Next Page, Last Page, Go To Page
- Add a page to the report
- Delete current page from the report
- Save to Disk
- Print

4 To insert a query in the report, left-click the report and select Insert Query. Select a query from the list, and then click Add.

5 To customize the report title and header/footer text, select the placeholder for the title, header, or footer text, type the text that you want to insert, and then click OK.

6 To add your company's logo to the report, click the colored logo placeholder, browse to the directory that contains the logo, select the logo file, and then click Open.
7 To add a page to the report, click the Add a page to the report icon.
8 To delete a page from the report, click the Delete current page from the report (red X) icon.
9 To save the report changes, click the Save to Disk icon.
10 Run the report to verify the contents and appearance.

Publishing a query or report

Publishing a query or report saves a snapshot of the graphic and/or tabular results from running a query or report.

When publishing a query or report, you should note the following:

■ A published query or report is saved in a user-selected folder in the Published Results pane.

■ The date and time that a query or report was published is included in the file name. For example:
  Last Week Threat Detection Report (Wed, Dec 18, 2013)

■ You can view the published results for a query or report.

■ You cannot change the contents of a published query or report. If you need to change the contents of a published query or report, you must edit the query or report, rerun it, and then publish the new results.

■ Publishing a tabular query saves the first 10,000 rows of data.

■ You can export published queries and reports to .zip files.

■ You can export published reports as .html files.

To publish a query or report

1 In the Symantec Data Center: Server java console, click Reports.

2 Under the Reports tab, click Reports or Queries.

3 On the Reports or Queries page, select a query or report, and then right-click Publish Query or Publish Report.

4 In the Publish Query Wizard dialog box or Publish Report Wizard dialog box, select a folder in which to store the published query or report, and then click Finish.

The published query or report is saved in the Published Results pane, in the folder that you selected.
To view a published query, select the query in the Published Results under Reports tab, and then right-click Run Query.

To view a published report, select the report in the Published Results under Reports tab, and then right-click View Published Report.

Exporting a published report

You can export a report in HTML format.

Exporting a published report creates a .html file that contains a snapshot of the graphic and/or tabular results from a report.

The published date and time is included in the .html file name as follows. For example:

Recent_Threat_Detection_Summary.html (Wed, Dec 18, 2013)

While exporting a report to HTML, a folder that contains the graphic images for the .html file is created in the same folder with the .html file.

The folder name uses the name of the .html file and the text .html_files. For example:


To export a published report

1. In the Symantec Data Center Security: Server java console, click Reports.
2. Under the Reports tab, click Published Results.
3. On the Reports page, in the Published Results pane, select a published report, and then click Export.
4. In the Export to dialog box, in the Look In box, browse to the location where you want to store the file.
5. In the File Name box, type a file name for the file.
6. In the Files of Type box, select the format as .HTML.
7. Click Export to export the report in the format selected in the Files of Type box.
Managing alerts

This chapter includes the following topics:

■ About alerts
■ About the Notifications pane
■ Viewing the Alerts page
■ Configuring alert settings
■ Creating an alert
■ Creating an alert configuration
■ Enabling or disabling an alert
■ About copying alerts
■ Importing an alert
■ Exporting an alert
■ Deleting an alert
■ Purging alerts

About alerts

You use alerts to send events of interest to email messages, SNMP traps, and text files.

The Alert module polls the DCS:S database for events that match an alert filter. When a match is found, the Alert module generates and sends email messages, SNMP traps, and text files that are associated with the alert.
About email aggregation

Email aggregation combines all email messages that are sent to an email address, over a specified aggregation time interval, into a single email message.

There are two criteria for aggregation: time interval and maximum email message size. Email aggregation prevents flooding email addresses with too many messages or with messages that exceed size limitations. (Some email accounts may reject email messages based on message size.)

The aggregation time interval starts when the Alert module is first started or immediately after sending emails for alerts from the last time interval. Once the specified number of minutes has elapsed, an email message is sent to the email address with all the alerts over that time interval.

Email alerts aggregation uses the following rules:

- First-level aggregation:
  Combine similar repetitive alerts, over a specified time interval, into a single alert that includes aggregation start time, aggregation end time, and the number of events aggregated along with event information.

- Second-level aggregation:
  Aggregation occurs at the end of an aggregation time interval where multiple aggregated alerts and individual alerts are combined into a single email message. Alerts are written into the body of the email message, sorted by time of occurrence. The first alert that occurs is written at the top of email message body. The last alert to occur is written at the bottom of the email message body. For aggregated alerts, time of occurrence is the time of occurrence of the first event.

In any given aggregation time interval, only one email message is sent to one email address, unless the size of the email body exceeds the maximum specified size. In this case, the data is split into multiple email messages.

About SNMP traps

The Alert module polls the management server database for new events at every user-specified event polling interval. An SNMP trap is generated and dispatched over the network for each event that matches a user-specified alert filter. The Alert module generates one trap for each alert.

The Alert module sends the following types of SNMP traps:

- None
  No SNMP trap is sent.
Basic

A basic trap contains the alert name, policy name, rule name, agent computer name and IP address, and event type.

General

A general trap contains the alert name, policy name, rule name, event date, agent computer name and IP address, user name, event severity, event priority, event disposition, event type, event count, event operation, OS type, process name, local IP address, local port number, remote IP address, remote port number, product version, target information, and description.

About alert text files

An alert text file contains events of interest; the alert text file can contain text strings and event fields. The alert text file is created when an alert captures an event of interest; subsequent events are appended to the file.

The DCS:SA detection policy Global_Watch_Policy monitors alert text files. When an event in an alert text file matches the criteria specified in the policy, the policy sends the event to the java console.

About troubleshooting alert problems

A separate log file is used to record any problems that occur when sending SNMP traps and email alerts. You can use this file to help debug alert problems.

By default, the alert log file is stored in the following directory:

C:\Program Files\Symantec\Data Center Security Server\Server\Tomcat\logs\sis-alert.log

The question mark (?) in the log file name is the sequence number. When the management server rotates the log file, the current log file is closed and nothing more is written to it. A new log file is opened with the same base file name, but with the next highest sequence number added to the file name. The active log file uses sequence number 0 (for example, sis-alert.0.log). Inactive (rotated) log files use sequence numbers 1 through n.

About the Notifications pane

You can search and view the notifications that are generated for alerts. Notifications are generated for alerts created by a user, and is categorised under the following type of alerts:

- All
- File access violations
SVA failed integrity checks
SVA service failures
SVA oversubscribed
Risk outbreak for AV
Risk outbreak for guest network threat
Quarantine more than 70 percent full

To search for alert notification
1. Navigate to **Monitor > Notifications** in UMC.
2. On the **Notifications** page, select the alert type from the **Select Alerts** drop-down to search for notifications.

### Viewing the Alerts page

You use the Alerts page in the DCS:S to create and store the alerts that you send to users when specific events are observed.

You can do the following activities from the Alerts page:

- Configure alert settings.
- Create, edit, copy, delete, import, and export alerts.
- Specify alert filters, thresholds, SNMP traps, alert text files, and email addresses.
- Enable and disable alerts.

To view the Alerts page
1. Navigate to **Monitors > Alerts** in UMC.
2. In the **Alerts Configurations** page, double-click an alert to view your settings.
3. (Optional) To expand or collapse the panes in the Alerts page, click the size arrows.

### Configuring alert settings

The Alert Module uses alert settings to get polling intervals and email settings.

To configure alert settings
1. Click **Settings**.
2. In the **System** page, navigate to **Alert Management** section.
3  In the **Alert Management** section, specify the following alert settings:

- **Purge alerts older than**
  - The alerts will be purged for the number of days specified.
  - Default value is 30 days.

- **Configuration Polling Interval**
  - The frequency, in minutes, at which the Alert module polls for changes to the alert settings.
  - Default value is 5 minutes.

- **Event Polling Interval**
  - The frequency, in minutes, at which the Alert module polls the DCS:S database for events.
  - The event polling intervals, in minutes.
  - Default value is 5.

  Select this check box to enable email aggregation, and then specify the **Aggregation Interval**.

  - Default value is 2.

- **Aggregation Interval**
  - If email aggregation is enabled, aggregate emails are sent based on the frequency that you specify.

- **Maximum email size**
  - The maximum email message size, in KB.
  - Default value is 1024.

4  Click **Save** (save the current setting changes) or **Revert** (revert to the last settings that were saved).

5  Click **Refresh** to apply the alert updates.

**Creating an alert**

Alerts notify users when specific events are observed by DCS:S.

Alerts comprise of the following components:

- Alert filters
- Email address templates
- SNMP traps
- Alert text files
To create an alert

1. Navigate to **Monitors > Alerts** in UMC.
2. On the Alerts page, in the toolbar, click **Add** icon.
3. In the **New Alert** dialog box, on the **General** tab, specify the following alert information:

   - **Name**
     - The name of the alert.
   - **Description**
     - A description of the alert.
   - **Show this alert on my Dashboard**
     - Select this check box to display this alert on my Dashboard.
     - The alert is enabled by default. You can enable and disable an alert after you create it.
4. Edit the alert to specify filters, email address templates, SNMP traps, and text file.

Creating an alert filter

You use alert filters to specify which events you want DCS:S to observe.

When configuring alert filters, please note the following:

- Each filter rule comprises <field, operator, value>.
- Examples of valid fields include event type, event severity, event disposition, OS type, local IP address, remote IP address, host name.
- Examples of valid operators include equals, not equals, in, not in, contains, not contains, greater than, less than. Some operators support the use of wildcard characters in a value. Valid wildcard characters are asterisk (*), which represents zero or more consecutive characters, and question mark (?), which represents exactly one character.
- Valid values vary, depending on the field. Some fields are limited to a pre-defined list, while other fields allow free-form typing.
- The Preview Events button on the Filters tab lets you preview recent events that match the alert filters.

To create an alert filter

1. Navigate to **Monitors > Alerts** in UMC.
2. Under the **Monitors** tab, click **Alerts**.
3. In the **Alert Configurations** pane, click on an alert for which you want to create a filter.
4 In the Edit Alert page, under Filters section, select <field, operator, value>, and then click Add.

5 Repeat step 4 to add additional rules.

6 To edit an existing filter rule, edit <field, operator, value>, and then click Update.

7 To preview filtered events, click Preview Events.

8 Click Save.

Specifying an email address template

An email address template contains the email addresses that you want to receive the alert.

When including event date fields in the subject and body of an email message, you can select UTC or local agent date/time.

To specify an email address template

1 Navigate to Monitors > Alerts in UMC.

2 Under the Monitors tab, click Alerts.

3 In the Alert Configurations pane, click on an alert.

4 In the Edit Alert page, under the Email section, click Add.

5 In the Email Template dialog box, specify the following information:

   To
   In a comma-separated list, type the email addresses that you want to receive the alert.

   Subject
   Specify the subject of the email:
   ■ Type the text that you want to include in the subject line of the email.
   ■ Select the event fields that you want to include in the subject line.

   Body
   Specify the email message:
   ■ Type the message that you want to include in the email body.
   ■ Select the event fields that you want to include. Select Insert All to insert all of the available event fields, with each field shown on a separate line.

6 Click Save.
7 In the **Emails** section, click **Enable** to enable the email address template. All email addresses contained in the template will receive the alert. If you do not want to send the alert at this time, check **Disable**.

8 Click **Save**.

**Specifying an SNMP trap**

You configure the following when specifying an SNMP trap:

- Type of SNMP trap to send
- Server to which the SNMP trap is sent
- Port numbers used by the SNMP server

**To specify an SNMP trap**

1 Navigate to **Monitors > Alerts** in UMC.

2 In the **Alert Configurations** pane, click an alert to which you want to specify an SNMP trap.

3 In the alert dialog box, on the SNMP tab, specify the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Type the SNMP server address.</td>
</tr>
<tr>
<td>Server Port</td>
<td>Type the server port number used by the DCS:S when it connects to your SNMP server. Default: 162</td>
</tr>
<tr>
<td>Local Port</td>
<td>Type the local port number used by the DCS:S when it connects to your SNMP server. Optional. Default: 161</td>
</tr>
<tr>
<td>Community</td>
<td>Type the SNMP community name used when sending SNMP traps.                  Default: Public</td>
</tr>
</tbody>
</table>
Select the type of SNMP trap that you want to generate when an alert is triggered.

Select one of the following SNMP trap types:

- None
- Basic
- General

See “About SNMP traps” on page 107.

4 Click **Save**.

### Specifying an alert text file

You can set up an alert text file to save events of interest. The alert text file can contain text strings and event fields. The file is created when the alert captures an event; subsequent records are appended to the file.

An alert text file is stored on the DCS:S computer. The default alerts directory is as follows:

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

The DCS:SA detection policy Global_Watch_Policy monitors alert text files. When an event in an alert text file matches the criteria specified in the policy, the policy sends the event to the java console.


**To specify an alert text file**

1 Navigate to **Monitors > Alerts** in UMC.

2 In the **Alert Configurations** pane, click on an alert.

3 In the Edit Alert page, under the **File** section, specify the following information:

   **Name**
   
   Type the name of the alert text file.
   
   The file name may not contain any backward slashes.

   **Append Text**
   
   Type the text to save in the alert text file.
   
   The text can include event fields, selected form the menu.

4 Click **Save**.
Creating an alert configuration

DCS:S lets you configure notification alerts for events. For example, you want a notification to be displayed on the console when 100 file access events are reported within a timeframe of 5 minutes on an agent. You can configure an alert by using the Add New Alert page.

To create an alert configuration

1. Navigate to Monitor > Alerts in UMC.
2. In the Alert Configurations page, click Add icon to launch the Add New Alert page.
3. In the Add New Alert page, do the following in each section and then click Save.

<table>
<thead>
<tr>
<th>Section</th>
<th>Action required</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>■ Name - Enter a name for the alert that you want to create.</td>
</tr>
<tr>
<td></td>
<td>■ Description - Enter a brief description about the alert that you want to create. This is an optional step.</td>
</tr>
<tr>
<td></td>
<td>■ Show this alert on my Dashboard - Check to enable the alert to appear on your dashboard.</td>
</tr>
<tr>
<td>Filters</td>
<td>■ Select the parameters of the rule and then click Add.</td>
</tr>
<tr>
<td></td>
<td>■ Click Preview Events to view the events that match the filter that you are adding to the new alert.</td>
</tr>
<tr>
<td>Threshold</td>
<td>■ Minimum events - Enter the number of events that should trigger an alert notification. For example, 100 file access events within &lt;number of&gt; minutes should trigger an alert notification.</td>
</tr>
<tr>
<td></td>
<td>■ Timeframe - Enter the time in minutes that should be the threshold for the alert notification. For example, &lt;X number of&gt; file access events within a time window of 5 minutes should trigger an alert notification.</td>
</tr>
<tr>
<td></td>
<td>■ Select attributes to group events - Select an attribute.</td>
</tr>
<tr>
<td>Section</td>
<td>Action required</td>
</tr>
<tr>
<td>---------</td>
<td>----------------</td>
</tr>
</tbody>
</table>
| SNMP    | ■ **Server Name** - Enter the server name  
          ■ **Community** - Enter a value.  
          ■ **Trap level** - Select a level for the alert from the drop-down list. |
| File    | ■ **Name** - Enter a name for the alert configuration file that you want to create.  
          ■ **Append Text** - From the drop-down list, select the event details that you want to add in the alert configuration file. When you enter the first few characters, the associated values appear in the drop-down.  
          ■ **Add Summary Text** - Select this option if you want to add the default summary into the Append Text field. |
| Emails  | ■ Click **Add** icon to launch the **Email Template** dialog.  
          ■ **To** - Enter the recipient's email address.  
          ■ Select a value from the **Subject** drop-down list. When you enter the first few characters, the associated values appear in the drop-down.  
          ■ Select a value from the **Body** drop-down list and then click **Save**.  
          The email template that you have created is displayed in the **Emails** section.  
          Click on the email address to modify, and **Remove** icon to delete an email template.  
          Click **Enable** to enable the email notification, and click **Disable** to disable email notification. |

**Enabling or disabling an alert**

Enabled alerts send email messages and SNMP traps. Disabled alerts do not send email messages and SNMP traps.
To enable or disable an alert

1. Navigate to **Monitors > Alerts** in UMC.
2. In the **Alert Configurations** pane, select an alert and do one of the following:
   - To enable an alert, click **Enabled**.
   - To disable an alert, click **Disable**.

**About copying alerts**

The DCS:S Copy Alerts function lets you create copies of alerts. For example, if there are existing alerts with complex filters and you want to create another alert with similar filters and some additional filters, you can copy an existing alert and add the required filter to it instead of creating an alert from the start.

The copied alert appears in the format **Copy of_Alert name**. For example, a copied alert for an existing alert named ALERT1 would appear as Copy of_ALERT1.

**Creating copies of alert**

To create copies of alert

1. Navigate to **Monitor > Alerts** in UMC.
2. In the **Alerts Configuration** pane, select an alert, and click **Copy** icon.

**Importing an alert**

You can import an alert in DCS:S. The alert which you want to import can be an alert previously exported from another DCS:S system.

The DCS:S imports the alerts to the alerts page.

To import alerts

1. Navigate to **Monitor > Alerts** in UMC.
2. To import an alert, click **Import**.
   - The alert that you import must be a .zip file.
3. In the **Import** dialog box, browse to the alert zip file that you want to import.
4. Click **Import** to import the alert zip file.
Exporting an alert

You can export an alert from DCS:S.

Exported alerts are saved in .zip files.

To export policies

1. Navigate to Monitor > Alerts in UMC.
2. On the Alerts page, select the alerts which you want to export, and then click Export.
   
   To select multiple policies, hold down the Ctrl key while selecting the files.
3. In the Export dialog box, browse to the folder where you want to export the alerts.
4. In the Export dialog box, in the File Name box, type a name for the export file, and then click Export.

   The selected alerts are exported to a .zip file, using the file name that you specified.

Deleting an alert

You can delete alerts that you no longer need.

To delete an alert

1. Navigate to Monitor > Alerts in UMC.
2. In the Alert Configurations pane, select an alert, and then click Delete icon.
3. In the Confirm Deletion dialog box, click Yes to delete the alert.

Purging alerts

You can specify how long to retain the alert notifications in the DCS:S database.

To purge alert notifications

1. Navigate to Admin > Settings in UMC.
2. In the System page, under the Alert Management section, check Purge Alerts older than <number of days>.
   
   The default value is 30 days.
   
   A batch of 1000 alert notifications can be purged at the same time.

See “About alerts” on page 106.