Symantec™ Data Center Security: Server Advanced

Operations Director Reference Guide

Version 6.5
Legal Notice

Copyright © 2015 Symantec Corporation. All rights reserved.

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

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TP1P ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

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

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

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Symantec as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.
Technical Support

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

Symantec’s support offerings include the following:

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

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

www.symantec.com/business/support/

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

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

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

**Licensing and registration**

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

www.symantec.com/business/support/

**Customer service**

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

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

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

Chapter 10 Managing Firewall Templates ........................................... 67

About firewall templates ................................................................. 67
Creating a firewall template ............................................................ 68
Viewing a firewall template ............................................................. 69
Editing precedence order value of firewall template ......................... 70
Editing a firewall template .............................................................. 71
Creating copy of a firewall template ................................................ 71
Provisioning Palo Alto Networks Next Generation Firewall for new
application ............................................................................ 72
Deleting a firewall template ............................................................ 75

Chapter 11 Monitoring Operations ..................................................... 77

About Notifications page ................................................................ 77
Viewing notifications and its details .................................................. 79
Approving a notification or provisioning request ............................ 79
Denying a notification or provisioning request ............................... 80
Process of approval and exception request ................................. 81
Monitoring synchronization status .................................................... 83
Viewing security provisioning failure ................................................. 84
Retrying failed security provisioning ................................................ 85

Appendix A Troubleshooting ............................................................ 86

Operations Director fails to register with UMC .................................. 86
Viewing registration status of Operations Director with UMC ............ 88
Unable to connect to Operations Director server .......................... 88
Manually registering and unregistering Symantec Data Center Security
plug-in .................................................................................... 89
Command-line options to use the registerPlugin utility ................. 90
Committing firewall rules to Panorama fails ................................ 92
Symantec Data Center Security plug-in installation fails with an
error .................................................................................... 92
Appendix B  Additional Resources ......................................................... 93
Where to get more information ........................................................ 93
Introduction

This chapter includes the following topics:

- About Operations Director
- Advantages of Operations Director
- Orchestrating security using Operations Director
- About micro-segmentation
- About the Operations Director Home Page
- About Unified Management Console
- Using Unified Management Console

About Operations Director

Operations Director is a security orchestration feature of Data Center Security: Server. Operations Director automates and simplifies security provisioning for virtual applications by assessing the security requirements for applications and applying the appropriate security policies. Operations Director automates policy provisioning through orchestration with security point products and the VMware NSX, an industry leading software-defined data center (SDDC) network virtualization and security platform. Operations Director is the software-defined security service for the NSX SDDC platform.

Operations Director delivers automated security management for software-defined data centers. A SDDC extends the virtualization concepts such as abstraction, pooling, and automation — to all data center resources and services. In a SDDC, new applications are provisioned on-demand and are ready for business consumption almost instantaneously. However, with traditional security processes and workflows, identification of the right security controls and the provisioning of the security policies by using various security point products can take days or weeks.
Operations Director integrates into the SDDC automation framework to ensure that security provisioning is completed in the order of minutes.

The security orchestration feature powered by Symantec Operations Director is the latest addition to the Symantec Data Center Security portfolio and is intended to:

- Automate security provisioning workflow.
- Provide application-centric security service.
- Seamlessly integrate with VMware NSX.
- Provide out-of-box security product integration.

All you have to do is:

- Configure Symantec Data Center Security plug-in in vSphere Web client.
- Deploy the Symantec Data Center Security Unified Management Console (UMC) appliance in vCenter.
- Deploy Operations Director appliance in vCenter.
- Register the Operations Director appliance with UMC.

To know more about configuration and product deployment, refer any of the following:

- Symantec Data Center Security Operations Director Reference Guide
- Symantec Data Center Security online help
- Symantec Data Center Security: Server Advanced Planning and Deployment Guide

The documents are available at:
www.symantec.com/business/support/index?page=content&id=DOC8101

See “Advantages of Operations Director” on page 12.


Advantages of Operations Director

Following are the advantages of Operations Director:

- Integrated into vSphere Web client and NSX; easy to deploy and get into action.
- Leverages Symantec-defined tags along with vCenter tags to derive the right security posture for you.
Interoperates with security point products.

Automates complex and manual decision making.

Delivers out-of-box security intelligence using security tags mapped to best-practice mandates, controls, and security product policies, and can be easily customized to map user-defined best practice policies.

See “About Operations Director” on page 11.


Orchestrating security using Operations Director

Operations Director automates a lot of manual activity involved in security provisioning where the security administrator is unable to decide the right security policies for a virtual machine/application. Based on the state of your production environment, Operations Director derives the right security profile and security policies to be applied to secure an application.

Operations Director provides a robust workflow to manage communication and sequence of security provisioning operations between:

- Server administrator (who manages the virtual infrastructure and has requirements for securing the virtual infrastructure) and
- Security administrator (who manages the security provisioning).

Operations Director interoperates with registered security products such as Symantec Data Center Security: Server, Symantec Data Center Security: Server Advanced, and Palo Alto Networks Next Generation Firewall to synchronize and leverage the latest security policies from these security products for securing a virtual machine/vApp.

See “About Operations Director” on page 11.

See “Advantages of Operations Director” on page 12.

About micro-segmentation

Micro-segmentation is an approach where each application instance in a data center has its own security zone. This application-specific security zone (also known as the application micro-segment) can now be assigned end-point security policies and network security policies that are highly specific to the security requirements of the application.

If an application has been detected with a critical vulnerability, quarantine controls or hardening controls can be applied to only the application’s micro-segment to
protect the application. There is no impact to other applications which are in their own micro-segments.

Traditional approaches involved creating a broad security zone and several applications that met a certain criteria were placed in the security zone. For example, all applications in production mode were added to the production security zone. There was no distinction between production applications that processed inventory data and those that processed sensitive healthcare data. If a certain application had a vulnerability either the entire security zone had to be updated with new policies to ensure that the vulnerability was not exploited in the entire zone. This approach is time consuming as well as poses overheads on other applications that do not need additional security policies.

Software-defined data center and software-defined network platforms make it easy to implement micro-segmentation.

**Role of Operations Director in micro-segmentation**

Operations Director delivers micro-segmentation support out-of-the-box by creating a security profile for each vApp or VM and identifies security policies based on the application’s unique security requirements based on Operations Director tags. Operations Director also implements micro-segmentation at the application tier level by creating separate NSX security groups or Palo Alto Networks address groups for each tier of an application and applying the necessary network security policies to govern traffic between the tiers.

For example, in the case of a three-tier Microsoft Exchange application containing App, Web, and DB tiers, Operations Director creates micro-segments for App, Web, and DB by adding only database servers to the DB micro-segment, Web servers to the Web micro-segment, and so on so forth. Operations Director then applies firewall policies that specifically govern traffic between the Web and App tiers, between the Web and the Internet, and the App and the DB tiers.

**About the Operations Director Home Page**

Operations Director is available only after you register Operations Director appliance with UMC. After you log in to DCS:SA UMC console, on the top right select Operations Director in the drop-down to navigate to the Operations Director home page.

Operations Director home page serves as a dashboard that gives an insight into your virtual data center security posture.

The filter buttons in the **Key Security Provisioning Metrics** area display the count of:

- Policy provisioning errors.
- New applications that are pending approval for security provisioning.
- Notifications that pending an approval by the server administrator.
- Exceptions requested that need attention.

Clicking on any of the filter buttons will take you to the respective page and the filter will be applied while displayed the data. For example, if you click the filter button 13 New App Pending approval, you will be navigated to the Monitor > Notifications page and only the notifications about 13 new applications that are pending approval will be displayed. You can clear or change the filters on the Notifications page.

The Current Data Center Security Status donut chart shows the applications that are at risk and that are secured.

The granular details of the count of applications are shown in the Security Provisioning Status donut chart. The granular details include:

- Pending Approval
- Waiting
- Provisioned
- In Progress
- Exception Requested
- Failed

Clicking any region in the donut chart takes you to the respective page and the filter will be applied while displaying the data. For example, if you click Exception Requested in the Security Provisioning Status donut chart, you will be navigated to the Assets > VMs page and the associated virtual machines will be displayed. You can clear or change the filters on the VMs page.

The Overall Security Requirements by Tags area chart displays the tags that are in use. The area chart acts as a filter. Clicking a specific tag in the area chart takes you to the Tag Details page. For example, if you click PCI-DSS, you will be navigated to the tag details page where you can view the tag description, security mappings, mandates, security controls, and questions associated to the tag.

---

**Note:** The home page only displays a real-time snapshot. You cannot perform any tasks from this page.
About 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.

See “Using Unified Management Console” on page 16.

Using Unified Management Console

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

Using the Unified Management Console, you can do the following:

Home page

You can view the following from the Home page:

- Provide step by step guidance to configure DCS: S.
- View direct links to related workspaces and product help for respective step.

Monitor page

You can do the following from the Monitor page:

- Facilitates download of UMC and Operations Director logs directly from the console.
You can do the following from the Settings page:

**User Management**
- Search users and groups in the configured Active Directory and assign them roles in DCS: S.

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

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

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

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

See “About the Operations Director Home Page” on page 14.
Achieving your Business Objectives

This chapter includes the following topics:

- Provisioning security to a vApp/VM on day zero

Provisioning security to a vApp/VM on day zero

Operations Director simplifies the process of provisioning security to a vApp/VM on day zero in easy steps. The three primary personas involved are:

- **Server administrator**
  manages the vCenter environment including related virtual components.

- **Operations Director administrator**
  Manages Operations Director configuration and setup tasks.

- **Security administrator**
  Manages security provisioning and related operations.

Prerequisites

Ensure that the following prerequisites are satisfied:

- Questions must be published from the Manage > Questions page of Operations Director to vSphere Web client. See “Publishing questions” on page 44.

- Tags must be published from the Manage > Tags page of Operations Director. See “Publishing tags” on page 53.

- Questions and responses must be mapped to the tags. See “Mapping a question and response to a tag” on page 45.

- All required product configuration must be completed from the Settings > Integration page of UMC.
If Palo Alto Networks Next Generation Firewall is configured then you must satisfy these additional prerequisites:

- Create necessary tier tags in vCenter. See “Creating and assigning tier tags to VM” on page 21.
  
  or

- Define regular expressions for tier tag identification. See “Defining regular expressions for identifying tiers based on VM names” on page 49.

**Note:** UMC administrator is the point of contact for operations related to user/role management, product configuration, and integrations that are related to the UMC.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Server administrator logs in the vSphere Web client and creates a vApp. The security status of the vApp/VM is <strong>Not Secured</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>To secure the vApp/VM, the server administrator submits response to assessment questions and gets the recommended security policies.</td>
</tr>
<tr>
<td>3</td>
<td>Server administrator reviews the recommended security policies.</td>
</tr>
<tr>
<td>4</td>
<td>Server administrator can either accept the recommended policies or request an exception.</td>
</tr>
</tbody>
</table>
|      | - If the server administrator accepts the recommended profile, the security policies are applied on the vApp/VM and the security status of the vApp/VM changes to **Secured**.  
  |      |   **Note:** This happens only after the security administrator approves the notification from Operations Director. |
|      | - If the server administrator requests an exception, the security administrator can go to the Settings > Notifications page to view the notification. The security administrator can approve or deny the exception. |
| 5    | Security administrator reviews the recommended security policies and approves or denies the notification. |

See “Process of approval and exception request” on page 81.
Getting Started

This chapter includes the following topics:

- System requirements for Operations Director
- Configuring components required for Operations Director
- Creating and assigning tier tags to VM
- Configuring Operations Director to commit firewall rules to Panorama
- About configuring orchestrated security products
- Configuring orchestrated security products
- Adding an orchestrated security product
- Rescanning to discover security products

System requirements for Operations Director

Refer the Platform Feature Matrix for information on:

- Supported platforms and browsers for Unified Management Console and Operations Director.
- Supported VMware platform for Unified Management Console and Operations Director.

See “Configuring components required for Operations Director” on page 20.

Configuring components required for Operations Director

Refer the Installer Help for Setting up Operations Director that involves:
■ Importing and deploying Operations Director virtual appliance on VMware infrastructure.

■ Registering Operations Director with UMC.

After the Operations Director appliance has been imported and registered with the UMC, here are the next steps that you must complete.

Configure the orchestrated security products

Once the security products are configured, security policies and services get synchronized with Operations Director. The capabilities and library of security policies get integrated with Operations Director’s software-defined security (SDS) services. This is managed from the Settings > Integration page of UMC.

See “Configuring orchestrated security products” on page 24.

Prerequisite for Symantec Data Center Security plug-in

You must register Operations Director with UMC while deploying the Operations Director appliance and also configure vCenter server from the Settings > Integration page of UMC. This ensures that the Symantec Data Center Security plug-in gets deployed to the vCenter.

If vCenter server is already configured and if you register Operations Director with UMC later, go to the Settings > Integration page of UMC to verify the vCenter server configuration.

See “About configuring orchestrated security products” on page 23.

Creating and assigning tier tags to VM

Note: You must perform this step only if you have Palo Alto Networks Next Generation Firewall configured.

Before you create and assign tier tags, you may want to understand the significance of tier tags. See “About tier tags ” on page 48.

Operations Director is unable to derive tier tags when the regular expressions configured in the od.properties file do not match the virtual machine names. In such a scenario, you may have to manually create and assign tier tags to the virtual machines.

Tier tags can be applied to a stand-alone virtual machine or vApps. Tier tags cannot be applied to virtual machines that are part of a vApp.
To create and assign tags to virtual machines

1. Log in to the vSphere Web client.
2. On the home page, select **vCenter**.
3. Under **Inventory Lists**, select **Virtual Machines**.
   The list of virtual machines is displayed.
4. Select the virtual machine that you want to assign tags to in the left panel.
5. In the right panel, go to **Manage > Tags** portlet.
6. In the top-left, click the **New Tag** icon and create the tags WEB, APP, and DB and assign the category as **Tier**.
   The new tags that you create and save will be listed in the **Assign Tag** portlet.
7. Now click the **Assign Tags** icon in the top left.
8. Select the desired tag and click **Assign** to assign it to the virtual machine.

See “Defining regular expressions for identifying tiers based on VM names” on page 49.

### Configuring Operations Director to commit firewall rules to Panorama

**Note:** You must perform this step only if you have Palo Alto Networks Next Generation Firewall configured.

Panorama is the centralized management console for Palo Alto Networks Next Generation Firewall.

Operations Director can orchestrate with Panorama to apply firewall policies for new applications. By default, Operations Director is configured to only update Panorama with firewall rules but not commit them to the firewall. This is to enable the firewall administrator to review the rules before committing them.

If you configure Operations Director to not commit rules to Panorama, the changes may be lost in an event when Panorama gets restarted before a commit is performed. However, you can configure Operations Director to commit firewall rules after the security administrator's approval in Operations Director. You can do so by editing the Operations Director configuration file.
To configure Operations Director to commit changes to Panorama

1. Log in to the Operations Director appliance as ODAdmin user which was created during Operations Director appliance deployment and the password that was provided then.

2. Edit the Operations Director appliance file.

   ```bash
   sudo vi /usr/local/Symantec/so/config/od.properties
   ```

3. Change the value of the following parameters from:
   - `od.provisioningservice.panplugin.commitoperation.configtopanorama.enable=no`
   - `od.provisioningservice.panplugin.commitoperation.panaromatofirewalldevices.enable=no`
   to
   - `od.provisioningservice.panplugin.commitoperation.configtopanorama.enable=yes`
   - `od.provisioningservice.panplugin.commitoperation.panaromatofirewalldevices.enable=yes`

4. Enter the values for retry count and retry interval in the following parameters:
   - **Retry count** is the number of times the commit operation will be retried.
     ```java
     od.provisioningservice.panplugin.httpclient.commitoperationretrycount=3
     ```
   - **Retry interval** is the number of seconds after which the commit operation will be retried.
     ```java
     od.provisioningservice.panplugin.httpclient.commitoperation.retryinterval=120
     ```

5. Save the `od.properties` file.

You must restart the security orchestration services by restarting the Apache Tomcat Web server for the changes to take effect. To do this, run the following commands from the appliance:

   ```bash
   sh /opt/apache-tomcat-7.0.53/bin/shutdown.sh
   sh /opt/apache-tomcat-7.0.53/bin/startup.sh
   ```

See “Committing firewall rules to Panorama fails” on page 92.

See “Configuring components required for Operations Director” on page 20.

### About configuring orchestrated security products

Orchestrated security products are the security products that Operations Director discovers as part of the NSX server configuration. These products include:

- Symantec Data Center Security: Server
- Palo Alto Networks Next Generation Firewall
These security products get listed on the Settings > Integration page of UMC once NSX discovers them.

You need at least one security product for Operations Director to orchestrate security. In absence of a security product, Operations Director will be unable to synchronize the security policies of that security product. In that case, Operations Director orchestrates security only with the available security product and its security policies.

For more information, refer the following topics in the DCS:SA online help:

- Configuring VMware vCenter server
- Configuring VMware NSX server
- About alerts and notifications

See “Configuring orchestrated security products” on page 24.

See “Rescanning to discover security products” on page 26.

Configuring orchestrated security products

You can manage the configuration of orchestrated security products required for Operations Director from the Settings > Integration page of UMC.

Note: To perform this configuration, you must have the UMC administrator role.

Orchestrated security products are the security products that are auto-discovered as part of the NSX server configuration. Before you proceed with configuring the orchestrated security products, make sure that the NSX server is configured.

Security product configuration after the NSX server is configured

- Symantec Data Center Security: Server
  The status of this product will be Configured. No configuration is necessary for DCS:S.

- Palo Alto Networks Next Generation Firewall
  The status will be Not Configured. When the NSX server detects Palo Alto Networks Next Generation Firewall service, the edit action will be enabled. You can edit the configuration and configure Palo Alto Networks Next Generation Firewall.
To configure Palo Alto Networks Next Generation Firewall

1. Go to the **Settings > Integration** page of UMC.
   
   Under the **Orchestrated Security Products**, the auto-discovered security products after the NSX server configuration will be listed.

2. Click the edit icon under the **Action** column.
   
   In the **Configure Palo Alto Network Firewall** dialog box, enter the correct IP address or host name NSX server.

3. Enter a connection name.

4. Enter the valid user name and password.

5. Click **Test Connection** to test your connection before saving.

6. Click **Save** to save the configuration.
   
   After a successful configuration, Palo Alto Networks Next Generation Firewall will be in a **Configured** state.

To troubleshoot any error in connection of the security product, click the edit icon and try re-entering and saving the connection details.

**Points to remember**

- Refer the product online help for details on *Configuring VMware vCenter Server with UMC* and *Configuring VMware NSX Server with UMC*.

- You cannot use Operations Director to point to a different Palo Alto Networks Next Generation Firewall server other than the one initially configured. However, if the IP address of Palo Alto Networks Next Generation Firewall server changes, you can edit the Palo Alto Networks Next Generation Firewall server configuration in UMC (**Settings > Integration** page) to update the new IP address for the previously configured Palo Alto Networks Next Generation Firewall server. If Palo Alto Networks Next Generation Firewall server is changed to point to another server, the firewall templates must be edited/re-created.

See “About configuring orchestrated security products” on page 23.

See “Adding an orchestrated security product” on page 25.

See “Rescanning to discover security products” on page 26.

---

**Adding an orchestrated security product**

Operations Director allows you to add only DCS:SA for automated policy orchestration. DCS:S and Palo Alto Networks Next Generation Firewall are auto discovered as part of NSX configuration.
To add DCS:SA

1. Go to the Settings > Integration page of UMC.
2. In the Orchestrated Security Products section, click Add. The Add Product dialog box is displayed. The product displayed will be DCS: Server Advanced.
3. Enter the IP address or host name and port number (4443).
4. Enter the domain\user name and password. Click Test Connection to verify your connection.

   **Note:** The user name that you specify here must have UMC administrator role.

5. Click Add to save the product configuration.
6. DCS:SA gets listed in under Orchestrated Security Products with the status as Configured.

**Point to remember**

- Refer the product online help for details on Configuring VMware vCenter Server with UMC and Configuring VMware NSX Server with UMC.
- You cannot use Operations Director to point to a different DCS:SA other than the one initially configured. However, if the IP Address of DCS:SA changes, you can edit the DCS:SA configuration in UMC (Settings > Integration page) to update the new IP address for the previously configured DCS:SA.
- If DCS:SA is changed to point to another server, Symantec-defined security policies are not impacted.

See "Configuring orchestrated security products" on page 24.

**Rescanning to discover security products**

Rescanning helps you to discover the security products DCS:S and Palo Alto Networks Next Generation Firewall if they have been configured after configuring the NSX server in UMC. Rescan would check if they are present and would add under the entry under the Orchestrated Security Products grid accordingly.

Before you rescan, NSX server must be configured correctly configured from the Settings > Integration page of UMC.
To initiate a rescan

1. On the **Settings > Integration** page of UMC, under the **Orchestrated Security Products** grid, click **Rescan**.

   The rescan operation may take a couple of minutes. You may navigate away from this page and come back to check the status.

2. On a successful rescan:

   - Palo Alto Networks Next Generation Firewall should be listed in the **Orchestrated Security Products** grid. You can click the edit icon and edit the configuration to configure Palo Alto Networks Next Generation Firewall.
   - DCS:S should be listed in the **Orchestrated Security Products** grid in a Configured state.

See “Configuring orchestrated security products” on page 24.

See “About configuring orchestrated security products” on page 23.
Using Operations Director plug-in for vSphere Web client

This chapter includes the following topics:

- About Symantec Data Center Security plug-in
- Deploying Symantec Data Center Security plug-in for vCenter
- Configuring Symantec Data Center Security plug-in in vCenter
- Viewing configuration details of the Symantec Data Center Security plug-in for vCenter
- Editing configuration details of Symantec Data Center Security plug-in for vCenter
- Responding to the security assessment
- Monitoring the security status of a vApp/VM
- Accepting the recommended policies
- Requesting exception on recommended policies
- Provisioning security to a vApp/VM based on custom questions and tags

About Symantec Data Center Security plug-in

The Symantec Data Center Security plug-in for vSphere lets you manage and monitor security of a vApp/VM in a software-defined data center.
Features of the Symantec Data Center Security plug-in

The Symantec Data Center Security plug-in lets you:

■ Determine the current security status of a vApp/VM.
■ Respond to a security assessment questionnaire.
■ Accept or request an exception on the recommended security policies. See “Requesting exception on recommended policies” on page 35.
■ Monitor the security status of a vApp/VM.

Note: The Symantec Data Center Security plug-in is only compatible with the vSphere Web client.

See “Responding to the security assessment” on page 33.
See “Monitoring the security status of a vApp/VM” on page 34.
See “Deploying Symantec Data Center Security plug-in for vCenter” on page 29.

Deploying Symantec Data Center Security plug-in for vCenter

Deploying the Symantec Data Center Security plug-in involves the following:

■ Registering Operations Director appliance with UMC as explained in the chapter Setting up Operations Director of the installation guide online help.
■ Configuring the vCenter server correctly. After you configure vCenter, the system connects to the vCenter server and deploys the Symantec Data Center Security plug-in to vCenter. This process happens in the background and may take some time. Other operations on the user interface are not blocked while this happens.
To deploy Symantec Data Center Security plug-in for vCenter

1. Go to the **Settings > Integration** page of UMC.

   The status of the VMware vCenter server connection will show as **Not Configured**.

2. Edit the connection and configure it by providing the correct details of the vCenter server.

   Enter the vCenter credentials and save them successfully.

   System connects to vCenter and registers the Symantec Data Center Security plug-in with vCenter.

   This may take a few minutes.

To verify if the deployment of the Symantec Data Center Security plug-in has been successful, log in to the vSphere Web client and check if the shortcut for **Symantec Data Center Security** plug-in is available. If the shortcut for **Symantec Data Center Security** plug-in is not available, the deployment of the plug-in might have failed.

In that case, check the log file available at the location `/var/log/Symantec/DCSC/od/odregistration.log`. **Resolve the error and navigate to the **Settings > Integration** page again to trigger the **Symantec Data Center Security** plug-in deployment in the background.**

If you are unable to fix the error that is logged in the log file then you will have to manually deploy the **Symantec Data Center Security** plug-in.

See “Manually registering and unregistering Symantec Data Center Security plug-in” on page 89.

See “Symantec Data Center Security plug-in installation fails with an error” on page 92.


See “Viewing configuration details of the Symantec Data Center Security plug-in for vCenter” on page 32.

See “Editing configuration details of Symantec Data Center Security plug-in for vCenter” on page 32.
Configuring Symantec Data Center Security plug-in in vCenter

To configure Symantec Data Center Security plug-in in vCenter

1. Log in to the vSphere Web client.

2. Navigate to the Home page > Administration. You will see the shortcut for Symantec Data Center Security.

3. Click the shortcut for Symantec Data Center Security to launch the Register Symantec Data Center Security Plug-in dialog box.

   - Enter the hostname/IP address and port number (default 8443) of the Operations Director appliance.
     For example: 11.111.111.111:8443
   
   - Enter your domain and user name.
   
   - Enter your password.

   Note: The user that you enter here must have Operations Director administrator role in UMC to use the Symantec Data Center Security plug-in. For any login issues, contact the UMC administrator.

4. Click Save.

   System connects to Operations Director and configures the connection.

   - A successful registration shows a notification window at the bottom right of the Web client.
   
   - A failure message is displayed at the top of the Web client.
     To troubleshoot, make sure to enter the correct host name/IP address of the Operations Director server and valid credentials and then try connecting again.
     
   - Ensure that the vCenter server and Operations Director appliance are reachable.

See “Viewing configuration details of the Symantec Data Center Security plug-in for vCenter” on page 32.

See “Editing configuration details of Symantec Data Center Security plug-in for vCenter” on page 32.

See “Deploying Symantec Data Center Security plug-in for vCenter” on page 29.
Viewing configuration details of the Symantec Data Center Security plug-in for vCenter

To view the configuration details of the Symantec Data Center Security plug-in
1 Log in to the vSphere Web client.
2 Navigate to the Home page > Administration.
   You will see the shortcut for Symantec Data Center Security.
3 Click the shortcut for Symantec Data Center Security. The Register Symantec Data Center Security Plug-in settings information is displayed as read-only.
4 Verify the hostname/IP address of the Operations Director appliance.
5 Verify the user name and the connection status. The status will show as either Connected or Not Connected.

See “Editing configuration details of Symantec Data Center Security plug-in for vCenter” on page 32.

See “Deploying Symantec Data Center Security plug-in for vCenter” on page 29.

Editing configuration details of Symantec Data Center Security plug-in for vCenter

To edit the configuration details of Symantec Data Center Security plug-in
1 View the connection details of the Symantec Data Center Security plug-in.
   See “Viewing configuration details of the Symantec Data Center Security plug-in for vCenter” on page 32.
2 Click Edit to edit the information.
   ■ Enter the host name/IP address of the Operations Director appliance.
   ■ Enter your user name.
   ■ Enter your password.
3 Click Save after you are done with editing the information.
4 System connects to Operations Director and configures the connection.
   A failure message is displayed at the top of the Web client. You may refer the online help or contact the Symantec support for more information.
Responding to the security assessment

Note: If you want to use Palo Alto Networks Next Generation Firewall templates, ensure that you have created and assigned tier tags to virtual machines in the vApp. See “Creating and assigning tier tags to VM” on page 21.

Assuming that this is a day zero scenario. After you deploy the Symantec Data Center Security plug-in, in vSphere Web client:

1. Log in to the vSphere Web client.
2. Go to vCenter > Inventory Lists > vApps > <vApp_name>
   or
   vCenter > Inventory Lists > Virtual Machines > <VM_name>.
3. Select the vApp/VM that you want to secure.
4. In the right pane, go to Manage > Security tab.
   The Symantec Data Center Security - Security Status portlet displays the status as Not Secured.
5. Click Apply Security....
   A security assessment questionnaire is launched. You must respond to the questionnaire for Operations Director to determine the right security policies for the vApp/VM.

Note: It might take a few minutes to load the vApp/VM details and load the security assessment questionnaire.

6. Select responses to all the questions.
7. Click Submit to submit the security assessment.

Points to remember

- Questions must be published by the security administrator in Operations Director before you submit the responses.
Make sure that all virtual machines of the vApp are powered on and VMware tools are running.

You must select a business application if you want firewall policies to be applied. Business application is the application type that is selected while creating the firewall template on the Manage > Firewall Templates page in Operations Director.

Operations Director will not be able to apply firewall policies if you submit the security assessment by retaining the business application as None, which is the default selection.

What happens in the background?
After you submit the responses to the security assessment questions, depending on the responses, the tags and security policies are determined.

For example, based on your responses to the security assessment, if the tag that is identified based on the responses is PCI by Operations Director then the security policies associated to the PCI tag are recommended.

Note: The vApp/VM for which you just applied the security in vSphere is displayed in Operations Director under Monitor > Notifications. The security status of the vApp/VM is still Not Secured because the notification is pending approval. Only after the security administrator approves the notification the security policies get applied on the vApp/VM.

See “Monitoring the security status of a vApp/VM” on page 34.

Monitoring the security status of a vApp/VM

To monitor the security status of a vApp/VM:

1. Select the vApp/VM and go to the Summary tab.

2. Symantec Data Center Security displays the security controls and policies that are active on the vApp/VM.

3. Under the Monitor > Security tab the security status of the vApp/VM is displayed as well. Symantec Data Center Security - Security Status displays the type of security controls, the product names and the policies that are applied on the vApp/VM as part of the active security profile.

Manage > Security tab also displays the security status of the vApp/VM. Symantec Data Center Security - Security Status displays the type of security controls, the
product names and the policies that are applied on the vApp/VM as part of the active security profile.

**Note:** The Manage > Security tab will be available only for a stand-alone VM. It will be unavailable if the VM is part of a vApp. If a VM is part of a vApp, you will have to perform this operation at the vApp level.

See “Responding to the security assessment” on page 33.

### Accepting the recommended policies

**To accept the recommended policies**

1. As a server administrator, after responding to the security assessment you can view the recommended policies of the security profile for the vApp/VM in the **Manage > Security > Symantec Data Center Security - Review Recommended Policies** portlet of vSphere Web client.
2. Click **Accept** to accept the approved recommendation.

**Note:** On accepting the recommendation, there is a notification in Operations Director for the security administrator in **Pending Approval** state. Once the security administrator approves the notification, the security profile and the associated policies are applied on the vApp/VM.

3. The security status of the vApp/VM now changes to **Secured**.

See “Requesting exception on recommended policies” on page 35.

###Requesting exception on recommended policies

It is possible to take an exception from the security policies that Operations Director recommends based on the security assessment questions that you respond to. The **Symantec Data Center Security** portlet under **Manage > Security** tab displays the recommended security policies.
To request an exception

1. Click Request Exception.

   The Exception request on system recommended policies portlet is displayed below the Symantec Data Center Security portlet.

2. Add any comments that you would like to send to the security administrator about the exception under the Comments field.

3. Click Submit.

   The comments are submitted to Operations Director where the security administrator can view them. The title of Exception Request on Recommended Policies portlet changes to Exception History with the comments displayed inline. The comments field is available to add more comments. Note that every comment that you add is applicable to the exception request. Each exception request gets a unique number, which is visible above the comment in the Exception History portlet.

   You cannot perform any further action on the policies until the security administrator responds to the exception that you requested. The Accept and Request Exception buttons appear inactive.

After receiving a response from the security administrator

1. New policies that are recommended by the security administrator based on the modifications to the security profile are visible in the Symantec Data Center Security portlet.

   The Exception History portlet displays the response that is received from the security administrator for that exception.

2. You may click Accept to accept the new recommendations or click Request Exception to request another exception.

   In either case, whether you accept the new policies or request another exception, the Comments field under the Exception History portlet is used to add your comments.

If you choose to accept the new policies

1. Click Accept in the Symantec Data Center Security Service - Review Recommended Policies portlet.

2. The security status in the Symantec Data Center Security portlet now changes to Secured with a check mark icon against each policy that is now applied.

   You may continue to request an exception, if you wish to.

See “Accepting the recommended policies” on page 35.

See “Process of approval and exception request” on page 81.
Provisioning security to a vApp/VM based on custom questions and tags

Operations Director is shipped with a rich set of predefined questions and tags that can be used for security provisioning. However, Operations Director also lets you import custom questions, create custom tags, and map policies to the custom tags.

Import and publish new questions

1. Go to Manage > Questions page of Operations Director.
2. Import custom questions in a CSV file format. You may download the CSV template available on this page.
   
   See “Importing custom questions” on page 43.
3. The imported questions are listed on the page in a Draft state.
4. Select the questions and click Publish to publish them to the vSphere Web client.
   
   Once the question is published, that question is available for provisioning a vApp.
   
   See “Publishing questions” on page 44.

Create a custom tag based on the custom question

1. Go to the Manage > Tags page.
2. Click + to create a custom tag.
3. Enter the name, description, and select or enter a category.
4. Map the mandates to the tag.
   
   This step is optional.
5. Under Select Security Controls and Policies, select at least one security control or policy or firewall template from the available groups.
   
   See “Creating a new tag” on page 49.
6. Map the imported questions to this tag and make sure that you select the responses. Multiple questions can be mapped to a tag.
7. Click Save to save the tag.
   
   See “Creating a new tag” on page 49.

Note: The tags must be published else they will not be recommended on submitting the security assessment questionnaire. See “Publishing tags” on page 53.
Provisioning a vApp/VM based on custom tag recommendation

1. Go to the vSphere Web client and select the vApp/VM. Go to Manage > Security tab. Wait a couple of minutes for the page to load.

2. Click Apply Security... to launch the security assessment questionnaire and submit the responses.
Monitoring Assets

This chapter includes the following topics:

- **About Assets: vApps page**
- **Viewing details of vApp**
- **About Assets: VMs page**
- **Viewing details of virtual machine**

**About Assets: vApps page**

Assets for Operations Director are the vApps in your virtual environment. The **Assets > vApps** page displays only the vApps for which the server administrator has submitted the security assessment responses from the vSphere Web client. The vApps are categorized by application type.

You may cross-navigate from the vApps page to the VMs page and vice versa. The grid on the vApps page displays the count of VMs that are associated to the vApps. You may click on the count of VMs to navigate to the VMs page.

You may click on the count of notifications in the grid to navigate to the Notifications page and view notification that is associated with the vApp.

**Page summary filters on vApps page**

Following is what the page summary filters on the **Assets > vApps** page mean:

- **All** - Count of all vApps irrespective of the security status.
- **Not Secured** - Count of vApps on which the security policies are yet to be applied.
- **Pending Approval** - Count of vApps that need the security administrator’s approval.
This means that the server administrator has already submitted the security assessment responses and the security administrator needs to review the Operations Director-recommended security profile and then approve.

- **Secured** - Count of vApps on which the recommended security policies have been applied.

---

**Note:** Page summary filters will be hidden if the count is zero at any point, except in the case of **All**.

See “Viewing details of vApp” on page 40.

## Viewing details of vApp

To view the details of a vApp

1. Go to the **Assets > vApps** page.
2. Click on a vApp.

   The **vApp Details** tab displays the application name, application type, assessment date, security status, and provisioning status.

   The **Security Profile** tab displays the name of the security profile and an exception applied, if any.

   The **Assessment** tab displays the security assessment questions and the responses that were submitted from the vSphere Web client.

   The **Tags** tab displays the tag name, tag category, count of virtual machines that carry the tag, and description.


## About Assets: VMs page

Assets for Operations Director are the virtual machines in your virtual environment. The **Assets > VMs** page displays the virtual machines for which the server administrator has submitted the security assessment responses from the vSphere Web client. The virtual machines are categorized by application type.

You may cross-navigate from the VMs page to the vApps page and vice versa. The grid on the VMs page displays the name of vApp that is associated to the VMs. You may click on the vApp name to navigate to the vApps page.

You may click on the count of notifications in the grid to navigate to the Notifications page and view notification that is associated with the VM.
Page summary filters on VMs page

Following is what the page summary filters on the Assets > VMs page mean

- **All** - Count of all VMs irrespective of the security status.
- **Not Secured** - Count of virtual machines on which the security policies are yet to be applied.
- **Pending Approval** - Count of virtual machines that need the security administrator's approval.
  This means that the server administrator has already submitted the security assessment responses and the security administrator needs to review the Operations Director-recommended security policies and then approve.
- **Secured** - Count of virtual machines on which the recommended security policies have been applied.

---

**Note:** Page summary filters will be hidden if the count is zero at any point, except in the case of All.

---

See “Viewing details of virtual machine” on page 41.

---

Viewing details of virtual machine

To view the details of a VM

1. Go to the Assets > VMs page.
2. Click on a virtual machine.

The **VM Details** tab displays the details of the virtual machine such as the OS type, IP address, host name, application type, assessment date, security status, and provisioning status.

The **Security Profile** tab displays the name of the active security profile and exception requested, if any.

The **Assessment** tab displays the security assessment questions and the responses that were submitted from the vSphere Web client.

The **Tags** tab displays the tag details such as, the name of the tag, the tag category, and description.

See “About Assets: VMs page” on page 40.
Managing Questions

This chapter includes the following topics:

- About questions
- Importing custom questions
- Deleting questions
- Publishing questions
- Mapping a question and response to a tag

About questions

Questions are used to understand the production environment scenario. Based on the responses that you provide as a server administrator, Operations Director recommends the security policies.

A set of questions that are published from Operations Director by the security administrator are made available in the Security tab of the vSphere Web client, after you install the Symantec Data Center Security plug-in. As a server administrator, you must apply security by responding to the questions.

Note: Security administrator must use the Manage > Questions page of Operations Director to publish the questions to vSphere Web client. Questions are visible in vSphere Web client only after they are published.

The Manage > Questions page of Operations Director displays a list of questions in draft and published state, the name of the user who imported the questions, the type of question, and the date and time of import. The Tags column displays a count of tags that are mapped with a question. If you click on the count, you will be
navigated to the Manage > Tags page, which lists the tags that are mapped to the question.

See “Importing custom questions” on page 43.

See “Publishing questions” on page 44.

See “Responding to the security assessment” on page 33.

See “Deleting questions” on page 44.

See “Mapping a question and response to a tag” on page 45.

Importing custom questions

To import custom questions

1. Go to the Manage > Questions page of Operations Director.
2. Click CSV format to download a template that you can use to add questions.
3. Click Import to select the CSV file and import the questions in Operations Director.

Note: You can import a file only in a CSV format.

The imported questions are listed at the top of the list. Notice the status of the imported questions is Draft and by default the questions are selected.

4. Click Publish to publish the questions to the vSphere Web client.

Once the questions are published, they are available in the security assessment questionnaire.

Contents of the sample CSV file

Following are the columns provided in the sample CSV file:

- Question Text
  Enter the question here. Question text must be up to 100 characters.

- Question Description
  Enter a description for the question. This is optional.

- Question Type
  Enter the value 1 for single choice question.

- Answer Text
  Enter answer for the question. Answer text must be up to 1000 characters.

- Answer Description
Enter a description for the answer. This is optional.

- **Is Default**
  Enter the value as either True or False. For example, in the case of a question that has an answer as Yes or No, you can set the default answer that you want to be selected by setting the value as True.

**Note:** Questions that are invalid (content is not adhering to the expected CSV format) or duplicates are not imported in Operations Director. If the same question is repeated in the assessment, ensure that the response is unique for the two instances of the same question.

See "Deleting questions" on page 44.
See "Mapping a question and response to a tag" on page 45.
See “Publishing questions” on page 44.
See “About questions” on page 42.

## Deleting questions

To delete questions from the question bank, go to the Manage > Questions page. Select the questions that you want to delete and click the X icon.

Questions that have tags associated with them cannot be deleted. You must first resolve the question to tag mapping on the Manage > Tags page and then delete the question.

**Note:** Questions that are only in a Draft state and not mapped to any tags can be deleted.

See "Importing custom questions " on page 43.
See “Mapping a question and response to a tag” on page 45.
See “Publishing questions” on page 44.
See “About questions” on page 42.

## Publishing questions

To publish questions to the vSphere Web client, use the Manage > Questions page of Operations Director. The questions that you import using the CSV template are available in a draft mode. Select the draft questions and click **Publish**.
Only the published questions are available in the vSphere Web client.
You can publish multiple questions. Questions that you import and publish must be mapped to some tags while creating tags.

**Note:** Ensure that the question to tag mapping is correctly done. You will not be able to revert the publish action.

See “Mapping a question and response to a tag” on page 45.
See “Importing custom questions” on page 43.
See “Deleting questions” on page 44.
See “Mapping a question and response to a tag” on page 45.
See “Importing custom questions” on page 43.
See “About questions” on page 42.

### Mapping a question and response to a tag

You can map single or multiple questions and response to a tag while creating a new tag.

**To map a question and response to a tag**

1. Go to the Manage > tags page.
2. Click the + icon to add a new tag.
3. When creating a new tag, in the Map Security Questions section, select and add a question and select a response for each question.

When you save the tag, the questions and responses are associated to the tag.

See “Importing custom questions” on page 43.
See “Deleting questions” on page 44.
See “Publishing questions” on page 44.
See “About questions” on page 42.
Managing Tags

This chapter includes the following topics:

- About tags
- How tags are used to derive the right security
- About tier tags
- Defining regular expressions for identifying tiers based on VM names
- Creating a new tag
- Viewing tag details
- Editing a tag
- Creating copy of a tag
- Publishing tags

About tags

Operations Director is shipped with a comprehensive library of Symantec-defined security tags to allow users to get value out of the product.

As a security administrator, you can create custom security tags and tag categories unique to your environment and also edit them.

Tags can be managed from the Manage > Tags page of Operations Director.

Page summary filters on Tags page

Following is what the page summary filters on the tags page mean:

- All
  The count of all available tags.
Published

The count of tags published by Operations Director that are recommended after submitting the security assessment questionnaire in vSphere Web client.

Draft

The count of tags that are in a draft state and yet to be published.

You can add, edit, and delete tags from the Manage > Tags page.

See “How tags are used to derive the right security” on page 47.

See “How tags are used to derive the right security” on page 47.

See “About tier tags” on page 48.

See “Creating a new tag” on page 49.

See “Creating copy of a tag” on page 52.

See “Publishing tags” on page 53.

See “Viewing tag details” on page 51.

See “Editing a tag” on page 52.

How tags are used to derive the right security

Questions and tags together play a crucial role in determining the security policies. Operations Director is shipped with Symantec-defined tags. Operations Director also lets you create custom tags. Each tag is mapped to mandates (optional), security policies, questions and their responses.

Operations Director determines security policies based on the responses to the security assessment questions that the server administrator submits.
Let us understand how Operations Director derives the right security for you behind the scenes

1. The server administrator responds to the security assessment questionnaire in vSphere Web client.

2. Tags have been published and the questions are associated to the tags by the security administrator already.

3. Operations Director analyzes the responses and recommends tags. For example, PCI, SLA-Silver, and so on.

4. Each tag has security controls and policies of security products that have been configured with Operations Director mapped to it based on which Operations Director recommends the security policies to secure a vApp/VM.

See “About tags” on page 46.

See “Viewing tag details” on page 51.

See “Creating a new tag” on page 49.

See “Creating copy of a tag” on page 52.

See “Publishing tags” on page 53.

See “Editing a tag” on page 52.

About tier tags

Tier tags are the tags added in vCenter on virtual machines to indicate the specific application tier that the VM belongs to. For example, a VM can be tagged as “DB” if the VM has a database running on it. Tier tags on the virtual machines are used to determine the firewall provisioning policies.

Tiers must be assigned to a virtual machine if you choose a business application when responding to the security assessment. If you do not select a business application and retain the default value of None, the firewall policies will not be applied.

See “Defining regular expressions for identifying tiers based on VM names” on page 49.

Operations Director gives first preference to tier tags. If Operations Director does not find tier tags associated to one or more virtual machines, it can derive tiers based on the name of the VM.

If tiers cannot be derived by Operations Director based on the virtual machine names, you must manually apply tier tags or rename the virtual machines with the standard format to allow tier identification.
Defining regular expressions for identifying tiers based on VM names

For Operations Director to determine tiers based on virtual machine names, you can define regular expressions in the od.properties file.

To define regular expressions

1. On the Operations Director appliance, edit the /usr/local/Symantec/so/config/od.properties file.

2. In this file, look for the following default values:
   - od.tiergeneration.webtierregex=.*_WEB
   - od.tiergeneration.apptierregex=.*_APP
   - od.tiergeneration.dbtierregex=.*_DB

3. Update the values in the above entries with the virtual machine name. The virtual machine name that you update in these entries must satisfy this format. A valid regular expression is supported.

4. Restart the security orchestration services.

   You must restart the security orchestration services by restarting the Apache Tomcat Web server for the changes to take effect. To do this, run the following commands from the appliance:

   sh /opt/apache-tomcat-7.0.53/bin/shutdown.sh
   sh /opt/apache-tomcat-7.0.53/bin/startup.sh

   This reloads the od.properties file.

Creating a new tag

To create custom security tags, go to Manage > Tags page of Operations Director. Symantec-defined tag categories and tags are listed on this page. The Author column in the grid on the Manage > Tags page displays System for tags that are shipped with Operations Director.
To create a new tag

1. Click the + icon to add a new tag.

2. On the Add Tag page, enter a name, description, and select or type a category for the tag.

   The name and category fields are mandatory.

   *Note:* The name and category fields do not accept the following special characters

   ! $ % ^ & * ( ) [ ] + - = ` { } : " ; ' < > , . / 

3. Under *Mandates* section, select the mandates that you want to map to the tag. This step is optional.

4. Under *Select Security Controls and Policies*, select at least one IDS/IPS policy or anti-malware policy or firewall template.
   - IDS/IPS is intrusion detection service and intrusion prevention service that is available only after you configure DCS:SA successfully. Expand *IDS/IPS* and select a policy.
   - Anti-malware policies are available only after you configure DCS:S successfully. Expand *Anti-malware* and select a policy.
   - Firewall lists the Palo Alto Networks Next Generation Firewall templates. Palo Alto Networks Next Generation Firewall must be configured successfully. Firewall template applies the firewall rules of Palo Alto Networks Next Generation Firewall. Expand *Firewall > Palo Alto Networks Next Generation Firewall*. The available templates are listed. Select a template to apply to the appropriate firewall rules. Make sure to select one firewall template for every application type. This way the tag you create gets mapped to Palo Alto Networks Next Generation Firewall rules with the help of the firewall template that you select.
5 Under Map Security Questions section, select at least one question and its response to map to the tag.

Note: If you select the same question twice make sure that the responses that you select for the questions are unique.

All available questions in Operations Director on the Manage > Questions page are also listed under the drop-down. The list of questions can contain draft as well as published questions.

6 Click Save to save the new tag.

7 This tag is listed in the list of tags in a draft state.

You must publish the tag. Only after you publish the tag, the tag is recommended by Operations Director when the server administrator responds to the security assessment from the vSphere Web client.

See “About tags” on page 46.
See “How tags are used to derive the right security” on page 47.
See “Publishing tags” on page 53.
See “Creating copy of a tag” on page 52.
See “Viewing tag details” on page 51.
See “Editing a tag” on page 52.

Viewing tag details

To view the details of a tag go to the Manage > Tags page of Operations Director. Click on the desired tag name to view the tag details.

The tag details are a summary of what all is mapped to the tag. The tag details page displays the following:

- Description, state, and category of the tag.
- Security mappings
- Mandates
- Security controls and policies
- Questions

See “About tags” on page 46.
See “Creating a new tag ” on page 49.
Editing a tag

You can select and edit only one tag at a time that is in a **Draft** state. A published tag cannot be edited.

To edit a tag

1. Go to the **Manage > Tags** page.
2. Select the tag that you want to edit and click the edit icon.
   - The **Edit Tag** page is displayed.
3. Make the necessary changes to the tag details and click **Save** to save the values. For specifics of each field See “Creating a new tag” on page 49.

---

**Note:** Reset clears any values that you may have saved in a draft state.

---

**Note:** If one or more policies that were previously associated with the security control or firewall template are deleted, you must select and map another firewall template or policies within the security control and save the tag.

---

See “About tags” on page 46.

See “Creating a new tag” on page 49.

See “Creating copy of a tag” on page 52.

See “Viewing tag details” on page 51.

See “How tags are used to derive the right security” on page 47.

Creating copy of a tag

You have the edit permissions by default in the role of ODAadmin to create a copy of a tag.
To create copy of a tag

1. Go to the Manage > Tags page.
2. Select a tag that is in Draft state and then click the edit icon.
   The Edit Tag - <Tag_Name> page is displayed.
3. Edit the Name field and save the tag.
   You may or may not update the remaining fields on this page. Editing the Name field and saving the tag creates a copy of the tag in a draft state.

See “Creating a new tag” on page 49.
See “Publishing tags” on page 53.
See “Viewing tag details” on page 51.
See “Editing a tag” on page 52.

Publishing tags

You can publish tags that are in a draft state from the Manage > Tags page of Operations Director.

To publish a tag
Select the tags that are in a draft state and click Publish.
The tags get published to the security assessment questionnaire in the vSphere Web client.

Points to remember

- Tags must be published else they will not be recommended upon submitting the security assessment questionnaire.
- Tags cannot be published if policies of non-configured products are mapped to the tag.
- Tags cannot be published if the policies mapped to them are deleted from the security products.
- Tags that have questions in a draft state mapped to them cannot be published. The questions mapped to the tags must be in a published state.

See “About tags” on page 46.
See “Creating a new tag” on page 49.
See “Creating copy of a tag” on page 52.
See “Viewing tag details” on page 51.
See “How tags are used to derive the right security” on page 47.
See “Editing a tag” on page 52.
Managing Policies

This chapter includes the following topics:

- About policies
- Editing precedence order value of policies
- Viewing policy details

About policies

The Manage > Policies page lets you manage policies that get imported when you add a security product in Operations Director from the Settings > Integration page of UMC.

The left navigation displays the security products and security controls whose policies are imported in Operations Director.

The Tags tab in the drawer pane displays the tags that are mapped to the policy. Select a policy to view this information.

Note: The Tags tab displays all tags that are mapped to the selected security policy.

Page summary filters on Policies page

Following is what the page summary filters mean:

- All
  The count of all policies that are imported.
- Applied
  The count of policies that are applied on a vApp/VM.
- Unused
  Count of policies that have not been applied on any vApp/VM.
- Tagged
  Count of policies that are associated with tags.
- Untagged
  Count of policies that are not associated with any tags.

The columns **Applied on VMs** and **Applied on Profiles** displays a count of VMs and profiles respectively on which the policies have been applied. You can click on the count and navigate to the VMs or Profiles page to view the details of VMs and profiles, respectively.

See “**Editing precedence order value of policies**” on page 56.

See “**Viewing policy details**” on page 57.

**Editing precedence order value of policies**

When a security product is configured, Operations Director imports policies and auto-assigns the precedence order values. Auto-assignment of policies is derived from a combination of the security product and platform.

**Significance of precedence order value**

Although, Operations Director auto-assigns the precedence order value, you may edit the precedence order value. Setting a lower precedence order value ensures a higher significance of the policy. Based on the precedence, the policies are considered for security provisioning.

Let us understand this with an example.

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Precedence Order</th>
<th>Platform</th>
<th>Product</th>
</tr>
</thead>
<tbody>
<tr>
<td>A_6.0</td>
<td>1</td>
<td>Windows</td>
<td>DCS:S</td>
</tr>
<tr>
<td>B_6.0</td>
<td>2</td>
<td>Windows</td>
<td>DCS:S</td>
</tr>
<tr>
<td>C_5.5</td>
<td>1</td>
<td>Windows</td>
<td>DCS:S</td>
</tr>
<tr>
<td>D_5.5</td>
<td>2</td>
<td>Windows</td>
<td>DCS:S</td>
</tr>
</tbody>
</table>

- Policy C and D or policy A and B cannot have the same precedence order value because their platform, product, and version is common.

- However, policy A and C or policy A and D can have the same precedence order value because the version is unique. Therefore, you can edit the precedence order value of policy D to 1.

Editing policy precedence lets you re-arrange the default order in which the policies are listed on the **Manage > Policies** page.
To edit policy precedence

1. Go to the Manage > Policies page.
   The policies are displayed in an ascending order (default) in the grid.
2. Select the policy for which you want to change the precedence order and click Edit Order.
   The Order column is enabled for editing.
3. Enter the precedence value that you wish to and click Save Order.

Note: Precedence order value must be unique for policies having same platform, product, and version (displayed in the policy name). Precedence order value can be same for policies having same platform, product but different version. Precedence order value must be a number from 1 through 999.

See “Viewing policy details” on page 57.
See “About policies” on page 55.

Viewing policy details

To view the details of a policy

1. Go to the Manage > Policies page and select a row in the policy grid.
2. The Tags tab in the details drawer displays the list of tags that are mapped to the policy.

Note: You can view the details of only one selected policy at a time.

See “Editing precedence order value of policies” on page 56.
See “About policies” on page 55.
Managing Profiles

This chapter includes the following topics:

- About security profiles
- About Profiles page
- Viewing the details of a profile
- Editing a recommended security profile in draft state
- Adding a custom policy to a profile
- Enabling a policy
- Disabling a policy
- Deleting a policy
- Deleting a security profile

About security profiles

Profiles are a set of parameters and instructions unique to a particular vApp and a standalone virtual machine that describes how the security policies should be applied, typically to maximize the security or compliance of that resource. These parameters are calculated by Operations Director using a number of relevant inputs such as responses to security assessment and tags.

How does Operations Director derive a security profile recommendation?

Operations Director has its own intelligence that is based on the application context and security tags. Operations Director decides which policies need to be enforced. It generates application context based on the information received from vCenter,
responses to the security assessment and associated tags to decide what actions need to be taken for securing the application.

You cannot manually create or add security profiles to Operations Director. Operations Director creates security profiles for you at run time.

The security administrator has to approve the notification of a recommended security profile that is in a **Pending Approval** state after which the security profile is applied on the application and listed on the **Manage > Profiles** page of Operations Director in **Applied** state.

See “About Profiles page” on page 59.
See “Viewing the details of a profile” on page 60.

## About Profiles page

The **Manage > Profiles** page displays the security profiles that Operations Director recommends for a new application. By default, the security profile is in a **Pending Approval** state when it is recommended by Operations Director.

The state changes to **Applied** only after the security administrator approves the notification for the new application on the **Monitor > Notifications** page.

### Page summary filters on Profiles page

Following is what the filter buttons mean:

- **All**
  - Displays the count of all security profiles.

- **Pending Approval**
  - Displays the count of notifications that are pending the security administrator's approval.

- **In Progress**
  - Displays the count of profiles that have been approved by the security administrator but in the process of getting applied on the application.

- **Applied**
  - Displays the count of profiles that are applied and active on an application.

The details of what a security profile is composed of is shown under the tabs **Summary**, **Policies**, and **Orchestrated Groups**.

See “Viewing the details of a profile” on page 60.
See “About security profiles” on page 58.
See “Deleting a security profile” on page 65.
Viewing the details of a profile

There are two ways to view the details of a security profile.

1. Go to the Manage > Profiles page.
2. Select a profile.

Alternatively, before you approve a notification you can:

1. Go to the Monitor > Notifications page.
2. Select a notification that is pending approval.
3. Under the Recommendations tab, click the security profile that is recommended by Operations Director.

You are redirected to the profile details page.

The Summary tab displays the aggregated association of:

- Tags associated to mandates.
- Mandates associated to control statements.
- Control statements associated to security products.
- Security products associated to security policies.

The Policies tab displays the policies associated to the profile. You can add, delete, enable, and disable policies from this tab. Policies that are recommended by Operations Director are prefixed with an asterisk (*).

The Orchestrated Groups tab shows the security groups such as NSX security group, DCS:SA groups, and Palo Alto Networks Next Generation Firewall address groups that are associated with the profile. It also shows the count of virtual machines that are part of the security group, and the policies that are applied. This is shown only if the profile is in Applied state or Error state. There is no information shown in this tab when the profile is In progress or Draft state.

See “About security profiles” on page 58.
See “Deleting a security profile” on page 65.
Editing a recommended security profile in draft state

To edit a recommended security profile that is in draft state

1. Go to the Monitor > Notifications page.

   The notification for the new application is listed at the top in the grid. The state of the notification is Pending Approval and the security status of the vApp is Not Secured.

2. Select the notification.

   The Assessment tab displays the details of the questions and responses.
   The Analysis tab displays the identified tags, recommended security policies, and recommended security profile.
   The Recommendations tab lists the recommended security policies as part of the recommended security profile.

   **Note:** The policies that are prefixed with an asterisk (*) are the system recommended security policies.

3. Let us assume you are the security administrator and you want to add a new security policy to a recommended security profile.

   Click on the recommended security profile name. You will be navigated to the Manage > Profiles page. The profile will be selected by default as the first entry in the grid on this page.

4. Click on the Policies tab in the details drawer and add a custom policy.

   See “Adding a custom policy to a profile” on page 62.

   After adding a custom policy to the recommended security profile, a message is displayed at the top of the page.

   Click Profile Approval to notify the server administrator of the update or click Notifications to navigate back to the Manage > Notifications page. You may choose to notify the server administrator later as explained in the next step.

5. Because the recommended security profile is now updated with a new security policy, it needs an approval from the server administrator. Under the Recommendations tab, click Notify server administrator for approval. A notification is sent to the vSphere Web client.

   The state of the notification now changes to Waiting. The server administrator must either accept the recommended security profile or request an exception.
On the vSphere Web client

1. Select the vApp in the vSphere Web client.
2. Go to vCenter > Inventory Lists > vApps > <vApp_name> > Manage > Security tab.
   
   Under the Symantec Data Center Security - Review Recommended Policies portlet, the recommended security policies are listed.
3. As a server administrator, review the security policies and either accept them or request an exception if you would like to change them.
   
   - If you click Accept, the notification in Operations Director changes to Pending Approval state. The security administrator has to approve the notification to apply the policies.
   
   - If you click Request Exception, the Exception Request on Recommended Policies portlet is displayed.
     Enter comments for the security administrator and click Submit to submit the exception.

The communication between the server administrator and the security administrator is displayed in this portlet. On submitting the exception, the existing notification gets updated in Operations Director on the Monitor > Notifications page. The title of the Exception Request on Recommended Policies portlet changes to Exception History.

See “Process of approval and exception request” on page 81.

Adding a custom policy to a profile

You can add a custom policy to a profile. Profile must be in a Pending Approval state as well as the notification must not be in a Waiting or Pending Approval state. This means that the recommended policies should have been either accepted or have an exception requested from vCenter Web client.

To add a policy

1. Go to the Manage > Profiles page.
2. Select the profile to which you want to add a new policy.
3. Select the Policies tab.
4 Click the + icon.

In the Add Policy dialog box, select the security control, security product, and policy from the respective drop-down.

You can type free text in the Policy drop-down. Based on a close match to what you type the policy is retrieved and displayed in the drop-down as you type.

**Note:** The Policy drop-down is dynamic. If you are adding Palo Alto Networks Next Generation Firewall templates, the control changes to Firewall Templates. Templates are auto-filtered by the application type of the security profile. If the vApp does not have an application type set, selection of Palo Alto Networks Next Generation Firewall templates is disabled.

5 Click Add to save the new policy.

The newly added policy is displayed in the grid under the Policies tab. Notice that a custom policy that you add does not have an asterisk (*) prefixed.

**Points to remember**

- Only one policy of a platform and a specific version from the same product can be enabled. You can have multiple policies of a different platforms or different versions enabled in a security profile. You must remove or disable existing policy to proceed.

- Only one firewall template can be enabled. You must remove or disable existing firewall template to proceed.

- Firewall template cannot be added for a vApp if it does not have an application type associated. If you want to set an application type for a vApp, the security provisioning process will have to be redone for the vApp. The server administrator will have to select the business application while responding to the security assessment.

See “About policies” on page 55.

**Enabling a policy**

Policies that are recommended by Operations Director and custom policies that you define can be enabled and disabled.

Profile must be in a **Pending Approval** state as well as the notification must not be in a waiting state. This means that the recommended policies should have been either accepted or have an exception requested from vCenter Web client.
To enable a policy

1. Go to the Manage > Profiles page.
2. Select a profile and click the Policies tab.
3. Under the Policies tab, select the policy that you want to enable.
4. Click Enable.

See “Disabling a policy” on page 64.

Disabling a policy

Policies that are recommended by Operations Director and custom policies that you define can be enabled and disabled.

Profile must be in a Pending Approval state as well as the notification must not be in a waiting state. This means that the recommended policies should have been either accepted or have an exception requested from vCenter Web client.

To disable a policy

1. Go to the Manage > Profiles page.
2. Select a profile and click the Policies tab.
3. Under the Policies tab, select the policy that you want to disable.
4. Click Disable.

See “Deleting a policy” on page 64.

See “Editing precedence order value of policies” on page 56.
See “Viewing policy details” on page 57.
See “About policies” on page 55.

Deleting a policy

You can delete custom policies that you may have added to the security profile. Policies that are recommended by Operations Director cannot be deleted, they can only be disabled.

Profile must be in a Pending Approval state as well as the notification must not be in a waiting state. This means that the recommended policies should have been either accepted or have an exception requested from vCenter Web client.
To delete a policy
1  Go to the Manage > Profiles page.
2  Select the profile from which you want to delete a policy.
3  Select the Policies tab.
4  Select a custom policy that you want to delete.
5  Click the X icon to delete.
See “Editing precedence order value of policies” on page 56.
See “Viewing policy details” on page 57.
See “Disabling a policy” on page 64.
See “About policies” on page 55.

Deleting a security profile
As a security administrator, you may delete a security profile when you want the security policies removed for a given application or when the application itself has been deleted and the security policies associated with it need to be cleaned up.

To delete a security profile
1  Go to the Manage > Profiles page.
2  Select the profile that you want to delete and click the X icon.
   This triggers the delete operation. A confirmation message is displayed.
3  Click OK to proceed with the delete operation.
   Delete action deletes all the security policies that are currently applied to the vApp/virtual machine.

---

**Note:** Deleting a profile deletes the NSX security groups/policies, Palo Alto Networks Next Generation Firewall address groups/policies, and DCS:SA asset groups/policy associations.

Points to remember
- If the delete operation succeeds, the security profile is no longer visible.
- Deleting a security profile in Applied state will remove security policies that are applied on assets.
Deleting a security profile may fail if, the security products are unreachable or the connections credentials have changed. Verify if the security products are configured correctly.

If the delete action fails, the state of the security profile changes to **Delete Failed**.

Deleting a security profile in **Delete Failed** state will remove it from Operations Director. You may have to manually delete the NSX security groups/policies, Palo Alto Networks Next Generation Firewall address groups/policies, and DCS:SA asset groups/policy associations from the security products.

Once you manually delete the corresponding objects in the security product, you can retry deleting the security profile from the Operations Director console. This time since the underlying security product objects have been manually deleted, Operations Director should delete the security profile successfully.

See “Viewing the details of a profile” on page 60.

See “About security profiles” on page 58.
Managing Firewall Templates

This chapter includes the following topics:

- About firewall templates
- Creating a firewall template
- Viewing a firewall template
- Editing precedence order value of firewall template
- Editing a firewall template
- Creating copy of a firewall template
- Provisioning Palo Alto Networks Next Generation Firewall for new application
- Deleting a firewall template

About firewall templates

Palo Alto Networks Next Generation Firewall creates rules for each application type and application configuration. These rules are used as reference by Operations Director. Palo Alto Networks Next Generation Firewall rules have application-specific port/protocol details and traffic restrictions defined. Palo Alto Networks Next Generation Firewall rules have source and destination address groups as empty/any. They are replaced by the right address groups for each new application instance.

For a given application type such as SharePoint, you can create multiple firewall templates. For example, Sharepoint_Critical, Sharepoint_Base, Sharepoint_Medium. Each firewall template is mapped to pre-existing rules in Palo Alto Networks Next Generation Firewall.
The Manage > Firewall Templates page displays templates in Active and Draft state. The count of associated VMs is displayed in the grid. You may click on the count to navigate to the Assets > VMs page to view the associated VMs. The templates are categorized according to the application types. You can select the row in the grid and view the Details and Firewall Rules tab to view the description and the associated firewall rules with the source and destination tiers.

See “Creating a firewall template” on page 68.

See “Editing precedence order value of firewall template” on page 70.

See “Deleting a firewall template” on page 75.

See “Editing a firewall template” on page 71.

See “Creating copy of a firewall template” on page 71.

Creating a firewall template

Refer the article Creating rules in Palo Alto Networks® Panorama for detailed steps on how to create empty address groups in Panorama and how to create rules in Panorama with empty address groups.

When you create a firewall template, if there are no firewall rules available you have to make sure that the rules are created in Palo Alto Networks Next Generation Firewall. Contact Panorama administrator for creating firewall rules.

Once firewall rules are created in Palo Alto Networks Next Generation Firewall you must go to the Monitor > Synchronization Status page and synchronize the policies of Palo Alto Networks Next Generation Firewall with Operations Director. This will ensure that the firewall rules are available when you create a firewall template. You will not be able to create and save a firewall template unless there are firewall rules available.

To add a new firewall template

1. Go to the Manage > Firewall Templates page. Click the + icon.

2. On the Add Template page, type the name and description, and enter or select a type for the firewall template.

Note: The name and type fields accept a maximum of 50 characters. The description field accepts a maximum of 256 characters. The name and type fields do not accept the following special characters

! $ % ^ & * ( ) [ ] + | ~ = ` { } : " ; ' < > ? . / \
3 Under the **Firewall Rules** section, select the firewall rules. All rules that are imported from Palo Alto Networks Next Generation Firewall are listed in the **Select Rule** drop-down list.

4 Click **Save** to save the firewall template.

The new firewall template is listed on the **Manage > Firewall Templates** page. The precedence is automatically assigned to the firewall template. By default, any new firewall template that you create gets the lowest precedence in the application type. You may click **Edit Precedence Order** to modify the precedence.

**What happens after you create a new firewall template?**

When a firewall template is created, it appears on the **Add tag** page under **Manage > Tags** when you add a new tag by clicking the + icon. Thereafter, the application type of the new firewall template is available under the business application drop-down of the security assessment questionnaire in vSphere Web client.

See “**Editing precedence order value of firewall template**” on page 70.

See “**Deleting a firewall template**” on page 75.

See “**Editing a firewall template**” on page 71.

See “**About firewall templates**” on page 67.

See “**Creating copy of a firewall template**” on page 71.

---

**Viewing a firewall template**

To view a firewall template

1 Go to the **Manage > Firewall Templates** page.
   
The **Firewall Templates** page lists all types of available firewall templates.
   
You may use the filters in the left navigation or the click the filter buttons on the top to filter the list of firewall templates in the grid.

2 Select a row to view the **Details** and **Firewall Rules** tabs in the details drawer.
   
   - The **Details** tab displays the description of the firewall template.
   
   - The **Firewall Rules** tab displays the Palo Alto Networks Next Generation Firewall rules that are mapped to the firewall template and corresponding source tier and destination tier.

3 You may click on the firewall template name to drill-down and view the details.
   
As a security administrator, you have edit permissions by using which you can modify the template on the **Edit Template** page.
Editing precedence order value of firewall template

When you create a new firewall template, the precedence is automatically assigned to the firewall template. By default, any new firewall template that you create gets the lowest precedence in the application type. Setting a lower precedence order value ensures a higher significance of the firewall template.

Significance of setting the firewall template precedence

When you create a firewall template, the type of application that you select/enter is listed under the business application drop-down in the security assessment questionnaire in the vSphere Web client that the server administrator responds to. Each firewall template belongs to an application type. Multiple firewall templates can belong to the same application type.

When the server administrator responds to the security assessment in vSphere Web client and selects the business application, the firewall template that gets associated depends on the precedence order value that is set from this page.

To update the precedence order value

1. Go to the Manage > Firewall Templates page of Operations Director.
2. Select the firewall template and click Edit Precedence Order.
3. The Order column in the grid is enabled for editing.
4. Type the precedence order value and save the changes.

Following are some points to be noted while setting the precedence order value:

- Precedence order value must be a number from 1 through 999.
- Precedence order value of a firewall template must be unique for an application type.

See “About firewall templates” on page 67.
See “Deleting a firewall template” on page 75.
See “Editing a firewall template” on page 71.
Editing a firewall template

To edit a firewall template

1. Go to the Manage > Firewalls Templates page.
2. Click the firewall template in draft state to go to the edit mode.
3. On the edit page, the values that are set are displayed. You may change the name, type, description, and rules.
4. Click Save to save the changes.

Points to remember

- As a security administrator, you can edit the firewall template in Draft state by clicking on the firewall template name. You cannot edit or create a copy of a firewall template that is in Active state.
- If one or more firewall rules that were previously associated with the template are deleted, you must select another firewall rule.

Creating copy of a firewall template

You have the edit permissions by default in the role of ODAadmin to create a copy of a firewall template.
To create copy of a firewall template

1. Go to the Manage > Firewall Templates page.
2. Click on a firewall template that is not active.
   If you have edit permissions, the Edit Template page is displayed.

   **Note:** You can only edit a template that is inactive.

3. Edit the Name field and save the firewall template.
   You may or may not update the remaining fields on this page. Editing the Name field and saving the template creates a copy of the firewall template.

See “Creating a firewall template” on page 68.
See “Editing precedence order value of firewall template” on page 70.
See “Deleting a firewall template” on page 75.
See “Editing a firewall template” on page 71.
See “About firewall templates” on page 67.

**Provisioning Palo Alto Networks Next Generation Firewall for new application**

Refer the article Creating rules in Palo Alto Networks® Panorama for detailed steps on how to create empty address groups in Panorama and how to create rules in Panorama with empty address groups.

Palo Alto Networks Next Generation Firewall creates rules for each application type and application configuration. These are used as reference rules by Operations Director.

- Palo Alto Networks Next Generation Firewall rules have application specific port/protocol details and traffic restrictions defined.
- Palo Alto Networks Next Generation Firewall rules have source and destination address groups as empty/any. These are replaced by the right address groups for each new application instance.

To understand this workflow, let us take an example of a SharePoint application that is deployed on a virtual machine.
To create a firewall template

1. Go to the **Manage > Firewall Templates** page to create a new firewall template as explained in See “Creating a firewall template” on page 68.

2. Enter the application type as SharePoint. The application type that you enter here will be available in the vSphere Web client as a business application.

3. Name the firewall template as **Sharepoint_Critical**, for this example.

4. Select the firewall rules to secure the tier-to-tier traffic:
   - Select the firewall rule **PAN_Sharepoint_Critical_R1** and set it as the Web to App rule.
   - Select the firewall rule **PAN_Sharepoint_Critical_R2** and set it as the App to DB rule.
   - Select the firewall rule **PAN_Sharepoint_Critical_R3** and set it as the Web to External rule.

5. Click **Save** to save the template.

---

**Note:** For a given application type (that is SharePoint), you can create multiple firewall templates for example Sharepoint_Critical, Sharepoint_Base, and Sharepoint_Medium. Each firewall template will be mapped to the preexisting rules in Palo Alto Networks Next Generation Firewall.

---

To configure Operations Director tags to map to Palo Alto Networks Next Generation Firewall rules by using firewall templates

1. Go to the **Manage > Tags** page and create a new tag **DMZ**, for this example.

2. Add a description and select a set of mandates.

3. Select the set of security product policies for the DMZ tag:
   - Select the product **Palo Alto Networks Next Generation Firewall**.
   - All application types and corresponding application templates that are created on the **Manage > Firewall Templates** page will be listed in this section.
   - Select few application templates for example Sharepoint_Critical, Sharepoint_Base, and Sharepoint_Medium that belong to the same application type (that is SharePoint).
   - You may select firewall templates from multiple application types.
4 Under **Map Security Questions** section, select at least one question and its response to map to the tag.

5 Save and publish the tag.

**To set up Palo Alto Networks Next Generation Firewall for a new application**

1 In vSphere Web client, apply the tier tags **Web, App, DB** to the virtual machines of the newly created **Marketing_Sharepoint** vApp.

2 Initiate security assessment for a newly created **Marketing_Sharepoint** vApp.

3 While answering the security assessment questions, select the business application as **SharePoint**.

4 Submit the security assessment responses.

5 On submitting the security assessment, Operations Director now analyzes the security policies.
   - Operations Director adds the tag **DMZ** to the **Marketing_Sharepoint** vApp.
   - Operations Director identifies that the Palo Alto Networks Next Generation Firewall template to be applied is **Sharepoint_Critical** (because **Sharepoint_Critical** is the most significant template among all the templates mapped with tag **DMZ**.)
     See “Editing precedence order value of firewall template” on page 70.

6 In vSphere Web client, review the list of security policies selected for the vApp and accept the policies. On accepting the policies, a notification is sent to the security administrator.

7 Go to the **Monitor > Notifications** page and approve the notification.

**What actions does Operations Director perform?**

- Operations Director creates NSX security groups (**Marketing_Sharepoint_Web**, **Marketing_Sharepoint_App**, and **Marketing_Sharepoint_DB**) and adds virtual machines with the corresponding tags (**Web, App, DB**) in the NSX security groups.

- Operations Director creates Palo Alto Networks Next Generation Firewall address groups (**Marketing_Sharepoint_Web**, **Marketing_Sharepoint_App**, and **Marketing_Sharepoint_DB**) and sets up a dynamic membership relationship with the corresponding NSX security group.

- Name of NSX and Palo Alto Networks Next Generation Firewall groups will be suffixed with Operations Director generated number.

- Operations Director refers to the firewall template mapped to security profile and identifies Palo Alto Networks Next Generation Firewall rules
PAN_Sharepoint_Critical_R1, PAN_Sharepoint_Critical_R2, and PAN_Sharepoint_Critical_R3.

- Operations Director creates copies of the above rules to create new firewall rules PAN_Sharepoint_Critical_R1, PAN_Sharepoint_Critical_R2, and PAN_Sharepoint_Critical_R3.

- Name of the newly created rule will be suffixed with _od_<OD-generated number>.

- For each rule, Operations Director updates the source and destination addresses with the vApp specific address groups. For example, for the Marketing_Sharepoint_R1, Operations Director sets the source as Marketing_Sharepoint_Web and the destination as Marketing_Sharepoint_App in Palo Alto Networks Next Generation Firewall.

- Operations Director does not commit the rules to the firewall yet however waits for the Palo Alto Networks Next Generation Firewall administrator to commit the rules to the necessary firewall appliances.

See “Editing a firewall template” on page 71.

See “Configuring Operations Director to commit firewall rules to Panorama” on page 22.

See “About tier tags” on page 48.

See “Deleting a firewall template” on page 75.

See “Creating a firewall template” on page 68.

See “Editing precedence order value of firewall template” on page 70.

See “Creating copy of a firewall template” on page 71.

### Deleting a firewall template

To delete a firewall template

1. Go to the Manage > Firewall Templates page.
2. Select the firewall template that you want to delete and click the X icon.

**Note:** Firewall templates that are active or have tags associated cannot be deleted.

See “About firewall templates” on page 67.

See “Editing a firewall template” on page 71.

See “Creating a firewall template” on page 68.
See “Editing precedence order value of firewall template” on page 70.

See “Creating copy of a firewall template” on page 71.
Monitoring Operations

This chapter includes the following topics:

- About Notifications page
- Viewing notifications and its details
- Approving a notification or provisioning request
- Denying a notification or provisioning request
- Process of approval and exception request
- Monitoring synchronization status
- Viewing security provisioning failure
- Retrying failed security provisioning

About Notifications page

The Monitor > Notifications page, displays notifications about:

- Applications that are provisioned in the vCenter.
- Approval request for acceptance of recommended security profile.
- Exception request raised by the server administrator.
- Provisioning requests that have been denied.

Notification status

The filter buttons displayed on the Notifications page are:

- All
  
  Displays a count of all notification.
- **Pending Approval**
  Displays the count of notifications that are pending approval after the server administrator has responded to the assessment questions from vCenter.

- **Applied**
  Displays the count of notifications where the security policies have been applied and the vApp/VM is secured.

- **In Progress**
  Displays the count of notifications in progress.

- **Failed**
  Displays the count of notifications that have failed.

- **Waiting**
  Displays the count of notifications in waiting state in the following two cases:
  - The server administrator has submitted the security assessment responses however not yet accepted the policy recommendations given by Operations Director.
  - On editing the security profile the security administrator has notified the server administrator however, the server administrator is yet to accept it.

Let us understand what each tab in the details drawer of the **Notifications** page means for the following scenarios:

- **When a new application is provisioned on day zero**
  - **Assessment** tab displays the security assessment questions and responses that have been submitted by the server administrator.
  - **Analysis** tab displays more granular details of the tags identified by Operations Director, the name of the recommended security profile, and the policies that are mapped to the security profile. You may click the security profile and the tag if you wish to view the details.
  - **Recommendations** tab displays the recommended security policies for the virtual machine/vApp. Only after you approve the notification, the recommended security policies get applied on the application. You may click on the security profile to view the details or make modifications such as adding/deleting custom policies. The grid in this tab displays the Operations Director-recommended security policies that are associated to the security profile.

---

**Note:** If you modify the recommended security profile, you must click **Notify the server administrator for approval** to send a notification about the modification to the server administrator.
Status tab displays the status of the security policies. For example, if the recommended security policy is pending approval, in progress, or applied. Certain notifications may have an exception request associated with it that is initiated by the server administrator from vCenter.

See “Viewing notifications and its details” on page 79.
See “Approving a notification or provisioning request” on page 79.

Viewing notifications and its details

To view a notification and the recommendation:
1. Go to the Monitor > Notifications page in Operations Director.
2. Click and select a notification to view the recommendations, analysis, and status in the respective tabs under the grid.

Status of any notification is Pending Approval until the security administrator approves it. The status changes to In Progress when the recommended security policies are getting applied after approval. The status changes to Applied when the security policies are applied and active.

See “About Notifications page” on page 77.
See “Approving a notification or provisioning request” on page 79.

Approving a notification or provisioning request

To approve a notification or provisioning request
1. Go to the Monitor > Notifications page in Operations Director.
2. Click the notification to select it.
3. Under the Recommendations tab, select the recommendation actions.
4. Select the check box and click Approve to approve it.

Note: Only notifications that are in Pending Approval state can be approved.

You can approve multiple notifications as well.

You cannot approve multiple notifications if:
- The notification has an open exception request.
- The selected notifications are in a state other than Pending Approval.
The selected notification’s profile is updated but it is not yet sent to the server administrator for approval.

The security profile contains all disabled or some deleted policies or firewall template. The security profile must have at least one enabled policy or firewall template.

See “About Notifications page” on page 77.

See “Viewing notifications and its details” on page 79.

Denying a notification or provisioning request

To deny a notification or provisioning request

1. Go to the Monitor > Notifications page. The notification for a new application is displayed in the grid.

   The security status will be Not Secured.

2. Select the notification and click Deny.

   Note: Only notifications in Waiting or Pending Approval state can be denied. Denying a notification will cancel the provisioning request and delete the associated security profile. You may select multiple notifications and deny them.

   A dialog box is displayed confirming the deny action.

3. Click Yes to deny.

   The State column shows the state as Denied.

   Notice under the Analysis tab, the link to the security profile is now disabled because the profile is deleted. The other details under this tab are retained.

   Under the Recommendations tab, the link to the security profile is now disabled because the profile is deleted.

   The Status tab displays the details about when the notification was denied and by whom.

   The Audit History tab records the notification denied action with the date and time details.

See “About Notifications page” on page 77.

See “Viewing notifications and its details” on page 79.
Process of approval and exception request

To understand how the communication between the server administrator and the security administrator happens with the course of actions, let us assume the following day zero scenario:

- The server administrator creates a new vApp for the first time.

Server administrator responds to the security assessment

1. In the vSphere Web Client, under vCenter > Inventory Lists > vApps > <vApp_name> > Summary tab, in the Symantec Data Center Security portlet, notice that the security status of the vApp is Not Secured.

2. Click Apply Security... to respond to the security assessment questionnaire. See “Responding to the security assessment” on page 33.

   Operations Director recommends security policies after you submit responses to the security assessment.

   At the same time, a notification is generated on the Monitor > Notifications page of Operations Director. This notification is in a Waiting state. This means it is waiting on the server administrator for the next action that is to accept or request an exception.

Server administrator accepts recommendations or requests exception

1. As a server administrator, you can view the recommended policies of the security profile for the vApp in the Manage > Security > Symantec Data Center Security - Review Recommended Policies portlet of vSphere Web client.

   In the Symantec Data Center Security portlet, click Accept to accept the security policies recommended by Operations Director or click Request Exception if you wish to change the recommendations by requesting an exception.

2. The state of the notification in Operations Director now changes to Pending Approval. This is means it is waiting on the security administrator to either approve the action of the server administrator or deny it.

Server administrator requests an exception in vSphere Web client

1. After reviewing the security policies associated with the recommended security profile for the vApp in the Manage > Security > Symantec Data Center Security - Review Recommended Policies portlet of vSphere Web client, you may choose to request an exception.

2. Click Request Exception.

   See “Requesting exception on recommended policies” on page 35.
Security administrator approves a notification in Operations Director

1. Go to the **Monitor > Notifications** page of Operations Director.
   
   The notification for a new application provisioned is displayed in the grid.

2. Click the notification to view the details. See “Viewing notifications and its details” on page 79.

3. Select the notification and click **Approve**. See “Approving a notification or provisioning request” on page 79.

Security administrator denies a notification in Operations Director

1. Go to the **Monitor > Notifications** page of Operations Director.
   
   The notification for a new application provisioned is displayed in the grid.

2. Click the notification to view the details.

3. Select the notification and click **Deny**. See “Denying a notification or provisioning request” on page 80.

Security administrator responds to the exception request from Operations Director

1. A notification gets generated and displayed on the **Monitor > Notifications** page after you request an exception for the security policies recommended by Operations Director.

2. You can select the notification to view the details. Only, if there is an exception, the **Exception** tab is displayed below the grid with the details.

   Following are the states of the exceptions requested:

   - **Open**
     Notification has an exception request associated.

   - **No**
     There is no exception request.

   - **Approved**
     The exception is approved by the security administrator.

   - **Denied**
     The exception is denied by the security administrator.

   The **Exception** tabs displays the following:

   - Name of the security profile.
     You may click on the name to view/edit the details of the profile.

---

**Note:** If you edit the security profile, you must manually navigate back to the **Monitor > Notifications** page when you save the changes.
See “Viewing the details of a profile” on page 60.

- **Exception Response** text box that lets you type a response to the server administrator.

- Exception request description that was sent by the server administrator from vCenter along with its date and time.

- **Profile updated to accommodate exception**
  Select this checkbox to acknowledge that the security profile is updated based on the exception that was requested.

- **Send Response**
  Click to send a response to vCenter.

- **Approve Exception**
  Click to approve the exception.

---

**Note:** Make sure to select the **Profile updated to accommodate exception** check box before you approve an exception. Approving an exception will update the security profile information that is displayed in vCenter.

---

- **Deny Exception**
  Click to deny the exception request in vCenter.

---

See “About Notifications page” on page 77.

See “Viewing notifications and its details” on page 79.

---

**Monitoring synchronization status**

To make sure that Operations Director is synchronized with the security policies of all the security products, NSX Server, and vCenter, you can monitor and update the synchronization status. Updating the synchronization status also lets you retrieve the latest security policies of the configured security products.

**To monitor the synchronization status**

1. Go to **Monitor > Synchronization Status** page.

2. Select the product that you want to synchronize. You can select multiple products as well.

3. Click **Synchronize** to initiate synchronization.

   A message is displayed to confirm the synchronization. Click **Synchronize**.
On successful synchronization, a success message is displayed and the synchronization status under the **Synchronization Status** column is updated to **Completed**. The **Last Synchronized** date and time also gets updated accordingly.

The grid lists the configured security products and the details such as the product name, security control, configuration status, synchronization status, and the last synchronization date and time.

The status can be either **Configured** or **Error**.

The synchronization status can be **Failed**, **In Progress**, or **Completed**.

If the status is **Error** or the synchronization status is **Failed**, a message is displayed above the grid. In the message, you can click **Settings** to navigate to the **Settings** page and fix the problem.

**Note:** If synchronization fails, verify the product configuration on the **Settings > Integration** page of UMC.

See "Retry failed security provisioning" on page 85.
See “About Notifications page” on page 77.
See “Viewing notifications and its details” on page 79.

### Viewing security provisioning failure

**To view provisioning failures**

1. Go to the **Monitor > Notifications** page.
   
   If a new application provisioning has failed, the filter buttons above the grid show a filter named **Failed** with the count of notifications.
   
   The state of the notification for a failed provisioning is shown as **Failed** in the grid.

2. Select the notification for failed provisioning.
   
   The details drawer displays the **Failure Causes** tab by default. The reasons for the failure are displayed under this tab. This tab is visible in the details drawer only in case of a failure.

See “Retry failed security provisioning” on page 85.
See “Monitoring synchronization status” on page 83.
See “About Notifications page” on page 77.
See “Viewing notifications and its details” on page 79.
Retry failed security provisioning

You can retry security provisioning if it has failed.

To retry security provisioning

1. Go to the Monitor > Notifications page and view the provisioning failure details.

2. The Status tab displays the policies that failed to apply. The status of the policies in the grid is Error. Click Reapply Policies to retry. Only policies that have failed to apply and that are in an Error state will be reapplied.

**Note:** Reapplying policies may fail if the security profile contains deleted policies. You must disable all deleted policies in that case and then try.

The status of the policies will change to In Progress while the policies are being reapplied.

See “Viewing security provisioning failure” on page 84.
See “Monitoring synchronization status” on page 83.
See “About Notifications page” on page 77.
See “Viewing notifications and its details” on page 79.
Troubleshooting

This appendix includes the following topics:

- Operations Director fails to register with UMC
- Viewing registration status of Operations Director with UMC
- Unable to connect to Operations Director server
- Manually registering and unregistering Symantec Data Center Security plug-in
- Command-line options to use the registerPlugin utility
- Committing firewall rules to Panorama fails
- Symantec Data Center Security plug-in installation fails with an error

Operations Director fails to register with UMC

If Operations Director fails to register with UMC during deployment, you must manually register Operations Director with UMC using the Operations Director registration tool.
To execute Operations Director registration with UMC manually

1. Connect to the Operations Director appliance using SSH.
2. Go to the location:
   
   \texttt{cd /usr/local/Symantec/so/}

3. Enter the command:
   
   \texttt{java -cp "./lib/odregistration-6.5.0.1252.jar:/lib/*" com.symantec.dcsc.common.odregistration.ODRegistration <umc_ipaddress> <umc_port> <umc_user> <umc_password> <od_ipaddress/od_hostname> <od_port>}

   \textbf{Example:}

   \texttt{java -cp "./lib/odregistration-6.5.0.1252.jar:/lib/*" com.symantec.dcsc.common.odregistration.ODRegistration xx.xxx.xxx.xx 8443 testumcadmin testpassword xx.xxx.xxx.xxx 8443}

\textbf{Note:} If \texttt{<umc_user>} is a domain user, the credentials must be either within double quotation " " with or without domain name or separated by a double backward slash.

For example:

"<domain name>\umcadmin"

or

"umcadmin"

or

\texttt{<domain name>\umcadmin}

The port number is 8443 for HTTPS communication.

If you are providing UMC host name/Operations Director host name while registration, make sure the DNS server is configured correctly to resolve the host name. If DNS server is not configured, provide UMC IP address/Operations Director IP address instead of the host name for Operations Director registration tool to work correctly.

Refer to log file at \texttt{/var/log/Symantec/DCSC/od/odregistration.log}. 
Viewing registration status of Operations Director with UMC

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

**Table A-1**  
Operations Director registration status

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

Unable to connect to Operations Director server

Connection with Operations Director server may not be established in cases if the server is unreachable for some reason or the trusted certificate is not installed.

Refer **Installing the UMC root certificate** in the installation wizard online help for more details to troubleshoot this problem.
Manually registering and unregistering Symantec Data Center Security plug-in

After logging in the vCenter Web client, if the Symantec Data Center Security plug-in short cut is not created, the registration of the Symantec Data Center Security plug-in has failed.

The registration of Symantec Data Center Security plug-in with vCenter may fail because of the following reasons:

- Operations Director server is not reachable.
- vCenter Web client cannot be download the plug-in from the Operations Director appliance.
- If Write access on the vCenter appliance folder is not granted because of which the downloaded plug-in zip file cannot be extracted.

You must manually register Symantec Data Center Security plug-in with vCenter. The registerPlugin utility provides options to register/unregister Symantec Data Center Security plug-in. This utility can be run from Operations Director appliance or it can be run remotely by using the command prompt. You must be an Operations Director administrator user (ODadmin) to run this utility.

Note: You must have write access to the folder on vCenter appliance so that downloaded zip file is extracted successfully.

To register the plug-in

Run the following command from the command prompt:

```
java -jar RegisterPlugin.jar --register
    --vcenterip <vCenter IP Address>
    --username <vCenter user name>
    --password <vCenter password>
    --odserverip <OD IP Address>
    --serverthumbprint <OD Server Certificate Thumbprint>
```

Example:

```
java -jar registerPlugin.jar --register --vcenterip xx.xxx.xxx.xxx
    --username testusername --password testpassword --odserverip
    xx.xxx.xxx.xxx --serverthumbprint
```
Note: It is mandatory to have the server thumbprint in the same format as shown in the example.

You can get the server thumbprint under the od.server.thumbprint property in the od.properties file located on the Operations Director appliance at:

/usr/local/Symantec/so/config/od.properties

To unregister the plug-in

Run the following command from the command prompt:

```
java -jar RegisterPlugin.jar --unregister
    --vcenterip <vCenter IP Address>
    --username <vCenter user name>
    --password <vCenter password>
```

Example:

```
java -jar registerPlugin.jar --unregister --vcenterip xx.xxx.xxx.xxx
    --username testusername --password testpassword
```

Delete the plug-in folder from the following location on vCenter appliance:

```
/var/lib/vmware/vsphere-client/vc-packages/vsphere-client-serenity/
```

Delete the od.properties file from the following location on vCenter appliance:

```
/storage/vsphere-client/Symantec/securityPlugin/od.properties
```

Restart vSphere Web Client service using the following URL:

```
https://<vCenter_IP_Address>:5480/
```

See “Command-line options to use the registerPlugin utility” on page 90.

Command-line options to use the registerPlugin utility

Table A-2 lists the commands that you can use to work with the registerPlugin utility.

**Table A-2** Command line options for registerPlugin utility

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>help</td>
<td>This command lists all the commands supported by this utility along with their usage.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>java -jar registerPlugin.jar --help</td>
</tr>
</tbody>
</table>
### Table A-2: Command line options for registerPlugin utility (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>check</strong></td>
<td>This command checks if vCenter plugin for Symantec Data Center Security is already registered with the vCenter.</td>
</tr>
<tr>
<td></td>
<td>java -jar registerPlugin.jar --check --vcenterip &lt;vCenter IP Address&gt; --username &lt;vCenter user name&gt; --password &lt;vCenter password&gt;</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>java -jar registerPlugin.jar --check --vcenterip xx.xxx.xxx.xxx --username testusername --password testpassword</td>
</tr>
<tr>
<td><strong>register</strong></td>
<td>This command registers the Symantec Data Center Security plug-in in vCenter.</td>
</tr>
<tr>
<td></td>
<td>java -jar RegisterPlugin.jar --register --vcenterip &lt;vCenter IP Address&gt; --username &lt;vCenter user name&gt; --password &lt;vCenter password&gt; --odserverip &lt;OD IP Address&gt; --serverthumbprint &lt;OD Server Certificate Thumbprint&gt;</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td><strong>unregister</strong></td>
<td>This command unregisters the Symantec Data Center Security plug-in from vCenter.</td>
</tr>
<tr>
<td></td>
<td>java -jar RegisterPlugin.jar --unregister --vcenterip &lt;vCenter IP Address&gt; --username &lt;vCenter user name&gt; --password &lt;vCenter password&gt;</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>java -jar registerPlugin.jar --unregister --vcenterip xx.xxx.xxx.xxx --username testusername --password testpassword</td>
</tr>
</tbody>
</table>
Committing firewall rules to Panorama fails

In a scenario where Operations Director is configured to commit firewall rules to Panorama, if you have an administrator role in Panorama with minimum rights, the commit operation fails.

Make sure that the administrator user specified in Panorama has Superuser role assigned.

See “Configuring Operations Director to commit firewall rules to Panorama” on page 22.

Symantec Data Center Security plug-in installation fails with an error

Symantec Data Center Security plug-in installation fails with an error **Error occurred while storing the certificate.** This may happen if you provide host name while configuring the vCenter server on the **Settings > Integration** page of UMC.

To resolve this issue, you must add the host name of vCenter appliance in the hosts file of the Operations Director appliance if the plug-in installation fails.

**To do this**

1. Edit the /etc/hosts file of the Operations Director appliance.
2. Append the host name of the vCenter server to the IP address and save the file.

This ensures that Operations Director recognizes the vCenter server to establish a connection and get the required information.

Retry configuring the vCenter server connection after making these changes.

See “Deploying Symantec Data Center Security plug-in for vCenter” on page 29.
Additional Resources

This appendix includes the following topics:

- Where to get more information

Where to get more information

Product manuals for DCS:SA are available on the DCS:SA product media. Updates to the documentation are available from the Symantec Technical Support and Business Critical Services (BCS) Web sites.

The DCS:SA product manuals are as follows:

- Installation Guide Online Help
- DCS:SA Online Help
- Planning and Deployment Guide
- Overview Guide
- Administrator's Guide
- Prevention Policy Reference Guide
- Detection Policy Reference Guide
- Agent Guide
- Implementation Guide Integration with VMware NSX (for Security Virtual Appliance)
- Operations Director Reference Guide
- vSphere Support Guide
- Release Notes
- Platform and Feature Matrix
The following table lists additional information that is available from the Symantec Web sites.

**Table B-1**  
Symantec Web sites

<table>
<thead>
<tr>
<th>Type of information</th>
<th>Web address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Knowledge Base</td>
<td><a href="http://www.symantec.com/business/support/">http://www.symantec.com/business/support/</a></td>
</tr>
<tr>
<td>Releases and updates</td>
<td></td>
</tr>
<tr>
<td>Manuals and other documentation</td>
<td></td>
</tr>
<tr>
<td>Contact options</td>
<td></td>
</tr>
<tr>
<td>Virus and other threat information</td>
<td><a href="http://securityresponse.symantec.com">http://securityresponse.symantec.com</a></td>
</tr>
<tr>
<td>and updates</td>
<td></td>
</tr>
</tbody>
</table>