



CHAPTER 11

Catalyst Switches and 7600 Devices

This chapter contains the following topics:

- [FAQs about Catalyst Switches and 7600 Devices, page 11-1](#)
- [Migrating from Security Manager 3.0.x to 3.2, page 11-2](#)
- [Discovering Failover Pairs, page 11-2](#)
- [Deployment Fails for Interface Settings, page 11-3](#)
- [Deployment Fails for Internal VLANs, page 11-3](#)
- [Performing Rollback on Catalyst Switches and 7600 Devices, page 11-3](#)



Note

For more detailed information on, see the “Managing Cisco Catalyst Switches and Cisco 7600 Series Routers” chapter in the [User Guide for Cisco Security Manager](#) for your release.

FAQs about Catalyst Switches and 7600 Devices

This section answers the following questions about Catalyst Switches and 7600 devices:

- [Q. Which VTP modes are supported by Security Manager?](#)
- [Q. How do I add a Catalyst 6503-E switch to Security Manager? The device does not appear in the list of supported devices in the New Device wizard.](#)
- [Q. What kinds of matching ACLs are supported by VLAN ACLs \(VACLs\) configured on Catalyst Switches and 7600 devices?](#)
- [Q. What are the limitations in support for IDSM settings in Security Manager?](#)
- [Q. Can I reference an undefined VLAN in Security Manager?](#)

Q. Which VTP modes are supported by Security Manager?

A. Before 3.2, Security Manager supported only VTP transparent mode for Catalyst switches and 7600 devices. Security Manager 3.2 can now also manage switches configured in the VTP client/server mode. CSM 3.2 manages switches configured in client/server mode by bypassing vlan database management on the device (including vlan creation, deletion, and monitoring vlans in the vlan database on switches).

Q. How do I add a Catalyst 6503-E switch to Security Manager? The device does not appear in the list of supported devices in the New Device wizard.

- A.** The Catalyst 6503-E switch shares the same System Object ID as the Catalyst 6503; therefore, only the 6503 appears in the list of devices. Both devices, however, are supported. The same holds true for the Catalyst 6506-E and the Catalyst 6509-E.
- Q.** What kinds of matching ACLs are supported by VLAN ACLs (VACLs) configured on Catalyst Switches and 7600 devices?
- A.** Security Manager supports the use of standard and extended ACLs as matching criteria for VACLs on Catalyst switches and 7600 devices. MAC-layer ACLs are not supported.
- Q.** What are the limitations in support for IDSM settings in Security Manager?
- A.** Security Manager supports a subset of IDSM settings on chassis running IOS 12.2(18)SXF4 or later. Trunk (IPS) and Capture (IDS) modes are supported; inline mode is not supported. Security Manager cannot manage IDSM data ports that are part of a spanning tree or access VLAN.
- Q.** Can I reference an undefined VLAN in Security Manager?
- A.** Yes, you can reference an undefined VLAN in VLAN group, VACL, and IDSM definitions. However, when you submit your changes, a warning message is displayed that recommends you either define the VLAN or delete it, as the configuration might interfere with device operation. Bear in mind that deleting a VLAN does not delete its references. Therefore, if you have defined a VACL that references an undefined VLAN, deleting the VLAN does not remove the reference in the VACL.

Migrating from Security Manager 3.0.x to 3.2

Security Manager 3.2 (as well as version 3.1.x) differs significantly from 3.0.x in its features for managing Catalyst switches and Cisco 7600 Series routers, as well as their associated firewall services modules (FWSMs) and security contexts:

- Security Manager 3.0.x used features from an embedded variant of CiscoView Device Manager, which is not included in Security Manager 3.2.
- Security Manager 3.2 offers a fully integrated management tool that is consistent with other Security Manager features.

This change to an integrated management tool affects the installation process when upgrading from Security Manager 3.0.x to Security Manager 3.2. For more information about how to migrate Catalyst switches and 7600 devices after the upgrade, please see “Migrating Inventory from an Earlier Security Manager Release” in the [User Guide for Cisco Security Manager](#) for your release.

Discovering Failover Pairs

Only one device of a failover pair should be managed by Security Manager. During discovery, use the wizard to set the discovery mode of the second device to Do Not Discover Module. Security Manager always manages the active admin context, regardless of whether you added the primary or secondary failover service module.

Deployment Fails for Interface Settings

Problem Deployment fails for interface settings on a Catalyst 6550/7600 device.

Solution Certain interface settings (such as speed, duplex, and MTU settings) are specific to particular card types and are not validated prior to deployment. Make sure to enter the correct values for your specific card type to ensure successful deployment.

Deployment Fails for Internal VLANs

Problem Deployment fails when Security Manager tries to create a VLAN with an ID that is within the range of the device's internal VLAN list.

Solution Security Manager cannot detect internal VLANs. Therefore, you must define a VLAN ID that falls outside of the device's internal VLAN list. Use the **show vlan internal usage** command to view the list of internal VLANs.

Performing Rollback on Catalyst Switches and 7600 Devices

The proper order for performing rollback on Catalyst Switches and 7600 devices is as follows:

- Security contexts.
- Service modules.
- Chassis.

We recommend performing rediscovery after the rollback operation is complete.

If you are rolling back an FWSM deployment and the system is configured to retrieve security certificates when adding devices, you might need to retrieve the certificate after the rollback operation is complete. This can be done using either of the following methods:

- Retrieving the certificate on a per-device basis from Device Properties.
- Configuring Security Manager to automatically retrieve certificates after rollback. To do this, select **Tools > Security Manager Administration > Device Communication**, then select the **Retrieve while adding devices** option under SSL Certificate Parameters.

