



CHAPTER 16

Managing Catalyst Devices

Cisco Security Manager supports the management and configuration of security services and other platform-specific services on Catalyst 6500 Series switches and Cisco 7600 Series routers (referred to in this User Guide as Catalyst 6500/7600 devices).

[Appendix M, “Catalyst Platform User Interface Reference,”](#) describes the Security Manager pages and dialog boxes that are specific to Catalyst 6500/7600 devices. The following topics describe how to configure platform-specific services and policies on this platform:

- [Migrating Inventory From an Earlier Security Manager Release, page 16-2](#)
- [Discovering Policies on 6500 Series and 7600 Series Devices, page 16-6](#)
- [Interfaces, page 16-8](#)
 - [Creating or Editing Ports on Catalyst 6500/7600 Devices, page 16-9](#)
 - [Deleting Ports on Catalyst 6500/7600 Devices, page 16-12](#)
- [VLANs, page 16-12](#)
 - [Creating or Editing VLANs, page 16-13](#)
 - [Deleting VLANs, page 16-15](#)
- [VLAN Groups, page 16-16](#)
 - [Creating or Editing VLAN Groups, page 16-16](#)
 - [Deleting VLAN Groups, page 16-18](#)

- [VLAN ACLs \(VACLs\), page 16-19](#)
 - [Creating or Editing VACLs, page 16-20](#)
 - [Deleting VACLs, page 16-23](#)
- [IDS/IPS Settings, page 16-24](#)
 - [Creating or Editing EtherChannel VLAN Definitions, page 16-25](#)
 - [Deleting EtherChannel VLAN Definitions, page 16-27](#)
 - [Creating or Editing Data Port VLAN Definitions, page 16-28](#)
 - [Deleting Data Port VLAN Definitions, page 16-30](#)
- [Viewing Configuration Summaries, page 16-31](#)

Migrating Inventory From an Earlier Security Manager Release

Security Manager 3.1.x differs significantly from 3.0.x in its features for managing Catalyst 6500 Series switches and Cisco 7600 Series routers, as well as their associated services modules (blades) 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 3.1.x.
- Security Manager 3.1.x 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 3.1.x. In most cases, information from the older Security Manager database is added to the new database as part of the process of upgrading to the newer Security Manager version. However, the new methods for managing Catalyst 6500/7600 devices are different enough from the old methods that you must do more than simply install the newer Security Manager version in order to manage these devices in your network.

Before You Begin

- We recommend that you perform an inventory discovery on the chassis and service modules immediately before performing migration. This discovery option discovers the interfaces, VLANs, and VLAN groups configured on the live devices. See [Discovering Policies on Devices Already in Security Manager, page 6-10](#).
- Use Common Services to back up the Security Manager 3.0.x database. See [Backup and Restore, page 20-25](#).



Note

Do **not** make any out-of-band changes on the chassis or any of the service modules (for example, using the CLI) from the time migration starts until the operation is complete, as described in this procedure.

Procedure

Step 1 Upgrade from the older Security Manager version to the newer version.

To understand the prerequisites, tasks, and options that apply to an upgrade, see the “Upgrading Server Applications” topic in Chapter 4 of *Installation Guide for Cisco Security Manager 3.1*.

Catalyst 6500 Series switches, Cisco 7600 Series routers, their services modules, and their security contexts are migrated automatically, along with all associated VPN policies and firewall policies. However, old inventory information from Security Manager 3.0.x is discarded—including, for example, the records of described interfaces and configured VLANs.



Note

When the installation utility reaches its “Important Instructions” page, it specifies a location on your server from which to access a migration report file. In most cases, the location will be `NMSROOT\MDC\log\readme.txt`, where `NMSROOT` is the path to the Security Manager installation directory. The default is `C:\Program Files\CSCOpX`.

Step 2 Open and print the migration report. It contains important information that you should read.

- Step 3** Install the newest Security Manager Client software version on a client system, then use that client system to log in to your upgraded Security Manager server.
- Step 4** To use [Device view](#) (*not Policy view*), click the **Device View** button on the main toolbar.

In the Device selector, a red X partially covers each icon that represents your 6500 Series and 7600 Series chassis, as well as the services modules (blades) and security contexts associated with those chassis. The red X serves as a visual cue to indicate that inventory information is not yet available for that device.

- Step 5** Click any red X icon in the Device selector, then click **Yes** in the popup message to confirm that Security Manager should discover the device. Security Manager contacts the live device and retrieves its inventory information.



Note The discovery operation performed during migration retrieves *only* inventory information; it does *not* discover the device configuration, such as firewall and VPN policies on the chassis and FWSM security contexts.

- Step 6** Submit your changes (or approve your activity when working in workflow mode). The red X is cleared from the icon. The chassis, services module, or security context is now available to you for deployments from Security Manager.



-
- Note**
- If there are any FWSM 2.x devices that continue to display the red X icon after you complete this procedure, do the following:
 - Click the red X icon for each FWSM system context, then repeat steps [5](#) and [6](#) until the icons are cleared.
 - After you clear the system contexts, click the red X icon for each security context, then repeat steps [5](#) and [6](#) until the icons are cleared.
 - You do not need to perform this procedure when you migrate FWSMs that were added individually to Security Manager without the chassis.
 - Certain types of service modules do not display the red X icon and are marked instead as unmanaged. See [Migrating Unmanaged Service Modules](#), page [16-5](#).
 - Do *not* deploy any chassis, services module, or security context that displays a red X icon. If you try, the deployment fails.

- Other device lists in the Security Manager interface (such as the lists for deployment and policy assignment) do not include *any* icons for these chassis, services modules, or security contexts.
-

Related Topics

- [Migrating Unmanaged Service Modules, page 16-5](#)
- [Managing Catalyst Devices, page 16-1](#)
- [Migrating Inventory From an Earlier Security Manager Release, page 16-2](#)

Migrating Unmanaged Service Modules

The first time that you launch the Security Manager client after upgrading from version 3.0.1 to 3.1, the 6500/7600 chassis and the firewall service modules (FWSMs) and security contexts associated with the chassis are displayed with a red X icon in the Device selector. As described in [Migrating Inventory From an Earlier Security Manager Release, page 16-2](#), you must click the icon in order to retrieve the inventory information for that device.

The following service modules, however, are not marked with the red X icon:

- FWSM 3.x service modules.
- Any FWSMs, such as standby failover blades, that were marked as unmanaged in Security Manager 3.0.1.
- Any FWSMs that were not discovered in Security Manager 3.0.1.

All of these FWSMs are displayed in the Device selector with a light blue icon, which indicates that they are unmanaged.

You have two options for each unmanaged FWSM:

- You can leave the FWSM unmanaged.
- You can delete the FWSM and then rediscover the chassis. The following procedure describes how this is done.

Procedure

-
- Step 1** Upgrade Security Manager, install and launch the new client, and perform discovery on at least one device marked with the red X icon, as described in [Migrating Inventory From an Earlier Security Manager Release, page 16-2](#). The discovery operation ignores any unmanaged FWSMs.
- Step 2** Delete the FWSMs marked with the light blue icon that you want to manage with Security Manager 3.1. Make sure that you perform this step *after* performing discovery, as described in [Step 1](#).
- Step 3** Right-click the chassis, then select **Discover Policies on Device**.
- Step 4** In the discovery wizard, enter the credentials for each FWSM that you deleted in [Step 2](#).
- After discovery is complete, you can manage the FWSMs in Security Manager.
-



Note

The discovery operation performed during migration retrieves *only* inventory information, not the device configuration.

Related Topics

- [Migrating Inventory From an Earlier Security Manager Release, page 16-2](#)
- [Discovering Policies on 6500 Series and 7600 Series Devices, page 16-6](#)
- [Managing Catalyst Devices, page 16-1](#)

Discovering Policies on 6500 Series and 7600 Series Devices

You can discover the configurations of your 6500 Series and 7600 Series chassis (as well as the configurations of the services modules and security contexts associated with those chassis) and import the configurations as policies into Security Manager. This makes it possible to add existing devices and manage

them with Security Manager without having to configure each device manually, policy by policy. For more information, see [Adding Devices to the Security Manager Inventory, page 5-30](#).

You can discover any command that Security Manager can configure. Discovery ignores unsupported commands, which means that they are left intact on the device even after subsequent deployments. Additionally, in cases where Security Manager can discover the command, but not all the subcommands and keywords related to that command, the unsupported elements are ignored and left intact on the device.

At any time, you can also *rediscover* the configurations of devices that you are already managing with Security Manager. Be aware, however, that we do not recommend rediscovery generally because performing rediscovery overwrites the policies that you have defined in Security Manager. For more information, see [Discovering Policies on Devices Already in Security Manager, page 6-10](#).

**Note**

We recommend that you perform deployment immediately after you discover the policies on a 6500 Series or 7600 Series chassis, *before* you make any changes to policies or unassign policies from the device. (This recommendation also applies to any services module or security context associated with a 6500 Series or 7600 Series chassis.) Otherwise, the changes that you configure in Security Manager might not be deployed to the device. See [Working with Deployment, page 18-36](#).

Related Topics

- [Understanding Policies, page 6-1](#)
- [Discovering Policies, page 6-7](#)
- [Managing Catalyst Devices, page 16-1](#)
- [Managing Routers, page 14-1](#)
- [Working with Deployment, page 18-36](#)

Interfaces

You use the Interfaces tab on the Interfaces/VLANs page to view and manage the following types of ports:

- Access ports—A switching port that is used to connect host machines or servers. An access port belongs to and carries the traffic of only one VLAN. Traffic is received and sent in native formats with no VLAN tagging.
- Trunk ports—A switching port operating at Layer 2 to carry the traffic of multiple VLANs. Traffic is tagged with a VLAN number to differentiate traffic from each VLAN. A trunk port is used to connect switches to switches or to connect switches to routers.
- Routed ports—A physical port that acts like a port on a router. A routed port is not associated with a particular VLAN, and it behaves like a regular router interface. You can configure a routed port with a Layer 3 routing protocol.
- Dynamic ports—A port that can change dynamically to a trunk port if the neighboring port is configured as a trunk port.
- Unsupported ports—Ports on the Catalyst device that are not supported by Security Manager.

To display the Interfaces tab, select a Catalyst device in [Device view](#), select **Interfaces/VLANs** from the Policy selector, then click the **Interfaces** tab in the work area.

The following topics describe the actions you can perform when defining interfaces on Catalyst devices:

- [Creating or Editing Ports on Catalyst 6500/7600 Devices, page 16-9](#)
- [Deleting Ports on Catalyst 6500/7600 Devices, page 16-12](#)

Related Topics

- [Interfaces/VLANs Page—Interfaces Tab, page M-14](#)
- [VLANs, page 16-12](#)
- [VLAN Groups, page 16-16](#)
- [VLAN ACLs \(VACLs\), page 16-19](#)
- [Managing Catalyst Devices, page 16-1](#)

Creating or Editing Ports on Catalyst 6500/7600 Devices

You can create access ports, routed ports, or trunk ports on Catalyst 6500/7600 devices, with these restrictions:

- Each interface must have a name.
- You can associate an access port with only one VLAN.
- You can associate a trunk port with one or more VLANs.

Procedure

Step 1 ([Device view](#)) Select a Catalyst device, select **Interfaces/VLANs** from the Policy selector, then click the **Interfaces** tab in the work area.

The Interfaces tab is displayed. For a description of the fields on this tab, see [Interfaces/VLANs Page—Interfaces Tab, page M-14](#).

Step 2 Do one of the following:

- To define the attributes of a new interface, click **Add Row**.
- To edit the attributes of an interface, select it in the list, then click **Edit Row**.

Step 3 (Optional) Deselect the **Enable Interface** check box if you want this interface to be in shutdown mode.

Step 4 From the Type list, select **Interface** or **Subinterface**:

- If you select Interface, proceed with Step 5.
- If you select Subinterface, proceed with Step 7.

Step 5 [Interfaces only] Enter a name for the interface, or click **Select** to display the utility for generating an automatic name for the interface. See [Generating an Interface Name for Catalyst Devices, page 16-11](#).

Step 6 [Interfaces only] Select an option from the **Mode** list to specify the port configuration type. The fields in the dialog box vary according to your selection. Proceed with Step 8.

Step 7 [Subinterfaces only] Select the parent interface of the subinterface, then enter the ID number.

Step 8 Define or configure the settings for the type that you selected:

- Access Port—See [Create and Edit Interface Dialog Boxes—Access Port Mode, page M-17](#) for a description of the fields.

- Routed Port—See [Create and Edit Interface Dialog Boxes—Routed Port Mode](#), page M-22 for a description of the fields.
- Trunk Port—See [Create and Edit Interface Dialog Boxes—Trunk Port Mode](#), page M-25 for a description of the fields.
- Dynamic Port—See [Create and Edit Interface Dialog Boxes—Dynamic Mode](#), page M-31 for a description of the fields.
- Subinterface—See [Create and Edit Interface Dialog Boxes—Subinterfaces](#), page M-37 for a description of the fields.
- Unsupported—See [Create and Edit Interface Dialog Boxes—Unsupported Mode](#), page M-39 for a description of the fields.

- Step 9** From the **Speed** list, select an option to define the speed of the interface.
- Step 10** If you defined a specific speed for the interface, and therefore the Duplex list is enabled, select a duplexing option.
- Step 11** In the MTU field, enter the maximum transmission unit value.
- Step 12** Configure whether to use flow control on inbound (Receive) and outbound (Send) traffic.
- Step 13** (Optional) Enter a description for the interface in the **Description** field.
- Step 14** Click **OK** to save your definitions locally on the client and close the dialog box.
- Step 15** Click **Save** to save your definitions to the Security Manager server.



Note To publish your changes, click the **Submit** button on the toolbar.

Related Topics

- [Deleting Ports on Catalyst 6500/7600 Devices](#), page 16-12
- [Creating or Editing VLANs](#), page 16-13
- [Creating or Editing VLAN Groups](#), page 16-16
- [Interfaces/VLANs Page—Interfaces Tab](#), page M-14
- [Interfaces](#), page 16-8

Generating an Interface Name for Catalyst Devices

To streamline the process of manually defining an interface on a Catalyst device, Security Manager includes a utility for generating a name for the interface. This name is based on the interface type and details about the interface's location, such as card, slot, and subinterface.

Procedure

- Step 1** Open the Create Interface dialog box for defining ports/interfaces on Catalyst devices. See [Creating or Editing Ports on Catalyst 6500/7600 Devices, page 16-9](#).
- Step 2** Select **Interface** from the Type list.
- Step 3** In the Name field, click **Select** to open the [Interface Auto Name Generator Dialog Box, page K-27](#).
- Step 4** Select the interface type from the Type list.
- Step 5** Enter information regarding the location of the interface in one or more of the following fields:
- Card
 - Slot
 - Port
- As you enter information, the interface name is generated and displayed in the Result field.
- Step 6** Click **OK** to save your definitions. The new interface name is displayed in the Name field in the Create Interface dialog box. You can modify this name manually.
-

Related Topics

- [Interfaces, page 16-8](#)
- [Deleting Ports on Catalyst 6500/7600 Devices, page 16-12](#)

Deleting Ports on Catalyst 6500/7600 Devices

Although you can delete the definition of an interface at any time, use this option with great care. If the relevant device includes the interface definition in any policy definitions, deleting the interface causes these policy definitions to fail when they are deployed to the device.

Procedure

- Step 1** Select **View > Device View** or click the **Device View** button on the toolbar.
- Step 2** Select a Catalyst 6500 Series switch or Cisco 7600 Series router from the Device selector.
- Step 3** Select **Interfaces/VLANs** from the Policy selector to display the [Interfaces/VLANs Page, page M-3](#).
- Step 4** Click the **Interfaces** tab in the work area.
The Interfaces tab is displayed. For a description of the fields on this tab, see [Interfaces/VLANs Page—Interfaces Tab, page M-14](#).
- Step 5** Select an interface from the table, then click **Delete Row**. The interface is deleted.
-

Related Topics

- [Creating or Editing Ports on Catalyst 6500/7600 Devices, page 16-9](#)
- [Interfaces/VLANs Page—Interfaces Tab, page M-14](#)
- [Interfaces, page 16-8](#)

VLANs

A VLAN is a switched network that is segmented logically instead of on the basis of geography. For example, a VLAN might interconnect members of a geographically dispersed workgroup. VLANs offer a practical convenience for many organizations because they reduce the need to rearrange the physical placement of personnel, equipment, and network infrastructure. Properly configured VLANs are scalable, secure, and can simplify the tasks of network management.

A VLAN consists of hosts and network devices (such as bridges and routers), connected by a single bridging domain. Traffic between VLANs must be routed.

Security Manager helps you to create VLANs and define VLAN settings for the defined interfaces on Catalyst 6500 Series switches and Cisco 7600 Series routers, their supported services modules, and their security contexts.

The following topics describe the actions you can perform when defining VLANs on Catalyst devices:

- [Creating or Editing VLANs, page 16-13](#)
- [Deleting VLANs, page 16-15](#)

Related Topics

- [Interfaces/VLANs Page—VLANs Tab, page M-4](#)
- [VLAN Groups, page 16-16](#)
- [VLAN ACLs \(VACLs\), page 16-19](#)
- [Managing Catalyst Devices, page 16-1](#)

Creating or Editing VLANs

You can create a VLAN or reconfigure the attributes of a VLAN.

Procedure

Step 1 ([Device view](#)) Select a Catalyst device, select **Interfaces/VLANs** from the Policy selector, then click the **VLANs** tab in the work area.

The VLANs tab is displayed. For a description of the fields on this tab, see [Interfaces/VLANs Page—VLANs Tab, page M-4](#).

Step 2 Do one of the following:

- To define the attributes of a new VLAN, click **Add Row**.
- To edit the attributes of a VLAN, select it in the list, then click **Edit Row**.

See [Create and Edit VLAN Dialog Boxes, page M-6](#), for a description of the fields in the dialog box.

Step 3 In the VLAN ID field, enter a unique ID number for the VLAN. The number that you enter must not be assigned to any other VLAN in the bridging group.

- Step 4** (Optional) Enter a name for the VLAN.
- Step 5** (Optional) If the VLAN is part of a VLAN group, select the group ID, or select **Add Group** to open the Create VLAN Group dialog box. For more information, see [Creating or Editing VLAN Groups, page 16-16](#).
- Step 6** From the Status list, specify the status of the VLAN (active or suspended).
- Step 7** From the Type list, select either **Layer 2** or **Layer 3**. If you select Layer 3, continue with Step 8. Otherwise, continue with Step 9.
- Step 8** (Optional) For a Layer 3 VLAN, define a switched virtual interface (SVI):
- To make the SVI active, select the **Enable Interface** check box. An SVI enables routing between VLANs and provides IP host connectivity to the switch. If you do not select this check box, the SVI is created in shutdown mode.
 - Enter the IP address for the SVI.
 - Enter the SVI subnet mask by typing it, or select a netmask value from the Subnet Mask list.
 - Enter an optional description, if required.
- Step 9** Do one or both of the following:
- To associate access ports with the VLAN, enter their names in the Access Ports text box or click **Select** to open an interface selector.
 - To associate trunk ports with the VLAN, enter their names in the Trunk Ports text box or click **Select** to open an interface selector.
- See [Interface Selector Dialog Box—VLAN ACL Content, page M-55](#), for a description of the fields in the dialog box. For more information about defining ports, see [Creating or Editing Ports on Catalyst 6500/7600 Devices, page 16-9](#).
- Step 10** Click **OK** to save your definitions locally on the client and close the dialog box.
- Step 11** Click **Save** to save your definitions to the Security Manager server.



Note To publish your changes, click the **Submit** button on the toolbar.

Related Topics

- [Deleting VLANs, page 16-15](#)

- [Creating or Editing VLAN Groups, page 16-16](#)
- [Creating or Editing VACLs, page 16-20](#)
- [Create and Edit VLAN Dialog Boxes, page M-6](#)
- [VLANs, page 16-12](#)

Deleting VLANs

You can delete a VLAN.

Procedure

- Step 1** Select **View > Device View** or click the **Device View** button on the toolbar.
- Step 2** Select a Catalyst 6500 Series switch or Cisco 7600 Series router from the Device selector.
- Step 3** Select **Interfaces/VLANs** from the Policies selector to display the [Interfaces/VLANs Page, page M-3](#).
- Step 4** Click the **VLANs** tab in the work area.
The VLANs tab is displayed. For a description of the fields on this tab, see [Interfaces/VLANs Page—VLANs Tab, page M-4](#).
- Step 5** Select a VLAN from the table, then click **Delete Row**.
The VLAN is deleted.
-

Related Topics

- [Creating or Editing VLANs, page 16-13](#)
- [Interfaces/VLANs Page—VLANs Tab, page M-4](#)
- [VLANs, page 16-12](#)

VLAN Groups

A VLAN group defines a logical collection of VLANs. The VLAN Groups tab on the Interfaces/VLANs page displays:

- All VLAN groups that are defined on the selected device.
- The service module slots to which a VLAN group is bound.
- Which VLANs belong to each VLAN group.

VLAN groups can be used when assigning VLANs to an FWSM security context. A VLAN group can be assigned to multiple FWSMs, and each FWSM can have multiple VLAN groups assigned to it. To perform this assignment, see [Add/Edit a Security Context for FWSM, page 15-108](#).

The following topics describe the actions you can perform when defining VLAN groups on Catalyst devices:

- [Creating or Editing VLAN Groups, page 16-16](#)
- [Deleting VLAN Groups, page 16-18](#)

Related Topics

- [Interfaces/VLANs Page—VLAN Groups Tab, page M-10](#)
- [Interfaces, page 16-8](#)
- [VLANs, page 16-12](#)
- [VLAN ACLs \(VACLs\), page 16-19](#)
- [Managing Catalyst Devices, page 16-1](#)

Creating or Editing VLAN Groups

You can create VLAN groups. When you create a VLAN group, remember that:

- Each group must have an ID.
- You can associate a VLAN group with one or more FWSM modules.
- Each VLAN can be a member of only one VLAN group.

Procedure

Step 1 ([Device view](#)) Select a Catalyst device, select **Interfaces/VLANs** from the Policy selector, then click the **VLAN Groups** tab in the work area.

The VLAN Groups tab is displayed. For a description of the fields on this tab, see [Interfaces/VLANs Page—VLAN Groups Tab, page M-10](#).

Step 2 Do one of the following:

- To define the attributes of a new VLAN group, click **Add Row**.
- To edit the attributes of a VLAN group, select it in the list, then click **Edit Row**.

See [Create and Edit VLAN Group Dialog Boxes, page M-11](#), for a description of the fields in this dialog box.

Step 3 In the VLAN Group ID field, enter a unique ID number for the VLAN group. The number that you enter must not be assigned to any other VLAN group.

Step 4 To associate the VLAN group with specific service module slots, enter their slot numbers in the Service Module Slots text box, or click **Select** to open a selector.



Note Defining this association makes it possible to later assign this VLAN group to a security context on the FWSM. See [Add/Edit a Security Context for FWSM, page 15-108](#).

Step 5 Enter the VLANs to add to the VLAN group, or click **Select** to open a selector.

Step 6 Click **OK** to save your definitions locally on the client and close the dialog box.

Step 7 Click **Save** to save your definitions to the Security Manager server.



Note To publish your changes, click the **Submit** button on the toolbar.

Related Topics

- [Deleting VLAN Groups, page 16-18](#)
- [Creating or Editing VLANs, page 16-13](#)

- [Creating or Editing VACLs, page 16-20](#)
- [Interfaces/VLANs Page—VLAN Groups Tab, page M-10](#)
- [VLAN Groups, page 16-16](#)

Deleting VLAN Groups

You can delete VLAN groups. Deleting a VLAN group has no effect on the VLANs in the group.

Procedure

- Step 1** Select **View > Device View** or click the **Device View** button on the toolbar.
 - Step 2** Select a Catalyst 6500 Series switch or Cisco 7600 Series router from the Device selector.
 - Step 3** Select **Interfaces/VLANs** from the Policy selector to display the [Interfaces/VLANs Page, page M-3](#).
 - Step 4** Click the **VLAN Groups** tab in the work area.
The VLANs tab is displayed. For a description of the fields on this tab, see [Interfaces/VLANs Page—VLAN Groups Tab, page M-10](#).
 - Step 5** Select a VLAN group from the table, then click **Delete Row**. The VLAN group is deleted.
-

Related Topics

- [Creating or Editing VLAN Groups, page 16-16](#)
- [Interfaces/VLANs Page—VLAN Groups Tab, page M-10](#)
- [VLAN Groups, page 16-16](#)

VLAN ACLs (VACLs)

Cisco IOS standard or extended ACLs are configured on router interfaces only, and are applied on routed packets only. In contrast, Catalyst 6500 Series switches and Cisco 7600 Series routers can use VLAN ACLs (VACLs) to control the access of all packets that are bridged within a VLAN or that are routed to or from a VLAN for VACL capture through a WAN interface. VACLs:

- Are processed in hardware.
- Use Cisco IOS ACLs.
- Ignore any Cisco IOS ACL fields that are not supported in hardware.

**Note**

Security Manager does not support the creation or configuration of MAC ACLs (MACLS), which are named ACLs that are sometimes used with VACLs to filter IPX, DECnet, AppleTalk, VINES, or XNS traffic based on MAC addresses.

When you configure a VACL and apply it to a VLAN, all packets entering the VLAN are checked against the VACL.

If you apply a VACL to a VLAN and you apply an ACL to a routed interface in that same VLAN, any packet coming into the VLAN is first checked against the VACL. Then, if permitted, the packet is checked against the input ACL before it reaches the routed interface.

When a packet is routed from one VLAN to another, it is first checked against the output ACL that is applied to the routed interface. Then, if permitted, the packet is checked against any VACLs that are configured for the destination VLAN.

If a VACL is configured for a packet type, and a packet of that type does not match the VACL, the default action is deny.

VLAN Access Maps

Security Manager uses *VLAN access maps* to configure VACLs. Conceptually similar to a route map, a VLAN access map is a container in which you place one or more *statements* (conditions that match an action) and number them by their order of importance. A VLAN access map must also identify the VLANs to which it is applied, contain the map name, and identify at least one VACL sequence.

A VACL sequence must have a sequence number and at least one action, and must match at least one ACL.

Devices evaluate map statements in sequence and you can associate more than one VLAN access map with any device chassis.

To manage a VACL, select a Catalyst device in Device View, then select **Platform > VLAN Access Lists**. You use VLAN access maps to configure VACLs for IP traffic.

The following topics describe the actions you can perform when defining VACLs on Catalyst devices:

- [Creating or Editing VACLs, page 16-20](#)
- [Deleting VACLs, page 16-23](#)

Related Topics

- [VLAN Access Lists Page, page M-50](#)
- [Create and Edit VLAN ACL Dialog Boxes, page M-52](#)
- [Create and Edit VLAN ACL Content Dialog Boxes, page M-54](#)
- [VLANs, page 16-12](#)
- [VLAN Groups, page 16-16](#)
- [Managing Catalyst Devices, page 16-1](#)

Creating or Editing VACLs

When you can create or edit a VACL, you must:

- Name the VACL.
- Define the VLANs to which the VACL applies.
- Define a sequence map containing at least one VACL sequence.

Procedure

- Step 1** Do one of the following:
- ([Device view](#)) Select a Catalyst device, then select **Platform > VLAN Access Lists** from the Policy selector.
 - ([Policy view](#)) Select **Catalyst Platform > VLAN Access Lists**.

The VLAN Access Lists page is displayed. For a description of the fields on this page, see [VLAN Access Lists Page, page M-50](#).

Step 2 Do one of the following:

- To define the attributes of a new VACL, click **Add Row**.
- To edit the attributes of a VACL, select it in the list, then click **Edit Row**.

A dialog box opens. See [Create and Edit VLAN ACL Dialog Boxes, page M-52](#), for a description of the fields in the dialog box.

Step 3 Enter a name for the VACL in the **VLAN ACL Name** field.

Step 4 In the VLANs field, specify the VLANs to which the VACL should be applied, or click **Select** to open a VLAN selector.

Step 5 Define the sequence map:

- a. Click **Add Row** or **Edit Row** beneath the Sequence Map table. A dialog box opens. See [Create and Edit VLAN ACL Content Dialog Boxes, page M-54](#).
- b. Enter a number to identify the sequence.
- c. Specify the standard and extended ACLs to assign to the sequence, or click **Select** to display a selector (see [Object Selectors, page F-559](#)). For more information about ACL objects, see [Understanding Access Control List Objects, page 8-31](#).
- d. Specify the action to perform on traffic that matches the ACLs defined in this sequence. (When you select **Redirect** as the action, you must specify the physical destination interfaces, or click **Select** to display a selector. See [Specifying Interfaces During Policy Definition, page 8-117](#).)
- e. Click **OK** to save your definitions locally on the client and close the dialog box. The sequence is displayed in the Sequence Map table.
- f. Repeat steps a through e to add sequences to the sequence map.
- g. Use the up and down arrows to reorder the sequences, if required.



Note The order in which you place the sequences is significant. When a flow matches a permit ACL entry, the associated action is taken without checking the remaining sequences. When a flow matches a deny ACL entry, it is checked against the next ACL in the same sequence or the next sequence. If a flow does not match any ACL entry and at least one ACL is configured for that packet type, the packet is denied.

Step 6 Click **Save** to save your definitions to the Security Manager server.



Note To publish your changes, click the **Submit** button on the toolbar.

Related Topics

- [Deleting VACLs, page 16-23](#)
- [Creating or Editing VLANs, page 16-13](#)
- [Creating or Editing VLAN Groups, page 16-16](#)
- [Create and Edit VLAN ACL Dialog Boxes, page M-52](#)
- [VLAN Access Lists Page, page M-50](#)

Deleting VACLs

You can delete a VACL if it is not being used by any device, policy, or object.

Before You Begin

You must delete all references to the VACL before you can remove it from the database. To locate all references to the VACL, run an object usage report for it. See [Generating Object Usage Reports, page 8-14](#).

Procedure

-
- Step 1** Do one of the following:
- ([Device view](#)) Select a Catalyst device, then select **Platform > VLAN Access Lists** from the Policy selector.
 - ([Policy view](#)) Select **Catalyst Platform > VLAN Access Lists**.
- The VLAN Access Lists page is displayed. For a description of the fields on this page, see [VLAN Access Lists Page, page M-50](#).
- Step 2** Click in a row to select a VACL, then click **Delete**.
- Step 3** Click **OK** to save your definitions locally on the client and close the dialog box.
- Step 4** Click **Save** to save your definitions to the Security Manager server.



Note To publish your changes, click the **Submit** button on the toolbar.

Related Topics

- [Creating or Editing VACLs, page 16-20](#)
- [Interfaces/VLANs Page—VLANs Tab, page M-4](#)
- [VLAN ACLs \(VACLs\), page 16-19](#)

IDSM Settings

When you select a Catalyst device in [Device view](#), then select **Platform > IDSM Settings** from the Policy selector, a list is displayed that:

- Displays the settings for data ports on Intrusion Detection System Service Modules (IDSMs).
- Helps you to organize IDSM data ports in channel groups.

The IDSM card detects and stops security threats on network connections. The card inspects the traffic that enters its two data ports and drops packets if a security threat is detected. The data port settings define:

- Which traffic is received by the data ports, as defined by the VLAN IDs.
- The sensing mode used by the data ports:
 - Trunk (IPS)—The IDSM performs VLAN bridging between pairs of VLANs within the same data port, operating as an 802.1q trunk. The IDSM inspects the traffic it receives on each VLAN in a VLAN pair and can either forward the packets on the other VLAN in the pair or drop the packet if an intrusion attempt is detected.
 - Capture (IDS)—The IDSM passively monitors network traffic that was copied to the data ports by the Catalyst switch using either VACL capture or SPAN. The data ports operate as 802.1q trunks that can be configured to trunk different VLANs. When operating in this passive mode, the IDSM cannot drop packets in response to a network intrusion attempt, but it can send TCP resets over the data ports in an attempt to block the intrusion.

For high-traffic networks, EtherChannel is used to perform load balancing among multiple data ports. These data ports might be located on different IDSM cards within the same Catalyst device.

EtherChannel is also used to redirect traffic in the event of port failure to the remaining ports within the channel group. This resiliency help preserve intrusion detection and prevention without user intervention and with minimum packet loss.

The following topics describe the actions you can perform when defining IDSM settings:

- [Creating or Editing EtherChannel VLAN Definitions, page 16-25](#)
- [Deleting EtherChannel VLAN Definitions, page 16-27](#)

- [Creating or Editing Data Port VLAN Definitions](#), page 16-28
- [Deleting Data Port VLAN Definitions](#), page 16-30

Related Topics

- [VLANs](#), page 16-12
- [Managing Catalyst Devices](#), page 16-1

Creating or Editing EtherChannel VLAN Definitions

When defining an EtherChannel VLAN definition, you must:

- Define the slot-port combination containing the data ports to include in the channel group.
- Select the sensing mode used by the data ports.
- Define which VLANs are forwarded to the data ports.

The following restrictions apply:

- You may have a single definition only for each channel group.
- You may have a single definition only for each slot-data port combination. This means that you cannot create an EtherChannel VLAN definition if a data port definition already exists for this slot-data port.

Procedure

Step 1 Do one of the following:

- ([Device view](#)) Select a Catalyst device, then select **Platform > IDSM Settings** from the Policy selector.
- ([Policy view](#)) Select **Catalyst Platform > IDSM Settings**.

The IDSM Settings page is displayed. For a description of the fields on this page, see [Table M-17 on page M-44](#).

- Step 2** Do one of the following:
- To create an IDSM EtherChannel VLAN definition, click **Add Row** beneath the EtherChannel VLANs table.
 - To edit an IDSM EtherChannel VLAN definition, select it in the list, then click **Edit Row** beneath the table.

The IDSM EtherChannel VLAN dialog box is displayed. For a description of the fields in this dialog box, see [Table M-18 on page M-46](#).

- Step 3** To assign a channel group number to the Ethernet interface for the VLAN, or to change the channel group number, enter a number in the **Channel Group** text box.

- Step 4** To associate the VLAN with the numbered chassis slot where you installed your IDSM services module and to associate one module data port with the VLAN, do one of the following:
- Enter the slot-port number in the **Slot-Ports** text box.
 - Click **Select** to open the IDSM Slot-Port Selector dialog box.



Note Associating one module data port with the VLAN enables you to configure the port at the group level instead of configuring it manually.

- Step 5** From the Mode list, select the running mode of the EtherChannel VLAN. If you select Capture, select the check box to configure the specified channel group as a capture destination.



Note If you do not select this check box, the capture port is created in shutdown mode.

- Step 6** To include a VLAN in the specified channel group, do one of the following:
- Enter its numeric ID in the VLAN IDs text box.
 - Click **Select** to open the VLAN Selector dialog box.

You can enter or select more than one VLAN ID.

- Step 7** Click **OK** to save your definitions locally on the client and close the dialog box.

- Step 8** Click **Save** to save your definitions to the Security Manager server.



Note To publish your changes, click the **Submit** button on the toolbar.

Related Topics

- [Deleting EtherChannel VLAN Definitions, page 16-27](#)
- [Creating or Editing Data Port VLAN Definitions, page 16-28](#)
- [IDSM Settings, page 16-24](#)

Deleting EtherChannel VLAN Definitions

You can delete an EtherChannel VLAN definition on the IDSM.

Procedure

- Step 1** Do one of the following:
- ([Device view](#)) Select a Catalyst device, then select **Platform > IDSM Settings** from the Policy selector.
 - ([Policy view](#)) Select **Catalyst Platform > IDSM Settings**.
The IDSM Settings page is displayed. For a description of the fields on this page, see [IDSM Settings Page, page M-44](#).
- Step 2** Click a row in the table to select the VLAN definition to delete.
- Step 3** Click **Delete Row**.
- Step 4** Click **Save** to save your definitions to the Security Manager server.



Note To publish your changes, click the **Submit** button on the toolbar.

Related Topics

- [Creating or Editing EtherChannel VLAN Definitions, page 16-25](#)

- [Deleting Data Port VLAN Definitions, page 16-30](#)
- [IDSM Settings, page 16-24](#)

Creating or Editing Data Port VLAN Definitions

When defining a data port VLAN definition, you must:

- Define the slot-port combination where the data port is located.
- Select the sensing mode used by the data port.
- Define which VLANs are forwarded to the data port.

The following restrictions apply:

- You may have a single definition only for each data port.
- You cannot create a data port definition if the port is already defined as part of a channel group.

Procedure

-
- Step 1** Do one of the following:
- ([Device view](#)) Select a Catalyst device, then select **Platform > IDSM Settings** from the Policy selector.
 - ([Policy view](#)) Select **Catalyst Platform > IDSM Settings**.
- The IDSM Settings page is displayed. For a description of the fields on this page, see [Table M-17 on page M-44](#).
- Step 2** Do one of the following:
- To create an IDSM data port VLAN definition, click **Add Row** beneath the Data Port VLANs table.
 - To edit an IDSM data port VLAN definition, select it in the list, then click **Edit Row** beneath the table.
- The IDSM Data Port VLAN dialog box is displayed. For a description of the fields in this dialog box, see [Table M-19 on page M-47](#).
- Step 3** To associate the VLAN with the numbered chassis slot where you installed your IDSM services module and to associate one module data port with the VLAN, do one of the following:

- Enter the slot-port number in the **Slot-Ports** text box.
- Click **Select** to open the IDSMS Slot-Port Selector dialog box.



Note Associating one module data port with the VLAN enables you to configure the port at the group level instead of configuring it manually.

Step 4 From the Mode list, select the running mode of the data port VLAN. If you select Capture, select the check box to configure the specified data port as a capture destination.



Note If you do not select this check box, the capture port is created in shutdown mode.

Step 5 To assign a VLAN to the specified data port, do one of the following:

- Enter its numeric ID in the VLAN IDs text box.
- Click **Select** to open the VLAN Selector dialog box.

You can enter or select more than one VLAN ID.

Step 6 Click **OK** to save your definitions locally on the client and close the dialog box.

Step 7 Click **Save** to save your definitions to the Security Manager server.



Note To publish your changes, click the **Submit** button on the toolbar.

Related Topics

- [Deleting Data Port VLAN Definitions, page 16-30](#)
- [Creating or Editing EtherChannel VLAN Definitions, page 16-25](#)
- [IDSMS Settings, page 16-24](#)

Deleting Data Port VLAN Definitions

You can delete a data port VLAN definition on the IDSM.

Procedure

- Step 1** Do one of the following:
- ([Device view](#)) Select a Catalyst device, then select **Platform > IDSM Settings** from the Policy selector.
 - ([Policy view](#)) Select **Catalyst Platform > IDSM Settings**.
- The IDSM Settings page is displayed. For a description of the fields on this page, see [IDSM Settings Page, page M-44](#).
- Step 2** Click a row in the table to select the VLAN definition to delete.
- Step 3** Click **Delete Row**.
- Step 4** Click **Save** to save your definitions to the Security Manager server.



Note To publish your changes, click the **Submit** button on the toolbar.

Related Topics

- [Creating or Editing Data Port VLAN Definitions, page 16-28](#)
- [Deleting EtherChannel VLAN Definitions, page 16-27](#)
- [IDSM Settings, page 16-24](#)

Viewing Configuration Summaries

You can view a summary of the configurations saved to your Catalyst 6500 Series switches and Cisco 7600 Series routers.

Procedure

- Step 1** ([Device view](#)) Select a Catalyst device, then select **Interfaces/VLANs** from the Policy selector.
- Step 2** Click the **Summary** tab in the work area. The Summary tab is displayed. For a description of the fields on this tab, see [Interfaces/VLANs Page—Summary Tab, page M-42](#).
-

Related Topics

- [Managing Catalyst Devices, page 16-1](#)
- [Interfaces/VLANs Page—Summary Tab, page M-42](#)
- [Interfaces/VLANs Page, page M-3](#)

