Managing Cisco Catalyst Switches and Cisco 7600 Series Routers

Cisco Security Manager supports the management and configuration of security services and other platform-specific services on Cisco Catalyst switches and Cisco 7600 Series routers.

You can manage Catalyst switches and 7600 devices configured in VTP transparent or VTP client/server mode. Security Manager 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).

This chapter contains the following topics:

Discovering Policies on Cisco Catalyst Switches and Cisco 7600 Series Routers

You can discover the configurations of your Cisco Catalyst switches and Cisco 7600 Series Routers (as well as the configurations of the services modules and security contexts associated with them) 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 Device Inventory, page 3-7.

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 5-15.

Note We recommend that you perform deployment immediately after you discover policies, *before* you make any changes to policies or unassign policies from the device. (This recommendation also applies to any services module or security context hosted by the device.) Otherwise, the changes that you configure in Security Manager might not be deployed to the device. See Working with Deployment and the Configuration Archive, page 8-25.

Related Topics

- Understanding Policies, page 5-1
- Discovering Policies, page 5-12
- Chapter 67, “Managing Cisco Catalyst Switches and Cisco 7600 Series Routers”
- Working with Deployment and the Configuration Archive, page 8-25

Viewing Catalyst Summary Information

Use the Catalyst Summary Info page to view high-level system information, including any service modules, ports, and VLANs that Security Manager has discovered.

To view Catalyst summary information, in Device view, right-click a Catalyst switch or Cisco 7600 Series router, then select **Catalyst Summary Info**, or select **Tools > Catalyst Summary Info**.

Note If Security Manager has not completed discovery for a particular Cisco Catalyst switch or Cisco 7600 Series router, the Catalyst Summary Info page for that device displays this message: “No information is available. This information is acquired during device discovery.”

Related Topics

- IDSM Settings Page, page 67-47
- VLAN Access Lists Page, page 67-39
- Filtering Tables, page 1-48

Field Reference

Table 67-1 Catalyst Summary Info Page

Element	Description
Hostname	Displays the configured hostname of the device.
Device Type	Displays the device type.
Serial Number	Displays the serial number of the device.
OS Version	Displays the Cisco IOS image version the device is running.
Image	Displays the name of the image running on the device.

Table 67-1 Catalyst Summary Info Page (Continued)

Element	Description
Last Update	Displays a time stamp for the most recent discovery.
Total Ports	Displays the total number of configured ports, combining access ports, routed ports, and trunk ports.
Access Ports	Displays the number of configured access ports on the chassis.
Trunk Ports	Displays the number of configured trunk ports on the chassis.
Routed Ports	Displays the number of configured routed ports on the chassis.
Total VLANs	Displays the total number of configured VLANs on the chassis and all its services modules.
Layer 2 VLANs	Displays the number of VLANs that run on Layer 2.
Layer 3 VLANs	Displays the number of VLANs that run on Layer 3.
Service Module Table	
Slot	Identifies the slot to which a service module is attached.
Device Type	Displays a brief description of the service module.
Serial Number	Displays the serial number of the service module.
Model	Displays the model type of the service module.
OS Version	Identifies the OS version that is installed and running on the service module.
Assigned VLANs	Displays the total number of VLANs to which an FWSM is assigned. **Tip** Click the Summary tab of the Interfaces/VLANs policy to learn which VLANs are assigned to an IDSM or a VPNSM.
Contexts	Displays the total number of configured security contexts for an FWSM that runs in multicontext mode. **Tip** Click the Summary tab of the Interfaces/VLANs policy to learn how many virtual sensors are configured for an IDSM.

Viewing a Summary of Catalyst Interfaces, VLANs, and VLAN Groups

Use the Summary tab of the Interfaces/VLAN policy to view attributes of all VLANs, VLAN groups, interfaces, and subinterfaces configured on supported Catalyst 6500 Series and 7600 Series chassis and their associated services modules.

To view summary interface information, in Device view, select **Interfaces/VLANs** from the Policy selector, then click the **Summary** tab.

Note The Summary tab is available only for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers.

Related Topics

- Interfaces/VLANs Page—VLANs Tab, page 67-27

- Interfaces/VLANs Page—VLAN Groups Tab, page 67-33
- Interfaces/VLANs Page—Interfaces Tab, page 67-7
- Viewing Catalyst Summary Information, page 67-2
- Filtering Tables, page 1-48

Field Reference

Table 67-2 Interfaces/VLANs Page—Summary Tab

Element	Description
VLAN ID	The VLAN ID associated with an interface or subinterface. The VLAN ID specifies where 802.1Q tagged packets are sent and received on the specified an interface or subinterface; without a VLAN ID, the interface or subinterface cannot send or receive traffic. **Note** All VLAN IDs must be unique among all subinterfaces configured on the same physical interface.
VLAN Name	Name of the VLAN that corresponds to an interface or subinterface. For example, VLAN003 or Trunk1.
VLAN Group	Numeric identity of a VLAN group that is configured on the VLAN that a table row describes.
VLAN Type	Specifies whether a VLAN has access to Layer 2 or Layer 3.
IP Address/Mask	The IP address and corresponding subnet mask of the VLAN configured on an interface or subinterface.
Access Port	Displays the assigned name, if a name is assigned, of the access port that a VLAN uses.
Trunk Port	Specifies which VLANs are permitted to carry traffic over the trunk.
Slot (-Port)	Associates the chassis slot number (in which the relevant services module is installed) with the port number, as a hyphenated pair in the format *x* -*y*, for example 3-1.
Blade Type	Identifies the kind of services module on which a particular VLAN is configured, such as FWSM or VPNSM.
Security Context	Identifies the security context associated with an interface, but only if Multiple Mode is active on the installed module and an Admin context is configured for the module.
Security Context Interface	Displays the physical interface and subinterface IDs for which a security context inspects traffic. The displayed ID can represent a physical interface, a single sub-interface (defined as a range of one), or a range of sub-interfaces.
Security Level	Displays the security level of an interface, where values range from 0 (the lowest security) to 100 (the highest): • For an outside interface, the default is 0. • For an inside interface, the default is 100. • For an interface in the DMZ, the default is typically from 1 to 99.

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 Cisco Catalyst Switches and Cisco 7600 Series Routers, page 67-5
- Deleting Ports on Cisco Catalyst Switches and Cisco 7600 Series Routers, page 67-7
- Interfaces/VLANs Page—Interfaces Tab, page 67-7

Related Topics

- VLANs, page 67-25
- VLAN Groups, page 67-31
- VLAN ACLs (VACLs), page 67-36
- Chapter 67, “Managing Cisco Catalyst Switches and Cisco 7600 Series Routers”

Creating or Editing Ports on Cisco Catalyst Switches and Cisco 7600 Series Routers

You can create access ports, routed ports, or trunk ports on Cisco Catalyst Switches and Cisco 7600 Series Routers, 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.

Related Topics

- Deleting Ports on Cisco Catalyst Switches and Cisco 7600 Series Routers, page 67-7
- Creating or Editing VLANs, page 67-26
- Creating or Editing VLAN Groups, page 67-32

- Interfaces/VLANs Page—Interfaces Tab, page 67-7
- Interfaces, page 67-5

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 67-7.

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**:

Step 5 (Interfaces only) Enter a name for the interface. You can click **Select** to open a dialog box that will help you generate a standard name based on interface type and details about the interface's location, such as card, slot, and subinterface. For more information on using the dialog box to generate an interface name, see Interface Auto Name Generator Dialog Box, page 61-12.

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.

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 67-9 for a description of the fields.
- Routed Port—See Create and Edit Interface Dialog Boxes—Routed Port Mode, page 67-12 for a description of the fields.
- Trunk Port—See Create and Edit Interface Dialog Boxes—Trunk Port Mode, page 67-14 for a description of the fields.
- Dynamic Port—See Create and Edit Interface Dialog Boxes—Dynamic Mode, page 67-18 for a description of the fields.
- Subinterface—See Create and Edit Interface Dialog Boxes—Subinterfaces, page 67-22 for a description of the fields.
- Unsupported—See Create and Edit Interface Dialog Boxes—Unsupported Mode, page 67-24 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.

Deleting Ports on Cisco Catalyst Switches and Cisco 7600 Series Routers

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.

Related Topics

- Creating or Editing Ports on Cisco Catalyst Switches and Cisco 7600 Series Routers, page 67-5
- Interfaces, page 67-5

Step 1 (Device view) Select a Cisco Catalyst switch or Cisco 7600 Series router from the Device selector.

Step 2 Select **Interfaces/VLANs** from the Policy selector.

Step 3 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 67-7.

Step 4 Select an interface from the table, then click **Delete Row**. The interface is deleted.

Interfaces/VLANs Page—Interfaces Tab

Use the Interfaces tab to view and configure interfaces and subinterfaces on supported Cisco Catalyst switches and Cisco 7600 Series routers and their associated services modules (blades).

Navigation Path

(Device view) Select **Interfaces/VLANs** from the Device selector, then click the **Interfaces** tab.

Related Topics

- Interfaces/VLANs Page—VLANs Tab, page 67-27
- Interfaces/VLANs Page—VLAN Groups Tab, page 67-33
- Viewing a Summary of Catalyst Interfaces, VLANs, and VLAN Groups, page 67-3
- Filtering Tables, page 1-48

Field Reference

Table 67-3 Interfaces/VLANs Page—Interfaces Tab

Element	Description
Name	Interface type, chassis slot, and the number of the interface card. For example, *FastEthernet 2/7* means Fast Ethernet, slot 2, interface 7.

Table 67-3 Interfaces/VLANs Page—Interfaces Tab (Continued)

Element	Description
Mode	Configuration mode for physical ports: • Access • Routed • Trunk • Dynamic Auto • Dynamic Desirable • Unsupported
VLAN ID	The VLAN ID associated with the described subinterface, displayed only for Ethernet interfaces and VLAN interfaces.
IP Address	The IP address of the interface.
Enabled	Indicates whether the interface is enabled or disabled (shutdown state).
Interface Roles	The interface roles whose naming patterns match this interface. See Understanding Interface Role Objects, page 6-72.
Description	An optional description of the interface.
Add Row button	Opens the Create Interface dialog box, where you can define a new interface. For more information, see the instructions for the relevant mode: • Access Port Mode—Create and Edit Interface Dialog Boxes—Access Port Mode, page 67-9. • Routed Port Mode—Create and Edit Interface Dialog Boxes—Routed Port Mode, page 67-12 • Trunk Port Mode—Create and Edit Interface Dialog Boxes—Trunk Port Mode, page 67-14 • Dynamic Mode—Create and Edit Interface Dialog Boxes—Dynamic Mode, page 67-18
Edit Row button	Opens the Edit Interface dialog box, where you can edit the selected interface. For more information, see the instructions for the relevant mode: • Access Port Mode—Create and Edit Interface Dialog Boxes—Access Port Mode, page 67-9. • Routed Port Mode—Create and Edit Interface Dialog Boxes—Routed Port Mode, page 67-12 • Trunk Port Mode—Create and Edit Interface Dialog Boxes—Trunk Port Mode, page 67-14 • Dynamic Mode—Create and Edit Interface Dialog Boxes—Dynamic Mode, page 67-18 • Unsupported—Create and Edit Interface Dialog Boxes—Unsupported Mode, page 67-24
Delete Row button	Deletes the selected interface.

Create and Edit Interface Dialog Boxes—Access Port Mode

Use the Create Interface dialog box (or the Edit Interface dialog box) to configure the attributes of physical and virtual interfaces that run in access port mode.

Navigation Path

Go to the Interfaces/VLANs Page—Interfaces Tab, page 67-7, click **Add** or **Edit** to open the Create/Edit Interface dialog box, then select **Access Port** from the Mode list.

Related Topics

- Create and Edit Interface Dialog Boxes—Routed Port Mode, page 67-12
- Create and Edit Interface Dialog Boxes—Trunk Port Mode, page 67-14
- Create and Edit Interface Dialog Boxes—Dynamic Mode, page 67-18
- Interface Auto Name Generator Dialog Box, page 61-12
- Understanding FlexConfig Policies and Policy Objects, page 7-2
- Understanding Interface Role Objects, page 6-72

Field Reference

Table 67-4 Create and Edit Interface Dialog Boxes—Access Port Mode

Element	Description
Enable Interface	When selected, enables the interface. When deselected, disables the interface using the shutdown command.
Type	Specifies whether the definitions apply to an interface or a subinterface. For details about defining a subinterface, see Create and Edit Interface Dialog Boxes—Subinterfaces, page 67-22.
Name (Select button)	Displays the generated interface name, if the name has been set. Click **Select** to open the Interface Auto Name Generator Dialog Box, page 61-12. From here, you can enter or edit the details that Security Manager uses to generate an interface name.
Mode	The port configuration type for this interface. Select **Access Port** to display the configuration options that are relevant for access ports.

Table 67-4 Create and Edit Interface Dialog Boxes—Access Port Mode (Continued)

Element	Description
Access Port settings	
VLAN ID (Select button)	Displays the interface-specific identity of the VLAN to use in access port mode, if you have selected a VLAN. Otherwise, click **Select** to open the VLAN Selector Dialog Box, page 67-35. The VLAN ID specifies where 802.1Q tagged packets are sent and received on the subinterface; without a VLAN ID, the subinterface cannot send or receive traffic. Valid values range from 1 to 4094. Some VLAN IDs might be reserved on connected devices, so see the device documentation for more information. For multiple context mode, you can only set the VLAN in the system configuration. **Note** All VLAN IDs must be unique among all subinterfaces configured on the same physical interface. **Tip** To configure DOT1Q encapsulation on an Ethernet interface without associating the VLAN with a subinterface, enter the **vlan-id dot1q** command using CLI commands or FlexConfigs. Configuring VLANs on the main interface increases the number of VLANs that can be configured on the device.
Enable Port Security	When selected, enables you to restrict input to an interface by limiting the MAC addresses that are allowed to access the port. When deselected, disables port security.
Max. MAC Addresses	Applies only when Enable Port Security is selected. The maximum number of secure MAC addresses for the interface. Valid values range from 1 to 4097. **Note** Secure MAC addresses are configured dynamically using the MAC addresses of connected devices.
Violation Policy	The action to take if a security violation occurs: • Port Security Protect—Drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses and the count drops below the maximum value. • Port Security Restrict—Drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses and the count drops below the maximum value. In addition, it causes the SecurityViolation counter to increment. • Port Security Shutdown—Immediately puts the interface into the error-disabled state and sends an SNMP trap notification. A security violation occurs if a workstation whose MAC address is not in the address table attempts to access the interface after the maximum number of secure MAC addresses is configured.
Enable VACL Capture	When selected, enables VACL capture. If the capture bit is set, ports with the capture function enabled can receive forwarded packets. When deselected, disables VACL capture.

Table 67-4 Create and Edit Interface Dialog Boxes—Access Port Mode (Continued)

Element	Description
Capture VLANs (Select button)	Enables you to identify the VLANs where VACLs should receive forwarded VLAN packets. This option is available if you selected the Enable VACL Capture check box. Enter a comma-separated list of VLAN IDs or click **Select** to open the VLAN Selector Dialog Box, page 67-35. VACLs can capture VLAN packets only when they are initially routed or bridged into the VLAN. Only forwarded packets can be captured.
Common interface settings	
Speed	The speed of the physical interface: • 10—Transmits at 10 Mbps. • 100—Transmits at 100 Mbps. • 1000—Transmits at 1,000 Mbps. • 10000—Transmits at 10,000 Mbps. • Auto—If Speed is set to Auto, both Speed and Duplex are autonegotiated. • Non-Negotiate—Disables link negotiation.
Duplex	The duplex setting of the interface: • Auto—Autonegotiates the duplex. • Half—Sends and receives data, but not at the same time • Full—Sends and receives data at the same time. If the speed is set to Auto, the duplex setting must also be set to Auto.
MTU	The maximum transmission unit, which refers to the largest packet size (in bytes) that can be handled by the interface. The range of valid values depends on the interface type.
Description	A text description of the interface. Enter up to 240 characters on a single line, without using carriage returns. **Note** For multiple context mode, the system description is independent of the context description.
Flow Control Receive	The flow control setting for incoming frames: • Off—The port does not use flow control, regardless of whether the neighboring port requests flow control. • On—The port uses flow control, as dictated by the neighboring port. • Desired—The port allows, but does not require, flow control frames. Flow control frames (also called pause frames) are special packets that signal a source to stop sending frames for a defined interval when buffers are full.

Table 67-4 Create and Edit Interface Dialog Boxes—Access Port Mode (Continued)

Element	Description
Flow Control Send	The flow control setting for outgoing frames: • Off—The port does not send flow control frames to the neighboring port. • On—The port sends flow control frames to the neighboring port. • Desired—The port allows, but does not require, flow control frames.
Roles	Lists the interface roles associated with the interface. Interface roles are objects that are replaced with the actual interface IP addresses when the configuration is generated for each device. They allow you to define generic rules—ones that can apply to multiple interfaces. See Understanding Interface Role Objects, page 6-72.

Create and Edit Interface Dialog Boxes—Routed Port Mode

Use the Create Interface dialog box (or the Edit Interface dialog box) to configure the attributes of physical interfaces that run in routed port mode on Layer 3.

Navigation Path

Go to the Interfaces/VLANs Page—Interfaces Tab, page 67-7, click **Add** or **Edit** to open the Create/Edit Interface dialog box, then select **Routed Port** from the Mode list.

Related Topics

- Create and Edit Interface Dialog Boxes—Access Port Mode, page 67-9
- Create and Edit Interface Dialog Boxes—Trunk Port Mode, page 67-14
- Create and Edit Interface Dialog Boxes—Dynamic Mode, page 67-18
- Understanding Interface Role Objects, page 6-72
- Selecting Objects for Policies, page 6-2
- Understanding Networks/Hosts Objects, page 6-79

Field Reference

Table 67-5 Create and Edit Interface Dialog Boxes—Routed Port Mode

Element	Description
Enable Interface	When selected, enables the interface. When deselected, disables the interface using the shutdown command.
Type	Specifies whether the definitions apply to an interface or a subinterface. For details about defining a subinterface, see Create and Edit Interface Dialog Boxes—Subinterfaces, page 67-22.

Table 67-5 Create and Edit Interface Dialog Boxes—Routed Port Mode (Continued)

Element	Description
Name (Select button)	Displays the generated interface name, if the name has been set. Click **Select** to open the Interface Auto Name Generator Dialog Box, page 61-12. From here, you can enter or edit the details that Security Manager uses to generate an interface name.
Mode	The port configuration type for this interface. Select **Routed Port** to display the configuration options that are relevant for routed ports.
Routed Port settings	
IP Type	The type of IP address used by the port: • Static IP—Specifies that the interface uses a permanent IP address and activates related GUI elements.
IP Address (Select button)	Enables you to enter an IP address, or you can click **Select** to open the Networks/Hosts Selector, where you can select an IP address.
Helper IP Addresses (Select button)	Enables you to assign a helper IP address to the interface. A helper IP address converts broadcast DHCP requests to unicast requests that are directed exclusively to the DHCP server.
Mask	Enables you to specify the subnet mask. You can enter a netmask value or you can select a netmask from the list. If you enter a netmask, you can express its value in dotted decimal format (for example, 255.255.255.0) or you can enter the number of bits (for example, 24). **Note** Do not use 255.255.255.254 or 255.255.255.255 for any interface that is connected to your network; these netmasks cause all traffic on an interface to stop.
Common interface settings	
Speed	The speed of the physical interface: • 10—Transmits at 10 Mbps. • 100—Transmits at 100 Mbps. • 1000—Transmits at 1,000 Mbps. • 10000—Transmits at 10,000 Mbps. • Auto—If Speed is set to Auto, both Speed and Duplex are autonegotiated. • Non-Negotiate—Disables link negotiation.
Duplex	The duplex setting of the interface: • Auto—Autonegotiates the duplex. • Half—Sends and receives data, but not at the same time • Full—Sends and receives data at the same time. If the speed is set to Auto, the duplex setting must also be set to Auto.
MTU	The maximum transmission unit, which refers to the largest packet size (in bytes) that can be handled by the interface. The range of valid values depends on the interface type.

Table 67-5 Create and Edit Interface Dialog Boxes—Routed Port Mode (Continued)

Element	Description
Description	A text description of the interface. Enter up to 240 characters on a single line, without using carriage returns. **Note** For multiple context mode, the system description is independent of the context description.
Flow Control Receive	The flow control setting for incoming frames: • Off—The port does not use flow control, regardless of whether the neighboring port requests flow control. • On—The port uses flow control, as dictated by the neighboring port. • Desired—The port allows, but does not require, flow control frames. Flow control frames (also called pause frames) are special packets that signal a source to stop sending frames for a defined interval when buffers are full.
Flow Control Send	The flow control setting for outgoing frames: • Off—The port does not send flow control frames to the neighboring port. • On—The port sends flow control frames to the neighboring port. • Desired—The port allows, but does not require, flow control frames.
Roles	Lists the interface roles associated with the interface. Interface roles are objects that are replaced with the actual interface IP addresses when the configuration is generated for each device. They allow you to define generic rules—ones that can apply to multiple interfaces. See Understanding Interface Role Objects, page 6-72.

Create and Edit Interface Dialog Boxes—Trunk Port Mode

Use the Create Interface dialog box (or the Edit Interface dialog box) to configure the attributes of physical and virtual interfaces that run in trunk port mode.

Navigation Path

Go to the Interfaces/VLANs Page—Interfaces Tab, page 67-7, click **Add** or **Edit** to open the Create/Edit Interface dialog box, then select **Trunk Port** from the Mode list.

Related Topics

- Create and Edit Interface Dialog Boxes—Access Port Mode, page 67-9
- Create and Edit Interface Dialog Boxes—Routed Port Mode, page 67-12
- Create and Edit Interface Dialog Boxes—Dynamic Mode, page 67-18
- Understanding FlexConfig Policies and Policy Objects, page 7-2
- Understanding Interface Role Objects, page 6-72

Field Reference

Table 67-6 Create and Edit Interface Dialog Boxes—Trunk Port Mode

Element	Description
Enable Interface	When selected, enables the interface. When deselected, disables the interface using the shutdown command.
Type	Specifies whether the definitions apply to an interface or a subinterface. For details about defining a subinterface, see Create and Edit Interface Dialog Boxes—Subinterfaces, page 67-22.
Name (Select button)	Displays the generated interface name, if the name has been set. Click **Select** to open the Interface Auto Name Generator Dialog Box, page 61-12. From here, you can enter or edit the details that Security Manager uses to generate an interface name.
Mode	The port configuration type for this interface. Select **Trunk Port** to display the configuration options that are relevant for trunk ports.
Trunk Port settings	
Encapsulation	Select one of the following: • DOT1Q—Specifies VLAN encapsulation on the trunk link, as defined by the IEEE 802.1Q standard. Applies only to Ethernet subinterfaces. • ISL—Specifies ISL encapsulation on the trunk link. 10-Gigabit Ethernet ports do not support ISL encapsulation. **Tip** To configure DOT1Q encapsulation on an Ethernet interface without associating the VLAN with a subinterface, enter the **vlan-id dot1q** command using CLI commands or FlexConfigs. Configuring VLANs on the main interface increases the number of VLANs that can be configured on the router.

Table 67-6 Create and Edit Interface Dialog Boxes—Trunk Port Mode (Continued)

Element	Description
Native VLAN (Select button)	Enables you to select the Native VLAN to associate with this interface, using the ID specified in the VLAN ID field. (If no VLAN ID is specified for the Native VLAN, the default is 1.) This option applies to you only if you are configuring a physical interface that is meant to serve as an 802.1Q trunk interface. You must first specify DOT1Q as the encapsulation type. The Native VLAN of a trunk interface is the VLAN to which all untagged VLAN packets are logically assigned. This includes the management traffic associated with the VLAN. When deselected, the Native VLAN is not associated with this interface. **Note** The Native VLAN cannot be configured on a subinterface of the trunk interface. Be sure to configure the same Native VLAN value at both ends of the link; otherwise, traffic may be lost or sent to the wrong VLAN. Click **Select** to open the VLAN Selector Dialog Box, page 67-35. From here, you can associate a native VLAN with the described interface.
Enable DTP negotiation	When selected, enables Dynamic Trunking Protocol (DTP) negotiation. DTP manages trunk auto-negotiation (ISL and 802.1Q) between devices. When deselected, disables DTP negotiation.
Allowed VLANs (Select button)	Enables you to specify which VLANs are allowed on the trunk. Enter the VLAN IDs. Use commas to separate multiple VLANs or use a hyphen to indicate a range of VLANs (for example, 12,17,22 or 2-200). Valid IDs range from 1 to 4094. Or, click **Select** to open the VLAN Selector Dialog Box, page 67-35. From here, you can select the VLANs to include on the trunk.
Prune VLANs (Select button)	Enables you to specify which VLANs are eligible for pruning. Enter the VLAN IDs. Use commas to separate multiple VLANs or use a hyphen to indicate a range of VLANs (for example, 12,17,22 or 2-200.) Or, click **Select** to open the VLAN Selector Dialog Box, page 67-35. From here, you can select the VLANs that are eligible for pruning.
Enable VACL Capture	When selected, enables VACL capture. If the capture bit is set, ports with the capture function enabled can receive forwarded packets. When deselected, disables VACL capture.
Capture VLANs (Select button)	Enables you to identify the VLANs where VACLs should receive forwarded VLAN packets. This option is available if you selected the Enable VACL Capture check box. Enter a comma-separated list of VLAN IDs, or click **Select** to open the VLAN Selector Dialog Box, page 67-35. VACLs can capture VLAN packets only when they are initially routed or bridged into the VLAN. Only forwarded packets can be captured.

Table 67-6 Create and Edit Interface Dialog Boxes—Trunk Port Mode (Continued)

Element	Description
Enable Port Security	Applies only to devices running IOS Software Version 12.2(18)SXE2 or later. When selected, enables you to restrict input to an interface by limiting the MAC addresses that are allowed to access the port. When deselected, disables port security. **Note** If you select this option, the Enable DTP Negotiation option is automatically deselected.
Max. MAC Addresses	Applies only when Enable Port Security is selected. The maximum number of secure MAC addresses for the interface. Valid values range from 1 to 4097. **Note** Secure MAC addresses are configured dynamically using the MAC addresses of connected devices.
Violation Policy	The action to take if a security violation occurs: • Port Security Protect—Drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses and the count drops below the maximum value. • Port Security Restrict—Drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses and the count drops below the maximum value. In addition, it causes the SecurityViolation counter to increment. • Port Security Shutdown—Immediately puts the interface into the error-disabled state and sends an SNMP trap notification. A security violation occurs if a workstation whose MAC address is not in the address table attempts to access the interface after the maximum number of secure MAC addresses is configured.
Common interface settings	
Speed	The speed of the physical interface: • 10—Transmits at 10 Mbps. • 100—Transmits at 100 Mbps. • 1000—Transmits at 1,000 Mbps. • 10000—Transmits at 10,000 Mbps. • Auto—If Speed is set to Auto, both Speed and Duplex are autonegotiated. • Non-Negotiate—Disables link negotiation.
Duplex	The duplex setting of the interface: • Auto—Autonegotiates the duplex. • Half—Sends and receives data, but not at the same time • Full—Sends and receives data at the same time. If the speed is set to Auto, the duplex setting must also be set to Auto.

Table 67-6 Create and Edit Interface Dialog Boxes—Trunk Port Mode (Continued)

Element	Description
MTU	The maximum transmission unit, which refers to the largest packet size (in bytes) that can be handled by the interface. The range of valid values depends on the interface type.
Description	A text description of the interface. Enter up to 240 characters on a single line, without using carriage returns. **Note** For multiple context mode, the system description is independent of the context description.
Flow Control Receive	The flow control setting for incoming frames: • Off—The port does not use flow control, regardless of whether the neighboring port requests flow control. • On—The port uses flow control, as dictated by the neighboring port. • Desired—The port allows, but does not require, flow control frames. Flow control frames (also called pause frames) are special packets that signal a source to stop sending frames for a defined interval when buffers are full.
Flow Control Send	The flow control setting for outgoing frames: • Off—The port does not send flow control frames to the neighboring port. • On—The port sends flow control frames to the neighboring port. • Desired—The port allows, but does not require, flow control frames.
Roles	Lists the interface roles associated with the interface. Interface roles are objects that are replaced with the actual interface IP addresses when the configuration is generated for each device. They allow you to define generic rules—ones that can apply to multiple interfaces. See Understanding Interface Role Objects, page 6-72.

Create and Edit Interface Dialog Boxes—Dynamic Mode

Use the Create Interface dialog box (or the Edit Interface dialog box) to configure the attributes of physical and virtual interfaces that run in dynamic mode. Dynamic ports can convert the link into a trunk link based on the settings of the neighboring port.

Navigation Path

Go to the Interfaces/VLANs Page—Interfaces Tab, page 67-7, click **Add** or **Edit** to open the Create/Edit Interface dialog box, then select **Dynamic** from the Mode list.

Related Topics

- Create and Edit Interface Dialog Boxes—Access Port Mode, page 67-9
- Create and Edit Interface Dialog Boxes—Routed Port Mode, page 67-12
- Create and Edit Interface Dialog Boxes—Trunk Port Mode, page 67-14

- Interface Auto Name Generator Dialog Box, page 61-12
- Understanding FlexConfig Policies and Policy Objects, page 7-2
- Understanding Interface Role Objects, page 6-72

Field Reference

Table 67-7 Create and Edit Interface Dialog Boxes—Dynamic Mode

Element	Description
Enable Interface	When selected, enables the interface. When deselected, disables the interface using the shutdown command.
Type	Specifies whether the definitions apply to an interface or a subinterface. For details about defining a subinterface, see Create and Edit Interface Dialog Boxes—Subinterfaces, page 67-22.
Name (Select button)	Displays the generated interface name, if the name has been set. Click **Select** to open the Interface Auto Name Generator Dialog Box, page 61-12. From here, you can enter or edit the details that Security Manager uses to generate an interface name.
Mode	The port configuration type for this interface. Select **Dynamic** to display the configuration options that are relevant for dynamic ports.
Dynamic Port settings	
Dynamic Mode	The dynamic trunk mode: • Auto—Allows the port to convert the link to a trunk link. The port becomes a trunk port if the neighboring port is set to Trunk or Desirable mode. • Desirable—Makes the port actively attempt to convert the link to a trunk link.
Access VLAN ID	The access VLAN ID to use when the port does *not* function as a trunking link. This can occur when the neighboring interface is not set to trunk, auto, or desirable mode. Valid values range from 1 to 4094.

Table 67-7 Create and Edit Interface Dialog Boxes—Dynamic Mode (Continued)

Element	Description
Encapsulation	Select one of the following: • DOT1Q—Specifies VLAN encapsulation on the trunk link, as defined by the IEEE 802.1Q standard. Applies only to Ethernet subinterfaces. • ISL—Specifies ISL encapsulation on the trunk link. 10-Gigabit Ethernet ports do not support ISL encapsulation. • Negotiate—Specifies that the interface negotiates with the neighboring interface to become either an ISL or 802.1Q trunk, based on the configuration and capabilities of the neighboring interface. **Tip** To configure DOT1Q encapsulation on an Ethernet interface without associating the VLAN with a subinterface, enter the **vlan-id dot1q** command using CLI commands or FlexConfigs. Configuring VLANs on the main interface increases the number of VLANs that can be configured on the router.
Native VLAN (Select button)	Enables you to select the Native VLAN to associate with this interface, using the ID specified in the VLAN ID field. (If no VLAN ID is specified for the Native VLAN, the default is 1.) This option applies to you only if you are configuring a physical interface that is meant to serve as an 802.1Q trunk interface. You must first specify DOT1Q as the encapsulation type. The Native VLAN of a trunk interface is the VLAN to which all untagged VLAN packets are logically assigned. This includes the management traffic associated with the VLAN. When deselected, the Native VLAN is not associated with this interface. **Note** The Native VLAN cannot be configured on a subinterface of the trunk interface. Be sure to configure the same Native VLAN value at both ends of the link; otherwise, traffic may be lost or sent to the wrong VLAN. Click **Select** to open the VLAN Selector Dialog Box, page 67-35. From here, you can associate a native VLAN with the described interface.
Allowed VLANs (Select button)	Enables you to specify which VLANs are allowed on the trunk. Enter the VLAN IDs. Use commas to separate multiple VLANs or use a hyphen to indicate a range of VLANs (for example, 12,17,22 or 2-200). Valid IDs range from 1 to 4094. Alternatively, click **Select** to open the VLAN Selector Dialog Box, page 67-35. From here, you can select the VLANs to include on the trunk.

Table 67-7 Create and Edit Interface Dialog Boxes—Dynamic Mode (Continued)

Element	Description
Prune VLANs (Select button)	Enables you to specify which VLANs are eligible for pruning. Enter the VLAN IDs. Use commas to separate multiple VLANs or use a hyphen to indicate a range of VLANs (for example, 12,17,22 or 2-200.) Alternatively, click **Select** to open the VLAN Selector Dialog Box, page 67-35. From here, you can select the VLANs that are eligible for pruning.
Enable VACL Capture	When selected, enables VACL capture. If the capture bit is set, ports with the capture function enabled can receive forwarded packets. When deselected, disables VACL capture.
Capture VLANs (Select button)	Enables you to identify the VLANs where VACLs should receive forwarded VLAN packets. This option is available if you selected the Enable VACL Capture check box. Enter a comma-separated list of VLAN IDs or click **Select** to open the VLAN Selector Dialog Box, page 67-35. VACLs can capture VLAN packets only when they are initially routed or bridged into the VLAN. Only forwarded packets can be captured.
Common interface settings	
Speed	The speed of the physical interface: • 10—Transmits at 10 Mbps. • 100—Transmits at 100 Mbps. • 1000—Transmits at 1,000 Mbps. • 10000—Transmits at 10,000 Mbps. • Auto—If Speed is set to Auto, both Speed and Duplex are autonegotiated. • Non-Negotiate—Disables link negotiation.
Duplex	The duplex setting of the interface: • Auto—Autonegotiates the duplex. • Half—Sends and receives data, but not at the same time • Full—Sends and receives data at the same time. If the speed is set to Auto, the duplex setting must also be set to Auto.
MTU	The maximum transmission unit, which refers to the largest packet size (in bytes) that can be handled by the interface. The range of valid values depends on the interface type.
Description	A text description of the interface. Enter up to 240 characters on a single line, without using carriage returns. **Note** For multiple context mode, the system description is independent of the context description.

Table 67-7 Create and Edit Interface Dialog Boxes—Dynamic Mode (Continued)

Element	Description
Flow Control Receive	The flow control setting for incoming frames: • Off—The port does not use flow control, regardless of whether the neighboring port requests flow control. • On—The port uses flow control, as dictated by the neighboring port. • Desired—The port allows, but does not require, flow control frames. Flow control frames (also called pause frames) are special packets that signal a source to stop sending frames for a defined interval when buffers are full.
Flow Control Send	The flow control setting for outgoing frames: • Off—The port does not send flow control frames to the neighboring port. • On—The port sends flow control frames to the neighboring port. • Desired—The port allows, but does not require, flow control frames.
Roles	Lists the interface roles associated with the interface. Interface roles are objects that are replaced with the actual interface IP addresses when the configuration is generated for each device. They allow you to define generic rules—ones that can apply to multiple interfaces. See Understanding Interface Role Objects, page 6-72.

Create and Edit Interface Dialog Boxes—Subinterfaces

Use the Create Interface dialog box (or the Edit Interface dialog box) to configure the attributes of subinterfaces defined on Catalyst 6500/7600 devices.

Navigation Path

Go to the Interfaces/VLANs Page—Interfaces Tab, page 67-7, click **Add** or **Edit** to open the Create/Edit Interface dialog box, then select **Subinterface** from the Type list.

Related Topics

- Create and Edit Interface Dialog Boxes—Access Port Mode, page 67-9
- Create and Edit Interface Dialog Boxes—Routed Port Mode, page 67-12
- Create and Edit Interface Dialog Boxes—Trunk Port Mode, page 67-14
- Create and Edit Interface Dialog Boxes—Dynamic Mode, page 67-18
- Understanding Interface Role Objects, page 6-72

Field Reference

Table 67-8 Create and Edit Interface Dialog Boxes—Subinterfaces

Element	Description
Enable Interface	When selected, enables the subinterface. When deselected, disables the subinterface using the shutdown command.
Type	Specifies whether the definitions apply to an interface or a subinterface. Select **Subinterface**.
Parent	Identifies the parent interface of the subinterface.
Subint. ID	Specifies the ID for the subinterface. The numeric ID string cannot exceed 10 characters.
IP Type	The type of IP address used by the subinterface: • Static IP—Specifies that the subinterface uses a permanent IP address and activates related GUI elements.
IP Address	Enables you to enter an IP address.
Helper IP Addresses	Enables you to assign a helper IP address to the subinterface. A helper IP address converts broadcast DHCP requests to unicast requests that are directed exclusively to the DHCP server.
Mask	Enables you to specify the subnet mask. You can enter a netmask value or you can select a netmask from the list. If you enter a netmask, you can express its value in dotted decimal format (for example, 255.255.255.0) or you can enter the number of bits (for example, 24). **Note** Do not use 255.255.255.254 or 255.255.255.255 for any interface that is connected to your network; these netmasks cause all traffic on an interface to stop.
Encapsulation	The encapsulation type defined for the subinterface: • [blank]—No encapsulation is defined. • DOT1Q—Specifies VLAN encapsulation on the trunk link, as defined by the IEEE 802.1Q standard. Applies only to Ethernet subinterfaces. • ISL—Specifies ISL encapsulation on the trunk link. 10-Gigabit Ethernet ports do not support ISL encapsulation. **Tip** To configure DOT1Q encapsulation on an Ethernet interface without associating the VLAN with a subinterface, enter the **vlan-id dot1q** command using CLI commands or FlexConfigs. Configuring VLANs on the main interface increases the number of VLANs that can be configured on the router.
VLAN ID	Applies only when encapsulation is defined for the subinterface. The VLAN ID associated with the subinterface.
Description	A text description of the interface. Enter up to 240 characters on a single line, without using carriage returns. **Note** For multiple context mode, the system description is independent of the context description.

Create and Edit Interface Dialog Boxes—Unsupported Mode

If you discover an interface configured with a mode that is not supported by Security Manager (such as dot1q-tunnel or private-vlan), the interface is displayed in Unsupported mode. You can view the attributes of this interface, but you cannot make any changes to the configuration unless you first change the mode. All definition fields, other than Mode, are read-only.

Navigation Path

Go to the Interfaces/VLANs Page—Interfaces Tab, page 67-7, select an interface whose mode is defined as Unsupported, then click **Add** or **Edit** to open the Create/Edit Interface dialog box.

Related Topics

- Create and Edit Interface Dialog Boxes—Access Port Mode, page 67-9
- Create and Edit Interface Dialog Boxes—Routed Port Mode, page 67-12
- Create and Edit Interface Dialog Boxes—Trunk Port Mode, page 67-14
- Create and Edit Interface Dialog Boxes—Dynamic Mode, page 67-18

Field Reference

Table 67-9 Create and Edit Interface Dialog Boxes—Unsupported Mode

Element	Description
Enable Interface	When selected, indicates that the interface is enabled. When deselected, indicates that the interface has been disabled using the shutdown command.
Type	Specifies whether the definitions apply to an interface or a subinterface.
Name (Select button)	Displays the name of the interface.
Mode	Displays Unsupported, which designates an interface whose mode is not supported by Security Manager. Select a different option to change the interface mode. **Note** If you change the interface mode, you can then modify the other settings in this dialog box.
Speed	Displays the speed of the physical interface: • 10—Transmits at 10 Mbps. • 100—Transmits at 100 Mbps. • 1000—Transmits at 1,000 Mbps. • 10000—Transmits at 10,000 Mbps. • Auto—If Speed is set to Auto, both Speed and Duplex are autonegotiated. • Non-Negotiate—Disables link negotiation.

Table 67-9 Create and Edit Interface Dialog Boxes—Unsupported Mode (Continued)

Element	Description
Duplex	Displays the duplex setting of the interface: • Auto—Autonegotiates the duplex. • Half—Sends and receives data, but not at the same time • Full—Sends and receives data at the same time. If the speed is set to Auto, the duplex setting must also be set to Auto.
MTU	Displays the maximum transmission unit, which refers to the largest packet size (in bytes) that can be handled by the interface. The range of valid values depends on the interface type.
Description	Displays a text description of the interface. For multiple context mode, the system description is independent of the context description.
Flow Control Receive	Displays the flow control setting for incoming frames: • Off—The port does not use flow control, regardless of whether the neighboring port requests flow control. • On—The port uses flow control, as dictated by the neighboring port. • Desired—The port allows, but does not require, flow control frames. Flow control frames (also called pause frames) are special packets that signal a source to stop sending frames for a defined interval when buffers are full.
Flow Control Send	Displays the flow control setting for outgoing frames: • Off—The port does not send flow control frames to the neighboring port. • On—The port sends flow control frames to the neighboring port. • Desired—The port allows, but does not require, flow control frames.
Roles	Lists the interface roles associated with the interface. Interface roles are objects that are replaced with the actual interface IP addresses when the configuration is generated for each device. They allow you to define generic rules—ones that can apply to multiple interfaces. See Understanding Interface Role Objects, page 6-72.

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 Cisco Catalyst 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 67-26
- Deleting VLANs, page 67-27
- Interfaces/VLANs Page—VLANs Tab, page 67-27

Related Topics

- VLAN Groups, page 67-31
- VLAN ACLs (VACLs), page 67-36
- Chapter 67, "Managing Cisco Catalyst Switches and Cisco 7600 Series Routers"

Creating or Editing VLANs

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

Related Topics

- Deleting VLANs, page 67-27
- Creating or Editing VLAN Groups, page 67-32
- Creating or Editing VACLs, page 67-37
- Create and Edit VLAN Dialog Boxes, page 67-28
- VLANs, page 67-25

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 67-27.

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 67-28, 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 67-32.

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**.

Step 8 (Optional) For a Layer 3 VLAN, define a switched virtual interface (SVI):

a. 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.

b. Enter the IP address for the SVI.

c. Enter the SVI subnet mask by typing it, or select a netmask value from the Subnet Mask list.

d. 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 67-42 for a description of the fields in the dialog box. For more information about defining ports, see Creating or Editing Ports on Cisco Catalyst Switches and Cisco 7600 Series Routers, page 67-5.

Step 10 Click **OK** to save your definitions locally on the client and close the dialog box.

Deleting VLANs

You can delete a VLAN. However, deleting a VLAN does not delete it from any policy that might reference it. Ensure that your other policies do not use the VLAN before you delete it. When you submit your changes to the database, Security Manager points out any undefined VLANs that are referenced by other policies.

Related Topics

- Creating or Editing VLANs, page 67-26
- VLANs, page 67-25

Step 1 (Device view) Select a Cisco Catalyst switch or Cisco 7600 Series router from the Device selector.

Step 2 Select **Interfaces/VLANs** from the Policies selector.

Step 3 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 67-27.

Step 4 Select a VLAN from the table, then click **Delete Row**.

The VLAN is deleted.

Interfaces/VLANs Page—VLANs Tab

Use the VLANs tab to view and configure VLANs on supported Cisco Catalyst switches and Cisco 7600 Series routers.

Navigation Path

- (Device view) Select **Interfaces/VLANs** from the Device selector, then click the **VLANs** tab.

Related Topics

- Interfaces/VLANs Page—VLAN Groups Tab, page 67-33
- Interfaces/VLANs Page—Interfaces Tab, page 67-7
- Viewing a Summary of Catalyst Interfaces, VLANs, and VLAN Groups, page 67-3
- Understanding FlexConfig Policies and Policy Objects, page 7-2
- Create and Edit VLAN Dialog Boxes, page 67-28
- Filtering Tables, page 1-48

Field Reference

Table 67-10 Interfaces/VLANs Page—VLANs Tab

Element	Description
VLAN ID	Interface-specific identity of the VLAN that a table row describes. The VLAN ID specifies where 802.1Q tagged packets are sent and received on the subinterface; without a VLAN ID, the subinterface cannot send or receive traffic. Valid values range from 2 to 4094 (VLAN ID 1 is reserved). **Note** All VLAN IDs must be unique among all subinterfaces configured on the same physical interface. **Tip** To configure DOT1Q encapsulation on an Ethernet interface without associating the VLAN with a subinterface, enter the **vlan-id dot1q** command using CLI commands or FlexConfigs. Configuring VLANs on the main interface increases the number of VLANs that can be configured on the device.
Name	Name of the corresponding VLAN for an interface or subinterface.
Interface	Identifies the logical name of the interface (interface role) or physical interface.
Type	Specifies whether a VLAN has access to Layer 2 or Layer 3.
Status	Indicates whether a VLAN is active or suspended.
Add Row button	Opens the Create VLAN dialog box to define a new VLAN.
Edit Row button	Opens the Edit VLAN dialog box to edit the selected VLAN.
Delete Row button	Deletes the selected VLAN.

Create and Edit VLAN Dialog Boxes

Use the Create VLAN dialog box (or the Edit VLAN dialog box) to configure or reconfigure VLAN settings and attributes.

Navigation Path

Go to the Interfaces/VLANs Page—VLANs Tab, page 67-27, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Understanding FlexConfig Policies and Policy Objects, page 7-2
- Create and Edit VLAN Group Dialog Boxes, page 67-34
- Interface Selector Dialog Box—VLAN ACL Content, page 67-42

Field Reference

Table 67-11 Create and Edit VLAN Dialog Box

Element	Description
VLAN ID	Displays the VLAN ID if one is configured. Otherwise, enter the ID manually. The VLAN ID specifies where 802.1Q tagged packets are sent and received on an interface or subinterface; without a VLAN ID, the interface or subinterface cannot send or receive traffic. Each VLAN must have an ID. Valid values range from 1 to 4094. **Note** All VLAN IDs must be unique among all subinterfaces configured on the same physical interface. **Tip** To configure DOT1Q encapsulation on an Ethernet interface without associating the VLAN with a subinterface, enter the **vlan-id dot1q** command using CLI commands or FlexConfigs. Configuring VLANs on the main interface increases the number of VLANs that can be configured on the device.
Name	Enter a name for the VLAN, or view the VLAN name if you entered one previously. Each VLAN must have an ID, and can optionally have a name. The maximum length is 32 characters.
Group	The VLAN group to which the VLAN belongs. A VLAN can be associated with one group only. You can associate the VLAN with an existing group, or select **Add Group** to open the Create VLAN Group dialog box.
Status	The current status of the VLAN: • Active—The VLAN carries traffic. • Suspended—The VLAN does not pass packets.
Type	Indicates whether the specified VLAN is configured for Layer 2 or Layer 3, and enables you to choose the kind of VLAN that you prefer. A Layer 3 VLAN requires an IP address and creates a VLAN interface.

Table 67-11 Create and Edit VLAN Dialog Box (Continued)

Element	Description
Switch Virtual Interface	Applies only when defining a Layer 3 VLAN. • Enable Interface—When selected, enables the switched virtual interface (SVI), which is a virtual interface that you can attach to any VLAN. The SVI enables routing between VLANs and provides IP host connectivity to the switch. When deselected, disables the SVI. • IP Address—The IP address for the SVI. An IP address is required for management access. • Subnet Mask—The subnet mask for the SVI. Select any option from the list of valid subnet mask entries. • Description—Enables you to enter a description of up to 240 characters on a single line, without carriage returns. For multiple context mode, the system description is independent of the context description.
Access Ports (Select button)	Lists which access ports are associated with the specified VLAN, if any are associated, and enables you to add or remove access port associations for the specified VLAN. You can associate any number of access ports with a VLAN. Click **Select** to open the Access Port Selector Dialog Box, page 67-30. From here, you can associate access ports with the specified VLAN, or remove access port associations from the VLAN.
Trunk Ports (Select button)	Lists which trunk ports are associated with the specified VLAN, if any are associated, and enables you to add or remove trunk port associations for the specified VLAN. A VLAN can belong to the allowed list of one or more trunk ports. You can include a VLAN in a trunk port group. Click **Select** to open the Trunk Port Selector Dialog Box, page 67-31. From here, you can associate trunk ports with the specified VLAN, or remove trunk port associations from the VLAN.

Access Port Selector Dialog Box

Use the Access Port Selector dialog box to define which access ports are associated with a selected VLAN.

Navigation Path

Open the Create and Edit VLAN Dialog Boxes, page 67-28, then click **Select** in the Access Ports field.

Related Topics

- Create and Edit Interface Dialog Boxes—Access Port Mode, page 67-9
- Trunk Port Selector Dialog Box, page 67-31
- Filtering Tables, page 1-48

Field Reference

Table 67-12 Access Port Selector Dialog Box

Element	Description
Available Access Ports	Displays the access ports that are not assigned to a particular VLAN.
Add >> button	Adds interfaces that are selected in the Available Access Ports list to the Selected Access Ports list.
Remove << button	Removes selected interfaces from the Selected Access Ports list.
Selected Access Ports	Displays the interface objects that are selected.
Add Row button	Opens the Create Interface dialog box to define a new interface.
Edit Row button	Opens the Edit Interface dialog box to edit the selected interface.

Trunk Port Selector Dialog Box

Use the Trunk Port Selector dialog box to define which trunk ports are associated with a selected VLAN.

Navigation Path

Open the Create and Edit VLAN Dialog Boxes, page 67-28, then click **Select** in the Trunk Ports field.

Related Topics

- Create and Edit Interface Dialog Boxes—Trunk Port Mode, page 67-14
- Access Port Selector Dialog Box, page 67-30
- Filtering Tables, page 1-48

Field Reference

Table 67-13 Trunk Port Selector Dialog Box

Element	Description
Available Trunk Ports	Displays all available trunk ports.
Add >> button	Adds interfaces that are selected in the Available Trunk Ports list to the Selected Trunk Ports list.
Remove << button	Removes selected interfaces from the Selected Trunk Ports list.
Selected Trunk Ports	Displays the interface objects that are selected.
Add Row button	Opens the Create Interface dialog box to define a new interface.
Edit Row button	Opens the Edit Interface dialog box to edit the selected interface.

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 Security Context Dialog Box (FWSM), page 58-8.

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

- Creating or Editing VLAN Groups, page 67-32
- Deleting VLAN Groups, page 67-33
- Interfaces/VLANs Page—VLAN Groups Tab, page 67-33

Related Topics

- Interfaces, page 67-5
- VLANs, page 67-25
- VLAN ACLs (VACLs), page 67-36
- Chapter 67, “Managing Cisco Catalyst Switches and Cisco 7600 Series Routers”

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.

Related Topics

- Deleting VLAN Groups, page 67-33
- Creating or Editing VLANs, page 67-26
- Creating or Editing VACLs, page 67-37
- Interfaces/VLANs Page—VLAN Groups Tab, page 67-33
- VLAN Groups, page 67-31

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 67-33.

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 67-34, 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 Security Context Dialog Box (FWSM), page 58-8.

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.

Deleting VLAN Groups

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

Related Topics

- Creating or Editing VLAN Groups, page 67-32
- VLAN Groups, page 67-31

Step 1 (Device view) Select a Catalyst 6500 Series switch or Cisco 7600 Series router from the Device selector.

Step 2 Select **Interfaces/VLANs** from the Policy selector.

Step 3 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 67-33.

Step 4 Select a VLAN group from the table, then click **Delete Row**. The VLAN group is deleted.

Interfaces/VLANs Page—VLAN Groups Tab

Use the VLAN Groups tab to view and configure VLAN groups on supported 6500 Series switches and 7600 Series routers.

Note The VLAN Groups tab is available only for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers.

Navigation Path

- (Device view) Select **Interfaces/VLANs** from the Device selector, then click the **VLAN Groups** tab.

Related Topics

- Interfaces/VLANs Page—VLANs Tab, page 67-27
- Interfaces/VLANs Page—Interfaces Tab, page 67-7
- Viewing a Summary of Catalyst Interfaces, VLANs, and VLAN Groups, page 67-3

- Create and Edit VLAN Group Dialog Boxes, page 67-34
- Filtering Tables, page 1-48

Field Reference

Table 67-14 Interfaces/VLANs Page—VLAN Groups Tab

Element	Description
VLAN Group	Numeric ID of a VLAN group that is configured on the selected device.
Service Module Slots	Associates the chassis slot number (in which the relevant services module is installed) with the interface through which a particular VLAN participates in the VLAN group.
VLAN IDs	The VLAN IDs associated with this group. Valid values range from 1 to 65535.
Add Row button	Opens the Create VLAN Group dialog box to define a new VLAN group.
Edit Row button	Opens the Edit VLAN Group dialog box to edit the selected VLAN group.
Delete Row button	Deletes the selected VLAN group.

Create and Edit VLAN Group Dialog Boxes

Use the Create and Edit VLAN Group dialog box to configure or reconfigure the attributes of VLAN groups, which are logical groups of VLANs that you want to associate with one another when you define VLAN port policies.

Navigation Path

Do one of the following:

- Go to the Interfaces/VLANs Page—VLAN Groups Tab, page 67-33, then click the **Add** or **Edit** button beneath the table.
- Go to the Interfaces/VLANs Page—VLANs Tab, page 67-27, click the **Add** or **Edit** button beneath the table, then select **Add Group** from the Group list.

Related Topics

- Service Module Slot Selector Dialog Box, page 67-35

Field Reference

Table 67-15 Create and Edit VLAN Group Dialog Boxes

Element	Description
VLAN Group ID	The 802.1q VLAN group name. Valid values range from 1 to 65535.

Table 67-15 Create and Edit VLAN Group Dialog Boxes (Continued)

Element	Description
Service Module Slots (Select button)	The chassis slot number (in which the relevant services module is installed) that is associated with the interface through which a particular VLAN participates in the VLAN group. Enter the slot number or click **Select** to open the Service Module Slot Selector Dialog Box, page 67-35. **Note** After you associate the VLAN group with a service module, such as an FWSM, you can assign the VLAN group to the security contexts of the FWSM. See Add/Edit Security Context Dialog Box (FWSM), page 58-8.
VLAN IDs (Select button)	The comma-separated IDs of all VLANs that are part of the group. Each VLAN can be a member of only one group. Click **Select** to open the Service Module Slot Selector Dialog Box, page 67-35. From here, you can select VLANs to include in the VLAN group.

Service Module Slot Selector Dialog Box

Use the Service Module Slot Selector dialog box to associate a service module with a VLAN.

Navigation Path

Go to the Create and Edit VLAN Group Dialog Boxes, page 67-34, then click **Select** in the Service Module Slots field.

Related Topics

- VLAN Selector Dialog Box, page 67-35
- Filtering Tables, page 1-48

Field Reference

Table 67-16 Service Module Selector Dialog Box

Element	Description
Available Service Module Slots	Displays the defined service module slots.
Add >> button	Moves selected service module slots from the Available Service Module Slots list to the Selected Service Module Slots list.
Remove << button	Removes selected service module slots from the Selected Service Modules list.
Selected Service Module Slots	Displays the selected service module slots.

VLAN Selector Dialog Box

Use the VLAN Selector dialog box to associate VLANs with interfaces, VLAN groups, security contexts, and VACLs.

Navigation Path

You can access this dialog box when you define interfaces, VLAN groups, IDSM settings, or VACLs by clicking the **Select** button in any field used for defining VLANs.

Related Topics

- Service Module Slot Selector Dialog Box, page 67-35
- Filtering Tables, page 1-48

Field Reference

Table 67-17 VLAN Selector Dialog Box

Element	Description
Available VLANs	Displays defined VLANs that are available to be associated with the object you are configuring. **Note** The VLANs that are available will depend on the type of object you are configuring and other settings defined on the device. For example, when selecting VLANs to assign to a VLAN group, the Available VLANs list will only contain VLANs that have not been assigned to another VLAN group. When selecting VLANs to assign to a security context, the Available VLANs list will only contain VLANs that are part of a VLAN group that has been assigned to the service module you are configuring.
Add >> button	Moves selected VLANs from the Available VLANs list to the Selected VLANs list.
Remove << button	Removes selected VLANs from the Selected VLANs list.
Selected VLANs	Displays the selected VLANs.
VLAN Ranges	The VLAN ranges entered manually before the selector was opened, if any.

VLAN ACLs (VACLs)

Cisco IOS standard or extended ACLs are configured on router interfaces only, and are applied on routed packets only. In contrast, Cisco Catalyst 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 67-37
- Deleting VACLs, page 67-38
- VLAN Access Lists Page, page 67-39

Related Topics

- VLANs, page 67-25
- VLAN Groups, page 67-31
- Chapter 67, “Managing Cisco Catalyst Switches and Cisco 7600 Series Routers”

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.

Related Topics

- Deleting VACLs, page 67-38
- Creating or Editing VLANs, page 67-26
- Creating or Editing VLAN Groups, page 67-32
- Create and Edit VLAN ACL Dialog Boxes, page 67-41

- VLAN Access Lists Page, page 67-39

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 67-39.

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 67-41, 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 67-41.

b. Enter a number to identify the sequence.

c. Specify the standard and extended ACLs to assign to the sequence, or click **Select** to select the ACL object from a list or to create a new ACL object. For more information about ACL objects, see Creating Access Control List Objects, page 6-53.

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 6-75.)

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 the process 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.

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 6-15.

Related Topics

- Creating or Editing VACLs, page 67-37
- Interfaces/VLANs Page—VLANs Tab, page 67-27
- VLAN ACLs (VACLs), page 67-36

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 67-39.

Step 2 Click in a row to select a VACL, then click **Delete**.

Step 3 Click **OK** to save your changes.

VLAN Access Lists Page

Use the VLAN Access Lists page to view and configure VLAN access lists for Cisco Catalyst switches and Cisco 7600 Series routers.

Navigation Path

You can access this page from:

- (Device view) Select **Platform > VLAN Access Lists** from the Device Policy selector.
- (Device view) Select **Catalyst Platform >VLAN Access Lists** from the Policy Types selector.

Related Topics

- Creating Access Control List Objects, page 6-53
- Create and Edit VLAN ACL Dialog Boxes, page 67-41
- Create and Edit VLAN ACL Content Dialog Boxes, page 67-41
- Filtering Tables, page 1-48

Field Reference

Table 67-18 VLAN Access Lists Page

Element	Description
VLAN Access Lists table	
VLAN ACL	Displays the VLAN ACL name.

Table 67-18 VLAN Access Lists Page (Continued)

Element	Description
Sequence	Specifies the map sequence number. VACL sequences are applied in order of sequence, from lowest number to highest.
Matching	Displays the Match ACLs, if any are defined. VACL matching occurs only when an ACL permit is encountered. ACL denies are ignored.
Action	Specify whether the action is to drop, drop and log, forward, forward and capture, or redirect packets. **Note** The redirect action helps you to specify as many as five interfaces, which can be physical interfaces or EtherChannels. You cannot redirect packets to an EtherChannel member or a VLAN interface.
VLAN IDs	Interface-specific identity of the VLAN that a table row describes. The VLAN ID specifies where 802.1Q tagged packets are sent and received on the subinterface; without a VLAN ID, the subinterface cannot send or receive traffic.
Add Row button	Opens the Create VLAN ACL dialog box, where you can define a new VACL.
Edit Row button	Opens the Edit VLAN ACL dialog box, where you can edit the selected VACL.
Delete Row button	Deletes the selected access list.
Additional fields	
Log Table Size	Displays the log table size. Valid sizes range from 0 to 2048 and the default is 500. Logged packets from new flows are dropped when the table is full.
Max. Packet Rate	Displays the maximum redirect VACL logging packet rate per second. Valid rates range from 10 to 5000 packets per second and the default rate is 2000. Packets that exceed the limit are dropped.
Logging Threshold	Displays the logging threshold if one is set. By default, no threshold is set. When you configure VACL logging, IP packets that are denied generate log messages on a per-flow basis if the threshold for a flow is reached in any interval of less than 5 minutes. Only dropped IP packets can be logged.
Capture Interfaces	Identifies the interface that captures forwarded packets in which the capture bit is set. You can configure any interface as the capture interface. The capture action sets the capture bit for the forwarded packets so that ports with the capture function enabled can receive the packets. Only forwarded packets can be captured. **Note** The information shown here is read-only. To define capture interfaces, use the Create/Edit Interface dialog box. See Interfaces/VLANs Page—Interfaces Tab, page 67-7.

Create and Edit VLAN ACL Dialog Boxes

Use the Create VLAN ACL dialog box (or the Edit VLAN ACL dialog box) to configure or reconfigure VACL attributes.

Navigation Path

Go to the VLAN Access Lists Page, page 67-39, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Create and Edit VLAN Dialog Boxes, page 67-28
- Create and Edit VLAN Group Dialog Boxes, page 67-34
- Filtering Tables, page 1-48

Field Reference

Table 67-19 Create and Edit VLAN ACL Dialog Boxes

Element	Description
VLAN ACL Name	The user-defined name for the VACL.
VLANs (Select button)	Enables you to designate the VLANs to which the VACL should be applied. Do one of the following: • Enter VLAN IDs. You can use commas to separate multiple VLANs or use a hyphen to indicate a range of VLANs. For example: 12,17,22 or 2-200. Valid IDs range from 1 to 4094. • Click **Select** to open the VLAN Selector Dialog Box, page 67-35.
Sequence Map table	The sequence maps included in the VLAN access map. A VLAN access map can consist of one or more map sequences, where each sequence pairs a *match clause*, which specifies an ACL object for traffic filtering, to an *action clause*, which specifies the action to take on packets that meet the criteria defined in the match ACLs. • To add a sequence map, click the Add Row (+) button and fill in the Create VLAN ACL Content dialog box (see Create and Edit VLAN ACL Content Dialog Boxes, page 67-41). • To edit a sequence map, select it and click the Edit Row button. • To delete a sequence map, select it and click the Delete Row button. • To change the order of a map, select it and click the Up or Down arrow buttons until it is in the desired position. The sequence number changes as you move it.

Create and Edit VLAN ACL Content Dialog Boxes

Use the Create VLAN ACL Content dialog box (or the Edit VLAN ACL Content dialog box) to configure or reconfigure VACL sequences.

Navigation Path

Go to the Create and Edit VLAN ACL Dialog Boxes, page 67-41, then click the **Add** or **Edit** button beneath the Sequence Map table.

Related Topics

- Create and Edit VLAN Dialog Boxes, page 67-28
- Create and Edit VLAN Group Dialog Boxes, page 67-34

Field Reference

Table 67-20 Create and Edit VLAN ACL Content Dialog Boxes

Element	Description
Sequence	Specify the map sequence number for the VLAN access map. Valid values range from 1 to 65535.
Match ACLs	Specify which ACLs the sequence should include in its match clause. Enter the names of the standard and extended ACL objects to include in the sequence, or click **Select** to select them from a list or to create new ones. You cannot use a MAC-layer ACL.
Action	The option to perform on packets that meet the criteria defined in the match ACLs: • Drop—Drops the packets. • Drop/Log—Logs the dropped packets. • Forward—Forwards the packets to their destination (using hardware switching). • Forward/Capture—Sets the capture bit for the forwarded packets so that ports with the capture function enabled also receive the packets. • Redirect—Redirects packets to the Ethernet interfaces defined in the Interfaces field.
Interfaces (Select button)	Applies only when the specified action is Redirect. The destination interfaces for redirect packets. Enter the names of up to five physical interfaces, or click **Select** to open the Interface Selector Dialog Box—VLAN ACL Content, page 67-42. The redirect interfaces must be in the VLAN for which the VACL access map is configured. **Note** You cannot redirect packets to an EtherChannel member or a VLAN interface. You also cannot redirect packets to a subinterface.

Interface Selector Dialog Box—VLAN ACL Content

Use the Interface Selector dialog box to define redirect interfaces when you create entries for a VACL sequence map.

Navigation Path

Open the Create and Edit VLAN ACL Content Dialog Boxes, page 67-41, select **Redirect** as the action, then click **Select** in the Interfaces field.

Related Topics

- Create and Edit VLAN ACL Dialog Boxes, page 67-41
- VLAN Access Lists Page, page 67-39
- Filtering Tables, page 1-48

Field Reference

Table 67-21 Interface Selector Dialog Box

Element	Description
Available Interfaces	Displays the physical interfaces that are defined in the Interfaces/VLANs policy.
Add >> button	Adds interfaces that are selected in the Available Interfaces list to the Selected Interfaces list.
Remove << button	Removes selected interfaces from the Selected Interfaces list.
Selected Interfaces	Displays the interfaces that are selected.

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.

Note 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.

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 67-44
- Deleting EtherChannel VLAN Definitions, page 67-45
- Creating or Editing Data Port VLAN Definitions, page 67-46
- Deleting Data Port VLAN Definitions, page 67-47
- IDSM Settings Page, page 67-47

Related Topics

- VLANs, page 67-25
- Chapter 67, "Managing Cisco Catalyst Switches and Cisco 7600 Series Routers"

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 can have a single definition only for each channel group.
- You can 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.

Related Topics

- Deleting EtherChannel VLAN Definitions, page 67-45
- Creating or Editing Data Port VLAN Definitions, page 67-46
- IDSM Settings, page 67-43

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 67-47.

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 Create and Edit IDSM EtherChannel VLANs Dialog Boxes, page 67-49.

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.

Deleting EtherChannel VLAN Definitions

You can delete an EtherChannel VLAN definition on the IDSM.

Related Topics

- Creating or Editing EtherChannel VLAN Definitions, page 67-44
- Deleting Data Port VLAN Definitions, page 67-47
- IDSM Settings, page 67-43

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 67-47.

Step 2 Click a row in the table to select the VLAN definition to delete.

Step 3 Click **Delete Row**.

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.

Related Topics

- Deleting Data Port VLAN Definitions, page 67-47
- Creating or Editing EtherChannel VLAN Definitions, page 67-44
- IDSM Settings, page 67-43

Step 1 Do one of the following:

- (Device view) Select a Catalyst device, then select **Platform > IDSM Settings** from the Policy selector.
- (Device 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 67-47.

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 Create and Edit IDSM Data Port VLANs Dialog Boxes, page 67-49.

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 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 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.

Deleting Data Port VLAN Definitions

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

Related Topics

- Creating or Editing Data Port VLAN Definitions, page 67-46
- Deleting EtherChannel VLAN Definitions, page 67-45
- IDSM Settings, page 67-43

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 67-47.

Step 2 Click a row in the table to select the VLAN definition to delete.

Step 3 Click **Delete Row**.

IDSM Settings Page

Use the IDSM Settings page to view and configure the VLAN settings for data ports and channel groups on Intrusion Detection System Service Modules (IDSM).

Navigation Path

You can access this page from:

- (Device view) Select **Platform > IDSM Settings** from the Device Policy selector.
- (Policy view) Select **Catalyst Platform > IDSM Settings** from the Policy Types selector.

Related Topics

- Create and Edit IDSM EtherChannel VLANs Dialog Boxes, page 67-49

- Create and Edit IDSM Data Port VLANs Dialog Boxes, page 67-49
- Chapter 46, "Managing Firewall Devices"
- Filtering Tables, page 1-48

Field Reference

Table 67-22 IDSM Settings Page

Element	Description
EtherChannel VLANs table	
Channel Group	Identifies the EtherChannel group to which the Ethernet interface is assigned.
Module Slot-Data Port	Identifies the IDSM service module data port by number (1 or 2) to distinguish between the two ports. Each IDSM service module (blade) has two data ports. You can configure a data port individually or you can assign it to an EtherChannel group. All data ports in a channel group are configured at the group level
Mode	Indicates whether the running mode is trunk (IPS) or capture (IDS).
Capture Enabled	Indicates whether the specified channel group is configured as a capture destination.
Allowed VLANs	Lists which VLANs are allowed for the specified channel group.
Add Row button	Opens the Create IDSM EtherChannel VLANs dialog box. From here you can define which traffic is directed to the data ports in an EtherChannel group and which sensing mode is used.
Edit Row button	Opens the Edit IDSM EtherChannel VLANs dialog box. From here you can modify the attributes of an EtherChannel VLAN definition.
Delete Row button	Deletes the selected VLAN from the IDSM.
Data Port VLANs table	
Module Slot-Data Port	Identifies the IDSM service module data port by number (1 or 2), to distinguish between the two ports.
Mode	Indicates whether the running mode is trunk (IPS) or capture (IDS). To change the mode, select and edit the relevant table row.
Capture Enabled	Indicates whether the specified data port is configured as a capture destination.
Allowed VLANs	Lists which VLANs are allowed for the specified data port.
Add Row button	Opens the Create IDSM Data Port VLANs dialog box. From here you can define which traffic is directed to a specific data port and which sensing mode is used.
Edit Row button	Opens the Edit IDSM Data Port VLANs dialog box. From here you can modify the attributes of a data port VLAN definition.
Delete Row button	Deletes the selected VLAN from the IDSM.

Create and Edit IDSM EtherChannel VLANs Dialog Boxes

Use the Create IDSM EtherChannel VLANs dialog box (or the Edit IDSM EtherChannel VLANs dialog box) to configure or reconfigure the attributes of an IDSM EtherChannel VLAN.

Navigation Path

Go to the IDSM Settings Page, page 67-47, then click the **Add** or **Edit** button beneath the EtherChannel VLANs table.

Related Topics

- Create and Edit IDSM Data Port VLANs Dialog Boxes, page 67-49
- IDSM Slot-Port Selector Dialog Box, page 67-50
- Service Module Slot Selector Dialog Box, page 67-35

Field Reference

Table 67-23 Create and Edit IDSM EtherChannel VLANs Dialog Boxes

Element	Description
Channel Group	The EtherChannel group to which the Ethernet interface is assigned.
Slot-Ports (Select button)	Associates the chassis slot number (in which the relevant services module is installed) with the data port in the format *x* -*y*, where *x* is the slot number and *y* is the port number. For example, 2-1 refers to data port 1 in slot 2. Click **Select** to open the IDSM Slot-Port Selector Dialog Box, page 67-50. From here, you can select the IDSM slot-port combinations to include in the EtherChannel group.
Mode	The running mode of the EtherChannel group: • Capture (IDS)—The IDSM2 passively monitors network traffic that was copied to its data ports by the Catalyst switch using either VACL capture or SPAN. • Trunk (IPS)—The IDSM2 operates as an 802.1Q trunk by performing VLAN bridging between pairs of VLANs within the same data port.
Capture Enabled	Applies only when the running mode is Capture (IDS). When selected, configures the specified channel group as a capture destination. When deselected, the channel group does not act as a capture destination.
VLAN IDs (Select button)	Identifies which VLANs the specified channel group should allow. Click **Select** to open the VLAN Selector Dialog Box, page 67-35. From here, you can select VLANs to include or exclude.

Create and Edit IDSM Data Port VLANs Dialog Boxes

Use the Create IDSM Data Port VLANs dialog box (or the Edit IDSM Data Port VLANs dialog box) to define which traffic is directed to an IDSM data port and which sensing mode is used on that traffic.

Navigation Path

Go to the IDSM Settings Page, page 67-47, then click the **Add** or **Edit** button beneath the Data Port VLANs table.

Related Topics

- Create and Edit IDSM EtherChannel VLANs Dialog Boxes, page 67-49
- IDSM Slot-Port Selector Dialog Box, page 67-50
- Service Module Slot Selector Dialog Box, page 67-35

Field Reference

Table 67-24 Create and Edit IDSM Data Port VLANs Dialog Boxes

Element	Description
Slot-Port	Associates the chassis slot number (in which the relevant services module is installed) with the data port in the format *x* -*y*, where *x* is the slot number and *y* is the port number. For example, 2-1 refers to data port 1 in slot 2. Click **Select** to open the IDSM Slot-Port Selector Dialog Box, page 67-50. From here, you can select the IDSM slot-port combinations to include in the data port VLAN definition.
Mode	The running mode of the data port: • Capture (IDS)—The IDSM2 passively monitors network traffic that was copied to its data ports by the Catalyst switch using either VACL capture or SPAN. • Trunk (IPS)—The IDSM2 operates as an 802.1Q trunk by performing VLAN bridging between pairs of VLANs within the same data port.
Capture Enabled	Applies only when the running mode is Capture (IDS). When selected, configures the specified channel group as a capture destination. When deselected, the channel group does not act as a capture destination.
VLAN IDs (Select button)	Identifies which VLANs the specified data port should allow. Click **Select** to open the VLAN Selector Dialog Box, page 67-35. From here, you can select VLANs to include or exclude.

IDSM Slot-Port Selector Dialog Box

Use the IDSM Slot-Port Selector dialog box to associate slot-port objects with EtherChannel groups.

Navigation Path

Go to the Create and Edit IDSM EtherChannel VLANs Dialog Boxes, page 67-49 or the Create and Edit IDSM Data Port VLANs Dialog Boxes, page 67-49, then click **Select** in the Slot-Port field.

Related Topics

- VLAN Selector Dialog Box, page 67-35
- Filtering Tables, page 1-48

Field Reference

Table 67-25 IDSM Slot-Port Selector Dialog Box

Element	Description
Available IDSM Slot-Ports list	Displays the available slot-port definitions.
Add >> button	Applies only when selecting slot-ports for EtherChannel VLANs. Adds IDSM slot-port objects that you selected in the Available IDSM Slot-Ports list to the Selected IDSM Slot-Ports list.
Remove << button	Applies only when selecting slot-ports for EtherChannel VLANs. Removes selected IDSM slot-port objects from the Selected IDSM Slot-Ports list.
Selected IDSM Slot-Ports list	Displays the IDSM slot-port objects that are selected for an association with a data port or an EtherChannel group.