APPENDIX K

Router Platform User Interface Reference

The main pages available in Cisco Security Manager for configuring and managing platform-specific policies on Cisco IOS routers are discussed in the following topics:

NAT policies:

- NAT Policy Page, page K-3

Interface policies:

- Router Interfaces Page, page K-17
- Never Block Networks Dialog Box, page N-132
- AIM-IPS Interface Settings Page, page K-34
- Dialer Policy Page, page K-36
- ADSL Policy Page, page K-42
- SHDSL Policy Page, page K-47
- PVC Policy Page, page K-54
- PPP/MLP Policy Page, page K-76

Device Admin policies:

- AAA Policy Page, page K-87
- Accounts and Credential s Policy Page, page K-98
- Bridging Policy Page, page K-102
- Clock Policy Page, page K-104

- CPU Policy Page, page K-107
- Device Access policies:
  - HTTP Policy Page, page K-110
  - Console Policy Page, page K-117
  - VTY Policy Page, page K-129
  - Secure Shell Policy Page, page K-147
  - SNMP Policy Page, page K-149
- DNS Policy Page, page K-158
- Hostname Policy Page, page K-160
- Memory Policy Page, page K-161
- Secure Device Provisioning Policy Page, page K-163
- Server Access policies:
  - DHCP Policy Page, page K-167
  - NTP Policy Page, page K-174

Identity policies:

- 802.1x Policy Page, page K-179
- Network Admission Control Policy Page, page K-183

Logging policies:

- Logging Setup Policy Page, page K-192
- Syslog Servers Policy Page, page K-197

Quality of Service policies:

- Quality of Service Policy Page, page K-199

Routing policies:

- BGP Routing Policy Page, page K-219
- EIGRP Routing Policy Page, page K-226
- OSPF Interface Policy Page, page K-236
- OSPF Process Policy Page, page K-243
- RIP Routing Policy Page, page K-255
- Static Routing Policy Page, page K-263

Tip Use the Policy Management page in the Security Manager Administration window to control which router platform policy pages are available in Security Manager. For more information, see Policy Management Page, page A-40.

NAT Policy Page

You can configure NAT policies on a Cisco IOS router from the following tabs on the NAT policy page:

- NAT Page—Interface Specification Tab, page K-3
- NAT Page—Static Rules Tab, page K-6
- NAT Page—Dynamic Rules Tab, page K-12
- NAT Page—Timeouts Tab, page K-15

Network Address Translation (NAT) converts private, internal LAN addresses into globally routable IP addresses. NAT enables a small number of public IP addresses to provide global connectivity for a large number of hosts.

For more information, see NAT on Cisco IOS Routers, page 15-5.

Navigation Path

- (Device view) Select **NAT** from the Policy selector.
- (Policy view) Select **NAT (Router)** from the Policy Type selector. Right-click **NAT (Router)** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- Chapter K, "Router Platform User Interface Reference"

NAT Page—Interface Specification Tab

Use the NAT Interface Specification tab to define the inside and outside interfaces on the router used for NAT. Inside interfaces are interfaces that connect to the private networks served by the router. Outside interfaces are interfaces that connect to the WAN or the Internet.

Navigation Path

Go to the NAT Policy Page, page K-3, then click the **Interface Specification** tab.

Related Topics

- NAT Page—Static Rules Tab, page K-6
- NAT Page—Dynamic Rules Tab, page K-12
- NAT Page—Timeouts Tab, page K-15

Field Reference

Table K-1 NAT Interface Specification Tab

Element	Description
NAT Inside Interfaces	The interfaces that act as the inside interfaces for address translation. Click **Edit** to display the Edit Interfaces Dialog Box—NAT Inside Interfaces, page K-4. From here you can define these interfaces.
NAT Outside Interfaces	The interfaces that act as the outside interfaces for address translation. Click **Edit** to display the Edit Interfaces Dialog Box—NAT Outside Interfaces, page K-5. From here you can define these interfaces.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.

Edit Interfaces Dialog Box—NAT Inside Interfaces

When you configure a translation rules policy on a Cisco IOS router, use the Edit Interfaces dialog box to specify which interfaces will act as the inside interfaces for address translation. Inside interfaces typically connect to a LAN that the router serves.

Navigation Path

Go to the NAT Page—Interface Specification Tab, page K-3, then click the **Edit** button in the NAT Inside Interfaces field.

Related Topics

- Designating Inside and Outside Interfaces, page 15-6
- Edit Interfaces Dialog Box—NAT Outside Interfaces, page K-5

Field Reference

Table K-2 Edit Interfaces Dialog Box—NAT Inside Interfaces

Element	Description
Interfaces	The interfaces that act as the inside interfaces for address translation. You can enter interfaces, interface roles, or both. For more information, see Specifying Interfaces During Policy Definition, page 9-135.
Select button	Opens an Object Selectors, page F-593 for selecting interfaces and interface roles. Using the selector eliminates the need to manually enter this information. If the interface role you want is not listed, click the **Create** button in the selector to display the Interface Role Dialog Box, page F-464. From here you can define an interface role object.
OK button	Saves your changes and closes the dialog box. Your selections are displayed in the NAT Inside Interfaces field of the NAT Interface Specification tab.

Edit Interfaces Dialog Box—NAT Outside Interfaces

When you configure a translation rules policy on a Cisco IOS router, use the Edit Interfaces dialog box to specify which interfaces will act as the outside interfaces for address translation. Outside interfaces typically connect to your organization's WAN or to the Internet.

Navigation Path

Go to the NAT Page—Interface Specification Tab, page K-3, then click the **Edit** button in the NAT Outside Interfaces field.

Related Topics

- Designating Inside and Outside Interfaces, page 15-6
- Edit Interfaces Dialog Box—NAT Inside Interfaces, page K-4

Field Reference

Table K-3 Edit Interfaces Dialog Box—NAT Outside Interfaces

Element	Description
Interfaces	The interfaces that act as the outside interfaces for address translation. You can enter interfaces, interface roles, or both. For more information, see Specifying Interfaces During Policy Definition, page 9-135.
Select button	Opens an Object Selectors, page F-593 for selecting interfaces and interface roles. Using the selector eliminates the need to manually enter this information. If the interface role you want is not listed, click the **Create** button in the selector to display the Interface Role Dialog Box, page F-464. From here you can define an interface role object.
OK button	Saves your changes and closes the dialog box. Your selections are displayed in the NAT Outside Interfaces field of the NAT Interface Specification tab.

NAT Page—Static Rules Tab

Use the NAT Static Rules tab to create, edit, and delete static address translation rules. For more information, see Defining Static NAT Rules, page 15-8.

Navigation Path

Go to the NAT Policy Page, page K-3, then click the **Static Rules** tab.

Related Topics

- NAT Page—Interface Specification Tab, page K-3
- NAT Page—Dynamic Rules Tab, page K-12
- NAT Page—Timeouts Tab, page K-15

Field Reference

Table K-4 NAT Static Rules Tab

Element	Description
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
Original Address	The original address (and optionally, the subnet mask) that is being translated.
Translated Address	The IP address to which the traffic is translated.
Port Redirection	(When the static rule is defined on a port) Information about the port that is being translated, including the local and global port numbers.
Advanced	The advanced options that are enabled.
Add button	Opens the NAT Static Rule Dialog Box, page K-7. From here you can create a static translation rule.
Edit button	Opens the NAT Static Rule Dialog Box, page K-7. From here you can edit the selected static translation rule.
Delete button	Deletes the selected static translation rules from the table.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** icon on the toolbar.

Tip To choose which columns to display in the table, right-click a column header, then select **Show Columns**. For more information about table display options, see Table Columns and Column Heading Features, page 3-26.

NAT Static Rule Dialog Box

Use the NAT Static Rule dialog box to add or edit static address translation rules.

Navigation Path

Go to the NAT Page—Static Rules Tab, page K-6, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Defining Static NAT Rules, page 15-8
- Disabling the Alias Option for Attached Subnets, page 15-15
- Disabling the Payload Option for Overlapping Networks, page 15-15
- Basic Interface Settings on Cisco IOS Routers, page 15-20
- Understanding Interface Role Objects, page 9-132

Field Reference

Table K-5 NAT Static Rule Dialog Box

Element	Description
Static Rule Type	The type of local address requiring translation by this static rule: • Static Host—A single host requiring static address translation. • Static Network—A subnet requiring static address translation. • Static Port—A single port requiring static address translation. If you select this option, you must define port redirection parameters.
Original Address	Enter an address or the name of a network/host object, or click **Select** to display an Object Selectors, page F-593. • When Static Network is selected as the Static Rule Type, this field defines the network address and subnet mask. For example, if you want to create n-to-n mappings between the private addresses in a subnet to corresponding inside global addresses, enter the address of the subnet you want translated, and then enter the network mask in the Mask field. • When Static Port or Static Host is selected as the Static Rule Type, this field defines the IP address only. For example, if you want to create a one-to-one mapping for a single host, enter the IP address of the host to translate. Do not enter a subnet mask in the Mask field. If the network or host you want is not listed, click the **Create** button in the selector to display the Network/Host Dialog Box, page F-477. From here you can define a network/host object. **Note** We recommend not entering a local address belonging to this router, as it could cause Security Manager management traffic to be translated. Translating this traffic will cause a loss of communication between the router and Security Manager.

Table K-5 NAT Static Rule Dialog Box (Continued)

Translated Address	The type of address translation to perform: • Specify IP—The IP address that acts as the translated address. Enter an address or the name of a network/host object in the Translated IP/Network field, or click **Select** to display an Object Selectors, page F-593. – If you selected Static Port or Static Host as the static rule type (to create a one-to-one mapping between a single inside local address and a single inside global address), enter the global address in this field. A subnet mask is not required. – If you selected Static Network as the static rule type (to map the original, local addresses of a subnet to the corresponding global addresses), enter the IP address that you want to use in the translation in this field. The network mask is taken automatically from the mask entered in the Original Address field. If the network or host you want is not listed, click the **Create** button in the selector to display the Network/Host Dialog Box, page F-477. From here you can define a network/host object. • Use Interface IP—The interface whose address should be used as the translated address. (This is typically the interface from which translated packets leave the router.) Enter the name of an interface or interface role in the Interface field, or click **Select** to display an Object Selectors, page F-593. If the interface role you want is not listed, click the **Create** button or the **Edit** button in the selector to display the Interface Role Dialog Box, page F-464. From here you can create an interface role object. **Note** The Interface option is not available when Static Network is the selected static rule type. Only one static rule may be defined per interface.

Table K-5 NAT Static Rule Dialog Box (Continued)

Port Redirection	Applies only when Static Port is the selected static rule type. Redirect Port—When selected, specifies port information for the inside device in the translation. This enables you to use the same public IP address for multiple devices as long as the port specified for each device is different. Enter information in the following fields: • Protocol—The protocol type: TCP or UDP. • Local Port—The port number on the source network. Valid values range from 1 to 65535. • Global Port—The port number on the destination network that the router is to use for this translation. Valid values range from 1 to 65535. When deselected, port information is not included in the translation.

Table K-5 NAT Static Rule Dialog Box (Continued)

Advanced	Applies only when using the Translated IP option for address translation. Defines advanced options: • No Alias—When selected, prohibits an alias from being created for the global address. The alias option is used to answer Address Resolution Protocol (ARP) requests for global addresses that are allocated by NAT. You can disable this feature for static entries by selecting the No alias check box. When deselected, global address aliases are permitted. • No Payload—When selected, prohibits an embedded address or port in the payload from being translated. The payload option performs NAT between devices on overlapping networks that share the same IP address. When an outside device sends a DNS query to reach an inside device, the local address inside the payload of the DNS reply is translated to a global address according to the relevant NAT rule. You can disable this feature by selecting the No payload check box. When deselected, embedded addresses and ports in the payload may be translated, as described above. • Create Extended Translation Entry—When selected, creates an extended translation entry (addresses and ports). This enables you to associate multiple global addresses with a single local address. This is the default. When deselected, creates a simple translation entry that allows you to associate a single global address with the local address.
OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

NAT Page—Dynamic Rules Tab

Use the NAT Dynamic Rules tab to create, edit, and delete dynamic address translation rules. A dynamic address translation rule dynamically maps hosts to addresses, using either the globally registered IP address of a specific interface or addresses included in an address pool that are globally unique in the destination network.

For more information, see Defining Dynamic NAT Rules, page 15-16.

Navigation Path

Go to the NAT Policy Page, page K-3, then click the **Dynamic Rules** tab.

Related Topics

- NAT Page—Interface Specification Tab, page K-3
- NAT Page—Static Rules Tab, page K-6
- NAT Page—Timeouts Tab, page K-15

Field Reference

Table K-6 NAT Dynamic Rules Tab

Element	Description
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
Traffic Flow	The ACL that defines the traffic that is being translated.
Translated Address	Indicates whether the translated address is based on an interface or on a defined address pool.
Port Translation	Indicates whether Port Address Translation (PAT) is being used by this dynamic NAT rule.
Add button	Opens the NAT Dynamic Rule Dialog Box, page K-13. From here you can create a dynamic translation rule.
Edit button	Opens the NAT Dynamic Rule Dialog Box, page K-13. From here you can edit the selected dynamic translation rule.
Delete button	Deletes the selected dynamic translation rules from the table.

Table K-6 NAT Dynamic Rules Tab (Continued)

Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** icon on the toolbar.

Tip To choose which columns to display in the table, right-click a column header, then select **Show Columns**. For more information about table display options, see Table Columns and Column Heading Features, page 3-26.

NAT Dynamic Rule Dialog Box

Use the NAT Dynamic Rule dialog box to add or edit dynamic address translation rules.

Navigation Path

Go to the NAT Page—Dynamic Rules Tab, page K-12, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Defining Dynamic NAT Rules, page 15-16
- Understanding Access Control List Objects, page 9-30
- Basic Interface Settings on Cisco IOS Routers, page 15-20
- Understanding Interface Role Objects, page 9-132

Field Reference

Table K-7 NAT Dynamic Rule Dialog Box

Element	Description
Traffic Flow	Access List—The extended ACL that specifies the traffic requiring dynamic translation. Enter the name of an ACL object, or click **Select** to display an Object Selectors, page F-593. If the ACL you want is not listed, click the **Create** button in the selector to display the dialog box for defining an extended ACL object. For more information, see Add and Edit Extended Access List Pages, page F-34. **Note** Make sure that the ACL you select does not permit the translation of Security Manager management traffic over any device address on this router. Translating this traffic will cause a loss of communication between the router and Security Manager.
Translated Address	The method for performing dynamic address translation: • Interface—The router interface used for address translation. PAT is used to distinguish each host on the network. Enter the name of an interface or interface role, or click **Select** to display an Object Selectors, page F-593. If the interface role you want is not listed, click the **Create** button in the selector to display the Interface Role Dialog Box, page F-464. From here you can create an interface role object. • Address Pool—Translates addresses using a set of addresses defined in an address pool. Enter one or more address ranges, including the prefix, using the format min1-max1/prefix (in CIDR notation). You can add as many address ranges to the address pool as required, but all ranges must share the same prefix. Separate multiple entries with commas.
Enable Port Translation (Overload)	When selected, the router uses port addressing (PAT) if the pool of available addresses runs out. When deselected, PAT is not used. **Note** PAT is selected by default when you use an interface on the router as the translated address.

Table K-7 NAT Dynamic Rule Dialog Box (Continued)

Do Not Translate VPN Traffic (Site-to-Site VPN only)	This setting applies only in situations where the NAT ACL overlaps the crypto ACL used by the site-to-site VPN. Because the interface performs NAT first, any traffic arriving from an address within this overlap would get translated, causing the traffic to be sent unencrypted. Leaving this check box selected prevents that from happening. When selected, address translation is not performed on VPN traffic. When deselected, the router performs address translation on VPN traffic in cases of overlapping addresses between the NAT ACL and the crypto ACL. **Note** We recommend that you leave this check box selected, even when performing NAT into IPsec, as this setting does not interfere with the translation that is performed to avoid a clash between two networks sharing the same set of internal addresses. **Note** This option does not apply to remote access VPNs.
OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

NAT Page—Timeouts Tab

Use the NAT Timeouts tab to view or modify the default timeout values for PAT (overload) translations. These timeouts cause a dynamic translation to expire after a defined period of non-use. In addition, you can use this page to place a limit on the number of entries allowed in the dynamic NAT table and to modify the default timeout on all dynamic translations that are not PAT translations.

Note For more information about the Overload feature, see NAT Dynamic Rule Dialog Box, page K-13.

Navigation Path

Go to the NAT Policy Page, page K-3, then click the **Timeouts** tab.

Related Topics

- Specifying NAT Timeouts, page 15-19
- NAT Page—Interface Specification Tab, page K-3
- NAT Page—Static Rules Tab, page K-6
- NAT Page—Dynamic Rules Tab, page K-12

Field Reference

Table K-8 NAT Timeouts Tab

Element	Description
Max Entries	The maximum number of entries allowed in the dynamic NAT table. Values range from 1 to 2147483647. By default, this field is left blank, which means that the number of entries in the table is unlimited.
Timeout (sec.)	The timeout value applied to all dynamic translations except PAT (overload) translations. The default is 86400 seconds (24 hours).
UDP Timeout (sec.)	The timeout value applied to User Datagram Protocol (UDP) ports. The default is 300 seconds (5 minutes). **Note** This value applies only when the Overload feature is enabled.
DNS Timeout (sec.)	The timeout value applied to Domain Naming System (DNS) server connections. The default is 60 seconds. **Note** This value applies only when the Overload feature is enabled.
TCP Timeout (sec.)	The timeout value applied to Transmission Control Protocol (TCP) ports. The default is 86400 seconds (24 hours). **Note** This value applies only when the Overload feature is enabled.
FINRST Timeout (sec.)	The timeout value applied when a Finish (FIN) packet or Reset (RST) packet (both of which terminate connections) is found in the TCP stream. The default is 60 seconds. **Note** This value applies only when the Overload feature is enabled.

Table K-8 NAT Timeouts Tab (Continued)

ICMP Timeout (sec.)	The timeout value applied to Internet Control Message Protocol (ICMP) flows. The default is 60 seconds. **Note** This value applies only when the Overload feature is enabled.
PPTP Timeout (sec.)	The timeout value applied to NAT Point-to-Point Tunneling Protocol (PPTP) flows. The default is 86400 seconds (24 hours). **Note** This value applies only when the Overload feature is enabled.
SYN Timeout (sec.)	The timeout value applied to TCP flows after a synchronous transmission (SYN) message (used for precise clocking) is encountered. The default is 60 seconds. **Note** This value applies only when the Overload feature is enabled.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.

Router Interfaces Page

Use the Router Interfaces page to view, create, edit, and delete interface definitions (physical and virtual) on a selected Cisco IOS router. The Router Interfaces page displays interfaces that were discovered by Security Manager as well as interfaces added manually after you added the device to the system.

For more information, see Basic Interface Settings on Cisco IOS Routers, page 15-20.

Navigation Path

Select a Cisco IOS router from the Device selector, then select **Interfaces > Interfaces** from the Policy selector.

Related Topics

- Available Interface Types, page 15-21
- Deleting a Cisco IOS Router Interface, page 15-27

Field Reference

Table K-9 Router Interfaces Page

Element	Description
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
Interface Type	The interface type. Subinterfaces are displayed indented beneath their parent interface.
Interface Name	The name of the interface.
Enabled	Indicates whether the interface is currently enabled (managed by Security Manager) or disabled (shutdown state).
IP Address	The IP address of interfaces defined with a static address.
IP Address Type	The type of IP address assigned to the interface—static, DHCP, PPPoE, or unnumbered. (IP address is defined by a selected interface role.)
Interface Role	The interface roles that are assigned to the selected interface.
Add button	Opens the Create Router Interface Dialog Box, page K-18. From here you can create an interface on the selected router.
Edit button	Opens the Create Router Interface Dialog Box, page K-18. From here you can edit the selected interface.
Delete button	Deletes the selected interfaces from the table.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.

Tip To choose which columns to display in the table, right-click a column header, then select **Show Columns**. For more information about table display options, see Table Columns and Column Heading Features, page 3-26.

Create Router Interface Dialog Box

Use the Create Router Interface dialog box to create and edit physical and virtual interfaces on the selected Cisco IOS router.

Note Unlike other router policies, the Interfaces policy cannot be shared among multiple devices. The Advanced Settings policy, however, may be shared. See Local Policies vs. Shared Policies, page 7-4.

Navigation Path

Go to the Router Interfaces Page, page K-17, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Basic Interface Settings on Cisco IOS Routers, page 15-20
- Deleting a Cisco IOS Router Interface, page 15-27
- Never Block Networks Dialog Box, page N-132

Field Reference

Table K-10 Create Router Interface Dialog Box

Element	Description
Enabled	When selected, the router interface is enabled. When deselected, the router interface is in shutdown state. However, its definition is not deleted.
Type	Specifies whether you are defining an interface or subinterface.
Name	Applies only to interfaces. The name of the interface. Enter a name manually, or click **Select** to display a dialog box for generating a name automatically. See Interface Auto Name Generator Dialog Box, page K-24. **Note** Logical interfaces require a number after the name: —The valid range for dialer interfaces is 0-799. —The valid range for loopback interfaces is 0-2147483647. —The valid range for BVI interfaces is 1-255. —The only valid value for null interfaces is 0.
Parent	Applies only to subinterfaces. The parent interface of the subinterface. Select the parent interface from the displayed list.

Table K-10 Create Router Interface Dialog Box (Continued)

Subinterface ID	Applies only to subinterfaces. The ID number of the subinterface.
IP	The source of the IP address for the interface: • Static IP—Defines a static IP address and subnet mask for the interface. Enter this information in the fields that appear below the option. **Note** You can define the mask using either dotted decimal (for example, 255.255.255.255) or CIDR notation (/32). See Contiguous and Discontiguous Network Masks, page 9-146. • DHCP—The interface obtains its IP address dynamically from a DHCP server. • PPPoE—The router automatically negotiates its own registered IP address from a central server (via PPP/IPCP). The following interface types support PPPoE: – Async – Serial – High-Speed Serial Interface (HSSI) – Dialer – BRI, PRI (ISDN) – Virtual template – Multilink • Unnumbered—The interface obtains its IP address from a different interface on the device. Choose an interface from the Interface list. This option can be used with point-to-point interfaces only. **Note** Layer 2 interfaces do not support IP addresses. Deployment fails if you define an IP address on a Layer 2 interface.

Table K-10 Create Router Interface Dialog Box (Continued)

Layer Type	The OSI layer at which the interface is defined: • Unknown—The layer is unknown. • Layer 2—The data link layer, which contains the protocols that control the physical layer (Layer 1) and how data is framed before being transmitted on the medium. Layer 2 is used for bridging and switching. Layer 2 interfaces do not have IP addresses. • Layer 3—The network layer, which is primarily responsible for the routing of data in packets across logical internetwork paths. This routing is accomplished through the use of IP addresses.
Duplex	The interface transmission mode: • None—The transmission mode is returned to its device-specific default setting. • Full—The interface transmits and receives at the same time (full duplex). • Half—The interface can transmit or receive, but not at the same time (half duplex). This is the default. • Auto—The router automatically detects and sets the appropriate transmission mode, either full or half duplex. **Note** When using Auto mode, be sure that the port on the active network device to which you connect this interface is also set to automatically negotiate the transmission mode. Otherwise, select the appropriate fixed mode. **Note** You can configure a duplex value only if you set the Speed to a fixed speed, not Auto. **Note** This setting does not apply to serial, HSSI, ATM, PRI, DSL, tunnel, or loopback interfaces.

Table K-10 Create Router Interface Dialog Box (Continued)

Speed	Applies only to Fast Ethernet and Gigabit Ethernet interfaces. The speed of the interface: • 10—10 megabits per second (10Base-T networks). • 100—100 megabits per second (100Base-T networks). This is the default for Fast Ethernet interfaces. • 1000—1000 megabits per second (Gigabit Ethernet networks). This is the default for Gigabit Ethernet interfaces. • Auto—The router automatically detects and sets appropriate interface speed. **Note** When using Auto mode, be sure that the port on the active network device to which you connect this interface is also set to automatically negotiate the transmission speed. Otherwise, select the appropriate fixed speed.
MTU	The maximum transmission unit, which refers to the maximum packet size, in bytes, that this interface can handle. Valid values for serial, Ethernet, and Fast Ethernet interfaces range from 64 to 17940 bytes. Valid values for Gigabit Ethernet interfaces range from 1500 to 9216 bytes.
Encapsulation	The type of encapsulation performed by the interface: • None—No encapsulation. • DOT1Q—VLAN encapsulation, as defined by the IEEE 802.1Q standard. Applies only to Ethernet subinterfaces. • Frame Relay—IETF Frame Relay encapsulation. Applies only to serial interfaces (not serial subinterfaces). **Note** IETF Frame Relay encapsulation provides interoperability between a Cisco IOS router and equipment from other vendors. To configure Cisco Frame Relay encapsulation, use CLI commands or FlexConfigs.

Table K-10 Create Router Interface Dialog Box (Continued)

VLAN ID	Applies only to subinterfaces with encapsulation type DOT1Q. The VLAN ID associated with this subinterface. The VLAN ID specifies where 802.1Q tagged packets are sent and received on this subinterface; without a VLAN ID, the subinterface cannot send or receive traffic. 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. See Understanding FlexConfig Objects, page 9-52. Configuring VLANs on the main interface increases the number of VLANs that can be configured on the router.
Native VLAN	Applies only when the encapsulation type is DOT1Q and you are configuring a physical interface that is meant to serve as an 802.1Q trunk interface. Trunking is a way to carry traffic from several VLANs over a point-to-point link between two devices. When selected, the Native VLAN is associated 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.) The native VLAN is the VLAN to which all untagged VLAN packets are logically assigned by default. This includes the management traffic associated with the VLAN. If no VLAN ID is defined, the default is 1. For example, if the VLAN ID of this interface is 1, all incoming untagged packets and packets with VLAN ID 1 are received on the main interface and not on a subinterface. Packets sent from the main interface are transmitted without an 802.1Q tag. 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.

Table K-10 Create Router Interface Dialog Box (Continued)

DLCI	Applies only to serial subinterfaces with Frame Relay encapsulation. Enter the data-link connection identifier to associate with the subinterface. Valid values range from 16 to 1007. **Note** Security Manager configures serial subinterfaces as point-to-point not multipoint.
Description	Additional information about the interface (up to 1024 characters).
Roles	The interface roles assigned to this interface. A message is displayed if no roles have yet been assigned.
OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

Interface Auto Name Generator Dialog Box

Use the Interface Auto Name Generator dialog box to have Security Manager generate a name for the interface based on the interface type and its location in the router.

Navigation Path

Go to the Create Router Interface Dialog Box, page K-18, select **Interface** from the Type list, then click **Select** in the Name field**.**

Related Topics

- Generating an Interface Name, page 15-26
- Router Interfaces Page, page K-17
- Basic Interface Settings on Cisco IOS Routers, page 15-20

Field Reference

Table K-11 Interface Auto Name Generator Dialog Box

Element	Description
Type	The type of interface. Your selection from this list forms the first part of the generated name, as displayed in the Result field. For more information, see Table 15-1 on page 15-21.
Card	The card related to the interface. **Note** When defining a BVI interface, enter the number of the corresponding bridge group.
Slot	The slot related to the interface.
Port	The port related to the interface. **Note** The information you enter in these fields forms the remainder of the generated name, as displayed in the Result field.
Result	The name generated by Security Manager from the information you entered for the interface type and location. The name displayed in this field is read-only. **Tip** After closing this dialog box, you can edit the generated name in the Create Router Interface dialog box, if required.
OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

Advanced Interface Settings Page

Use the Advanced Interface Settings page to view, create, edit, and delete advanced interface definitions (physical and virtual) on a selected Cisco IOS router. Examples of advanced settings include Cisco Discovery Protocol (CDP) settings, ICMP message settings, and virtual fragment reassembly settings.

For more information, see Advanced Interface Settings on Cisco IOS Routers, page 15-28.

Navigation Path

- (Device view) Select **Interfaces > Settings > Advanced Settings** from the Policy selector.
- (Policy view) Select **Router Interfaces > Settings > Advanced Settings** from the Policy Type selector. Right-click **Advanced Settings** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- Router Interfaces Page, page K-17
- Available Interface Types, page 15-21
- Deleting a Cisco IOS Router Interface, page 15-27

Field Reference

Table K-12 Advanced Interface Settings Page

Element	Description
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
Interface	The interface or interface role for which advanced settings are defined.
Max Bandwidth	The bandwidth value to communicate to higher-level protocols in kilobits per second (kbps).
Load Interval	The length of time used to calculate the average load for this interface.
CDP	Indicates whether CDP and CDP logging are enabled on this interface.
Redirects	Indicates whether ICMP redirect messages are enabled on this interface.
Unreachables	Indicates whether ICMP unreachable messages are enabled on this interface.
Mask Reply	Indicates whether ICMP mask reply messages are enabled on this interface.
Directed Broadcasts	Indicates whether directed broadcasts that are intended for the subnet to which this interface is attached are exploded as broadcasts on that subnet.
Add button	Opens the Advanced Interface Settings Dialog Box, page K-27. From here you can define advanced settings on the selected interface.
Edit button	Opens the Advanced Interface Settings Dialog Box, page K-27. From here you can edit the selected interface.
Delete button	Deletes the selected advanced interface definitions from the table.

Table K-12 Advanced Interface Settings Page (Continued)

Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.

Tip To choose which columns to display in the table, right-click a column header, then select **Show Columns**. For more information about table display options, see Table Columns and Column Heading Features, page 3-26.

Advanced Interface Settings Dialog Box

Use the Advanced Interface Settings dialog box to define a variety of advanced settings on a selected interface, including:

- Cisco Discovery Protocol (CDP) settings.
- Internet Control Message Protocol (ICMP) settings.
- Virtual fragmentation reassembly (VFR) settings.
- Directed broadcast settings.
- Load interval for determining the average load.
- Enabling proxy ARP.
- Enabling NBAR protocol discovery.

Navigation Path

Go to the Never Block Networks Dialog Box, page N-132, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Basic Interface Settings on Cisco IOS Routers, page 15-20
- Advanced Interface Settings on Cisco IOS Routers, page 15-28
- Deleting a Cisco IOS Router Interface, page 15-27
- Available Interface Types, page 15-21

Field Reference

Table K-13 Advanced Interface Settings Dialog Box

Element	Description
Interface	The interface on which the advanced settings are defined. Enter the name of an interface or interface role, or click **Select** to display an Object Selectors, page F-593. If the interface role you want is not listed, click the **Create** button in the selector to display the Interface Role Dialog Box, page F-464. From here you can create an interface role object. **Note** You can define only one set of advanced settings per interface. **Note** The only advanced settings supported on Layer 2 interfaces are Max. Bandwidth, Load Interval, and CDP.
Max Bandwidth	The bandwidth value to communicate to higher-level protocols in kilobits per second (kbps). **Note** The value you define in this field is an informational parameter only; it does not affect the physical interface.
Load Interval	The length of time, in seconds, used to calculate the average load on the interface. Valid values range from 30 to 600 seconds, in multiples of 30 seconds. The default is 300 seconds (5 minutes). Modify the default to shorten the length of time over which load averages are computed. You can do this if you want load computations to be more reactive to short bursts of traffic. Load data is gathered every 5 seconds. This data is used to compute load statistics, including input/output rate in bits and packets per second, load, and reliability. Load data is computed using a weighted-average calculation in which recent load data has more weight in the computation than older load data. **Tip** You can use this option to increase or decrease the likelihood of activating a backup interface; for example, a backup dial interface may be triggered by a sudden spike in the load on an active interface. **Note** Load interval is not supported on subinterfaces.

Table K-13 Advanced Interface Settings Dialog Box (Continued)

TCP Maximum Segment Size	The maximum segment size (MSS) of TCP SYN packets that pass through this interface. Valid values range from 500 to 1460 bytes. If you do not specify a value, the MSS is determined by the originating host. This option helps prevent TCP sessions from being dropped as they pass through the router. Use this option when the ICMP messages that perform auto-negotiation of TCP frame size are blocked (for example, by a firewall). We highly recommend using this option on the tunnel interfaces of DMVPN networks. For more information, see *TCP MSS Adjustment* at this URL: http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a00804247fc.html **Note** Typically, the optimum MSS is 1452 bytes. This value plus the 20-byte IP header, the 20-byte TCP header, and the 8-byte PPPoE header add up to a 1500-byte packet that matches the MTU size for the Ethernet link.
Helper Addresses	The helper addresses that are used to forward User Datagram Protocol (UDP) broadcasts that are received on this interface. Enter one or more addresses or network/host objects, or click **Select** to display an Object Selectors, page F-593. If the network you want is not listed, click the **Create** button in the selector to display the Network/Host Dialog Box, page F-477. From here, you can define a network/host object. By default, routers do not forward broadcasts outside of their subnet. Helper addresses provide a solution by enabling the router to forward certain types of UDP broadcasts as a unicast to an address on the destination subnet. For more information, see Understanding Helper Addresses, page 15-29.

Table K-13 Advanced Interface Settings Dialog Box (Continued)

Cisco Discovery Protocol settings	
Enable CDP	When selected, the Cisco Discovery Protocol (CDP) is enabled on this interface. This the default. When deselected, CDP is disabled on this interface. CDP is a media- and protocol-independent device-discovery protocol that runs on all Cisco-manufactured equipment including routers, access servers, bridges, and switches. It is primarily used to obtain protocol addresses of neighboring devices and discover the platform of those devices. **Note** ATM interfaces do not support CDP.
Log CDP Messages	Applies only to Ethernet interfaces. When selected, duplex mismatches for this interface are displayed in a log. This is the default. When deselected, duplex mismatches for this interface are not logged.
NetFlow settings	
Enable Ingress Accounting	When selected, NetFlow accounting is enabled on traffic arriving on this interface. When deselected, NetFlow accounting on arriving traffic is disabled. This is the default. Cisco IOS NetFlow provides the metering base for a key set of applications including network traffic accounting, usage-based network billing, network planning, as well as Denial Services monitoring capabilities, network monitoring, outbound marketing, and data mining capabilities for both service provider and enterprise customers. **Note** You must use the CLI or FlexConfigs to enable Cisco Express Forwarding (CEF) or distributed CEF (dCEF) before using this option.
Enable Egress Accounting	When selected, enables NetFlow accounting on traffic leaving this interface. When deselected, disables NetFlow accounting on traffic leaving this interface. This is the default. **Note** You must use the CLI or FlexConfigs to enable Cisco Express Forwarding (CEF) or distributed CEF (dCEF) before using this option.

Table K-13 Advanced Interface Settings Dialog Box (Continued)

ICMP Messages settings	
Enable Redirect Messages	When selected, enables the sending of Internet Control Message Protocol (ICMP) redirect messages if the device is forced to resend a packet through the same interface on which it was received to another device on the same subnet. This is the default. When deselected, disabled redirect messages. Redirect messages are sent when the device wants to instruct the originator of the packet to remove it from the route and substitute a different device that offers a more direct path to the destination.
Enable Unreachable Messages	When selected, enables the sending of ICMP unreachable messages. This is the default. When deselected, disables unreachable messages. Unreachable messages are sent in two circumstances: • If the interface receives a nonbroadcast packet destined for itself that uses an unknown protocol. In this case, it sends an ICMP unreachable message to the source. • If the device receives a packet that it cannot deliver to its ultimate destination because it knows of no route to the destination address. In this case, it sends an ICMP host unreachable message to the originator of the packet. **Note** This is the only advanced setting supported by the null0 interface.
Enable Mask Reply Messages	When selected, enables the sending of ICMP mask reply messages. When deselected, disables mask reply messages. This is the default. Mask reply messages are sent in response to mask request messages, which are sent when a device needs to know the subnet mask for a particular subnetwork.

Table K-13 Advanced Interface Settings Dialog Box (Continued)

Additional settings	
Enable Virtual Fragment Reassembly (VFR)	When selected, virtual fragmentation reassembly (VFR) is enabled on this interface. When deselected, disables VFR. This is the default. VFR is a feature that enables the Cisco IOS Firewall to create dynamic ACLs that can protect the network from various fragmentation attacks. For more information, see *Virtual Fragmentation Reassembly* at this URL: http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_virt_frag_reassm_ps6441_TSD_Products_Configuration_Guide_Chapter.html
Enable Proxy ARP	When selected, enables proxy Address Resolution Protocol (ARP) on the interface. This is the default. When deselected, disables proxy ARP. Proxy ARP, defined in RFC 1027, is the technique in which one host, usually a router, answers ARP requests intended for another machine, thereby accepting responsibility for routing packets to the real destination. Proxy ARP can help machines on a subnet reach remote subnets without configuring routing or a default gateway.
Enable NBAR Protocol Discovery	When selected, enables network-based application recognition (NBAR) on this interface to discover traffic and keep traffic statistics for all protocols known to NBAR. When deselected, disables NBAR. This is the default. Protocol discovery provides a method to discover application protocols traversing an interface so that QoS policies can be developed and applied to them. For more information, go to: http://www.cisco.com/en/US/products/ps6616/products_qanda_item09186a00800a3ded.shtml

Table K-13 Advanced Interface Settings Dialog Box (Continued)

Enable Directed Broadcasts	When selected, directed broadcast packets are "exploded" as a link-layer broadcast when this interface is directly connected to the destination subnet. When deselected, directed broadcast packets that are intended for the subnet to which this interface is directly connected are dropped rather than being broadcast. This is the default. An IP directed broadcast is an IP packet whose destination address is a valid broadcast address on a different subnet from the node on which it originated. In such cases, the packet is forwarded as if it was a unicast packet until it reaches its destination subnet. This option affects only the final transmission of the directed broadcast on its destination subnet; it does not affect the transit unicast routing of IP directed broadcasts. **Note** Because directed broadcasts, and particularly ICMP directed broadcasts, have been abused by malicious persons, we recommend deselecting this option on interfaces where directed broadcasts are not needed.
ACL	Applies only when directed broadcasts are enabled. The standard access list that determines which directed broadcasts are permitted to be broadcast on the destination subnet. All other directed broadcasts destined for the subnet to which this interface is directly connected are dropped. Enter the name of an ACL object, or click **Select** to display an Object Selectors, page F-593. If the standard ACL you want is not listed, click the **Create** button in the selector to display the Add and Edit Standard Access List Pages, page F-42. From here you can create an ACL object. **Note** To prevent misuse by malicious persons, we recommend using ACLs to restrict the use of directed broadcasts.
Advanced Interface Settings buttons	
OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

AIM-IPS Interface Settings Page

Use the AIM-IPS Interface Settings page to define the settings on the Cisco Intrusion Prevention System Advanced Integration Module. You can install AIM-IPS in Cisco 1841, 2800 series, and 3800 series routers.

Note AIM-IPS must be running IPS 6.0 or later.

Caution Cisco IOS IPS and the Cisco IPS AIM cannot be used together. Cisco IOS IPS must be disabled when the AIM IPS is installed.

Navigation Path

- (Device view) Select **Interfaces > Settings > AIM-IPS** from the Policy selector.
- (Policy view) Select **Router Interfaces > Settings > AIM-IPS** from the Policy Type selector. Right-click **AIM-IPS** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- Chapter K, "Router Platform User Interface Reference"

Field Reference

Table K-14 AIM-IPS Interface Settings Page

Element	Description
AIM-IPS Interface Settings table	
Interface Name	A name selected from among available interfaces.
Select button	Opens the Interface Selector dialog box.
Fail Over Mode	Fail open or fail closed. The default value is fail open.
AIM-IPS Service Module Monitoring Settings table	
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.

Table K-14 AIM-IPS Interface Settings Page (Continued)

Interface Name	The name of the interface role that the AIM-IPS uses.
Monitoring Mode	Inline or Promiscuous: Inline mode puts the AIM-IPS directly into the traffic flow, allowing it to stop attacks by dropping malicious traffic before it reaches the intended target. In promiscuous mode, packets do not flow through the sensor; the sensor analyzes a copy of the monitored traffic rather than the actual forwarded packet.
Access List	Optional. Used to configure a standard monitoring access list on the router and apply that access list to filter traffic for inspection. A matched ACL causes traffic not to be inspected for that ACL. More information on the options for the access-list command is available in the Cisco IOS Command Reference.
Add button	Opens the IPS Monitoring Information Dialog Box, page K-35. From here you can define an IPS monitoring interface.
Edit button	Opens the IPS Monitoring Information Dialog Box, page K-35. From here you can edit an IPS monitoring interface.
Delete button	Deletes the selected IPS monitoring interfaces from the table.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** icon on the toolbar.

Tip To choose which columns to display in the table, right-click a column header, then select **Show Columns**. For more information about table display options, see Table Columns and Column Heading Features, page 3-26.

IPS Monitoring Information Dialog Box

Use the IPS Monitoring Information dialog box to add or edit the properties of AIM-IPS interfaces.

Navigation Path

Go to the AIM-IPS Interface Settings Page, page K-34, then click the **Add** or **Edit** button beneath the AIM-IPS Service Module Monitoring Settings table.

Related Topics

- Basic Interface Settings on Cisco IOS Routers, page 15-20

Field Reference

Table K-15 IPS Monitoring Information Dialog Box

Element	Description
Interface Name	A name selected from among available interfaces.
Select button	Opens the Interface Selector dialog box.
Monitoring Mode	Inline or Promiscuous: Inline mode puts the AIM-IPS directly into the traffic flow, allowing it to stop attacks by dropping malicious traffic before it reaches the intended target. In promiscuous mode, packets do not flow through the sensor; the sensor analyzes a copy of the monitored traffic rather than the actual forwarded packet.
Access List	Optional. Used to configure a standard monitoring access list on the router and apply that access list to filter traffic for inspection. A matched ACL causes traffic not to be inspected for that ACL. More information on the options for the access-list command is available in the Cisco IOS Command Reference.
OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

Dialer Policy Page

Use the Dialer page to define the relationship between physical Basic Rate Interface (BRI) and virtual dialer interfaces. You use these dialer interfaces when you configure the dial backup feature for site-to-site VPNs.

For more information, see Dialer Interfaces on Cisco IOS Routers, page 15-33.

Navigation Path

- (Device view) Select **Interfaces > Settings > Dialer** from the Policy selector.

- (Policy view) Select **Router Interfaces > Settings > Dialer** from the Policy Type selector. Right-click **Dialer** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- Configuring Dial Backup, page 10-37
- Chapter K, "Router Platform User Interface Reference"

Field Reference

Table K-16 Dialer Page

Element	Description
Dialer Profiles table	
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
Interface	The interface role that the dialer interface uses.
Profile Name	The name of the dialer profile.
Dial Pool	The dialing pool that this dialer profile uses.
Dial Group	The dialer group that this dialer profile uses.
Interesting Traffic ACL	The ACL that defines which traffic can use this dialer profile.
Dial String	The phone number that the dialer calls.
Idle Timeout	The defined interval after which an uncontested idle line is disconnected.
Fast Idle	The defined interval after which a contested idle line is disconnected.
Add button	Opens the Dialer Profile Dialog Box, page K-38. From here you can define a dialer profile.
Edit button	Opens the Dialer Profile Dialog Box, page K-38. From here you can edit the selected dialer profile.
Delete button	Deletes the selected dialer profiles from the table.
Dialer Physical Interfaces (BRI) table	
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
Interface	The name of the interface role that the physical interface uses.

Table K-16 Dialer Page (Continued)

Pools	The dial pools related to this physical interface.
Switch Type	The ISDN switch type that the physical interface uses.
SPID1	The first service provider identifier (SPID) related to this interface.
SPID2	The second SPID related to this interface.
Add button	Opens the Dialer Physical Interface Dialog Box, page K-40. From here you can define a dialer physical interface.
Edit button	Opens the Dialer Physical Interface Dialog Box, page K-40. From here you can edit the selected dialer physical interface.
Delete button	Deletes the selected dialer physical interfaces from the table.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** icon on the toolbar.

Tip To choose which columns to display in the table, right-click a column header, then select **Show Columns**. For more information about table display options, see Table Columns and Column Heading Features, page 3-26.

Dialer Profile Dialog Box

Use the Dialer Profile dialog box to add or edit dialer profiles.

Navigation Path

Go to the Dialer Policy Page, page K-36, then click the **Add** or **Edit** button beneath the Dialer Profile table.

Related Topics

- Dialer Physical Interface Dialog Box, page K-40
- Defining Dialer Profiles, page 15-34
- Dialer Interfaces on Cisco IOS Routers, page 15-33

- Basic Interface Settings on Cisco IOS Routers, page 15-20
- Understanding Interface Role Objects, page 9-132

Field Reference

Table K-17 Dialer Profile Dialog Box

Element	Description
Name	A descriptive name for the dialer profile. This name enables you to assign the correct dialer pool to the physical interface. You can also use the profile name as a reference to the site to which this dialer interface serves as a backup.
Interface	The virtual dialer interface to associate with the dialer profile. Enter the name of an interface or interface role, or click **Select** to display an Object Selectors, page F-593. If the interface role you want is not listed, click the **Create** button in the selector to display the Interface Role Dialog Box, page F-464. From here you can create an interface role object.
Pool ID	The dialer pool ID. Each pool can contain multiple physical interfaces and can be associated with multiple dialer interfaces. Each dialer interface, however, is associated with only one pool.
Group	The group ID, which identifies the dialer group that this dialer interface uses.
Interesting Traffic ACL	The extended, numbered ACL that defines which packets are permitted to initiate calls using this dialer profile. Enter the name of an extended, numbered ACL object, or click **Select** to display an Object Selectors, page F-593. The valid ACL number range is 100 to 199. If the extended ACL you want is not listed, click the **Create** button in the selector to display the Extended Tab, page F-32. From here you can create an ACL object.
Dialer String (Remote Phone Number)	The phone number of the destination that the dialer contacts.
Idle Timeout	The default amount of idle time before an uncontested line is disconnected. The default is 120 seconds.

Table K-17 Dialer Profile Dialog Box (Continued)

Fast Idle Timeout	The default amount of idle time before a contested line is disconnected. The default is 20 seconds. Line contention occurs when a busy line is requested to send another packet to a different destination.
OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

Dialer Physical Interface Dialog Box

Use the Dialer Physical Interface dialog box to add or edit the properties that associate physical BRI interfaces with dialer interfaces.

Note Use FlexConfigs to define other types of physical dialer interfaces, such as ATM and Ethernet. For more information, see Understanding FlexConfig Objects, page 9-52.

Navigation Path

Go to the Dialer Policy Page, page K-36, then click the **Add** or **Edit** button beneath the Dialer Physical Interfaces table.

Related Topics

- Dialer Profile Dialog Box, page K-38
- Defining BRI Interface Properties, page 15-36
- Dialer Interfaces on Cisco IOS Routers, page 15-33
- Basic Interface Settings on Cisco IOS Routers, page 15-20
- Understanding Interface Role Objects, page 9-132

Field Reference

Table K-18 Dialer Physical Interface Dialog Box

Element	Description
ISDN BRI	The physical BRI interface associated with the dialer interface. Enter the name of an interface or interface role, or click **Select** to display an Object Selectors, page F-593. If the interface role you want is not listed, click the **Create** button in the selector to display the Interface Role Dialog Box, page F-464. From here you can create an interface role object.
Pools	Associates dialer pools with a physical interface. Enter the names of one or more pools (as defined in the Dialer Profile Dialog Box, page K-38), or click **Select** to display a selector. Use commas to separate multiple entries.
Switch Type	The ISDN switch type. Options for North America are: • basic-5ess—Lucent (AT&T) basic rate 5ESS switch • basic-dms100—Northern Telecom DMS-100 basic rate switch • basic-ni—National ISDN switches Options for Australia, Europe, and the UK are: • basic-1tr6—German 1TR6 ISDN switch • basic-net3—NET3 ISDN BRI for Norway NET3, Australia NET3, and New Zealand NET3 switch types; ETSI-compliant switch types for Euro-ISDN E-DSS1 signaling system • vn3—French VN3 and VN4 ISDN BRI switches Option for Japan is: • ntt—Japanese NTT ISDN switches Option for Voice/PBX system is: • basic-qsig—PINX (PBX) switches with QSIG signaling per Q.931 ()

Table K-18 Dialer Physical Interface Dialog Box (Continued)

SPID1	Applies only when you select Basic-DMS-100, Basic-NI, or Basic-5ess as the switch type. The service provider identifier (SPID) for the ISDN service to which the interface subscribes. Some service providers in North America assign SPIDs to ISDN devices when you first subscribe to an ISDN service. If you are using a service provider that requires SPIDs, your ISDN device cannot place or receive calls until it sends a valid assigned SPID to the service provider when accessing the switch to initialize the connection. Valid SPIDs can contain up to 20 characters, including spaces and special characters. **Note** We recommend that you do not enter a SPID for interfaces using the AT&T 5ESS switch type, even though they are supported.
SPID2	Applies only when you select DMS-100 or NI as the switch type. The service provider identifier (SPID) for a second ISDN service to which the interface subscribes. Valid SPIDs can contain up to 20 alphanumeric characters (no spaces are permitted).
OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

ADSL Policy Page

Use the ADSL page to create, edit, and delete ADSL definitions on the ATM interfaces of the router. For more information, see Defining ADSL Settings, page 15-40.

Navigation Path

- (Device view) Select **Interfaces > Settings > DSL > ADSL** from the Policy selector.
- (Policy view) Select **Router Interfaces > Settings > DSL > ADSL** from the Policy Type selector. Right-click **ADSL** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- PVC Policy Page, page K-54
- SHDSL Policy Page, page K-47
- ADSL on Cisco IOS Routers, page 15-38
- Chapter K, "Router Platform User Interface Reference"

Field Reference

Table K-19 ADSL Page

Element	Description
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
ATM Interface	The ATM interface on which ADSL settings are defined.
Interface Card	The type of device or ADSL interface card on which the ATM interface resides.
Bandwidth Change	Indicates whether the router makes dynamic adjustments to VC bandwidth as overall bandwidth changes. (This is relevant only when IMA groups are configured on the ATM interface.)
DSL Operating Mode	The DSL operating mode for this interface.
Tone Low	Indicates whether the interface is using the low tone set (carrier tones 29 through 48).
Add button	Opens the ADSL Settings Dialog Box, page K-44. From here you can define the ADSL settings for a selected ATM interface.
Edit button	Opens the ADSL Settings Dialog Box, page K-44. From here you can edit the selected ADSL definition.
Delete button	Deletes the selected ADSL definition from the table.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.

Tip To choose which columns to display in the table, right-click a column header, then select **Show Columns**. For more information about table display options, see Table Columns and Column Heading Features, page 3-26.

ADSL Settings Dialog Box

Use the ADSL Settings dialog box to configure ADSL settings on a selected ATM interface.

Note When you configure ADSL settings, we highly recommend that you select the type of device or interface card on which the ATM interface is defined. ADSL settings are highly dependent on the hardware. Defining the hardware type in Security Manager enables proper validation of your configuration for a successful deployment to your devices.

Navigation Path

Go to the ADSL Policy Page, page K-42, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Defining ADSL Settings, page 15-40
- PVC Policy Page, page K-54

Field Reference

Table K-20 ADSL Settings Dialog Box

Element	Description
ATM Interface	The ATM interface on which ADSL settings are defined. Enter the name of an interface or interface role, or click **Select** to display an Object Selectors, page F-593. If the interface role you want is not listed, click the **Create** button in the selector to display the Interface Role Dialog Box, page F-464. From here you can define an interface role object. **Note** We recommend that you do not define an interface role that includes ATM interfaces from different interface cards. The different settings supported by each card type may cause deployment to fail. **Note** You can create only one ADSL definition per interface.
Interface Card	The device type or the type of interface card installed on the router: • [blank]—The interface card type is not defined. • WIC-1ADSL—A 1-port ADSL WAN interface card that provides ADSL over POTS (ordinary telephone lines). • WIC-1ADSL-I-DG—A 1-port ADSL WAN interface card that provides ADSL over ISDN with Dying Gasp support. (With Dying Gasp, the router warns the DSLAM of imminent line drops when the router is about to lose power.) • WIC-1ADSL-DG—A 1-port ADSL WAN interface card that provides ADSL over POTS with Dying Gasp support. • HWIC-1ADSL—A 1-port high-speed ADSL WAN interface card that provides ADSL over POTS. • HWIC-1ADSLI—A 1-port high-speed ADSL WAN interface card that provides ADSL over ISDN. • HWIC-ADSL-B/ST—A 2-port high-speed ADSL WAN interface card that provides ADSL over POTS with an ISDN BRI port for backup. • HWIC-ADSLI-B/ST—A 2-port high-speed ADSL WAN interface card that provides ADSL over ISDN with an ISDN BRI port for backup.

Table K-20 ADSL Settings Dialog Box (Continued)

Interface Card (continued)	• 857 ADSL—Cisco 857 Integrated Service Router with an ADSL interface. • 876 ADSL—Cisco 876 Integrated Services Router with an ADSL interface. • 877 ADSL—Cisco 877 Integrated Services Router with an ADSL interface. • 1801 ADSLoPOTS—Cisco 1801 Integrated Services Router that provides ADSL over POTS. • 1802 ADSLoISDN—Cisco 1802 Integrated Services Router that provides ADSL over ISDN. **Note** When discovering from a live device, the correct interface card type will already be displayed. If you did not perform discovery on a live device, or if Security Manager cannot detect the type of interface card installed on the device, this field displays "Unknown".
Allow bandwidth change on ATM PVCs	When selected, the router makes dynamic adjustments to VC bandwidth in response to changes in the overall bandwidth of the Inverse Multiplexing over ATM (IMA) group defined on the ATM interface. When deselected, PVC bandwidth must be adjusted manually (using the CLI) whenever an individual physical link in the IMA group goes up or down.

Table K-20 ADSL Settings Dialog Box (Continued)

DSL Operating Mode	The operating mode configured for this ADSL line: • auto—Performs automatic negotiation with the DSLAM located at the central office (CO). This is the default. • ansi-dmt—The line trains in ANSI T1.413 Issue 2 mode. • itu-dmt—The line trains in G.992.1 mode. • splitterless—The line trains in G.992.2 (G.Lite) mode. • etsi—The line trains in ETSI (European Telecommunications Standards Institute) mode. • adsl2—The line trains in G.992.3 (adsl2)mode. • adsl2+—The line trains in G.992.5 (adsl2+) mode. **Note** See Table 15-3 on page 15-39 for a description of the operating modes that are supported by each card type.
Use low tone set	When selected, the interface card uses carrier tones 29 through 48. When deselected, the interface card uses carrier tones 33 through 56. **Note** Leave this option deselected when the interface card is operating in accordance with Deutsche Telekom specification U-R2.
OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

SHDSL Policy Page

Use the SHDSL page to create, edit, and delete DSL controller definitions on the router. For more information, see Defining SHDSL Controllers, page 15-44.

Navigation Path

- (Device view) Select **Interfaces > Settings > DSL > SHDSL** from the Policy selector.

- (Policy view) Select **Router Interfaces > Settings > DSL > SHDSL** from the Policy Type selector. Right-click **SHDSL** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- PVC Policy Page, page K-54
- ADSL Policy Page, page K-42
- SHDSL on Cisco IOS Routers, page 15-43
- Chapter K, "Router Platform User Interface Reference"

Field Reference

Table K-21 SHDSL Page

Element	Description
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
Name	The name of the DSL controller.
Description	An optional description of the controller.
Shutdown	Indicates whether the DSL controller is in shutdown mode.
Configure ATM Mode	Indicates whether the DSL controller has been set into ATM mode.
Line Termination	The line termination set for the router (CPE or CO).
DSL Mode	The operating mode defined for the DSL controller.
Line Mode	The line mode defined for the DSL controller.
Line Rate	The line rate (in kbps) defined for the DSL controller. **Note** A value is displayed in this column only if the line mode is not set to Auto.
SNR Margin Current	The current signal-to-noise ratio on the controller.
SNR Margin Snext	The self near-end crosstalk (Snext) signal-to-noise ratio on the controller.
Add button	Opens the SHDSL Controller Dialog Box, page K-49. From here you can define the settings for a DSL controller.
Edit button	Opens the SHDSL Controller Dialog Box, page K-49. From here you can edit the selected DSL controller definition.

Table K-21 SHDSL Page (Continued)

Delete button	Deletes the selected DSL controller definition from the table.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.

Tip To choose which columns to display in the table, right-click a column header, then select **Show Columns**. For more information about table display options, see Table Columns and Column Heading Features, page 3-26.

SHDSL Controller Dialog Box

Use the SHDSL Controller dialog box to configure SHDSL controllers.

Navigation Path

Go to the SHDSL Policy Page, page K-47, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Defining SHDSL Controllers, page 15-44
- PVC Policy Page, page K-54
- Discovering Policies on Devices Already in Security Manager, page 7-10

Field Reference

Table K-22 SHDSL Dialog Box

Element	Description
Name	The name of the controller. Enter a name manually, or click **Select** to display a dialog box for generating a name. See Controller Auto Name Generator Dialog Box, page K-53.
Description	Additional information about the controller (up to 80 characters).

Table K-22 SHDSL Dialog Box (Continued)

Shutdown	When selected, the DSL controller is in shutdown state. However, its definition is not deleted. When deselected, the DSL controller is enabled. This is the default.
Configure ATM mode	When selected, sets the controller into ATM mode and creates an ATM interface with the same ID as the controller. This is the default. You must enable ATM mode and then perform rediscovery to configure ATM or PVCs on the device. When deselected, ATM mode is disabled. No ATM interface is created on deployment. **Note** You cannot remove ATM mode from a controller after it has been saved in Security Manager.
Line Termination	The line termination that is set for the router: • CPE—Customer premises equipment. This is the default. • CO—Central office.
DSL Mode	The DSL operating mode, including regional operating parameters, used by the controller: • [blank]—The operating mode is not defined. (When deployed, the Annex A standard for North America is used.) • A—Supports Annex A of the G.991.2 standard for North America. • A-B—Supports Annex A or Annex B. Available only when the Line Term is set to CPE. The appropriate mode is selected when the line trains. • A-B-ANFP—Supports Annex A or Annex B-ANFP. Available only when the Line Term is set to CPE. The appropriate mode is selected when the line trains. • B—Supports Annex B of the G.991.2 standard for Europe. • B-ANFP—Supports Annex B-ANFP (Access Network Frequency Plan). **Note** The available DSL modes are dependent on the selected line termination.
Line Mode settings	

Table K-22 SHDSL Dialog Box (Continued)

Line Mode	The line mode used by the controller: • auto—The controller operates in the same mode as the other line termination (2-wire line 0, 2-wire line 1, or 4-wire enhanced). This is the default for CPE line termination. • 2-wire—The controller operates in two-wire mode. This is the default for CO line termination. • 4-wire—The controller operates in four-wire mode. **Note** You can select Auto only when you configure the controller as the CPE.
Line	Applies only when the Line Mode is defined as 2-wire. The pair of wires to use: • line-zero—RJ-11 pin 1 and pin 2. This is the default for CO line termination. • line-one—RJ-11 pin 3 and pin 4.
Exchange Handshake	Applies only when the Line Mode is defined as 4-wire. The type of handshake mode to use: • [blank]—The handshake mode is not specified. (When deployed, the enhanced option is used.) This is the default. • enhanced—Exchanges handshake status on both wire pairs. • standard—Exchanges handshake status on the master wire pair only.

Table K-22 SHDSL Dialog Box (Continued)

Line Rate	Does not apply when the Line Mode is defined as Auto. The DSL line rate (in kbps) available for the SHDSL port: • auto—The controller selects the line rate. This is available only in 2-wire mode. • Supported line rates: – For 2-wire mode: 192, 256, 320, 384, 448, 512, 576, 640, 704, 768, 832, 896, 960, 1024, 1088, 1152, 1216, 1280, 1344, 1408, 1472, 1536, 1600, 1664, 1728, 1792, 1856, 1920, 1984, 2048, 2112, 2176, 2240, and 2304. – For 4-wire mode: 384, 512, 640, 768, 896, 1024, 1152, 1280, 1408, 1536, 1664, 1792, 1920, 2048, 2176, 2304, 2432, 2560, 2688, 2816, 2944, 3072, 3200, 3328, 3456, 3584, 3712, 3840, 3968, 4096, 4224, 4352, 4480, and 4608. **Note** Third-party equipment may use a line rate that includes an additional SHDSL overhead of 8 kbps for 2-wire mode or 16 kbps for 4-wire mode.
SNR Margin settings	
Current	The current signal-to-noise (SNR) ratio on the controller, in decibels (dB). Valid values range from -10 to 10 dB. This option can create a more stable line by making the line train more than current noise margin plus SNR ratio threshold during training time. If any external noise is applied that is less than the set SNR margin, the line will be stable. **Note** Select **disable** to disable the current SNR.
Snext	The Self Near-End Crosstalk (SNEXT) signal-to-noise ratio on the controller, in decibels. Valid values range from -10 to 10 dB. This option can create a more stable line by making the line train more than SNEXT threshold during training time. If any external noise is applied that is less than the set SNEXT margin, the line will be stable. **Note** Select **disable** to disable the SNEXT SNR.
SHDSL dialog box buttons	

Table K-22 SHDSL Dialog Box (Continued)

OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

Controller Auto Name Generator Dialog Box

Use the Controller Auto Name Generator dialog box to have Security Manager generate a name for the DSL controller based on its location in the router.

Navigation Path

Go to the SHDSL Controller Dialog Box, page K-49, then click **Select** in the Name field**.**

Related Topics

- Defining SHDSL Controllers, page 15-44
- SHDSL Policy Page, page K-47
- PVC Policy Page, page K-54

Field Reference

Table K-23 Controller Auto Name Generator Dialog Box

Element	Description
Type	The type of interface. This field displays the value DSL and is read-only.
Card	The card related to the controller.
Slot	The slot related to the controller.
Port	The port related to the controller. **Note** The information you enter in these fields forms the remainder of the generated name, as displayed in the Result field.

Table K-23 Controller Auto Name Generator Dialog Box (Continued)

Result	The name generated by Security Manager from the information you entered for the controller location. The name displayed in this field is read-only. **Tip** After closing this dialog box, you can edit the generated name in the SHDSL dialog box, if required.
OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

PVC Policy Page

Use the PVC page to create, edit, and delete permanent virtual connections (PVCs) on the router. PVCs allow direct and permanent connections between sites to provide a service that is similar to a leased line. These PVCs can be used in ADSL, SHDSL, or pure ATM environments. For more information, see Defining ATM PVCs, page 15-52.

Navigation Path

- (Device view) Select **Interfaces > Settings > PVC** from the Policy selector.
- (Policy view) Select **Router Interfaces > Settings > PVC** from the Policy Type selector. Right-click **PVC** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- ADSL Policy Page, page K-42
- SHDSL Policy Page, page K-47
- PVCs on Cisco IOS Routers, page 15-46
- Chapter K, “Router Platform User Interface Reference”

Field Reference

Table K-24 PVC Page

Element	Description
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
ATM Interface	The ATM interface on which the PVC is defined.
Interface Card	The type of device or WAN interface card on which the ATM interface resides.
PVC ID	The Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) of the PVC.
Settings	Additional settings configured for the PVC, including encapsulation, the number of PPPoE sessions, and the VPN service name.
QoS	Quality-of-service settings defined for the PVC, such as traffic shaping.
Protocol	The IP protocol mappings (static maps or Inverse ARP) configured for the PVC.
OAM	The F5 Operation, Administration, and Maintenance (OAM) loopback, continuity check, and AIS/RDI definitions configured for the PVC.
OAM-PVC	The OAM management cells that are configured for the PVC.
Add button	Opens the PVC Dialog Box, page K-56. From here you can define a PVC.
Edit button	Opens the PVC Dialog Box, page K-56. From here you can edit the selected PVC.
Delete button	Deletes the selected PVC from the table.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.

Tip To choose which columns to display in the table, right-click a column header, then select **Show Columns**. For more information about table display options, see Table Columns and Column Heading Features, page 3-26.

PVC Dialog Box

Use the PVC dialog box to configure ATM permanent virtual circuits (PVCs).

Navigation Path

Go to the PVC Policy Page, page K-54, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Defining ATM PVCs, page 15-52

Field Reference

Table K-25 PVC Dialog Box

Element	Description
ATM Interface	The ATM interface on which the PVC is defined. Enter the name of an interface, subinterface, or interface role, or click **Select** to display an Object Selectors, page F-593. If the interface role you want is not listed, click the **Create** button in the selector to display the Interface Role Dialog Box, page F-464. From here you can define an interface role object. **Note** We strongly recommend not defining an interface role that includes ATM interfaces from different interface cards. The different settings supported by each card type may cause deployment to fail.

Table K-25 PVC Dialog Box (Continued)

Interface Card	The type of WAN interface card installed on the router or the router type: • [blank]—The interface card type is not defined. • WIC-1ADSL—A 1-port ADSL WAN interface card that provides ADSL over POTS (ordinary telephone lines). • WIC-1ADSL-I-DG—A 1-port ADSL WAN interface card that provides ADSL over ISDN with Dying Gasp support. (With Dying Gasp, the router warns the DSLAM of imminent line drops when the router is about to lose power.) • WIC-1ADSL-DG—A 1-port ADSL WAN interface card that provides ADSL over POTS with Dying Gasp support. • HWIC-1ADSL—A 1-port high-speed ADSL WAN interface card that provides ADSL over POTS. • HWIC-1ADSLI—A 1-port high-speed ADSL WAN interface card that provides ADSL over ISDN. • HWIC-ADSL-B/ST—A 2-port high-speed ADSL WAN interface card that provides ADSL over POTS with an ISDN BRI port for backup. • HWIC-ADSLI-B/ST—A 2-port high-speed ADSL WAN interface card that provides ADSL over ISDN with an ISDN BRI port for backup. • WIC-1-SHDSL-V2—A 1-port multiline G.SHDSL WAN interface card with support for 2-wire mode and enhanced 4-wire mode. • WIC-1-SHDSL-V3—A 1-port multiline G.SHDSL WAN interface card with support for 2-wire mode and 4-wire mode (standard & enhanced). • NM-1A-T3—A 1-port ATM network module with a T3 link. • NM-1A-OC3-POM—A 1-port ATM network module with an optical carrier level 3 (OC-3) link and three operating modes (multimode, single-mode intermediate reach (SMIR), and single-mode long-reach (SMLR)).

Table K-25 PVC Dialog Box (Continued)

Interface Card (continued)	• NM-1A-E3—A 1-port ATM network module with an E3 link. • 857 ADSL—Cisco 857 Integrated Service Router with an ADSL interface. • 876 ADSL—Cisco 876 Integrated Services Router with an ADSL interface. • 877 ADSL—Cisco 877 Integrated Services Router with an ADSL interface. • 878 G.SHDSL—Cisco 878 Integrated Services Router with a G.SHDSL interface. • 1801 ADSLoPOTS—Cisco 1801 Integrated Services Router that provides ADSL over POTS. • 1802 ADSLoISDN—Cisco 1802 Integrated Services Router that provides ADSL over ISDN. • 1803 G.SHDSL—Cisco 1803 Integrated Services Router that provides 4-wire G.SHDSL. **Note** To ensure proper policy validation, we highly recommend that you define a value in this field. When you discover a live device, the correct interface card type will already be displayed. If you did not perform discovery on a live device, or if Security Manager cannot detect the type of interface card installed on the device, this field displays “Unknown”.
Settings tab	Defines basic PVC settings, such as the VPI/VCI and encapsulation. See PVC Dialog Box—Settings Tab, page K-59.
QoS tab	Defines ATM traffic shaping and other quality-of-service settings for the PVC. See PVC Dialog Box—QoS Tab, page K-63.
Protocol tab	Defines the IP protocol mappings configured for the PVC (static maps or Inverse ARP). See PVC Dialog Box—Protocol Tab, page K-67.
Advanced button	Defines F5 Operation, Administration, and Maintenance (OAM) settings for the PVC. See PVC Advanced Settings Dialog Box—OAM Tab, page K-70.

Table K-25 PVC Dialog Box (Continued)

OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

PVC Dialog Box—Settings Tab

Use the Settings tab of the PVC dialog box to configure the basic settings of the PVC, including:

- ID settings.
- Encapsulation settings.
- Whether ILMI and Inverse ARP are enabled.
- The maximum number of PPPoE sessions.
- The static domain (VPN service) name to use for PPPoA.

Navigation Path

Go to the PVC Dialog Box, page K-56, then click the **Settings** tab.

Related Topics

- PVC Dialog Box—QoS Tab, page K-63
- PVC Dialog Box—Protocol Tab, page K-67
- PVC Advanced Settings Dialog Box, page K-69
- Defining ATM PVCs, page 15-52

Field Reference

Table K-26 PVC Dialog Box—Settings Tab

Element	Description
PVC ID settings	
VPI	The virtual path identifier of the PVC. In conjunction with the VCI, identifies the next destination of a cell as it passes through a series of ATM switches on the way to its destination. Valid values for most platforms range from 0 to 255. For Cisco 2600 and 3600 Series routers using Inverse Multiplexing for ATM (IMA), valid values range from 0 to 15, 64 to 79, 128 to 143, and 192 to 207. **Note** VPI/VCI values must be unique for all the PVCs configured on a selected interface. VPI/VCI values are unique to a single link only and might change as cells traverse the ATM network.
VCI	The 16-bit virtual channel identifier of the PVC. In conjunction with the VPI, identifies the next destination of a cell as it passes through a series of ATM switches on the way to its destination. Valid values vary by platform. Typically, values up to 31 are reserved for special traffic (such as ILMI) and should not be used. 3 and 4 are invalid. **Note** VPI/VCI values must be unique for all the PVCs configured on a selected interface. VPI/VCI values are unique to a single link only and might change as cells traverse the ATM network.
Handle	An optional name to identify the PVC. The maximum length is 15 characters.
Management PVC (ILMI)	Does not apply when configuring the PVC on a subinterface. When selected, designates this PVC as the management PVC for this ATM interface by enabling communication with the Interim Local Management Interface (ILMI). ILMI is a protocol defined by the ATM Forum for setting and capturing physical layer, ATM layer, virtual path, and virtual circuit parameters on ATM interfaces. See Understanding ILMI, page 15-50. When deselected, this PVC does not act as the management PVC. This is the default. **Note** The VPI/VCI for the management PVC is typically set to 0/16.

Table K-26 PVC Dialog Box—Settings Tab (Continued)

Encapsulation settings	
Type	Does not apply when the Management PVC (ILMI) check box is enabled. The ATM adaptation layer (AAL) and encapsulation type to use on the PVC: • [blank]—The encapsulation type is not defined. (When deployed, aal5snap is applied.) • aal2—For PVCs dedicated to AAL2 Voice over ATM. AAL2 is used for variable bit rate (VBR) traffic, which can be either realtime (VBR-RT) or non-realtime (VBR-NRT). • aal5autoppp—Enables the router to distinguish between incoming PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE) sessions and create virtual access for both PPP types based on demand. • aal5ciscoppp—For the proprietary Cisco version of PPP over ATM. • aal5mux—Enables you to dedicate the PVC to a single protocol, as defined in the Protocol field. • aal5nlpid—Enables ATM interfaces to work with High-Speed Serial Interfaces (HSSI) that are using an ATM data service unit (ADSU) and running ATM-Data Exchange Interface (DXI). • aal5snap—Supports Inverse ARP and incorporates the Logical Link Control/Subnetwork Access Protocol (LLC/SNAP) that precedes the protocol datagram. This allows multiple protocols to traverse the same PVC.

Table K-26 PVC Dialog Box—Settings Tab (Continued)

Virtual Template	The virtual template used for PPP over ATM on this PVC. Enter the name of a virtual template interface or interface role, or click **Select** to display an Object Selectors, page F-593. If the interface role you want is not listed, click the **Create** button in the selector to display the Interface Role Dialog Box, page F-464. From here you can define an interface role object. When a user dials in, the virtual template is used to configure a virtual access interface. When the user is done, the virtual access interface goes down and the resources are freed for other dial-in users. **Note** If you modify the virtual template settings on an existing PVC, you must enter the shutdown command followed by the no shutdown command on the ATM subinterface to restart the interface. This causes the newly configured parameters to take effect.
Protocol	Applies only when aal5mux is the defined encapsulation type. The protocol carried by the MUX-encapsulated PVC: • frame-relay—Frame-Relay-ATM Network Interworking (FRF.5) on the Cisco MC3810. • fr-atm-srv—Frame-Relay-ATM Service Interworking (FRF.8) on the Cisco MC3810. • ip—IP protocol. • ppp—IETF-compliant PPP over ATM. You must specify a virtual template when using this protocol type. • voice—Voice over ATM.
Additional settings	
Enable ILMI	When selected, enables ILMI management on this PVC. When deselected, ILMI management on this PVC is disabled.

Table K-26 PVC Dialog Box—Settings Tab (Continued)

Inverse ARP	When selected, the Inverse Address Resolution Protocol (Inverse ARP) is enabled on the PVC. When deselected, Inverse ARP is disabled. This is the default. Inverse ARP is used to learn the Layer 3 addresses at the remote ends of established connections. These addresses must be learned before the virtual circuit can be used. **Note** Use the Protocol tab to define static mappings of IP addresses instead of dynamically learning the addresses using Inverse ARP. See PVC Dialog Box—Protocol Tab, page K-67.
PPPoE Max Sessions	The maximum number of PPP over Ethernet sessions that are permitted on the PVC.
VPN Service Name	The static domain name to use on this PVC. The maximum length is 128 characters. Use this option when you want PPP over ATM (PPPoA) sessions in the PVC to be forwarded according to the domain name supplied, without starting PPP.

PVC Dialog Box—QoS Tab

Use the QoS tab of the PVC dialog box to configure the ATM traffic shaping and other quality-of-service settings of the PVC, including:

- The limit on packets placed on transmission rings.
- The QoS service.
- Whether random detection is enabled.

These settings regulate the flow of traffic over the PVC by queuing traffic that exceeds the defined allowable bit rates.

Note QoS values are highly hardware dependent. Please refer to your router documentation for additional details about the settings that can be configured on your device.

Navigation Path

Go to the PVC Dialog Box, page K-56, then click the **QoS** tab.

Related Topics

- PVC Dialog Box—Settings Tab, page K-59
- PVC Dialog Box—Protocol Tab, page K-67
- PVC Advanced Settings Dialog Box, page K-69
- Defining ATM PVCs, page 15-52
- Quality of Service Policy Page, page K-199
- Understanding Policing and Shaping Parameters, page 15-159

Field Reference

Table K-27 PVC Dialog Box—QoS Tab

Element	Description
Tx Ring Limit	The maximum number of transmission packets that can be placed on a transmission ring on the WAN interface card (WIC) or interface. The range of valid values depends on the type of interface card selected in the Settings tab. See PVC Dialog Box—Settings Tab, page K-59.

Table K-27 PVC Dialog Box—QoS Tab (Continued)

Traffic Shaping settings	
Traffic Shaping	The type of service to define on the PVC: • [null]—The bit rate is not defined. • ABR—Available Bit Rate. A best-effort service suitable for applications that do not require guarantees against cell loss or delays. • CBR—Constant Bit Rate service. Delay-sensitive data, such as voice or video, is sent at a fixed rate, providing a service similar to a leased line. • UBR—Unspecified Bit Rate service. A best-effort service suitable for applications that are tolerant to delay and do not require realtime responses. • UBR+—Unspecified Bit Rate service. Unlike UBR, UBR+ attempts to maintain a guaranteed minimum rate. • VBR-NRT—Variable Bit Rate - Non-Real Time service. A service suitable for non-realtime applications that are bursty in nature. VBR is more efficient than CBR and more reliable than UBR. • VBR-RT—Variable Bit Rate - Real Time service. A service suitable for realtime applications that are bursty in nature. For more information about each service class, see Understanding ATM Service Classes, page 15-48.
ABR	The following fields are displayed when ABR is selected as the Bit Rate: • PCR—The peak cell rate in kilobits per second (kbps). It specifies the maximum value of the ABR. • MCR—The minimum cell rate in kilobits per second (kbps). It specifies the minimum value of the ABR. The ABR varies between the MCR and the PCR. It is dynamically controlled using congestion control mechanisms.
CBR	The following field is displayed when CBR is selected as the Bit Rate: • Rate—The constant bit rate (also known as the average cell rate) for the PVC in kilobits per second (kbps). An ATM VC configured for CBR can send cells at this rate for as long as required.

Table K-27 PVC Dialog Box—QoS Tab (Continued)

UBR	The following field is displayed when UBR is selected as the Bit Rate: • PCR—The peak cell rate for output in kilobits per second (kbps). Cells in excess of the PCR may be discarded.
UBR+	The following fields are displayed when UBR+ is selected as the Bit Rate: • PCR—The peak cell rate for output in kilobits per second (kbps). Cells in excess of the PCR may be discarded. • MCR—The minimum guaranteed cell rate for output in kilobits per second (kbps). Traffic is always allowed to be sent at this rate. **Note** UBR+ requires Cisco IOS Software Release 12.4(2)XA or later, or version 12.4(6)T or later.
VBR-NRT	The following fields are displayed when VBR-NRT is selected as the Bit Rate: • PCR—The peak cell rate for output in kilobits per second (kbps). Cells in excess of the PCR may be discarded. • SCR—The sustained cell rate for output in kilobits per second (kbps). This value, which must be lower than or equal to the PCR, represents the maximum rate at which cells can be transmitted without incurring data loss. • MBS—The maximum burst cell size for output. This value represents the number of cells that can be transmitted above the SCR but below the PCR without penalty.
VBR-RT	The following fields are displayed when VBR-RT is selected as the Bit Rate: • Peak Rate—The peak information rate for realtime traffic in kilobits per second (kbps). • Average Rate—The average information rate for realtime traffic in kilobits per second (kbps). This value must be lower than or equal to the peak rate. • Burst—The burst size for realtime traffic, in number of cells. Configure this value if the PVC carries bursty traffic. These values configure traffic shaping between realtime traffic (such as voice and video) and data traffic to ensure that the carrier does not discard realtime traffic, for example, voice calls.

Table K-27 PVC Dialog Box—QoS Tab (Continued)

IP QoS settings	
Random Detect	When selected, enables Weighted Random Early Detection (WRED) or VIP-distributed WRED (DWRED) on the PVC. When deselected, WRED and DWRED are disabled. This is the default. WRED is a queue management method that selectively drops packets as the interface becomes congested. See Tail Drop vs. WRED, page 15-156.

PVC Dialog Box—Protocol Tab

Use the Protocol tab of the PVC dialog box to add, edit, or delete the protocol mappings configured for the PVC. You may configured static mappings or Inverse ARP (broadcast or nonbroadcast) for each PVC, but not both.

Note IP is the only protocol supported by Security Manager for protocol mapping on ATM networks.

Note You cannot define protocol mappings on the Management PVC (ILMI).

Navigation Path

Go to the PVC Dialog Box, page K-56, then click the **Protocol** tab.

Related Topics

- PVC Dialog Box—Settings Tab, page K-59
- PVC Dialog Box—QoS Tab, page K-63
- PVC Advanced Settings Dialog Box, page K-69
- Defining ATM PVCs, page 15-52

Field Reference

Table K-28 PVC Dialog Box—Protocol Tab

Element	Description
IP Protocol Mapping	Displays the IP protocol mappings configured for the PVC.
Add button	Opens the Define Mapping Dialog Box, page K-68. From here you can define an IP protocol mapping.
Edit button	Opens the Define Mapping Dialog Box, page K-68. From here you can edit the selected mapping.
Delete button	Deletes the selected mapping from the table.

Define Mapping Dialog Box

Use the Define Mapping dialog box to configure the IP protocol mappings to use on the ATM PVC. Mappings are required by the PVC to discover which IP address is reachable at the other end of a connection. Mappings can either be learned dynamically using Inverse ARP (InARP) or defined statically. Static mappings are best suited for simple networks that contain only a few nodes.

Note Inverse ARP is only supported for the aal5snap encapsulation type. See PVC Dialog Box—Settings Tab, page K-59.

Tip Use the CLI or FlexConfigs to configure mappings for protocols other than IP.

Navigation Path

Go to the PVC Dialog Box—Protocol Tab, page K-67, then click **Add** or **Edit**.

Related Topics

- PVC Dialog Box, page K-56
- Defining ATM PVCs, page 15-52

Field Reference

Table K-29 Define Mapping Dialog Box

Element	Description
IP Options	The type of IP protocol mapping to use: • IP Address—Select this option when using static mapping. Enter the address or network/host object, or click **Select** to display an Object Selectors, page F-593. If the network you want is not listed, click the **Create** button in the selector to display the Network/Host Dialog Box, page F-477. From here, you can define a network/host object. • InARP—Inverse ARP. Select this option when using dynamic mapping. This allows the PVC to resolve its own network addresses without configuring a static map. Dynamic mappings age out and are refreshed periodically every 15 minutes by default. **Note** InARP can be used only when aal5snap is the defined encapsulation type for the PVC. See PVC Dialog Box—Settings Tab, page K-59.
Broadcast Options	Indicates whether to use this map entry when sending IP broadcast packets (such as EIGRP updates): • Broadcast—The map entry is used for broadcast packets. • No Broadcast—The map entry is used only for unicast packets. • None—Broadcast options are disabled.
OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

PVC Advanced Settings Dialog Box

Use the PVC Advanced Settings dialog box to configure F5 Operation, Administration, and Maintenance (OAM) functionality on an ATM PVC. OAM is used to detect connectivity failures at the ATM layer.

For more information, see Defining OAM Management on ATM PVCs, page 15-56.

Navigation Path

Go to the PVC Dialog Box, page K-56, then click **Advanced**.

Related Topics

- PVC Policy Page, page K-54

Field Reference

Table K-30 PVC Advanced Settings Dialog Box

Element	Description
OAM tab	Defines loopback, connectivity check, and AIS/RDI settings. See PVC Advanced Settings Dialog Box—OAM Tab, page K-70.
OAM-PVC tab	Enables OAM loopbacks and connectivity checks on the PVC. See PVC Advanced Settings Dialog Box—OAM-PVC Tab, page K-73.
OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

PVC Advanced Settings Dialog Box—OAM Tab

Use the OAM tab of the PVC Advanced Settings dialog box to define:

- The number of loopback cell responses that move the PVC to the down or up state.
- The number of alarm indication signal/remote defect indication (AIS/RDI) cells that move the PVC to the down or up state.
- The number and frequency of segment/end continuity check (CC) activation and deactivation requests that are sent on this PVC.

For more information, see Defining OAM Management on ATM PVCs, page 15-56.

Note The settings defined in this tab are dependent on the settings defined in the OAM-PVC tab. See PVC Advanced Settings Dialog Box—OAM-PVC Tab, page K-73.

Navigation Path

Go to the PVC Advanced Settings Dialog Box, page K-69, then click the **OAM** tab.

Related Topics

- PVC Dialog Box, page K-56

Field Reference

Table K-31 PVC Advanced Settings Dialog Box—OAM Tab

Element	Description
Retry settings	
Enable OAM Retry	When selected, OAM management settings can be defined. When deselected, OAM management settings cannot be defined. **Note** If Enable OAM Management is deselected in the OAM-PVC tab, these settings are saved in the device configuration but are not applied.
Down Count	The number of consecutive, unreceived, end-to-end loopback cell responses that cause the PVC to move to the down state. The default is 3.
Up Count	The number of consecutive end-to-end loopback cell responses that must be received in order to move the PVC to the up state. The default is 5.
Retry Frequency	The interval between loopback cell verification transmissions in seconds. The default is 1 second. If a PVC is up and a loopback cell response is not received within the specified interval (as defined in the Frequency field of the PVC-OAM tab), loopback cells are transmitted at the frequency defined here to verify whether the PVC is down. If the number of consecutive cells that do not receive a response matches the defined down count, the PVC is moved to the down state.

Table K-31 PVC Advanced Settings Dialog Box—OAM Tab (Continued)

AIS-RDI settings	
Enable AIS-RDI Detection	When selected, alarm indication signal (AIS) cells and remote defect indication (RDI) cells are used to report connectivity failures at the ATM layer of the PVC. When deselected, AIS/RDI cells are disabled. AIS cells notify downstream devices of the connectivity failure. The last ATM switch then generates RDI cells in the upstream direction towards the device that sent the original failure notification.
Down Count	The number of consecutive AIS/RDI cells that cause the PVC to go down. Valid values range from 1 to 60. The default is 1.
Up Count	The number of seconds after which a PVC is brought up if no AIS/RDI cells are received. Valid values range from 3 to 60 seconds. The default is 3.
Segment Continuity Check settings	
Enable Segment Continuity Check	When selected, OAM F5 continuity check (CC) activation and deactivation requests are sent to a device at the other end of a segment. When deselected, segment CC activation and deactivation requests are disabled. **Note** If Configure Continuity Check is deselected in the OAM-PVC tab, these settings are saved in the device configuration but are not applied.
Activation Count	The maximum number of times that the activation request is sent before the receipt of an acknowledgement. Valid values range from 3 to 600. The default is 3.
Deactivation Count	The maximum number of times that the deactivation request is sent before the receipt of an acknowledgement. Valid values range from 3 to 600. The default is 3.
Retry Frequency	The interval between activation/deactivation retries, in seconds. The default is 30 seconds.

Table K-31 PVC Advanced Settings Dialog Box—OAM Tab (Continued)

End-to-End Continuity Check settings	
Enable End-to-End Continuity Check	When selected, OAM F5 continuity check (CC) activation and deactivation requests are sent to a device at the other end of the PVC. When deselected, segment CC activation and deactivation requests are disabled. **Note** If Configure Continuity Check is deselected in the OAM-PVC tab, these settings are saved in the device configuration but are not applied.
Activation Count	The maximum number of times that the activation request is sent before the receipt of an acknowledgement. Valid values range from 3 to 600. The default is 3.
Deactivation Count	The maximum number of times that the deactivation request is sent before the receipt of an acknowledgement. Valid values range from 3 to 600. The default is 3.
Retry Frequency	The interval between activation/deactivation retries, in seconds. The default is 30 seconds.

PVC Advanced Settings Dialog Box—OAM-PVC Tab

Use the OAM-PVC tab of the PVC Advanced Settings dialog box to enable loopback cells and connectivity checks (CCs) on the PVC. These functions test the connectivity of the virtual connection.

For more information, see Defining OAM Management on ATM PVCs, page 15-56.

Note Use the OAM tab to define additional settings related to the settings on this tab. See PVC Advanced Settings Dialog Box—OAM Tab, page K-70.

Navigation Path

Go to the PVC Advanced Settings Dialog Box, page K-69, then click the **OAM-PVC** tab.

Related Topics

- PVC Dialog Box, page K-56

Field Reference

Table K-32 PVC Advanced Settings Dialog Box—OAM-PVC Tab

Element	Description
OAM settings	
Enable OAM Management	When selected, OAM loopback cell generation and OAM management are enabled on the PVC. When deselected, OAM loopback cells and OAM management are disabled. However, continuity checks can still be performed.
Frequency	The interval between loopback cell transmissions. Valid values range from 0 to 600 seconds.
Segment Continuity Check settings	
Segment Continuity Check	The current configuration of OAM F5 continuity checks performed on PVC segments: • None—Segment continuity checks (CC) are disabled. • Deny Activation Requests—The PVC rejects activation requests from peer devices, which prevents OAM F5 CC management from being activated on the PVC. • Configure Continuity Check—Segment CCs are enabled on the PVC. The router on which CC management is configured sends a CC activation request to the router at the other end of the segment, directing it to act as either a source or a sink. Segment CCs occur on a PVC segment between the router and a first-hop ATM switch.

Table K-32 PVC Advanced Settings Dialog Box—OAM-PVC Tab (Continued)

Direction	Applies only when CC management is enabled. The direction in which CC cells are transmitted: • both—CC cells are transmitted in both directions. • sink—CC cells are transmitted toward the router that initiated the CC activation request. • source—CC cells are transmitted away from the router that initiated the CC activation request.
Keep VC up after segment failure	When selected, the PVC is kept in the up state when CC cells detect connectivity failure. When deselected, the PVC is brought down when CC cells detect connectivity failure.
Keep VC up after end-to-end failure	When selected, specifies that if AIS/RDI cells are received, the PVC is not brought down because of end CC failure or loopback failure. When deselected, the PVC is brought down because of end CC failure or loopback failure.
End-to-End Continuity Check settings	
End-to-End Continuity Check	The current configuration of OAM F5 end-to-end continuity checks on the PVC: • None—End-to-end continuity checks (CC) are disabled. • Deny Activation Requests—The PVC rejects activation requests from peer devices, which prevents OAM F5 CC management from being activated on the PVC. • Configure Continuity Check—End-to-end CCs are enabled on the PVC. The router on which CC management is configured sends a CC activation request to the router at the other end of the connection, directing it to act as either a source or a sink. End-to-end CC monitoring is performed on the entire PVC between two ATM end stations.

Table K-32 PVC Advanced Settings Dialog Box—OAM-PVC Tab (Continued)

Direction	Applies only when CC management is enabled. The direction in which CC cells are transmitted: • both—CC cells are transmitted in both directions. • sink—CC cells are transmitted toward the router that initiated the CC activation request. • source—CC cells are transmitted away from the router that initiated the CC activation request.
Keep VC up after end-to-end failure	When selected, the PVC is kept in the up state when CC cells detect connectivity failure. When deselected, the PVC is brought down when CC cells detect connectivity failure.
Keep VC up after segment failure	When selected, specifies that if AIS/RDI cells are received, the PVC is not brought down because of a segment CC failure. When deselected, the PVC is brought down because of a segment CC failure.

PPP/MLP Policy Page

Use the PPP/MLP page to create, edit, and delete PPP connections on the router. For more information, see Defining PPP Connections, page 15-61.

Navigation Path

- (Device view) Select **Interfaces > Settings > PPP/MLP** from the Policy selector.
- (Policy view) Select **Router Interfaces > Settings > PPP/MLP** from the Policy Type selector. Right-click **PPP/MLP** to create a policy, or select an existing policy from the Shared Policies selector.

Related Topics

- PPP on Cisco IOS Routers, page 15-58
- Chapter K, “Router Platform User Interface Reference”

Field Reference

Table K-33 PPP/MLP Page

Element	Description
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
Interface	The interface that is configured for PPP/MLP.
Authentication	The types of authentication used on the PPP connection.
Authorization	The method list used for AAA authorization on the PPP connection.
Multilink	Indicates whether Multilink PPP (MLP) is enabled on this PPP connection.
Endpoint	The type of default endpoint discriminator to use when negotiating the use of MLP with the peer.
Multiclass	Indicates whether the Multiclass Multilink PPP (MCMP) feature is enabled on this PPP connection.
Group	The number of the multilink-group interface to which the physical link is restricted.
Interleave	Indicates whether the PPP multilink interleave feature is enabled on this PPP connection.
Add button	Opens the PPP Dialog Box, page K-78. From here you can define the authentication and multilink settings for the PPP connection.
Edit button	Opens the PPP Dialog Box, page K-78. From here you can edit the selected PPP connection.
Delete button	Deletes the selected PPP connection from the table.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.

Tip To choose which columns to display in the table, right-click a column header, then select **Show Columns**. For more information about table display options, see Table Columns and Column Heading Features, page 3-26.

PPP Dialog Box

Use the PPP dialog box to configure PPP connections on the router. When you configure a PPP connection, you can define the type of authentication and authorization to perform and define multilink parameters.

Navigation Path

Go to the PPP/MLP Policy Page, page K-76, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Defining PPP Connections, page 15-61

Field Reference

Table K-34 PPP Dialog Box

Element	Description
Interface	The interface on which PPP encapsulation is enabled. Enter the name of an interface or interface role, or click **Select** to display an Object Selectors, page F-593. The following interface types support PPP: • Async • Group-Async • Serial • High-Speed Serial Interface (HSSI) • Dialer • BRI, PRI (ISDN) • Virtual template • Multilink If the interface role you want is not listed, click the **Create** button in the selector to display the Interface Role Dialog Box, page F-464. From here you can create an interface role object. You cannot define PPP on: • Subinterfaces. • Serial interfaces with Frame Relay encapsulation. • Virtual template interfaces defined as Ethernet or tunnel types (serial is supported). **Note** You can define only one PPP connection per interface. **Note** Deployment might fail if you define PPP on a virtual template that is also used in an 802.1x policy. See 802.1x Policy Page, page K-179.
PPP tab	Defines the type of authentication and authorization to perform on the PPP connection. See PPP Dialog Box—PPP Tab, page K-80.

Table K-34 PPP Dialog Box (Continued)

MLP tab	Defines how to split and recombine sequential datagrams across multiple logical data links using Multilink PPP (MLP). See PPP Dialog Box—MLP Tab, page K-84.
OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

PPP Dialog Box—PPP Tab

Use the PPP tab of the PPP dialog box to define the types of authentication and authorization to perform on the PPP connection.

Navigation Path

Go to the PPP Dialog Box, page K-78, then click the **PPP** tab.

Related Topics

- PPP Dialog Box—MLP Tab, page K-84

Field Reference

Table K-35 PPP Dialog Box—PPP Tab

Element	Description
Authentication settings	
PPP Encapsulation	When selected, indicates that PPP encapsulation is enabled for the selected interface. This field is read-only.

Table K-35 PPP Dialog Box—PPP Tab (Continued)

Protocol	The authentication protocols to use: • CHAP—Challenge-Handshake Authentication Protocol. • PAP—Password Authentication Protocol. • MS-CHAP—Version 1 of the Microsoft version of CHAP (RFC 2433). • MS-CHAP-2—Version 2 of the Microsoft version of CHAP (RFC 2759). • EAP—Extensible Authentication Protocol. You may select one or more authentication protocols, as required.
Options	The authentication options to use: • Call In—When selected, authentication is performed on incoming calls. • Call Out—When selected, authentication is performed on outgoing calls. • Call Back—When selected, authentication is performed on callback. • One Time—When selected, one-time passwords are used for authentication. One-time passwords are considered highly secure since each one is used only once. When deselected, one-time passwords are not used. **Note** AAA authentication must be enabled in order to use one-time passwords. See AAA Policy Page, page K-87. One-time passwords cannot be used with CHAP. • Optional—When selected, allows a mobile station in a Packet Data Serving Node (PDSN) configuration to receive Simple IP and Mobile IP services without using CHAP or PAP. When deselected, mobile stations must use CHAP or PAP to receive Simple IP and Mobile IP services.

Table K-35 PPP Dialog Box—PPP Tab (Continued)

Authenticate Using	AAA authentication settings for the PPP connection: • PPP Default List—Defines a default list of methods to be queried when authenticating a user for PPP. Enter the names of one or more AAA server group objects (up to four) in the Prioritized Method List field, or click **Select** to display an Object Selectors, page F-593. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. The device tries initially to authenticate users using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received. **Tip** After you create the default list for one PPP connection, you can use it for other PPP connections on this device. If the AAA server group you want is not listed, click the **Create** button in the selector to display the AAA Server Group Dialog Box, page F-12. From here you can define a AAA server group object. • Prioritized Method List—Defines a sequential list of methods to be queried when authenticating a user for this PPP connection only. **Note** Leave this field blank to perform authentication using the local database on the router.
PAP Authentication settings	
Username	The username to send in PAP authentication requests. The username is case sensitive.
Password	The password to send in PAP authentication requests. Enter the password again in the Confirm field. The password can contain 1 to 25 uppercase or lowercase alphanumeric characters. The password is case sensitive. The username and password are sent if the peer requests the router to authenticate itself using PAP.
Encrypted Password	When selected, this indicates that the password you entered is already encrypted. When deselected, this indicates that the password you entered is in clear text.

Table K-35 PPP Dialog Box—PPP Tab (Continued)

CHAP Authentication settings	
Hostname	By default, the router uses its hostname to identify itself to the peer. If required, you can enter a different hostname to use for all CHAP challenges and responses. For example, use this field to specify a common alias for all routers in a rotary group.
Secret	The secret used to compute the response value for any CHAP challenge from an unknown peer. Enter the secret again in the Confirm field.
Encrypted Secret	When selected, this indicates that the password you entered is already encrypted. When deselected, this indicates that the password you entered is in clear text.
Authorization settings	
Authorize Using	AAA authorization settings for the PPP connection: • AAA Policy Default List—Uses the default authorization method list that is defined in the device's AAA policy. See AAA Policy Page, page K-87. • Prioritized Method List—Defines a sequential list of methods to be queried when authorizing a user. Enter the names of one or more AAA server group objects (up to four), or click **Select** to display an Object Selectors, page F-593. Use the tranverse arrows in the AAA Sever Groups Selector to select server groups and then the up and down arrows to define the order in which selected server groups should be used. **Note** The device tries initially to authorize users using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received. If the AAA server group you want is not listed, you can click the **Create** button in the selector to display the AAA Server Group Dialog Box, page F-12. From here you can define a AAA server group object. **Note** Leave this field blank to perform authorization using the local database on the router.

PPP Dialog Box—MLP Tab

Use the MLP tab of the PPP dialog box to define Multilink PPP (MLP) parameters for the selected PPP connection.

Navigation Path

Go to the PPP Dialog Box, page K-78, then click the **MLP** tab.

Related Topics

- PPP Dialog Box—PPP Tab, page K-80

Field Reference

Table K-36 PPP Dialog Box—MLP Tab

Element	Description
Enable Multilink PPP (MLP)	When selected, MLP is enabled on this PPP connection. When deselected, MLP is disabled.
Allow Multiple Data Classes	When selected, enables multiple data classes on the MLP bundle. Delay-sensitive traffic is placed into Class 1, where it can be interleaved but never fragmented. Normal data traffic is placed into Class 0, which is subject to fragmentation just as regular multilink packets are. When deselected, all traffic is subject to fragmentation.
Enable Interleaving of Packets Among Fragments of Larger Packets	When selected, enables the interleaving of packets among the fragments of larger packets on the MLP bundle. **Note** If you enable interleaving without defining a fragment delay, the default delay of 30 seconds is configured. This value does not appear in Security Manager or in the device configuration. When deselected, interleaving is disabled. **Note** Serial interfaces do not support interleaving.

Table K-36 PPP Dialog Box—MLP Tab (Continued)

Multilink Group	Applies only to serial, Group-Async, and multilink interfaces. Restricts the physical link to the selected multilink-group interface. Enter the name of a multilink interface or interface role, or click **Select** to display an Object Selectors, page F-593. If the interface role you want is not listed, click the **Create** button in the selector to display the Interface Role Dialog Box, page F-464. From here you can create an interface role object. This option is typically used in static leased-line environments, where the remote systems to which the device's serial lines are connected are known in advance. In effect, this option dedicates a specific interfaces to a particular user, even when that user is not connected. If a peer at the other end of the link tries to join a different bundle, the connected is severed.
Maximum Fragment Delay	The maximum amount of time that should be required to transmit a fragment on the MLP bundle. Valid values range from 1 to 1000 milliseconds. Fragment size is determined by the defined fragment delay and the bandwidth of the links. **Note** Serial interfaces do not support this feature.

Table K-36 PPP Dialog Box—MLP Tab (Continued)

Endpoint Type	The identifier used by the router when transmitting packets on the MLP bundle: • [null]—Negotiation is conducted without using an endpoint discriminator. (No CLI command is generated.) • Hostname—The hostname of the router. This option is useful when multiple routers are using the same username to authenticate but have different hostnames. • IP—A defined IP address. Enter an address or the name of a network/host object, or click **Select** to display an Object Selectors, page F-593. • MAC—The MAC address of a specific interface. Enter the name of an interface or interface role, or click **Select** to display an Object Selectors, page F-593. • None—Negotiation is conducted without using an endpoint discriminator. (The relevant CLI command is generated, but no endpoint discriminator is provided.) This option is useful when the router is connected to a malfunctioning peer that does not handle the endpoint discriminator properly. • Phone—An E.164-compliant telephone number. Enter the number in the field displayed. • String—A character string. Enter the string in the field displayed. The default endpoint discriminator is either the globally configured hostname, or the PAP username or CHAP hostname (depending on the authentication protocol being used), if you have configured those values on the PPP tab.
MRRU Local Peer	The maximum receive reconstructed unit (MRRU) value of the local peer. This value represents the maximum size packet that the local router is capable of receiving. Valid values range from 128 to 16384 bytes. The default is the maximum transmission unit (MTU) of the multilink group interface and 1524 bytes for all other interfaces.

Table K-36 PPP Dialog Box—MLP Tab (Continued)

MRRU Remote Peer	The maximum receive reconstructed unit (MRRU) value of the remote peer. This value represents the maximum size packet that the remote peer is capable of receiving. Valid values range from 128 to 16384 bytes. The default is 1524 bytes.
Maximum FIFO Queue Size	The maximum queue depth when the bundle uses first-in, first-out (FIFO) queuing. Valid values range from 2 to 255 packets. The default is 8.
Maximum QoS Queue Size	The maximum queue depth when the bundle uses non-FIFO queuing. Valid values range from 2 to 255 packets. The default is 2.

AAA Policy Page

Use the AAA page to define the default authentication, authorization, and accounting methods to use on the router. You do this by configuring method lists, which define which methods to use and the sequence in which to use them.

Note You can use the method lists defined in this policy as default settings when you configure AAA on the router's console port and VTY lines. See Console Policy Page, page K-117 and VTY Policy Page, page K-129.

Navigation Path

- (Device view) Select **Platform > Device Admin > AAA** from the Policy selector.
- (Policy view) Select **Router Platform > Device Admin > AAA** from the Policy Type selector. Right-click **AAA** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- AAA on Cisco IOS Routers, page 15-66
- Understanding AAA Server Objects, page 9-22
- Understanding AAA Server Group Objects, page 9-15
- Console Policy Page, page K-117

- VTY Policy Page, page K-129
- Chapter K, "Router Platform User Interface Reference"

Field Reference

Table K-37 AAA Page

Element	Description
Authentication tab	Defines the login authentication methods to use and the sequence in which to use them. See AAA Page—Authentication Tab, page K-88.
Authorization tab	Defines the types of network, EXEC, and command authorization to perform and the methods to use for each type. See AAA Page—Authorization Tab, page K-90.
Accounting tab	Defines types of connection, EXEC, and command accounting to perform and the methods to use for each type. See AAA Page—Accounting Tab, page K-93.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** icon on the toolbar.

AAA Page—Authentication Tab

Use the Authentication tab of the AAA page to define the methods used to authenticate users who access the device. Authentication methods are defined in a method list, which define the security protocols to use, such as RADIUS and TACACS+.

Note You can use the method list defined in this policy on the console and VTY lines that are used to communicate with the device. See Console Policy Page, page K-117 and VTY Line Dialog Box—Authentication Tab, page K-136.

Navigation Path

Go to the AAA Policy Page, page K-87, then click the **Authentication** tab.

Related Topics

- Defining AAA Services, page 15-70

- Understanding Method Lists, page 15-69
- AAA Server Group Dialog Box, page F-12
- Predefined AAA Authentication Server Groups, page 9-15

Field Reference

Table K-38 AAA Page—Authentication Tab

Element	Description
Enable Device Login Authentication	When selected, enables the authentication of all users when they log in to the device, using the methods defined in the method list. When deselected, authentication is not performed.
Prioritized Method List	Defines a sequential list of methods to be queried when authenticating a user. Enter the names of one or more AAA server group objects (up to four), or click **Select** to display an Object Selectors, page F-593. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. The device tries initially to authenticate users using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received. Supported methods include Line, Local, Kerberos, RADIUS, TACACS+, and None. **Note** If you select None as a method, it must appear as the last method in the list.
Maximum Number of Attempts	The maximum number of unsuccessful authentication attempts before a user is locked out. This feature is disabled by default. Valid values range from 1 to 65535. **Note** From the standpoint of the user, there is no distinction between a normal authentication failure and an authentication failure due to being locked out. The system administrator has to explicitly clear the status of a locked-out user using **clear** commands.

AAA Page—Authorization Tab

Use the Authorization tab of the AAA page to define the type of authorization services to enable on the device and the methods to use for each type. Security Manager supports the following types of authorization:

- Network—Authorizes various types of network connections, such as PPP.
- EXEC—Authorizes the launching of EXEC sessions.
- Command—Authorizes the use of all EXEC mode commands that are associated with specific privilege levels.

Note You can use the method lists defined in this policy on the console and VTY lines that are used to communicate with the device. See Console Policy Page, page K-117 and VTY Line Dialog Box—Authentication Tab, page K-136.

Navigation Path

Go to the AAA Policy Page, page K-87, then click the **Authorization** tab.

Related Topics

- Defining AAA Services, page 15-70
- Supported Authorization Types, page 15-67
- Understanding Method Lists, page 15-69
- AAA Server Group Dialog Box, page F-12

Field Reference

Table K-39 AAA Page—Authorization Tab

Element	Description
Network Authorization settings	
Enable Network Authorization	When selected, enables the authorization of network connections, such as PPP, SLIP, or ARAP connections, using the methods defined in the method list. When deselected, network authorization is not performed.

Table K-39 AAA Page—Authorization Tab (Continued)

Prioritized Method List	Defines a sequential list of methods to be queried when authorizing a user. Enter the names of one or more AAA server group objects (up to four), or click **Select** to display an Object Selectors, page F-593. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. The device tries initially to authorize users using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received. Supported methods include RADIUS, TACACS+, Local, and None. **Note** RADIUS uses the same server for authentication and authorization. Therefore, if you use define a RADIUS method list for authentication, you must define the same method list for authorization. **Note** If you select None as a method, it must appear as the last method in the list.
EXEC Authorization settings	
Enable CLI/EXEC Operations Authorization	When selected, this type of authorization determines whether the user is permitted to open an EXEC (CLI) session, using the methods defined in the method list. When deselected, EXEC authorization is not performed.
Prioritized Method List	Defines a sequential list of methods to be queried when authorizing a user. Enter the names of one or more AAA server group objects (up to four), or click **Select** to display an Object Selectors, page F-593. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. The device tries initially to authorize users using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received.
Command Authorization settings	
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
Privilege Level	The privilege level to which the command authorization definition applies.
Prioritized Method List	The method list to use when authorizing users with this privilege level.

Table K-39 AAA Page—Authorization Tab (Continued)

Add button	Opens the Command Authorization Dialog Box, page K-92. From here you can configure a command authorization definition.
Edit button	Opens the Command Authorization Dialog Box, page K-92. From here you can edit the command authorization definition.
Delete button	Deletes the selected command authorization definitions from the table.

Command Authorization Dialog Box

Use the Command Authorization dialog box to define which methods to use when authorizing the EXEC commands that are associated with a given privilege level. This enables you to authorize all commands associated with a specific privilege level, from 0 to 15.

Navigation Path

From the AAA Page—Authorization Tab, page K-90, click the **Add** button beneath the Command Authorization table.

Related Topics

- Defining AAA Services, page 15-70
- Supported Authorization Types, page 15-67
- Understanding Method Lists, page 15-69

Field Reference

Table K-40 Command Authorization Dialog Box

Element	Description
Privilege Level	The privilege level for which you want to define a command accounting list. Valid values range from 0 to 15.

Table K-40 Command Authorization Dialog Box (Continued)

Prioritized Method List	Defines a sequential list of methods to be used when authorizing a user. Enter the names of one or more AAA server group objects (up to four), or click **Select** to display an Object Selectors, page F-593. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. The device tries initially to authorize users using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received. If the AAA server group you want is not listed, click the **Create** button in the selector to display the AAA Server Group Dialog Box, page F-12. From here you can define a AAA server group object. Supported methods include TACACS+, Local, and None. **Note** If you select None as a method, it must appear as the last method in the list.
OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

AAA Page—Accounting Tab

Use the Accounting tab of the AAA page to define the type of accounting services to enable on the device and the methods to use for each type. Security Manager supports the following types of accounting:

- Connection—Records information about all outbound connections made from this device.
- EXEC—Records information about user EXEC sessions on the devices, including the username, date, start and stop times, and the IP address.
- Command—Records information about the EXEC commands executed on the device by users with specific privilege levels.

In addition, you use the Accounting page to determine when accounting records should be generated and whether they should be broadcast to more than one AAA server.

Note You can use the method lists defined in this policy on the console and VTY lines that are used to communicate with the device. See Console Policy Page, page K-117 and VTY Line Dialog Box—Authentication Tab, page K-136.

Navigation Path

Go to the AAA Policy Page, page K-87, then click the **Accounting** tab.

Related Topics

- Defining AAA Services, page 15-70
- Supported Accounting Types, page 15-67
- Understanding Method Lists, page 15-69
- AAA Server Group Dialog Box, page F-12

Field Reference

Table K-41 AAA Page—Accounting Tab

Element	Description
Connection Accounting settings	
Enable Connection Accounting	When selected, enables the recording of information about outbound connections (such as Telnet) made over this device, using the methods defined in the method list. When deselected, connection accounting is not performed.
Generate Accounting Records for	Defines when the device sends an accounting notice to the accounting server: • Start and Stop—Generates accounting records at the beginning and the end of the user process. The user process begins regardless of whether the accounting server receives the “start” accounting record. • Stop Only—Generates an accounting record at the end of the user process only. • None—Disables this type of accounting.

Table K-41 AAA Page—Accounting Tab (Continued)

Prioritized Method List	Defines a sequential list of methods to be queried when creating connection accounting records for a user. Enter the names of one or more AAA server group objects (up to four), or click **Select** to display an Object Selectors, page F-593. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. Supported methods include RADIUS and TACACS+.
Enable Broadcast to Multiple Servers	When selected, enables the sending of accounting records to multiple AAA servers. Accounting records are sent simultaneously to the first server in each AAA server group defined in the method list. If the first server is unavailable, failover occurs using the backup servers defined within that group. When deselected, accounting records are sent only to the first server in the first AAA server group defined in the method list.
EXEC Accounting Settings	
Enable CLI/EXEC Operations Accounting	When selected, enables the recording of basic information about user EXEC sessions, using the methods defined in the method list. When deselected, EXEC accounting is not performed.
Generate Accounting Records for	See description Table N-91 on page N-131.
Prioritized Method List	Defines a sequential list of methods to be queried when creating connection accounting records for a user. Enter the names of one or more AAA server group objects (up to four), or click **Select** to display an Object Selectors, page F-593. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used.
Enable Broadcast to Multiple Servers	When selected, enables the sending of accounting records to multiple AAA servers. Accounting records are sent simultaneously to the first server in each AAA server group defined in the method list. If the first server is unavailable, failover occurs using the backup servers defined within that group.
Command Accounting settings	
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
Privilege Level	The privilege level to which the command authorization definition applies.

Table K-41 AAA Page—Accounting Tab (Continued)

Generate Accounting Records for	The points in the process where the device sends an accounting notice to the accounting server.
Enable Broadcast	Whether accounting records are broadcast to multiple servers simultaneously.
Prioritized Method List	The method list to use when authorizing users with this privilege level.
Add button	Opens the Command Accounting Dialog Box, page K-96. From here you can configure a command accounting definition.
Edit button	Opens the Command Accounting Dialog Box, page K-96. From here you can edit the command accounting definition.
Delete button	Deletes the selected command accounting definitions from the table.

Command Accounting Dialog Box

Use the Command Accounting dialog box to define which methods to use when recording information about the EXEC commands that are executed for a given privilege level. Each accounting record includes a list of the commands executed for that privilege level, as well as the date and time each command was executed, and the name of the user who executed it.

Navigation Path

From the AAA Page—Accounting Tab, page K-93, click the **Add** button beneath the Command Accounting table.

Related Topics

- Defining AAA Services, page 15-70
- Supported Accounting Types, page 15-67
- Understanding Method Lists, page 15-69

Field Reference

Table K-42 Command Accounting Dialog Box

Element	Description
Privilege Level	The privilege level for which you want to define a command accounting list. Valid values range from 0 to 15.
Generate Accounting Records for	Defines when the device sends an accounting notice to the accounting server: • Start and Stop—Generates accounting records at the beginning and the end of the user process. The user process begins regardless of whether the accounting server receives the "start" accounting record. • Stop Only—Generates an accounting record at the end of the user process only. • None—No accounting records are generated.
Prioritized Method List	Defines a sequential list of methods to be used when creating accounting records for a user. Enter the names of one or more AAA server group objects (up to four), or click **Select** to display an Object Selectors, page F-593. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. The device tries initially to perform accounting using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received. If the AAA server group you want is not listed, click the **Create** button in the selector to display the AAA Server Group Dialog Box, page F-12. From here you can define a AAA server group object. TACACS+ is the only supported method, but you can select multiple AAA server groups configured with TACACS+. **Note** If you select None as a method, it must appear as the last method in the list.
Enable Broadcast to Multiple Servers	When selected, enables the sending of accounting records to multiple AAA servers. Accounting records are sent simultaneously to the first server in each AAA server group defined in the method list. If the first server is unavailable, failover occurs using the backup servers defined within that group. When deselected, accounting records are sent only to the first server in the first AAA server group defined in the method list.

Table K-42 Command Accounting Dialog Box (Continued)

OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

Accounts and Credential s Policy Page

Use the Accounts and Credentials page to define the enable password or enable secret password assigned to the router. In addition, you can define a list of usernames that can be used to access the router.

For more information, see Defining Accounts and Credential Policies, page 15-73.

Navigation Path

- (Device view) Select **Platform > Device Admin > Accounts and Credentials** from the Policy selector.
- (Policy view) Select **Router Platform > Device Admin > Accounts and Credentials** from the Policy Type selector. Right-click **Accounts and Credentials** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- User Accounts and Device Credentials on Cisco IOS Routers, page 15-72
- Chapter K, “Router Platform User Interface Reference”
- User Account Dialog Box, page K-100

Field Reference

Table K-43 Accounts and Credentials Page

Element	Description
Enable Secret Password	The enable secret password for entering privileged EXEC mode on the router. This option offers better security than the Enable Password option. The enable secret password can contain between 1-25 alphanumeric characters. The first character must be a letter. Spaces are allowed, but leading spaces are ignored. Question marks are also allowed. **Note** You can discover an encrypted password, but any password you enter must be in clear text. If you modify an encrypted password, it is saved as clear text. **Note** After you set an enable secret password, you can switch to an enable password only if the enable secret is disabled or an older version of Cisco IOS software is being used, such as when running an older rxboot image.
Enable Password	The enable password for entering privileged EXEC mode on the router. The enable password can contain between 1-25 alphanumeric characters. The first character must be a letter. Spaces are allowed, but leading spaces are ignored. Question marks are also allowed. **Note** You must enter the password in clear text.
Enable Password Encryption Service	When selected, encrypts all passwords on the device, including the enable password (which is otherwise saved in clear text). For example, use this option to encrypt username passwords, authentication key passwords, console and VTY line access passwords, and BGP neighbor passwords. This command is primarily used for keeping unauthorized individuals from viewing your passwords in your configuration file. When deselected, device passwords are stored unencrypted in the configuration file. **Note** This option does not provide a high level of network security. You should also take additional network security measures.
User Accounts Table	
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.

Table K-43 Accounts and Credentials Page (Continued)

Username	The username that can be used to access the router. The username must be a single word up to 64 characters in length. Spaces and quotation marks are not allowed.
Encryption	Indicates whether password information for the user is encrypted using MD5 encryption.
Privilege Level	The privilege level assigned to the user.
Add button	Opens the User Account Dialog Box, page K-100. From here you can define a user account.
Edit button	Opens the User Account Dialog Box, page K-100. From here you can edit the selected user.
Delete button	Deletes the selected user accounts from the table.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** icon on the toolbar.

Tip To choose which columns to display in the table, right-click a column header, then select **Show Columns**. For more information about table display options, see Table Columns and Column Heading Features, page 3-26.

User Account Dialog Box

Employ the User Account dialog box to define a username and password combination that can be used by Security Manager to access the router. You can also define the privilege level of the user account, which determines whether you can configure all commands on this router or only a subset of them.

Note Remember—there may be additional user accounts defined on the router using other methods, such as the CLI.

Navigation Path

Go to the Accounts and Credential s Policy Page, page K-98, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Defining Accounts and Credential Policies, page 15-73
- User Accounts and Device Credentials on Cisco IOS Routers, page 15-72
- Understanding FlexConfig Objects, page 9-52

Field Reference

Table K-44 User Account Dialog Box

Element	Description
Username	The username for accessing the router.
Password	The password for accessing the router with this user account. **Note** You can discover an encrypted password, but any password you enter must be in clear text.
Confirm	Confirms the password for this user account.
Encrypt password using MD5	When selected, uses MD5 encryption to encrypt the password for this user account. This is the default. When deselected, the password is sent to the router unencrypted.
Privilege Level	The privilege level assigned to the user account. Valid values range from 0 to 15: • 0—Grants access to these commands only: **disable**, **enable**, **exit**, **help**, and **logout**. • 1—Enables nonprivileged access to the router (normal EXEC-mode use privileges). • 15—Enables privileged access to the router (traditional enable privileges). **Note** Levels 2-14 are not normally used in a default configuration, but custom configurations can be created by moving commands that are normally at level 15 to a lower level and commands that are normally at level 1 to a higher level. You can configure the privilege levels of commands using the CLI or by defining a FlexConfig.

Table K-44 User Account Dialog Box (Continued)

OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

Bridging Policy Page

Use the Bridging page to define bridge groups that can perform integrated routing and bridging on the router. For more information, see Defining Bridge Groups, page 15-78.

Navigation Path

- (Device view) Select **Platform > Device Admin > Bridging** from the Policy selector.
- (Policy view) Select **Router Platform > Device Admin > Bridging** from the Policy Type selector. Right-click **Bridging** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- Bridging on Cisco IOS Routers, page 15-75
- Chapter K, "Router Platform User Interface Reference"

Field Reference

Table K-45 Bridging Page

Element	Description
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
Group Number	The number that identifies the bridge group.
Group Interfaces	The interfaces and interface roles that are included in the bridge group.
Add button	Opens the Bridge Group Dialog Box, page K-103. From here you can define a bridge group.

Table K-45 Bridging Page (Continued)

Edit button	Opens the Bridge Group Dialog Box, page K-103. From here you can edit the bridge group.
Delete button	Deletes the selected bridge groups from the table.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** icon on the toolbar.

Tip To choose which columns to display in the table, right-click a column header, then select **Show Columns**. For more information about table display options, see Table Columns and Column Heading Features, page 3-26.

Bridge Group Dialog Box

Use the Bridge Group dialog box to define bridge groups on the router. Each bridge group can contain multiple Layer 3 interfaces of various types, including serial interfaces.

Note All bridge groups use the standard Spanning Tree Protocol (IEEE 802.1D). Use CLI commands or FlexConfigs to bridge other protocols, such as AppleTalk or IPX, and to use other spanning tree protocols, such as VLAN-Bridge.

Navigation Path

Go to the Bridging Policy Page, page K-102, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Defining Bridge Groups, page 15-78
- Bridging on Cisco IOS Routers, page 15-75
- Understanding Interface Role Objects, page 9-132

Field Reference

Table K-46 Bridge Group Dialog Box

Element	Description
Group Number	The number assigned to the bridge group. Valid values range from 1 to 255.
Group Interfaces	The interfaces that are included in the bridge group. Enter the name of one or more interfaces and interface roles, or click **Select** to display an Object Selectors, page F-593. You can select most Layer 3 interfaces, including serial interfaces, provided the serial interface is configured with high-level data link control (HDLC) or Frame Relay encapsulation. Each interface can belong to only one bridge group. You can select a LAN subinterface only if the parent interface is configured with Inter-Switch Link (ISL) or 802.1Q encapsulation. **Note** Certain types of interfaces, such as loopback, tunnel, null, and BVI, cannot be bridged. If the interface role you want is not listed, click the **Create** button in the selector to display the Interface Role Dialog Box, page F-464. From here you can create an interface role object. **Note** Make sure that your bridge group does not prevent Security Manager from communicating with the device.
OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

Clock Policy Page

Use the Clock page to configure the time zone in which the router is located and the settings for Daylight Saving Time (DST). For more information, see Time Zone Settings on Cisco IOS Routers, page 15-79.

Tip You can configure the local time on the router by defining an NTP policy or by configuring the **clock set** command using the CLI.

Navigation Path

- (Device view) Select **Platform > Device Admin > Clock** from the Policy selector.
- (Policy view) Select **Router Platform > Device Admin > Clock** from the Policy Type selector. Right-click **Clock** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- NTP Policy Page, page K-174
- Chapter K, "Router Platform User Interface Reference"

Field Reference

Table K-47 Clock Page

Element	Description
Device Time Zone	The time zone in which the router is located, expressed in relation to GMT (Greenwich Mean Time), also known as UTC (Coordinated Universal Time).
Daylight Savings Time (Summer Time)	The type of DST to apply to the local time on the router: • Set by Date—Enables you to define the exact date and time when DST begins and ends. • Set by Day—Enables you to define the relative recurring date and time when DST begins and ends. For example, you can use this option when DST begins the last Sunday of March and ends the last Sunday of October. • None—Daylight savings time is not used.

Table K-47 Clock Page (Continued)

Additional Set by Date fields	
Start	The date and time when DST begins: • Date—Click the calendar icon to select the start date. • Hour—Select the start hour. • Minute—Select the start minute.
End	The date and time when DST ends: • Date—Click the calendar icon to select the end date. • Hour—Select the end hour. • Minute—Select the end minute. **Note** Cisco IOS Software supports dates up to and including December 31st, 2035.
Additional Set by Day fields	
Specify Recurring Time	When selected, the router implements DST according to the dates and times specified in this policy. When deselected, the router implements DST according to the schedule used throughout most of the United States.
Start	The relative date and time when daylight savings time begins: • Month—Select the month. • Week—Select the week of the month (1, 2, 3, 4, first, or last). • Weekday—Select the day of the week. • Hour—Select the hour. • Minute—Select the minute. For example, if DST begins at 1:00 a.m. on the last Sunday of each March, select March, last, Sunday, 1, and 00.

Table K-47 Clock Page (Continued)

End	The relative date and time when daylight savings time ends: • Month—Select the month. • Week—Select the week of the month (1, 2, 3, 4, first, or last). • Weekday—Select the day of the week. • Hour—Select the hour. • Minute—Select the minute.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.

CPU Policy Page

Use the CPU page to configure settings related to router CPU utilization, including the thresholds for sending log messages, the size of the CPU history table, and whether to enable automatic CPU Hog profiling.

For more information, see Defining CPU Utilization Settings, page 15-82.

Navigation Path

- (Device view) Select **Platform > Device Access > CPU** from the Policy selector.
- (Policy view) Select **Router Platform > Device Access > CPU** from the Policy Type selector. Right-click **CPU** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- Memory Policy Page, page K-161
- Logging Setup Policy Page, page K-192
- Syslog Servers Policy Page, page K-197
- Chapter K, “Router Platform User Interface Reference”

Field Reference

Table K-48 CPU Page

Element	Description
CPU Utilization Statistics	Settings related to the history table for CPU utilization statistics: • History Table Entry Limit—The percentage of CPU utilization that a process must use to be included in the history table. • History Table Size—The length of time for which CPU statistics are stored in the history table. Valid values range from 5 to 86400 seconds (24 hours). The default is 600 seconds (10 minutes).
CPU Total Utilization	The thresholds for total CPU utilization that trigger notifications: • Enable CPU Total Utilization—When selected, CPU total utilization thresholds are enabled. When deselected, these thresholds are disabled and do not trigger notifications. This is the default. • Maximum Total Utilization Resources—The percentage of CPU resources that, when usage *exceeds* this level for the defined interval, triggers a notification. • Maximum Total Utilization Violation Duration—The violation interval that triggers a maximum CPU threshold notification. Valid values range from 5 to 86400 seconds (24 hours). • Minimum Total Utilization Resources—The percentage of CPU resources that, when usage *falls below* this level for the defined interval, triggers a notification. • Minimum Total Utilization Violation Duration—The violation interval that triggers a minimum CPU threshold notification. Valid values range from 5 to 86400 seconds (24 hours).

Table K-48 CPU Page (Continued)

CPU Interrupt Utilization	The thresholds for CPU interrupt utilization that trigger notifications: • Enable CPU Interrupt Utilization—When selected, CPU interrupt utilization thresholds are enabled. When deselected, these thresholds are disabled and do not trigger notifications. This is the default. • Maximum Interrupt Utilization Resources—The percentage of CPU resources that, when usage *exceeds* this level for the defined interval, triggers a notification. • Maximum Interrupt Utilization Violation Duration—The violation interval that triggers a maximum CPU threshold notification. Valid values range from 5 to 86400 seconds (24 hours). • Minimum Interrupt Utilization Resources—The percentage of CPU resources that, when usage *falls below* this level for the defined interval, triggers a notification. • Minimum Interrupt Utilization Violation Duration—The violation interval that triggers a minimum CPU threshold notification. Valid values range from 5 to 86400 seconds (24 hours).
CPU Process Utilization	The thresholds for CPU process utilization that trigger notifications: • Enable CPU Process Utilization—When selected, CPU process utilization thresholds are enabled. When deselected, these thresholds are disabled and do not trigger notifications. This is the default. • Maximum Process Utilization Resources—The percentage of CPU resources that, when usage *exceeds* this level for the defined interval, triggers a notification. • Maximum Process Utilization Violation Duration—The violation interval that triggers a maximum CPU threshold notification. Valid values range from 5 to 86400 seconds (24 hours). • Minimum Process Utilization Resources—The percentage of CPU resources that, when usage *falls below* this level for the defined interval, triggers a notification. • Minimum Process Utilization Violation Duration—The violation interval that triggers a minimum CPU threshold notification. Valid values range from 5 to 86400 seconds (24 hours).

Table K-48 CPU Page (Continued)

Extended CPU History Size	The size of the history to collect for the extended CPU load, in increments of 5 seconds. Valid values range from 2 to 720. The default is 12, which is equivalent to a 1-minute history.
Enable Automatic CPU Hog Profiling	When selected, automatic CPU Hog profiling is enabled. This is the default. When deselected, automatic CPU Hog profiling is disabled. This feature predicts when a process could hog the CPU and begins profiling that process. **Note** To view the CPU Hog profile data, use the **show processes cpu autoprofile hog** command in the CLI.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.

HTTP Policy Page

Use the HTTP page to configure HTTP and HTTPS access on the router. You can configure HTTP policies on a Cisco IOS router from the following tabs on the HTTP policy page:

- HTTP Page—Setup Tab, page K-111
- HTTP Page—AAA Tab, page K-112

For more information, see HTTP and HTTPS on Cisco IOS Routers, page 15-83.

Navigation Path

- (Device view) Select **Platform > Device Admin > Device Access > HTTP** from the Policy selector.
- (Policy view) Select **Router Platform > Device Admin > Device Access > HTTP** from the Policy Type selector. Right-click **HTTP** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- Chapter K, "Router Platform User Interface Reference"

HTTP Page—Setup Tab

Use the Setup tab of the HTTP page to enable HTTP and HTTP over Secure Socket Layer (HTTP over SSL or HTTPS) on the router. You can optionally limit access to these protocols to the addresses defined in an access control list.

Note As a general rule, Cisco IOS routers that have been discovered by Security Manager already have HTTPS enabled because Security Manager uses SSL as the default protocol for communicating with them. See Setting Up SSL on Cisco IOS Routers, page 5-6.

Navigation Path

Go to the HTTP Policy Page, page K-110, then click the **Setup** tab.

Related Topics

- HTTP Page—AAA Tab, page K-112
- HTTP and HTTPS on Cisco IOS Routers, page 15-83

Field Reference

Table K-49 HTTP Page—Setup Tab

Element	Description
Enable HTTP	When selected, an HTTP server is enabled on the router. When deselected, HTTP is disabled on the router. This is the default for devices that were not discovered.
HTTP Port	The port number to use for HTTP. Valid values are 80 or any value from 1024 to 65535. The default is 80.

Table K-49 HTTP Page—Setup Tab (Continued)

Enable SSL	When selected, a secure HTTP server (HTTP over SSL or HTTPS) is enabled on the router. When deselected, HTTPS is disabled. This is the default for devices that were not discovered. **Note** If SSL is disabled (or if the HTTP policy as a whole is unassigned), Security Manager cannot communicate with the device after deployment unless you change the transport protocol for this device to SSH. This setting can be found in Device Properties. **Note** We recommend that you disable HTTP when SSL is enabled. This is required to ensure only secure connections to the server.
SSL Port	The port number to use for HTTPS. Valid values are 443 or any value from 1025 to 65535. The default is 443.
Allow Connection From	The numbered ACL that restricts use of HTTP and HTTPS on this device. Enter the name of an ACL object, or click **Select** to display an Object Selectors, page F-593. If the standard ACL you want is not listed, click the **Create** button in the selector to display the Add and Edit Standard Access List Pages, page F-42. From here you can create an ACL object. **Note** If you define an ACL, make sure that it includes the Security Manager server. Otherwise, Security Manager cannot communicate with this device using SSL.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.

HTTP Page—AAA Tab

Use the AAA tab of the HTTP page to define the authentication and authorization methods to perform on users who attempt to access the router using HTTP or HTTPS.

Navigation Path

Go to the HTTP Policy Page, page K-110, then click the **AAA** tab.

Related Topics

- HTTP Page—Setup Tab, page K-111
- HTTP and HTTPS on Cisco IOS Routers, page 15-83

Field Reference

Table K-50 HTTP Page—AAA Tab

Element	Description
Authenticate Using	The type of authentication to use: • AAA—Performs AAA login authentication. • Enable Password—Uses the enable password configured on the router. This is the default. • Local Database—Uses the local username database configured on the router. • TACACS—Uses the TACACS or XTACACS server configured on the router. Applies only to devices using an IOS software version prior to 12.3(8) or 12.3(8)T.
Login Authentication settings	
Enable Device Login Authentication	Applies only when AAA is selected as the authentication method. When selected, authentication is based on the methods defined in the Prioritized Method List field. When deselected, the default authentication list defined in the router's AAA policy is used. See AAA Page—Authentication Tab, page K-88.

Table K-50 HTTP Page—AAA Tab (Continued)

Prioritized Method List	Applies only when the Enable Device Login Authentication check box is selected. Defines a sequential list of methods to be queried when authenticating a user. Enter the names of one or more AAA server group objects (up to four), or click **Select** to display an Object Selectors, page F-593. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. The device tries initially to authenticate users using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received. If the AAA server group you want is not listed, click the **Create** button in the selector to display the AAA Server Group Dialog Box, page F-12. From here you can define a AAA server group object. **Note** If you select None as a method, it must appear as the last method in the list.
EXEC Authorization settings	
Enable CLI/EXEC Operations Authorization	Applies only when AAA is selected as the authentication method. When selected, EXEC authorization is based on the methods defined in the Prioritized Method List field. This type of authorization determines whether the user is permitted to open an EXEC (CLI) session. When deselected, the default EXEC authorization list defined in the router's AAA policy is used. See AAA Page—Authorization Tab, page K-90. **Note** If you leave this option deselected, make sure that EXEC authorization is enabled in the router's AAA policy. Otherwise, you will be unable to connect to the device via HTTP or HTTPS (SSL). This applies to Security Manager as well as other applications, such as SDM and the device's web interface.

Table K-50 HTTP Page—AAA Tab (Continued)

Prioritized Method List	Applies only when the Enable CLI/EXEC Operations Authorization check box is selected. Defines a sequential list of methods to be queried when authorizing a user to open an EXEC (CLI) session. Enter the names of one or more AAA server group objects (up to four), or click **Select** to display an Object Selectors, page F-593. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. The device tries initially to authorize users using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received. If the AAA server group you want is not listed, click the **Create** button in the selector to display the AAA Server Group Dialog Box, page F-12. From here you can define a AAA server group object. **Note** If you select None as a method, it must appear as the last method in the list.
Command Authorization settings	
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
Privilege Level	The privilege level to which the command authorization definition applies.
Prioritized Method List	The method list to use when authorizing users with this privilege level.
Add button	Opens the Command Authorization Override Dialog Box, page K-116. From here you can configure a command authorization definition.
Edit button	Opens the Command Authorization Override Dialog Box, page K-116. From here you can edit the command authorization definition.
Delete button	Deletes the selected command authorization definitions from the table.
HTTP Page button	
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.

Command Authorization Override Dialog Box

Use the Command Authorization Override dialog box to define which methods to use when authorizing the EXEC commands that are associated with a given privilege. This enables you to authorize all commands associated with a specific privilege level, from 0 to 15.

Navigation Path

From the HTTP Page—AAA Tab, page K-112, click the **Add** button beneath the Command Authorization Override table.

Related Topics

- HTTP Policy Page, page K-110
- AAA Policy Page, page K-87

Field Reference

Table K-51 Command Authorization Dialog Box

Element	Description
Privilege Level	The privilege level for which you want to define a command accounting list. Valid values range from 0 to 15.
Prioritized Method List	Defines a sequential list of methods to be used when authorizing a user. Enter the names of one or more AAA server group objects (up to four), or click **Select** to display an Object Selectors, page F-593. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. The device tries initially to authorize users using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received. If the AAA server group you want is not listed, click the **Create** button in the selector to display the AAA Server Group Dialog Box, page F-12. From here you can define a AAA server group object. Supported methods include TACACS+, Local, and None. **Note** If you select None as a method, it must appear as the last method in the list.

Table K-51 Command Authorization Dialog Box (Continued)

OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

Console Policy Page

Use the Console page to configure access to the router over the console port. You can configure console policies on a Cisco IOS router from the following tabs on the Console policy page:

- Console Page—Setup Tab, page K-118
- Console Page—Authentication Tab, page K-121
- Console Page—Authorization Tab, page K-123
- Console Page—Accounting Tab, page K-125

For more information, see Line Access on Cisco IOS Routers, page 15-87.

Navigation Path

- (Device view) Select **Platform > Device Admin > Device Access > Line Access > Console** from the Policy selector.
- (Policy view) Select **Router Platform > Device Admin > Device Access > Line Access > Console** from the Policy Type selector. Right-click **Console** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- VTY Policy Page, page K-129
- Chapter K, "Router Platform User Interface Reference"

Console Page—Setup Tab

Use the Setup tab of the Console page to define the basic parameters of the console port. This includes the password for accessing the port, the privilege level assigned to users, the protocols that are permitted, and the ACLs that limit access.

Navigation Path

Go to the Console Policy Page, page K-117, then click the **Setup** tab.

Related Topics

- Console Page—Authentication Tab, page K-121
- Console Page—Authorization Tab, page K-123
- Console Page—Accounting Tab, page K-125
- VTY Line Dialog Box—Setup Tab, page K-132

Field Reference

Table K-52 Console Page—Setup Tab

Element	Description
Password	The password for accessing the console port. The password is case sensitive and can contain up to 80 alphanumeric characters. The first character cannot be a number. Spaces are not allowed. Enter the password again in the Confirm field.

Table K-52 Console Page—Setup Tab (Continued)

Privilege Level	The privilege level assigned to users connected to the console port. Valid values range from 0 to 15: • 0—Grants access to these commands only: **disable**, **enable**, **exit**, **help**, and **logout**. • 1—Enables nonprivileged access to the router (normal EXEC-mode use privileges). • 15—Enables privileged access to the router (traditional enable privileges). **Note** Levels 2-14 are not normally used in a default configuration, but custom configurations can be created by moving commands that are normally at level 15 to a lower level and commands that are normally at level 1 to a higher level. You can configure the privilege levels of commands using the CLI or by defining a FlexConfig. **Note** If you do not define a value, level 1 is assigned by default. This value does not appear in the device configuration.
Disable all the EXEC sessions to the router via this line	When selected, disables EXEC sessions over this line. Select this option when you want to allow only an outgoing connection on the console. This option is useful for keeping the console port free from unsolicited incoming data that can tie up the line. When deselected, EXEC sessions are enabled on the console port. This is the default. **Note** Selecting this option blocks all access to the device via the console port.
Exec Timeout	The amount of time (in seconds) that the EXEC command interpreter waits to detect user input on the console port. If no input is detected, the line is disconnected. Valid values range from 0 to 2147483. The default is 600 (10 minutes). Setting the value to 0 disables the timeout. **Note** Although the timeout is defined in seconds, it appears in the CLI in the format [mm ss].

Table K-52 Console Page—Setup Tab (Continued)

Output Protocols	The protocols that you can use for outgoing connections on the console port: • All—All supported protocols are permitted. Supported protocols include LAT, MOP, NASI, PAD, rlogin, SSH, Telnet, and V.120. • None—No protocols are permitted. This makes the port unusable by outgoing connections. • Protocol—Enables one or more of the following protocols: – SSH—Secure Shell protocol. – Telnet—Standard TCP/IP terminal emulation protocol. – rlogin—UNIX rlogin protocol. **Note** SSH and rlogin require that you configure AAA authentication. See Console Page—Authentication Tab, page K-121. **Note** Not all IOS Software Versions support rlogin as an output protocol.
Inbound Access List	The ACL that restricts incoming connections on the console port. Enter the name of an ACL object, or click **Select** to display an Object Selectors, page F-593. The object selector enables you to select either standard or extended ACLs as well as to select or create a filter. If the standard ACL you want is not listed, click the **Create** button in the selector to display the Add and Edit Standard Access List Pages, page F-42. From here you can create an ACL object.
Permit VRF Interface Connections	Applies only when an inbound ACL is defined on the console port. When selected, accepts incoming connections from interfaces that belong to a VRF. When deselected, rejects incoming connections from interfaces that belong to a VRF.
Outbound Access List	The ACL that restricts outgoing connections on the console port. Enter the name of an ACL object, or click **Select** to display an Object Selectors, page F-593. The object selector enables you to select either standard or extended ACLs as well as to select or create a filter. If the standard ACL you want is not listed, click the **Create** button in the selector to display the Add and Edit Standard Access List Pages, page F-42. From here you can create an ACL object.

Table K-52 Console Page—Setup Tab (Continued)

Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.

Console Page—Authentication Tab

Use the Authentication tab of the Console page to define the AAA authentication methods to perform on users who attempt to access the console port.

Navigation Path

Go to the Console Policy Page, page K-117, then click the **Authentication** tab.

Related Topics

- Console Page—Setup Tab, page K-118
- Console Page—Authorization Tab, page K-123
- Console Page—Accounting Tab, page K-125
- VTY Line Dialog Box—Authentication Tab, page K-136

Field Reference

Table K-53 Console Page—Authentication Tab

Element	Description
Authenticate Using	Authentication settings for the console port: • None—Authentication is not performed. This is the default. • Local Database—Uses the local username database for authentication. • AAA Policy Default List—Uses the default authentication method list that is defined in the device's AAA policy. See AAA Page—Authentication Tab, page K-88. • Custom Method List—Uses the authentication methods specified in the Authentication Method List field. **Note** If you select local authentication, preview the full configuration before deployment to make sure that the **aaa new-model** command is not configured by another policy (for example, by configuring a method list in the AAA policy) or is already configured on the device itself.
Prioritized Method List	Applies only when Custom Method List is selected as the authentication method. Defines a sequential list of methods to be queried when authenticating a user. Enter the names of one or more AAA server group objects (up to four), or click **Select** to display an Object Selectors, page F-593. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. The device tries initially to authenticate users using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received. If the AAA server group you want is not listed, click the **Create** button in the selector to display the AAA Server Group Dialog Box, page F-12. From here you can define a AAA server group object. **Note** If you select None as a method, it must appear as the last method in the list.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.

Console Page—Authorization Tab

Use the Authorization tab of the Console page to define the EXEC and command authorization methods to perform on users who access the console port.

Note You must enable AAA services on the router to use this feature; otherwise, deployment will fail. See Defining AAA Services, page 15-70.

Navigation Path

Go to the Console Policy Page, page K-117, then click the **Authorization** tab.

Related Topics

- Console Page—Setup Tab, page K-118
- Console Page—Authentication Tab, page K-121
- Console Page—Accounting Tab, page K-125
- VTY Line Dialog Box—Authorization Tab, page K-137

Field Reference

Table K-54 Console Page—Authorization Tab

Element	Description
EXEC Authorization settings	
Authorize EXEC Operations Using	The authorization method that determines whether a user is allowed to run an EXEC session: • None—Authorization is not performed. This is the default. • AAA Policy Default List—Uses the default authorization method list that is defined in the device's AAA policy. See AAA Page—Authorization Tab, page K-90. • Custom Method List—Uses the authorization methods specified in the EXEC Method List field.

Table K-54 Console Page—Authorization Tab (Continued)

Prioritized Method List	Applies only when Custom Method List is selected as the EXEC method. Defines a sequential list of methods to be queried when authorizing a user. Enter the names of one or more AAA server group objects (up to four), or click **Select** to display an Object Selectors, page F-593. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. The device tries initially to authorize users using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received. If the AAA server group you want is not listed, click the **Create** button in the selector to display the AAA Server Group Dialog Box, page F-12. From here you can define a AAA server group object. **Note** If you select None as a method, it must appear as the last method in the list. **Note** RADIUS uses the same server for authentication and authorization. Therefore, if you use define a RADIUS method list for authentication, you must define the same method list for authorization.
Command Authorization settings	
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
Privilege Level	The privilege level to which the command authorization definition applies.
Prioritized Method List	The method list to use when authorizing users with this privilege level.
Add button	Opens the Command Authorization Dialog Box—Line Access, page K-143. From here you can configure a command authorization definition.
Edit button	Opens the Command Authorization Dialog Box—Line Access, page K-143. From here you can edit the command authorization definition.
Delete button	Deletes the selected command authorization definitions from the table.
Authorization tab button	
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.

Console Page—Accounting Tab

Use the Accounting tab of the Console page to define the EXEC, connection, and command accounting methods to perform on users who access the console port.

Note You must enable AAA services on the router to use this feature; otherwise, deployment will fail. See Defining AAA Services, page 15-70.

Navigation Path

Go to the Console Policy Page, page K-117, then click the **Accounting** tab.

Related Topics

- Console Page—Setup Tab, page K-118
- Console Page—Authentication Tab, page K-121
- Console Page—Authorization Tab, page K-123
- VTY Line Dialog Box—Accounting Tab, page K-139

Field Reference

Table K-55 Console Page—Accounting Tab

Element	Description
EXEC Accounting settings	
Perform EXEC Accounting Using	The accounting method to use for recording basic information about user EXEC sessions: • None—Accounting is not performed. This is the default. • AAA Policy Default List—Uses the default EXEC accounting method list that is defined in the device's AAA policy. See AAA Page—Accounting Tab, page K-93. • Custom Method List—Uses the accounting methods specified in the EXEC Method List field. EXEC accounting records basic details about EXEC sessions, such as the username, date, start and stop times, and the access server IP address.

Table K-55 Console Page—Accounting Tab (Continued)

Generate Accounting Records for	Applies only when Custom Method List is selected as the EXEC method. Defines when the device sends an accounting notice to the accounting server: • Start and Stop—Generates accounting records at the beginning and the end of the user process. The user process begins regardless of whether the accounting server receives the "start" accounting record. This is the default. • Stop Only—Generates an accounting record at the end of the user process only. • None—No accounting records are generated.
Prioritized Method List	Applies only when Custom Method List is selected as the EXEC method. Defines a sequential list of methods to be queried when creating accounting methods for a user. Enter the names of one or more AAA server group objects (up to four), or click **Select** to display an Object Selectors, page F-593. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. The device tries initially to perform accounting using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received. **Note** If you select None as a method, it must appear as the last method in the list.
Enable Broadcast to Multiple Servers	Applies only when Method List is selected as the EXEC method. When selected, enables the sending of accounting records to multiple AAA servers. Accounting records are sent simultaneously to the first server in each AAA server group defined in the method list. If the first server is unavailable, failover occurs using the backup servers defined within that group. When deselected, accounting records are sent only to the first server in the first AAA server group defined in the method list.

Table K-55 Console Page—Accounting Tab (Continued)

Connection Accounting settings	
Perform Connection Accounting Using	The accounting method to use for recording information about outbound connections made over the console line: • None—Accounting is not performed. This is the default. • AAA Policy Default List—Uses the default connection accounting method list that is defined in the device's AAA policy. See AAA Page—Accounting Tab, page K-93. • Custom Method List—Uses the accounting methods specified in the Connection Method List field. Connection accounting records details about outgoing connections over the line, such as Telnet and rlogin connections.
Generate Accounting Records for	Applies only when Custom Method List is selected as the connection method. Defines when the device sends an accounting notice to the accounting server: • Start and Stop—Generates accounting records at the beginning and the end of the user process. The user process begins regardless of whether the accounting server receives the "start" accounting record. This is the default. • Stop Only—Generates an accounting record at the end of the user process only. • None—No accounting records are generated.

Table K-55 Console Page—Accounting Tab (Continued)

Prioritized Method List	Applies only when Custom Method List is selected as the connection method. Defines a sequential list of methods to be queried when creating accounting methods for a user. Enter the names of one or more AAA server group objects (up to four), or click **Select** to display an Object Selectors, page F-593. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. The device tries initially to perform accounting using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received. **Note** If you select None as a method, it must appear as the last method in the list.
Enable Broadcast to Multiple Servers	Applies only when Custom Method List is selected as the connection method. When selected, enables the sending of accounting records to multiple AAA servers. Accounting records are sent simultaneously to the first server in each AAA server group defined in the method list. If the first server is unavailable, failover occurs using the backup servers defined within that group. When deselected, accounting records are sent only to the first server in the first AAA server group defined in the method list.
Command Accounting settings	
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
Privilege Level	The privilege level to which the command authorization definition applies.
Generate Accounting Records for	The points in the process where the device sends an accounting notice to the accounting server.
Enable Broadcast	Whether accounting records are broadcast to multiple servers simultaneously.
Prioritized Method List	The method list to use when authorizing users with this privilege level.
Add button	Opens the Command Accounting Dialog Box—Line Access, page K-145. From here you can configure a command accounting definition.

Table K-55 Console Page—Accounting Tab (Continued)

Edit button	Opens the Command Accounting Dialog Box—Line Access, page K-145. From here you can edit the command accounting definition.
Delete button	Deletes the selected command accounting definitions from the table.
Accounting tab button	
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.

VTY Policy Page

Use the VTY page to configure up to 16 VTY lines for remote access to the router. In addition to configuring individual lines, you can configure a group of lines that share the same definition.

For more information, see Line Access on Cisco IOS Routers, page 15-87.

Navigation Path

- (Device view) Select **Platform > Device Admin > Device Access > Line Access > VTY** from the Policy selector.
- (Policy view) Select **Router Platform > Device Admin > Device Access > Line Access > VTY** from the Policy Type selector. Right-click **VTY** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- Console Policy Page, page K-117
- Chapter K, "Router Platform User Interface Reference"

Field Reference

Table K-56 VTY Lines Page

Element	Description
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.

Table K-56 VTY Lines Page (Continued)

Line	The relative line number of the VTY line. This field may also contain multiple VTY lines configured as a contiguous group.
Line/Line Group Parameters	
Input Protocols	The protocols that you can use for incoming connections on the VTY line.
Output Protocols	The protocols that you can use for outgoing connections on the VTY line.
Privilege Level	The privilege level assigned to users.
Exec Timeout	The amount of time the EXEC command interpreter waits until user input is detected.
Inbound ACL	The ACL used to limit inbound traffic.
Outbound ACL	The ACL used to limit outbound traffic.
Authentication	The type of AAA authentication used.
Authorization	The types of AAA authorization used.
Accounting	The types of AAA accounting used.
VTY Line Page Buttons	
Add button	Opens the VTY Line Dialog Box, page K-131. From here you can define a VTY line or line group.
Edit button	Opens the VTY Line Dialog Box, page K-131. From here you can edit the VTY line or line group.
Delete button	Deletes the selected VTY lines from the table. If you delete a VTY line from an IOS device, any subsequent lines are also deleted. For example, if the device contains lines 0-9 and you delete line 5, lines 6-9 are deleted as well. **Note** If you delete any of the default VTY lines (0-4) on the device, the input protocol settings are retained and the other default settings are restored. This helps prevent you from cutting off remote access to the device.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** icon on the toolbar.

Tip To choose which columns to display in the table, right-click a column header, then select **Show Columns**. For more information about table display options, see Table Columns and Column Heading Features, page 3-26.

VTY Line Dialog Box

Use the VTY Line dialog box to configure one or more VTY lines (up to 16) that enable remote users to access the router. When you configure a VTY line, you can define the type of authentication and authorization to perform on users who access the lines.

Navigation Path

Go to the VTY Policy Page, page K-129, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Line Access on Cisco IOS Routers, page 15-87
- Console Policy Page, page K-117

Field Reference

Table K-57 VTY Line Dialog Box

Element	Description
Setup tab	Defines the basic configuration of the VTY line or line group. See VTY Line Dialog Box—Setup Tab, page K-132.
Authentication tab	Defines the type of AAA authentication to perform on users who access the VTY line. See VTY Line Dialog Box—Authentication Tab, page K-136.
Authorization tab	Defines the types of AAA authorization to perform on users who access the VTY line. See VTY Line Dialog Box—Authorization Tab, page K-137.
Accounting tab	Defines the types of AAA accounting to perform on users who access the VTY line. See VTY Line Dialog Box—Accounting Tab, page K-139.

Table K-57 VTY Line Dialog Box (Continued)

OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

VTY Line Dialog Box—Setup Tab

Use the Setup tab of the VTY Line dialog box to define the basic parameters of the VTY line. This includes the password for accessing the line, the privilege level assigned to users, the protocols that are permitted on the line, and the ACLs that limit access.

Navigation Path

Go to the VTY Line Dialog Box, page K-131, then click the **Setup** tab.

Related Topics

- Defining VTY Line Setup Parameters, page 15-92
- VTY Line Dialog Box—Authentication Tab, page K-136
- VTY Line Dialog Box—Authorization Tab, page K-137
- VTY Line Dialog Box—Accounting Tab, page K-139
- Console Page—Setup Tab, page K-118

Field Reference

Table K-58 VTY Line Dialog Box—Setup Tab

Element	Description
Starting VTY Line Number	The relative line number of the VTY line. If you are configuring a group of VTY lines, enter the number of the first line in the group. Valid values range from 0 to 15. **Note** Although different routers support a different number of VTY lines (from four to several thousand), Security Manager supports a maximum of 16 lines per device. You cannot configure the same line number more than once.

Table K-58 VTY Line Dialog Box—Setup Tab (Continued)

Ending VTY Line Number	Applies only when configuring a group of lines. The relative line number of the last VTY line in the group. **Note** When you configure a group of lines, all the lines in the group must fall within one of two ranges, 0-4 or 6-15.
Password	The password for accessing this VTY line. The password is case sensitive and can contain up to 80 alphanumeric characters. The first character cannot be a number. Spaces are not allowed. Enter the password again in the Confirm field.
Privilege Level	The privilege level assigned to users on this VTY line. Valid values range from 0 to 15: • 0—Grants access to these commands only: **disable**, **enable**, **exit**, **help**, and **logout**. • 1—Enables nonprivileged access to the router (normal EXEC-mode use privileges). • 15—Enables privileged access to the router (traditional enable privileges). **Note** Levels 2-14 are not normally used in a default configuration, but custom configurations can be created by moving commands that are normally at level 15 to a lower level and commands that are normally at level 1 to a higher level. You can configure the privilege levels of commands using the CLI or by defining a FlexConfig. **Note** If you do not define a value, level 1 is assigned by default. This value does not appear in the device configuration.
Disable all the EXEC sessions to the router via this line	When selected, EXEC sessions are disabled over this line. Select this option when you want to allow only an outgoing connection on this line. This option is useful for keeping a particular line free from unsolicited incoming data that can tie up the line. When deselected, EXEC sessions are enabled over this line. This is the default.

Table K-58 VTY Line Dialog Box—Setup Tab (Continued)

Exec Timeout	The amount of time (in seconds) that the EXEC command interpreter waits to detect user input on the line. If no input is detected, the line is disconnected. Valid values range from 0 to 2147483. The default is 600 (10 minutes). Setting the value to 0 disables the timeout. **Note** Although the timeout is defined in seconds, it appears in the CLI in the format [mm ss].
Input Protocols	The protocols that you can use for incoming connections on this line: • All—All supported protocols are permitted. Supported protocols include LAT, MOP, NASI, PAD, rlogin, SSH, Telnet, and V.120. • None—No protocols are permitted. This makes the port unusable by incoming SSH, Telnet, and rlogin connections. **Note** Setting the input protocols setting to None might prevent Security Manager from connecting to the device after deployment. The device can still be managed using SSL, if SSL is enabled in the HTTP policy. See HTTP Page—Setup Tab, page K-111. • Protocol—Enables one or more of the following protocols: – SSH—Secure Shell protocol. – Telnet—Standard TCP/IP terminal emulation protocol. – rlogin—UNIX rlogin protocol. **Note** SSH and rlogin require that you configure AAA authentication. See VTY Line Dialog Box—Authentication Tab, page K-136. **Note** Not all IOS Software Versions support rlogin as an input protocol.

Table K-58 VTY Line Dialog Box—Setup Tab (Continued)

Output Protocols	The protocols that you can use for outgoing connections on this line: • All—All supported protocols are permitted. Supported protocols include LAT, MOP, NASI, PAD, rlogin, SSH, Telnet, and V.120. • None—No protocols are permitted. This makes the port unusable by outgoing connections. • Protocol—Enables one or more of the following protocols: – SSH—Secure Shell protocol. – Telnet—Standard TCP/IP terminal emulation protocol. – rlogin—UNIX rlogin protocol. **Note** SSH and rlogin require that you configure AAA authentication. See VTY Line Dialog Box—Authentication Tab, page K-136. **Note** Not all IOS Software Versions support rlogin as an output protocol.
Inbound Access List	The ACL that restricts incoming connections on this line. Enter the name of an ACL object, or click **Select** to display an Object Selectors, page F-593. If the extended ACL you want is not listed, click the **Create** button in the selector to display the Add and Edit Extended Access List Pages, page F-34. From here you can create an extended ACL object.
Permit VRF Interface Connections	Applies only when an inbound ACL is defined on this line. When selected, accepts incoming connections from interfaces that belong to a VRF. When deselected, rejects incoming connections from interfaces that belong to a VRF.
Outbound Access List	The ACL that restricts outgoing connections on this line. Enter the name of an ACL object, or click **Select** to display an Object Selectors, page F-593. If the extended ACL you want is not listed, click the **Create** button in the selector to display the Add and Edit Extended Access List Pages, page F-34. From here you can create an extended ACL object.

VTY Line Dialog Box—Authentication Tab

Use the Authentication tab of the VTY Line dialog box to define the authentication methods to perform on users who attempt to access the selected VTY line or group of lines.

Navigation Path

Go to the VTY Line Dialog Box, page K-131, then click the **Authentication** tab.

Related Topics

- Defining VTY Line AAA Settings, page 15-96
- VTY Line Dialog Box—Setup Tab, page K-132
- VTY Line Dialog Box—Authorization Tab, page K-137
- VTY Line Dialog Box—Accounting Tab, page K-139
- Console Page—Authentication Tab, page K-121

Field Reference

Table K-59 VTY Line Dialog Box—Authentication Tab

Element	Description
Authenticate Using	Authentication settings for the VTY line: • None—Authentication is not performed. This is the default. • Local Database—Uses the local username database for authentication. • AAA Policy Default List—Uses the default authentication method list that is defined in the device's AAA policy. See AAA Page—Authentication Tab, page K-88. • Custom Method List—Uses the authentication methods specified in the Prioritized Method List field. **Note** If you select local authentication, preview the full configuration before deployment to make sure that the **aaa new-model** command is not configured by another policy (for example, by configuring a method list in the AAA policy) or is already configured on the device itself.

Table K-59 VTY Line Dialog Box—Authentication Tab (Continued)

Prioritized Method List	Applies only when Custom Method List is selected as the authentication method. Defines a sequential list of methods to be queried when authenticating a user. Enter the names of one or more AAA server group objects (up to four), or click **Select** to display an Object Selectors, page F-593. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. The device tries initially to authenticate users using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received. If the AAA server group you want is not listed, click the **Create** button in the selector to display the AAA Server Group Dialog Box, page F-12. From here you can define a AAA server group object. **Note** If you select None as a method, it must appear as the last method in the list.

VTY Line Dialog Box—Authorization Tab

Use the Authorization tab of the VTY Line dialog box to define the EXEC and command authorization methods to perform on users who access the selected VTY line or group of lines.

Note You must enable AAA services on the router to use this feature; otherwise, deployment will fail. See Defining AAA Services, page 15-70.

Navigation Path

Go to the VTY Line Dialog Box, page K-131, then click the **Authorization** tab.

Related Topics

- Defining VTY Line AAA Settings, page 15-96
- VTY Line Dialog Box—Setup Tab, page K-132
- VTY Line Dialog Box—Authentication Tab, page K-136
- VTY Line Dialog Box—Accounting Tab, page K-139

- Console Page—Authentication Tab, page K-121

Field Reference

Table K-60 VTY Line Dialog Box—Authorization Tab

Element	Description
EXEC Authorization settings	
Authorize EXEC Operations Using	The authorization method that determines whether a user is allowed to run an EXEC session: • None—Authorization is not performed. This is the default. • AAA Policy Default List—Uses the default authorization method list that is defined in the device's AAA policy. See AAA Page—Authorization Tab, page K-90. • Custom Method List—Uses the authorization methods specified in the Prioritized Method List field.
Prioritized Method List	Applies only when Custom Method List is selected as the EXEC method. Defines a sequential list of methods to be queried when authorizing a user. Enter the names of one or more AAA server group objects (up to four), or click **Select** to display an Object Selectors, page F-593. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. The device tries initially to authorize users using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received. If the AAA server group you want is not listed, click the **Create** button in the selector to display the AAA Server Group Dialog Box, page F-12. From here you can define a AAA server group object. **Note** If you select None as a method, it must appear as the last method in the list. **Note** RADIUS uses the same server for authentication and authorization. Therefore, if you use define a RADIUS method list for authentication, you must define the same method list for authorization.

Table K-60 VTY Line Dialog Box—Authorization Tab (Continued)

Command Authorization settings	
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
Privilege Level	The privilege level to which the command authorization definition applies.
Prioritized Method List	The method list to use when authorizing users with this privilege level.
Add button	Opens the Command Authorization Dialog Box—Line Access, page K-143. From here you can configure a command authorization definition.
Edit button	Opens the Command Authorization Dialog Box—Line Access, page K-143. From here you can edit the command authorization definition.
Delete button	Deletes the selected command authorization definitions from the table.

VTY Line Dialog Box—Accounting Tab

Use the Accounting tab of the VTY Line dialog box to define the EXEC, connection, and command accounting methods to perform on users who access the selected VTY line or group of lines.

Note You must enable AAA services on the router to use this feature; otherwise, deployment will fail. See Defining AAA Services, page 15-70.

Navigation Path

Go to the VTY Line Dialog Box, page K-131, then click the **Accounting** tab.

Related Topics

- Defining VTY Line AAA Settings, page 15-96
- VTY Line Dialog Box—Setup Tab, page K-132
- VTY Line Dialog Box—Authentication Tab, page K-136
- Console Page—Accounting Tab, page K-125

Field Reference

Table K-61 VTY Line Dialog Box—Accounting Tab

Element	Description
EXEC Accounting settings	
Perform EXEC Accounting Using	The accounting method to use for recording basic information about user EXEC sessions: • None—Accounting is not performed. This is the default. • AAA Policy Default List—Uses the default EXEC accounting method list that is defined in the device's AAA policy. See AAA Page—Accounting Tab, page K-93. • Custom Method List—Uses the accounting methods specified in the Prioritized Method List field. EXEC accounting records basic details about EXEC sessions, such as the username, date, start and stop times, and the access server IP address.
Generate Accounting Records for	Applies only when Custom Method List is selected as the EXEC method. Defines when the device sends an accounting notice to the accounting server: • Start and Stop—Generates accounting records at the beginning and the end of the user process. The user process begins regardless of whether the accounting server receives the "start" accounting record. This is the default. • Stop Only—Generates an accounting record at the end of the user process only. • None—No accounting records are generated.

Table K-61 VTY Line Dialog Box—Accounting Tab (Continued)

Prioritized Method List	Applies only when Custom Method List is selected as the EXEC method. Defines a sequential list of methods to be queried when creating accounting methods for a user. Enter the names of one or more AAA server group objects (up to four), or click **Select** to display an Object Selectors, page F-593. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. The device tries initially to perform accounting using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received. **Note** If you select None as a method, it must appear as the last method in the list.
Enable Broadcast to Multiple Servers	Applies only when Method List is selected as the EXEC method. When selected, enables the sending of accounting records to multiple AAA servers. Accounting records are sent simultaneously to the first server in each AAA server group defined in the method list. If the first server is unavailable, failover occurs using the backup servers defined within that group. When deselected, accounting records are sent only to the first server in the first AAA server group defined in the method list.
Connection Accounting settings	
Perform Connection Accounting Using	The accounting method to use for recording information about outbound connections made over the VTY line: • None—Accounting is not performed. This is the default. • AAA Policy Default List—Uses the default connection accounting method list that is defined in the device's AAA policy. See AAA Page—Accounting Tab, page K-93. • Custom Method List—Uses the accounting methods specified in the Prioritized Method List field. Connection accounting records details about outgoing connections over the line, such as Telnet and rlogin connections.

Table K-61 VTY Line Dialog Box—Accounting Tab (Continued)

Generate Accounting Records for	Applies only when Custom Method List is selected as the connection method. Defines when the device sends an accounting notice to the accounting server: • Start and Stop—Generates accounting records at the beginning and the end of the user process. The user process begins regardless of whether the accounting server receives the "start" accounting record. This is the default. • Stop Only—Generates an accounting record at the end of the user process only. • None—No accounting records are generated.
Prioritized Method List	Applies only when Custom Method List is selected as the connection method. Defines a sequential list of methods to be queried when creating accounting methods for a user. Enter the names of one or more AAA server group objects (up to four), or click **Select** to display an Object Selectors, page F-593. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. The device tries initially to perform accounting using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received. **Note** If you select None as a method, it must appear as the last method in the list.
Enable Broadcast to Multiple Servers	Applies only when Custom Method List is selected as the connection method. When selected, enables the sending of accounting records to multiple AAA servers. Accounting records are sent simultaneously to the first server in each AAA server group defined in the method list. If the first server is unavailable, failover occurs using the backup servers defined within that group. When deselected, accounting records are sent only to the first server in the first AAA server group defined in the method list.

Table K-61 VTY Line Dialog Box—Accounting Tab (Continued)

Command Accounting settings	
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
Privilege Level	The privilege level to which the command authorization definition applies.
Generate Accounting Records for	The points in the process where the device sends an accounting notice to the accounting server.
Enable Broadcast	Whether accounting records are broadcast to multiple servers simultaneously.
Prioritized Method List	The method list to use when authorizing users with this privilege level.
Add button	Opens the Command Accounting Dialog Box—Line Access, page K-145. From here you can configure a command accounting definition.
Edit button	Opens the Command Accounting Dialog Box—Line Access, page K-145. From here you can edit the command accounting definition.
Delete button	Deletes the selected command accounting definitions from the table.

Command Authorization Dialog Box—Line Access

Use the Command Authorization dialog box to define which methods to use when authorizing the EXEC commands that are associated with a given privilege. This enables you to authorize all commands associated with a specific privilege level, from 0 to 15.

Navigation Path

From the Console Page—Authorization Tab, page K-123 or the VTY Line Dialog Box—Authorization Tab, page K-137, click the **Add** button beneath the Command Authorization table.

Related Topics

- Console Policy Page, page K-117
- VTY Policy Page, page K-129

Field Reference

Table K-62 Command Authorization Dialog Box—Line Access

Element	Description
Privilege Level	The privilege level for which you want to define a command authorization list. Valid values range from 0 to 15. **Note** If you do not define a value, level 1 is assigned by default. This value does not appear in the device configuration.
AAA Policy Default List	Select this option to apply the default authorization list defined in the device's AAA policy to the EXEC commands associated with this privilege level. See Command Accounting Dialog Box, page K-96.
Custom Method List	Select this option to define an authorization method list for this privilege level.
Prioritized Method List	Applies only when the Custom Method List option is selected. Defines a sequential list of methods to be queried when authorizing a user. Enter the names of one or more AAA server group objects (up to four), or click **Select** to display an Object Selectors, page F-593. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. The device tries initially to authorize users using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received. If the AAA server group you want is not listed, click the **Create** button in the selector to display the AAA Server Group Dialog Box, page F-12. From here you can define a AAA server group object. **Note** If you select None as a method, it must appear as the last method in the list.
OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

Command Accounting Dialog Box—Line Access

Use the Command Accounting dialog box to define which methods to use when recording information about the EXEC commands that are executed for a given privilege. Each accounting record includes a list of the commands executed for that privilege level, as well as the date and time each command was executed, and the name of the user who executed it.

Navigation Path

From the Console Page—Accounting Tab, page K-125 or the VTY Line Dialog Box—Accounting Tab, page K-139, click the **Add** button beneath the Command Accounting table.

Related Topics

- Console Policy Page, page K-117
- VTY Policy Page, page K-129

Field Reference

Table K-63 Command Accounting Dialog Box—Line Access

Element	Description
Privilege Level	The privilege level for which you want to define a command accounting list. Valid values range from 0 to 15. **Note** If you do not define a value, level 1 is assigned by default. This value does not appear in the device configuration.
AAA Policy Default List	Select this option to apply the default accounting list defined in the device's AAA policy to the EXEC commands executed for this privilege level.
Custom Method List	Select this option to define an accounting method list for this privilege level.

Table K-63 Command Accounting Dialog Box—Line Access (Continued)

Generate Accounting Records for	Applies only when Custom Method List is selected. Defines when the device sends an accounting notice to the accounting server: • Start and Stop—Generates accounting records at the beginning and the end of the user process. The user process begins regardless of whether the accounting server receives the "start" accounting record. This is the default. • Stop Only—Generates an accounting record at the end of the user process only. • None—No accounting records are generated.
Prioritized Method List	Applies only when the Custom Method List option is selected. Defines a sequential list of accounting methods to be used when creating accounting records for a user. Enter the names of one or more AAA server group objects (up to four), or click **Select** to display an Object Selectors, page F-593. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. The device tries initially to perform accounting using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received. If the AAA server group you want is not listed, click the **Create** button in the selector to display the AAA Server Group Dialog Box, page F-12. From here you can define a AAA server group object. **Note** If you select None as a method, it must appear as the last method in the list.
Enable Broadcast to Multiple Servers	Applies only when Custom Method List is selected. When selected, enables the sending of accounting records to multiple AAA servers. Accounting records are sent simultaneously to the first server in each AAA server group defined in the method list. If the first server is unavailable, failover occurs using the backup servers defined within that group. When deselected, accounting records are sent only to the first server in the first AAA server group defined in the method list.

Table K-63 Command Accounting Dialog Box—Line Access (Continued)

OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

Secure Shell Policy Page

Use the Secure Shell page to change the default SSH settings on the router and to define additional optional settings, if required.

For more information, see Optional SSH Settings on Cisco IOS Routers, page 15-98.

Note You must configure SSH on the device using CLI commands before adding the device to Security Manager. This is because Security Manager uses SSH (as well as SSL) to communicate with Cisco IOS routers. For more information, see Setting Up SSH, page 5-9.

Navigation Path

- (Device view) Select **Platform > Device Admin > Device Access > Secure Shell** from the Policy selector.
- (Policy view) Select **Router Platform > Device Admin > Device Access > Secure Shell** from the Policy Type selector. Right-click **Secure Shell** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- Chapter 5, “Preparing Devices for Management”
- VTY Policy Page, page K-129
- Console Policy Page, page K-117
- Chapter K, “Router Platform User Interface Reference”

Field Reference

Table K-64 Secure Shell Page

Element	Description
SSH Version	The version of SSH to use when connecting to the router: • 1 and 2—SSH version 1 and SSH version 2. This is the default. • 1—SSH version 1 only. • 2—SSH version 2 only.
Timeout	The amount of time the router should wait for the SSH client to respond during the negotiation phase before disconnecting. The default value (and the maximum) is 120 seconds. **Note** After negotiation finishes and the EXEC session begins, the timeout configured for the VTY line applies. See VTY Line Dialog Box—Setup Tab, page K-132.
Authentication Retries	The number of times the router attempts to authenticate SSH clients. Valid values range from 0 to 5. The default is 3.
Source Interface	The source address for all SSH packets sent to the SSH client. If you do not define a value in this field, the address of the closest interface to the destination (that is, the output interface through which SSH packets are sent) is used. Enter the name of an interface or interface role, or click **Select** to display an Object Selectors, page F-593. If the interface role you want is not listed, click the **Create** button in the selector to display the Interface Role Dialog Box, page F-464. From here you can define an interface role object.
RSA Key Pair	The name of the RSA key pair to use for SSH connections. If you do not enter a value, the router uses the RSA key pair generated from its hostname and domain name. This is the default. **Tip** Use the CLI command **show crypto key mypubkey rsa** to display the names and values of each key pair configured on the device. These are the valid names that can be entered in this field.

Table K-64 Secure Shell Page (Continued)

Regenerate Key During Deployment	When selected, regenerates the RSA key pair on the router during the next deployment. This option is useful if you are concerned that the secrecy of the keys might be compromised. When deselected, a new key pair is not generated. **Note** This check box is *not* deselected automatically after deployment. If you do not return to this policy to deselect the check box, the key is regenerated each time you deploy. **Note** This option requires interaction with the device during deployment. Therefore, you should use it only when deploying to live devices, not when deploying to a file. **Note** A key pair must already exist on the device *before* you select this option; otherwise, deployment will fail. (This will typically be the case, since IOS routers must have SSH enabled in order to be added to Security Manager.)
Modulus Size	Applies only when the Regenerate Key check box is selected. The size of the modulus used to generate a new key pair. A larger modulus is more secure but takes longer to generate. Valid values range from 360 to 2048 bits. The default is 1024 bits.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.

SNMP Policy Page

Use the SNMP page to configure the parameters necessary to send traps from the router to a designated SNMP host. These traps are unsolicited messages that notify the SNMP host of important events occurring on the router.

For more information, see Defining SNMP Agent Properties, page 15-102.

Navigation Path

- (Device view) Select **Platform > Device Admin > Device Access > SNMP** from the Policy selector.

- (Policy view) Select **Router Platform > Device Admin > Device Access > SNMP** from the Policy Type selector. Right-click **SNMP** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- SNMP on Cisco IOS Routers, page 15-101
- Chapter K, "Router Platform User Interface Reference"

Field Reference

Table K-65 SNMP Page

Element	Description
Permissions table	
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
Community String	The community string used for accessing the router's MIB.
Type	The community string type—read-only or read-write.
ACL	The standard ACL that defines the IP addresses permitted to access the router's MIB.
Add button	Opens the Permission Dialog Box, page K-151. From here you can enter the community string and type required to generate traps.
Edit button	Opens the Permission Dialog Box, page K-151. From here you can edit the selected permissions profile.
Delete button	Deletes the selected permissions profiles from the table.
Trap Receiver table	
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
Host IP Address	The IP address of the SNMP host receiving the traps generated by the router.
SNMP Version	The SNMP version being used by the router.
UDP Port	The UDP port that is being used by the SNMP host.
Add button	Opens the Trap Receiver Dialog Box, page K-153. From here you can define the SNMP host that receives the traps generated by the router.

Table K-65 SNMP Page (Continued)

Edit button	Open the Trap Receiver Dialog Box, page K-153. From here you can edit the selected SNMP host.
Delete button	Deletes the selected SNMP hosts from the table.
Additional fields and buttons	
SNMP Server Properties	The name and contact information of the system administrator responsible for the SNMP server/agent (that is, the router). The person managing the SNMP host can use this information when tracking down the source of unusual events. The maximum length of each of these properties is 255 characters, including spaces. **Note** The values entered in these fields are text-only and do not affect the operation of the router.
Configure Traps button	Opens a dialog box for selecting which SNMP traps the router should generate. See SNMP Traps Dialog Box, page K-155.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.

Tip To choose which columns to display in the table, right-click a column header, then select **Show Columns**. For more information about table display options, see Table Columns and Column Heading Features, page 3-26.

Permission Dialog Box

Use the Permission dialog box to define the community string and string type required by the SNMP policy. The community string is an embedded password for accessing the Management Information Base (MIB) that stores operational data about the router.

Navigation Path

Go to SNMP Policy Page, page K-149, then click the **Add** or **Edit** button beneath the Permissions table.

Related Topics

- SNMP Policy Page, page K-149
- Trap Receiver Dialog Box, page K-153
- SNMP Traps Dialog Box, page K-155
- Defining SNMP Agent Properties, page 15-102
- SNMP on Cisco IOS Routers, page 15-101

Field Reference

Table K-66 Permission Dialog Box

Element	Description
Community String	The community string for accessing the router's MIB. String length ranges from 1 to 128 characters.
Access Control Lists	Applies only to routers running Cisco IOS Software Release 12.3(2)T and up (T-train) or any 12.4 version. The standard ACL containing the IP addresses that can access the router's MIB. Defining an ACL provides an additional layer of security by limiting the source addresses that can make use of the community string. Enter the name of an ACL object, or click **Select** to display an Object Selectors, page F-593. If the standard ACL you want is not listed, click the **Create** button in the selector to display the Standard Tab, page F-41. From here you can create an ACL object.
Read-Write	This community string type provides read-write access to all objects in the MIB (except community strings).
Read-Only	This community string type provides read-only access to all objects in the MIB (except community strings). This is the default.
OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

Trap Receiver Dialog Box

Use the Trap Receiver dialog box to define the SNMP hosts that receive traps generated by the router. This includes defining the version of SNMP to use.

Navigation Path

Go to the SNMP Policy Page, page K-149, then click the **Add** or **Edit** button beneath the Trap Receiver table.

Related Topics

- SNMP Policy Page, page K-149
- Permission Dialog Box, page K-151
- SNMP Traps Dialog Box, page K-155
- Defining SNMP Agent Properties, page 15-102
- SNMP on Cisco IOS Routers, page 15-101

Field Reference

Table K-67 Trap Receiver Dialog Box

Element	Description
Host IP Address	The IP address of the SNMP host receiving the traps generated by the router. Enter an IP address or the name of a network/host object, or click **Select** to display an Object Selectors, page F-593. If the network you want is not listed, click the **Create** button in the selector to display the Network/Host Dialog Box, page F-477. From here you can define a network/host object.
SNMP Version	The version of SNMP to use—version 1, version 2c, or version 3.

Table K-67 Trap Receiver Dialog Box (Continued)

Community String	Applies only when version 1 or version 2c is selected. The password required to access the SNMP host. Enter the string again in the Confirm field. **Note** We recommend that you use one of the strings defined in the Permissions table as the password to the SNMP host. You may, however, enter a different password. String length ranges from 1 to 128 characters. Your entry does not appear in the Permissions table and is read-only.
User Name	Applies only when version 3 is selected. The password required to access the SNMP host. Enter the string again in the Confirm field. **Note** We recommend that you use one of the strings defined in the Permissions table as the password to the SNMP host. You may, however, enter a different password. String length ranges from 1 to 128 characters. Your entry does not appear in the Permissions table and is read-only.
SNMPv3 Security	Applies only when version 3 is selected. The level of security to apply to SNMP traffic: • No MD5, No DES—No packet authentication. • MD5 (auth)—MD5 authentication, but no encryption. • DES (priv)—MD5 authentication and DES encryption.
UDP Port	The port number for the SNMP host. The default is 162. Valid values range from 0 to 65535.
OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

SNMP Traps Dialog Box

Use the SNMP Traps dialog box to select the events in the router that should generate SNMP traps.

Tip You can configure SNMP traps not included in this dialog box by defining FlexConfigs. For more information, see Understanding FlexConfig Objects, page 9-52.

Note To lessen possible degradation of system performance, select only those traps that are needed for network monitoring purposes.

Navigation Path

Go to the SNMP Policy Page, page K-149, then click **Configure Traps**.

Related Topics

- SNMP Policy Page, page K-149
- Permission Dialog Box, page K-151
- Trap Receiver Dialog Box, page K-153
- Enabling SNMP Traps, page 15-104
- SNMP on Cisco IOS Routers, page 15-101

Field Reference

Table K-68 SNMP Traps Dialog Box

Element	Description
Standard SNMP Traps	Enables or disables standard SNMP traps. Options are: • Cold start—Sends a trap when the router reinitializes in a way that could change the configuration of the SNMP agent (or any other trap-receiving entity). • Warm start—Sends a trap when the router reinitializes in a way that does not change the configuration of the SNMP agent (or any other trap-receiving entity). • Authentication—Sends a trap if an SNMP request from the SNMP host fails because of an invalid community string.
IPsec Traps	Enables or disables individual IPsec-related traps. Options are: • Cryptomap—Sends a trap when a crypto map entry is added to, or removed from, the device's crypto map set. Additionally, this option sends a trap when a crypto map set is attached to, or detached from, an active interface. • Too Many SAs—Sends a trap if an attempt is made to create a security association (SA) when there is insufficient memory on the device. • Tunnel—Sends a trap when an IPsec Phase 2 tunnel becomes active or inactive. For more information, see Understanding IPsec Tunnel Policies, page 10-72.
ISAKMP Traps	Enables or disables individual Internet Security Association and Key Exchange Protocol (ISAKMP) traps. Options are: • Policy—Sends a trap when an ISAKMP policy is created or deleted. • Tunnel—Sends a trap when a Phase 1 IKE tunnel becomes active or inactive. For more information, see Understanding IKE, page 10-67.

Table K-68 SNMP Traps Dialog Box (Continued)

Other Traps	Enables or disables additional SNMP traps. Options are: • Syslog—Sends syslog messages to the SNMP host. • TTY—Sends Cisco-specific notifications when a Transmission Control Protocol (TCP) connection closes. • BGP—Sends notifications when Border Gateway Protocol (BGP) state changes occur. See BGP Routing on Cisco IOS Routers, page 15-179. • IP Multicast—(Applicable to multicast routers only) Sends a trap if the router fails to receive a defined number of heartbeat packets from heartbeat sources within a defined time interval. • CPU—Sends a trap when CPU usage rises and remains above an upper threshold or falls and remains below a lower threshold. **Note** To implement the IP multicast and CPU traps, you must define additional command-line interface (CLI) commands (ip multicast heartbeat and cpu threshold, respectively) using FlexConfigs or the CLI. For more information about the ip multicast heartbeat command, see *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*. For more information about the cpu threshold command, see *CPU Thresholding Notification*. Both of these documents are available on Cisco.com. • HSRP—Sends Hot Standby Routing Protocol (HSRP) notifications. **Note** Most Cisco 800 Series routers do not support the HSRP trap.
Select All button	Enables all the SNMP traps displayed in the dialog box.
Deselect All button	Disables all the SNMP traps displayed in the dialog box.
OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

DNS Policy Page

Use the DNS policy page to define the local IP host table and the Domain Name System (DNS) servers that the router should use for translating hostnames to IP addresses. You can also prevent the router from performing DNS lookups by disabling the DNS feature.

Navigation Path

- (Device view) Select **Platform > Device Admin > DNS** from the Policy selector.
- (Policy view) Select **Router Platform > Device Admin > DNS** from the Policy Type selector. Right-click **DNS** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- DNS on Cisco IOS Routers, page 15-105
- Chapter K, "Router Platform User Interface Reference"

Field Reference

Table K-69 DNS Page

Element	Description
Servers	The DNS servers used by the router to perform DNS lookups. Enter one or more addresses or network/host objects, or click **Select** to display an Object Selectors, page F-593. You can define a maximum of six DNS servers. If the address you want is not listed, click the **Create** button in the selector to display the Network/Host Dialog Box, page F-477. From here, you can define a network/host object.
Hosts	The local host table configured on the router. When a user types in a hostname, the router checks this table first before querying the DNS servers defined in the Servers field. Click **Add** to display the IP Host Dialog Box, page K-159. From here you can define a hostname and the IP addresses to associate with that hostname. **Note** To edit an entry in the host table, select it, then click **Edit**. To remove an entry, select it, then click **Delete**.

Table K-69 DNS Page (Continued)

Domain Lookup	When selected, the router performs lookups on the defined DNS servers. This is the default. When deselected, lookups on remote DNS servers are disabled.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** icon on the toolbar.

IP Host Dialog Box

Use the IP Host dialog box to configure the host table on the router. This is the table of static, local mappings that the router uses to translate hostnames to IP addresses. If the router does not find the required entry in the host table, it queries the DNS servers that are defined on the DNS page.

Navigation Path

Go to the DNS Policy Page, page K-158, then click **Add** under Hosts.

Related Topics

- DNS on Cisco IOS Routers, page 15-105

Field Reference

Table K-70 IP Host Dialog Box

Element	Description
Host Name	The hostname to include in the router's local host table.
Addresses	The addresses to associate with the hostname. Enter one or more addresses or network/host objects, or click **Select** to display an Object Selectors, page F-593. You can define a maximum of three addresses per hostname. If the address you want is not listed, click the **Create** button in the selector to display the Network/Host Dialog Box, page F-477. From here, you can define a network/host object.

Table K-70 IP Host Dialog Box (Continued)

OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

Hostname Policy Page

Use the Hostname page to define the hostname and domain name assigned to the router. For more information, see Defining Hostname Policies, page 15-107.

Navigation Path

- (Device view) Select **Platform > Device Admin > Hostname** from the Policy selector.
- (Policy view) Select **Router Platform > Device Admin > Hostname** from the Policy Type selector. Right-click **Hostname** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- Hostnames and Domain Names on Cisco IOS Routers, page 15-107
- Chapter K, "Router Platform User Interface Reference"

Field Reference

Table K-71 Hostname Page

Element	Description
Host Name	The hostname of the router. Names must start with a letter, end with a letter or digit, and include only letters, digits, and hyphens. The maximum length is 63 characters.
Domain Name	The default domain name of the router. The maximum length is 63 characters. The router uses this domain name for RSA key generation and in policies when you do not enter the fully-qualified domain name (FQDN).

Table K-71 Hostname Page (Continued)

Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** icon on the toolbar.

Memory Policy Page

Use the Memory page to define settings related to router memory, including:

- The amount of time to retain the memory log.
- The thresholds for available processor and I/O memory.
- The amount of memory reserved for critical log messages.
- Whether to perform sanity checks on buffers and queues.
- Whether to enable the "memory-allocation lite" feature.

For more information, see Defining Router Memory Settings, page 15-109.

Navigation Path

- (Device view) Select **Platform > Device Admin > Memory** from the Policy selector.
- (Policy view) Select **Router Platform > Device Admin > Memory** from the Policy Type selector. Right-click **Memory** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- Memory Settings on Cisco IOS Routers, page 15-108
- CPU Policy Page, page K-107
- Logging Setup Policy Page, page K-192
- Syslog Servers Policy Page, page K-197
- Chapter K, "Router Platform User Interface Reference"

Field Reference

Table K-72 Memory Page

Element	Description
Maintain Memory Log	The number of hours that the router should maintain the log containing the history of memory consumption on the device. Valid values range from 12 to 72 hours. The default is 24 (1 day). **Note** The memory log is enabled by default and cannot be disabled.
Processor Threshold	The processor memory threshold in kilobytes. When available processor memory falls below this threshold, a notification message is triggered. Valid values range from 1 to 4294967295 kilobytes (4096 gigabytes). **Note** Another notification message is generated when available free memory rises to 5% above the threshold.
I/O Threshold	The I/O memory threshold in kilobytes. When available processor memory falls below this threshold, a notification message is triggered. Valid values range from 1 to 4294967295 kilobytes (4096 gigabytes). **Note** Another notification message is generated when available free memory rises to 5% above the threshold.
Memory Allocation Lite	When selected, the “memory-allocation lite” (malloc_lite) feature on the router is enabled. This feature avoids excessive memory allocation overhead for situations where less than 128 bytes are required. This is the default. When deselected, the “memory-allocation lite” feature is disabled. **Note** This feature is supported for processor memory pools only.
Memory Region For Critical Notifications	The amount of memory (in kilobytes) reserved for critical system log messages. Valid values range from 1 to 4294967295 kilobytes (4096 gigabytes), but the value you specify cannot exceed 25% of total memory. This option reserves a region of memory on the router so that the router can issue critical system log messages even when system resources are overloaded.

Table K-72 Memory Page (Continued)

Perform Sanity Checks	The types of sanity checks to perform: • Buffer—When selected, performs sanity checks on all buffers. Sanity checks are performed when a packet buffer is allocated and when the packet buffer is returned to the buffer pool. • Queue—When selected, performs sanity checks on all queues. • All—When selected, performs sanity checks on all buffers and queues. **Note** Enabling any of these options may result in a slight degradation of router performance.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.

Secure Device Provisioning Policy Page

Secure Device Provisioning (SDP) policies (formerly known as Easy Secure Device Deployment or EzSDD) enable you to configure a Cisco IOS router as a *registrar*. This is the SDP component that retrieves bootstrap configurations for *petitioners*, which are remote-site devices that are enrolling in the network security infrastructure. These devices uses the bootstrap configuration for first-time configuration purposes. The registrar also verifies the identity of the *introducer*, which is the user who introduces the petitioner to the registrar.

For more information, see Defining Secure Device Provisioning Policies, page 15-113.

Navigation Path

- (Device view) Select **Platform > Device Admin > Secure Device Provisioning** from the Policy selector.
- (Policy view) Select **Router Platform > Device Admin > Secure Device Provisioning** from the Policy Type selector. Right-click **Secure Device Provisioning** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- Secure Device Provisioning on Cisco IOS Routers, page 15-110

- Chapter K, "Router Platform User Interface Reference"
- Secure Device Provisioning Workflow, page 15-112
- Understanding AAA Server Group Objects, page 9-15
- Understanding PKI Enrollment Objects, page 9-154
- Understanding FlexConfig Objects, page 9-52

Field Reference

Table K-73 Secure Device Provisioning Page

Element	Description
Introducer Authentication (AAA)	The AAA server group that authenticates the username and password supplied by the introducer. Enter the name of a AAA server group object, or click **Select** to display an Object Selectors, page F-593. If the server you want is not listed, click the **Create** button in either selector to display the AAA Server Group Dialog Box, page F-12. From here you can define a AAA server group object. **Note** Each AAA server in the selected group must be configured to communicate with an interface that exists on the router; otherwise, validation fails. **Note** To configure a separate AAA server group for authenticating administrative introducers, see Configuring a AAA Server Group for Administrative Introducers, page 15-116.

Table K-73 Secure Device Provisioning Page (Continued)

Petitioner Authentication	The CA server that authenticates the identity of the petitioner: • Local CA Server—Select this option when the router itself is already configured to act as the CA server. Enter the name of the local CA in the field provided. **Note** If you have not configured the router as the CA server, enter the command **Crypto pki server [name]** using the CLI or FlexConfigs. This command is mandatory when you deploy an SDP policy configured with a local CA server. • Remote CA Server—Select this option when using an external CA server. Enter the name of a a PKI enrollment object, or click **Select** to display an Object Selectors, page F-593. If the server you want is not listed, click the **Create** button in either selector to display the PKI Enrollment Dialog Box, page F-481. From here you can define a PKI enrollment object.
Introduction Page	The source of the introduction page to display to the introducer after authorization is performed: • Use default introduction page—Uses a default page provided with Security Manager. • Specify introduction page URL—Uses the introduction page specified in the URL field. Supported protocols include: FTP, HTTP, HTTPS, null, NVRAM, RCP, SCP, system, TFTP, Webflash, and XMODEM.

Table K-73 Secure Device Provisioning Page (Continued)

Bootstrap Configuration	The source of the bootstrap configuration to provide to the petitioner for first-time configuration: • Non-Security Manager URL—Used when the bootstrap configuration is located externally to Security Manager. Enter its location in the URL field. If required, enter a username and password to access the server containing the bootstrap configuration. • Security Manager URL—Used when Security Manager is providing the bootstrap configuration. Enter information in the following fields: – FlexConfig—The FlexConfig that contains the basic CLI structure required to create the bootstrap configuration. Enter the name of a FlexConfig object, or click **Select** to display a selector. After selecting the FlexConfig, you must enter a username and password to access the Security Manager server that contains the FlexConfig. – Device name formula—The formula required by Security Manager to determine the device name of the petitioner from the username that the introducer supplied. Typically a fixed relationship exists between the username and the device name, which enables a formula like this to be established. The default formula is $n, which uses the introducer name to determine the device name. The device name is required to determine the configuration file that the petitioner should receive. If required, enter a username and password to access the server containing the bootstrap configuration. The password can contain alphanumeric characters, but cannot consist of a single digit.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.

DHCP Policy Page

Use the DHCP policy page to define a DHCP server policy on the selected router. This includes specifying the address pools used by the DHCP server when assigning addresses to requesting clients.

For more information, see Defining DHCP Policies, page 15-121.

Navigation Path

- (Device view) Select **Platform > Device Admin > Server Access > DHCP** from the Policy selector.
- (Policy view) Select **Router Platform > Device Admin > Server Access > DHCP** from the Policy Type selector. Right-click **DHCP** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- DHCP on Cisco IOS Routers, page 15-117
- Chapter K, "Router Platform User Interface Reference"

Field Reference

Table K-74 DHCP Policy Page

Element	Description
Databases Table	
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
Database URL	The URL of the external DHCP database agent.
Timeout	The amount of time to wait (in seconds) for a response from the external DHCP database agent before aborting a database transfer.
Write Delay	The interval (in seconds) between DHCP assignment updates sent to the external DHCP database agent.
Add button	Opens the DHCP Database Dialog Box, page K-170. From here you can define a DHCP database agent.
Edit button	Opens the DHCP Database Dialog Box, page K-170. From here you can edit the selected DHCP database agent.

Table K-74 DHCP Policy Page (Continued)

Delete button	Deletes the selected DHCP database agents.
Excluded IPs	
Excluded IPs or IP Ranges	The IP addresses and/or address ranges to exclude from DHCP. These addresses are not assigned by the DHCP server to DHCP clients requesting addresses. Enter one or more network addresses or network/host objects, or click **Select** to display an Object Selectors, page F-593. If the network you want is not listed, click the **Create** button in the selector to display the Network/Host Dialog Box, page F-477. From here, you can define a network/host object. For more information, see Specifying IP Addresses During Policy Definition, page 9-153 and Supported IP Address Formats, page 9-145.
IP Pools Table	
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
Name	The name of the IP pool.
Network	The IP address and subnet mask of the IP pool.
Default Router	The IP addresses of the default routers used by DHCP clients.
DNS Server	The IP addresses of the DNS servers used by DHCP clients.
NetBIOS (WINS) Server	The IP addresses of the Windows Internet Naming Service (WINS) servers used by Microsoft DHCP clients.
Domain Name	The domain name for DHCP clients.
Import All	Indicates whether the remote DHCP server imports certain DHCP options from a centralized DHCP server.
Secured ARP	Indicates whether secured ARP is enabled on this IP pool to help prevent IP spoofing by unauthorized users.
Lease	The duration of the lease for each IP address assigned by the DHCP server from this IP pool.
Option 150	The IP address of the TFTP server required by IP phones for configuration, as defined using DHCP option 150.

Table K-74 DHCP Policy Page (Continued)

Option 66	The IP address of the TFTP server required by IP phones for configuration, as defined using DHCP option 66.
Add button	Opens the IP Pool Dialog Box, page K-171. From here you can define a DHCP IP address pool.
Edit button	Opens the IP Pool Dialog Box, page K-171. From here you can edit the selected IP pool.
Delete button	Deletes the selected IP pools.
Relay parameters	
Policy	The policy that DHCP relay agents implement when they receive messages already containing relay information: • Drop—The relay agent discards messages with existing relay information if option-82 information is also present. • Keep—The relay agent retains existing relay information. • Replace—The relay agent overwrites existing information with its own relay information.
Option	When selected, enables DHCP Option 82 data insertion in message requests forwarded from the DHCP client to the server. DHCP Option 82 provides the DHCP server with both the switch and port ID of the requesting client. This option makes it possible to locate where a user is physically connected to the network and prevent spoofing. See Understanding DHCP Option 82, page 15-119. When deselected, DHCP Option 82 is disabled.
Check	When selected, DHCP Option 82 reply packets received from the DHCP server are validated. Invalid messages are dropped; valid messages are stripped of the option-82 field before being forwarded to the DHCP client. When deselected, the option-82 field is removed from the packet without being checked first for validity.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.

Tip To choose which columns to display in the table, right-click a column header, then select **Show Columns**. For more information about table display options, see Table Columns and Column Heading Features, page 3-26.

DHCP Database Dialog Box

Use the DHCP Database dialog box to define external DHCP database agents that contain the automatic bindings. Each database URL that you define must be unique.

For more information, see Understanding DHCP Database Agents, page 15-118.

Navigation Path

Go to the DHCP Policy Page, page K-167, then click the **Add** or **Edit** button beneath the Databases table.

Related Topics

- Defining DHCP Policies, page 15-121
- DHCP on Cisco IOS Routers, page 15-117
- IP Pool Dialog Box, page K-171

Field Reference

Table K-75 DHCP Database Dialog Box

Element	Description
Database URL	The URL of the external DHCP database agent containing the automatic bindings. The URL can be in HTTP, FTP, TFTP, or RCP format. **Note** If you define a URL, it is not necessary to define an IP address pool. However, you may do so.
Timeout	The amount of time (in seconds) the DHCP server should wait for a response from the external DHCP database agent before aborting a database transfer. The default is 300 seconds (5 minutes). **Note** A value of 0 disables the timeout.

Table K-75 DHCP Database Dialog Box (Continued)

Write Delay	The interval (in seconds) between updates sent from the DHCP server to the external DHCP database agent. The minimum delay is 60 seconds. The default is 300 seconds (5 minutes).
OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

IP Pool Dialog Box

Use the IP Pool dialog box to define one or more address pools, which the DHCP server uses to assign dynamic addresses to DHCP clients. You must define at least one address pool, unless you have defined an external DHCP database agent.

Navigation Path

Go to the DHCP Policy Page, page K-167, then click the **Add** or **Edit** button beneath the IP Pools table.

Related Topics

- Defining DHCP Address Pools, page 15-123
- Understanding DHCP Database Agents, page 15-118
- DHCP Database Dialog Box, page K-170
- DHCP on Cisco IOS Routers, page 15-117

Field Reference

Table K-76 IP Pool Dialog Box

Element	Description
Pool Name	The name of the IP pool.

Table K-76 IP Pool Dialog Box (Continued)

Network	The IP address and subnet mask of the IP pool. This subnet contains the range of available IP addresses that the DHCP server may assign to clients. Enter an address and mask or the name of a network/host object, or click **Select** to display an Object Selectors, page F-593. If the network you want is not listed, click the **Create** button in the selector to display the Network/Host Dialog Box, page F-477. From here you can define a network/host object. **Tip** You can exclude specific addresses within the range by defining them in the Excluded IPs field. See DHCP Policy Page, page K-167.
Default Router Addresses	The IP addresses of the default routers for DHCP clients using this IP pool. After a DHCP client is booted, it begins sending packets to this router, which should be located on the same subnet as the client. Enter up to eight (8) network addresses or network/host objects, or click **Select** to display an Object Selectors, page F-593. If the network you want is not listed, click the **Create** button in the selector to display the Network/Host Dialog Box, page F-477. From here, you can define a network/host object.
DNS Server Addresses	The IP addresses of the DNS servers that DHCP clients using this IP pool should query when they need to correlate hostnames to IP addresses. Enter up to eight (8) network addresses or network/host objects, or click **Select** to display an Object Selectors, page F-593. If the network you want is not listed, click the **Create** button in the selector to display the Network/Host Dialog Box, page F-477. From here, you can define a network/host object.
NetBIOS (WINS) Server Addresses	The IP addresses of the Windows Internet Naming Service (WINS) servers used by Microsoft DHCP clients to correlate hostnames to IP addresses within a general grouping of networks. Enter up to eight (8) network addresses or network/host objects, or click **Select** to display an Object Selectors, page F-593. If the network you want is not listed, click the **Create** button in the selector to display the Network/Host Dialog Box, page F-477. From here, you can define a network/host object.

Table K-76 IP Pool Dialog Box (Continued)

Domain Name	The domain name for DHCP clients using this IP pool. This name places these clients in the general grouping of networks that make up the domain.
Import All	When selected, enables remote DHCP servers to import specific DHCP options (such as the DNS server) from a centralized server. Use this option to enable configuration information to be updated automatically. When deselected, all DHCP options are local to this specific server.
Secured ARP	When selected, enables the DHCP Authorized ARP feature, which limits the leasing of IP addresses to authorized mobile users. This feature helps prevent IP spoofing by unauthorized users. See Understanding Secured ARP, page 15-120. When deselected, the DHCP Authorized ARP feature is disabled. **Note** This feature also disables dynamic ARP learning on an interface.
Lease Never Expires	When selected, the DHCP server permanently assigns IP addresses to its clients. When deselected, addresses are leased for a predefined amount of time, as defined in the Time Length field.
Time Length (DD:HH:MM)	Applies only when the Lease Never Expires check box is deselected. The duration of the lease provided to each IP address assigned from this IP pool (using the format DD:HH:MM). After the lease expires, the assigned IP address is no longer valid and is returned to the pool.
Option 66 (IP Addresses)	The IP address of the TFTP server used to provide configuration files to IP phones. These configuration files define parameters required by IP phones to connect to Cisco CallManager. Enter up to eight (8) network addresses or network/host objects, or click **Select** to display an Object Selectors, page F-593. If the network you want is not listed, click the **Create** button in the selector to display the Network/Host Dialog Box, page F-477. From here, you can define a network/host object. **Note** This option is functionally similar to option 150. Either or both options may be used.

Table K-76 IP Pool Dialog Box (Continued)

Option 150 (IP Addresses)	The IP address of the TFTP server used to provide configuration files to IP phones. These configuration files define parameters required by IP phones to connect to Cisco CallManager. Enter up to eight (8) network addresses or network/host objects, or click **Select** to display an Object Selectors, page F-593. If the network you want is not listed, click the **Create** button in the selector to display the Network/Host Dialog Box, page F-477. From here, you can define a network/host object. **Note** This option is functionally similar to option 66. Either or both options may be used.
OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

NTP Policy Page

Use the NTP page to define one or more NTP servers that the router can use for time synchronization. This includes enabling authentication, if required, and defining a global source interface for all traffic sent to these servers.

For more information, see Defining NTP Servers, page 15-125.

Navigation Path

- (Device view) Select **Platform > Device Admin > Server Access > NTP** from the Policy selector.
- (Policy view) Select **Router Platform > Device Admin > Server Access > NTP** from the Policy Type selector. Right-click **NTP** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- NTP on Cisco IOS Routers, page 15-124
- Chapter K, "Router Platform User Interface Reference"

- Understanding Interface Role Objects, page 9-132

Field Reference

Table K-77 NTP Page

Element	Description
Source Interface	The source address for all packets sent to an NTP server. This setting might be necessary when the NTP server cannot respond to the address from which the packet originated (for example, due to a firewall). The source interface must have an IP address. If you do not define a value in this field, the address of the outgoing interface is used. Enter the name of an interface or interface role, or click **Select** to display an Object Selectors, page F-593. If the interface role you want is not listed, click the **Create** button in the selector to display the Interface Role Dialog Box, page F-464. From here you can define an interface role object. **Note** The source interface defined in this field is a global setting that you can override for individual NTP servers. For more information, see NTP Server Dialog Box, page K-176.
Enable NTP Authentication	When selected, enables authentication using MD5 when connecting to an NTP server. When deselected, authentication is disabled.
Servers Table	
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
IP Address	The IP address of the NTP server.
Source Interface	The source address for all packets sent to this NTP server. This setting overrides the global setting defined at the top of the page.
Preferred	Indicates whether this NTP server is preferred over other NTP servers of similar accuracy. **Note** By default, preferred servers are listed first in the table.
Key Number	The ID number of the key used for authentication with this NTP server.

Table K-77 NTP Page (Continued)

Trusted	Indicates whether the authentication key defined for this NTP server is a trusted key.
Add button	Opens the NTP Server Dialog Box, page K-176. From here you can define an NTP server.
Edit button	Opens the NTP Server Dialog Box, page K-176. From here you can edit the selected NTP server.
Delete button	Deletes the selected NTP server from the table. **Note** If the key defined on the server you delete is not defined on a different NTP server, the key is also deleted.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** icon on the toolbar.

Tip To choose which columns to display in the table, right-click a column header, then select **Show Columns**. For more information about table display options, see Table Columns and Column Heading Features, page 3-26.

NTP Server Dialog Box

Use the NTP Server dialog box to define the address of an NTP server that the router can use to perform time synchronization. In addition, you can use this dialog box to define a default source interface for NTP packets sent to this server and authentication parameters.

Navigation Path

Go to the NTP Policy Page, page K-174, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Defining NTP Servers, page 15-125
- NTP on Cisco IOS Routers, page 15-124
- Understanding Interface Role Objects, page 9-132

Field Reference

Table K-78 NTP Server Dialog Box

Element	Description
IP Address	The IP address of the NTP server. Enter an address or the name of a network/host object, or click **Select** to display an Object Selectors, page F-593. If the network you want is not listed, click the **Create** button in the selector to display the Network/Host Dialog Box, page F-477. From here, you can define a network/host object.
Source Interface	The source address for all packets sent to this NTP server. This setting might be necessary when the NTP server cannot respond to the address from which the packet originated (for example, due to a firewall). The source interface must have an IP address. If you do not define a value in this field and there is no global setting, the address of the outgoing interface is used. **Note** This setting overrides the global setting you defined on the NTP Policy Page, page K-174. Enter the name of an interface or interface role, or click **Select** to display an Object Selectors, page F-593. If the interface role you want is not listed, click the **Create** button in the selector to display the Interface Role Dialog Box, page F-464. From here you can define an interface role object.

Table K-78 NTP Server Dialog Box (Continued)

Preferred	When selected, this NTP server is preferred over other NTP servers of similar accuracy. If this server is used for synchronization, the time offset used to correct the local clock is calculated from this server only. **Note** If a different NTP server is significantly more accurate than the preferred server (for example, stratum 2 versus stratum 3), the router synchronizes to the more accurate server. When deselected, this NTP server is not given preference over other NTP servers of similar accuracy. The time offset used to correct the local clock is calculated by taking the combined offset of all NTP servers. We recommend that you configure an NTP server as preferred only when multiple servers have the same stratum and you can rely on the accuracy of the preferred server.
Authentication Key	The MD5 key that is used to authenticate associations with the NTP server. • Key Number—The ID number of the authentication key. Enter the key number or select a previously defined number from the list. • Key Value—An arbitrary string of up to eight characters that defines the authentication key. Enter the string again in the Confirm field. • Trusted—When selected, this key authenticates the identity of systems attempting to synchronize with this server. When deselected, this key is not used for authentication. If you select a key number from the list and then change the key value, you are warned that saving this change affects any other NTP servers using the same authentication key. **Note** To use authentication, you must enable it from the NTP Policy Page, page K-174.
OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

802.1x Policy Page

Use the 802.1x policy page to create policies that limit VPN access to authorized users. Authenticated traffic is allowed to pass through a designated physical interface on the router. Unauthenticated traffic is allowed to pass through a virtual interface to the Internet but is not allowed to access the VPN.

For more information, see Defining 802.1x Policies, page 15-131.

Note 802.1x policies require DHCP address pools in order to assign IP addresses to clients. You define these pools by defining a DHCP policy on the same router. See DHCP Policy Page, page K-167.

Navigation Path

- (Device view) Select **Platform > Identity > 802.1x** from the Policy selector.
- (Policy view) Select **Router Platform > Identity > 802.1x** from the Policy Type selector. Right-click **802.1x** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- 802.1x on Cisco IOS Routers, page 15-127
- Understanding AAA Server Group Objects, page 9-15
- Basic Interface Settings on Cisco IOS Routers, page 15-20
- Understanding Interface Role Objects, page 9-132
- Chapter K, “Router Platform User Interface Reference”

Field Reference

Table K-79 802.1x Page

Element	Description
AAA Server Group	The RADIUS AAA server group that authenticates the credentials of users trying to access a VPN tunnel. Enter the name of a AAA server group object, or click **Add** to display an Object Selectors, page F-593. If the AAA server group you want is not listed, click the **Create** button in the selector to display the AAA Server Group Dialog Box, page F-12. From here you can define a AAA server group object. **Note** Each AAA server in the selected group must be configured to communicate with an interface that exists on the router; otherwise, validation fails.
Virtual Template	Mandatory for all routers except Integrated Services Routers (ISRs). The untrusted, virtual interface that provides Internet access to unauthenticated traffic. Enter the name of an interface or interface role, or click **Select** to display an Object Selectors, page F-593. If the interface role you want is not listed, click the **Create** button in the selector to display the Interface Role Dialog Box, page F-464. From here you can create an interface role object. **Note** You do not need to configure a virtual template for ISRs, because they automatically use VLANs to provide access. If you do define a virtual template, however, it is used instead of the VLAN. **Note** Deployment might fail if PPP is defined on the virtual template defined here. See PPP Dialog Box, page K-78.

Table K-79 802.1x Page (Continued)

Interface	The trusted, physical interface that provides VPN access to authenticated traffic. Enter the name of an interface or interface role, or click **Select** to display an Object Selectors, page F-593. If the interface role you want is not listed, click the **Create** button in the selector to display the Interface Role Dialog Box, page F-464. From here you can create an interface role object. **Note** The pattern defined in the interface role must represent only one physical interface on the selected device. This interface should be the internal protected interface that you configured as part of the VPN topology. For more information, see Endpoints Page, page G-13.
Number of retries	The number of times the physical interface resends an Extensible Authentication Protocol (EAP) request/identity frame to a client if a response is not received before restarting authentication. Valid values range from 1 to 10. The default is 2. **Note** You should change the default only to adjust for unusual circumstances, such as unreliable links or specific problems with certain clients and authentication servers.
Control type	The control state of the interface, which determines whether the host is granted access to the network. Options are: • Force Authorize—Disables 802.1x authentication and causes the interface to move to the authorized state without requiring any authentication exchange. This means the interface transmits and receives normal traffic without 802.1x-based authentication of the host. This is the default. • Auto—Enables 802.1x authentication and causes the interface to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the interface. If a host is successfully authenticated, the interface state changes to authorized, which enables all frames from the host through the interface.
Enable client reauthentication	When selected, enables periodic reauthentication of client PCs on the 802.1x interface. Reauthentication is performed after the interval defined in the Client reauthentication period timeout field. The default period is 3600 seconds (1 hour). When deselected, periodic reauthentication is not performed.

Table K-79 802.1x Page (Continued)

Client reauthentication period timeout	Applies only when the Enable client reauthentication check box is selected. The number of seconds between client reauthentication attempts. Valid values range from 1 to 65535 seconds. The default is 3600 seconds (1 hour).
Quiet period	The amount of time the router remains in a quiet state after a failed authentication exchange with the client. Authentication exchanges might fail, for example, because the client provided an invalid password. Valid values range from 1 to 65535 seconds. The default is 120 seconds. **Note** Entering a value smaller than the default provides a faster response time to the user.
Rate Limit period	The interval after which the interface throttles the EAP-Start packets it receives from malfunctioning client PCs. Use this setting, called rate limiting, to prevent these clients from wasting router processing power. Valid values range from 1 to 65535 seconds. By default, rate limiting is disabled. **Note** To disable an existing rate limit, delete the value defined in this field and leave the field blank.
AAA Server timeout	The number of seconds the router waits before retransmitting packets to the AAA server. If the router sends an 802.1x packet to the AAA server and the server does not respond, the router sends another packet after this interval elapses. Valid values range from 1 to 65535 seconds. The default is 30 seconds.
Supplicant period	The number of seconds the router waits before retransmitting EAP-Request/Identity packets to the supplicant (client PC). If the router sends an EAP-Request/Identity packet to the client PC (supplicant) and the supplicant does not respond, the router sends the packet again after this interval elapses. Valid values range from 1 to 65535 seconds. The default is 30 seconds.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.

Network Admission Control Policy Page

Network Admission Control (NAC) policies enable Cisco IOS routers acting as network access devices (NADs) to enforce access privileges when an endpoint tries to connect to a network. Access decisions are made on the basis of information provided by the endpoint device, such as its current antivirus state, thus keeping insecure nodes from infecting the network.

You can configure NAC policies on a Cisco IOS router from the following tabs on the Network Admission Control policy page:

- Network Admission Control Page—Setup Tab, page K-183
- Network Admission Control Page—Interfaces Tab, page K-186
- Network Admission Control Page—Identities Tab, page K-189

For more information, see Network Admission Control on Cisco IOS Routers, page 15-134.

Navigation Path

- (Device view) Select **Platform > Identity > Network Admission Control** from the Policy selector.
- (Policy view) Select **Router Platform > Identity > Network Admission Control** from the Policy Type selector. Right-click **Network Admission Control** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- Chapter K, "Router Platform User Interface Reference"

Network Admission Control Page—Setup Tab

Use the Network Admission Control Setup tab to select the Cisco Secure Access Control Servers used for authentication during the NAC process, as well as to define the EAP over UDP settings for communications between the NAD and the client seeking access to the network.

Navigation Path

Go to the Network Admission Control Policy Page, page K-183, then click the **Setup** tab.

Related Topics

- Defining NAC Setup Parameters, page 15-138
- Network Admission Control Page—Interfaces Tab, page K-186
- Network Admission Control Page—Identities Tab, page K-189
- Understanding AAA Server Group Objects, page 9-15

Field Reference

Table K-80 Network Admission Control Setup Tab

Element	Description
AAA Server Group	The AAA server group used for NAC authentication. You must select a server group consisting of Cisco Secure Access Control Server (ACS) devices running the RADIUS protocol. Enter the name of a AAA server group object, or click **Select** to display an Object Selectors, page F-593. If the AAA server group you want is not listed, click the **Create** button in the selector to display the AAA Server Group Dialog Box, page F-12. From here you can define a AAA server group object. **Note** Each AAA server in the selected group must be configured to communicate with an interface that exists on the router; otherwise, validation fails.
Backup AAA Server Group 1	The backup AAA server group in case the AAA servers in the main group are down.
Backup AAA Server Group 2	The secondary backup AAA server group in case the AAA servers in the main group and the first backup group are down.
EAP over UDP (EoU) settings	
Allow IP Station ID	When selected, enables an IP address to be included in the calling-station-id field of RADIUS requests sent to the ACS. When deselected, IP addresses are not included in the calling-station-id field of RADIUS requests sent to the ACS.

Table K-80 Network Admission Control Setup Tab (Continued)

Allow Clientless	When selected, enables devices that do not have the Cisco Trust Agent (CTA) installed to be authenticated through the use of a username and password configured on the ACS. If you select this check box, enter the username and password (including confirmation) in the fields provided. When deselected, NAC prevents devices lacking the CTA from accessing the network, if their traffic matches the intercept ACL (see NAC Interface Configuration Dialog Box, page K-187). **Note** This feature is not supported on routers running Cisco IOS Software Release 12.4(6)T or later.
Max Retry	The maximum number of retries that all NAC interfaces on this router should make when initiating an EAP over UDP session with a connecting device. Valid values range from 1 to 3. The default is 3. **Note** You can override this global value on a specific interface, if required. See Network Admission Control Page—Interfaces Tab, page K-186.
Rate Limit	The number of EAP over UDP posture validations that the router can handle simultaneously. Additional devices cannot be validated until one or more devices drop off. Valid values range from 1 to 200. The default is 20. If you set this value to 0, rate limiting is turned off.
Port	The UDP port to use for EAP over UDP sessions. Valid values range from 1 to 65535. The default is 21862. **Note** For NAC to work, the default ACL on this router must permit UDP traffic over the port designated here for EAP over UDP traffic. For more information, see Working with Access Rules, page 13-63.
Enable Logging	When selected, EAP over UDP events on this router are logged to the device. When deselected, EAP over UDP logging is disabled. This is the default.
Setup tab button	
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.

Network Admission Control Page—Interfaces Tab

Use the Network Admission Control Interfaces tab to select and configure the router interfaces on which to perform NAC. This includes configuring the Intercept ACL and selected EoU interface parameters. A NAC policy must include at least one interface definition in order to function.

Navigation Path

Go to the Network Admission Control Policy Page, page K-183, then click the **Interfaces** tab.

Related Topics

- Defining NAC Interface Parameters, page 15-140
- Network Admission Control Page—Setup Tab, page K-183
- Network Admission Control Page—Identities Tab, page K-189

Field Reference

Table K-81 Network Admission Control Interfaces Tab

Element	Description
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
Interfaces	The name of the interface on which NAC is being performed.
Intercept ACL	The name of the Intercept ACL, which determines the incoming traffic that triggers the interface to make a posture validation check.
EoU Max Retries	The maximum number of retries that this interface should perform when it initializes an EoU session with a connecting device.
Revalidate	Indicates whether the interface revalidates its EoU sessions to make sure they are still active.
Add button	Opens the NAC Interface Configuration Dialog Box, page K-187. From here you can define a NAC interface.
Edit button	Opens the NAC Interface Configuration Dialog Box, page K-187. From here you can edit the selected NAC interface.
Delete button	Deletes the selected NAC interfaces from the table.

Table K-81 Network Admission Control Interfaces Tab (Continued)

Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** icon on the toolbar.

Tip To choose which columns to display in the table, right-click a column header, then select **Show Columns**. For more information about table display options, see Table Columns and Column Heading Features, page 3-26.

NAC Interface Configuration Dialog Box

Use the NAC Interface Configuration dialog box to add or edit the router interfaces on which NAC is being performed.

Navigation Path

Go to the Network Admission Control Page—Interfaces Tab, page K-186, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Defining NAC Interface Parameters, page 15-140
- Basic Interface Settings on Cisco IOS Routers, page 15-20
- Understanding Interface Role Objects, page 9-132
- Understanding Access Control List Objects, page 9-30

Field Reference

Table K-82 NAC Interface Configuration Dialog Box

Element	Description
Interface	The interface that will perform NAC on connecting devices. Enter the name of an interface or interface role, or click **Select** to display an Object Selectors, page F-593. If the interface role you want is not listed, click the **Create** button in the selector to display the Interface Role Dialog Box, page F-464. From here you can create an interface role object.
Intercept ACL	The ACL that defines the traffic requiring posture validation. Enter the name of an ACL object, or click **Add** to display an Object Selectors, page F-593. If the ACL you want is not listed, click the **Create** button in the selector to display the dialog box for defining an ACL object (see Access Control Lists Page, page F-31). **Note** If an authentication proxy is configured on the same interface as NAC, the same Intercept ACL must be used in both policies. Otherwise, deployment may fail. For more information about authentication proxies, see Configuring Settings for AAA (IOS), page 13-151.
EAP over UDP Max Retries	The maximum number of times that the router should try to initiate an EoU session with a connecting device. Valid values range from 1 to 3. The default is 3. **Note** Subinterfaces support the default value only.
Enable EoU Session Revalidation	When selected, the router revalidates its EoU sessions as required. This is the default. When deselected, EoU session revalidation is not performed. **Note** Subinterfaces support the default value only.
OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

Network Admission Control Page—Identities Tab

Use the Network Admission Control Identities tab to view, create, edit, and delete NAC identity profiles and identity actions. Identity profiles define a specific action to perform on traffic received from selected devices, as identified by their IP address, MAC address, or device type. In this way, devices with identity profiles are handled by NAC without having to undergo posture validation against an ACS.

Navigation Path

Go to the Network Admission Control Policy Page, page K-183, then click the **Interfaces** tab.

Related Topics

- Defining NAC Identity Parameters, page 15-143
- Network Admission Control Page—Setup Tab, page K-183
- Network Admission Control Page—Interfaces Tab, page K-186

Field Reference

Table K-83 Network Admission Control Identities Tab

Element	Description
Identity Profiles Table	
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
Profile Definition	The type of identity profile—device IP address, MAC address, or device type (IP phone).
Action Name	The name of the action (defined in the Identity Actions table) that is assigned to this NAC identity profile.
Add button	Opens the NAC Identity Profile Dialog Box, page K-190. From here you can define an identity profile.
Edit button	Opens the NAC Identity Profile Dialog Box, page K-190. From here you can edit a selected identity profile.
Delete button	Deletes the selected identity profiles from the table.

Table K-83 Network Admission Control Identities Tab (Continued)

Identity Actions Table	
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
Action Name	The name of the identity action.
ACL	The ACL applied to profiles to which this identity action is assigned.
Redirect URL	The URL to which traffic from devices to which this identity action is assigned are redirected.
Add button	Opens the NAC Identity Action Dialog Box, page K-191 for defining a NAC identity action.
Edit button	Opens the NAC Identity Action Dialog Box, page K-191 for editing a selected NAC identity action.
Delete button	Deletes the selected identity actions from the table.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** icon on the toolbar.

Tip To choose which columns to display in the table, right-click a column header, then select **Show Columns**. For more information about table display options, see Table Columns and Column Heading Features, page 3-26.

NAC Identity Profile Dialog Box

Use the NAC Identity Profile dialog box to add or edit the NAC profiles assigned to devices that match a specific identity. Identity profiles define a NAC action to apply to all traffic coming from a specific device, based on its IP address, MAC address, or device type (for IP phones).

Navigation Path

Go to the Network Admission Control Page—Identities Tab, page K-189, then click the **Add** or **Edit** button beneath the Identity Profiles table.

Related Topics

- NAC Identity Action Dialog Box, page K-191
- Defining NAC Identity Parameters, page 15-143

Field Reference

Table K-84 NAC Identity Profile Dialog Box

Element	Description
Action Name	The name of the action to assign to the profile. Enter the name of an action, or click **Select** to display a selector. For more information about creating actions, see NAC Identity Action Dialog Box, page K-191.
Profile Definition	The device to which this profile is assigned: • IP Address—The IP address of the device to which this profile should be assigned. The same IP address cannot be used in more than one profile. • MAC Address—The MAC address of the device to which this profile should be assigned. • Cisco IP Phone—Used when defining a NAC identity profile for Cisco IP phones.
OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

NAC Identity Action Dialog Box

Use the NAC Identity Action dialog box to add or edit the actions assigned to NAC identity profiles.

Navigation Path

Go to the Network Admission Control Page—Identities Tab, page K-189, then click the **Add** or **Edit** button beneath the Identity Actions table.

Related Topics

- NAC Identity Profile Dialog Box, page K-190

- Defining NAC Identity Parameters, page 15-143
- Understanding Access Control List Objects, page 9-30

Field Reference

Table K-85 NAC Identity Action Dialog Box

Element	Description
Name	A descriptive name for the identity action. Use this name when you select an action to assign to a NAC identity profile. See NAC Identity Profile Dialog Box, page K-190.
Access Control Lists	The ACL that defines how to handle traffic received from a device which is assigned a profile that includes this action. Enter the name of an ACL object, or click **Add** to display an Object Selectors, page F-593. If the ACL you want is not listed, click the **Create** button in the selector to display the dialog box for defining an ACL object (see Access Control Lists Page, page F-31). **Note** You cannot select the same ACL object that is being used for the intercept ACL. See NAC Interface Configuration Dialog Box, page K-187.
Redirect URL	The address of the remediation server to which traffic from the device should be redirected. Redirect URLs are usually of the form **http://URL** or **https://URL**.
OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

Logging Setup Policy Page

Use the Logging Setup page to enable logging and define basic logging parameters on the selected Cisco IOS router.

For more information, see Defining Logging Setup Parameters, page 15-146.

Note We strongly recommend that you define an NTP policy on all routers on which logging is enabled in order to create accurate timestamps for each log message. For more information, see NTP Policy Page, page K-174.

Note If you unassign a logging setup policy, the default logging configuration is restored on the device upon deployment.

Navigation Path

- (Device view) Select **Platform > Logging > Logging Setup** from the Policy selector.
- (Policy view) Select **Router Platform > Logging > Logging Setup** from the Policy Type selector. Right-click **Logging Setup** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- Logging on Cisco IOS Routers, page 15-144
- Syslog Servers Policy Page, page K-197
- NTP on Cisco IOS Routers, page 15-124
- Chapter K, “Router Platform User Interface Reference”
- Understanding Interface Role Objects, page 9-132

Field Reference

Table K-86 Logging Setup Page

Element	Description
Enable Logging	When selected, logging is enabled on the device. When deselected, logging is disabled on the device. This is the default. **Tip** To use the device’s default logging settings, select the Enable Logging check box, then click **Save**, without entering additional values.

Table K-86 Logging Setup Page (Continued)

Source Interface	The source address for all outgoing log messages sent to a syslog server. This setting may be necessary when the syslog server cannot respond to the address from which the log message originated (for example, due to a firewall). If you do not define a value in this field, the address of the outgoing interface is used. Enter the name of an interface or interface role, or click **Select** to display an Object Selectors, page F-593. If the interface role you want is not listed, click the **Create** button in the selector to display the Interface Role Dialog Box, page F-464. From here you can define an interface role object.
Trap	Defines which log messages are forwarded to a syslog server: • Enable Trap—When selected, log messages are sent to the syslog server. This is the default. When deselected, log messages are not sent. • Trap Level—The lowest severity level of messages that are logged and sent to the syslog server. All messages of this severity and greater are logged. Severity levels are identified by a name and a number. For more information, see Table 15-5 on page 15-145. **Tip** To restore the router's default trap settings, select **Enable Trap**, then select the blank setting from the Trap Level list.

Table K-86 Logging Setup Page (Continued)

Logging Buffer	Defines whether log messages are saved locally to a buffer on the device. • Enable Buffer—When selected, log messages are saved to a buffer on the device. This is the default. When deselected, a log buffer is not maintained on the device. • Buffer Size—The size of the buffer in bytes. Valid values range from 4096 to 4294967295 bytes (4 kilobytes to 4 gigabytes). The default size varies by platform. Make sure not to make the buffer so large that the router runs out of memory for other tasks; otherwise, deployment might fail. **Note** The maximum buffer size might be smaller on some devices. • Severity Level—The lowest severity level of messages that are saved in the buffer. All messages of this severity and greater are saved. On most Cisco IOS routers, the default severity level is 7 (debugging). Severity levels are identified by a name and a number. For more information, see Table 15-5 on page 15-145. • Use XML Format—When selected, log messages are saved to a buffer in XML format. (You can configure both the regular buffer and the XML buffer in the same policy.) When deselected, an XML buffer is not maintained on the device. • Buffer Size—The size of the XML buffer in bytes. Valid values range from 4096 to 4294967295 bytes (4 kilobytes to 4 gigabytes). **Note** The maximum buffer size might be smaller on some devices. **Tip** To restore the router's default buffer settings, select **Enable Trap**, erase the buffer size setting, then select the blank setting from the Severity Level list.

Table K-86 Logging Setup Page (Continued)

Rate Limit	Limits the rate of log messages sent to the syslog server. • Enable Rate Limit—When selected, the rate limit is enabled. When deselected, the rate limit is disabled. • Messages per Sec.—The maximum number of logging messages that can be sent per second. Valid values range from 1 to 10000. The default is 10 messages per second. • Exclude—The types of messages to *exclude* from the rate limit. This setting excludes the severity level you select as well as all messages with a lower severity level number (that is, more severe). The default is 3 (errors), which excludes all log messages with a severity level of 3, 2 (critical), 1 (alerts), or 0 (emergencies) from the rate limit. For more information about severity levels, see Table 15-5 on page 15-145. • All Messages—When selected, the rate limit applies to all messages except console messages. • Console Messages—When selected, the rate limit applies to console messages only. **Tip** To restore the router's default rate limit settings, select the **Enable Rate Limit** check box, then erase the rate limit value setting.
Origin ID	The origin identifier that is added to the beginning of all syslog messages sent from this device to the remote syslog server. The origin identifier is useful in cases where you send output from multiple devices to a single syslog server. • ID Type—The type of origin identifier added to the beginning of each syslog message. Options are: – IP Address—The IP address of the source device. – Hostname—The hostname of the source device. – String—User-defined text. • Value—Applies only when you select String as the ID type. Enter the text of the user-defined string. Spaces are permitted, except for the first character. **Note** The origin identifier is not added to messages sent to local destinations, such as the buffer, the console, and the monitor.

Table K-86 Logging Setup Page (Continued)

Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.

Syslog Servers Policy Page

Use the Syslog Servers page to create, edit, and delete servers that collect log messages from the router.

For more information, see Defining Syslog Servers, page 15-149.

Note To enable logging to the syslog servers defined on this page, you must enable logging and define basic parameters on the Logging Setup Policy Page, page K-192.

Navigation Path

- (Device view) Select **Platform > Logging > Syslog Servers** from the Policy selector.
- (Policy view) Select **Router Platform > Logging > Syslog Servers** from the Policy Type selector. Right-click **Syslog Servers** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- Logging on Cisco IOS Routers, page 15-144
- Chapter K, “Router Platform User Interface Reference”
- Syslog Server Dialog Box, page K-198

Field Reference

Table K-87 Syslog Servers Page

Element	Description
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.

Table K-87 Syslog Servers Page (Continued)

IP Address	The name of the syslog server, as represented by a network/host object, or its IP address.
XML	Indicates whether the syslog server receives log messages in XML format.
Add button	Opens the Syslog Server Dialog Box, page K-198. From here you can define a syslog server.
Edit button	Opens the Syslog Server Dialog Box, page K-198. From here you can edit the selected syslog server.
Delete button	Deletes the selected syslog server from the table.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** icon on the toolbar.

Tip To choose which columns to display in the table, right-click a column header, then select **Show Columns**. For more information about table display options, see Table Columns and Column Heading Features, page 3-26.

Syslog Server Dialog Box

Use the Syslog Server dialog box to define the server that collects syslog messages from the router. You can also define whether the log messages it receives are in XML format or plain text.

Note To enable logging to the syslog servers defined on this page, you must enable logging and define basic parameters on the Logging Setup Policy Page, page K-192.

Navigation Path

Go to the Syslog Servers Policy Page, page K-197, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Defining Syslog Servers, page 15-149
- Logging on Cisco IOS Routers, page 15-144
- Understanding Network/Host Objects, page 9-144

Field Reference

Table K-88 Syslog Server Dialog Box

Element	Description
IP Address	The IP address of the syslog server. Enter an IP address or the name of a network/host object, or click **Select** to display an Object Selectors, page F-593. If the network/host object you want is not listed, click the **Create** button in the selector to display the Network/Host Dialog Box, page F-477. From here you can define a network/host object.
Forward Messages in XML Format	When selected, log messages are sent to the syslog server in XML format. When deselected, log messages are sent to the syslog server as plain text.
OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

Quality of Service Policy Page

Use the Quality of Service page to view, create, and edit QoS classes on specific interfaces of the selected device or on the control plane. QoS policies enable you to define techniques for managing the delay, delay variation (jitter), bandwidth, and packet loss parameters on a network. In addition, you can use the Quality of Service page to configure hierarchical shaping on an interface as an alternative to configuring shaping parameters for individual QoS classes.

For more information, see Quality of Service on Cisco IOS Routers, page 15-151.

Navigation Path

- (Device view) Select **Platform > Quality of Service** from the Policy selector.

- (Policy view) Select **Router Platform > Quality of Service** from the Policy Type selector. Right-click **Quality of Service** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- Defining QoS Policies, page 15-164
- Chapter K, "Router Platform User Interface Reference"

Field Reference

Table K-89 Quality of Service Page

Element	Description
Apply To	The router component on which to define the QoS policy: • Interfaces—Configures QoS classes on specific interfaces. • Control Plane—Configures QoS on the router control plane. See Understanding Control Plane Policing, page 15-163. **Note** If you configure QoS on both the interfaces and the control plane of the same device, only the control plane configuration is deployed.
QoS Policy Table	
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
Interface	The interface on which you want to define QoS parameters.
Direction	The traffic direction on which the QoS parameters on this interface apply—input or output.
Shaping	Indicates whether hierarchical shaping is defined on this interface.
Type	Applies only when you enable hierarchical shaping on this interface. The type of hierarchical shaping performed on this interface—average or peak.
CIR	Applies only when you enable hierarchical shaping on this interface. The average data rate (also known as the committed information rate or CIR), which is represented as a percentage of the overall bandwidth available on this interface.

Table K-89 Quality of Service Page (Continued)

Sustained Burst	Applies only when you enable hierarchical shaping on this interface. The normal burst size allowed on this interface, in milliseconds.
Excess Burst	Applies only when you enable hierarchical shaping on this interface. The excess burst size allowed on this interface, in milliseconds.
Add button	Opens the QoS Policy Dialog Box, page K-203. From here you can select the interface on which you want to define QoS parameters.
Edit button	Opens the QoS Policy Dialog Box, page K-203. From here you can edit the selected QoS interface.
Delete button	Deletes the selected QoS interfaces from the table.
Interface QoS Classes Table	
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
No.	The sequential number of the class. QoS is applied to packets on a first-match basis, based on class order.
Default Class	Indicates whether this class is the default for all packets on the interface that do not match the criteria of the other defined classes.
Matching	The matching criteria that determine whether packets are considered members of this class. This includes the match method and any combination of protocols, precedence and DSCP values, and ACL names.
Marking	The IP Precedence (IPP) or Differentiated Services Code Point (DSCP) setting for the traffic in this class.
Queuing and Congestion Avoidance	The queuing settings that are defined for this class.
Policing	Indicates whether policing is configured for this class.
Shaping	Indicates whether Distributed Traffic Shaping (DTS) is configured for this class.
Up Row	Moves the selected class up one row.
Down Row	Moves the selected class down one row.
Add button	Opens the QoS Class Dialog Box, page K-205. From here you can create a QoS class definition for the selected interface.

Table K-89 Quality of Service Page (Continued)

Edit button	Opens the QoS Class Dialog Box, page K-205. From here you can edit the selected QoS class.
Delete button	Deletes the selected QoS classes from the table.
Control Plane QoS Classes Table	
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
No.	The sequential number of the class. QoS is applied to packets on a first-match basis, based on class order.
Default Class	Indicates whether this class is the default for all packets on the interface that do not match the criteria of the other defined classes.
Matching	Indicates whether packets must match any of the defined criteria or all of the criteria to be considered members of this class.
Policing	Indicates whether policing is configured for this class.
Add button	Opens the QoS Class Dialog Box, page K-205. From here you can create a QoS class definition for the control plane.
Edit button	Opens the QoS Class Dialog Box, page K-205. From here you can edit the selected QoS class.
Delete button	Deletes the selected QoS classes from the table.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** icon on the toolbar.

Tip To choose which columns to display in the table, right-click a column header, then select **Show Columns**. For more information about table display options, see Table Columns and Column Heading Features, page 3-26.

QoS Policy Dialog Box

Use the QoS Policy dialog box to select an interface on which you want to define QoS parameters. In addition, you can use this dialog box to configure a single set of shaping parameters for all the traffic on the selected interface (known as hierarchical shaping). Using hierarchical shaping eliminates the need to configure shaping parameters for each QoS class defined on the interface.

Note This dialog box is not applicable when defining a QoS policy on the control plane. For more information, see Defining QoS on the Control Plane, page 15-168.

After you create your QoS interface definitions, you can define one or more QoS classes for each interface. For more information, see QoS Class Dialog Box, page K-205.

Navigation Path

Go to the Quality of Service Policy Page, page K-199, then click the **Add** or **Edit** button beneath the upper table to define a QoS interface definition.

Related Topics

- Defining QoS Policies, page 15-164
- Quality of Service on Cisco IOS Routers, page 15-151
- Basic Interface Settings on Cisco IOS Routers, page 15-20
- Understanding Interface Role Objects, page 9-132

Field Reference

Table K-90 QoS Policy Dialog Box

Element	Description
Interface	The interface on which QoS is defined. Enter the name of an interface or interface role, or click **Select** to display an Object Selectors, page F-593. If the interface role you want is not listed, click the **Create** button in the selector to display the Interface Role Dialog Box, page F-464. From here you can create an interface role object.

Table K-90 QoS Policy Dialog Box (Continued)

Direction	The direction of the traffic on which to configure QoS: • Output—Traffic that exits the interface. • Input—Traffic that enters the interface.
Hierarchical Shaping settings	
Enable Shaping	When selected, configures hierarchical traffic shaping on the selected interface. When deselected, hierarchical shaping is not used. **Note** Shaping can be performed only on output traffic.
Type	The type of shaping to perform: • Average—Limits the data rate for each interval to the sustained burst rate (also known as the Committed Burst rate or Bc), achieving an average rate no higher than the committed information rate (CIR). Additional packets are buffered until they can be sent. • Peak—Limits the data rate for each interval to the sustained burst rate plus the excess burst rate (Be). Additional packets are buffered until they can be sent.
CIR	The average data rate (also known as the committed information rate or CIR). You can define this amount by: • Percentage—Valid values range from 0 to 100% of the overall available bandwidth. • Bit/sec—Valid values range from 8000 to 1000000000 bits per second. Although data bursts during an interval may exceed this rate, the average data rate over any multiple integral of the interval will not exceed this rate.

Table K-90 QoS Policy Dialog Box (Continued)

Sustained Burst	The normal burst size. If you select average as the shaping type, data bursts during an interval are limited to this value. The range of valid values is determined by the CIR: • When the CIR is defined by percentage—Valid values range from 10 to 2000 milliseconds. • When the CIR is defined by an absolute value—Valid values range from 1000 to 154400000 bytes, in multiples of 128 bytes. **Note** We recommend that you leave this field blank when the CIR is defined by an absolute value. This allows the algorithms used by the device to determine the optimal sustained burst value.
Excess Burst	The excess burst size. If you select peak as the shaping type, data bursts during an interval can equal the sum of the sustained burst value plus this value. The average data rate over multiple intervals, however, will continue to conform to the CIR. The range of valid values is determined by the CIR: • When the CIR is defined by percentage—Valid values range from 10 to 2000 milliseconds. • When the CIR is defined by an absolute value—Valid values range from 1000 to 154400000 bytes, in multiples of 128 bytes. **Note** If you do not configure this field when the CIR is defined by an absolute value, the sustained burst value is used.
OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

QoS Class Dialog Box

Use the QoS Class dialog box to create or edit a QoS class on a selected interface or control plane of a Cisco IOS router. You can define up to 16 classes on a single interface and 256 classes for the device as a whole.

Note QoS is applied to packets on a first-match basis. The router examines the table of QoS classes starting from the top and applies the properties of the first class whose matching criteria matches the packet. Therefore, it is important that you define and order your classes carefully. The default class should be placed last to prevent traffic that matches a specific class from being treated as unmatched traffic.

Navigation Path

Go to the Quality of Service Policy Page, page K-199. Complete the options at the top of the page, then do one of the following:

- To create a QoS class, select an interface from the upper table, then click the **Add** button beneath the QoS Class table. When creating a QoS class for the control plane, just click the **Add** button beneath the table.
- To edit a QoS class:
  - Select the interface whose class you want to edit from the upper table (Not required when selecting the control plane.).
  - Select the relevant class defined for that interface in the QoS Classes table. (Not required when selecting the control plane.)
  - Click the **Edit** button under the QoS Class table.

Related Topics

- QoS Policy Dialog Box, page K-203
- Defining QoS Policies, page 15-164
- Defining QoS on Interfaces, page 15-165
- Defining QoS on the Control Plane, page 15-168

Field Reference

Table K-91 QoS Class Dialog Box

Element	Description
Set as Default Class	When selected, enables you to define the default class for all traffic that does not match the other QoS classes on this interface. When deselected, enables you to define a specific QoS class on this interface. **Note** When you define the default class, you do not configure any matching parameters; by definition the class consists of all traffic that does not match any of the other classes. Therefore, the Matching tab is disabled.
Matching tab	Defines the traffic that is included in this QoS class. See QoS Class Dialog Box—Matching Tab, page K-208.
Marking tab	Marks the traffic in this class so that downstream devices can properly identify it. See QoS Class Dialog Box—Marking Tab, page K-211.
Queuing and Congestion Avoidance tab	Defines how to queue the output traffic in this class. See QoS Class Dialog Box—Queuing and Congestion Avoidance Tab, page K-212.
Policing tab	Limits the traffic flow for this class to a configured rate. See QoS Class Dialog Box—Policing Tab, page K-214.
Shaping tab	Controls the flow of output traffic for this class so that it conforms with the requirements of downstream devices. See QoS Class Dialog Box—Shaping Tab, page K-217.

Note When you configure a QoS policy on the control plane, only the Matching tab and Policing tab are available.

QoS Class Dialog Box—Matching Tab

Use the Matching tab of the QoS Class dialog box to define which traffic over the selected interface is considered to be part of this class.

Note When you define the default class, the Matching tab is disabled.

Navigation Path

Go to the QoS Class Dialog Box, page K-205, then click the **Matching** tab.

Related Topics

- Defining QoS Class Matching Parameters, page 15-170
- Defining QoS on Interfaces, page 15-165
- Defining QoS on the Control Plane, page 15-168
- Quality of Service Policy Page, page K-199
- Understanding Access Control List Objects, page 9-30

Field Reference

Table K-92 QoS Class Dialog Box—Matching Tab

Element	Description
Match Method	The traffic matching option used for this class: • Any—Assigns traffic matching any of the defined class map criteria to this QoS class. • All—Assigns only traffic matching all of the defined class map criteria to this QoS class.

Table K-92 QoS Class Dialog Box—Matching Tab (Continued)

Protocol	One or more protocols included in this class map. Click **Add** to display a selector. Select one or more items from the Available Protocols list, then click **>>** to add them to the Selected Protocols list. The only protocol available for the control plane is ARP; ARP and CDP are not available for input classes configured on an interface. When you finish, click **OK** to return to the QoS Class dialog box. Your selections are displayed in the Protocol field. **Note** To remove a protocol from the QoS class, select it from the Protocol field, then click **Delete**.
Precedence	One or more IP Precedence (IPP) values included in this class map. Click **Add** to display a selector. Select one or more items from the Available Precedences list, then click **>>** to add them to the Selected Precedences list. **Note** For more information about IP precedence values, see Table 15-6 on page 15-154. When you finish, click **OK** to return to the QoS Class dialog box. Your selections are displayed in the Precedence field. **Note** To remove an IPP value from the QoS class, select it from the Precedence field, then click **Delete**.
DSCP	One or more Differentiated Services Code Point (DSCP) values included in this class map. Click **Add** to display a selector. Select one or more items (up to eight) from the Available DSCPs list, then click **>>** to add them to the Selected DSCPs list. When you finish, click **OK** to return to the QoS Class dialog box. Your selections are displayed in the DSCP field. **Note** To remove a DSCP value from the QoS class, select it from the DSCP field, then click **Delete**.
ACL	The ACLs that are used for defining which traffic requires QoS. Enter one or more ACL objects, or click **Select** to display an Object Selectors, page F-593. For more information, see Edit ACLs Dialog Box—QoS Classes, page K-210. Use the up and down arrows to order the ACLs in the list. We recommend that you place frequently used ACLs at the top of the list to optimize the matching process.

Edit ACLs Dialog Box—QoS Classes

When configuring a QoS policy on a Cisco IOS router, use the Edit ACLs dialog box to specify which ACLs should be included in the matching criteria for the selected class. Traffic matching this criteria is included as part of the class.

Navigation Path

Go to the QoS Class Dialog Box—Matching Tab, page K-208, then click **Edit** in the ACL field.

Related Topics

- Defining QoS Class Matching Parameters, page 15-170
- Defining QoS on Interfaces, page 15-165
- Defining QoS on the Control Plane, page 15-168
- Quality of Service Policy Page, page K-199

Field Reference

Table K-93 Edit ACLs Dialog Box—QoS Classes

Element	Description
Access Control Lists	The ACLs to include as part of the matching criteria for the selected QoS class. Enter the names of the ACLs or click **Select** to use an Object Selectors, page F-593. For more information, see Understanding Access Control List Objects, page 9-30.
Select button	Opens an Object Selectors, page F-593 for selecting ACLs. Using the selector eliminates the need to manually enter this information. If the ACL you want is not listed, click the **Create** button in the selector to display the dialog box for defining an ACL object (see Access Control Lists Page, page F-31).
OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

QoS Class Dialog Box—Marking Tab

Use the Marking tab of the QoS Class dialog box to classify packets. Traffic policers and shapers use these classifications to ensure adherence to the contracted level of service. Downstream devices use this classification to identify the packets and apply the appropriate QoS functions to them.

Note The Marking tab is unavailable when you define a QoS policy on the control plane.

Navigation Path

Go to the QoS Class Dialog Box, page K-205, then click the **Marking** tab.

Related Topics

- Defining QoS Class Marking Parameters, page 15-172
- Defining QoS on Interfaces, page 15-165
- Defining QoS on the Control Plane, page 15-168
- Quality of Service Policy Page, page K-199

Field Reference

Table K-94 QoS Class Dialog Box—Marking Tab

Element	Description
Enable Marking	When selected, enables you to mark the traffic in this QoS class with a specific precedence or DSCP value (regardless of any value the traffic might have had when it first entered the device). This mark enables downstream devices to identify the traffic and apply the appropriate QoS features to it. When deselected, disables all marking options for the selected QoS class. The traffic in this QoS class maintains its original precedence or DSCP value, if any.

Table K-94 QoS Class Dialog Box—Marking Tab (Continued)

Precedence	The precedence value with which to mark the traffic in this class: • network (7) • internet match (6) • critical (5) • flash-override (4) • flash (3) • immediate (2) • priority (1) • routine (0)
DSCP	The DSCP value (0 to 63) with which to mark the traffic in this class.

QoS Class Dialog Box—Queuing and Congestion Avoidance Tab

Use the Queuing and Congestion Avoidance tab of the QoS Class dialog box to perform Class-Based Weighted Fair Queuing (CBWFQ) on the output traffic in the selected QoS class. Queuing prioritizes traffic and manages congestion on your network by determining the order in which packets are sent out over an interface.

The fields displayed in the Queuing tab depend on whether you are defining a specific QoS class or the default class.

Note The Queuing and Congestion Avoidance tab is unavailable when you define a QoS policy on the control plane or on input traffic.

Navigation Path

Go to the QoS Class Dialog Box, page K-205, then click the **Queuing and Congestion Avoidance** tab.

Related Topics

- Defining QoS Class Queuing Parameters, page 15-173
- Defining QoS on Interfaces, page 15-165

- Defining QoS on the Control Plane, page 15-168
- Quality of Service Policy Page, page K-199

Field Reference

Table K-95 QoS Class Dialog Box—Queuing and Congestion Avoidance Tab

Element	Description
Enable Queuing and Congestion Avoidance	When selected, enables you to define queuing parameters for the selected QoS class. When deselected, disables all queuing options for the selected QoS class. **Note** Queuing is available only for output traffic. Available queuing options depend on whether you are defining a specific QoS class or the default class.
Priority	Applies only when you are defining a specific QoS class for priority traffic (for example, voice traffic). The amount of bandwidth on this interface allocated to high-priority traffic. You can define this amount by: • Percentage—Valid values range from 0 to 100%. • Kbit/sec—Valid values range from 8-2000000 kilobits per second. Low-Latency Queuing, page 15-158 (LLQ) ensures that priority traffic receives this defined bandwidth. **Note** You can define this option for one class only per interface. If you select this option, the Shaping tab is disabled.
Fair Queue	Applies only when you are defining the default class. The number of dynamic queues to reserve for this class. By default, this number is based on the available bandwidth of the selected interface. Values range from 16 to 4096, based on powers of 2. For more information, see Table 15-7 on page 15-159. **Note** Failure to provide a sufficient number of queues for the default class (a condition known as starvation) could result in the traffic not being sent.

Table K-95 QoS Class Dialog Box—Queuing and Congestion Avoidance Tab (Continued)

Bandwidth	The minimum bandwidth to guarantee to this class (a specific class or the default class). You can define this amount by: • Percentage—Valid values range from 0 to 100% of the total available bandwidth. • Kbit/sec—Valid values range from 8-2000000 kilobits per second.
Queue Limit	The maximum number of packets that can be queued for the class. Any additional packets are dropped using tail drop until the congestion is gone. **Note** This is the default option for limiting queue size unless Weighted Random Early Detection (WRED) is configured.
WRED Weight for Mean Queue Depth	The exponential weight factor to use to calculate the average queue size. Use this option when defining WRED instead of tail drop for this class. When queue size exceeds the value determined by this weight factor, WRED randomly discards packets until the transmitting protocol decreases its transmission rate to ease congestion. Exponent values range from 1 to 16. The default is 9. **Note** This option is best suited for protocols like TCP, which respond to dropped packets by decreasing the transmission rate. We recommend that you do not change the default unless you determine that your applications would benefit from the change.

QoS Class Dialog Box—Policing Tab

Use the Policing tab of the QoS Class dialog box to configure rate limits on the traffic in a selected QoS class. Excess traffic is either dropped or transmitted with a different (typically lower) priority.

Navigation Path

Go to the QoS Class Dialog Box, page K-205, then click the **Policing** tab.

Related Topics

- Defining QoS Class Policing Parameters, page 15-175
- Defining QoS on Interfaces, page 15-165
- Defining QoS on the Control Plane, page 15-168

- Quality of Service Policy Page, page K-199

Field Reference

Table K-96 QoS Class Dialog Box—Policing Tab

Element	Description
Enable Policing	When selected, enables you to configure Class-Based Policing to control the maximum rate of traffic for this class. Security Manager uses a two-token bucket algorithm, which includes a defined violate action that is performed when neither bucket can accommodate the incoming packet. When deselected, disables all policing options for the selected QoS class.
CIR	The average data rate (also known as the committed information rate or CIR). You can define this amount by: • Percentage—Valid values range from 0 to 100% of the overall available bandwidth. • Bit/sec—Valid values range from 8000 to 2000000000 bits per second. In the token bucket algorithm, this rate represents the token arrival rate for filling both token buckets. Traffic that falls under this rate always conforms. **Note** When you configure Understanding Control Plane Policing, page 15-163, you must define the CIR in bits per second.
Conform Burst	The normal burst size, which determines how large traffic bursts can be before some traffic exceeds the rate limit. In the token bucket algorithm, it represents the full size of the first (conform) token bucket. The range of valid values is determined by the CIR: • When the CIR is defined by percentage—Valid values range from 1 to 2000 milliseconds. • When the CIR is defined by an absolute value—Valid values range from 1000-512000000 bytes.

Table K-96 QoS Class Dialog Box—Policing Tab (Continued)

Excess Burst	The excess burst size, which determines how large traffic bursts can be before all traffic exceeds the rate limit. In the token bucket algorithm, it represents the full size of the second (exceed) token bucket. The range of valid values is determined by the CIR: • When the CIR is defined by percentage—Valid values range from 1 to 2000 milliseconds. • When the CIR is defined by an absolute value—Valid values range from 1000-512000000 bytes.
Conform action	The action to take on packets that conform to the rate limit: • transmit—Transmits the packet. • set-prec-transmit—Sets the IP precedence to a value you specify (0 to 7) and then sends the packet. Not available on the control plane. • set-dscp-transmit—Sets the DSCP to a value you specify (0 to 63) and then sends the packet. Not available on the control plane. • drop—Drops the packet.
Exceed action	The action to take on packets that exceed the rate limit, but can be handled using the second (exceed) token bucket. The actions available for selection depend on the defined conform action. For example, if you select one of the set options as the conform action, you cannot select transmit as the exceed action. If you select drop as the conform action, then you must also select drop as the exceed action.
Violate action	The action to take on packets that cannot be serviced by either the conform bucket or the exceed bucket. The actions available for selection depend on the defined exceed action. For example, if you select one of the set options as the exceed action, you cannot select transmit as the violate action. If you select drop as the exceed action, then you must also select drop as the violate action.

QoS Class Dialog Box—Shaping Tab

Use the Shaping tab of the QoS Class dialog box to control the rate of output traffic for the selected QoS class. Shaping typically delays excess traffic by using a buffer, or queuing mechanism, to hold packets and shape the flow when the data rate of the source is higher than expected.

Note The Shaping tab is unavailable when you define a QoS policy on the control plane, use hierarchical shaping on the interface, define a QoS class for input traffic, or perform queuing on priority traffic.

Navigation Path

Go to the QoS Class Dialog Box, page K-205, then click the **Shaping** tab.

Related Topics

- Defining QoS Class Shaping Parameters, page 15-177
- Defining QoS on Interfaces, page 15-165
- Defining QoS on the Control Plane, page 15-168
- Quality of Service Policy Page, page K-199

Field Reference

Table K-97 QoS Class Dialog Box—Shaping Tab

Element	Description
Enable Shaping	When selected, enables you to configure Distributed Traffic Shaping (DTS) to control the rate of traffic for this class. DTS uses queues to buffer traffic surges that can congest the network. When deselected, disables all shaping options for the selected QoS class. **Note** Shaping can be performed only on output traffic.

Table K-97 QoS Class Dialog Box—Shaping Tab (Continued)

Type	The type of shaping to perform: • Average—Limits the data rate for each interval to the sustained burst rate (also known as the committed burst rate or Bc), achieving an average rate no higher than the committed information rate (CIR). Additional packets are buffered until they can be sent. • Peak—Limits the data rate for each interval to the sustained burst rate plus the excess burst rate (Be). Additional packets are buffered until they can be sent.
CIR	The average data rate (also known as the committed information rate or CIR). You can define this amount by: • Percentage—Valid values range from 0 to 100% of the overall available bandwidth. • Bit/sec—Valid values range from 8000 to 1000000000 bits per second. Although data bursts during an interval may exceed this rate, the average data rate over any multiple integral of the interval will not exceed this rate.
Sustained Burst	The normal burst size. If you select average as the shaping type, data bursts during an interval are limited to this value. The range of valid values is determined by the CIR: • When the CIR is defined by percentage—Valid values range from 10 to 2000 milliseconds. • When the CIR is defined by an absolute value—Valid values range from 1000 to 154400000 bytes, in multiples of 128 bytes. **Note** We recommend that you leave this field blank when the CIR is defined by an absolute value. This allows the algorithms used by the device to determine the optimal sustained burst value.

Table K-97 QoS Class Dialog Box—Shaping Tab (Continued)

Excess Burst	The excess burst size. If you select peak as the shaping type, data bursts during an interval can equal the sum of the sustained burst value plus this value. The average data rate over multiple intervals, however, will continue to conform to the CIR. The range of valid values is determined by the CIR: • When the CIR is defined by percentage—Valid values range from 10 to 2000 milliseconds. • When the CIR is defined by an absolute value—Valid values range from 1000 to 154400000 bytes, in multiples of 128 bytes. **Note** If you do not configure this field when the CIR is defined by an absolute value, the sustained burst value is used.

BGP Routing Policy Page

Border Gateway Protocol (BGP) is an exterior gateway protocol (EGP) that performs routing between multiple autonomous systems or domains and exchanges routing and reachability information with other BGP systems. BGP is used to exchange routing information on the Internet and is the protocol used between Internet service providers.

You can configure BGP routing policies from the following tabs on the BGP Routing page:

- BGP Page—Setup Tab, page K-220
- BGP Page—Redistribution Tab, page K-223

For more information, see BGP Routing on Cisco IOS Routers, page 15-179.

Navigation Path

- (Device view) Select **Platform > Routing > BGP** from the Policy selector.
- (Policy view) Select **Router Platform > Routing > BGP** from the Policy Type selector. Right-click **BGP** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- Chapter K, "Router Platform User Interface Reference"

BGP Page—Setup Tab

Use the BGP Setup tab to define the number of the autonomous system (AS) in which the selected router is located. You must then define which networks are included in the AS and which networks are the internal and external neighbors of the router. Additionally, you can enable or disable options that govern the interaction between BGP and Interior Gateway Protocols (IGPs), such as OSPF and EIGRP. Use a third option to enable the logging of messages from BGP neighbors.

Navigation Path

Go to the BGP Routing Policy Page, page K-219, then click the **Setup** tab.

Related Topics

- Defining BGP Routes, page 15-180
- BGP Page—Redistribution Tab, page K-223
- Supported IP Address Formats, page 9-145
- Understanding Network/Host Objects, page 9-144

Field Reference

Table K-98 BGP Setup Tab

Element	Description
AS Number	The number of the autonomous system in which the router is located. Valid values range from 1 to 65535. This number enables a BGP routing process.

Table K-98 BGP Setup Tab (Continued)

Networks	The networks associated with the BGP route. Enter one or more network addresses or network/host objects, or click **Select** to display an Object Selectors, page F-593. If the network you want is not listed, click the **Create** button in the selector to display the Network/Host Dialog Box, page F-477. From here you can define a network/host object. **Note** To remove a network from the route, select it from the Network field, then click **Delete**.
Neighbors	The *internal* neighbors (those located in the same AS as the router) and *external* neighbors (located in different ASs) of the router. See Neighbors Dialog Box, page K-222.
Auto-Summary	When selected, automatic summarization is enabled. When a subnet is redistributed from an IGP (such as RIP, OSPF or EIGRP) into BGP, this BGP version 3 feature injects only the network route into the BGP table. Automatic summarization reduces the size and complexity of the routing table that the router must maintain. When deselected, automatic summarization is disabled. This is the default.
Synchronization	When selected, synchronization is enabled. Use this feature to ensure that all routers in your network are consistent about the routes they advertise. Synchronization forces BGP to wait until the IGP propagates routing information across the AS. When deselected, synchronization is disabled. You can disable synchronization if this router does not pass traffic from a different AS to a third AS, or if all the routers in the AS are running BGP. Disabling this feature has the benefit of reducing the number of routes the IGP must carry, which improves convergence times. This is the default.
Log-Neighbor	When selected, enables the logging of messages that are generated when a BGP neighbors resets, connects to the network, or is disconnected. This is the default. When deselected, message logging is disabled.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.

Neighbors Dialog Box

Use the Neighbors dialog box to define the internal and external neighbors of the selected router.

Navigation Path

Go to the BGP Page—Setup Tab, page K-220, then click the **Add** or **Edit** button in the Neighbors field.

Related Topics

- Defining BGP Routes, page 15-180
- Supported IP Address Formats, page 9-145
- Understanding Network/Host Objects, page 9-144

Field Reference

Table K-99 Neighbors Dialog Box

Element	Description
AS Number	The number of the AS containing BGP neighbors. Internal neighbors have the same AS number as the network of the selected router. External neighbors have a different AS number.
IP Address	The IP addresses of the hosts that are neighbors of the router. BGP neighbors exchange routing information with each other whenever changes to the routing table are detected. When you define BGP neighbors, the IP addresses cannot belong to an interface on the selected router. In addition, you cannot define the same IP address in more than one AS. Enter one or more addresses or network/host objects, or click **Select** to display an Object Selectors, page F-593. If the host you want is not listed, click the **Create** button in the selector to display the Network/Host Dialog Box, page F-477. From here you can define a network/host object. **Note** To remove a host from the list of BGP neighbors, select it from the Hosts field, then click **Delete**.

Table K-99 Neighbors Dialog Box (Continued)

OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

BGP Page—Redistribution Tab

Use the BGP Redistribution tab to view, create, edit, and delete redistribution settings when performing redistribution into a BGP autonomous system (AS).

Note You must define BGP setup parameters before you can access the BGP Redistribution tab. See BGP Page—Setup Tab, page K-220.

Navigation Path

Go to the BGP Routing Policy Page, page K-219, then click the **Redistribution** tab.

Related Topics

- Redistributing Routes into BGP, page 15-182
- BGP Page—Setup Tab, page K-220

Field Reference

Table K-100 BGP Redistribution Tab

Element	Description
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
Protocol	The protocol that is being redistributed.
AS/Process ID	The AS number or process ID of the route being redistributed.
Metric	The value that determines the priority of the redistributed route.
Match	When redistributing an OSPF process, indicates the types of OSPF routes that are being redistributed.

Table K-100 BGP Redistribution Tab (Continued)

Static Type	When redistributing static routes, indicates the type of static route, IP or OSI.
Add button	Opens the BGP Redistribution Mapping Dialog Box, page K-224. From here you can define BGP redistribution mappings.
Edit button	Opens the BGP Redistribution Mapping Dialog Box, page K-224. From here you can edit the selected BGP redistribution mapping.
Delete button	Deletes the selected BGP redistribution mappings from the table.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** icon on the toolbar.

Tip To choose which columns to display in the table, right-click a column header, then select **Show Columns**. For more information about table display options, see Table Columns and Column Heading Features, page 3-26.

BGP Redistribution Mapping Dialog Box

Use the BGP Redistribution Mapping dialog box to add or edit the properties of a BGP redistribution mapping.

Navigation Path

Go to the BGP Page—Redistribution Tab, page K-223, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Redistributing Routes into BGP, page 15-182

Field Reference

Table K-101 BGP Redistribution Mapping Dialog Box

Element	Description
Protocol to Redistribute	The routing protocol that is being redistributed: • Static—Redistributes IP or OSI static routes. You can define a single mapping for each route. • EIGRP—Redistributes an EIGRP autonomous system. Enter the AS number in the displayed field. You can define a single mapping for each AS. • RIP—Redistributes RIP routes. You can define a single mapping for each route. • OSPF—Redistributes a different OSPF process. You can define a single mapping for each process. Select a process from the displayed list, then select one or more match criteria: – Internal—Routes that are internal to a specific AS. – External1—Routes that are external to the AS and imported into OSPF as a Type 1 external route. – External2—Routes that are external to the AS and imported into the selected process as a Type 2 external route. – NSAAExternal1—Not-So-Stubby Area (NSSA) routes that are external to the AS and imported into the selected process as Type 1 external routes. – NSAAExternal2—(NSSA) routes that are external to the AS and imported into the selected process as Type 2 external routes. • Connected—Redistributes routes that are established automatically by virtue of having enabled IP on an interface. These routes are redistributed as external to the AS.
Metric	A value representing the cost of the redistributed route. Valid values range from 0 to 4294967295.
OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

EIGRP Routing Policy Page

Enhanced Interior Gateway Routing Protocol (EIGRP) is a scalable interior gateway protocol that provides extremely quick convergence times with minimal network traffic.

You can configure EIGRP routing policies from the following tabs on the EIGRP Routing page:

- EIGRP Page—Setup Tab, page K-226
- EIGRP Page—Interfaces Tab, page K-229
- EIGRP Page—Redistribution Tab, page K-232

For more information, see EIGRP Routing on Cisco IOS Routers, page 15-184.

Navigation Path

- (Device view) Select **Platform > Routing > EIGRP** from the Policy selector.
- (Policy view) Select **Router Platform > Routing > EIGRP** from the Policy Type selector. Right-click **EIGRP** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- Chapter K, "Router Platform User Interface Reference"

EIGRP Page—Setup Tab

Use the EIGRP Setup tab to view, create, edit, and delete EIGRP routes.

Navigation Path

Go to the EIGRP Routing Policy Page, page K-226, then click the **Setup** tab.

Related Topics

- Defining EIGRP Routes, page 15-185
- EIGRP Page—Interfaces Tab, page K-229
- EIGRP Page—Redistribution Tab, page K-232

Field Reference

Table K-102 EIGRP Setup Tab

Element	Description
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
AS Number	The autonomous system number that identifies the autonomous system to other routers.
Networks	The names of the networks included in the route.
Passive Interfaces	The interfaces that neither send nor receive routing updates from their neighbors.
Auto-Summary	Indicates whether auto summarization is activated on the selected route.
Add button	Opens the EIGRP Setup Dialog Box, page K-227. From here you can create an EIGRP route.
Edit button	Opens the EIGRP Setup Dialog Box, page K-227. From here you can edit the selected EIGRP route.
Delete button	Deletes the selected EIGRP routes from the table.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** icon on the toolbar.

Tip To choose which columns to display in the table, right-click a column header, then select **Show Columns**. For more information about table display options, see Table Columns and Column Heading Features, page 3-26.

EIGRP Setup Dialog Box

Use the EIGRP Setup dialog box to add or edit EIGRP routes.

Navigation Path

Go to the EIGRP Page—Setup Tab, page K-226, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Defining EIGRP Routes, page 15-185
- Supported IP Address Formats, page 9-145
- Understanding Network/Host Objects, page 9-144

Field Reference

Table K-103 EIGRP Setup Dialog Box

Element	Description
AS Number	The autonomous system number for the EIGRP route. This number is used to identify the autonomous system to other routers. Valid values are from 1 to 65535.
Networks	The networks associated with the EIGRP route. Enter one or more network addresses or network/host objects, or click **Select** to display an Object Selectors, page F-593. If the network you want is not listed, click the **Create** button in the selector to display the Network/Host Dialog Box, page F-477. From here you can define a network/host object.
Passive Interfaces	The interfaces that do not send updates to their routing neighbors. Click **Edit** to display the Edit Interfaces Dialog Box—EIGRP Passive Interfaces, page K-229. From here you can define these interfaces. **Note** When you make an interface passive, EIGRP suppresses the exchange of hello packets between routers, resulting in the loss of their neighbor relationship. This not only stops routing updates from being advertised but also suppresses incoming routing updates.
Auto-Summary	When selected, enables the automatic summarization of subnet routes into network-level routes. Summarization reduces the size of routing tables, thereby reducing the complexity of the network. When deselected, automatic summarization is disabled.
OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

Edit Interfaces Dialog Box—EIGRP Passive Interfaces

When you configure an EIGRP routing policy on a Cisco IOS router, use the Edit Interfaces dialog box to specify which interfaces will not send updates to their routing neighbors.

Navigation Path

Go to the EIGRP Setup Dialog Box, page K-227, then click the **Edit** button in the Passive Interfaces field.

Related Topics

- EIGRP Page—Setup Tab, page K-226

Field Reference

Table K-104 Edit Interfaces Dialog Box—EIGRP Passive Interfaces

Element	Description
Interfaces	The interfaces that do not send updates to their routing neighbors. You can enter interfaces, interface roles, or both. For more information, see Specifying Interfaces During Policy Definition, page 9-135.
Select button	Opens an Object Selectors, page F-593 for selecting interfaces and interface roles. Using a selector eliminates the need to manually enter this information. If the interface role you want is not listed, click the **Create** button in the selector to display the Interface Role Dialog Box, page F-464. From here you can define an interface role object.
OK button	Saves your changes and closes the dialog box. Your selections are displayed in the Passive Interfaces field of the EIGRP Setup dialog box.

EIGRP Page—Interfaces Tab

Use the EIGRP Interfaces tab to create, edit, and delete interface properties for selected EIGRP autonomous systems. This includes modifying the default hello interval and disabling split horizon.

Note You can access the EIGRP Interfaces tab only after defining at least one EIGRP autonomous system in the Setup tab. See EIGRP Page—Setup Tab, page K-226.

Navigation Path

Go to the EIGRP Routing Policy Page, page K-226, then click the **Interfaces** tab.

Related Topics

- Defining EIGRP Interface Properties, page 15-187
- EIGRP Page—Setup Tab, page K-226
- EIGRP Page—Redistribution Tab, page K-232

Field Reference

Table K-105 EIGRP Interfaces Tab

Element	Description
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
AS Number	The EIGRP autonomous system number for which interface properties are defined.
Interfaces	The interfaces related to the selected EIGRP autonomous system that have specially defined values.
Split Horizon	Indicates whether the split horizon feature is enabled or disabled for the selected interface.
Hello Interval	The defined interval between hello packets sent to neighboring routers.
Add button	Opens the EIGRP Interface Dialog Box, page K-231. From here you can create an EIGRP interface definition.
Edit button	Opens the EIGRP Interface Dialog Box, page K-231. From here you can edit the selected EIGRP interface definition.
Delete button	Deletes the selected EIGRP interface definitions from the table.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** icon on the toolbar.

Tip To choose which columns to display in the table, right-click a column header, then select **Show Columns**. For more information about table display options, see Table Columns and Column Heading Features, page 3-26.

EIGRP Interface Dialog Box

Use the EIGRP Interface dialog box to add or edit interface definitions for a selected EIGRP autonomous system.

Navigation Path

Go to the EIGRP Page—Interfaces Tab, page K-229, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Defining EIGRP Interface Properties, page 15-187
- Basic Interface Settings on Cisco IOS Routers, page 15-20
- Understanding Interface Role Objects, page 9-132

Field Reference

Table K-106 EIGRP Interface Dialog Box

Element	Description
AS Number	Selects the EIGRP autonomous system number whose interface properties you want to modify. For more information about EIGRP autonomous systems, see EIGRP Setup Dialog Box, page K-227.
Interface	Specifies the EIGRP interface you wish to configure. Enter the name of an interface or interface role, or click **Select** to display an Object Selectors, page F-593. If the interface role you want is not listed, click the **Create** button in the selector to display the Interface Role Dialog Box, page F-464. From here you can create an interface role object.

Table K-106 EIGRP Interface Dialog Box (Continued)

Hello Interval	The default interval between hello packets sent by the router to its neighbors. Routers send hello packets to each other to dynamically learn of other routers on their directly attached networks. Valid values range from 1 to 65535 seconds. The default is 5 seconds.
Split Horizon	When selected, the split horizon feature is used to prevent routing loops. When deselected, split horizon is disabled. When split horizon is disabled, the router can advertise a route out of the same interface through which it learned the route. Disabling split horizon is often useful when dealing with nonbroadcast networks, such as Frame Relay and SMDS. **Note** Changing the split horizon setting on an interface resets all adjacencies with EIGRP neighbors that are reachable over that interface.
OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

EIGRP Page—Redistribution Tab

Use the EIGRP Redistribution tab to create, edit, and delete EIGRP redistribution mappings.

Navigation Path

Go to the EIGRP Routing Policy Page, page K-226, then click the **Redistribution** tab.

Related Topics

- Redistributing Routes into EIGRP, page 15-190
- EIGRP Page—Setup Tab, page K-226
- EIGRP Page—Interfaces Tab, page K-229

Field Reference

Table K-107 EIGRP Redistribution Tab

Element	Description
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
EIGRP AS Number	The area ID of the EIGRP route into which other routes are being redistributed.
Protocol	The protocol that is being redistributed.
AS/Process ID	The AS number or process ID of the route being redistributed.
Bandwidth	The minimum bandwidth of the path for the EIGRP route, as defined for the route metric.
Delay	The mean latency of the path, as defined for the route metric.
Reliability	A value representing the estimated reliability of the path, as defined for the route metric.
Effective Bandwidth	A value representing the effective load on the link, as defined for the route metric.
MTU	The minimum MTU of the path, as defined for the route metric.
Match	When redistributing an OSPF process, indicates the types of OSPF routes that are being redistributed.
Add button	Opens the EIGRP Redistribution Mapping Dialog Box, page K-234. From here you can define EIGRP redistribution mappings.
Edit button	Opens the EIGRP Redistribution Mapping Dialog Box, page K-234. From here you can edit the selected EIGRP redistribution mapping.
Delete button	Deletes the selected EIGRP redistribution mappings from the table.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** icon on the toolbar.

Tip To choose which columns to display in the table, right-click a column header, then select **Show Columns**. For more information about table display options, see Table Columns and Column Heading Features, page 3-26.

EIGRP Redistribution Mapping Dialog Box

Use the EIGRP Redistribution Mapping dialog box to add or edit the properties of an EIGRP redistribution mapping.

Navigation Path

Go to the EIGRP Page—Redistribution Tab, page K-232, then click the **Add** or **Edit** button beneath the table.

Note You must create at least one EIGRP AS before you can access the EIGRP Redistribution dialog box. See EIGRP Page—Setup Tab, page K-226.

Related Topics

- Redistributing Routes into EIGRP, page 15-190

Field Reference

Table K-108 EIGRP Redistribution Mapping Dialog Box

Element	Description
EIGRP AS Numbers	The EIGRP AS into which other routes are being redistributed. You must select an ID number from the list of EIGRP autonomous systems defined in the EIGRP Page—Setup Tab, page K-226.
Protocol to Redistribute	The routing protocol that is being redistributed: • Static—Redistributes static routes. You can define a single mapping for each route. • EIGRP—Redistributes an EIGRP autonomous system. Enter the AS number in the displayed field. You can define a single mapping for each AS. • BGP—Redistributes a BGP autonomous system. You can define a single BGP mapping on each device. If you configured a BGP AS in the BGP Setup tab, the AS number is displayed. Otherwise, a message is displayed indicating that no BGP AS was defined. See BGP Page—Redistribution Tab, page K-223.

Table K-108 EIGRP Redistribution Mapping Dialog Box (Continued)

Protocol to Redistribute (continued)	• OSPF—Redistributes a different OSPF process. You can define a single mapping for each process. Select a process from the displayed list, then select one or more match criteria: – Internal—Routes that are internal to a specific AS. – External1—Routes that are external to the AS and imported into OSPF as a Type 1 external route. – External2—Routes that are external to the AS and imported into the selected process as a Type 2 external route. – NSAAExternal1—Not-So-Stubby Area (NSSA) routes that are external to the AS and imported into the selected process as Type 1 external routes. – NSAAExternal2—(NSSA) routes that are external to the AS and imported into the selected process as Type 2 external routes. • RIP—Redistributes RIP routes. • Connected—Redistributes routes that are established automatically by virtue of having enabled IP on an interface. These routes are redistributed as external to the AS.
Metrics	The default metric (cost) of the redistributed route. Metric parameters include: • Bandwidth—The minimum bandwidth of the path in kilobits per second. Valid values range from 1 to 4294967295. • Delay—The mean latency of the path in units of 10 microseconds. Valid values range from 0 to 4294967295. • Reliability—A value expressing the estimated reliability of the link. Valid values range from 0 to 255, where 255 represents 100% reliability. • Effective Bandwidth—A value expressing the effective load on the link. Valid values range from 1 to 255, where 255 represents 100% utilization. • MTU of Path—The maximum transmission unit of the path. Valid values range from 1 to 65535 bytes.

Table K-108 EIGRP Redistribution Mapping Dialog Box (Continued)

OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

OSPF Interface Policy Page

Use the OSPF Interface page to view, create, edit, and delete interface-specific OSPF settings. For more information, see Defining OSPF Interface Settings, page 15-200.

Navigation Path

- (Device view) Select **Platform > Routing > OSPF Interface** from the Policy selector.
- (Policy view) Select **Router Platform > Routing > OSPF Interface** from the Policy Type selector. Right-click **OSPF Interface** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- OSPF Process Policy Page, page K-243
- Chapter K, "Router Platform User Interface Reference"

Field Reference

Table K-109 OSPF Interface Page

Element	Description
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
Interfaces	The name of an interface (as defined by an interface role) on which OSPF is enabled.
Authentication	The type of OSPF neighbor authentication enabled for the selected interface.

Table K-109 OSPF Interface Page (Continued)

Key ID	The identification number of the authentication key used for MD5 authentication.
Cost	The cost of sending packets over the selected interface, if this value is different from the cost as normally calculated.
Priority	The priority of the selected interface.
MTU Ignore	Indicates whether Maximum Transmission Rate (MTU) detection is disabled on the selected interface.
Database Filter	Indicates whether link-state advertisement (LSA) flooding is disabled on the selected interface.
Hello Interval	The interval between hello packets (in seconds) sent over this interface.
Transmit Delay	The amount of time OSPF waits (in seconds) before flooding an LSA over the link.
Retransmit Interval	The interval between LSA retransmissions (in seconds) over the selected interface.
Dead Interval	The interval OSPF waits (in seconds) before declaring a neighboring router dead because of an absence of hello packets.
Network Type	The network type configured for the selected interface, if it differs from the default medium.
Add button	Opens the OSPF Interface Dialog Box, page K-238. From here you can define the properties of an OSPF interface.
Edit button	Opens the OSPF Interface Dialog Box, page K-238. From here you can edit the properties of the selected OSPF interface.
Delete button	Deletes the selected OSPF interface definitions from the table.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** icon on the toolbar.

Tip To choose which columns to display in the table, right-click a column header, then select **Show Columns**. For more information about table display options, see Table Columns and Column Heading Features, page 3-26.

OSPF Interface Dialog Box

Use the OSPF Interface dialog box to add or edit the properties of OSPF interfaces.

Navigation Path

Go to the OSPF Interface Policy Page, page K-236, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Defining OSPF Interface Settings, page 15-200
- OSPF Routing on Cisco IOS Routers, page 15-192
- Basic Interface Settings on Cisco IOS Routers, page 15-20
- Understanding Interface Role Objects, page 9-132

Field Reference

Table K-110 OSPF Interface Dialog Box

Element	Description
Interface	The OSPF interface to configure. Enter the name of an interface or interface role, or click **Select** to display an Object Selectors, page F-593. If the interface role you want is not listed, click the **Create** button in the selector to display the Interface Role Dialog Box, page F-464. From here you can define an interface role object.

Table K-110 OSPF Interface Dialog Box (Continued)

Authentication	Type—The authentication type used by the selected interface: • MD5—Uses the MD5 hash algorithm for authentication. This is the default. • Clear Text—Uses a clear text password for authentication. • None—Uses no authentication. **Note** The authentication type used on an interface must match the authentication type defined for the area. **Note** Use plain text authentication only when security is not an issue, for example, to ensure that misconfigured hosts do not participate in routing. • Key ID—Available only when MD5 is selected as the authentication type. The identification number of the authentication key. This number must be shared with all other devices sending updates to, and receiving updates from, the selected device. Valid values range from 1 to 255. • Key—The shared key used for authentication (MD5 or clear text). This key must be shared with all other devices sending updates to, and receiving updates from, the selected device. Enter this key again in the Confirm field. When using clear text, the key can include any continuous string of characters that can be entered from the keyboard (up to 8 bytes). When using MD5, the key can include alphanumeric characters only (up to 16 bytes).
Cost	The cost of sending packets over this interface. A value entered here overrides the default calculated cost (10 8 /bandwidth in bits per second). Valid values range from 1 to 65535.

Table K-110 OSPF Interface Dialog Box (Continued)

Priority	The default priority of the interface. The priority is used to determine which routers become the designated router (DR) and backup designated router (BDR) for that segment. The higher the number, the higher the priority. The default priority is 1. Valid values range from 0 to 255. **Note** To exclude the interface from election as DR or BDR, assign a priority of 0. Configure router priority only for interfaces to multiaccess networks, not point-to-point networks.
MTU Ignore	When selected, ignores MTU mismatches between neighboring routers. When deselected, MTU mismatch detection is enabled. **Note** Typically, this option is not used, because it can cause routers to become stuck in exstart/exchange state, which prevents OSPF adjacency from being established.
Database Filter	When selected, blocks link-state advertisement (LSA) flooding to the selected interface. When deselected, LSA flooding is permitted. **Note** We recommend that you enable this option on fully-meshed networks. This option is not available for point-to-multipoint networks.
Hello Interval	The default interval (in seconds) between hello packets sent over the selected interface. These packets are used by neighboring routers to confirm the router sending the packets is still operating. Valid values range 1 to 65535 seconds. **Note** The hello interval must be the same for all routers and access servers in the network.
Transmit Delay	The amount of time OSPF waits (in seconds) before flooding an LSA over the link. The default is 1 second. Valid values range from 1 to 65535 seconds. **Note** When you configure slow links or on-demand links that queue traffic before sending it in bursts, we recommend that you take these link delays into account when defining this value.

Table K-110 OSPF Interface Dialog Box (Continued)

Retransmit Interval	The interval between LSA retransmissions (in seconds) over the selected interface. The default is 5 seconds. Valid values range from 1 to 65535 seconds. **Note** We recommend that you increase this value for serial lines and virtual links.
Dead Interval	The interval (in seconds) after which an interface declares its neighbor dead if no hello packets are received. Valid values range from 1 to 655335 seconds. **Note** The value of the dead interval is typically the hello interval value multiplied by 4. The dead interval must be the same for all routers and access servers in the network.

Table K-110 OSPF Interface Dialog Box (Continued)

Configure Network Type	When selected, enables you to select a network type that differs from the default medium used by the interface. When deselected, the network type is equivalent to the default medium used by the interface. For nonbroadcast multiaccess (NBMA) networks (such as ATM and Frame Relay), options are: • Broadcast—Treats the NBMA network as a broadcast network, which eliminates the need to configure neighbors. Use this option when there are virtual circuits from every router to every router (fully meshed network). • Point-to-Multipoint—Treats the nonbroadcast network as a series of point-to-point links. This option is easier to configure, less costly, and more reliable than NBMA or point-to-point networks. • Point-to-Multipoint Non-Broadcast—Statically maintains the known neighbors of the network. Selecting this option helps avoid the problem of losing neighbors that were learned dynamically through the reception of hello packets. **Note** Another option for NBMA networks is to configure neighbors manually using FlexConfigs. See Understanding FlexConfig Objects, page 9-52. For broadcast networks (such as Ethernet, Token Ring, and FDDI), you can select: • Non-Broadcast—Treats the broadcast network as a nonbroadcast network. • Point-to-Point—Treats the broadcast network as a point-to-point network. You can use this option, for example, to configure a broadcast network (such as Ethernet) as a nonbroadcast multiaccess (NBMA) network if not all routers in the network support multicast addressing.
OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

OSPF Process Policy Page

OSPF is an interior gateway routing protocol that uses link states instead of distance vectors for path selection. OSPF propagates link-state advertisements (LSAs) instead of routing table updates, which enables OSPF networks to converge quickly.

You can configure OSPF process policies from the following tabs on the OSPF Process page:

- OSPF Process Page—Setup Tab, page K-243
- OSPF Process Page—Area Tab, page K-247
- OSPF Process Page—Redistribution Tab, page K-249

For more information, see OSPF Routing on Cisco IOS Routers, page 15-192.

Note For more information about OSPF interface policies, see OSPF Interface Policy Page, page K-236.

Navigation Path

- (Device view) Select **Platform > Routing > OSPF Process** from the Policy selector.
- (Policy view) Select **Router Platform > Routing > OSPF Process** from the Policy Type selector. Right-click **OSPF Process** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- Chapter K, "Router Platform User Interface Reference"

OSPF Process Page—Setup Tab

Use the OSPF Process Setup tab to create, edit, and delete OSPF processes. This includes selecting those interfaces that will remain passive, which means that they will not send routing updates to their neighbors. You can create as many processes for each router as required.

Navigation Path

Go to the OSPF Process Policy Page, page K-243, then click the **Setup** tab.

Related Topics

- Defining OSPF Process Settings, page 15-193
- OSPF Process Page—Area Tab, page K-247
- OSPF Process Page—Redistribution Tab, page K-249
- OSPF Interface Policy Page, page K-236

Field Reference

Table K-111 OSPF Process Setup Tab

Element	Description
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
Process ID	The process ID that identifies the OSPF routing process to other routers.
Passive Interfaces	The interfaces that do not send out routing updates.
Add button	Opens the OSPF Setup Dialog Box, page K-245. From here you can define an OSPF process.
Edit button	Opens the OSPF Setup Dialog Box, page K-245. From here you can edit the selected OSPF process.
Delete button	Deletes the selected OSPF processes from the table.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** icon on the toolbar.

Tip To choose which columns to display in the table, right-click a column header, then select **Show Columns**. For more information about table display options, see Table Columns and Column Heading Features, page 3-26.

OSPF Setup Dialog Box

Use the OSPF Setup dialog box to add or edit an OSPF process.

Navigation Path

Go to the OSPF Process Page—Setup Tab, page K-243, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Defining OSPF Process Settings, page 15-193

Field Reference

Table K-112 OSPF Setup Dialog Box

Element	Description
Process ID	The process ID number for the OSPF process. This number identifies the OSPF process to other routers. It does not need to match the process ID on other devices. Valid values are from 1 to 65535.
Passive Interfaces	The interfaces that do not send updates to their routing neighbors. Click **Edit** to display the Edit Interfaces Dialog Box—OSPF Passive Interfaces, page K-246. From here you can define these interfaces. **Note** When you make an interface passive, OSPF suppresses the sending of hello packets to neighboring routers. The interface will continue to receive routing updates, however.
OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

Edit Interfaces Dialog Box—OSPF Passive Interfaces

When you configure an OSPF routing policy on a Cisco IOS router, use the Edit Interfaces dialog box to specify which interfaces will not send updates to their routing neighbors.

Navigation Path

Go to the OSPF Setup Dialog Box, page K-245, then click the **Edit** button in the Passive Interfaces field.

Related Topics

- OSPF Process Page—Setup Tab, page K-243
- Defining OSPF Process Settings, page 15-193

Field Reference

Table K-113 Edit Interfaces Dialog Box—OSPF Passive Interfaces

Element	Description
Interfaces	The interfaces that do not send updates to their routing neighbors. You can enter interfaces, interface roles, or both. For more information, see Specifying Interfaces During Policy Definition, page 9-135.
Select button	Opens an Object Selectors, page F-593 for selecting interfaces and interface roles. Using the selector eliminates the need to manually enter this information. If the interface role you want is not listed, click the **Create** button in the selector to display the Interface Role Dialog Box, page F-464. From here you can define an interface role object.
OK button	Saves your changes and closes the dialog box. Your selections are displayed in the Passive Interfaces field of the OSPF Setup dialog box.

OSPF Process Page—Area Tab

Use the OSPF Area tab to create, edit, and delete the areas and networks contained in each OSPF process. This includes selecting the type of authentication used by each area.

Navigation Path

Go to the OSPF Process Policy Page, page K-243, then click the **Area** tab.

Related Topics

- Defining OSPF Area Settings, page 15-194
- OSPF Process Page—Setup Tab, page K-243
- OSPF Process Page—Redistribution Tab, page K-249
- OSPF Interface Policy Page, page K-236

Field Reference

Table K-114 OSPF Process Area Tab

Element	Description
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
Area ID	The ID number of the area associated with the process.
Process ID	The process ID that identifies the OSPF routing process to other routers.
Networks	The networks included in the area.
Authentication	The authentication type used by the area—MD5, clear text, or none.
Add button	Open the OSPF Area Dialog Box, page K-248. From here you can define an OSPF area.
Edit button	Opens the OSPF Area Dialog Box, page K-248. From here you can edit the selected OSPF area.
Delete button	Deletes the selected OSPF areas from the table.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** icon on the toolbar.

Tip To choose which columns to display in the table, right-click a column header, then select **Show Columns**. For more information about table display options, see Table Columns and Column Heading Features, page 3-26.

OSPF Area Dialog Box

Use the OSPF Area dialog box to add or edit the properties of an OSPF area. You should define at least one area for each OSPF process (see OSPF Setup Dialog Box, page K-245), but deployment will not fail if you do not.

Navigation Path

Go to the OSPF Process Page—Area Tab, page K-247, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Defining OSPF Area Settings, page 15-194
- Supported IP Address Formats, page 9-145
- Understanding Network/Host Objects, page 9-144

Field Reference

Table K-115 OSPF Area Dialog Box

Element	Description
Process ID	The process ID associated with the OSPF area. The list contains the OSPF processes defined in the OSPF Process Page—Setup Tab, page K-243.
Area ID	The area ID number associated with the selected process. Valid values range from 0 to 4294967295.
Networks	The networks to add to the OSPF area. Enter one or more network addresses or network/host objects, or click **Select** to display an Object Selectors, page F-593. If the network you want is not listed, click the **Create** button in the selector to display the Network/Host Dialog Box, page F-477. From here you can define a network/host object.

Table K-115 OSPF Area Dialog Box (Continued)

Authentication	The type of authentication used for the area: • MD5—(Recommended) Uses the MD5 hash algorithm for authentication. • Clear Text—Uses clear text for authentication. • None—No authentication is used. **Note** The authentication type must be the same for all routers and access servers in an area.
OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

OSPF Process Page—Redistribution Tab

Use the OSPF Process Redistribution tab to create, edit, and delete OSPF redistribution mappings. This includes defining the maximum number of routes that can be redistributed into OSPF from other protocols or other OSPF processes.

Navigation Path

Go to the OSPF Process Policy Page, page K-243, then click the **Redistribution** tab.

Related Topics

- Redistributing Routes into OSPF, page 15-196
- OSPF Process Page—Setup Tab, page K-243
- OSPF Process Page—Area Tab, page K-247
- OSPF Interface Policy Page, page K-236

Field Reference

Table K-116 OSPF Process Redistribution Tab

Element	Description
OSPF Redistribution Mapping Table	
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
OSPF Process ID	The ID of the OSPF routing domain into which other routes are being redistributed.
Protocol	The protocol that is being redistributed.
AS/Process ID	The AS number or process ID of the route that is being redistributed.
Match	When redistributing an OSPF process, indicates the types of OSPF routes that are being redistributed.
Metric	The value that determines the priority of the redistributed route.
Metric Type	The external link type associated with the default route advertised into the OSPF routing domain.
Subnets	Indicates whether routes that are subnetted are also being redistributed.
Add button	Opens the OSPF Redistribution Mapping Dialog Box, page K-251. From here you can define OSPF redistribution mappings.
Edit button	Opens the OSPF Redistribution Mapping Dialog Box, page K-251. From here you can edit the selected OSPF redistribution mapping.
Delete button	Deletes the selected redistribution mappings from the table.
OSPF Max Prefix Mapping Table	
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
OSPF Process ID	The ID of the OSPF routing domain for which a maximum prefix values has been defined.
Max Prefix	The maximum number of prefixes (routes) that may be redistributed to the selected OSPF process.
Threshold	The percentage of the maximum prefix value that acts as a threshold for triggering a warning message.
Action	Indicates whether redistribution to this OSPF process will stop when the maximum is reached, or whether only a warning is displayed.

Table K-116 OSPF Process Redistribution Tab (Continued)

Add button	Opens the OSPF Max Prefix Mapping Dialog Box, page K-254. From here you can define maximum prefix values for OSPF processes.
Edit button	Opens the OSPF Max Prefix Mapping Dialog Box, page K-254. From here you can edit the maximum prefix value defined for the selected OSPF process.
Delete button	Deletes the selected max prefix mappings from the table.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** icon on the toolbar.

Tip To choose which columns to display in the table, right-click a column header, then select **Show Columns**. For more information about table display options, see Table Columns and Column Heading Features, page 3-26.

OSPF Redistribution Mapping Dialog Box

Use the OSPF Redistribution Mapping dialog box to add or edit the properties of an OSPF redistribution mapping.

Navigation Path

Go to the OSPF Process Page—Redistribution Tab, page K-249, then click the **Add** or **Edit** button beneath the Redistribution Mapping table.

Note You must create at least one OSPF process before you can access the OSPF Redistribution dialog box. See OSPF Process Page—Setup Tab, page K-243.

Related Topics

- OSPF Max Prefix Mapping Dialog Box, page K-254
- Redistributing Routes into OSPF, page 15-196

Field Reference

Table K-117 OSPF Redistribution Mapping Dialog Box

Element	Description
Process ID	The OSPF process into which other routes are being redistributed. You must select a process ID number from the list of OSPF processes defined in the OSPF Process Page—Setup Tab, page K-243.
Protocol to Redistribute	The routing protocol that is being redistributed: • Static—Redistributes static routes. You can define a single mapping for each route. • EIGRP—Redistributes an EIGRP autonomous system. Enter the AS number in the displayed field. You can define a single mapping for each AS. • BGP—Redistributes a BGP autonomous system. You can define a single BGP mapping on each device. If you configured a BGP AS in the BGP Setup tab, the AS number is displayed. Otherwise, a message is displayed indicating that no BGP AS was defined. See BGP Page—Redistribution Tab, page K-223.

Table K-117 OSPF Redistribution Mapping Dialog Box (Continued)

Protocol to Redistribute (continued)	• OSPF—Redistributes a different OSPF process. You can define a single mapping for each process. Select a process from the displayed list, then select one or more match criteria: – Internal—Routes that are internal to a specific AS. – External1—Routes that are external to the AS and imported into OSPF as a Type 1 external route. – External2—Routes that are external to the AS and imported into the selected process as a Type 2 external route. – NSAAExternal1—Not-So-Stubby Area (NSSA) routes that are external to the AS and imported into the selected process as Type 1 external routes. – NSAAExternal2—(NSSA) routes that are external to the AS and imported into the selected process as Type 2 external routes. • RIP—Redistributes RIP routes. You can define a single mapping for each route. • Connected—Redistributes routes that are established automatically by virtue of having enabled IP on an interface. These routes are redistributed as external to the AS.
Default Metric	A value representing the cost of the redistributed route.
Metric Type	The external link type that is associated with the route being redistributed into the OSPF routing domain: • 1—Type 1 external route. The metric is the sum of the external redistributed cost and the internal OSPF cost. • 2—Type 2 external route. The metric is equal to the external redistributed cost, as defined in the Metric field. This is the default.
Limit to Subnets	When selected, only subnetted routes are redistributed. When deselected, subnetted routes are not redistributed.
OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

OSPF Max Prefix Mapping Dialog Box

Use the OSPF Max Prefix Mapping dialog box to add or edit the maximum number of routes that can be redistributed into an OSPF process.

Navigation Path

Go to the OSPF Process Page—Redistribution Tab, page K-249, then click the **Add** or **Edit** button beneath the Prefix Mapping table.

Related Topics

- OSPF Redistribution Mapping Dialog Box, page K-251
- Redistributing Routes into OSPF, page 15-196

Field Reference

Table K-118 OSPF Max Prefix Mapping Dialog Box

Element	Description
Process ID	The OSPF process into which other routes are being redistributed. The list contains the OSPF processes defined in the OSPF Process Page—Setup Tab, page K-243.
Max Prefix	The maximum number of prefixes (routes) that can be redistributed into the selected OSPF process. Limiting the number of redistributed routes helps prevent the router from being flooded by an excessive number of routes.
Threshold	The percentage of the maximum prefix value that acts as a threshold for triggering warning messages. The default is 75%. **Note** This warning is triggered whether or not the Warning-Only check box is selected.
When maximum routes reached	The action to take when the maximum number of redistributed routes is reached: • Enforce Maximum Route—Prevents additional routes from being redistributed when the defined maximum prefix value is reached. This is the default. • Warning Only—Issues a warning when the maximum number of routes is reached, but does not prevent additional routes from being redistributed.

Table K-118 OSPF Max Prefix Mapping Dialog Box (Continued)

OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

RIP Routing Policy Page

RIP is a distance-vector routing protocol that uses hop count as the metric for path selection. Security Manager supports RIP version 2 only, which includes support for neighbor authentication when routing updates are exchanged.

You can configure RIP routing policies from the following tabs on the RIP Routing page:

- RIP Page—Setup Tab, page K-255
- RIP Page—Authentication Tab, page K-257
- RIP Page—Redistribution Tab, page K-260

For more information, see RIP Routing on Cisco IOS Routers, page 15-208.

Navigation Path

- (Device view) Select **Platform > Routing > RIP** from the Policy selector.
- (Policy view) Select **Router Platform > Routing > RIP** from the Policy Type selector. Right-click **RIP** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- Chapter K, "Router Platform User Interface Reference"

RIP Page—Setup Tab

Use the RIP Setup tab to create, edit, and delete RIP routes.

Navigation Path

Go to the RIP Routing Policy Page, page K-255, then click the **Setup** tab.

Related Topics

- Defining RIP Setup Parameters, page 15-210
- RIP Page—Authentication Tab, page K-257
- RIP Page—Redistribution Tab, page K-260
- Supported IP Address Formats, page 9-145
- Understanding Network/Host Objects, page 9-144

Field Reference

Table K-119 RIP Setup Tab

Element	Description
Networks	The directly connected networks associated with the RIP route. Enter one or more network addresses or network/host objects, or click **Select** to display an Object Selectors, page F-593. If the network you want is not listed, click the **Create** button in the selector to display the Network/Host Dialog Box, page F-477. From here, you can define a network/host object.
Passive Interfaces	The interfaces that do not send updates to their routing neighbors. Click **Edit** to display the Edit Interfaces Dialog Box—RIP Passive Interfaces, page K-257. From here you can define these interfaces.
Auto-Summary	When selected, enables the automatic summarization of subnet routes into network-level routes. Summarization reduces the size of routing tables, thereby reducing the complexity of the network. This feature is enabled by default. When deselected, automatic summarization is disabled. **Note** Disable automatic summarization when performing routing between disconnected subnets. When this feature is disabled, subnets are advertised.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.

Edit Interfaces Dialog Box—RIP Passive Interfaces

When you configure a RIP routing policy on a Cisco IOS router, use the Edit Interfaces dialog box to specify which interfaces will not send updates to their routing neighbors.

Navigation Path

Go to the RIP Page—Setup Tab, page K-255, then click the **Edit** button in the Passive Interfaces field.

Related Topics

- Defining RIP Setup Parameters, page 15-210

Field Reference

Table K-120 Edit Interfaces Dialog Box—RIP Passive Interfaces

Element	Description
Interfaces	The interfaces that do not send updates to their routing neighbors. You can enter interfaces, interface roles, or both. For more information, see Specifying Interfaces During Policy Definition, page 9-135.
Select button	Opens an Object Selectors, page F-593 for selecting interfaces and interface roles. Using the selector eliminates the need to manually enter this information. If the interface role you want is not listed, click the **Create** button in the selector to display the Interface Role Dialog Box, page F-464. From here you can define an interface role object.
OK button	Saves your changes and closes the dialog box. Your selections are displayed in the Passive Interfaces field of the RIP Setup tab.

RIP Page—Authentication Tab

Use the RIP Authentication tab to view, create, edit, and delete the neighbor authentication settings of RIP interfaces.

Navigation Path

Go to the RIP Routing Policy Page, page K-255, then click the **Authentication** tab.

Related Topics

- Defining RIP Interface Authentication Settings, page 15-211
- RIP Page—Setup Tab, page K-255
- RIP Page—Redistribution Tab, page K-260
- RIP Routing Policy Page, page K-255

Field Reference

Table K-121 RIP Authentication Tab

Element	Description
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
Interfaces	The name of an interface (as defined by an interface role) on which RIP is enabled.
Authentication	The type of RIP neighbor authentication that is enabled for the selected interface role—clear text or MD5.
Key ID	The identification number of the authentication key used for MD5 authentication.
Add button	Opens the RIP Authentication Dialog Box, page K-259. From here you can define authentication for an additional RIP interface.
Edit button	Opens the RIP Authentication Dialog Box, page K-259. From here you can edit the authentication properties of the selected RIP interface.
Delete button	Deletes the selected authentication definitions from the table.

Tip To choose which columns to display in the table, right-click a column header, then select **Show Columns**. For more information about table display options, see Table Columns and Column Heading Features, page 3-26.

RIP Authentication Dialog Box

Use the RIP Authentication dialog box to add or edit the neighbor authentication properties of RIP interfaces.

Navigation Path

Go to the RIP Page—Authentication Tab, page K-257, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Defining RIP Interface Authentication Settings, page 15-211

Field Reference

Table K-122 RIP Authentication Dialog Box

Element	Description
Interface	The interface for which you want to define authentication properties. Enter the name of an interface or interface role, or click **Select** to display an Object Selectors, page F-593. If the interface role you want is not listed, click the **Create** button in the selector to display the Interface Role Dialog Box, page F-464. From here you can define an interface role object. **Note** You cannot specify two different authentication configurations for the same interface.
Authentication	The type of authentication to apply to the interface: • MD5—(Recommended) Uses the MD5 hash algorithm for authentication. • Clear Text—Uses clear text for authentication. **Note** Use plain text authentication only when security is not an issue, for example, to ensure that misconfigured hosts do not participate in routing.
Key ID	Available only when MD5 is selected as the authentication type. The identification number of the authentication key. This number must be shared with all other devices sending updates to, and receiving updates from, the selected device. Valid values range from 0 to 2147483647.

Table K-122 RIP Authentication Dialog Box (Continued)

Key	The shared key used for authentication (MD5 or clear text). This key must be shared with all other devices sending updates to, and receiving updates from, the selected device. The key can contain up to 80 alphanumeric characters; the first character cannot be a number. Spaces are allowed. Enter the key again in the Confirm field.
OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

RIP Page—Redistribution Tab

Use the RIP Redistribution tab to view, create, edit, and delete redistribution settings when performing redistribution into an RIP routing domain.

Note You must define RIP setup parameters before you can access the RIP Redistribution tab. See RIP Page—Setup Tab, page K-255.

Navigation Path

Go to the RIP Routing Policy Page, page K-255, then click the **Redistribution** tab.

Related Topics

- Redistributing Routes into RIP, page 15-213
- RIP Page—Authentication Tab, page K-257

Field Reference

Table K-123 RIP Redistribution Tab

Element	Description
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
Protocol	The protocol that is being redistributed.
AS/Process ID	The autonomous system (AS) number or process ID of the route being redistributed.
Metric	The value that determines the priority of the redistributed route.
Match	When redistributing an OSPF process, indicates which types of OSPF routes are being redistributed.
Add button	Opens the RIP Redistribution Mapping Dialog Box, page K-261. From here you can define a RIP redistribution mapping.
Edit button	Opens the RIP Redistribution Mapping Dialog Box, page K-261. From here you can edit the selected RIP redistribution mapping.
Delete button	Deletes the selected redistribution mappings from the table.

RIP Redistribution Mapping Dialog Box

Use the RIP Redistribution Mapping dialog box to add or edit the properties of an RIP redistribution mapping.

Navigation Path

Go to the RIP Page—Redistribution Tab, page K-260, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Redistributing Routes into RIP, page 15-213

Field Reference

Table K-124 RIP Redistribution Mapping Dialog Box

Element	Description
Protocol to Redistribute	The routing protocol that is being redistributed: • Static—Redistributes static routes. You can define a single mapping for each route. • EIGRP—Redistributes an EIGRP autonomous system. Enter the AS number in the displayed field. You can define a single mapping for each AS. • BGP—Redistributes a BGP autonomous system. You can define a single BGP mapping on each device. If you configured a BGP AS in the BGP Setup tab, the AS number is displayed. Otherwise, a message is displayed indicating that no BGP AS was defined. See BGP Page—Redistribution Tab, page K-223.
Protocol to Redistribute (continued)	• OSPF—Redistributes a different OSPF process. You can define a single mapping for each process. Select a process from the displayed list, then select one or more match criteria: – Internal—Routes that are internal to a specific AS. – External1—Routes that are external to the AS and imported into OSPF as a Type 1 external route. – External2—Routes that are external to the AS and imported into the selected process as a Type 2 external route. – NSAAExternal1—Not-So-Stubby Area (NSSA) routes that are external to the AS and imported into the selected process as Type 1 external routes. – NSAAExternal2—(NSSA) routes that are external to the AS and imported into the selected process as Type 2 external routes. • Connected—Redistributes routes that are established automatically by virtue of having enabled IP on an interface. These routes are redistributed as external to the AS.
Default Metric	Establishes a default value for the redistributed route. Valid values range from 0 to 16.

Table K-124 RIP Redistribution Mapping Dialog Box (Continued)

Transparent Metric	When selected, maintains the original metric of the route being redistributed. When deselected, the value specified in the Metric field is used.
OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.

Static Routing Policy Page

Use the Static Routing page to create, edit, and delete static routes. For more information, see Defining Static Routes, page 15-215.

Navigation Path

- (Device view) Select **Platform > Routing > Static Routing** from the Policy selector.
- (Policy view) Select **Router Platform > Routing > Static Routing** from the Policy Type selector. Right-click **Static Routing** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- Static Routing on Cisco IOS Routers, page 15-215
- Chapter K, “Router Platform User Interface Reference”

Field Reference

Table K-125 Static Routing Page

Element	Description
Filter	Enables you to filter the information displayed in the table. For more information, see Filtering Tables, page 3-24.
Prefix	The destination IP address of the static route.
Prefix Mask	The net mask of the selected IP address.

Table K-125 Static Routing Page (Continued)

Default Route	Indicates whether the static route is the default route for unknown packets being forwarded by this router.
Interface or IP Address	The IP address or the interface name associated with the gateway router that is the next hop address for this router.
Distance	The number of hops from the gateway IP to the destination. The metric determines the priority of this route. The fewer the hops, the higher the priority assigned to the route, based on lower costs. When two routing entries specify the same network, the entry with the lower metric (that is, the higher priority) is selected.
Permanent Route	Indicates whether the static route is defined as a permanent route, which means that it will not be removed even if the interface is shut down or if the router is unable to communicate with the next router.
Add button	Opens the Static Routing Dialog Box, page K-264. From here you can create a static route.
Edit button	Opens the Static Routing Dialog Box, page K-264. From here you can edit the selected static route.
Delete button	Deletes the selected static routes from the table.
Save button	Saves your changes to the Security Manager server but keeps them private. **Note** To publish your changes, click the **Submit** icon on the toolbar.

Tip To choose which columns to display in the table, right-click a column header, then select **Show Columns**. For more information about table display options, see Table Columns and Column Heading Features, page 3-26.

Static Routing Dialog Box

Use the Static Routing dialog box to add or edit static routes.

Navigation Path

Go to the Static Routing Policy Page, page K-263, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Defining Static Routes, page 15-215
- Static Routing on Cisco IOS Routers, page 15-215

Field Reference

Table K-126 Static Routing Dialog Box

Element	Description
Destination Network	Address information for the destination network defined by this static route. • Use as Default Route—When selected, makes this the default route on this router. A default route is used when the route from a source to a destination is unknown or when it is not feasible for the router to maintain many routes in its routing table. All unknown outbound packets are forwarded over the default route. When deselected, this static route is not the default route. • Prefix—The IP address of the destination network. Enter an IP address or the name of a network/host object, or click **Select** to display an Object Selectors, page F-593. The prefix must be a class A, B, or C network or host IP. A host IP can begin with 0 unless it contains a discontiguous mask. All subnet addresses are valid. If the network you want is not listed, click the **Create** button in the selector to display the Network/Host Dialog Box, page F-477. From here you can define a network/host object.

Table K-126 Static Routing Dialog Box (Continued)

Forwarding (Next Hop)	The method of forwarding data to the destination network: • Forwarding Interface—The router interface that forwards packets to the remote network. Enter the name of an interface or interface role, or click **Select** to display an Object Selectors, page F-593. If the interface role you want is not listed, click the **Create** button in the selector to display the Interface Role Dialog Box, page F-464. From here, you can define an interface role object. • Forwarding IP—The IP address of the next hop router that receives and forwards packets to the remote network. Enter an IP address or the name of a network/host object, or click **Select** to display an Object Selectors, page F-593. If the network you want is not listed, click the **Create** button in the selector to display the Network/Host Dialog Box, page F-477. From here you can define a network/host object.
Distance Metric	The number of hops to the destination network (gateway IP). The default is 1 if no value is specified. The range is from 1 to 255. This metric (also known as *administrative distance*) is a measurement of route expense based on the number of hops to the network on which a specified host resides. This hop count includes all the networks a packet must traverse, including the destination network. Therefore, all directly connected networks have a metric of 1. Because the metric is based on expense, it is used to identify the priority of the static route. If two routing entries specify the same network, the route with the lower metric value (that is, the lower cost) is given a higher priority and is selected. **Note** Under certain circumstances, it is useful to assign a static route a lower priority (larger distance metric) than a dynamic route. This enables the static route to act as a backup, "floating," route when the dynamic route is unavailable.
Permanent route	When selected, prevents this static route entry from being deleted, even in cases where the interface is shut down or the router cannot communicate with the next router. When deselected, this static route can be deleted.

Table K-126 Static Routing Dialog Box (Continued)

OK button	Saves your changes locally on the client and closes the dialog box. **Note** To save your changes to the Security Manager server so that they are not lost when you log out or close your client, click **Save** on the source page.