Configuring Logging Policies on Firewall Devices

The Logging feature lets you enable and manage NetFlow "collectors," and enable system logging, set up logging parameters, configure event lists (syslog filters), apply the filters to a destination, set up syslog messages, configure syslog servers, and specify e-mail notification parameters.

After you enable logging and set up the logging parameters using the Logging Setup page, the Event Lists page lets you configure filters (for a set of syslogs) which can be sent to a logging destination. The Logging Filters page lets you specify a logging destination for the syslogs to be sent. Finally, the Syslog and E-Mail pages configure syslog and e-mail setup.

This chapter contains the following topics:

NetFlow Page

A device configured for NetFlow data export captures flow-based traffic statistics on the device. This information is periodically transmitted from the device to a NetFlow collection server, in the form of User Datagram Protocol (UDP) datagrams.

The NetFlow page lets you enable NetFlow export on the selected device, and define and manage NetFlow "collectors" to which collected flow information is transmitted.

Navigation Path

- (Device view) Select **Platform > Logging > NetFlow** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Logging > NetFlow** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

Related Topics

- Using Rules Tables
- Filtering Tables
- Table Columns and Column Heading Features

Field Reference

Table 1: NetFlow Page

Element	Description
Enable Flow Export	If checked, NetFlow data export is enabled.
Template Export Interval	Interval (in minutes) between transmissions of flow information to the collectors. The value can be from one to 3600 minutes; the default is 30.
Active Refresh Interval	For active connections, specifies the time interval between flow-update events in minutes. Valid values are from 1 to 60 minutes. The default value is 1 minute.
Delay Flow Create	Delays the sending of a flow-create event by the specified number of seconds. The value can be from one to 180 seconds. If no value is entered, there is no delay, and the flow-create event is exported as soon as the flow is created. If the flow is torn down before the configured delay, the flow-create event is not sent; an extended flow teardown event is sent instead.
Collectors table	Lists the currently defined NetFlow collectors. Use the Add Row, Edit Row and Delete Row buttons below the table to manage these entries. The Add Row and Edit Row buttons open the Add and Edit Collector Dialog Boxes (NetFlow) , on page 2. **Note** Cisco Security Manager does not allow duplicate netflow collectors for ASA 9.6(4) to 9.7.0, and 9.8(2) and above devices. Change the current configuration or remove the duplicate or overlapping configuration (**Platform> Logging > Netflow**) for the device.

Add and Edit Collector Dialog Boxes (NetFlow)

Use the Add Collector and Edit Collector dialog boxes to define and edit NetFlow “collectors.” Except for the title, the two dialog boxes are identical; the following information applies to both.

Navigation Path

You can open the Add and Edit Collector dialog boxes from the NetFlow Page , on page 1.

Field Reference

Table 2: Add and Edit Collector Dialog Boxes

Element	Description
Interface	Enter or Select the name of the device interface through which the collector is contacted.
Collector	Enter the IP address or the network name of the server to which NetFlow packets will be sent. You also can Select a Networks/Hosts object.
UDP Port	Specify the UDP port on the specified Collector to which NetFlow packets will be sent. Values can range from 1 to 65535; the default is 2055.

Embedded Event Manager

The Embedded Event Manager (EEM) enables you to debug problems and provides general purpose logging for troubleshooting. There are two components: events to which the EEM responds or listens, and event manager applets that define actions as well as the events to which the EEM responds. You may configure multiple event manager applets to respond to different events and perform different actions.

Note Embedded Event Manager is supported on ASA 9.2(1)+ only.

Supported Events

The EEM supports the following events:

- Syslog—The ASA uses syslog message IDs to identify syslog messages that trigger an event manager applet. You may configure multiple syslog events, but the syslog message IDs may not overlap within a single event manager applet.
- Timers—You may use timers to trigger events. You may configure each timer only once for each event manager applet. Each event manager applet may have up to three timers. The three types of timers are the following:
  - Watchdog (periodic) timers trigger an event manager applet after the specified time period following the completion of the applet's actions and restart automatically.
  - Countdown (one-shot) timers trigger an event manager applet once after the specified time period and do not restart unless they are removed, then re-added.
  - Absolute (once-a-day) timers cause an event to occur once a day at a specified time, and restart automatically. The time-of-day format is in hh:mm:ss.

You may configure only one timer event of each type for each event manager applet.

- None—The none event is triggered when you run an event manager applet manually.
- Crash—The crash event is triggered when the ASA crashes. Regardless of the value of the output command, the action commands are directed to the crashinfo file. The output is generated before the show tech command.

Note Be careful when using a range of Syslog IDs and when using timers. Incorrect configuration can cause an ASA loop and prevent the applet from executing normally.

Configuring Actions

When an event manager applet is triggered, the actions on the event manager applet are performed. Each action has a number that is used to specify the sequence of the actions. The sequence number must be unique within an event manager applet. You may configure multiple actions for an event manager applet. The commands are typical CLI commands, such as **show blocks**.

Configuring Output Destinations

You may send the output of the action CLI commands to one of three locations:

- None, which is the default and discards the output
- Console, which sends the output to the ASA console
- File, which sends the output to a file. The following four file options are available:
  - new—creates a new, uniquely named file each time that an event manager applet is invoked.
  - overwrite—overwrites a specified file each time that an event manager applet is invoked.
  - append—appends to a specified file each time that an event manager applet is invoked. If the file does not yet exist, it is created.
  - rotate—creates a set of uniquely named files that are rotated each time that an event manager applet is invoked.

Guidelines and Limitations

- Supported in single mode only. Not supported in multiple context mode.
- Supported in routed and transparent firewall modes.
- EEM will be enabled irrespective of whether logging functionality is enabled on the device or not.
- The EEM functionality on the ASA only contains a subset of the EEM functionality found on Cisco routers.
- During a crash, the state of the ASA is generally unknown. Some commands may not be safe to run during this condition.
- The name of an event manager applet may not contain spaces.
- You cannot modify the None event and Crashinfo event parameters.
- Performance may be affected because syslog messages are sent to the EEM for processing.
- The default output is none for each event manager applet. To change this setting, you must enter a different output value.
- You may have only one output option defined for each event manager applet.

The Embedded Event Manager table lists the currently defined event manager applets. Use the Add Row, Edit Row and Delete Row buttons below the table to manage these entries. The Add Row and Edit Row buttons open the Add and Edit Applet Dialog Boxes , on page 5.

Navigation Path

- (Device view) Select **Platform > Logging > Embedded Event Manager** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Logging > Embedded Event Manager** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

Related Topics

- Add and Edit Applet Dialog Boxes , on page 5
- Table Columns and Column Heading Features

Add and Edit Applet Dialog Boxes

Use the Add Applet and Edit Applet dialog boxes to define and edit event manager applets. Except for the title, the two dialog boxes are identical; the following information applies to both.

Navigation Path

You can open the Add and Edit Applet dialog boxes from the Embedded Event Manager , on page 3.

Field Reference

Table 3: Add and Edit Applet Dialog Boxes

Element	Description
Name	Enter a unique name for the event manager applet. The name cannot contain spaces and must be less than 32 characters.
Description	Enter a description for the event manager applet. The description may be up to 256 characters long.
Configuration Tab	
Crashinfo	When selected, the event manager applet is triggered when the ASA crashes. Regardless of the value of the Output field, the action commands are directed to the crashinfo file. The output is generated before the show tech command. **Note** The state of the ASA is generally unknown when it crashes. Some CLI commands may not be safe to run during this condition.
None	When selected, you can trigger the event manager applet manually. **Note** Manual triggering of the EEM applet is not supported in Cisco Security Manager. To manually trigger an applet, you must use a FlexConfig. See Managing Flexconfigs for more information.

Element	Description
Syslog table	The Syslog table lists the currently defined syslog message IDs for the selected applet. Use the Add Row, Edit Row and Delete Row buttons below the table to manage these entries. The Add Row and Edit Row buttons open the Add and Edit Syslog Configuration Dialog Boxes , on page 7.
Absolute	Configure an absolute (once-a-day) timer event Absolute timers cause an event to occur once a day at a specified time, and restart automatically. Use the fields provided to enter the time of day in hours, minutes, and seconds. The time range is from 00:00:00 (midnight) to 23:59:59.
Countdown	Configures a countdown (one-shot) timer event. Countdown timers trigger an event manager applet once after the specified time period and do not restart unless they are removed, then re-added. Enter the time period in seconds. The number of seconds may range from 1- 604800.
Watchdog	Configures a watchdog (periodic) timer event. Watchdog timers trigger an event manager applet after the specified time period following the completion of the applet's actions and restart automatically. Enter the time period in seconds. The number of seconds may range from 1- 604800.
Output	To configure specific destinations for sending output from an action, choose one of the available output destination options: • none—(default) discards the output. • console—sends the output to the ASA console. • file—sends the output to a file. Select the file option in the Action list.
Action	The following four file options are available: • new—creates a new, uniquely named file each time that an event manager applet is invoked. The filename has the format of eem-applet-timestamp.log, in which applet is the name of the event manager applet and timestamp is a dated timestamp in the format of YYYYMMDD-hhmmss. • overwrite—overwrites a specified file each time that an event manager applet is invoked. Specify the file details using the File Location and File Name fields. • append—appends to a specified file each time that an event manager applet is invoked. If the file does not yet exist, it is created. Specify the file details using the File Location and File Name fields. • rotate—creates a set of uniquely named files that are rotated each time that an event manager applet is invoked. Specify the number of files to be rotated in the File Count field (valid values range from 2 - 100). When a new file is to be written, the oldest file is deleted, and all subsequent files are renumbered before the first file is written. The newest file is indicated by 0, and the oldest file is indicated by the highest number. The filename format is eem-applet-x.log, in which applet is the name of the applet, and x is the file number.

Element	Description
File Location	Specifies the location of the output file. The location may also use FTP, TFTP, and SMB targeted files.
File Name	Specifies the filename of the output file.
File Count	Specify the number of files to be rotated when "rotate" is the selected Action. When a new file is to be written, the oldest file is deleted, and all subsequent files are renumbered before the first file is written. The newest file is indicated by 0, and the oldest file is indicated by the highest number. Valid values for the rotate value range from 2 - 100. The filename format is eem-applet-x.log, in which applet is the name of the applet, and x is the file number.
Action Tab	
Action table	The Action table lists the currently defined actions for the selected applet. Use the Add Row, Edit Row and Delete Row buttons below the table to manage these entries. The Add Row and Edit Row buttons open the Add and Edit Action Configuration Dialog Boxes , on page 8.

Add and Edit Syslog Configuration Dialog Boxes

Use the Add Syslog Configuration and Edit Syslog Configuration dialog boxes to configure the syslog message IDs for an event manager applet. Except for the title, the two dialog boxes are identical; the following information applies to both.

Navigation Path

You can open the Add and Edit Syslog Configuration dialog boxes from the Add and Edit Applet Dialog Boxes , on page 5.

Field Reference

Table 4: Add and Edit Syslog Configuration Dialog Boxes

Element	Description
ID	Enter a single syslog message or a range of syslog messages. If a syslog message occurs that matches the specified individual syslog message or range of syslog messages, an event manager applet is triggered. **Note** Syslog message IDs may not be entered twice or overlap within a single event manager applet.
Occurs	(Optional) In the occurrences field, enter the number of times that the syslog message must occur for an event manager applet to be invoked. The default is 1 occurrence every 0 seconds. Valid values are from 1 - 4294967295.
Period	(Optional) In the period field, enter the number of seconds within which the syslog messages must occur to invoke the action. This value limits how frequently an event manager applet is invoked to at most once in the configured period. Valid values are from 0 - 604800. A value of 0 means that no period is defined.

Add and Edit Action Configuration Dialog Boxes

Use the Add Action Configuration and Edit Action Configuration dialog boxes to configure the actions for an event manager applet. Except for the title, the two dialog boxes are identical; the following information applies to both.

Navigation Path

You can open the Add and Edit Action Configuration dialog boxes from the Add and Edit Applet Dialog Boxes , on page 5.

Field Reference

Table 5: Add and Edit Action Configuration Dialog Boxes

Element	Description
Ordinal ID	Enter the unique sequence number in the Ordinal ID field. Valid sequence numbers range from 0 - 4294967295. When adding an action configuration, the Ordinal ID will default to one greater than the highest Ordinal ID used.
CLI	Enter the CLI command in the CLI field. The command runs in global configuration mode as a user with privilege level 15 (the highest). The command may not accept any input, because it is disabled.

E-Mail Setup Page

The E-Mail Setup page (PIX 7.0/ASA Only) lets you set up a source e-mail address, as well as a list of recipients for specified syslog messages to be sent as e-mails. You can filter the syslog messages sent to a destination e-mail address by severity. The table shows which entries have been set up.

The syslog severity filter used for the destination e-mail address will be the higher of the severity selected in this section and the global filter set for all e-mail recipients in the Logging Filters page.

Navigation Path

- (Device view) Select **Platform > Logging > Syslog > E-Mail Setup** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Logging > Syslog > E-Mail Setup** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

Field Reference

Table 6: E-Mail Setup Page

Element	Description
Source Email Address	Enter the email address to be used as the source address when syslogs are sent as emails.

Element	Description
Destination Address table	Lists the currently defined email recipients of syslog messages. Use the Add Row, Edit Row and Delete Row buttons below the table to manage this list; the Add Row and Edit Row buttons open the Add/Edit Email Recipient Dialog Box , on page 9.

Add/Edit Email Recipient Dialog Box

The Add/Edit Email Recipient dialog box lets you configure a destination address to be sent emails containing syslog messages; you can limit the messages sent according to severity.

The syslog severity filter used for the destination email address will be the higher of the severity selected in this section and the global filter set for all email recipients on the Logging Filters Page , on page 13.

Navigation Path

You can access the Add/Edit Email Recipient dialog box from the E-Mail Setup Page , on page 8.

Field Reference

Table 7: Add/Edit Email Recipient Dialog Box

Element	Description
Destination Email Address	Enter the recipient email address for the chosen type of syslog messages.
Syslog Severity list	Choose the severity of the syslogs to be emailed to this recipient; messages of the chosen severity and higher are sent. Message severity levels are described in Logging Levels , on page 25.

Event Lists Page

The Event Lists page (PIX 7.0+/ASA only) lets you define a set of syslog message filters for logging. After you enable logging and set up global logging parameters on the Logging Setup page, use this page to configure event lists used to filter syslog messages sent to different logging destinations. (The Logging Filters Page , on page 13 lets you specify logging destinations for event lists.)

Use the Add Row, Edit Row and Delete Row buttons below the Event Lists table to manage the entries. Add Row and Edit Row open the Add/Edit Event List Dialog Box , on page 11.

Navigation Path

- (Device view) Select **Platform > Logging > Syslog > Event Lists** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Logging > Syslog > Event Lists** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

Related Topics

- Logging Setup Page , on page 16
- Configuring Logging Setup , on page 16

Message Classes and Associated Message ID Numbers

The following table lists the message classes and the range of message IDs in each class.

Table 8: Message Classes and Associated Message ID Numbers

Class	Definition	Message ID Numbers
auth	User Authentication	109, 113
bridge	Transparent Firewall	110, 220
ca	PKI Certification Authority	717
config	Command interface	111, 112, 208, 308
e-mail	E-mail Proxy	719
ha	Failover (High Availability)	101, 102, 103, 104, 210, 311, 709
ids	Intrusion Detection System	400, 401, 415
ip	IP Stack	209, 215, 313, 317, 408
np	Network Processor	319
ospf	OSPF Routing	318, 409, 503, 613
rip	RIP Routing	107, 312
rm	Resource Manager	321
session	User Session	106, 108, 201, 202, 204, 302, 303, 304, 305, 314, 405, 406, 407, 500, 502, 607, 608, 609, 616, 620, 703, 710
snmp	SNMP	212
sys	System	199, 211, 214, 216, 306, 307, 315, 414, 604, 605, 606, 610, 612, 614, 615,701, 711
vpdn	PPTP and L2TP Sessions	213, 403, 603
vpn	IKE and IPsec	316, 320, 402, 404, 501, 602, 702, 713, 714, 715
vpnc	VPN Client	611
vpnfo	VPN Failover	720
vpnlb	VPN Load Balancing	718

Class	Definition	Message ID Numbers
webvpn	Web-based VPN	716

Add/Edit Event List Dialog Box

The Add/Edit Event List dialog box lets you create or edit an event list, and specify which syslog messages to include in the event list filter.

You can use the following criteria to define an event list:

- Class and Severity
- Message ID

Class represents specific types of related syslog messages. For example, the class auth represents all syslog messages related to user authentication.

Severity classifies syslogs based on the relative importance of the event in the normal functioning of the network. The highest severity is Emergency, which means the resource is no longer available. The lowest severity is Debugging, which provides detailed information about every network event.

The message ID is a numeric value that uniquely identifies each individual message. You can specify a single message ID, or a range of IDs, in an event list.

Navigation Path

You can access the Add/Edit Event List dialog box from the Event Lists Page , on page 9.

Field Reference

Table 9: Add/Edit Event List Dialog Box

Element	Description
Event List Name	Enter a name that uniquely identifies this event list.
Event Class/Severity Filters	This table lists the event class and severity level filters defined for this event list. Use the Add Row, Edit Row and Delete Row buttons below this table to manage the entries. Add Row and Edit Row open the Add/Edit Syslog Class Dialog Box , on page 11.
Message ID Filters	This table list the message ID filters defined for this event list. Use the Add Row, Edit Row and Delete Row buttons below this table to manage the entries. Add Row and Edit Row open the Add/Edit Syslog Message ID Filter Dialog Box , on page 12.

Add/Edit Syslog Class Dialog Box

The Add/Edit Syslog Class dialog box lets you specify an event class and a related severity level as an event list filter.

Class represents specific types of related syslog messages, so you do not have to select the syslogs individually. For example, the class auth represents all syslog messages related to user authentication.

Severity classifies syslogs based on the relative importance of the event in the normal functioning of the network. The highest severity is Emergency, which means the resource is no longer available. The lowest severity is Debugging, which provides detailed information about every network event.

Navigation Path

You access the Add/Edit Syslog Class dialog box from the Add/Edit Event List Dialog Box , on page 11.

Related Topics

- Add/Edit Syslog Message ID Filter Dialog Box , on page 12
- Event Lists Page , on page 9

Field Reference

Table 10: Add/Edit Syslog Class Dialog Box

Element	Description
Event Class	Choose the desired event class. Event classes are described in Message Classes and Associated Message ID Numbers , on page 10.
Severity	Choose the desired message severity level. Severity levels are described in Logging Levels , on page 25.

Add/Edit Syslog Message ID Filter Dialog Box

The Add/Edit Syslog Message ID Filter dialog box lets you specify a syslog message ID, or a range of IDs, as an the event list filter.

Navigation Path

You can access the Add/Edit Syslog Message ID Filter dialog box from the Add/Edit Event List Dialog Box , on page 11.

Related Topics

- Add/Edit Syslog Class Dialog Box , on page 11
- Event Lists Page , on page 9

Field Reference

Message IDs – Enter a syslog message ID, or a range of IDs. Use a hyphen to specify a range; for example, 101001-101010 . Message IDs must be between 100000 and 999999.

Message IDs and their corresponding messages are listed in the System Log Message guides for the appropriate product. You can access these guides from cisco.com:

PIX Firewall

- http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_system_message_guides_list.html

ASA

- http://www.cisco.com/en/US/products/ps6120/products_system_message_guides_list.html

FWSM

- http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/tsd_products_support_model_home.html

Logging Filters Page

The Logging Filters page lets you configure a logging destination for event lists (syslog filters) that have been configured using the Event Lists page, or for only the syslog messages that you specify using the Edit Logging Filters page. Syslog messages from specific or all event classes can be selected using the Edit Logging Filters page.

Navigation Path

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

Related Topics

- Configuring Logging Setup , on page 16
- Edit Logging Filters Dialog Box , on page 14

Field Reference

Table 11: Logging Filters Page

Element	Description
Logging Destination	Lists the name of the logging destination to which messages matching this filter are sent. Logging destinations are as follows: • **Internal Buffer**. Messages matching this filter are published to the internal buffer of the security appliance. • **Console**. Messages matching this filter are published to any console port connections. • **Telnet Sessions**. Messages matching this filter are published to any Telnet sessions connected to the security appliance. • **Syslog Servers**. Messages matching this filter are published to any syslog servers specified on the **Platform > Logging > Syslog Servers page**. • **E-Mail**. Messages matching this filter are published to any recipients specified on the **Platform > Logging > E-mail Setup (PIX7.0/ASA Only)** page. • **SNMP Trap**. Messages matching this filter are published to any SNMP management stations specified on the **Platform > Device Admin > Device Access > SNMP** page. • **ASDM**. Messages matching this filter are published to any ASDM sessions.
Syslogs From All Event Classes	Lists the severity on which to filter, the event list to use, or whether logging is disabled from all event classes. Event classes are described in Message Classes and Associated Message ID Numbers , on page 10.
Syslogs From Specific Event Classes	Lists event class and severity set up as the filter. Event classes are described in Message Classes and Associated Message ID Numbers , on page 10. Severity levels are described in Logging Levels , on page 25.

Edit Logging Filters Dialog Box

The Edit Logging Filters dialog box lets you edit filters for a logging destination. Syslogs can be configured from all or specific event classes, or disabled for a specific logging destination.

Navigation Path

You can access the Edit Logging Filters dialog box from the Logging Filters page. For more information about the Logging Filters page, see Logging Filters Page , on page 13.

Related Topics

- Configuring Logging Setup , on page 16
- Logging Filters Page , on page 13

Field Reference

Table 12: Edit Logging Filters Dialog Box

Element	Description
Logging Destination list	Specifies the logging destination for this filter: • **Internal Buffer**. Messages matching this filter are published to the internal buffer of the security appliance. • **Console**. Messages matching this filter are published to any console port connections. • **Telnet Sessions**. Messages matching this filter are published to any Telnet sessions connected to the security appliance. • **Syslog Servers**. Messages matching this filter are published to any syslog servers specified on the **Platform > Logging > Syslog Servers page**. • **E-Mail**. Messages matching this filter are published to any recipients specified on the **Platform > Logging > E-mail Setup (PIX7.0/ASA Only)** page. • **SNMP Trap**. Messages matching this filter are published to any SNMP management stations specified on the **Platform > Device Admin > Device Access > SNMP** page. • **ASDM**. Messages matching this filter are published to any ASDM sessions.
Syslog from All Event Classes	
Filter on severity option	Filters on the severity of the logging messages.
Filter on severity list	Specifies the level of logging messages on which to filter.
Use event list option	Specifies to use an event list.
Use event list	Specifies the event list to use. Event lists are defined on the Event Lists Page , on page 9.
Disable logging option	Disables all logging to the selected destination.
Syslog from Specific Event Classes (PIX7.0)	
Event Class	Specifies the event class and severity. Event classes include one or all available items. Event classes are described in Message Classes and Associated Message ID Numbers , on page 10.
Severity	Specifies the level of logging messages. Severity levels are described in Logging Levels , on page 25.

Configuring Logging Setup

The Logging Setup page lets you enable system logging on the security appliance and configure other logging options. These options include enabling logging on the security appliance and failover unit, specifying the base log format and detail, and logging to longer-term storage devices, FTP server or Flash, before purging the internal buffer.

Related Topics

- Logging Setup Page , on page 16

Step 1 Select **Platform** > **Logging** > **Syslog** > **Logging Setup** to display the Logging Setup page.

Step 2 Check **Enable Logging**.

This option enables logging on the security appliance.

Step 3 To enable logging on the failover unit paired with this security appliance, select the **Enable logging on the standby failover unit** check box.

Step 4 To enable EMBLEM format, or to send debug messages as part of the syslog messages, select the corresponding check boxes.

If you enable EMBLEM, you must use the UDP protocol to publish syslog messages. It is not compatible with TCP.

Step 5 To write the internal buffer data to an FTP server for future processing prior to clearing the buffer, do the following:

a) Check **FTP Server Buffer wrap**.
b) Enter the IP address of the FTP server in the **IP Address** field.
c) Enter the user name of the account used to log into the FTP server in the **User Name** field.
d) Enter the path in the **Path** field, relative to the FTP root, where the file should be stored.
e) Enter and confirm the password used to authenticate the user name.

Step 6 To write the internal buffer data to Flash for future processing prior to clearing the buffer, do the following:

a) Check **Flash**.
b) Specify the maximum amount of memory to allocate to the storage of internal buffer data.
c) Specify the minimum memory that should remain free on the Flash drive. If this minimum value cannot be retained while writing out the data from the internal buffer, the messages will be pruned to meet the space requirements.

Step 7 To specify the maximum queue size maintained on the appliance for viewing by an ASDM client, enter that value in the **Message Queue Size (Messages)** field.

Logging Setup Page

The Logging Setup page lets you enable system logging on the security appliance and configure other logging options.

Navigation Path

- (Device view) Select **Platform** > **Logging** > **Syslog** > **Logging Setup** from the Device Policy selector.

- (Policy view) Select **PIX/ASA/FWSM Platform > Logging > Syslog > Logging Setup** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

Field Reference

Table 13: Logging Setup Page

Element	Description
Enable Logging	Turns on logging for the main security appliance.
Enable Logging on the Failover Standby Unit	Turns on logging for the standby security appliance, if available.
Send syslogs in EMBLEM format (PIX7.x+, ASA, FWSM 3.x+)	Enables EMBLEM format logging for every logging destination. If you enable EMBLEM, you must use the UDP protocol to publish syslog messages; EMBLEM is not compatible with TCP. **Note** This setting is not compatible with CS-MARS.
Send debug messages as syslogs (PIX7.x+, ASA, FWSM 3.x+)	Redirects all the debug trace output to the syslog. The syslog message does not appear in the console if this option is enabled. Therefore, to see debug messages, you must enable logging at the console and configure it as the destination for the debug syslog message number and logging level. The syslog message number used is *711011* . Default logging level for this syslog is *debug* .
Memory Size of Internal Buffer (bytes)	Specify the size of the internal buffer to which syslogs is saved if the logging buffer is enabled. When the buffer fills up, it is overwritten. The default is 4096 bytes. The range is 4096 to 1048576.
Specify FTP Server Information (PIX7.x+, ASA, FWSM 3.x+)	
FTP Server Buffer Wrap	To save the buffer contents to the FTP server before it is overwritten, check this box and enter the necessary destination information in the following fields. To remove the FTP configuration, deselect this option.
IP Address	Enter the IP address of the FTP server.
User Name	Enter the user name to use when connecting to the FTP server.
Path	Enter the path, relative to the FTP root, where the buffer contents should be saved.
Password/Confirm	Enter and confirm the password used to authenticate the user name to the FTP server.
Specify flash size	
Flash	To save the buffer contents to the flash memory before it is overwritten, check this box. This option is only available in routed or transparent single mode.

Element	Description
Maximum flash to be used by logging (KB)	Specify the maximum space to be used in the flash memory for logging (in KB). This option is available only in routed or transparent single mode.
Minimum free space to be preserved (KB)	Specifies the minimum free space to be preserved in flash memory (in KB). This option is available only in routed or transparent single mode.
ASDM Logging (PIX7.x+, ASA, FWSM 3.x+)	
Message Queue Size	Specify the queue size for syslogs intended for viewing in ASDM.

Configuring Rate Limit Levels

The Rate Limit page lets you specify the maximum number of log messages of specific types (e.g., “alert” or “critical”), and messages with specific Syslog IDs, that can be generated within given periods of time. You can specify individual limits for each logging level, and each Syslog message ID. If the settings conflict, the Syslog message ID limits take precedence.

The Add/Edit Rate Limited Syslog Message Dialog Box , on page 20 is used to specify the maximum number of messages that can be generated for a particular Syslog message ID within a given period of time.

The Add/Edit Rate Limit for Syslog Logging Levels Dialog Box , on page 20 is used to specify the maximum number of messages that can be generated for a particular Syslog logging level within a given period of time.

Related Topics

- Rate Limit Page , on page 19

Follow these steps to manage rate limits for message logging:

Step 1 Access the Rate Limit page by doing one of the following:

- (Device view) Select **Platform > Logging > Syslog > Rate Limit** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Logging > Syslog > Rate Limit** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new policy.

Step 2 Add, edit and delete rate limits for Syslog logging levels:

- To specify the maximum number of messages that can be generated within a given period of time for particular logging level, click the **Add Row** button under the Rate Limits for Syslog Logging Levels table to open the Add/Edit Rate Limit for Syslog Logging Levels Dialog Box , on page 20. Choose a logging level and define a rate limit.
- To edit the rate limit for a particular logging level, select the appropriate entry in the Rate Limits for Syslog Logging Levels table, and then click the **Edit Row** button under the table to open the Add/Edit Rate Limit for Syslog Logging Levels Dialog Box , on page 20. Alter the rate limit as necessary.
- To delete a rate limit entry from the Rate Limits for Syslog Logging Levels table, select it and then click the **Delete Row** button under the table. A confirmation dialog box may be displayed; click OK to delete the entry.

Step 3 Add, edit and delete limits for log messages according to message IDs:

- To specify the maximum number of messages that can be generated within a given period of time for particular message ID, click the **Add Row** button under the Individually Rate Limited Syslog Messages table to open the Add/Edit Rate Limited Syslog Message Dialog Box , on page 20. Choose a Syslog message ID and define a rate limit.
- To edit the rate limit for a particular Syslog message ID, select the appropriate entry in the Individually Rate Limited Syslog Messages table, and then click the **Edit Row** button under the table to open the Add/Edit Rate Limited Syslog Message Dialog Box , on page 20. Alter the rate limit as necessary.
- To delete a message limit entry from the Individually Rate Limited Syslog Messages table, select it and then click the **Delete Row** button under the table. A confirmation dialog box may be displayed; click OK to delete the entry.

Rate Limit Page

The Rate Limit page allows you to specify the maximum number of log messages of a particular type (for example, alert or critical) that should be generated within a given period of time. You can specify a limit for each logging level and Syslog message ID. If the settings differ, Syslog message ID limits take precedence.

Navigation Path

- (Device view) Select **Platform > Logging > Syslog > Rate Limit** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Logging > Syslog > Rate Limit** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new policy.

Related Topics

- Configuring Logging Setup , on page 16
- Add/Edit Rate Limit for Syslog Logging Levels Dialog Box , on page 20
- Add/Edit Rate Limited Syslog Message Dialog Box , on page 20

Field Reference

Table 14: Rate Limit Page

Element	Description
Rate Limits for Syslog Logging Levels Table	
Logging Level	The Syslog logging level for which you are specifying a rate limit.
No. of Messages	Maximum number of messages of the specified type allowed in the specified time period.
Interval (seconds)	Number of seconds before the rate limit counter resets.
Individually Rate Limited Syslog Messages Table	

Element	Description
Syslog ID	Identification number of the Syslog message for which you are specifying a rate limit.
No. of Messages	Maximum number of messages with the specified ID allowed in the specified time period.
Interval (seconds)	Number of seconds before the rate limit counter resets.

Add/Edit Rate Limit for Syslog Logging Levels Dialog Box

Using the Add/Edit Rate Limit for Syslog Logging Levels dialog box, you can specify the maximum number of log messages for particular log level that should be generated within a given period of time. You can specify a limit for each logging level or syslog message ID (see Add/Edit Rate Limited Syslog Message Dialog Box , on page 20). If the settings differ, the rate limited syslog message-level settings override rate limit logging level settings.

Navigation Path

You can access the Add/Edit Rate Limit for Syslog Logging Levels dialog box from the Rate Limit page. For more information, see Rate Limit Page , on page 19.

Related Topics

- Configuring Logging Setup , on page 16
- Add/Edit Rate Limited Syslog Message Dialog Box , on page 20
- Rate Limit Page , on page 19

Field Reference

Table 15: Add/Edit Rate Limit for Syslog Logging Levels Dialog Box

Element	Description
Logging Level	The syslog logging level for which you are specifying the rate limit.
Number of Messages	Maximum number of messages of the specified type allowed in the specified time period.
Interval (Seconds)	Number of seconds before the rate limit counter resets.

Add/Edit Rate Limited Syslog Message Dialog Box

Using the Add/Edit Rate Limited Syslog Message dialog box you can specify the maximum number of log messages of a particular Syslog ID that can be generated within a given period of time. You can specify a limit for each syslog message ID or logging level (see Add/Edit Rate Limit for Syslog Logging Levels Dialog Box , on page 20). If the settings differ, the rate limited syslog message-level settings override rate limit logging level settings.

Navigation Path

You can access the Add/Edit Rate Limited Syslog Message dialog box from the Rate Limit page. For more information, see Rate Limit Page , on page 19.

Related Topics

- Configuring Logging Setup , on page 16
- Rate Limit Page , on page 19
- Add/Edit Rate Limit for Syslog Logging Levels Dialog Box , on page 20

Field Reference

Table 16: Add/Edit Rate Limited Syslog Message Dialog Box

Element	Description
Syslog ID	Identification number of the syslog message for which you are specifying a rate limit.
Number of Messages	Maximum number of messages with the specified ID allowed in the specified time period.
Interval (Seconds)	Number of seconds before the rate limit counter resets.

Configuring Syslog Server Setup

You can configure general syslog server settings to set the facility code to be included in syslog messages that are sent to syslog servers, specify whether a timestamp is included in each message, specify the device ID to include in messages, view and modify the severity levels for messages, and disable the generation of specific messages.

Related Topics

- Defining Syslog Servers , on page 27

Step 1 Do one of the following:

- (Device view) Select **Platform > Logging > Syslog > Server Setup** to open the Server Setup Page , on page 23.
- (Policy view) Select **PIX/ASA/FWSM Platform > Logging > Syslog > Server Setup** from the Policy Type selector. Select an existing policy or create a new one.

Step 2 Change the basic message configuration as required:

- If your syslog server expects a different facility than the default, select the required facility in the **Facility** list.
- If you want to include the date and time a message was generated in the message, select **Enable Timestamp on Each Syslog Message**.
  - If you want to configure logging timestamp in the rfc5424 format, select Enable Timestamp Format(rfc5424). This option is applicable for ASA 9.12.1 devices and later. Example output of the timestamp:

Example:

```
2003-08-24T05:14:15.000003-07:00
```

- If you want to add a device identifier to syslog messages (which is placed at the beginning of the message), select **Enable Syslog Device ID** and then select the type of ID:

Note For an ASA cluster, each unit in the cluster generates its own syslog messages. You can configure logging so that each unit uses either the same or a different device ID in the syslog message header field. For example, the hostname configuration is replicated and shared by all units in the cluster. If you configure logging to use the hostname as the device ID, syslog messages generated by all units look as if they come from a single unit. If you configure logging to use the local-unit name that is assigned in the cluster bootstrap configuration as the device ID (Cluster ID option), syslog messages look as if they come from different units. You can also specify whether or not the interface IP address of the Control unit should be used for all cluster devices.

- **Interface**—To use the IP address of the specified interface, regardless of the interface through which the appliance sends the message. Click **Select** to select the interface or the interface role that identifies the interface. Interface roles must map to a single interface.

For ASA clusters, to specify that the interface IP address of the Control unit should be used for all cluster devices, select the corresponding option under the Interface Name field.

- **User Defined ID**—To use a text string (up to 16 characters) of your choosing.
- **Host Name**—To use the hostname of the device.
- **Cluster ID**—To use the unique name in the boot configuration of an individual ASA unit in the cluster as the device ID.

Step 3 Use the Syslog Message table to alter the default settings for specific syslog messages. You need to configure rules in this table only if you want to change the default settings. You can change the severity assigned to a message, or you can suppress (disable) the generation of a message.

- To add a rule, click the **Add Row** button and fill in the Add/Edit Syslog Message Dialog Box , on page 26.

You select the message number whose configuration you want to change, and then select the new severity level, or select **Suppressed** to disable the generation of the message. Typically, you would not change the severity level and disable the message, but you can make changes to both fields if desired. Click **OK** to add the rule to the table.

For a description of message severity levels, see Logging Levels , on page 25.

- To edit a rule, select it and click the **Edit Row** button, make the desired changes, and click **OK**.
- To delete a rule, select it and click the **Delete Row** button.
- If you are using NetFlow, you can easily disable the generation of syslog messages that have NetFlow equivalents by clicking the **Disable NetFlow Equivalent Syslogs** button. This adds the messages to the table as suppressed messages. Note that if any of these syslog equivalents are already in the table, your existing rules are not overwritten.

Syslog Relay Configuration

In addition to events being received by the Cisco Security Manager server, they can be forwarded to a maximum of two external/remote controllers (syslog hosts). Syslog relay will forward the received messages to another syslog host using the UDP syslog protocol.

If you want the syslog messages that are forwarded from the Cisco Security Manager server to have the Cisco Security Manager server's IP address as the source IP address of the syslog message, you must enable it through CLI command:

1. Navigate to CSCOpx\MDC\logrelay and open the logrelay.properties file.
2. Set the values of ext1 and ext2 to false like this:

```
## Source Preservation
#logrelay.dp.txring.ext0.preserve.source=true logrelay.dp.txring.ext1.preserve.source=false
logrelay.dp.txring.ext2.preserve.source=false
```

Note By default the value is true for all collectors, by setting ext1 and ext2 as false, Cisco Security Manager will send the sylog messages with Cisco Security Manager IP. This modification can be done only for remote collectors and not for the local collector (ext0).

Server Setup Page

The Server Setup page allows you to set the facility code to be included in syslog messages that are sent to syslog servers, specify whether a timestamp is included in each message, specify the device ID to include in messages, view and modify the severity levels for messages, and disable the generation of specific messages.

Navigation Path

- (Device view) Select **Platform > Logging > Syslog > Server Setup** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Logging > Syslog > Server Setup** from the Policy Type selector. Select an existing policy or create a new one.

Related Topics

- Configuring Syslog Server Setup , on page 21
- Defining Syslog Servers , on page 27
- Configuring Logging Setup , on page 16
- Logging Levels , on page 25

Field Reference

Table 17: Server Setup Page

Element	Description
Facility	The syslog facility code that the appliance includes in messages destined for syslog servers. The default is LOCAL4(20), which is what most UNIX systems expect. You can select a facility between LOCAL0(16) and LOCAL7(23). Syslog facility is useful when you have a central syslog monitoring system that needs to distinguish among the various network devices that generate syslog data streams. Because your network devices share the eight available facilities, you might need to change this value.
Enable Timestamp on Each Syslog Message	Whether to include the date and time a message was generated in syslog messages. The default is to not include time stamps.
Enable Syslog Device ID	Whether to configure a device ID in non-EMBLEM-format syslog messages. If you select this option, select one of the following to use as the device ID, which is place at the start of all syslog messages: **Note** For an ASA cluster, each unit in the cluster generates its own syslog messages. You can configure logging so that each unit uses either the same or a different device ID in the syslog message header field. For example, the hostname configuration is replicated and shared by all units in the cluster. If you configure logging to use the hostname as the device ID, syslog messages generated by all units look as if they come from a single unit. If you configure logging to use the local-unit name that is assigned in the cluster bootstrap configuration as the device ID (Cluster ID option), syslog messages look as if they come from different units. You can also specify whether or not the interface IP address of the Control unit should be used for all cluster devices. • Interface—The IP address of the selected interface. Enter the name of the interface or click **Select** to select it from a list (or to select an interface role that specifies the interface). Messages include the IP address of the interface specified, regardless of which interface the adaptive security appliance uses to send the log data to the external server. If you select an interface role, that role must map to a single interface on the device. For ASA clusters, to specify that the interface IP address of the Control unit should be used for all cluster devices, select the corresponding option under the Interface Name field. • User Defined ID—A text string you define as the device ID. This string can be up to 16 characters, but cannot contain any of the following special characters: & ’ " < > ? • Host Name—The hostname of the security appliance. • Cluster ID—Use the unique name in the boot configuration of an individual ASA unit in the cluster as the device ID.

Element	Description
Syslog Message table	Use this table to enable or disable the generation of specific syslog messages, or to change the severity level of a message. If you do not want to constrict which message types are generated, or change any message severity levels, you do not need to configure anything in this table. The table shows the messages you have configured with the message level and whether generation is suppressed ("true" in the table). • To add a rule, click the **Add Row** button and fill in the Add/Edit Syslog Message Dialog Box , on page 26. • To edit a rule, select it and click the **Edit Row** button. • To delete a rule, select it and click the **Delete Row** button.
Disable/Enable NetFlow Equivalent Syslogs	If you are using NetFlow logging, you might want to disable the generation of syslog messages that duplicate NetFlow messages. If you click the Disable button, these duplicate syslog messages are added to the Syslog Message table as suppressed messages, and the button is renamed Enable NetFlow Equivalent Syslogs. Clicking the Enable button removes the duplicate syslog messages from the table, meaning that they will no longer be suppressed, and the device will start sending them again. However, if you manually edited any message that was added to the list by the Disable button, the Enable button does not remove them.

Logging Levels

The following table describes logging levels.

Table 18: Logging Levels

Logging Level	Type	Description
0	Emergency	System unusable. Generates messages that identify system instabilities.
1	Alerts	Immediate action needed. Generates messages that identify system integrity issues that require immediate administrative action.
2	Critical	Critical condition. Generates messages that identify critical system issues.
3	Errors	Error condition. Generates messages that identify system errors during operation.
4	Warnings	Warning condition. Generates messages that identify system warnings. For example, device might be configured incorrectly.
5	Notifications	Normal but significant condition. Generates messages that identify normal operations that are typically considered significant events.
6	Information	Informational only. Generates messages that identify system information that is typical of day-to-day activity, such as network session records.

Logging Level	Type	Description
7	Debugging	Generates syslog messages that assist you in debugging. Also generates logs that identify the commands issued during FTP sessions and the URLs requested during HTTP sessions. Includes all emergency, alert, critical, error, warning, notification, and information messages.
-	Disabled	No logging.

Add/Edit Syslog Message Dialog Box

The Add/Edit Syslog Message dialog box lets you modify the logging level or suppression setting for a syslog message.

Navigation Path

You can access the Add/Edit Syslog Message dialog box from the Server Setup Page , on page 23.

Field Reference

Table 19: Add/Edit Syslog Message Dialog Box

Element	Description
Syslog ID list	The message log ID of the message whose severity level or suppression setting you want to alter. These values and their corresponding messages are identified in the System Log Message guides for the appropriate product: **PIX Firewall** http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_system_message_guides_list.html **ASA** http://www.cisco.com/en/US/products/ps6120/products_system_message_guides_list.html **FWSM** http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/tsd_products_support_model_home.html **Note** Starting from Cisco Security Manager 4.10, you can enter a syslog message in the Syslog ID field. Make sure that you enter a valid syslog ID corresponding to the device; else the deployment may fail.
Logging Level list	The logging level that you want to assign to the message. For logging levels and descriptions, see Logging Levels , on page 25. Select (default) to use the default level assigned to the message.
Suppressed	Whether to suppress the generation of the syslog message. Suppressing a message disables its generation, so you will not see it in syslogs.

Element	Description
Disable Syslogs on Standby	Whether to block specific syslog messages from being generated on standby ASA devices. This feature is available from ASA version 9.4(1) and Security Manager supports this feature starting from version 4.9.

Defining Syslog Servers

The Syslog Servers page lets you specify the syslog servers to which the security appliance will send syslog messages. To make use of the syslog servers you define, you must enable logging using the Logging Setup page and set up the appropriate filters for destinations using the Logging Filters page.

Tip If you want to view events from an ASA device using Security Manager Event Viewer, ensure that you define the Security Manager server as a syslog server. Also, if you use CS-MARS or other applications to manage syslog events, include those servers in this policy.

By directing syslog records generated by a security appliance to a syslog server, you can process and study the records.

Before You Begin

Enable logging. See Configuring Logging Setup , on page 16.

Related Topics

- Syslog Servers Page , on page 28
- Add/Edit Syslog Server Dialog Box , on page 29

Step 1 Select **Platform** > **Logging** > **Syslog** > **Syslog Servers** to display the Syslog Servers page.

Step 2 Do one of the following:

- To add a new syslog target, click the **Add Row** button.
- To edit an existing syslog target, select the check box for the row, then click the **Edit Row** button.

Step 3 Enter or select the interface name in the **Interface** field.

The list displays all interfaces defined at the current scope.

Step 4 Enter or select the IP address of the syslog server in the **IP Address** field.

Step 5 Determine whether to use UDP or TCP, then click the appropriate radio button under Protocol.

Step 6 Enter the port from which the security appliance sends either UDP or TCP syslog messages. The port must be the same port on which the syslog server listens.

- TCP—1470 (Default). TCP ports work only with a security appliance syslog server.
- UDP—514 (Default).

Step 7 To generate syslog messages using the EMBLEM format, select the **Log messages in Cisco EMBLEM format** check box.

To enable this option, you must select UDP protocol to publish messages to this syslog server.

Step 8 Click **OK**.

The definition appears in the Syslog Servers table.

Syslog Servers Page

The Syslog Servers page lets you specify the syslog servers to which the security appliance sends syslog messages. To make use of the syslog servers you define, you must enable logging using the Logging Setup page and set up the appropriate filters for destinations using the Logging Filters page.

Tip If you want to view events from an ASA device using Security Manager Event Viewer, ensure that you define the Security Manager server as a syslog server. Also, if you use CS-MARS or other applications to manage syslog events, include those servers in this policy.

Navigation Path

- (Device view) Select **Platform > Logging > Syslog > Syslog Servers** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Logging > Syslog > Syslog Servers** from the Policy Type selector. Select an existing policy or create a new one.

Related Topics

- Defining Syslog Servers , on page 27
- Configuring Logging Setup , on page 16

Field Reference

Table 20: Syslog Servers Page

Element	Description
Syslog Servers table	The syslog servers to which this device sends syslog messages. The table shows the device interface that publishes messages to the server, the server's IP address, syslog protocol and port number, and whether the messages are in Cisco EMBLEM syslog format. There is a limit of four syslog servers that can be set up per context. • To add a server, click the **Add Row** button and fill in the Add/Edit Syslog Server Dialog Box , on page 29. • To edit a server, select it and click the **Edit Row** button. • To delete a server, select it and click the **Delete Row** button.
Queue Size	Specifies the size of the queue for storing syslog messages on the security appliance when syslog server is busy. Minimum is 1 message. Default is 512. Specify 0 to allow an unlimited number of messages to be queued (subject to available block memory).
Allow user traffic to pass when TCP syslog server is down	Whether to restrict all traffic if any syslog server that is using the TCP protocol is down.

Add/Edit Syslog Server Dialog Box

The Add/Edit Syslog Servers dialog box lets you add or edit the syslog servers to which the security appliance will send syslog messages. To make use of the syslog servers you define, you must enable logging using the Logging Setup page and set up the appropriate filters for destinations using the Logging Filters page.

Note There is a limit of four syslog servers that can be set up per context.

Navigation Path

You can access the Add Syslog Servers dialog box from the Syslog Servers page. For more information about the Syslog Servers page, see Syslog Servers Page , on page 28.

Related Topics

- Defining Syslog Servers , on page 27
- Configuring Logging Setup , on page 16

Field Reference

Table 21: Add/Edit Syslog Server Dialog Box

Element	Description
Interface	The interface used to communicate with the syslog server. Enter the name of the interface or interface role object, or click **Select** to select it from a list or to create a new object.
IP Address	The IP address of syslog server. Enter the IP address or the name of the network/host policy object that defines the address, or click **Select** to select the network/host object. **Note** Starting with Cisco Security Manager 4.13, IPv6 addresses are supported for the syslog server.
Protocol	The protocol used by syslog server, either TCP or UDP. UDP is the default. TCP ports work only with a security appliance syslog server. **Note** You must select UDP if you intend to use the EMBLEM format.
Port	The TCP or UDP port from which the security appliance sends syslog messages and on which the syslog server receives them. The default ports for each protocol are: • TCP—1470. • UDP—514. **Tip** If you are defining the Security Manager server as a syslog server, you can find the port number on the Security Manager Administration Event Management Page. **Note** During the installation or upgrade of Security Manager, the Common Services syslog service port is changed from 514 to 49514. Later, if Security Manager is uninstalled, the port is not reverted to 514.
Log messages in Cisco EMBLEM format (UDP only)	Whether to log messages in Cisco EMBLEM format. The syslog server must use UDP. **Note** If the syslog server is a Cisco Security MARS appliance, do not select this option. Cisco Security MARS does not process the EMBLEM format.
Reference Identity	Beginning with version 4.12, Security Manager enables you to select Reference Identity policy object name from the Policy Objects Selector. Reference Identity is enabled only if the Port is TCP and is disabled if the Port is UDP. For more information, see Reference Identities.