



CHAPTER 17

Configuring Logging

The logging feature lets you enable logging and specify how log information is handled. The Log viewing feature lets you view syslog messages in real-time. For a description of the log viewing feature, see [Chapter 45, “Monitoring Logging.”](#)

About Logging

The security appliance supports the generation of an audit trail of syslog messages that describes its activities (for example, what types of network traffic has been allowed and denied) and enables you to configure system logging.

All syslog messages have a default severity level. You can reassign a message to a new severity level, if necessary. When you choose a severity level, logging messages from that level and lower levels are generated. Messages from a higher level are not included. The higher the severity level, the more messages are included. For more information about logging and syslog messages, see the *Cisco Security Appliance Logging Configuration and System Log Messages*.

Security Contexts in Logging

Each security context includes its own logging configuration and generates its own messages. If you log in to the system or admin context, and then change to another context, messages that you view in your session are only those that are related to the current context.

Syslog messages that are generated in the system execution space, including failover messages, are viewed in the admin context along with messages generated in the admin context. You cannot configure logging or view any logging information in the system execution space.

You can configure the security appliance to include the context name with each message, which helps you differentiate context messages that are sent to a single syslog server. This feature also helps you to determine which messages are from the admin context and which are from the system; messages that originate in the system execution space use a device ID of **system**, and messages that originate in the admin context use the name of the admin context as the device ID. To use the device ID, see [Advanced Syslog Configuration, page 17-6](#).

Using Logging

After you have defined the security context, choose **Configuration > Device Management > Logging**. Under Logging, you can do the following:

- In the Logging Setup pane, enable logging and configure the logging parameters. For more information, see [Logging Setup, page 17-2](#).
- In the Syslog Setup pane, set the facility code to be included in syslog messages that are sent to syslog servers, specify that a timestamp is included in each message, view the severity levels for messages, modify the severity level for messages, and disable messages. For more information, see [Syslog Setup, page 17-4](#).
- In the E-Mail Setup pane, specify syslog messages to be sent by e-mail for notification purposes. For more information, see [Syslog Setup, page 17-4](#).
- In the Event Lists pane, create custom lists of events that specify which messages should be logged; these lists are then used when you set up log filters. For more information, see [Event Lists, page 17-8](#).
- In the Logging Filters pane, specify the criteria that should be used to filter the messages sent to each log destination. The criteria you use for creating filters are severity level, message class, message ID, or events lists. For more information, see [Logging Filters, page 17-10](#).
- In the Rate Limit pane, limit the number of messages that can be generated in a specified time interval. For more information, see [Rate Limit, page 17-14](#).
- In the Syslog Server pane, specify one or more syslog servers to which the security appliance sends syslog messages. For more information, see [Syslog Servers, page 17-16](#).
- In the SMTP pane, specify one or more SMTP servers to which the ASDM sends e-mail alerts and notification messages. For more information, see [SMTP, page 17-18](#).
- In the NetFlow pane, export the information about the progression of a flow of packets. For more information, see [Using NetFlow, page 17-18](#).

Logging Setup

The Logging Setup pane lets you enable system logging on the security appliance and lets you specify general logging parameters, including whether standby units can take over logging, whether to send debug messages, and whether to use the EMBLEM format. This pane also lets you change default settings for the internal log buffer and the security appliance logging queue. To access this pane, choose **Configuration > Device Management > Logging > Logging Setup**.

To configure logging, perform the following steps:

-
- Step 1** Check the **Enable logging** check box to turn on logging for the main security appliance.
 - Step 2** Check the **Enable logging on the failover standby unit** check box to turn on logging for the standby security appliance, if available.
 - Step 3** Check the **Send debug messages as syslogs** check box to redirect all debug trace output to system logs. The syslog message does not appear on the console if this option is enabled. Therefore, to view debug messages, you must have logging enabled at the console and have it configured as the destination for the debug syslog message number and severity level. The syslog message number to use is **711001**. The default severity level for this syslog message is debug.

- Step 4** Check the **Send syslogs in EMBLEM format** check box to enable EMBLEM format so that it is used for all log destinations, except syslog servers.
- Step 5** In the Buffer Size field, specify the size of the internal log buffer to which syslog messages are saved if the logging buffer is enabled. When the buffer fills up, messages will be overwritten unless you save the logs to an FTP server or to internal flash memory. The default buffer size is 4096 bytes. The range is 4096 to 1048576.
- Step 6** To save the buffer content to the FTP server before it is overwritten, check the **Save Buffer To FTP Server** check box. To allow overwriting of the buffer content, uncheck this check box.
- Step 7** Click **Configure FTP Settings** to identify the FTP server and configure the FTP parameters used to save the buffer content. For more information, see [Configure FTP Settings, page 17-3](#).
- Step 8** To save the buffer content to internal flash memory before it is overwritten, check the **Save Buffer To Flash** check box.



Note This option is only available in routed or transparent single mode.

- Step 9** Click **Configure Flash Usage** to specify the maximum space to be used in internal flash memory for logging and the minimum free space to be preserved (in KB). Enabling this option creates a directory called “syslog” on the device disk on which messages are stored. For more information, see [Configure Logging Flash Usage, page 17-4](#).



Note This option is only available in single, routed or transparent mode.

- Step 10** In the Queue Size field, specify the queue size for system logs that are to be viewed in the security appliance.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Configure FTP Settings

The Configure FTP Settings dialog box lets you specify the configuration for the FTP server that is used to save the log buffer content.

To configure FTP settings, perform the following steps:

- Step 1** Check the **Enable FTP client** check box to enable configuration of the FTP client.
- Step 2** In the Server IP Address field, specify the IP address of the FTP server.
- Step 3** In the Path field, specify the directory path on the FTP server to store the saved log buffer content.

- Step 4** In the Username field, specify the username to log in to the FTP server.
- Step 5** In the Password field, specify the password associated with the username to log in to the FTP server.
- Step 6** In the Confirm Password field, reenter the password, and click **OK**.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Configure Logging Flash Usage

The Configure Logging Flash Usage dialog box lets you specify the limits for saving log buffer content to internal flash memory.

To configure logging flash usage, perform the following steps:

- Step 1** In the Maximum Flash to Be Used by Logging field, specify the maximum amount of internal flash memory that can be used for logging (in KB).
- Step 2** In the Minimum Free Space to Be Preserved field, specify the amount of internal flash memory that is preserved (in KB). When the internal flash memory approaches that limit, new logs are no longer saved.
- Step 3** Click **OK** to close this dialog box.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	—

Syslog Setup

The Syslog Setup pane lets you set the facility code to include in messages destined for syslog servers and determine whether syslog messages should include the timestamp. You can change message severity levels and disable messages that you do not want to be logged. To access this pane, choose **Configuration > Device Management > Logging > Syslog Setup**.

To configure syslog messaging, perform the following steps:

-
- Step 1** From the Facility code to include in syslogs drop-down list, choose a system log facility for syslog servers to use as a basis to file messages. The default is LOCAL(4)20, which is what most UNIX systems expect. However, because your network devices share eight available facilities, you might need to change this value for system logs.
- Step 2** To add the date and time in each syslog message sent, check the **Include timestamp in syslogs** check box.
- Step 3** From the Show drop-down list, choose the information to be displayed in the Syslog ID table. Available options are as follows:
- To specify that the Syslog ID table should display the entire list of syslog message IDs, choose **Show all syslog IDs**.
 - To specify that the Syslog ID table should display only those syslog message IDs that have been explicitly disabled, choose **Show disabled syslog IDs**.
 - To specify that the Syslog ID table should display only those syslog message IDs with severity levels that have changed from their default values, choose **Show syslog IDs with changed logging**.
 - To specify that the Syslog ID table should display only those syslog message IDs with severity levels that have been modified and the IDs of syslog messages that have been explicitly disabled, choose **Show syslog IDs that are disabled or with a changed logging level**.
- Step 4** The Syslog ID Setup Table displays the list of syslog messages based on the setting in the Syslog ID Setup Table. Choose individual messages or ranges of message IDs that you want to modify. You can either disable the selected message IDs or modify their severity levels. To select more than one message ID in the list, click the first ID in the range and Shift-click the last ID in the range.
- Step 5** To configure syslog messages to include a device ID, click **Advanced**. For more information, see [Edit Syslog ID Settings, page 17-5](#) and [Advanced Syslog Configuration, page 17-6](#).
-

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Edit Syslog ID Settings

The Edit Syslog ID Settings dialog box lets you modify the severity level of the selected syslog messages or specify that the selected syslog messages should be disabled.

To change syslog message settings, perform the following steps:



Note

The Syslog ID(s) field is display-only. The values that appear in this area are determined by the entries you chose in the Syslog ID table, located in the Syslog Setup pane.

-
- Step 1** Check the **Disable Message(s)** check box to disable messages for the syslog message ID(s) displayed in the Syslog ID(s) list.
- Step 2** From the Logging Level drop-down list, choose the severity level of messages to be sent for the syslog message ID(s) displayed in the Syslog ID(s) list. Severity levels are defined as follows:
- Emergency (level 0, system unusable)
 - Alert (level 1, immediate action needed)
 - Critical (level 2, critical condition)
 - Error (level 3, error condition)
 - Warning (level 4, warning condition)
 - Notification (level 5, normal but significant condition)
 - Informational (level 6, informational message only)
 - Debugging (level 7, appears during debugging only)
- Step 3** Click **OK** to close this dialog box.
-

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Advanced Syslog Configuration

You can configure the security appliance to include a device ID in non-EMBLEM-formatted syslog messages. You can specify only one type of device ID for syslog messages. The device ID can be the hostname of the adaptive security appliance, an interface IP address, the context, or a text string.

The Advanced Syslog Configuration dialog box lets you determine whether syslog messages should include a device ID. If this feature is enabled, the device ID is automatically included in all non-EMBLEM formatted syslog messages.

To specify additional syslog message settings, perform the following steps:

-
- Step 1** Check the **Enable syslog device ID** check box to specify that a device ID should be included in all non-EMBLEM formatted syslog messages.
- Step 2** To specify which to use as the device ID, choose one of the following options:
- Hostname
 - IP address
 - Choose the interface name that corresponds to the specified IP address from the drop-down list.
 - String

In the User-Defined ID field, specify an alphanumeric, user-defined string.

Step 3 Click **OK** to close this dialog box.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

E-Mail Setup

The E-Mail Setup pane 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-mail messages for notification purposes. You can filter the syslog messages sent to a destination e-mail address by severity level. The table shows which entries have been created. To access this pane, choose **Configuration > Device Management > Logging > E-Mail Setup**.

To configure e-mail to send notification of selected syslog messages, perform the following steps:

- Step 1** In the Source E-Mail Address field, specify the e-mail address that is used as the source address for syslog messages that are sent as e-mail messages.
- Step 2** Click **Add** to enter a new e-mail address recipient of the specified syslog messages.
- Step 3** Choose the severity level of the syslog messages that are sent to the recipient from the drop-down list. The syslog message severity filter used for the destination e-mail address causes messages of the specified severity level and higher to be sent. The global filter specified in the Logging Filters pane is also applied to each e-mail recipient. For more information, see [Logging Filters, page 17-10](#).
- Step 4** Click **Edit** to modify an existing the severity level of the syslog messages that are sent to this recipient.
- Step 5** Click **OK** to close this dialog box.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit E-Mail Recipients

The Add/Edit E-Mail Recipient dialog box lets you set up a destination e-mail address for a specified severity of syslog messages to be sent as e-mail messages.

The severity level used to filter messages for the destination e-mail address is the higher of the severity level specified in this dialog box and the global filter set for all e-mail recipients in the Logging Filters pane.

To add or edit e-mail recipients and severity levels, see [Syslog Setup, page 17-4](#).

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Event Lists

The Event Lists pane lets you create custom lists of events that are used to choose which syslog messages are sent to a specific destination. After you enable logging and configure the logging parameters using the Logging Setup pane, create one or more lists of events in the Event Lists pane. Use these event lists in the Logging Filters pane to specify a logging destination for each list of events. To access this pane, choose **Configuration > Device Management > Logging > Event Lists**.

You use three criteria to define an event list:

- Message Class
- Severity
- Message ID

A message class is a group of syslog messages related to a security appliance feature that enables you to specify an entire class of messages rather than specifying a class for each message individually. For example, use the auth class to select all syslog messages that are related to user authentication.

Severity level classifies syslog messages based on the relative importance of the event in the normal functioning of the network. The highest severity level is emergency, which means the resource is no longer available. The lowest severity level is debugging, which provides detailed information about every network event.

The message ID is a numeric value that uniquely identifies each message. You can use the message ID in an event list to identify a range of syslog messages, such as 101001-1990120.

To create custom lists of events to send to a specific logging destination, perform the following steps:

-
- Step 1** Click **Add** to display the Add Event List dialog box.
 - Step 2** In the Name field, enter the name of the event list. No spaces are allowed.
 - Step 3** In the Event Class/Severity area, click **Add** to display the Add Class and Severity Filter dialog box.
 - Step 4** Choose the event class from the drop-down list. Available event classes include the following:

- All—All event classes
- auth—User Authentication
- bridge—Transparent firewall
- ca—PKI Certification Authority
- config—Command Interface
- ha—Failover
- ips—Intrusion Protection Service
- ip—IP Stack
- np—Network Processor
- ospf—OSPF Routing
- rip—RIP Routing
- rm—Resource Manager
- session—User Session
- snmp—SNMP
- sys—System

Step 5 Choose the severity level from the drop-down list. Severity levels include the following:

- Emergency (level 0, system unusable)
- Alert (level 1, immediate action needed)
- Critical (level 2, critical condition)
- Error (level 3, error condition)
- Warning (level 4, warning condition)
- Notification (level 5, normal but significant condition)
- Informational (level 6, informational message only)
- Debugging (level 7, appears during debugging only)

Step 6 Click **OK** to close this dialog box.

Step 7 In the Message ID Filters area, click **Add** to display the Add Syslog Message ID Filter dialog box.

Step 8 In the Message IDs field, enter a syslog message ID or range of IDs (for example, 101001-199012) to include in the filter.

Step 9 Click **OK** to close this dialog box.

The event of interest appears in the list. To change this entry, click **Edit**.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit Event List

The Add/Edit Event List dialog box lets you create or edit an event list that you can use to specify which messages should be sent to a log destination. You can create event lists that filter messages according to message class and severity level, or by message ID.

To add or edit an event list, see [Event Lists, page 17-8](#).

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit Syslog Message ID Filter

The Add/Edit Syslog Message ID Filter dialog box lets you specify one or more syslog message IDs to be included in the event list.

To add or edit a syslog message ID filter, see [Event Lists, page 17-8](#).

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Logging Filters

The Logging Filters pane lets you apply message filters to a log destination. Filters applied to a log destination select the messages that are sent to that destination. You can filter messages according to message class and severity level, or use an event list that you can create in the Event Lists pane. To access this pane, choose **Configuration > Device Management > Logging > Logging Filters**.

To apply message filters to a log destination, perform the following steps:

-
- Step 1** Choose the name of the logging destination to which you want to apply a filter. Available logging destinations are as follows:
- Console
 - Security appliance
 - Syslog Servers
 - SNMP Trap
 - E-Mail
 - Internal Buffer
 - Telnet Sessions
- Included in this selection are the second column, Syslogs From All Event Classes, and the third column, Syslogs From Specific Event Classes. The second column lists the severity or the event class to use to filter messages for the log destination, or whether logging is disabled for all event classes. The third column lists the event class to use to filter messages for that log destination. For more information, see [Add/Edit Syslog Message ID Filter, page 17-10](#), [Add/Edit Class and Severity Filter, page 17-13](#), and [Event Lists, page 17-8](#).
- Step 2** Click **Edit** to display the Edit Logging Filters dialog box. To apply, edit, or disable filters, see [Edit Logging Filters, page 17-11](#).
-

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Edit Logging Filters

The Edit Logging Filters dialog box lets you apply filters to each log destination, edit filters already applied to a log destination, or disable logging from all event classes. You can filter messages according to message class and severity level, or use an event list that you create in the Event Lists pane.

The selected logging destination for this filter appears at the top.

To apply filters, perform the following steps:

-
- Step 1** Choose the **Filter on severity** option to filter syslog messages according to their severity level.
- Step 2** Choose the **Use event list** option to filter syslog messages according to an event list.
- Step 3** Choose the **Disable logging from all event classes** option to disable all logging to the selected destination.
- Step 4** Click **New** to add a new event list. To add a new event list, see [Event Lists, page 17-8](#).

- Step 5** Choose the event class from the drop-down list. Available event classes include the following:
- All—All event classes
 - auth—User Authentication
 - bridge—Transparent firewall
 - ca—PKI Certification Authority
 - config—Command Interface
 - ha—Failover
 - ips—Intrusion Protection Service
 - ip—IP Stack
 - np—Network Processor
 - ospf—OSPF Routing
 - rip—RIP Routing
 - rm—Resource Manager
 - session—User Session
 - snmp—SNMP
 - sys—System
- Step 6** Choose the level of logging messages from the drop-down list. Severity levels include the following:
- Emergency (level 0, system unusable)
 - Alert (level 1, immediate action needed)
 - Critical (level 2, critical condition)
 - Error (level 3, error condition)
 - Warning (level 4, warning condition)
 - Notification (level 5, normal but significant condition)
 - Informational (level 6, informational message only)
 - Debugging (level 7, appears during debugging only)
- Step 7** Click **Add** to add the event class and severity level, and then click **OK**.
-

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit Class and Severity Filter

The Add/Edit Class and Severity Filter dialog box lets you specify a message class and severity level to be used to filter messages.

To add or edit a message class and severity level for filtering messages, perform the following steps:

-
- Step 1** Choose the event class from the drop-down list. Available event classes include the following:
- All—All event classes
 - auth—User Authentication
 - bridge—Transparent firewall
 - ca—PKI Certification Authority
 - config—Command Interface
 - ha—Failover
 - ips—Intrusion Protection Service
 - ip—IP Stack
 - np—Network Processor
 - ospf—OSPF Routing
 - rip—RIP Routing
 - rm—Resource Manager
 - session—User Session
 - snmp—SNMP
 - sys—System
- Step 2** Choose the level of logging messages from the drop-down list. Severity levels include the following:
- Emergency (level 0, system unusable)
 - Alert (level 1, immediate action needed)
 - Critical (level 2, critical condition)
 - Error (level 3, error condition)
 - Warning (level 4, warning condition)
 - Notification (level 5, normal but significant condition)
 - Informational (level 6, informational message only)
 - Debugging (level 7, appears during debugging only)
- Step 3** Click **OK** when you are done making selections.
-

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit Syslog Message ID Filter

The Add/Edit Syslog Message ID Filter dialog box lets you specify individual syslog message IDs or ranges of IDs to include in the event list filter.

To add or edit a syslog message ID filter, see [Event Lists, page 17-8](#).

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Rate Limit

The Rate Limit pane lets you specify the number of syslog messages that the firewall can send. You can specify a rate limit for message logging levels or limit the rate of a specific message. The rate level is applied to the severity level or to the message ID, not to a destination. Therefore, rate limits affect the volume of messages being sent to all configured destinations. To access this pane, choose **Configuration > Device Management > Logging > Rate Limit**.

To assign rate limits for all syslog messages in a logging level, perform the following steps:

- Step 1** Choose the logging level (message severity level) to which you want to assign rate limits. Severity levels are defined as follows:

Description	Severity Level
Disabled	No logging
Emergency	0—System unusable
Alert	1—Immediate action needed
Critical	2—Critical condition
Error	3—Error condition
Warning	4—Warning condition
Notification	5—Normal but significant condition
Informational	6—Informational message only
Debugging	7—Debugging only

- Step 2** The No of Messages field displays the number of messages sent. The Interval (Seconds) field displays the interval, in seconds, that is used to limit how many messages at this logging level can be sent. Choose a logging level from the table and click **Edit** to display the Edit Rate Limit for Syslog Logging Level dialog box. To continue, see [Edit Rate Limit for Syslog Logging Level, page 17-15](#).

To assign or change rate limits to individual syslog messages, perform the following steps:

- Step 1** To assign the rate limit of a specific syslog message, click **Add** to display the Add Rate Limit for Syslog Message dialog box. To continue, see [Add/Edit Rate Limit for Syslog Message, page 17-16](#).
- Step 2** To change the rate limit of a specific syslog message, click **Edit** to display the Edit Rate Limit for Syslog Message dialog box. To continue, see [Add/Edit Rate Limit for Syslog Message, page 17-16](#).

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Edit Rate Limit for Syslog Logging Level

The Edit Rate Limit for Syslog Logging Level **dialog** box lets you limit the number of messages that the adaptive security appliance can send in a specified time interval. The selected message severity level displays.

To change the rate limit of a specified logging level, perform the following steps:

- Step 1** Enter the maximum number of messages at this logging level that can be sent.
- Step 2** Enter the amount of time, in seconds, that is used to limit the rate of messages at this logging level, and click **OK**.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit Rate Limit for Syslog Message

The Add/Edit Rate Limit for Syslog Message dialog box lets you assign rate limits to a specific syslog message.

To add or change the rate limit for a specific syslog message, perform the following steps:

-
- Step 1** To add a rate limit to a specific syslog message, click **Add** to display the Add Rate Limit for Syslog Message dialog box. To change a rate limit for a syslog message, click **Edit** to display the Edit Rate Limit for Syslog Message dialog box.
 - Step 2** Enter the message ID of the syslog message that you want to limit.
 - Step 3** Enter the maximum number of messages that can be sent in the specified time interval.
 - Step 4** Enter the amount of time, in seconds, that is used to limit the rate of the specified message, and click **OK**.



Note

To allow an unlimited number of messages, leave both the Number of Messages and Time Interval fields blank.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Syslog Servers

The Syslog Servers pane lets you specify the syslog servers to which the adaptive security appliance should send syslog messages. To use the syslog server(s) you define, you must enable logging using the Logging Setup pane and set up the available destinations in the Logging Filters pane. To access this pane, choose **Configuration > Device Management > Logging > Syslog Server**.

To specify the syslog servers to which the adaptive security appliance should send syslog messages, perform the following steps:

-
- Step 1** To add a new syslog server, click **Add** to display the Add Syslog Server dialog box. To change an existing syslog server settings, click **Edit** to display the Edit Syslog Server dialog box.
 - Step 2** Specify the number of messages that are allowed to be queued on the adaptive security appliance when a syslog server is busy. A zero value means an unlimited number of messages may be queued.
 - Step 3** Check the **Allow user traffic to pass when TCP syslog server is down** check box to specify whether or not to restrict all traffic if any syslog server is down.
 - Step 4** To continue, see [Add/Edit Syslog Server, page 17-17](#).

**Note**

You can set up a maximum of four syslog servers per security context (up to a total of 16).

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Add/Edit Syslog Server

The Add/Edit Syslog Server dialog box lets you add or edit the syslog servers to which the adaptive security appliance sends syslog messages. To use the syslog server(s) you define, you must enable logging in the Logging Setup pane and set up the specific filters for log destinations in the Logging Filters pane.

To add or edit a syslog server, perform the following steps:

- Step 1** Choose the interface used to communicate with the syslog server from the drop-down list.
- Step 2** Enter the IP address that is used to communicate with the syslog server.
- Step 3** Choose the protocol (either TCP or UDP) that is used by the syslog server to communicate with the security appliance.
- Step 4** Enter the port number used by the syslog server to communicate with the adaptive security appliance.
- Step 5** Check the **Log messages in Cisco EMBLEM format (UDP only)** check box to specify whether to log messages in Cisco EMBLEM format (available only if UDP is selected as the protocol).
- Step 6** Check the **Enable secure logging using SSL/TLS (TCP only)** check box to specify that the connection to the syslog server is secure through the use of SSL/TLS over TCP, and that the syslog message content is encrypted.
- Step 7** Click **OK** to complete the configuration.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

SMTP

The SMTP pane allows you to configure the remote SMTP server IP address to which e-mail alerts and notifications are sent in response to specific events. To access this pane, choose **Configuration > Device Setup > Logging > SMTP**.

To configure the remote SMTP server, perform the following steps:

-
- Step 1** Enter the IP address of the primary SMTP server.
 - Step 2** (Optional) Enter the IP address of the standby SMTP server, and click **Apply**.
-

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Using NetFlow

The NetFlow pane lets you enable the transmission of data about a flow of packets. To access this pane, choose **Configuration > Device Management > Logging > NetFlow**.

To use NetFlow, perform the following steps:

-
- Step 1** Specify the template timeout rate, which is the interval (in minutes) at which template records are sent to all configured collectors. The default value is 30 minutes.
 - Step 2** To delay the export of flow-creation events and process a single flow-teardown event instead of a flow-creation event and a flow-teardown event, check the **Delay export of flow creation events for short-lived flows** check box, and then enter the number of seconds for the delay in the Delay By field.
 - Step 3** Specify the collector(s) to which NetFlow packets will be sent. You can configure a maximum of five collectors. To configure a collector, click **Add** to display the Add Collector dialog box, and perform the following steps:
 - a. Enter the IP address or hostname and the UDP port number in the associated fields.
 - b. Choose the interface to which NetFlow packets will be sent from the drop-down list.



Note IP address and hostname assignments should be unique throughout the NetFlow configuration.


- Step 4** To configure more collectors, repeat Step 2 for each additional collector, and click **OK**.
- Step 5** To change collector configuration details, select a collector and click **Edit**. To remove a configured collector, select it and click **Delete**.

- Step 6** When NetFlow is enabled, certain syslog messages become redundant. To maintain system performance, we recommend that you disable all redundant syslog messages, because the same information is exported through NetFlow. To disable all redundant syslog messages, check the **Disable redundant syslog messages** check box. To display the redundant syslog messages and their status, click **Show Redundant Syslog Messages**.
- The Redundant Syslog Messages dialog box appears. The Syslog ID field displays the redundant syslog message numbers. The Disabled field indicates whether or not the specified syslog message is disabled. Click **OK** to close this dialog box.
- To disable individual redundant syslog messages, choose **Configuration > Device Management > Logging > Syslog Setup**.
- Step 7** To continue, see the [“Matching NetFlow Events to Configured Collectors”](#) section on page 17-19.
- Step 8** Click **Apply** to save your changes. Click **Reset** to enter new settings.

Matching NetFlow Events to Configured Collectors

After you configure NetFlow collectors, you can match a NetFlow event with any of these configured collectors.

To specify which NetFlow events should be sent to which collector, perform the following steps:

- Step 1** In the ASDM main application window, choose **Configuration > Firewall > Service Policy Rules**.
- Step 2** Choose **Global Policy** in the table, and click **Add** to display the Add Service Policy Rule dialog box. For more information about service policy rules, see the [“Adding a Service Policy Rule for Through Traffic”](#) section on page 22-6.
-  **Note** NetFlow actions are available only for global service policy rules and are applicable only to the class-default traffic class and to traffic classes with traffic match criteria of “Source and Destination IP Address (uses ACL)” or “Any traffic.”
- Step 3** Click the **Rule Actions** tab, and then click the **NetFlow** tab.
- Step 4** Click **Add** to display the Add Flow Event dialog box.
- Step 5** Choose the flow event type from the drop-down list. Available options are created, torn down, denied, or all events.
- Step 6** Choose collectors to which you want events sent by checking the corresponding check boxes in the Send column.
- Step 7** To add, edit or delete collectors, click **Manage** to display the list of configured collectors in the Manage NetFlow Collectors dialog box. To continue, see [Step 3](#) of the [“Using NetFlow”](#) section on page 17-18.
- Step 8** To change settings for a configured collector, select it from the list and click **Edit**. To remove a collector from this list, select it from the list and click **Delete**.
- Step 9** In the Redundant Syslog Messages area, to disable redundant syslog messages and maintain current performance levels, check the **Disable redundant syslog messages** check box. Click **Show Redundant Syslog Messages** to display a list of redundant syslog messages and their status (disabled or not). You can disable or enable individual syslog messages later by choosing **Configuration > Device Management > Logging**. Click **OK** to close the Redundant Syslog Messages dialog box.

- Step 10** Click **OK** to close the Manage NetFlow Collectors dialog box and return to the Add Flow Event dialog box. Click **OK** again to close the Add Flow Event dialog box and return to the NetFlow tab.
- Step 11** To change flow event entries, choose an entry from the list, and click **Edit**. To remove flow event entries, choose an entry from the list, and click **Delete**.
- Step 12** Click **Finish** to exit the wizard.
-

For more information about NetFlow, see the *Cisco Security Appliance Command Line Configuration Guide* and *Implementation Note for NetFlow Collectors*.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—