



CHAPTER 15

Configuring Logging

The logging feature lets you enable logging and specify how log information is handled. The Log viewing feature lets you view system log messages in real-time. For a description of the log viewing feature, see [Chapter 41, “Monitoring Logging.”](#)

About Logging

The security appliance supports the generation of an audit trail of system log 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 system log 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 system log messages, see the *Cisco Security Appliance System Log Messages Guide*.

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.

System log 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 15-6](#).

Using Logging

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

-
- Step 1** In the Logging Setup pane, enable logging and configure the logging parameters. For more information, see [Logging Setup, page 15-2](#).
 - Step 2** In the Syslog Setup pane, set the facility code to be included in system log 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 suppress messages. For more information, see [Syslog Setup, page 15-4](#).
 - Step 3** In the E-Mail Setup pane, specify system log messages to be sent by e-mail for notification purposes. For more information, see [Syslog Setup, page 15-4](#).
 - Step 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 15-8](#).
 - Step 5** 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 15-12](#).
 - Step 6** 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 15-15](#).
 - Step 7** In the Syslog Server pane, specify one or more syslog servers to which the security appliance sends system log messages. For more information, see [Syslog Servers, page 15-18](#).
 - Step 8** 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 15-19](#).
-

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**.

Fields

- 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 debug messages as syslogs—Redirects all debug trace output to system logs. The system log message does not appear in 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 system log message number and severity level. The system log message number to use is **711001**. The default severity level for this system log message is debug.
- Send syslogs in EMBLEM format—Enables EMBLEM format so that it is used for all log destinations, except syslog servers.

- **Buffer Size**—Specifies the size of the internal log buffer to which system log 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.
- **Save Buffer To FTP Server**—To save the buffer content to the FTP server before it is overwritten, check this check box. To allow overwriting of the buffer content, uncheck this check box.
- **Configure FTP Settings**—Click to identify the FTP server and configure the FTP parameters used to save the buffer content.
- **Save Buffer To Flash**—To save the buffer content to internal Flash memory before it is overwritten, check this check box.



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

- **Configure Flash Usage**—Click 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.



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

- **Queue Size**—Specifies the queue size for system logs that are to be viewed in 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
•	•	•	•	—

For More Information

- See [Configure FTP Settings, page 15-3](#).
- See [Configure Logging Flash Usage, page 15-4](#).

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.

Fields

- **Enable FTP client**—Enables the configuration of the FTP client.
- **Server IP Address**—Specifies the IP address of the FTP server.
- **Path**—Specifies the directory path on the FTP server to store the saved log buffer content.
- **Username**—Specifies the username to log in to the FTP server.

- Password—Specifies the password associated with the username to log in to the FTP server.
- Confirm Password—Confirms the password.

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.

Fields

- Maximum Flash to Be Used by Logging—Specifies the maximum amount of internal Flash memory that can be used for logging (in KB).
- Minimum Free Space to Be Preserved—Specifies the amount of internal Flash memory that is preserved (in KB). When the internal Flash memory approaches that limit, new logs are not saved.

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 system log messages should include the timestamp. This pane also lets you change message severity levels and suppress messages you do not want to be logged. To access this pane, choose **Configuration > Device Management > Logging > Syslog Setup**.

Fields

- Facility code to include in syslogs—Specifies 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 the eight available facilities, you might need to change this value for system logs.
- Include timestamp in syslogs—Includes date and time in every system log message sent.

- Syslog ID Setup—Selects the information to be displayed in the Syslog ID table. Options are defined as follows:
 - Show all syslog IDs—Specifies that the Syslog ID table should display the entire list of system log message IDs.
 - Show suppressed syslog IDs—Specifies that the Syslog ID table should display only those system log message IDs that have been explicitly suppressed.
 - Show syslog IDs with changed logging—Specifies that the Syslog ID table should display only those system log message IDs with severity levels that have changed from their default values.
 - Show syslog IDs that are suppressed or with a changed logging level—Specifies that the Syslog ID table should display only those system log message IDs with severity levels that have been modified and the IDs of system log messages that have been explicitly suppressed.
- Syslog ID Table—Displays the list of system log messages based on the setting in the Syslog ID Table View. Choose individual messages or ranges of message IDs that you want to modify. You can either suppress 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.
- Advanced—Lets you configure system log messages to include a device ID.

Modes

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

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

For More Information

- See [Edit Syslog ID Settings, page 15-5](#).
- See [Advanced Syslog Configuration, page 15-6](#).

Edit Syslog ID Settings

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

Fields

- Syslog ID(s)—*Display-only*. The values displayed in this area are determined by the entries selected in the Syslog ID table, located in the Syslog Setup pane.
- Suppress Message(s)—Check this check box to suppress messages for the system log message ID(s) displayed in the Syslog ID(s) list.
- Logging Level—Choose the severity level of messages to be sent for the system log 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)

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 system log messages. You can specify only one type of device ID for system log 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 system log messages should include a device ID. If this feature is enabled, the device ID is included in all non-EMBLEM formatted system log messages.

Fields

- Enable Syslog Device ID—Specifies that a device ID should be included in all non-EMBLEM formatted system log messages.
- Hostname—Specifies that the hostname is used as the device ID.
- IP Address—Specifies the IP address of the interface that is used as the device ID.
 - Interface Name—Specifies the interface name corresponding to the specified IP address.
- String—Specifies that a user-defined string is used as the device ID.
 - User-defined ID—Specifies an alphanumeric user-defined string.

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 system log messages to be sent as e-mail messages for notification purposes. You can filter the system log 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**.

The system log message severity level used to filter messages for a destination e-mail address is the higher of the severity level selected in this section, compared to the global filter set for all e-mail recipients in the Logging Filters pane.

The system log 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.

Fields

- Source E-Mail address—Specifies the e-mail address that is used as the source address for system log messages that are sent as e-mail messages.
- Destination E-Mail Address—Specifies the e-mail address of the recipient of the specified system log messages.
- Syslog Severity—Specifies the severity level of the system log messages that are sent to this recipient. Messages with the specified severity level and higher are sent.

Modes

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

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

For More Information

- See [Add/Edit E-Mail Recipients, page 15-7](#).
- See [SMTP, page 15-8](#).
- See [Logging Filters, page 15-12](#).

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 system log 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 selected in this section, compared to the global filter set for all e-mail recipients in the Logging Filters pane.

Fields

- Destination E-Mail Address—Specifies the e-mail address of the recipient of selected system log messages.
- Syslog Severity—Specifies the severity level of the system log messages sent to this recipient.

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 lets you enable or disable the SMTP client to provide e-mail notification, such as alerts, that a significant event has occurred. You can add the IP address of an SMTP server and optionally, the IP address of a backup SMTP server. ASDM does not verify whether the IP address is valid, so be sure to type the address correctly. To access this pane, choose **Configuration > Properties > Logging > Email Setup**.

Fields

- Remote SMTP Server—Lets you configure the primary and secondary SMTP servers.
- Primary Server IP Address—Specifies the IP address of the SMTP server.
- Secondary Server IP Address (Optional)—Specifies the IP address of an optional, backup SMTP server.

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 system log 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 on the Event Lists pane. Use these event lists on 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 system log 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 system log messages that are related to user authentication.

Severity level classifies system log 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 system log messages, such as 101001-101010.

Fields

- Name—Lists the name of the event list.
- Event Class/Severity—Lists the event class and the severity level of logging messages. Event classes include:
 - 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

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)
- Message IDs—Lists a system log message ID or range of IDs (for example, 101001-101010) to include in the filter.

Modes

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

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

For More Information

- See [Add/Edit Event List, page 15-10](#).
- See [Add/Edit Syslog Message ID Filter, page 15-11](#).
- See [Logging Filters, page 15-12](#).

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.

A message class is a group of system log messages related to an adaptive security appliance feature. When creating an event list, you can specify an entire class of messages rather than specifying each message individually. For example, use the auth class to select all system log messages that are related to user authentication.

Severity level defines system log 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 system log messages, such as 101001-101010.

Fields

- Name—Enter the name of the event list.
- Event Class—Lists the event class. Event classes include:
 - 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
- Severity—Lists the level of logging messages. 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)
 - Message IDs Filters—Lists a system log message ID or range of system log message IDs, such as 101001-101010, to include in the filter.

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 system log message IDs to be included in the event list.

Fields

- Message IDs—Specify a system log message ID or range of IDs to be logged. Use a hyphen to specify a range (for example, 101001-101010).

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 on the Event Lists pane. To access this pane, choose **Configuration > Device Management > Logging > Logging Filters**.

Fields

- **Logging Destination**—Lists the name of the logging destination to which you can apply a filter. Logging destinations are as follows:
 - Console
 - security appliance
 - Syslog Servers
 - SNMP Trap
 - E-Mail
 - Internal Buffer
 - Telnet Sessions
- **Syslogs From All Event Classes**—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.
- **Syslogs From Specific Event Classes**—Lists the event class to use to filter messages for that log destination.

Modes

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

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

For More Information

- See [Edit Logging Filters](#), page 15-13.
- See [Add/Edit Syslog Message ID Filter](#), page 15-11.
- See [Add/Edit Class and Severity Filter](#), page 15-14.
- See [Event Lists](#), page 15-8.

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 filters for the log destination. You can filter messages according to message class and severity level, or use an event list that you can create on the Event Lists pane.

Fields

- Logging Destination—Specifies the logging destination for this filter.
- Filter on severity—Filters system log messages according to their severity level.
 - Filter on severity—Specifies the level of system log messages on which to filter.
- Use event list—Specifies that an event list will be used for this filter.
 - Use event—Specifies the event list to use.
- New—Lets you add a new event list.
- Disable logging from all event classes—Disables all logging to the selected destination.
- Event Class—Specifies the event class. Event classes include:
 - 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
- Severity—Specifies the level of logging messages. Severity levels include:
 - 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)

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.

A message class is a group of system log messages related to an adaptive security appliance feature. When creating an event list, you can specify an entire class of messages rather than specifying each message individually. For example, use the auth class to select all of the system log messages that are related to user authentication.

Severity level defines system logs 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.

Fields

- Event Class—Specifies the event class. Event classes include:
 - 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
- Severity—Specifies the level of logging messages. Severity levels include:
 - 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)

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 system log message IDs or ranges of IDs to include in the event list filter.

Fields

- Message IDs—Specifies the system log message ID or range of IDs. Use a hyphen to specify a range (for example, 101001-101010).

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 system log messages that the firewall can send. You can specify a rate limit for message logging levels or be more specific and 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**.

Fields

Rate limits for syslog logging levels section

- Logging Level—Lists the message severity level. Levels are defined as follows:
 - Disabled (no logging)
 - 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)
- No of Messages—Displays the number of messages sent. To allow an unlimited number of messages, leave both the Number of Messages and Time Interval fields blank.
- Interval (Seconds)—Displays the interval, in seconds, used to limit how many messages at this logging level can be sent. To allow an unlimited number of messages, leave both the Number of Messages and Time Interval blank.
- Edit—Select a logging level from the table and click to open the Edit Rate Limit dialog box, where you can edit the properties of the selected logging level.

Individually rate-limited syslog messages section

- Syslog ID—Displays the ID for the system log message that is limited.
- Logging Level—Displays the message severity level. For a list of severity levels, see [Rate limits for syslog logging levels section, page 15-16](#).
- No of Messages—Displays the maximum number of messages that can be sent in the specified time interval.
- Interval (Seconds)—Displays the interval, in seconds, used to limit the system log message rate.
- Add—Click to limit the rate of a specific message.

Modes

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

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

For More Information

- See [Edit Rate Limit for Syslog Logging Level, page 15-17](#).
- See [Add/Edit Rate Limit for Syslog Message, page 15-17](#).

Edit Rate Limit for Syslog Logging Level

The Edit Rate Limit for Syslog Logging Level box lets you limit the number of messages that the firewall can send in a specified time interval.

Fields

Rate limit for syslog logging levels section

- **Logging Level**—Displays the selected message severity level. If you are modifying a specific message ID rate limit, you may specify the logging level. Levels are defined as follows:
 - Disabled (no logging)
 - 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)
- **No of Messages**—Specifies the maximum number of messages at this logging level that can be sent.
- **Time Interval (seconds)**—Specifies the amount of time, in seconds, used to limit the rate of messages at this logging level.

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 system log message.

Fields

- **Syslog Message ID**—Specifies the message ID of the system log message that you want to limit.
- **Number of Messages**—Specifies the maximum number of times this message can be sent in the specified time interval.
- **Time Interval**—Specifies the amount of time, in seconds, used to limit the specified message.

**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 security appliance should send system log 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**.

**Note**

You can set up a maximum of four syslog servers per security context.

Fields

- **Interface**—Displays the interface used to communicate with the syslog server.
- **IP Address**—Displays the IP address of the interface that will be used to communicate with the syslog server.
- **Protocol/Port**—Displays the protocol and port that the syslog server uses to communicate with the security appliance.
- **EMBLEM**—Specifies whether to log messages in Cisco EMBLEM format (available only if UDP is selected in the Protocol/Port settings).
- **Queue Size**—Specifies the number of messages that are allowed to be queued on the security appliance if any syslog server is busy. A zero value means an unlimited number of messages may be queued.
- **Allow user traffic to pass when TCP syslog server is down**—Specifies whether to restrict all traffic if any syslog server is down.

Modes

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

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

For More Information

- See [Add/Edit Syslog Server](#), page 15-19.
- See [Logging Setup](#), page 15-2.
- See [Logging Filters](#), page 15-12.

Add/Edit Syslog Server

The Add/Edit Syslog Server dialog box lets you add or edit the syslog servers to which the security appliance sends system log 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.

**Note**

You can set up a maximum of four syslog servers per context.

Fields

- Interface—Specifies the interface used to communicate with the syslog server.
- IP Address—Specifies the IP address used to communicate with the syslog server.
- Protocol—Displays the protocol (either TCP or UDP) used by the syslog server to communicate with the security appliance.
- Port—Specifies the port used by the syslog server to communicate with the security appliance.
- Log messages in Cisco EMBLEM format (UDP only)—Specifies whether to log messages in Cisco EMBLEM format (available only if UDP is selected as the protocol).
- Enable secure logging using SSL/TLS (TCP only)—Specifies that the connection to the syslog server is secure through the use of SSL/TLS over TCP, and that the system log message content is encrypted.

**Note**

The PIX security appliances do not support the secure logging option.

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 send e-mail alerts and notifications in response to specific events. To access this pane, choose **Configuration > Device Setup > Logging > SMTP**.

Fields

- Primary Server IP Address—Specifies the IP address of the primary SMTP server.
- Secondary Server IP Address (optional)—Specifies the IP address of the standby SMTP server.

Modes

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

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