



Configuring Logging on the Security Appliance

This chapter describes commands that you can use to configure and manage logging on the security appliance. It also describes the syslog message format and remote management and monitoring tools.

This chapter does not provide comprehensive information about all logging commands and options. For detailed descriptions and additional logging commands, see the *Cisco Security Appliance Command Reference*.

This chapter includes the following topics:

- [Logging Overview, page 2](#)
- [Basic Logging Commands, page 3](#)
- [Specifying and Managing Syslog Output Locations, page 4](#)
- [Modifying the Content and Format of Syslog Messages, page 10](#)
- [Logging Command Examples, page 11](#)
- [Understanding Log Messages, page 18](#)
- [Other Remote Management and Monitoring Tools, page 22](#)

Logging Overview

The system message logging feature provides you with logging information for monitoring and troubleshooting the security appliance. The logging configuration is very flexible and enables you to customize many aspects of how the security appliance handles messages.

Using the system message logging feature, you can do the following:

- Specify which messages should be logged.
- Disable or change the severity level of a message.
- Specify one or more locations where messages should be sent, including the console, an internal buffer, one or more syslog servers, the ASDM, an SNMP management station, specified e-mail addresses, or to Telnet and SSH sessions.
- Configure and manage messages in groups, such as by severity level or class of message.
- Specify what happens to the contents of the internal buffer when the buffer becomes full and wraps around: you can configure the security appliance to send the buffer contents to an FTP server or to save the contents to Flash.
- Monitor system messages remotely by using ASDM, Telnet and SSH sessions, or by downloading to a Web browser the contents of the internal log buffer.

Most logging commands are entered in configuration mode. To access configuration mode, enter the **configure terminal** command.

To view logs generated by the security appliance, you must configure an output location. You can choose to send all messages, or subsets of messages, to any or all output locations. You can limit which messages are sent to which locations by the severity of the message, the class of the message, or by creating a message list. Creating a message list is a flexible way to specify the messages you want to be sent to one or more syslog destinations.

Many logging commands require you to specify a severity level threshold to identify to which messages a command should be applied. Severity level values are 0 to 7; the lower the level number, the more severe the error. Specify the severity level as either a number or a keyword as described in [Table 1-6](#). The level you specify causes the security appliance to apply the command to messages of that level or lower; for example, if you enter a command that specifies severity level 3, the security appliance applies the command results to messages with a severity level of 1, 2, and 3.

**Note**

The security appliance does not generate messages with a severity level of 0 (emergencies). This level is provided in the **logging** command for compatibility with the UNIX syslog feature, but is not used by the security appliance.

Some logs and logging commands support the **format emblem** option. The EMBLEM syslog format is designed to be consistent with the Cisco IOS software format and is more compatible with CiscoWorks management applications.

**Note**

Not all system messages indicate an error condition. Some messages merely report normal events or log a configuration change.

Basic Logging Commands

Common uses of the logging commands may include starting logging, stopping logging, changing the severity level of a message, disabling a message, and reversing configuration changes, among others. This section includes the following topics:

- [Enabling and Disabling Logging, page 3](#)
- [Changing the Severity Level or Disabling a Message, page 3](#)
- [Reverting Configuration Settings to Default Values, page 4](#)

Enabling and Disabling Logging

Use the following commands to enable logging, to view logs, and to view configuration settings.

Purpose	Command	Description
Enable and disable logging	logging enable	Enables transmission of syslog messages to all output locations. You must set a logging output location to view any logs. Note The logging on command is still supported for backward compatibility.
	no logging enable	Disables logging to all output locations.
View logs and configuration settings	show logging	Lists the contents of the syslog buffer and the current logging configuration. Note To be able to view the contents of the syslog buffer, you must first configure the buffer output location. For more information, see the “Configuring and Managing the Logging Buffer” section on page 7.

Changing the Severity Level or Disabling a Message

Use the following commands to change the severity level of an individual message or to disable an individual message. For a listing of severity levels, see the [“Severity Levels”](#) section on page 19.

Purpose	Command Syntax	Description
Change the severity level of a message	logging message <i>message_number level</i> <i>severity_level</i>	Sets the severity level of a specific syslog message.
	no logging message <i>message_number level</i> <i>severity_level</i>	
	show logging message	Displays a list of syslog messages that have been modified from the default setting (messages that have been assigned a different severity level and messages that have been disabled).
	clear config logging level	Resets all logging severity level changes back to the default.

Disable a message	no logging message <i>message_number</i>	Disables a specific syslog message.
	logging message <i>message_number</i>	Resumes logging of a disabled message.
	show logging message	Displays a list of syslog messages that have been modified from the default setting (messages that have been assigned a different severity level, and messages that have been disabled).
	clear config logging disabled	Reenables logging of all messages previously disabled.

Reverting Configuration Settings to Default Values

Use this command to reset all configuration options to their default values.

Purpose	Command Syntax	Description
Revert logging configuration settings to default values	clear config logging	Reverts all logging configuration settings to their default values. This command affects all configuration settings, including message severity level changes, disabled messages, buffer wrap options, and Flash options.

Specifying and Managing Syslog Output Locations

You can configure the security appliance to send syslog messages to a variety of locations. You can also limit which syslog messages are sent to those locations by specifying individual syslog messages or groups of messages.

Output locations include:

- An internal buffer
- One or more syslog servers
- One or more e-mail destinations
- ASDM (Adaptive Security Device Manager)
- Telnet and SSH sessions
- The console
- An SNMP management station

This section includes the following topics:

- [Commands for Setting and Managing Output Destinations, page 5](#)
- [Configuring and Managing the Logging Queue, page 7](#)
- [Configuring and Managing the Logging Buffer, page 7](#)
- [Managing Groups of Messages, page 8](#)

Commands for Setting and Managing Output Destinations

Use the following commands to specify where the security appliance should send syslog messages.

Table 1-1 Commands for Setting Log Output Destinations

Output Destination	Command Syntax	Description
Internal buffer	logging buffered <i>message_list</i> <i>severity_level</i>	Stores syslog messages in an internal buffer. You can limit the messages sent to the buffer with the <i>message_list</i> and <i>severity_level</i> variables. View the contents of the buffer with the show logging command. For more information about commands to use when configuring and managing the internal buffer, see the “Configuring and Managing the Logging Buffer” section on page 7.
	no logging buffered <i>message_list</i> <i>severity_level</i>	
Syslog message server	logging host <i>interface_name</i> <i>ip_address</i> [tcp / <i>port</i>] udp / <i>port</i>] [format emblem]	Specifies a host that receives the syslog messages (a syslog server). The security appliance can send messages across UDP or TCP. The default protocol and port are UDP/514. The default TCP port (if specified) is 1468. The format emblem option enables EMBLEM formatting (UDP only).
	no logging host <i>interface_name</i> <i>ip_address</i> [tcp / <i>port</i>] udp / <i>port</i>] [format emblem]	
	logging trap <i>message_list</i> <i>severity_level</i>	
	no logging trap <i>message_list</i> <i>severity_level</i>	Enables syslog messages to be sent to a syslog server (see the logging host command to identify the server). Set the <i>severity_level</i> from 1 to 7, or enter the severity level name. You can also specify which messages are sent with the <i>message_list</i> variable.
	logging facility <i>number</i>	Sets the logging facility for a syslog server. The default is 20.
	no logging facility <i>number</i>	
E-mail address	logging mail <i>message_list</i> <i>severity_level</i>	Specifies that syslog messages should be sent to one or more e-mail recipients. Use the <i>message_list</i> or <i>severity_level</i> variables to specify which syslog messages should be sent.
	no logging mail <i>message_list</i> <i>severity_level</i>	
	logging recipient-address	
	no logging recipient-address	Specifies recipient e-mail addresses to be used when sending syslog messages to an e-mail destination. A maximum of five recipient addresses can be configured. Specify each recipient with a new command entry.
	logging from-address	Source e-mail address to be used when sending syslog messages to an e-mail destination.
	no logging from-address	

Table 1-1 Commands for Setting Log Output Destinations (continued)

Output Destination	Command Syntax	Description
Console	logging console <i>message_list</i> <i>severity_level</i> no logging console <i>message_list</i> <i>severity_level</i>	<p>Enables syslog messages to display on the security appliance console (tty) as they occur.</p> <p>Set the <i>severity_level</i> from 1 to 7 or use the level name. You can also specify which messages are sent with the <i>message_list</i> variable.</p> <p>Use this command when you are debugging problems or when there is minimal load on the network. Do not use this command when the network is busy as it can degrade performance.</p>
Telnet or SSH session to console	logging monitor <i>message_list</i> <i>severity_level</i> no logging monitor <i>message_list</i> <i>severity_level</i>	<p>Enables syslog messages to display as they occur when accessing the security appliance console with Telnet or SSH.</p> <p>Set the <i>severity_level</i> from 1 to 7 or specify the severity level name. See Table 1-6 for more information. You can also specify which messages are sent with the <i>message_list</i> variable.</p> <p>To view messages using a Telnet or SSH session, you must establish the Telnet or SSH session, enter the logging monitor command, then enter the terminal monitor command.</p>
ASDM	logging asdm <i>message_list</i> <i>severity_level</i> no logging asdm <i>message_list</i> <i>severity_level</i> show logging asdm logging asdm-buffer-size <i>num_of_messages</i> no logging asdm-buffer-size <i>num_of_messages</i> clear logging asdm	<p>Sends specified messages to the ASDM.</p> <p>Displays the content of the ASDM syslog buffer.</p> <p>Specify the number of messages to be stored in the ASDM syslog buffer before they are sent to ASDM.</p> <p>The no form of this command resets the buffer size to the default value, 100.</p> <p>Clears the ASDM syslog buffer.</p>
SNMP management station	logging history <i>message_list</i> <i>severity_level</i> no logging history <i>message_list</i> <i>severity_level</i>	<p>Enables syslog messages for SNMP.</p> <p>Set the <i>severity_level</i> from 1 to 7 or the level name. See Table 1-6 for more information. You can also specify which messages are sent with the <i>message_list</i> variable. See the logging list command for more information.</p> <p>Use the following commands to set up SNMP on the security appliance:</p> <pre>snmp-server host [if_name] ip_addr snmp-server location text snmp-server contact text snmp-server community key snmp-server enable traps</pre> <p>For more information about using the SNMP commands, see the <i>Cisco Security Appliance Command Reference</i>.</p>

Configuring and Managing the Logging Queue

The security appliance has a fixed number of blocks in memory that can be allocated for buffering syslog messages. The number of blocks required depends on the length of the message queue and the number of syslog hosts specified.

Use the following commands to change the number of messages that can be stored in the logging queue while awaiting processing.

Purpose	Command Syntax	Description
Change the size of the logging queue	logging queue <i>msg_count</i> no logging queue <i>msg_count</i>	Specifies the number of syslog messages that can remain in the message queue while awaiting processing. The default is 512 messages; set to 0 (zero) to specify unlimited messages.
View queue statistics	show logging queue	Use this command to view queue statistics.

Configuring and Managing the Logging Buffer

To store logging messages internally on the security appliance, you must configure the internal buffer as an output location.

Use the following commands to configure the security appliance to:

- Store syslogs internally in a buffer.
- Specify the size of the buffer.
- Specify what the security appliance should do with the contents of the internal buffer when it wraps (that is, when the buffer is full). You can save the contents of the internal buffer to Flash or to an FTP server.

Table 1-2 Commands for Configuring the Logging Buffer

Purpose	Command Syntax	Description
Specify that syslog messages be saved in buffer	logging buffered <i>message_list severity_level</i> no logging buffered <i>message_list severity_level</i>	Stores syslog messages internally in a buffer. Use the <i>message_list</i> or <i>severity_level</i> options when you want only certain types of messages to be saved to the internal buffer.
Erase the contents of the logging buffer	clear logging buffer	Clears the contents of the buffer.
Specify the amount of Flash to be used	logging flash-minimum-free <i>kbytes</i> no logging flash-minimum-free <i>kbytes</i> logging flash-maximum-allocation <i>kbytes</i> no logging flash-maximum-allocation <i>kbytes</i>	Specifies the amount of Flash that can be used by the logging command for saving syslog messages. This command applies to the logging flash-bufferwrap and logging-savelog commands. Use the flash-minimum-free option to specify in kilobytes the minimum amount of Flash space that should remain available at all times. Use the flash-maximum-allocation option to specify in kilobytes the maximum amount of Flash space that can be used for saving syslog messages. Note The logging flash related commands are only available in single mode.

Table 1-2 Commands for Configuring the Logging Buffer

Purpose	Command Syntax	Description
Save buffer wraps to Flash	logging flash-bufferwrap no logging flash-bufferwrap	If enabled, buffer contents are saved to Flash when the buffer wraps (that is, when the buffer is full).
Save current contents of buffer to Flash	logging savelog filename	Saves contents of syslog buffer to Flash in a file with the specified filename. If a filename is not specified, the default timestamp format will be used for the filename. This is a privileged EXEC mode command.
Send buffer wraps to an FTP server	logging ftp-bufferwrap no logging ftp-bufferwrap	When the messages buffer is full, sends contents of buffer to the configured FTP server. Configure the FTP server with the logging ftp-server command.
	logging ftp-server ftp_server path username password no logging ftp-server ftp_server path username password	Configures the FTP server. Use options to provide necessary information about the FTP server, as follows: <ul style="list-style-type: none"> <i>ftp-server</i>—External FTP server name or IP address. <i>path</i>—Directory path on FTP server to save syslog messages. <i>username</i>—User login to FTP server. <i>password</i>—Password for username.

Managing Groups of Messages

The security appliance provides several mechanisms that enable you to configure and manage syslog messages in groups, including message severity level, message class (message source), or a custom message list that you create. Using these mechanisms, you can enter a single command that applies to small or large groups of messages.

Some examples of managing groups of messages are:

- Logging all messages with severity levels of 1, 2 and 3 to the internal buffer
- Sending all messages in the “ha” class to a particular syslog server
- Creating a list of messages that you name “high-priority,” then sending messages in this list to an e-mail address to notify system administrators of a problem

The **logging class** command enables you to specify an output location for an entire category of system messages with a single command. Classes are categories of messages that are associated with a functional area of the security appliance. For example, the “vpnc” class denotes the VPN client.

Use the *message_class* variable when you want to enter a command and apply it to all messages associated with the related functional area.

Message ID numbers are referenced by the first 3 digits of the message number. For example, 611 includes to all system messages from number 611101 to 611323. This group of messages are associated with the vpnc (VPN client) class.

Use the following commands to create message lists and to send groups of messages to an output location.

Table 1-3 Commands for Managing Groups of Messages

Command / Option	Syntax	Description
logging list	logging list <i>message_list</i> level <i>severity_level</i> [class <i>message_class</i>]	Creates custom list of messages. The <i>message_list</i> is a name that you choose to identify the list you are creating.
	no logging list <i>message_list</i> level <i>severity_level</i> [class <i>message_class</i>]	Note Do not use the names of severity levels as the name of a message list. Prohibited <i>message_list</i> names include “emergencies,” “alert,” “critical,” “error,” “warning,” “notification,” “informational,” and “debugging.” Do not use even the first three characters of these words at the beginning of a file name. For example, do not use a filename that starts with the characters “err.”
	logging list <i>message_list</i> level <i>severity_level</i> [class <i>message_class</i>] no logging list <i>message_list</i> level <i>severity_level</i> [class <i>message_class</i>]	Use this syntax option to create a message list containing all messages in a particular class that have a severity of the specified level.
logging class	logging list <i>message_list</i> message <i>syslog_id</i> - [<i>syslog_id2</i>] no logging list <i>message_list</i> message <i>syslog_id</i> - [<i>syslog_id2</i>]	Use this syntax option to create a message list containing a range of message ID numbers.
	logging class <i>message_class</i> buffered console history mail monitor trap <i>severity_level</i> no logging class <i>message_class</i> buffered console history mail monitor trap <i>severity_level</i>	Sends all messages associated with that class to the specified output location. You can further limit the number of messages sent to the output location by specifying a severity level threshold.

Values for the Message Class Variable

Table 1-4 lists the message classes and the range of message IDs in each class.

Table 1-4 Message Classes and Associated Message ID Numbers

Class	Definition	Message ID Numbers
ha	Failover (High Availability)	101, 102, 103, 104, 210, 311, 709
rip	RIP Routing	107, 312
auth	User Authentication	109, 113
bridge	Transparent Firewall	110, 220
config	Command interface	111, 112, 208, 308

Table 1-4 Message Classes and Associated Message ID Numbers (continued)

Class (continued)	Definition	Message ID Numbers
sys	System	199, 211, 214, 216, 306, 307, 315, 414, 604, 605, 606, 610, 612, 614, 615, 701, 711
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
ip	IP Stack	209, 215, 313, 317, 408
snmp	SNMP	212
vpdn	PPTP and L2TP Sessions	213, 403, 603
vpn	IKE and IPsec	316, 320, 402, 404, 501, 602, 702, 713, 714, 715
ospf	OSPF Routing	318, 409, 503, 613
np	Network Processor	319
rm	Resource Manager	321
ids	Intrusion Detection System	400, 401, 415
vpnc	VPN Client	611
webvpn	Web-based VPN	716
ca	PKI Certification Authority	717
e-mail	E-mail Proxy	719
vpnlb	VPN Load Balancing	718
vpnfo	VPN Failover	720

Modifying the Content and Format of Syslog Messages

Use the following commands to configure the security appliance to:

- Include the device ID in all syslog messages
- Include a timestamp in all syslog messages.
- Use EMBLEM format for syslog messages.

Table 1-5 *Commands for Modifying Message Content and Format*

Purpose	Command Syntax	Description
Include the device ID in syslog messages	logging device-id {hostname ipaddress <i>if_name</i> string <i>text</i> } no logging device-id {hostname ipaddress <i>if_name</i> string <i>text</i> }	If enabled, the security appliance displays the device ID in all non-EMBLEM syslog messages. If you use the ipaddress option, the device ID becomes the specified security appliance interface IP address, regardless of the interface from which the message is sent. This option provides a single consistent device ID for all messages sent from the device. Note If enabled, the device ID does not appear in EMBLEM-formatted messages or SNMP traps.
Include a timestamp in syslog messages	logging timestamp no logging timestamp	If enabled, the security appliance displays a timestamp in all syslog messages.
Modify syslog messages to use the EMBLEM format	logging emblem no logging emblem	If enabled, syslog messages appear in the EMBLEM format. Note This command does not affect syslog messages going to a syslog host. To cause syslog messages going to a host to use the EMBLEM format, use the logging host command.

Logging Command Examples

This section describes step-by-step examples that demonstrates how you can use the **logging** command. This section includes the following topics:

- [Enabling Logging, page 11](#)
- [Testing the Logging Output, page 12](#)
- [Sending Syslog Messages to the Buffer, page 13](#)
- [Sending Syslog Messages to a Syslog Server, page 14](#)
- [Sending Syslog Messages to an E-mail Address, page 15](#)
- [Sending Syslog Messages to a Telnet Console Session, page 16](#)
- [Sending Syslog Messages to an SNMP Management Station, page 17](#)
- [Disabling Specific Syslog Messages, page 18](#)
- [Viewing a List of Disabled Syslog Messages, page 18](#)
- [Reenabling Specific Disabled Syslog Messages, page 18](#)
- [Reenabling All Disabled Syslog Messages, page 18](#)

Enabling Logging

These steps enable logging; however, you must also set an output location to view the log messages. See the “[Setting the Syslog Output Location](#)” section on [page 13](#) for more information.

To enable logging, perform the following steps:

Step 1 To enable configuration mode, enter the following command:

```
enable
(Enter your password at the prompt)
configure terminal
```

Step 2 To enable logging, enter the following command:

```
logging enable
```

Step 3 To change the logging level, enter the following command:

```
logging output_destination severity_level (1-7)
```

Valid *output_destination* values are: **asdm**, **console**, **buffered**, **history**, **mail**, **monitor**, and **trap**.

Step 4 To view your logging settings, enter the following command:

```
show all
```

Testing the Logging Output

Step 1 To enable configuration mode, enter the following command:

```
enable
(Enter your password at the prompt)
configure terminal
```

Step 2 To initiate a log message to be sent to the console, enter the following command:

```
logging console 7
quit
```

This test generates the following syslog message:

```
111005: End configuration: OK
```

This message states that you exited configuration mode. “111005” is the message identifier number (see [Chapter 2, “System Log Messages,”](#) for more information about this message).

Step 3 To disable logging to the console, enter the following commands:

```
configure terminal
no logging console 7
quit
```



Note

You should only use the **logging console** command for testing. Using the console for ongoing syslog message output can degrade system performance. When the security appliance is in production, only use the **logging buffered** command to store messages, the **show logging** command to view messages, and the **clear logging buffer** command to clear the messages displayed by the **logging buffered** command.

Setting the Syslog Output Location

This section describes how to configure the security appliance to send syslog messages to the output location of your choice. The security appliance provides several output locations for sending syslog messages, including:

- An internal buffer
- One or more syslog servers
- One or more e-mail addresses
- ASDM (through the Monitoring tab)
- An SNMP management station
- Telnet and SSH sessions
- The tty console

This section includes the following topics:

- [Sending Syslog Messages to the Buffer, page 13](#)
- [Sending Syslog Messages to a Syslog Server, page 14](#)
- [Sending Syslog Messages to an E-mail Address, page 15](#)
- [Sending Syslog Messages to a Telnet Console Session, page 16](#)
- [Sending Syslog Messages to a Telnet Console Session, page 16](#)
- [Receiving SNMP Requests, page 17](#)
- [Sending SNMP Traps, page 17](#)

Sending Syslog Messages to the Buffer

To send syslog messages to the buffer, perform the following steps. This example creates a message list first in order to simplify the process of specifying multiple messages to be sent to the buffer.

- Step 1** To create a message list that includes messages with a specified severity level or message list, enter the following command:

```
logging list message_list | level severity_level [class message_class]
```

where *message_list* is the name of the file you are creating, *severity_level* is the severity level of the messages to be included in the list, and *message_class* is the category of messages to be included in the list.

For example:

```
logging list my_critical_messages level 2
```



Note Do not use the names of severity levels as the filename of a message list.

- Step 2** To add additional messages to the message list you just created, enter the following command:

```
logging list message_list message syslog_id-syslog_id2
```

where *message_list* is the name of the file that contains the list of messages you are modifying, and *syslog_id-syslog_id2* is a range of message ID numbers to be added to the list.

For example:

```
logging list my_critical_messages message 101001-102034
```

- Step 3** To specify that the messages in the message list you just created should be sent to the buffer, enter the following command:

```
logging buffered message_list
```

where *message_list* is the name of the file that contains the list of messages to be sent to the buffer.

For example:

```
logging buffered my_critical_messages
```

Sending Syslog Messages to a Syslog Server

If you send messages to a host, they are sent using either UDP or TCP. The host must run a program (known as a server) called syslogd. UNIX provides a syslog server as part of its operating system. For Windows 95 or Windows 98, obtain a syslog server from another vendor.

See the *Cisco Security Appliance Configuration Guide* for the procedure to configure **syslogd**. On the logging server, you can specify actions to execute when certain types of messages are logged; for example, sending e-mail, saving records to a log file, or displaying messages on a workstation.

To configure the security appliance to send messages to a syslog server, perform the following steps:

- Step 1** To designate a host to receive the messages, enter the following command:

```
logging host if_name ip_address [tcp[/port] | udp[/port]] [format emblem]
```

where *if_name* is the name of the host's interface, *ip_address* is the IP address of the host, and *port* is the TCP or UDP port number where the messages should be sent.

For example:

```
logging host dmz1 192.168.1.5
```

You can designate more than one host; however, you must enter a separate command for each host.

- Step 2** To set the logging level, enter the following command:

```
logging trap severity_level (1-7)
```

where *severity_level* is the severity level of the messages to be sent.

We recommend that you use the **debugging (7)** level during initial setup and during testing. Thereafter, set the level from **debugging** to **errors (3)** for production use.

- Step 3** If you want to include the device ID in each message, enter the following command:

```
logging device-id {hostname | ipaddress if_name | string text}
```

The message includes the specified device ID (either the hostname and IP address of the specified interface or a string) in messages sent to a syslog server.

- Step 4** If needed, set the logging facility to a value other than its default of 20. Most UNIX systems expect the messages to arrive at facility 20. To set the logging facility, enter the following command:
- ```
logging facility number
```
- 

## Sending Syslog Messages to an E-mail Address

To send syslog messages to an e-mail address, perform the following steps:

---

- Step 1** Specify the messages to be sent to one or more e-mail addresses. Use the message severity level or message list variables to specify which messages should be sent.
- This example uses an *message\_list* with the name “high-priority,” previously set up with the **logging list** command.

To specify the messages to be sent, enter the following command:

```
logging mail message_list|severity_level level
```

For example:

```
logging mail high-priority
```

- Step 2** To specify the source e-mail address to be used when sending syslog messages to an e-mail address, enter the following command:

```
logging from-address email_address
```

For example,

```
logging from-address xxx-001@example.com
```

- Step 3** Specify the recipient e-mail address to be used when sending syslog messages to an e-mail destination. You can configure up to five recipient addresses. You must enter each recipient separately.

To specify a recipient address, enter the following command:

```
logging recipient-address e-mail_address [level severity_level]
```

For example:

```
logging recipient-address admin@example.com
```



---

**Note** If a severity level is not specified, the default severity level is used (error condition, severity level 3).

---

- Step 4** To specify the SMTP server to be used when sending syslog messages to an e-mail destination, enter the following command:

```
smtp-server hostname
```

For example:

```
smtp-server smtp-host-1
```

---

## Sending Syslog Messages to a Telnet Console Session

To view syslog messages in a Telnet console session, perform the following steps:

- 
- Step 1** If you have not done so already, configure the security appliance to let a host on the inside interface access the security appliance.
- a. Enter the following command:
 

```
telnet ip_address [subnet_mask] [if_name]
```

For example, if a host has the IP address 192.168.1.2, the command is:

```
telnet 192.168.1.2 255.255.255.255
```
  - b. You should also set the duration that a Telnet session can be idle before security appliance disconnects the session to a value greater than the default of 5 minutes. A good value is at least 15 minutes. To set the duration of a Telnet session, enter the following command:
 

```
telnet timeout 15
```
- Step 2** Start Telnet on your host and specify the inside interface of the security appliance. When Telnet connects, the security appliance prompts you with **passwd:**.
- Step 3** Enter the Telnet password, which is **cisco** by default.
- Step 4** To enable configuration mode, enter the following command:
- ```
enable
(Enter your password at the prompt)
configure terminal
```
- Step 5** To start message logging, enter the following command:
- ```
logging monitor severity_level (1-7)
```
- Step 6** To send logs to this Telnet session, enter the following command:
- ```
terminal monitor
```
- This command enables logging only for the current Telnet session. The **logging monitor** command sets the logging preferences for all Telnet sessions, while the **terminal monitor** (and **terminal no monitor**) commands control logging for each individual Telnet session.
- Step 7** Trigger several messages by pinging a host or starting a web browser. The syslog messages then appear in the Telnet session window.
- Step 8** When done, disable this feature with the following commands:
- ```
terminal no monitor
no logging monitor
```
-

## Sending Syslog Messages to an SNMP Management Station

This section describes how to configure the security appliance to send syslog messages to an SNMP management station. It includes the following topics:

- [Receiving SNMP Requests](#), page 17
- [Sending SNMP Traps](#), page 17

### Receiving SNMP Requests

To configure the security appliance to receive requests from an SNMP management station, perform the following steps:

---

**Step 1** To set the IP address of the SNMP management station, enter the following command:

```
snmp-server host [if_name] ip_addr
```

**Step 2** Set other snmp server settings as required the following command:

```
snmp-server location text
snmp-server contact text
snmp-server community key
```

See the *Cisco Security Appliance Command Line Configuration Guide* for more information.

---

### Sending SNMP Traps

To send log messages as traps from the security appliance to an SNMP management station, perform the following steps. Note that cold start, link up, and link down generic traps are already enabled by the “[Receiving SNMP Requests](#)” procedure.

---

**Step 1** To enable SNMP traps, enter the following command:

```
snmp-server enable traps
```

**Step 2** To set the logging level, enter the following command:

```
logging history severity_level (1-7)
```

We recommend that you use the **debugging (7)** level during initial setup and during testing. Thereafter, set the level from **debugging** to a lower value for production use.

**Step 3** To disable sending syslog traps, enter the following command:

```
no snmp-server enable traps
```

---

## Disabling and Enabling Specific Syslog Messages

This section describes how to disable, reenab, or view disabled syslog messages. This section includes the following topics:

- [Disabling Specific Syslog Messages, page 18](#)
- [Viewing a List of Disabled Syslog Messages, page 18](#)
- [Reenabling Specific Disabled Syslog Messages, page 18](#)
- [Reenabling All Disabled Syslog Messages, page 18](#)

### Disabling Specific Syslog Messages

To disable specific syslog messages, enter the following command:

```
no logging message message_number
```

where *message\_number* is the specific message you want to disable.

### Viewing a List of Disabled Syslog Messages

To view a list of disabled syslog messages, enter the following command:

```
show logging message
```

### Reenabling Specific Disabled Syslog Messages

To reenab disabled syslog messages, enter the following command:

```
logging message message_number
```

where *message\_number* is the specific message you want to reenab.

### Reenabling All Disabled Syslog Messages

To reenab all disabled syslog messages, enter the following command:

```
clear config logging disabled
```

## Understanding Log Messages

This section describes the contents of system log messages for the security appliance. This section includes the following topics:

- [Log Message Format, page 19](#)
- [Severity Levels, page 19](#)
- [Variables, page 20](#)

## Log Message Format

System log messages begin with a percent sign (%) and are structured as follows:

*%PIX|ASA-Level-Message\_number: Message\_text*

See the following descriptions:

|                       |                                                                                                                                                                                                                           |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>PIX ASA</i>        | Identifies the message facility code for messages generated by the security appliance. This value is always PIX ASA.                                                                                                      |
| <i>Level</i>          | 1-7. The level reflects the severity of the condition described by the message. The lower the number, the more severe the condition. See <a href="#">Table 1-6</a> for more information.                                  |
| <i>Message_number</i> | A unique 6-digit number that identifies the message.                                                                                                                                                                      |
| <i>Message_text</i>   | A text string describing the condition. This portion of the message sometimes includes IP addresses, port numbers, or usernames. <a href="#">Table 1-7</a> lists the variable fields and the type of information in them. |



### Note

Syslog messages received at the security appliance serial console contain only the code portion of the message. When you view the message description in [Chapter 2, “System Log Messages,”](#) the description also provides the severity level.

## Severity Levels

[Table 1-6](#) lists the severity levels.

**Table 1-6 Log Message Severity Levels**

| Level Number | Level Keyword        | Description                       |
|--------------|----------------------|-----------------------------------|
| 0            | <b>emergencies</b>   | System unusable.                  |
| 1            | <b>alert</b>         | Immediate action needed.          |
| 2            | <b>critical</b>      | Critical condition.               |
| 3            | <b>error</b>         | Error condition.                  |
| 4            | <b>warning</b>       | Warning condition.                |
| 5            | <b>notification</b>  | Normal but significant condition. |
| 6            | <b>informational</b> | Informational message only.       |
| 7            | <b>debugging</b>     | Appears during debugging only.    |

[Appendix A, “Messages Listed by Severity Level”](#) lists which messages occur at each severity level.



### Note

The security appliance does not generate messages with a severity level of 0 (emergencies). This level is provided in the **logging** command for compatibility with the UNIX syslog feature, but is not used by the security appliance.

## Variables

Log messages often contain variables. [Table 1-7](#) lists most variables that are used in this guide to describe log messages. Some variables that appear in only one log message are not listed.

**Table 1-7** Variable Fields in Syslog Messages

| Variable                | Type of Information                                                                                                                                                                                                                    |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>acl_ID</i>           | An ACL name.                                                                                                                                                                                                                           |
| <i>bytes</i>            | The number of bytes.                                                                                                                                                                                                                   |
| <i>code</i>             | A decimal number returned by the message to indicate the cause or source of the error, depending on the message.                                                                                                                       |
| <i>command</i>          | A command name.                                                                                                                                                                                                                        |
| <i>command_modifier</i> | The <i>command_modifier</i> is one of the following strings: <ul style="list-style-type: none"> <li>• cmd (this string means the command has no modifier)</li> <li>• clear</li> <li>• no</li> <li>• show</li> </ul>                    |
| <i>connections</i>      | The number of connections.                                                                                                                                                                                                             |
| <i>connection_type</i>  | The connection type: <ul style="list-style-type: none"> <li>• SIGNALLING UDP</li> <li>• SIGNALLING TCP</li> <li>• SUBSCRIBE UDP</li> <li>• SUBSCRIBE TCP</li> <li>• Via UDP</li> <li>• Route</li> <li>• RTP</li> <li>• RTCP</li> </ul> |
| <i>dec</i>              | Decimal number.                                                                                                                                                                                                                        |
| <i>dest_address</i>     | The destination address of a packet.                                                                                                                                                                                                   |
| <i>dest_port</i>        | The destination port number.                                                                                                                                                                                                           |
| <i>device</i>           | The memory storage device. For example, the floppy disk, Flash memory, TFTP, the failover standby unit, or the console terminal.                                                                                                       |
| <i>econns</i>           | Number of embryonic connections.                                                                                                                                                                                                       |
| <i>elimit</i>           | Number of embryonic connections specified in the <b>static</b> or <b>nat</b> command.                                                                                                                                                  |
| <i>filename</i>         | A filename of the type security appliance image, PDM file, or configuration.                                                                                                                                                           |
| <i>ftp-server</i>       | External FTP server name or IP address.                                                                                                                                                                                                |
| <i>gateway_address</i>  | The network gateway IP address.                                                                                                                                                                                                        |
| <i>global_address</i>   | Global IP address, an address on a lower security level interface.                                                                                                                                                                     |

**Table 1-7 Variable Fields in Syslog Messages (continued)**

| <b>Variable</b>        | <b>Type of Information</b>                                                                                                                  |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <i>global_port</i>     | The global port number.                                                                                                                     |
| <i>hex</i>             | Hexadecimal number.                                                                                                                         |
| <i>inside_address</i>  | Inside (or local) IP address, an address on a higher security level interface.                                                              |
| <i>inside_port</i>     | The inside port number.                                                                                                                     |
| <i>interface_name</i>  | The name of the interface.                                                                                                                  |
| <i>IP_address</i>      | IP address in the form <i>n.n.n.n</i> , where <i>n</i> is an integer from 1 to 255.                                                         |
| <i>MAC_address</i>     | The MAC address.                                                                                                                            |
| <i>mapped_address</i>  | The translated IP address.                                                                                                                  |
| <i>mapped_port</i>     | The translated port number.                                                                                                                 |
| <i>message_class</i>   | Category of messages associated with a functional area of the security appliance.                                                           |
| <i>message_list</i>    | Name of a file you create containing a list of message ID numbers, message classes, or message severity levels.                             |
| <i>message_number</i>  | The message identification number.                                                                                                          |
| <i>nconns</i>          | Number of connections permitted for the static or xlate table.                                                                              |
| <i>netmask</i>         | The subnet mask.                                                                                                                            |
| <i>number</i>          | A number. The exact form depends on the log message.                                                                                        |
| <i>octal</i>           | Octal number.                                                                                                                               |
| <i>outside_address</i> | Outside (or foreign) IP address, an address of a host typically on a lower security level interface in a network beyond the outside router. |
| <i>outside_port</i>    | The outside port number.                                                                                                                    |
| <i>port</i>            | The TCP or UDP port number.                                                                                                                 |
| <i>privilege_level</i> | The user privilege level.                                                                                                                   |
| <i>protocol</i>        | The protocol of the packet, for example, ICMP, TCP, or UDP.                                                                                 |
| <i>real_address</i>    | The real IP address, before Network Address Translation (NAT).                                                                              |
| <i>real_port</i>       | The real port number, before NAT.                                                                                                           |
| <i>reason</i>          | A text string describing the reason for the message.                                                                                        |
| <i>service</i>         | The service specified by the packet, for example, SNMP or Telnet.                                                                           |
| <i>severity_level</i>  | The severity level of a message.                                                                                                            |
| <i>source_address</i>  | The source address of a packet.                                                                                                             |
| <i>source_port</i>     | The source port number.                                                                                                                     |
| <i>string</i>          | Text string (for example, a username).                                                                                                      |

**Table 1-7** Variable Fields in Syslog Messages (continued)

| Variable         | Type of Information                                                                                                                                                 |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>tcp_flags</i> | Flags in the TCP header such as: <ul style="list-style-type: none"> <li>• ACK</li> <li>• FIN</li> <li>• PSH</li> <li>• RST</li> <li>• SYN</li> <li>• URG</li> </ul> |
| <i>time</i>      | Duration, in the format <i>hh:mm:ss</i> .                                                                                                                           |
| <i>url</i>       | A URL.                                                                                                                                                              |
| <i>user</i>      | A username.                                                                                                                                                         |

## Other Remote Management and Monitoring Tools

This section describes the options on the security appliance that enable you to monitor the security appliance remotely with tools other than the command line. This section includes the following topics:

- [Cisco ASDM, page 1-22](#)
- [Cisco Secure Policy Manager, page 1-22](#)
- [SNMP Traps, page 1-23](#)
- [Telnet, page 1-23](#)

### Cisco ASDM

The Cisco Adaptive Security Device Manager (ASDM) is a browser-based configuration tool designed to help you set up, configure, and monitor your security appliance graphically, without requiring an extensive knowledge of the security appliance command-line interface (CLI).

### Cisco Secure Policy Manager

Cisco Secure Policy Manager (CSPM) is a security policy management system that enables you to define, distribute, enforce, and audit network-wide security policies from a central location. CSPM streamlines the tasks of managing complicated network security events, such as perimeter access control, Network Address Translation (NAT), IDS, and IPSec-based VPNs. CSPM provides system-auditing functions, including monitoring, event notification, and web-based reporting.

CSPM can receive syslog messages from the security appliance and provide notifications including e-mail, paging, and scripting for designated syslogs. CSPM also provides reports of syslogs, including the top ten users and top ten websites. These reports can be provided both on-demand and by schedule. Reports can be e-mailed or viewed remotely from an SSL-enabled web browser.

Refer to the following websites for more information:

<http://www.cisco.com/go/policymanager>

<http://www.cisco.com/univercd/cc/td/doc/product/ismg/policy/index.htm>

## SNMP Traps

The security appliance events can be reported using SNMP. This feature requires loading the Cisco SYSLOG MIB and the Cisco SMI MIB onto the SNMP management station.

## Telnet

You can log in to the security appliance console using Telnet from an internal host and monitor system status. If IPsec is enabled, you can also access the console from an external host. You can use the **debug icmp trace** and **debug sqlnet** commands from Telnet to view ICMP (ping) traces and SQL\*Net accesses.

The Telnet console session also lets you use the **logging monitor** and **terminal monitor** commands to view syslog messages, as described in the “[Sending Syslog Messages to a Telnet Console Session](#)” section on page 16.

