



Configuring Logging and SNMP

This chapter describes how to configure logging and SNMP. It also describes the contents of system log messages and the system log message format. This chapter does not provide comprehensive information about all monitoring and logging commands and options. For detailed descriptions and additional commands, see the *Cisco Security Appliance Command Reference*.

This chapter includes the following sections:

- [Configuring SNMP, page 1-1](#)
- [Configuring and Managing Logs, page 1-4](#)

Configuring SNMP

This section describes how to use SNMP and includes the following topics:

- [SNMP Overview, page 1-1](#)
- [Enabling SNMP, page 1-3](#)

SNMP Overview

The security appliance provides support for network monitoring using SNMP V1 and V2c. The security appliance supports traps and SNMP read access, but does not support SNMP write access.

You can configure the security appliance to send traps (event notifications) to a network management station (NMS), or you can use the NMS to browse the MIBs on the security appliance. MIBs are a collection of definitions, and the security appliance maintains a database of values for each definition. Browsing a MIB entails issuing an SNMP get request from the NMS. Use CiscoWorks for Windows or any other SNMP V1, MIB-II compliant browser to receive SNMP traps and browse a MIB.

[Table 1-1](#) lists supported MIBs and traps for the security appliance and, in multiple mode, for each context. You can download Cisco MIBs from the following website.

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

After you download the MIBs, compile them for your NMS.

Table 1-1 **SNMP MIB and Trap Support**

MIB or Trap Support	Description
SNMP core traps	<p>The security appliance sends the following core SNMP traps:</p> <ul style="list-style-type: none"> • authentication—An SNMP request fails because the NMS did not authenticate with the correct community string. • linkup—An interface has transitioned to the “up” state. • linkdown—An interface is down, for example, if you removed the nameif command. • coldstart—The security appliance is running after a reload.
MIB-II	<p>The security appliance supports browsing of the following groups and tables:</p> <ul style="list-style-type: none"> • system
IF-MIB	<p>The Cisco ASA supports browsing of the following tables:</p> <ul style="list-style-type: none"> • ifTable • ifXTable
RFC1213-MIB	<p>The Cisco ASA supports browsing of the following table:</p> <ul style="list-style-type: none"> • ip.ipAddrTable
SNMPv2-MIB	<p>The Cisco ASA supports browsing the following:</p> <ul style="list-style-type: none"> • snmp
ENTITY-MIB	<p>The security appliance supports browsing of the following groups and tables:</p> <ul style="list-style-type: none"> • entPhysicalTable • entLogicalTable <p>The security appliance supports browsing of the following traps:</p> <ul style="list-style-type: none"> • snmp-server enable traps entity {config-changelfru-insertlfu-remove}
CISCO-IPSEC-FLOW-MONITOR-MIB	<p>The security appliance supports browsing of the MIB.</p> <p>The security appliance supports browsing of the following traps:</p> <ul style="list-style-type: none"> • snmp-server enable traps ipsec {startlstop}
CISCO-REMOTE-ACCESS-MONITOR-MIB	<p>The security appliance supports browsing of the MIB.</p> <p>The security appliance supports browsing of the following traps:</p> <ul style="list-style-type: none"> • snmp-server enable traps remote-access {session-threshold-exceeded}
CISCO-CRYPTO-ACCELERATOR-MIB	<p>The security appliance supports browsing of the MIB.</p>
ALTIGA-GLOBAL-REG	<p>The security appliance supports browsing of the MIB.</p>
Cisco Firewall MIB	<p>The security appliance supports browsing of the following groups:</p> <ul style="list-style-type: none"> • cfwSystem <p>The information is cfwSystem.cfwStatus, which relates to failover status, pertains to the entire device and not just a single context.</p>

Table 1-1 SNMP MIB and Trap Support (Continued)

MIB or Trap Support	Description
Cisco Memory Pool MIB	The security appliance supports browsing of the following table: <ul style="list-style-type: none"> ciscoMemoryPoolTable—The memory usage described in this table applies only to the security appliance general-purpose processor, and not to the network processors.
Cisco Process MIB	The security appliance supports browsing of the following table: <ul style="list-style-type: none"> cpmCPUTotalTable
Cisco Syslog MIB	The security appliance supports the following trap: <ul style="list-style-type: none"> clogMessageGenerated You cannot browse this MIB.

Enabling SNMP

The SNMP agent that runs on the security appliance performs two functions:

- Replies to SNMP requests from NMSs.
- Sends traps (event notifications) to NMSs.

To enable the SNMP agent and identify an NMS that can connect to the security appliance, follow these steps:

-
- Step 1** To identify the IP address of the NMS that can connect to the security appliance, enter the following command:
- ```
hostname(config)# snmp-server host interface_name ip_address [trap | poll] [community text] [version 1 | 2c] [udp-port port]
```
- Specify **trap** or **poll** if you want to limit the NMS to receiving traps only or browsing (polling) only. By default, the NMS can use both functions.
- SNMP traps are sent on UDP port 162 by default. You can change the port number using the **udp-port** keyword.
- Step 2** To specify the community string, enter the following command:
- ```
hostname(config)# snmp-server community key
```
- The SNMP community string is a shared secret between the security appliance and the NMS. The key is a case-sensitive value up to 32 characters in length. Spaces are not permitted.
- Step 3** (Optional) To set the SNMP server location or contact information, enter the following command:
- ```
hostname(config)# snmp-server {contact | location} text
```
- Step 4** To enable the security appliance to send traps to the NMS, enter the following command:
- ```
hostname(config)# snmp-server enable [traps [all | feature [trap1] [trap2]] [...]]
```
- By default, SNMP core traps are enabled (**snmp**). If you do not enter a trap type in the command, **syslog** is the default. To enable or disable all traps, enter the **all** option. For **snmp**, you can identify each trap type separately. See [Table 1-1 on page 1-2](#) for a list of traps.

Step 5 To enable system messages to be sent as traps to the NMS, enter the following command:

```
hostname(config)# logging history level
```

You must also enable **syslog** traps using the preceding **snmp-server enable traps** command.

Step 6 To enable logging, so system messages are generated and can then be sent to an NMS, enter the following command:

```
hostname(config)# logging on
```

The following example sets the security appliance to receive requests from host 192.168.3.2 on the inside interface.

```
hostname(config)# snmp-server host 192.168.3.2
hostname(config)# snmp-server location building 42
hostname(config)# snmp-server contact Pat lee
hostname(config)# snmp-server community ohwhatakeyisthee
```

Configuring and Managing Logs

This section describes the logging functionality and configuration. It also describes the system log message format, options and variables.

- [Logging Overview, page 1-4](#)
- [Logging in Multiple Context Mode, page 1-5](#)
- [Enabling and Disabling Logging, page 1-5](#)
- [Configuring Log Output Destinations, page 1-7](#)
- [Filtering System Log Messages to be Sent to an Output Destination, page 1-15](#)
- [Customizing the Log Configuration, page 1-19](#)
- [Understanding System Log Messages, page 1-23](#)

Logging Overview

security appliance system logs provide 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 system log messages.

Using the logging feature, you can do the following:

- Specify which system log messages should be logged.
- Disable or change the severity level of a system log message.
- Specify one or more locations where system log 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 system log 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 internal Flash memory.
- Send log files to an FTP server.
- Save log files in internal Flash memory.
- Monitor system log messages remotely by using ASDM, Telnet and SSH sessions, or by downloading to a Web browser the contents of the internal log buffer.

You can choose to send all system log messages, or subsets of system log messages, to any or all output locations. You can filter which system log messages are sent to which locations by the severity of the system log message, the class of the system log message, or by creating a custom log message list.

Logging in Multiple Context Mode

Logging for an Cisco ASA running in multiple context mode functions somewhat differently than for an Cisco ASA running in single context mode. In single context mode, all logging messages generated by the system appear in a single log. In multiple context mode, there are two types of logs that are configured and accessed in different locations: logs that appear in individual security contexts, and a log that appears in the Admin context.

Just as each security context has its own configuration, each security context also has its own logging configuration and system message logs. A security context's message log includes messages related to features that are enabled for that context. For example, context logs include messages related to security policies, routing, logging, and configuration changes for that context. Like an Cisco ASA running in single context mode, logging in security contexts is not enabled by default. If you want logs to be kept for a security context, you must access the security context and configure logging. Similarly, you must access the security context in order to view log messages for that context.

In contrast, logs in the Admin context contain messages related to the overall physical device and overall system configuration. This includes messages related to events and features configured in the Admin context, such as failover, and it also includes messages related to events and features configured in the system execution space, such as interface settings. In the Admin context, you can only view the administration log; you cannot view logs for individual security contexts in the Admin context. If you want logs to be kept for the Admin context, you must access the Admin context and configure logging. Similarly, you must access the Admin context in order to view log messages for that context.

You cannot configure logging or view any logging information in the system execution space.

You can configure logging so that each messages includes the logging device ID for a security context; if you do so, each message includes the name of the context in which the message occurred. If you enable the logging device ID for the Admin context, messages that originate in the system execution space use a device ID of **system**; messages that originate in the Admin context use a device ID of **Admin**. For more information about enabling logging device IDs, see [Including the Device ID in System Log Messages, page 1-19](#).

For more information about security contexts, see the chapter titled "Enabling Multiple Context Mode" in the *Cisco Security Appliance Command Line Configuration Guide*.

Enabling and Disabling Logging

This section describes how to enable and disable logging on the security appliance. It includes the following sections:

- [Enabling Logging to All Configured Output Destinations, page 1-6](#)

- [Disabling Logging to All Configured Output Destinations, page 1-6](#)
- [Viewing the Log Configuration, page 1-6](#)

Enabling Logging to All Configured Output Destinations

The following steps enable logging; however, you must also specify at least one output destination so that you can view or save the logged messages. If you do not specify an output destination, the security appliance does not save system log messages generated when events occur.

For more information about configuring log output destinations, see the “[Configuring Log Output Destinations](#)” section on page 1-7.

To enable logging, complete the following steps:

-
- Step 1** To access configuration mode, enter the following command:
- ```
hostname># config t
```
- Step 2** To start logging, enter the following command:
- ```
hostname(config)# logging enable
```
- Step 3** To view what types of logging are enabled, enter the following command:
- ```
hostname(config)# show logging
Syslog logging: enabled
 Facility: 20
 Timestamp logging: disabled
 Standby logging: disabled
 Deny Conn when Queue Full: disabled
 Console logging: disabled
 Monitor logging: disabled
 Buffer logging: disabled
 Trap logging: disabled
 History logging: disabled
 Device ID: disabled
 Mail logging: disabled
 ASDM logging: disabled
```

## Disabling Logging to All Configured Output Destinations

To disable all logging to all configured log output destinations, enter the following command:

```
hostname(config)# no logging enable
```

## Viewing the Log Configuration

To view the running log configuration, enter the following command:

```
hostname(config)# show logging
```

The output of the **show logging** command is similar to the following:

```
Syslog logging: enabled
 Facility: 16
 Timestamp logging: disabled
 Standby logging: disabled
 Deny Conn when Queue Full: disabled
 Console logging: disabled
```

```

Monitor logging: disabled
Buffer logging: disabled
Trap logging: level errors, facility 16, 3607 messages logged
 Logging to infrastructure 10.1.2.3
History logging: disabled
Device ID: 'inside' interface IP address "10.1.1.1"
Mail logging: disabled
ASDM logging: disabled

```

Definitions of the status line entries are as follows:

| Logging Status Line       | Description                                                                                                                       |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| System Log logging        | Status of overall system logging.                                                                                                 |
| Facility                  | Logging facility used for system log messages sent to syslog servers.                                                             |
| Timestamp logging         | Indicates whether timestamps are included in system log messages.                                                                 |
| Standby logging           | If enabled, ensures that the system log messages of the failover standby security appliance stay synchronized if failover occurs. |
| Deny Conn when Queue Full | If enabled, denies all traffic when the log queue is full.                                                                        |
| Console logging           | Indicates whether the console has been enabled as a log output destination.                                                       |
| Monitor logging           | Indicates whether logging on the console can be viewed via a Telnet or SSH session.                                               |
| Buffer logging            | Indicates whether the internal log buffer is enabled as a log output destination.                                                 |
| Trap logging              | Indicates whether logs are enabled to be sent to one or more syslog servers.                                                      |
| History logging           | Indicates whether logs are enabled to be sent to an SNMP management station.                                                      |
| Device ID                 | Indicates whether the device ID is included in system log messages.                                                               |
| Mail logging              | Indicates whether logs are enabled to be sent to one or more e-mail addresses.                                                    |
| ASDM logging              | Indicates whether logs are enabled to be sent to ASDM.                                                                            |

## Configuring Log Output Destinations

This section describes how to specify where the security appliance should save or send the log messages it generates, and it includes the following topics:

- [Log Output Destination Overview, page 1-8](#)
- [Designating a Syslog Server as an Output Destination, page 1-8](#)
- [Designating an E-mail Address as an Output Destination, page 1-10](#)
- [Designating ASDM as an Output Destination, page 1-11](#)
- [Viewing Logs Using a Telnet Session, page 1-12](#)
- [hostname\(config\)# no logging monitor, page 1-12](#)

## Log Output Destination Overview

To view logs generated by the security appliance, you must specify a log output destination. If you enable logging without specifying a log output destination, the security appliance generates messages but does not save them to a location from which you can view them.

You can configure the security appliance to send logs to the following locations:

- One or more syslog servers
- One or more e-mail addresses
- ASDM (Adaptive Security Device Manager)
- Telnet sessions
- Internal log buffer

## Designating a Syslog Server as an Output Destination

This section describes how to configure the security appliance to send logs to a syslog server.

Configuring the security appliance to send logs to a syslog server enables you to archive logs, limited only by the available disk space on the server, and it enables you to manipulate log data after it is saved. For example, you could specify actions to be executed when certain types of system log messages are logged, extract data from the log and save the records to another file for reporting, or track statistics using a site-specific script.

The syslog server must run a program (known as a server) called `syslogd`. UNIX provides a syslog server as part of its operating system. For Windows 95 and Windows 98, obtain a `syslogd` server from another vendor.

You can configure the security appliance to send data to a syslog server using either UDP or TCP, but not both. If you specify TCP, the security appliance discovers when the syslog server fails and discontinues sending logs. If you specify UDP, the security appliance continues to send logs regardless of whether the syslog server is operational.

You can enable the logging timestamp if you want each log message to contain a timestamp. If you choose UDP for sending logs to the syslog server, you can enable EMBLEM-format logging for each syslog server.

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

---

**Step 1** To designate a syslog server to receive the logs, enter the following command:

```
hostname(config)# logging host if_name ip_address {[tcp/port] | udp/port]} [format emblem]
```

where

**format emblem**—enables EMBLEM format logging for the syslog server. (UDP only).

*interface\_name*—specifies the interface on which the syslog server resides.

*port*—specifies the port that the syslog server listens to for system log messages. Valid port values are 1025 through 65535, for either protocol. To display the *port* and *protocol* values you used when entering commands previously, use the **show running-config logging** command and find the command in the listing—the TCP protocol is listed as 6 and the UDP protocol is listed as 17.

*ip\_address*—specifies the IP address of the syslog server.

**tcp**—specifies that the security appliance should use TCP to send system log messages to the syslog server.

**udp**—specifies that the security appliance should use TCP to send system log messages to the syslog server.

For example:

```
hostname(config)# logging host dmz1 192.168.1.5
```

If you want to designate more than one syslog server as output destinations, enter a new command for each syslog server.

**Step 2** To specify which system log messages should be sent to the syslog server, enter the following command:

```
hostname(config)# logging trap {severity_level (1-7) | message_list}
```

where

*severity\_level*—specifies the severity levels of messages to be sent to the syslog server. For example, if you set the level to 3, then the security appliance sends system log messages for level 3, 2, 1, and 0. You can specify either the number (for example, 2) or the name (for example, critical).

For more information about message severity levels, see [Severity Levels, page 1-24](#).

*message\_list*—specifies a customized message list that identifies the system log messages to send to the syslog server. For information about creating custom message lists, see [Filtering System Log Messages with Custom Message Lists, page 1-17](#).

The following example specifies that the security appliance should send to the syslog server all system log messages with a severity level of level 3 (errors) and higher. The security appliance will send messages with the severity of 3, 2, and 1.

```
hostname(config)# logging trap errors
```

**Step 3** If you want the device ID to be included in each system log message sent to the server, enter the following command:

```
hostname(config)# logging device-id {hostname | ipaddress if_name | string text}
```

The system log message includes the specified device ID (either the hostname and IP address of the specified interface or a string) in system log 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 system log messages to arrive at facility 20.)

To modify the logging facility setting, enter the following command:

```
hostname(config)# logging facility number
```

For example:

```
hostname(config)# logging facility 16
```

**Step 5** To see the result of the configuration changes made, enter the following command:

```
hostname(config)# show logging
```

The following example shows the output of the **show logging** command:

```
Syslog logging: enabled
 Facility: 16
 Timestamp logging: disabled
 Standby logging: disabled
 Deny Conn when Queue Full: disabled
 Console logging: disabled
 Monitor logging: disabled
 Buffer logging: disabled
```

```

Trap logging: level errors, facility 16, 3607 messages logged
 Logging to infrastructure 10.1.2.3
History logging: disabled
Device ID: 'inside' interface IP address "10.1.1.1"
Mail logging: disabled
ASDM logging: disabled

```

---

## Designating an E-mail Address as an Output Destination

You can configure the security appliance to send some or all system log messages to an e-mail address. When sent by e-mail, a system log message appears in the subject line of the e-mail message. For this reason, we recommend configuring this option to notify administrators of system log messages with high severity levels, such as critical, alert, and emergency.

To designate an e-mail address as an output destination, perform the following steps:

- Step 1** Specify the system log messages to be sent to one or more e-mail addresses. Use the system log message severity level or system log message list variables to specify which system log messages should be sent.

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

```
hostname(config)# logging mail {message_list|severity_level level}
```

The following example uses a *message\_list* with the name “high-priority,” previously set up with the **logging list** command.

```
hostname(config)# logging mail high-priority
```

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

```
hostname(config)# logging from-address email_address
```

For example:

```
hostname(config)# logging from-address xxx-001@example.com
```

- Step 3** Specify the recipient e-mail address to be used when sending system log 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:

```
hostname(config)# logging recipient-address e-mail_address [level severity_level]
```

For example:

```
hostname(config)# 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 system log messages to an e-mail destination, enter the following command:

```
hostname(config)# smtp-server hostname
```

For example:

```
hostname(config)# smtp-server smtp-host-1
```

## Designating ASDM as an Output Destination

You can configure the security appliance to send system log messages to the ASDM. The security appliance sets aside a buffer area for system log messages waiting to be sent to ASDM and saves messages in the buffer as they occur. The ASDM log buffer is a different buffer than the internal log buffer. For information about the internal log buffer, see [Log Buffer Overview, page 1-13](#).

When the ASDM log buffer is full, security appliance deletes the oldest system log message to make room in the buffer for new system log messages. To control the number of system log messages retained in the ASDM log buffer by changing the size of the buffer.

To specify ASDM as an output destination, perform the following steps:

**Step 1** To specify which system log messages should go to ASDM, enter the following command:

```
hostname(config)# logging asdm {message_list|severity_level}
```

Command option descriptions are as follows:

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>level</i>        | Sets the maximum level for system log messages. For example, if you set the level to 3, then the security appliance generates system log messages for level 3, 2, 1, and 0. You can specify either the number or the name, as follows: <ul style="list-style-type: none"> <li>• <b>0</b> or <b>emergencies</b>—System unusable.</li> <li>• <b>1</b> or <b>alerts</b>—Take immediate action.</li> <li>• <b>2</b> or <b>critical</b>—Critical condition.</li> <li>• <b>3</b> or <b>errors</b>—Error.</li> <li>• <b>4</b> or <b>warnings</b>—Warning.</li> <li>• <b>5</b> or <b>notifications</b>—Normal but significant condition.</li> <li>• <b>6</b> or <b>informational</b>—Information.</li> <li>• <b>7</b> or <b>debugging</b>—Debug messages, log FTP commands, and WWW URLs.</li> </ul> |
| <i>message_list</i> | Specifies the list that identifies the system log messages to send to the ASDM log buffer. For information about creating lists, see <a href="#">Filtering System Log Messages with Custom Message Lists, page 1-17</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

The following example shows how enable logging and send to the ASDM log buffer system log messages of severity levels 0, 1, and 2.

```
hostname(config)# logging asdm 2
```

**Step 2** To specify the number of system log messages retained in the ASDM log buffer, use the **logging asdm-buffer-size** command in global configuration mode, as follows:

```
hostname(config)# logging asdm-buffer-size num_of_msgs
```

where *num\_of\_msgs* specifies the number of system log messages that the security appliance retains in the ASDM log buffer.

The following example shows how to set the ASDM log buffer size to 200 system log messages.

```
hostname(config)# logging asdm-buffer-size 200
```

---

To erase the current contents of the ASDM log buffer, enter the following command:

```
hostname(config)# clear logging asdm
```

## Viewing Logs Using a Telnet Session

To view syslog messages in a Telnet session, follow these 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 by performing the following steps.
- a. To specify the IP address and interface name, enter the following command:
 

```
hostname(config)# telnet ip_address [subnet_mask] [if_name]
```

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

```
hostname(config)# telnet 192.168.1.2 255.255.255.255
```
  - b. 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, which you can set as follows:
 

```
hostname(config)# telnet timeout 15
```
- Step 2** Start Telnet on your host and specify the inside interface of the security appliance.
- Step 3** Enter the Telnet password, which is **cisco** by default.
- Step 4** To enable configuration mode, enter the following command:
- ```
hostname(config)# enable
```
- (Enter your password at the prompt)
- ```
hostname(config)# configure terminal
```
- Step 5** To start message logging, enter the following command:
- ```
hostname(config)# logging monitor level (1-7)
```
- Step 6** To send logs to this Telnet session, enter the following command:
- ```
hostname(config)# 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 some events 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:
- ```
hostname(config)# terminal no monitor
hostname(config)# no logging monitor
```

Designating the Log Buffer as an Output Destination

This section describes how to configure the security appliance to save system log messages in the internal log buffer, and it includes the following topics:

- [Enabling the Log Buffer as an Output Destination, page 1-13](#)
- [Specifying What Happens When the Log Buffer Wraps, page 1-14](#)
- [Saving the Contents of the Log Buffer to Internal Flash Memory, page 1-15](#)
- [Clearing the Contents of the Log Buffer, page 1-15](#)

Log Buffer Overview

If configured as an output destination, the log buffer serves as a temporary storage location for system log messages. New messages are appended to the end of the listing. When the buffer is full, that is, when the buffer wraps, old messages are overwritten as new messages are generated. If you want to save log messages, you can configure the security appliance to save the buffer contents to an FTP server or to internal Flash memory each time the buffer fills so that old messages are not overwritten.

The log buffer size determines how many messages can be held in the buffer before it wraps. The default log buffer size is 4 KB.

When you enable the log buffer as an output destination, you can also specify which messages should be saved. Otherwise, all messages are saved in the log buffer as they are generated. You can configure the security appliance to select messages to be saved based on their severity level or based on a set of criteria that you specify in a customized message list. For information about limiting which messages are saved, see [Filtering System Log Messages to be Sent to an Output Destination, page 1-15](#).

Enabling the Log Buffer as an Output Destination

The following procedure describes how to enable the log buffer as a log output destination and how to configure optional log buffer settings.

- Step 1** To enable the security appliance to save system log messages to the log buffer and specify which messages should be saved in the log buffer, enter the following command:

```
hostname(config)# logging buffered {level | message_list}
```

where *level* represents the severity level of messages to be saved and *message_list* is the name of a customized list that is used to select messages to be saved in the log buffer.

For the *level* option, specify the severity level either by its number (such as 3) or its name (such as error), both of which select messages of that severity level and higher. This means that if you specify severity level 3, messages with severity levels of 3, 2 and 1 will be saved in the log buffer.

For example, to specify that messages with severity levels 1 and 2 should be saved in the log buffer, enter one of the following commands:

```
hostname(config)# logging buffered critical
```

or

```
hostname(config)# logging buffered level 2
```

For the *message_list* option, specify the name of a message list containing criteria for selecting messages to be saved in the log buffer.

```
hostname(config)# logging buffered notif-list
```

You can create a custom message list with the **logging list** command. For information about how to create a customized message list, see [Filtering System Log Messages with Custom Message Lists, page 1-17](#).

Step 2 (Optional) To change the size of the log buffer, enter the following command:

```
hostname(config)# logging buffer-size bytes
```

where the *bytes* option sets the amount of memory used for the log buffer, in bytes. For example, if you specify 8192, the security appliance uses 8 KB of memory for the log buffer.

The following example specifies that the security appliance uses 16 KB of memory for the log buffer:

```
hostname(config)# logging buffer-size 16384
```

Specifying What Happens When the Log Buffer Wraps

Unless configured otherwise, the security appliance address messages to the log buffer on a continuing basis, overwriting old messages when the buffer is full. If you want to keep a history of logs, you can configure the security appliance to send the buffer contents to another output location each time the buffer fills. Buffer contents can be saved either to internal Flash memory or to an FTP server.

When saving the buffer content to another location, the security appliance creates log files with names that use a default time-stamp format, as follows:

```
LOG-YYYY-MM-DD-HHMMSS.TXT
```

where *YYYY* is the year, *MM* is the month, *DD* is the day of the month, and *HHMMSS* is the time in hours, minutes, and seconds.

While the security appliance writes the log buffer contents to internal Flash memory or an FTP server, it continues saving new messages to the log buffer.

To specify that messages in the log buffer should be saved to internal Flash memory each time the buffer wraps, enter the following command:

```
hostname(config)# logging flash-bufferwrap
```

To specify that messages in the log buffer should be saved to an FTP server each time the buffer wraps, perform the following steps:

Step 1 To enable the security appliance to send the log buffer contents to an FTP server every time the buffer wraps, enter the following command:

```
hostname(config)# logging ftp-bufferwrap
```

Step 2 To provide details about the FTP server, entering the following command:

```
hostname(config)# logging ftp-server {server_address | server_hostname} path username password
```

where

server_address—Specifies the external FTP server's IP address

server_hostname—Specifies the external FTP server’s IP hostname

path—Specifies the directory path on the FTP server where the log buffer data is to be saved. This path is relative to the FTP root directory. For example: `/security_appliances/syslogs/appliance107`

username—Specifies a username that is valid for logging into the FTP server

password—Specifies the password for the username specified

The following example command specifies the server name `logserver-352`, the path `/syslogs`, the username `logsupervisor`, and the password `1luvMy10gs`.

```
hostname(config)# logging ftp-server logserver-352 /syslogs logsupervisor 1luvMy10gs
```

Saving the Contents of the Log Buffer to Internal Flash Memory

At any time, you can save the contents of the buffer to internal Flash memory. To save the current contents of the log buffer to internal Flash memory, issue the following command:

```
hostname(config)# logging savelog [savefile]
```

For example, the following example saves the contents of the log buffer to internal Flash memory using the file name `latest-logfile.txt`:

```
hostname(config)# logging savelog latest-logfile.txt
```

Clearing the Contents of the Log Buffer

To erase the contents of the log buffer, enter the following command:

```
hostname(config)# clear logging buffer
```

Filtering System Log Messages to be Sent to an Output Destination

This section describes how to specify which system log messages should go to a particular output destination. It includes the following topics:

- [Message Filtering Overview, page 1-15](#)
- [Filtering System Log Messages by Class, page 1-16](#)
- [Filtering System Log Messages with Custom Message Lists, page 1-17](#)

Message Filtering Overview

You can filter generated system log messages so that only certain system log messages are sent to a particular output destination. For example, you could configure the security appliance to send all system log messages to one output destination and also to send a subset of those system log messages to a different output destination.

Specifically, you can configure the security appliance so that system log messages are directed to an output destination according to the following:

- System log message ID number
- System log message severity level
- System log message class (equivalent to a functional area of the security appliance)

- System log message list that you create

For example, you could configure the security appliance to send to the internal log buffer all system log messages with severity levels of 1, 2 and 3, send all system log messages in the “ha” class to a particular syslog server, or create a list of messages that you name “high-priority” that are sent to an e-mail address to notify system administrators of a possible problem.

Filtering System Log Messages by Class

The system log message class provides a method of categorizing system log messages by type, equivalent to a feature or function of the security appliance. For example, the “vpnc” class denotes the VPN client.

With logging classes, you can specify an output location for an entire category of system log messages with a single command.

You can use system message classes in two ways:

- Issue the **logging class** command to specify an output location for an entire category of system log messages.
- Use the *message_class* variable when creating a custom list of system log messages to include that entire class of system log messages in the custom list.

All system log messages in a particular class share the same initial 3 digits in their system log message ID numbers. For example, all system log message IDs that begin with the digits 611 are associated with the vpnc (VPN client) class. System log messages associated with the VPN client feature range from 611101 to 611323.

Sending All Messages in a Class to a Specified Output Destination

To configure the security appliance to send an entire system log message class to a configured output destination, enter the following command:

```
hostname(config)# logging class message_class {buffered | console | history | mail |
monitor | trap} [severity_level]
```

where:

message_class—specifies a class of system log messages to be sent to the specified output destination. See [Table 1-2](#) for a list of system log message classes.

buffered | console | history | mail | monitor | trap—specifies the output destination to which system log messages in this class should be sent. Select one destination per command line entry. If you want to specify that a class should go to more than one destination, enter a new command for each output destination.

severity_level—further restricts the system log messages to be sent to the output destination by specifying a severity level. For more information about message severity levels, see [Severity Levels, page 1-24](#).

The following example specifies that all system log messages related to the class ha (high availability, also known as failover) with a severity level of 1 (alerts) should be sent to the internal logging buffer.

```
hostname(config)# logging ha buffered alerts
hostname(config)#
```

Table 1-2 lists the system log message classes and the ranges of system log message IDs associated with each class.

Table 1-2 System Log Message Classes and Associated Message ID Numbers

Class	Definition	System Log 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
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
npssl	NP SSL	725

Filtering System Log Messages with Custom Message Lists

Creating a custom message list is a flexible way to exercise fine control over which system log messages are sent to which output destination. In a custom system log message list, you specify groups of system log messages using any or all of the following criteria: severity level, message IDs, ranges of system message IDs, or by message class.

For example, message lists can be used to:

- Select system log messages with severity levels of 1 and 2 and send them to one or more e-mail addresses.
- Select all system log messages associated with a message class (such as “ha”) and save them to the internal buffer.

A message list can include multiple criteria for selecting messages. However, you must add each message selection criteria with a new command entry. It is possible to create a message list containing overlapping message selection criteria. If two criteria in a message list select the same message, the message is logged only once.

**Note**

Do not use the names of severity levels as the name of a system log message list. Prohibited *message_list* names include “emergencies,” “alert,” “critical,” “error,” “warning,” “notification,” “informational,” and “debugging.” Similarly, do not use 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.”

To create a customized list that the security appliance can use to select messages to be saved in the log buffer, perform the following steps:

Step 1 Create a message list containing criteria for selecting messages by entering the following command:

```
hostname(config)# logging list {message_list |
[severity_level|message_class|message_ID|range_of_IDs]}
```

where

message_list—specifies the name of the list containing message selection criteria

severity_level—specifies that all messages with the specified severity level should go to the log buffer

message_class—specifies that all messages associated with the specified message class should be saved in the log buffer

message_ID—specifies an individual system log message ID number

range_of_IDs—specifies a range of message ID numbers (for example, 103401-103599)

The following example creates a message list named *notif-list* that specifies messages with a severity level of 3 or higher should be saved in the log buffer:

```
hostname(config)# logging list notif-list level 3
```

Step 2 (Optional) If you want to add more criteria for message selection to the list, enter the same command as in the previous step specifying the name of the existing message list and the additional criterion. Enter a new command for each criterion you want to add to the list.

The following example adds criteria to the message list: a range of message ID numbers, and the message class *ha* (high availability or failover). See [Filtering System Log Messages by Class, page 1-16](#) for more information about message classes.

```
hostname(config)# logging list notif-list 104024-105999
hostname(config)# logging list my-list level critical
hostname(config)# logging list notif-list class ha
(config)# logging list my-list level warning class vpn
```

The preceding example states that system log messages that match the criteria specified will be sent to the log buffer. The specified criteria for system log messages to be included in the list are:

- System log message IDs that fall in the range of 100100 to 100110
- All system log messages with critical level or higher (emergency, alert, or critical)
- All VPN class system log messages with warning level or higher (emergency, alert, critical, error, or warning)

A system log message is logged if it satisfies any of these conditions. If a system log satisfies more than one of the conditions, the message is logged only once.

Customizing the Log Configuration

This section describes other options for fine tuning the logging configuration. It includes the following topics:

- [Configuring the Logging Queue, page 1-19](#)
- [Including the Date and Time in System Log Messages, page 1-19](#)
- [Including the Device ID in System Log Messages, page 1-19](#)
- [Generating System Log Messages in EMBLEM Format, page 1-20](#)
- [Disabling a System Log Message, page 1-21](#)
- [Changing the Severity Level of a System Log Message, page 1-21](#)
- [Changing the Amount of Internal Flash Memory Available for Logs, page 1-22](#)

Configuring the Logging Queue

The Cisco ASA has a fixed number of blocks in memory that can be allocated for buffering system log messages while they are waiting to be sent to the configured output destination. The number of blocks required depends on the length of the system log message queue and the number of syslog servers specified.

To specify the number of system log messages the security appliance can hold in its queue before sending them to the configured output destination, enter the following command:

```
hostname(config)# logging queue message_count
```

where the *message_count* variable specifies the number of system log messages that can remain in the system log message queue while awaiting processing. The default is 512 system log messages. A setting of 0 (zero) indicates unlimited system log messages, that is, the queue size is limited only by block memory availability.

To view the queue and queue statistics, enter the following command:

```
hostname(config)# show logging queue
```

Including the Date and Time in System Log Messages

To specify that system log messages should include the date and time that the system log messages was generated, enter the following command:

```
hostname(config)# logging timestamp
```

Including the Device ID in System Log Messages

To configure the security appliance to include a device ID in non-EMBLEM-format system log messages, enter the following command:

```
hostname(config)# logging device-id {context-name | hostname | ipaddress interface_name |
string text}
```

where

context-name—indicates that the name of the current context should be used as the device ID (applies only to security appliances running in multiple context mode only).

hostname—specifies that the hostname of the security appliance should be used as the device ID.

ipaddress interface_name—specifies that the IP address of the interface specified as *interface_name* should be used as the device ID.

If you use the **ipaddress** option, the device ID becomes the specified security appliance interface IP address, regardless of the interface from which the system log message is sent. This keyword provides a single, consistent device ID for all system log messages that are sent from the device.

string text—specifies that the characters entered in the *text* option should be used as the device ID. The string contain as many as 16 characters. You cannot use white space characters or any of the following characters in *text*:

- & (ampersand)
- ' (single quote)
- " (double quote)
- < (less than)
- > (greater than)
- ? (question mark)



Note

If enabled, the device ID does not appear in EMBLEM-formatted system log messages or SNMP traps.

The following example enables the logging device ID for the security appliance:

```
hostname(config)# logging device-id hostname
```

The following example enables the logging device ID for a security context on the security appliance:

```
hostname(config)# logging device-id context-name
```

If you enable the logging device ID for the Admin context in multiple context mode, 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.

Generating System Log Messages in EMBLEM Format

To use the EMBLEM format for system log messages sent to destinations other than a syslog server, enter the following command:

```
hostname(config)# logging emblem
```

To use the EMBLEM format for system log messages sent to a syslog server over UDP, specify the **format emblem** option when you configure the syslog server as a n output destination. Enter the following command:

```
hostname(config)# logging host interface_name ip_address {tcp[/port] | udp[/port]}
[format emblem]
```

where

interface_name and *IP_address* specifies the syslog server to receive the system log messages, **tcp**[/port] and **udp**[/port] indicate the protocol and port that should be used, and **format emblem** enables EMBLEM formatting for messages sent to the syslog server.

The Cisco ASA can send system log messages using either the UDP or TCP protocol; however, you can enable the EMBLEM format only for messages sent over UDP. The default protocol and port are UDP/514.

For example:

```
hostname(config)# logging host interface_1 122.243.006.123 udp format emblem
```

Disabling a System Log Message

To prevent the security appliance from generating a particular system log message, enter the following command:

```
hostname(config)# no logging message message_number
hostname(config)#
```

For example:

```
hostname(config)# no logging message 113019
hostname(config)#
```

To reenale a disabled system log message, enter the following command:

```
hostname(config)# logging message message_number
```

For example:

```
hostname(config)# logging message 113019
hostname(config)#
```

To see a list of disabled system log messages, enter the following command:

```
hostname(config)# show logging message
```

To reenale logging of all disabled system log messages, enter the following command:

```
hostname(config)# clear config logging disabled
```

Changing the Severity Level of a System Log Message

To specify the logging level of a system log message, enter the following command:

```
hostname(config)# logging message message_ID level severity_level
```

The following example modifies the severity level of system log message ID 113019 from 4 (warnings) to 5 (notifications):

```
hostname(config)# logging message 113019 level 5
hostname(config)#
```

To reset the logging level of a system log message to its default level, enter the following command.

```
hostname(config)# logging message message_ID level severity_level
```

The following example modifies the severity level of system log message ID 113019 to its default value of 4 (warnings).

```
hostname(config)# no logging message 113019 level 5
hostname(config)#
```

To see a list of system log messages with modified severity levels, enter the following command:

```
hostname(config)# show logging message
```

To reset the severity level of all modified system log messages back to their defaults, enter the following command:

```
hostname(config)# clear config logging level
hostname(config)#
```

The series of commands in the following example illustrates the use of the **logging message** command to control both whether a system log message is enabled and the severity level of the system log message.

```
hostname(config)# show logging message 403503
syslog 403503: default-level errors (enabled)

hostname(config)# logging message 403503 level 1
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)

hostname(config)# no logging message 403503
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (disabled)

hostname(config)# logging message 403503
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)

hostname(config)# no logging message 403503 level 3
hostname(config)# show logging message 403503
syslog 403503: default-level errors (enabled)
```

Changing the Amount of Internal Flash Memory Available for Logs

You can cause the security appliance to save the contents of the log buffer to Internal flash memory in two ways:

- Configure logging so that the contents of the log buffer are saved to internal Flash memory each time the buffer wraps
- Enter a command instructing the security appliance to save the current contents of the log buffer to internal Flash memory immediately

By default, the security appliance can use up to 1 MB of internal Flash memory for log data. The default minimum amount of internal Flash memory that must be free for the security appliance to save log data is 3 MB.

If a log file being saved to internal Flash memory would cause the amount of free internal Flash memory to fall below the configured minimum limit, the security appliance deletes the oldest log files to ensure that the minimum amount of memory remains free after saving the new log file. If there are no files to delete or if, after all old files are deleted, free memory would still be below the limit, the security appliance fails to save the new log file.

To modify the settings for the amount of internal Flash memory available for logs, complete the following steps:

- Step 1** To specify the maximum amount of internal Flash memory available for saving log files, enter the following command:

```
hostname(config)# logging flash-maximum-allocation kbytes
```

where *kbytes* specifies the maximum amount of internal Flash memory, in kilobytes, that can be used for saving log files.

The following example sets the maximum amount of internal Flash memory that can be used for log files to approximately 1.2 MB:

```
hostname(config)# logging flash-maximum-allocation 1200
```

- Step 2** To specify the minimum amount of internal Flash memory that must be free for the security appliance to save a log file, enter the following command:

```
hostname(config)# logging flash-minimum-free kbytes
```

where *kbytes* specifies the minimum amount of internal Flash memory, in kilobytes, that must be available before the security appliance saves a new log file.

The following example specifies that the minimum amount of free internal Flash memory must be 4000 KB before the security appliance can save a new log file:

```
hostname(config)# logging flash-minimum-free 4000
```

Understanding System Log Messages

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

- [System Log Message Format, page 1-23](#)
- [Severity Levels, page 1-24](#)
- [Variables Used in System Log Messages, page 1-24](#)

System Log Message Format

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

```
%PIX|ASA Level Message_number: Message_text
```

Field descriptions are as follows:

<i>PIX ASA</i>	Identifies the system log message facility code for messages generated by the Cisco ASA. This value is always PIX ASA.
<i>Level</i>	1-7. The level reflects the severity of the condition described by the system log message. The lower the number, the more severe the condition. See Table 1-3 for more information.
<i>Message_number</i>	A unique 6-digit number that identifies the system log message.
<i>Message_text</i>	A text string describing the condition. This portion of the system log message sometimes includes IP addresses, port numbers, or usernames. Table 1-4 lists the variable fields and the type of information in them.

Severity Levels

Table 1-3 lists the system log message severity levels.

Table 1-3 System Log Message Severity Levels

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



Note

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

Variables Used in System Log Messages

System log messages often contain variables. Table 1-4 lists most variables that are used in this guide to describe system log messages. Some variables that appear in only one system log message are not listed.

Table 1-4 Variable Fields in System Log 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 system log message to indicate the cause or source of the error, depending on the system log 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"> • cmd (this string means the command has no modifier) • clear • no • show
<i>connections</i>	The number of connections.

Table 1-4 Variable Fields in System Log Messages (Continued)

Variable	Type of Information
<i>connection_type</i>	The connection type: <ul style="list-style-type: none"> • SIGNALLING UDP • SIGNALLING TCP • SUBSCRIBE UDP • SUBSCRIBE TCP • Via UDP • Route • RTP • RTCP
<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, internal 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 static or nat command.
<i>filename</i>	A filename of the type Cisco ASA image, ASDM 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.
<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 system log messages associated with a functional area of the security appliance.
<i>message_list</i>	Name of a file you create containing a list of system log message ID numbers, classes, or severity levels.
<i>message_number</i>	The system log message ID.

Table 1-4 Variable Fields in System Log Messages (Continued)

Variable	Type of Information
<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 system log message.
<i>octal</i>	Octal number.
<i>outside_address</i>	Outside (or foreign) IP address, an address of a syslog server 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 system log message.
<i>service</i>	The service specified by the packet, for example, SNMP or Telnet.
<i>severity_level</i>	The severity level of a system log 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).
<i>tcp_flags</i>	Flags in the TCP header such as: <ul style="list-style-type: none"> • ACK • FIN • PSH • RST • SYN • URG
<i>time</i>	Duration, in the format <i>hh:mm:ss</i> .
<i>url</i>	A URL.
<i>user</i>	A username.