CHAPTER 42

Monitoring the Security Appliance

This chapter describes how to monitor the security appliance, and includes the following sections:

Using SNMP

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

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 42-1 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.

Note In software versions 7.2(1), 8.0(2), and later, the SNMP information refreshes about every five seconds. As a result, we recommend that you wait for at least five seconds between consecutive polls.

Table 42-1 SNMP MIB and Trap Support

MIB or Trap Support	Description
SNMP core traps	The security appliance sends the following core SNMP traps: • 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	The security appliance supports browsing of the following groups and tables: • system
IF-MIB	The security appliance supports browsing of the following tables: • ifTable • ifXTable
RFC1213-MIB	The security appliance supports browsing of the following table: • ip.ipAddrTable
SNMPv2-MIB	The security appliance supports browsing the following: • snmp
ENTITY-MIB	The security appliance supports browsing of the following groups and tables: • entPhysicalTable • entLogicalTable The security appliance supports browsing of the following traps: • config-change • fru-insert • fru-remove
CISCO-IPSEC-FLOW-MONITOR-MIB	The security appliance supports browsing of the MIB. The security appliance supports browsing of the following traps: • start • stop
CISCO-REMOTE-ACCESS-MONITOR-MIB	The security appliance supports browsing of the MIB. The security appliance supports browsing of the following traps: • session-threshold-exceeded
CISCO-CRYPTO-ACCELERATOR-MIB	The security appliance supports browsing of the MIB.
ALTIGA-GLOBAL-REG	The security appliance supports browsing of the MIB.

Table 42-1 SNMP MIB and Trap Support (continued)

MIB or Trap Support	Description
Cisco Firewall MIB	The security appliance supports browsing of the following groups: • cfwSystem The information is cfwSystem.cfwStatus, which relates to failover status, pertains to the entire device and not just a single context.
Cisco Memory Pool MIB	The security appliance supports browsing of the following table: • 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: • cpmCPUTotalTable
Cisco Syslog MIB	The security appliance supports the following trap: • 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 Ensure that the SNMP server on the security appliance is enabled by entering the following command:

```
hostname(config)# snmp-server enable
```

The SNMP server is enabled by default.

Step 2 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 3 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 4 (Optional) To set the SNMP server location or contact information, enter the following command:

```
hostname(config)# snmp-server {contact | location} text
```

Step 5 To enable the security appliance to send traps to the NMS, enter the following command:

```
hostname(config)# snmp-server enable traps [all | syslog | snmp [trap] [...] |
entity [trap] [...] | ipsec [trap] [...] | remote-access [trap]]
```

Enter this command for each feature type to enable individual traps or sets of traps, or enter the **all** keyword to enable all traps.

The default configuration has all **snmp** traps enabled (**snmp-server enable traps snmp authentication linkup linkdown coldstart**). You can disable these traps using the **no** form of this command with the **snmp** keyword. However, the **clear configure snmp-server** command restores the default enabling of SNMP traps.

If you enter this command and do not specify a trap type, then the default is **syslog**. (The default **snmp** traps continue to be enabled along with the **syslog** trap.)

Traps for **snmp** include:

- **authentication**
- **linkup**
- **linkdown**
- **coldstart**

Traps for **entity** include:

- **config-change**
- **fru-insert**
- **fru-remove**

Traps for **ipsec** include:

- **start**
- **stop**

Traps for remote-access include:

- **session-threshold-exceeded**

Step 6 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 7 To enable logging, so system messages are generated and can then be sent to an NMS, enter the following command:

```
hostname(config)# logging enable
```

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

The security appliance system logs provide you with information for monitoring and troubleshooting the security appliance. 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 an internal buffer, one or more syslog servers, 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: overwrite the buffer, send the buffer contents to an FTP server, or save the contents to internal Flash memory.

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

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

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

You can configure the security appliance to include the context name with each message, which helps you differentiate context messages that are sent to a single syslog server. This feature also helps you to determine which messages are from the admin context and which are from the system; messages that originate in the system execution space use a device ID of **system**, and messages that originate in the admin context use the name of the admin context as the device ID. For more information about enabling logging device IDs, see the "Including the Device ID in System Log Messages" section on page 42-19.

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

The following command enables 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 42-7.

To enable logging, enter the following command:

```
hostname(config)# logging enable
```

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
```

Configuring Log Output Destinations

This section describes how to specify where the security appliance should save or send the log messages it generates. 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.

This section includes the following topics:

Sending System Log Messages to a Syslog Server

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.

Note To start logging to a syslog server you define in this procedure, be sure to enable logging for all output locations. See the "Enabling Logging to All Configured Output Destinations" section on page 42-6. To disable logging, see the "Disabling Logging to All Configured Output Destinations" section on page 42-6.

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 interface_name ip_address [tcp[/port] | udp[/port]]
[format emblem]
```

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

The *interface_name* argument specifies the interface through which you access the syslog server.

The *ip_address* argument specifies the IP address of the syslog server.

The **tcp[**/*port*] or **udp[**/*port*] argument specifies that the security appliance should use TCP or UDP to send system log messages to the syslog server. The default protocol is UDP. 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. The *port* argument specifies the port that the syslog server listens to for system log messages. Valid port values are 1025 through 65535, for either protocol. The default UDP port is 514. The default TCP port is 1470.

For example:

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

If you want to designate more than one syslog server as an output destination, 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 | message_list}
```

Where the *severity_level* argument specifies the severity levels of messages to be sent to the syslog server. You can specify the severity level number (0 through 7) or name. For severity level names, see the "Severity Levels" section on page 42-23. For example, if you set the level to 3, then the security appliance sends system log messages for level 3, 2, 1, and 0.

The *message_list* argumentspecifies a customized message list that identifies the system log messages to send to the syslog server. For information about creating custom message lists, see the "Filtering System Log Messages with Custom Message Lists" section on page 42-17.

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 level of 3, 2, and 1.

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

Step 3 (Optional) If needed, set the logging facility to a value other than its default of 20 by entering the following command:

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

Most UNIX systems expect the system log messages to arrive at facility 20.

Step 4 (Optional) To continue to pass traffic when the TCP syslog server is down, enter the following command:

hostname(config)# **logging host** *interface_name server_ip* [**tcp**/port] [**permit-hostdown**]

Sending System Log Messages to the Console Port

This section describes how to configure the security appliance to send logs to the console port.

Note To start logging to the console port as defined in this procedure, be sure to enable logging for all output locations. See the "Enabling Logging to All Configured Output Destinations" section on page 42-6. To disable logging, see the "Disabling Logging to All Configured Output Destinations" section on page 42-6.

To specify which system log messages should be sent to the console port , enter the following command:

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

Where the *severity_level* argument specifies the severity levels of messages to be sent to the console port. You can specify the severity level number (0 through 7) or name. For severity level names, see the "Severity Levels" section on page 42-23. For example, if you set the level to 3, then the security appliance sends system log messages for level 3, 2, 1, and 0.

The *message_list* argumentspecifies a customized message list that identifies the system log messages to send to the console port. For information about creating custom message lists, see the "Filtering System Log Messages with Custom Message Lists" section on page 42-17.

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 console errors
```

Sending System Log Messages to an E-mail Address

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.

Note To start logging to an e-mail address you define in this procedure, be sure to enable logging for all output locations. See the "Enabling Logging to All Configured Output Destinations" section on page 42-6. To disable logging, see the "Disabling Logging to All Configured Output Destinations" section on page 42-6.

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

Step 1 To specify the system log messages to be sent to one or more e-mail addresses, enter the following command:

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

Where the *severity_level* argument specifies the severity levels of messages to be sent to the e-mail address. You can specify the severity level number (0 through 7) or name. For severity level names, see the "Severity Levels" section on page 42-23. For example, if you set the level to 3, then the security appliance sends system log messages for level 3, 2, 1, and 0.

The *message_list* argumentspecifies a customized message list that identifies the system log messages to send to the e-mail address. For information about creating custom message lists, see the "Filtering System Log Messages with Custom Message Lists" section on page 42-17.

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 [severity_level]
```

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

For example:

```
hostname(config)# logging recipient-address admin@example.com
```

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 ip_address
```

For example:

```
hostname(config)# smtp-server 10.1.1.1
```

Sending System Log Messages to ASDM

You can configure the security appliance to send system log messages to 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 the "Sending System Log Messages to the Log Buffer" section on page 42-12.

When the ASDM log buffer is full, the 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, you can change the size of the buffer.

This section includes the following topics:

Configuring Logging for ASDM

Note To start logging to ASDM as defined in this procedure, be sure to enable logging for all output locations. See the "Enabling Logging to All Configured Output Destinations" section on page 42-6. To disable logging, see the "Disabling Logging to All Configured Output Destinations" section on page 42-6.

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 {severity_level | message_list}
```

Where the *severity_level* argument specifies the severity levels of messages to be sent to ASDM. You can specify the severity level number (0 through 7) or name. For severity level names, see the "Severity Levels" section on page 42-23. For example, if you set the level to 3, then the security appliance sends system log messages for level 3, 2, 1, and 0.

The *message_list* argumentspecifies a customized message list that identifies the system log messages to send to ASDM. For information about creating custom message lists, see the "Filtering System Log Messages with Custom Message Lists" section on page 42-17.

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, enter the following command:

```
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
```

Clearing the ASDM Log Buffer

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

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

Sending System Log Messages to a Telnet or SSH Session

Viewing system log messages in a Telnet or SSH session requires two steps:

1. Specify which messages should be sent to Telnet or SSH sessions.
2. View logs in the current session.

This section includes the following topics:

Configuring Logging for Telnet and SSH Sessions

Note To start logging to a Telnet or SSH session as defined in this procedure, be sure to enable logging for all output locations. See the "Enabling Logging to All Configured Output Destinations" section on page 42-6. To disable logging, see the "Disabling Logging to All Configured Output Destinations" section on page 42-6.

To specify which messages should be sent to Telnet or SSH sessions, enter the following command:

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

Where the *severity_level* argument specifies the severity levels of messages to be sent to the session. You can specify the severity level number (0 through 7) or name. For severity level names, see the "Severity Levels" section on page 42-23. For example, if you set the level to 3, then the security appliance sends system log messages for level 3, 2, 1, and 0.

The *message_list* argumentspecifies a customized message list that identifies the system log messages to send to the session. For information about creating custom message lists, see the "Filtering System Log Messages with Custom Message Lists" section on page 42-17.

Viewing System Log Messges in the Current Session

Step 1 After you log in to the security appliance, enable logging to the current session by entering the following command:

```
hostname# terminal monitor
```

This command enables logging only for the current session. If you log out, and then log in again, you need to reenter this command.

Step 2 To disable logging to the current session, enter the following command:

```
hostname(config)# terminal no monitor
```

Sending System Log Messages to the Log Buffer

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, unless you configure the security appliance to save the full buffer to another location.

This section includes the following topics:

Enabling the Log Buffer as an Output Destination

Note To start logging to the buffer as defined in this procedure, be sure to enable logging for all output locations. See the "Enabling Logging to All Configured Output Destinations" section on page 42-6. To disable logging, see the "Disabling Logging to All Configured Output Destinations" section on page 42-6.

To enable the log buffer as a log output destination, enter the following command:

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

Where the *severity_level* argument specifies the severity levels of messages to be sent to the buffer. You can specify the severity level number (0 through 7) or name. For severity level names, see the "Severity Levels" section on page 42-23. For example, if you set the level to 3, then the security appliance sends system log messages for level 3, 2, 1, and 0.

The *message_list* argumentspecifies a customized message list that identifies the system log messages to send to the buffer. For information about creating custom message lists, see the "Filtering System Log Messages with Custom Message Lists" section on page 42-17.

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
```

Viewing the Log Buffer

To view the log buffer, enter the following command:

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

Changing the Log Buffer Size

By default, the log buffer size is 4 KB. To change the size of the log buffer, enter the following command:

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

Where the *bytes* argument 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
```

Automatically Saving the Full Log Buffer to Flash Memory

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
```

Automatically Saving the Full Log Buffer to an FTP Server

See the "Saving the Current Contents of the Log Buffer to Internal Flash Memory" section for more information about saving the buffer.

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 identify the FTP server, entering the following command:

```
hostname(config)# logging ftp-server server path username password
```

Where the *server* argument specifies the IP address of the external FTP server

The *path* argument 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.

The *username* argument specifies a username that is valid for logging into the FTP server.

The *password* argument specifies the password for the username specified.

For example:

```
hostname(config)# logging ftp-server 10.1.1.1 /syslogs logsupervisor 1luvMy10gs
```

Saving the Current 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, enter 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

This section describes how to specify which system log messages should go to output destinations, and includes the following topics:

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 criteria:

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

You customize the above criteria by creating a message list that you can specify when you set the output destination in the "Configuring Log Output Destinations" section on page 42-7.

You can alternatively configure the security appliance to send a particular message class to each type of output destination independently of the message list.

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.

This section includes the following topics:

Message Class Overview

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 log message classes in two ways:

- Issue the **logging class** command to specify an output location for an entire category of system log messages.
- Create a message list using the **logging list** command that specifies the message class. See the "Filtering System Log Messages with Custom Message Lists" section on page 42-17 for this method.

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

When you configure all messages in a class to go to a type of output destination, this configuration overrides the configuration in the specific output destination command. For example, if you specify that messages at level 7 should go to the log buffer, and you also specify that ha class messages at level 3 should go to the buffer, then the latter configuration takes precedence.

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 the *message_class* argument specifies a class of system log messages to be sent to the specified output destination. See Table 42-2 for a list of system log message classes.

The **buffered**, **history**, **mail**, **monitor**, and **trap** keywords specify the output destination to which system log messages in this class should be sent. The **history** keyword enables SNMP logging. The **monitor** keyword enables Telnet and SSH logging. The **trap** keyword enables syslog server logging. 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.

The *severity_level* argument 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 the "Severity Levels" section on page 42-23.

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 class ha buffered alerts
```

Table 42-2 lists the system log message classes and the ranges of system log message IDs associated with each class.

Table 42-2 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

Table 42-2 System Log Message Classes and Associated Message ID Numbers

Class (continued)	Definition	System Log Message ID Numbers
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 log 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.

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 name {level level [class message_class] |
message start_id[-end_id]}
```

Where the *name* argument specifies the name of the list. Do not use the names of severity levels as the name of a system log message list. Prohibited 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.”

The **level** *level* argument specifies the severity level. You can specify the severity level number (0 through 7) or name. For severity level names, see the “Severity Levels” section on page 42-23. For example, if you set the level to 3, then the security appliance sends system log messages for level 3, 2, 1, and 0.

The **class** *message_class* argument specifies a particular message class. See Table 42-2 on page 42-16 for a list of class names.

The **message** *start_id*[**-***end_id*] argument specifies an individual system log message ID number or a range of numbers.

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).

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

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

- System log message IDs that fall in the range of 104024 to 105999
- All system log messages with critical level or higher (emergency, alert, or critical)
- All ha 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

Customizing the Log Configuration

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

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}
```

You can specify only one type of device ID for the system log messages.

The **context-name** keyword indicates that the name of the current context should be used as the device ID (applies to multiple context mode only). 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.

The **hostname** keyword specifies that the hostname of the security appliance should be used as the device ID.

The **ipaddress** *interface_name* argument specifies that the IP address of the interface specified as *interface_name* should be used as the device ID. If you use the **ipaddress** keyword, 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.

The **string** *text* argument specifies that the text string should be used as the device ID. The string can contain as many as 16 characters. You cannot use blank spaces or any of the following characters:

- & (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 FWSM:

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

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

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

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. See the "Sending System Log Messages to a Syslog Server" section on page 42-7 for more information about syslog servers. Enter the following command:

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

  Where the *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
  ```

  For example:

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

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

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

For example:

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

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

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

- To reenable 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
```

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

```
hostname(config)# no logging message message_ID level current_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
```

- To see the severity level of a specific message, enter the following command:

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

- 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 configure logging level
```

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, perform 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

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:

PIX|ASA	Identifies the system log message facility code for messages generated by the Cisco ASA . This value is always PIX|ASA .
Level	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 42-3 for more information.
Message_number	A unique 6-digit number that identifies the system log message.
Message_text	A text string describing the condition. This portion of the system log message sometimes includes IP addresses, port numbers, or usernames.

Severity Levels

Table 42-3 lists the system log message severity levels.

Table 42-3 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 .