



Monitoring the Firewall Services Module

This chapter describes how to configure logging and SNMP for the FWSM. 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 *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*.

This chapter includes the following sections:

- [Configuring SNMP, page 23-1](#)
[Configuring and Managing Logs, page 23-4](#)

Configuring SNMP

- [SNMP Overview, page 23-1](#)
- [Enabling SNMP, page 23-3](#)

SNMP Overview

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

You can configure the FWSM to send traps (event notifications) to a network management station (NMS), or you can use the NMS to browse the MIBs on the FWSM. MIBs are a collection of definitions, and the FWSM 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 23-1](#) lists supported MIBs and traps for the FWSM 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 23-1 SNMP MIB and Trap Support

| MIB or Trap Support | Description |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <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. <p>linkdown—An interface is down, for example, if you removed the nameif</p> |
| | |
| | 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 | <p>The FWSM supports browsing of the following groups and tables: entPhysicalTable entLogicalTable</p> <p>The FWSM supports browsing of the following traps: config-change fru-insert fru-remove</p> |
| CISCO-IPSEC-FLOW-MONITOR-MIB | <p>The FWSM supports browsing of the MIB.</p> <p>The FWSM supports browsing of the following traps: start stop</p> |
| CISCO-REMOTE-ACCESS-MONITOR-MIB | <p>The FWSM supports browsing of the MIB.</p> <p>The FWSM supports browsing of the following traps: session-threshold-exceeded</p> |
| CISCO-CRYPTO-ACCELERATOR-MIB | The FWSM supports browsing of the MIB. |
| ALTIGA-GLOBAL-REG | The FWSM supports browsing of the MIB. |
| Cisco Firewall MIB | <p>The FWSM supports browsing of the following groups: cfwSystem</p> <p>The information is cfwSystem.cfwStatus, which relates to failover status, pertains to the entire device and not just a single context.</p> |

SNMP MIB and Trap Support (continued)

| | |
|--|--|
| | |
| | |
| | |
| | |

Enabling SNMP

-
-

Step 1

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

Step 2

```
snmp-server host interface_name ip_address [ ]  
[community text version {1 2c}] [udp-port port]  
trap poll
```

SNMP traps are sent on UDP port 162 by default. You can change the port number using the **udp-port**

Step 3

key

Step 4

text

Step 5

```
[ ] [...] | [ ] [...] | syslog snmp [ ] [...] |
```

```

snmp
snmp-server enable traps snmp authentication
linkup linkdown coldstart
no
snmp keyword. However, the clear configure snmp-server

```

```

syslog
syslog
snmp
authentication
linkup
linkdown
coldstart
entity
config-change
fru-insert
fru-remove
ipsec
start
stop
session-threshold-exceeded

```

Step 6

level

Step 7

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

```

snmp-server host 192.168.3.2
snmp-server location building 42
snmp-server contact Pat lee
snmp-server community ohwhatakeyisthee

```

Configuring and Managing Logs

- [, page 23-5](#)

-
-
-
- [Customizing the Log Configuration, page 23-17](#)
- [Understanding System Log Messages, page 23-22](#)

Logging Overview

-
-
-
-
-
-

Logging in Multiple Context Mode

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 23-18.

Enabling and Disabling Logging

-
-
-

Enabling Logging to All Configured Output Destinations

Disabling Logging to All Configured Output Destinations

Viewing the Log Configuration

```
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

-
-
-

Sending System Log Messages to a Syslog Server



Note

Step 1

```
format emblem / udp /
```

interface_name

ip_address

tcp[] or [] argument specifies that the FWSM should use TCP or UDP to send system log messages to the syslog server. The default protocol is UDP. You can configure the FWSM to send data to a syslog server using either UDP or TCP, but not both. If you specify TCP, the FWSM discovers when the syslog server fails and discontinues sending logs. If you specify UDP, the FWSM continues to send logs regardless of whether the syslog server is operational. The [] 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:

```
logging host dmz1 192.168.1.5
```

```
logging trap message_list
```

message_list

number

Sending System Log Messages to an E-mail Address



Note

Step 1

severity_level message_list

Step 2

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

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

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

For example:

To specify the SMTP server to be used when sending system log messages to an e-mail destination, enter the following command:

For example:

You can configure the FWSM to send system log messages to ASDM. The FWSM 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 23-11.

When the ASDM log buffer is full, the FWSM 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, page 23-9](#)

[Clearing the ASDM Log Buffer, page 23-10](#)

Configuring Logging for ASDM**Note**

Step 1

Step 2

Clearing the ASDM Log Buffer

Sending System Log Messages to a Switch Session, Telnet Session, or SSH Session

- 1.
- 2.
-
-

Configuring Logging for Telnet and SSH Sessions



Note

Viewing System Log Messages in the Current Session

Step 1

Step 2

Sending System Log Messages to the Log Buffer

-
-
-
-
-
-

Enabling the Log Buffer as an Output Destination



Note

Viewing the Log Buffer

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:

Where the *bytes*

Automatically Saving the Full Log Buffer to Flash Memory

LOG-YYYY-MM-DD-HHMMSS.TXT

YYYY

MM

DD

HHMMSS

Automatically Saving the Full Log Buffer to an FTP Server

Step 1

Step 2

server path username password

```
logging ftp-server 10.1.1.1 /syslogs logsupervisor 1luvMy10gs
```

Saving the Current Contents of the Log Buffer to Internal Flash Memory

Clearing the Contents of the Log Buffer

Filtering System Log Messages

-
-
-

Message Filtering Overview

-
-
-

Filtering System Log Messages by Class

-
-

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 message-list` command that specifies the message class. See the [“Filtering System Log Messages with Custom Message Lists”](#) section on page 23-16 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.

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 FWSM to send an entire system log message class to a configured output destination, enter the following command:

Where the `class` argument specifies a class of system log messages to be sent to the specified output destination. See [Table 23-2](#) for a list of system log message classes.

The `buffer`, `log`, `log-buffer`, and `syslog` keywords specify the output destination to which system log messages in this class should be sent. The `snmp` keyword enables SNMP logging. The `telnet` keyword enables Telnet and SSH logging. The `server` 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` 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 23-22.

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.

[Table 23-2](#) lists the system log message classes and the ranges of system log message IDs associated with each class.

System Log Message Classes and Associated Message ID Numbers

| Class | Definition | System Log Message ID Numbers |
|-------|------------|-------------------------------|
| | | |
| | | |
| | | |

Step 2

-
-
-

Customizing the Log Configuration

- [Configuring the Logging Queue, page 23-18](#)
- [Including the Date and Time in System Log Messages, page 23-18](#)
- [Including the Device ID in System Log Messages, page 23-18](#)
- [Generating System Log Messages in EMBLEM Format, page 23-19](#)
- [Disabling a System Log Message, page 23-19](#)
- [Changing the Severity Level of a System Log Message, page 23-20](#)

- [Changing the Amount of Internal Flash Memory Available for Logs, page 23-21](#)

Configuring the Logging Queue

```
logging queue
```

```
show logging queue
```

Including the Date and Time in System Log Messages

Including the Device ID in System Log Messages

```
logging device-id { context | hostname | interface | text }
```

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

The `context` 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 `admin`, 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 FWSM should be used as the device ID.

The `interface` argument specifies that the IP address of the interface specified as `interface` should be used as the device ID. If you use the `hostname` keyword, the device ID becomes the specified FWSM 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 `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)



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:

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

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:

- To use the EMBLEM format for system log messages sent to a syslog server over UDP, specify the `udp` 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 23-7](#) for more information about syslog servers. Enter the following command:

```
[format emblem]                               [/ ] |
                                               IP_address
port      port
```

```
logging host interface_1 122.243.006.123 udp format emblem
```

```
no logging message
```

```
no logging message 113019
```

logging message

logging message 113019

show logging message

clear config logging disabled

logging message *message_ID* *severity_level*

message_ID *current_severity_level*

message_ID

syslog 403503: default-level errors (enabled)

hostname(config)#

hostname(config)#

syslog 403503: default-level errors, current-level alerts (enabled)

hostname(config)#

hostname(config)#

syslog 403503: default-level errors, current-level alerts (disabled)

hostname(config)#

hostname(config)#

syslog 403503: default-level errors, current-level alerts (enabled)

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

```
hostname(config)#  
kbytes
```

```
hostname(config)#
```

```
hostname(config)#  
kbytes
```

```
hostname(config)#
```

Understanding System Log Messages

-
-

System Log Message Format

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

```
%FWSM Level Message_number: Message_text
```

Level

Message_number

Message_text

System Log Message Severity Levels

| Level Number | Level Keyword | Description |
|--------------|---------------|-------------|
| 0 | emergencies | |
| 1 | alert | |
| 2 | critical | |
| 3 | error | |
| 4 | warning | |
| 5 | notification | |
| 6 | informational | |
| 7 | debugging | |

