CHAPTER 19

# logging asdm through logout Commands

# logging asdm

To send syslog messages to ASDM, use the **logging asdm** command in global configuration mode. To disable logging to ASDM, use the **no** form of this command.

**logging asdm** [*message_list* | *level*]

**no logging asdm** [*message_list* | *level*]

## Syntax Description

| | |
|---|---|
| *level* | Sets the maximum severity level for syslog messages. For example, if you set the severity level to 3, then the FWSM generates syslog messages for levels 3, 2, 1, and 0. You can specify either the number or the name, as follows:<br>• **0** or **emergencies**—System unusable.<br>• **1** or **alerts**—Take immediate action.<br>• **2** or **critical**—Critical condition.<br>• **3** or **errors**—Error.<br>• **4** or **warnings**—Warning.<br>• **5** or **notifications**—Normal but significant condition.<br>• **6** or **informational**—Information.<br>• **7** or **debugging**—Debug messages, log FTP commands, and WWW URLs. |
| *message_list* | Specifies the name of the list that identifies the messages to be sent to ASDM. For information about creating lists, see the **logging list** command. |

## Defaults

ASDM logging is disabled by default.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | • | • | • | • |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## Usage Guidelines

Before any messages are sent to ASDM, you must enable system logging using the **logging enable** command.

When the ASDM log buffer is full, the FWSM deletes the oldest message to make room in the buffer for new messages. To control the number of syslog messages retained in the ASDM log buffer, use the **logging asdm-buffer-size** command.

The ASDM log buffer is a different buffer than the internal log buffer enabled by the **logging buffered** command. The FWSM only places messages in the ASDM log buffer if they are destined to be sent to ASDM.

## Examples

The following example shows how to enable logging and send to the ASDM log buffer messages of severity levels 0, 1, and 2. It also shows how to set the ASDM log buffer size to 200 messages.

```
hostname(config)# logging enable
hostname(config)# logging asdm 2
hostname(config)# logging asdm-buffer-size 200
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: level critical, 48 messages logged
```

## Related Commands

| Command | Description |
|---|---|
| **clear logging asdm** | Clears the ASDM log buffer of all of the syslog messages it contains. |
| **logging asdm-buffer-size** | Specifies the number of ASDM messages retained in the ASDM log buffer. |

# logging asdm-buffer-size

To specify the number of syslog messages retained in the ASDM log buffer, use the **logging asdm-buffer-size** command in global configuration mode. To reset the ASDM log buffer to its default size of 100 messages, use the **no** form of this command.

**logging asdm-buffer-size** *num_of_msgs*

**no logging asdm-buffer-size** *num_of_msgs*

## Syntax Description

| | |
|---|---|
| *num_of_msgs* | Specifies the number of syslog messages that the FWSM retains in the ASDM log buffer. |

## Defaults

The default ASDM syslog buffer size is 100 messages.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | • | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## Usage Guidelines

When the ASDM log buffer is full, FWSM deletes the oldest message to make room in the buffer for new messages. To control whether logging to the ASDM log buffer is enabled or to control the kind of syslog messages retained in the ASDM log buffer, use the **logging asdm** command.

The ASDM log buffer is a different buffer than the internal log buffer enabled by the **logging buffered** command. The FWSM only places messages in the ASDM log buffer if they are destined to be sent to ASDM.

## Examples

The following example shows how enable logging and send to the ASDM log buffer messages of severity levels 0, 1, and 2. It also shows how to set the ASDM log buffer size to 200 messages.

```
hostname(config)# logging enable
hostname(config)# logging asdm 2
hostname(config)# logging asdm-buffer-size 200
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: level critical, 48 messages logged
```

## Related Commands

| Command | Description |
|---|---|
| **clear logging asdm** | Clears the ASDM log buffer of all of the syslog messages it contains. |
| **logging asdm** | Enables logging to the ASDM log buffer. |
| **logging enable** | Enables logging to all specified output locations. |
| **show logging** | Displays the enabled logging options. |
| **show running-config logging** | Displays the currently running logging configuration. |

# logging buffered

To enable the FWSM to save syslog messages in the log buffer, use the **logging buffered** command in global configuration mode. To disable logging to the log buffer, use the **no** form of this command.

**logging buffered** [*message_list* | *level*]

**no logging buffered** [*message_list* | *level*]

## Syntax Description

| | |
|---|---|
| *level* | Sets the maximum severity level for syslog messages. For example, if you set the severity level to 3, then the FWSM generates syslog messages for severity levels 3, 2, 1, and 0. You can specify either the number or the name, as follows:<br>• **0** or **emergencies**—System unusable.<br>• **1** or **alerts**—Take immediate action.<br>• **2** or **critical**—Critical condition.<br>• **3** or **errors**—Error.<br>• **4** or **warnings**—Warning.<br>• **5** or **notifications**—Normal but significant condition.<br>• **6** or **informational**—Information.<br>• **7** or **debugging**—Debug messages, log FTP commands, and WWW URLs. |
| *message_list* | Specifies the list that identifies the messages to send to the internal log buffer. For information about creating message lists, see the **logging list** command. |

## Defaults

The defaults are as follows:

- Logging to the internal log buffer is disabled.
- Log buffer size is 4 KB.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | • | • | • | • |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## Usage Guidelines

For the FWSM to generate syslog messages, you must enable logging using the **logging enable** command. Use the **logging buffered** command to specify the internal log buffer as an output destination.

The FWSM appends new messages to the end of the log buffer. When the log buffer is full, it "wraps" to the first message in the buffer. Unless configured otherwise, the FWSM writes over messages, oldest message first, when new messages are generated.

You can configure the FWSM so that the log buffer content is automatically saved each time the buffer wraps. For more information, see the **logging flash-bufferwrap** and **logging ftp-bufferwrap** commands.

In addition, you can you can save the buffer contents at any time to internal flash memory. For more information, see the **logging savelog** command.

Syslog messages in the internal buffer can be viewed with the **show logging** command.

## Examples

The following example configures logging to the buffer for level 0 and level 1 events:

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

The following example creates a list named notif-list with a maximum logging level of 7 and configures logging to the buffer for syslog messages identified by the notif-list message list that you created.

```
hostname(config)# logging list notif-list level 7
hostname(config)# logging buffered notif-list
hostname(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **clear logging buffer** | Clears the log buffer of all syslog messages it contains. |
| **logging buffer-size** | Specifies log buffer size. |
| **logging flash-bufferwrap** | Writes the log buffer to internal flash memory when the log buffer wraps. |
| **logging ftp-bufferwrap** | Sends the log buffer to an FTP server when the log buffer wraps. |
| **logging list** | Creates a reusable list of message selection criteria. |
| **logging savelog** | Saves the contents of the log buffer to internal flash memory. |

# logging buffer-size

To specify the size of the system log buffer, use the **logging buffer-size** command in global configuration mode. To reset the system log buffer to its default size of 4 KB of memory, use the **no** form of this command.

**logging buffer-size** *bytes*

**no logging buffer-size** *bytes*

## Syntax Description

| | |
|---|---|
| *bytes* | Sets the amount of memory used for the log buffer, in bytes. For example, if you specify 8192, the FWSM uses 8 KB of memory for the log buffer. |

## Defaults

The log buffer size is 4 KB of memory.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | • | • | • | • |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## Usage Guidelines

To see whether the FWSM is using a log buffer of a size other than the default buffer size, use the **show running-config logging** command. If the logging buffer size is not shown, then the FWSM uses a log buffer size of 4 KB.

For more information about how the FWSM uses the system log buffer, see the **logging buffered** command.

## Examples

The following example enables system logging, enables the system log buffer as a log output destination, and specifies that the FWSM uses 16 KB of memory for the log buffer:

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

## Related Commands

| Command | Description |
|---|---|
| **clear logging buffer** | Clears the log buffer of all syslog messages it contains. |
| **logging buffered** | Enables logging to the system log buffer. |
| **logging flash-bufferwrap** | Writes the contents of the system log buffer to internal flash memory when the log buffer wraps. |
| **logging savelog** | Saves the contents of the log buffer to internal flash memory. |
| **show logging** | Displays the contents of the internal log buffer and the enabled logging options. |

# logging class

To specify an output destination for an entire class of messages, use the **logging class** command in global configuration mode. To remove the output destination for a messages class, use the **no** form of the command.

**logging class** *message_class output_destination* [*severity_level*]

**no logging class** *class*

## Syntax Description

| | |
|---|---|
| *class* | Specifies the message class to be sent to the specified output destination.<br>For valid values of *class*, see the "Usage Guidelines" section that follows. |
| *destination* | Specifies a log output destination for *class*. For valid values of *output_destination*, see the "Usage Guidelines" section that follows. |
| *level* | Sets the maximum severity level for syslog messages. For example, if you set the severity level to 3, then the FWSM generates syslog messages for severity levels 3, 2, 1, and 0. You can specify either the number or the name, as follows:<br>• **0** or **emergencies**—System unusable.<br>• **1** or **alerts**—Take immediate action.<br>• **2** or **critical**—Critical condition.<br>• **3** or **errors**—Error.<br>• **4** or **warnings**—Warning.<br>• **5** or **notifications**—Normal but significant condition.<br>• **6** or **informational**—Information.<br>• **7** or **debugging**—Debug messages, log FTP commands, and WWW URLs. |

## Defaults

By default, the FWSM does not apply logging levels on a logging destination and message class basis. Instead, each enabled logging destination receives messages for all classes at the logging level determined by the logging list or level specified when you enabled the logging destination.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | • | • | • | • |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## Usage Guidelines

Valid values for *class* are as follows:

- **auth**—User authentication
- **bridge**—Transparent firewall
- **ca**—PKI certificate authority
- **config**—Command interface
- **email**—Email proxy
- **ha**—Failover
- **ids**—Intrusion detection system
- **ip**—IP stack
- **np**—Network processor
- **ospf**—OSPF routing
- **rip**—RIP routing
- **session**—User session
- **snmp**—SNMP
- **sys**—System
- **vpn**—IKE and IPSec
- **vpnc**—VPN client
- **vpnfo**—VPN failover
- **vpnlb**—VPN load balancing

Valid logging destinations are as follows:

- **asdm**—To learn about this destination, see the **logging asdm** command.
- **buffered**—To learn about this destination, see the **logging buffered** command.
- **console**—To learn about this destination, see the **logging console** command.
- **history**—To learn about this destination, see the **logging history** command.
- **mail**—To learn about this destination, see the **logging mail** command.
- **monitor**—To learn about this destination, see the **logging monitor** command.
- **trap**—To learn about this destination, see the **logging trap** command.

## Examples

The following example specifies that, for failover-related messages, the maximum logging level for the ASDM log buffer is 2 and the maximum logging level for the syslog buffer is 7:

```
hostname(config)# logging class ha asdm 2 buffered 7
hostname(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **logging enable** | Enables logging. |

| Command | Description |
|---|---|
| **show logging** | Displays the enabled logging options. |
| **show running-config logging** | Displays the logging-related portion of the running configuration. |

# logging console

To enable the FWSM to display syslog messages in console sessions, use the **logging console** command in global configuration mode. To disable the display of syslog messages in console sessions, use the **no** form of this command.

**logging console** [*message_list* | *level*]

**no logging console**

**Note** We recommend that you do not use this command because it may cause many syslog messages to be dropped due to buffer overflow. For more information, see the "Usage Guidelines" section that follows.

## Syntax Description

| | |
|---|---|
| *level* | Sets the maximum severity level for syslog messages. For example, if you set the severity level to 3, then the FWSM generates syslog messages for levels 3, 2, 1, and 0. You can specify either the number or the name, as follows:<br>• **0** or **emergencies**—System unusable.<br>• **1** or **alerts**—Take immediate action.<br>• **2** or **critical**—Critical condition.<br>• **3** or **errors**—Error.<br>• **4** or **warnings**—Warning.<br>• **5** or **notifications**—Normal but significant condition.<br>• **6** or **informational**—Information.<br>• **7** or **debugging**—Debug messages, log FTP commands, and WWW URLs. |
| *message_list* | Specifies the list that identifies the messages to send to the console session. For information about creating lists, see the **logging list** command. |

## Defaults

The FWSM does not display syslog messages in console sessions by default.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | • | • | • | • |

## Command History

| Release | Modification |
|---|---|
| Preexisting | This command was preexisting. |

## Usage Guidelines

Before any messages are sent to the console, you must enable system logging using the **logging enable** command.

**Caution** Using the **logging console** command could drastically degrade system performance. Instead, use the **logging buffered** command to designate the internal log buffer as an output destination, then use the **show logging** command to see the messages. To make viewing the most current messages easier, use the **clear logging buffer** command to clear the buffer.

## Examples

The following example shows how to enable syslog messages of severity levels 0, 1, 2, and 3 to appears in console sessions:

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

## Related Commands

| Command | Description |
|---|---|
| **logging enable** | Enables logging to all specified output destinations. |
| **logging list** | Creates a reusable list of message selection criteria. |
| **show logging** | Displays the contents of the internal log buffer and the enabled logging options. |
| **show running-config logging** | Displays the logging-related portion of the running configuration. |

# logging debug-trace

To redirect debugging messages to logs such as syslog message 711011 issued at severity level 7, use the **logging debug-trace** command in global configuration mode. To stop sending debugging messages to logs, use the **no** form of this command.

**logging debug-trace**

**no logging debug-trace**

## Syntax Description

This command has no arguments or keywords.

## Defaults

By default, the FWSM does not include debugging output in syslog messages.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | • | • | • | • |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## Usage Guidelines

Debugging messages are generated as severity level 7 messages. They appear in logs with the syslog message number 711011.

## Examples

The following example shows how to enable logging, send log messages to the log buffer, redirect debugging output to logs, and turn on debugging disk activity.

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging debug-trace
hostname(config)# debug disk filesystem
```

An example of a debug message that could appear in the logs follows:

```
%FWSM-7-711001: IFS: Read: fd 3, bytes 4096
```

## Related Commands

| Command | Description |
|---|---|
| **logging enable** | Enables logging to all output destinations. |
| **show logging** | Displays the contents of the internal log buffer and the enabled logging options. |
| **show running-config logging** | Displays the logging-related portion of the running configuration. |

# logging deny-conn-queue-full

To prevent the creation of new transit connections through the FWSM when the logging queue is full, use the **logging deny-conn-queue-full** command in global configuration mode. To allow the creation of new transit connections through the FWSM when the logging queue is full, use the **no** form of this command.

**logging deny-conn-queue-full**

**no logging deny-conn-queue-full**

## Syntax Description

| | |
|---|---|
| **deny-conn-queue-full** | This option does not allow the creation of new transit connections through the FWSM when the logging queue is full.<br>**Note** If the logging queue is set to zero, the queue will be the maximum configurable size (8192 messages). |

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| **Command Mode** | **Routed** | **Transparent** | **Single** | **Context** | **System** |
| Global configuration | • | • | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## Usage Guidelines

When traffic is so heavy that the logging queue fills up, the FWSM might discard messages. You can prevent the creation of new transit connections through the FWSM to avoid discarding messages.

## Examples

The following example shows how to display the output of the **logging deny-conn-queue-full** and **show logging queue** commands:

```
hostname(config)# logging deny-conn-queue-full
hostname(config)# show logging queue

Logging Queue length limit: Unlimited
1 msg(s) discarded due to queue overflow
Current 5 msgs on queue, 3513 msgs most on queue
```

In this example, the **logging deny-conn-queue-full** command prevents the creation of new transit connections through the FWSM when the logging queue is full. The syslog messages currently in the queue are processed by the FWSM in the manner specified by the current logging configuration, such as sending syslog messages to e-mail recipients, saving buffer overflows to internal flash memory, and so on. The logging queue does not discard any messages.

The sample output of the **show logging queue** command shows the following:

- Five messages are queued.
- The largest number of messages in the queue at one time since the FWSM was last booted was 3513.
- One message was discarded.

Even though the queue length was set for unlimited, a message was discarded because no block memory was available to add the message to the queue.

## Related Commands

| Command | Description |
|---|---|
| **logging queue** | Specifies how many syslog messages that the FWSM can hold in its system log queue before processing them. |
| **show logging queue** | Displays syslog messages currently in the logging queue. |

# logging device-id

To configure the FWSM to include a device ID in non-EMBLEM-format syslog messages, use the **logging device-id** command in global configuration mode. To disable the inclusion of a device ID in messages, use the **no** form of this command.

**logging device-id** {**context-name** | **hostname** | **ipaddress** *interface_name* | **string** *text*}

**no logging device-id** {**context-name** | **hostname** | **ipaddress** *interface_name* | **string** *text*}

## Syntax Description

| | |
|---|---|
| **context-name** | Use the name of the current context as the device ID. |
| **hostname** | Use the hostname of the FWSM as the device ID. |
| **ipaddress** *interface_name* | Use as the device ID the IP address of the interface specified as *interface_name*. If you use the **ipaddress** keyword, syslog messages sent to an external server contain the IP address of the interface specified, regardless of which interface the FWSM uses to send the log data to the external server. |
| **string** *text* | Use as the device ID the characters contained in *text*, which can be up to 16 characters long. You cannot use white space characters or any of the following characters in *text*:<br>• &—ampersand<br>• '—single quote<br>• "—double quote<br>• <—less than<br>• >—greater than<br>• ?—question mark |

## Defaults

No default device ID is used in syslog messages.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | • | • | • | • |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## Usage Guidelines

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

## Examples

The following example shows how to specify a device ID of secappl-1 and the output from the **show logging** command:

```
hostname(config)# logging device-id secappl1
hostname(config)# show logging
Syslog logging: disabled
Facility: 20
Timestamp logging: disabled
Standby logging: disabled
Console logging: disabled
Monitor logging: disabled
Buffer logging: level informational, 991 messages logged
Trap logging: disabled
History logging: disabled
Device ID: hostname "secappl-1"
```

In syslog messages, the hostname secappl-1 appears at the beginning of the message, such as the following:

```
secappl-1 %FWSM-5-111008: User 'enable_15' executed the 'logging buffer-size 4096'
command.
```

## Related Commands

| Command | Description |
|---|---|
| **logging enable** | Enables logging to all specified output destinations. |
| **show logging** | Displays contents of the internal log buffer and the enabled logging options. |
| **show running-config logging** | Displays the logging-related portion of the running configuration. |

# logging emblem

To use the EMBLEM format for syslog messages that are sent to output destinations other than a syslog server, use the **logging emblem** command in global configuration mode. To disable the use of the EMBLEM format, use the **no** form of this command.

**logging emblem**

**no logging emblem**

## Syntax Description

This command has no arguments or keywords.

## Defaults

By default, the FWSM does not use EMBLEM format for syslog messages.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | • | • | • | • |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## Usage Guidelines

The **logging emblem** command enables you to configure the FWSM to use the EMBLEM-format for all messages being sent to output destinations other than to syslog servers; specifically, messages sent to one or more e-mail addresses, the internal log buffer, ASDM, a Telnet session, or an SNMP management station use the EMBLEM-format. If you also enable the **logging timestamp** keyword, the messages also include a timestamp.

To enable EMBLEM-format logging for syslog servers, use the **format emblem** option with the **logging host** command.

## Examples

The following example shows how to enable logging and enable the use of EMBLEM-format for logging to all logging destinations except syslog servers:

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

## Related Commands

| Command | Description |
|---|---|
| **logging enable** | Enables logging. |
| **show logging** | Displays the enabled logging options. |
| **show running-config logging** | Displays the logging-related portion of the running configuration. |

# logging device-id

To configure the FWSM to include a device ID in non-EMBLEM-format syslog messages, use the **logging device-id** command in global configuration mode. To disable the inclusion of a device ID in messages, use the **no** form of this command.

**logging device-id** {**context-name** | **hostname** | **ipaddress** *interface_name* | **string** *text*}

**no logging device-id** {**context-name** | **hostname** | **ipaddress** *interface_name* | **string** *text*}

## Syntax Description

| | |
|---|---|
| **context-name** | Use the name of the current context as the device ID. |
| **hostname** | Use the hostname of the FWSM as the device ID. |
| **ipaddress** *interface_name* | Use as the device ID the IP address of the interface specified as *interface_name*. If you use the **ipaddress** keyword, syslog messages sent to an external server contain the IP address of the interface specified, regardless of which interface the FWSM uses to send the log data to the external server. |
| **string** *text* | Use as the device ID the characters contained in *text*, which can be up to 16 characters long. You cannot use white space characters or any of the following characters in *text*:<br>• &—ampersand<br>• '—single quote<br>• "—double quote<br>• <—less than<br>• >—greater than<br>• ?—question mark |

## Defaults

No default device ID is used in syslog messages.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | • | • | • | • |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## Usage Guidelines

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

## Examples

The following example shows how to specify a device ID of secappl-1 and the output from the **show logging** command:

```
hostname(config)# logging device-id secappl1
hostname(config)# show logging
Syslog logging: disabled
Facility: 20
Timestamp logging: disabled
Standby logging: disabled
Console logging: disabled
Monitor logging: disabled
Buffer logging: level informational, 991 messages logged
Trap logging: disabled
History logging: disabled
Device ID: hostname "secappl-1"
```

In syslog messages, the hostname secappl-1 appears at the beginning of the message, such as the following:

```
secappl-1 %FWSM-5-111008: User 'enable_15' executed the 'logging buffer-size 4096'
command.
```

## Related Commands

| Command | Description |
|---|---|
| **logging enable** | Enables logging to all specified output destinations. |
| **show logging** | Displays contents of the internal log buffer and the enabled logging options. |
| **show running-config logging** | Displays the logging-related portion of the running configuration. |

# logging facility

To specify the logging facility used for messages sent to system message servers, use the **logging facility** command in global configuration mode. To reset the logging facility to its default of 20, use the **no** form of this command.

**logging facility** *facility*

**no logging facility**

## Syntax Description

| | |
|---|---|
| *facility* | Specifies the system log facility; valid values are 16 through 23. |

## Defaults

The default facility is 20 (LOCAL4).

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | • | • | • | • |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## Usage Guidelines

System log servers file messages based on the *facility* number in the message. There are eight possible facilities, 16 (LOCAL0) through 23 (LOCAL7).

## Examples

The following example shows how to set the logging facility as 16. The output of the **show logging** command includes the facility being used by the FWSM in syslog messages.

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

## Related Commands

| Command | Description |
|---|---|
| **logging host** | Defines a syslog server. |
| **logging trap** | Enables logging to syslog servers. |
| **show logging** | Displays the enabled logging options. |
| **show running-config logging** | Displays the logging-related portion of the running configuration. |

# logging flash-bufferwrap

To configure the FWSM to write the contents of the log buffer to internal flash memory every time the buffer wraps, use the **logging flash-bufferwrap** command in global configuration mode. To disable writing the contents of the log buffer to internal flash memory, use the **no** form of this command.

**logging flash-bufferwrap**

**no logging flash-bufferwrap**

## Syntax Description

This command has no arguments or keywords.

## Defaults

The defaults are as follows:

- Log buffer is not specified as an output destination.
- Writing the contents of the log buffer to internal flash memory is disabled.
- Log buffer size is 4 KB.
- Minimum free internal flash memory is 3 MB.
- Maximum internal flash memory allocation for buffer logging is 1 MB.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | • | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## Usage Guidelines

For the FWSM to write the log buffer contents to internal flash memory when the buffer wraps, you must first configure the log buffer as an output destination; otherwise, the log buffer remains empty. To configure the log buffer as an output destination, use the **logging buffered** command.

While the FWSM writes the log buffer contents to internal flash memory, it continues storing to the log buffer any new event messages.

The FWSM 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.

The availability of internal flash memory affects how the FWSM saves logs using the **logging flash-bufferwrap** command. For more information, see the **logging flash-maximum-allocation** and the **logging flash-minimum-free** commands.

## Examples

The following example shows how to enable system logging, specify the log buffer as an output destination, and enable the FWSM to write the log buffer contents to internal flash memory when the buffer wraps:

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

## Related Commands

| Command | Description |
|---|---|
| **clear logging buffer** | Clears the log buffer of all system log messages it contains. |
| **logging buffered** | Specifies the log buffer as an output destination, enabling event messages to be written to the log buffer. |
| **logging buffer-size** | Specifies the log buffer size. |
| **logging flash-maximum-allocation** | Specifies the maximum amount of internal flash memory that can be used for logs. |
| **logging flash-minimum-free** | Specifies the minimum amount of internal flash memory that must be available for the FWSM to permit writing the log buffer contents to internal flash memory. |
| **show logging** | Displays the enabled logging options. |

# logging flash-maximum-allocation

To specify the maximum amount of internal flash memory that the FWSM uses to store log data, use the **logging flash-maximum-allocation** command in global configuration mode. To reset the maximum amount of internal flash memory used for this purpose to its default size of 1 MB, use the **no** form of this command.

**logging flash-maximum-allocation** *kbytes*

**no logging flash-maximum-allocation** *kbytes*

## Syntax Description

| | |
|---|---|
| *kbytes* | The largest amount of internal flash memory, in kilobytes, that the FWSM can use to save log buffer data. |

## Defaults

The default maximum internal flash memory allocation for log data is 1 MB.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | • | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## Usage Guidelines

This command determines how much internal flash memory is available for the **logging savelog** and **logging flash-bufferwrap** commands.

If a log file to be saved by **logging savelog** or **logging flash-bufferwrap** requires more internal flash memory than the maximum amount specified by the **logging flash-maximum-allocation** command, the FWSM deletes the oldest log files to free sufficient memory for the new log file. If there are no files to delete or if, after all old files are deleted, free memory is too small for the new log file, the FWSM fails to save the new log file.

To determine whether the FWSM has a maximum internal flash memory allocation of a size different than the default size, use the **show running-config logging** command. If the **logging flash-maximum-allocation** command is not shown, then the FWSM uses a maximum of 1 MB for log buffer data. The memory allocated is used for both the **logging savelog** and **logging flash-bufferwrap** commands.

For more information about how the FWSM uses the log buffer, see the **logging buffered** command.

## Examples

The following example shows how to enable logging, specify the log buffer as an output destination, enable the FWSM to write the log buffer contents to internal flash memory, with the maximum amount of internal flash memory used for log data set to approximately 1.2 MB of memory:

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

## Related Commands

| Command | Description |
|---|---|
| **logging buffered** | Specifies the log buffer as an output destination, enabling event messages to be written to the log buffer as they occur. |
| **logging flash-bufferwrap** | Enables the log buffer contents to be written to internal flash memory when the log buffer wraps. |
| **logging flash-minimum-free** | Specifies the minimum amount of internal flash memory that must be available for the FWSM to permit writing the log buffer contents to internal flash memory. |
| **logging savelog** | Saves the contents of the log buffer to internal flash memory each time the command is entered at the command line. |

# logging flash-minimum-free

To specify the minimum amount of free internal flash memory that must exist before the FWSM saves a new log file, use the **logging flash-minimum-free** command in global configuration mode. To reset the minimum required amount of free internal flash memory to its default size of 3 MB, use the **no** form of this command.

**logging flash-minimum-free** *kbytes*

**no logging flash-minimum-free** *kbytes*

## Syntax Description

| | |
|---|---|
| *kbytes* | The minimum amount of internal flash memory, in kilobytes, that must be available before the FWSM saves a new log file. |

## Defaults

The default minimum free internal flash memory is 3 MB.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | • | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## Usage Guidelines

This command affects how much free internal flash memory must exist before the FWSM saves log files created by the **logging savelog** and **logging flash-bufferwrap** commands.

The **logging flash-minimum-free** command specifies how much internal flash memory the **logging savelog** and **logging flash-bufferwrap** commands must preserve at all times.

If a log file to be saved by **logging savelog** or **logging flash-bufferwrap** would cause the amount of free internal flash memory to fall below the limit specified by the **logging flash-minimum-free** command, the FWSM 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 FWSM fails to save the new log file.

## Examples

The following example shows how to specify that the minimum amount of free internal flash memory must be 4000 KB:

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

## Related Commands

| Command | Description |
|---|---|
| **logging buffered** | Specifies the log buffer as an output destination, enabling event messages to be written to the log buffer as they occur. |
| **logging flash-bufferwrap** | Writes the log buffer to internal flash memory when the log buffer wraps. |
| **logging flash-maximum-allocation** | Specifies the maximum amount of internal flash memory that can be used for log data. |
| **logging savelog** | Saves the contents of the log buffer to internal flash memory each time the command is entered at the command line. |

# logging from-address

To specify the source e-mail address for syslog messages e-mailed by the FWSM, use the **logging from-address** command in global configuration mode. This e-mail address appears in the From: line of all e-mailed syslog messages. To remove the source e-mail address, use the **no** form of this command.

**logging from-address** *from-email-address*

**no logging from-address** *from-email-address*

## Syntax Description

| | |
|---|---|
| *from-email-address* | Source e-mail address, that is, the e-mail address that appears in the From: line of each e-mailed syslog message. |

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | • | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## Usage Guidelines

Sending syslog messages by e-mail is enabled by the **logging mail** command.

The address specified with this command need not correspond to an existing e-mail account.

## Examples

The following example shows how set up the FWSM to send a limited number of syslog messages by e-mail. The example commands are based on the following example criteria:

- Send messages that are critical, alerts, or emergencies.
- Send messages using ciscosecurityappliance@example.com as the address from whom messages are sent.
- Send messages to admin@example.com.
- Send messages using SMTP the primary servers pri-smtp-host and secondary server sec-smtp-host.

To enable the FWSM to e-mail system messages according to the example criteria, enter the following commands:

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

```
hostname(config)# logging from-address ciscosecurityappliance@example.com
hostname(config)# logging recipient-address admin@example.com
hostname(config)# smtp-server pri-smtp-host sec-smtp-host
```

## Related Commands

| Command | Description |
|---|---|
| **logging mail** | Enables the FWSM to send syslog messages by e-mail and specifies which messages are sent by e-mail. |
| **logging recipient-address** | Specifies the e-mail address to which e-mailed syslog messages are sent. |
| **smtp-server** | Configures an SMTP server. |

# logging ftp-bufferwrap

To enable the FWSM to write the contents of the log buffer to an FTP server every time the buffer wraps, use the **logging ftp-bufferwrap** command in global configuration mode. To disable writing the contents of the log buffer to an FTP server, use the **no** form of this command.

**logging ftp-bufferwrap**

**no logging ftp-bufferwrap**

## Syntax Description

This command has no arguments or keywords.

## Defaults

The defaults are as follows:

- Logging to the buffer is disabled.
- Sending the log buffer to an FTP server is disabled.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | • | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## Usage Guidelines

When you enable **logging ftp-bufferwrap**, the FWSM sends log buffer data to the FTP server every time the log buffer wraps. You specify the FTP server to be sent the log buffer data with the **logging ftp-server** command.

For the FWSM to send the log buffer contents to the FTP server when the buffer wraps, you must first configure the log buffer as an output destination; otherwise, the log buffer remains empty. To configure the log buffer as an output destination, use the **logging buffered** command.

While the FWSM sends log data to the FTP server, it continues storing new messages to the log buffer.

The FWSM 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.

## Examples

The following example shows how to enable the log buffer, specify an FTP server, and enable the FWSM to write the log buffer contents to an FTP server each time the buffer wraps. This example specifies an FTP server whose hostname is logserver-352. The server can be accessed with the username logsupervisor and password 1luvMy10gs. Log files are to be stored in the /syslogs directory.

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

## Related Commands

| Command | Description |
|---|---|
| **clear logging buffer** | Clears the log buffer of all syslog messages it contains. |
| **logging buffered** | Specifies the log buffer as an output destination, enabling event messages to be written to the log buffer as they occur. |
| **logging buffer-size** | Specifies log buffer size. |
| **logging ftp-server** | Specifies FTP server parameters for use with the **logging ftp-bufferwrap** command. |

# logging ftp-server

To specify details about the FTP server the FWSM sends log buffer data to when **logging ftp-bufferwrap** is enabled, use the **logging ftp-server** command in global configuration mode. To remove all details about an FTP server, use the **no** form of this command.

**logging ftp-server** *ftp-server ftp_server path username password*

**no logging ftp-server** *ftp-server ftp_server path username password*

## Syntax Description

| | |
|---|---|
| *ftp-server* | External FTP server IP address or hostname.<br>**Note** If you specify a hostname, be sure DNS is operating correctly on your network. |
| *password* | The password for the username specified. |
| *path* | 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:<br>`/security_appliances/syslogs/appliance107` |
| *username* | A username that is valid for logging in to the FTP server. |

## Defaults

No FTP server is specified by default.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | • | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## Usage Guidelines

You can only specify one FTP server. If a logging FTP server is already specified, using the **logging ftp-server** command replaces that FTP server configuration with the new one you enter.

The FWSM does not verify the FTP server information you specify. If you misconfigure any of the details, the FWSM fails to send log buffer data to the FTP server.

## Examples

The following example shows how to specify an FTP server and enable the FWSM to write the contents of the log buffer to an FTP server. This example specifies an FTP server whose hostname is logserver-352. The server can be accessed with the username logsupervisor and password 1luvMy10gs. Log files are to be stored in the */syslogs* directory.

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

## Related Commands

| Command | Description |
|---|---|
| **clear logging buffer** | Clears the log buffer of all syslog messages it contains. |
| **logging buffered** | Specifies the log buffer as an output destination, enabling event messages to be written to the log buffer as they occur. |
| **logging buffer-size** | Specifies log buffer size. |
| **logging ftp-bufferwrap** | Sends the log buffer contents to the specified FTP server when the log buffer wraps. |
| **show running-config logging** | Displays the currently running logging configuration. |

# logging history

To enable SNMP logging and specify which messages are to be sent to SNMP servers, use the **logging history** command in global configuration mode. To disable SNMP logging, use the **no** form of this command.

**logging history** [*message_list* | *level*]

**no logging history**

## Syntax Description

| | |
|---|---|
| *level* | Sets the maximum severity level for syslog messages. For example, if you set the severity level to 3, then the FWSM generates syslog messages for levels 3, 2, 1, and 0. You can specify either the number or the name, as follows:<br>• **0** or **emergencies**—System unusable.<br>• **1** or **alerts**—Take immediate action.<br>• **2** or **critical**—Critical condition.<br>• **3** or **errors**—Error.<br>• **4** or **warnings**—Warning.<br>• **5** or **notifications**—Normal but significant condition.<br>• **6** or **informational**—Information.<br>• **7** or **debugging**—Debug messages, log FTP commands, and WWW URLs. |
| *message_list* | Specifies the list that identifies the messages to send to the SNMP server. For information about creating lists, see the **logging list** command. |

## Defaults

The FWSM does not log to SNMP servers by default.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | • | • | • | — |

## Command History

| Release | Modification |
|---|---|
| Preexisting | This command was preexisting. |

## Usage Guidelines

The **logging history** command lets you enable logging to an SNMP server and set the SNMP message level or event list. You must also configure the FWSM for SNMP.

Examples

The following example shows how to enable SNMP logging and specify that messages of severity levels 0, 1, 2, and 3 are sent to the SNMP server:

```
hostname(config)# snmp-server host infrastructure 10.2.3.7 trap community gam327
hostname(config)# snmp-server enable traps syslog
hostname(config)# logging history errors
hostname(config)#
```

**Related Commands**

| Command | Description |
|---|---|
| **snmp-server** | Specifies SNMP server details. |

# logging host

To define a syslog server as a log output destination, use the **logging host** command in global configuration mode. To remove a syslog server definition, use the **no** form of this command.

**logging host** *interface_name server_ip* [**tcp/***port* | **udp/***port*] [**format emblem**] [**permit-hostdown**]

**no logging host** *interface_name server_ip*

## Syntax Description

| | |
|---|---|
| **format emblem** | (Optional) Enables EMBLEM format logging for the syslog server, which is available only for UDP messages. |
| **host** | Specifies a syslog server that will receive the messages that are sent from the FWSM. |
| *interface_name* | Interface on which the syslog server resides. |
| **permit-hostdown** | Allows new network access sessions for a TCP-based syslog server |
| *port* | The port that the syslog server listens to for messages. Valid port values for either protocol are 1025 through 65535. |
| *server_ip* | The IP address of the syslog server. |
| **tcp** | Specifies that the FWSM should use TCP to send messages to the syslog server. |
| **udp** | Specifies that the FWSM should use TCP to send messages to the syslog server. |

## Defaults

The default values are as follows:

- The default protocol is UDP.
- The default UDP port is 514.
- The default TCP port is 1470.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| **Command Mode** | **Routed** | **Transparent** | **Single** | **Context** | **System** |
| Global configuration | • | • | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 7.0(1) | This command was introduced. |
| 7.2(2) | The **permit-hostdown** keyword was added. |

## Usage Guidelines

The **logging host** *ip_address* **format emblem** command lets you enable EMBLEM-format logging for each syslog server. EMBLEM-format logging is available for UDP syslog messages only. If you enable EMBLEM-format logging for a particular syslog server, then the messages are sent to that server in the EMBLEM format. If you also enable the **logging timestamp** keyword, messages sent to that server include a time stamp.

You can use multiple **logging host** commands to specify additional servers that would all receive the syslog messages. For each server, you specify whether the server should receive messages using either the TCP or UDP protocol. You cannot specify a server to receive messages using both TCP and UDP.

To display *port* and *protocol* values that you entered previously, use the **show running-config logging** command and finding the command in the listing—the TCP protocol is listed as 6 and the UDP protocol is listed as 17. TCP ports work only with the FWSM syslog server. The *port* must be the same port on which the syslog server listens.

**Note** When the **tcp** option is used, the FWSM drops connections across the firewall if the syslog server is unreachable. To allow traffic through even when the TCP syslog server is down or unreachable, use the **permit-hostdown** keyword.

## Examples

The following example shows how to send syslog messages of severity levels 0, 1, 2, and 3 to a syslog server that resides on the inside interface and uses the default protocol and port number:

```
hostname(config)# logging host inside 10.2.2.3
hostname(config)# logging trap errors
hostname(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **logging trap** | Enables logging to syslog servers. |

# logging list

To create a list of message selection criteria to be used by other commands to specify which messages are sent to a particular output destination, use the **logging list** command in global configuration mode. To remove the list, use the **no** form of this command.

**logging list** *name* {**level** *level* [**class** *message_class*] | **message** *start_id*[**-***end_id*]}

**no logging list** *name*

## Syntax Description

| | |
|---|---|
| **class** *message_class* | (Optional) Specifies a class of syslog messages to be included in the list.<br>See "Usage Guidelines" for a list of classes. |
| **level** *level* | Sets the maximum level for syslog messages. For example, if you set the level to 3, then the FWSM generates syslog messages for level 3, 2, 1, and 0. You can specify either the number or the name, as follows:<br>• **0** or **emergencies**—System unusable.<br>• **1** or **alerts**—Take immediate action.<br>• **2** or **critical**—Critical condition.<br>• **3** or **errors**—Error.<br>• **4** or **warnings**—Warning.<br>• **5** or **notifications**—Normal but significant condition.<br>• **6** or **informational**—Information.<br>• **7** or **debugging**—Debug messages, log FTP commands, and WWW URLs.<br>To look up the default level of a message, use the **show logging** command or see the *Catalyst 6500 Series Switch and Cisco 7600 Series Internet Router Firewall Services Module System Message Guide*. |
| **message** *start_id*[**-***end_id*] | Specifies a message ID or range of message IDs. |
| *name* | Specifies the message list name. |

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | • | • | • | • |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## Usage Guidelines

When you enable a log output destination, you can also specify which syslog messages should be sent to that destination. The message list enables you to specify one or more sets of criteria that the FWSM uses to select messages to be sent to a single output destination.

Criteria you can specify for message selection include severity level, message class, a message ID, or a range of message IDs.

You can specify more than one set of criteria for a single message list. To add a new set of criteria, reissue the command specifying the list name and the new criteria. The new criteria is appended to the existing message list.

Logging commands with which you can use message lists are as follows:

- **logging asdm**
- **logging buffered**
- **logging console**
- **logging history**
- **logging mail**
- **logging monitor**
- **logging trap**

Possible values for the *message_class* include the following:

- **auth**—User authentication
- **bridge**—Transparent firewall
- **ca**—PKI certificate authority
- **config**—Command interface
- **e-mail**—E-mail proxy
- **ha**—Failover
- **ids**—Intrusion detection system
- **ip**—IP stack
- **np**—Network processor
- **ospf**—OSPF routing
- **rip**—RIP routing
- **session**—User session
- **snmp**—SNMP
- **sys**—System
- **vpn**—IKE and IPSec
- **vpnc**—VPN client
- **vpnfo**—VPN failover
- **vpnlb**—VPN load balancing

## Examples

The following example shows how to use the **logging list** command to create a new message list, append additional message selection criteria to the list, and specify that all messages matching the list criteria should be sent to the internal log buffer.

```
hostname(config)# logging list my-list 100100-100110
hostname(config)# logging list my-list level critical
hostname(config)# logging list my-list level warning class vpn
hostname(config)# logging buffered my-list
```

The message selection criteria specified in this example are:

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

If a syslog message satisfies any one of these conditions, it is logged to the internal log buffer.

**Note** When you design list criteria, criteria can specify overlapping sets of messages. Syslog messages matching more than one criteria are logged normally.

## Related Commands

| Command | Description |
|---|---|
| **show running-config logging** | Displays the logging-related portion of the running configuration. |

# logging mail

To enable the FWSM to send syslog messages by e-mail and to determine which messages are sent by e-mail, use the **logging mail** command in global configuration mode. To disable e-mailing syslog messages, use the **no** form of this command.

**logging mail** [*message_list* | *level*]

**no logging mail** [*message_list* | *level*]

## Syntax Description

| | |
|---|---|
| *level* | Sets the maximum severity level for logging event messages. For example, if you set the severity level to 3, then the FWSM generates syslog messages for severity levels 3, 2, and 1. You can specify either the number or the name, as follows:<br>• **0** or **emergencies**—System unusable.<br>• **1** or **alerts**—Take immediate action.<br>• **2** or **critical**—Critical condition.<br>• **3** or **errors**—Error.<br>• **4** or **warnings**—Warning.<br>• **5** or **notifications**—Normal but significant condition.<br>• **6** or **informational**—Information.<br>• **7** or **debugging**—Debug messages, log FTP commands, and WWW URLs. |
| *message_list* | Specifies the list that identifies the messages to send to the e-mail recipient. For information about creating message lists, see the **logging list** command. |

## Defaults

Logging to e-mail is disabled by default.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | • | • | • | — |

## Command History

| Release | Modification |
|---|---|
| Preexisting | This command was preexisting. |

## Usage Guidelines

E-mailed syslog messages appear in the subject line of the e-mails sent.

## Examples

The following example shows how to enable e-mail as an output destination, enabling syslog messages to be sent by e-mail. The example commands are based on the following example criteria:

- Send messages that are critical, alerts, or emergencies.
- Send messages using ciscosecurityappliance@example.com as the sender's address.
- Send messages to admin@example.com.
- Send messages using SMTP the primary servers pri-smtp-host and secondary server sec-smtp-host.

To enable the FWSM to e-mail system messages according the example criteria, enter the following commands:

```
hostname(config)# logging mail critical
hostname(config)# logging from-address ciscosecurityappliance@example.com
hostname(config)# logging recipient-address admin@example.com
hostname(config)# smtp-server pri-smtp-host sec-smtp-host
```

## Related Commands

| Command | Description |
|---|---|
| **logging from-address** | Specifies the e-mail address that appears in the From: line of each e-mailed syslog message. |
| **logging list** | Creates a reusable list of message selection criteria. |
| **logging recipient-address** | Specifies the e-mail address to which e-mailed syslog messages are sent. |
| **smtp-server** | Configures an SMTP server. |

# logging message

To change the severity level of a syslog message, use the **logging message** command with the **level** keyword in global configuration mode. To reset the logging level of a message to its default level, use the **no** form of this command.

**logging message** *syslog_id* **level** *level*

**no logging message** *syslog_id* **level** *level*

**logging message** *syslog_id*

**no logging message** *syslog_id*

## Syntax Description

| | |
|---|---|
| **level** *level* | Sets the maximum severity level for syslog messages. For example, if you set the severity level to 3, then the FWSM generates syslog messages for levels 3, 2, 1, and 0. You can specify either the number or the name, as follows:<br>• **0** or **emergencies**—System unusable.<br>• **1** or **alerts**—Take immediate action.<br>• **2** or **critical**—Critical condition.<br>• **3** or **errors**—Error.<br>• **4** or **warnings**—Warning.<br>• **5** or **notifications**—Normal but significant condition.<br>• **6** or **informational**—Information.<br>• **7** or **debugging**—Debug messages, log FTP commands, and WWW URLs. |
| *syslog_id* | The ID of the syslog message that you want to enable or disable or whose severity level you want to modify. To look up the default level of a message, use the **show logging** command or see the *Catalyst 6500 Series Switch and Cisco 7600 Series Internet Router Firewall Services Module System Message Guide*. |

## Defaults

By default, all syslog messages are enabled and the severity levels of all messages are set to their default levels.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | • | • | • | • |

## Command History

| Release | Modification |
|---|---|
| Preexisting | This command was preexisting. |

## Usage Guidelines

To prevent the FWSM from generating a particular syslog message, use the **no** form of the **logging message** command (without the **level** keyword) in global configuration mode. To let the FWSM generate a particular syslog message, use the **logging message** command (without the **level** keyword). These two purposes of the **logging message** command can be used in parallel. See the "Examples" section that follows.

You can use the **logging message** command for two purposes:

- To control whether a message is enabled or disabled.
- To change the severity level of a message.

You can use the **show logging** command to determine the severity level currently assigned to a message and whether the message is enabled.

## Examples

The series of commands in the following example illustrates the use of the **logging message** command to enable and disable messages and change the severity level of messages:

```
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)
```

## Related Commands

| Command | Description |
|---|---|
| **clear configure logging** | Clears all logging configuration or message configuration only. |
| **show running-config logging** | Displays the logging-related portion of the running configuration. |

# logging monitor

To enable the FWSM to display syslog messages in SSH and Telnet sessions, use the **logging monitor** command in global configuration mode. To disable the display of syslog messages in SSH and Telnet sessions, use the **no** form of this command.

**logging monitor** [*logging_list* | *level*]

**no logging monitor**

## Syntax Description

| | |
|---|---|
| *level* | Sets the maximum severity level for syslog messages. For example, if you set the severity level to 3, then the FWSM generates syslog messages for severity level 3, 2, 1, and 0. You can specify either the number or the name, as follows:<br>• **0** or **emergencies**—System unusable.<br>• **1** or **alerts**—Take immediate action.<br>• **2** or **critical**—Critical condition.<br>• **3** or **errors**—Error.<br>• **4** or **warnings**—Warning.<br>• **5** or **notifications**—Normal but significant condition.<br>• **6** or **informational**—Information.<br>• **7** or **debugging**—Debug messages, log FTP commands, and WWW URLs. |
| *logging_list* | Specifies the list that identifies the messages to send to the SSH or Telnet session. For information about creating lists, see the **logging list** command. |

## Defaults

The FWSM does not display syslog messages in SSH and Telnet sessions by default.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | • | • | • | — |

## Command History

| Release | Modification |
|---|---|
| Preexisting | This command was preexisting. |

## Usage Guidelines

The **logging monitor** command enables syslog messages for all sessions in the current context; however, in each session, the **terminal** command controls whether syslog messages appear in that session.

## Examples

The following example shows how to enable the display of syslog messages in console sessions. The use of the **errors** keyword indicates that messages of severity levels 0, 1, 2, and 3 should be shown in SSH and Telnet sessions. The **terminal** command enables the messages to appear in the current session.

```
hostname(config)# logging enable
hostname(config)# logging monitor errors
hostname(config)# terminal monitor
hostname(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **logging list** | Creates a reusable list of message selection criteria to identify messages that should be sent to a particular output destination. |
| **show logging** | Displays the enabled logging options. |
| **show running-config logging** | Displays the logging-related portion of the running configuration. |
| **terminal** | Sets terminal line parameters. |

# logging permit-hostdown

To specify that the FWSM should allow new network access sessions for a TCP-based syslog server that is not operational, use the **logging permit-hostdown** command in global configuration mode. To specify that the FWSM should deny new user sessions when a TCP-based syslog server is unavailable, use the **no** form of this command.

**logging permit-hostdown**

**no logging permit-hostdown**

## Syntax Description

This command has no arguments or keywords.

## Defaults

By default, if you have enabled logging to a syslog server that uses a TCP connection, the FWSM does not allow new network access sessions when the syslog server is unavailable for any reason.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | • | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## Usage Guidelines

If you are using TCP as the logging transport protocol for sending messages to a syslog server, the FWSM denies new network access sessions as a security measure if the FWSM is unable to reach the syslog server. You can use the **logging permit-hostdown** command to remove this restriction.

## Examples

The following example makes the status of TCP-based syslog servers irrelevant to whether the FWSM permits new sessions. When the **logging permit-hostdown** command includes in its output the **show running-config logging** command, the status of TCP-based syslog servers is irrelevant to new network access sessions.

```
hostname(config)# logging permit-hostdown
hostname(config)# show running-config logging
logging enable
logging trap errors
logging host infrastructure 10.1.2.3 6/1470
logging permit-hostdown
hostname(config)#
```

**Related Commands**

| Command | Description |
|---|---|
| **logging host** | Specifies a syslog server as an output destination. |
| **logging trap** | Enables logging to specified syslog servers. |

# logging queue

To specify how many syslog messages the FWSM can hold in its system log queue prior to processing them according to the current logging configuration, use the **logging queue** command in global configuration mode. To reset the logging queue size to the default of 512 messages, use the **no** form of this command.

**logging queue** *queue_size*

**no logging queue** *queue_size*

## Syntax Description

| | |
|---|---|
| *queue_size* | The number of syslog messages permitted in the queue used for storing syslog messages before processing them. Valid values are from 0 to 8192 messages. If the logging queue is set to zero, the queue will be the maximum configurable size (8192 messages). |

## Defaults

The default queue size is 512 messages.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | • | • | • | • |

## Command History

| Release | Modification |
|---|---|
| Preexisting | This command was preexisting. |

## Usage Guidelines

When traffic is so heavy that the queue fills up, the FWSM might discard messages.

## Examples

The following example shows how to display the output of the **logging queue** and **show logging queue** commands:

```
hostname(config)# logging queue 0
hostname(config)# show logging queue
Logging Queue length limit : Unlimited
Current 5 msg on queue, 3513 msgs most on queue, 1 msg discard.
```

In this example, the **logging queue** command is set to zero, which means that the queue is set to the maximum of 8192. The syslog messages in the queue are processed by the FWSM in the manner dictated by the current logging configuration, such as sending syslog messages to e-mail recipients, saving buffer overflows to internal flash memory, and so forth.

The sample output of the **show logging queue** command shows that five messages are queued, 3513 messages was the largest number of messages in the queue at one time because the FWSM was last booted, and that one message was discarded. Even though the queue was set for unlimited, the messages was discarded because no block memory was available to add the message to the queue.

## Related Commands

| Command | Description |
|---|---|
| **show logging** | Displays the enabled logging options. |
| **show running-config logging** | Displays the logging-related portion of the running configuration. |

# logging rate-limit

To limit the rate at which syslog messages are generated, use the **logging rate-limit** command in privileged EXEC mode. To disable rate limiting, use the **no** form of this command.

**logging rate-limit** {**unlimited** | {*num* [*interval*]}} **message** *syslog_id* | **level** *severity_level*

**[no] logging rate-limit** [**unlimited** | {**num** [*interval*]}} **message** *syslog_id* ] **level** *severity_level*

## Syntax Description

| | |
|---|---|
| *interval* | (Optional) Time interval (in seconds) to use for measuring the rate at which messages are generated. The valid range of values for *interval* is 0 through 2147483647. |
| **level** *severity_level* | Applies the set rate limits on all syslog messages that belong to a certain severity level. All syslog messages at a specified severity level are rate-limited individually. The valid range for *severity_level* is 1 through 7. |
| **message** | Suppresses reporting of this syslog message. |
| *num* | Number of system messages that can be generated during the specified time interval. The valid range of values for *num* is 0 through 2147483647. |
| *syslog_id* | ID of the syslog message to be suppressed. The valid range of values for *syslog_id* is 100000-999999. |
| **unlimited** | Disables rate limiting, which means that there is no limit on the logging rate. |

## Defaults

The default setting for *interval* is 1.

## Command Modes

The following table shows the modes in which you can enter the command:

| Command Mode | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| | Routed | Transparent | Single | Context | System |
| Privileged EXEC | • | • | • | • | • |

## Command History

| Release | Modification |
|---|---|
| 2.2(1) | This command was introduced in FWSM. |

## Usage Guidelines

The system message severity levels are as follows:

•0—System Unusable

•1—Take Immediate Action

•2—Critical Condition

•3—Error Message

•4—Warning Message

•5—Normal but significant condition

•6—Informational

•7—Debug Message

## Examples

The following example shows how to limit the rate of syslog message generation using a specific message ID and time interval:

```
fwsm(config)# logging rate-limit 100 600 message 302020
```

This example suppresses syslog message 302020 from being sent to the host after the rate-limit of 100 is reached in the specified interval of 600 seconds.

The following example shows how to limit the rate of syslog message generation using a specific severity level and time interval. To limit the rate of syslog message generation, you can enter a specific severity level:

```
fwsm(config)# logging rate-limit 1000 600 level 6
```

This example suppresses all syslog messages under severity level 6 to the specified rate-limit of 1000 in the specified time interval of 600 seconds. Each syslog message in severity level 6 has a rate-limit of 1000.

## Related Commands

| Command | Description |
|---|---|
| **clear running-config logging rate-limit** | Resets the logging rate-limit setting to its default. |
| **show logging** | Shows the messages currently in the internal buffer or logging configuration settings. |
| **show running-config logging rate-limit** | Shows the current logging rate-limit setting. |

# logging recipient-address

To specify the receiving e-mail address for syslog messages e-mailed by the FWSM, use the **logging recipient-address** command in global configuration mode. To remove the receiving e-mail address, use the **no** form of this command.

**logging recipient-address** *email_address* [**level** *level*]

**no logging recipient-address** *email_address* [**level** *level*]

## Syntax Description

| | |
|---|---|
| *email_address* | Specifies recipient e-mail address when sending syslog messages by e-mail. |
| **level** | Indicates that a logging level follows. |
| *level* | Sets the maximum severity level for syslog messages. For example, if you set the severity level to 3, then the FWSM generates syslog messages for levels 3, 2, 1, and 0. You can specify either the number or the name, as follows:<br>• **0** or **emergencies**—System unusable.<br>• **1** or **alerts**—Take immediate action.<br>• **2** or **critical**—Critical condition.<br>• **3** or **errors**—Error.<br>• **4** or **warnings**—Warning.<br>• **5** or **notifications**—Normal but significant condition.<br>• **6** or **informational**—Information.<br>• **7** or **debugging**—Debug messages, log FTP commands, and WWW URLs.<br>**Note** We do not recommend using a level greater than 3 with the **logging recipient-address** command. Higher logging levels are likely to cause dropped syslog messages due to buffer overflow.<br>The message level specified by a **logging recipient-address** command overrides the message level specified by the **logging mail** command. For example, if a **logging recipient-address** command specifies a level of 7 but the **logging mail** command specifies a severity level of 3, the FWSM sends all messages to the recipient, including those of severity levels 4, 5, 6, and 7. |

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | • | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## Usage Guidelines

You can configure up to five recipient addresses. You can choose to specify a different message level for each recipient address. The message level specified with this command takes precedence over the message level specified by the **logging mail** command.

Sending syslog messages by e-mail is enabled by the **logging mail** command.

You can configure up to five e-mail addresses to receive syslog messages from the FWSM. Enter a new command for each recipient you want to specify. Each recipient can have a different logging level than the others. This is useful when you want more urgent messages to go to a larger number of recipients than less urgent messages.

## Examples

The following example shows how to set up the FWSM to send a limited number of syslog messages by e-mail. The example commands are based on the following example criteria:

- Send messages that are critical, alerts, or emergencies.
- Send messages using ciscosecurityappliance@example.com as the address of the sender.
- Send messages to admin@example.com.
- Send messages using SMTP the primary servers pri-smtp-host and secondary server sec-smtp-host.

To enable the FWSM to e-mail system messages according to the example criteria, enter the following commands:

```
hostname(config)# logging mail critical
hostname(config)# logging from-address ciscosecurityappliance@example.com
hostname(config)# logging recipient-address admin@example.com
hostname(config)# smtp-server pri-smtp-host sec-smtp-host
```

## Related Commands

| Command | Description |
|---|---|
| **logging enable** | Enables logging to all specified output locations. |
| **logging from-address** | Specifies the e-mail address that appears in the From: line of each e-mailed syslog message. |
| **logging mail** | Enables the FWSM to send syslog messages by e-mail and specifies which messages are sent by e-mail. |
| **smtp-server** | Configures an SMTP server. |
| **show logging** | Displays the enabled logging options. |
| **show running-config logging** | Displays the currently running logging configuration. |

# logging savelog

To save the current contents of the log buffer to internal flash memory, use the **logging savelog** command in privileged EXEC mode.

**logging savelog** [*savefile*]

## Syntax Description

| | |
|---|---|
| *savefile* | (Optional) File name to use for saving log data to internal flash memory. If you do not specify a file name, the FWSM saves the file using a default time-stamp format, as follows:<br>`LOG-YYYY-MM-DD-HHMMSS.TXT`<br>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. |

## Defaults

The defaults are as follows:

- Buffer size is 4 KB.
- Minimum free flash memory is 3 MB.
- Maximum flash memory allocation for buffer logging is 1 MB.
- The default log file name is described in the preceding table.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Privileged EXEC | • | • | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## Usage Guidelines

Before you can save the contents of the log buffer to internal flash memory, you must enable logging to the buffer; if logging to the buffer is not enabled, the FWSM does not save syslog messages to the buffer, and therefore the buffer is empty. To enable logging to the buffer, use the **logging buffered** command.

**Note** The **logging savelog** command does not clear the buffer. To clear the buffer, use the **clear logging buffer** command.

## Examples

The following example enables the log buffer as an output destination, exits global configuration mode, and saves the log buffer to internal flash memory, using the file name latest-logfile.txt:

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

## Related Commands

| Command | Description |
|---|---|
| **clear logging buffer** | Clears the log buffer of all syslog messages it contains. |
| **copy** | Copies a file from one location to another, including to a TFTP or FTP server. |
| **delete** | Deletes a file from the disk partition, such as saved log files. |
| **logging buffered** | Enables logging to the internal log buffer. |
| **show logging** | Displays contents of the internal log buffer and the enabled logging options. |

# logging standby

To enable the failover standby FWSM to send the syslog messages of this FWSM to configured logging destinations, use the **logging standby** command in global configuration mode. To disable system log and SNMP logging, use the **no** form of this command.

**logging standby**

**no logging standby**

## Syntax Description

This command has no arguments or keywords.

## Defaults

The **logging standby** command is disabled by default.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | • | • | • | • |

## Command History

| Release | Modification |
|---|---|
| Preexisting | This command was preexisting. |

## Usage Guidelines

You can enable **logging standby** to ensure that the syslog messages of the failover standby FWSM stay synchronized if failover occurs.

**Note** Using the **logging standby** command creates twice as much traffic on shared logging destinations, such as syslog servers, SNMP servers, and FTP servers.

## Examples

The following example enables the FWSM to send syslog messages to the failover standby FWSM. The output of the **show logging** command reveals that this feature is enabled.

```
hostname(config)# logging standby
hostname(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: enabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
```

```
Trap logging: disabled
History logging: disabled
Device ID: 'inside' interface IP address "10.1.1.1"
Mail logging: disabled
ASDM logging: disabled
```

## Related Commands

| Command | Description |
|---|---|
| **failover** | Enables the failover feature. |
| **logging host** | Defines a syslog server. |
| **show running-config logging** | Displays the logging-related portion of the running configuration. |

# logging timestamp

To specify that syslog messages should include the date and time that the messages was generated, use the **logging timestamp** command in global configuration mode. To remove the date and time from syslog messages, use the **no** form of this command.

**logging timestamp**

**no logging timestamp**

## Syntax Description

This command has no arguments or keywords.

## Defaults

The FWSM does not include the date and time in syslog messages by default.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | • | • | • | — |

## Command History

| Release | Modification |
|---|---|
| Preexisting | This command was preexisting. |

## Usage Guidelines

The **logging timestamp** command causes the FWSM to include a timestamp in all syslog messages.

## Examples

The following example enables the inclusion of timestamp information in all syslog messages:

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

## Related Commands

| Command | Description |
|---|---|
| **logging enable** | Enables logging to all specified output destinations. |
| **show logging** | Displays contents of the internal log buffer and the enabled logging options. |
| **show running-config logging** | Displays the logging-related portion of the running configuration. |

# login

To log in to privileged EXEC mode using the local user database (see the **username** command) or to change usernames, use the **login** command in user EXEC mode.

**login**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| User EXEC | • | • | • | • | • |

## Command History

| Release | Modification |
|---|---|
| 1.1(1) | This command was introduced. |

## Usage Guidelines

From user EXEC mode, you can log in to privileged EXEC mode as any username in the local database using the **login** command. The **login** command is similar to the **enable** command when you have enable authentication turned on (see the **aaa authentication console** command). Unlike enable authentication, the **login** command can only use the local username database, and authentication is always required with this command. You can only use the **login** command in user EXEC mode. If you are already in privileged EXEC mode, you need to enter the **disable** command to go back to user EXEC mode where you can enter the **login** command.

To allow users to access privileged EXEC mode (and all commands) when they log in, set the user privilege level to 2 (the default) through 15. If you configure local command authorization, then the user can only enter commands assigned to that privilege level or lower. See the **aaa authorization command** for more information.

When you use the **login** command in the system execution space, the FWSM uses the username database in the admin context. You cannot enter the **username** command directly in the system execution space.

**Caution** If you add users to the local database who can gain access to the CLI and whom you do not want to enter privileged EXEC mode, you should configure command authorization. Without command authorization, users can access privileged EXEC mode (and all commands) at the CLI using their own password if their privilege level is 2 or greater (2 is the default). Alternatively, you can use RADIUS or TACACS+ authentication, or you can set all local users to level 1 so you can control who can use the system enable password to access privileged EXEC mode.

## Examples

The following example shows the prompt after you enter the **login** command:

```
hostname> login
Username:
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authorization command** | Enables command authorization for CLI access. |
| **aaa authentication console** | Requires authentication for console, Telnet, HTTP, SSH, or **enable** command access. |
| **logout** | Logs out of the CLI. |
| **username** | Adds a user to the local database. |

# logout

To exit from the CLI, use the **logout** command in user EXEC mode.

**logout**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No default behaviors of values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| User EXEC | • | • | • | • | • |

## Command History

| Release | Modification |
|---|---|
| 1.1(1) | This command was introduced. |

## Usage Guidelines

The **logout** command lets you log out of the FWSM. You can use the **exit** or **quit** commands to go back to user EXEC mode.

## Examples

The following example shows how to log out of the FWSM:

```
hostname> logout
```

## Related Commands

| Command | Description |
|---|---|
| **login** | Initiates the log-in prompt. |
| **exit** | Exits an access mode. |
| **quit** | Exits configuration or privileged mode. |