Configuring Logging

This chapter describes how to configure and manage logs for the ASASM/ASASM and includes the following sections:

- Information About Logging, page 52-1
- Licensing Requirements for Logging, page 52-5
- Prerequisites for Logging, page 52-5
- Guidelines and Limitations, page 52-5
- Configuring Logging, page 52-6
- Monitoring the Logs, page 52-19
- Configuration Examples for Logging, page 52-20
- Feature History for Logging, page 52-20

Information About Logging

System logging is a method of collecting messages from devices to a server running a syslog daemon. Logging to a central syslog server helps in aggregation of logs and alerts. Cisco devices can send their log messages to a UNIX-style syslog service. A syslog service accepts messages and stores them in files, or prints them according to a simple configuration file. This form of logging provides protected long-term storage for logs. Logs are useful both in routine troubleshooting and in incident handling.

The ASASM system logs provide you with information for monitoring and troubleshooting the ASASM. With the logging feature, you can do the following:

- Specify which syslog messages should be logged.
- Disable or change the severity level of a syslog message.
- Specify one or more locations where syslog messages should be sent, including an internal buffer, one or more syslog servers, ASDM, an SNMP management station, specified e-mail addresses, or to Telnet and SSH sessions.
- Configure and manage syslog messages in groups, such as by severity level or class of message.
- Specify whether or not a rate-limit is applied to syslog generation.
- Specify what happens to the contents of the internal log buffer when it becomes full: overwrite the buffer, send the buffer contents to an FTP server, or save the contents to internal flash memory.
- Filter syslog messages by locations, severity level, class, or a custom message list.
Information About Logging

This section includes the following topics:

- Logging in Multiple Context Mode, page 52-2
- Analyzing Syslog Messages, page 52-2
- Syslog Message Format, page 52-3
- Severity Levels, page 52-3
- Message Classes and Range of Syslog IDs, page 52-4
- Filtering Syslog Messages, page 52-4
- Using Custom Message Lists, page 52-4

Logging in Multiple Context Mode

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

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

You can configure the ASASM/ASASM to include the context name with each message, which helps you differentiate context messages that are sent to a single syslog server. This feature also helps you to determine which messages are from the admin context and which are from the system; messages that originate in the system execution space use a device ID of `system`, and messages that originate in the admin context use the name of the admin context as the device ID.

Analyzing Syslog Messages

The following are some examples of the type of information you can obtain from a review of various syslog messages:

- Connections that are allowed by ASASM/ASASM security policies. These messages help you spot holes that remain open in your security policies.
- Connections that are denied by ASASM/ASASM security policies. These messages show what types of activity are being directed toward your secured inside network.
- Using the ACE deny rate logging feature shows attacks that are occurring on your ASASM/ASASM.
- IDS activity messages can show attacks that have occurred.
- User authentication and command usage provide an audit trail of security policy changes.
- Bandwidth usage messages show each connection that was built and torn down as well as the duration and traffic volume used.
- Protocol usage messages show the protocols and port numbers used for each connection.
- Address translation audit trail messages record NAT or PAT connections being built or torn down, which are useful if you receive a report of malicious activity coming from inside your network to the outside world.
Syslog Message Format

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

```
%ASA Level Message_number: Message_text
```

Field descriptions are as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASASM</td>
<td>The syslog message facility code for messages that are generated by the ASASM/ASASM. This value is always ASA.</td>
</tr>
<tr>
<td>Level</td>
<td>1 through 7. The level reflects the severity of the condition described by the syslog message—the lower the number, the more severe the condition. See Table 52-1 for more information.</td>
</tr>
<tr>
<td>Message_number</td>
<td>A unique six-digit number that identifies the syslog message.</td>
</tr>
<tr>
<td>Message_text</td>
<td>A text string that describes the condition. This portion of the syslog message sometimes includes IP addresses, port numbers, or usernames.</td>
</tr>
</tbody>
</table>

Severity Levels

Table 52-1 lists the syslog message severity levels. You can assign custom colors to each of the severity levels to make it easier to distinguish them in the ASDM log viewers. To configure syslog message color settings, either choose the Tools > Preferences > Syslog tab or, in the log viewer itself, click Color Settings on the toolbar.

Table 52-1 Syslog Message Severity Levels

<table>
<thead>
<tr>
<th>Level Number</th>
<th>Severity Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>emergencies</td>
<td>System is unusable.</td>
</tr>
<tr>
<td>1</td>
<td>alert</td>
<td>Immediate action is needed.</td>
</tr>
<tr>
<td>2</td>
<td>critical</td>
<td>Critical conditions.</td>
</tr>
<tr>
<td>3</td>
<td>error</td>
<td>Error conditions.</td>
</tr>
<tr>
<td>4</td>
<td>warning</td>
<td>Warning conditions.</td>
</tr>
<tr>
<td>5</td>
<td>notification</td>
<td>Normal but significant conditions.</td>
</tr>
<tr>
<td>6</td>
<td>informational</td>
<td>Informational messages only.</td>
</tr>
<tr>
<td>7</td>
<td>debugging</td>
<td>Debugging messages only.</td>
</tr>
</tbody>
</table>

Note

The ASASM/ASASM does not generate syslog messages with a severity level of zero (emergencies). This level is provided in the logging command for compatibility with the UNIX syslog feature but is not used by the ASASM.
**Message Classes and Range of Syslog IDs**

For a list of syslog message classes and the ranges of syslog message IDs that are associated with each class, see the syslog messages guide.

**Filtering Syslog Messages**

You can filter generated syslog messages so that only certain syslog messages are sent to a particular output destination. For example, you could configure the ASASM/ASASM to send all syslog messages to one output destination and to send a subset of those syslog messages to a different output destination. Specifically, you can configure the ASASM/ASASM so that syslog messages are directed to an output destination according to the following criteria:

- Syslog message ID number
- Syslog message severity level
- Syslog message class (equivalent to a functional area of the ASASM/ASASM)

You customize these criteria by creating a message list that you can specify when you set the output destination. Alternatively, you can configure the ASASM/ASASM to send a particular message class to each type of output destination independently of the message list.

You can use syslog message classes in two ways:

- Specify an output location for an entire category of syslog messages using the **logging class** command.
- Create a message list that specifies the message class using the **logging list** command.

The syslog message class provides a method of categorizing syslog messages by type, equivalent to a feature or function of the ASASM/ASASM. For example, the vpnc class denotes the VPN client. All syslog messages in a particular class share the same initial three digits in their syslog message ID numbers. For example, all syslog message IDs that begin with the digits 611 are associated with the vpnc (VPN client) class. Syslog messages associated with the VPN client feature range from 611101 to 611323.

In addition, most of the ISAKMP syslog messages have a common set of prepended objects to help identify the tunnel. These objects precede the descriptive text of a syslog message when available. If the object is not known at the time that the syslog message is generated, the specific **heading = value** combination does not appear.

The objects are prefixed as follows:

- Group = *groupname*, Username = *user*, IP = *IP_address*

Where the group is the tunnel-group, the username is the username from the local database or AAA server, and the IP address is the public IP address of the remote access client or L2L peer.

**Using Custom Message Lists**

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

For example, you can use message lists to do the following:
Select syslog messages with the severity levels of 1 and 2 and send them to one or more e-mail addresses.

Select all syslog messages associated with a message class (such as ha) and save them to the internal buffer.

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

**Licensing Requirements for Logging**

The following table shows the licensing requirements for this feature:

<table>
<thead>
<tr>
<th>Model</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>All models</td>
<td>Base License.</td>
</tr>
</tbody>
</table>

**Prerequisites for Logging**

Logging has the following prerequisites:

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

- To view logs generated by the ASASM/ASASM, you must specify a logging output destination. If you enable logging without specifying a logging output destination, the ASASM/ASASM generates messages but does not save them to a location from which you can view them. You must specify each different logging output destination separately. For example, to designate more than one syslog server as an output destination, enter a new command for each syslog server.

**Guidelines and Limitations**

This section includes the guidelines and limitations for this feature.

**Context Mode Guidelines**
Supported in single and multiple context modes.

**Firewall Mode Guidelines**
Supported in routed and transparent firewall modes.

**IPv6 Guidelines**
Does not support IPv6.

**Additional Guidelines**
- Sending syslogs over TCP is not supported on a standby ASASM.
The ASASM supports the configuration of 16 syslog servers with the `logging host` command in single context mode. In multiple context mode, the limitation is 4 servers per context.

## Configuring Logging

This section describes how to configure logging and includes the following topics:

- Enabling Logging, page 52-6
- Configuring an Output Destination, page 52-6

**Note**

The minimum configuration depends on what you want to do and what your requirements are for handling syslog messages in the ASASM/ASASM.

### Enabling Logging

To enable logging, enter the following command:

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>logging enable</td>
<td>Enables logging. To disable logging, enter the <code>no logging enable</code> command.</td>
</tr>
</tbody>
</table>

**Example:**

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

### Configuring an Output Destination

To optimize syslog message usage for troubleshooting and performance monitoring, we recommend that you specify one or more locations where syslog messages should be sent, including an internal log buffer, one or more external syslog servers, ASDM, an SNMP management station, the console port, specified e-mail addresses, or Telnet and SSH sessions.

This section includes the following topics:

- Sending Syslog Messages to an External Syslog Server, page 52-8
- Sending Syslog Messages to the Internal Log Buffer, page 52-9
- Sending Syslog Messages to an E-mail Address, page 52-10
- Sending Syslog Messages to ASDM, page 52-11
- Sending Syslog Messages to the Console Port, page 52-11
- Sending Syslog Messages to an SNMP Server, page 52-12
- Sending Syslog Messages to a Telnet or SSH Session, page 52-12
- Creating a Custom Event List, page 52-13
• Generating Syslog Messages in EMBLEM Format to a Syslog Server, page 52-14
• Generating Syslog Messages in EMBLEM Format to Other Output Destinations, page 52-14
• Changing the Amount of Internal Flash Memory Available for Logs, page 52-15
• Configuring the Logging Queue, page 52-15
• Sending All Syslog Messages in a Class to a Specified Output Destination, page 52-16
• Enabling Secure Logging, page 52-16
• Including the Device ID in Non-EMBLEM Format Syslog Messages, page 52-17
• Including the Date and Time in Syslog Messages, page 52-18
• Disabling a Syslog Message, page 52-18
• Changing the Severity Level of a Syslog Message, page 52-18
• Limiting the Rate of Syslog Message Generation, page 52-19
Sending Syslog Messages to an External Syslog Server

You can archive messages according to the available disk space on the external syslog server, and manipulate logging data after it is saved. For example, you could specify actions to be executed when certain types of syslog messages are logged, extract data from the log and save the records to another file for reporting, or track statistics using a site-specific script.

To send syslog messages to an external syslog server, perform the following steps:

### Command Purpose

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | **logging host interface_name syslog_ip [tcp[/port] | udp[/port] [format emblem]]** | Configures the ASASM/ASASM to send messages to a syslog server. The **format emblem** keyword enables EMBLEM format logging for the syslog server with UDP only. The **interface_name** argument specifies the interface through which you access the syslog server. The **syslog_ip** argument specifies the IP address of the syslog server. The tcp[/port] or udp[/port] keyword and argument pair specify that the ASASM and ASASM should use TCP or UDP to send syslog messages to the syslog server.

You can configure the ASASM to send data to a syslog server using either UDP or TCP, but not both. The default protocol is UDP if you do not specify a protocol. If you specify TCP, the ASASM/ASASM discover when the syslog server fails and as a security protection, new connections through the ASASM/ASASM are blocked. To allow new connections regardless of connectivity to a TCP syslog server, see Step 3. If you specify UDP, the ASASM/ASASM continue to allow new connections whether or not the syslog server is operational. Valid port values for either protocol are 1025 through 65535. The default UDP port is 514. The default TCP port is 1470. **Example:**

```
hostname(config)# logging host dmz1 192.168.1.5 udp 1026 format emblem
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 2** | **logging trap {severity_level | message_list}** | Specifies which syslog messages should be sent to the syslog server. You can specify the severity level number (1 through 7) or name. For example, if you set the severity level to 3, then the ASASM/ASASM send syslog messages for severity levels 3, 2, and 1. You can specify a custom message list that identifies the syslog messages to send to the syslog server. **Example:**

```
hostname(config)# logging trap errors
```
Sending Syslog Messages to the Internal Log Buffer

To send syslog messages to the internal log buffer, perform the following steps:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> logging buffered</td>
<td>Specifies which syslog messages should be sent to the internal log buffer, which serves as a temporary storage location. New messages are appended to the end of the list. When the buffer is full, that is, when the buffer wraps, old messages are overwritten as new messages are generated, unless you configure the ASASM/ASASM to save the full buffer to another location. To empty the internal log buffer, enter the <code>clear logging buffer</code> command.</td>
</tr>
<tr>
<td>(severity_level</td>
<td>message_list)</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>hostname(config)# logging buffered critical</td>
<td></td>
</tr>
<tr>
<td>hostname(config)# logging buffered level 2</td>
<td></td>
</tr>
<tr>
<td>hostname(config)# logging buffered notif-list</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> logging buffer-size bytes</td>
<td>Changes the size of the internal log buffer. The buffer size is 4 KB.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>hostname(config)# logging buffer-size 16384</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> Choose one of the following options:</td>
<td></td>
</tr>
</tbody>
</table>
| logging flash-bufferwrap         | When saving the buffer content to another location, the ASASM/ASASM create log files with names that use the following time-stamp format:
| Example:                         | LOG-YYYY-MM-DD-HHMMSS.TXT
| hostname(config)# logging flash-bufferwrap | 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 ASASM/ASASM continues to save new messages to the internal log buffer and saves the full log buffer content to the internal flash memory. |
Chapter 52  Configuring Logging

Configuring Logging

Sending Syslog Messages to an E-mail Address

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td>logging mail {severity_level</td>
<td>message_list}</td>
</tr>
<tr>
<td>Example:</td>
<td>hostname(config)# logging mail high-priority</td>
</tr>
</tbody>
</table>

| Step 2  |         |
| logging from-address email_address | Specifies the source e-mail address to be used when sending syslog messages to an e-mail address. |
| Example: | hostname(config)# logging from-address xxx-001@example.com |

Command  Purpose

logging ftp-bufferwrap

Example:
hostname(config)# logging ftp-bufferwrap

When saving the buffer content to another location, the ASASM/ASASM creates log files with names that use the following time-stamp format:

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 ASASM/ASASM continues saving new messages to the internal log buffer and saves the full log buffer content to an FTP server.

logging ftp-server server path username password

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

Identifies the FTP server on which you want to store log buffer content. The server argument specifies the IP address of the external FTP server. The path argument specifies the directory path on the FTP server where the log buffer data is to be saved. This path is relative to the FTP root directory. The username argument specifies a username that is valid for logging into the FTP server. The password argument indicates the password for the username specified.

logging savelog [savefile]

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

Saves the current log buffer content to the internal flash memory.

Step 1

logging mail {severity_level | message_list} | Specifies which syslog messages should be sent to an e-mail address. When sent by e-mail, the device name appears in the subject line of the e-mail message and the syslog message appears in the body of the e-mail message. For this reason, we recommend configuring this option to notify administrators of syslog messages with high severity levels, such as critical, alert, and emergency. |

Example: | hostname(config)# logging mail high-priority |

Step 2

logging from-address email_address | Specifies the source e-mail address to be used when sending syslog messages to an e-mail address. |

Example: | hostname(config)# logging from-address xxx-001@example.com |
### Configuring Logging

#### Sending Syslog Messages to ASDM

To send syslog messages to ASDM, perform the following steps:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>`logging asdm {severity_level</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>hostname(config)# logging asdm 2</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>logging asdm-buffer-size num_of_msgs</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>hostname(config)# logging asdm-buffer-size 200</code></td>
</tr>
</tbody>
</table>

---

### Sending Syslog Messages to the Console Port

To send syslog messages to the console port, enter the following command:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`logging console {severity_level</td>
<td>message_list}`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>hostname(config)# logging console errors</code></td>
</tr>
</tbody>
</table>
## Sending Syslog Messages to an SNMP Server

To enable logging to an SNMP server, enter the following command:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`logging history [logging_list</td>
<td>Enables SNMP logging and specifies which messages are to be sent to SNMP servers. To disable SNMP logging, enter the <code>no logging history</code> command.</td>
</tr>
<tr>
<td>level]`</td>
<td></td>
</tr>
</tbody>
</table>

**Example:**
```
hostname(config)# logging history errors
```

## Sending Syslog Messages to a Telnet or SSH Session

To send syslog messages to a Telnet or SSH session, perform the following steps:

**Step 1**
```
logging monitor (severity_level | message_list)
```

**Example:**
```
hostname(config)# logging monitor 6
```

**Step 2**
```
terminal monitor
```

**Example:**
```
hostname(config)# terminal monitor
```

Enables logging to the current session only. If you log out and then log in again, you need to reenter this command. To disable logging to the current session, enter the `terminal no monitor` command.
# Creating a Custom Event List

To create a custom event list, perform the following steps:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
**logging list** name {**level** level [**class** message_class] | message start_id[-end_id])

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

Specifies criteria for selecting messages to be saved in the internal log buffer. For example, if you set the severity level to 3, then the ASASM sends syslog messages for severity levels 3, 2, and 1.
The **name** argument specifies the name of the list. The **level level** keyword and argument pair specify the severity level. The **class message_class** keyword and argument pair specify a particular message class. The **message start_id[-end_id]** keyword and argument pair specify an individual syslog message number or a range of numbers.

**Note** Do not use the names of severity levels as the name of a syslog message list. Prohibited names include emergencies, alert, critical, error, warning, notification, informational, and debugging. Similarly, do not use the first three characters of these words at the beginning of an event list name. For example, do not use an event list name that starts with the characters err.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 2**
**logging list** name {**level** level [**class** message_class] | message start_id[-end_id])

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

(Optional) Adds more criteria for message selection to the list. Enter the same command as in the previous step, specifying the name of the existing message list and the additional criterion. Enter a new command for each criterion that you want to add to the list. For example, you can specify criteria for syslog messages to be included in the list as the following:

- Syslog message IDs that fall into the range of 104024 to 105999.
- All syslog messages with the critical severity level or higher (emergency, alert, or critical).
- All ha class syslog messages with the warning severity level or higher (emergency, alert, critical, error, or warning).

**Note** A syslog message is logged if it satisfies any of these conditions. If a syslog message satisfies more than one of the conditions, the message is logged only once.
Generating Syslog Messages in EMBLEM Format to a Syslog Server

To generate syslog messages in EMBLEM format to a syslog server, enter the following command:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>logging host interface_name ip_address {tcp[/port]</td>
<td>udp[/port]} [format emblem]</td>
</tr>
</tbody>
</table>

Example:
hostname(config)# logging host interface_1 127.0.0.1 udp format emblem

Generating Syslog Messages in EMBLEM Format to Other Output Destinations

To generate syslog messages in EMBLEM format to other output destinations, enter the following command:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>logging emblem</td>
<td>Sends syslog messages in EMBLEM format to output destinations other than a syslog server, such as Telnet or SSH sessions.</td>
</tr>
</tbody>
</table>

Example:
hostname(config)# logging emblem
Changing the Amount of Internal Flash Memory Available for Logs

To change the amount of internal flash memory available for logs, perform the following steps:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>logging flash-maximum-allocation kbytes</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;hostname(config)# logging flash-maximum-allocation 1200</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>logging flash-minimum-free kbytes</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;hostname(config)# logging flash-minimum-free 4000</td>
</tr>
</tbody>
</table>

Configuring the Logging Queue

To configure the logging queue, enter the following command:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **logging queue message_count**<br>**Example:**<br>hostname(config)# logging queue 300 | Specifies the number of syslog messages that the ASASM/ASASM can hold in its queue before sending them to the configured output destination. The ASASM/ASASM has a fixed number of blocks in memory that can be allocated for buffering syslog messages while they are waiting to be sent to the configured output destination. The number of blocks required depends on the length of the syslog message queue and the number of syslog servers specified. The default queue size is 512 syslog messages. The queue size is limited only by block memory availability. Valid values are from 0 to 8192 messages, depending on the platform. If the logging queue is set to zero, the queue is the maximum configurable size (8192 messages), depending on the platform. The maximum queue size by platform is as follows:
- ASA-5505—1024
- ASA-5510—2048
- On all other platforms—8192 |
Sending All Syslog Messages in a Class to a Specified Output Destination

To send all syslog messages in a class to a specified output destination, enter the following command:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`logging class message_class {buffered</td>
<td>console</td>
</tr>
</tbody>
</table>

Example:
```
hostname(config)# logging class ha buffered alerts
```

Enabling Secure Logging

To enable secure logging, enter the following command:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`logging host interface_name syslog_ip [tcp/port</td>
<td>udp/port] [format emblem] [secure]`</td>
</tr>
</tbody>
</table>

Example:
```
hostname(config)# logging host inside 10.0.0.1 TCP/1500 secure
```


Including the Device ID in Non-EMBLEM Format Syslog Messages

To include the device ID in non-EMBLEM format syslog messages, enter the following command:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| logging device-id [context-name | hostname | ipaddress interface_name | string text] | Configures the ASASM/ASASM to include a device ID in non-EMBLEM-format syslog messages. You can specify only one type of device ID for syslog messages. The **context-name** keyword indicates that the name of the current context should be used as the device ID (applies to multiple context mode only). If you enable the logging device ID for the admin context in multiple context mode, messages that originate in the system execution space use a device ID of **system**, and messages that originate in the admin context use the name of the admin context as the device ID. The **hostname** keyword specifies that the hostname of the ASASM should be used as the device ID. The **ipaddress interface_name** keyword and argument pair specify that the interface IP address specified as **interface_name** should be used as the device ID. If you use the **ipaddress** keyword, the device ID becomes the specified ASASM interface IP address, regardless of the interface from which the syslog message is sent. This keyword provides a single, consistent device ID for all syslog messages that are sent from the device. The **string text** keyword and argument pair specify that the text string should be used as the device ID. The string can include as many as 16 characters. You cannot use blank spaces or any of the following characters:

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

**Note** If enabled, the device ID does not appear in EMBLEM-formatted syslog messages nor in SNMP traps.

Example:

hostname(config)# logging device-id hostname
hostname(config)# logging device-id context-name
Including the Date and Time in Syslog Messages

To include the date and time in syslog messages, enter the following command:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>logging timestamp</code></td>
<td>Specifies that syslog messages should include the date and time that they were generated. To remove the date and time from syslog messages, enter the <code>no logging timestamp</code> command.</td>
</tr>
</tbody>
</table>

Example:
```
hostname(config)# logging timestamp
LOG-2008-10-24-081856.TXT
```

Disabling a Syslog Message

To disable a specified syslog message, enter the following command:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no logging message message_number</code></td>
<td>Prevents the ASASM/ASASM from generating a particular syslog message. To reenable a disabled syslog message, enter the <code>logging message message_number</code> command (for example, <code>logging message 113019</code>). To reenable logging of all disabled syslog messages, enter the <code>clear config logging disabled</code> command.</td>
</tr>
</tbody>
</table>

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

Changing the Severity Level of a Syslog Message

To change the severity level of a syslog message, enter the following command:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>logging message message_ID level severity_level</code></td>
<td>Specifies the severity level of a syslog message. To reset the severity level of a syslog message to its setting, enter the <code>no logging message message_ID level current_severity_level</code> command (for example, <code>no logging message 113019 level 5</code>). To reset the severity level of all modified syslog messages to their settings, enter the <code>clear configure logging level</code> command.</td>
</tr>
</tbody>
</table>

Example:
```
hostname(config)# logging message 113019 level 5
```
Limiting the Rate of Syslog Message Generation

To limit the rate of syslog message generation, enter the following command:

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

Example:
```
hostname(config)# logging rate-limit 1000 600 level 6
```

Monitoring the Logs

To monitor the logs and assist in monitoring the system performance, enter one of the following commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show logging</td>
<td>Shows syslog messages, including the severity level.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>  The maximum number of syslog messages that are available to view is 1000, which is the default setting. The maximum number of syslog messages that are available to view is 2000.</td>
</tr>
<tr>
<td>show logging message</td>
<td>Shows a list of syslog messages with modified severity levels and disabled syslog messages.</td>
</tr>
<tr>
<td>show logging message message_ID</td>
<td>Shows the severity level of a specific syslog message.</td>
</tr>
<tr>
<td>show logging queue</td>
<td>Shows the logging queue and queue statistics.</td>
</tr>
<tr>
<td>show logging rate-limit</td>
<td>Shows the disallowed syslog messages.</td>
</tr>
<tr>
<td>show running-config logging rate-limit</td>
<td>Shows the current logging rate-limit setting.</td>
</tr>
</tbody>
</table>

Examples

The following example shows the logging information that displays for the `show logging` command:

```
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
```
Configuration Examples for Logging

The following examples show how to control both whether a syslog message is enabled and the severity level of the specified syslog message:

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

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

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

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

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

Feature History for Logging

Table 52-2 lists each feature change and the platform release in which it was implemented.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging</td>
<td>7.0(1)</td>
<td>Provides ASASM network logging information through various output destinations, and includes the option to view and save log files.</td>
</tr>
<tr>
<td>Rate limit</td>
<td>7.0(4)</td>
<td>Limits the rate at which syslog messages are generated. We introduced the following command: logging rate-limit.</td>
</tr>
<tr>
<td>Logging list</td>
<td>7.2(1)</td>
<td>Creates a logging list to use in other commands to specify messages by various criteria (logging level, event class, and message IDs). We introduced the following command: logging list.</td>
</tr>
</tbody>
</table>
Secure logging 8.0(2) Specifies that the connection to the remote logging host should use SSL/TLS. This option is valid only if the protocol selected is TCP. We modified the following command: `logging host`.

Logging class 8.0(4), 8.1(1) Added support for the ipaa event class of logging messages. We modified the following command: `logging class`.

Logging class and saved logging buffers 8.2(1) Added support for the dap event class of logging messages. We modified the following command: `logging class`. Added support to clear the saved logging buffers (ASDM, internal, FTP, and flash). We introduced the following command: `clear logging queue bufferwrap`.

Password encryption 8.3(1) Added support for password encryption. We modified the following command: `logging ftp server`.

Enhanced logging and connection blocking 8.3(2) When you configure a syslog server to use TCP, and the syslog server is unavailable, the ASASM blocks new connections that generate syslog messages until the server becomes available again (for example, VPN, firewall, and cut-through-proxy connections). This feature has been enhanced to also block new connections when the logging queue on the ASASM is full; connections resume when the logging queue is cleared.

This feature was added for compliance with Common Criteria EAL4+. Unless required, we recommend allowing connections when syslog messages cannot be sent or received. To allow connections, continue to use the `logging permit-hostdown` command.

We modified the following command: `show logging`.

We introduced the following syslog messages: 414005, 414006, 414007, and 414008.