



CHAPTER 29

Configuring Logging

This chapter describes how to configure and manage logs for the ASA 1000V and includes the following sections:

- [Information About Logging, page 29-1](#)
- [Prerequisites for Logging, page 29-4](#)
- [Guidelines and Limitations, page 29-5](#)
- [Configuring Logging, page 29-5](#)
- [Monitoring the Logs, page 29-18](#)
- [Configuration Examples for Logging, page 29-18](#)
- [Feature History for Logging, page 29-19](#)

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 ASA 1000V system logs provide you with information for monitoring and troubleshooting the ASA 1000V. 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.

This section includes the following topics:

- [Analyzing Syslog Messages, page 29-2](#)
- [Syslog Message Format, page 29-2](#)
- [Severity Levels, page 29-3](#)
- [Message Classes and Range of Syslog IDs, page 29-3](#)
- [Filtering Syslog Messages, page 29-3](#)
- [Using Custom Message Lists, page 29-4](#)

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 ASA 1000V security policies. These messages help you spot holes that remain open in your security policies.
- Connections that are denied by ASA 1000V 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 ASA 1000V.
- 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:

<i>ASA</i>	The syslog message facility code for messages that are generated by the ASA 1000V. This value is always ASA.
<i>Level</i>	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 29-1 for more information.
<i>Message_number</i>	A unique six-digit number that identifies the syslog message.
<i>Message_text</i>	A text string that describes the condition. This portion of the syslog message sometimes includes IP addresses, port numbers, or usernames.

Severity Levels

Table 29-1 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 29-1 Syslog Message Severity Levels

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



Note

The ASA 1000V 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 ASA 1000V.

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 ASA 1000V 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 ASA 1000V 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 ASA 1000V)

You customize these criteria by creating a message list that you can specify when you set the output destination. Alternatively, you can configure the ASA 1000V 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 ASA 1000V. For example, the `snmp` class denotes the SNMP agent.

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 212 are associated with the `snmp` class. Syslog messages associated with the SNMP feature range from 212001 to 212012.

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 IPsec 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.

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 ASA 1000V, you must specify a logging output destination. If you enable logging without specifying a logging output destination, the ASA 1000V 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 describes the guidelines and limitations of this feature.

- Sending syslogs over TCP is not supported on a standby ASA 1000V.
- The ASA 1000V 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 29-5](#)
- [Configuring an Output Destination, page 29-6](#)



Note

The minimum configuration depends on what you want to do and what your requirements are for handling syslog messages in the ASA 1000V.

Enabling Logging

To enable logging, enter the following command:

Command	Purpose
<code>logging enable</code>	Enables logging. To disable logging, enter the no logging enable command.
Example: <code>hostname(config)# logging enable</code>	

What to Do Next

See the “[Configuring an Output Destination](#)” section on page 29-6.

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 29-7](#)
- [Sending Syslog Messages to the Internal Log Buffer, page 29-8](#)
- [Sending Syslog Messages to an E-mail Address, page 29-9](#)
- [Sending Syslog Messages to ASDM, page 29-10](#)
- [Sending Syslog Messages to the Console Port, page 29-10](#)
- [Sending Syslog Messages to an SNMP Server, page 29-11](#)
- [Sending Syslog Messages to a Telnet or SSH Session, page 29-11](#)
- [Creating a Custom Event List, page 29-12](#)
- [Generating Syslog Messages in EMBLEM Format to a Syslog Server, page 29-13](#)
- [Generating Syslog Messages in EMBLEM Format to Other Output Destinations, page 29-13](#)
- [Changing the Amount of Internal Flash Memory Available for Logs, page 29-14](#)
- [Configuring the Logging Queue, page 29-14](#)
- [Sending All Syslog Messages in a Class to a Specified Output Destination, page 29-15](#)
- [Enabling Secure Logging, page 29-15](#)
- [Including the Device ID in Non-EMBLEM Format Syslog Messages, page 29-16](#)
- [Including the Date and Time in Syslog Messages, page 29-16](#)
- [Disabling a Syslog Message, page 29-17](#)
- [Changing the Severity Level of a Syslog Message, page 29-17](#)
- [Limiting the Rate of Syslog Message Generation, page 29-17](#)

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
Step 1	<pre>logging host interface_name syslog_ip [tcp[/port] udp[/port] [format emblem]]</pre> <p>Example: <pre>hostname(config)# logging host dmz1 192.168.1.5 udp 1026 format emblem</pre></p>	<p>Configures the ASA 1000V to send messages to a syslog server.</p> <p>The format emblem keyword enables EMBLEM format logging for the syslog server with UDP only. The <i>interface_name</i> argument specifies the Ethernet interface through which you access the syslog server. The <i>syslog_ip</i> argument specifies the IP address of the syslog server. The tcp[/port] or udp[/port] keyword and argument pair specify that the ASA 1000V should use TCP or UDP to send syslog messages to the syslog server.</p> <p>You can configure the ASA 1000V 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.</p> <p>If you specify TCP, the ASA 1000V discovers when the syslog server fails and as a security protection, new connections through the ASA 1000V are blocked. To allow new connections regardless of connectivity to a TCP syslog server, see Step 3. If you specify UDP, the ASA 1000V continues 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.</p>
Step 2	<pre>logging trap {severity_level message_list}</pre> <p>Example: <pre>hostname(config)# logging trap errors</pre></p>	<p>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 ASA 1000V sends 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.</p>

	Command	Purpose
Step 3	<p>logging permit-hostdown</p> <p>Example: hostname(config)# logging permit-hostdown</p>	(Optional) Disables the feature to block new connections when a TCP-connected syslog server is down. If the ASA 1000V is configured to send syslog messages to a TCP-based syslog server, and if either the syslog server is down or the log queue is full, then new connections are blocked. New connections are allowed again after the syslog server is back up and the log queue is no longer full. For more information about the log queue, see the “Configuring the Logging Queue” section on page 29-14.
Step 4	<p>logging facility number</p> <p>Example: hostname(config)# logging facility 21</p>	(Optional) Sets the logging facility to a value other than 20, which is what most UNIX systems expect.

Sending Syslog Messages to the Internal Log Buffer

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

	Command	Purpose
Step 1	<p>logging buffered {severity_level message_list}</p> <p>Example: hostname(config)# logging buffered critical hostname(config)# logging buffered level 2 hostname(config)# logging buffered notif-list</p>	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 ASA 1000V to save the full buffer to another location. To empty the internal log buffer, enter the clear logging buffer command.
Step 2	<p>logging buffer-size bytes</p> <p>Example: hostname(config)# logging buffer-size 16384</p>	Changes the size of the internal log buffer. The buffer size is 4 KB.
Step 3	<p>Choose one of the following options:</p> <p>logging flash-bufferwrap</p> <p>Example: hostname(config)# logging flash-bufferwrap</p>	<p>When saving the buffer content to another location, the ASA 1000V creates log files with names that use the following time-stamp format:</p> <p><i>LOG-YYYY-MM-DD-HHMMSS.TXT</i></p> <p>where <i>YYYY</i> is the year, <i>MM</i> is the month, <i>DD</i> is the day of the month, and <i>HHMMSS</i> is the time in hours, minutes, and seconds.</p> <p>The ASA 1000V continues to save new messages to the internal log buffer and saves the full log buffer content to the internal flash memory.</p>

Command	Purpose
logging ftp-bufferwrap Example: hostname(config)# logging ftp-bufferwrap	When saving the buffer content to another location, the ASA 1000V creates log files with names that use the following time-stamp format: <i>LOG-YYYY-MM-DD-HHMMSS.TXT</i> where <i>YYYY</i> is the year, <i>MM</i> is the month, <i>DD</i> is the day of the month, and <i>HHMMSS</i> is the time in hours, minutes, and seconds. The ASA 1000V continues saving new messages to the internal log buffer and saves the full log buffer content to an FTP server.
logging ftp-server <i>server path username password</i> Example: hostname(config)# logging ftp-server 10.1.1.1 /syslogs logsupervisor lluvMy10gs	Identifies the FTP server on which you want to store log buffer content. The <i>server</i> argument specifies the IP address of the external FTP server. The <i>path</i> 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 <i>username</i> argument specifies a username that is valid for logging into the FTP server. The <i>password</i> argument indicates the password for the username specified.
logging saveolog [<i>savefile</i>] Example: hostname(config)# logging saveolog latest-logfile.txt	Saves the current log buffer content to the internal flash memory.

Sending Syslog Messages to an E-mail Address

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

	Command	Purpose
Step 1	logging mail { <i>severity_level</i> <i>message_list</i> } Example: hostname(config)# logging mail high-priority	Specifies which syslog messages should be sent to an e-mail address. When sent by e-mail, a syslog message appears in the subject line 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.
Step 2	logging from-address <i>email_address</i> Example: hostname(config)# logging from-address xxx-001@example.com	Specifies the source e-mail address to be used when sending syslog messages to an e-mail address.

	Command	Purpose
Step 3	<code>logging recipient-address e-mail_address [severity_level]</code> Example: hostname(config)# logging recipient-address admin@example.com	Specifies the recipient e-mail address to be used when sending syslog messages to an e-mail address.
Step 4	<code>smtp-server ip_address</code> Example: hostname(config)# smtp-server 10.1.1.1	Specifies the SMTP server to be used when sending syslog messages to an e-mail address.

Sending Syslog Messages to ASDM

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

	Command	Purpose
Step 1	<code>logging asdm {severity_level message_list}</code> Example: hostname(config)# logging asdm 2	Specifies which syslog messages should be sent to ASDM. The ASA 1000V sets aside a buffer area for syslog messages waiting to be sent to ASDM and saves messages in the buffer as they occur. The ASDM log buffer is a different buffer than the internal log buffer. When the ASDM log buffer is full, the ASA 1000V deletes the oldest syslog message to make room in the buffer for new ones. Deleting the oldest syslog message to make room for new ones is the default setting in ASDM. To control the number of syslog messages retained in the ASDM log buffer, you can change the size of the buffer.
Step 2	<code>logging asdm-buffer-size num_of_msgs</code> Example: hostname(config)# logging asdm-buffer-size 200	Specifies the number of syslog messages to be retained in the ASDM log buffer. To empty the current content of the ASDM log buffer, enter the clear logging asdm command.

Sending Syslog Messages to the Console Port

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

	Command	Purpose
	<code>logging console {severity_level message_list}</code> Example: hostname(config)# logging console errors	Specifies which syslog messages should be sent to the console port.

Sending Syslog Messages to an SNMP Server

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

Command	Purpose
logging history [<i>logging_list</i> <i>level</i>] Example: hostname(config)# logging history errors	Enables SNMP logging and specifies which messages are to be sent to SNMP servers. To disable SNMP logging, enter the no logging history command.

Sending Syslog Messages to a Telnet or SSH Session

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

	Command	Purpose
Step 1	logging monitor { <i>severity_level</i> <i>message_list</i> } Example: hostname(config)# logging monitor 6	Specifies which syslog messages should be sent to a Telnet or SSH session.
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:

	Purpose
<p>Step 1</p> <p>Command</p> <pre>logging list name {level level [class message_class] message start_id[-end_id]}</pre> <p>Example:</p> <pre>hostname(config)# logging list notif-list level 3</pre>	<p>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 ASA 1000V sends syslog messages for severity levels 3, 2, and 1.</p> <p>The <i>name</i> 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.</p> <p>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 <i>err</i>.</p>
<p>Step 2</p> <p>Command</p> <pre>logging list name {level level [class message_class] message start_id[-end_id]}</pre> <p>Example:</p> <pre>hostname(config)# logging list notif-list 104024-105999</pre> <pre>hostname(config)# logging list notif-list level critical</pre> <pre>hostname(config)# logging list notif-list level warning class ha</pre>	<p>(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:</p> <ul style="list-style-type: none"> • 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). <p>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.</p>

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:

Command	Purpose
<pre>logging host interface_name ip_address {tcp[/port] udp[/port]] [format emblem]</pre> <p>Example:</p> <pre>hostname(config)# logging host interface_1 127.0.0.1 udp format emblem</pre>	<p>Sends syslog messages in EMBLEM format to a syslog server over UDP using port 514.</p> <p>The format emblem keyword enables EMBLEM format logging for the syslog server (UDP only). The <i>interface_name</i> argument specifies the Ethernet interface through which you access the syslog server. The <i>ip_address</i> argument specifies the IP address of the syslog server. The tcp[/port] or udp[/port] keyword and argument pair specify that the ASA 1000V should use TCP or UDP to send syslog messages to the syslog server.</p> <p>You can configure the ASA 1000V 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.</p> <p>You can use multiple logging host commands to specify additional servers that would all receive syslog messages. If you configure two or more logging servers, make sure that you limit the logging severity level to warnings for all logging servers.</p> <p>If you specify TCP, the ASA 1000V discovers when the syslog server fails and as a security protection, new connections through the ASA 1000V are blocked. If you specify UDP, the ASA 1000V continues 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.</p> <p>Note Sending syslogs over TCP is not supported on a standby ASA 1000V.</p>

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:

Command	Purpose
<pre>logging emblem</pre> <p>Example:</p> <pre>hostname(config)# logging emblem</pre>	<p>Sends syslog messages in EMBLEM format to output destinations other than a syslog server, such as Telnet or SSH sessions.</p>

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:

	Command	Purpose
Step 1	logging flash-maximum-allocation <i>kbytes</i> Example: hostname(config)# logging flash-maximum-allocation 1200	<p>Specifies the maximum amount of internal flash memory available for saving log files. By default, the ASA 1000V can use up to 1 MB of internal flash memory for log data. The minimum amount of internal flash memory that must be free for the ASA 1000V to save log data is 3 MB.</p> <p>If a log file being saved to internal flash memory would cause the amount of free internal flash memory to fall below the configured minimum limit, the ASA 1000V 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 have been deleted, free memory is still below the limit, the ASA 1000V fails to save the new log file.</p>
Step 2	logging flash-minimum-free <i>kbytes</i> Example: hostname(config)# logging flash-minimum-free 4000	<p>Specifies the minimum amount of internal flash memory that must be free for the ASA 1000V to save a log file.</p>

Configuring the Logging Queue

To configure the logging queue, enter the following command:

Command	Purpose
logging queue <i>message_count</i> Example: hostname(config)# logging queue 300	<p>Specifies the number of syslog messages that the ASA 1000V can hold in its queue before sending them to the configured output destination. The ASA 1000V 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. If the logging queue is set to zero, the queue is the maximum configurable size (8192 messages).</p>

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:

Command	Purpose
<pre>logging class message_class {buffered console history mail monitor trap} [severity_level]</pre> <p>Example: hostname(config)# logging class ha buffered alerts</p>	<p>Overrides the configuration in the specified output destination command. For example, if you specify that messages at severity level 7 should go to the internal log buffer and that ha class messages at severity level 3 should go to the internal log buffer, then the latter configuration takes precedence. The buffered, history, mail, monitor, and trap keywords specify the output destination to which syslog messages in this class should be sent. The history keyword enables SNMP logging. The monitor keyword enables Telnet and SSH logging. The trap keyword enables syslog server logging. Select one destination per command line entry. To specify that a class should go to more than one destination, enter a new command for each output destination.</p>

Enabling Secure Logging

To enable secure logging, enter the following command:

Command	Purpose
<pre>logging host interface_name syslog_ip [tcp/port udp/port] [format emblem] [secure]</pre> <p>Example: hostname(config)# logging host inside 10.0.0.1 TCP/1500 secure</p>	<p>Enables secure logging.</p> <p>The <i>interface_name</i> argument specifies the interface on which the syslog server resides. The <i>syslog_ip</i> argument specifies the IP address of the syslog server. The <i>port</i> argument specifies the port (TCP or UDP) that the syslog server listens to for syslog messages. The tcp keyword specifies that the ASA 1000V should use TCP to send syslog messages to the syslog server. The udp keyword specifies that the ASA 1000V should use UDP to send syslog messages to the syslog server. The format emblem keyword enables EMBLEM format logging for the syslog server. The secure keyword specifies that the connection to the remote logging host should use SSL/TLS for TCP only.</p> <p>Note Secure logging does not support UDP; an error occurs if you try to use this protocol.</p>

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:

Command	Purpose
<pre>logging device-id [hostname ipaddress interface_name string text]</pre> <p>Example: hostname(config)# logging device-id hostname</p>	<p>Configures the ASA 1000V to include a device ID in non-EMBLEM-format syslog messages. You can specify only one type of device ID for syslog messages.</p> <p>The hostname keyword specifies that the hostname of the ASA 1000V should be used as the device ID. The ipaddress interface_name keyword and argument pair specify that the interface IP address specified as <i>interface_name</i> should be used as the device ID. If you use the ipaddress keyword, the device ID becomes the specified ASA 1000V 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:</p> <ul style="list-style-type: none"> • & (ampersand) • ' (single quote) • " (double quote) • < (less than) • > (greater than) • ? (question mark) <p>Note If enabled, the device ID does not appear in EMBLEM-formatted syslog messages nor in SNMP traps.</p>

Including the Date and Time in Syslog Messages

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

Command	Purpose
<pre>logging timestamp</pre> <pre>hostname(config)# logging timestamp</pre> <p>Example: hostname(config)# logging timestamp LOG-2008-10-24-081856.TXT </p>	<p>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 no logging timestamp command.</p>

Disabling a Syslog Message

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

Command	Purpose
<pre>no logging message <i>message_number</i></pre> <p>Example: hostname(config)# no logging message 113019</p>	Prevents the ASA 1000V from generating a particular syslog message. To reenble a disabled syslog message, enter the logging message <i>message_number</i> command (for example, logging message 113019). To reenble logging of all disabled syslog messages, enter the clear config logging disabled command.

Changing the Severity Level of a Syslog Message

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

Command	Purpose
<pre>logging message <i>message_ID</i> level <i>severity_level</i></pre> <p>Example: hostname(config)# logging message 113019 level 5</p>	Specifies the severity level of a syslog message. To reset the severity level of a syslog message to its setting, enter the no logging message <i>message_ID</i> level <i>current_severity_level</i> command (for example, no logging message 113019 level 5). To reset the severity level of all modified syslog messages to their settings, enter the clear configure logging level command.

Limiting the Rate of Syslog Message Generation

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

Command	Purpose
<pre>logging rate-limit {unlimited {<i>num</i> [<i>interval</i>]}}</pre> <pre><i>message syslog_id</i> <i>level severity_level</i></pre> <p>Example: hostname(config)# logging rate-limit 1000 600 level 6</p>	Applies a specified severity level (1 through 7) to a set of messages or to an individual message (not the destination) within a specified time period. Rate limits affect the volume of messages being sent to all configured destinations. To reset the logging rate limit to the default value, enter the clear running-config logging rate-limit command. To reset the logging rate limit, enter the clear configure logging rate-limit command.

Monitoring the Logs

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

Command	Purpose
<code>show logging</code>	Shows syslog messages, including the severity level. Note 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.
<code>show logging message</code>	Shows a list of syslog messages with modified severity levels and disabled syslog messages.
<code>show logging message <i>message_ID</i></code>	Shows the severity level of a specific syslog message.
<code>show logging queue</code>	Shows the logging queue and queue statistics.
<code>show logging rate-limit</code>	Shows the disallowed syslog messages.
<code>show running-config logging rate-limit</code>	Shows the current logging rate-limit setting.

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

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 29-2 lists each feature change

Table 29-2 Feature History for Logging

Feature Name	Platform Releases	Feature Information
Syslog messages	8.7(1)	We introduced the following syslog messages: 450002 and 771001-771003.

