

Logging

This chapter describes how to log system messages and use them for troubleshooting.

- About Logging, on page 1
- Guidelines for logging, on page 8
- Configure Logging, on page 10
- Monitoring the Logs, on page 29
- History for Logging, on page 33

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 system logs provide you with information for monitoring and troubleshooting the ASA. 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
  - Console
  - 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.

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 ASA 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.

Syslog Message Analysis

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

```
[<PRI>]: [Timestamp] [Device-ID] : %ASA-Level-Message_number: Message_text
```

Field descriptions are as follows:

<PRI>	Priority value. When the logging EMBLEM is enabled, this value is displayed in the syslog message. Logging EMBLEM is compatible with UDP and not with TCP.
Timestamp	Date and time of the event is displayed. When logging of timestamps is enabled, and if the timestamp is configured to be in the RFC 5424 format, all timestamp in syslog messages display the time in UTC, as indicated by the RFC 5424 standard.
Device-ID	The device identifier string that was configured while enabling the logging device-id option through the user interface. If enabled, the device ID does not appear in EMBLEM-formatted syslog messages.
ASA	The syslog message facility code for messages that are generated by the ASA. This value is always `ASA`.
Level	0 through 7. The level reflects the severity of the condition described by the syslog message—the lower the number, the more severe the condition.
Message_number	A unique six-digit number that identifies the syslog message.
Message_text	A text string that describes the condition. This portion of the syslog message sometimes includes IP addresses, port numbers, or usernames.

All syslog messages that are generated by the device are documented in the Cisco Secure Firewall ASA Series Syslog Messages guide.

The EMBLEM syslog format is a Cisco-specific convention that is built upon the RFC 3164 and RFC 5424 standards. Hence, when EMBLEM is enabled, the syslog message prints colon (:) after <PRI> field.

Example of a syslog message with logging EMBLEM, logging timestamp rfc5424, and device-id enabled. Note the colon (:) after the <PRI> field (*<166>*).

```
<166>:2018-06-27T12:17:46Z: %ASA-6-110002: Failed to locate egress interface for protocol
from src interface :src IP/src port to dest IP/dest port
```

Example of a syslog message with logging timestamp rfc5424 and device-id enabled. No colon (:) is present before the timestamp.

```
2018-06-27T12:17:46Z asa : %ASA-6-110002: Failed to locate egress interface for protocol
from src interface :src IP/src port to dest IP/dest port
```

Syslog message severity levels

The syslog message severity levels define the importance of system messages. You can assign custom colors to each severity level to make them easier to distinguish 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 1: Syslog message severity levels

Level Number	Severity Level	Description
0	**emergencies**	You cannot use the system.
1	**alert**	You need to take immediate action.

Level Number	Severity Level	Description
2	**critical**	The system has critical conditions to be addressed.
3	**error**	Error conditions.
4	**warning**	The system has warnings you should review.
5	**notification**	The system reports significant events you should monitor.
6	**informational**	Informational messages only.
7	**debugging**	The system generates only debugging messages Log at this level only temporarily, when debugging issues. This log level can generate many messages, which might affect system performance.



Note ASA does not generate syslog messages with a severity level of zero (emergencies).

Syslog message filters

Syslog message filter criteria

You can direct syslog messages to an output destination according to these criteria:

- Syslog message ID number
- Syslog message severity level
- Syslog message class (equivalent to a functional area)

You can create a message list with specific criteria, which you can then specify as the output destination is set. Alternatively, you can configure the ASA to send a particular message class to each type of output destination independently of the message list.

Syslog message classes and associated message ID numbers

You can use syslog message classes in two ways:

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

Use the syslog message class to categorize syslog messages by type, such as features or functions of the device. For example, use the RIP class for RIP routing.

Syslog messages in the same class have the same three initial digits in their message ID numbers. For example, the syslog messages for the VPN client feature use ID numbers 611101 to 611323.

Most ISAKMP syslog messages include prepended objects that identify the tunnel. When available, these objects appear before the descriptive text of a syslog message. If the object is unknown when the syslog message is generated, the heading and value combination is omitted.

The objects are prefixed in this manner:

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

The term 'group' here refers to the tunnel-group configuration. The username is from the local database or AAA server. The IP address is the public IP address of the remote access client or Layer 2 peer.

See the message classes and the range of message ID numbers in each class in this table.

Table 2: Syslog message classes and associated message ID numbers

Class	Definition	Syslog Message ID Numbers
auth	User Authentication	109, 113
—	Access Lists	106
—	Application Firewall	415
—	Botnet Traffic Filtering	338
bridge	Transparent Firewall	110, 220
ca	PKI Certification Authority	717
citrix	Citrix Client	723
—	Clustering	747
—	Card Management	323
config	Command Interface	111, 112, 208, 308
csd	Secure Desktop	724
cts	Cisco TrustSec	776
dap	Dynamic Access Policies	734
EAP, eapoudp	EAP or EAPoUDP for Network Admission Control	333, 334
EIGRP	EIGRP Routing	336
email	E-mail Proxy	719
—	Environment Monitoring	735
ha	Failover	101, 102, 103, 104, 105, 210, 311, 709
—	Identity-based Firewall	746
ids	Intrusion Detection System	400, 733

Class	Definition	Syslog Message ID Numbers
—	IKEv2 Toolkit	750, 751, 752
IP	IP Stack	209, 215, 313, 317, 408
ipaa	IP Address Assignment	735
ips	Intrusion Protection System	400, 401, 420
—	IPv6	325
—	Licensing	444
MDM-proxy	MDM Proxy	802
NAC	Network Admission Control	731, 732
nacpolicy	NAC Policy	731
nacsettings	NAC Settings to apply NAC Policy	732
—	NAT and PAT	305
—	Network Access Point	713
NP	Network Processor	319
—	NP SSL	725
OSPF	OSPF Routing	318, 409, 503, 613
—	Password Encryption	742
—	Phone Proxy	337
RIP	RIP Routing	107, 312
rm	Resource Manager	321
—	Smart Call Home	120
session	User Session	106, 108, 201, 202, 204, 302, 303, 304, 305, 314, 405, 406, 407, 500, 502, 607, 608, 609, 616, 620, 703, 710
SNMP	SNMP	212
—	ScanSafe	775
SSL	SSL Stack	725
svc	SSL VPN Client	722

Class	Definition	Syslog Message ID Numbers
sys	System	199, 211, 214, 216, 306, 307, 315, 414, 604, 605, 606, 610, 612, 614, 615,701, 711, 741
—	Threat Detection	733
tag-switching	Service Tag Switching	779
transactional-rule-engine-tre	Transactional Rule Engine	780
uc-IMS	UC-IMS	339
vm	VLAN Mapping	730
vpdn	PPTP and L2TP Sessions	213, 403, 603
VPN	IKE and IPsec	316, 320, 402, 404, 501, 602, 702, 713, 714, 715
vpnc	VPN Client	611
vpnfo	VPN Failover	720
vpnlb	VPN Load Balancing	718
—	VXLAN	778
webfo	WebVPN Failover	721
webvpn	WebVPN and Secure Client	716

Sort Messages in the Log Viewers

You can sort messages in all ASDM log viewers (that is, the Real-Time Log Viewer, the Log Buffer Viewer, and the Latest ASDM Syslog Events Viewer). To sort tables by multiple columns, click the header of the first column that you want to sort by, then press and hold down the **Ctrl** key and at the same time, click the headers of the other column(s) that you want to include in the sort order. To sort messages chronologically, select both the date and time columns; otherwise, the messages are sorted only by date (regardless of the time) or only by time (regardless of the date).

When you sort messages in the Real-Time Log Viewer and in the Latest ASDM Syslog Events Viewer, the new messages that come in appear in the sorted order, instead of at the top, as they normally would be. That is, they are mixed in with the rest of the messages.

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
- 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.

Clustering

Syslog messages are an invaluable tool for accounting, monitoring, and troubleshooting in a clustering environment. Each ASA unit in the cluster (up to eight units are allowed) generates syslog messages independently; certain **logging** commands then enable you to control header fields, which include a time stamp and device ID. The syslog server uses the device ID to identify the syslog generator. You can use the **logging device-id** command to generate syslog messages with identical or different device IDs to make messages appear to come from the same or different units in the cluster.



Note To monitor syslog messages from units in a cluster, you must open an ASDM session to each of the units that you want to monitor.

Guidelines for logging

Restrictions for IPv6 logging

- IPv6 is supported. Syslog message can be sent using TCP or UDP.
- Ensure that the interface configured for sending syslogs is enabled, IPv6 capable, and the syslog server is reachable through the designated interface.
- You cannot use IPv6 for secure logging.

Syslog server configuration guidelines

- The syslog server must run a server program called syslogd. Windows includes a syslog server as part of its operating system.
- The syslog server operates based on the syslog-ng process of the firewall system. Do not use external configuration files, such as the *scwx.conf* file from SecureWorks. Because these files are not compatible with the device, using them causes parsing errors and the syslog-ng process fails.

- You can configure up to 16 syslog servers. However, in multiple context mode, the limitation is four servers per context.
- Assign only one list or class to each syslog server and location.
- The syslog server should be reachable through the ASA. Configure the device to deny ICMP unreachable messages on the interface through which the syslog server is reachable, and to send syslogs to the same server. Enable logging for all severity levels. To prevent the syslog server from crashing, suppress the generation of syslogs 313001, 313004, and 313005.
- To view logs generated by the ASA, you must specify a logging output destination. If you enable logging without specifying a logging output destination, the ASA 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, specify separate entries in the **Syslog Server** pane for each syslog server.
- The Firewall Threat Defense syslog supports one-way TLS for secure logging. It does not support client certificate authentication, trustpoint configuration for syslog, or mutual TLS (X.509 certificate authentication).
- The server certificate received from a Syslog Server must contain "ServAuth" in the Extended Key Usage field. This check will be done on non self-signed certificates only, self-signed certificates do not provide any value in this field.

Interfaces for syslog configuration

- Determining the egress interface for the syslog:
  - If the specified management-only interface has management-access enabled, the management center will perform route table lookups and determine the egress interface (could be data or management) based on best routing logic.
  - If you configure a management-only interface as logging host, that does not have management-access enabled, the management center will use the interface regardless of routing table entries.

    Thus, for the management center to always uses a dedicated management path for syslog traffic, configure the management interface without management-access, and then specify the interface in the logging host:

```
interface <management-interface>
management-only ----->Do not include management-access
logging host <management-interface> <syslog-server-ip>
```

- When the syslog rate exceeds 50,000 messages per second, ensure that a data interface is used as egress interface rather than a management interface.
- When you use a custom message list to match only access list hits, the access list logs are not generated for access lists that have had their logging severity level increased to debugging (level 7). The default logging severity level is set to 6 for the **logging list** command. This default behavior is by design. If you explicitly change the logging severity level of the access list configuration to debugging, you must also change the logging configuration itself.

  This is sample output from the **show running-config logging** command that does not include access list hits, because their logging severity level has been changed to debugging:

```
ciscoasa# show running-config logging
logging enable
logging timestamp
logging list test message 106100
logging buffered test
```

This is sample output from the **show running-config logging** command that does include access list hits:

```
ciscoasa# show running-config logging
logging enable
logging timestamp
logging buffered debugging
```

In this case, the access list configuration does not change, and the number of access list hits appears, as shown in this example:

```
ciscoasa(config)# access-list global line 1 extended
permit icmp any host 4.2.2.2 log debugging interval 1 (hitcnt=7) 0xf36b5386
ciscoasa(config)# access-list global line 2 extended
permit tcp host 10.1.1.2 any eq www log informational interval 1 (hitcnt=18) 0xe7e7c3b8
ciscoasa(config)# access-list global line 3 extended
permit ip any any (hitcnt=543) 0x25f9e609
```

TCP and UDP connections for syslog

- Sending syslogs over TCP is not supported on a standby device.
- If you use TCP as the transport protocol, the system opens 4 connections to the syslog server to ensure that messages are not lost. If you collect messages from many devices and the combined connection overhead is too much for the server, use UDP instead.
- The number of UDP connections for syslog is directly related to the number of CPUs on the hardware platform and the number of syslog servers you configure. At any point in time, there can be as many UDP syslog connections as there are CPUs times the number of configured syslog servers. The global UDP connection idle timeout applies to these sessions, and the default duration is two minutes. You can adjust this setting to close sessions more quickly, but the timeout applies to all UDP connections, not just syslog. This is the intended behavior.
- When the ASA sends syslogs via TCP, the connection takes about one minute to initiate after the syslogd service restarts.
- When the TCP logging host goes down, it takes approximately six minutes to change its connection status from *Connected* to *Not connected*. Logging relies on TCP to detect the channel state; until then, logging sends the logs through the channel. During this time, when you execute the **show log**, the output would display the TCP logging host as connected. Once the TCP channel is closed, the TCP logging host state is updated to *Not connected*.

Configure Logging

This section describes how to configure logging.

Enable Logging

To enable logging, perform the following steps:

Procedure

Step 1 In ASDM, choose one of the following:

- **Home** > **Latest ASDM Syslog Messages** > **Enable Logging**
- **Configuration** > **Device Management** > **Logging** > **Logging Setup**
- **Monitoring** > **Real-Time Log Viewer** > **Enable Logging**
- **Monitoring** > **Log Buffer** > **Enable Logging**

Step 2 Check the **Enable logging** check box to turn on logging.

Configure 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.

When you configure syslog logging on an interface with management-only access enabled, the dataplane related logs (syslog IDs 302015, 302014, 106023, and 304001) are dropped and does not reach the syslog server. The syslog messages are dropped because the datapath routing table does not have the management interface routing. Hence, ensure the interface that you are configuring has management-only access disabled.

Send 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:

Procedure

Step 1 Choose **Configuration** > **Device Management** > **Logging** > **Logging Setup**.

Step 2 Check the **Enable logging** check box to turn on logging for the ASA.

Step 3 Check the **Enable logging on the failover standby unit** check box to turn on logging for the standby ASA, if available.

Step 4 Check the **Send debug messages as syslogs** check box to redirect all debugging trace output to system logs. The syslog message does not appear on the console if this option is enabled. Therefore, to view debugging

messages, you must have logging enabled at the console and have it configured as the destination for the debugging syslog message number and severity level. The syslog message number to use is **711001**. The default severity level for this syslog message is debugging.

Step 5 Check the **Send syslogs in EMBLEM format** check box to enable EMBLEM format so that it is used for all logging destinations, except syslog servers.

Step 6 Specify the size of the internal log buffer to which syslog messages are saved if the logging buffer is enabled. When the buffer fills up, messages are overwritten unless you save the logs to an FTP server or to internal flash memory. The default buffer size is 4096 bytes. The range is 4096 to 1048576.

Step 7 To save the buffer content to the FTP server before it is overwritten, check the **Save Buffer To FTP Server** check box. To allow overwriting of the buffer content, uncheck this check box.

Step 8 Click **Configure FTP Settings** to identify the FTP server and configure the FTP parameters used to save the buffer content.

Step 9 Check the **Save Buffer To Flash** check box To save the buffer content to internal flash memory before it is overwritten.

Note
This option is only available in routed or transparent single mode.

Step 10 Click **Configure Flash Usage** to specify the maximum space to be used in internal flash memory for logging and the minimum free space to be preserved (in KB). Enabling this option creates a directory called “syslog” on the device disk on which messages are stored.

Note
This option is only available in single routed or transparent mode.

Step 11 Specify the queue size for system logs that are to be viewed in the ASA.

Configure FTP Settings

To specify the configuration for the FTP server that is used to save the log buffer content, perform the following steps:

Procedure

Step 1 Check the **Enable FTP client** check box to enable configuration of the FTP client.

Step 2 Specify the IP address of the FTP server.

Step 3 Specify the directory path on the FTP server to store the saved log buffer content.

Step 4 Specify the username to log in to the FTP server.

Step 5 Specify the password associated with the username to log in to the FTP server.

Step 6 Confirm the password, then click **OK**.

Configure Logging Flash Usage

To specify the limits for saving the log buffer content to internal flash memory, perform the following steps:

Procedure

Step 1 Specify the maximum amount of internal flash memory that can be used for logging (in KB).

Step 2 Specify the amount of internal flash memory that is preserved (in KB). When the internal flash memory approaches that limit, new logs are no longer saved.

Step 3 Click **OK** to close the **Configure Logging Flash Usage** dialog box.

Enable Secure Logging

Procedure

Step 1 Choose **Configuration** > **Device Management** > **Logging** > **Syslog Server**.

Step 2 Select a syslog server for which you want to enable secure logging, then click **Edit**.

The **Edit Syslog Server** dialog box appears.

Step 3 Click the **TCP** radio button.

Secure logging does not support UDP; an error occurs if you try to use this protocol.

Step 4 Check the **Enable secure syslog with SSL/TLS** check box, then click **OK**.

Step 5 (Optional) Specify a **Reference Identity** object by name to enable RFC 6125 reference identity checks on the certificate received from the Syslog server.

See Configure Reference Identities for details on the reference identity object.

Generate Syslog Messages in EMBLEM Format to a Syslog Server

To generate syslog messages in EMBLEM format to a syslog server, perform the following steps:

Procedure

Step 1 Choose **Configuration** > **Device Management** > **Logging** > **Syslog Server**.

Sending syslogs over IPv6 is supported.

Step 2 Click **Add** to add a new syslog server.

The **Add Syslog Server** dialog box appears.

Note
You can set up a maximum of four syslog servers per security context (up to a total of 16).

Step 3 Specify the number of messages that are allowed to be queued on the ASA when a syslog server is busy. A zero value means an unlimited number of messages may be queued.

Step 4 Check the **Allow user traffic to pass when TCP syslog server is down** check box to allow all traffic if any syslog server is down.

When the ASA is configured to send syslog messages to a TCP-connected syslog server, and if the syslog server fails, as a security protection, new connections through the ASA are blocked. To permit new connections, even when the syslog server is not operational, select this check box.

If you specify UDP, the ASA 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.

Note
Sending syslogs over TCP is not supported on a standby ASA.

Generate Syslog Messages in EMBLEM Format to Other Output Destinations

To generate syslog messages in EMBLEM format to other output destinations, perform the following steps:

Procedure

Step 1 Choose **Configuration** > **Device Management** > **Logging** > **Logging Setup**.

Step 2 Check the **Send syslogs in EMBLEM format** check box.

Add or Edit Syslog Server Settings

To add or edit syslog server settings, perform the following steps:

Procedure

Step 1 Choose the interface used to communicate with the syslog server from the drop-down list.

Step 2 Enter the IP address that is used to communicate with the syslog server.

Choose the protocol (either TCP or UDP) that is used by the syslog server to communicate with the ASA or ASASM. You can configure the ASA and ASASM to send data to a syslog server using either UDP or TCP. The default protocol is UDP if you do not specify a protocol.

Warning
If you specify TCP, when the ASA discovers syslog server failures, for security reasons, new connections through the ASA are blocked. To permit new connections despite syslog server failures, see Step 4 of Generate Syslog Messages in EMBLEM Format to a Syslog Server, on page 13.

Step 3 Enter the port number used by the syslog server to communicate with the ASA or ASASM.

Step 4 Check the **Log messages in Cisco EMBLEM format (UDP only)** check box to specify whether to log messages in Cisco EMBLEM format (available only if UDP is selected as the protocol).

Step 5 Check the **Enable secure logging using SSL/TLS (TCP only)** check box to specify that the connection to the syslog server is secure through the use of SSL/TLS over TCP, and that the syslog message content is

encrypted. You can optionally mention reference identity to validate the certificate based on the previously configured reference identity object. For more information, see Enable Secure Logging, on page 13.

Step 6 Click **OK** to complete the configuration.

Send Syslog Messages to the Internal Log Buffer

You need to specify 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 to save the full buffer to another location.

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

Procedure

Step 1 Choose one of the following options to specify which syslog messages should be sent to the internal log buffer:

- **Home** > **Latest ASDM Syslog Messages** > **Configure ASDM Syslog Filters**
- **Configuration** > **Device Management** > **Logging** > **Logging Filters**

Step 2 Choose **Monitoring** > **Logging** > **Log Buffer** > **View**. Then choose **File** > **Clear Internal Log Buffer** in the **Log Buffer** pane to empty the internal log buffer.

Step 3 Choose **Configuration** > **Device Management** > **Logging** > **Logging Setup** to change the size of the internal log buffer. The default buffer size is 4 KB.

Note
When you change the logging buffer size, the existing logs in the buffer are purged, and a new buffer is created with the newly configured size.

The ASA continue to save new messages to the internal log buffer and save the full log buffer content to internal flash memory. When saving the buffer content to another location, the ASA create 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.

Step 4 To save new messages to another location, choose one of the following options:

- Check the **Flash** check box to send new messages to internal flash memory, then click Configure **Flash Usage**. The **Configure Logging Flash Usage** dialog box appears.
  a. Specify the maximum amount of flash memory in KB that you want to use for logging.
  b. Specify the minimum amount of free space in KB that logging will preserve in flash memory.
  c. Click **OK** to close this dialog box.

- Check the **FTP Server** check box to send new messages to an FTP server, then click **Configure FTP Settings**. The **Configure FTP Settings** dialog box appears.
  a. Check the **Enable FTP Client** check box.
  b. Enter the following information in the fields provided: FTP server IP address, path, username, and password.
  c. Confirm the password, then click **OK** to close this dialog box.

Save an Internal Log Buffer to Flash

To save the internal log buffer to flash memory, perform the following steps:

Procedure

Step 1 Choose **File** > **Save Internal Log Buffer to Flash**.

The **Enter Log File Name** dialog box appears.

Step 2 Choose the first option to save the log buffer with the default filename, LOG-YYYY-MM-DD-hhmmss.txt.

Step 3 Choose the second option to specify a filename for the log buffer.

Step 4 Enter the filename for the log buffer, then click **OK**.

Change the Amount of Internal Flash Memory Available for Logs

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

Procedure

Step 1 Choose **Configuration** > **Device Management** > **Logging** > **Logging Setup**.

Step 2 Check the **Enable Logging** check box.

Step 3 Check the **Save Buffer to Flash** check box in the **Logging to Internal Buffer** area.

Step 4 Click **Configure Flash Usage**.

The **Configure Logging Flash Usage** dialog box appears.

Step 5 Enter the maximum amount of flash memory in KB allowed to be used for logging.

By default, the ASA can use up to 50 MB of internal flash memory for log data. The minimum amount of internal flash memory that must be free for the ASA to save log data is 3 MB. If a log file being saved to internal flash memory would cause the amount of free internal flash memory to fall below the configured minimum limit, the ASA 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 fails to save the new log file. The maximum limit of the flash-maximum-allocation value is 2 GB.

Step 6 Enter the minimum amount of free space in KB to be preserved for logging in flash memory.

Step 7 Click **OK** to close the **Configure Logging Flash Usage** dialog box.

View and Copy Logged Entries with the ASDM Java Console

Use the ASDM Java console to view and copy logged entries in a text format, which may help you troubleshoot ASDM errors.

To access the ASDM Java Console, perform the following steps:

Procedure

Step 1 Choose **Tools** > **ASDM Java Console**.

Step 2 Enter **m** in the console to show the virtual machine memory statistics.

Step 3 Enter **g** in the console to perform garbage collection.

Step 4 Open the Windows Task Manager and double-click the **asdm_launcher.exe** file to monitor memory usage.

Note
The maximum memory allocation allowed is 256 MB.

Send Syslog Messages to an E-mail Address

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

Procedure

Step 1 Choose **Configuration** > **Device Management** > **Logging** > **E-Mail Setup**.

Step 2 Specify the e-mail address that is used as the source address for syslog messages that are sent as e-mail messages.

Step 3 Click **Add** to enter a new e-mail address recipient of the specified syslog messages.

Step 4 Choose the severity level of the syslog messages that are sent to the recipient from the drop-down list. The syslog message severity filter used for the destination e-mail address causes messages of the specified severity level and higher to be sent. The global filter specified in the **Logging Filters** pane is also applied to each e-mail recipient.

Step 5 Click **Edit** to modify an existing severity level of the syslog messages that are sent to this recipient.

Step 6 Click **OK** to close the **Add E-mail Recipient** dialog box.

Add or Edit E-Mail Recipients

To add or edit e-mail recipients and severity levels, perform the following steps:

Procedure

Step 1 Choose **Configuration** > **Device Management** > **Logging** > **E-mail Setup**.

Step 2 Click **Add** or **Edit** to display the **Add/Edit E-Mail Recipient** dialog box.

Step 3 Enter the destination e-mail address, and choose the syslog severity level from the drop-down list. Severity levels are defined as follows:

- Emergency (level 0, system is unusable)

  Note
  Using a severity level of zero is not recommended.

- Alert (level 1, immediate action is needed)
- Critical (level 2, critical conditions)
- Error (level 3, error conditions)
- Warning (level 4, warning conditions)
- Notification (level 5, normal but significant conditions)
- Informational (level 6, informational messages only)
- Debugging (level 7, debugging messages only)

Note
The severity level used to filter messages for the destination e-mail address is the higher of the severity level specified in the **Add/Edit E-Mail Recipient** dialog box and the global filter set for all e-mail recipients in the **Logging Filters** pane.

Step 4 Click **OK** to close the **Add/Edit E-Mail Recipient** dialog box.

The added or revised entry appears in the **E-mail Recipients** pane.

Step 5 Click **Apply** to save your changes to the running configuration.

Configure the Remote SMTP Server

To configure the remote SMTP server to which e-mail alerts and notifications are sent in response to specific events, perform the following steps:

Procedure

Step 1 Choose **Configuration** > **Device Setup** > **Logging** > **SMTP**.

Step 2 Enter the IP address of the primary SMTP server.

Step 3 (Optional) Enter the IP address of the standby SMTP server, then click **Apply** to save your changes to the running configuration.

Send Syslog Messages to the Console Port

To send syslog messages to the console port, perform the following steps:

Procedure

Step 1 Choose one of the following options:

- **Home** > **Latest ASDM Syslog Messages** > **Configure ASDM Syslog Filters**
- **Configuration** > **Device Management** > **Logging** > **Logging Filters**

Step 2 Select the console in the **Logging Destination** column, then click **Edit**.

The **Edit Logging Filters** dialog box appears.

Step 3 Choose either syslogs from all event classes or syslogs from specific event classes to specify which syslog messages should be sent to the console port.

Send Syslog Messages to a Telnet or SSH Session

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

Procedure

Step 1 Choose one of the following options:

- **Home** > **Latest ASDM Syslog Messages** > **Configure ASDM Syslog Filters**
- **Configuration** > **Device Management** > **Logging** > **Logging Filters**

Step 2 Select the **Telnet** and **SSH Sessions** in the **Logging Destination** column, then click **Edit**.

The **Edit Logging Filters** dialog box appears.

Step 3 Choose either syslogs from all event classes or syslogs from specific event classes to specify which syslog messages should be sent to a Telnet or an SSH session..

Step 4 Choose **Configuration** > **Device Management** > **Logging** > **Logging Setup** to enable logging for the current session only.

Step 5 Check the **Enable logging** check box, then click **Apply**.

Configure Syslog Messages

Configure Syslog Messaging

To configure syslog messaging, perform the following steps:

Procedure

Step 1 Choose **Configuration** > **Device Management** > **Logging** > **Syslog Setup**.

Step 2 Choose a system log facility for syslog servers to use as a basis to file messages. The default is LOCAL(4)20, which is what most UNIX systems expect. However, because your network devices share eight available facilities, you might need to change this value for system logs.

Step 3 Check the **Include timestamp in syslogs** check box to add the date and time in each syslog message sent.

Use the **Timestamp Format** drop-down to select the legacy (mm:dd:yyyy hh:mm:ss) or RFC 5424 (yyyy:dd:mmTHH:mm:ssZ) format.

Step 4 Uncheck the **Hide username if its validity cannot be determined** check box to show invalid usernames in syslog messages for unsuccessful login attempts. The default setting is to hide usernames when the username is invalid or if the validity is unknown. If a user accidentally types a password instead of a username, for example, then it is more secure to hide the "username" in the resultant syslog message. You might want to show invalid usernames to help with troubleshooting login issues.

Step 5 Choose the information to be displayed in the **Syslog ID** table. Available options are as follows:

- Choose **Show all syslog IDs** to specify that the **Syslog ID** table should display the entire list of syslog message IDs.
- Choose **Show disabled syslog IDs** to specify that the **Syslog ID** table should display only those syslog message IDs that have been explicitly disabled.
- Choose **Show syslog IDs with changed logging** to specify that the **Syslog ID** table should display only those syslog message IDs with severity levels that have changed from their default values.
- Choose **Show syslog IDs that are disabled or with a changed logging level** to specify that the **Syslog ID** table should display only those syslog message IDs with severity levels that have been modified and the IDs of syslog messages that have been explicitly disabled.

Step 6 The **Syslog ID Setup Table** displays the list of syslog messages based on the setting in the Syslog ID Setup Table. Choose individual messages or ranges of message IDs that you want to modify. You can either disable the selected message IDs or modify their severity levels. To select more than one message ID in the list, click the first ID in the range and Shift-click the last ID in the range.

Step 7 Click **Advanced** to configure syslog messages to include a device ID.

Edit Syslog ID Settings

To change syslog message settings, perform the following steps:

Note The **Syslog ID**(s) field is display-only. The values that appear in this area are determined by the entries you chose in the **Syslog ID** table, located in the **Syslog Setup** pane.

Procedure

Step 1 Check the **Disable Message(s)** check box to disable messages for the syslog message ID(s) displayed in the **Syslog ID**(s) list.

Step 2 Choose the severity logging level of messages to be sent for the syslog message ID(s) displayed in the **Syslog ID**(s) list. Severity levels are defined as follows:

- Emergency (level 0, system is unusable)

  Note
  Using a severity level of zero is not recommended.

- Alert (level 1, immediate action is needed)
- Critical (level 2, critical conditions)
- Error (level 3, error conditions)
- Warning (level 4, warning conditions)
- Notification (level 5, normal but significant conditions)
- Informational (level 6, informational messages only)
- Debugging (level 7, debugging messages only)

Step 3 Click **OK** to close the **Edit Syslog ID Settings** dialog box.

Include a Device ID in Non-EMBLEM Formatted Syslog Messages

To include a device ID in non-EMBLEM formatted syslog messages, perform the following steps:

Procedure

Step 1 Check the **Enable syslog device ID** check box to specify that a device ID should be included in all non-EMBLEM formatted syslog messages.

Step 2 To specify which to use as the device ID, choose one of the following options:

- Hostname of the ASA
- Interface IP address

  Choose the interface name that corresponds to the selected IP address from the drop-down list.

Check the **In an ASA cluster, always use control's IP address for the selected interface** check box if you are using clustering.

- String

  Specify an alphanumeric, user-defined string.

- ASA cluster name

Step 3 Click **OK** to close the **Advanced Syslog Configuration** dialog box.

Include the Date and Time in Syslog Messages

To include the date and time in syslog messages, perform the following steps:

Procedure

Step 1 Choose **Configuration** > **Device Management** > **Logging** > **Syslog Setup**.
Step 2 Check the **Include timestamp in syslogs** check box in the **Syslog ID Setup** area.
Step 3 Click **Apply** to save your changes.

Disable a Syslog Message

To disable a specified syslog message, perform the following steps:

Procedure

Step 1 Choose **Configuration** > **Device Management** > **Logging** > **Syslog Setup**.
Step 2 Select the syslog that you want to disable from the table, then click **Edit**.

The **Edit Syslog ID Settings** dialog box appears.

Step 3 Check the **Disable messages** check box, then click **OK**.

Change the Severity Level of a Syslog Message

To change the severity level of a syslog message, perform the following steps:

Procedure

Step 1 Choose **Configuration** > **Device Management** > **Logging** > **Syslog Setup**.
Step 2 Select the syslog whose severity level you want to change from the table, then click **Edit**.

The **Edit Syslog ID Settings** dialog box appears.

Step 3 Choose the desired severity level from the **Logging Level** drop-down list, then click **OK**.

Block Syslog Messages on a Standby Unit

To block specific syslog messages from being generated on a standby unit, perform the following steps:

Procedure

Step 1 Choose **Configuration** > **Device Management** > **Logging** > **Syslog Settings**.

Step 2 Choose a syslog ID in the table, then click **Edit**.

The **Edit Syslog ID Settings** dialog box appears.

Step 3 Check the **Disable messages on standby unit** check box to block syslog messages from being generated on a standby unit.

Step 4 Click **OK** to close this dialog box.

Include the Device ID in Non-EMBLEM Format Syslog Messages

To include the device ID in non-EMBLEM format syslog messages, perform the following steps:

Procedure

Step 1 Choose **Configuration** > **Device Management** > **Logging** > **Syslog Setup** > **Advanced** > **Advanced Syslog Configuration.**

Step 2 Check the **Enable syslog device ID** check box.

Step 3 Click the **Hostname**, **Interface IP Address**, or **String** radio button in the **Device ID** area.

- If you chose the **Interface IP Address** option, make sure that the correct interface is selected in the drop-down list.
- If you chose the **String** option, enter the device ID in the **User-Defined ID** field. The string can include as many as 16 characters.

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

Step 4 Click **OK** to close the **Advanced Syslog Configuration** dialog box.

Create a Custom Event List

You use the following three criteria to define an event list:

- Event Class
- Severity
- Message ID

To create a custom event list to send to a specific logging destination (for example, an SNMP server), perform the following steps:

Procedure

Step 1 Choose **Configuration** > **Device Management** > **Logging** > **Event Lists**.

Step 2 Click **Add** to display the **Add Event List** dialog box.

Step 3 Enter the name of the event list. No spaces are allowed.

Step 4 Click **Add** to display the **Add Class and Severity Filter** dialog box.

Step 5 Choose the event class from the drop-down list. Available event classes change according to the device mode that you are using.

Step 6 Choose the severity level from the drop-down list. Severity levels include the following:

- Emergency (level 0, system is unusable)

  Note
  Using a severity level of zero is not recommended.

- Alert (level 1, immediate action is needed)
- Critical (level 2, critical conditions)
- Error (level 3, error conditions)
- Warning (level 4, warning conditions)
- Notification (level 5, normal but significant conditions)
- Informational (level 6, informational messages only)
- Debugging (level 7, debugging messages only)

Step 7 Click **OK** to close the **Add Event List** dialog box.

Step 8 Click **Add** to display the **Add Syslog Message ID Filter** dialog box.

Step 9 Enter a syslog message ID or range of IDs (for example, 101001-199012) to include in the filter.

Step 10 Click **OK** to close the **Add Event List** dialog box.

The event of interest appears in the list.

Configure Logging Filters

Apply Message Filters to a Logging Destination

To apply message filters to a logging destination, perform the following steps:

Procedure

Step 1 Choose **Configuration** > **Device Management** > **Logging** > **Logging Filters**.

Step 2 Choose the name of the logging destination to which you want to apply a filter. Available logging destinations are as follows:

- ASDM
- Console port
- E-Mail
- Internal buffer
- SNMP server
- Syslog server
- Telnet or SSH session

Included in this selection are the second column, Syslogs From All Event Classes, and the third column, Syslogs From Specific Event Classes. The second column lists the severity or the event class to use to filter messages for the logging destination, or whether logging is disabled for all event classes. The third column lists the event class to use to filter messages for that logging destination.

Step 3 Click **Edit** to display the **Edit Logging Filters** dialog box. To apply, edit, or disable filters, see Apply Logging Filters, on page 25.

Apply Logging Filters

To apply filters, perform the following steps:

Procedure

Step 1 Choose the **Filter on severity** option to filter syslog messages according to their severity level.

Step 2 Choose the **Use event list** option to filter syslog messages according to an event list.

Step 3 Choose the **Disable logging from all event classes** option to disable all logging to the selected destination.

Step 4 Click **New** to add a new event list. To add a new event list, see Create a Custom Event List, on page 24.

Step 5 Choose the event class from the drop-down list. Available event classes change according to the device mode that you are using.

Step 6 Choose the level of logging messages from the drop-down list. Severity levels include the following:

- Emergency (level 0, system is unusable)

  Note
  Using a severity level of zero is not recommended.

- Alert (level 1, immediate action is needed)
- Critical (level 2, critical conditions)
- Error (level 3, error conditions)
- Warning (level 4, warning conditions)
- Notification (level 5, normal but significant conditions)
- Informational (level 6, informational messages only)
- Debugging (level 7, debugging messages only)

Step 7 Click **Add** to add the event class and severity level, then click **OK**.

The selected logging destination for a filter appears at the top.

Add or Edit a Syslog Message ID Filter

To add or edit a syslog message ID filter, see Edit Syslog ID Settings, on page 20.

Add or Edit a Message Class and Severity Filter

To add or edit a message class and severity level for filtering messages, perform the following steps:

Procedure

Step 1 Choose the event class from the drop-down list. Available event classes change according to the device mode that you are using.

Step 2 Choose the level of logging messages from the drop-down list. Severity levels include the following:

- Emergency (level 0, system is unusable)

  Note
  Using a severity level of zero is not recommended.

- Alert (level 1, immediate action is needed)
- Critical (level 2, critical conditions)
- Error (level 3, error conditions)
- Warning (level 4, warning conditions)
- Notification (level 5, normal but significant conditions)
- Informational (level 6, informational messages only)

- Debugging (level 7, debugging messages only)

Step 3 Click **OK** when you are done making selections.

Send All Syslog Messages in a Class to a Specified Output Destination

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

Procedure

Step 1 Choose **Configuration** > **Device Management** > **Logging** > **Logging Filters**.

Step 2 To override the configuration in the specified output destination, choose the output destination that you want to change, then click **Edit**.

The **Edit Logging Filters** dialog box appears.

Step 3 Revise the settings in either the **Syslogs from All Event Classes** or **Syslogs from Specific Event Classes** area, then click **OK** to close this dialog box.

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.

To specify that a class should go to more than one destination, select a different filtering option for each output destination.

Limit the Rate of Syslog Message Generation

To limit the rate of syslog message generation, perform the following steps:

Procedure

Step 1 Choose **Configuration** > **Device Management** > **Logging** > **Rate Limit**.

Step 2 Choose the logging level (message severity level) to which you want to assign rate limits. Severity levels are defined as follows:

- Emergency (level 0, system is unusable)
- Alert (level 1, immediate action is needed)
- Critical (level 2, critical conditions)
- Error (level 3, error conditions)
- Warning (level 4, warning conditions)
- Notification (level 5, normal but significant conditions)

- Informational (level 6, informational messages only)
- Debugging (level 7, debugging messages only)

Step 3 The **No of Messages** field displays the number of messages sent. The **Interval** (Seconds) field displays the interval, in seconds, that is used to limit how many messages at this logging level can be sent. Choose a logging level from the table and click **Edit** to display the **Edit Rate Limit for Syslog Logging Level** dialog box.

Step 4 To continue, see Assign or Change Rate Limits for Individual Syslog Messages, on page 28.

Assign or Change Rate Limits for Individual Syslog Messages

To assign or change rate limits to individual syslog messages, perform the following steps:

Procedure

Step 1 To assign the rate limit of a specific syslog message, click **Add** to display the **Add Rate Limit for Syslog Message** dialog box.

Step 2 To continue, see Add or Edit the Rate Limit for a Syslog Message, on page 28.

Step 3 To change the rate limit of a specific syslog message, click **Edit** to display the **Edit Rate Limit for Syslog Message** dialog box.

Step 4 To continue, see Edit the Rate Limit for a Syslog Severity Level, on page 29.

Add or Edit the Rate Limit for a Syslog Message

To add or change the rate limit for a specific syslog message, perform the following steps:

Procedure

Step 1 To add a rate limit to a specific syslog message, click **Add** to display the **Add Rate Limit for Syslog Message** dialog box. To change a rate limit for a syslog message, click **Edit** to display the **Edit Rate Limit for Syslog Message** dialog box.

Step 2 Enter the message ID of the syslog message that you want to limit.

Step 3 Enter the maximum number of messages that can be sent in the specified time interval.

Step 4 Enter the amount of time, in seconds, that is used to limit the rate of the specified message, then click **OK**.

Note
To allow an unlimited number of messages, leave both the **Number of Messages** and **Time Interval** fields blank.

Edit the Rate Limit for a Syslog Severity Level

To change the rate limit of a specified syslog severity level, perform the following steps:

Procedure

Step 1 Enter the maximum number of messages at this severity level that can be sent.

Step 2 Enter the amount of time, in seconds, that is used to limit the rate of messages at this severity level, and click **OK**.

The selected message severity level appears.

Note
To allow an unlimited number of messages, leave both the **Number of Messages** and **Time Interval** fields blank.

Assign or Change Rate Limits for Dynamic Logging

You can assign rate limits for logging based on used resources (block size). By specifying a threshold value (percentage), the rate of syslog message generation is limited. You can further define the number of the messages permitted to be generated when the block size usage exceeds the threshold value.

Procedure

Step 1 Choose **Configuration** > **Device Management** > **Logging** > **Rate Limit**.

Step 2 Under **Rate Limits for Dynamic Logging**, specify the following:

- **Block**—Specify the percentage of free blocks that act as the threshold to trigger the dynamic rate-limit.
- **Message Limit**—Specify the number of messages allowed for the dynamic rate-limit. The default value is 10.

Step 3 Click **Apply**.

Step 4 To modify the saved values, enter the new values, and then click **Apply**.

Step 5 To disable the dynamic logging rate-limit, leave the fields blank.

Monitoring the Logs

See the following commands for monitoring logging status.

- **Monitoring** > **Logging** > **Log Buffer** > **View**

  This pane allows you to view the log buffer.

- **Monitoring** > **Logging** > **Real-Time Log Viewer** > **View**

  This pane allows you to view the real-time log.

- **Tools** > **Command Line Interface**

  This pane allows you to issue various non-interactive commands and view results.

- **Configuration** > **Firewall** > **Access Rules**

  This pane allows you to filter the live viewer of logging to that specific logs based on the search criteria (Rule Hex Id). To view the results, select the rule and click **Show Log**.

Filter Syslog Messages Through the Log Viewers

You can filter syslog messages based on one or multiple values that correspond to any column of the Real-Time Log Viewer and the Log Buffer Viewer.

To filter syslog messages through one of the log viewers, perform the following steps:

Procedure

Step 1 Choose one of the following options:

- **Monitoring** > **Logging** > **Real-Time Log Viewer** > **View**
- **Monitoring** > **Logging** > **Log Buffer** > **View**

Step 2 In either the **Real-Time Log Viewer** or the **Log Buffer Viewer** dialog box, click **Build Filter** on the toolbar.

Step 3 In the **Build Filter** dialog box, specify the filtering criteria to apply to syslog messages:

a) Choose one of the following three options in the **Date and Time** area: real-time, a specific time, or a time range. If you chose a specific time, indicate the time by entering the number and choosing hours or minutes from the drop-down list. If you chose a time range, click the drop-down arrow in the **Start Time** field to display a calendar. Choose a start date and a start time from the drop-down list, then click **OK**. Click the drop-down arrow in the **End Time** field to display a calendar. Choose an end date and an end time from the drop-down list, then click **OK**.

b) Enter a valid severity level in the **Severity** field. Alternatively, click the **Edit** icon on the right of the **Severity** field. Click the severity levels in the list on which you want to filter. To include severity levels 1-7, click **All**. Click **OK** to display these settings in the **Build Filter** dialog box. Click the **Info** icon on the right of the **Severity** field for additional information about the correct input format to use.

c) Enter a valid syslog ID in the **Syslog ID** field. Alternatively, click the **Edit** icon on the right of the **Syslog ID** field. Choose a condition on which to filter from the drop-down list, then click **Add**. Click **OK** to display these settings in the **Build Filter** dialog box. Click the **Info** icon on the right of the **Syslog ID** field for additional information about the correct input format to use.

d) Enter a valid source IP address in the **Source IP Address** field, or click the **Edit** icon on the right of the **Source IP Address** field. Choose a single IP address or a specified range of IP addresses, then click **Add**. Check the **Do not include (exclude) this address or range** check box to exclude a specific IP address or range of IP addresses, Click **OK** to display these settings in the **Build Filter** dialog box. Click the **Info** icon on the right of the **Source IP Address** field for additional information about the correct input format to use.

e) Enter a valid source port in the **Source Port** field, or click the **Edit** icon on the right of the **Source Port** field. Choose a condition on which to filter from the drop-down list, then click **Add**. Click **OK** to display these settings in the **Build Filter** dialog box. Click the **Info** icon on the right of the **Source Port** field for additional information about the correct input format to use.

f) Enter a valid destination IP address in the **Destination IP Address** field, or click the **Edit** icon on the right of the **Destination IP Address** field. Choose a single IP address or a specified range of IP addresses, then click **Add**. Check the **Do not include (exclude) this address or range** check box o exclude a specific IP address or range of IP addresses. Click **OK** to display these settings in the **Build Filter** dialog box. Click the **Info** icon on the right of the **Destination IP Address** field for additional information about the correct input format to use.

g) Enter a valid destination port in the **Destination Port** field, or click the **Edit** icon on the right of the **Destination Port** field. Choose a condition on which to filter from the drop-down list, then click **Add**. Click **OK** to display these settings in the **Build Filter** dialog box. Click the **Info** icon on the right of the **Destination Port** field for additional information about the correct input format to use.

h) Enter filtering text for the **Description** field. The text may be any string of one or more characters, including a regular expression. However, semicolons are not valid characters, and this setting is case-sensitive. Multiple entries must be separated by commas.

i) Click **OK** to add the filter settings you have just specified to the **Filter By** drop-down list in the log viewers. The filter strings follow a specific format. The prefix FILTER: designates all custom filters that appear in the **Filter By** drop-down list. You may still type random text into this field.

The following table shows examples of the format used.

Build Filter Example	Filter String Format
Source IP = 192.168.1.1 or 0.0.0.0 Source Port = 67	FILTER: srcIP=192.168.1.1,0.0.0.0;srcPort=67;
Severity = Informational Destination IP = 1.1.1.1 through 1.1.1.10	FILTER: sev=6;dstIP=1.1.1.1-1.1.1.10;
Syslog ID not in the range 725001 through 725003	FILTER: sysID=!725001-725003;
Source IP = 1.1.1.1 Description = Built outbound	FILTER: srcIP=1.1.1.1;descr=Built outbound

Step 4 Choose one of the settings in the **Filter By** drop-down list to filter syslog messages, then click **Filter** on the toolbar. This setting also applies to all future syslog messages. Click **Show All** on the toolbar to clear all filters.

Note
You cannot save filters that you have specified with the **Build Filter** dialog box. These filters are valid only for the ASDM session during which they were created.

Edit Filtering Settings

To edit filtering settings that you created using the **Build Filter** dialog box, perform the following steps:

Procedure

Choose one of the following options:

- Revise a filter directly by entering the changes in the **Filter By** drop-down list.
- Choose a filter in the **Filter By** drop-down list, then click **Build Filter** to display the **Build Filter** dialog box. Click **Clear Filter** to remove the current filter settings and enter new ones. Otherwise, change the settings that appear, and click **OK**.

  Note
  These filter settings apply only to those defined in the **Build Filter** dialog box.

- Click **Show All** on the toolbar to stop filtering and show all syslog messages.

Issue Certain Commands Using the Log Viewers

You can issue the following commands using either of the log viewers: **ping**, **traceroute**, **whois**, and **dns lookup**.

To run any of these commands, perform the following steps:

Procedure

Step 1 Choose one of the following options:

- **Monitoring** > **Logging** > **Real-Time Log Viewer** > **View**
- **Monitoring** > **Logging** > **Log Buffer** > **View**

Step 2 Click **Tools** from the **Real-Time Log Viewer** or **Log Buffer** pane, then choose the command that you want to execute. Alternatively, you can right-click a specific syslog message that is listed to display a context menu, then choose the command that you want to execute.

The **Entering command** dialog box appears, with the command that you selected automatically showing in the drop-down list.

Step 3 Enter either the source or destination IP address of the selected syslog message in the **Address** field, then click **Go**.

The command output appears in the area provided.

Step 4 Click **Clear** to remove the output, and choose another command to execute from the drop-down list. Repeat Step 3, if necessary. Click **Close** when you are done.

History for Logging

Table 3: History for Logging

Feature Name	Platform Releases	Description
Logging	7.0(1)	Provides ASA network logging information through various output destinations, and includes the option to view and save log files. We introduced the following screen: Configuration > Device Management > Logging > Logging Setup.
Rate limit	7.0(4)	Limits the rate at which syslog messages are generated. We modified the following screen: Configuration > Device Management > Logging > Rate Limit.
Logging list	7.2(1)	Creates a logging list to use in other commands to specify messages by various criteria (logging level, event class, and message IDs). We modified the following screen: Configuration > Device Management > Logging > Event Lists.
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 screen: Configuration > Device Management > Logging > Syslog Server.
Logging class	8.0(4), 8.1(1)	Added support for the ipaa event class of logging messages. We modified the following screen: Configuration > Device Management > Logging > Logging Filters.
Logging class and saved logging buffers	8.2(1)	Added support for the dap event class of logging messages. Added support to clear the saved logging buffers (ASDM, internal, FTP, and flash). We modified the following screen: Configuration > Device Management > Logging > Logging Setup.
Password encryption	8.3(1)	Added support for password encryption.
Log viewers	8.3(1)	The source and destination IP addresses were added to the log viewers.

Feature Name	Platform Releases	Description
Enhanced logging and connection blocking	8.3(2)	When you configure a syslog server to use TCP, and the syslog server is unavailable, the ASA 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 ASA is full; connections resume when the logging queue is cleared. This feature was added for compliance with Common Criteria EAL4+. Unless required, we recommended allowing connections when syslog messages cannot be sent or received. To allow connections, continue to check the **Allow user traffic to pass when TCP syslog server is down** check box on the Configuration > Device Management > Logging > Syslog Servers pane. We introduced the following syslog messages: 414005, 414006, 414007, and 414008. We did not modify any ASDM screens.
Syslog message filtering and sorting	8.4(1)	Support has been added for the following: • Syslog message filtering based on multiple text strings that correspond to various columns • Creation of custom filters • Column sorting of messages. For detailed information, see the ASDM configuration guide. This feature interoperates with all ASA versions. We modified the following screens: Monitoring > Logging > Real-Time Log Viewer > View. Monitoring > Logging > Log Buffer Viewer > View.
Clustering	9.0(1)	Added support for syslog message generation in a clustering environment on the ASA 5580 and 5585-X. We modified the following screen: Configuration > Logging > Syslog Setup > Advanced > Advanced Syslog Configuration.
Blocking syslogs on a standby unit	9.4(1)	We added support for blocking the generation of specific syslog messages on the standby unit in a failover configuration. We modified the following screen: Configuration > Device Management > Logging > Syslog Setup.
Reference Identities for Secure Syslog Server connections	9.6(2)	TLS client processing now supports rules for verification of a server identity defined in RFC 6125, Section 6. Identity verification will be done during PKI validation for TLS connections to the Syslog Server. If the presented identity cannot be matched against the configured reference identity, the connection is not established. We modifed the following pages: **ASDM Configuration > Remote Access VPN > Advanced**, and **Configuration > Device Management > Logging > Syslog Servers -> Add or Edit.**

Feature Name	Platform Releases	Description
IPv6 address support for syslog servers	9.7(1)	You can now configure syslog servers with IPv6 addresses to record, send, and receive syslogs over TCP and UDP. We modified the following screen: **Configuration** > **Device Management** > **Logging** > **Syslog Servers** > **Add Syslog Server**
Logging class	9.12(1)	Added support for the BFD, BGP, interface, IPv6, Muticast, Object-Group-Search, PBR, routing, SLA class of logging messages. We modified the following screen: **Configuration** > **Device Management** > **Logging** > **Logging Filters**.
Loopback interface support for syslog	9.18(2)	You can now add a loopback interface and use it for syslog. New/Modified commands: **interface loopback**, **logging host** New/Modified screens: **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** > **Add Loopback Interface** ASDM support was added in 7.19.
Rate limiting for SNMP syslogs	9.20(1)	If you do not set system-wide rate limiting, you can now configure rate limiting separately for syslogs sent to an SNMP server.