CHAPTER 45

Logging

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 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, 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:

- Syslog Message Format, page 45-3
- Severity Levels, page 45-3
- Message Classes and Range of Syslog IDs, page 45-4
- Filtering Syslog Messages, page 45-4
- Sorting in the Log Viewers, page 45-4
- Using Custom Message Lists, page 45-5
- Using Clustering, page 45-5

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

Analyzing Syslog Messages

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

- Connections that are allowed by ASA and ASASM security policies. These messages help you spot holes that remain open in your security policies.
- Connections that are denied by ASA and ASASM security policies. These messages show what types of activity are being directed toward your secured inside network.
- Using the ACE deny rate logging feature shows attacks that are occurring on your ASA or ASA Services Module.
- 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:

ASA	The syslog message facility code for messages that are generated by the ASA and ASASM. This value is always ASA.
Level	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 45-1 for more information.
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.

Severity Levels

Table 45-1 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 45-1 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 and ASASM do 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.

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 and ASASM to send all syslog messages to one output destination and to send a subset of those syslog messages to a different output destination.

Specifically, you can configure the ASA and ASASM so that syslog messages are directed to an output destination according to the following criteria:

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

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

You can use syslog message classes in two ways:

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

The syslog message class provides a method of categorizing syslog messages by type, equivalent to a feature or function of the ASA and ASASM. For example, the vpnc class denotes the VPN client.

All syslog messages in a particular class share the same initial three digits in their syslog message ID numbers. For example, all syslog message IDs that begin with the digits 611 are associated with the vpnc (VPN client) class. Syslog messages associated with the VPN client feature range from 611101 to 611323.

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

The objects are prefixed as follows:

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

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

Sorting 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.

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.

Using 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 timestamp 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.

Licensing Requirements for Logging

Model	License Requirement
ASAv	Standard or Premium License.
All other models	Base License.

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 or ASASM, you must specify a logging output destination. If you enable logging without specifying a logging output destination, the ASA and ASASM generate 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.

Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

Supported in single and multiple context modes.

Firewall Mode Guidelines

Supported in routed and transparent firewall modes.

IPv6 Guidelines

Does not support IPv6.

Additional Guidelines

- Sending syslogs over TCP is not supported on a standby ASA.
- The ASA 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.
- The syslog server should be reachable through the ASA and ASASM. You should configure the ASA SM to deny ICMP unreachable messages on the interface through which the syslog server is reachable and to send syslogs to the same server. Make sure that you have enabled logging for all severity levels. To prevent the syslog server from crashing, suppress the generation of syslogs 313001, 313004, and 313005.
- 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. When you explicitly change the logging severity level of the access list configuration to debugging, you must also change the logging configuration itself.

  The following is sample output from the **show running-config logging** command that will 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
  ```

The following is sample output from the **show running-config logging** command that will 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 the following 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
```

Configuring Logging

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

- Enabling Logging, page 45-7
- Configuring an Output Destination, page 45-8

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

Enabling Logging

To enable logging, perform the following steps:

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.

What to Do Next

See Configuring an Output Destination, page 45-8.

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:

- Including the Date and Time in Syslog Messages, page 45-22
- Disabling a Syslog Message, page 45-22
- Changing the Severity Level of a Syslog Message, page 45-23
- Limiting the Rate of Syslog Message Generation, page 45-23
- Assigning or Changing Rate Limits for Individual Syslog Messages, page 45-24
- Adding or Editing the Rate Limit for a Syslog Message, page 45-24
- Editing the Rate Limit for a Syslog Severity Level, page 45-24

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:

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

Step 2 Check the **Enable logging** check box to turn on logging for the main 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 In the Buffer Size field, 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. For more information, see Configuring FTP Settings, page 45-10.

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

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. For more information, see Configuring Logging Flash Usage, page 45-10.

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

Step 11 In the Queue Size field, specify the queue size for system logs that are to be viewed in the ASA or ASASM.

Configuring FTP Settings

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

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

Step 2 In the Server IP Address field, specify the IP address of the FTP server.

Step 3 In the Path field, specify the directory path on the FTP server to store the saved log buffer content.

Step 4 In the Username field, specify the username to log in to the FTP server.

Step 5 In the Password field, specify the password associated with the username to log in to the FTP server.

Step 6 In the Confirm Password field, reenter the password, and click **OK**.

Configuring Logging Flash Usage

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

Step 1 In the Maximum Flash to Be Used by Logging field, specify the maximum amount of internal flash memory that can be used for logging (in KB).

Step 2 In the Minimum Free Space to Be Preserved field, 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 this dialog box.

Configuring Syslog Messaging

To configure syslog messaging, perform the following steps:

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

Step 2 From the Facility code to include in syslogs drop-down list, 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 To add the date and time in each syslog message sent, check the **Include timestamp in syslogs** check box.

Step 4 From the Show drop-down list, choose the information to be displayed in the Syslog ID table. Available options are as follows:

- To specify that the Syslog ID table should display the entire list of syslog message IDs, choose **Show all syslog IDs**.
- To specify that the Syslog ID table should display only those syslog message IDs that have been explicitly disabled, choose **Show disabled syslog IDs**.
- 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 with changed logging**.
- 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, choose **Show syslog IDs that are disabled or with a changed logging level**.

Step 5 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 6 To configure syslog messages to include a device ID, click **Advanced**. For more information, see Editing Syslog ID Settings, page 45-11 and the Including a Device ID in Non-EMBLEM Formatted Syslog Messages, page 45-12.

Editing 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.

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 From the Logging Level drop-down list, choose the severity 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 this dialog box.

Including a Device ID in Non-EMBLEM Formatted Syslog Messages

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

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.

  If you are using clustering, check the **In an ASA cluster, always use master's IP address for the selected interface** check box.
- String

  In the User-Defined ID field, specify an alphanumeric, user-defined string.
- ASA cluster name

Step 3 Click **OK** to close this dialog box.

Sending 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 and ASASM to save the full buffer to another location.

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

Step 1 To specify which syslog messages should be sent to the internal log buffer, choose one of the following:

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

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

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

The ASA and ASASM 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 and ASASM 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:

- To send new messages to internal flash memory, check the **Flash** check box, 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.
- To send new messages to an FTP server, check the **FTP Server** check box, 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.

Saving an Internal Log Buffer to Flash

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

Step 1 In the main ASDM application window, 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**.

Viewing and Copying Logged Entries with the ASDM Java Console

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

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

Step 1 In the main ASDM application window, choose **Tools > ASDM Java Console**.

Step 2 To show the virtual machine memory statistics, enter **m** in the console.

Step 3 To perform garbage collection, enter **g** in the console.

Step 4 To monitor memory usage, open the Windows Task Manager and double-click the **asdm_launcher.exe** file.

Note The maximum memory allocation allowed is 256 MB.

Step 5 To continue, see the firewall configuration guide.

Sending Syslog Messages to an E-mail Address

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

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

Step 2 In the Source E-Mail Address field, 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. For more information, see Adding or Editing E-Mail Recipients, page 45-14.

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. For more information, see Applying Logging Filters, page 45-16.

Step 5 Click **Edit** to modify an existing severity level of the syslog messages that are sent to this recipient. For more information, see Adding or Editing E-Mail Recipients, page 45-14.

Step 6 Click **OK** to close this dialog box.

Step 7 To continue, see Configuring the Remote SMTP Server, page 45-15.

Adding or Editing E-Mail Recipients

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

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 this 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.

Configuring 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:

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.

Viewing Syslog Messages in ASDM

To view the latest syslog messages that have been sent to ASDM, choose **Home > Latest ASDM Syslog Messages**. The ASA or ASASM 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 or ASASM 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.

Applying Message Filters to a Logging Destination

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

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. For more information, see Adding or Editing a Message Class and Severity Filter, page 45-17 and the Adding or Editing a Syslog Message ID Filter, page 45-17.

Step 3 Click **Edit** to display the Edit Logging Filters dialog box. To apply, edit, or disable filters, see Applying Logging Filters, page 45-16.

Applying Logging Filters

To apply filters, perform the following steps:

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 Creating a Custom Event List, page 45-18.

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, and then click **OK**.

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

Adding or Editing a Message Class and Severity Filter

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

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.

Adding or Editing a Syslog Message ID Filter

To add or edit a syslog message ID filter, see Editing Syslog ID Settings, page 45-11.

Sending Syslog Messages to the Console Port

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

Step 1 In ASDM, 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 To specify which syslog messages should be sent to the console port, choose either syslogs from all event classes or syslogs from specific event classes.

Step 4 To continue, see Applying Logging Filters, page 45-16.

Sending Syslog Messages to a Telnet or SSH Session

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

Step 1 In ASDM, choose one of the following:

- **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 To specify which syslog messages should be sent to a Telnet or an SSH session, choose either syslogs from all event classes or syslogs from specific event classes.

Step 4 To continue, see Applying Logging Filters, page 45-16.

Step 5 To enable logging for the current session only, choose **Configuration > Device Management > Logging > Logging Setup.**

Step 6 Check the **Enable logging** check box, then click **Apply**.

Creating a Custom Event List

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

- Event Class
- Severity
- Message ID

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

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

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

Step 3 In the Name field, enter the name of the event list. No spaces are allowed.

Step 4 In the Event Class/Severity area, 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 this dialog box.

Step 8 In the Message ID Filters area, click **Add** to display the Add Syslog Message ID Filter dialog box.

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

Step 10 Click **OK** to close this dialog box.

The event of interest appears in the list. To change this entry, click **Edit**.

Generating Syslog Messages in EMBLEM Format to a Syslog Server

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

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

Step 2 To add a new syslog server, click **Add** to display the Add Syslog Server dialog box. To change an existing syslog server settings, click **Edit** to display the Edit Syslog Server dialog box.

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 or ASASM when a syslog server is busy. A zero value means an unlimited number of messages may be queued.

Check the **Allow user traffic to pass when TCP syslog server is down** check box to specify whether or not to restrict all traffic if any syslog server is down. If you specify TCP, the ASA or ASASM discovers when the syslog server fails and as a security protection, new connections through the ASA are blocked. If you specify UDP, the ASA or ASASM 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.

Step 4 To continue, see Adding or Editing Syslog Server Settings, page 45-19.

Adding or Editing Syslog Server Settings

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

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, but not both. The default protocol is UDP if you do not specify a protocol.

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.

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

Generating Syslog Messages in EMBLEM Format to Other Output Destinations

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

Step 1 In ASDM, choose **Configuration > Device Management > Logging > Logging Setup**.

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

Step 3 To continue, see Applying Logging Filters, page 45-16.

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:

Step 1 In ASDM, choose **Configuration > Device Management > Logging > Logging Setup**.

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

Step 3 In the Logging to Internal Buffer area, check the **Save Buffer to Flash** check box.

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 1 MB of internal flash memory for log data. The minimum amount of internal flash memory that must be free for the ASA and ASASM 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 or ASASM 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 or ASASM fails to save the new log file.

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 this dialog box.

Configuring the Logging Queue

To configure the logging queue, perform the following steps:

Step 1 In ASDM, choose **Configuration > Device Management > Logging > Logging Setup.**

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

Step 3 In the ASDM Logging area, enter the number of syslog messages that the ASA and ASASM can hold in its queue before sending them to the configured output destination.

The ASA and ASASM have a fixed number of blocks in memory that can be allocated for buffering syslog messages while they are waiting to be sent to the configured output destination. The number of blocks required depends on the length of the syslog message queue and the number of syslog servers specified. The default queue size is 512 syslog messages. The queue size is limited only by block memory availability. Valid values are from 0 to 8192 messages, depending on the platform. If the logging queue is set to zero, the queue is the maximum configurable size (8192 messages), depending on the platform. The maximum queue size by platform is as follows:

- ASA-5505—1024
- On all other platforms—8192

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

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, perform the following steps:

Step 1 In ASDM, choose **Configuration > Device Management > Logging > Logging Filters.**

Step 2 To overrides 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.

Enabling Secure Logging

To enable secure logging, perform the following steps:

Step 1 In ASDM, 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.

Note 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**.

Including the Device ID in Non-EMBLEM Format Syslog Messages

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

Step 1 In ASDM, choose **Configuration > Device Management > Logging > Syslog Setup > Advanced > Advanced Syslog Configuration.**

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

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

- 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.

Including the Date and Time in Syslog Messages

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

Step 1 In ASDM, choose **Configuration > Device Management > Logging > Syslog Setup.**

Step 2 In the Syslog ID Setup area, check the **Include timestamp in syslogs** check box.

Step 3 Click **Apply** to save your changes.

Disabling a Syslog Message

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

Step 1 In ASDM, choose **Configuration > Device Management > Logging > Syslog Setup**.

Step 2 Select the syslog that you want to disable from the table, t hen click **Edit**.

The Edit Syslog ID Settings dialog box appears.

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

Changing the Severity Level of a Syslog Message

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

Step 1 In ASDM, choose **Configuration > Device Management > Logging > Syslog Setup**.

Step 2 Select the syslog whose severity level you want to change from the table, t hen 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**.

Limiting the Rate of Syslog Message Generation

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

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:

Description	Severity Level
Emergency	0—System is unusable
Alert	1—Immediate action is needed
Critical	2—Critical conditions
Error	3—Error conditions
Warning	4—Warning conditions
Notification	5—Normal but significant conditions
Informational	6—Informational messages only
Debugging	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 Assigning or Changing Rate Limits for Individual Syslog Messages, page 45-24.

Assigning or Changing Rate Limits for Individual Syslog Messages

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

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 Adding or Editing the Rate Limit for a Syslog Message, page 45-24.

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 Editing the Rate Limit for a Syslog Severity Level, page 45-24.

Adding or Editing the Rate Limit for a Syslog Message

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

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, and click **OK**.

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

Editing the Rate Limit for a Syslog Severity Level

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

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.

Monitoring the Logs

This section includes the following topics:

- Filtering Syslog Messages Through the Log Viewers, page 45-25
- Editing Filtering Settings, page 45-27
- Executing Certain Commands Using the Log Viewers, page 45-27

To monitor the logs in the log buffer or in real-time and assist in monitoring the system performance, eperform the following steps:

Step 1 In ASDM, choose one of the following:

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

The Real-Time Log Viewer or Log Buffer dialog box that appears displays the message explanations, additional details, and recommended actions to take, if necessary, to resolve an error in a separate window.

Step 2 To continue, see Filtering Syslog Messages Through the Log Viewers, page 45-25.

Filtering 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:

Step 1 Choose one of the following:

- **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. In the Date and Time area, choose one of the following three options: 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, in the Start Time field, click the drop-down arrow to display a calendar. Choose a start date and a start time from the drop-down list, then click **OK**. In the End Time field, click the drop-down arrow 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. In the Severity dialog box, 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. For additional information about the correct input format to use, click the **Info** icon on the right of the Severity field.

c. Enter a valid syslog ID in the Syslog ID field. Alternatively, click the **Edit** icon on the right of the Syslog ID field. In the Syslog ID dialog box, 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 **Delete** to remove these settings and enter new ones. For additional information about the correct input format to use, click the **Info** icon on the right of the Syslog ID field.

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. In the Source IP Address dialog box, choose a single IP address or a specified range of IP addresses, then click **Add**. To exclude a specific IP address or range of IP addresses, check the **Do not include (exclude) this address or range** check box. Click **OK** to display these settings in the Build Filter dialog box. Click **Delete** to remove these settings and enter new ones. For additional information about the correct input format to use, click the **Info** icon on the right of the Source IP Address field.

e. Enter a valid source port in the Source Port field, or click the **Edit** icon on the right of the Source Port field. In the Source Port dialog box, 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 **Delete** to remove these settings and enter new ones. For additional information about the correct input format to use, click the **Info** icon on the right of the Source Port field.

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. In the Destination IP Address dialog box, choose a single IP address or a specified range of IP addresses, then click **Add**. To exclude a specific IP address or range of IP addresses, check the **Do not include (exclude) this address or range** check box. Click **OK** to display these settings in the Build Filter dialog box. Click **Delete** to remove these settings and enter new ones. For additional information about the correct input format to use, click the **Info** icon on the right of the Destination IP Address field.

g. Enter a valid destination port in the Destination Port field, or click the **Edit** icon on the right of the Destination Port field. In the Destination Port dialog box, 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 **Delete** to remove these settings and enter new ones. For additional information about the correct input format to use, click the **Info** icon on the right of the Destination Port field.

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

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.

Editing Filtering Settings

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

Choose one of the following:

- 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. To remove the current filter settings and enter new ones, click **Clear Filter**. Otherwise, change the settings that appear, and click **OK**.

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

- To stop filtering and show all syslog messages, click **Show All** on the toolbar.

Executing Certain Commands Using the Log Viewers

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

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

Step 1 Choose one of the following:

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

Step 2 From the Real-Time Log Viewer or Log Buffer pane, click **Tools**, 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.

Feature History for Logging

Table 45-2 lists each feature change and the platform release in which it was implemented. ASDM is backward-compatible with multiple platform releases, so the specific ASDM release in which support was added is not listed.

Table 45-2 Feature History for Logging

Feature Name	Platform Releases	Feature Information
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.

Table 45-2 Feature History for Logging (continued)

Feature Name	Platform Releases	Feature Information
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. We modified the following screens: Monitoring > Logging > Real-Time Log Viewer > View. Monitoring > Logging > Log Buffer Viewer > View. This feature interoperates with all ASA versions.
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.