



CHAPTER 45

Monitoring Logging

You can view real-time syslog messages that appear in the log buffer. When you open the Cisco ASDM 6.1(3) for ASA 8.0(4) main application window, the most recent ASDM system log messages appear at the bottom of a scrolling window.

You can use these messages to help troubleshoot errors or monitor system usage and performance. For a description of the Logging feature, see [Chapter 17, “Configuring Logging.”](#)

About Log Viewing

This section describes syslog message viewing, and includes the following topics:

- [Log Buffer, page 45-1](#)
- [Real-Time Log Viewer, page 45-3](#)

Log Buffer

The Log Buffer pane lets you view syslog messages that have been saved in the buffer in a separate window. To access this pane, choose **Monitoring > Logging > Log Buffer**.

To view the log buffer, perform the following steps:

-
- Step 1** Choose the level of logging messages to view, ranging from Emergency to Debugging, from the drop-down list. For more information about severity levels, see [Chapter 17, “Configuring Logging.”](#)
 - Step 2** Click **View** to open a separate window in which log messages appear. To continue, see [Log Buffer Viewer, page 45-2](#).
-

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Log Buffer Viewer

The Log Buffer Viewer pane lets you view messages that appear in the log buffer, an explanation of the message, details about the message, and recommended actions to take, if necessary, to resolve an error. To access this pane, choose **Monitoring > Logging > Log Buffer > View**.

To use the log buffer viewer, perform the following steps:

Step 1 Right-click a message to display a menu from which you can select from the Refresh, Copy Selected Log Entry, Save Log, Clear Display, Color Settings, Create Access Rule, Show Access Rule, and Show Details options. A list of icons associated with each severity level appears at the bottom of this pane.

Step 2 Choose from the following actions:

- Click **Refresh** to refresh the display.
- Click **Copy Selected Log Entry** to copy a selected message.
- Click **Save Log** to save the contents of the log to your computer.
- Click **Clear Display** to clear the list of messages.
- Click **Color Settings** to specify that messages of different severity levels display in different colors.
- Click **Create Access Rule** to create an access control rule that performs the opposite action of the access control rule that originally generated the message.
- Click **Show Access Rule** to show the access control rule that caused the selected message to be generated. This feature applies only to system log message IDs 106100 and 106023.
- Click **Show Details** to show or hide the Explanation, Recommended Action, and Details tabs. The Explanation tab provides the message syntax, an explanation for the message, and the suggested corrective action to take, if any. The Recommended Action tab describes what you should do when you receive this message. The Details tab lists the date, time, severity level, syslog ID, source IP address, destination IP address, and a description of the message.
- In the Find field, enter text that you want to find in messages, and click the **Search** icon to start the search.
- Click **Help** to obtain more information.
- Enter text to filter messages by in the Filter By drop-down list, then press **Enter** or click **Filter** to apply the filter to the displayed messages. Click **Show All** to display all messages. Filters are removed from the display. This button is only active if a filter has been applied to the displayed syslog messages.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Real-Time Log Viewer

The Real-Time Log Viewer lets you view real-time syslog messages in a separate window. To access this pane, choose **Monitoring > Logging > Real-Time Log Viewer**.

To view syslog messages in real-time, perform the following steps:

-
- Step 1** Choose the level of logging messages to view, ranging from Emergency to Debugging, from the drop-down list.
 - Step 2** Enter the buffer limit, which is the maximum number of syslog messages to view. The default is 1000.
 - Step 3** Click **View** to open a separate window in which syslog messages appear. To continue, see [Real-Time Log Viewer, page 45-3](#).
-

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Real-Time Log Viewer

The Real-Time Log Viewer pane lets you view incoming messages in real-time and filter them based on text that you specify. To access this pane, choose **Monitoring > Logging > Real-Time Log Viewer > View**.

To use the real-time log viewer, perform the following steps:

-
- Step 1** Right-click a message in the viewer to display a menu from which you can select from the Pause, Copy Selected Log Entry, Save Log, Clear Display, Color Settings, Create Access Rule, Show Access Rule, and Show Details options. A list of color-coded icons that are associated with each severity level appears at the bottom of this pane. For more information about severity levels, see [Chapter 17, “Configuring Logging.”](#)
 - Step 2** Choose from the following actions:
 - Click **Pause** to stop the scrolling of the display.
 - Click **Copy Selected Log Entry** to copy a selected message.

- Click **Save Log** to save the contents of the log to your computer.
- Click **Clear Display** to clear the list of messages.
- Click **Color Settings** to specify that messages of different severity levels display in different colors.
- Click **Create Access Rule** to create an access control rule that performs the opposite action of the access control rule that originally generated the message.
- Click **Show Access Rule** to show the access control rule that caused the selected message to be generated. This feature applies only to syslog message IDs 106100 and 106023.
- Click **Show Details** to show or hide the Explanation, Recommended Action, and Details tabs. The Explanation tab provides the message syntax, an explanation for the message, and the suggested corrective action to take, if any. The Recommended Action tab describes what you should do when you receive this message. The Details tab lists the date, time, severity level, syslog ID, source IP address, destination IP address, and a description of the message.
- In the Find field, enter text that you want to find in messages, and click the **Search** icon to start the search.
- Click **Help** to obtain more information.
- Enter text to filter messages by in the Filter By drop-down list, then press **Enter** or click **Filter** to apply the filter to the displayed messages. Click **Show All** to display all messages. Filters are removed from the display. This button is only active if a filter has been applied to the displayed log messages.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—