



CHAPTER 28

Monitoring Logging

This chapter provides information about how to monitor logging and includes the following sections:

- [About Log Viewing, page 28-1](#)
- [Log Buffer, page 28-1](#)
- [Real-Time Log Viewer, page 28-3](#)

You can view real-time syslog messages that appear in the log buffer. When you open the ASDM main application window, the most recent ASDM syslog 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 information about how to configure logging, see [Chapter 16, “Configuring Logging.”](#)

About Log Viewing

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

- [Log Buffer, page 28-1](#)
- [Real-Time Log Viewer, page 28-3](#)

Log Buffer

Use the Log Buffer pane to view syslog messages saved in the buffer in a separate window. To access this pane, choose **Monitoring > Logging > Log Buffer**.

To view syslog messages in the buffer, perform the following steps:

-
- Step 1** Chose the level of syslog messages to view, ranging from Emergency to Debugging, from the drop-down list.
 - Step 2** Click **View** to open a separate window in which syslog messages appear. You can clear the message window, and save the contents of the log. You can also search messages for specific text.
-

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

Use the Log Buffer Viewer pane to 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 the Log Buffer Viewer pane, choose **Monitoring > Logging > Log Buffer > View**. A list of icons associated with each severity level appears at the bottom of this pane. For more information about severity levels, see [Chapter 16, “Configuring Logging.”](#)

To view messages and information about them in the log buffer, perform the following steps:

-
- Step 1** Right-click a message in this pane to display a menu from which you can choose from the following options: Refresh, Copy, Save, Clear, Color Settings, Create Rule, Show Rule, and Show Details.
 - Step 2** Click **Refresh** to update the display.
 - Step 3** Click **Copy** to copy a selected message.
 - Step 4** Click **Save** to save the contents of the log to a local file on your computer.
 - Step 5** Click **Clear** to clear the list of messages.
 - Step 6** Click **Color Settings** to specify that messages of different severity levels display in different colors.
 - Step 7** Click **Create Rule** to create an access control rule that performs the opposite action of the access control rule that originally generated the message.
 - Step 8** Click **Show Rule** to show the access control rule that caused the selected message to be generated. This feature applies only to syslog messages 106100 and 106023.
 - Step 9** 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, source port, destination port, and a description of the message.
 - Step 10** Click **Find** to enter the text you want to find in the messages. Searches the messages based on the text you enter.
 - Step 11** Click **Help** to obtain more information.
 - Step 12** Choose **Filter By** to enter text to filter the messages by. Press **Enter** or click **Filter** to apply the filter to the displayed messages.
 - Step 13** 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 messages.
 - Step 14** Click **Filter** to apply the filter to the message list.
-

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

Use the Real-Time Log Viewer pane to view real-time syslog messages in a separate window. To access the Real-Time Log Viewer pane, choose **Monitoring > Logging > Real-Time Log Viewer**.

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

-
- Step 1** Chose the level of logging messages to view, ranging from Emergency to Debugging, from the drop-down list.
 - Step 2** In the Buffer Limit field, enter 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. You can pause incoming messages, clear the message window, and save the contents of the log. You can also search messages for specific text, set color settings for different severity levels, create and show access rules, and show message details.
-

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

Use the Real-Time Log Viewer pane to view incoming messages in real time and filter them based on text you specify. To access this pane, choose **Monitoring > Logging > Real-Time Log Viewer > View**. 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 16, “Configuring Logging.”](#)

To view messages and information about them in 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 choose from the following options: Pause, Copy, Save, Clear, Color Settings, Create Rule, Show Rule, and Show Details.
 - Step 2** Click **Pause** to pause the scrolling of messages.
 - Step 3** Click **Copy** to copy a selected message.
 - Step 4** Click **Save** to save the contents of the log to a local file on your computer.

- Step 5** Click **Clear** to clear the list of messages.
- Step 6** Click **Color Settings** to specify that messages of different severity levels display in different colors.
- Step 7** Click **Create Rule** to create an access control rule that performs the opposite action of the access control rule that originally generated the message.
- Step 8** Click **Show Rule** to show the access control rule that caused the selected message to be generated. This feature applies only to syslog messages 106100 and 106023.
- Step 9** 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, source port, destination port, and a description of the message.
- Step 10** Click **Find** to enter the text you want to find in the messages. Searches the messages based on the text you enter.
- Step 11** Click **Help** to obtain more information.
- Step 12** Choose **Filter By** to enter text to filter the messages by. Press **Enter** or click **Filter** to apply the filter to the displayed messages.
- Step 13** 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 messages.
- Step 14** Click **Filter** to apply the filter to the message list.

Modes

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

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