



CHAPTER 41

Monitoring Logging

You can view real-time system log messages that appear in the log buffer. When you open the Cisco ASDM 6.0(2) for ASA 8.0(2) 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 15, “Configuring Logging.”](#)

About Log Viewing

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

- [Log Buffer, page 41-1](#)
- [Real-Time Log Viewer, page 41-3](#)

Log Buffer

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

Fields

- **Logging Level**—Lets you choose the level of logging messages to view, ranging from Emergency to Debugging.
- **View**—Opens a separate window in which log messages appear. From here 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 this 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 this pane, choose **Monitoring > Logging > Log Buffer > View**.

Right-click a message in the viewer to display a menu from which you can select from the Refresh, Copy, Save, Clear, Color Settings, Create Rule, Show Rule, and Show Details options. A list of icons associated with each severity level appears at the bottom of this pane. For more information about severity levels, see [Chapter 15, “Configuring Logging.”](#)

Fields

- Refresh—Refreshes the display.
- Copy—Copies a selected message.
- Save—Saves the contents of the log to your computer.
- Clear—Clears the list of messages.
- Color Settings—Enables you to specify that messages of different severity levels display in different colors.
- Create Rule—Enables you to create an access control rule that performs the opposite action of the access control rule that originally generated the message.
- Show Rule—Shows the access control rule that caused the selected message to be generated. This feature applies only to system log message IDs 106100 and 106023.
- Show Details—Shows or hides 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.
- Find—Lets you enter the text you want to find in the messages. Searches the messages based on the text you enter.
- Help—Provides more information.
- Filter By—Lets you enter text to filter the messages by. Press **Enter** or click **Filter** to apply the filter to the displayed messages.
- Show All—Displays all messages. Filters are removed from the display. This button is only active if a filter has been applied to the displayed log messages.
- Filter—Applies 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 this pane to view real-time system log messages in a separate window. To access this pane, choose **Monitoring > Logging > Real-Time Log Viewer**.

Fields

- **Logging Level**—Select the level of logging messages to view, ranging from Emergency to Debugging.
- **Buffer Limit**—Maximum number of log messages to view. The default is 1000.
- **View**—Opens a separate window in which log 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 this 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**.

Right-click a message in the viewer to display a menu from which you can select from the Refresh, Copy, Save, Clear, Color Settings, Create Rule, Show 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 15, “Configuring Logging.”](#)

Fields

- **Pause**—Pauses scrolling of the Real-time Log Viewer.
- **Copy**—Copies a selected message.
- **Save**—Saves the log to your computer.
- **Clear**—Clears the list of messages.
- **Color Settings**—Enables you to specify that messages of different severity levels display in different colors.
- **Create Rule**—Enables you to create an access control rule that performs the opposite action of the access control rule that originally generated the message.
- **Show Rule**—Shows the access control rule that caused the selected message to be generated. This feature applies only to system log message IDs 106100 and 106023.

- **Show Details**—Shows or hides 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.
- **Find**—Enter the text you want to find in the log. Searches the messages based on the text you enter.
- **Help**—Provides more information.
- **Filter By**—Lets you enter text to filter the messages by. Press **Enter** or click **Filter** to apply the filter to the displayed log messages.
- **Show All**—Displays all messages. Filters are removed from the display. This button is only active if a filter has been applied to the displayed log messages.
- **Filter**—Applies a filter to the displayed messages.

Modes

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

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