

Monitoring System Log Messages

Purpose Use the monitoring functionality to filter and view system log messages.

Action To view events in the J-Web interface, select **Monitor > Events and Alarms > View Events**.

Apply a filter or a combination of filters to view messages. You can use filters to display relevant events. Table 1 on page 1 describes the different filters, their functions, and the associated actions.

To view events in the CLI, enter the following command:

```
show log
```

Table 1: Filtering System Log Messages

Field	Function	Your Action
System Log File	<p>Specifies the name of a system log file for which you want to display the recorded events.</p> <p>Lists the names of all the system log files that you configure.</p> <p>By default, a log file, messages, is included in the <code>/var/log/</code> directory.</p>	<p>To specify events recorded in a particular file, select the system log filename from the list—for example, messages.</p>
Event ID	<p>Specifies the event ID for which you want to display the messages.</p> <p>Allows you to type part of the ID and completes the remainder automatically.</p> <p>An event ID, also known as a system log message code, uniquely identifies a system log message. It begins with a prefix that indicates the generating software process or library.</p>	<p>To specify events with a specific ID, type the partial or complete ID—for example, TFTPD_AF_ERR.</p>
Text in Event Description	<p>Specifies text from the description of events that you want to display.</p> <p>Allows you to use regular expressions to match text from the event description.</p> <p>NOTE: Regular expression matching is case-sensitive.</p>	<p>To specify events with a specific description, type a text string from the description with regular expression.</p> <p>For example, type ^Initial* to display all messages with lines beginning with the term <i>Initial</i>.</p>
Process	<p>Specifies the name of the process generating the events you want to display.</p> <p>To view all the processes running on your system, enter the CLI command show system processes.</p> <p>For more information about processes, see the <i>JUNOS Software Installation and Upgrade Guide</i> at www.juniper.net/techpubs</p>	<p>To specify events generated by a process, type the name of the process.</p> <p>For example, type mgd to list all messages generated by the management process.</p>

Table 1: Filtering System Log Messages (continued)

Field	Function	Your Action
Start Time End Time	Specifies the time period in which the events you want displayed are generated. Displays a calendar that allows you to select the year, month, day, and time. It also allows you to select the local time. By default, the messages generated in the last hour are displayed. End Time shows the current time and Start Time shows the time one hour before End Time.	To specify the time period: <ul style="list-style-type: none"> ■ Select the Start Time checkbox and select the year, month, date, and time—for example, 02/10/2007 11:32. ■ Select the End Time checkbox and select the year, month, date, and time—for example, 02/10/2007 3:32. To select the current time as the start time, select local time .
Number of Events to Display	Specifies the number of events to be displayed on the View Events page. By default, the View Events page displays 25 events.	To view a specified number of events, select the number from the list—for example, 50 .
OK	Applies the specified filter and displays the matching messages.	To apply the filter, click OK .

Meaning Table 2 on page 2 describes the Event Summary fields.



NOTE: By default, the View Events page in the J-Web interface displays the most recent 25 events, with severity levels highlighted in different colors. After you specify the filters, Event Summary displays the events matching the specified filters. Click **First**, **Next**, **Prev**, and **Last** links to navigate through messages.

Table 2: Viewing System Log Messages

Field	Function	Additional Information
Time	Displays the time at which the message was logged.	
Process	Displays the name and ID of the process that generated the system log message.	The information displayed in this field is different for messages generated on the local Routing Engine than for messages generated on another Routing Engine (on a system with two Routing Engines installed and operational). Messages from the other Routing Engine also include the identifiers re0 and re1 to identify the Routing Engine.

Table 2: Viewing System Log Messages (continued)

Field	Function	Additional Information
Event ID	<p>Displays a code that uniquely identifies the message.</p> <p>The prefix on each code identifies the message source, and the rest of the code indicates the specific event or error.</p> <p>Displays context-sensitive help that provides more information about the event:</p> <ul style="list-style-type: none"> ■ Help—Short description of the message. ■ Description—More detailed explanation of the message. ■ Type—Category to which the message belongs. ■ Severity—Level of severity. 	<p>The event ID begins with a prefix that indicates the generating software process.</p> <p>Some processes on a switching platform do not use codes. This field might be blank in a message generated from such a process.</p> <p>An Event can belong to one of the following Type categories:</p> <ul style="list-style-type: none"> ■ Error—Indicates an error or failure condition that might require corrective action. ■ Event—Indicates a condition or occurrence that does not generally require corrective action.
Event Description	<p>Displays a more detailed explanation of the message.</p>	
Severity	<p>Severity level of a message is indicated by different colors.</p> <ul style="list-style-type: none"> ■ Unknown—Gray—Indicates no severity level is specified. ■ Debug/Info/Notice—Green— Indicates conditions that are not errors but are of interest or might warrant special handling. ■ Warning—Yellow—Indicates conditions that warrant monitoring. ■ Error—Blue— Indicates standard error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels. ■ Critical—Pink—Indicates critical conditions, such as hard drive errors. ■ Alert—Orange—Indicates conditions that require immediate correction, such as a corrupted system database. ■ Emergency—Red—Indicates system panic or other conditions that cause the switching platform to stop functioning. 	<p>A severity level indicates how seriously the triggering event affects switch functions. When you configure a location for logging a facility, you also specify a severity level for the facility. Only messages from the facility that are rated at that level or higher are logged to the specified file.</p>

- Related Topics**
- Checking Active Alarms with the J-Web Interface
 - Understanding Alarm Types and Severity Levels on EX-series Switches

