EventLog Navigation

EventLog User interface

When EventLog module is selected main screen will show the following parts:

1. **Mode Panel** - choose between the Syslog and SNMP Trap mode.
2. **Main Panel** - displays results of SNMP request and MIB search operations.

For the purpose of this chapter, we will focus on the navigation in the Syslog mode.

Navigating in Syslog mode

To view syslog go to EventLog module and click Syslog tab. Here you can see syslog messages sent from different exporters for a chosen Time Window.

1. Show Options
2. EventLog Chart
3. Severity Table
4. Exporter Table
5. EventLog Table

Table and charts will show logs that have (1) the same severity as set in Severity Table (2) for the time set in Time Window. For these logs Exporter table will show distribution by exporters and Severity Table will show distribution by log's severity.

For example, on the screenshot to the left, you can see that logs that occurred during the selected Time Window and severity 0 to 5 are shown. You can also see that there was 523,918 such logs (Severity Table) of which most numerous were Warnings (55%) and Errors (29%).

You can also see the distribution of these logs by exporters in the Exporter table: exporter x.x.6.201 generated the most logs (139,130).

Show Options

Show Options:

1. Refresh Data – manually refresh data on charts and tables
2. Clear filters – clear all filters
3. Show Exporter Names – show names of exporters (routers) instead of their IP address

Syslog Chart

EventLog Chart shows distribution of syslog messages (logs) by severity:

1. Logs per bar (y-axis)
2. Time axis (x-axis)
3. Bar width
4. Zoom out

On this page:

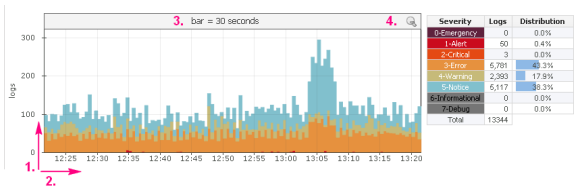


Chart shows number of logs in certain time chunks (1 minute, 1 day, 1 hour). Width of the chart bars and number of bars depends on the Time Window selected. See table below:

Time Window	Bar Width	Number of Bars
Last hour	30 seconds	120
Last 6 hours	5 minutes	72
Last 12 hours	5 minutes	144
Last day	15 minutes	96
Last week	1 hour	168
Last month	6 hours	120

Chart has two axis: numerical y-axis and time x-axis. Numerical axis shows the number of logs per bar. Time shown on the x-axis of the chart is the same time as set in the Time Window. Next to the Syslog Chart is the Severity Table in which you can select if syslog messages of the certain severity will be displayed on the chart or not. Colors on the chart correspond with the colors of the syslog Severity in the Severity Table.

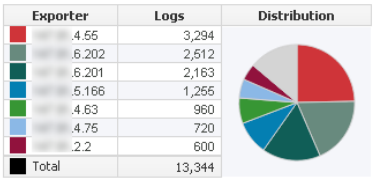
On the EventLog Chart above you can see that one bar on the chart represents logs during 30 seconds (bar = 30 seconds).

Severity Table

Severity Table shows log distribution by severity, for the logs of selected severity that occurred in the selected Time Window. On screenshot to the right currently selected severity levels are 0, 1, 2 and 3. This means that Syslog chart and tables will show only logs with this severity levels. By clicking on the corresponding severity in the Severity Table you can switch on/off logs of that severity. Switched off severity is shown with a gray background and logs with that severity are not shown on the carts and graphs.

Severity	Logs	Distribution
0-Emergency	0	0.0%
1-Alert	959	1.3%
2-Critical	39	0.1%
3-Error	71,679	98.6%
4-Warning	0	0.0%
5-Notice	0	0.0%
6-Informational	0	0.0%
7-Debug	0	0.0%
Total	72,677	

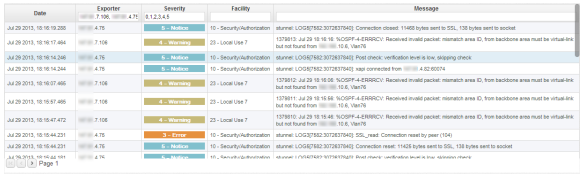
Exporter Table



Exporter Table shows log distribution by exporter, for the logs of selected severity that occurred in the selected Time Window. Top 7 exporters have a color assigned, while other exporters are grey and under Others on the pie chart. To see other exporters, scroll down the exporter list. Clicking on an exporter will show only logs for that exporter on the charts and table. By clicking on it again, you can switch back to seeing logs for all exporters.

Syslog Table

EventLog Table shows messages with selected severity (in Severity Table) that were received during time set in the Time Window. For each message Date, Exporter, Severity, Facility and Message content is displayed. Severity levels are shown with the corresponding color, as in the chart and Severity Table. 9/19 Figure 7: Exporter Table Figure 6: Severity Table Syslog Table can be filtered by Exporter, Severity, Facility and Message content. Note that the filters can be activated by selecting items in the Severity and Exporter Tables, as described above. To clear all filters, click the Clear button above the Syslog chart. To show exporter DNS names, click the Show Names button above the Syslog chart.



Continue reading about Inspecting Syslogs.