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.

	bar	= hour	Q	Severity	Logs	Distribution	Exporter	Logs	Distribution
5 k -				0-Emergency	0	0.0%	6.201	139,130	
				1-Alert	4,472	0.9%	.7.105	102,103	
		1		2-Offical	6,834	1.3%	.6.202	61,320	
K I				3-Error	154,264	29.4%	5.105	42,029	
				4-Warning	288,420	55.1%	1.00	30.210	
				5-100000	09,928	13.3%	7.110	19.674	
	M	All Latin India		e-priornational	0	0.0%	7.8	17,118	
		Mar		7-Debug	0	0.0%	4.63	16.619	
and the second second	ALC: NOT THE REAL PROPERTY OF	Barry and the second se	and the second	Total	523,918		Total	523,918	
30/03. 31/03. 02:00 02:00	01/04, 02/04, 03/64, 02:00 02:00 02:00	04/04, 05/04, 06/04, 02:00 02:00 02:00	07/04, 08/04, 09/04, 02:00 02:00 02:00						
Data	Exporter	Severity	Facility	Message					
Unite		0, 1, 2, 3, 4, 5							
				307848 Oct 10 21 01 05 MORPELEBBROV Banaked invalid narket mismatch area ID from harkh			D. from backbone are		
r 09 2015, 21:01:06.426	10.0.7.106	4 - Warning	23 - Local Use 7 must be virtual-link but not found from 10.6, Vian76						
09 2015, 21:01:02 232	10.0.4.63	5 - Notice	10 - Security/Authorization	stunnel: LOO5(8910.3070999440). Connection closed: 11820 bytes sent to SSL, 138 bytes sent to socket					
r 09 2015, 21:01:01.404	10.0.3.11	5 - Notice	9 - Clock Daemon	Oct 10 21:01:01 syslog run-partsiletokron.hourly/(1096 finished Ganacron					
r 09 2015, 21:01:01:398	10.0.3.11	5 - Notice	9 - Clock Daemon	Oct 10 21:01:01 syslog run-parts(Wtolcron.hourly)(1055 starting Danacron					
00 2015 21 00 50 272	10.0.0.201	3.5000	E - Surject Internal	Regional Internal cisco5500-L: "dot1xMsgTask: Oct 10 21:00:59.966: %DOT1X-3-MA		EAP_RETRIES: 1>	auth_pae.c:3136 M		
100 2010, 21.00 30 21 5	10.00.201	2 Child	5.0) #000 million	EAP identity request retries (3) exceeded for client :42.3a					
109 2015, 21:00:57:163	10.0.4.63	5 - Notice	10 - Security/Authorization	stunnel: LOG5[5910.3070999440]; xapi connected from 4.47/51068					
09 2015, 21:00:56.426	10.0.7.106	4 - Warning	23 - Local Use 7	397845: Oct 10 21 must be virtual-lini	but not four	%C6PF-6-ERRRCV: Received invalid packet mismatch area ID, from ba tound from 10.6, Vian76			O, from backbone are
r 09 2015, 21 00 55 069	10.0.6.201	3 - Error	5 - Svalood-Internal	cisco5506-L: "Dottx_NW_MsgTask_6: Oct 10 21:02:56:760: %DOT1X-3-MAX_EAP_RETRIES			RES.		
				11_3081_208.2.31	90 Max EAP	identity request rea	ies (3) exceeded to	If Coeffi	50.00
r 09 2015, 21:00:47:638	10.0.7.8	4 - Warning	23 - Local Use 7	130650: 12w5d % GloabitEthernet3.0	3d:%CDP-4-NATIVE_VLAN_MSWATCH: Native VLAN mismatch discovered on rel0/2 (223), with LjuficeBogdana_1 GigabilEthemet0/24 (1).			no be	
09 2015, 21:00:47.003	10.0.0.127	4 - Warning	3 - System Daemons	Oct 10 21:00:47 rp Local version: 2 R	(pd)47243 RPD_MLD_ROUTER_VERSION_MISMATCH: MLD version mismatch on g Remote version: 3			nismatch on ge-1/0/0.	
09 2015, 21:00 46.427	10.0.7.106	4 - Warning	23 - Local Use 7	397844: Oct 10 21 must be virtual-link	844: Oct 10 21 50:45: %OBPF-4-ERRRCV: Received invalid packet mismatch area ID, from backt the virtual-link but not found from 10.6: Vtan76			D, from backborne are	
				cisco5508-L: "dottixMagTask: Oct 10 21:00:42:768: %DOTTX-3-MAX_EAP_RETRIES: 1x_auth_pag.c.3 EAR blanch: researcheding: Operanded for class: 55:05			auth_pae.c:3136 M		
r 09 2015, 21:00:41:075	10.0.6.201	3 - 11107	5 - bysiogo-internal	EAP identity reque	at retries (3)		56.05		

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:

- Refresh Data manually refresh data on charts and tables
 Clear filters – clear all filters
- 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:

- Show Options
- Syslog Chart
- Severity Table
- Exporter Table
- Syslog Table



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		Logs	Distribution	
.4	.66	3,294		
.6	.202	2,512		
.6	.201	2,163		
.5	.166	1,255		
.4	.63	960		
.4	.76	720		
.2	.2	600		
Total		13.344		

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.

Date	Exporter .7.108	Severity 0.12,34.5	Facility	Message
Jul 29 2013, 18:16:19.268	4.75	5 - Notice	10 - Security/Authorization	sturnet LOG8(7582.3072637540) Connection closed: 11465 bytes sent to 55L, 135 bytes sent to socket
Jul 29 2013, 18:16:17.494	7.106	4 - Warning	23 - Local Use 7	1379913: Jul 29 10 16 16: %CSPF-4-ERRRCV. Received invalid packet: mismatch area ID, from backdone area must be virtual-link but not found from 10.6, Van76
Jul 29 2013, 18:16:14:246	4.75	5 - Notice	10 - Security/Authorization	stunnet: LOG6(7582:3072837640) Post check: verification level is low, skipping check:
Jul 29 2013, 18:16:14:244	4.75	5 - Notice	10 - Security/Authorization	sturnet: LOG6(7582.3072837840) xapi connected from 4.82.60074
Jul 29 2013, 10:16:07.466	7.106	4 - Warning	23 - Local Use 7	1378912: Jul 29 15 16 06: %CSPF-4-ERRRCV. Received invalid packet: mismatch area ID, from backdone area must be virtual-link but not found from
Jul 29 2013, 18 16:57.466	7.108	4 - Warning	23 - Local Use 7	13798111 Jul 29 19 15 56: %COPF-4-ERRRCV. Received invalid packet: mismatch area ID, from backdone area must be virtual-link but not found from 10.6, Van78
Jul 29 2013, 18:16:47.472	7.106	4 - Warning	23 - Local Use 7	1578910. Jul 29 18 15 48. %COSPF-4-ERRIPICV. Received invalid pecket: mismatch area ID, from backbone area must be virtual-link but not found from
Jul 29 2013, 18:15:44.231	4.75	3 - Error	10 - Security/Authorization	sturnet LOG3(7552.3072637540) SSL_read. Connection reset by peer (154)
Jul 29 2013, 10:16:44.231	4.75	5 - Notice	10 - Security/Authorization	stunnel: LOG6(7502:3072637040) Connection reset: 11425 bytes sent to SSL, 138 bytes sent to socket
Page 1	4.76	5 - Matice	10, Renark (Scholaston	stannel 1/0587582 3029832888 Post rises' verification level is low stansion rises'