

Initial EventLog Configuration

After configuring your devices and installing NetVizura EventLog you should verify that:

1. Devices are exporting syslog and trap messages to the same port that NetVizura EventLog is listening to.
2. Messages are passing the network firewall and reaching the NetVizura Server
3. NetVizura Server Ports to which syslog and trap messages are sent is open

The screenshot shows the NetVizura EventLog Configuration interface. On the left, there is a sidebar with 'Settings' and 'Control Panel'. Under 'Settings', 'Modules' are listed: 'NetFlow Settings', 'MIB Settings', and 'EventLog Settings'. The 'EventLog Settings' is selected. The main area has tabs for 'Syslog filtering', 'SNMP Trap filtering', 'Alarms', and 'Configuration'. The 'Configuration' tab is active, showing 'Service options'. Under 'Service options', there are four fields: 'Syslog socket port' (33514), 'Syslog port number listening for Syslog data' (33514), 'Trap socket port' (33162), and 'Trap port number listening for SNMP Trap data' (33162). Below these is a 'Maximal severity level shown' dropdown menu set to '3 - Error'.

By default, syslog messages are exported from the devices to port 514, while NetVizura listens on the port 33514 in Linux systems and on the port 514 in Windows systems. If you use Linux systems, you need to (1) redirect syslog messages to the 33514 on NetVizura server, (2) export syslog messages to 33514 from device, or (3) change NetVizura EventLog configuration. Same applies to trap socket port.



On Linux systems ports lower than 1024 can not be used by application, unless the root privileges are given to NetVizura EventLog.

To change NetVizura EventLog configuration go to **Settings > EventLog Settings > Configuration** and under **Service options** change the **Socket port** values.