Using EventLog Alarms

On this page:

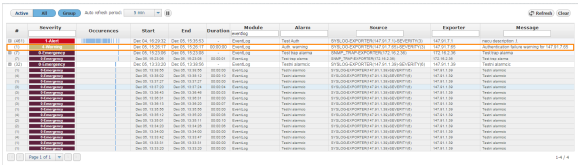
You can setup alarms to trigger if a specific condition is met on a syslog or trap message:

- For Syslogs, threshold is based on source IP, severity, facility and message content
- For SNMP traps, threshold is based on source IP, OID and variable bindings.
  It is possible to combine more threshold criteria (AND logical operand is implied).

Each alarm has its severity and you can override the severity of the syslog alarm. This is useful if the default severity of a syslog does not correspond to alarm severity. For example, a fan is malfunctioning in the data center. Usually, syslog for this event will have a severity warning, but in this case data center is critical so it is wise to set the alarm severity higher.

Viewing All Alarms (Alarm Module)

To view all EventLog alarms, go to **Alarm** Module.



Here you can see the list off all alarms that occurred within the selected time period. In our case, we can see Auth. warning alarm that we previously defined in Settings.

Occurrence indicators visualize approximate time (withing selected time window) when alarm occurred.

You are also able to filter, sort alarms and view only active alarms according to your need.

Creating EventLog Alarms

To add a new alarm in EventLog:

1. Click **Add**
2. Set **Alarm information** (type, name, description and level)
3. Set **Alarm threshold**
   For Syslogs, threshold is based on source IP, severity, facility and message content
   For SNMP traps, threshold is based on source IP, OID and variable bindings.
   It is possible to combine more threshold criteria (AND logical operand is implied).

If you do not define a value to a certain criterion, that criterion will not be included in the Alarm condition.

? Unknown Attachment

Screenshot above shows an example of an Alarm confguration. This alarms will trigger if syslog message is sent from 147.91.7.65, with severity level 3 and message containing Authentication failure.