Alarm Settings (ELA)

Adding new alarm

On this page:

All EventLog users can view alarms, however only users with write privileges can add, edit or delete them.

To set EventLog alarms, go to blocked URL **> Settings > EventLog Settings > Alarms.**

To add a new alarm in EventLog:

1. Click **Add**
2. Set **Alarm information**
3. Set **Alarm condition**

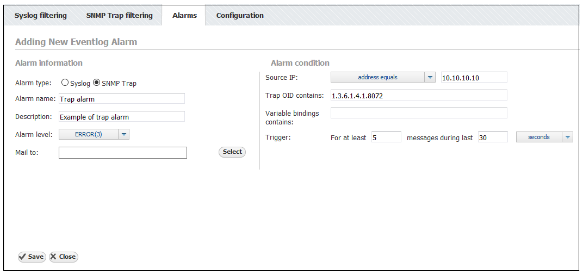
There are two types of alarms:

1. **Syslog alarm** - alarm activated with syslog messages
2. **SNMP Trap alarm** - alarm activated with SNMP trap messages

Common settings for both types of alarm are name, description and alarm level. For Syslogs, condition is based on source IP, severity, facility and message content. For SNMP traps, condition is based on source IP, SNMP Trap OID and variable bindings.

Both types of alarm have additional settings for triggering condition. You can create alarm condition based on number of messages in unit of time - **group alarm** (alarm will be triggered and displayed only if all conditions are met more than defined number of times in specified time frame).

It is possible to combine more condition criteria. If you do not define a value to a certain criterion, that criterion will not be included in the Alarm condition.



Adding New Eventlog Alarm

Alarm information

Alarm type: ○ Syslog ● SNMP Trap

Alarm name: Trap alarm

Description: Example of trap alarm

Alarm level: ERROR(3)

Mail to:

Alarm condition

Source IP: address equals 10.10.10.10

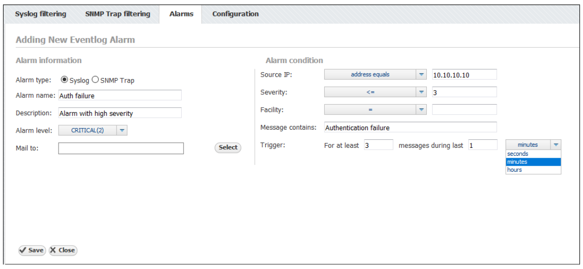
Trap OID contains: 1.3.6.1.4.1.8072

Variable bindings contains:

Trigger: For at least 5 messages during last 30 seconds

Screenshot above shows an example of an Alarm configuration. This Error level alarm will trigger if SNMP Trap message is sent from 10.10.10.10, with Trap OID 1.3.6.1.4.1.8072.

In following example, Critical alarm will trigger if 3 or more Syslog message is sent form exporter 10.10.10.10 in one minute. This messages need to have severity from 0 to 3 and need to have "Authentication failure" in text of message also.



Adding New Eventlog Alarm

Alarm information

Alarm type: ● Syslog ○ SNMP Trap

Alarm name: Auth failure

Description: Alarm with high severity

Alarm level: CRITICAL(2)

Mail to:

Alarm condition

Source IP: address equals 10.10.10.10

Severity: <= 3

Facility: =

Message contains: Authentication failure

Trigger: For at least 3 messages during last 1 minutes

You can also define mail notification. Selected users will receive two mails, one when alarm is activated and second one when alarm is deactivated.

Alarm Examples

Type	Alarm name	Description	
Networking	Link is down	Interface changed state to down	See these alarms in action at our Live Demo.
Networking	BGP peer drop	BGP peer has reset the connections	
System	Failed password	Failed password	
System /Security	Auth failure	Unauthorized access attempt on a vital server	

Security	Severity = Alert	Received syslog with Severity 1	

Read more about Event Alarms.