THE POWER OF BUILDING AND
MANAGING NETWORKS

Operations

Contents

1 Introduction

The operation of a network management system requires a number of functions to support the network administrators. This involves SNMP trap or syslog processing as much as an intelligent event correlation.

One example to illustrate this: A component on a WAN router with 20 connected circuits fails. In this scenario, systems without event correlation would report the component's failure plus 20 circuit faults (and the same again once operations resume. ERAMON would only report the failure of that particular component in such an event. The window showing the reported network statuses would thus remain clear and uncluttered. It is however possible that the affected components are also displayed. These kinds of functions are particularly helpful in more complex network structures.

Integral components in the operations module are, among others:

2 ERAMON Event Processing (EEP)

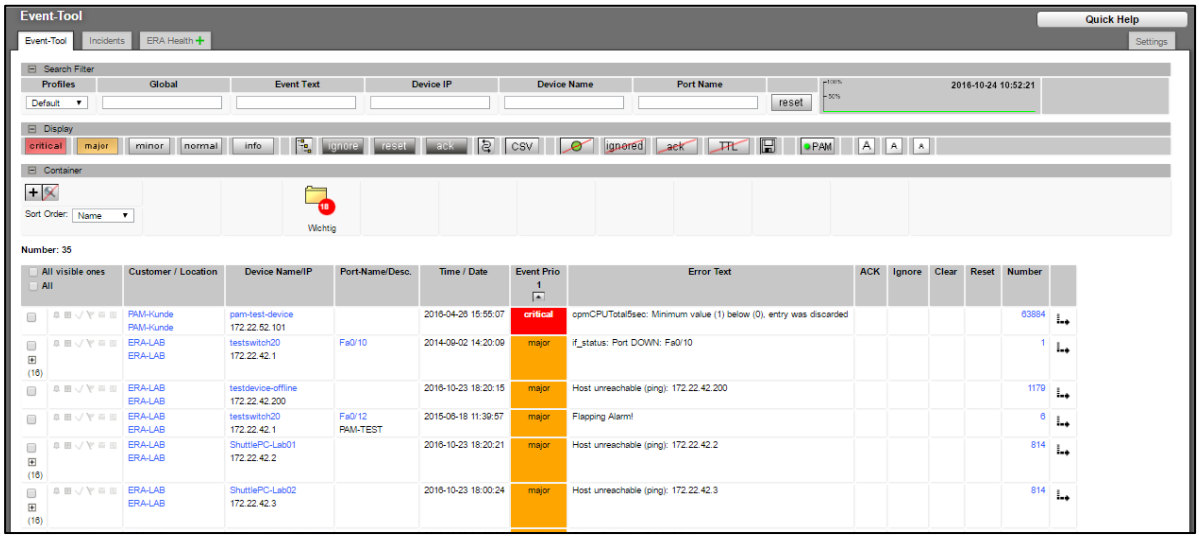
The central event recipients are the SATs, which contain the necessary capabilities to receive these events. They will then send the relevant alerts to the CENTER, from where all events are processed and prepared so they can be viewed.

ERAMON distinguishes between the following event types, according to the type or the event to be announced:

- SNMP traps
- SNMP port status
- IP polling
- Syslog
- Program messages
- Ping groups
- EPM
- ERA Health

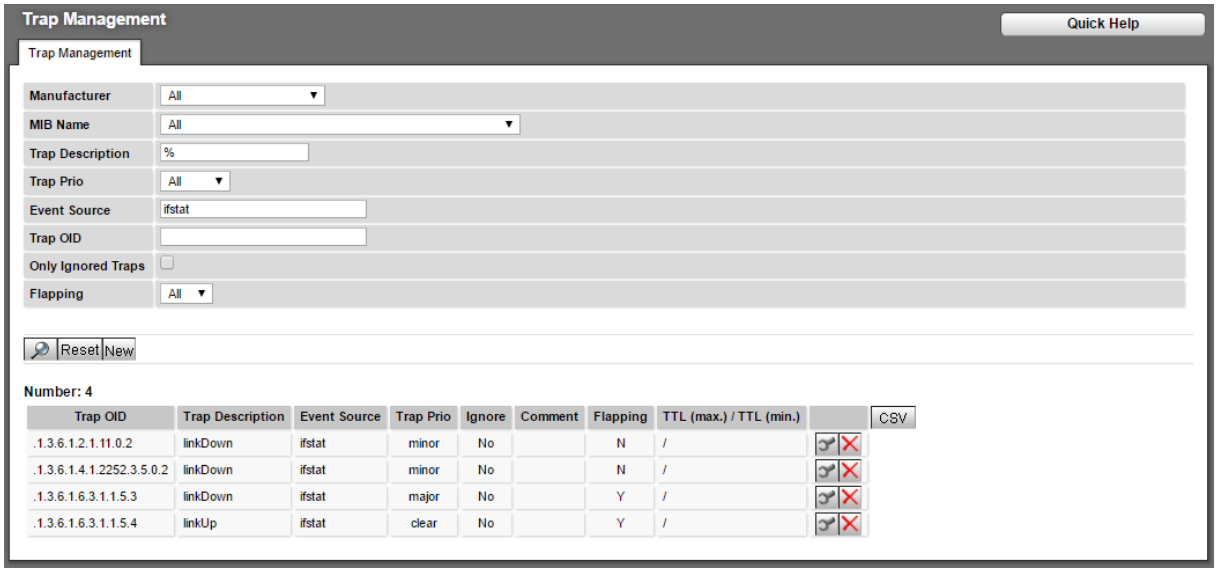
2.1 Event-Tool

The messages are displayed in more detail in the event tool.

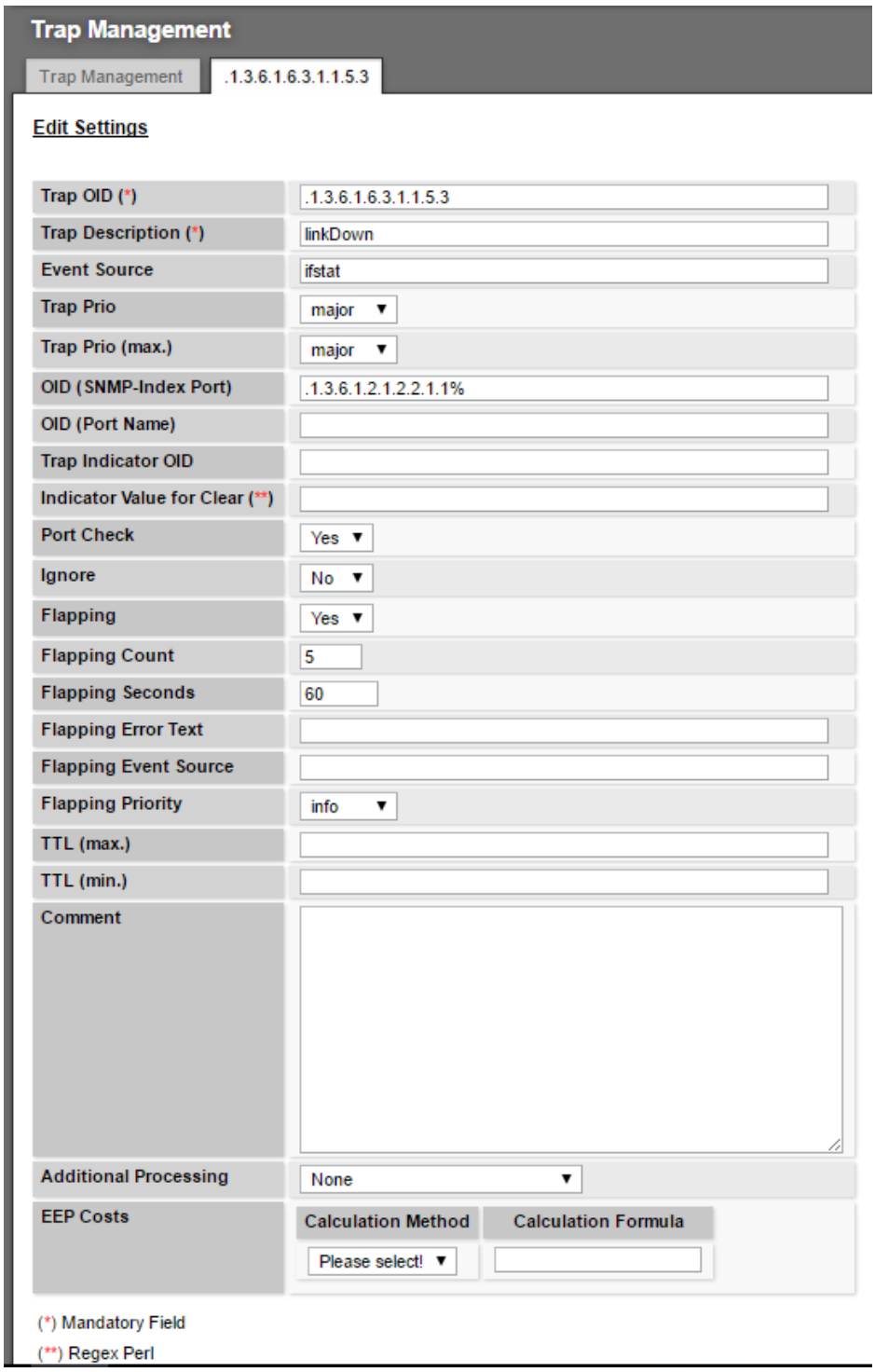


2.2 Traps

Traps are received via these ERAMON SATs. They are stored in ERAMON within the trap settings. It is here where all traps already specified and delivered with ERAMON are listed and categorized; while ERAMON is completely independent of any manufacturer.

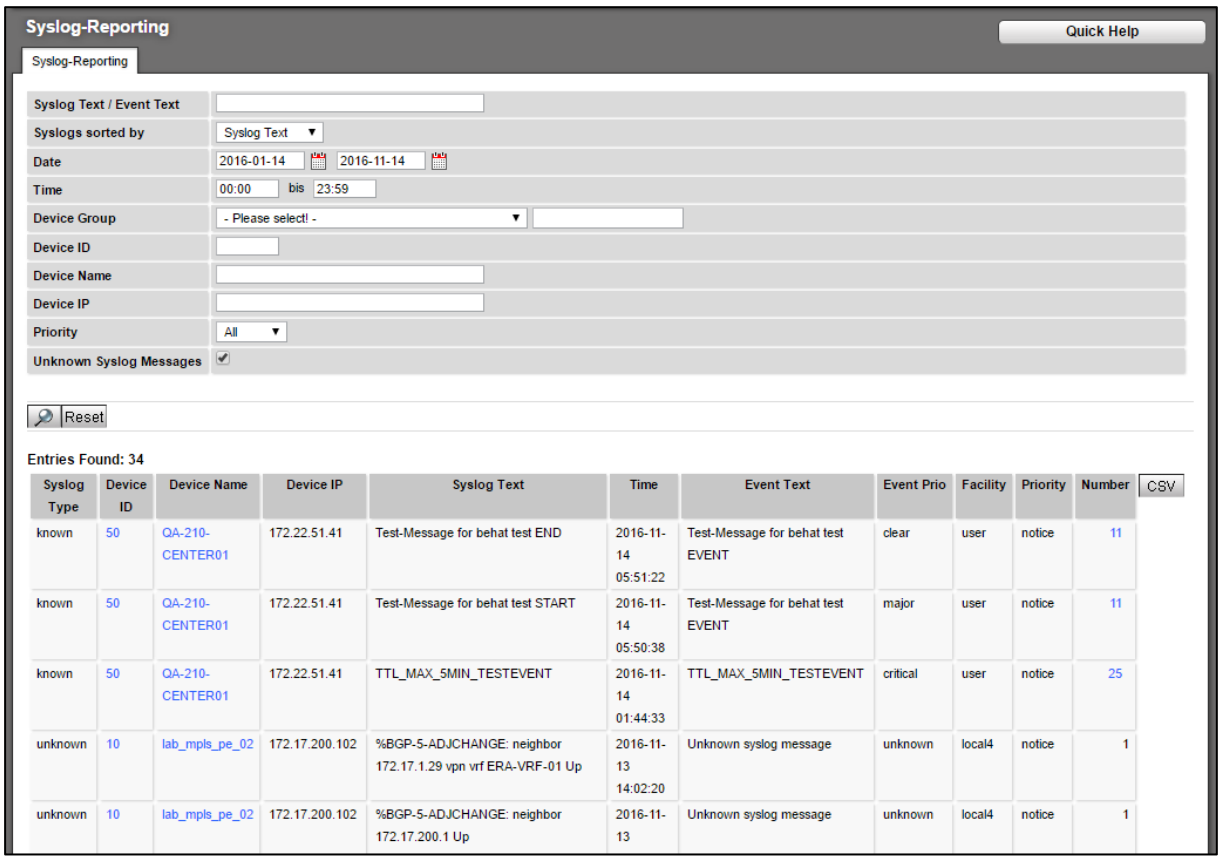


The following screenshot shows the different setting options for traps:



2.3 Syslog

Syslog messages are received by ERAMON's SATs and then transmitted to the CENTER. Only known syslogs are listed and processed (entry in syslog management) in the event tool.



Syslog Type	Device ID	Device Name	Device IP	Syslog Text	Time	Event Text	Event Prio	Facility	Priority	Number
known	50	QA-210-CENTER01	172.22.51.41	Test-Message for behat test END	2016-11-14 05:51:22	Test-Message for behat test EVENT	clear	user	notice	11
known	50	QA-210-CENTER01	172.22.51.41	Test-Message for behat test START	2016-11-14 05:50:38	Test-Message for behat test EVENT	major	user	notice	11
known	50	QA-210-CENTER01	172.22.51.41	TTL_MAX_5MIN_TESTEVENT	2016-11-14 01:44:33	TTL_MAX_5MIN_TESTEVENT	critical	user	notice	25
unknown	10	lab_mpls_pe_02	172.17.200.102	%BGP-5-ADJCHANGE: neighbor 172.17.1.29 vpn vrf ERA-VRF-01 Up	2016-11-13 14:02:20	Unknown syslog message	unknown	local4	notice	1
unknown	10	lab_mpls_pe_02	172.17.200.102	%BGP-5-ADJCHANGE: neighbor 172.17.200.1 Up	2016-11-13	Unknown syslog message	unknown	local4	notice	1

For this purpose regular expressions can be set up and the event priorities can be specified in the syslog management. Syslogs with the same event source are correlated. Messages that are not included will be listed in "Unknown Syslog Messages". Syslogs of devices not registered with ERAMON will be listed in "Unknown Host IP".

2.4 Correlation

2.4.1 Standard Correlation

Within ERAMON we understand correlation as a pooling of related events in the event tool. Their relationship was established – and at times assessed – through various methods (RCA).

The advantages are varied:

- Improved clarity through pooling
- Relationships are made immediately evident
- Targeted announcements
- Simplified error analysis

It is also possible to adjust the correlation to individual requirements. You yourself can decide which events are to be correlated and which priority each event should be given.

2.4.1.1 Normal

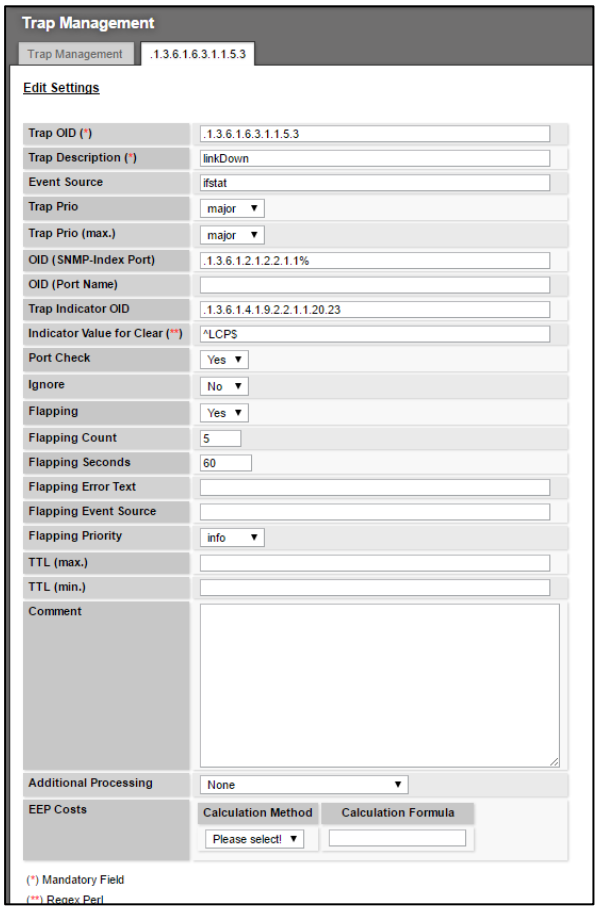
This correlation is applied when an event occurs several times over. Where an event would be generated in the event tool at its first occurrence, this would no longer occur for subsequent identical events. In this case the number of how often that particular event occurred would simply be increased accordingly.

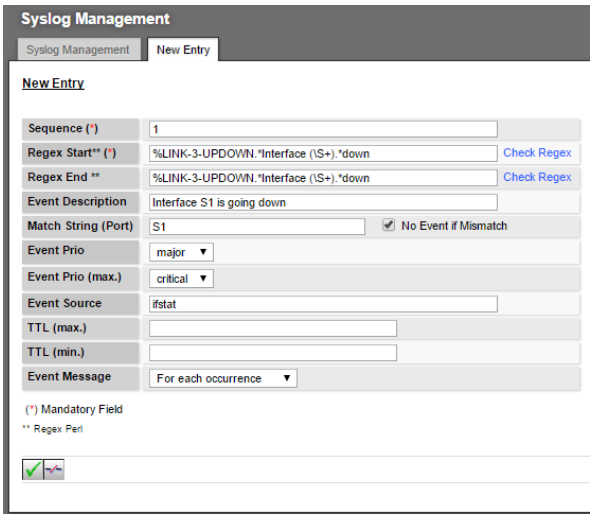
The following three criteria are crucial for the correlation:

- Device ID
- Port ID
- Event Source

You can adjust the event source in a number of places in ERAMON, for example in the trap settings or syslog management menu. Allowing you to freely decide on which of the various events should be correlated.

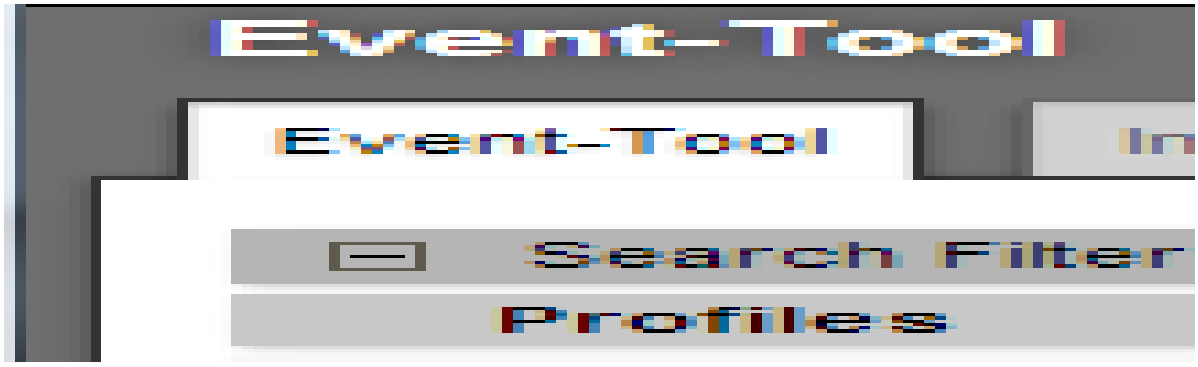
Below is an example of the configuration of a LinkDown as a syslog and trap.





The event source: "interfaceAlarmLinkDown" is used for both entries, which correlates the trap and syslog messages.

The corresponding event would look as follows:



It is now possible to clear such an event (consisting of a trap and syslog message) with one single "Clear" message.

2.4.1.2 Subinterfaces

Since physical ports can also have logical ones, which would obviously also be affected should the physical one fail, it is only sensible to correlate these events. The events of the subinterfaces are therefore correlated with the events of the physical ports.

2.4.2 Expanded Correlation

2.4.2.1 Transfer Points

Once ERAMON has recognized a remote station via a transfer point (/30), the relevant events are correlated with the ones of the remote station.

2.4.2.2 Port Channels

This correlation represents an expansion of the transfer point correlation. A port channel consists of two or more physical ports as well as a logical (virtual) channel port. If one individual physical port goes down, this behavior would be equivalent to the normal correlation. If, however, the second physical port then goes down (and thus the virtual tunnel), this would result in all events being correlated. In this event, the root event would be the failure of the channel port.

In addition to this, the transfer network correlation correlates all events of the remote stations – physical as well as logical interfaces.

2.4.2.3 BGP and OSPF Neighborhoods

Here, the corresponding port is identified from the original source event (e.g. "BGP Session Down"). A failure is then generated for this one and the events from the remote station correlated to it.

2.4.3 Correlation via the Network Topology

Within ERAMON this correlation is defined as a collation of events based on very diverse connection data (CDP, L3, …).

As soon as an entire device goes down, the system checks if remote stations went down as well – so, an entire device or one or several ports; if that is the case, these events are then correlated.

If, for example, a core switch goes down and the connection to the entire network behind this breaks down, you would want to know if the reason for the network failure is the core switch. The events of the failed network component would then be correlated within the events of the core switch.

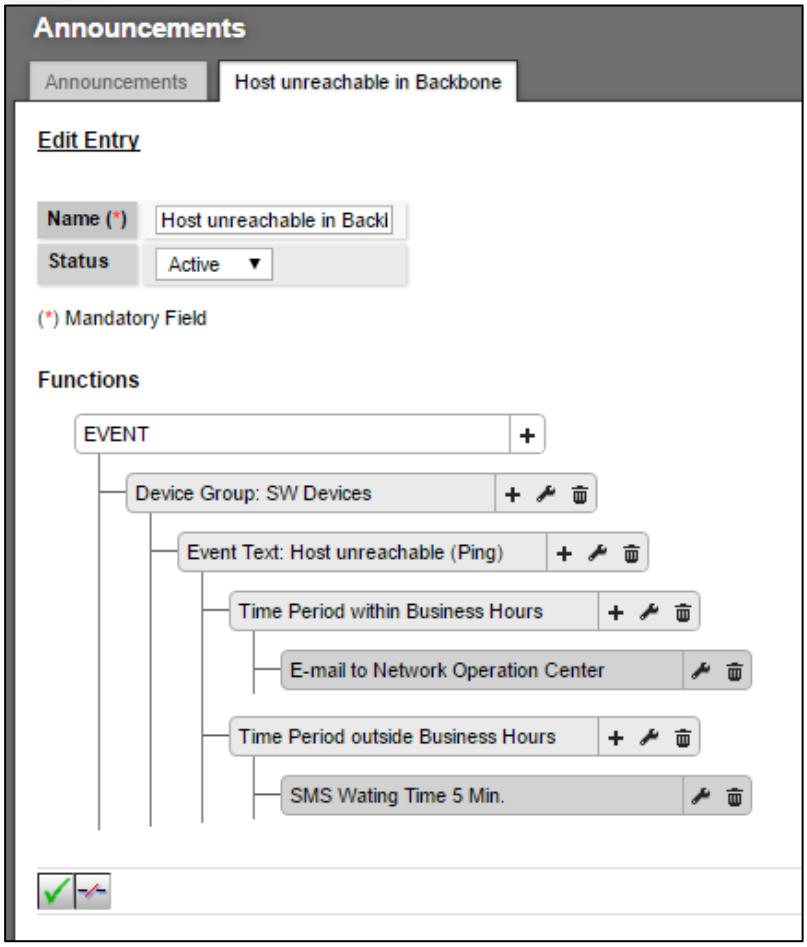
Another example would be the failure of an individual port and as a result of this, a failure of the devices connected to it. Since the connected devices are not the cause of this, they are only of secondary relevance; the failure of the port would therefore be considered the root/cause event and all remaining events correlated to it.

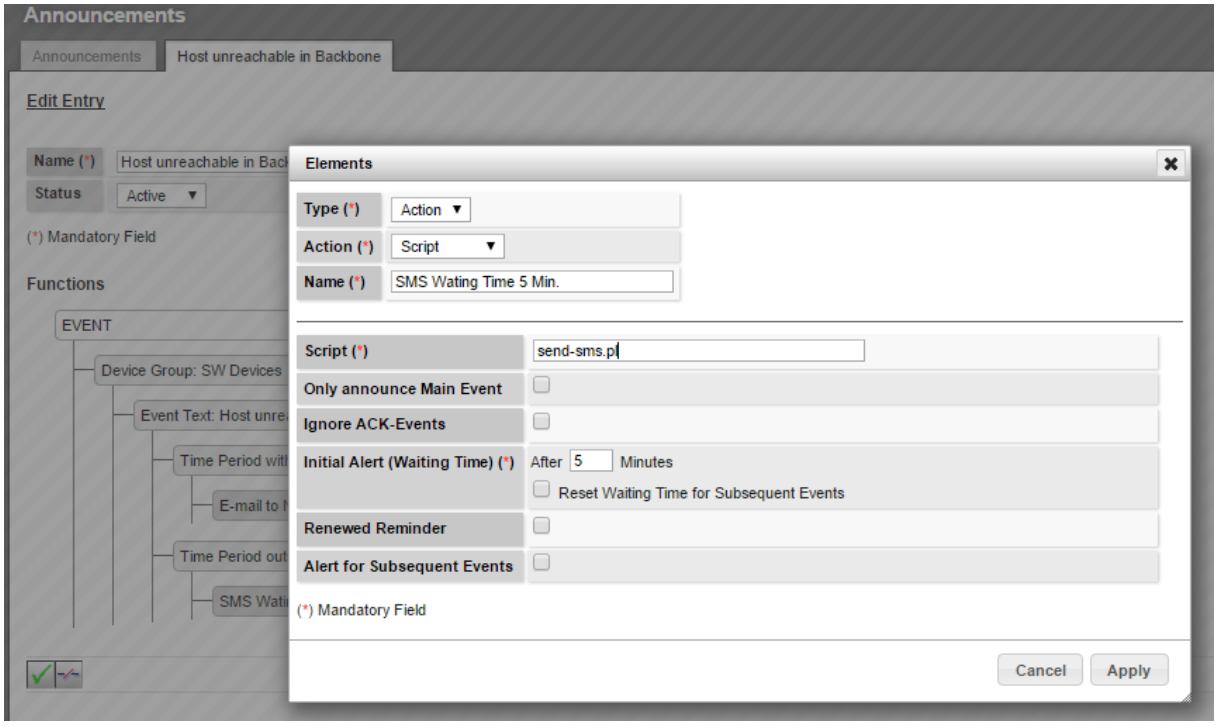
2.5 Announcements

Announcements enable automatic actions for the announcement of certain events in ERAMON to be set up.

The announcement settings contain specifications when, based on an event, which action should be performed. A wide range of parameters are available for this:

- Filter
  - Event Text, Event Priority
  - Device/Port/Location Groups
  - Customers, Locations, Queues
  - Time Period
- Action — The action to be carried out
  - E-mail — The address is in the next field, several recipients are separated by a semi-colon.
  - Bulk E-Mail — Announcements are collected until they are sent in one batch by e-mail.
  - Script — A script is carried out.
  - Trap — A trap is sent.
  - Syslog — A syslog message is sent.
  - PAM — Proactive Management


Announcements
Announcements
Host unreachable in Backbone
Edit Entry
Name (*)
Host unreachable in Backl
Status
Active
(*) Mandatory Field
Functions
EVENT
Device Group: SW Devices
Event Text: Host unreachable (Ping)
Time Period within Business Hours
E-mail to Network Operation Center
Time Period outside Business Hours
SMS Wating Time 5 Min.


Announcements
Announcements
Host unreachable in Backbone
Edit Entry
Name (*)
Host unreachable in Bac
Status
Active
(*) Mandatory Field
Functions
EVENT
Device Group: SW Devices
Event Text: Host unre
Time Period with
E-mail to
Time Period out
SMS Wati
Elements
Type (*)
Action
Action (*)
Script
Name (*)
SMS Wating Time 5 Min.
Script (*)
send-sms.pl
Only announce Main Event
Ignore ACK-Events
Initial Alert (Waiting Time) (*)
After
5
Minutes
Reset Waiting Time for Subsequent Events
Renewed Reminder
Alert for Subsequent Events
(*) Mandatory Field
Cancel
Apply

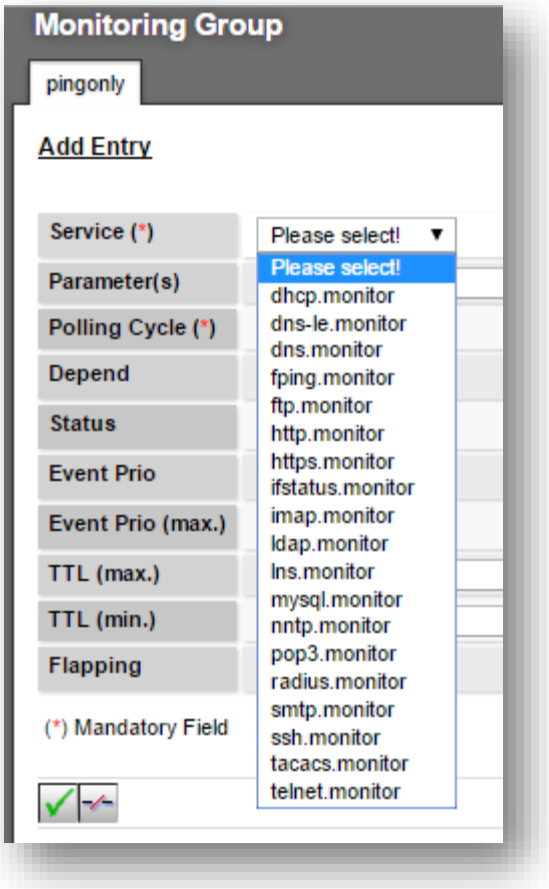
3 More Functions

ERAMON's Operations has a number of other functions available. Some of them are listed below:

- Shift Planning
- Scheduled Maintenance Tasks

  Scheduled maintenance tasks can be set up, which can then also be included in any subsequent SLA calculation. The alerted events during this time period are automatically assigned to the maintenance and are not actively announced.

- IP-based availability polling
- IP Services Monitoring

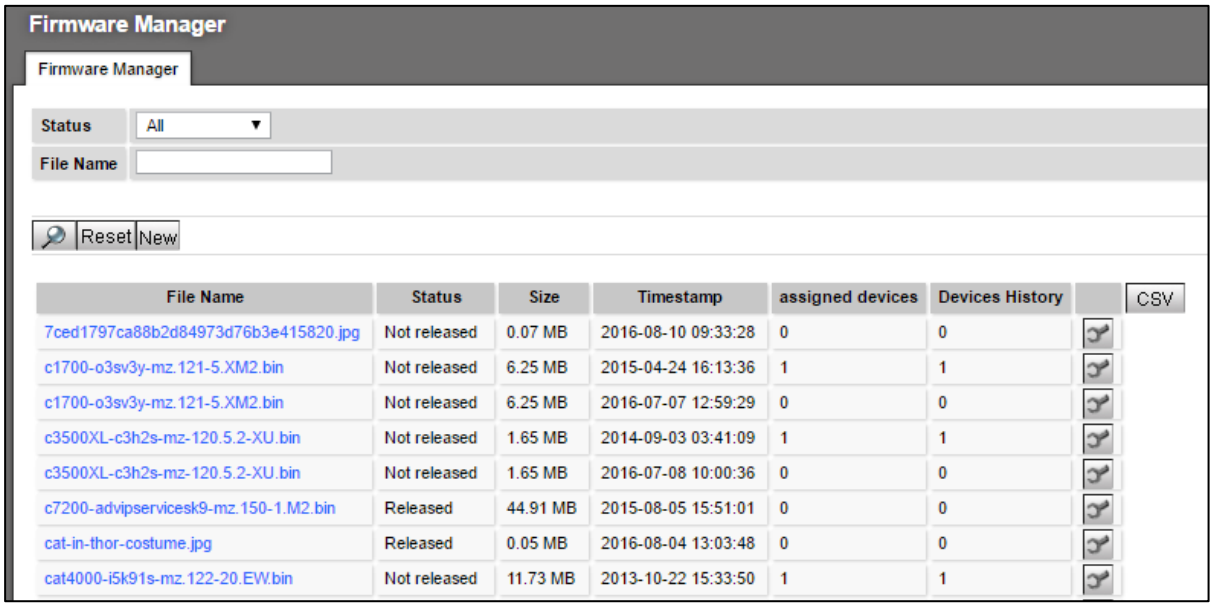


- Polling Scripts

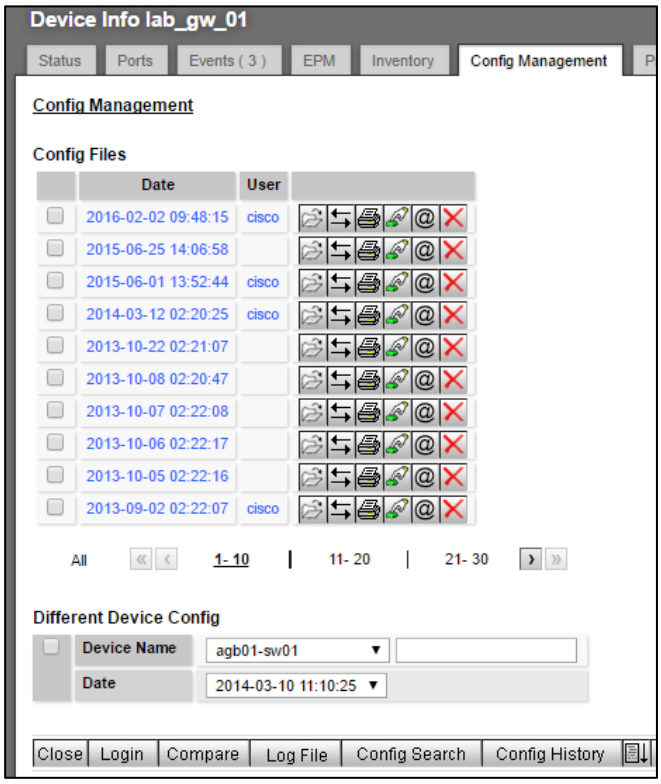
  Enables you to save any number of PERL scripts, which could, for example, be used to carry out specific pollings on a device – and then issue the corresponding output value.

- Route Table Trace
- One-Click Login with multi-layered user permissions and automatic logins onto devices

- Firmware management and Firmware upgrade tool



- Administration of router and switch configurations



-

® ERAMON is the registered trademark of ERAMON GmbH.