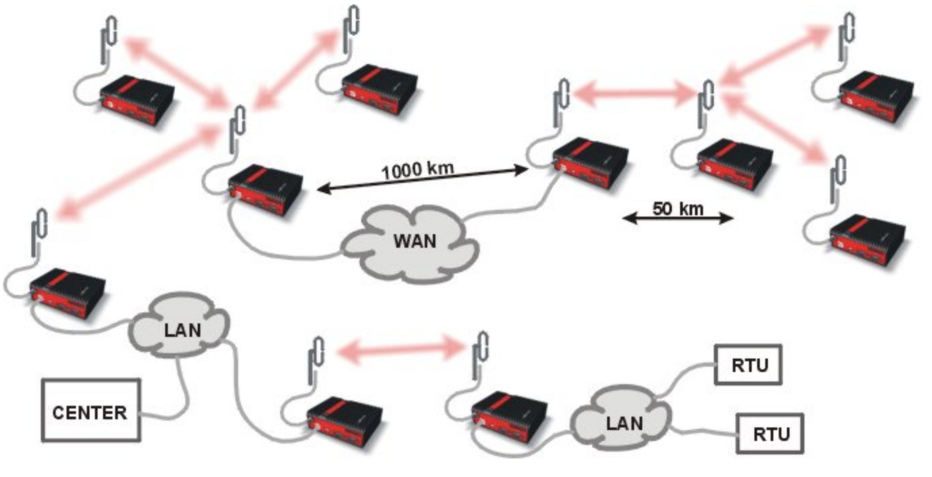
RADIO DATA NETWORKS

Application notes



RipEX2, M!DGE3
SNMP

version 1.0
2023-12-11

RACOM s.r.o. | Mirova 1283 | 592 31 Nove Mesto na Morave | Czech Republic
Tel.: +420 722 937 522 | E-mail: racom@racom.eu

www.racom.eu

Table of Contents

Shared RipEX2 and M!DGE3 SNMP

Important

RipEX2 and M!DGE3 share the same "RA2" MIB and the complete operation is the same for both products. Keep in mind the whole application note is written for RipEX2, but applies to M!DGE3 as well. If there is anything particular for M!DGE3, it is noted appropriately. E.g., there is no "Radio" interface in M!DGE3 and corresponding OID values are not readable/supported.

1. Introduction - Simple Network Management Protocol

SNMP is a simple, widely used and useful standardised protocol typically used by Network Management Software (NMS) to read values from devices. Values can be obtained at regular intervals or on requests, saved to a database and then displayed as graphs or tables.

SNMP also enables devices to generate (trigger) the alarms by themselves and notify the NMS explicitly (SNMP traps/informs).

1.1. How does SNMP work?

SNMP requires two parties for communication:

1. *SNMP “manager”* (software installed at your computer)
   - You can use commercial software or free software such as Zabbix, Zenoss, Nagios, Cacti, etc. If you want to read values manually, you can use tools such as snmpwalk, snmpget or Mibbrowser software.
2. *SNMP “agent”* (a part of firmware in remote devices such as RipEX)
   - The agent receives SNMP requests to query information and responds to the manager. Several managers may read values at once and they can send their requests at any time. Alternatively, the agent sends SNMP traps/informs whenever the monitored values are outside the threshold range (RipEX2 events). RipEX is capable of sending SNMP traps/informs to up to multiple SNMP managers.

1.2. SNMP communication

In SNMP, each value is uniquely identified using Object Identifier (OID).

The standard SNMPv1/v2c communication starts by sending a request and then the response is returned. Alternatively, an agent can send an SNMP trap or inform.

SNMPv3 shall be used if the higher security of the monitoring traffic is required. SNMPv3 provides security with authentication and Encryption. The manager is required to know an authentication, encryption methods and common secrets to authenticate itself and decrypt SNMP packets.

A **request** is sent
the manager sets message-type to GET, includes OID for the required value and sets this value to NULL.

A **response** is returned
the agent sets message-type to RESPONSE and sends the requested value along with its OID back to the manager.

A **trap** is sent
to the manager without its request.

An **inform** is sent
to the manager without its request and the manager acknowledges its successful delivery.

1.2.1. Basic Message Types

GetRequest
returns a single value.

GetNextRequest returns the next value (using the next OID).

GetBulkRequest returns several values in a single packet (useful for data bandwidth optimization)

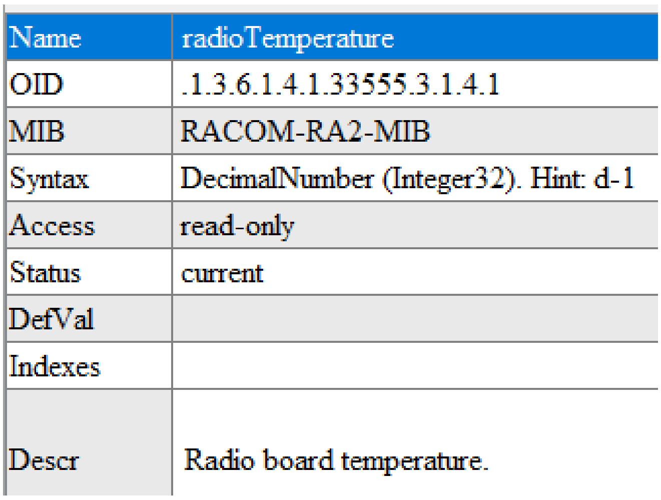
Trap/Inform sent from the agent to the manager whenever any monitored value is beyond its thresholds.

SetRequest used to set various parameters (unsupported by RipEX2).

1.3. MIB database – Management Information Base

The MIB is a virtual database used for managing the entities in a communications network. The MIB hierarchy can be depicted as a tree with a nameless root, the levels of which are assigned by different organizations. “Higher-level” MIB OIDs belong to different standards organizations, while “lower-level” OIDs are allocated by associated organizations (e.g. RACOM).

OID example:



Name	radioTemperature
OID	.1.3.6.1.4.1.33555.3.1.4.1
MIB	RACOM-RA2-MIB
Syntax	DecimalNumber (Integer32). Hint: d-1
Access	read-only
Status	current
DefVal	
Indexes	
Descr	Radio board temperature.

As you can see, numbers 1.3.6.1.4.1.33555 are the “higher-level” OIDs. The “lower-level” OIDs are .3.1.4.1 which are allocated by RACOM.

2. Simple Network Management Protocol in RipEX

SNMPv1, v2c and v3 are supported by RipEX2. Both can be configured separately for the SNMP agent and for SNMP notifications (traps and informs).

The communication is operated on standard UDP ports 161 (SNMP agent) and 162 (notifications).

RipEX2 supports read-only regime only, i.e., it is not possible to “set” values via SNMPSET commands.

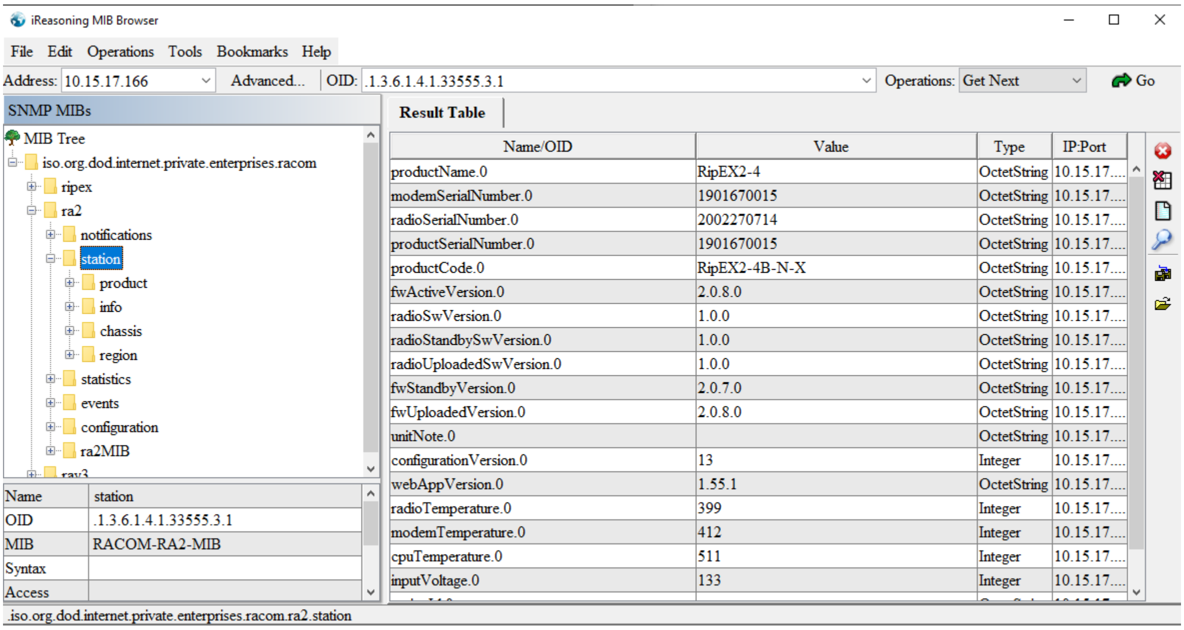
USM Security model is supported with AES-192 and AES-256 encryption extension.

SNMPv3 security is solved by a combination of USM (User-based Security Model) and VACM (View Access Control Model). SNMPv3 can be configured with or without Encryption and Authentication methods.

When using SNMP over radio channel, we recommend setting RipEX2 to the Router mode. From the point of radio network, SNMP is typically a standalone application sharing the radio channel with others. Thus, it causes collisions, which are automatically resolved by the radio channel protocol in the Flexible Router protocol, or handled optimally in the Base Driven Router protocol (no collisions at all). The radio channel uses no anti-collision protocol in the Bridge mode, meaning two competing applications can only be run at a great risk of collisions and with the knowledge that packets from both applications may be irretrievably lost.

2.1. RipEX2 proprietary MIB

MIB can be read via any text editor, but it might be better to browse it in some special SNMP browser such as MIBbrowser from iReasoning. The following section explains some details about RipEX2 MIB for firmware version 2.0.10.0. MIB consists of “revision history” information so you can quickly find out what has been changed.



Address: 10.15.17.166

OID: .1.3.6.1.4.1.33555.3.1

Operations: Get Next

Name	station
OID	.1.3.6.1.4.1.33555.3.1
MIB	RACOM-RA2-MIB
Syntax	
Access	

Name/OID	Value	Type	IP:Port
productName.0	RipEX2-4	OctetString	10.15.17....
modemSerialNumber.0	1901670015	OctetString	10.15.17....
radioSerialNumber.0	2002270714	OctetString	10.15.17....
productSerialNumber.0	1901670015	OctetString	10.15.17....
productCode.0	RipEX2-4B-N-X	OctetString	10.15.17....
fwActiveVersion.0	2.0.8.0	OctetString	10.15.17....
radioSwVersion.0	1.0.0	OctetString	10.15.17....
radioStandbySwVersion.0	1.0.0	OctetString	10.15.17....
radioUploadedSwVersion.0	1.0.0	OctetString	10.15.17....
fwStandbyVersion.0	2.0.7.0	OctetString	10.15.17....
fwUploadedVersion.0	2.0.8.0	OctetString	10.15.17....
unitNote.0		OctetString	10.15.17....
configurationVersion.0	13	Integer	10.15.17....
webAppVersion.0	1.55.1	OctetString	10.15.17....
radioTemperature.0	399	Integer	10.15.17....
modemTemperature.0	412	Integer	10.15.17....
cpuTemperature.0	511	Integer	10.15.17....
inputVoltage.0	133	Integer	10.15.17....

.iso.org.dod.internet.private.enterprises.racom.ra2.station

Fig. 2.1: MIB Browser example

Note

SMS counters were added in the 2.0.10.0 firmware.

The RipEX2 MIB module complies with the highest Severity level validation (level 6).

Supported MIBs and its OIDs:

- Values from general MIBs such as SNMPv2-MIB, IF-MIB, IP-MIB, TCP-MIB, UDP-MIB or MIB-II
- Proprietary MIB - RACOM-RA2-MIB
  - Statistics – complete Statistics are readable via SNMP – i.e., all the tables displayed in RipEX2 web interface Statistics menu are readable via SNMP as well (radio, Ethernet, cellular and serial statistics)
  - Notifications – traps and informs based on status of RipEX2 events
  - Station information – values such as product code, serial number, radio or CPU temperature, input voltage, …
  - Events – reading status, severities etc. about all supported Events
  - And some other values – e.g., Hardware capabilities, SNMP Update period

RipEX2 MIB utilizes custom types declaration so that SNMP reply is numeric, but each number corresponds to a particular meaning. E.g., type for Event severities:

```
EventSeverity ::= TEXTUAL-CONVENTION
   STATUS      current
   DESCRIPTION "Severity of event - based on syslog"
   SYNTAX      INTEGER {
        emergency (1),
         alert (2),
         critical (3),
         error (4),
         warning (5),
         notice (6),
         informational (7),
         debug (8)
   }
```

Make sure your NMS is configured to translate numeric values to their meaning correctly (Value mapping in Zabbix).

Some of the returned values are in decimal notations. E.g., CPU temperature returned as 487 means 48.7. If a particular value requires it, it also has a predefined unit such as degrees of Celsius, Volts, decibels, percent, … Again, make sure you utilize your NMS with correct unit.

Current MIB can always be downloaded from RACOM website together with Zabbix templates, see *https://www.racom.eu/eng/products/radio-modem-ripex-detail#dnl_fwr2*.

2.2. Bandwidth utilization

SNMP is primarily designed for Ethernet networks, where generally, bandwidth capacity is not an issue. By contrast, radio bandwidth capacity is very limited and RipEX2 mostly works over the radio channel. For this reason, special care is recommended while configuring NMS. If badly configured, NMS can take a significant portion of the network capacity or can even overload the network completely.

It is important to realize that getting all RACOM specific OIDs from a single RipEX2 with one neighbouring unit can be approximately 100 kilobytes using SNMPv2. With encrypted and authenticated SNMPv3, this data volume can be doubled.

Note

Number of values which can be obtained from each RipEX2 highly depends on number of neighbouring units, configured features (Protocols on RS232/Terminal servers, …) and HW capabilities (LTE, …).

We recommend to query most of the values from units connected via Ethernet and query only carefully selected OIDs over the radio channel and not all possible data. Set SNMP query time intervals in your NMS as long as possible. The shortest recommended interval ranges from several minutes to tens of minutes.

It is also recommended to utilize SNMP BULK requests which significantly reduce amount of data being exchanged between RipEX2 and NMS, because it is possible to query multiple OIDs within a single packet, as well as reply to such multiple requests within just one SNMP reply packet.

Note

There are many Network Management Systems available on the market. Whichever you choose, keep in mind the described limitations. E.g., never use NMS, which can download only the entire remote device MIB and not single OIDs.

2.3. Statistics via SNMP

Complete set of Statistic tables can be downloaded via SNMP. There are multiple principles which must be taken into account while getting such values from RipEX2 units.

Discovery procedure

Each unit can have different number of RipEX2 neighbours, different functionalities configured or different HW options, such as presence of LTE module. SNMP mechanism needs to discover such indexes to every supported table and then, query for currently enabled/supported values within these tables.

Typical mechanism in static RipEX2 network is to run Discovery procedure once and then just query values based on found indexes until there is any change in the network topology or configured functionalities in RipEX2 units. In such situation, it is required that this Discovery procedure updates all the indexes – i.e., adds new lines/indexes and removes those which are no longer supported.

Tables requiring Discovery:

Radio interface statistics, Radio protocol statistics and Radio signal statistics

- Both tables consist of lines for each neighbouring RipEX2 unit, indexes which are discovered are unique MAC or Link addresses. You can use IP addresses in your NMS for better understanding (see more details in Zabbix NMS section).
- You need to re-run Discovery every time you add a new unit into the network. Removing of such unit can usually be automatic (after specified time of inaccessibility).

Serial protocols statistics

- This table consist of enabled COM and TS ports

- Re-run the discovery every time you enable a new COM or TS port

Ethernet statistics

- This table consist of enabled ETH ports
- Re-run the discovery every time you enable another Ethernet port or e.g., install the SFP port (ETH5)

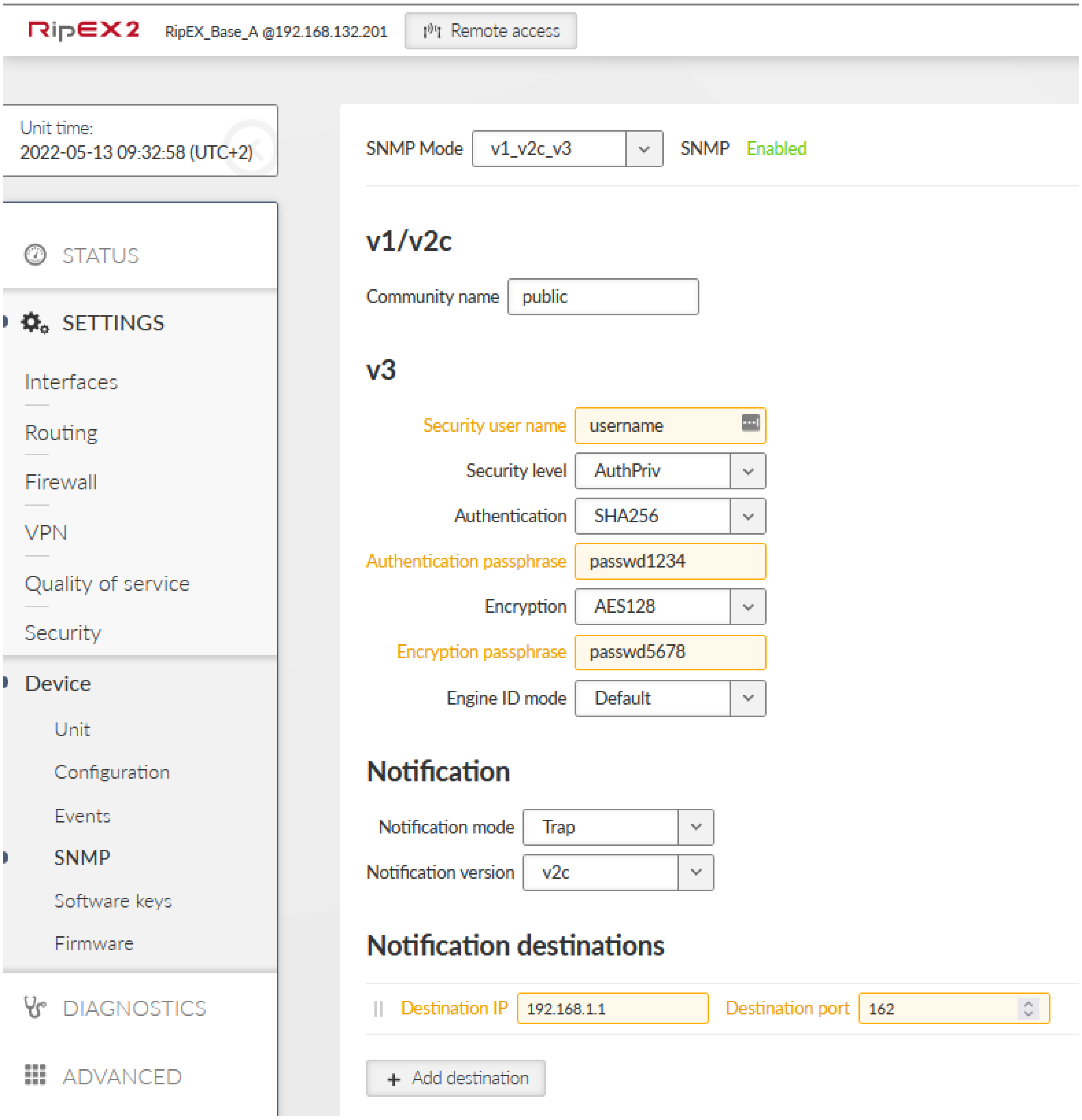
Statistics Update Period

In general, we have two types of Statistics tables.

- Tables consisting counters – The Counter64 type represents a non-negative integer which monotonically increases until it reaches a maximum value of 2^64-1 (18446744073709551615 decimal), when it wraps around and starts increasing again from zero.
  - Every time you read any value from these tables, you read a current counter value – it is usually suggested to re-calculate this value to either changes per second or to simple changes (difference between two readings)
  - List of tables: Radio interface statistics, Radio protocol statistics, Radio protocol non-addressable statistics, Serial protocols statistics, Ethernet statistics, Cellular interface statistics
- Tables consisting Statistics based on “Update period” parameter
  - Tables are periodically updated with this period
  - Default value is 15 minutes (see the Advanced menu and set “Statistics table update period” variable to different value, if required
  - If you use a default value equal to 15 minutes, the values within these tables are updated every 15 minutes
    - Values are not changed within this period (no matter how many times you query for particular values)
    - Once 15 minutes pass, a new update to tables is done and you can read new values from these last 15 minutes (e.g., average RSS value).
    - You cannot read current values from the period which is not yet “closed/finished”
  - Your NMS interval for querying these values should equal to this Update period
  - List of tables: Radio signal statistics, Radio signal non-addressable statistics, Cellular signal statistics, Cellular state statistics

2.4. RipEX2 SNMP Settings

Basic SNMP parameters are described in *RipEX2 user manual*[1] and can be configured in SETTINGS – Device – SNMP menu. The following section highlights some important parameters or explains something in more details.



Unit time: 2022-05-13 09:32:58 (UTC+2)

SNMP Mode: v1_v2c_v3 SNMP Enabled

v1/v2c

Community name: public

v3

Security user name: username
Security level: AuthPriv
Authentication: SHA256
Authentication passphrase: passwd1234
Encryption: AES128
Encryption passphrase: passwd5678
Engine ID mode: Default

Notification

Notification mode: Trap
Notification version: v2c

Notification destinations

Destination IP: 192.168.1.1 Destination port: 162

Fig. 2.2: RipEX2 SNMP menu

Make sure that your NMS supports Authentication and Encryption algorithms you choose in RipEX2. For example, since Zabbix 6.0 LTS, SHA224 and higher are supported, but in previous versions, Zabbix could only select MD5 or SHA1 from the Authentication listbox.

Another not very common option is “**Engine ID**”. This option is valid for SNMPv3 only. It serves for unambiguous SNMP instance identification. Every SNMPv3 enabled device within a network must have a unique Engine ID.

[1] https://www.racom.eu/eng/products/m/ripex2/set.html#set_snmp

By default, Engine ID is generated automatically based on RipEX2 MAC address (ETH1 interface). If it is set to “UserDefined” option, you can set or generate your own Engine ID.

Example of default Engine ID: 80 008313 03 00 02 a9 20 06 ef

- 80 – engine ID as described in RFC3411 – engine ID must start with standard identification
- 008313 – enterprise OID – 33555 – RACOM s.r.o.
- 03 – engine ID assembled according to MAC address
- 00 02 a9 XX XX XX – ETH1 MAC address

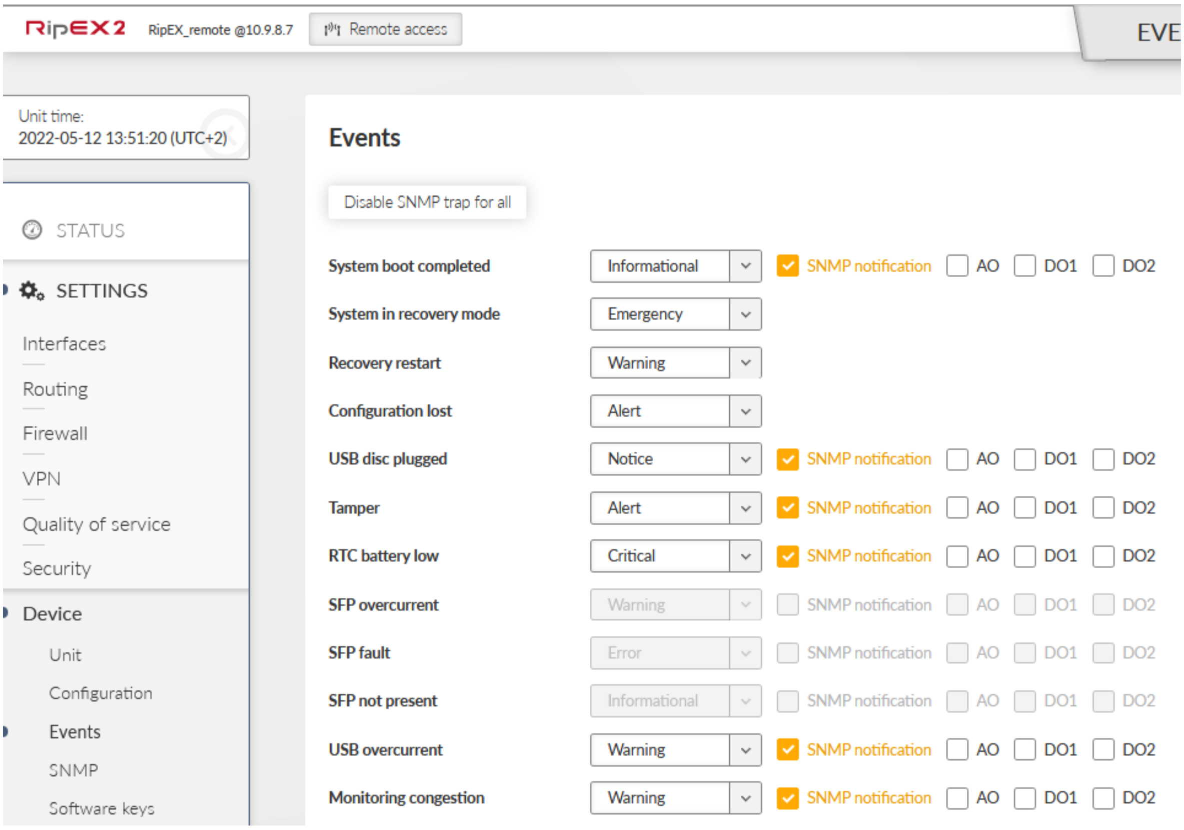
Example of own Engine ID:
80 008313 04 61494F6730346743574A31376970386345305A6D456C4B2D697059

- 04 – Engine ID is assembled according to user defined string
- 61494F6730346743574A31376970386345305A6D456C4B2D697059 – HEX string from configuration

The differentiated part of the Engine ID can be entered as ASCII characters or generated (e.g., aIOg04gCWJ17ip8cE0ZmElK-ipY). This string is converted into HEX number (i.e., 61 49 4F 67 30 34 67 43 57 4A 31 37 69 70 38 63 45 30 5A 6D 45 6C 4B 2D 69 70 59).

Notifications are being sent based on Events. Select events for which you want notifications to be sent in SETTINGS – Device – Events menu. Check the particular check-box “SNMP notification”. You can also Enable SNMP notifications for all supported Events with one button “Enable SNMP trap for all”.

Current EngineID can be checked by capturing the SNMP data in Wireshark. It can also be obtained by SNMP request for .1.3.6.1.6.3.10.2.1.1 OID (implemented in newer firmware versions than 2.0.10.0).



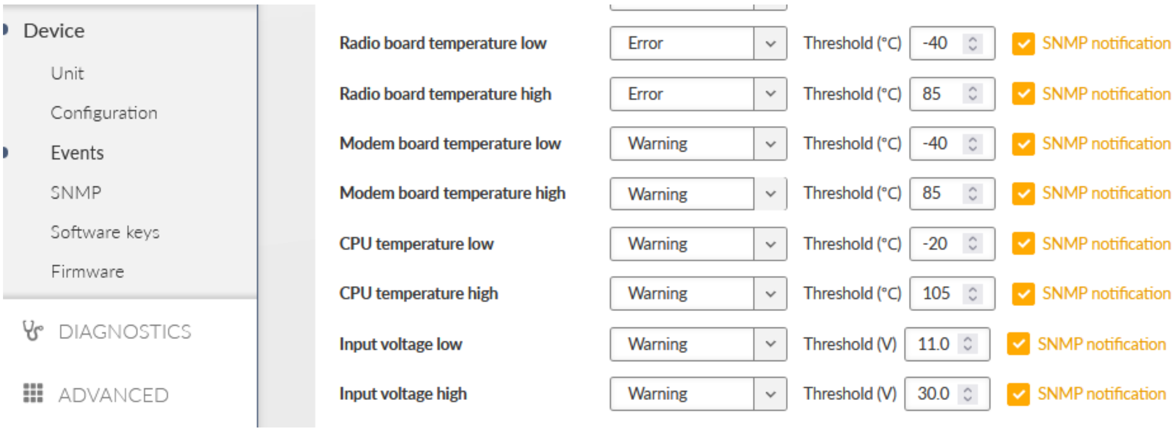
Events

System boot completed	Informational	☑ SNMP notification	□ AO	□ DO1	□ DO2
System in recovery mode	Emergency				
Recovery restart	Warning				
Configuration lost	Alert				
USB disc plugged	Notice	☑ SNMP notification	□ AO	□ DO1	□ DO2
Tamper	Alert	☑ SNMP notification	□ AO	□ DO1	□ DO2
RTC battery low	Critical	☑ SNMP notification	□ AO	□ DO1	□ DO2
SFP overcurrent	Warning	□ SNMP notification	□ AO	□ DO1	□ DO2
SFP fault	Error	□ SNMP notification	□ AO	□ DO1	□ DO2
SFP not present	Informational	□ SNMP notification	□ AO	□ DO1	□ DO2
USB overcurrent	Warning	☑ SNMP notification	□ AO	□ DO1	□ DO2
Monitoring congestion	Warning	☑ SNMP notification	□ AO	□ DO1	□ DO2

Fig. 2.3: RipEX2 Events

If required, you can change severities for some of the Events, others are fixed to a particular level.

Several Events can be configured with Thresholds – temperatures and voltage. Set the required values if not satisfied with default limits.



Radio board temperature low	Error	Threshold (°C)	-40	☑ SNMP notification
Radio board temperature high	Error	Threshold (°C)	85	☑ SNMP notification
Modem board temperature low	Warning	Threshold (°C)	-40	☑ SNMP notification
Modem board temperature high	Warning	Threshold (°C)	85	☑ SNMP notification
CPU temperature low	Warning	Threshold (°C)	-20	☑ SNMP notification
CPU temperature high	Warning	Threshold (°C)	105	☑ SNMP notification
Input voltage low	Warning	Threshold (V)	11.0	☑ SNMP notification
Input voltage high	Warning	Threshold (V)	30.0	☑ SNMP notification

Fig. 2.4: RipEX2 Events – configurable thresholds

Radio board temperature severity is set to “Error”, because too low/high temperatures can corrupt radio transmission. Others are set to “Warning”.

Another difference in Events is that some Events are just informational – such as that a new user was created, or Recovery restart has been triggered. Other events consist of “Status” so that if the Event happens, a “Raise” SNMP notification is sent causing a unit and eventually the NMS to display some “error” state. Once the Event is no longer active, the “Clear” notifications is sent and the particular “error” state is also cleared. E.g., CPU temperature goes to too high value (110°C) and raises the alarm. Once the temperature is below the limit again (for example 90°C), RipEX2 clears this event and sends a corresponding notification as well. Your NMS should be configured for both types.

Note

The SNMPv3 Inform is not supported in 2.0.10.0 firmware and older. There is an opened issue in SNMP daemon and we wait for that fix. Once done, we will enable this option again.

The last parameter is only accessible via Advanced menu – **Statistics table update period**. If you require different value than default 15 minutes, do it via the Advanced menu.

3. Network Management System – ZABBIX

To access our SNMP values, any Network Management System (NMS) can be used. However, we recommend using the ZABBIX open source monitoring system. It can be downloaded at *http://www.zabbix.com/download.php*[1].

Zabbix features are explained here - *https://www.zabbix.com/features*.

If you have chosen the Zabbix software, please read the following pages where we offer a basic Starting Guide to RipEX2 and Zabbix co-working.

Whatever your choice of NMS, these sections may provide general hints and tips anyway.

Note

The following guide was tested with Zabbix LTS version 6.0. There is no RipEX2 application note for older Zabbix releases.

Take the opportunity to remotely access and test a live *Zabbix demo*[2]. See the credentials within the text on the given link.

3.1. Installation and Documentation

Follow the Zabbix documentation at: *https://www.zabbix.com/documentation/current/en/manual*, download packages from *https://www.zabbix.com/download* and install Zabbix 6.0 LTS. We suggest using Debian11 (or newer) OS, MySQL database and Apache web server, because of our good experience and knowledge. If using different solution, our help can be limited.

Note

With previous Zabbix versions, we suggested using CentOS7 and CentOS8, but due to changes in distributing these operating systems, Debian OS seems to be much more appropriate.

Zabbix also offers paid support – see all the possible support tiers at *https://www.zabbix.com/support*.

Once Zabbix 6.0 LTS is installed, multiple additional installation steps are required so that you can monitor and maintain your RipEX2 (and any other RACOM products) network(s). Required steps are explained later within this application note.

We also offer Zabbix 6.0 LTS as a virtual, ready-to-be-used, image. It is called “RACOM Zabbix Appliance” or in short “**RZA6**”. Within this .ova image, functionality for all RACOM products is already installed and ready to be used. Contact our *support*[3] to obtain this virtual machine and stay in touch with us for more details.

You can run this RZA6 as a virtual machine, e.g., within your VMware or VirtualBox environment (or any similar one).

[1] http://www.zabbix.com/download
[2] https://www.racom.eu/eng/products/m/ripex/demo/zabbix.html
[3] mailto:support@racom.eu

3.1.1. Zabbix Installation from packages

Once you finish basic Zabbix 6.0 LTS installation following the Zabbix documentation, you can and should check this part for more details about required steps for RACOM products Zabbix support. The order of explained steps is not so important usually.

Note

If there is any particular Linux command, it is based on Debian11 OS.

We suggest various applications for future usage:

- traceroute
- nmap
- zabbix-sender
- sshpas

All the commands can be installed from the command line with:

```
# apt-get install traceroute nmap zabbix-sender sshpass
```

If you need, you can implement sending **PDF reports** automatically. The installation and functionality can vary from version to version so we do not describe step-by-step procedure here. Use Zabbix documentation for more details.
https://www.zabbix.com/documentation/current/en/manual/appendix/install/web_service

For RACOM products, multiple steps are required. Upload all the MIBs from respective devices (RipEX2 in our case) to /usr/share/snmp/mibs/ directory. For a proper functionality, add them to SNMP configuration file /etc/snmp/snmp.conf. E.g.:

```
mibs +/usr/share/snmp/mibs/MG-MIB.txt
mibs +/usr/share/snmp/mibs/RacomRay3.mib
mibs +/usr/share/snmp/mibs/RacomRay2.mib
mibs +/usr/share/snmp/mibs/RACOM-RipEX-1.0.4.0.mib
mibs +/usr/share/snmp/mibs/SNMPv2-TC.txt
mibs +/usr/share/snmp/mibs/RACOM-RA2-MIB
```

Templates

Download RipEX2 Zabbix 6.0 template from our *website*[4]. Unzip the file and import zbx_export_ripex2.yaml into your Zabbix instance in Configuration -> Templates menu via web interface. The template consists of:

- approximately 300 Item values (10 tags) which can be read from RipEX2 units (proprietary OIDs only – i.e., OID starting with 1.3.6.1.4.1.33555.3 prefix). For other general OIDs, use Zabbix predefined templates or do your own templates (e.g., SNMPv2-MIB::sysDescr.0, SNMPv2-MIB::sysName.0, …)
  - Most of the values are for Events and Traps
- Discovery rules
  - For the 2.0.10.0 firmware, there are 9 Discovery rules
  - We use Discovery rules for RipEX2 statistics, because most statistics consist of individual lines within tables where each line is e.g., another RipEX2 unit, Ethernet port or SIM card – and because

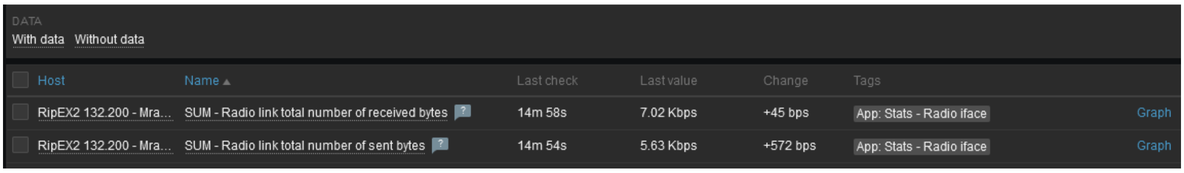
[4] https://www.racom.eu/eng/products/radio-modem-ripex-detail#dnl_fwr2

- these tables can change based on configuration, HW capabilities and network diagram/topology, individual items must be discovered first.
- Once discovered, new Items are automatically created and then, Zabbix handles them as basic Items. The only difference is that if a particular new Item becomes unsupported, Zabbix deletes it automatically after a predefined time.

Default Template settings:

- All Items are in Disabled state
  - Most values are being updated once a day
- All Discovery rules are disabled as well
  - Most values are being updated every 15 minutes
  - By default, each discovery rule is run every 8 hours – If you have a static network, it might be enough to run it once and disable the rules afterwards

Two calculated items were also predefined - they both sum all received/sent bytes for all neighbouring RipEX2 units (in GUI the values are displayed in Radio Protocol statistics table in "Total [B]" column). These values can be useful to show approximate value of data being transferred over the Radio channel, incl. control frames. Both can be found with a tag "Stats - Radio iface" or check the items with "SUM" key word.



DATA

With data Without data

□	Host	Name ▲	Last check	Last value	Change	Tags	
□	RipEX2 132.200 - Mra...	SUM - Radio link total number of received bytes ?	14m 58s	7.02 Kbps	+45 bps	App: Stats - Radio iface	Graph
□	RipEX2 132.200 - Mra...	SUM - Radio link total number of sent bytes ?	14m 54s	5.63 Kbps	+572 bps	App: Stats - Radio iface	Graph

Other important steps are for SNMP traps. Once the trap is received, it is handled by our script and for its proper functionality, the OID cannot be translated to text. Edit the snmptrapd:

```
# systemctl edit snmptrapd.service --force -full
```

Change the ExecStart variable:

```
ExecStart=/usr/sbin/snmptrapd -Lsd -f -p /run/snmptrapd.pid -On
```

The whole file should be:

```
# cat /etc/systemd/system/snmptrapd.service
[Unit]
Description=Simple Network Management Protocol (SNMP) Trap Daemon.
After=network.target
ConditionPathExists=/etc/snmp/snmptrapd.conf
[Service]
Type=simple
ExecStart=/usr/sbin/snmptrapd -Lsd -f -p /run/snmptrapd.pid -On
ExecReload=/bin/kill -HUP $MAINPID
[Install]
```

For a proper functionality of RipEX2 SNMP notifications, multiple additional steps are required. The following sections focuses on SNMPv2c traps and informs. The SNMPv3 notifications are described later on. Also keep in mind that you could configure RipEX2 notifications different way (e.g., via SNMPTT) – here is just one approach described.

If not yet installed, install ‘snmptrapd’ daemon and enable it to be run automatically.

Within the downloaded .zip templates from our website, snmptrap.sh script is included. Copy the script into /usr/lib/zabbix/externalscripts/ directory and change the file privileges and make it executable.

```
# chown zabbix:zabbix /usr/lib/zabbix/externalscripts/snmptrap.sh
# chmod +x /usr/lib/zabbix/externalscripts/snmptrap.sh
```

Note

Your ‘zabbix’ user should be enabled. It should have a HOME directory set to /var/lib/zabbix/ and this user should be able to run the shell. E.g., this command can be helpful:

```
# usermod --shell /bin/bash zabbix
```

Check your ‘zabbix_sender’ path and if required, change it within the provided snmptrap.sh script accordingly.

```
# which zabbix_sender
/usr/bin/zabbix_sender
```

So, the script has this line inside:

```
ZABBIX_SENDER="/usr/bin/zabbix_sender";
```

The script parses the output of each received SNMP trap, selects the appropriate host and declares an associative array containing trap descriptions. Eventually, it sends the whole message to your Zabbix server.

The default path to a LOG file from snmptrap.sh script is /var/log/snmptrap/snmptrap.log. Create the directory and a file manually, if not yet created.

Another required step from the command line is to edit /etc/zabbix/zabbix_server.conf file. Find the appropriate lines and edit them to:

```
SNMPTrapperFile=/var/log/snmptrap/snmptrap_snmptt.log
StartSNMPTrapper=1
```

Note

It is possible to configure log rotating. To do so, add two files into /etc/logrotate.d directory called "zabbix-snmp-trap" and "zabbix-snmp-trapper". The format of both the files is the same, excluding the file path:

```
/var/log/snmptrap/snmptrap.log {
    weekly
    rotate 12
    compress
    delaycompress
    missingok
    notifempty
    create 0640 root root
}
```

and

```
        /var/log/snmptrap/snmptrap_snmptt.log {
            weekly
            rotate 12
            compress
            delaycompress
            missingok
            notifempty
            create 0640 root root
        }
```

Zabbix, and especially your snmptrapd must know how to authenticate against the received traps/informs. If it is SNMPv2, it is quite easy – you just need to allow particular community strings and also explicitly say that our snmptrap.sh must be executed upon a received trap/inform. Do this via /etc/snmp/snmptrapd.conf file. Example of such file:

```
authCommunity log,execute public
authCommunity log,execute mwl-snmp
authCommunity log,execute racom-snmp
traphandle default /bin/bash /usr/lib/zabbix/externalscripts/snmptrap.sh
```

With SNMPv3 it gets more complicated.

Important

Due to a bug in SNMP daemon, SNMPv3 informs are not working and cannot be selected. Once this 3rd party daemon is fixed, we add the functionality back to our RipEX2 release. RipEX2 FW version is 2.0.10.0 or older.

For SNMPv3 Informs (not traps), you need to create the user via createUser command. Stop the snmptrapd daemon:

```
# systemctl stop snmptrapd
```

Now, edit the /etc/snmp/snmptrapd.conf file and add these lines:

```
createUser racom MD5 "racom1234" DES "racom5678"
authUser log,execute,net racom
```

This should add the User "racom" with MD5 and DES secrets and authenticate him. Save the changes and start the snmptrapd daemon.

```
# systemctl start snmptrapd
```

Now, the SNMPv3 informs can be successfully received and used.

SNMPv3 Traps need a bit different command. Everything is the same, but the EngineID must be configured.

Each RipEX2 has a unique EngineID by default, you can also generate your own. This was explained in *Section 2.4, “RipEX2 SNMP Settings”*.

Note

If you generate your own EngineID, it is given as a text, but the EngineID is then read as HEX number. E.g. A generated EngineID in GUI is: “UULhM_jp2ObIoN8CVP8aUoaG2Hg”, but the Engine ID in HEX format which you need to set in snmptrapd.conf file is “800083130455554c684d5f6a70324f62496f4e384356503861556f6147324867”.

Stop the snmptrapd daemon again and add a similar line in the /etc/snmp/snmptrapd.conf file:

```
createUser -e 80008313030002a9200ad3 racom MD5 "racom1234" DES "racom5678"
authUser log,execute,net racom
```

This creates a "racom" user the same way as for the Informs, but the EngineID 80008313030002a9200ad3 is fixed and must correspond to the created one in RipEX2 web interface.

Note

The same procedure must be met for any other SNMPv3 devices and their SNMPv3 traps/informs (not just RipEX2).

Once you apply all the mentioned changes, it is suggested to reboot your Linux OS and check the functionality.

RipEX2 images

Hosts can be displayed in graphs. For such a purpose, we created multiple RipEX2 images of different size and with different borders (e.g., red border in case the unit is in a problem state). These images are included in the mentioned .zip file with RipEX2 template. Import them one by one in Administration – General – Images menu, or via directly via MySQL.

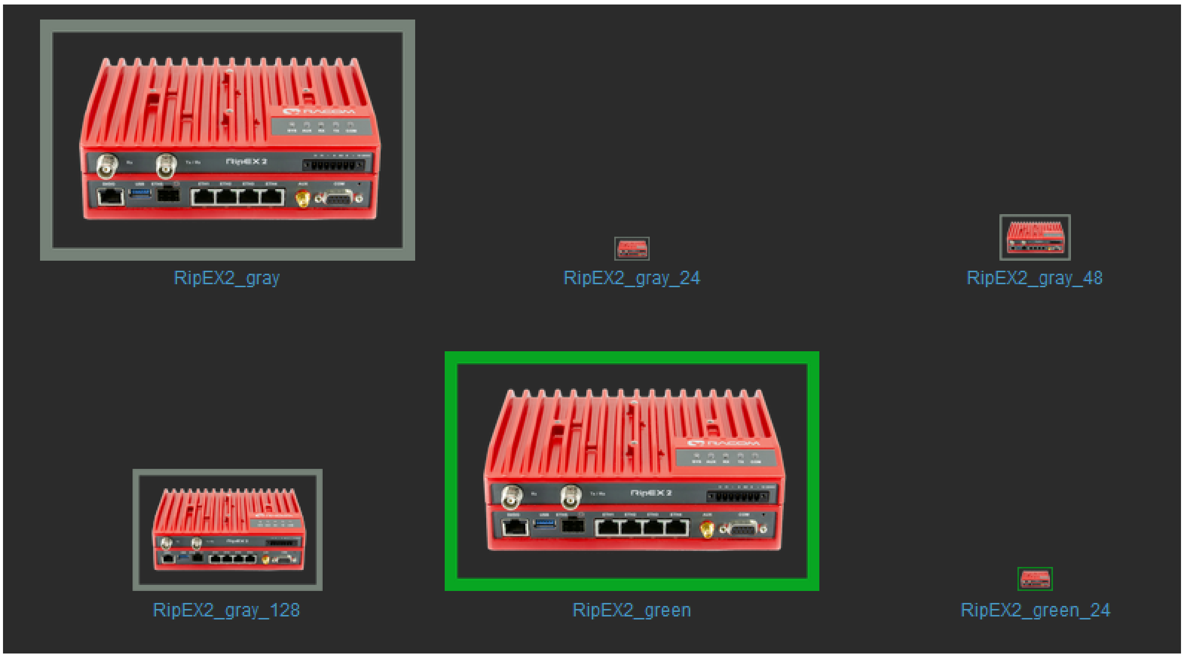


Fig. 3.1: RipEX2 images in Zabbix

3.1.2. RACOM Zabbix Appliance – RZA6

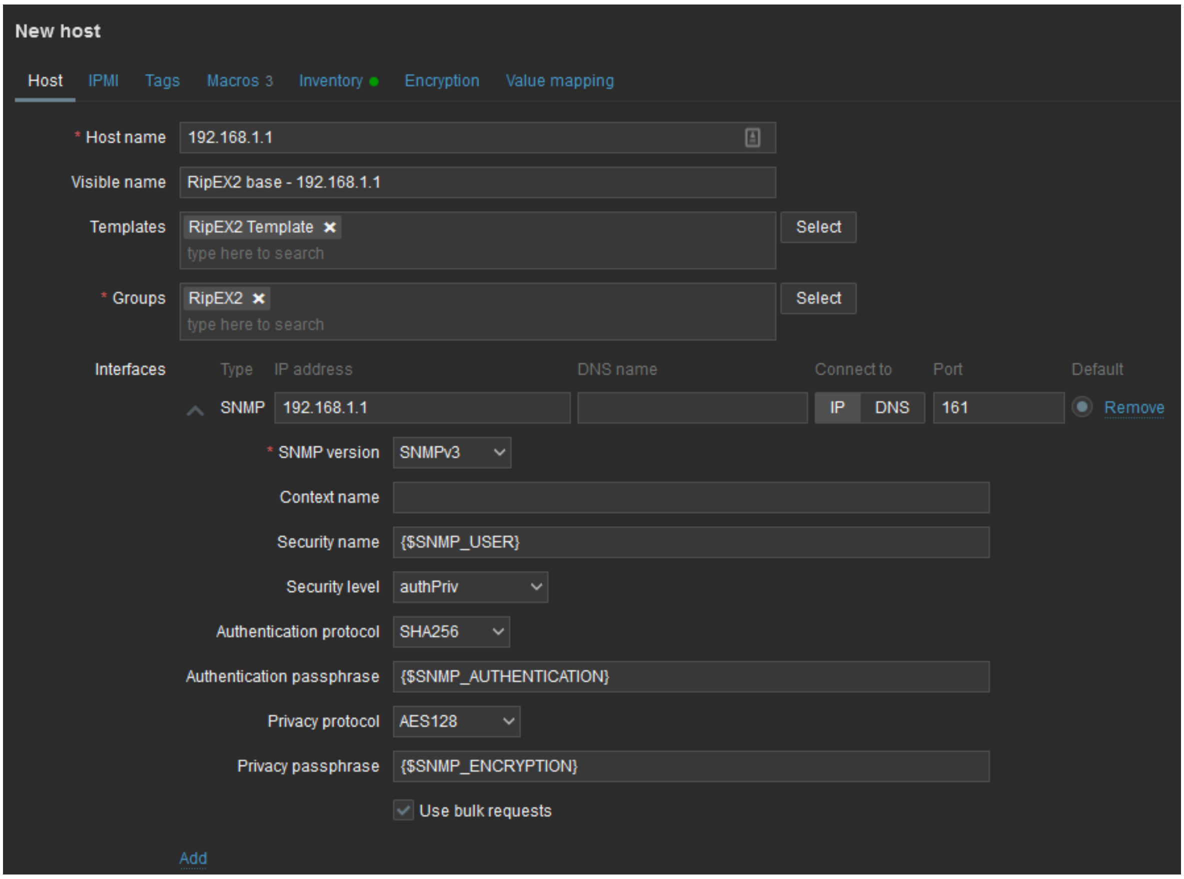
RZA6 is widely preconfigured.

You will still need to go through SNMP traps/informs section above so that you can use your particular community strings, and SNMv3 users. Otherwise, all should be prepared.

3.2. How to use RipEX2 template

Now, Zabbix should be ready for monitoring RipEX2 network. This chapter gives you a brief procedure to get started, but feel free to utilize different approach.

First, we suggest to create a Host – probably RipEX2 Base station accessible via Ethernet from Zabbix. Go to the Configuration – Hosts menu and click on the “Create host” button on top right corner.



* Host name: 192.168.1.1

Visible name: RipEX2 base - 192.168.1.1

Templates: RipEX2 Template ✕ (type here to search)

* Groups: RipEX2 ✕ (type here to search)

Interfaces:

Type	IP address	DNS name	Connect to	Port	Default
SNMP	192.168.1.1		IP DNS	161	● Remove

* SNMP version: SNMPv3

Context name:

Security name: {$SNMP_USER}

Security level: authPriv

Authentication protocol: SHA256

Authentication passphrase: {$SNMP_AUTHENTICATION}

Privacy protocol: AES128

Privacy passphrase: {$SNMP_ENCRYPTION}

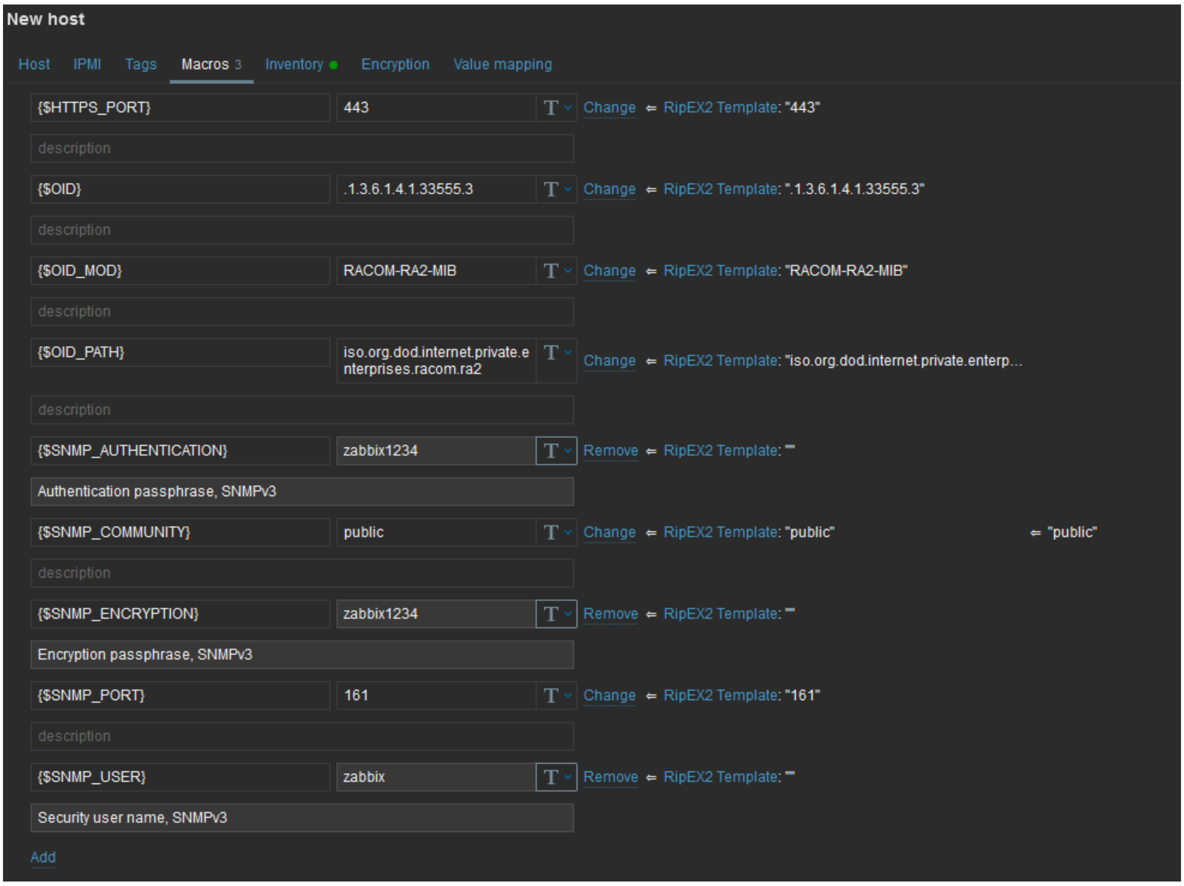
☑ Use bulk requests

Fig. 3.2: New RipEX2 host

Always put the IP address of the unit to the “Host name” field so the SNMP notifications work (the script works with IP addresses). The “Visible name” can be set to any required value.

Select the “RipEX2 Template” so that the unit is preconfigured with all RipEX2 supported Items. Create a new, or add it to an existing one, RipEX2 group. You can name it as required – e.g., based on RipEX2 network location or particular customer company name. Set the SNMP Interface:

- IP address
- Port (usually UDP/161)
- SNMP version (either v2c, or v3)
  - If v2c, set the community string to MACRO {$SNMP_COMMUNITY}
  - If v3, set the values according to your RipEX2 setup
    - Security name - {$SNMP_USER}
    - Authentication passphrase - {$SNMP_AUTHENTICATION}
    - Privacy passphrase - {$SNMP_ENCRYPTION}
  - Now, check and change MACROs in “Macros” tab



New host

Host IPMI Tags **Macros 3** Inventory ● Encryption Value mapping

{$HTTPS_PORT}	443	T	Change	⇐ RipEX2 Template: "443"
description				
{$OID}	.1.3.6.1.4.1.33555.3	T	Change	⇐ RipEX2 Template: ".1.3.6.1.4.1.33555.3"
description				
{$OID_MOD}	RACOM-RA2-MIB	T	Change	⇐ RipEX2 Template: "RACOM-RA2-MIB"
description				
{$OID_PATH}	iso.org.dod.internet.private.enterprises.racom.ra2	T	Change	⇐ RipEX2 Template: "iso.org.dod.internet.private.enterp…
description				
{$SNMP_AUTHENTICATION}	zabbix1234	T	Remove	⇐ RipEX2 Template: ""
Authentication passphrase, SNMPv3				
{$SNMP_COMMUNITY}	public	T	Change	⇐ RipEX2 Template: "public" ⇐ "public"
description				
{$SNMP_ENCRYPTION}	zabbix1234	T	Remove	⇐ RipEX2 Template: ""
Encryption passphrase, SNMPv3				
{$SNMP_PORT}	161	T	Change	⇐ RipEX2 Template: "161"
description				
{$SNMP_USER}	zabbix	T	Remove	⇐ RipEX2 Template: ""
Security user name, SNMPv3				

Add

Fig. 3.3: RipEX2 Host MACROs

You can either change the values in Template so it is the same in all your RipEX2 units, or you can set it per Host.

- Check the “Use bulk requests” option because it optimizes data traffic being sent

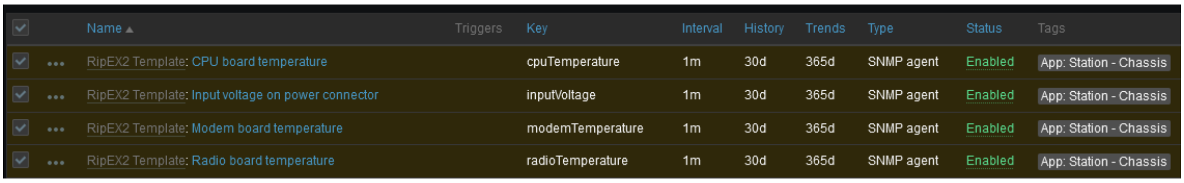
Verify the Inventory tab – it should be set to “Automatic” so some of the values are automatically filled by SNMP queries. Click on the “Add” button – a new Host is created.

But the host is not monitored yet, because all the Items and Discoveries are disabled by default.

Only monitor the values which you really need and with reasonable update times. This is important for units accessible via the Radio channel – so that you limit data being sent over the narrow RipEX2 radio network.

Default update intervals are either 15 minutes, or 1 day. A template keeps up to 1 year of trends/history.

Go to the Host’s Items and enable required Items, you can also edit the SNMP query intervals and other parameters. As an example, we enable 4 Items with an App “tag” equal to “Station – Chassis” and we decrease Interval to just 1 minute.



☑		Name ▲	Triggers	Key	Interval	History	Trends	Type	Status	Tags
☑	•••	RipEX2 Template: CPU board temperature		cpuTemperature	1m	30d	365d	SNMP agent	Enabled	App: Station - Chassis
☑	•••	RipEX2 Template: Input voltage on power connector		inputVoltage	1m	30d	365d	SNMP agent	Enabled	App: Station - Chassis
☑	•••	RipEX2 Template: Modem board temperature		modemTemperature	1m	30d	365d	SNMP agent	Enabled	App: Station - Chassis
☑	•••	RipEX2 Template: Radio board temperature		radioTemperature	1m	30d	365d	SNMP agent	Enabled	App: Station - Chassis

If you want Traps/Informs to be working, you need to enable particular traps with App tag equal to TRAPS and enable Triggers accordingly (i.e., if you enable “Input voltage too high” Item, you also need to enable a Trigger for this Item).

Last important menu is “Discovered rules”. They are already explained on previous pages. If you want to discover particular Items, just enable required Discovery rule(s). E.g., enable “Discovery – Radio Signal Statistics” for receiving values from Statistics table containing RSS, MSE etc. with all neighbouring RipEX2 units.

You can check the data in the Monitoring – Latest data menu. Filter the values are required. All numeric values can be depicted in graphs. String values have their own history.

Other units can be easily added by a “Clone” button from this Host configuration. Just change appropriate IP addresses and ports. Divide them into groups (e.g., geographically). Choose wisely the monitored values and enabled discovery rules.

3.3. Zabbix Usage Hints and Tips

This application note cannot target all possible information about Zabbix and its usage. Check Zabbix documentation and Google forums for general help and guides. The following section provides several hints and tips for quicker and easier RipEX2 network monitoring. Information provided might not be fully explained or might be different in any other Zabbix version other than 6.0 LTS.

3.3.1. Maps

Having a map is handy way for a network overview. On a single map, or multiple maps (even hierarchical) you may see all RipEX2 units (and any other devices) and their status overview. There can be a plain/empty background, or e.g., some picture of a map (static).

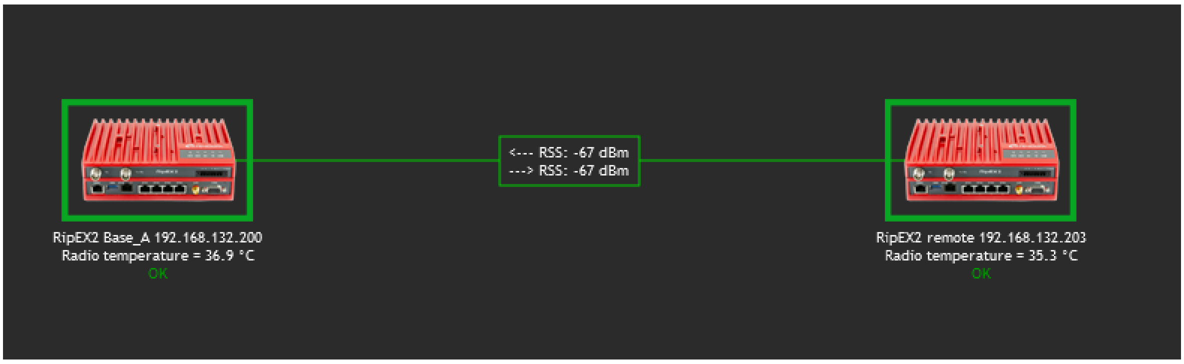
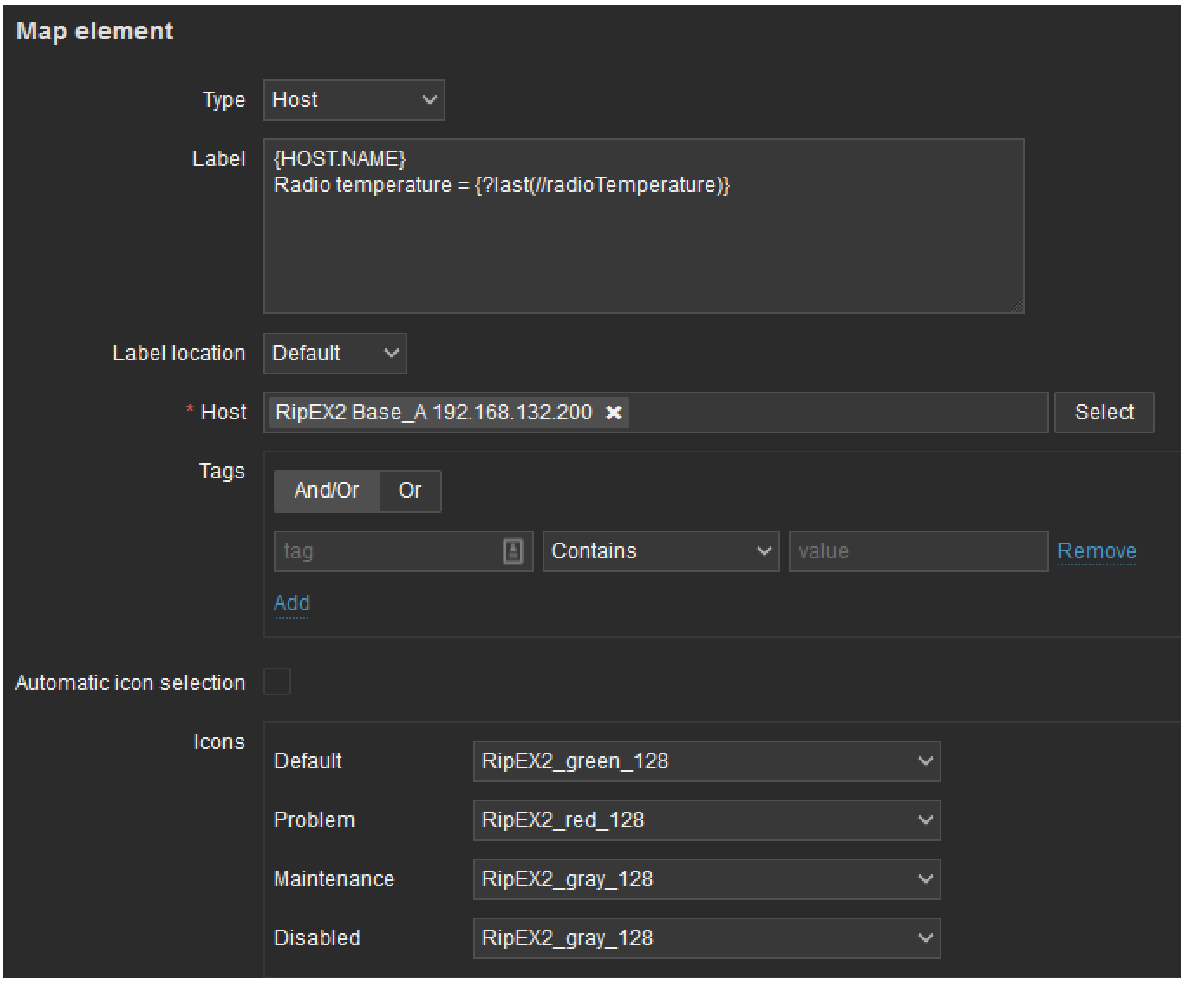

<--- RSS: -67 dBm
---> RSS: -67 dBm
RipEX2 Base_A 192.168.132.200
Radio temperature = 36.9 °C
OK
RipEX2 remote 192.168.132.203
Radio temperature = 35.3 °C
OK

Fig. 3.4: Zabbix simple RipEX2 map

On the map above, we can see two RipEX2 units with a displayed name and current Radio temperature. If the unit has no Problem, an “OK” message is displayed and the Host borders are in green color. We also depict a radio link between these units and its RSS values. Details:

Host details:



Map element

Type	Host

Label	{HOST.NAME}
	Radio temperature = {?last(//radioTemperature)}

Label location	Default
* Host	RipEX2 Base_A 192.168.132.200 ✖
Tags	And/Or · Or tag · Contains · value · Remove Add
Automatic icon selection	☐
Icons	Default: RipEX2_green_128 Problem: RipEX2_red_128 Maintenance: RipEX2_gray_128 Disabled: RipEX2_gray_128

Fig. 3.5: Host details in maps

Label is set as follows:

```
{HOST.NAME}
Radio temperature = {?last(//radioTemperature)}
```

Select a particular host and you can change icons for various situations.

Example of the link Label:

```
<--- RSS: {?last(/192.168.132.200/radioSignalRssAvg[10.10.10.2])}
---> RSS: {?last(/192.168.132.203/radioSignalRssAvg[10.10.10.1])}
```

Even the link color can change in time – for example lower RSS than -90 dBm. You can create your own Trigger monitoring average RSS values.

3.3.2. Geographical Maps

New feature from 6.0 LTS Zabbix version are Geographical maps. If you add GPS coordinates to your RipEX2 hosts, you can display them on geographical maps.

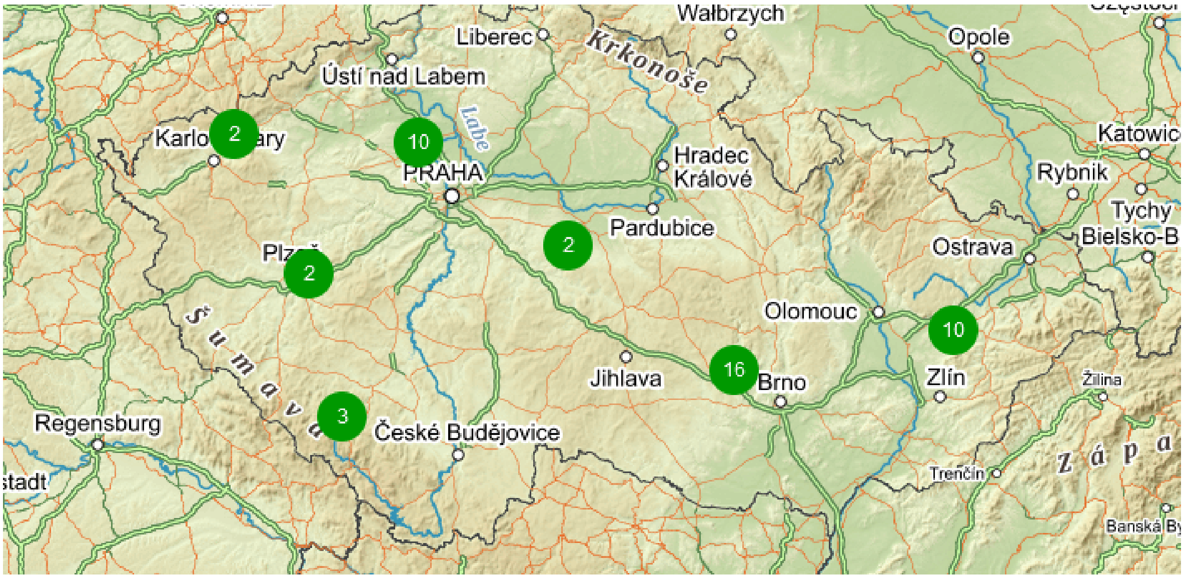
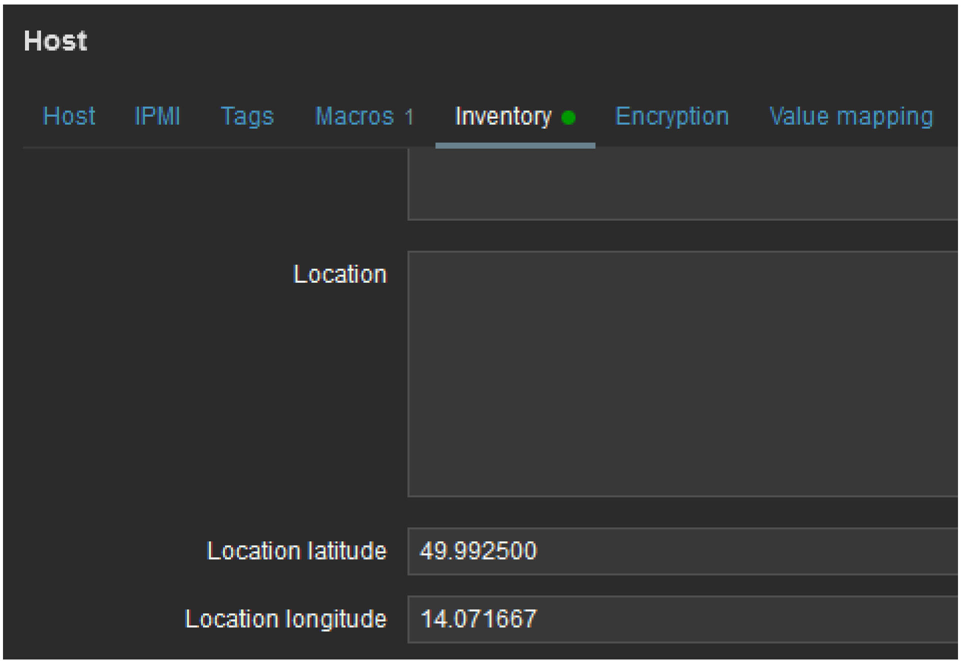


Fig. 3.6: Geographical map

First, you need to add GPS coordinates in the Host Inventory.

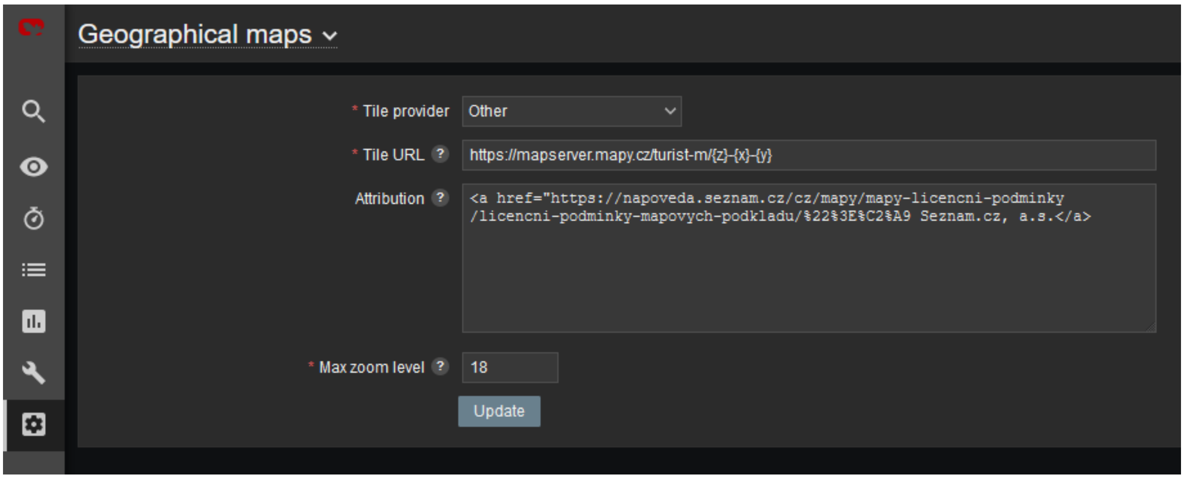

Host

Host | IPMI | Tags | Macros 1 | Inventory ● | Encryption | Value mapping

Location	
Location latitude	49.992500
Location longitude	14.071667

Fig. 3.7: Host GPS coordinates

Another step is to enable and configure Geographical graphs. Go to Administration – General – Geographical maps menu. Set the required map source/provider. There is a list of default supported map sources, but you can also add “other”. Here is the example for Czech mapy.cz map source.



* Tile provider: Other

* Tile URL: https://mapserver.mapy.cz/turist-m/{z}-{x}-{y}

Attribution: <a href="https://napoveda.seznam.cz/cz/mapy/mapy-licencni-podminky/licencni-podminky-mapovych-podkladu/%22%3E%C2%A9 Seznam.cz, a.s.</a>

* Max zoom level: 18

Fig. 3.8: Zabbix Geographical maps

Tile URL: *https://mapserver.mapy.cz/turist-m/{z}-{x}-{y}*[5]

Attribution: <a href="https://napoveda.seznam.cz/cz/mapy/mapy-licencni-podminky/licencni-podminky-mapovych-podkladu/%22%3E%C2%A9 Seznam.cz, a.s.</a>

Max zoom level: 18

The last step is to add Geographical map to your Dashboard. Edit the dashboard and add “Geomap” widget. Select its name, host group(s) and host(s). Save the changes.

Within the map, you can use a “zoom” feature. You can either see multiple hosts within one icon, or one icon is one host (it is zoomed enough). You can then be forwarded into particular menus etc. Color of the Icons can be changed upon Host status. Read more in Zabbix documentation.

[5] https://mapserver.mapy.cz/turist-m/%7bz%7d-%7bx%7d-%7by%7d

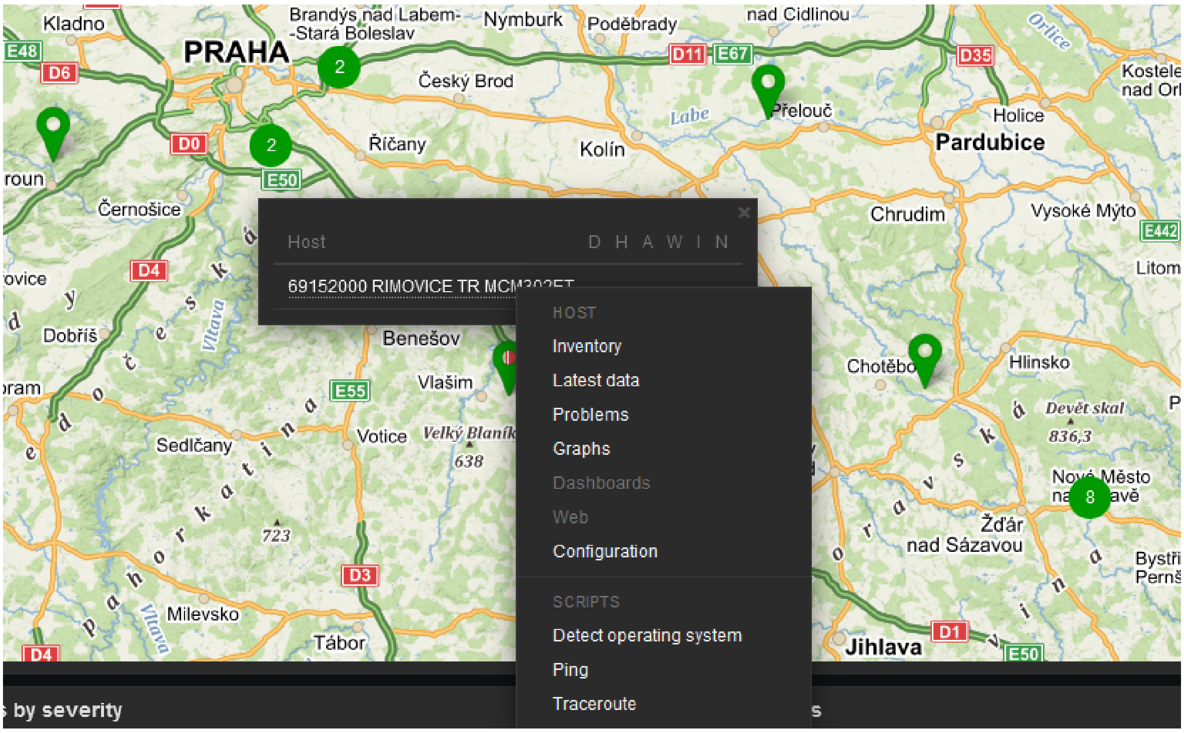


Fig. 3.9: Geographical map host details

3.3.3. Links from Zabbix to RipEX2 GUI

Units’ GUI can be accessed from Zabbix web interface from multiple menus.

A typical one is from simple maps. Configure the URL within the Host on the map and once you click on the Host in this map afterwards, you can be forwarded there. Keep in mind it is not possible from geographical maps.

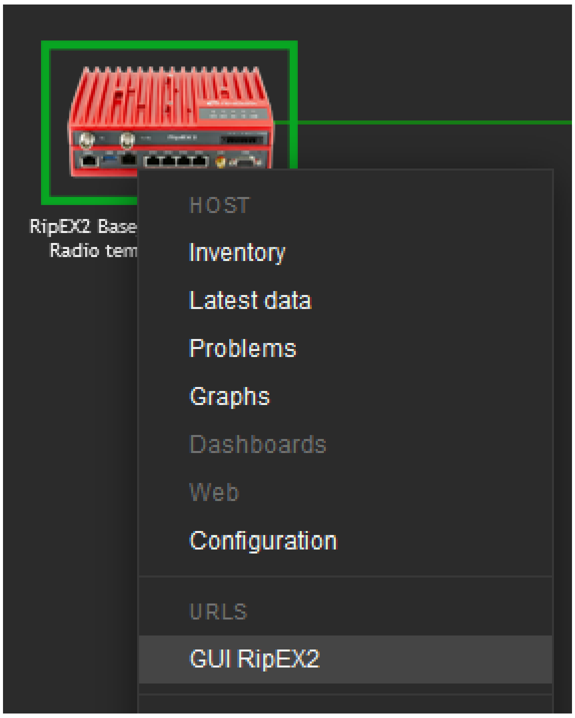
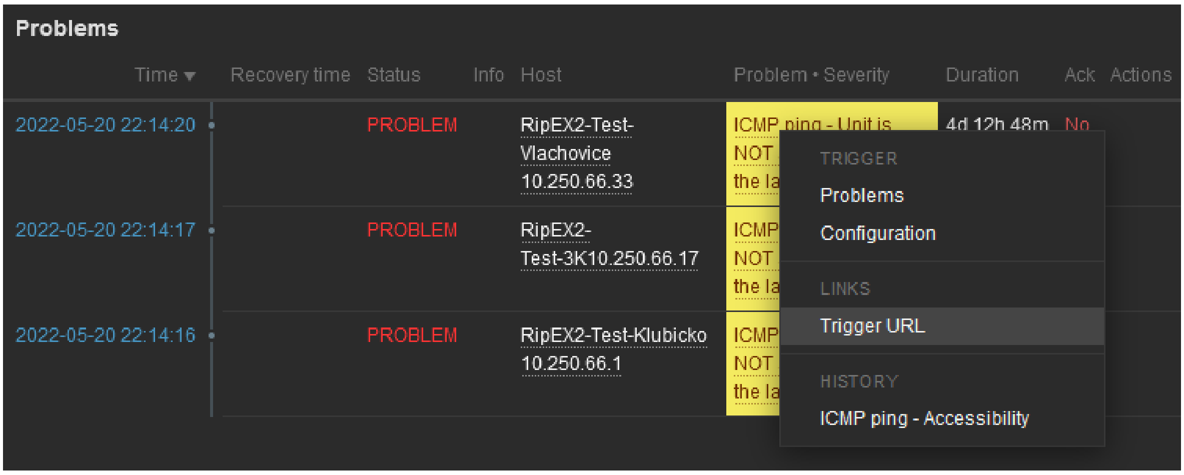


Fig. 3.10: URL link – maps

Another way is a link from Triggers so that if a Problem occurs, you can quickly go to the required web interface.

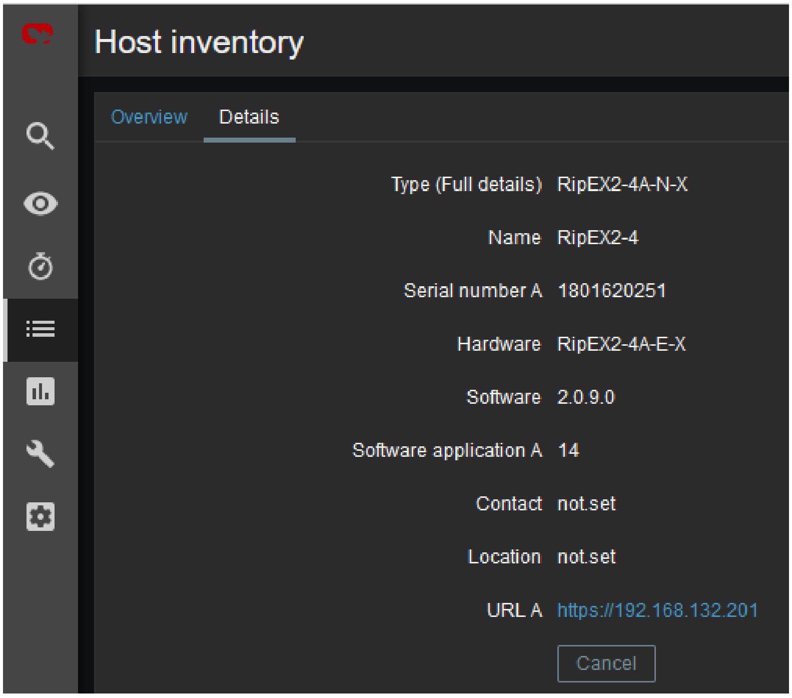


Problems

Time ▾	Recovery time	Status	Info	Host	Problem • Severity	Duration	Ack	Actions
2022-05-20 22:14:20		PROBLEM		RipEX2-Test-Vlachovice 10.250.66.33	ICMP ping - Unit is NOT the la	4d 12h 48m	No	
2022-05-20 22:14:17		PROBLEM		RipEX2-Test-3K10.250.66.17	ICMP NOT the la			
2022-05-20 22:14:16		PROBLEM		RipEX2-Test-Klubicko 10.250.66.1	ICMP NOT the la			

Fig. 3.11: URL link – triggers

The third option is to use Inventory for configuring URL. For every Host, you can enable the Inventory (serial number, OS, host type, ...). Within many Inventory options, the URL can be defined.



Host inventory

Type (Full details)	RipEX2-4A-N-X
Name	RipEX2-4
Serial number A	1801620251
Hardware	RipEX2-4A-E-X
Software	2.0.9.0
Software application A	14
Contact	not set
Location	not set
URL A	https://192.168.132.201

Fig. 3.12: URL link – Inventory

3.3.4. Scheduled Reports

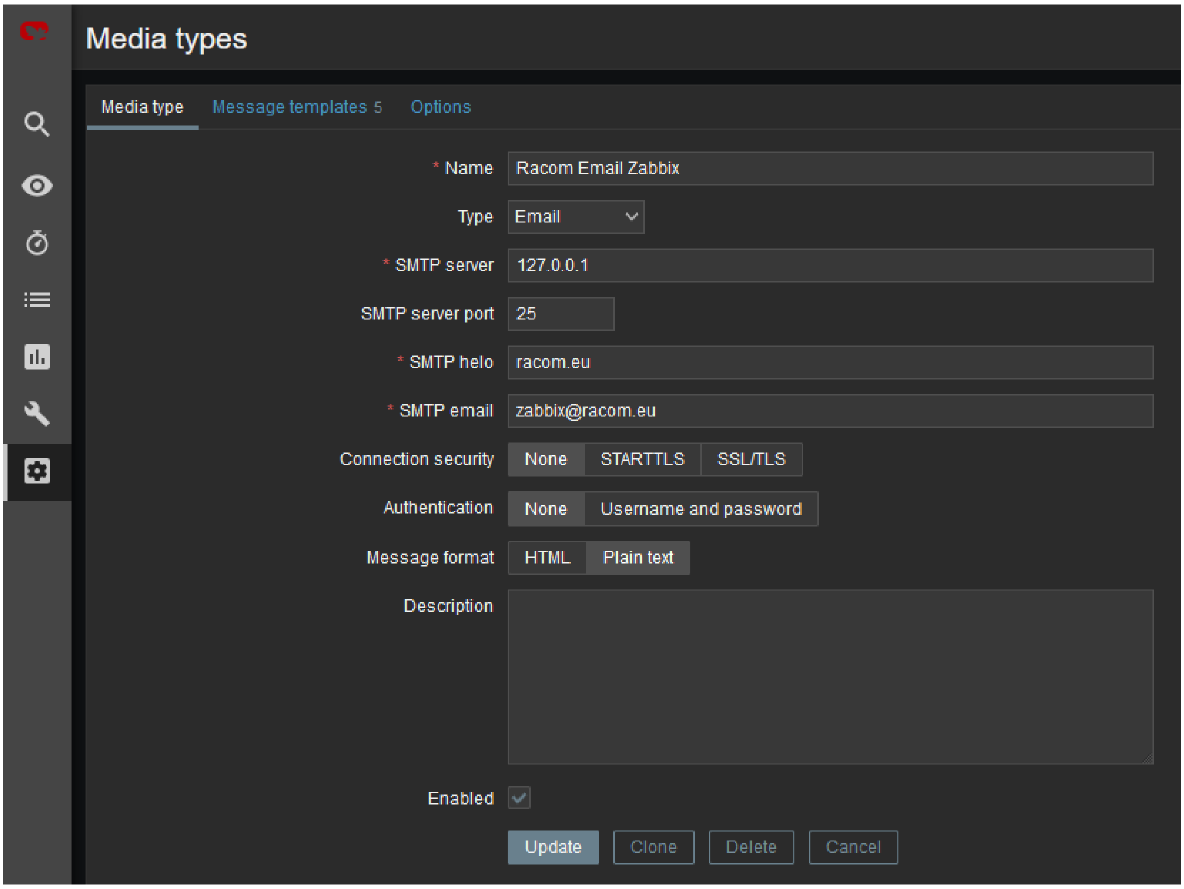
Another useful feature is generating scheduled reports. You need to configure Scheduled reports in general. Once you have it, go to the Report – Scheduled reports menu and create a new one. Basically, Zabbix can send multiple users in regular intervals its Dashboard(s) as PDF.

More information e.g., here:
https://www.zabbix.com/documentation/current/en/manual/config/reports#configuration

3.3.5. Actions, Email notifications

In case of any issue within your network, e.g., drop in the signal quality, or the unit being unreachable, Zabbix can automatically send an e-mail to predefined e-mail addresses. See the following example for your reference, but customize it to suit your needs.

The e-mail can be set in the Administration – Media Types menu. Edit the E-mail type corresponding to your server settings. In our example, we use our own SMTP server reachable from Zabbix server. No special security or password is required. You should be able to use any SMTP server.



* Name: Racom Email Zabbix

Type: Email

* SMTP server: 127.0.0.1

SMTP server port: 25

* SMTP helo: racom.eu

* SMTP email: zabbix@racom.eu

Connection security: [✓ None] STARTTLS SSL/TLS

Authentication: [✓ None] Username and password

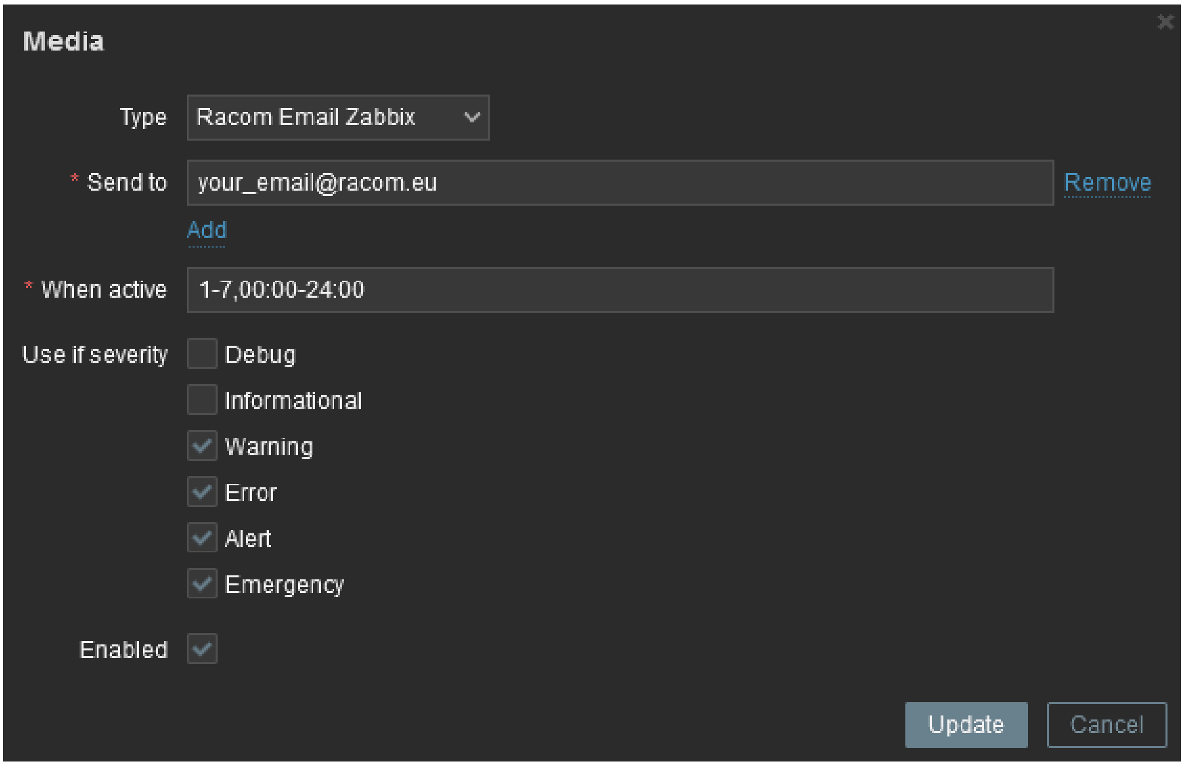
Message format: HTML [✓ Plain text]

Description:

Enabled: ☑

Fig. 3.13: Zabbix Media type – Email

The e-mails are sent to the users’ e-mail addresses. Go to the Administration – Users menu and configure the required e-mail addresses within the user’s details (Media).



Media

Type: Racom Email Zabbix

* Send to: your_email@racom.eu

* When active: 1-7,00:00-24:00

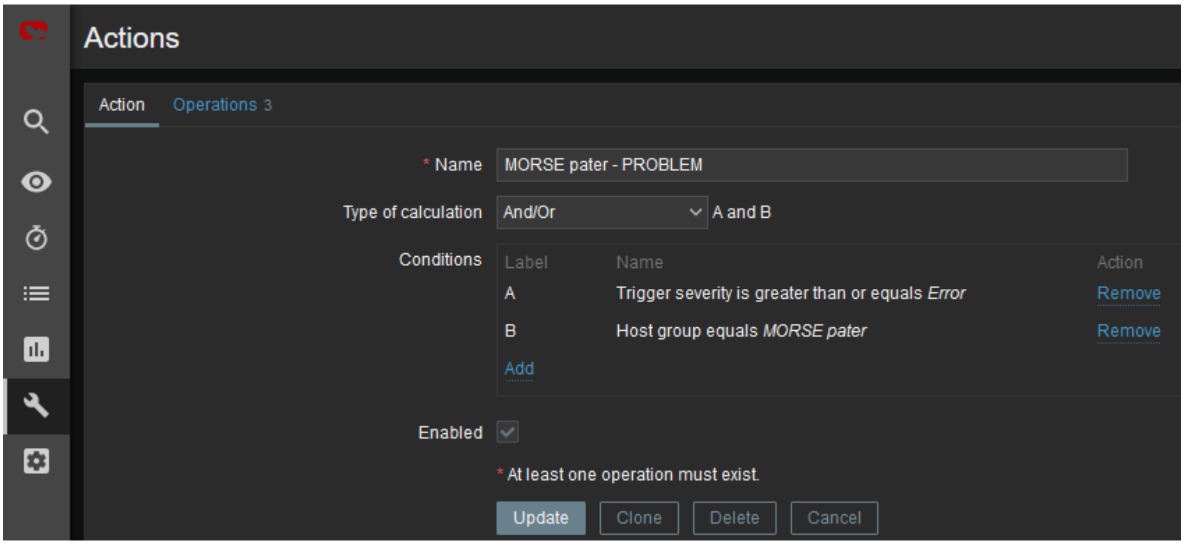
Use if severity:
- □ Debug
- □ Informational
- ☑ Warning
- ☑ Error
- ☑ Alert
- ☑ Emergency

Enabled: ☑

Fig. 3.14: User’s e-mail

You define the time when the e-mail will be sent (e.g., do not send it over the night) and the severity of the issue (e.g., send me the e-mail just in case of a critical issue).

The last step is to configure the action – configure which issue causes the e-mail to be sent. Go to the Configuration – Actions – Trigger actions menu and create a new Action. Set a Name of the Action and its Conditions – trigger severities and host group are used within the screenshot below.



Actions

* Name: MORSE pater - PROBLEM

Type of calculation: And/Or A and B

Conditions:

Label	Name	Action
A	Trigger severity is greater than or equals *Error*	Remove
B	Host group equals *MORSE pater*	Remove

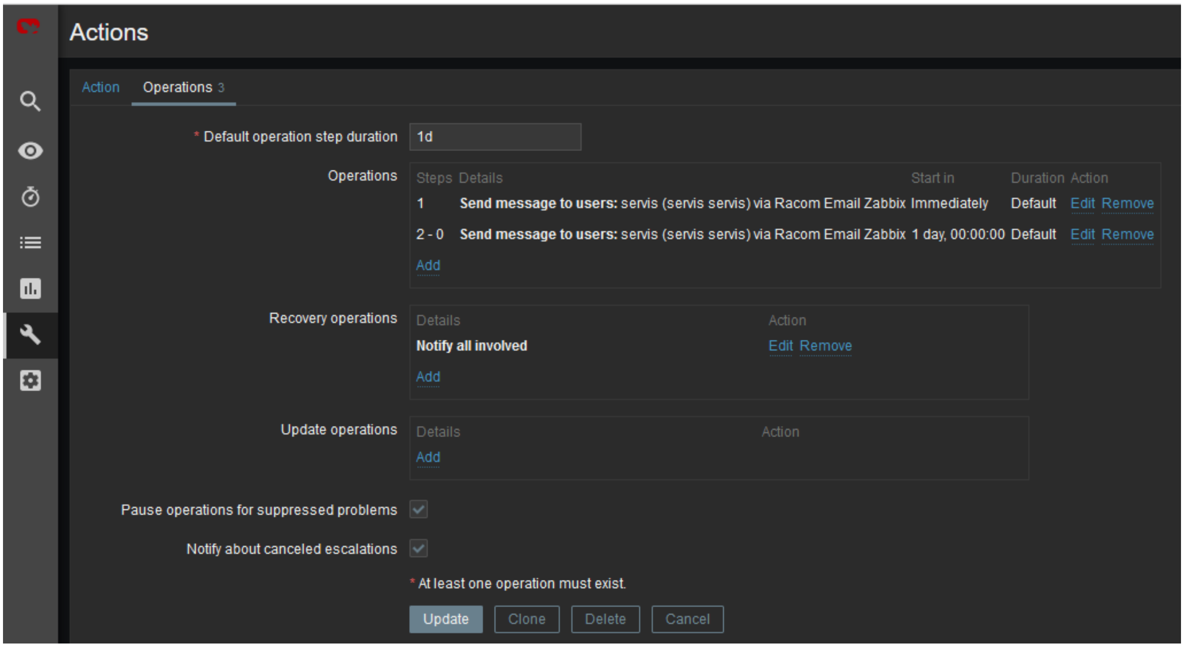
Enabled: ☑

* At least one operation must exist.

Fig. 3.15: Action and its conditions

Within the Operations tab, define one or multiple operations. In the example, once the Problem occurs, Zabbix sends an email. It sends such email every other day until the problem is fixed.

We also send a Recovery email to all involved recipients.



Actions

* Default operation step duration: 1d

Operations

Steps	Details	Start in	Duration	Action
1	**Send message to users:** servis (servis servis) via Racom Email Zabbix	Immediately	Default	Edit Remove
2 - 0	**Send message to users:** servis (servis servis) via Racom Email Zabbix	1 day, 00:00:00	Default	Edit Remove

Add

Recovery operations

Details	Action
Notify all involved	Edit Remove

Add

Update operations

Details	Action

Add

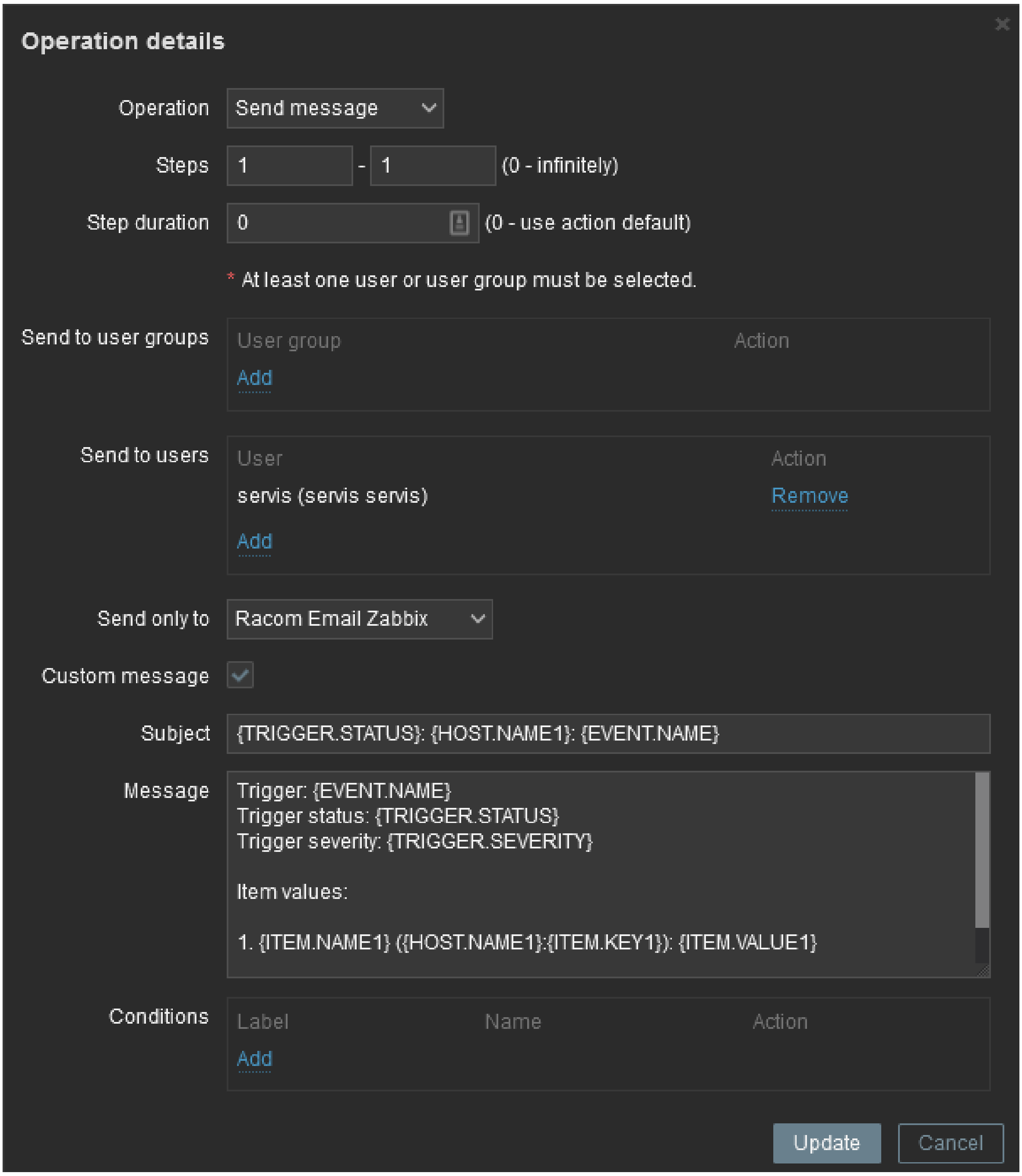
Pause operations for suppressed problems ☑

Notify about canceled escalations ☑

* At least one operation must exist.

Fig. 3.16: Action Operations

Usually, you will use the MACROs for the e-mail body/subject. In this example, the Subject of the email will consist of the host's Name, Trigger status (Problem or OK) and Event Name. Within the body of the message, there can be additional information such as the Trigger Severity, URL and the Issue details.



Operation details

Operation: Send message

Steps: 1 - 1 (0 - infinitely)

Step duration: 0 (0 - use action default)

* At least one user or user group must be selected.

Send to user groups

User group	Action

Send to users

User	Action
servis (servis servis)	Remove

Send only to: Racom Email Zabbix

Custom message: ☑

Subject: {TRIGGER.STATUS}: {HOST.NAME1}: {EVENT.NAME}

Message:

```
Trigger: {EVENT.NAME}
Trigger status: {TRIGGER.STATUS}
Trigger severity: {TRIGGER.SEVERITY}

Item values:

1. {ITEM.NAME1} ({HOST.NAME1}:{ITEM.KEY1}): {ITEM.VALUE1}
```

Conditions

Label	Name	Action

Fig. 3.17: Action Operations details

3.3.6. Branding

Zabbix 6.0 LTS offers you to use your own company's branding instead of Zabbix ones, or RACOM logos in case of using RZA6.

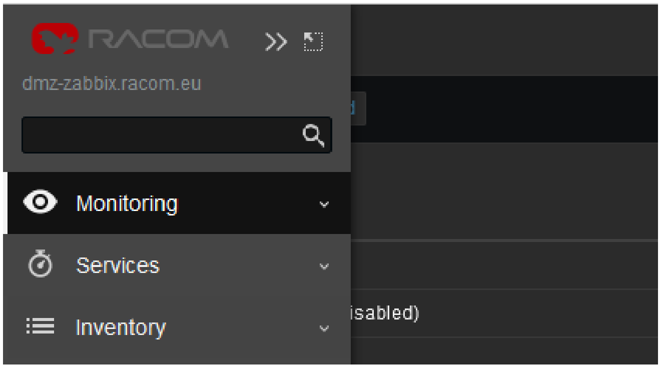


Fig. 3.18: RACOM Branding

General and brief procedure is described here:
https://www.zabbix.com/documentation/current/en/manual/web_interface/rebranding

For the RZA6, we created a file /usr/share/zabbix/local/conf/brand.conf.php with this content:

```
<?php
return [
'BRAND_LOGO' => 'racom/racom_logo.png',
'BRAND_LOGO_SIDEBAR' => 'racom/racom_logo.png',
'BRAND_LOGO_SIDEBAR_COMPACT' => 'racom/racom_logo_compact.png',
#'BRAND_HELP_URL' => 'https://www.racom.eu/ APP NOTE LINK '
];
```

Logos were scaled to 140x20 and 20x13 (compact one). The logos are placed in /usr/share/zabbix/racom/ directory. After these changes, the Login screen can look like:

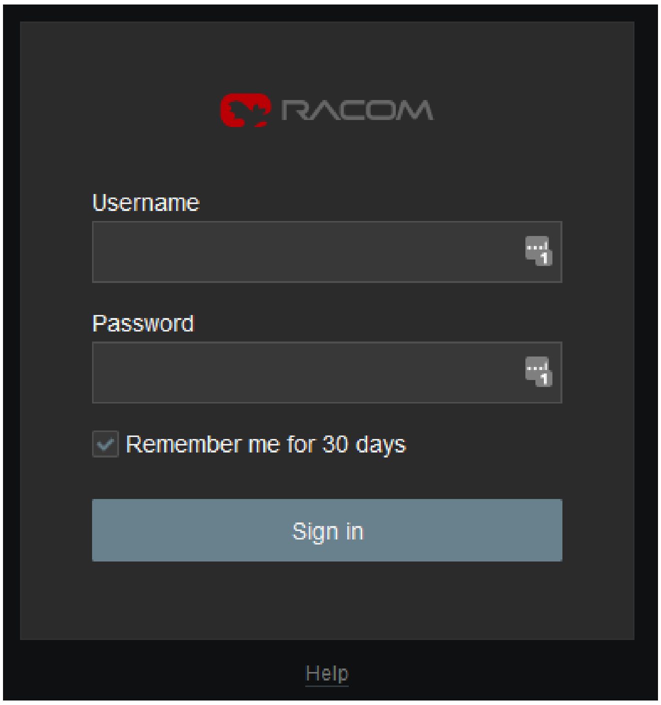


Fig. 3.19: RACOM Branding login page

If you need any additional help or information, don’t hesitate to contact us at *support@racom.eu*[6]. We are ready and happy to help you.

We do recommend using our RZA6 solution. If not in your real network, then as a start for getting familiar with RipEX2 SNMP and Zabbix NMS, because RZA6 has many configuration steps pre-configured and done.

[6] mailto:support@racom.eu

Revision History

Revision 1.0 2022-06-16

First issue, RipEX2 FW 2.0.10.0, Zabbix 6.0 LTS