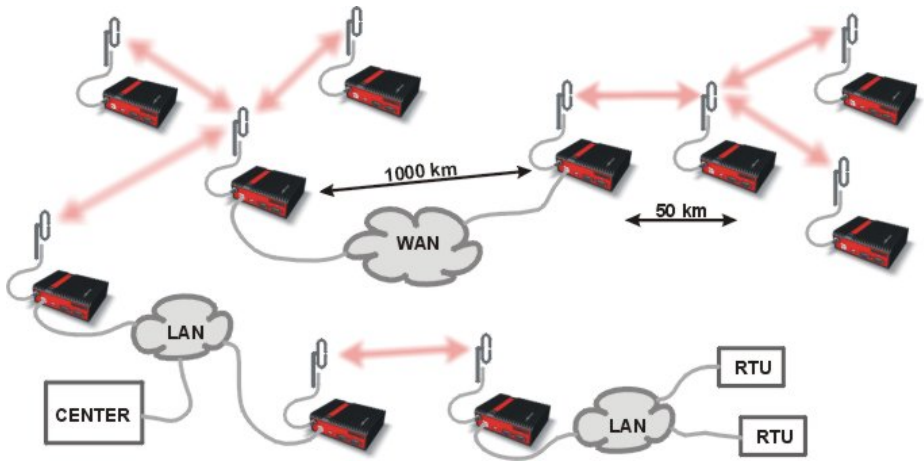
RACOM
RADIO DATA NETWORKS

Application notes



RipEX
SNMP

version 1.3
08/02/2022

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

1. 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 (RipEX alarm management). RipEX is capable of sending SNMP traps/informs to up to three SNMP managers.

1.2. SNMP communication

In SNMP, each value is uniquely identified using Object Identifier (OID). Standard communication starts by sending a request and then the response is returned. Alternatively, an agent can send an SNMP trap or inform (acknowledged trap).

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 privacy. The manager is required to know an authentication and 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 RipEX).

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	stationName
OID	.1.3.6.1.4.1.33555.2.1.1.1
MIB	RIPEX
Syntax	DisplayString (OCTET STRING) (SIZE(0..64))
Access	read-only
Status	current
DefVal	
Indexes	
Descr	Station Name.

As you can see, numbers 1.3.6.1.4.1.33555 are the “higher-level” OIDs. The “lower-level” OIDs are .2.1.1.1 which are allocated by RACOM.

2. Simple Network Management Protocol in RipEX

SNMPv1&v2c and v3 are supported by RipEX. 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).

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

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 (DES, AES) and Authentication (MD5, SHA) methods.

When using SNMP over radio channel, we recommend setting RipEX 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. RipEX proprietary MIB

MIB can be read via any text editor, but it might be better to browse it (see the notification’s variable bindings, OID’s unit, descriptions, OID tree, getting values from RipEX units, receiving and testing notifications, etc.) in some special SNMP browser such as MIBBrowser from iReasoning. The following section explains some details about RipEX MIB for firmware version 1.9.7.0. MIB consists of “revision history” information so you can quickly find out what has been changed.

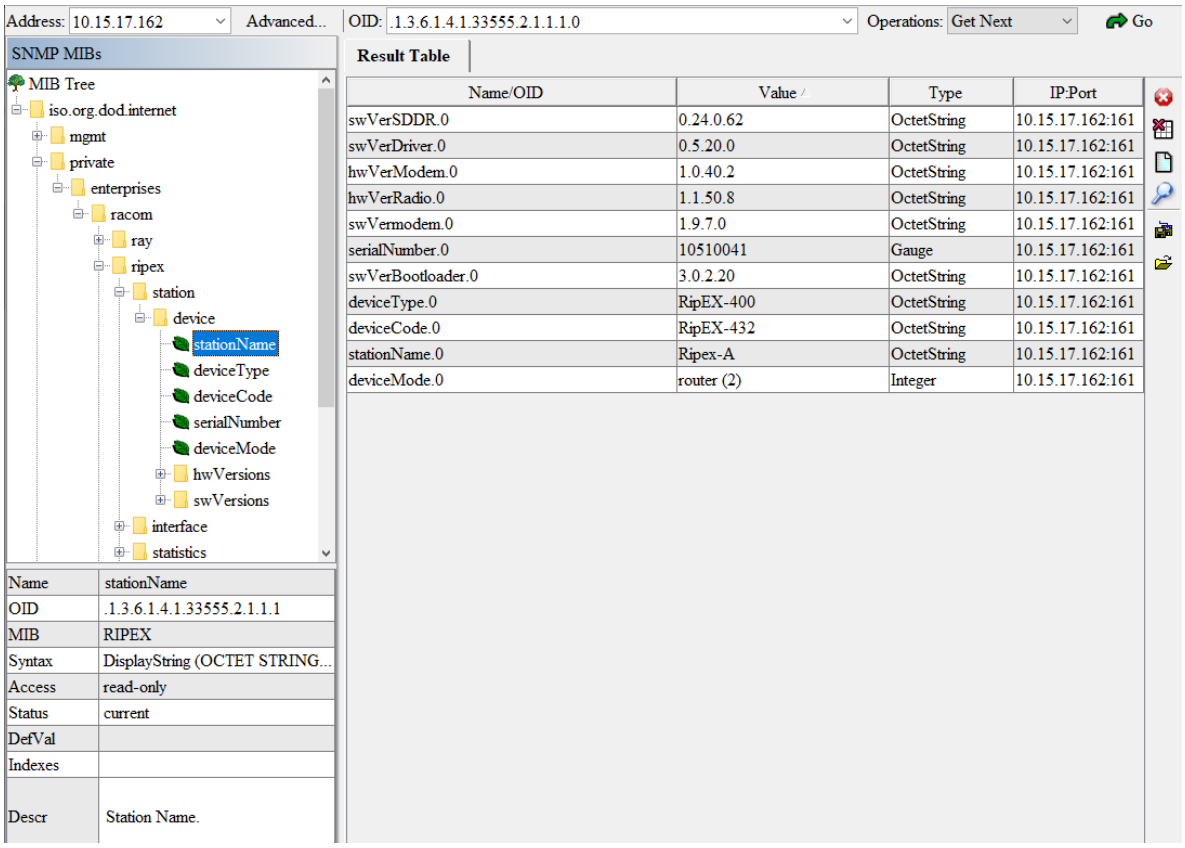


Fig. 2.1: MIB Browser example

Note

CSV file containing all proprietary RipEX OIDs can be sent upon request, or exported from MIBBrowser software.

The RipEX MIB module complies with the Severity level 3 validation.

Supported MIBs and its OIDs:

- Values from general MIBs such as SNMPv2-MIB, IF-MIB, IP-MIB, ...
- Proprietary MIB - RACOM-RipEX
  - Reading configuration parameters
  - Reading operation statistics (interfaces, …)
  - Backup routes status
  - Local and Remote watched values
  - Sending traps/informs (thresholds are configurable)

RipEX MIB utilizes custom types declaration so that SNMP reply is numeric, but each number corresponds to a particular meaning. E.g., Alarm states:

- -1 unknown
- 0 inactive
- 1 active

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., temperature returned as 39500 means 39.5. 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*[1] together with Zabbix templates.

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 RipEX 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 RipEX with one neighbouring unit can be approximately 48 kilobytes using SNMPv2. With encrypted and authenticated SNMPv3, this data volume can be doubled.

Note

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

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 RipEX 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. Bandwidth Efficiency Tip – Remote watched values

If you wish to monitor many watched values (VSWR, Temperature, UCC, …) from remote stations connected over the radio channel and you have a star topology network, you can improve bandwidth efficiency by reading OID values only from the Master (Repeater) RipEX station.

The advantage of the above is that the watched values from remote stations are broadcast in regular intervals (by default, 2 hours) and saved in the Master (Repeater) RipEX. These values from neighbouring stations have their own OID's and can be downloaded from the Master (Repeater) RipEX.

In the picture below – Master RipEX station periodically obtains watched values from its neighbouring Slave stations. Whenever the NMS requests any value mentioned, the reply is sent only from the Master station (over Ethernet) saving radio bandwidth. SNMP uses radio link only for sending SNMP Traps from any Slave to the NMS.

[1] https://www.racom.eu/eng/products/radio-modem-ripex.html#dnl_fwr1

Note

The diagram is simplified - there are no flows for SNMPv3 PDUs, neither Inform's Acknowledgments.

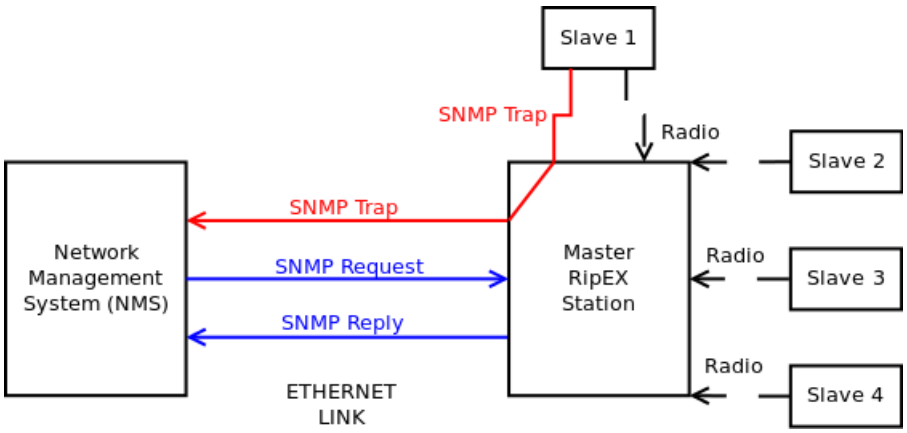


Fig. 2.2: NMS communication with Slave stations

Note

In such a case, watched values from neighbouring stations are displayed as part of the Master (Repeater) station.

2.4. Discovery Procedure and Dynamic Indexes

Indexes for remote watched values are dynamic. This is the reason, Zabbix (or another) NMS must utilize dynamic indexes together with Discovery rules. Discovery rules are also necessary other tables.

Tables requiring Discovery:

Remote watched values

- Average and last radio statistics for each neighbouring unit
  - RSS [dBm], DQ – updated with every received packet (weighted average values based on last several minutes) – e.g., possible NMS update interval can be 5 minutes
  - Temperature [°C], RF power [W], TX lost [%], Voltage [V], VSWR – updated every 2 hours by default
- Neighbouring IP address and total number of heard packets

Statistics – Radio

- Neighbouring IP address
- Packet and Byte counters – RX and TX
- Data error, duplicate, lost, rejected, repeated counters

Backup paths

- Peer IP and symbolic name
- Alternative path – currently used gateway and its priority and state

Typical mechanism in static RipEX 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. 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.

It is more difficult with remote watched values, because the order and thus, indexes, can vary every “log save period” set in RipEX (24 hours by default). You need to run the discovery rule on regular basis so that watched values are not mixed within multiple neighbouring units.

Dynamic indexes are used to match a particular neighbour IP address and use a correct index afterwards. This is implemented in Zabbix NMS and a solution can differ in other NMS.

2.5. RipEX SNMP Settings

Basic SNMP parameters are described in *RipEX user manual*[2] and can be configured in SETTINGS – Device – SNMP menu. The following section highlights some important parameters or explains something in more details.

Fig. 2.3: RipEX SNMP menu

Make sure that your NMS supports Authentication and Encryption algorithms you choose in RipEX.

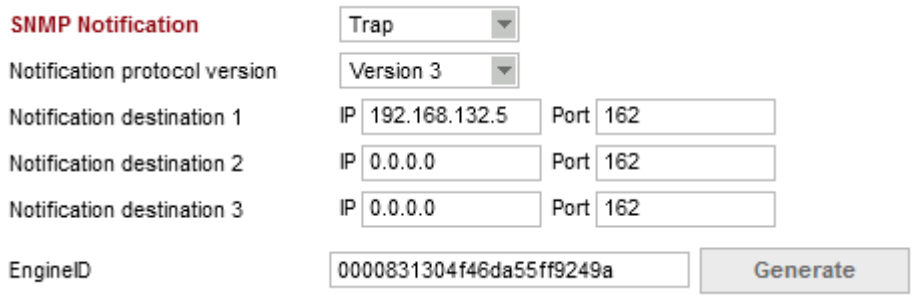


Fig. 2.4: RipEX Notification menu

[2] https://www.racom.eu/eng/products/m/ripex/h-menu.html#snmp-menu

Another not very common option is “**Engine ID**”. This option is valid for SNMPv3 notifications only. This Engine ID for notifications conforms to RFC1910.

Example of generated Engine ID for SNMPv3 notifications: 80 008313 04 f46da55ff9249a

- 80 – engine ID must start with standard identification
- 008313 – enterprise OID – 33555 – RACOM s.r.o.
- 04 – Engine ID is assembled according to user defined string
- f4 6d a5 5f f9 24 9a – HEX string from configuration

The differentiated part of the Engine ID can be entered as HEX characters or generated.

Note

Every SNMPv3 enabled device within a network must have a unique Engine ID. This message ID used for SNMPv3 requests and replies is not configurable, conforms to RFC3411, and it is dynamically chosen (does not depend on any ETH MAC address).

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 (not the one for SNMPv3 notifications).

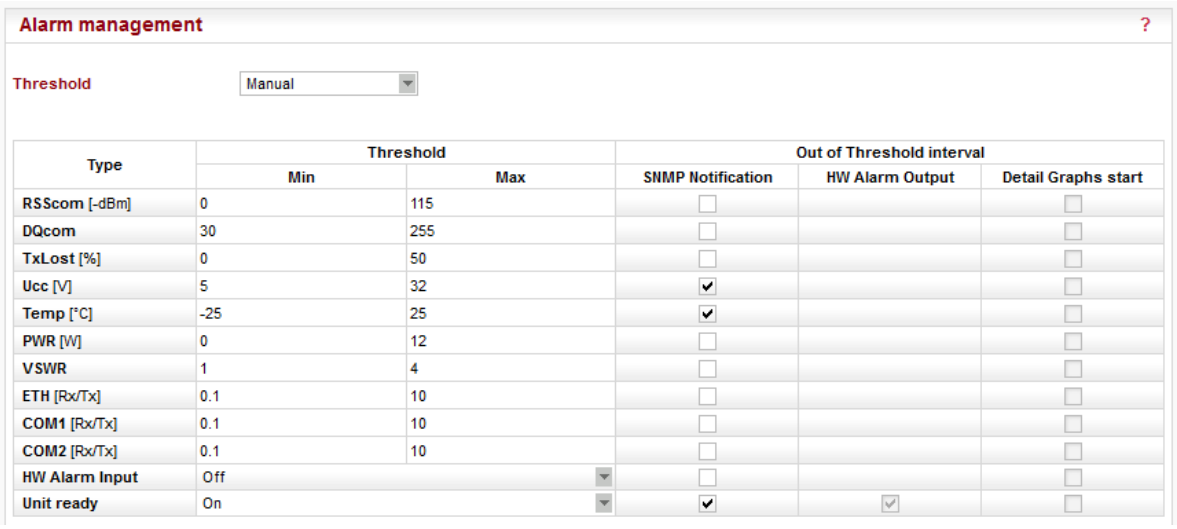


Fig. 2.5: RipEX Alarm management

Notifications are being sent based on Alarm Management setup. Select Type of Event for which you want notifications to be sent in SETTINGS – Device – Alarm management menu. Check the particular check-box “SNMP notification”.

Thresholds are fully configurable.

The traps/informs are sent whenever any of the following watched values are beyond their threshold ranges and whenever the value falls back within the corresponding range. Each trap can either be in the alarm state or in the OK state.

- RSS (Received Signal Strength) – one general threshold for all neighbours
- DQ (Data Quality) – one general threshold for all neighbours
- TX Lost [%] (The probability of a transmitted frame being lost)
- UCC (Power voltage [V])
- Temperature [C]

- RF Power [W]
- VSWR (Voltage Standing Wave Ratio, 1.0 = the best ratio, 1.0 – 1.8 = acceptable ratio, > 2.5 = indicates a serious problem in antenna or feeder)
- Ethernet RX/TX Packets ratio (Ratio between received and sent packets over Ethernet)
- COM1/2 RX/TX Packets ratio (Ratio between received and sent packets over COM ports)
- HW Alarm input
- Hot-Standby (SNMP trap containing active station identity – sent by the active station)
- Backup paths system (Backup path state and Alternative path state changes)
- Unit ready (the hardware alarm output or the SNMP trap indicates that the RipEX radio is ready to operate)
- Nomadic remote device is offline (A notification to indicate that Nomadic remote device is offline/online; i.e., status of connection to Nomadic base)

Note

Watched values broadcasting period can be set in Settings – Device - Neighbours&Statistics menu. If you set it to 0, you completely disable remote watched values. Feel free to change it as required, but keep in mind that setting this value too low might send too much of broadcast traffic to the radio channel. Setting this value too high might result in situation in which remote watched values are not useful.

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 RipEX 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. If you have older Zabbix releases, check the *RipEX Archive download section*[2] for previous versions of this application note.

Take the opportunity to remotely access and test a live *Zabbix demo*[3]. See the credentials within the text on the given link.

3.1. Installation and Documentation

Follow the *Zabbix documentation*[4], 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 RipEX (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 *RACOM support*[5] 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/radio-modem-ripex.html#dnl_archive
[3] https://www.racom.eu/eng/products/m/ripex/demo/zabbix.html
[4] https://www.zabbix.com/documentation/current/en/manual
[5] 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
- sshpass

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*[6] for more details.

For RACOM products, multiple steps are required. Upload all the MIBs from respective devices (RipEX 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
```

3.1.1.1. Templates

Download RipEX Zabbix 6.0 template from *RACOM website*[7]. Unzip the file and import zbx_export_ripex.yaml into your Zabbix instance in Configuration -> Templates menu via web interface. The template consists of:

- approximately 300 Item values (~ 20 tags) which can be read from RipEX units (proprietary OIDs only – i.e., OID starting with 1.3.6.1.4.1.33555.2 prefix). For other general OIDs, use Zabbix predefined templates or do your own templates (e.g., SNMPv2-MIB::sysDescr.0, SNMPv2-MIB::sysName.0, …)
  - RFC1213 and RS232 OIDs are included
- Discovery rules
  - For the 1.9.7.0 firmware, there are 3 Discovery rules

[6] https://www.zabbix.com/documentation/current/en/manual/appendix/install/web_service
[7] https://www.racom.eu/eng/products/radio-modem-ripex.html#dnl_fwr1

  - We use Discovery rules for RipEX radio statistics, remote watched values and backup routes, because these tables consist of individual lines where each line is e.g., another RipEX unit, another alternative path or TX lost counter, 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, except:
  - Modem temperature (°C), RF power (W), TX lost (%), UCC (V) and VSWR (updated every 30 minutes)
  - Other update times: 30 minutes, 1 hour and 1 day
- All Discovery rules are disabled as well
  - Update times can vary from 5 minutes to 2 hours
  - By default, each discovery rule is run every 8 hours

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 RipEX 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 RipEX 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.log
StartSNMPTrapper=1
```

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.

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.

Generate, copy&paste or manually configure RipEX EngineID. This was explained in *Section 2.5, "RipEX SNMP Settings"*.

Note

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

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

3.1.1.2. RipEX images

Hosts can be displayed in graphs. For such a purpose, we created multiple RipEX 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 RipEX template. Import them one by one in Administration – General – Images menu, or via directly via MySQL.

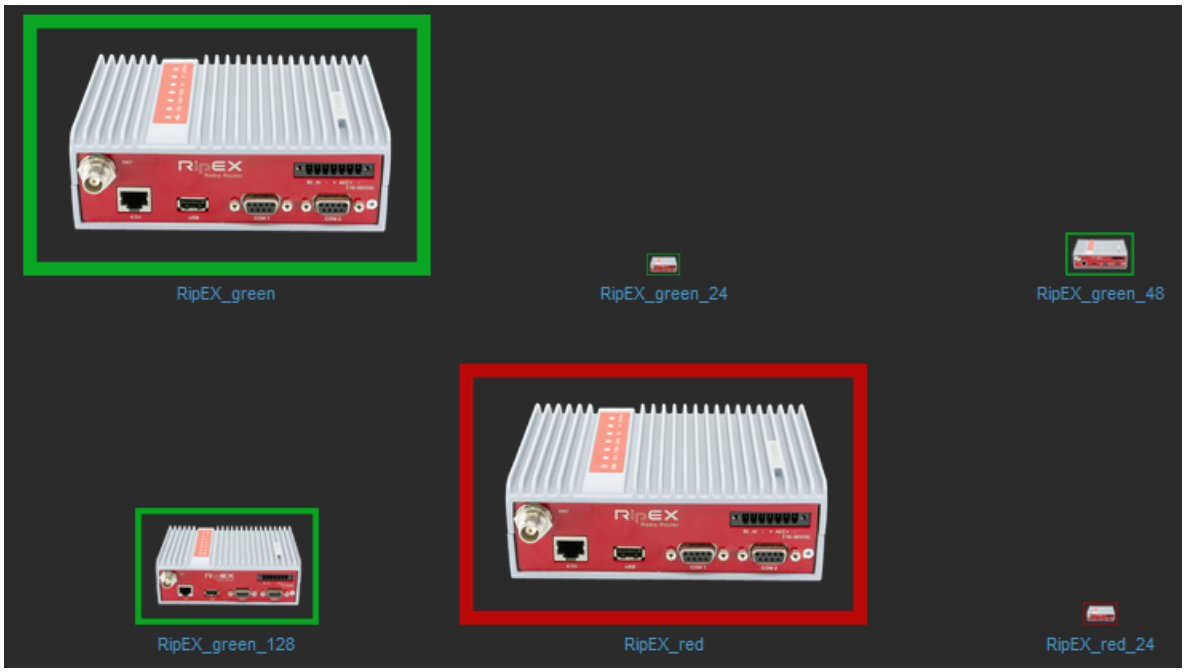


Fig. 3.1: RipEX images in Zabbix

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 RipEX template

Now, Zabbix should be ready for monitoring RipEX 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 RipEX Base station accessible via Ethernet from Zabbix. Go to the Configuration – Hosts menu and click on the “Create host” button on top right corner.

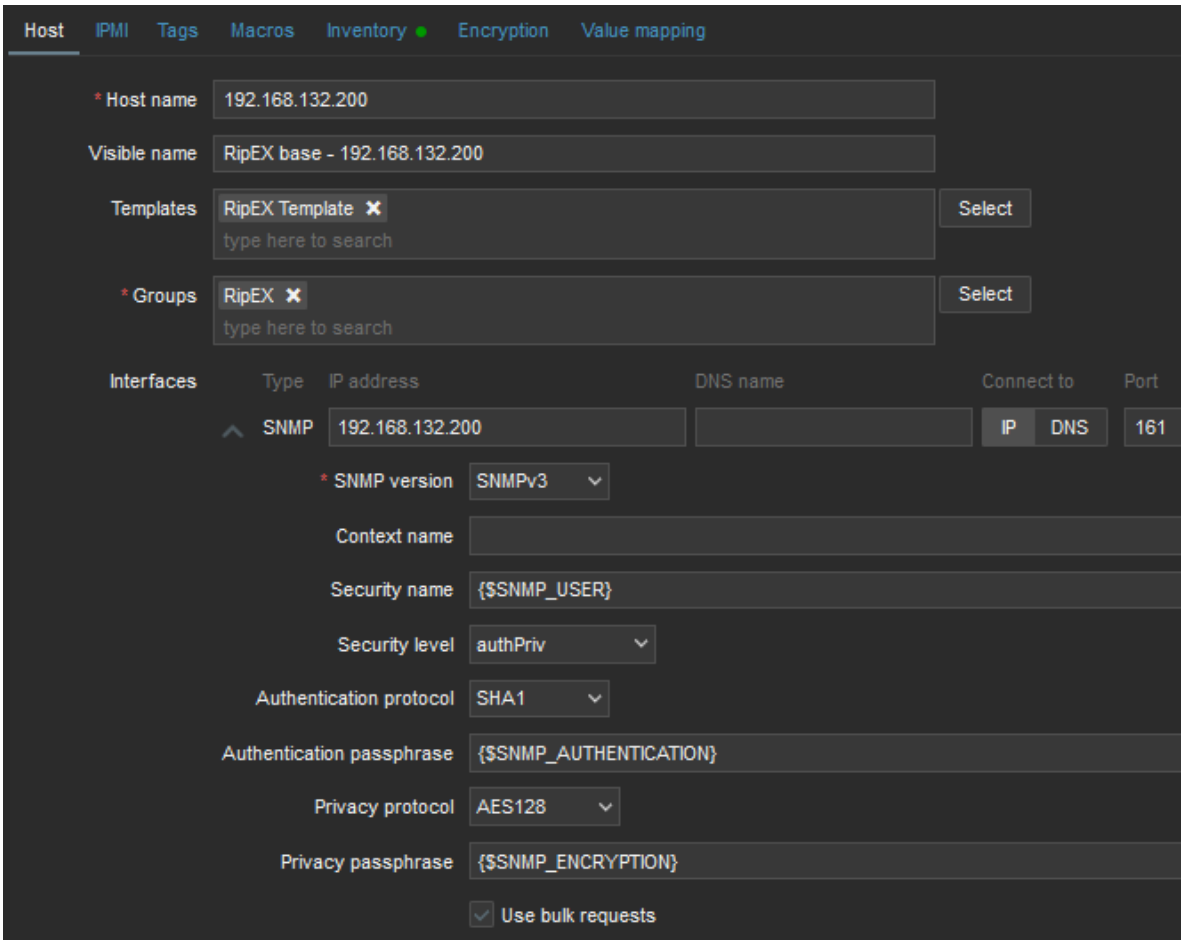


Fig. 3.2: New RipEX host

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 “RipEX Template” so that the unit is preconfigured with all RipEX supported Items. Create a new, or add it to an existing one, RipEX group. You can name it as required – e.g., based on RipEX 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 {$SNMP_COMMUNITY}
  - If v3, set the values according to your RipEX setup
    - Security name - {$SNMP_USER}
    - Authentication passphrase - {$SNMP_AUTHENTICATION}
    - Privacy passphrase - {$SNMP_ENCRYPTION}

- Now, check and change MACROs in “Macros” tab
  - HOST_SSHKEY and HOST_SSHPORT macros are used for RipEX scripts

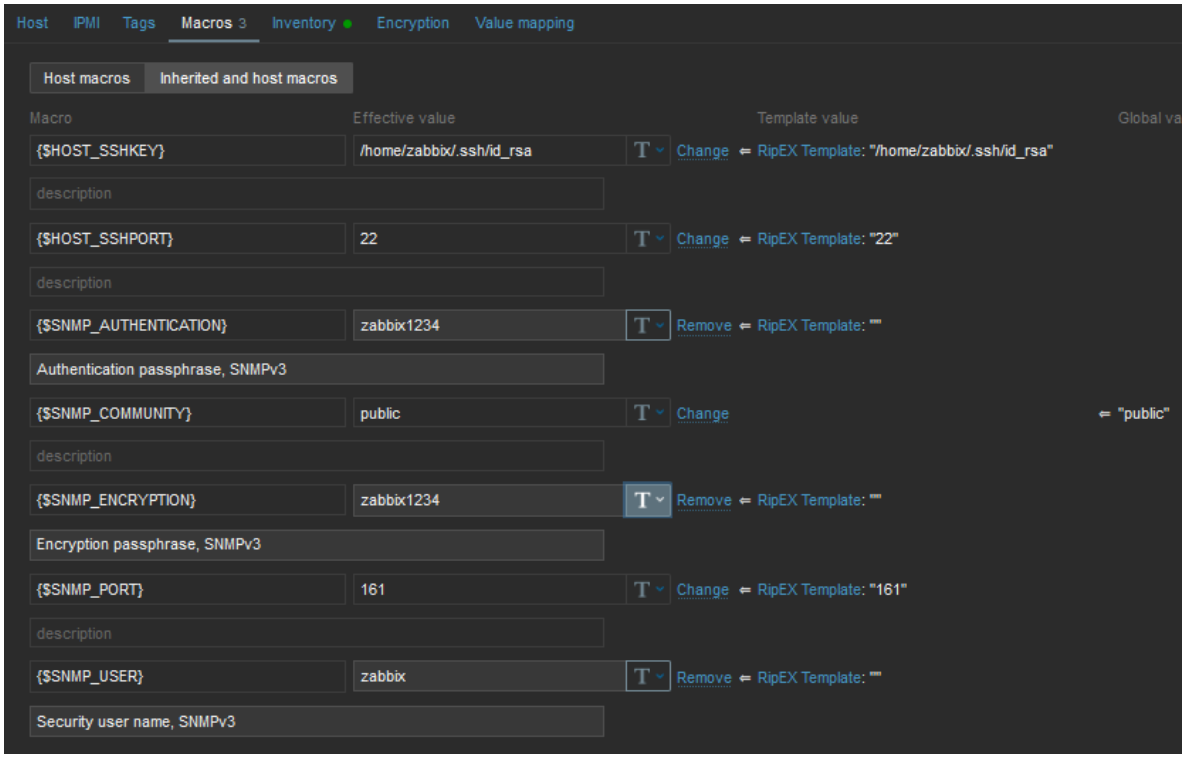


Fig. 3.3: RipEX Host MACROs

You can either change the values in Template so it is the same in all your RipEX 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 RipEX radio network.

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.

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 “TX Lost value out of range” Item, you also need to enable a Trigger for this Item).

RSS and DQ trap items are disabled in the template by default. The reason is that we need to define remote RipEX IP addresses first. See the following example for enabling a DQ trap.

Go to the Zabbix web front-end and select a RipEX host for which you want to process DQ traps. Click on the Items button and find an item with the following key*: trpDqX.Y.Z.W.*

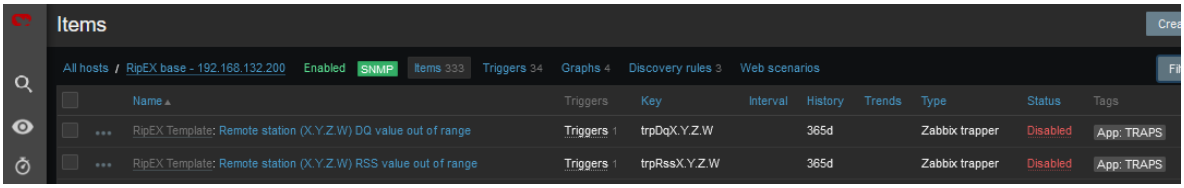


Fig. 3.4: Default RSS and DQ trap items

Click on the item and then click on the Clone button. Now you can edit the item. Replace the "X.Y.Z.W" string in the item Name with the remote RipEX radio IP address (e.g. 10.10.10.2). Do the same in the Key field and select the Enabled option in the Status field. See the following example:

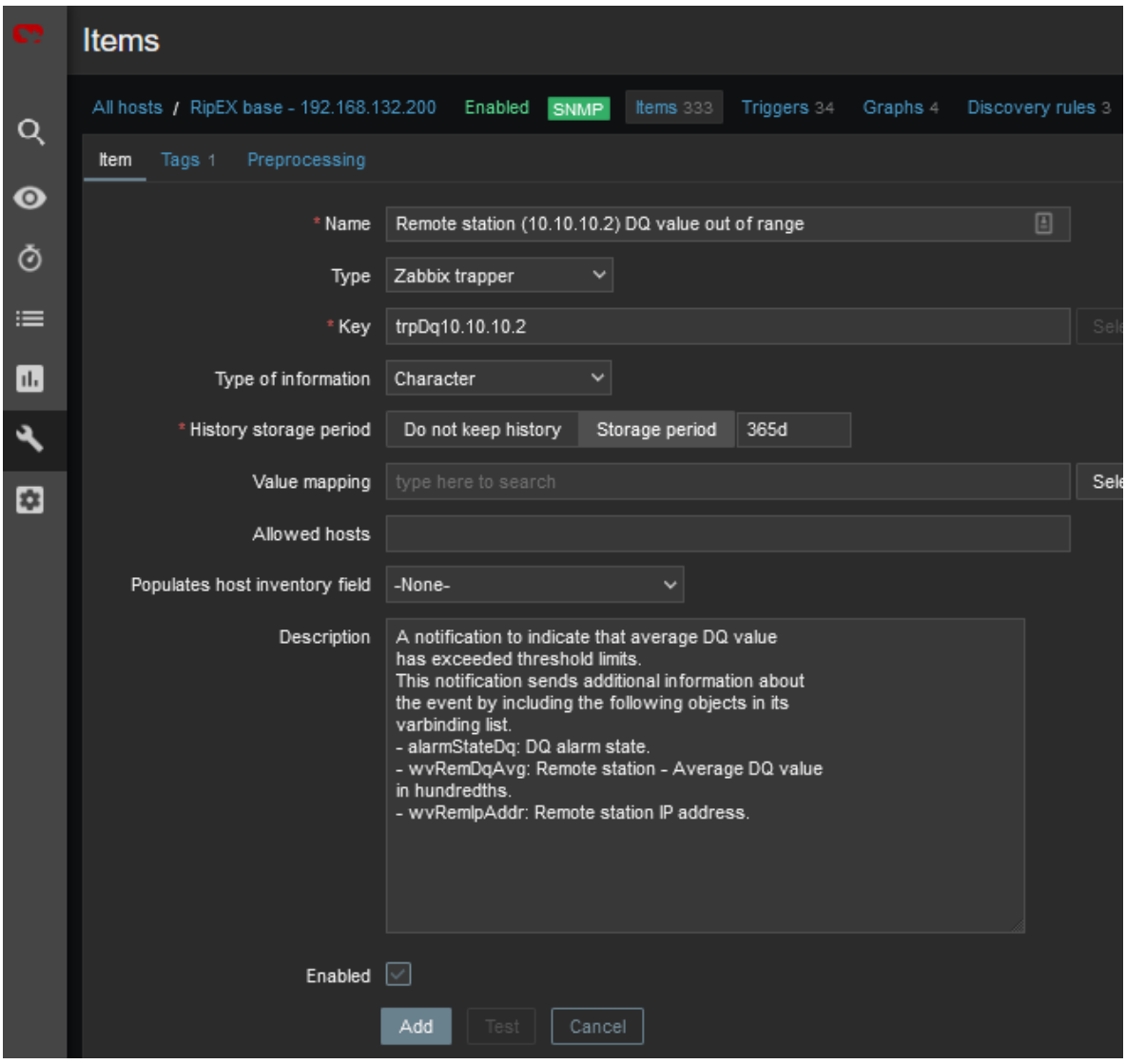


Fig. 3.5: Edited DQ trap item details

Save the changes and open the host Triggers list. Repeat the above steps for the DQ trigger and save the changes. You should see the trigger with the enabled status.

Fig. 3.6: Edited DQ trigger

Follow the same procedure (DQ and RSS) for other remote RipEX units as needed.

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 - Remote watched values” for receiving values from Statistics table containing RSS, DQ, remote VSWR etc. with all neighbouring RipEX 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 RipEX 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 RipEX 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).

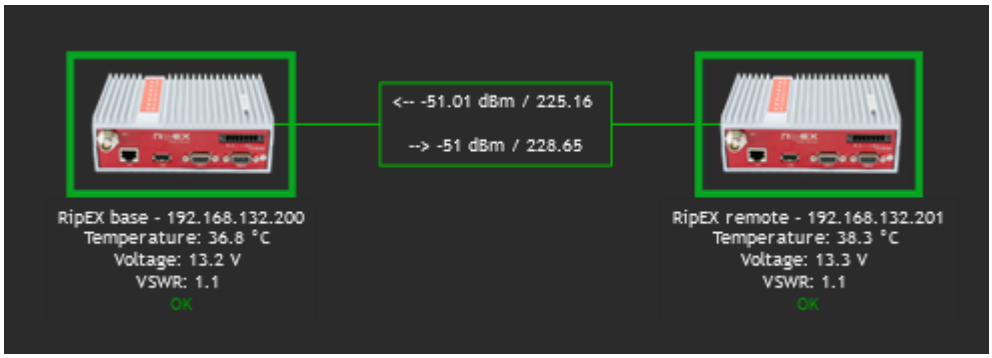


Fig. 3.7: Zabbix simple RipEX map

On the map above, we can see two RipEX units with a displayed name and current Radio temperature, voltage and VSWR. 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/DQ values.

Host details:

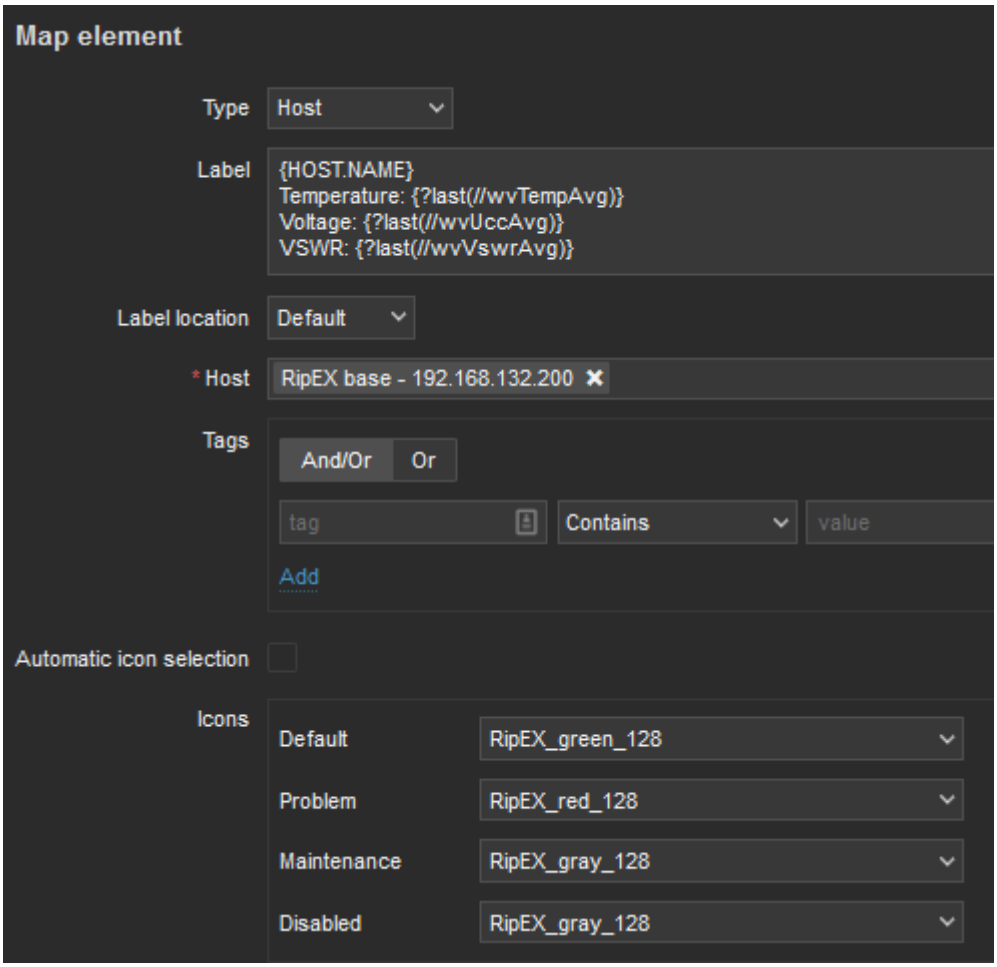


Fig. 3.8: Host details in maps

Label is set as follows:

```
{HOST.NAME}
Temperature: {?last(//wvTempAvg)}
Voltage: {?last(//wvUccAvg)}
VSWR: {?last(//wvVswrAvg)}
```

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

Example of the link Label:

```
<-- {?last(/192.168.132.200/wvRemRssAvg[10.10.10.2])} /
{?last(/192.168.132.200/wvRemDqAvg[10.10.10.2])}

--> {?last(/192.168.132.201/wvRemRssAvg[10.10.10.1])} /
{?last(/192.168.132.201/wvRemDqAvg[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 RipEX hosts, you can display them on geographical maps.

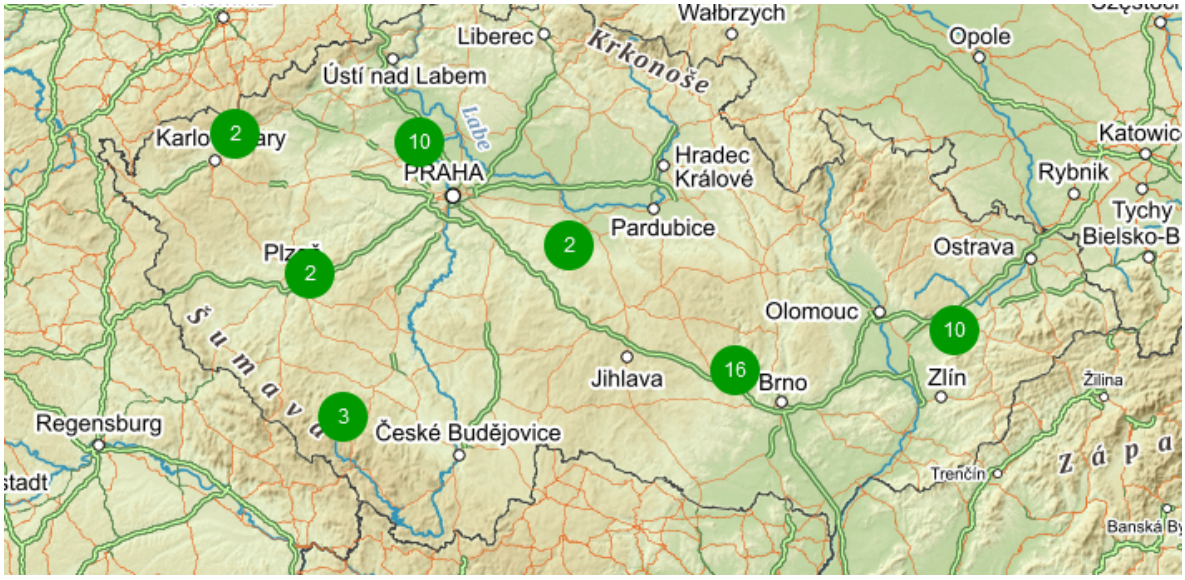


Fig. 3.9: Geographical map

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

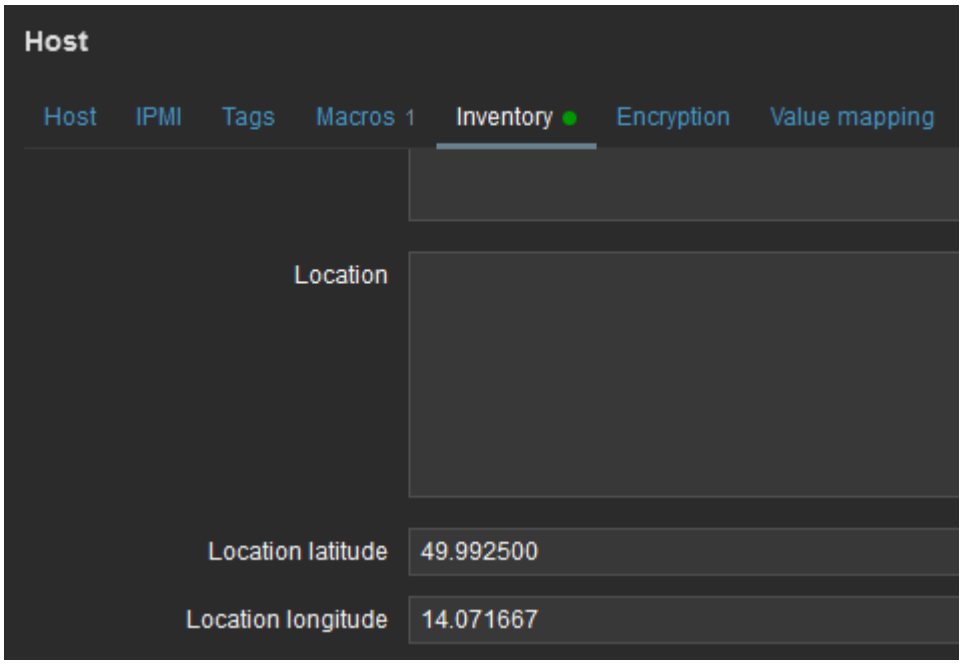


Fig. 3.10: Host GPS coordinates

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.

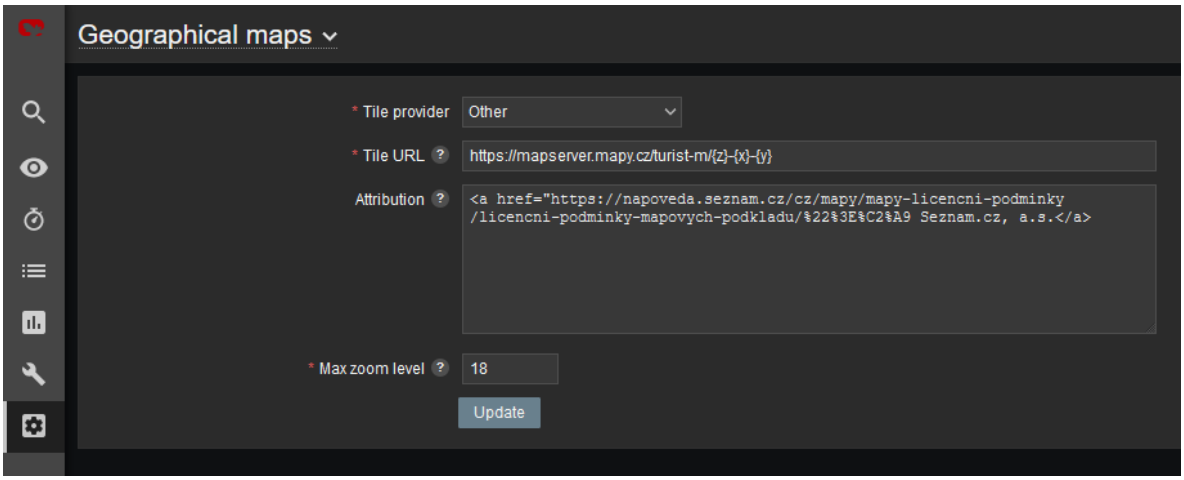


Fig. 3.11: Zabbix Geographical maps

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.
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.

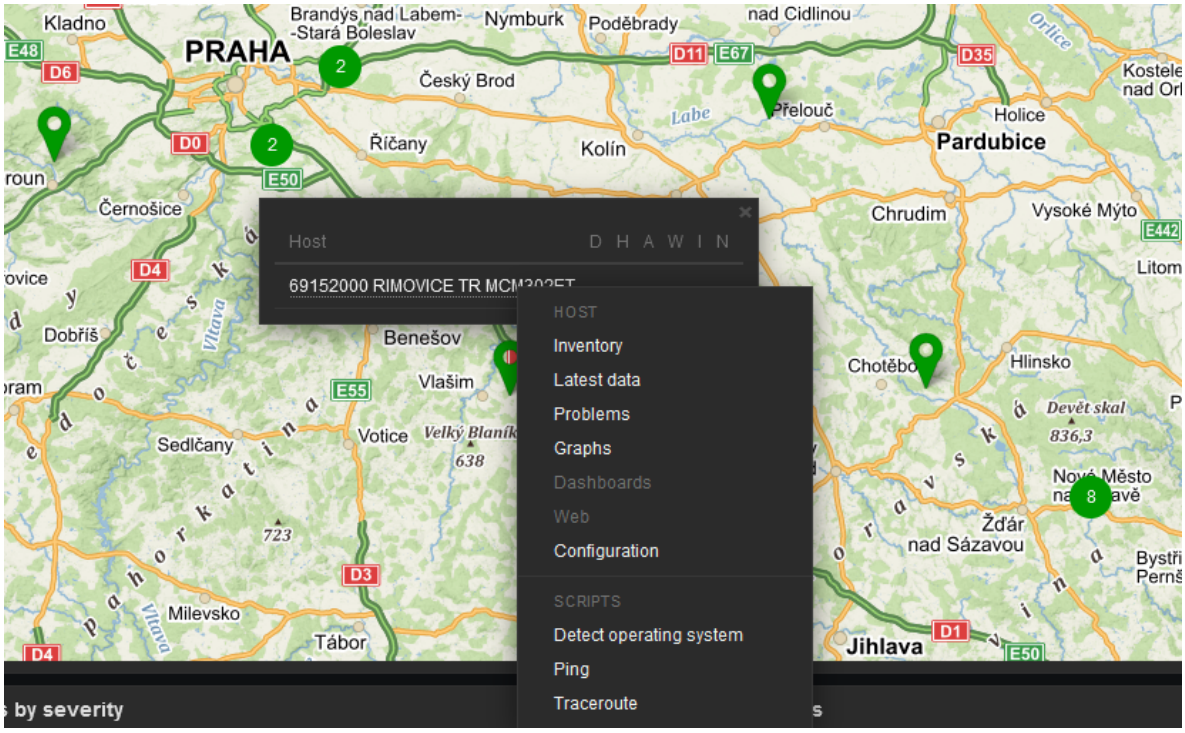


Fig. 3.12: Geographical map host details

3.3.3. Links from Zabbix to RipEX 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.

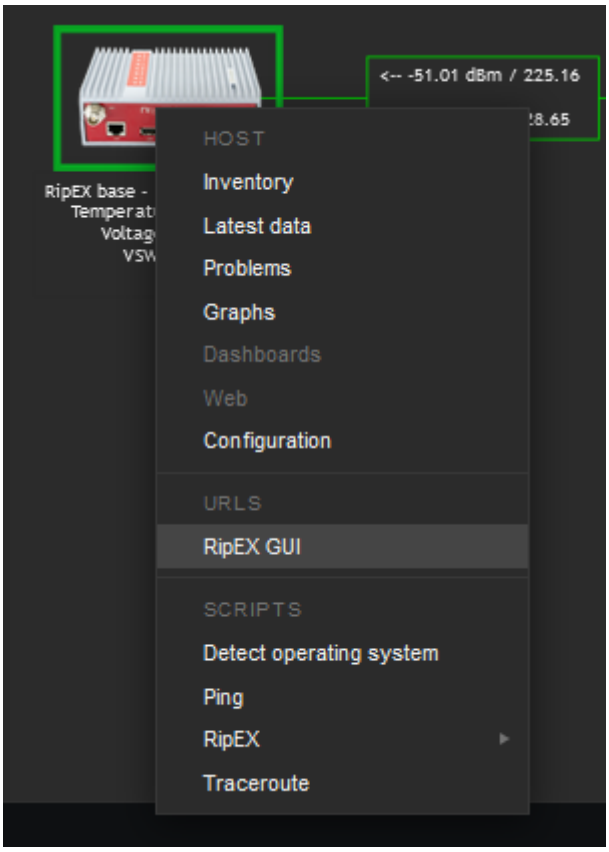


Fig. 3.13: URL link – maps

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

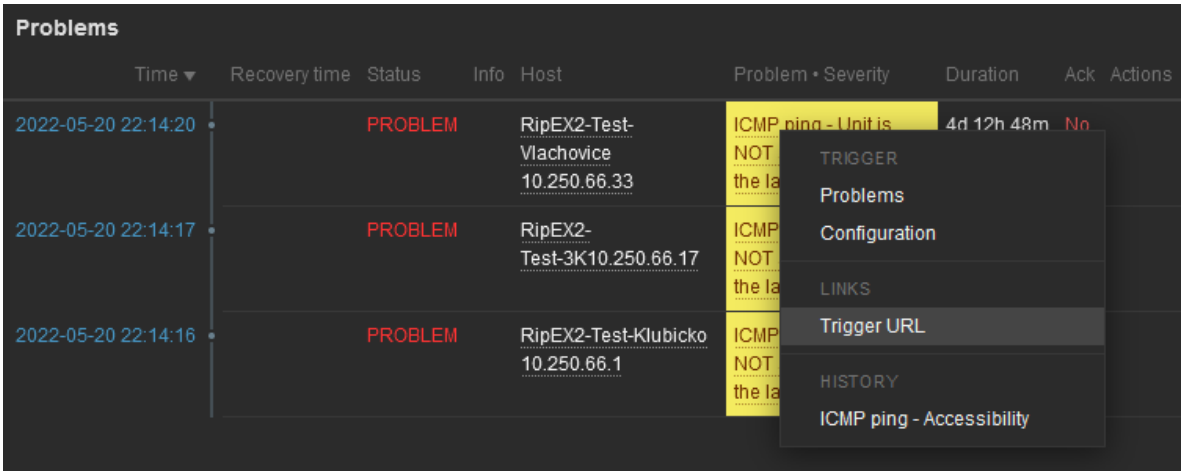


Fig. 3.14: URL link – triggers

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.

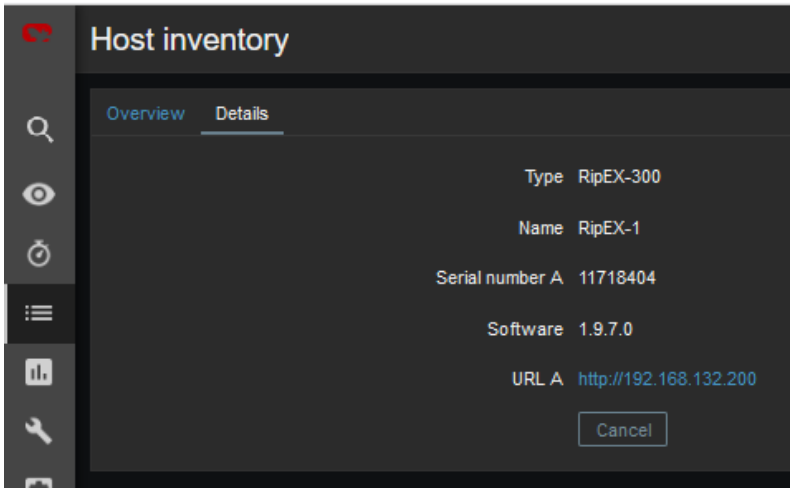


Fig. 3.15: URL link – Inventory

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., see *Zabbix website*[8].

[8] 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.

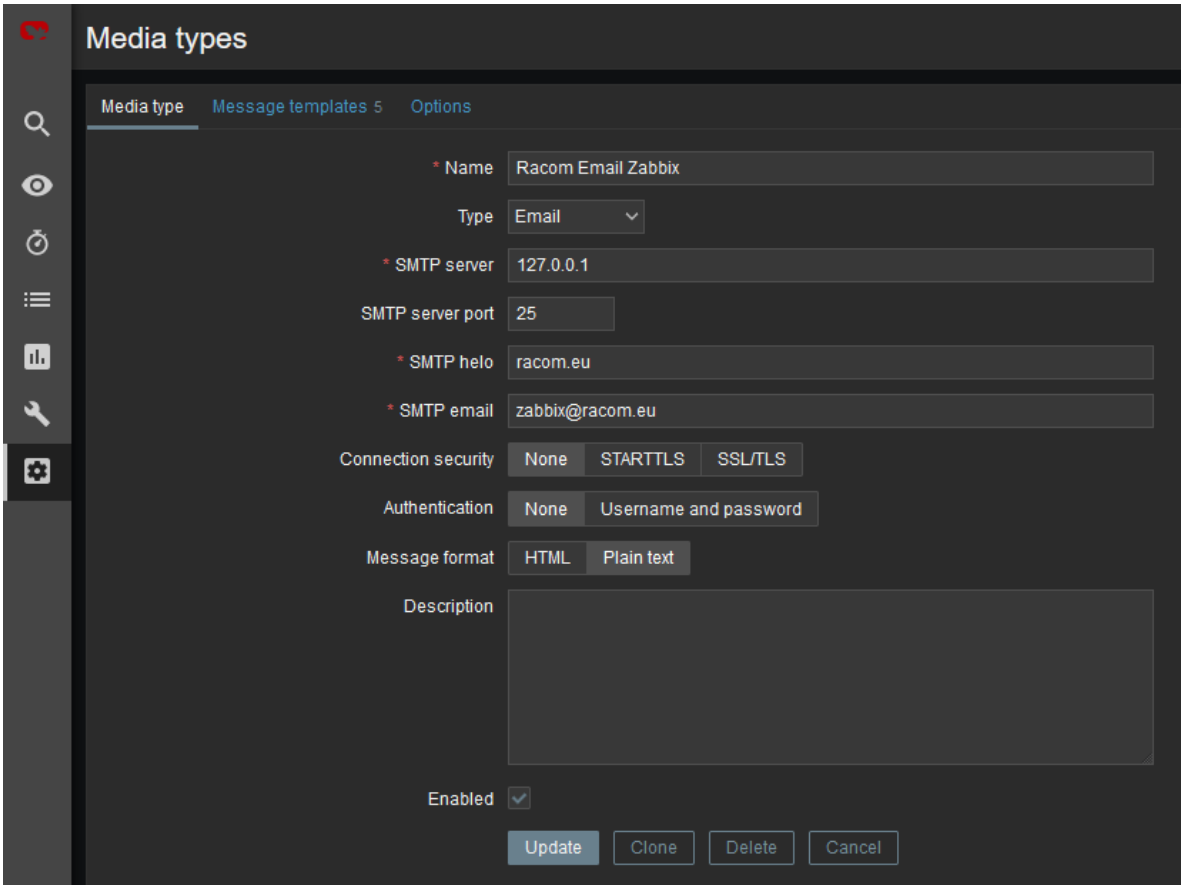


Fig. 3.16: Zabbix Media type – Email

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).

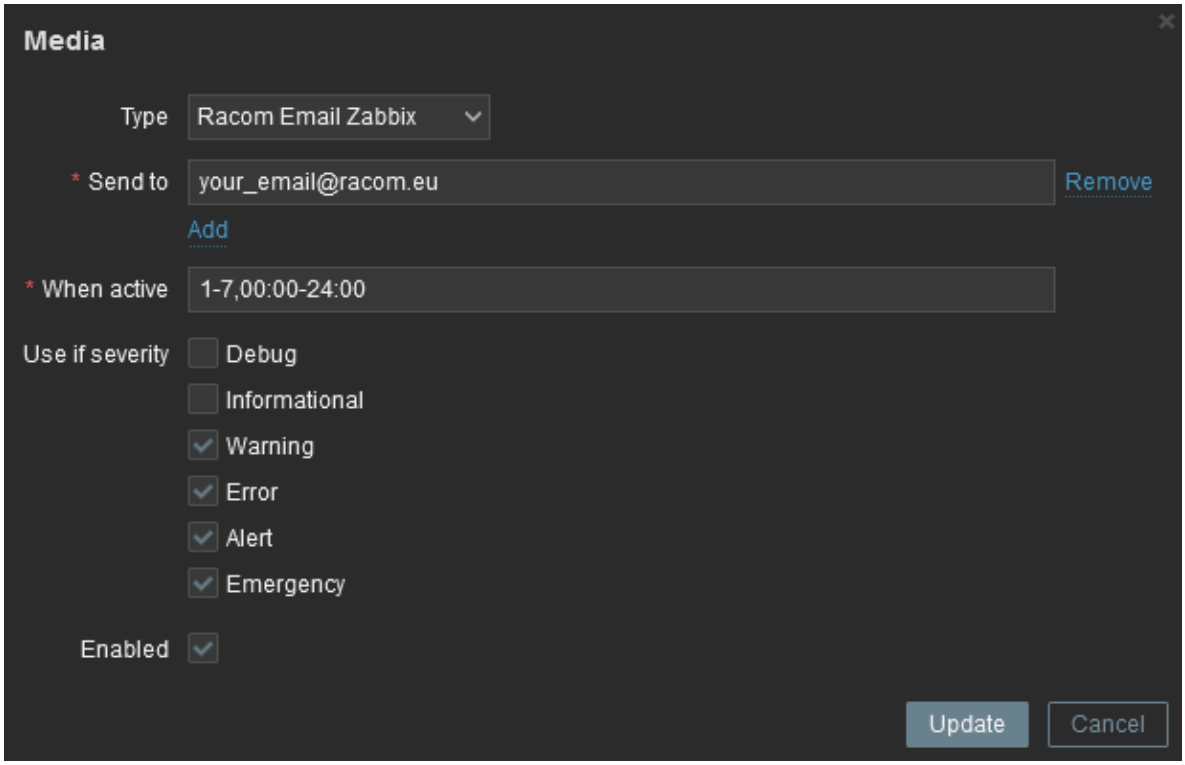


Fig. 3.17: User's e-mail

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.

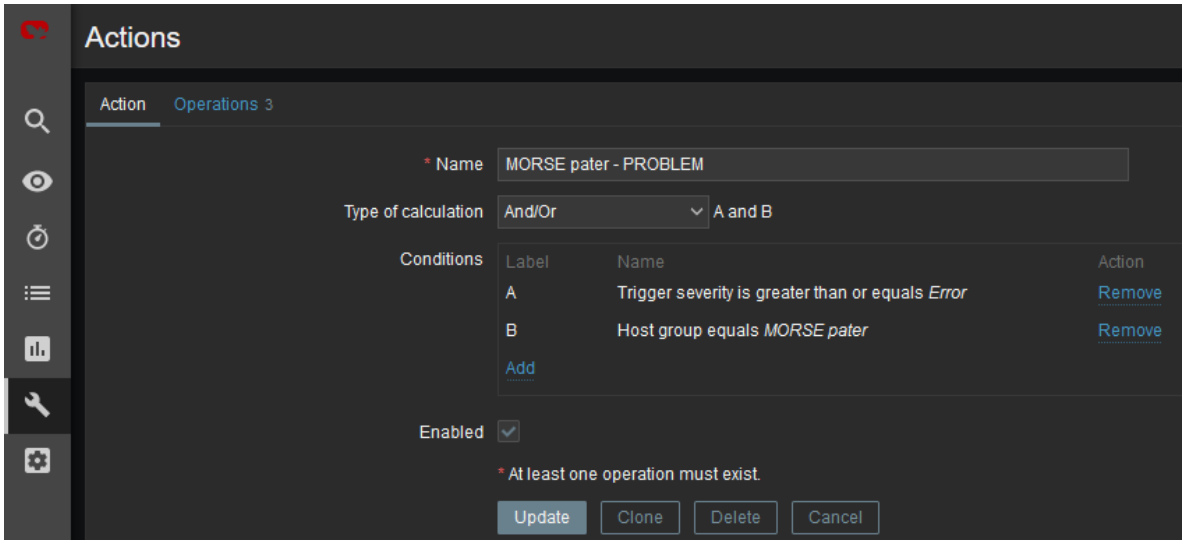


Fig. 3.18: Action and its conditions

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.

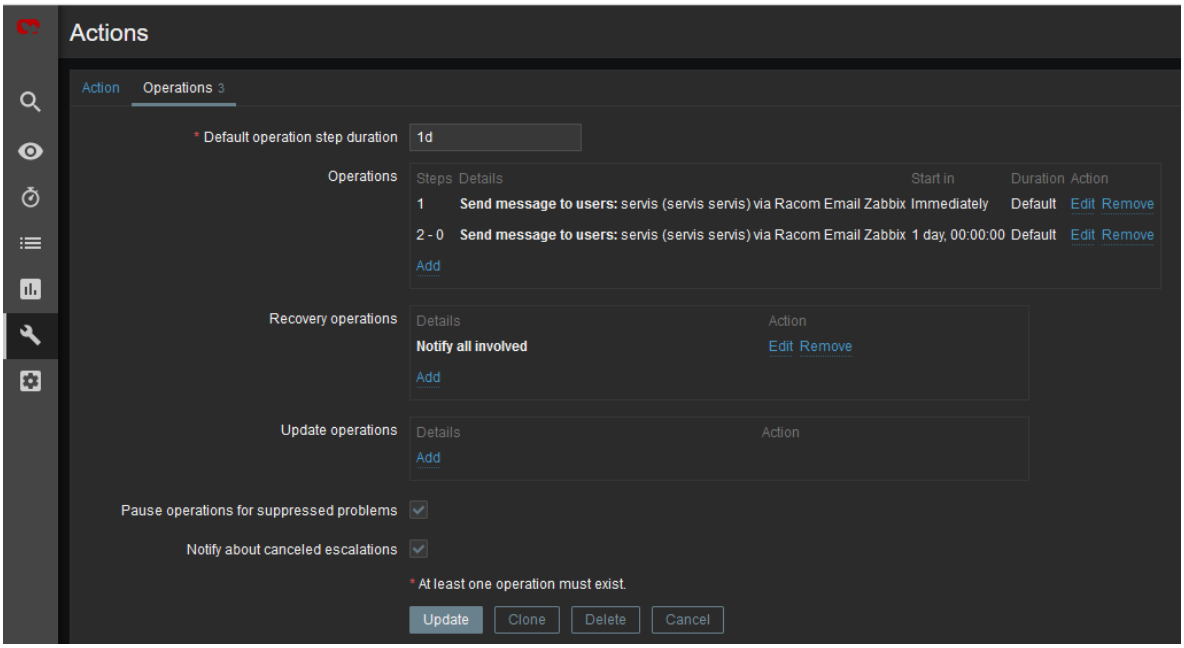


Fig. 3.19: Action Operations

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.

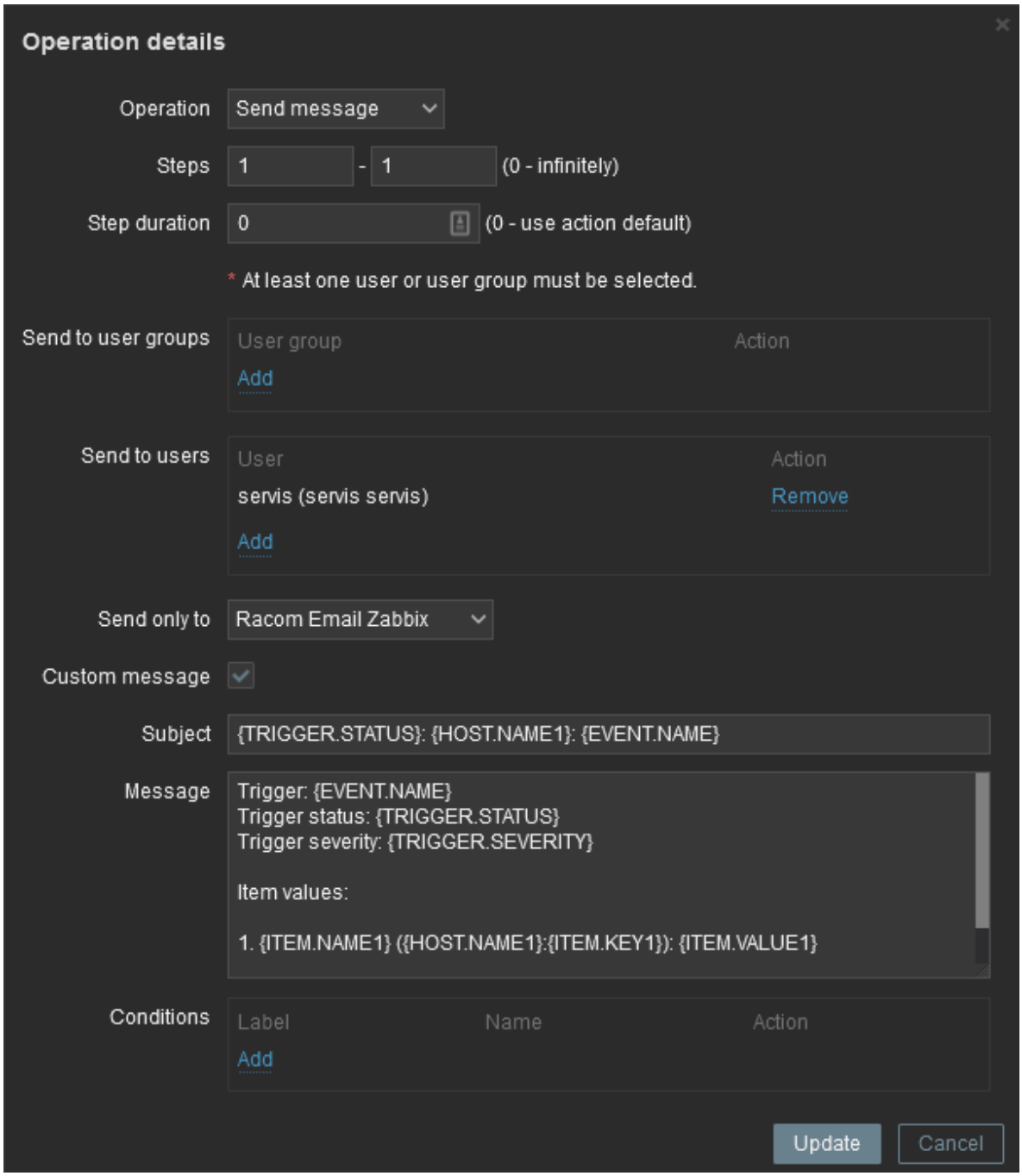


Fig. 3.20: Action Operations details

3.3.6. RipEX Scripts in Zabbix

By default, there are no ready-to-be-used actions in Zabbix such as configuration backup or firmware upgrade. The Zabbix NMS is a general system which requires special features to be implemented by RACOM or by the user himself.

We provide the user with a guide how to use and define these special features and within the RipEX template, we already prepared several examples:

- Configuration backup
- Displaying the current RSS

Note

If you have troubles running those scripts or making your own, contact us on *support@racom.eu*[9].

The whole implementation can be quite time consuming, but once you successfully run the first script, the others are very similar and its implementation is straightforward.

Within the Template, there are two scripts. As you realize, having the configuration backup files can be crucial if replacing the unit. There is nothing easier than just uploading the configuration file into a brand new RipEX unit.

Before creating and running the first scripts, you need to prepare the Zabbix server (and the Linux operating system). In this example, we configure the Debian11 OS with Zabbix 6.0 LTS installed via packaging system.

The following steps can be done in different order, but following this order is absolutely fine.

By default, the zabbix_server configuration file is located in the /etc/zabbix/zabbix_server.conf file. Find the line with "SSHKeyLocation" parameter and define it with this value:

```
SSHKeyLocation=/var/lib/zabbix/.ssh
```

This is the location of the private SSH key which will be used to access the RipEX units. Restart the Zabbix server afterwards.

```
systemctl restart zabbix-server
```

The scripts must be uploaded manually to a correct directory. The default directory is /usr/lib/zabbix/externalscripts/. Copy the script files from the ZIP Template file to this directory. The target state should look similar to this output:

```
ls -l /usr/lib/zabbix/externalscripts/
-rwxr-xr-x 1 zabbix zabbix    686 May  4 10:21 ripex_cli_cnf_textfile_get.sh
-rwxr-xr-x 1 zabbix zabbix    111 Mar  8  2016 ripex_cli_rss_show.sh
-rw-r--r-- 1 zabbix zabbix   9612 May 25 09:31 script-log.txt
-rwxr-xr-x 1 zabbix zabbix  39262 May 26 08:44 snmptrap.sh
```

There are two executable scripts via the Zabbix web interface (starting with “ripex_”). The LOG output of those scripts is in script-log.txt file. There is also the snmptrap.sh file which you should have there for the SNMP TRAP/INFORM functionality.

[9] mailto:support@racom.eu

Make sure that the files have the zabbix user/group and are executable.

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

The Zabbix user cannot login to the bash by default. We need to enable it as follows (if not already done in RZA6).

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

If not already created, create the HOME directory for the Zabbix user.

```
usermod -m -d /var/lib/zabbix zabbix
chown zabbix:zabbix /var/lib/zabbix
chmod 755 /var/lib/zabbix
```

Create the directories for the saved configuration and firmware files and change the access rights.

```
mkdir /var/lib/zabbix/configuration-backup
mkdir /var/lib/zabbix/configuration-backup/ripex
chown -R zabbix:zabbix /var/lib/zabbix/
```

The directory for the SSH key should now be located in /var/lib/zabbix/.ssh directory. Change the current directory to this one and login as zabbix.

```
su zabbix
```

A new prompt appears. We need to upload the SSH keys into every unit we want to control. You can either have you own RSA/DSA key or you can create a new one following this example. Run

```
ssh-keygen -t rsa
```

Follow the guide of the ssh-keygen application and leave the passphrase empty. To copy our RSA key into RipEX units, copy the public part of the key and run the following command:

```
ssh admin@192.168.132.200
```

Just replace 192.168.132.200 with the correct RipEX IP address. The prompt will ask for the admin password, fill it in and click Enter. Now, you should be logged in RipEX CLI. Run the following command:

```
vi .ssh/authorized_keys
```

Note

Browse the Internet for how to use ‘vi’ text editor if you are in trouble.

Insert (paste) your public part of the key to a new line. Save the changes and close the file. Logout and check, if you can access the unit without a password.

```
ssh -i rsa admin@192.168.132.200
```

We completed all Linux tasks, but we still need to edit Zabbix web interface.

Scripts must be manually created in the Zabbix Administration - Scripts menu. See the example below and create Zabbix scripts for RipEX units.

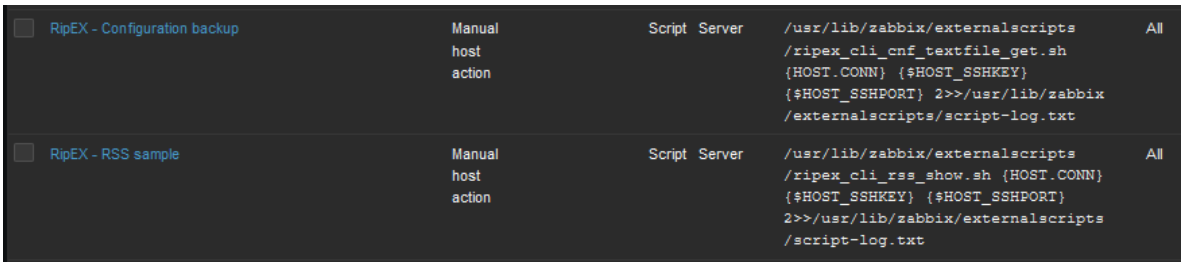


Fig. 3.21: RipEX scripts in Zabbix

If you open one of them, you can modify them as required. If you do not have any, you need to create them from scratch.

RSS sample – this script runs the RipEX Maintenance – RSS sample feature. The current level of Received Signal Strength (one sample) on Radio channel is measured. This sample is measured regardless of the current Radio channel status (Quiet/Rx/Tx).

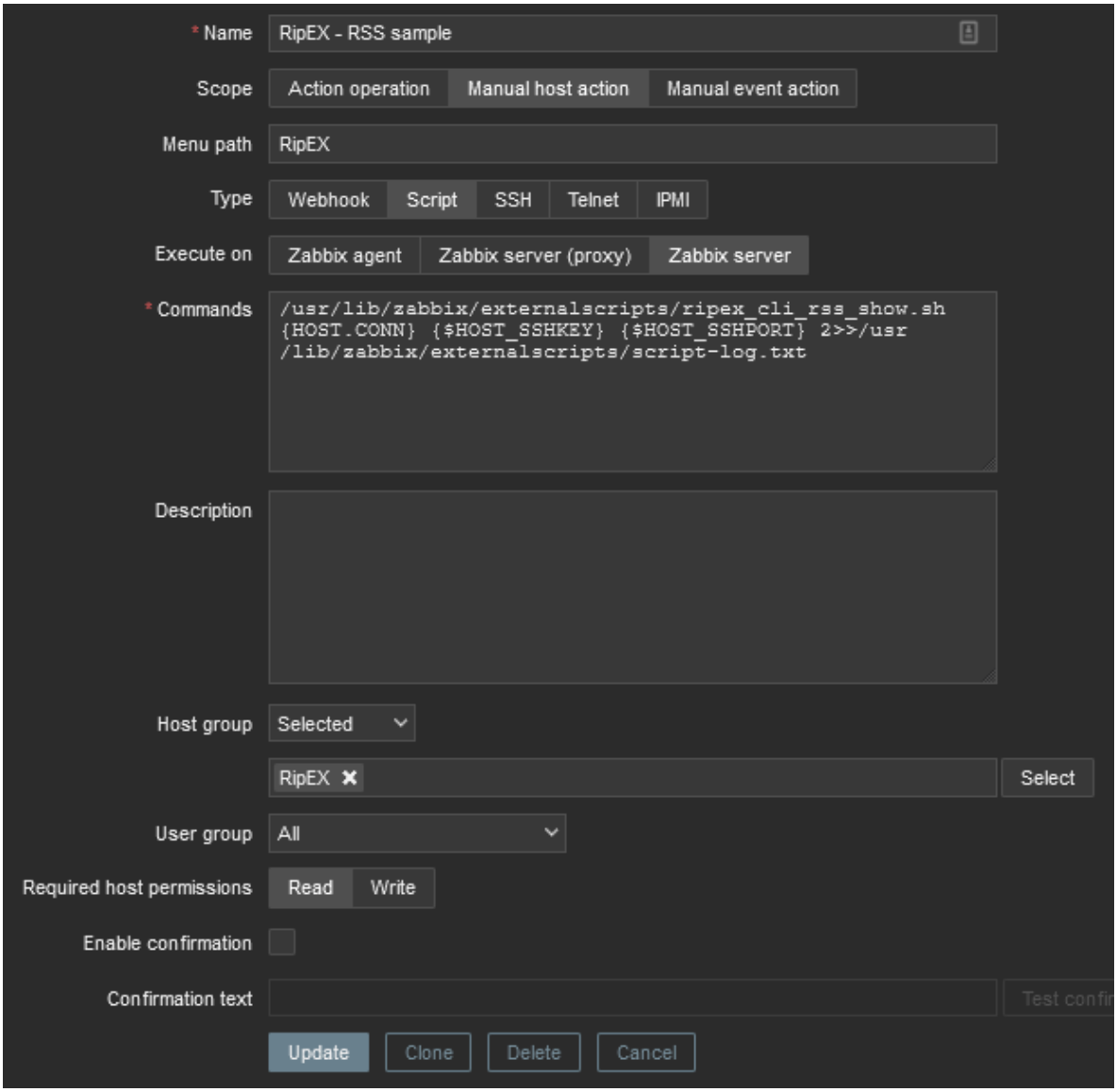


Fig. 3.22: RSS sample script details

- Name: RipEX – RSS sample
- Scope: Manual host action
- Menu path: RipEX
- Type: Script
- Execute on: Zabbix server
- Commands: */usr/lib/zabbix/externalscripts/ripex_cli_rss_show.sh {HOST.CONN} {$HOST_SSHKEY} {$HOST_SSHPORT} 2>>/usr/lib/zabbix/externalscripts/script-log.txt*

Set other parameters to suit your needs.

Configuration backup – the script creates a configuration backup file in /var/lib/zabbix/configuration-backup/ripex/ directory. The name is taken from RipEX S/N and Ethernet IP.

All is the same, except the “Commands” parameter:
/usr/lib/zabbix/externalscripts/ripex_cli_cnf_textfile_get.sh {HOST.CONN} {$HOST_SSHKEY} {$HOST_SSHPORT} 2>>/usr/lib/zabbix/externalscripts/script-log.txt

The parameters are MACROs which should be enabled by default due to our Template. Each RipEX unit uses the SSH port 22 and the SSH key saved in /var/lib/zabbix/.ssh/rsa file by default. If you need to modify any of these parameters, go to the Configuration – Hosts menu and edit the particular Host’s MACROs.

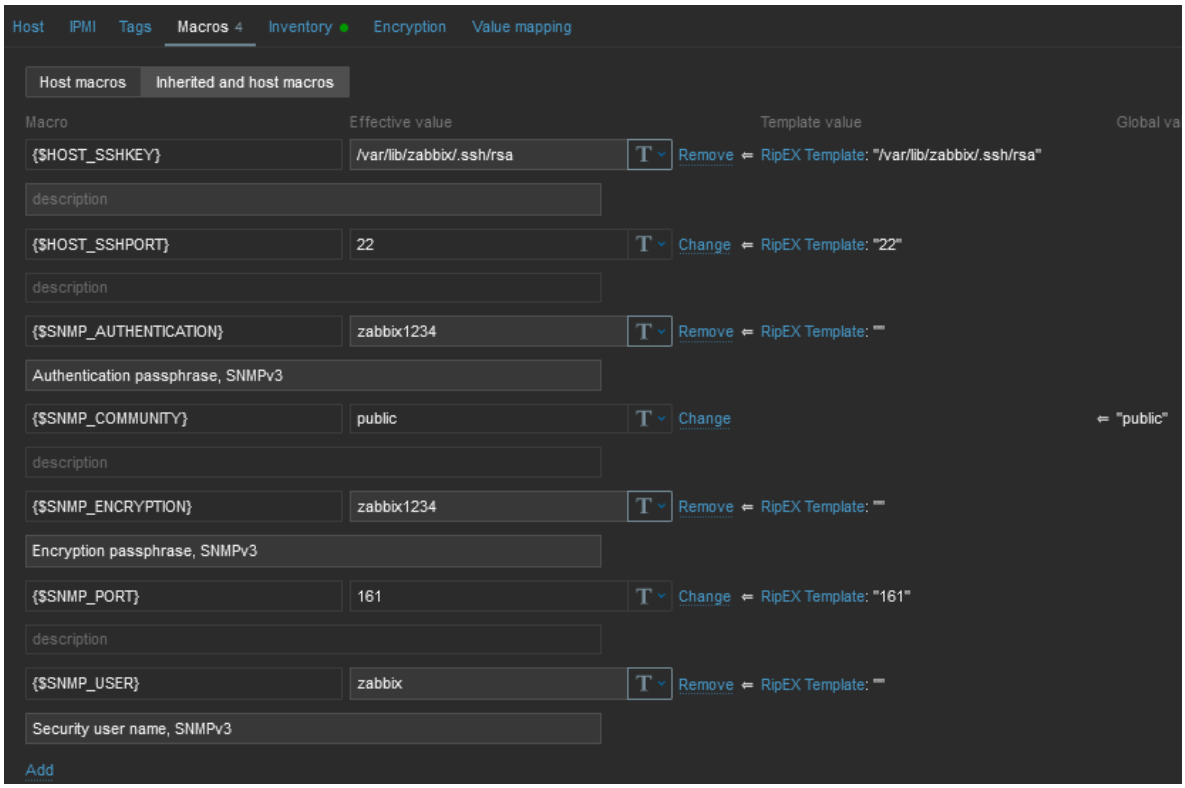


Fig. 3.23: Host MACROs

Test the scripts now. Scripts are e.g., available from maps.

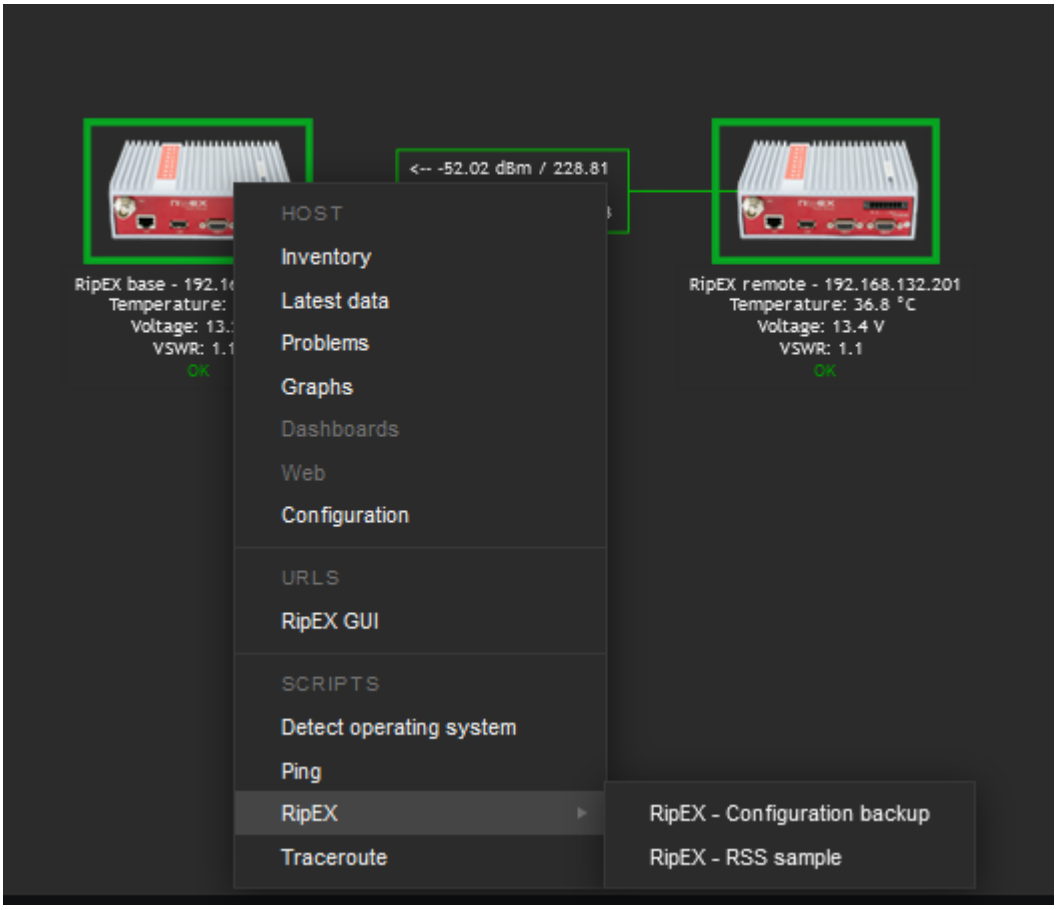


Fig. 3.24: RipEX scripts – map

The easiest script displays the RSS sample. The level (in dBm) should be displayed within several seconds in the pop-up window.

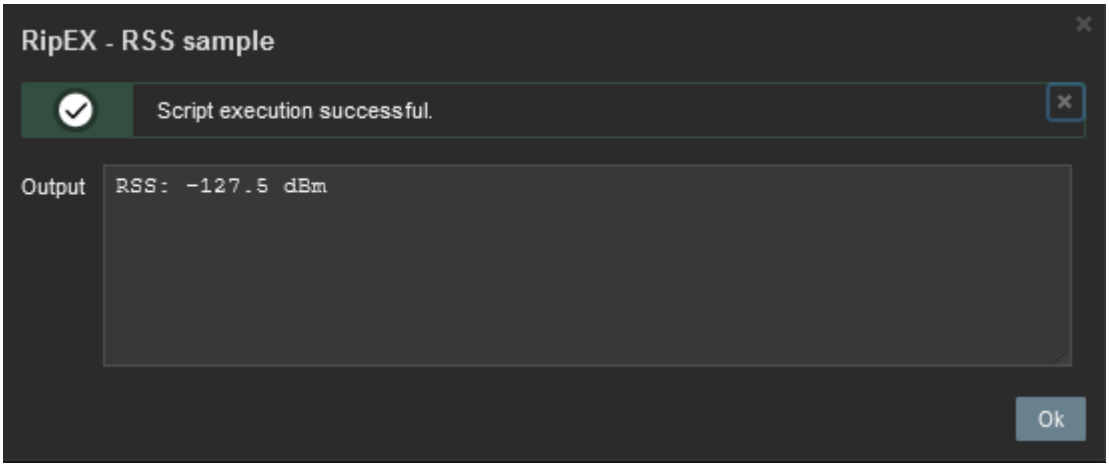


Fig. 3.25: RSS sample script output

Another script is the Configuration backup. The expected output should display a full path to the stored file.

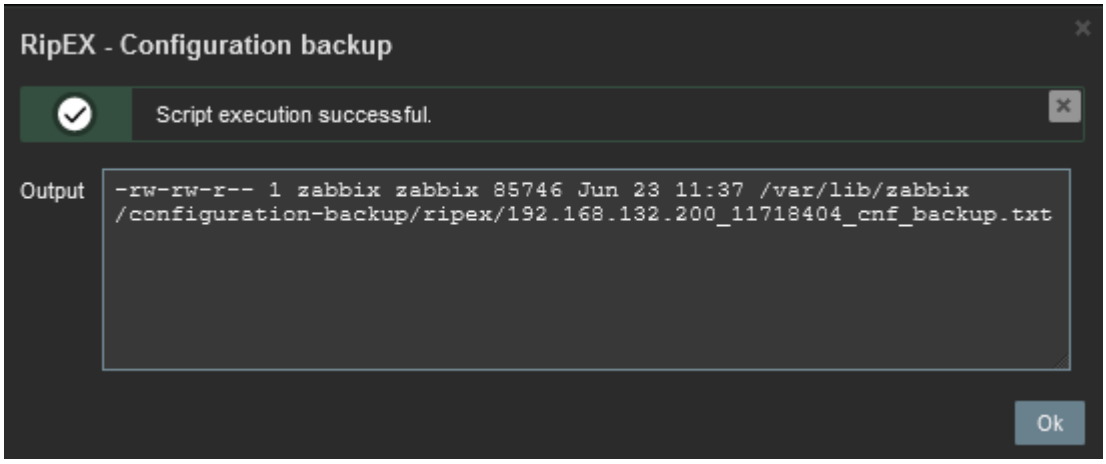


Fig. 3.26: RipEX Configuration backup script output

3.3.7. 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.

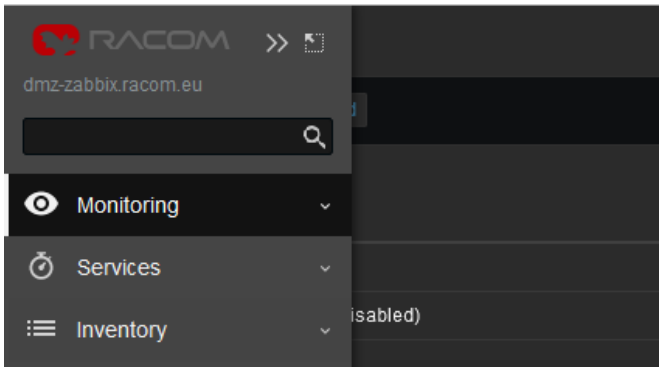


Fig. 3.27: RACOM Branding

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:

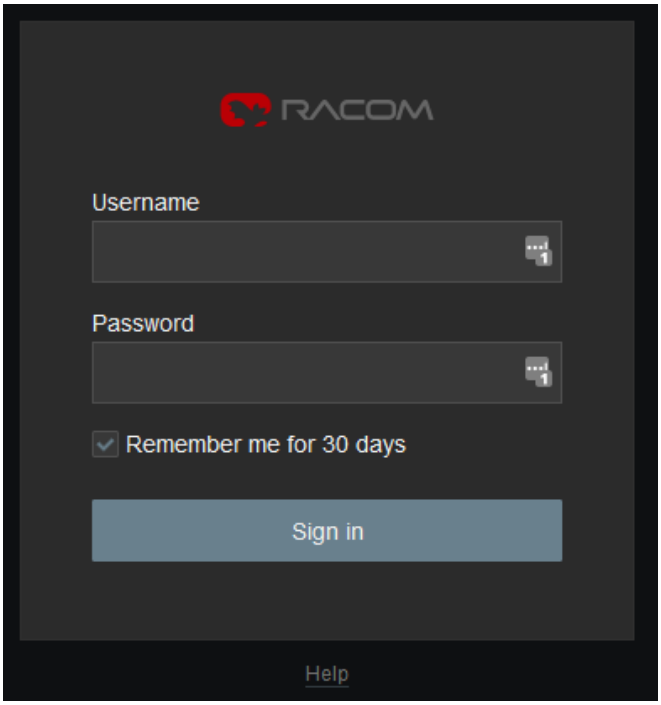


Fig. 3.28: RACOM Branding login page

If you need any additional help or information, do not hesitate to contact *support@racom.eu*[10]. 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 RipEX SNMP and Zabbix NMS, because RZA6 has many configuration steps pre-configured and done.

[10] mailto:support@racom.eu

Revision History

Revision 1.0 2017-11-27
First issue.

Revision 1.1 2018-03-20
Nomadic trap added (RipEX FW 1.8.2.0).

Revision 1.2 2021-01-20
Small changes regarding CentOS8 and Zabbix5.

Revision 1.3 2022-08-01
Zabbix 6.0 LTS, Debian11 update.