Содержание

QoE Triggers & Notifications

Purpose of use

In the "Triggers and Notification" section you can configure sending periodic reports and operational alerts to Telegram or E-mail and display them in the GUI. When a trigger is activated, you will receive a message with information about the specified event and links to the corresponding reports. By default, there are 4 reports in .csv, .tsv, .xlsx, .pdf formats, but the message template can be edited.

> Triggers and Notification section requires an active subscription – Standard license for GUI.

Let's make the settings using two scenarios as an example:

1. **Periodic report to track the RTT delay from a subscriber.**
   The report will show subscribers whose "RTT from subscriber" value is greater than or equal to 150000 ms. It will be sent on Mondays and Thursdays **in Telegram**.
2. **Alert about subscribers being a part of a botnet.**
   We will set up a table check once a minute every day. Notification will be sent **to your email** as soon as at least one infected subscriber is detected in the table.

How to create and configure triggers

1. In the GUI, go to QoE analytics → Triggers and Notification.
2. Click the + on the Triggers dashboard to add a trigger. This will open the configuration pop-up window.

It takes 5 steps to create a new trigger. Trigger settings are divided into blocks, you need to fill all of them.

Step 1. Schedule

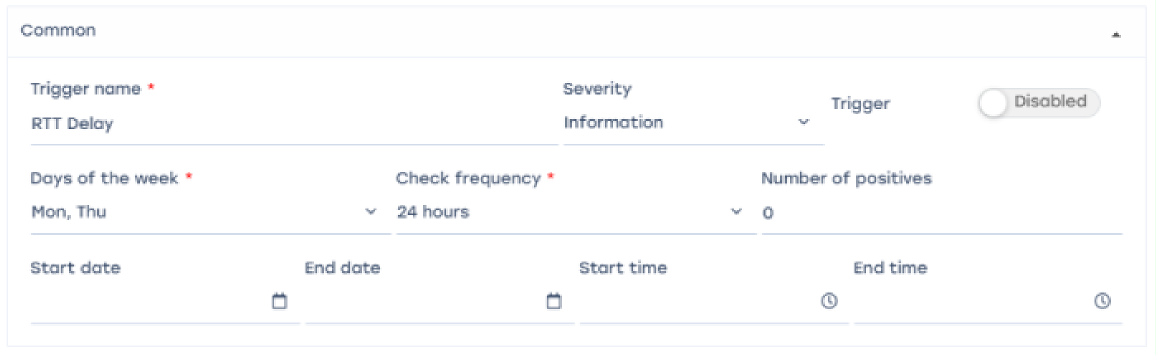
Fill in the required fields:

- Name – choose any unique name for the trigger.
- Severity – select the level of importance: information, warning, medium/high importance. For example, “Information” can be set for a regular report, and all others can be set for different notifications as you see fit. **Optional field.**
- Days of the week – on which days of the week the trigger will run.
- Check frequency — how often the validation script will be run. For example, if the value “1 min” is set – the check script will be run once a minute on the specified days of the week.
- Start and end date and time. **Optional fields.**

Also in this block there is a switch to enable/disable the trigger. **After the configuration is**

finished, make sure to enable it.

Example of filling out a block for a report to check RTT delay from a subscriber:



Common

Trigger name * RTT Delay

Severity Information

Trigger Disabled

Days of the week * Mon, Thu

Check frequency * 24 hours

Number of positives 0

Start date

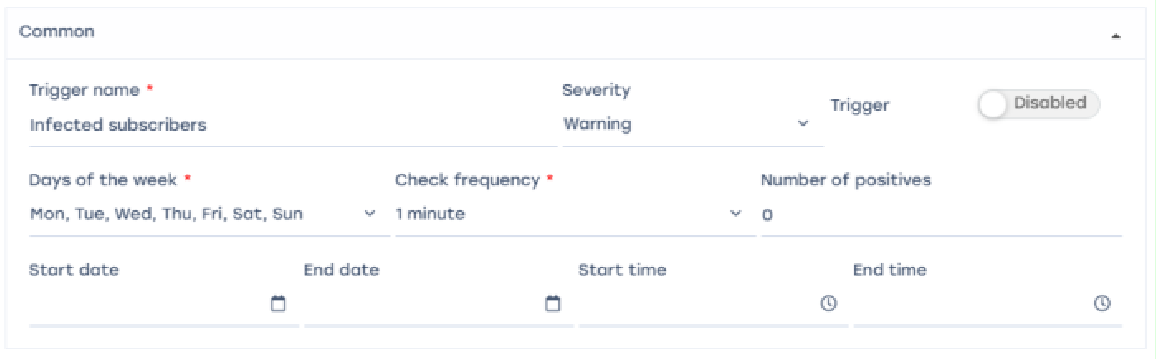
End date

Start time

End time

In this case, the check script will run on the specified days once every 24 hours - once on Monday and once on Thursday.

Example of filling out a block for notification about subscribers with cyber threats:



Common

Trigger name * Infected subscribers

Severity Warning

Trigger Disabled

Days of the week * Mon, Tue, Wed, Thu, Fri, Sat, Sun

Check frequency * 1 minute

Number of positives 0

Start date

End date

Start time

End time

In this case, the verification script will run once a minute every day, i.e. it will run continuously.

Step 2: Select a data source and metrics

Select a metric and data table. Triggers only work with ready-made tables found in Netflow and Clickstream, to start customization you need to find a table that has the required metric.

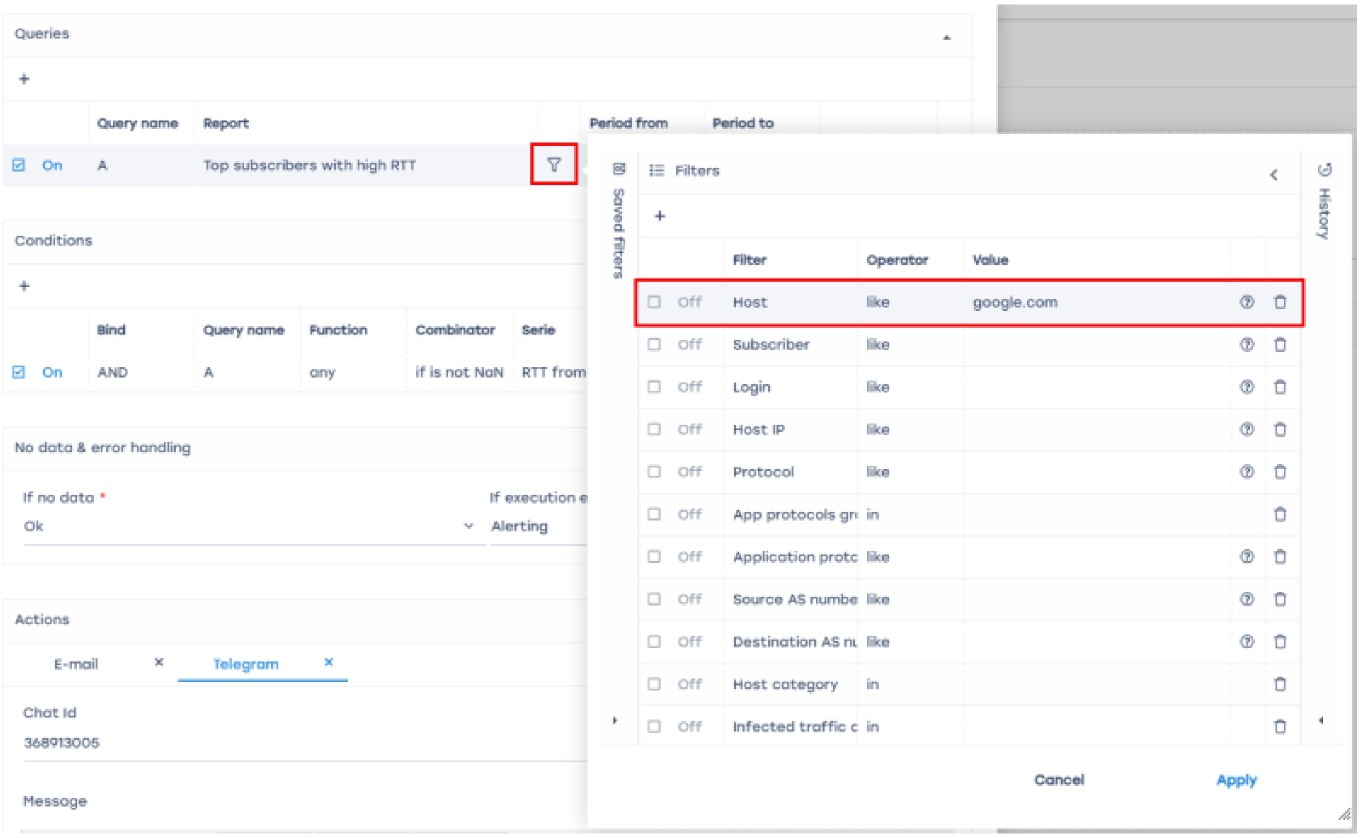
Table selection hint in the video:

To create a query, click on the **+** under the block name.

- Report – select a table with data from the ready-made reports of the system, which are analyzed.
- “Period from” and “-to”. For example, if you need to analyze data for the last 24 hours, set “Period from” – 24 hours, “Period to” – now.

> The value "Now" in the query parameters "Period from" and "Period to" means when the trigger is started. It is summarized from the "Days of Week" and "Check Frequency" values from step 1.

For each query, you can create a filter where you can set the value of IP host, subscriber login, etc. For example, you can customize the generation of a report or notification for one specific host, if you set the filter like this:



Queries

+

	Query name	Report		Period from	Period to
☑ On	A	Top subscribers with high RTT			

Conditions

+

	Bind	Query name	Function	Combinator	Serie
☑ On	AND	A	any	if is not NaN	RTT from

No data & error handling

If no data * Ok

If execution e Alerting

Actions

E-mail × Telegram ×

Chat Id 368913005

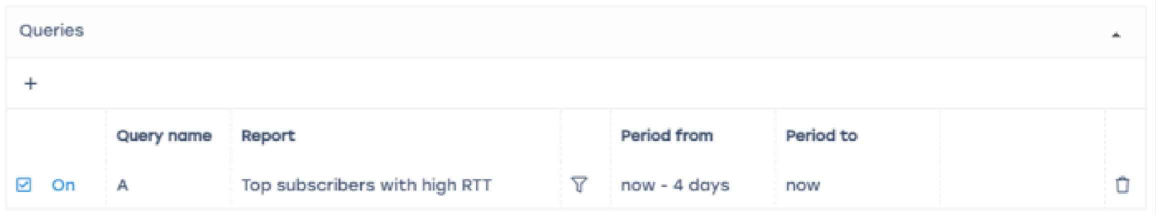
Message

Filters

+

	Filter	Operator	Value
□ Off	Host	like	google.com
□ Off	Subscriber	like	
□ Off	Login	like	
□ Off	Host IP	like	
□ Off	Protocol	like	
□ Off	App protocols gr	in	
□ Off	Application protc	like	
□ Off	Source AS numbe	like	
□ Off	Destination AS nu	like	
□ Off	Host category	in	
□ Off	Infected traffic c	in	

> Example of filling out a block for a report to track RTT delay from a subscriber. Here you need to select the report “Top subscribers with high RTT”, it has the required metrics for this trigger. Since you want the report to come on Mondays and Thursdays, “Period from” should be set equal to the interval between these days – “Now – 4 days”, the data for the last 4 days will be analyzed.

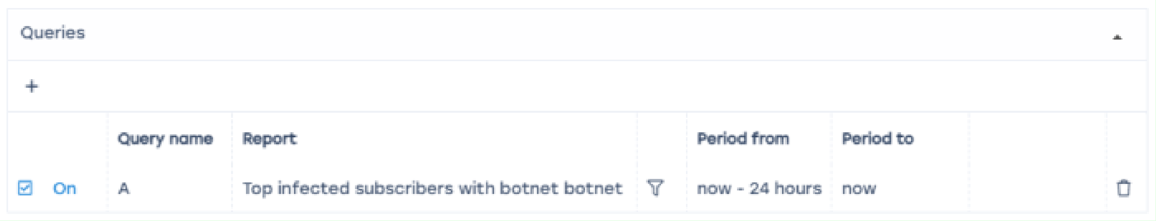


Queries

+

	Query name	Report		Period from	Period to
☑ On	A	Top subscribers with high RTT		now - 4 days	now

Example of filling out the block for notification about subscribers with cyber threats. Here you need to select the report “Top infected subscribers with botnet traffic”, it has the required metrics for this trigger. In this case, the data for the last 24 hours will be analyzed.



Queries

+

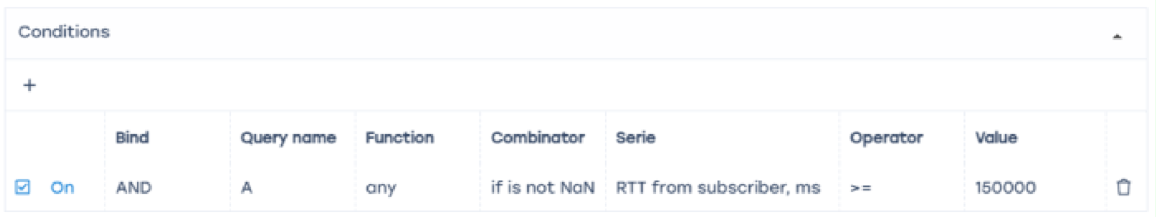
	Query name	Report	Period from	Period to
☑ On	A	Top infected subscribers with botnet botnet	now - 24 hours	now

Step 3: Conditions

Set conditions – what should happen to the metric to run the trigger.
To create a condition, click the **+** below the block name.
For each condition, you need to configure the following parameters:

- AND/OR relationship – compare with the names of queries for fulfillment of either several conditions at once or at least one of the specified conditions.
- Name – select one of the created queries.
- Function – select the type of aggregate function to be applied to the values in the condition:
    - "count" counts the number of items or records in the dataset,
    - "any" returns any value available in the dataset,
    - "anyLast" returns the last value available in the dataset,
    - "avg" calculates the average value of the numeric data in the dataset,
    - "min" returns the minimum value from the available data in the dataset,
    - "max" returns the maximum value from the available data set,
    - "sum" calculates the sum of the numeric data in the set,
    - "uniq" returns unique values in the dataset, removing duplicates.
- Combinator – select a non-numeric/non-zero/numeric/zero value or leave blank.
- Series – select the desired metric from the report.
- Operator – select: =, !=, >, >=, <, ⇐, between *(will return records where the expression is between value1 and value2 inclusive)*, not between *(returns all records where the expression is NOT between value1 and value2 inclusive)*.
- Value – assign the required value for the condition.

Example of filling out a block for a report to track RTT delay from a subscriber:



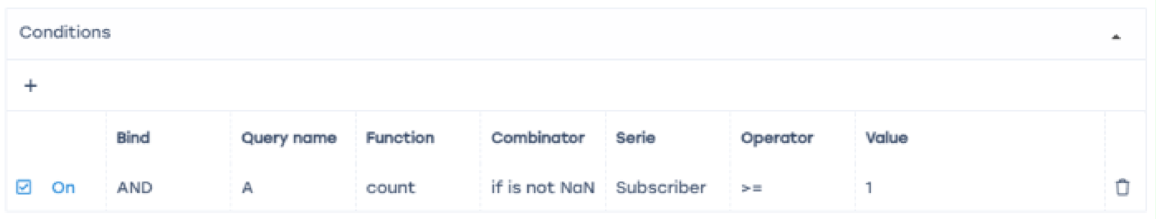
Conditions

+

	Bind	Query name	Function	Combinator	Serie	Operator	Value
☑ On	AND	A	any	if is not NaN	RTT from subscriber, ms	>=	150000

In this case, the trigger will go off if the RTT value from the subscriber is greater than or equal to 150000 ms in the table from step 2.

Example of filling out the block for alerts about subscribers with cyber threats:



Conditions

+

	Bind	Query name	Function	Combinator	Serie	Operator	Value	
☑ On	AND	A	count	if is not NaN	Subscriber	>=	1	🗑

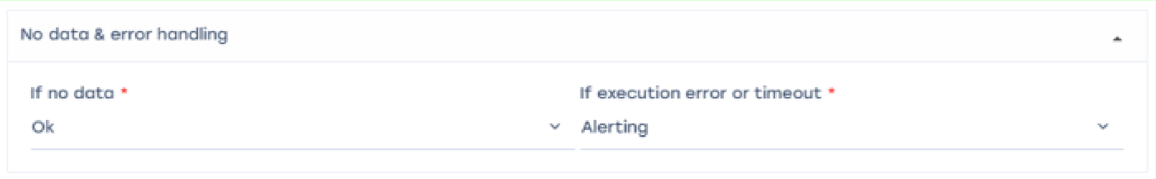
In this case, the trigger will be fired if there is at least one subscriber in the table from step 2.

Step 4: Error handling

Set the trigger behavior when errors occur.
Select one of the values in the “If there is no data” and “If there is a runtime error or timeout” fields:

- “Notification” – there is the condition specified in the trigger.
- “No data” – no data is found when processing the reports set in the trigger.
- “Save last condition” – no action needed.
- “Ok” – the conditions set in the trigger did not work, everything is fine, and no actions needed.

Example of filling out the block for report and for alerts:



No data & error handling

If no data * : Ok

If execution error or timeout * : Alerting

In both cases, if there is no data – the trigger will not be fired and the message will not be sent; if there is an error or timeout – notification will be sent.

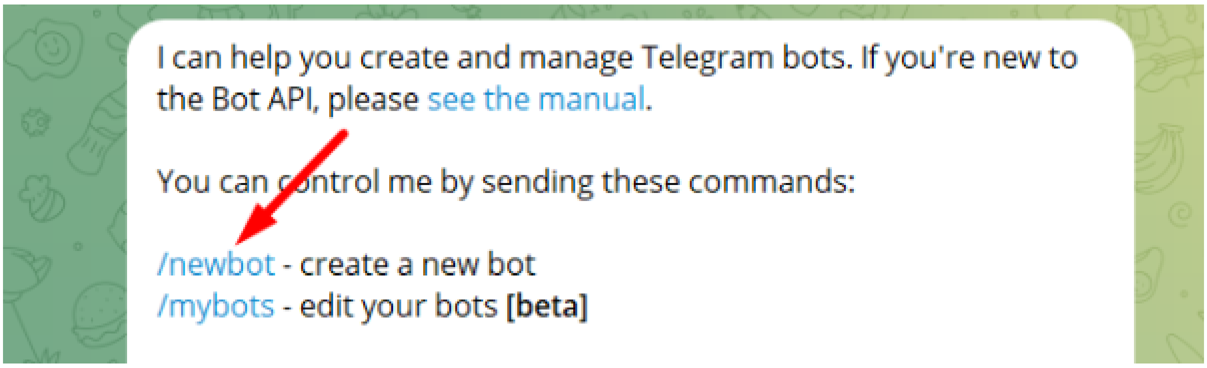
Step 5: Actions

Setting up an action will allow you to receive a message to E-mail or Telegram in case of triggering.
To create an action, press **+** under the block name.
To delete an action, press ✕ next to the action name.

Telegram

Step 1: Register your bot via https://t.me/BotFather.

1. Start BotFather with the `/start` command.
2. Type `/newbot` to create a new bot.

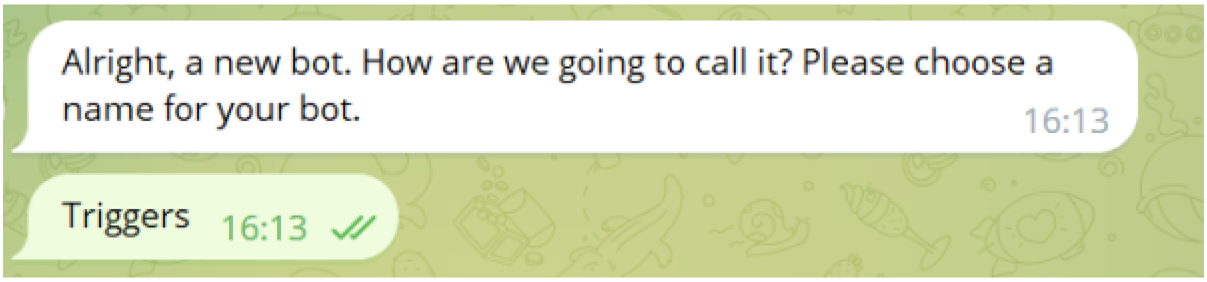


I can help you create and manage Telegram bots. If you're new to the Bot API, please see the manual.

You can control me by sending these commands:

/newbot - create a new bot
/mybots - edit your bots **[beta]**

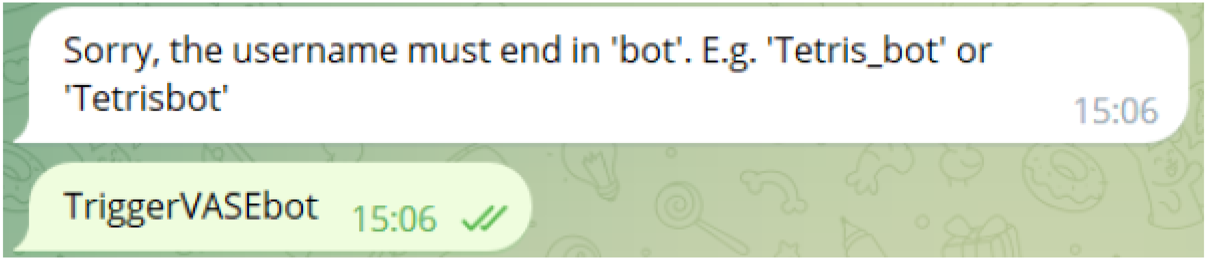
3. Enter the name of the bot.



Alright, a new bot. How are we going to call it? Please choose a name for your bot. 16:13

Triggers 16:13 ✓✓

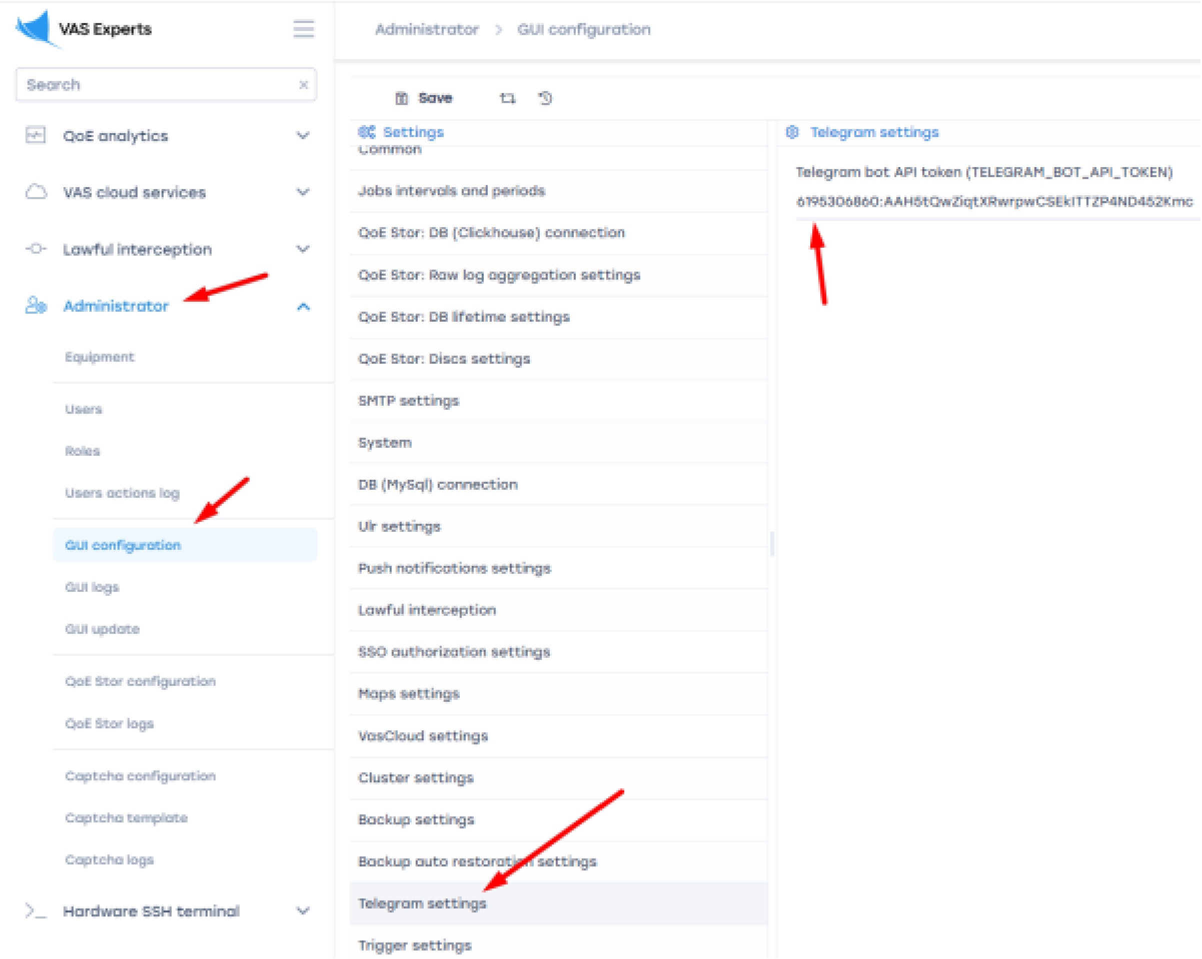
4. Enter a unique `username` (Latin only, ending in "bot").



Sorry, the username must end in 'bot'. E.g. 'Tetris_bot' or 'Tetrisbot' 15:06

TriggerVASEbot 15:06 ✓✓

5. Copy the HTTP API access token from the bot registration message, it looks like this: `5995002635:AAGdSR0udY9K9uxENaPu2HF4azmpsKQq98X`
6. Paste the copied token into the GUI settings (Administrator → GUI Configuration → Telegram Settings → Telegram bot API token).



Telegram bot API token (TELEGRAM_BOT_API_TOKEN)

6195306860:AAH5tQwZiqtXRwrpwCSEkITTZP4ND452Kmc

Step 2: Get a chat ID for your personal Telegram account via https://t.me/RawDataBot

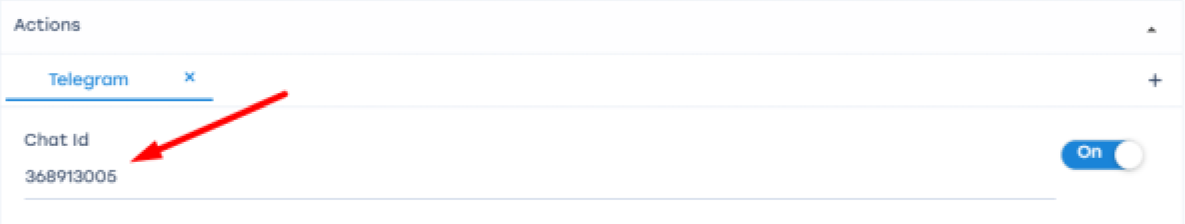
⚠ To get chat ID, user must have `username` in Telegram profile!

1. Start Telegram Bot Raw with the `/start` command.
2. Copy the `ID`, it looks like this:

```
"chat": {
      "id": 222455434,
      "first_name": "Ivan",
      "last_name": "Nat",
      "username": "HardNat",
      "type": "private"
},
```

Step 3: Connect Telegram to the configured trigger

Add the ID from step 2 to the Telegram action in the "Chat ID" field.



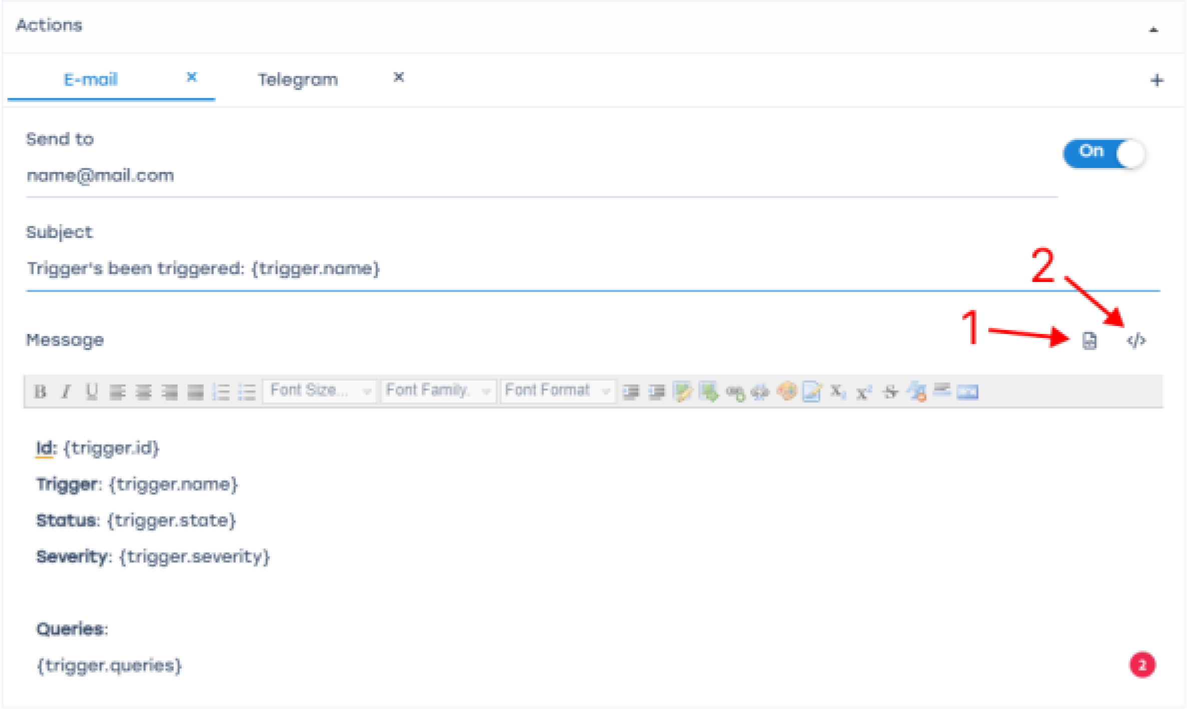
Chat Id

368913005

E-Mail

Creates a notification and sends it to the specified e-mail address.

1. If the “Message” field is not filled in – click on the “Set default template” button (1) to fill the action fields with default values. If necessary, all values can be edited.
2. If you click on the “Template parameters” button (2), it will open a menu with identifiers that can be used to compose the message.



Send to
name@mail.com

Subject
Trigger's been triggered: {trigger.name}

Message

Id: {trigger.id}
Trigger: {trigger.name}
Status: {trigger.state}
Severity: {trigger.severity}

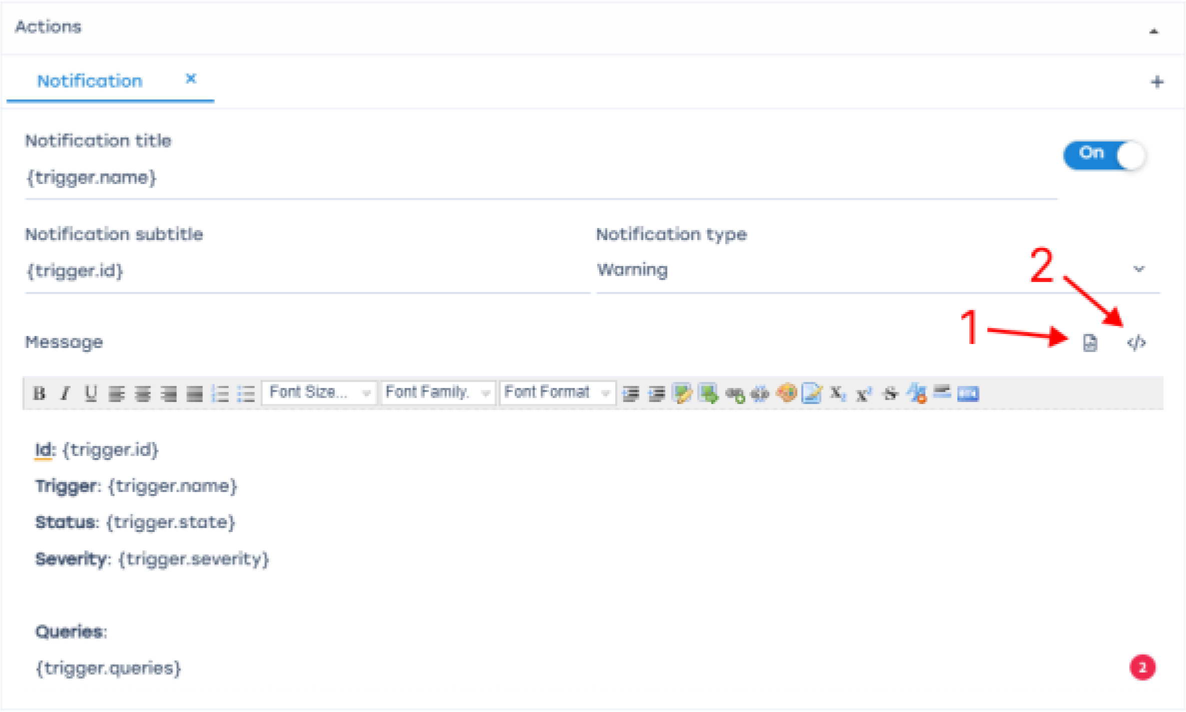
Queries:
{trigger.queries}

For E-mail actions to work, you need to configure SMTP. Go to Administrator → GUI Configuration, select "SMTP Settings".

GUI Notifications

Notification can be used to test the functionality of triggers.

1. Click on the “Set default template” button (1) to fill the action fields with default values. All values can be edited if necessary.
2. Clicking on the “Template Options” button (2) opens a menu with identifiers that can be used to compose the message.



Actions

Notification ×

Notification title

{trigger.name}

On

Notification subtitle

{trigger.id}

Notification type

Warning

Message

Id: {trigger.id}

Trigger: {trigger.name}

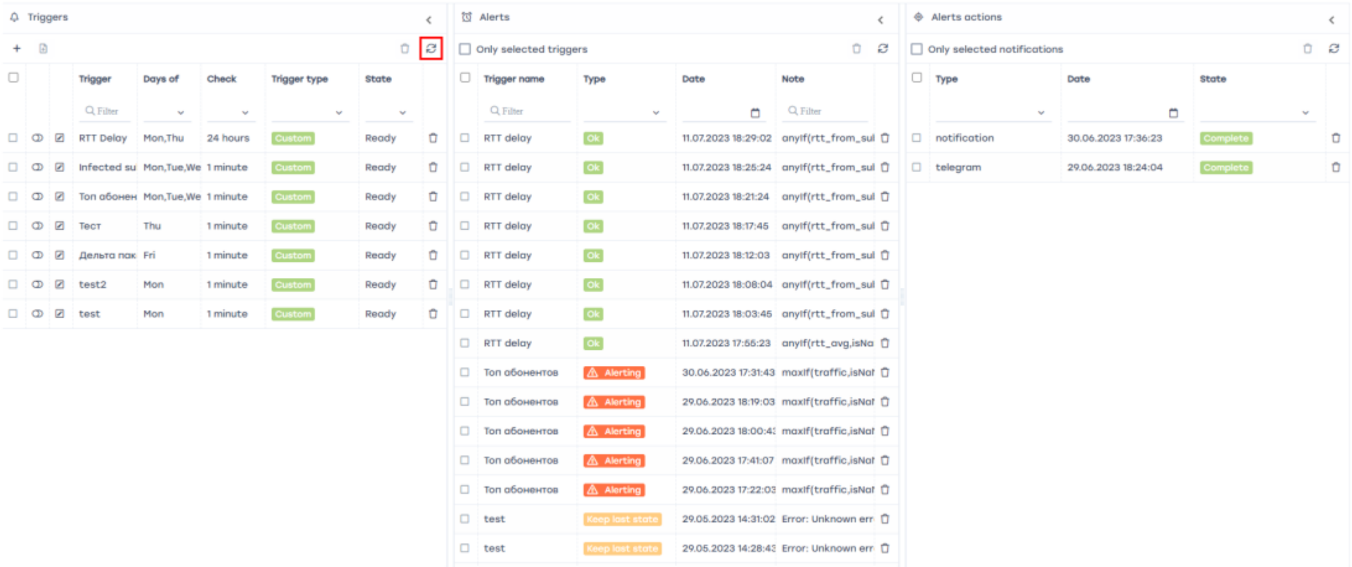
Status: {trigger.state}

Severity: {trigger.severity}

Queries:

{trigger.queries}

After creating a trigger, click “Save”. On the “Triggers” dashboard, enable the necessary triggers. If the GUI page has not been refreshed – refresh the page in the browser or click the “Refresh” button.



Triggers

☐			Trigger	Days of	Check	Trigger type	State	
☐			RTT Delay	Mon,Thu	24 hours	Custom	Ready	
☐			Infected su	Mon,Tue,We	1 minute	Custom	Ready	
☐			Топ абонен	Mon,Tue,We	1 minute	Custom	Ready	
☐			Тест	Thu	1 minute	Custom	Ready	
☐			Дельта пак	Fri	1 minute	Custom	Ready	
☐			test2	Mon	1 minute	Custom	Ready	
☐			test	Mon	1 minute	Custom	Ready	

Alerts

☐ Only selected triggers

☐	Trigger name	Type	Date	Note
☐	RTT delay	Ok	11.07.2023 18:29:02	anyIf(rtt_from_sul
☐	RTT delay	Ok	11.07.2023 18:25:24	anyIf(rtt_from_sul
☐	RTT delay	Ok	11.07.2023 18:21:24	anyIf(rtt_from_sul
☐	RTT delay	Ok	11.07.2023 18:17:45	anyIf(rtt_from_sul
☐	RTT delay	Ok	11.07.2023 18:12:03	anyIf(rtt_from_sul
☐	RTT delay	Ok	11.07.2023 18:08:04	anyIf(rtt_from_sul
☐	RTT delay	Ok	11.07.2023 18:03:45	anyIf(rtt_from_sul
☐	RTT delay	Ok	11.07.2023 17:55:23	anyIf(rtt_avg,isNa
☐	Топ абонентов	Alerting	30.06.2023 17:31:43	maxIf(traffic,isNat
☐	Топ абонентов	Alerting	29.06.2023 18:19:03	maxIf(traffic,isNat
☐	Топ абонентов	Alerting	29.06.2023 18:00:4:	maxIf(traffic,isNat
☐	Топ абонентов	Alerting	29.06.2023 17:41:07	maxIf(traffic,isNat
☐	Топ абонентов	Alerting	29.06.2023 17:22:0:	maxIf(traffic,isNat
☐	test	Keep last state	29.05.2023 14:31:02	Error: Unknown err
☐	test	Keep last state	29.05.2023 14:28:4:	Error: Unknown err

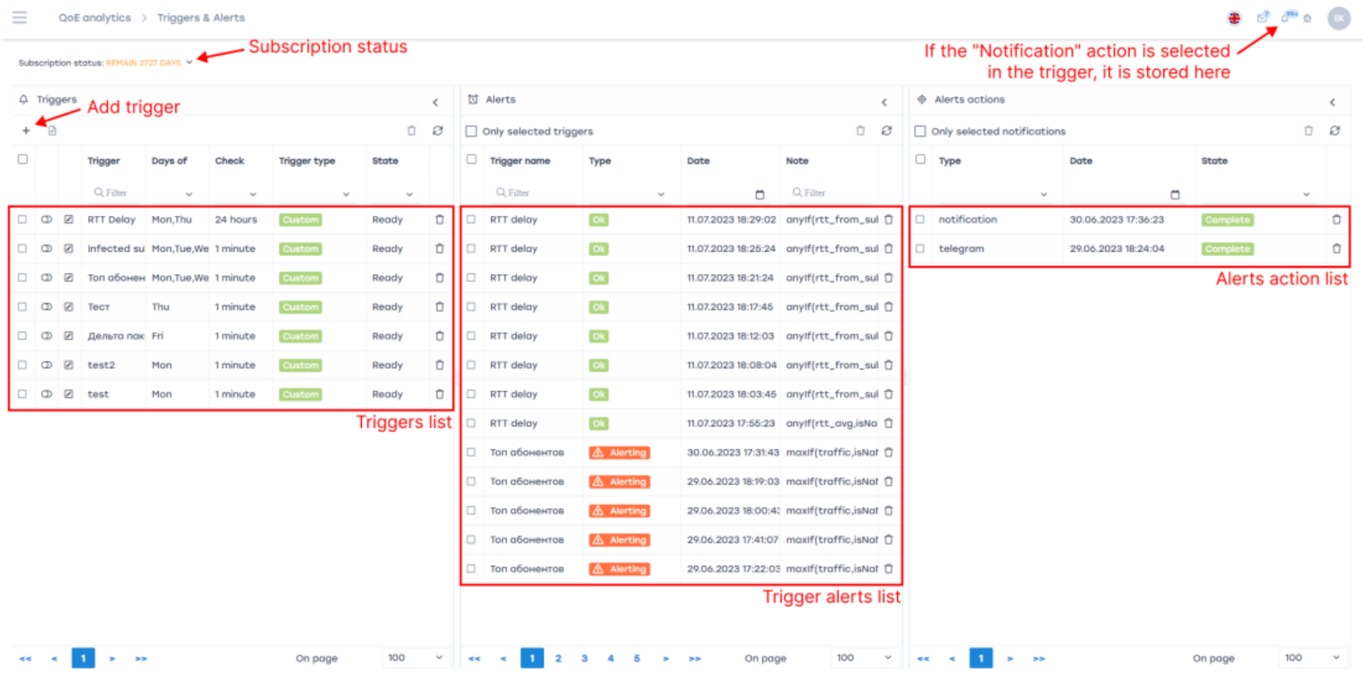
Alerts actions

☐ Only selected notifications

☐	Type	Date	State
☐	notification	30.06.2023 17:36:23	Complete
☐	telegram	29.06.2023 18:24:04	Complete

“Triggers and Notification” page elements description

Go to QoE Analytics → Triggers and Notification.
This will open the section as shown in the image below.



QoE analytics > Triggers & Alerts

Subscription status: REMAIN 2727 DAYS

Subscription status

If the "Notification" action is selected in the trigger, it is stored here

Triggers

Add trigger

□			Trigger	Days of	Check	Trigger type	State	
□		☑	RTT Delay	Mon,Thu	24 hours	Custom	Ready	
□		☑	Infected su	Mon,Tue,We	1 minute	Custom	Ready	
□		☑	Топ абонен	Mon,Tue,We	1 minute	Custom	Ready	
□		☑	Тест	Thu	1 minute	Custom	Ready	
□		☑	Дельта пак	Fri	1 minute	Custom	Ready	
□		☑	test2	Mon	1 minute	Custom	Ready	
□		☑	test	Mon	1 minute	Custom	Ready	

Triggers list

Alerts

□ Only selected triggers

□	Trigger name	Type	Date	Note	
□	RTT delay	Ok	11.07.2023 18:29:02	anyIf(rtt_from_sul	
□	RTT delay	Ok	11.07.2023 18:25:24	anyIf(rtt_from_sul	
□	RTT delay	Ok	11.07.2023 18:21:24	anyIf(rtt_from_sul	
□	RTT delay	Ok	11.07.2023 18:17:45	anyIf(rtt_from_sul	
□	RTT delay	Ok	11.07.2023 18:12:03	anyIf(rtt_from_sul	
□	RTT delay	Ok	11.07.2023 18:08:04	anyIf(rtt_from_sul	
□	RTT delay	Ok	11.07.2023 18:03:45	anyIf(rtt_from_sul	
□	RTT delay	Ok	11.07.2023 17:55:23	anyIf(rtt_avg,isNa	
□	Топ абонентов	⚠ Alerting	30.06.2023 17:31:43	maxIf(traffic,isNat	
□	Топ абонентов	⚠ Alerting	29.06.2023 18:19:03	maxIf(traffic,isNat	
□	Топ абонентов	⚠ Alerting	29.06.2023 18:00:4:	maxIf(traffic,isNat	
□	Топ абонентов	⚠ Alerting	29.06.2023 17:41:07	maxIf(traffic,isNat	
□	Топ абонентов	⚠ Alerting	29.06.2023 17:22:03	maxIf(traffic,isNat	

Trigger alerts list

Alerts actions

□ Only selected notifications

□	Type	Date	State	
□	notification	30.06.2023 17:36:23	Complete	
□	telegram	29.06.2023 18:24:04	Complete	

Alerts action list

This section contains three sections:

- List of the triggers.
- List of the notifications.
- List of actions performed by triggers as a result of notifications.

Types of triggers:

- System. These are set by the vendor and can only be enabled/disabled.
- Custom. User-defined and can be freely configured.

For a detailed description of configuring a trigger, see How to create and configure triggers.