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

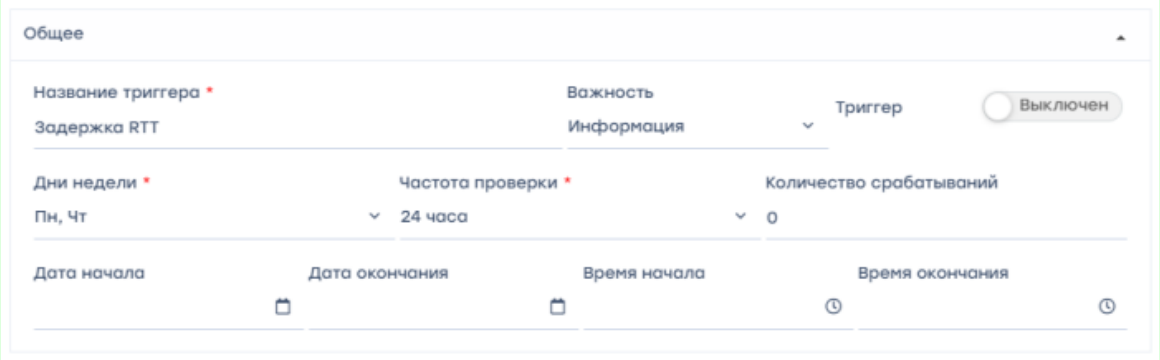
Fill in the required fields:

- 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**

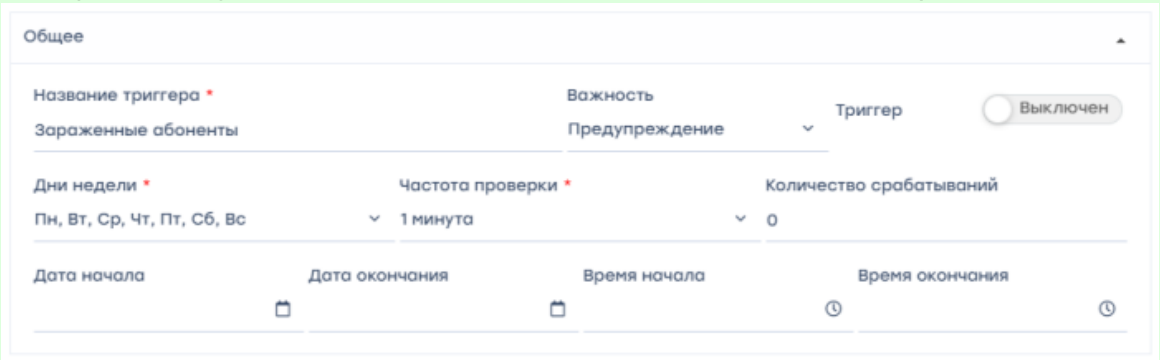
finished, make sure to enable it.

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



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:



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.

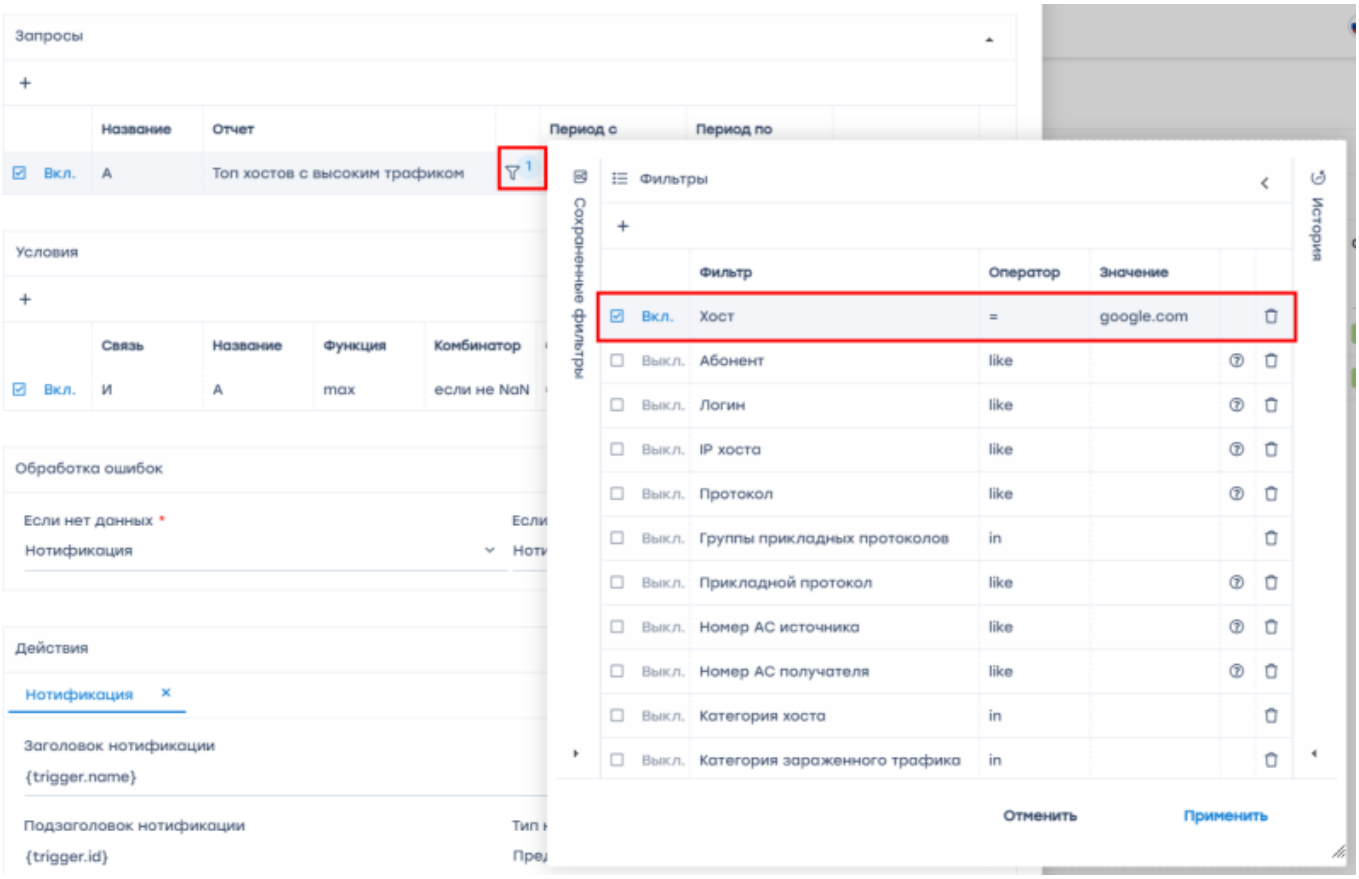
To create a query, click on the **+** under the block name.

- 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.

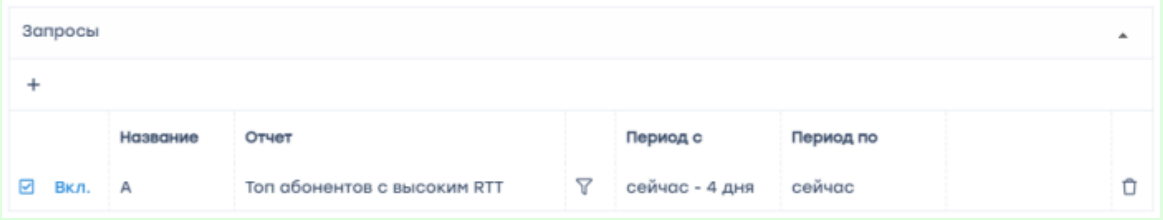
”Now” in the from/to period means the moment of trigger start. It is made up of the days of the trigger week and the upper limit of the check frequency (from the “General” settings block).

For each request, 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

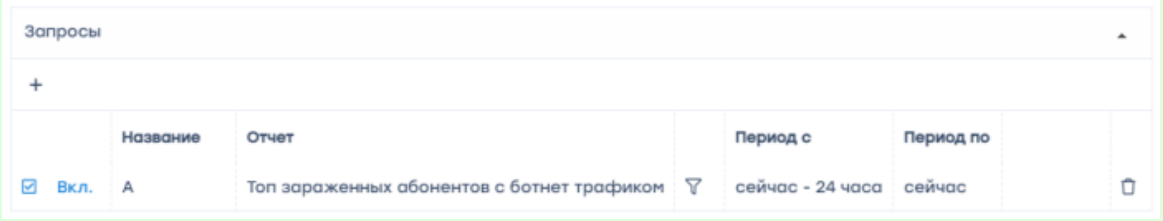
set the filter like this:



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.



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.

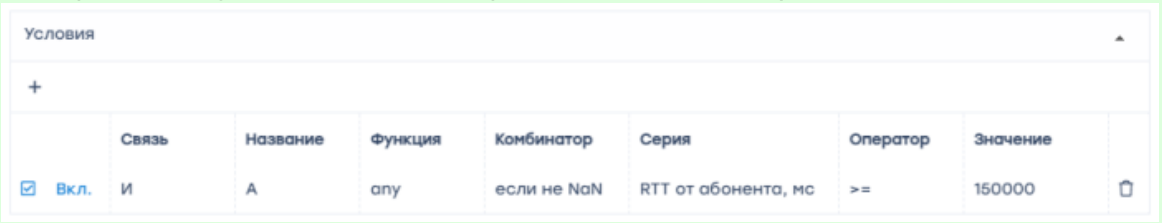


Step 3: Conditions

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:

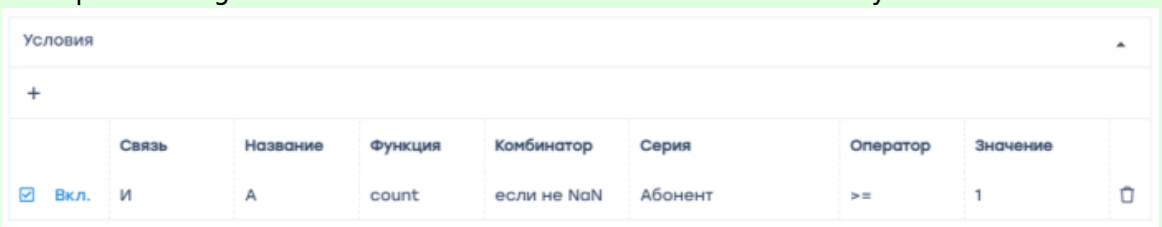
- AND/OR relationship – compare with the names of requests for fulfillment of either several conditions at once or at least one of the specified conditions.
- Name – select one of the created requests.
- Function – select the type of aggregate function to be applied to the values in the condition:
  - "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:



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:



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

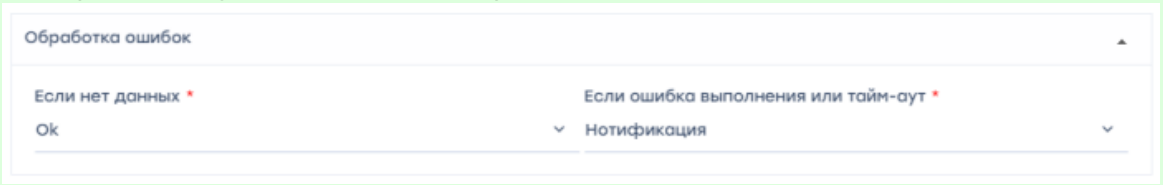
Step 4: Error handling

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:



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.

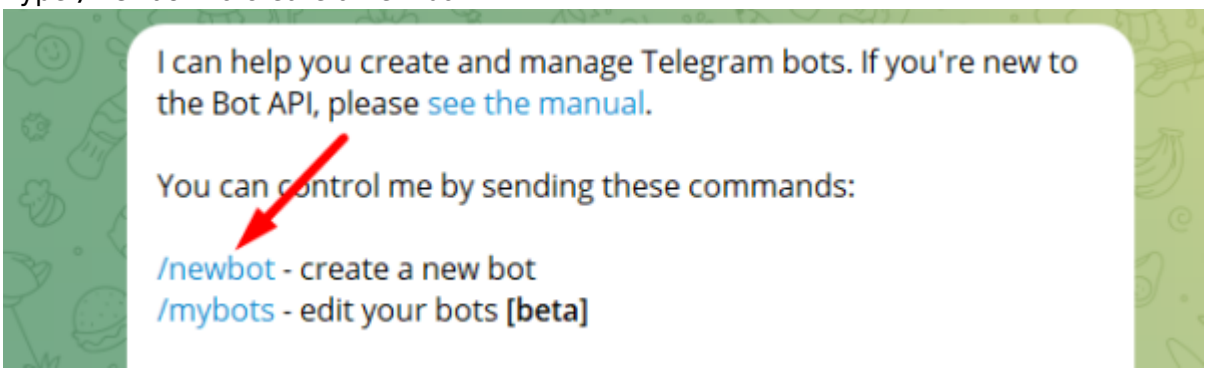
Step 5: Actions

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.

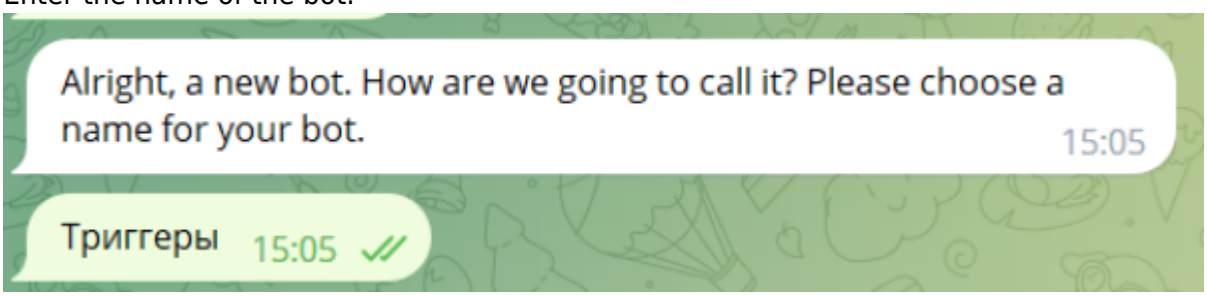
Telegram

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

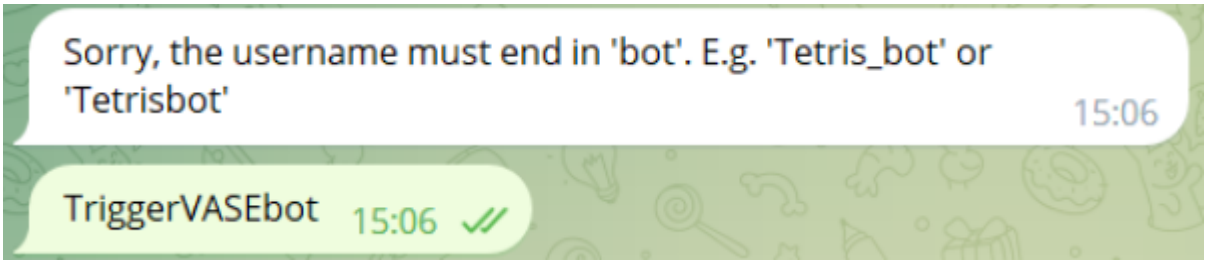
1. Start BotFather with the `/start` command.
2. Type `/newbot` to create a new bot.



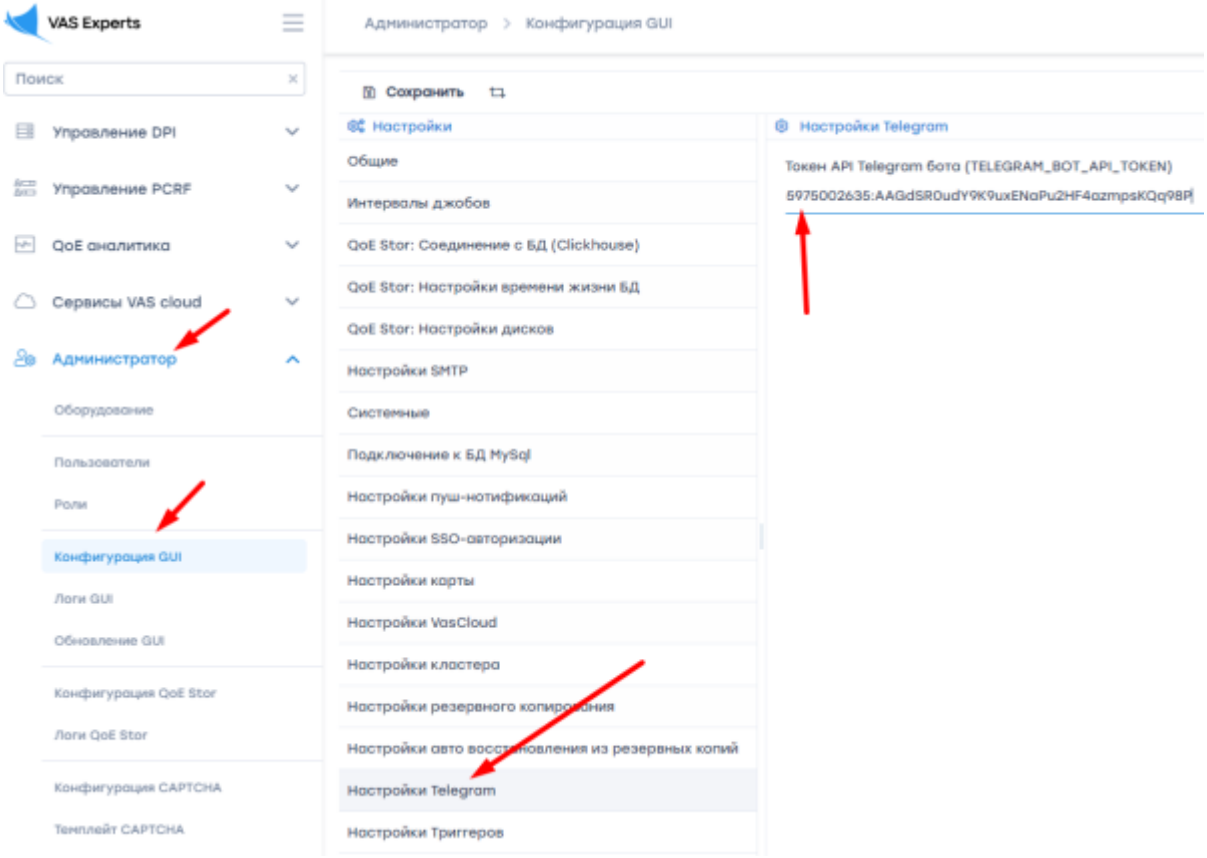
3. Enter the name of the bot.



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



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).



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

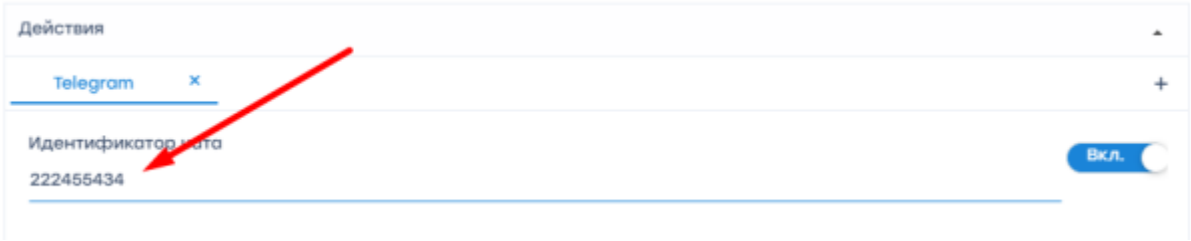
To get chat ID, user must have `username` in Telegram profile!

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

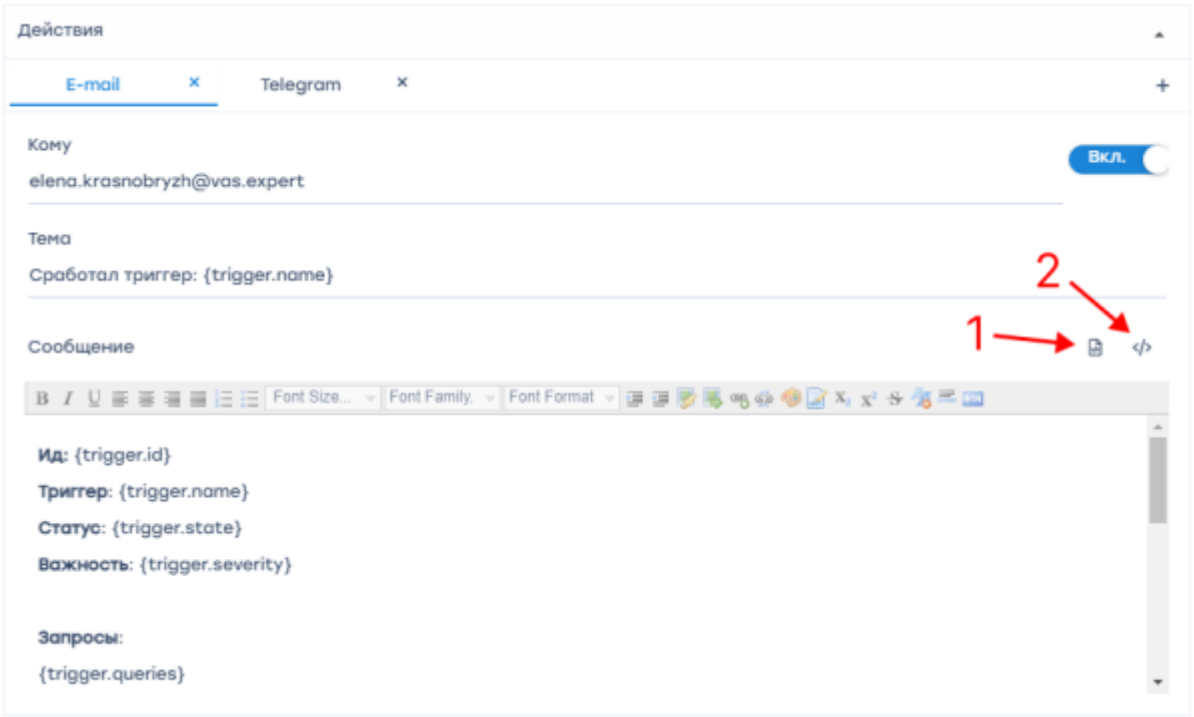
Add the ID from step 2 to the Telegram action in the "Chat ID" field.



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.



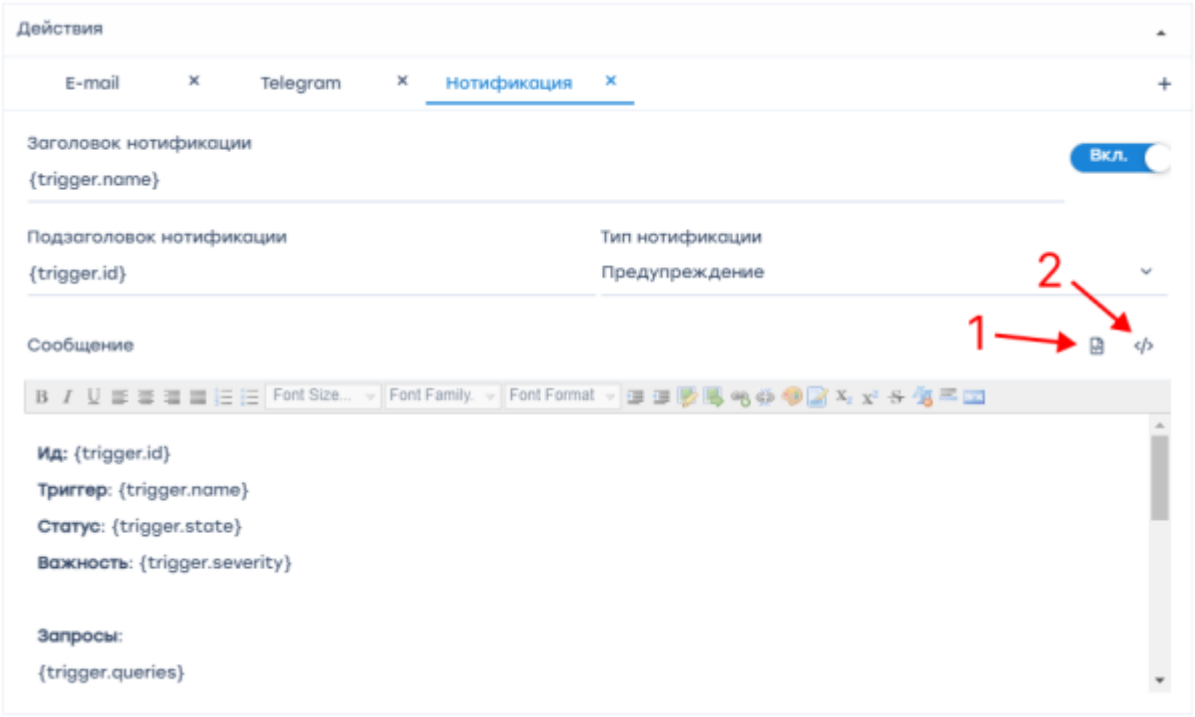
For E-mail actions to work, you need to configure SMTP. Go to Administrator → GUI Configuration, select "SMTP Settings".

GUI Notifications

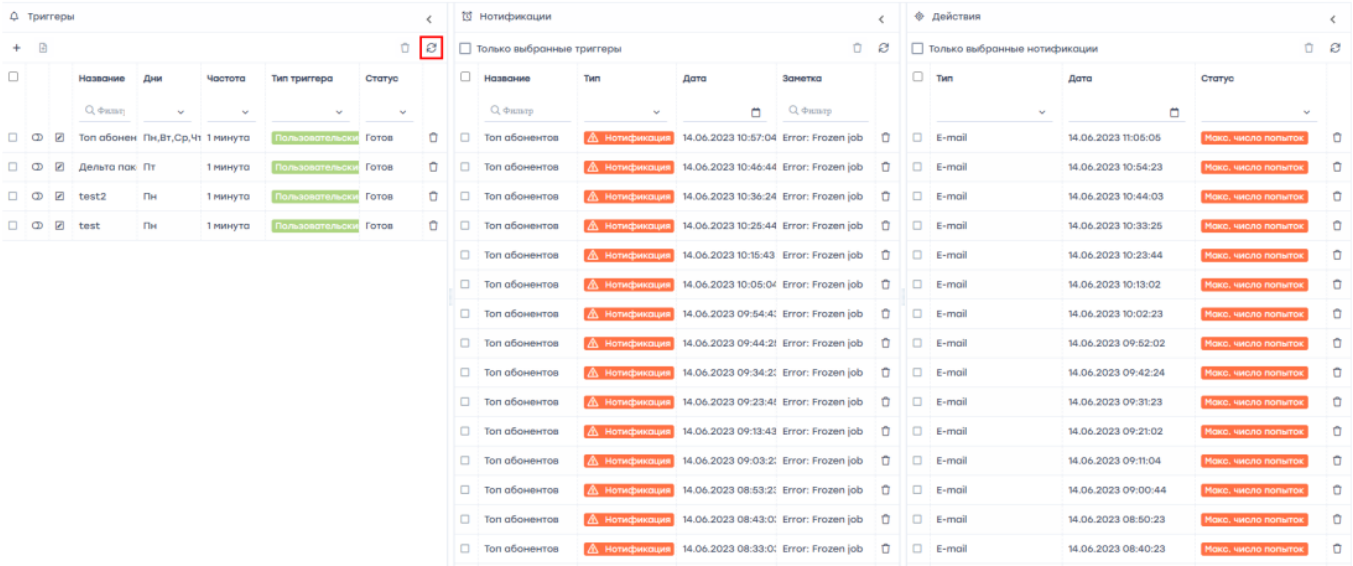
Notification can be used to test the functionality of triggers.

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.

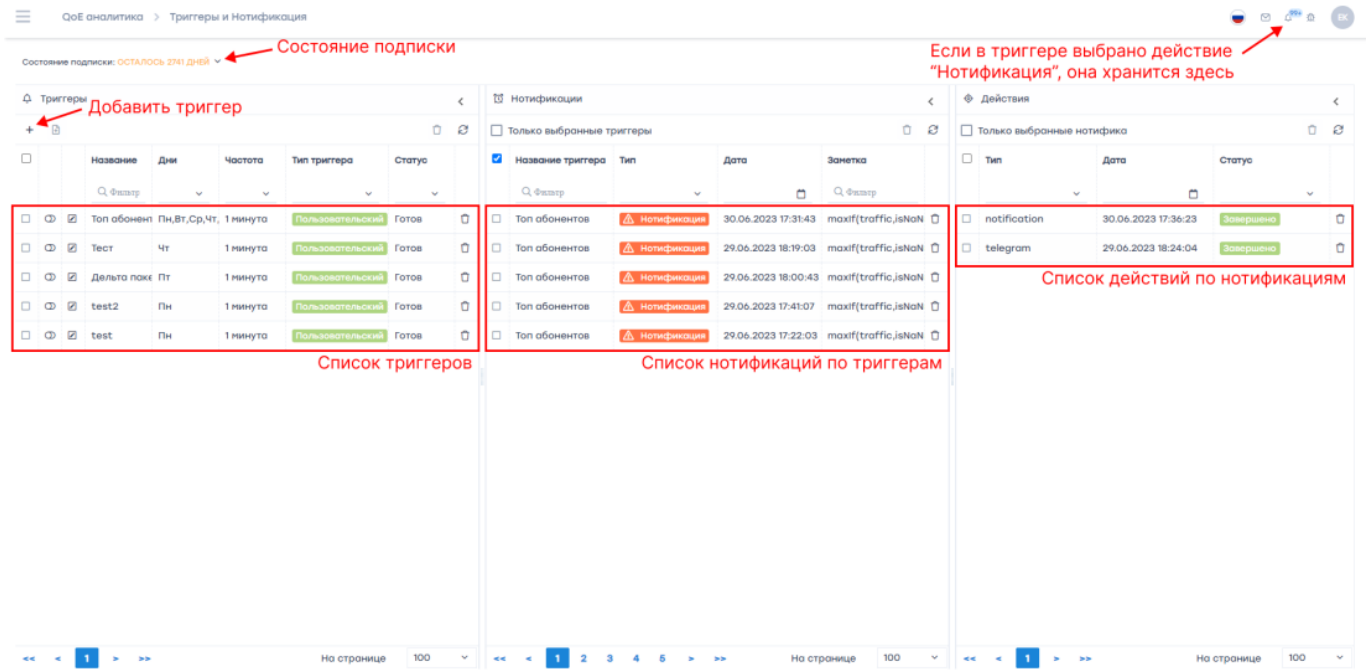


After creating a trigger, click “Save”. On the “Triggers” dashboard, enable the necessary triggers. If the GUI page has not been refreshed – refresh the page in the browser or click the “Refresh” button.



“Triggers and Notification” page elements description

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



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.