

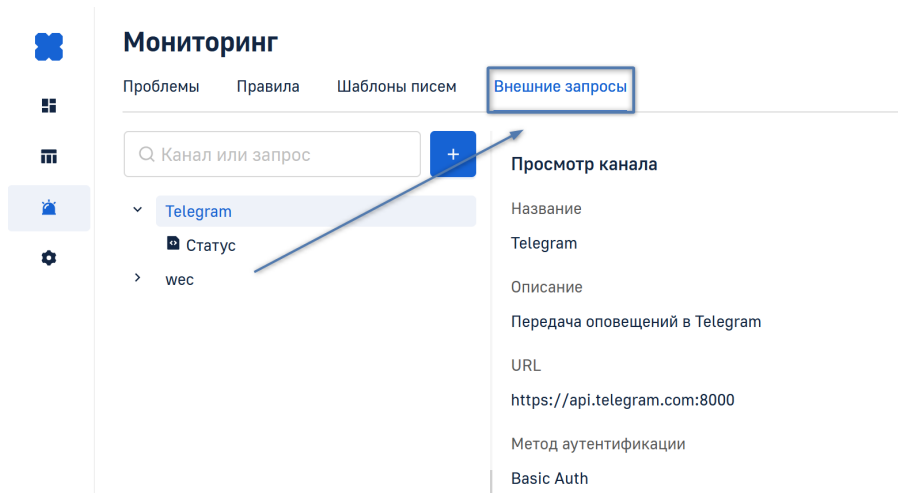
## Управление внешними каналами оповещений

В данной статье описано взаимодействие с внешними каналами и запросами для оповещений в Системе: как их добавить, просмотреть, найти, отредактировать, копировать и удалить.

### Общие сведения

Система позволяет отправлять оповещения об определенных событиях во внешние системы, такие как Zabbix, Jira, Telegram и т.д.

Для управления внешними каналами и запросами необходимо перейти на вкладку **Мониторинг** → **Внешние запросы**.



На вкладке **Внешние запросы** расположена таблица со списком всех существующих внешних каналов оповещений и запросов. Вся информация представлена в виде дерева с двумя уровнями вложенности: первый уровень отвечает за каналы оповещений, второй уровень отвечает за HTTP-запросы, с помощью которых оповещения отправляются в данные каналы.

### Добавление канала для оповещений

Для того чтобы добавить новый канал для оповещений, нажмите кнопку **+** в левой части таблицы и в выпадающем списке выберите **Создать канал**. После этого откроется модальное окно для конфигурации канала оповещений.

#### Создание канала оповещений

Название

Описание

URL

Метод аутентификации

Bearer Token

Токен

Ограничение запросов

Не больше 50 сообщений в 10 минут

Проверка TLS

[Отменить](#) [Создать](#)

В данном окне вам доступны следующие параметры для конфигурации:

- **Название** — название канала, которое будет отображаться в списке каналов и запросов;
- **Описание** — описание канала, которое будет отображаться в подробной информации о канале;
- **URL** — адрес для доступа к API внешнего канала для оповещений;
- **Метод аутентификации** — метод, который будет использоваться для аутентификации в данном канале:
  - **No Auth** — доступ без аутентификации;
  - **Bearer Token** — аутентификация с помощью токена в заголовке Authorization;
  - **Basic Auth** — аутентификация с помощью имени пользователя и пароля;
  - **Custom Headers** — аутентификация с помощью произвольных HTTP-заголовков;
  - **Cookies** — аутентификация с помощью куков.
- **Аутентификационные данные** — данные поля используются для ввода аутентификационных данных и различаются для каждого из методов аутентификации:
  - **No Auth** — для данного метода аутентификации поля отсутствуют;
  - **Bearer Token**:
    - **Токен** — поле для ввода токена аутентификации (**пример значения**: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0...36POk6yJV\_adQssw5c).

- **Basic Auth:**
  - **Логин** — поле для ввода имени пользователя для аутентификации (**пример значения:** username);
  - **Пароль** — поле для ввода пароля для аутентификации (**пример значения:** \$00perPa\$\$wd).
- **Custom Headers:**
  - **Ключ** — поле для ввода параметра, который будет использоваться для аутентификации (**пример значения:** X-API-Key);
  - **Значение** — поле для ввода значения параметра (**пример значения:** ar1cnpnctsuprwd).
- **Cookies:**
  - **Значение** — поле для ввода параметра и его значения для аутентификации (**пример значения:** PHPSESSID:n1goi0vnc9man9vcu01rvgdfr4).
- **Ограничение запросов** — максимальное количество запросов, которые должны отправляться по данному каналу в указанное количество минут/часов/дней;
- **Проверка TLS** — с помощью данного параметра вы можете отключить принудительную проверку SSL-сертификата при использовании протокола HTTPS.

Чтобы сохранить изменения, нажмите кнопку **Сохранить** в правом нижнем углу страницы. После этого вы будете автоматически перенаправлены на страницу со списком всех добавленных каналов и запросов. Нажмите кнопку **Отменить**, чтобы сбросить все внесенные изменения.

## Добавление запроса

Для того чтобы добавить новый HTTP-запрос, нажмите кнопку **+** в левой части таблицы и в выпадающем списке выберите **Создать запрос**. Вы также можете нажать кнопку **+** справа от имени канала в списке, чтобы автоматически выбрать канал для запроса. После этого откроется модальное окно для конфигурации запроса.

### Создание запроса

Название

1 Статус

Описание

2 Отправка статуса проблемы

Канал

3 Telegram

URL

4 https://api.telegram.com:8000 /status

Таймаут

5 20 сек

Повторять при ошибке

6 5 раз

### Настройки сообщения

Тип контента

7 application/json text/plain

Тело запроса

8 

```
{
  "rule": {
    "id": 0,
    "name": ""
  },
  "status": "",
  "lastExecution": "",
  "lastClosing": "",
  "level": "",
  "label": [""],
  "tenants": [
    {
      "id": 0,
      "name": ""
    }
  ]
}
```

Тест запроса

В данном окне вам доступны следующие параметры для конфигурации:

1. **Название** — название запроса, которое будет отображаться в списке каналов и запросов;
2. **Описание** — описание запроса, которое будет отображаться в подробной информации о запросе;
3. **Канал** — канал, в который будет отправляться данный запрос;
4. **URL** — путь для отправки запроса;
5. **Таймаут** — время в секундах до завершения запроса при отсутствии ответа;
6. **Повторять при ошибке** — количество повторных отправок запроса при ошибке;
7. **Тип контента** — тип содержимого тела запроса. Возможные значения:
  - **application/json;**
  - **text/plain.**
8. **Тело запроса** — поле для ввода HTTP-запроса.

Для того чтобы проверить работу написанного вами запроса, нажмите **Тест запроса**. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в правом нижнем углу страницы. После этого вы будете автоматически перенаправлены на страницу со списком всех добавленных каналов и запросов. Нажмите кнопку **Отменить**, чтобы сбросить все внесенные изменения.

## Переменные для запросов

При формировании HTTP-запросов вы можете использовать следующие переменные, разделенные на три группы:

- **Правило** — переменные, связанные с правилами оповещений:
  - **name;**
  - **description;**
  - **labels;**
  - **tenants;**
  - **executionCondition;**
  - **closingCondition.**
- **Проблема** — переменные, связанные с проблемами, по которым отправляются оповещения:
  - **status;**
  - **level;**
  - **executedAt;**
  - **closedAt;**
  - **link;**
  - **interval.from;**
  - **interval.to.**
- **События** — переменные, связанные с событиями, по которым заводятся проблемы:
  - **events.timestamp;**
  - **events.uuid;**
  - **events.event\_type;**
  - **events.action\_id;**
  - **events.action\_name;**
  - **events.key;**
  - **events.message;**
  - **events.registered\_process;**
  - **events.msgid;**

- events.id;
- events.category\_generic;
- events.category\_high;
- events.category\_low;
- events.assigned\_src\_host;
- events.assigned\_src\_ip;
- events.assigned\_src\_port;
- events.src\_asset;
- events.src\_fqdn;
- events.src\_geo\_asn;
- events.src\_geo\_city;
- events.src\_geo\_country;
- events.src\_geo\_org;
- events.src\_host;
- events.src\_hostname;
- events.src\_ip;
- events.src\_mac;
- events.src\_port;
- events.event\_src\_category;
- events.event\_src\_fqdn;
- events.event\_src\_host;
- events.event\_src\_hostname;
- events.event\_src\_id;
- events.event\_src\_ip;
- events.event\_src\_rule;
- events.event\_src\_subsys;
- events.event\_src\_title;
- events.event\_src\_vendor;
- events.assigned\_dst\_host;
- events.assigned\_dst\_ip;
- events.assigned\_dst\_port;
- events.dst\_asset;
- events.dst\_fqdn;
- events.dst\_geo\_asn;
- events.dst\_geo\_city;
- events.dst\_geo\_country;
- events.dst\_geo\_org;
- events.dst\_host;
- events.dst\_hostname;
- events.dst\_ip;
- events.dst\_mac;
- events.dst\_port;
- events.action;
- events.chain\_id;
- events.direction;
- events.duration;
- events.importance;
- events.logon\_auth\_method;
- events.logon\_service;
- events.logon\_type;
- events.protocol;
- events.protocol\_layer7;
- events.reason;
- events.start\_time;
- events.status;
- events.subject;
- events.subject\_account\_contact;
- events.subject\_account\_dn;
- events.subject\_account\_domain;
- events.subject\_account\_fullname;
- events.subject\_account\_group;
- events.subject\_account\_id;
- events.subject\_account\_name;
- events.subject\_account\_privileges;
- events.subject\_account\_session\_id;
- events.subject\_domain;
- events.subject\_group;
- events.subject\_id;
- events.subject\_name;
- events.subject\_privileges;
- events.subject\_process\_cmdline;
- events.subject\_process\_cwd;
- events.subject\_process\_fullpath;
- events.subject\_process\_guid;
- events.subject\_process\_hash;
- events.subject\_process\_id;
- events.subject\_process\_meta;
- events.subject\_process\_name;
- events.subject\_process\_original\_name;
- events.subject\_process\_parent\_cmdline;
- events.subject\_process\_parent\_fullpath;
- events.subject\_process\_parent\_guid;
- events.subject\_process\_parent\_hash;
- events.subject\_process\_parent\_id;
- events.subject\_process\_parent\_name;
- events.subject\_process\_parent\_path;
- events.subject\_process\_path;
- events.subject\_process\_version;
- events.subject\_state;
- events.subject\_type;
- events.subject\_version;
- events.object;
- events.object\_account\_contact;
- events.object\_account\_dn;
- events.object\_account\_domain;

- events.object\_account\_fullname;
- events.object\_account\_group;
- events.object\_account\_id;
- events.object\_account\_name;
- events.object\_account\_privileges;
- events.object\_account\_session\_id;
- events.object\_domain;
- events.object\_fullpath;
- events.object\_group;
- events.object\_hash;
- events.object\_id;
- events.object\_name;
- events.object\_new\_value;
- events.object\_num\_value;
- events.object\_path;
- events.object\_process\_cmdline;
- events.object\_process\_cwd;
- events.object\_process\_fullpath;
- events.object\_process\_guid;
- events.object\_process\_hash;
- events.object\_process\_id;
- events.object\_process\_meta;
- events.object\_process\_name;
- events.object\_process\_original\_name;
- events.object\_process\_parent\_cmdline;
- events.object\_process\_parent\_fullpath;
- events.object\_process\_parent\_guid;
- events.object\_process\_parent\_hash;
- events.object\_process\_parent\_id;
- events.object\_process\_parent\_name;
- events.object\_process\_parent\_path;
- events.object\_process\_path;
- events.object\_process\_version;
- events.object\_property;
- events.object\_query;
- events.object\_state;
- events.object\_storage\_fullpath;
- events.object\_storage\_id;
- events.object\_storage\_name;
- events.object\_storage\_path;
- events.object\_type;
- events.object\_value;
- events.object\_vendor;
- events.object\_version;
- events.recv\_host;
- events.recv\_ipv4;
- events.recv\_ipv6;
- events.recv\_time;
- events.count;
- events.count\_bytes;
- events.count\_bytes\_in;
- events.count\_bytes\_out;
- events.count\_packets;
- events.count\_packets\_in;
- events.count\_packets\_out;
- events.datafield1;
- events.datafield2;
- events.datafield3;
- events.datafield4;
- events.datafield5;
- events.datafield6;
- events.datafield7;
- events.datafield8;
- events.datafield9;
- events.datafield10;
- events.external\_link;
- events.interface;
- events.nas\_fqdn;
- events.numfield1;
- events.numfield2;
- events.numfield3;
- events.numfield4;
- events.numfield5;
- events.nas\_ip;
- events.tcp\_flag;
- events.tags;
- events.mime;
- events.correlation\_rule;
- events.original\_time;
- events.generator;
- events.datafield11;
- events.datafield12;
- events.datafield13;
- events.datafield14;
- events.datafield15;
- events.datafield16;
- events.datafield17;
- events.datafield18;
- events.datafield19;
- events.datafield20;
- events.src\_mac\_vendor;
- events.dst\_mac\_vendor;
- events.event\_src\_mac\_vendor;
- events.event\_src\_mac;
- events.external\_dst\_fqdn;

- events.external\_dst\_geo\_asn;
- events.external\_dst\_geo\_city;
- events.external\_dst\_geo\_country;
- events.external\_dst\_geo\_org;
- events.external\_dst\_host;
- events.external\_dst\_hostname;
- events.external\_dst\_ip;
- events.external\_dst\_mac\_vendor;
- events.external\_dst\_mac;
- events.external\_src\_fqdn;
- events.external\_src\_geo\_asn;
- events.external\_src\_geo\_city;
- events.external\_src\_geo\_country;
- events.external\_src\_geo\_org;
- events.external\_src\_host;
- events.external\_src\_hostname;
- events.external\_src\_ip;
- events.external\_src\_mac\_vendor;
- events.external\_src\_mac;
- events.object\_account\_company;
- events.object\_account\_department;
- events.object\_account\_provider;
- events.object\_account\_title;
- events.object\_application\_account\_domain;
- events.object\_application\_account\_id;
- events.object\_application\_account\_name;
- events.object\_application\_account\_privileges;
- events.object\_application\_account\_session\_id;
- events.object\_application\_name;
- events.object\_hash\_imphash;
- events.object\_hash\_md5;
- events.object\_hash\_sha1;
- events.object\_hash\_sha256;
- events.object\_process\_chain\_info;
- events.object\_process\_chain;
- events.object\_process\_decoded\_data;
- events.object\_process\_hash\_imphash;
- events.object\_process\_hash\_md5;
- events.object\_process\_hash\_sha1;
- events.object\_process\_hash\_sha256;
- events.object\_process\_parent\_decoded\_data;
- events.object\_process\_parent\_hash\_imphash;
- events.object\_process\_parent\_hash\_md5;
- events.object\_process\_parent\_hash\_sha1;
- events.object\_process\_parent\_hash\_sha256;
- events.subject\_account\_company;
- events.subject\_account\_department;
- events.subject\_account\_provider;
- events.subject\_account\_title;
- events.subject\_application\_account\_domain;
- events.subject\_application\_account\_id;
- events.subject\_application\_account\_name;
- events.subject\_application\_account\_privileges;
- events.subject\_application\_account\_session\_id;
- events.subject\_application\_name;
- events.subject\_process\_chain\_info;
- events.subject\_process\_chain;
- events.subject\_process\_decoded\_data;
- events.subject\_process\_hash\_imphash;
- events.subject\_process\_hash\_md5;
- events.subject\_process\_hash\_sha1;
- events.subject\_process\_hash\_sha256;
- events.subject\_process\_parent\_decoded\_data;
- events.subject\_process\_parent\_hash\_imphash;
- events.subject\_process\_parent\_hash\_md5;
- events.subject\_process\_parent\_hash\_sha1;
- events.subject\_process\_parent\_hash\_sha256.

По умолчанию максимальное количество элементов в списке — 10. При необходимости данное количество может быть увеличено с помощью конфигурационного файла.

## Поиск каналов и запросов

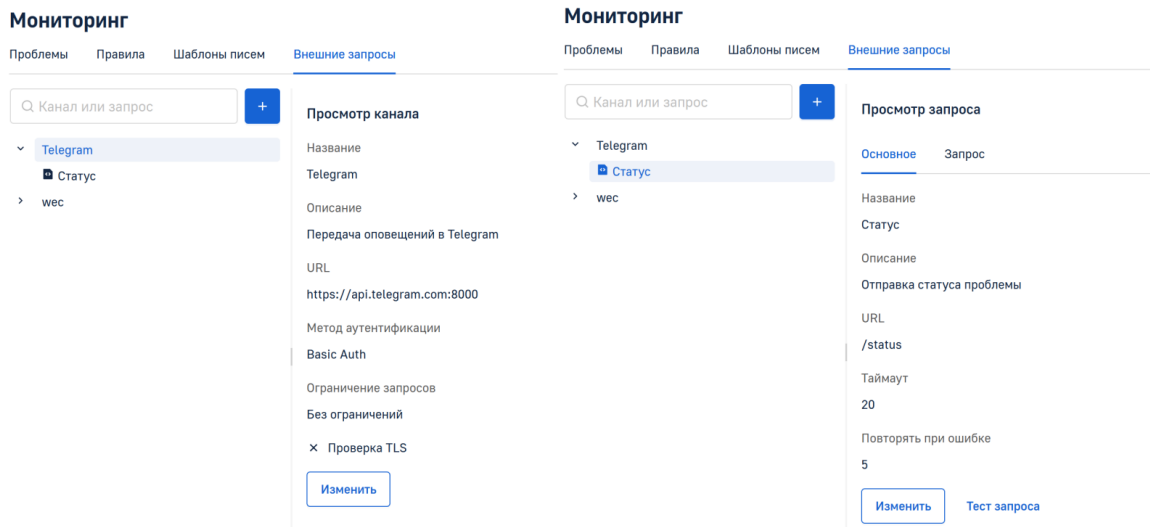
Для того чтобы найти определенный канал или запрос в списке, нажмите на форму поиска в левом верхнем углу таблицы и введите ключевое слово, после чего нажмите **Enter**.

The screenshot shows the 'Мониторинг' (Monitoring) interface. At the top, there are tabs for 'Проблемы', 'Правила', 'Шаблоны писем', and 'Внешние запросы'. Below the tabs is a search bar with the placeholder text 'Канал или запрос' and a blue '+' button. A blue arrow points to the search bar. Below the search bar is a list of items: 'Telegram', 'Статус', and 'wec'. To the right of the list is a 'Просмотр запро' (View request) button. Below the list is a table with columns 'Основное' and 'Зап'. The table has three rows: 'Название' and 'Статус'.

В качестве ключевых слов для поиска могут быть использованы названия каналов и запросов.

## Просмотр каналов и запросов

Для того чтобы просмотреть подробную информацию о параметрах канала или запроса, нажмите на него в списке и в правой части страницы отобразятся подробные данные.

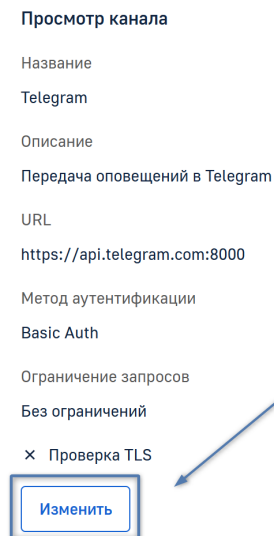


При просмотре канала все доступные данные будут отображены на одной вкладке. При просмотре HTTP-запроса на основной вкладке будут отображены основные параметры запроса, а его тело будет отображено на вкладке **Запрос**. В режиме просмотра вы также можете протестировать написанный вами запрос.

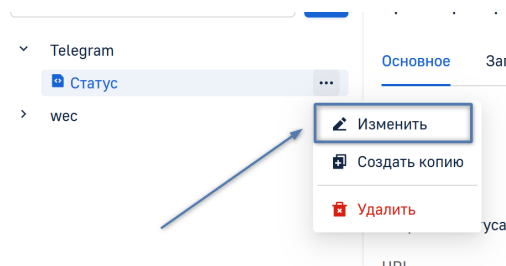
## Редактирование канала и запроса

Для того чтобы отредактировать ранее добавленный канал или запрос:

- Нажмите на канал или запрос в списке, после чего нажмите кнопку **Изменить** в левом нижнем углу:



- Нажмите на три точки справа от канала или запроса в списке, после чего в выпадающем списке выберите **Изменить**:



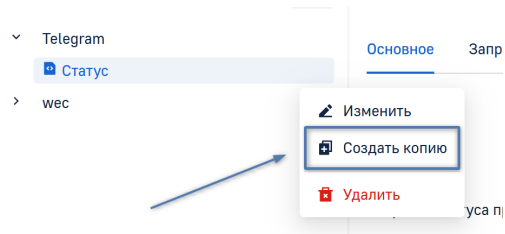
При нажатии будет открыто окно редактирования канала или запроса.

Чтобы сохранить изменения, нажмите кнопку **Сохранить** в правом нижнем углу страницы. После этого вы будете автоматически перенаправлены на страницу со списком всех добавленных каналов и запросов. Нажмите кнопку **Отменить**, чтобы сбросить все внесенные изменения.

## Копирование запроса

Копирование позволяет создать дубликат запроса для последующего редактирования. Для того чтобы скопировать запрос, нажмите на три точки справа

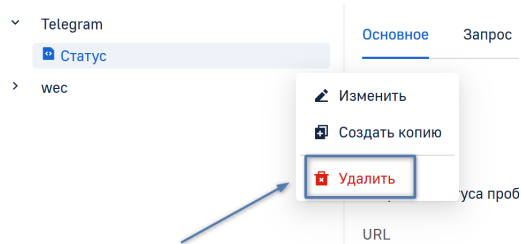
от его имени в списке, после чего выберите в выпадающем списке **Создать копию**.



После этого откроется страница редактирования скопированного запроса. Для сохранения копии нажмите **Сохранить** после внесения всех изменений.

## Удаление канала и запроса

Для того чтобы удалить канал или запрос, нажмите на три точки справа от его имени в списке, после чего выберите в выпадающем списке **Удалить**.



После этого, во всплывающем окне нажмите кнопку **Да, удалить** для подтверждения удаления. Если вы передумали удалять канал или запрос, нажмите кнопку **Отменить**.

---

ID статьи: 1566

Последнее обновление: 3 апр., 2026

Обновлено от: Михалева А.

Ревизия: 1

База знаний Логикор -> Документация -> Система хранения и обработки данных «Логикор». Версия 2.7.0 -> Логикор. Руководство администратора ->

Мониторинг и оповещения -> Управление внешними каналами оповещений

<https://docs.axel.pro/entry/1566/>