

# Работа в режиме ручного ввода SQL-запроса

В данной статье описана работа с событиями в режиме ручного ввода SQL-запросов.

## Общие сведения

При необходимости, вы можете ввести SQL-запрос вручную. Для этого нажмите на поле ввода SQL-запроса и отредактируйте его содержимое под свои нужды.



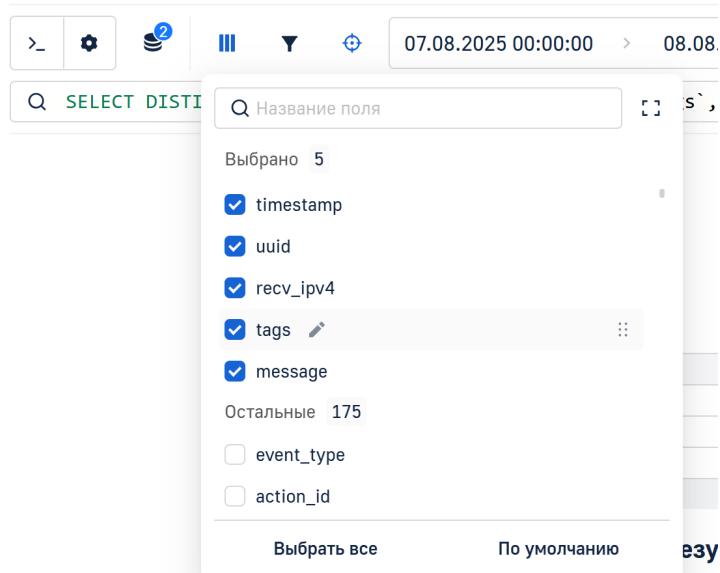
В данном режиме доступен следующий функционал:

- Выбор режима** — выбор режима построения запроса;
- Автоматическое определение синтаксиса SQL** — подсвечивает синтаксис SQL-запроса в поле для его ввода (параметр активирован по умолчанию);
- Выбор тенанта** — позволяет выбирать тенанты, в которых будет выполняться поиск событий;
- Выбор колонок (SELECT)** — позволяет выбирать колонки, которые будут использоваться в запросе;
- Выбор фильтров (WHERE)** — позволяет выбирать фильтры, которые будут использоваться в запросе;
- Только уникальные строки** — позволяет исключить повторяющиеся строки из результатов выполнения запроса;
- Определение временных рамок** — позволяет выбрать промежуток времени, за который будут отображаться события.

## Выбор колонок (SELECT)

Для упрощения навигации по списку, вы можете выбирать список и порядок отображаемых колонок. Используйте переключатель слева от имени поля, для того, чтобы включить или выключить отображение колонки в таблице. По умолчанию выбраны первые 3 поля.

Для того, чтобы изменить порядок отображения колонок, наведите курсор на иконку сортировки справа от имени колонки, зажмите левую кнопку мыши и перенесите элемент в необходимое место.



Вы также можете установить псевдонимы для каждой из колонок. Для этого наведите курсор на имя интересующей вас колонки и нажмите на всплывающую иконку карандаша. После этого появится поле для ввода псевдонима. Нажмите на галочку чтобы подтвердить применение псевдонима. После обновления запроса имя колонки будет заменено на установленный псевдоним.

Название поля

Выбрано 5

- timestamp
- uuid
- recv\_ipv4
- tags
- message

Остальные 175

## Фильтры (WHERE)

### Условия

Для работы с условиями можно использовать функционал фильтров таблицы.

После этого откроется список всех примененных к таблице фильтров. Для того, чтобы добавить условие, нажмите **+ Добавить условие** и заполните всю необходимую информацию:

- **Поле** — поле в базе данных, по которому будет выполняться фильтрация;
- **Оператор** — выбор оператора для фильтрации. Возможные значения **И** и **ИЛИ**;
- **Значение** — значение, по которому будет выполняться фильтрация.

При добавлении двух и более фильтров вы можете построить более сложные выборки с использованием операторов **И** и **ИЛИ**.

Чтобы удалить условие нажмите на иконку корзины справа от него.

### Групповые фильтры

Вы также можете добавить группу для условий. Для этого в окне выбора фильтров нажмите **Добавить группу**.

Показать события

Где message Равно REJECT  
И uuid Не равно 0

+ Добавить условие + Добавить группу

**ИЛИ**

Где message Равно ACCEPT  
И uuid Не равно 0

+ Добавить условие + Добавить группу

И action\_id Содержит %login%

+ Добавить условие + Добавить группу

Включая пустые значения для оператора «не равно»

Очистить всё

Условия, сформированные в группы, можно использовать для построения сложных выборок с использованием операторов **И** и **ИЛИ**.

Группа 1 +   
Подгруппа 1.1 ...

Чтобы удалить группу нажмите на иконку корзины справа от нее.

## Определение временных рамок

Для того, чтобы отфильтровать список событий по времени их регистрации, нажмите **Выберите диапазон** справа от конструктора запроса. Во всплывающем окне вы можете ввести диапазон дат и времени вручную, либо выбрать одно из предустановленных значений.

Начальная дата > Конечная дата Выполнить

mp` , Диапазон дат, в часовом поясе Etc/GMT-7, UTC + 07:00

Свой формат	август 2025	сентябрь 2025	
5 минут	Пн Вт Ср Чт Пт Сб Вс	Пн Вт Ср Чт Пт Сб Вс	
19-5f9	15 минут	28 29 30 31 1 2 3	1 2 3 4 5 6 7
j3-83c	30 минут	4 5 6 7 8 9 10	8 9 10 11 12 13 14
j0-09j	1 час	11 12 13 14 15 16 17	15 16 17 18 19 20 21
6-427	4 часа	18 19 20 21 22 23 24	22 23 24 25 26 27 28
70-937	12 часов	25 26 27 28 29 30 31	29 30 1 2 3 4 5
d7-2e1	24 часа	1 2 3 4 5 6 7	6 7 8 9 10 11 12
I1-822	2 дня	-	wstintdtqycyqmkcbc... etaqzrbm...
41-7afa-1435-0...	-	-	-

После того как вы выбрали временной диапазон, нажмите **Выполнить**, чтобы обновить список событий.

ID статьи: 1395

Последнее обновление: 19 авг., 2025

Обновлено от: Егоров В.

Ревизия: 1

База знаний LogIQ -> Документация -> Система хранения и обработки данных «LogIQ». Версия 2.6.0 -> LogIQ. Руководство пользователя -> Раздел «События» -> Работа в режиме ручного ввода SQL-запроса

<https://docs.axel.pro/entry/1395/>