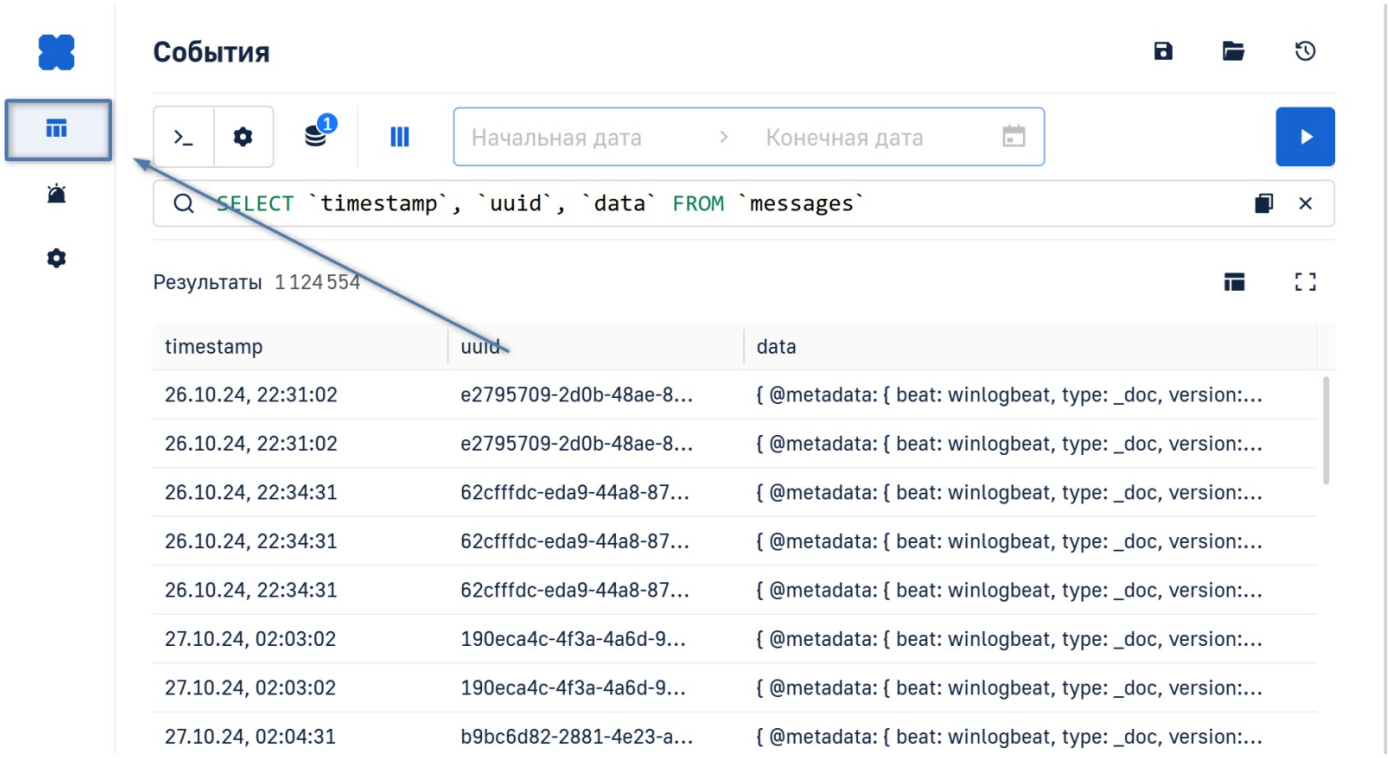
Работа с событиями в формате JSON

В данной статье описана работа с событиями в формате JSON: как просматривать и фильтровать такие события, а также сохранять запросы фильтрации.

Режим просмотра JSON-событий активируется с помощью внесения изменений в конфигурационные файлы системы. Подробное описание процесса описано в Руководстве разработчика.

Раздел **События** позволяет формировать запрос на выборку событий в формате JSON. Для перехода в раздел нажмите на иконку **События** в левом боковом меню.



На данной странице отображаются все зарегистрированные в Системе события в формате JSON. Здесь вы можете просмотреть список событий, отфильтровать и экспортировать события.

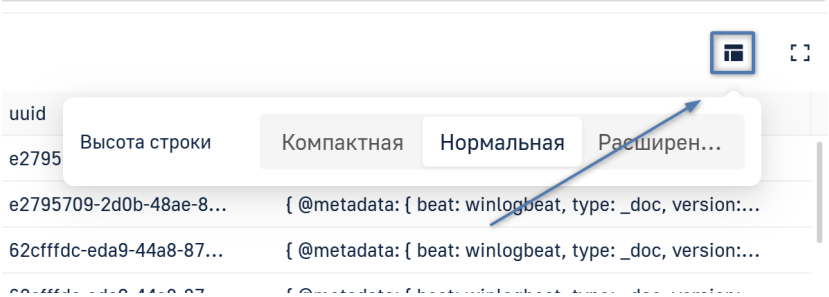
Управление таблицей

По умолчанию на странице отображается 100 записей, однако вы можете выбрать отображение 20, 50, 100 и 500 записей на странице. Для этого нажмите на поле в правом верхнем углу списка и выберите в выпадающем списке необходимое количество для отображения.

Для переключения между страницами используйте блок в левом нижнем углу списка, или введите конкретную страницу и нажмите клавишу **Enter**:

Конфигурация отображения таблицы

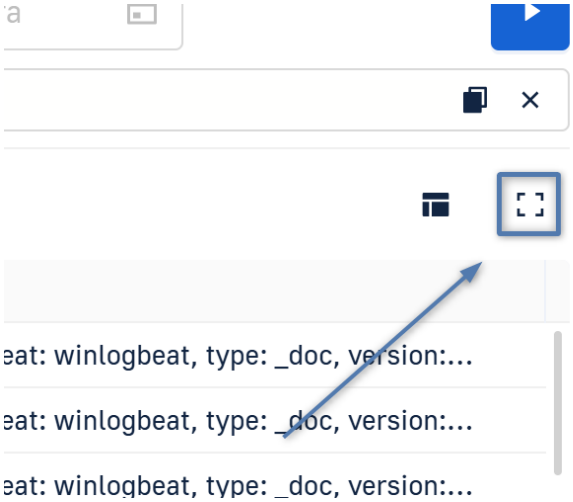
Вы можете сконфигурировать отображение таблицы событий. Для этого нажмите на иконку шестеренки в правом верхнем углу таблицы:



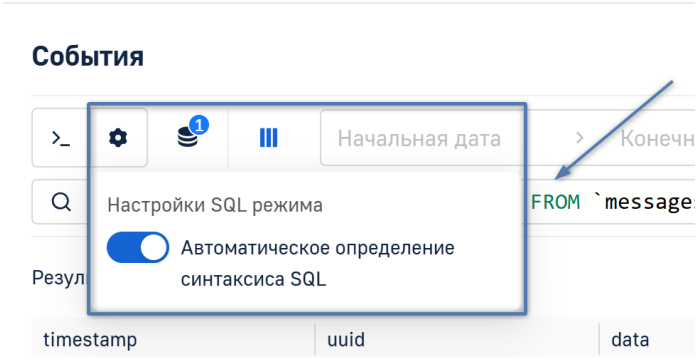
В выпадающем меню вы можете настроить следующие параметры:

- **Высота строки** — высота строк в таблице событий. Доступные значения: **Компактная**, **Нормальная** и **Расширенная**.

Также вы можете развернуть таблицу в режим полноэкранного отображения. Для этого нажмите на иконку рамок в правом верхнем углу таблицы:

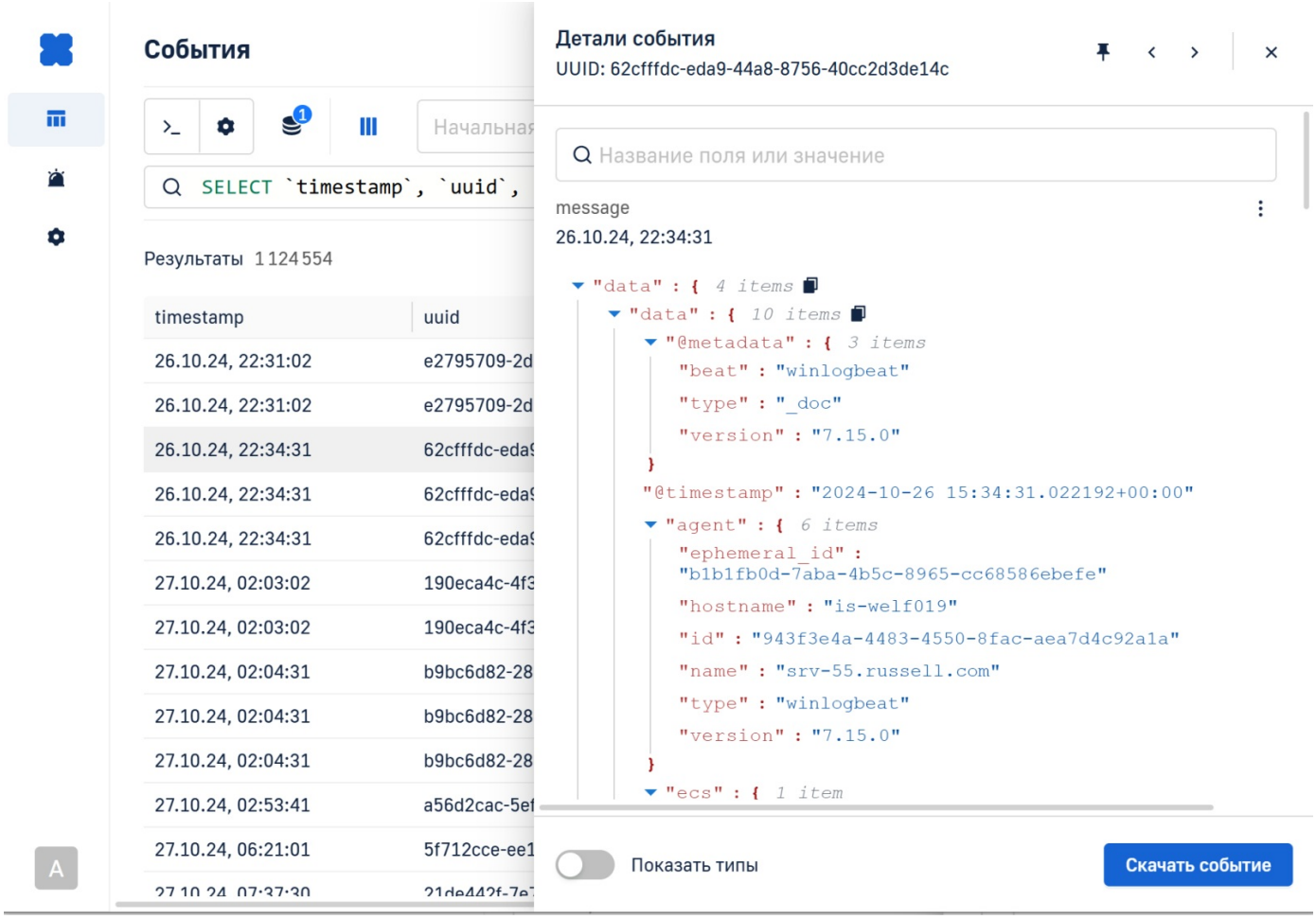


Вы можете активировать автоматическую подсветку синтаксиса в ваших SQL-запросах. Для этого нажмите на иконку шестеренки в левой верхней части страницы и активируйте параметр **Автоматическое определение синтаксиса SQL**.



Просмотр событий

Все события отображаются в виде списка в таблице. Для того, чтобы просмотреть содержимое JSON-события, нажмите на его строку. После этого содержимое отобразится в правом сайдбаре.



Для быстрого переключения между событиями нажмите на иконки стрелочек в правом верхнем углу сайдбара. Чтобы подсветить определенный элемент в содержимом, нажмите на поле поиска и введите имя данного элемента. Переключатель **Показать типы** активирует/деактивирует отображение типов полей (**Int64**, **string** и т.д.). Вы также можете скопировать содержимое блока в запросе, нажав на иконку копии, которая появляется при наведении курсора на строку.

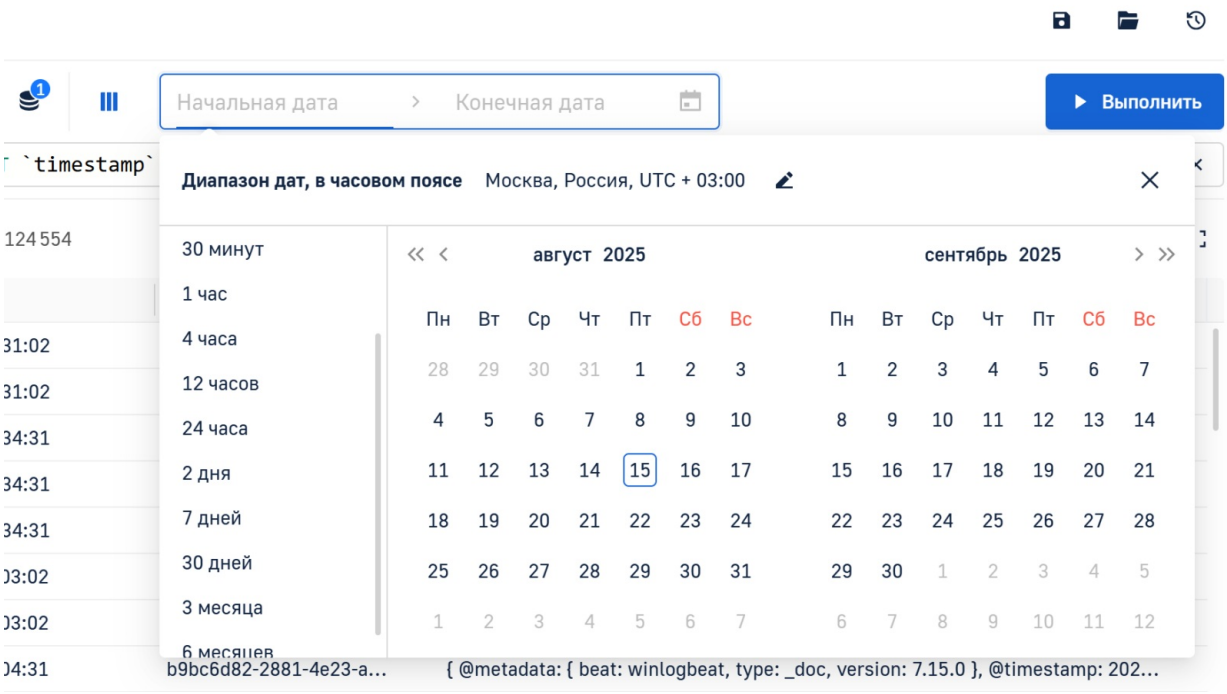
Фильтрация, сортировка и группировка событий

Для того, чтобы отфильтровать события, можно использовать следующие инструменты:

- Определение временных рамок;
- Поле ввода SQL-запроса;
- Сортировка таблицы с помощью колонок.

Определение временных рамок

Для того, чтобы отфильтровать список событий по времени их регистрации, нажмите на поле выбора даты, расположенное в верхнем левом углу страницы. В модальном окне вы можете ввести диапазон дат и времени вручную, либо выбрать одно из предустановленных значений.



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

Поле ввода SQL-запроса

Для того, чтобы отфильтровать, отсортировать или сгруппировать события, вы можете отредактировать исходный SQL-запрос.

При вводе SQL-запроса необходимо соблюдать следующие правила:

1. Следует использовать только запрос **SELECT**. Попытка обновить таблицу с любым другим запросом приведет к ошибке.
2. В запросе нельзя указывать параметр пагинации **OFFSET**.
3. Наименование полей необходимо указывать в апострофах, например **`event.type`**.

Ниже приведены примеры запросов для каждого из действий.

Поиск событий (SELECT)

```
SELECT data.json.computer_name, data.winlog.api FROM `messages`
```

Установка псевдонима (Alias) для поля

```
SELECT data.agent.id AS agid, data.agent.name AS agname, data.json.task AS jtask
FROM messages
WHERE (agid LIKE '%0d%') AND (agname LIKE '%-%') AND (jtask LIKE '%else%')
```

Фильтрация событий (WHERE)

```
SELECT data.agent.id, data.agent.name, data.json.task
FROM messages
WHERE (data.agent.id LIKE '%0d%') AND (data.agent.name LIKE '%-%') AND (data.json.task LIKE '%else%')
```

Подсчет количества событий (COUNT)

```
SELECT COUNT(*) FROM messages
WHERE (data.agent.id LIKE '%0d%') AND (data.agent.name LIKE '%-%') AND (data.json.task LIKE '%else%') AND (timestamp != '2025-01-02')
FORMAT TabSeparated
```

Группировка событий (GROUP BY)

```
SELECT
   data.json.process.pid.:Int64
FROM messages
GROUP BY data.json.process.pid.:Int64
```

Сортировка событий (ORDER BY)

```
SELECT
   data.json.process.pid.:Int64
```

```
FROM messages
ORDER BY data.json.process.pid.:Int64 DESC
```

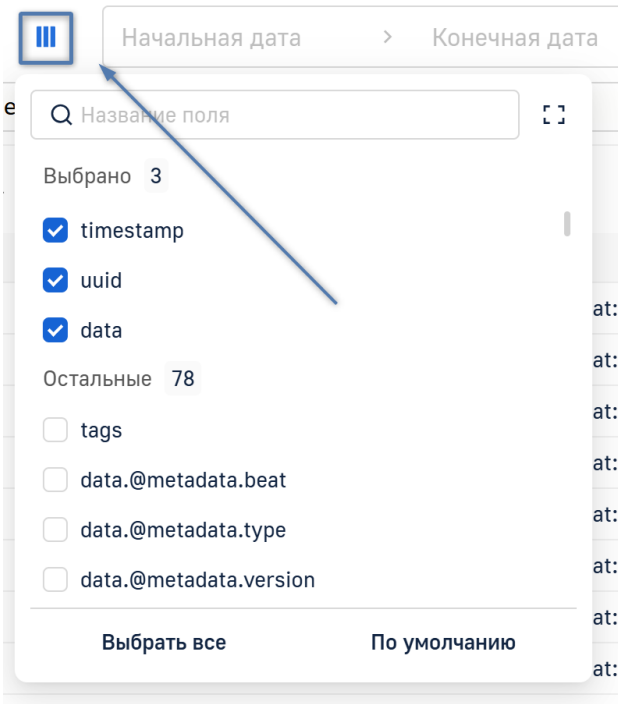
Для корректной работы команд **GROUP BY**, **COUNT** и **ORDER BY** необходимо указать в запросе типы полей в формате **имя_поля.:тип_поля**.

Сортировка таблицы с помощью колонок

Данный функционал доступен только при использовании режима **Автоматического определения синтаксиса SQL**.

Для упрощения навигации по списку, вы можете выбрать список и порядок отображаемых колонок. Для этого нажмите на иконку колонок в левом верхнем углу таблицы. Отметьте те поля, которые должны отображаться в таблице. По умолчанию выбраны первые 3 поля.

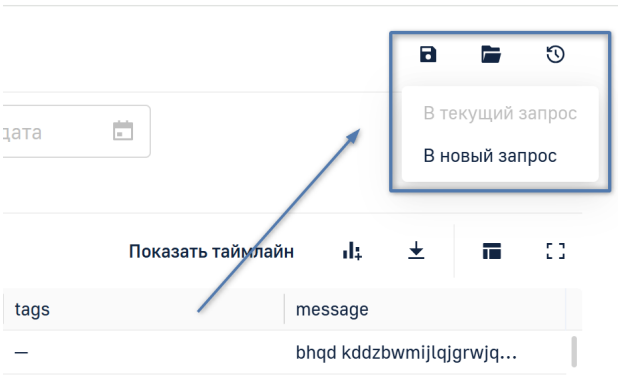
Для того, чтобы изменить порядок отображения колонок, наведите курсор на иконку сортировки справа от имени колонки, зажмите левую кнопку мыши и перенесите элемент в необходимое место.



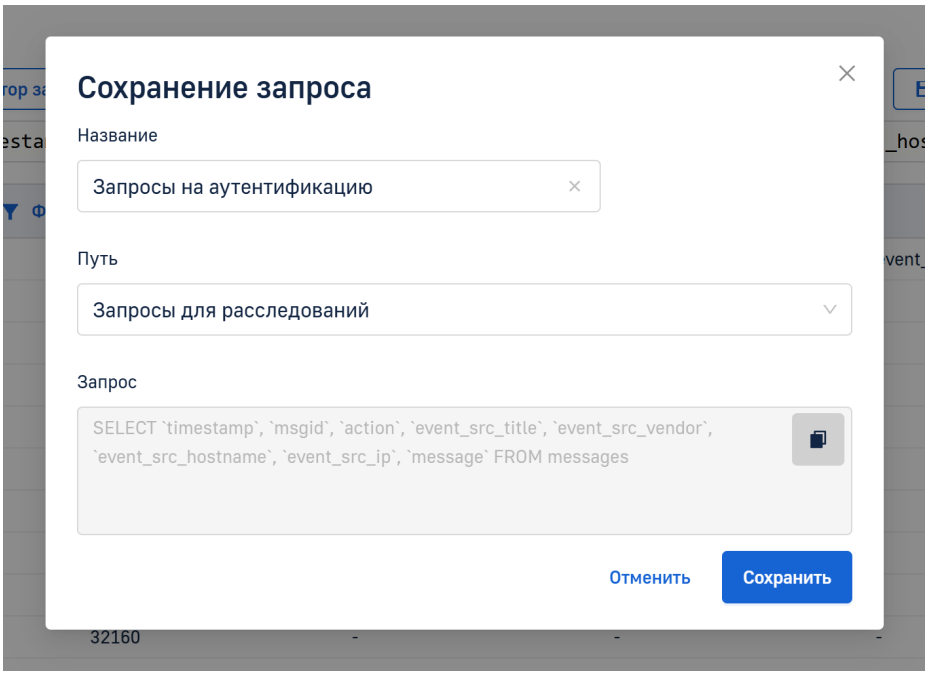
Сохраненные запросы

Сохранение запросов

Для удобства ежедневного использования вы можете сохранить ваши запросы и фильтры. Для этого нажмите на иконку дискеты в правом верхнем углу страницы, затем в выпадающем меню выберите вариант сохранения — в текущий запрос, или в новый.

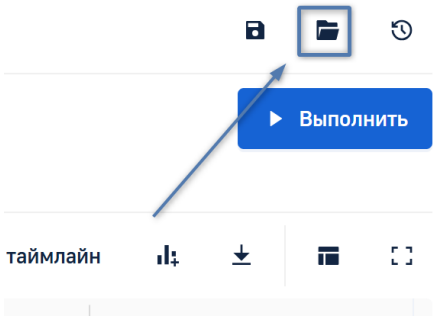


Если вы выбрали **В новый запрос**, откроется новое окно, в котором вы сможете задать имя запроса и указать путь для его сохранения. Для сохранения запроса нажмите **Сохранить**.



Использование сохраненных запросов

Для того, чтобы отфильтровать список событий по ранее сохраненным параметрам, нажмите на иконку сохраненных запросов правом верхнем углу страницы, затем в правом сайдбаре выберите ранее сохраненный запрос.

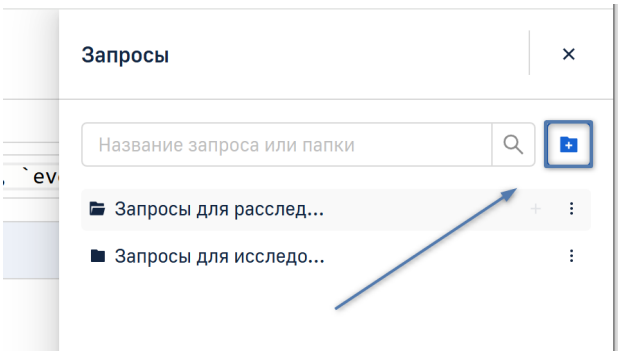


Управление хранилищем сохраненных запросов

Вы можете управлять файловой системой хранения запросов: создавать папки, а также переименовывать, перемещать и удалять папки и сохраненные запросы.

Создание новой папки

Для того, чтобы добавить новую папку, нажмите на иконку добавления в правом верхнем углу дашборда.



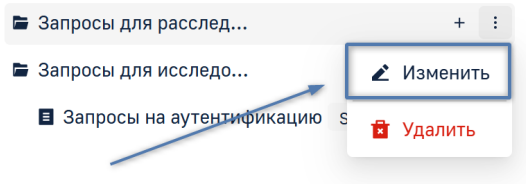
Введите имя для новой папки и нажмите **Создать**.

Если вы хотите создать папку внутри уже существующей, наведите на мышку на корневую папку и нажмите на появившуюся иконку **+**, введите имя для новой папки и нажмите **Создать**.

Редактирование содержимого

Для того, чтобы отредактировать сохраненный запрос или папку, нажмите на три точки справа от имени и в выпадающем

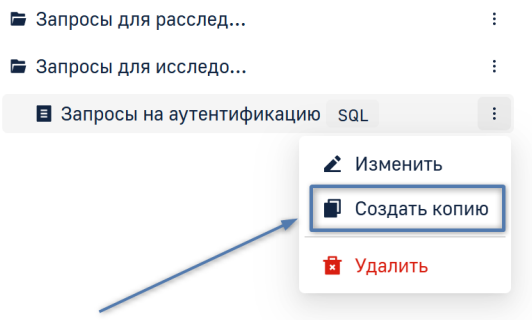
списке выберите **Изменить**.



В открывшемся окне вы можете переименовать и изменить путь к запросу или папке, а также просмотреть содержимое сохраненного запроса. Нажмите **Сохранить** для применения изменений.

Создание копии сохраненного запроса

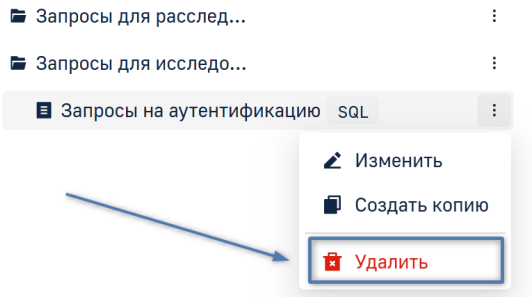
Для того, чтобы создать копию сохраненного запроса, нажмите на три точки справа от имени и в выпадающем списке выберите **Создать копию**.



Выберите путь для сохранения копии запроса и нажмите **Создать копию**.

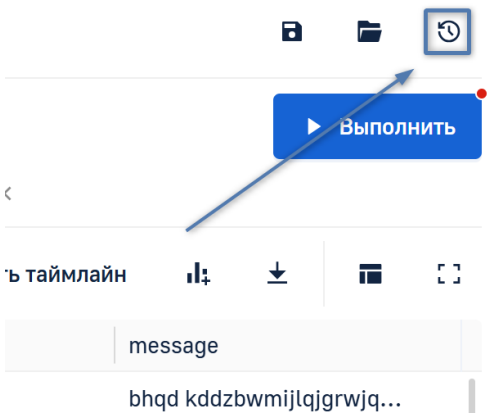
Удаление содержимого

Для того, чтобы удалить сохраненный запрос или папку, нажмите на три точки справа от имени и в выпадающем списке выберите **Удалить**.



Просмотр истории запросов

Для того, чтобы повторить один из ранее использованных запросов, вы можете воспользоваться историей запросов. Для этого нажмите на иконку истории и выберите интересующий вас запрос в правом сайдбаре.

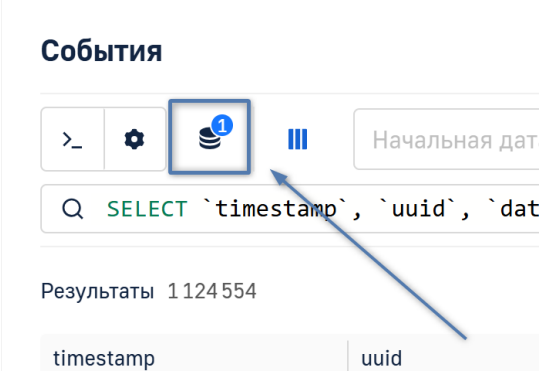


В данном сайдбаре вы можете просмотреть следующую информацию о запросах:

- Дата выполнения запроса;
- Режим выполнения запроса;
- Продолжительность выполнения запроса;
- Содержимое запроса;
- Срок хранения данного запроса в истории.

Выбор тенантов

Для того, чтобы просмотреть события только для определенных тенантов, нажмите на иконку базы данных в левом верхнем углу и выберите тенанты, для которых вы хотите просмотреть выборку.



ID статьи: 1267
Последнее обновление: 19 авг., 2025
Обновлено от: Егоров В.
Ревизия: 8
База знаний LogIQ -> Документация -> Система хранения и обработки данных «LogIQ». Версия 2.5.0 -> LogIQ. Руководство пользователя -> Раздел «События» -> Работа с событиями в формате JSON
https://docs.axel.pro/entry/1267/