

Просмотр и конфигурация журнала аудита

В данной статье описано взаимодействие с историей действий пользователей в Системе: как просмотреть и отфильтровать действия пользователей в Системе, а также описан процесс настройки длительности хранения записей в журнале.

Общие сведения

Для просмотра истории действий пользователей в Системе, необходимо перейти на страницу **Настройки → Журнал аудита**.

☒

☐

☐

🔔

⚙️

Журнал аудита

Срок хранения

Обновить

Полнотекстовый поиск

🔍

🔼 Фильтры

Когда	Логин	Пользователь	Событие
Сегодня, 17:41	admin	Локальный	Изменен виджет «Статистика по action» на дашборде «Основной ...
Сегодня, 17:41	admin	Локальный	Загружен дашборд «Основной дашборд»
Сегодня, 17:39	admin	Локальный	Отправлен IQL запрос на просмотр событий: «select timestamp, m...
Сегодня, 17:15	admin	Локальный	Вход 10.31.230.158
Сегодня, 16:41	admin	Локальный	Отправлен IQL запрос на просмотр событий: «select timestamp, m...
Сегодня, 16:40	—	—	Уведомление о проблеме отправлено: responder@axel.pro
Сегодня, 16:40	—	—	Создана проблема из правила «Demo Rule» с уровнем критичеснос...
Сегодня, 16:39	admin	Локальный	Отправлен IQL запрос на просмотр событий: «select timestamp, m...
Сегодня, 16:31	admin	Локальный	Изменено правило оповещения «Критичное правило New»
Сегодня, 16:30	admin	Локальный	Изменено правило оповещения «Demo Rule»

<

1

2

3

4

5

...

29

>

Перейти к

20

На данной странице отображается таблица со списком всех произведенных пользователями действий в различных разделах Системы:

- Дашборды: События:
 - Создан дашборд;
 - Переименован дашборд;
 - Удален дашборд;
 - Импортирован дашборд;
 - Экспортирован дашборд;
 - Доступ пользователя к дашборду предоставлен;
 - Доступ пользователя к дашборду отозван;
 - На дашборде создан виджет;
 - На дашборде изменен виджет;
 - С дашборда удален виджет;
 - На дашборд импортирован виджет;
 - С дашборда экспортирован виджет.
 - Скачаны события из тенанта;
 - Создан SQL-запрос;
 - Изменен SQL-запрос;
 - Удален SQL-запрос;
 - Создана папка SQL-запросов;
 - Изменена папка SQL-запросов;
 - Удалена папка SQL-запросов;
 - Отправлен запрос на просмотр событий.
- Оповещения:
 - Создано правило оповещения;
 - Изменено правило оповещения <"Название правила">
 - Удалено правило оповещения;
 - Создан шаблон письма;
 - Изменен шаблон письма;
 - Удален шаблон письма;
 - Закрыто оповещение по правилу;
 - Открыто оповещение по правилу.

- **Тенанты:**
 - Создан тенант;
 - Изменен тенант;
 - Удален тенант.
- **Пользователи:**
 - Авторизация пользователя;
 - Неудачная попытка входа;
 - Окончание сессии пользователя;
 - Создан пользователь;
 - Изменены данные пользователя;
 - Удалён пользователь;
 - Заблокирован пользователь;
 - Разблокирован пользователь.
- **Роли:**
 - Создана роль;
 - Изменена роль;
 - Удалена роль;
 - Изменена роль по умолчанию.
- **LDAP:**
 - Изменены настройки LDAP-подключения.
- **SMTP:**
 - Изменены настройки SMTP-подключения.
- **Компоненты системы:**
 - Попытка запуска синхронизации правил корреляции;
 - Попытка запуска синхронизации правил нормализации.
- **Конфигурационные файлы:**
 - Загружен файл;
 - Загружена папка;
 - Скачан объект;
 - Создан файл;
 - Создана папка;
 - Удален файл;
 - Удалена папка;
 - Переименован файл.

Таблица содержит следующие поля:

- **Когда** — точная дата и время, когда было произведено то или иное действие;
- **Логин** — имя пользователя, совершившего то или иное действие;
- **Пользователь** — тип пользователя, совершившего то или иное действие;
- **Событие** — описание действия, которое произвел пользователь.

Поиск и фильтрация событий

Для того, чтобы найти определенного пользователя в списке, нажмите на форму поиска в левом верхнем углу таблицы и введите ключевое слово.

Журнал аудита

Полнотекстовый поиск			Фильтры
Когда	Логин	Пользователь	
Сегодня, 13:28	admin	Локал	
Сегодня, 13:28	admin	Локал	
Сегодня, 13:28	admin	Локал	

В качестве ключевых слов для поиска могут быть использованы:

- Имя пользователя;
- Текст события.

Вы также можете отфильтровать список событий по следующим параметрам:

- **Кто** — фильтрация по пользователю, совершившему то или иное действие;
- **Когда** — фильтрация по дате и времени, когда было произведено то или иное действие;
- **Раздел** — фильтрация по разделу Системы, в котором было произведено то или иное действие;
- **Что произошло** — фильтрация по типу действия, совершенному в Системе.

Для этого нажмите на иконку фильтра и выберите параметры для фильтрации списка.

Журнал аудита

Полнотекстовый поиск		Фильтры	
Когда	Логин	Пользователь	Событие
Сегодня, 13:28	admin	Локальный	Попытка запуска
Сегодня, 13:28	admin	Локальный	Попытка запуска
Сегодня, 13:28	admin	Локальный	Попытка запуска
Сегодня, 12:10	admin	Локальный	Отправлен IQL
Сегодня, 09:16	admin	Локальный	Вход 10.31.230

Конфигурация срока хранения действий в Системе

Для того, чтобы настроить срок хранения действий, сохраненных в Системе, нажмите **Срок хранения** в правом верхнем углу страницы. После этого укажите количество дней хранения. Все изменения будут применены автоматически. По умолчанию срок хранения действий — 180 дней.

Журнал аудита		Срок хранения	Обновить
Полнотекстовый поиск		Фильтры	
Когда	Логин	Пользователь	Событие
Сегодня, 17:14	admin	Локальный	Скачан виджет «Тестовый график (1)» из дашборда «Волков А (1)»
Сегодня, 16:49	admin	Локальный	Скачан виджет «Тестовый график (1)» из дашборда «Волков А»
Сегодня, 16:48	admin	Локальный	Вход 10.31.231.4
Сегодня, 16:26	admin	Локальный	Предоставлен доступ к дашборду «local» для пользователя СтажёрОСА
Сегодня, 16:26	admin	Локальный	Предоставлен доступ к дашборду «local» для пользователя Иванов Иван Иванович
Сегодня, 16:13	admin	Локальный	Вход 10.31.230.158

Если вы хотите хранить действия бесконечно, активируйте переключатель **Бесконечно**.

ID статьи: 447

Последнее обновление: 29 апр., 2025

Обновлено от: Егоров В.

Ревизия: 6

База знаний LogIQ -> Документация -> Система хранения и обработки данных «LogIQ». Версия 2.4.0 -> LogIQ. Руководство администратора -> Журнал аудита -> Просмотр и конфигурация журнала аудита

<https://docs.axel.pro/entry/447/>