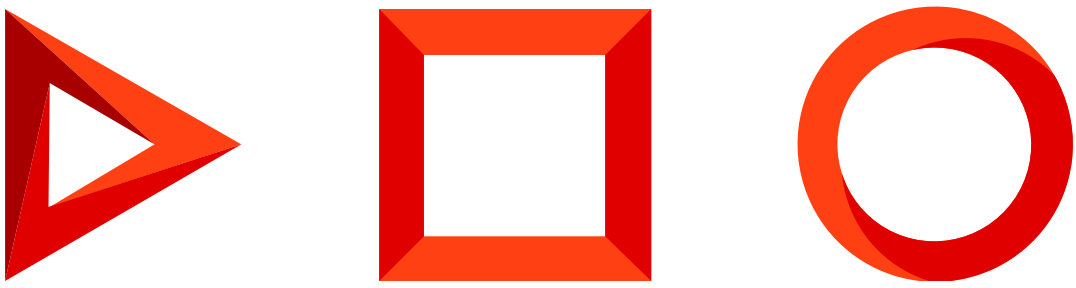
Creatio Academy

Журнал аудита

Версия 8.0



Эта документация предоставляется с ограничениями на использование и защищена законами об интеллектуальной собственности. За исключением случаев, прямо разрешенных в вашем лицензионном соглашении или разрешенных законом, вы не можете использовать, копировать, воспроизводить, переводить, транслировать, изменять, лицензировать, передавать, распространять, демонстрировать, выполнять, публиковать или отображать любую часть в любой форме или посредством любые значения. Обратный инжиниринг, дизассемблирование или декомпиляция этой документации, если это не требуется по закону для взаимодействия, запрещены.

Информация, содержащаяся в данном документе, может быть изменена без предварительного уведомления и не может гарантировать отсутствие ошибок. Если вы обнаружите какие-либо ошибки, сообщите нам о них в письменной форме.

Содержание

Настроить журнал аудита

ПРОДУКТЫ: ВСЕ ПРОДУКТЫ

Журнал аудита используется для логирования системных настроек, событий и данных. В нем регистрируются события, связанные с изменением структуры ролей пользователей, распределением прав доступа, изменением значений системных настроек, авторизацией пользователей в системе и т. д.

Для логирования бизнес-данных, например, отслеживания изменения цены продукта или остатка по счетам, используется **журнал изменений**. Подробнее: Настроить журнал изменений.

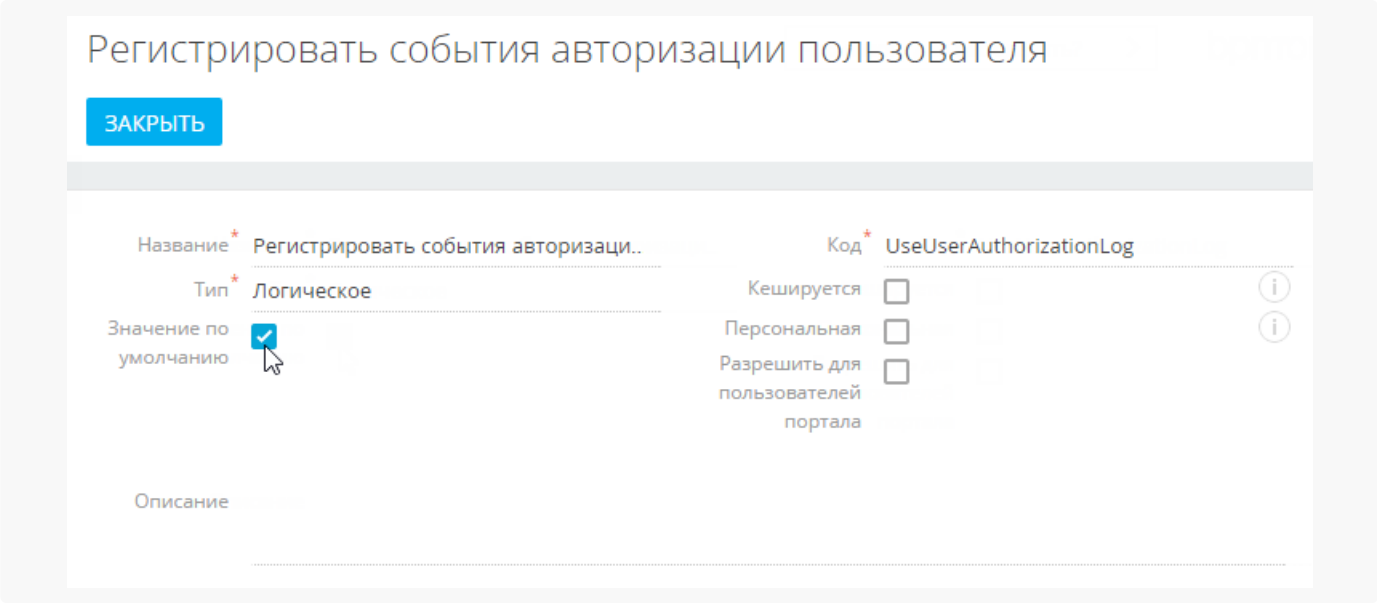
> **На заметку.** Для просмотра журнала аудита требуется доступ к системной операции “Просмотр раздела “Журнал аудита” (код “CanViewSysOperationAudit”). Для просмотра и выполнения архивации записей требуется доступ к системной операции “Управление разделом “Журнал аудита” (код “CanManageSysOperationAudit”). Подробнее: Права доступа на системные операции.

По умолчанию логирование журнала аудита отключено. Чтобы изменения логировались, выполните настройки, описанные в данной статье.

Для включения и настройки журнала аудита с помощью системных настроек:

1. Откройте дизайнер системы нажатием кнопки в правом верхнем углу приложения.
2. В блоке “Настройка системы” перейдите по ссылке “Системные настройки”.
3. В списке групп откройте группу “Администрирование” и выберите подгруппу “Журнал аудита”. Здесь содержатся все настройки, которые отвечают за логирование событий в Creatio. Каждому типу логируемого события соответствует системная настройка, которая включает или отключает его. Подробнее о системных настройках журнала аудита читайте в статье: Описание системных настроек.
4. Для включения настройки откройте ее и установите признак [*Значение по умолчанию*]. Например, установите признак для настройки [*Регистрировать события авторизации пользователя*], (Рис. 1) если необходимо логировать выполняемые пользователями вход в систему и выход из нее.

Рис. 1 — Включение системной настройки журнала аудита



После отключения системной настройки журнала аудита может потребоваться перезагрузка Redis, чтобы изменения вступили в силу.

На заметку. Если журнал аудита включен на уровне конфигурационных файлов системы, то значения системных настроек игнорируются.

Просмотреть и архивировать журнал аудита

ПРОДУКТЫ: ВСЕ ПРОДУКТЫ

В журнале аудита системных операций автоматически регистрируются события, связанные с изменением структуры ролей пользователей, распределением прав доступа, изменением значений системных настроек, а также авторизацией пользователей в системе.

Открыть журнал аудита

Перейдите в дизайнер системы, например, по кнопке в правом верхнем углу приложения и в блоке “Настройка системы” откройте ссылку “Системные настройки”. В группе “Пользователи и администрирование” кликните по ссылке “Журнал аудита” .

На заметку. Для просмотра журнала аудита системных операций требуется доступ к системной операции “Просмотр раздела “Журнал аудита” (код “CanViewSysOperationAudit”). Для просмотра и выполнения архивации записей требуется доступ к системной операции “Управление разделом “Журнал аудита” (код “CanManageSysOperationAudit”). Подробнее: Права доступа на системные операции.

В представлении [*Журнал аудита*] отображается список последних зарегистрированных событий. В представлении [*Архив журнала*] вы можете увидеть список событий, в отношении которых было выполнено действие [*Архивировать журнал*]. Архивные события хранятся в отдельной таблице.

На заметку. Если ваше приложение развернуто on-site на .NET Core с использованием горизонтального масштабирования, то для отображения IP-адресов пользователей необходимо выполнить дополнительную настройку балансировщика. Подробнее: Настроить отображение IP-адресов в журнале аудита для .NET Core.

В реестре раздела [*Журнал аудита*] доступны следующие данные:

- [*Тип события*] — перечень типов системных событий содержится в справочнике [*Типы событий*], например, “Авторизация пользователя”, “Сессия пользователя” и т. д.
- [*Дата события*] — дата и время наступления события.
- [*Результат*] — перечень результатов системных событий содержится в справочнике [*Результаты событий*]. Например, попытка авторизации пользователя может завершиться с результатом “Авторизация” или “Отказ авторизации”, если авторизация была неудачной.
- [*IP-адрес*] — IP-адрес пользователя, выполнившего операцию, в результате которой наступило системное событие. Например, IP-адрес пользователя, совершившего попытку авторизации в системе.

  На заметку. В случае, если пользователь заходит через VPN или запрос проходит через несколько прокси-серверов, перечислены IP-адреса каждого последующего прокси-сервера. В этом случае самый правый IP-адрес — это IP-адрес самого последнего прокси-сервера, а самый левый IP-адрес — это первый IP-адрес, который можно отследить.

- [*Ответственный*] — пользователь, выполнивший операцию, в результате которой наступило системное событие. Например, имя сотрудника, который совершил попытку авторизации в системе.
- [*Описание*] — подробное описание события, например, “Авторизация пользователя Евгений Мирный. IP-адрес: 192.168.0.7”. Описание событий генерируется системой автоматически.

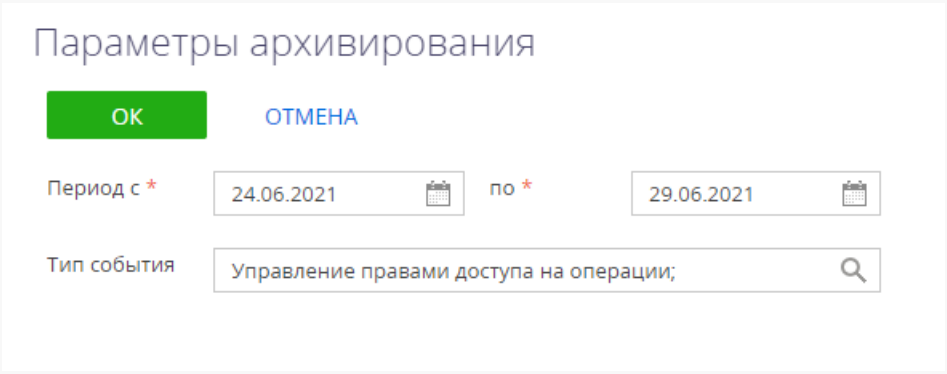
Архивировать журнал аудита

Журнал аудита системных операций содержит действие [*Архивировать журнал*], при выполнении которого записи журнала копируются в отдельную архивную таблицу.

Для архивации журнала аудита:

1. Нажмите , чтобы открыть реестр раздела [*Журнал аудита*].
2. Нажмите [*Действия*] —> [*Архивировать журнал*].
3. На открывшейся странице [*Параметры архивирования*] (Рис. 2) настройте параметры архивации.

Рис. 2 — Окно [*Параметры архивирования*]



4. [*Период с*], [*по*] — период, за который необходимо архивировать события. Будет выполнена архивация только тех событий, дата которых попадает в указанный диапазон.
5. [*Тип события*] — выберите типы событий для архивации. Будут архивированы только те события, типы которых совпадают с выбранными. Вы можете выбрать несколько типов.

> **На заметку.** Выполнение действия архивации логируется в журнале как “Управление журналом аудита администрирования”. По завершении операции отображается сообщение, информирующее о количестве архивированных записей.

В результате вы увидите список заархивированных событий, даты которых попадают в указанный период, в представлении «Архив журнала» ( ) раздела [*Журнал аудита*].