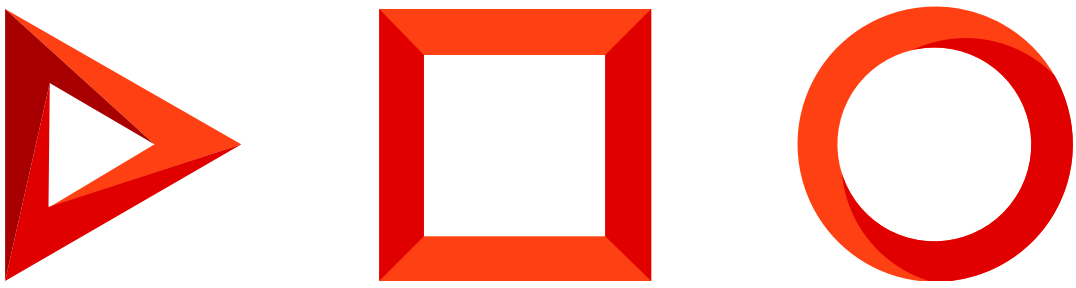
Creatio Academy

# Настройки безопасности

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

# Безопасная загрузка файлов

ПРОДУКТЫ: ВСЕ ПРОДУКТЫ

Для повышения безопасности работы в Creatio вы можете настроить ограничения форматов загружаемых в приложение сторонних файлов. Ограничения на загрузку файлов действуют как для пользователей, так и для интеграций, например, внешних веб-сервисов.

При настроенных ограничениях Creatio проверяет формат файлов, которые загружаются на деталь [ *Файлы и ссылки* ]. В случае соответствия настройкам файл будет успешно загружен. В другом случае файл загружен не будет, а пользователь получит уведомление, что загрузка данного файла запрещена настройками безопасности.  Для файлов, загруженных в систему до включения ограничений, настройки не применятся.

Ограничения действуют только на загрузку файлов в Creatio, скачивать файлы могут все пользователи, имеющие к ним доступ.

В системе предусмотрены следующие способы ограничения загрузки файлов:

- Ограничения для файлов **определенных типов** — вы можете настроить список **разрешенных расширений** или список **запрещенных расширений** файлов. В этом случае можно установить разрешение или запрет на загрузку в приложение файлов определенных типов.
- Ограничения для файлов **неизвестных типов**. В этом случае можно установить разрешение или запрет на загрузку в приложение файлов, у которых не указано расширение и невозможно определить тип по содержимому.

## Выбрать режим проверки файлов

1. Перейдите в **дизайнер системы** по кнопке  .
2. Перейдите в раздел [ ***Системные настройки*** ].
3. Откройте системную настройку “**Режим проверки файлов**” (код “FileSecurityMode”).
4. В поле [ ***Значение по умолчанию*** ] выберите необходимый тип ограничения:
   - “**Проверка файлов отключена**” — чтобы отменить все ограничения на загрузку файлов в приложение.
   - “**Список запрещенных расширений**” — чтобы запретить загрузку в приложение файлов определенных типов.
   - “**Список разрешенных расширений**” — чтобы разрешить загрузку в приложение только файлов определенных типов.
5. **Сохраните** изменения.

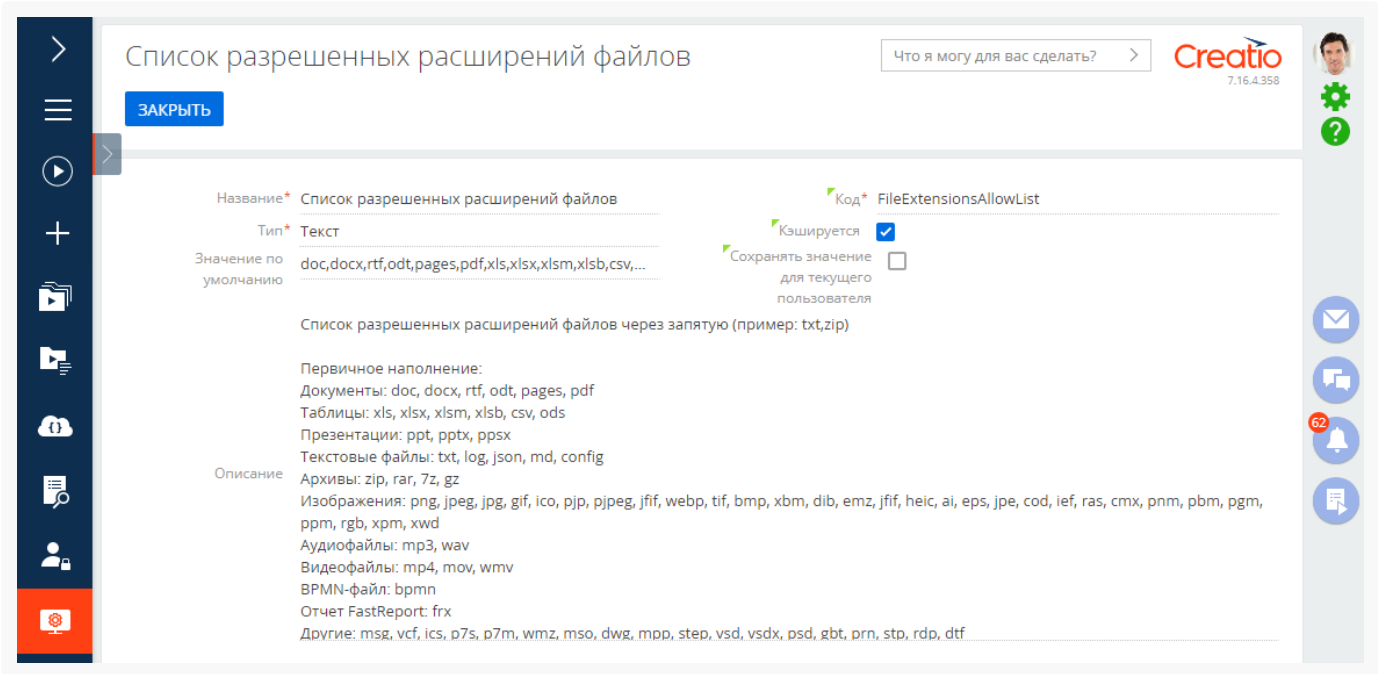
## Настроить список типов файлов

1. Перейдите в **дизайнер системы** по кнопке .
2. Перейдите в раздел [ ***Системные настройки*** ].
3. Откройте системную настройку

   - “**Список разрешенных расширений файлов**” (код “FileExtensionsAllowList”), чтобы настроить список разрешенных к загрузке типов файлов. По умолчанию в настройке приведены наиболее часто используемые типы файлов.
   - “**Список запрещенных расширений файлов**” (код “FileExtensionsDenyList”), чтобы настроить список запрещенных к загрузке типов файлов. По умолчанию в настройке приведены типы файлов, которые могут являться вредоносными.

4. В поле [ ***Значение по умолчанию*** ] через запятую без пробела укажите **расширения файлов** (Рис. 1) и проверьте корректность ввода.

Рис. 1 — Пример заполнения системной настройки “Список разрешенных расширений файлов”




5. **Сохраните** изменения.

## Настроить ограничения для неизвестных типов файлов

Creatio определяет типы загружаемых файлов по их расширению. В случае если расширение не указано, система определяет тип файла на основании его содержимого. По умолчанию в систему разрешено загружать файлы неизвестных типов. Запрет загрузки таких файлов повысит безопасность работы в приложении, но в этом случае обязательно потребуется настроить список разрешенных или запрещенных расширений.

Чтобы **запретить загрузку** в Creatio файлов неизвестных типов:

1. Перейдите в **дизайнер системы** по кнопке .

2. Перейдите в раздел [ ***Системные настройки*** ].
3. Откройте системную настройку “**Разрешить работу с неизвестными типами файлов**” (код “AllowFilesWithUnknownType”).
4. Снимите признак [ ***Значение по умолчанию*** ].
5. **Сохраните** изменения.

## Настроить исключение веб-сервисов из ограничений загрузки файлов

Ограничение загрузки файлов применяется для всех используемых в системе веб-сервисов, включая те, которые были добавлены в процессе кастомизации системы, в проектных решениях и приложениях Marketplace. Чтобы веб-сервисы могли добавлять в Creatio файлы тех типов, которые не разрешены пользователям, их необходимо **добавить в список исключений**. Для этого:

1. Перейдите в **дизайнер системы** по кнопке  .
2. Перейдите в раздел [ ***Справочники*** ].
3. Откройте справочник [ ***Список исключений из проверки безопасности файлов*** ].
4. Нажмите [ ***Добавить*** ].
5. В поле [ ***Название*** ] укажите **URI** веб-сервиса, который необходимо добавить в исключения. Запись сохраняется автоматически.
   - Пример для приложений на **.NET Framework**: /0/rest/[ *Название пользовательского сервиса* ]/[ *Конечная точка пользовательского сервиса* ], без указания [ *Адреса приложения* ].
   - Пример для приложений на **.NET CORE**: /rest/[ *Название пользовательского сервиса* ]/[ *Конечная точка пользовательского сервиса* ], без указания [ *Адреса приложения* ].
6. **Повторите** для всех веб-сервисов, которым необходимо разрешить загрузку файлов в приложение.

# Рекомендуемые настройки информационной безопасности

ПРОДУКТЫ: ВСЕ ПРОДУКТЫ

В статье приведены рекомендации по настройке информационной безопасности Creatio.

## Единая политика паролей в организации

Убедитесь, что настройки логина и пароля соответствуют политике безопасности компании. Вы можете использовать рекомендованные значения, если не определены точные требования.

**Длина пароля**. Рекомендуем использовать пароли, состоящие из 8 и более символов. Установить сложность пароля вы можете в системных настройках:

- “Сложность пароля: Минимальная длина” (код “MinPasswordLength”);
- “Сложность пароля: Минимальное количество символов нижнего регистра” (код “MinPasswordLowercaseCharCount”);
- “Сложность пароля: Минимальное количество символов верхнего регистра” (код “MinPasswordUppercaseCharCount”);
- “Сложность пароля: Минимальное количество цифр” (код “MinPasswordNumericCharCount”);
- “Сложность пароля: Минимальное количество специальных символов” (код “MinPasswordSpecialCharCount”).

**История изменения паролей**. Creatio сравнивает новый пароль пользователя с ранее использованными, чтобы убедиться, что они не совпадают. Вы можете управлять количеством старых паролей, которые будут использоваться для сравнения с новым, в системной настройке “Количество анализируемых паролей” (код “PasswordHistoryRecordCount”).

Количество **неуспешных попыток входа** и **время, по истечении которого учетная запись пользователя будет разблокирована**. Рекомендуем настроить ограничение до 5 попыток неуспешного входа и срок ожидания 15 минут до автоматического разблокирования пользователя. Управление блокированием учетной записи пользователя осуществляется с помощью системных настроек:

- “Количество попыток входа” (код “LoginAttemptCount”) — допустимое количество неудачных попыток ввода логина или пароля.
- “Количество попыток входа до предупреждающего сообщения“ (код “LoginAttemptBeforeWarningCount”) — количество неудачных попыток ввода пароля, после которого система отобразит предупреждающее сообщение о том, сколько попыток осталось до блокирования пользователя.
- “Время блокировки пользователя“ (код “UserLockoutDuration”) — время блокировки (в минутах) учетной записи пользователя после указанного количества неудачных попыток ввода логина или пароля.

Подробнее: Разблокировать учетную запись пользователя.

**Сообщение о неуспешной попытке входа** и **предупреждение о возможности блокировки** учетной записи. Рекомендуем использовать для сообщений универсальные формулировки, не зависящие от конкретной ошибки. Для этого убедитесь, что у следующих системных настроек установлено значение “false” (признак снят):

- “Отображать информацию о блокировке учетной записи при входе” (код “DisplayAccountLockoutMessageAtLogin”);
- “Отображать информацию о неверном пароле при входе” (код “DisplayIncorrectPasswordMessageAtLogin”).

## Время завершения сессии

Задайте интервал бездействия пользователя в минутах, по истечении которого сессия будет закрыта, в системной настройке “Таймаут сеанса пользователя” (код “UserSessionTimeout”). Значение по умолчанию: “60”.

# Протокол TLS для Creatio on-site

В Creatio реализована поддержка протокола TLS 1.2. Использование устаревших версий протокола TLS 1.0 и 1.1 делает систему безопасности уязвимой.

# Безопасные конфигурации HTML-заголовков для Creatio on-site

Защитите ваш браузер от уязвимостей, которые можно предотвратить. Для этого включите следующие заголовки, которые соответствуют OWASP Secure Headers Project (открытый проект обеспечения безопасности веб-приложений):

**HTTP Strict Transport Security (HSTS)**. Включите заголовок `Strict-Transport-Security` и установите срок хранения параметра в памяти браузера, равный одному году:

```
Strict-Transport-Security: max-age=3153600
```

**Защита от кликджекинга (clickjacking)**. Включите заголовок `X-Frame-Options` и разрешите встраивание веб-страниц только на тех же адресах, что и у вашего приложения Creatio:

```
X-Frame-Options: sameorigin
```

**Защита от атак межсайтового скриптинга (XSS)**. Включите заголовок `X-XSS-Protection` и установите блокировку попыток XSS-атак:

```
X-XSS-Protection: 1; mode=block
```

**Защита от MIME-сниффинга (MIME-sniffing)**. Включите заголовок `X-Content-Type-Options` и установите режим “nosniff”. Этот режим предотвращает попытку браузера переопределить тип контента ресурса, если он отличается от объявленного типа контента:

```
X-Content-Type-Options: nosniff
```

**Политика референта (Referrer Policy)**. Включите заголовок `Referrer-Policy` и установите значение “origin-when-cross-origin”. Этот заголовок определяет объем информации о референте (отправляется с заголовком “Referer”), который будет включен в запросы:

```
Referrer-Policy: origin-when-cross-origin
```

**Важно.** Перед тем как применить настройки **политики безопасности контента**, проверьте, какие интеграции уже используются или запланированы для добавления в вашем браузере, например, CTI коннекторы. Добавьте соответствующие домены в список политики безопасности контента (Content Security Policy list). Иначе интеграции перестанут работать.

**Политика безопасности контента**. Включите заголовок `Content Security Policy` и настройте его следующим образом:

```
Content-Security-Policy: default-src 'self'; script-src 'unsafe-inline' 'unsafe-eval'; script-sr
```

## Ответы на запросы для Creatio on-site

Ограничьте количество и тип информации, доступной в ответах на запросы. Для этого измените файл Web.config в корневом каталоге Creatio:

1. Отключите `X-Powered-By`.

```
<system.webServer>
    <httpProtocol>
        <customHeaders>
            <remove name="X-Powered-By" />
        </customHeaders>
    </httpProtocol>
</system.webServer>
```

2. Отключите `X-AspNet-Version`. Для этого выполните изменения во всех секциях httpRuntime файлов Web.config в корневой папке приложения и в папке Terrasoft.WebApp.

```
<httpRuntime enableVersionHeader="false" />
```

3. Отключите `Server Header` (доступно для IIS версии 10 и выше).

```
<system.webServer>
    <security>
        <requestFiltering removeServerHeader ="true" />
    </security>
</system.webServer>
```

## Настройка Redis для Creatio on-site

Рекомендуем использовать комбинацию из стабильной версии Debian и актуальной версии Redis.

Кроме того, рекомендуем использовать **авторизованный доступ к серверу Redis**.

- Для версии 8.0.1 и ниже используйте авторизацию по паролю сервера Redis.
- Для версии 8.0.2 и выше используйте любой способ авторизации на сервере Redis.

Подробнее: Настроить безопасное подключение к Redis.

# Управление заголовками ответов HTTP

ПРОДУКТЫ: ВСЕ ПРОДУКТЫ

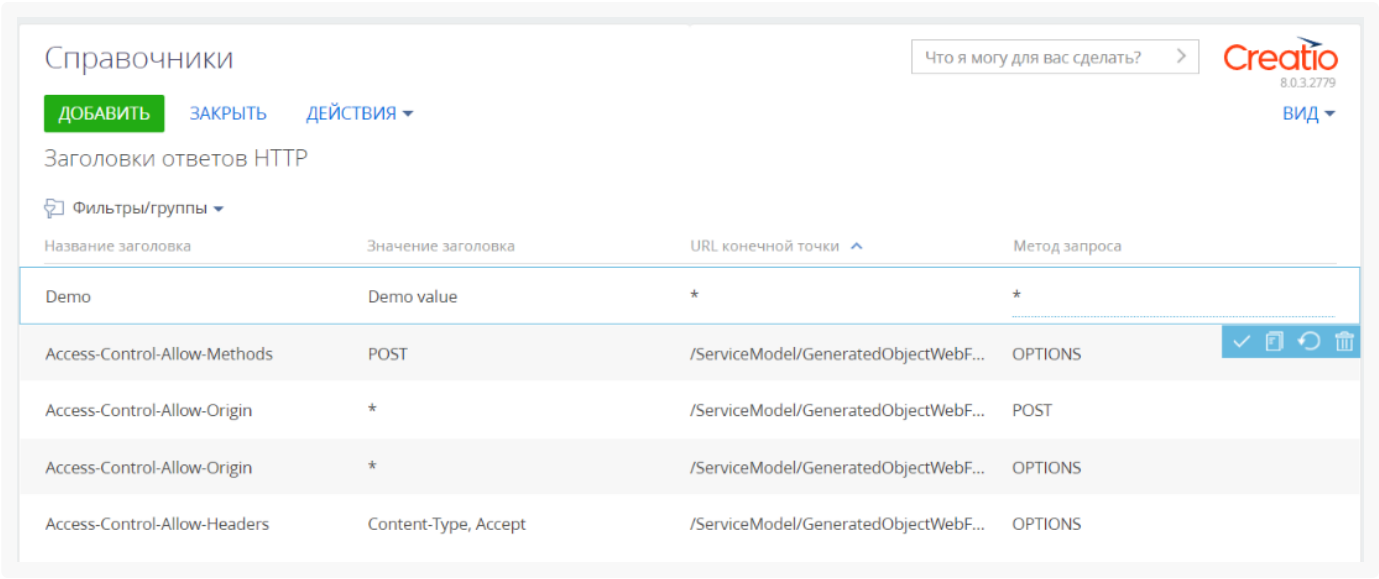
Механизм настраиваемых заголовков ответов HTTP используется для отправки заголовков **политики безопасности контента** (CSP). Для предотвращения подключения внешних ресурсов, которые нарушают заданные в системе политики безопасности, формируется HTTP заголовок специального вида, который отправляется в ответе сервера на любой запрос.

**Важно.** Крайне рекомендуется управлять заголовками ответов HTTP с помощью справочника [ *Заголовки ответов HTTP* ], а не с помощью конфигурационного файла приложения. Подробная информация о том, как перенести уже существующие заголовки из конфигурационного файла в справочник [ *Заголовки ответов HTTP* ] приведена ниже.

## Настроить заголовки ответов HTTP

1. Откройте дизайнер системы по кнопке ⚙ в правом верхнем углу приложения.
2. В группе [ *Настройка системы* ] кликните по ссылке [ *Справочники* ].
3. Откройте справочник [ *Заголовки ответов HTTP* ].
4. Создайте новый HTTP заголовок. Для этого нажмите кнопку [ *Добавить* ] и заполните обязательные поля: [ *Название заголовка* ], [ *Значение заголовка* ].

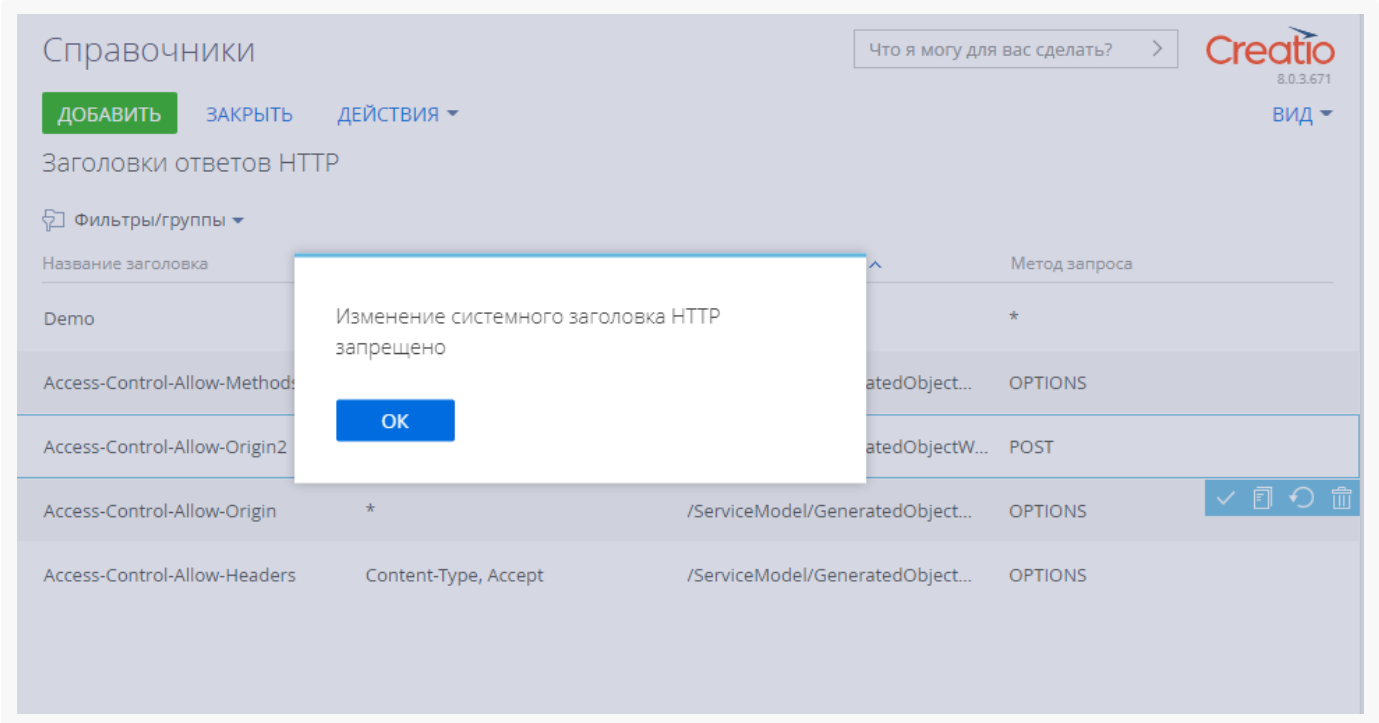
Рис. 1 — Создание нового HTTP заголовка




Если в конфигурационном файле приложения и в справочнике заголовков ответов HTTP есть заголовки с одинаковыми именами, то приоритет будут иметь заголовки из конфигурационного файла.

Заголовки, которые добавлены в справочник не могут быть **изменены или удалены**. При попытке изменить такой заголовок вы получите соответствующее уведомление.

Рис. 2 — Ошибка при удалении заголовка HTTP




По умолчанию заголовок применяется для всех запросов и для всех методов запроса (“*”). При необходимости дополнительно можно переопределить следующие необязательные поля:

- [ *URL конечной точки* ] — относительный путь URL;
- [ *Метод запроса* ] — значение метода запроса, допустимые значения: GET, OPTIONS, POST, PUT, DELETE

или PATCH;

Результат настройки и включения пользовательских заголовков HTTP можно увидеть в ответе HTTP.

Рис. 3 — Пользовательский заголовок HTTP


В случае наличия в справочнике заголовков с одинаковыми именами нужно учитывать приоритет выбора заголовков:

| URL конечной точки | Метод запроса | Приоритет |
|---|---|---|
| /api/HealthCheck/Ping | GET | 1 |
| /api/HealthCheck/Ping | * | 2 |
| * | POST | 3 |
| * | * | 4 |

Если в базе заданы заголовки с одинаковыми именами, то при запросе с определенной конечной точки (endpoint) и с определенным методом запроса приоритеты заголовков будут определяться следующим образом:

1. Первым ищется заголовок, у которого указана именно эта конечная точка и метод запроса.
2. Затем заголовок, у которого указана та же конечная точка, с которой пришел запрос, и метода запроса равный “*”.
3. Затем применяется заголовок, у которого конечная точка равна “*” а метод совпадает с методом запроса.
4. Затем применяется заголовок с конечной точкой равной “*” и с методом запроса равным “*”.

Для включения и отключения заголовков в ответе HTTP используется флаг `UseHttpHeaderProvider` в

конфигурационном файле `web.config` корневого каталога приложения.

```
<add key="UseHttpHeaderProvider" value="true" />
```

## Перенести заголовки из конфигурационного файла приложения в справочник

Для переноса пользовательских заголовков HTTP из конфигурационного файла `web.config` корневого каталога приложения в справочник необходимо:

1. В конфигурационном файле найдите секцию `<customHeaders>`. В ней указаны заголовки в формате:

   ```
   <add name="SomeHeaderName" value="SomeHeaderValue" />
   ```

   где:

   - `name` — название заголовка;
   - `value` — значение заголовка.

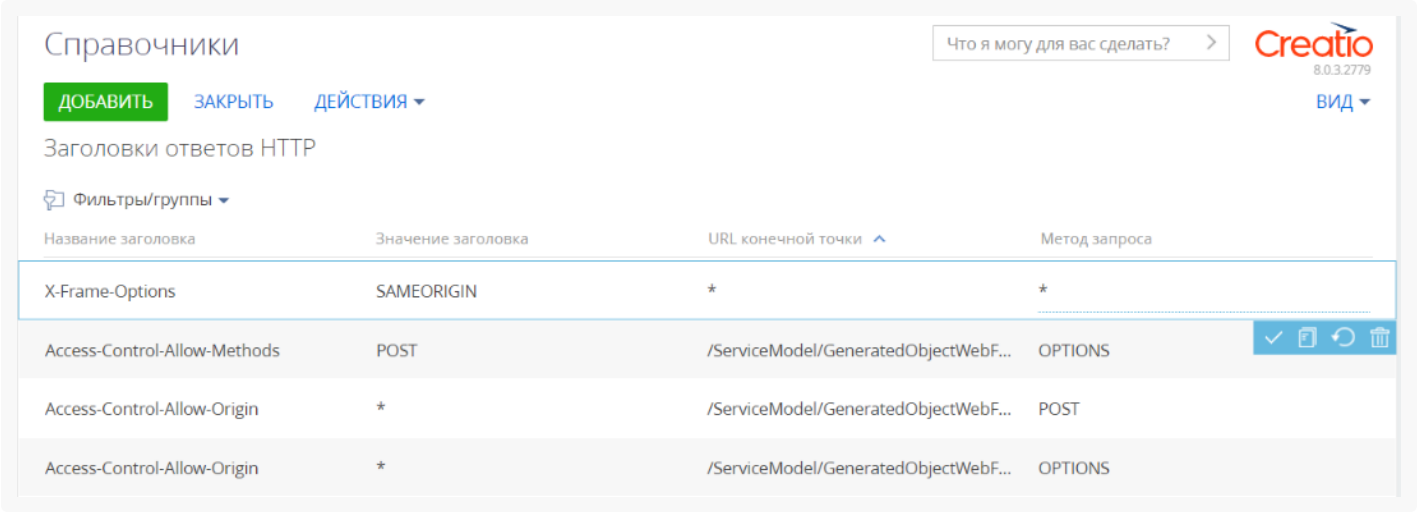
2. Все заголовки из данной секции перенесите в справочник [ *Заголовки ответов HTTP* ], указывая в качестве [ *Название заголовка* ] значение из атрибута `name`, а в качестве [ *Значение заголовка* ] значение атрибута `value`. Значения полей [ *URL конечной точки* ] и [ *Метод запроса* ] необходимо оставить со значениями по умолчанию — “*”.

Например, в конфигурационном файле указан заголовок:

```
<add name="X-Frame-Options" value="SAMEORIGIN" />
```

В справочник его необходимо перенести следующим образом:

Рис. 4 — Добавление заголовка HTTP в справочник




# Предоставить удаленный доступ службе поддержки Creatio

ПРОДУКТЫ: ВСЕ ПРОДУКТЫ

Пользователи развернутых в облаке приложений могут предоставлять сотрудникам службы технической поддержки Creatio безопасный и контролируемый доступ к своим сайтам. При этом нет необходимости сообщать службе поддержки свои логин и пароль для доступа к сайту, что обеспечит безопасность персональных и коммерческих данных клиента.

**На заметку.** Для предоставления безопасного доступа в системе должны быть заполнены системные настройки: “Идентификатор приложения для предоставления доступа (по умолчанию)” (DefaultExternalAccessClientId), “Секретный ключ для Identity сервера” (IdentityServerClientSecret), “Адрес Identity сервера”(IdentityServerUrl), ”Идентификатор приложения для Identity сервера” (IdentityServerClientId). Указанные настройки заполняются автоматически.

- Чтобы скрыть данные разделов системы от сотрудников службы поддержки, используется **режим изоляции данных**.
- Чтобы ограничить возможность менять настройки конфигурации для сотрудников службы поддержки используется **режим ограничения доступа на конфигурирование системы**. При этом настройки конфигурации, необходимые для решения обращения клиента, доступны для просмотра.

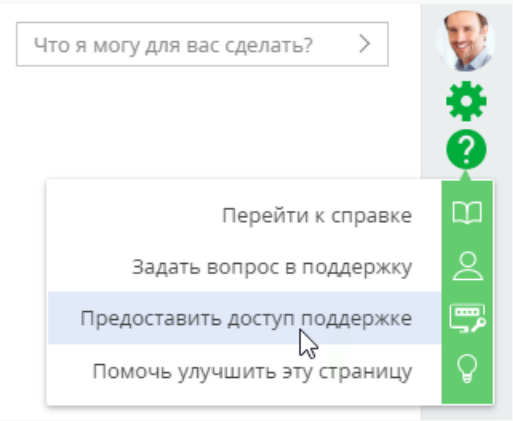
Настройка безопасного доступа выполняется администратором приложения (пользователем с ролью “System administrators”). Сотрудники службы поддержки могут подключаться под ученой записью администратора либо любого другого пользователя приложения. После того, как подключение состоялось, всю необходимую информацию по сеансу доступа можно получить в логах — когда состоялось подключение, а также какие данные были созданы при подключении.

## Настроить безопасный доступ

**На заметку.** Для настройки доступа службы поддержки у вас должно быть право на чтение и добавление записей в объекте “Доступ внешних приложений”. У пользователей с ролью “System administrators” это право есть по умолчанию. Больше информации о правах на выполнение операций в объекте читайте в статье “Настроить доступ по операциям”.

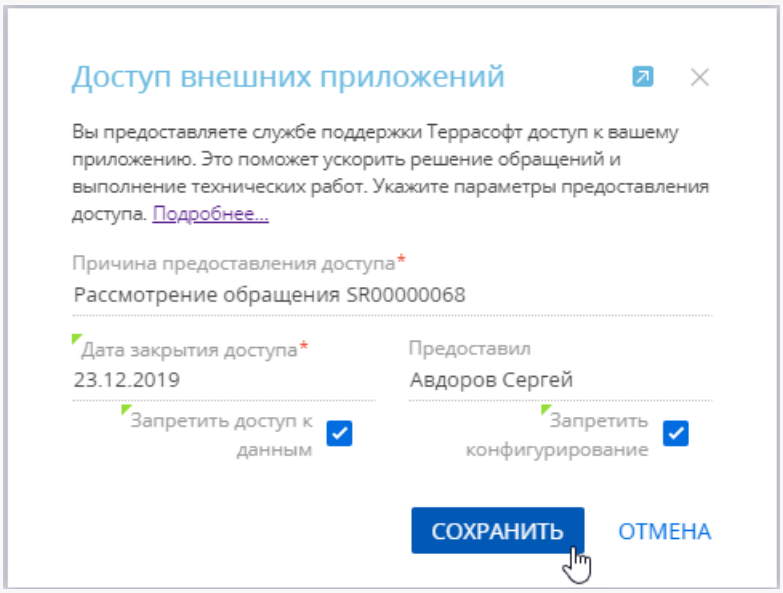
1. В правом верхнем углу приложения кликните —> “Предоставить доступ поддержке” (Рис. 1)

Рис. 1 — Переход к настройке доступа из справочного меню




2. Заполните поля открывшейся мини-карточки (Рис. 2):

Рис. 2 — Пример заполнения параметров доступа к клиентскому сайту




a. В поле [ ***Причина предоставления доступа*** ] укажите, какая проблема привела к необходимости доступа, номер обращения или перечень работ, которые должен провести сотрудник службы поддержки.

b. В поле [ ***Дата закрытия доступа*** ] укажите дату, до которой предоставляется доступ. В 23:59 указанной даты доступ будет автоматически отключен.

c. В поле [ ***Предоставил*** ] по умолчанию указан пользователь, который настраивает доступ. Вы

можете указать в этом поле любого пользователя, под учетной записью которого необходимо предоставить доступ сотрудникам службы поддержки.

d. Признаки [ ***Запретить доступ к данным*** ] и [ ***Запретить конфигурирование*** ] позволяют предоставлять доступ к системе в режимах изоляции данных и ограничения доступа на конфигурирование. По умолчанию оба признака включены. Это означает, что при доступе к вашему приложению сотрудник службы поддержки не сможет видеть данные в разделах, а также не сможет выполнять настройку системы.

   - Если необходимо, чтобы у службы поддержки были такие же права доступа, как и у пользователя, под чьими учетными данными выполняется подключение, то снимите оба признака.
   - Если необходимо, чтобы сотрудник службы поддержки мог внести изменения в конфигурацию, но не видел данных в разделах системы, то снимите только признак [ *Запретить конфигурирование* ]. Так у него будет доступ к функциональности дизайнера системы, необходимой для выполнения настроек (например, к разделам [ *Справочники* ], [ *Системные настройки* ], [ *Библиотека процессов* ] и др.). При этом данные основных разделов будут ему недоступны.
   - Если необходимо, чтобы сотрудник службы поддержки мог просматривать данные в разделах, но не мог изменять конфигурацию системы, то снимите только признак [ *Запретить доступ к данным* ]. При этом у него будет возможность просмотреть настройки конфигурации.

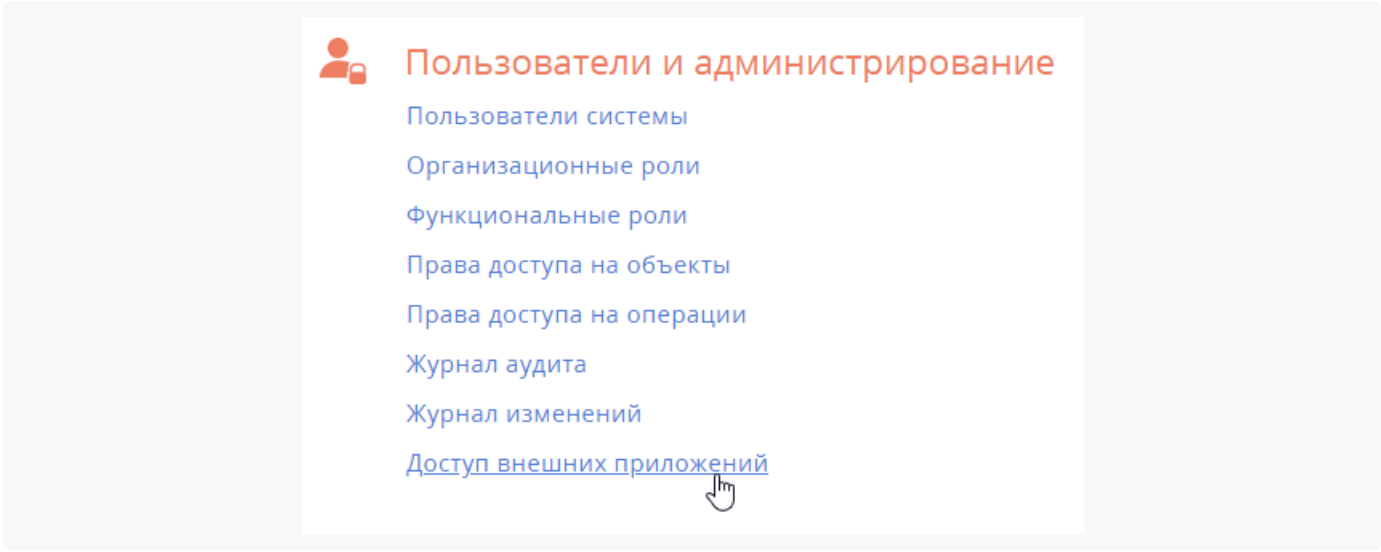
3. Сохраните запись.

   В результате в разделе [ *Доступ внешних приложений* ] вашей системы будет создана новая запись. Сотрудники службы поддержки смогут войти на сайт клиента под учетной записью и с правами пользователя, указанного при настройке доступа, не используя учетных данных клиента. В 23:59 даты, указанной в настройках, доступ будет отключен автоматически.

# Просмотреть результаты подключения

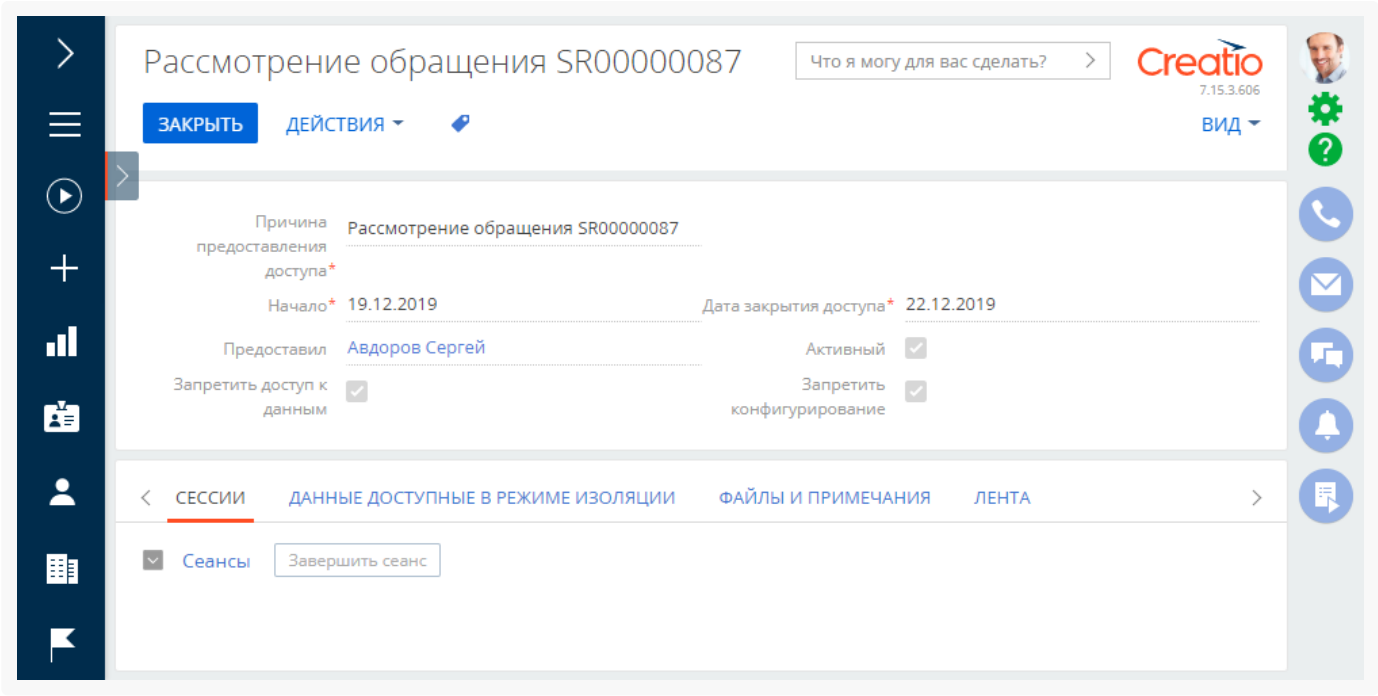
1. Перейдите в раздел [ *Доступ внешних приложений* ] дизайнера системы (Рис. 1).

Рис. 1 — Раздел [ *Доступ внешних приложений* ]



2. Откройте нужную запись в реестре раздела. На странице записи вы можете просмотреть все параметры доступа (Рис. 2). После того, как сеанс доступа службы поддержки состоится, на вкладке [ *Сессии* ] страницы записи автоматически отобразятся все данные, касающиеся этого сеанса — когда он состоялся, а также какие данные были созданы в системе во время сеанса.

Рис. 2 — Пример записи с параметрами доступа в разделе [ *Доступ внешних приложений* ]




# Настроить хранение чувствительной информации в Vault

ПРОДУКТЫ: ВСЕ ПРОДУКТЫ

Вы можете повысить безопасность использования Creatio отказавшись от хранения чувствительных данных в конфигурационных файлах. Для этого можно использовать приложение Vault by HashiCorp, которое позволяет безопасно хранить чувствительные данные и управлять ими. К таким данным относятся:

- пароли;
- имена пользователей;
- ключи API;
- токены доступа.

Вы можете вынести в защищенное хранилище Vault параметры подключений, которые обычно хранятся в файле ConnectionStrings.config вашего приложения:

- базы данных Creatio;
- Quartz (при условии хранения данных в отдельной БД);

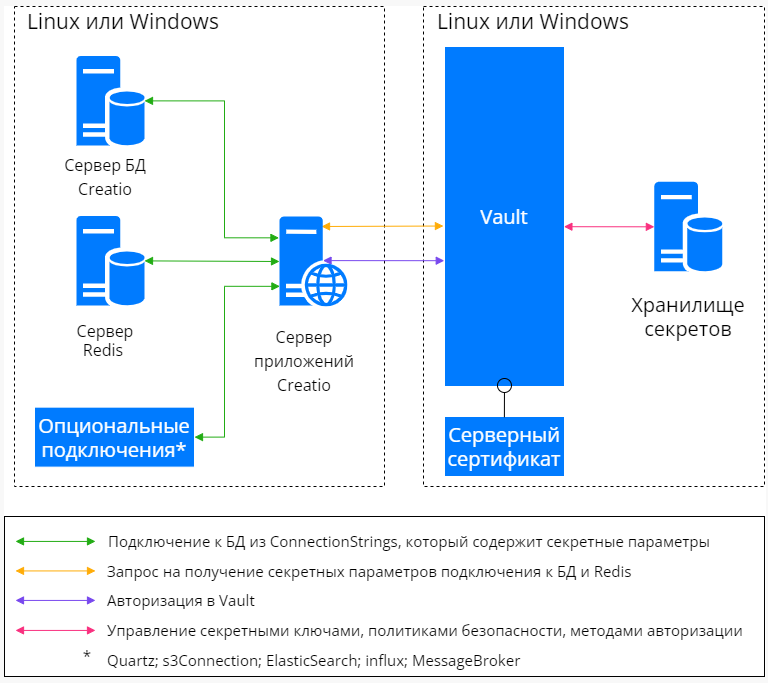
- Redis;
- s3Connection;
- ElasticSearch;
- influx;
- MessageBroker.

Эту настройку можно выполнять как во время развертывания вашего приложения Creatio, так и для уже работающих сред.

В Vault для хранения чувствительных данных используются секреты (secrets). Они записаны в специальных хранилищах секретов (Secrets Engines). Хранилища бывают различных типов. Для чувствительных данных Creatio необходимо использовать хранилище типа “ключ-значение” (key-value) — KV версии 2. Это позволяет хранить чувствительные данные в виде пар, состоящих из ключа и значения. Значение содержит чувствительную информацию, а ключ необходимо указать в файле ConnectionStrings.config вашего приложения Creatio. Также вы можете хранить в Vault ключи шифрования (AES).

**На заметку.** Дополнительно в Vault можно настроить сохранение истории изменений пар “ключ-значение”.

Рис. 1 — Схема взаимодействия Creatio и Vault




Общий порядок подключения и настройки функциональности включает следующие шаги:

1. Настройки на стороне Vault:
   a. Развертывание и запуск сервера Vault.
   b. Создание секретных ключей.

c. Настройка политик безопасности.

d. Настройка параметров авторизации.

2. Настройки на стороне Creatio:

a. Настройка параметров подключения к Vault.

b. Настройка строк подключения ConnectionStrings.config.

c. Включение признаков.

d. Перезапуск Creatio.

Рассмотрим эти этапы подробнее.

# Настройки на стороне Vault

## Развернуть и запустить сервер Vault

Перед использованием сервер Vault должен быть запущен в промышленном режиме. Допустимо разворачивать Vault как на отдельном сервере, так и на том же сервере, где развернуты другие элементы инфраструктуры Creatio, руководствуясь общими требованиями к серверам. Это можно сделать как при развертывании Creatio, так и позднее.

Сервер Vault необходимо развернуть на хосте под управлением Linux/Windows таким образом, чтобы было установлено https-соединение. Для этого используйте серверный сертификат, который должен храниться на том же хосте, где развернут сервер. Серверный сертификат может быть выдан и зарегистрирован любым доступным центром сертификации.

**Важно.** Приватный ключ серверного сертификата необходимо хранить в защищенной папке.

Развертывание и запуск Vault подробно описаны в документации приложения (на английском языке):

1. Установка.
2. Настройка.
3. Первый запуск.
4. Инициализация после первого запуска.

**Важно.** Сохраните unseal-ключи и токен, полученные при инициализации. Это позволит убедиться в безопасности запуска и осуществить его от имени администратора.

Действия, которые выполняются каждый раз при перезапуске сервера Vault:

1. Повторный запуск.
2. “Распаковка” с использованием unseal-ключей, полученных при инициализации Vault.

## Создать хранилище секретных ключей

Для хранения секретов используется хранилище (secrets engine) типа kv (key/value) версии 2.

В Vault чувствительные данные со всей историей изменений содержатся в специальных хранилищах (Secrets Engines). У каждого хранилища обязательным атрибутом является уникальный путь, который будет использоваться для подключения. Для хранилища, в котором будут содержаться чувствительные данные Creatio, рекомендуем указать в качестве пути имя вашего сайта.

1. В интерфейсе Vault перейдите в раздел [ *Secrets* ].
2. Создайте хранилище секретов (Secrets Engine), в котором будут храниться пары ключей и значений. Рекомендуем называть хранилище SecretsEngine по имени продукта, для которого создаются секреты. Например, Creatio. Подробно создание хранилища рассмотрено в документации Vault (на английском языке).

Хранилище может содержать несколько секретов, каждый из которых будет соответствовать определенной строке подключения или ключу шифрования. Для каждого секрета в хранилище необходимо указать уникальный путь к секрету. Каждый секрет может содержать необходимое количество пар “ключ-значение”, отдельная пара для каждого типа чувствительных данных. Например, если необходимо хранить в Vault логин и пароль, то это будет две пары “ключ-значение”.

## Создать секретные ключи

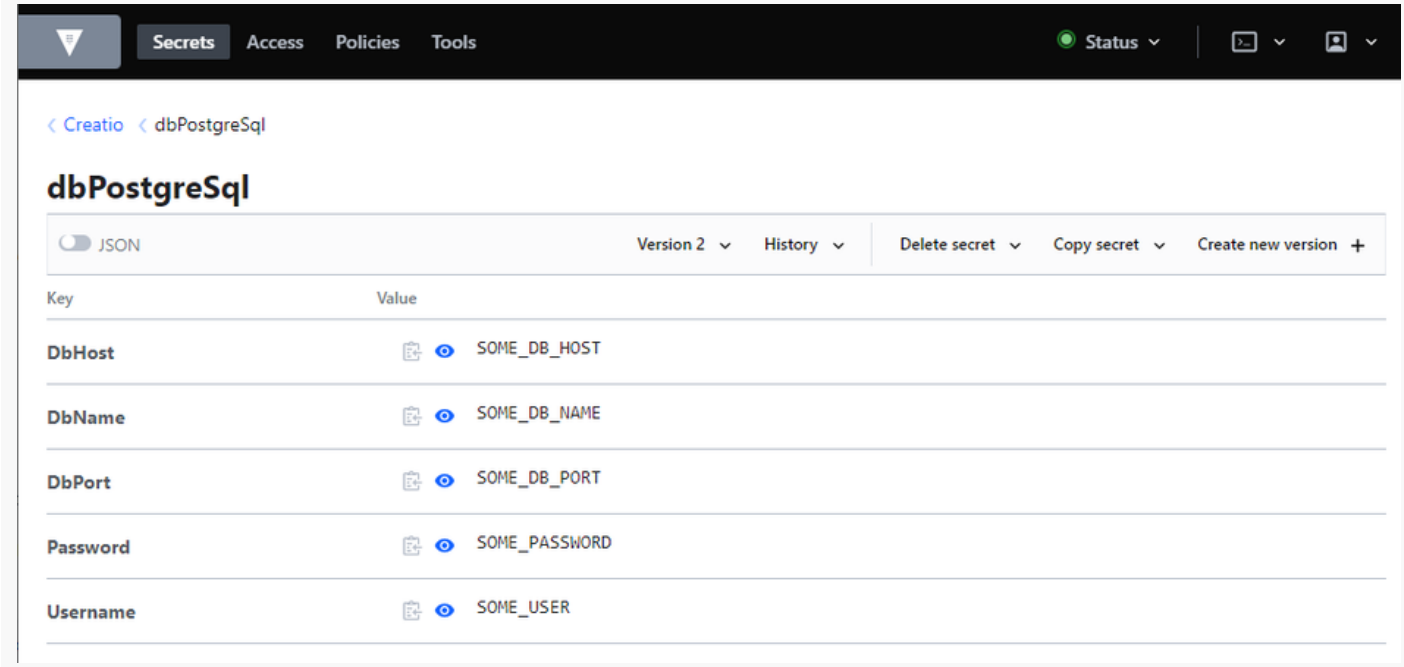
Чтобы создать секретные ключи для строки подключения к БД в файле ConnectionStrings.config:

1. В интерфейсе Vault перейдите в раздел [ *Secrets* ].
2. Откройте созданное хранилище секретов (Secrets Engine).
3. Укажите путь к секрету (Path). Для подключения к БД, а также к Redis путь к чувствительным данным должен совпадать с именем соответствующей строки подключения в ConnectionStrings.config. Например, если вы используете PostgreSql, то для строки подключения к БД необходимо указать `dbPostgreSql`.
4. Аналогичным способом настройте другие строки подключения, которые содержат секретную информацию.
5. В каждом секрете, соответствующем строке подключения, создайте все необходимые пары ключ/значение, где ключ будет содержать уникальное имя секрета (рекомендуем давать осмысленное имя, чтобы ключ было легко идентифицировать), а значение — секретную информацию. Для ключей и значений имеет значение регистр.

   В результате путь к созданному секрету имеет вид `<secretsEnginePath>/dbPostgreSql`, где `<secretsEnginePath>` — путь к хранилищу секретов, а `dbPostgreSql` — путь к секрету.

> **Важно.** При изменении значения секретов в Vault перезапустите Creatio, чтобы они применились.

Рис. 2 — Пример заполнения указанных ключей в Vault




В данном примере используются данные из следующей строки файла ConnectionStrings.config:

```
<add name="dbPostgreSql" connectionString="Pooling=true; Database=SOME_DB_NAME; Host=SOME_DB_HOS
```

где:

- `DbHost` — адрес сервера БД, который соответствует параметру Host со значением `SOME_DB_HOST`.
- `DbPort` — порт сервера БД, который соответствует параметру Port со значением `SOME_DB_PORT`.
- `DbName` — адрес сервера БД, который соответствует параметру Database со значением `SOME_DB_NAME`.
- `Username` — имя пользователя БД, который соответствует параметру Username со значением `SOME_USER`.
- `Password` — пароль пользователя БД, который соответствует параметру Password со значением `SOME_PASSWORD`.

Подробнее: Versioned Key/Value Secrets Engine, официальная документация Vault (на английском языке).

## Настроить политики безопасности

Так как в Vault может храниться чувствительная информация различного типа, рекомендуем создать отдельные политики безопасности (policies), чтобы разграничить уровни доступа к указанным ключам. Доступ Creatio к хранилищу секретов необходимо ограничить правом на чтение.

В дальнейшем данные политики могут быть использованы при генерации клиентских токенов, предназначенных для авторизации, или при добавлении в Vault клиентских сертификатов.

Настройка политики, которая дает Creatio доступ на чтение всех секретов, определенных в хранилище с путем `<secretsEnginePath>` случае выглядит следующим образом:

```
path "<secretsEnginePath>/*"
{capabilities = ["read", "list"]
}
```

где `<secretsEnginePath>` — путь к хранилищу секретов.

Подробнее: Policies (официальная документация Vault на английском языке).

## Настроить авторизацию в Vault

В Creatio вы можете настроить следующие типы авторизации в Vault:

- по клиентскому сертификату;
- по токену.

### Настроить авторизацию по сертификату

1. Выпустите отдельный клиентский сертификат и зарегистрируйте его на хосте, где работает приложение Creatio.
2. Добавьте сертификат в Vault как метод авторизации.
3. Укажите политику, которая позволит читать секреты, содержащие информацию из строк подключения.

Подробнее: Auth Methods, официальная документация Vault (на английском языке).

### Настроить авторизацию по токену

При инициализации сервера Vault генерируется токен администратора (Root Token), который строго не рекомендуется использовать для авторизации, поскольку он дает практически неограниченные права. Для авторизации Creatio необходимо сгенерировать клиентский токен с определенными политиками безопасности, которые позволяют читать только секреты, предназначенные для подстановок в строки соединения вашего приложения.

Чтобы сгенерировать клиентский токен, предназначенный для авторизации Creatio в Vault, нужно выполнить команду:

```
vault token create -policy=<policyName>
```

где `<policyName>` — название политики безопасности.

Подробнее: Tokens, Token create - Command, официальная документация Vault (на английском языке).

# Настройки на стороне Creatio

## Настроить параметры подключения к Vault

Настройки подключения к Vault должны быть заданы в секции `vaultConfig` конфигурационного файла **web.config** в корневой папке Creatio. Описание параметров данного раздела содержится в таблице ниже:

| Название параметра | Описание | Значение |
|---|---|---|
| hostUri | Строка, содержащая адрес сервера Vault | Формат параметра: https://<адрес сервера Vault>:<порт, на котором развернут сервер Vault>. |
| authMethodType | Тип авторизации | Допустимые значения:<br>**Token** — авторизация по токену.<br>**Cert** — авторизация по сертификату. |
| secretsEnginePath | Путь к хранилищу секретов в Vault | В качестве пути рекомендуется использовать имя сайта. |
| token | Строка, содержащая клиентский токен. | Задается, если используется авторизация по токену. |
| certFilePath | Путь к сертификату. | Задается, если используется авторизация по сертификату. |
| certPassword | Пароль к сертификату. | Задается, если для доступа к сертификату используется пароль. Иначе остается пустым (""). |

В случае, если в качестве `authMethodType` задано недопустимое значение, то в работе Creatio возникнет ошибка.

Пример подключения по токену

```
<vaultConfig hostUri="https://127.0.0.1:1024" authMethodType="Token"
token="s.on3zJH6fXZlodRAYqgTXYEot"
secretsEnginePath="<secretsEnginePath>" />
```

Пример подключения по сертификату

```
<vaultConfig hostUri="https://127.0.0.1:1024"
authMethodType="Cert"
certFilePath="<path>"
```

```
  certPassword="<password>"
  secretsEnginePath="<secretsEnginePath>" />
```

где

- `<secretsEnginePath>` — путь к хранилищу секретов,
- `<path>` — путь к файлу сертификата,
- `<password>` — пароль для доступа к сертификату.

## Настроить шаблоны строк подключения

Файл ConnectionStrings.config должен содержать шаблоны строк подключения для замены их секретами из Vault. В шаблонах вместо секретных значений указывается название ключа секрета в **квадратных скобках**.

Например, если строка подключения содержит значение пароля `Password="somePassword"`, то шаблон строки подключения должен иметь вид `Password="[DBPassword]"`, где `DBPassword` — название ключа с секретом в Vault.

Если строка подключения не содержит секретной информации, то оставьте ее в неизменном виде. В этом случае не будет происходить замена значения строки аналогом из Vault.

К примеру, если конфигурационный файл содержит строку подключения:

```
<add name="dbPostgreSql" connectionString="Pooling=true; Database=SOME_DB_NAME; Host=SOME_DB_HOS
```

То шаблон такой строки может выглядеть следующим образом:

```
<add name="dbPostgreSql" connectionString="Pooling=true; Database=[DbName]; Host=[DbHost]; Userr
```

где `DbHost`, `DbPort`, `DbName`, `Username`, `Password` — ключи соответствующих секретов, хранящихся в Vault.

## Включить признаки

Для настройки **строк подключения** в конфигурационном файле web.config, который находится в корневой папке Creatio, добавьте следующие строки в секцию `<appSettings>`:

```
<add key="UseConnectionStringProvider" value="true" />
<add key="UseSecretsInConnectionStrings" value="true" />
```

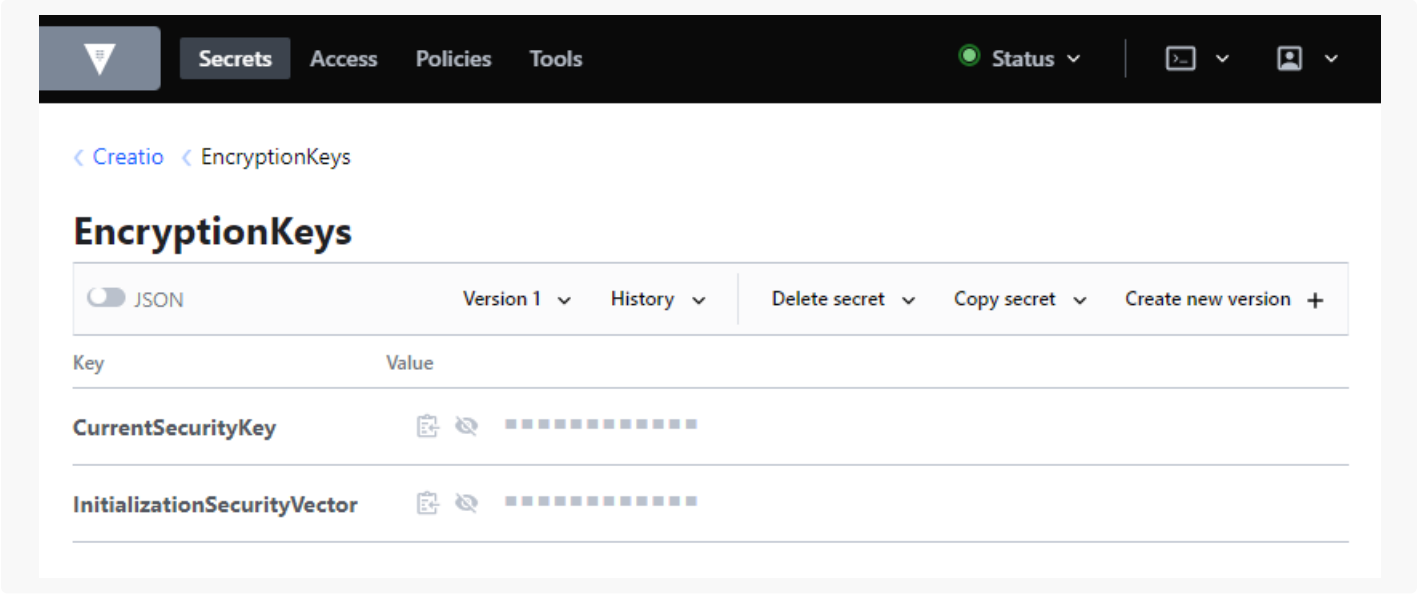
Если вы хотите использоваться также **ключи шифрования** (AES), то дополнительно выполните следующие настройки:

1. В конфигурационном файле web.config, который находится в корневой папке Creatio, добавьте

следующую строку в секцию `<appSettings>:<add key="UseSecretsInEncryptionKeys" value="true" />`

2. В хранилище секретов Vault, имя которого указано в конфигурационном файле в секции `vaultConfig` → параметр `secretsEnginePath`, добавьте секрет с названием `EncryptionKeys`.
3. В секрет EncryptionKeys добавьте ключи со значениями, которые указаны в конфигурационном файле приложения Creatio:
   - `InitializationSecurityVector`,
   - `CurrentSecurityKey`.
4. Удалите из конфигурационного файла признаки `InitializationSecurityVector`, `CurrentSecurityKey`.

Рис. 3 — Пример заполнения ключей




**Важно.** Названия секрета и ключей должны точно соответствовать указанным выше. В случае отключения указанных флагов хранение секретной информации в Creatio при помощи Vault не будет работать корректно.

Перезапустите Creatio, чтобы изменения вступили в силу.

## Отключить хранение ключей в Vault

Если необходимо отключить хранение ключей AES в Vault, то выполните следующие действия:

1. Добавьте в конфигурационный файл приложения Creatio признаки:
   - InitializationSecurityVector,
   - CurrentSecurityKey.

   Значения данных ключей хранятся в хранилище секретов Vault, имя которого указано в конфигурационном файле в секции `vaultConfig` → параметр `secretsEnginePath` → секрет `EncryptionKeys`:

```
<add key="InitializationSecurityVector" value="Значение_ключа_из_Vault" />

<add key="CurrentSecurityKey" value="Значение_ключа_из_Vault" />
```

2. В конфигурационном файле приложения Creatio выключите признак UseSecretsInEncryptionKeys:

```
<add key="UseSecretsInEncryptionKeys" value="false" />
```

3. Перезапустите Creatio, чтобы изменения вступили в силу.