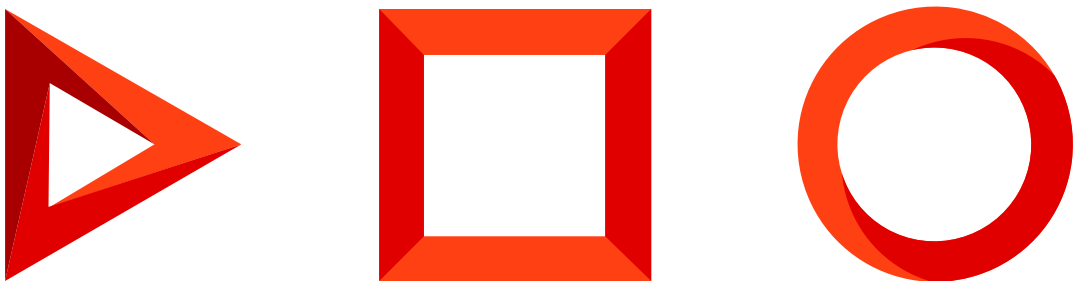
Creatio Academy

Настройка SSO через OneLogin

Настроить Single Sign-On через OneLogin

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.

© 2022 Terrasoft. Все права защищены.

Содержание

© 2022 Terrasoft. Все права защищены.

Настроить Single Sign-On через OneLogin

ПРОДУКТЫ: ВСЕ ПРОДУКТЫ

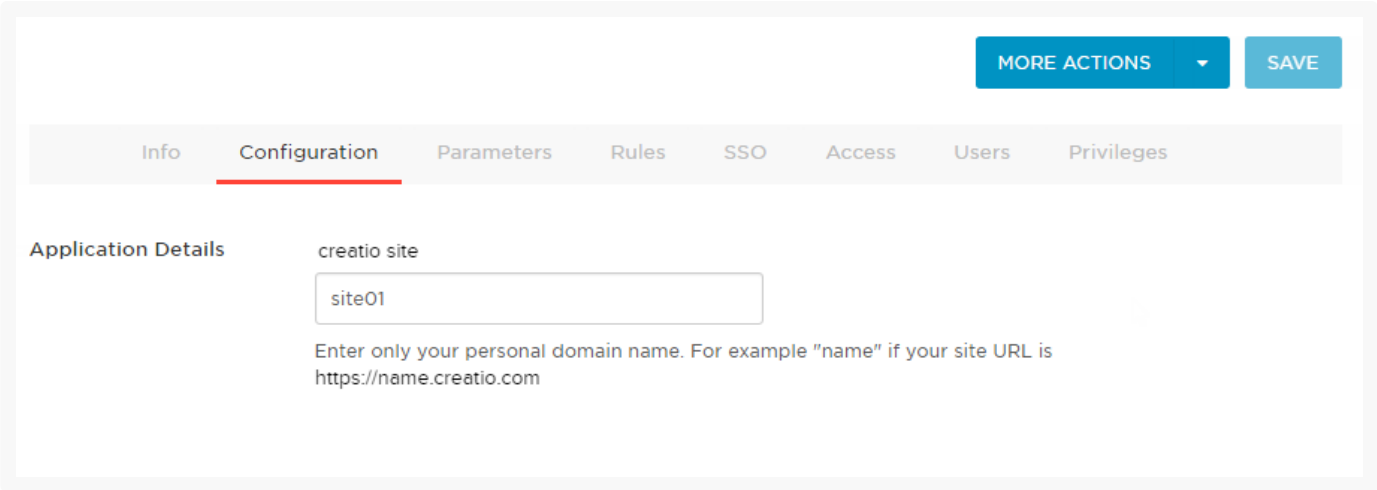
Вы можете использовать портал OneLogin в качестве единой точки входа для всех сервисов, которые используются в вашей компании, включая Creatio. Для этого нужно выполнить ряд настроек как на стороне OneLogin, так и на стороне Creatio.

Важно. В примере настройки использован адрес сайта Creatio https://site01.creatio.com/ и “appid” как id приложения на OneLogin. При выполнении настройки замените эти значения на адрес вашего сайта и id соответствующего приложения на OneLogin.

Выполнить настройки на стороне OneLogin

1. Войдите в OneLogin под учетной записью администратора.
2. Нажмите [*Приложения*] (“Apps”) и выберите [*Добавить приложения*] (“Add Apps”). В строке поиска введите “Creatio“ и выберите приложение Creatio.
3. Если необходимо, то измените значение в поле [*Отображаемое имя*] (“Display name”), измените иконки приложения или снимите признак [*Доступно на портале*] (“Visible in portal”). Эти настройки влияют на отображение сайта для пользователей на сайте OneLogin.
4. Нажмите [*Сохранить*] (“Save”).
5. После сохранения перейдите на вкладку [*Конфигурация*] (“Configuration”) и в поле [*Сайт Creatio*] (“Creatio site”) введите доменное имя вашего сайта, например, site01 (Рис. 1).

Рис. 1 — Страница конфигурации сайта



Выполнить настройки на стороне Creatio

Если вы используете **Creatio cloud**, то подготовьте информацию для настройки по инструкции ниже и

© 2022 Terrasoft. Все права защищены.

обратитесь в службу поддержки Creatio для применения настроек на сайте.

Ниже приведена инструкция по настройке единого входа для пользователей **on-site**. Настоятельно рекомендуем предоставить службе поддержки временный доступ к конфигурации Creatio, либо производить эту настройку под руководством службы технической поддержки.

Чтобы выполнить настройку на стороне Creatio, необходимо выполнить следующие настройки в конфигурационных файлах:

1. Внести настройки SAML-провайдера.
2. Настроить параметры SSO-аутентификации в Creatio.
3. Проверить базовые сценарии SSO.
4. Настроить Just-In-Time User Provisioning (JIT).
5. Включить использование SSO по умолчанию.

Рассмотрим эти пункты подробнее:

1. **Заполните настройки SAML-провайдера**, указав данные SAML-провайдера идентификации в saml.config.

   a. В параметре Name укажите FQDN вашего сайта.

   > **Важно.** Значение параметра ServiceProvider Name должно быть идентично значению Identifier, указанному на стороне провайдера идентификации ADFS. Таким образом выполняется проверка, что SAML Assertion выдан именно для вашего приложения. Для этого удобнее использовать FQDN вашего сайта, например, https://site01.creatio.com/Demo_161215/. Обратите внимание, URL должен совпадать полностью, включая “/” в конце.

   b. В секции Partner Identity Provider укажите настройки со стороны IdP. Эти настройки можно посмотреть в файле метаданных.

   - **WantAssertionSigned** — укажите “false“, если не будет использоваться сертификат шифрования при обмене SALM Assertion.

     ```
     WantAssertionSigned="false"
     ```

   - **SingleSignOnServiceUrl** — URL сервиса единого входа провайдера. Можно взять из строки SAML 2.0 Endpoint (HTTP) на странице trusted приложения.

     ```
     SingleSignOnServiceUrl="https://ts-dev.onelogin.com/trust/saml2/http-post/sso/appid"
     ```

   - **SingleLogoutServiceUrl** — URL сервиса единого входа провайдера. Можно взять из строки SLO Endpoint (HTTP) на странице trusted приложения.

     ```
     SingleLogoutServiceUrl="https://ts-dev.onelogin.com/trust/saml2/http-redirect/slo/appid"
     ```

© 2022 Terrasoft. Все права защищены.

2. **Включите использование SSO-провайдера в Creatio**. Для этого внесите необходимые настройки в web.config в корневой папке сайта:

   a. Включите использование SSO Auth-провайдеров при выполнении авторизации в Creatio:

   - **SsoAuthProvider** — провайдер входа в основное приложение.
   - **SSPSsoAuthProvider** — провайдер входа на портал.
     Указывать можно оба провайдера или только один, который нужен в конкретном случае.

   ```
   <terrasoft>
   <auth providerNames="InternalUserPassword,SSPUserPassword,SsoAuthProvider,SSPSsoAuthProv
   <providers>
   ```

   d. Укажите, какой из провайдеров идентификации, указанных в saml.config, нужно использовать по умолчанию в Service Provider initiated SSO-сценариях. В web.config App Loader задайте параметр PartnerIdP значением из строки Issuer URL в saml.config, например:

   ```
   <appSettings> ... <add key="PartnerIdP" value="https://app.onelogin.com/saml/metadata/appi
   ```

   e. Установите использование SSO-провайдера по умолчанию при входе на сайт. Для этого укажите в web.config App Loader ресурс по умолчанию Login/NuiLogin.aspx?use_sso=true.

   На заметку. Для возможности входа с использованием логина/пароля остается доступной прямая ссылка https://site01.creatio.com/Login/NuiLogin.aspx?. Для тестирования работы SSO до включения по умолчанию можно использовать ссылку https://site01.creatio.com/NuiLogin.aspx?use_sso=true.

   f. Установите отправку к провайдеру идентификации при переходе в корень сайта:

   ```
   <defaultDocument> <files> <add value="Login/NuiLogin.aspx?use_sso=true" /> </files> </defau
   ```

   g. Установите отправку к провайдеру идентификации при отсутствии сессии пользователя:

   ```
   <authentication mode="Forms">
   <forms loginUrl="~/Login/NuiLogin.aspx?use_sso=true" protection="All" timeout="60" name="./
   </authentication>
   ```

3. **Проверьте базовый сценарий** Identity Provider (IdP) initiated SSO, чтобы убедиться в корректности настроек:

   a. Переход на страницу доверенных приложений IdP (ссылка по умолчанию: https://sts.contoso.com/adfs/ls/idpinitiatedsignon.aspx).

   b. Выполнение авторизации.

   c. Переход на Creatio с результатом авторизации на IdP.

© 2022 Terrasoft. Все права защищены.

До включения провайдера SSO на стороне Creatio по умолчанию используйте для проверки корректности настроек IdP initiated сценарий. До выполнения проверки убедитесь, что в Creatio содержится активная учетная запись, логин которой совпадает с NameId, передаваемым Identity Provider. В противном случае процесс SSO настройки не будет успешно завершен, поскольку не удастся сопоставить пользователя из домена с пользователем в Creatio. Как только вход через SSO будет выполнен успешно, перейдите к дальнейшим настройкам.

4. **Настройте Just-In-Time User Provisioning (JIT)**. Функциональность Just-In-Time User Provisioning дополняет технологию единого входа. Она позволяет не только создать пользователя при первом входе в приложение, но и при каждом входе обновлять данные на странице контакта данными, полученными от провайдера идентификации. Подробнее читайте в статье Настроить Just-In-Time User Provisioning.

   a. В web.config в корневой папке приложения добавьте настройки для JIT**:**

   ```
   <add name="UseJit" value="true" />
   ```

   Тип пользователя определяется страницей, с которой им был выполнен вход в систему. Если для входа используется сценарий **IdP initiated**, то необходимо явно указать значение DefUserType:

   - General — обычный пользователь;
   - SSP — пользователь портала.

   d. Настройте сопоставление полей из SAML Assertion с колонками в Creatio в справочнике [*Преобразователь SAML атрибута в название поля контакта*]. Это необходимо для корректного заполнения полей контакта при создании нового пользователя с помощью Just-In-Time User Provisioning. Если поле пусто или отсутствует в данных провайдера идентификации, то оно может быть заполнено значением, указанным в поле[*Значение по умолчанию*] справочника. При следующем входе пользователя поля контакта, указанные в справочнике, будут заполнены значением, полученным из провайдера, или актуальным значением по умолчанию.

   > **На заметку.** Если справочника нет в списке справочников, то его необходимо зарегистрировать.

5. **Включите использование SSO-провайдера по умолчанию** при входе на сайт. Рекомендуем выполнять действие только в случае успешного выполнения предыдущих шагов и проверки корректности работы. После успешного выполнения этого шага будет доступен для использования Service Provider (SP) initiated SSO. Стандартный сценарий Service Provider (SP) initiated:

   a. Переход на Creatio, у пользователя нет активной сессии на сайте.

   b. Переадресация на IdP, выполнение авторизации.

   c. Переадресация Переход на Creatio с результатом авторизации из IdP.

   Для включения провайдера SSO по умолчанию:

   a. Включите Single Log Out в web.config в папке Terrasoft.WebApp:

© 2022 Terrasoft. Все права защищены.

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

b. Для использования технологии единого входа в мобильном приложении установите признак [*Значение по умолчанию*] в системной настройке “Использовать SSO в мобильном приложении“ (код “MobileUseSSO“).

© 2022 Terrasoft. Все права защищены.