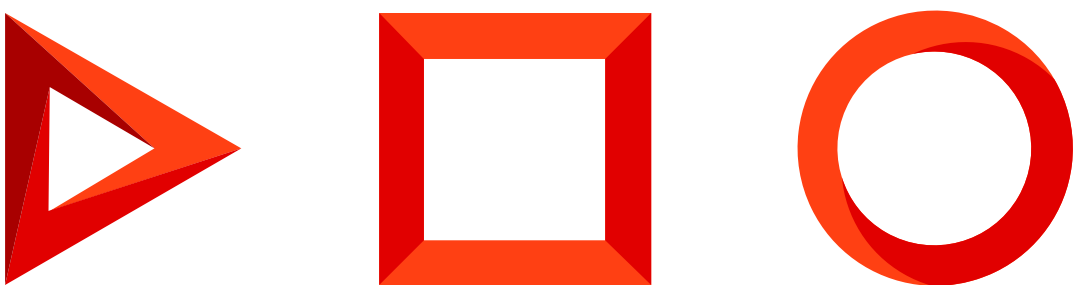
Creatio Academy

Настройка SSO через ADFS

Настроить Single Sign-On через ADFS

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 Single Sign-On через ADFS

ПРОДУКТЫ: ВСЕ ПРОДУКТЫ

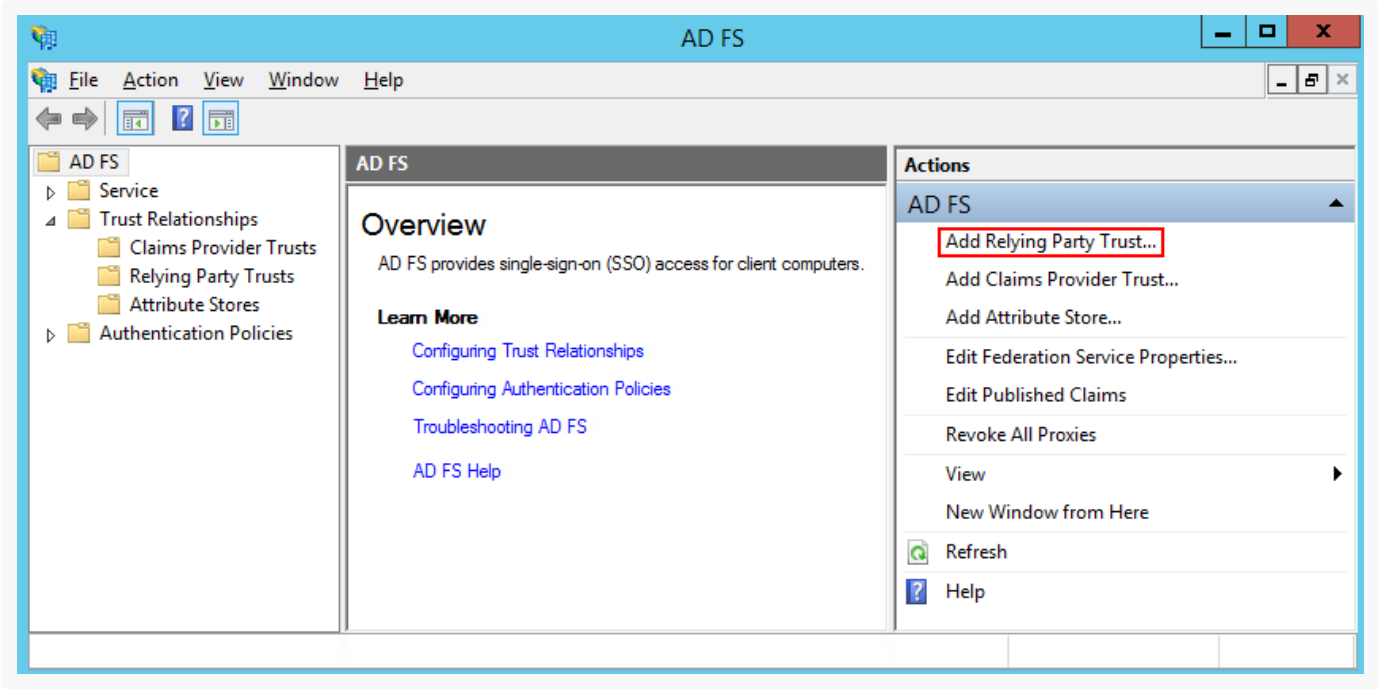
Вы можете настроить интеграцию Creatio с Active Directory Federation Services (ADFS), чтобы с ее помощью управлять возможностью единого входа для всех пользователей системы. Для этого нужно выполнить ряд настроек как на стороне ADFS, так и на стороне Creatio.

Важно. В примере использован адрес сайта Creatio https://site01.creatio.com/Demo_161215/ и адрес сайта сервиса ADFS http://adfs01.mysite.com/adfs/. При выполнении настройки замените адреса на соответствующие адреса ваших сайтов.

Выполнить настройки на стороне ADFS

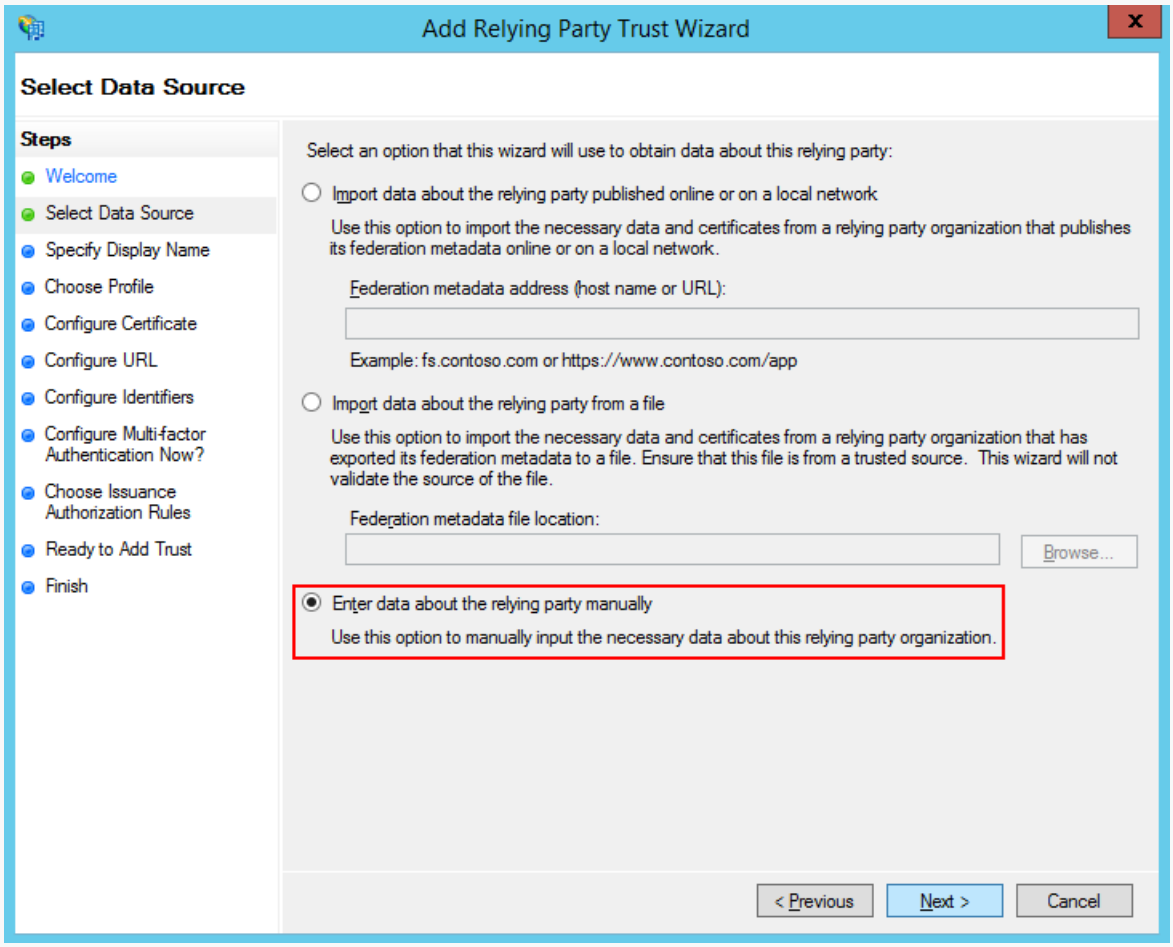
1. Добавьте в ADFS нового поставщика ресурсов (Relying Party Trusts) (Рис. 1).

Рис. 1 — Добавление нового поставщика ресурсов



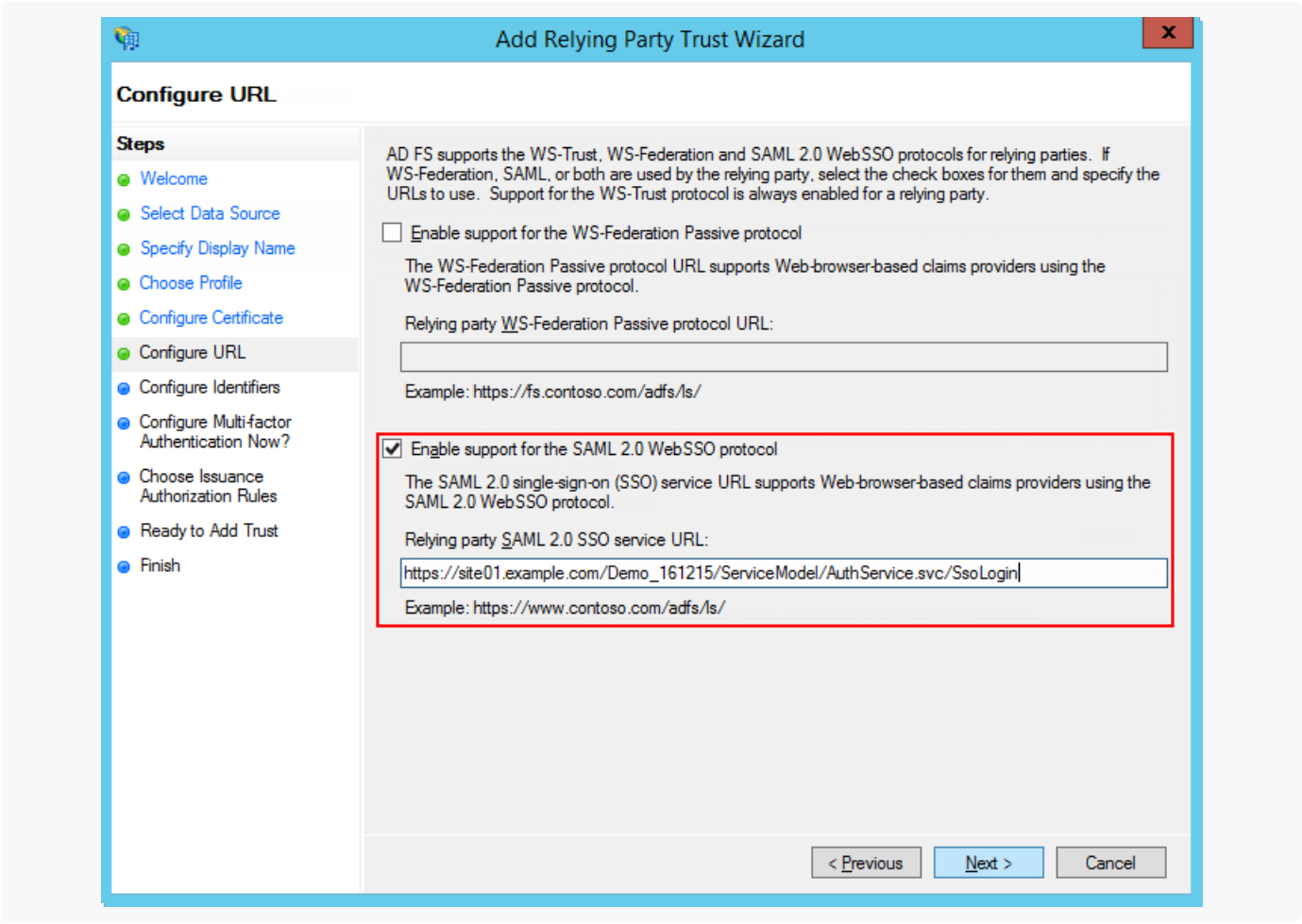
2. Выберите опцию ручного ввода данных (“Enter data about the relying party manually”), как показано на Рис. 2.

Рис. 2 — Выбор опции ручного ввода данных о поставщике ресусов



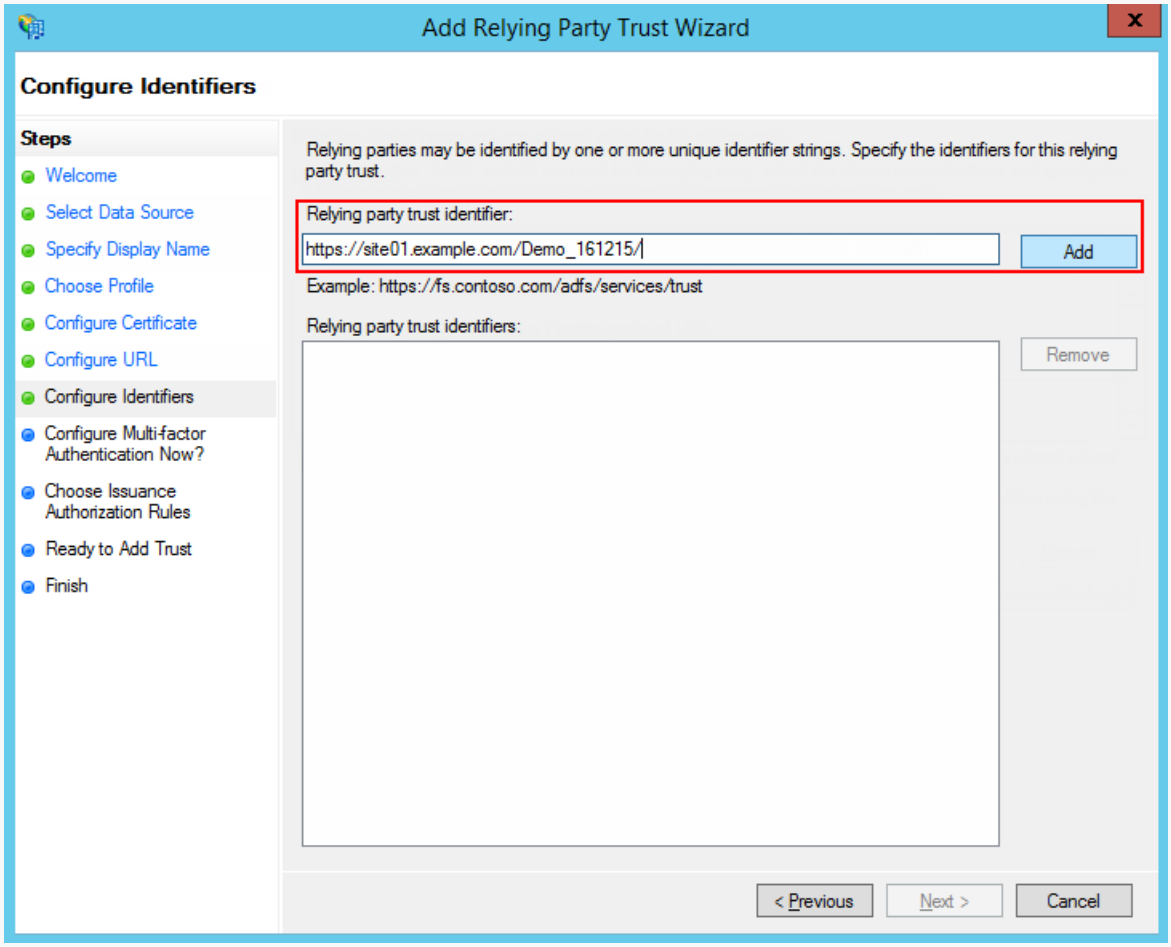
3. В поле [*Отображаемое имя*] (“Display name”) введите название Relying Party. Имя необходимо только для упорядоченного ведения списка доверенных приложений в ADFS.
4. Оставьте профиль “AD FS Profile”, выбранный по умолчанию. Нажмите кнопку [*Далее*] (“Next”).
5. На шаге выбора сертификата нажмите кнопку [*Далее*] (“Next”).
6. Включите поддержку протокола SAML 2.0. Укажите адрес сайта, добавьте к нему “/ServiceModel/AuthService.svc/SsoLogin” (Рис. 3).

Рис. 3 — Включение поддержки протокола SAML 2.0



7. В настройках идентификаторов укажите полный адрес сайта и нажмите кнопку [*Добавить*] (“Add”) как показано на Рис. 4.

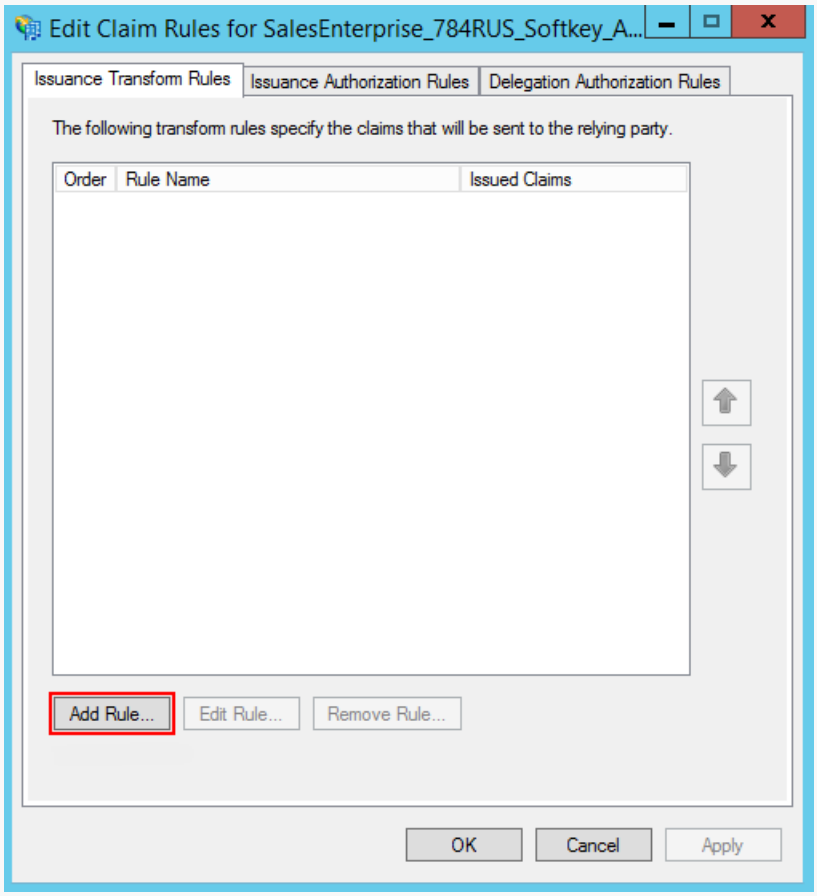
Рис. 4 — Указание идентификатора



Важно. Идентификатор используется при проверке подлинности источника, который запрашивает выполнение аутентификации. URL должен совпадать полностью, включая “/” в конце.

8. Значения остальных параметров настройте в соответствии с требованиями безопасности вашей организации. Для тестового использования эти настройки можно оставить по умолчанию.
9. Нажмите [*Завершить*] (“Finish”). В открывшемся окне по кнопке [*Добавить правило*] (“Add Rule”) добавьте новое правило формирования SAML Assertion в SAML Response (Рис. 5).

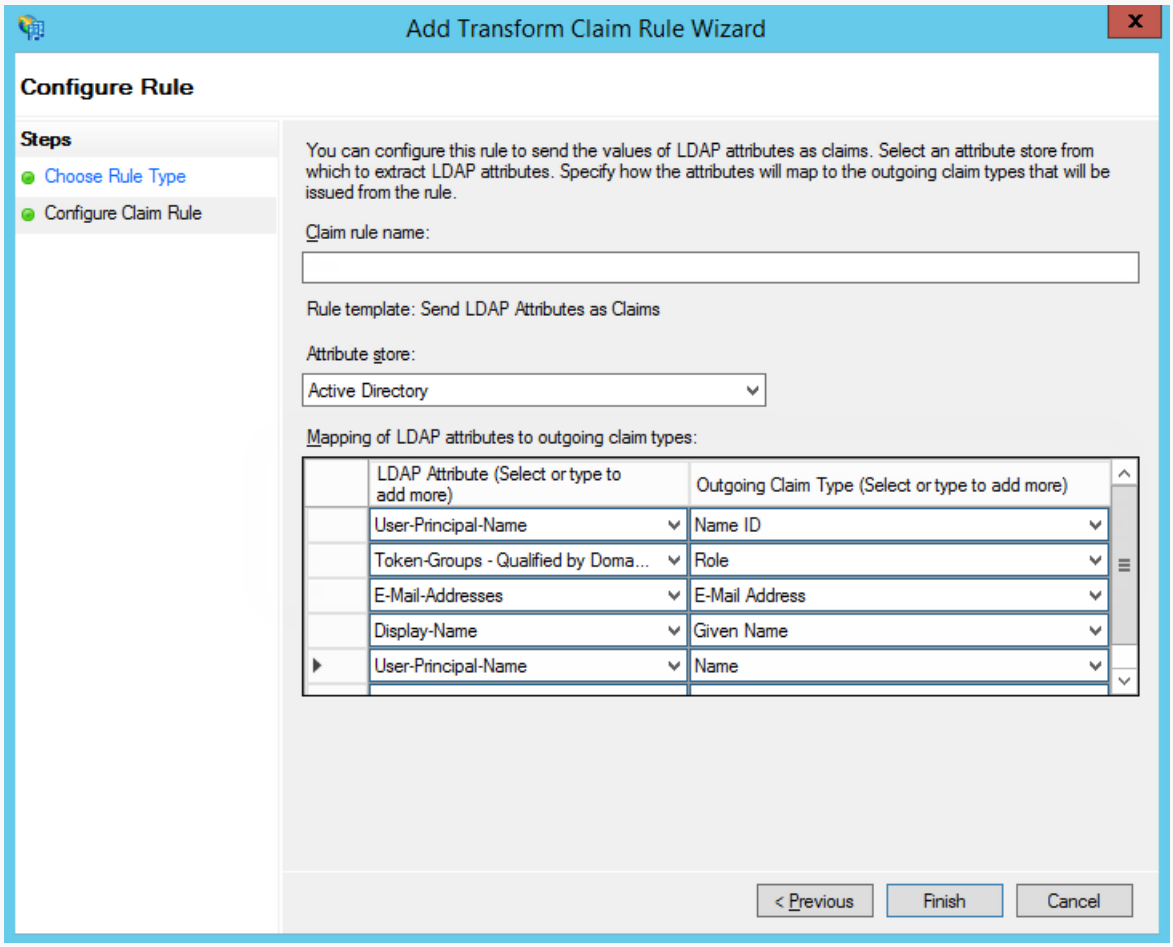
Рис. 5 — Добавление правила



На заметку. Данные, которые формируются новым правилом, будут использоваться приложением Creatio для поиска пользователя, актуализации его профиля и ролей.

10. На первом шаге добавления правила оставьте настройку, выбранную по умолчанию, и нажмите кнопку [*Далее*] (“Next”). Установите набор параметров, которые будут получены из данных пользователя (Рис. 6). В указанном примере в SAML Assertion будет передаваться имя (“Name”) пользователя и список групп домена, в которые он входит.

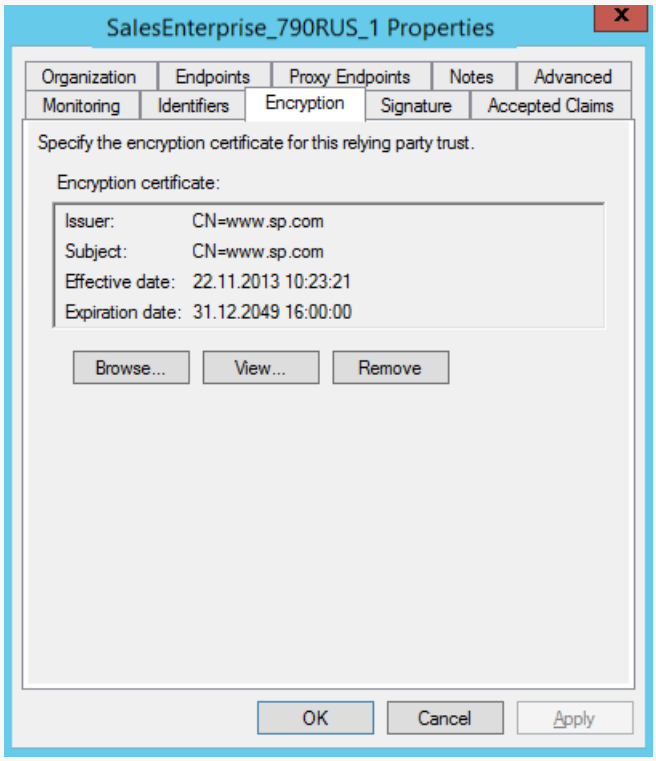
Рис. 6 — Установка параметров правила



11. Нажмите кнопку [*Сохранить*] (“Save”).
12. Откройте настройки созданного поставщика ресурсов “Trusted Relay” и на вкладке с расширенными настройками (“Advanced”) укажите шифрование SHA-1 согласно алгоритму сертификата сайта.
13. Для настройки шифрования SAML-пакета на вкладке с настройками шифрования (“Encryption”) добавьте публичный ключ сертификата (Рис. 7).

На заметку. Если вы используете Creatio cloud, то публичный ключ сертификата будет предоставлен службой поддержки.

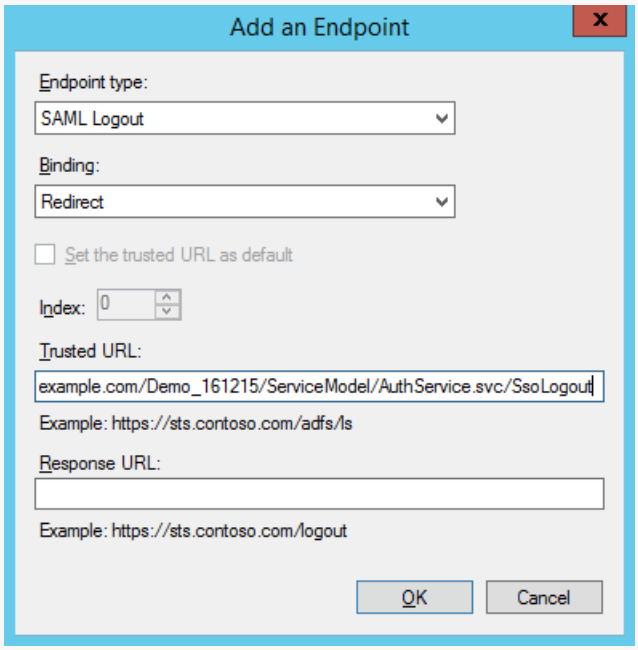
Рис. 7 — Добавление публичного ключа



14. На вкладке [*Конечные точки*] (“Endpoints”) добавьте конечную точку (“Logout endpoint”), и установите такие параметры (Рис. 8):

- **Endpoint type**: SAML Logout.
- **Binding**: Redirect.
- **Trusted URL**: https://site01.creatio.com/Demo_161215/ServiceModel/AuthService.svc/SsoLogout.

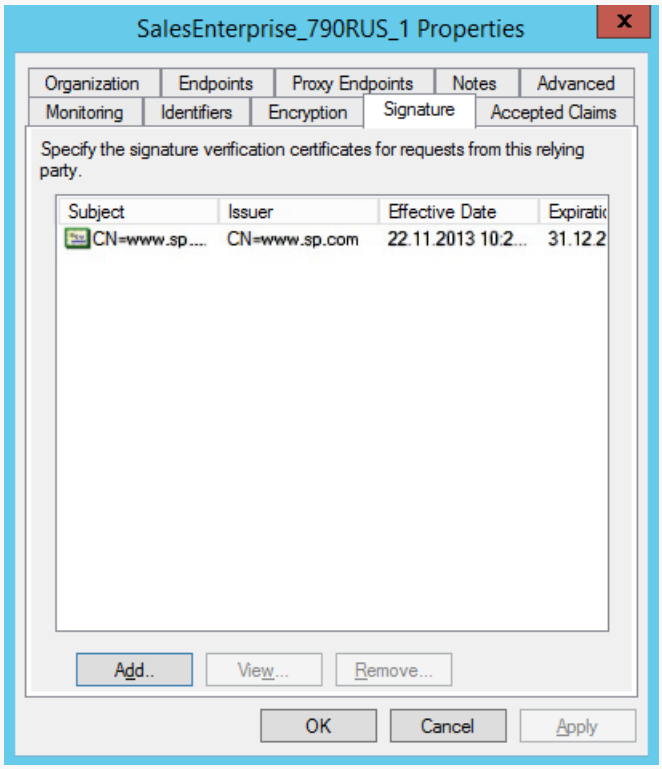
Рис. 8 — Установка параметров конечной точки



15. На вкладке [*Подпись*] (“Signature”) добавьте сертификат для подписывания (“Logout Request”) как

показано на Рис. 9.

Рис. 9 — Добавление сертификата



Важно. Без сертификата не будет работать выход из приложений.

Выполнить настройки на стороне Creatio

Если вы используете **Creatio cloud**, то подготовьте информацию для настройки по инструкции ниже и обратитесь в службу поддержки Creatio для применения настроек на сайте.

Ниже приведена инструкция по настройке единого входа для пользователей **Creatio 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.

Настройки для приложения на .NET Framework и приложения на .NET Core имеют ряд различий, которые ниже будут рассмотрены подробнее.

.NET Framework

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="false"** — если не будет использоваться сертификат шифрования при обмене SALM Assertion.
   - **SingleSignOnServiceUrl** — URL сервиса единого входа провайдера. Для ADFS, как правило, это: https://adfs01.mysite.com/adfs/ls.
   - **SingleLogoutServiceUrl** — URL сервиса единого выхода провайдера. Для ADFS, как правило, это: https://adfs01.mysite.com/adfs/ls.
   - **PartnerCertificateFile** — путь к сертификату безопасности в формате .*cer в файловой системе сервера относительно корня приложения Creatio. Нужно задавать, если WantAssertionSigned="true".
   - **SignLogoutRequest="true"** — важно указывать для ADFS, поскольку подписывание LogoutRequest обязательно. Если установлено значение “true”, то необходимо указать сертификат для формирования подписи в параметре LocalCertificateFile.
   - **SignLogoutResponse="true"** — важно указывать для ADFS, поскольку подписывание LogoutResponse обязательно. Если установлено значение “true”, то необходимо указать сертификат для формирования подписи в параметре LocalCertificateFile.
   - **OverridePendingAuthnRequest="true"** — опция, при включении которой не будет выполняться валидация на соответствие ответа IdP ранее созданным Auth Request.
   Пример saml.config для ADFS:

```
    <ServiceProvider Name="https://site01.creatio.com/Demo_161215/"

                Description="Example Creatio Service Provider"
                AssertionConsumerServiceUrl="~/ServiceModel/AuthService.svc/SsoLogin"
                LocalCertificateFile="sp.pfx"
                LocalCertificatePassword="password"
            />
    <PartnerIdentityProviders>

<!-- ADFS Creatio -->
```

```
        <PartnerIdentityProvider Name="http://adfs01.mysite.com/adfs/services/trust"
                                 OverridePendingAuthnRequest="true"
                                      Description="MVC Example Identity Provider"
                                      SignAuthnRequest="false"
                                      SignLogoutRequest="true"
                                      SignLogoutResponse="true"
                                      WantSAMLResponseSigned="false"
                                      WantAssertionSigned="false"
                                      WantAssertionEncrypted="false"
                                      SingleSignOnServiceUrl="https://adfs01.mysite.com/ad
                                      SingleLogoutServiceUrl="https://adfs01.mysite.com/ad
                                      PartnerCertificateFile="Certificates\idp.cer"/>
```

Если включен флаг SignLogoutRequest или SignLogoutResponse, то добавьте в файловую систему, в которой находится приложение Creatio, приватный ключ сертификата шифрования в формате .*pfx. Укажите путь к файлу, а также пароль в файлах конфигурации saml.config и убедитесь, что пользователь, под которым запущено приложение, имеет права на чтение файла. Важно, чтобы сертификат был физически добавлен в корневую папку сайта и в папку Terrasoft.WebApp.

```
LocalCertificateFile="sp.pfx"
LocalCertificatePassword="password"
```

Рис. 10 — Настройка шифрования SAML-пакета

```
<?xml version="1.0"?>
<SAMLConfiguration xmlns="urn:componentspace:SAML:2.0:configuration">
   <ServiceProvider Name="https://site01.creatio.com/Demo_161215/"

               Description="Example Creatio Service Provider"

               AssertionConsumerServiceUrl="~/ServiceModel/AuthService.svc/SsoLogin"
               LocalCertificateFile="sp.pfx"
               LocalCertificatePassword="password"
           />
   <PartnerIdentityProviders>
```

2. **Включите использование SSO-провайдера в Creatio**. После указания настроек SAML-провайдера необходимо включить использование SAML SSO 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> <authproviderNames="InternalUserPassword,SSPUserPassword,SsoAuthProvider,
```

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="http://adfs01.mysite.com/adfs/services/trust"/>

...

</appSettings>
```

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

   - Переход на страницу доверенных приложений IdP (ссылка по умолчанию: https://sts.contoso.com/adfs/ls/idpinitiatedsignon.aspx).
   - Выполнение авторизации.
   - Переход на Creatio с результатом авторизации на IdP.

     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 Identity Provider 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, 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:

   - Переход на Creatio, у пользователя нет активной сессии на сайте.
   - Переадресация на IdP, выполнение авторизации.
   - Переход на Creatio с результатом авторизации из IdP.

   Для включения провайдера SSO по умолчанию:

   a. Укажите в корневом web.config ресурс по умолчанию 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\

   b. Установите отправку к провайдеру идентификации при переходе в корень сайта в корневом web.config:

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

   <authentication mode="Forms">
           <forms loginUrl="~/Login/NuiLogin.aspx?use_sso=true ...
   </authentication>
   ```

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

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

d. Укажите в web.config в папке Terrasoft.WebApp ресурс для перенаправления при истечении активной сессии:

```
<authentication mode="Forms">
        <forms loginUrl="~/../Login/NuiLogin.aspx?use_sso=true...
</authentication>
```

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

.Net Core

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

   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.

     ```
     "WantLogoutRequestSigned":false
     ```

   - **SingleSignOnServiceUrl** — URL сервиса единого входа провайдера. Для ADFS, как правило, это: https://adfs01.mysite.com/adfs/ls.

     ```
     "SingleSignOnServiceUrl":"https://adfs01.mysite.com/adfs/ls"
     ```

   - **SingleLogoutServiceUrl** — URL сервиса единого выхода провайдера. Для ADFS, как правило, это: https://adfs01.mysite.com/adfs/ls.

     ```
     "SingleLogoutServiceUrl":"https://adfs01.mysite.com/adfs/ls"
     ```

   - **PartnerCertificates** — путь к сертификату безопасности в формате .*cer в файловой системе сервера относительно корня приложения Creatio. Нужно задавать, если

WantAssertionSigned="true".

```
"PartnerCertificates":[
   {
      "FileName":"adfs_sandbox.cer"
   }
```

- **SignLogoutRequest** – укажите “true” для ADFS, поскольку подписывание LogoutRequest обязательно. Если установлено значение “true”, то необходимо указать сертификат для формирования подписи в параметре LocalCertificateFile.

```
"SignLogoutRequest":true
```

- **SignLogoutResponse** — укажите “true” для ADFS, поскольку подписывание LogoutResponse обязательно. Если установлено значение “true”, то необходимо указать сертификат для формирования подписи в параметре LocalCertificateFile.

```
"SignLogoutResponse":true
```

2. Если включен флаг SignLogoutRequest или SignLogoutResponse, то добавьте в файловую систему, в которой находится приложение Creatio, приватный ключ сертификата шифрования в формате .*pfx. Укажите путь к файлу, а также пароль в файле конфигурации saml.json, и убедитесь, что пользователь, под которым запущено приложение, имеет права на чтение файла. Важно, чтобы сертификат был физически добавлен в корневую папку сайта и в папку Terrasoft.WebApp.

```
"..""LocalCertificates":[
   {
"FileName":"sp.pfx",
"Password":"password"}
]"..."
```

3. **Включите использование SSO-провайдера в Creatio**. После указания настроек SAML-провайдера необходимо включить использование SAML SSO в Creatio. Для этого внесите необходимые настройки в **Terrasoft.WebHost.dll.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.

```
"...

<auth providerNames=""LdapProvider,InternalUserPassword,SSPUserPassword,SsoAuthProvid
```

```
..."
```

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

```
"...""PartnerName":"http://adfs.sandbox.local/adfs/services/trust",
"..."
```

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

   - Переход на страницу доверенных приложений IdP (ссылка по умолчанию: https://sts.contoso.com/adfs/ls/idpinitiatedsignon.aspx).
   - Выполнение авторизации.
   - Переход на Creatio с результатом авторизации на IdP.

     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.

5. **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 **Terrasoft.WebHost.dll.config** в корневой папке приложения добавьте настройки для JIT (включается для пользователей системы в настройках SsoAuthProvider и для пользователей портала в настройках SSPSsoAuthProvider):

```
...
<provider name="SsoAuthProvider" type="Terrasoft.Authentication.Core.SSO.BaseSsoAuthProvider,
Terrasoft.Authentication">
<parameters>
<add name="UserType" value="General" />
<add name="UseJit" value="true" />
</parameters>
</provider>
<provider name="SSPSsoAuthProvider"
type="Terrasoft.Authentication.Core.SSO.BaseSsoAuthProvider, Terrasoft.Authentication">
<parameters>
<add name="UserType" value="SSP" />
<add name="UseJit" value="true" />
```

```
</parameters>
...
```

Тип пользователя определяется страницей, с которой им был выполнен вход в систему. Если для входа используется сценарий Identity Provider 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, 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.

6. **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:

   - Переход на Creatio, у пользователя нет активной сессии на сайте.
   - Переадресация на IdP, выполнение авторизации.
   - Переход на Creatio с результатом авторизации из IdP.

   Для включения провайдера SSO по умолчанию:

   a. Укажите в файле saml.json UseSsoByDefault": "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\

   b. Установите отправку к провайдеру идентификации при переходе в корень сайта в **Terrasoft.WebHost.dll.config**:

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

 <authentication mode="Forms">
        <forms loginUrl="~/Login/NuiLogin.aspx?use_sso=true ...
```

```
 </authentication>
```

c. Включите Single Log Out в **Terrasoft.WebHost.dll.config**:

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

d. Укажите в **Terrasoft.WebHost.dll.config** ресурс для перенаправления при истечении активной сессии:

```
<authentication mode="Forms">
 <forms loginUrl="~/../Login/NuiLogin.aspx?use_sso=true...
</authentication>
```

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