Настройка аутентификации SAML SSO

Следующая настройка предполагает, что у вас уже есть учетная запись с доверенным поставщиком удостоверений. Вам необходимо знать URL-адрес входа SAML и иметь сертификат x.509, предоставленный поставщиком удостоверений. Вы также должны быть знакомы с форматом ответа SAML от вашего поставщика.

Настройку может выполнять только пользователь, имеющий права администратора.

Включение SAML аутентификации

1. В Панели администратора откройте раздел **Настройки** и перейдите на вкладку **Аутентификация**.
2. На вкладке **SAML** установите флаг **Включить функцию единого входа**. Убедитесь, что в файле *admin/config.inc.php* для параметра **$conf['auth_remote']** установлено значение **1**.
3. В поле **Режим аутентификации** выберите требуемый режим. По умолчанию установлено **Разрешены обе аутентификации**. Доступны следующие значения:

    - **Разрешены обе аутентификации**. Пользователь сможет войти в KBPublisher, используя SSO и/или встроенную аутентификацию.
    - **Разрешена только SAML аутентификация**. Пользователь сможет войти в систему, используя только SSO аутентификацию.
    - **Разрешена только SAML аутентификация с автоматическим входом** . Пользователь сможет войти в систему, используя SSO аутентификацию, и, если возможно, на сервере SAML будет применяться автоматическая аутентификация.

4. Настройте следующие параметры **Провайдера идентификации**:

    - **Название** – имя вашего поставщика единого входа, которое будет отображаться на странице входа.
    - **Провайдер** – уникальный идентификатор вашего поставщика удостоверений (обычно URL). Иногда может называться Entity ID.
    - **URL службы единого входа** – URL-адрес входа SAML, куда Контроллер будет направлять запросы входа в систему, инициируемые поставщиком сервиса (SP). Параметр обязателен.
    - **Тип подключения службы единого входа** – вы можете изменить привязку для URL входа. По умолчанию используется **HTTP-Redirect**. Также для выбора доступен тип –**HTTP-POST**.
    - **URL службы единого выхода** – URL-адрес, куда Контроллер будет перенаправлять пользователей после их выхода из системы. Если URL выход не указан, то после выхода из системы пользователь попадет на страницу авторизации в KBPublisher.
    - **Тип подключения службы единого выхода** – вы можете изменить привязку для URL выхода. По умолчанию используется **HTTP-Redirect**. Также для выбора доступен тип –**HTTP-POST**.
    - **Контексты аутентификации** – задайте возможные значения контекста аутентификации. Каждое значение вводите с новой строки. Чтобы использовать значение по умолчанию, оставьте поле пустым.
      Примеры:
      urn:oasis:names:tc:SAML:2.0:ac:classes:Password
      urn:oasis:names:tc:SAML:2.0:ac:classes:X509
      Если поле пустое, то используется значение по умолчанию:
      urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
      Для Azure AD введите: urn:oasis:names:tc:SAML:2.0:ac:classes:Password
    - **Сертификат открытого ключа формата X.509** – сертификат x.509 из конфигурации поставщика удостоверений.

5. В секции **Соответствие полей пользователя** укажите, каким образом пользователи, прошедшие проверку подлинности SAML, будут идентифицированы в Контроллере KBPublisher:

    - **Атрибут SAML для ID Удаленного пользователя** – уникальный идентификатор пользователя в ответе SAML. Значение отвечает за идентификацию пользователя в запросах на аутентификацию. По умолчанию используется элемент SAML **NameID**.
    - **Атрибут SAML для имени пользователя** – укажите атрибут, содержащий имя пользователя. В приведенном примере значение равно User.firstName.
    - **Атрибут SAML для фамилии пользователя** – укажите атрибут, содержащий фамилию пользователя. В приведенном примере значение равно User.lastName.
    - **Атрибут SAML для email пользователя** – укажите атрибут, содержащий адрес электронной почты пользователя. Для всех пользователей SAML значение должно быть уникальным. В приведенном примере значение равно User.email.
    - **Атрибут SAML для логина пользователя** – укажите атрибут, содержащий логин пользователя. Для всех пользователей SAML значение должно быть уникальным. В приведенном примере значение равно User.email.

ПРИМЕР ОТВЕТА

```
<saml:AttributeStatement>
  ...
  <saml:Attribute Name="User.OpenIDName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">adynamo</saml:AttributeValue>
  </saml:Attribute>
  ...
  <saml:Attribute Name="User.firstName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
xsi:type="xs:string">John</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute Name="User.lastName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">Doo</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute Name="User.email" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">John.Doo@example.com</saml:AttributeValue>
  </saml:Attribute>
  ...
</saml:AttributeStatement>
```

6. Чтобы сопоставить атрибуты группы SAML с привилегиями и ролями KBPublisher, настройте **Атрибут SAML для привилегий** и **Атрибут SAML для ролей**. Используемые вами настройки зависят от структуры атрибута группы SAML в ответе.

   Примечание: Этот шаг можно пропустить. Если вы оставите поля пустыми, они не перезапишутся при входе пользователя в систему. Вы можете назначить необходимые привилегии и/или роли позже.

ПРИМЕР ОТВЕТА

```
<saml:AttributeStatement>
  ...
  <saml:Attribute Name="User.OpenIDName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">adynamo</saml:AttributeValue>
  </saml:Attribute>
  ...
  <saml:Attribute Name="User.group" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">Editor</saml:AttributeValue>
  </saml:Attribute>
  ...
</saml:AttributeStatement>
```

Внимание! Если сопоставить группы SAML с привилегиями KBPublisher, то всем подходящим пользователям будет назначена указанная привилегия. Если у вас отсутствует Неограниченная лицензия (**Unlimited**), и превышено количество разрешенных пользователей, то привилегия не назначится.

Используйте те же шаги для сопоставления атрибута SAML для ролей.

1. В поле **Атрибут SAML для привилегий** нажмите кнопку [**...**]. Откроется окно **Соответствия групп к привилегиям**.
2. Нажмите кнопку [**+**] для добавления соответствия.
3. В открывшихся полях введите название SAML-атрибута группы и значение SAML-атрибута группы. Выберите привилегию в KBPublisher для сопоставления. В приведенном примере группа User.group сопоставляется со значением Editor.
4. Нажмите кнопку **Добавить**.
5. После добавления всех необходимых правил нажмите кнопку **Готово**.

7. Настройте параметры **Сервис-провайдера**:

   - **Метаданные**. Используйте эту информацию, чтобы связать базу знаний с вашим поставщиком удостоверений.
   - **Сертификат открытого ключа формата X.509**. Если ваш поставщик удостоверений требует подпись и/или шифрование сообщений, скопируйте содержимое своего сертификата и вставьте его в поле окна, открывающегося при нажатии кнопки [**...**].
   - **Закрытый ключ**. Если ваш поставщик удостоверений требует подпись и/или шифрование сообщений, скопируйте содержимое своего закрытого ключа и вставьте его в поле окна, открывающегося при нажатии кнопки [**...**].
   - **Алгоритм подписи**. Выберите алгоритм подписи для всех запросов SAML.

Дополнительная конфигурация

- **Переписать пользователя при входе в систему** – предназначено для задания времени в секундах, которое необходимо для перезаписи пользовательских данных при входе в систему. Введите **0**, чтобы отключить обновления данных пользователя при входе в систему. Введите **1** для перезаписи пользовательских данных каждый раз когда приходит запрос на аутентификацию.
- **Информация об учетной записи пользователя** – поле указывает, может ли пользователь обновлять информацию о своей учетной записи. Доступны значения:
  - **0** - Выключено, пользователь не может обновлять информацию о своем аккаунте;
  - **1** - Включено, пользователь может обновлять информацию о своем аккаунте;
  - **2** - Авто, зависит от других настроек.

ID статьи: 442

Последнее обновление: 10 мая, 2023
Обновлено от: Черевко Ю.
Ревизия: 6
Руководство пользователя v8.0 -> Единый вход -> SAML аутентификация -> Настройка аутентификации SAML SSO
https://www.kbpublisher.com/ru/kb/entry/442/