

SimpleOne

SimpleOne (<https://simpleone.ru/>) - ESM-платформа для автоматизации бизнеса.

Подключение SimpleOne к Blitz Identity Provider выполняется по протоколу SAML и состоит из двух этапов:

- Этап 1. Настройки на стороне SimpleOne
- Этап 2. Настройки на стороне Blitz Identity Provider

Важно:

В инструкции для примера указано, что SimpleOne расположен на домене `https://company.simpleone.ru`, а Blitz IDP установлен на домене `https://login.company.com`. Уточните ваши адреса перед применением инструкции.

Этап 1. Настройки на стороне SimpleOne

Выполните следующие действия:

1. **Войдите** в SimpleOne под учетной записью администратора и **Перейдите** в раздел **Настройка SAML2**.
2. Заполните поля с обязательными параметрами:
 - **Имя:** укажите любое название. Например, `simple-dev-saml`.
 - **Колонка пользователя:** выберите `Электронная почта`.
 - Установите флажок рядом с `Активно`.
 - **Метаданные сервера SAML:** укажите URL `https://login.company.com/blitz/saml/profile/Metadata/SAML`.

Настройка SAML2 172355477997865574

Имя
simple-dev-saml

* Колонка пользователя
Электронная почта

Поле запроса

☒ Активно

* Метаданные сервера SAML Дополнительные сведения

* URL метаданных
 https:// /blitz/saml/profile/Metadata/SAML

Этап 2. Настройки на стороне Blitz Identity Provider

В консоли управления Blitz Identity Provider перейдите в раздел **SAML** и выполните следующие действия:

1. Нажмите **Добавить новый SAML-атрибут**.
2. Укажите название атрибута и его источник в хранилище. В данном случае источник `mail`. Выберите его из выпадающего списка.
3. После заполнения свойств атрибута нажмите **Добавить**.

Свойства SAML-атрибута

Название

Источник

Добавить Отмена

[+ Добавить новый SAML-атрибут](#)

4. Далее добавьте кодировщик для атрибута. Для этого выберите атрибут и нажмите **Добавить кодировщик**.
5. Для атрибута добавьте кодировщики `SAML2StringNameID` и `SAML2String`. Присвойте кодировщику название `EmailAddress`.
6. Нажмите **Сохранить** после каждого создания кодировщика.
7. Далее в консоли управления *Blitz Identity Provider* перейдите в раздел **Приложения**.

8. Создайте новое приложение, задав его базовые настройки:

- **Идентификатор (entityID или client_id):**
- **Название:** укажите название приложения, которое видно только внутри Blitz. Например, .
- **Домен:**

Новое приложение

Идентификатор (entityID или client_id)

Идентификатор приложения. Используется для идентификации приложения при доступе по протоколу SAML (соответствует entityID) и OAuth 2.0 (соответствует client_id).

Название


Отображаемое пользователям имя приложения. Используется только внутри Blitz Identity Provider.

Домен

Отмена

Сохранить

9. Нажмите **Сохранить**.

10. Далее нажмите кнопку **Параметры**  у предложения SimpleOne и отредактируйте параметры приложения:

- **Протоколы:** выберите и нажмите **Сконфигурировать**
- Выберите **SAML 2.0 Web SSO Profile** и нажмите **Сконфигурировать**. Установите следующие настройки:
 - **Подписывать утверждения:**
 - **Шифровать утверждения:**
 - **Шифровать идентификаторы (NameIDs):**
 - **Включить передачу SAML-утверждений о пользователе в специальном блоке AttributeStatement:** установить флажок.

SAML профиль

SAML 2.0 Web SSO Profile

WS-Federation Passive Requestor Profile

Подписывать
утверждения

never

Правило подписи SAML-утверждений (Sign assertions)

Шифровать
утверждения

never

Правило шифрования SAML-утверждений (Encrypt assertions)

Шифровать
идентификаторы
(Namelds)

never

Правило шифрования идентификаторов (Encrypt Namelds)

☒ Включить передачу SAML-утверждений о пользователе в специальном блоке
Attribute Statement

11. В разделе **Атрибуты пользователя** настройте передачу в SimpleOne атрибута `transientId`, а также созданного на первом этапе SAML-атрибута.
12. Нажмите **Сохранить**.
13. Далее в разделе **Метаданные** нажмите **Изменить**. Скопируйте и вставьте следующий код:

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    entityID="https://company.simpleone.ru">
  <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">

    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
      Location="https://company.simpleone.ru/login"/>

    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress</md:NameIDFormat>

    <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="https://company.simpleone.ru/v1/saml/post" index="0"
isDefault="true"/>
  </md:SPSSODescriptor>
</md:EntityDescriptor>
```

14. Нажмите **Сохранить**.

Совет:

После прохождения всех шагов рекомендуем проверить корректность входа в SimpleOne:
<https://company.simpleone.ru>

Версия #7

Admin создал 11 сентября 2024 09:54:27

Admin обновил 27 ноября 2024 11:01:16