

Содержание

- О Blitz IDP** 3
- Установка и настройка Blitz IDP** 4
 - Общая инструкция по установке 4
 - Настройки интеграции на стороне Blitz IDP 4
- Настройки в ADVANTA** 5
- Результат интеграции** 7
 - Вход в систему 7
 - Портлет в настройках пользователя 8

Интеграция ADVANTA с Blitz Identity Provider

Сервер аутентификации [Blitz Identity Provider](#) - это российское ПО для управления входом пользователей в приложения, позволяющее оснастить веб-сайты и мобильные приложения компании функциями защиты учетных записей пользователей. Благодаря интеграции возможно осуществлять авторизацию в Систему ADVANTA через сервер аутентификации по протоколу OpenIdConnect.

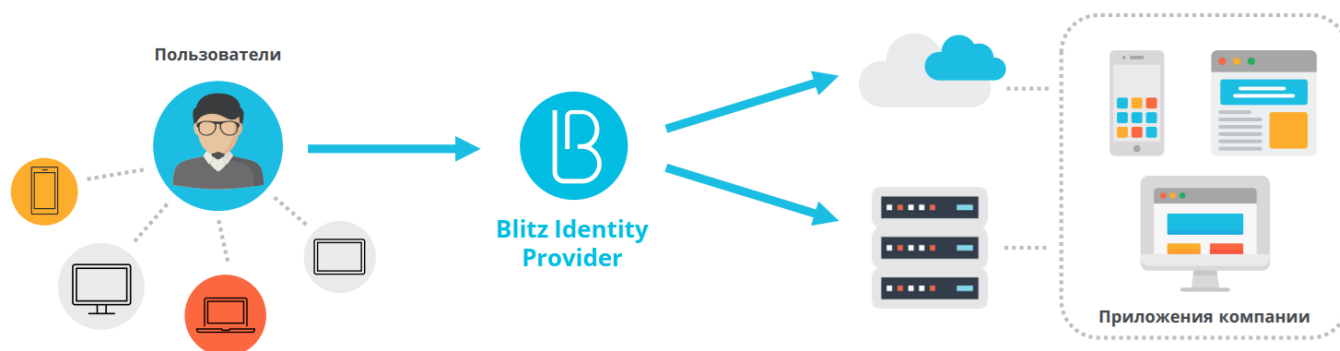
Подключение Системы ADVANTA к Blitz IDP выполняется по протоколу **OpenIdConnect** и состоит из двух этапов:

1. Настройки на стороне [Blitz Identity Provider](#).
2. Настройки на стороне Системы ADVANTA.

Для реализации интеграции у вас должен быть доступ по крайней мере к демо-версиям данных продуктов.

О Blitz IDP

[Blitz Identity Provider](#) - платформа создания единого сервиса доступа в организации. Единый сервис доступа обеспечивает идентификацию, аутентификацию и контроль доступа пользователей к приложениям организации.



Продукт разворачивается на серверах организации и позволяет оснастить внутреннюю ИТ-инфраструктуру функциями защиты учетных записей пользователей. Blitz IDP поддерживает современные протоколы аутентификации, популярные отечественные операционные системы и СУБД.

Основные функции Blitz IDP:

- обеспечение единого сквозного входа пользователя в приложения (Single Sign-On);
- двухфакторная аутентификация;
- конфигурируемый пользовательский интерфейс страниц входа, регистрации, восстановления доступа, управления учетной записью;
- вход с использованием сторонних поставщиков идентификации: вход с помощью аккаунтов социальных сетей, банков, Единой системы идентификации и аутентификации

(ЕСИА, Госуслуги), Mos ID (СУДИР), федеративный вход пользователей с использованием внешних поставщиков идентификации;

- проверка прав доступа на вход пользователей в приложения;
- проверка прав доступа пользователей и приложений при использовании REST-сервисов;
- протоколирование событий доступа и действий с учетными записями.

Подробнее о сервере можно узнать из [документации](#) на сайте [Blitz IDP](#) или скачать [PDF-файлы](#).

Blitz IDP зарегистрирован в Едином реестре российского ПО (№842) и сертифицирован ФСТЭК России (№4525 от 10.03.2022), что подтверждает соответствие требованиям информационной безопасности и допускает применение продукта в государственных информационных системах.

Установка и настройка Blitz IDP

Общая инструкция по установке

Подробная информация об установке и настройке Blitz IDP в документации на сайте Blitz IDP на странице [Общая инструкция по установке](#).

В зависимости от используемой операционной системы есть своя специфика по установке необходимого окружения.

Также можно посмотреть [демоверсию](#) приложения.

Настройки интеграции на стороне Blitz IDP

Для настройки интеграции в консоли управления Blitz IDP перейдите в раздел «Приложения» и выполните действия:

1. Создайте новое приложение ADVANTA, задав его базовые настройки:

- идентификатор (entityID или client_id): <client_id>;
- название: <name>;
- домен.

2. Нажмите «Сохранить».

3. Далее нажмите кнопку «Параметры» у предложения ADVANTA и отредактируйте параметры приложения:

- протоколы: выберите **OAuth 2.0 / OpenIdConnect** и нажмите «Сконфигурировать»;
- далее в параметрах укажите данные, как в конфигурационном файле client.config: секрет (client_secret), префиксы ссылок возврата, допустимые разрешения: profile.

4. Нажмите «Сохранить».

После прохождения всех шагов рекомендуем проверить корректность входа в ADVANTA.

Более подробную информацию о настройках интеграции можно найти в документации на сайте Blitz IDP в разделе [Интеграция](#).

Настройки в ADVANTA

Настройка авторизации через Open ID Connect производится Администратором системы.

В настройках конфигурационного файла системы `client.config`, начиная с версии системы 3.29, появился раздел, в котором в виде массива можно указать перечень внешних сервисов аутентификации по протоколу **OpenIdConnect**:

```
/* Массив */

...
<openIdConnect>
  <providers>
    <add caption="Имя кнопки входа с названием провайдера" clientId="advanta"
metadataURL="https://ssotest.yourcompany.ru/.well-known/openid-configuration"
    authenticationType="OIDC1" enabled="true" scope="openid profile"
    clientSecret="Секретный код провайдера" responseType="code"
claimType="user_id" />
    <add ... /> /* Описание второго провайдера */
  </providers>
</openIdConnect>
...
```

Параметр	Описание
caption	Обязательный параметр Название провайдера авторизации для отображения кнопки с этим именем
metadataURL	Обязательный параметр URL-адрес удаленного сервера с метаданными
authenticationType	Обязательный параметр Идентификатор провайдера авторизации, под этим именем данный провайдер OpenIdConnect будет отображаться в профиле пользователя, а также использоваться в API методах. Можно использовать любой удобный
clientId	Обязательный параметр Идентификатор клиента (приложения), выбирается согласно правилам именования сервисов для аутентификации в OpenIdConnect

Параметр	Описание
enabled	Обязательный параметр Включение/отключение провайдера, возможные значения: true и false
scope	Указываются запрашиваемые скоупы. Если параметр не задан, то используется только скоуп openid Может быть несколько
clientSecret	Обязательный параметр Указывается секрет приложения
responseType	Необязательный параметр. Тип ответа, по умолчанию id_token. Возможные значения: code, code id_token, code id_token token, code token, id_token, id_token token, token
claimType	Тип утверждения, используемый для получения идентификатора пользователя на сервере авторизации. Будет использоваться для связки пользователя системы с пользователем OpenIdConnect
disableSignatureValidation	Необязательный параметр Отключает валидацию токена. Если параметр не задан, то значение false и валидация включена
jwtFilePath	Опциональный параметр Файл, который содержит ключи валидации в формате JSON. Формат аналогичен странице jwks_uri. Если параметр не задан, то ключи берутся только с адреса jwks_uri Можно использовать, если по какой-то причине провайдер OpenIdConnect не предоставляет ключи валидации Пример использования: jwtFilePath = "C:\inetpub\wwwroot\a2key\jwksFile.txt"

В client.config также необходимо добавить индикацию, что необходимо использовать интеграцию с **OpenIdConnect**. Для этого опционально в разделе <configSections> предусмотреть размещение секции "<section name="openIdConnect" type="Config.OpenIdConnectConfigurationSection,smcorelib"/>". При отсутствии данной секции, использование **OpenIdConnect** невозможно.

Пример настройки конфигурационного файла системы client.config для авторизации через провайдера [Blitz IDP](#):

```
...
<configSections>
  ...
  <section name="openIdConnect"
type="Config.OpenIdConnectConfigurationSection, smcorelib"/>
```

```
</configSections>

...

<openIdConnect>
  <providers>
    <add caption="Blitz IDP" clientId="Advanta"
metadataURL="https://blitz.domain.ru/blitz/oauth/.well-known/openid-configuration"
authenticationType="blitz" enabled="true" scope="openid"
clientSecret="00000000"
responseType="code" claimType="user_id" />

    <add caption="SSO" clientId="a2nta"
metadataURL="https://blitz.domain2.ru/blitz/oauth/.well-known/11"
authenticationType="blitz2" enabled="true" scope="profile"
clientSecret="11111111"
responseType="code" claimType="user_id" />
  ...
</providers>
</openIdConnect>

...
```

При отключении провайдера (параметр `enabled`), кнопки авторизации не будет, но привязка пользователей в системе сохранится. Чтобы удалить связи с сервисами авторизации, необходимо:

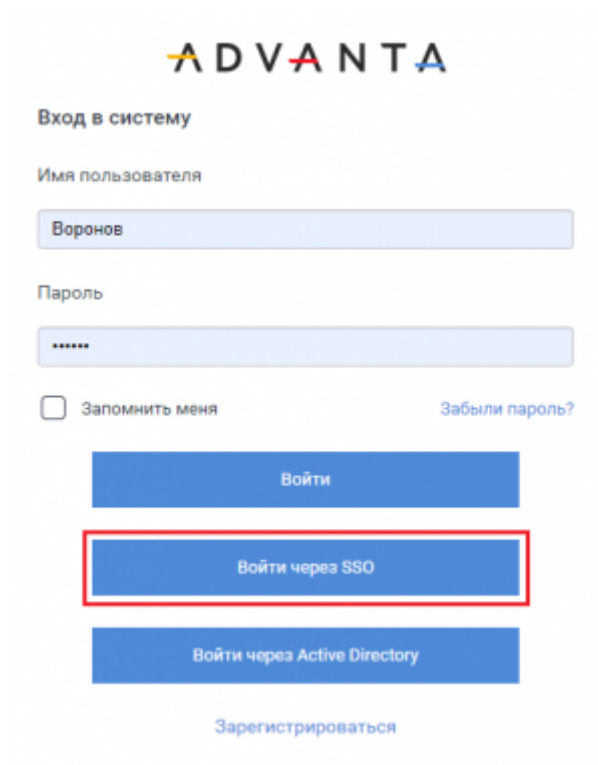
- в [портлете с сервисами авторизации](#) в настройках пользователя удалить привязку к сервису;
- использовать метод API [DeleteLinksWithOpenIdConnect](#). Подробнее о методах API на странице [Описание методов API](#).

Результат интеграции

Вход в систему

После корректных настроек конфигурационного файла и перезапуска системы, пользователю будет доступен вход в систему через новый провайдер аутентификации.

Например, пользователь, нажимая на кнопку «Войти через SSO», перенаправляется на адрес провайдера авторизации Blitz IDP, указанный в настройках файла `client.config`. После успешного прохождения авторизации у провайдера **OpenIdConnect**, запрос будет перенаправлен обратно в систему ADVANTA. Система ADVANTA производит идентификацию пользователя и, в случае успешной идентификации, авторизует пользователя в системе.



Подробную информацию о входе в систему через провайдера аутентификации можно прочесть на странице [Авторизация по протоколу Open ID Connect](#).

Портлет в настройках пользователя

После настройки интеграции с Blitz IDP в профиле пользователя также появится [раздел](#) для связывания учетной записи системы ADVANTA с учетной записью внешнего провайдера. Портлет находится в настройках пользователя, после портлета «Мои настройки».

В портлете указана информация:

- название - название провайдера **OpenIdConnect** (соответствует authenticationType в конфигурационном файле);
- заголовок - заголовок провайдера **OpenIdConnect** (соответствует caption в конфигурационном файле), название кнопки на странице входа;
- учетная запись - учетная запись данного пользователя у провайдера **OpenIdConnect**;
- столбец с кнопкой «Изменить» - нажимая на нее, открывается возможность редактирования соответствующей строки.

Запрещать авторизацию пользователя под локальной учетной записью	☐
Имя пользователя*	admin
изменить пароль	
Использовать ЭП в согласованиях	☐
Отправлять запросы на E-mail	Никогда
Отправлять события на E-mail	Никогда
Дублировать на дополнительный E-mail	Нет
Добавлять в таблицу начатые и завершенные мною задачи	Да
Добавлять в таблицу начатые и завершенные задачи, если я ресурс	Да
Сделать стартовой панель управления	Нет
Язык	RU

Учетные записи провайдеров openIdConnect

Название	Заголовок	Учетная запись	
authenticationType2	войти через провайдера caption2	sdfs	изменить
authenticationType1	войти через провайдера caption1	efremov	изменить
authenticationType3	войти через провайдера caption3		изменить

При нажатии кнопки «Изменить» в столбце «Учетная запись» появляется возможность ввести данные учетной записи данного пользователя у провайдера **OpenIdConnect**. Для сохранения данных необходимо нажать кнопку «Сохранить».

Сделать стартовой панель управления	☐
Доступ к редактированию профиля	☒
Язык	RU

Учетные записи провайдеров openIdConnect

Название	Заголовок	Учетная запись	
blitz	Войти через SSO	Ефремов	Сохранить Отмена
1	Войти через Active Directory		изменить

После того, как создана привязка и указана корректная информация учетной записи пользователя у провайдера **OpenIdConnect**, у пользователя появляется возможность входа в систему ADVANTA через Blitz IDP. Более подробную информацию можно прочесть на странице [Настройка авторизации через Open ID Connect](#).

Last
update:
12.09.2024 06:57 product:api:integration_examples:blitz-idp https://wiki.a2nta.ru/doku.php/product/api/integration_examples/blitz-idp?rev=1726124278

From:
<https://wiki.a2nta.ru/> - Wiki [3.x]

Permanent link:
https://wiki.a2nta.ru/doku.php/product/api/integration_examples/blitz-idp?rev=1726124278

Last update: **12.09.2024 06:57**

