

Содержание

| | |
|---|---|
| Настройка конфигурационного файла | 3 |
| Вход в систему | 4 |
| Настройка связки учетных записей | 5 |
| Пример настройки авторизации через Open ID Connect | 7 |

Настройка авторизации через Open ID Connect

Настройка конфигурационного файла

Начиная с версии системы 3.29 в настройках конфигурационного файла системы `client.config` появился раздел, в котором в виде массива можно указать перечень внешних сервисов аутентификации по протоколу **OAuth 2.0 / OpenIdConnect**.

Перечень провайдеров авторизации через **OpenIdConnect** задается в файле `client.config` в разделе `<openIdConnect>`:

```

/* Массив */

...
<openIdConnect>
  <providers>
    <add caption="Имя кнопки входа с названием провайдера" clientId="advanta"
metadataURL="https://sso.test.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 | Название провайдера авторизации на странице входа в систему |
| metadataURL | URL-адрес удаленного сервера с метаданными |
| authenticationType | Идентификатор провайдера авторизации |
| clientId | Идентификатор клиента (приложения), выбирается согласно правилам именования сервисов для аутентификации в OpenIdConnect |
| enabled | Включение/отключение провайдера, возможные значения: true и false |
| scope | Запрашиваемые скоупы. Если параметр не задан, то используется только скоуп openid |
| clientSecret | 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 |
| disableSignatureValidation | Необязательный параметр, отключает валидацию токена. Если параметр не задан, то значение false и валидация включена |

| Параметр | Описание |
|--------------|---|
| jwks_uri | Стандарт под OpenIdConnect провайдера |
| jwksFilePath | 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 |

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.

Вход в систему

Настройка авторизации через **Open ID Connect** производится Администратором системы, в том числе привязка профилей пользователей ADVANTA к провайдерам авторизации.

После корректных настроек конфигурационного файла `client.config` и перезапуска системы, пользователю будет доступен вход в систему через нового провайдера аутентификации. На странице входа для каждого нового настроенного провайдера появится отдельная кнопка с названием из настроек конфигурационного файла.

ADVANTA

Вход в систему

Имя пользователя

Воронов

Пароль

.....

Запомнить меня [Забыли пароль?](#)

Войти

Войти через SSO

Войти через Active Directory

[Зарегистрироваться](#)

Подробная информация о входе в систему через провайдера аутентификации на странице

Авторизация по протоколу Open ID Connect.

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](#).

Настройка связки учетных записей

После настройки в файле `client.config` сервисов авторизации, они станут отображаться в виде портлета в настройках пользователя, после портлета «Мои настройки». В данном портлете есть возможность указывать/удалять идентификатор сервиса авторизации (создавать/удалять привязку к сервису).

Также создать привязку пользователя к сервису авторизаций можно используя метод API [LinkUserToOpenIdConnect](#).

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 | sdfsfs | 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

| Учетные записи провайдеров openIdConnect | | | |
|--|------------------------------|--------------------------------------|--|
| Название | Заголовок | Учетная запись | |
| blitz | Войти через SSO | <input type="text" value="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 этого провайдера.

При удачном/неудачном входе пользователем в систему через **OpenIdConnect** Администратор может видеть соответствующие события в [Ленте событий](#).

Лог авторизаций


Все | Последние 10 | Все пользователи

| Время | Событие |
|---------------------|---|
| 20.03.2024 18:19:56 | Воронов Олег вошел(а) в систему через систему OpenIdConnect / Blitz IDP с удалённого адреса 178.205.55.188 |
| 20.03.2024 18:19:54 | Тестов тест вышел(а) из системы |
| 20.03.2024 18:19:18 | Тестов тест вошел(а) в систему с удалённого адреса 178.205.53.174 |
| 20.03.2024 18:19:10 | Воронов Олег вышел(а) из системы |
| 20.03.2024 18:18:17 | Воронов Олег вошел(а) в систему с удалённого адреса 178.205.53.174 |
| 20.03.2024 18:18:11 | Воронов Олег вышел(а) из системы |

Лента событий

Действия пользователей Настройка

[фильтр](#)

 Неудачная попытка входа через систему OpenIdConnect / Blitz IDP с удалённого адреса 178.205.55.188.

минуту назад

Пример настройки авторизации через Open ID Connect

В примере представлена настройка 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-configur  
ation"  
        authenticationType="blitz" enabled="true" scope="openid"  
clientSecret="00000000"  
        responseType="code" claimType="user_id" />  
    </providers>  
</openIdConnect>
```

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

Администратор может настроить авторизацию через любого провайдера
OpenIdConnect.

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

Permanent link:
https://wiki.a2nta.ru/doku.php/product/settings/system/open_id?rev=1724216778

Last update: **21.08.2024 05:06**

