Содержание

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://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	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

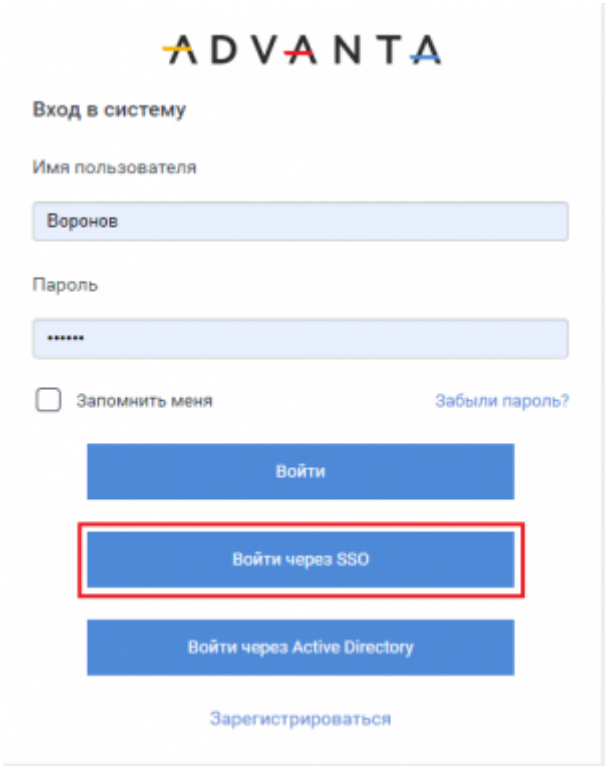
Параметр	Описание
jwks_uri	Стандарт под OpenIdConnect провайдера
jwksFilePath	Опциональный параметр. Файл, который содержит ключи валидации в формате JSON. Формат аналогичен странице `jwks_uri`. Если параметр не задан, то ключи берутся только с адреса `jwks_uri`. Можно использовать, если по какой-то 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.



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.

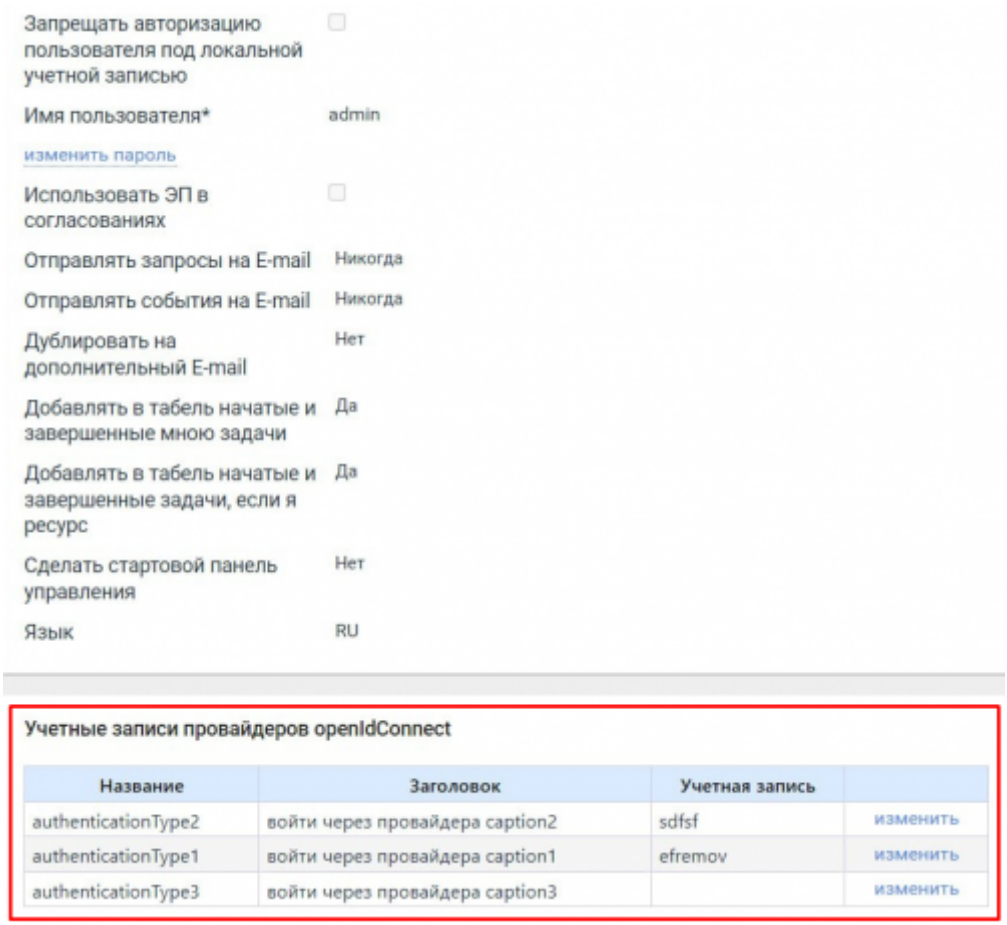
Настройка связки учетных записей

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).

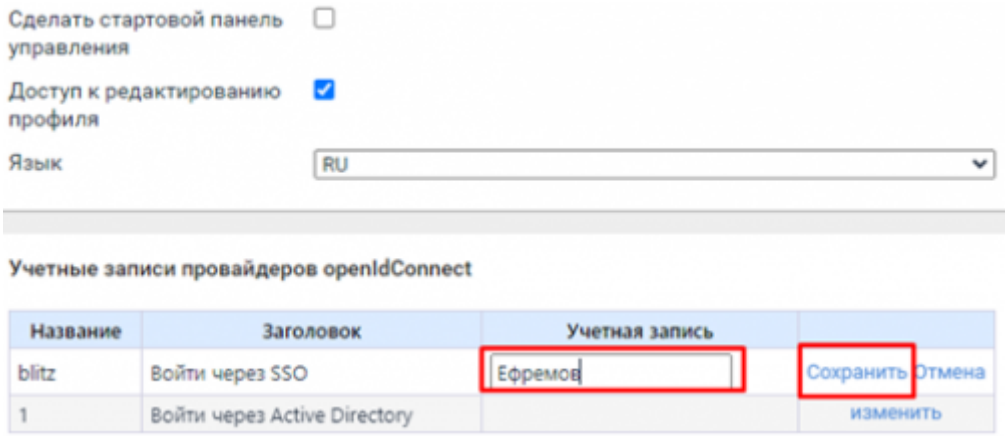
Также создать привязку пользователя к сервису авторизаций можно используя метод API LinkUserToOpenIdConnect .

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.



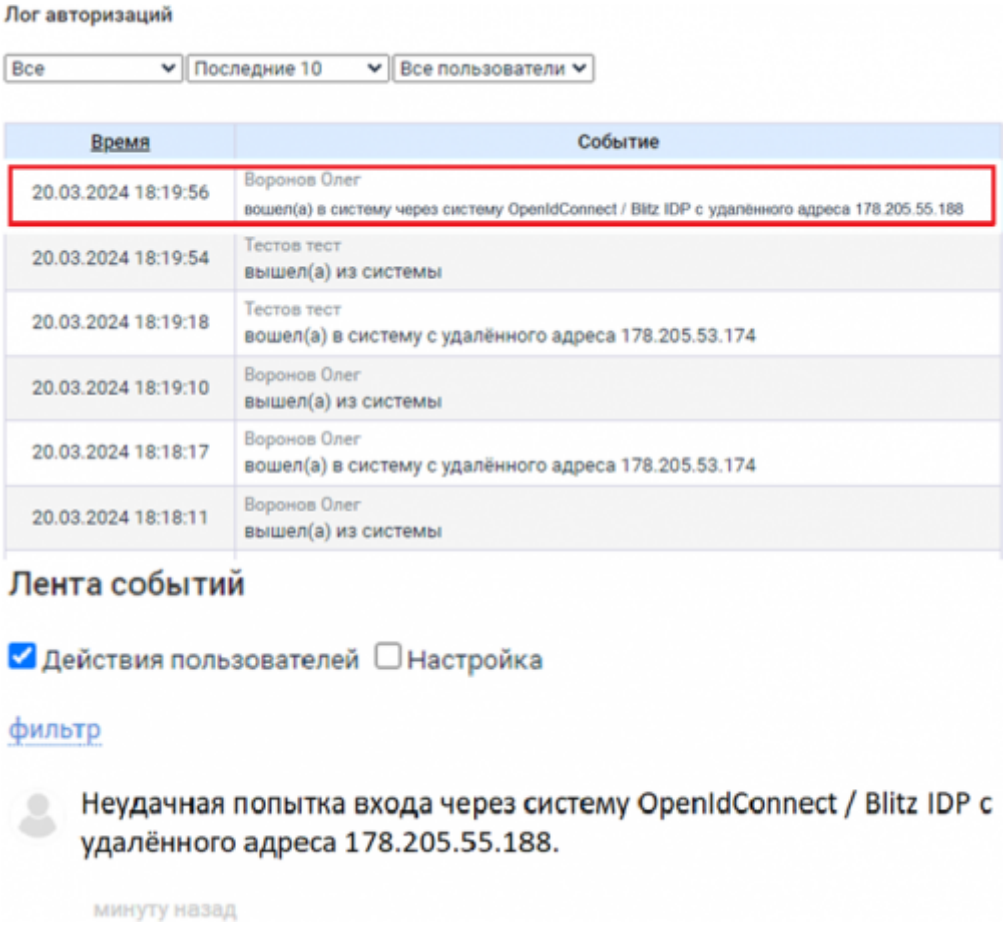
При нажатии кнопки «Изменить» в столбце «Учетная запись» появляется возможность ввести данные учетной записи данного пользователя у провайдера **OpenIdConnect**. Для сохранения данных необходимо нажать кнопку «Сохранить».



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.

Логирование событий входа

При удачном/неудачном входе пользователем в систему через **OpenIdConnect** Администратор может видеть соответствующие события в Ленте событий.



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" />
```

```
      <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>

...


<appSettings>
  <add key="AllowedExternalApplicationClientIds" value="1;2"/>
  ...
</appSettings>

...
```

Администратор может настроить авторизацию через любого провайдера **OpenIdConnect**.