

Как настроить интеграцию с Blitz

Инструкция для администраторов

Оглавление

Что такое Blitz IDP?	3
Шаг 1. Добавьте приложение и настройте протокол OAuth 2.0 в Blitz	3
Шаг 2. Добавьте поставщика идентификации в Blitz	6
Шаг 3. Выполните настройку в установщике Диска VK Workspace	7

Что такое Blitz IDP?

Сервер аутентификации Blitz Identity Provider — это программное обеспечение для управления входом пользователей в приложения. Основные функции Blitz:

- Обеспечение единого сквозного входа пользователя в приложения (Single Sign-On).
- Конфигурируемый пользовательский интерфейс страниц входа, регистрации, восстановления доступа, управления учетной записью.
- 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.

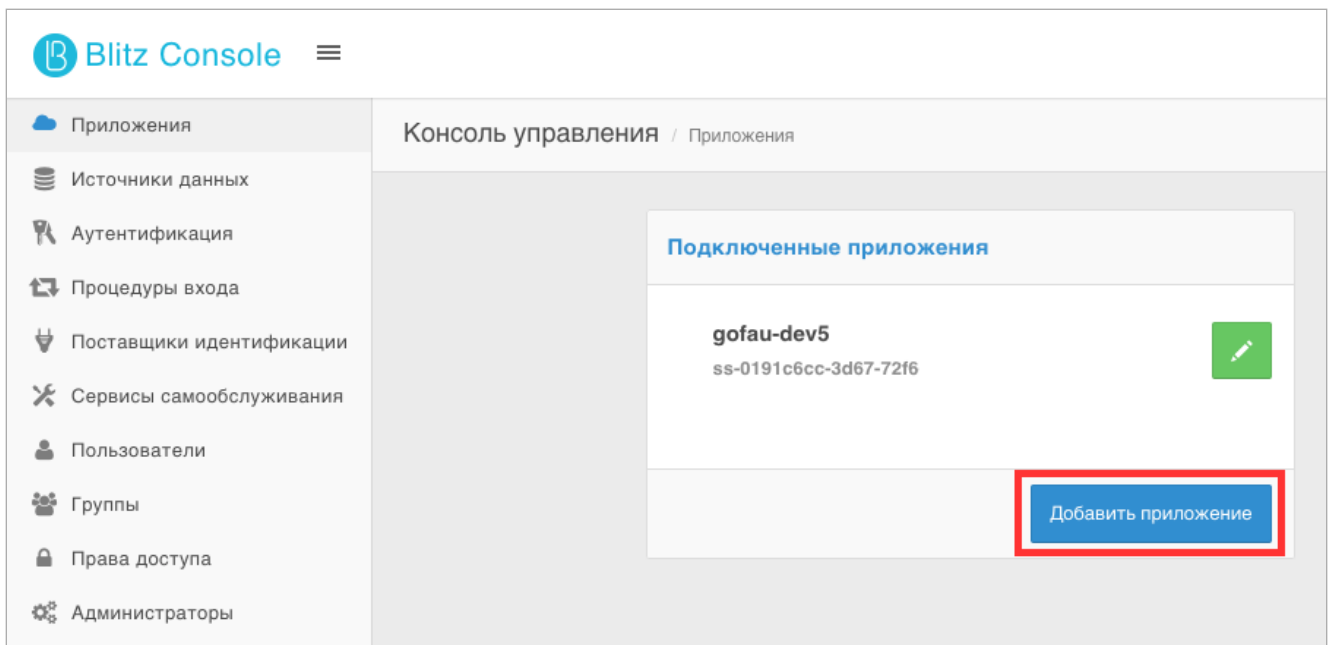
Шаг 1. Добавьте приложение и настройте протокол OAuth 2.0 в Blitz

Внимание

Перед настройкой интеграции с Диском обязательно настройте **Источники данных** в Blitz. В разделе **Пользователи** веб-интерфейса Blitz при поиске должны отображаться пользователи, которые синхронизируются из Active Directory.

Добавьте и настройте приложение:

1. Авторизуйтесь в панели администратора Blitz.
2. В левом меню перейдите в раздел **Приложения**.
3. Нажмите **Добавить приложение**.



4. Придумайте **Название** и **Идентификатор**, который будет использоваться при работе с IDP Blitz.
5. В поле **Домен** нужно указать **Домен для веб-интерфейса авторизации** из веб-интерфейса установщика. Перейдите в раздел **Настройки** → **Доменные имена** → **Настройки доменных имен**. Веб-интерфейс установщика находится по адресу `http://deployer-address:8888`.

The image shows the 'Параметры приложения' (Application Parameters) form. It contains three main input fields:

- Идентификатор (entityID или client_id)**: Value is 'ss-0191c6cc-3d67-72f6'. Description: 'Идентификатор приложения. Используется для идентификации приложения при доступе по протоколу SAML (соответствует entityID) и OAuth 2.0 (соответствует client_id).'
- Название**: Value is 'gofau-dev5'. Description: 'Отображаемое пользователям имя приложения. Используется только внутри Blitz Identity Provider'
- Домен**: Value is 'http://account.ws.dev5.on-premise.ru/login'. Description: 'Ссылка на стартовую страницу приложения, например, http://testdomain.ru/. При TLS-аутентификации приложения проверяется, что в сертификате приложения указан именно этот домен'

6. Нажмите кнопку **Сохранить**

Настройте протокол OAuth 2.0 на той же странице:

1. Придумайте и заполните поле **Секрет**. Его затем надо будет указать в веб-интерфейсе установщика.
2. В поле **Предопределенная ссылка возврата** укажите значение в следующей форме: `<Домен для доменной авторизации (внутренних запросов браузера)>/api/v1/oauth2/sso/callback`. Чтобы получить **Домен для доменной авторизации**, в веб-интерфейсе установщика перейдите в раздел **Настройки** → **Доменные имена** → **Настройки доменных имен**.
3. В **Префиксы ссылок возврата** укажите URL из поля **Предопределенная ссылка возврата**.
4. В поля **Допустимые разрешения** и **Разрешения по умолчанию** укажите следующие разрешения: `openid, profile, email`.

Примечание

Описание разрешений находится в файле конфигурации `gofau.yaml` сервиса `gofau`, блок `oauth2.sso.scopes`.

Настройки взаимодействия с приложением

Секрет (`client_secret`)

.....



Секретный ключ подключаемого приложения (`client_secret`). Если указан, то именно этот секрет должен использоваться подключенным приложением при обращении к Blitz Identity Provider

Дополнительный секрет (`client_secret`)

Укажите дополнительный секрет для аутентификации приложения



Дополнительный секретный ключ подключаемого приложения (`client_secret`). Если указан, то может использоваться в качестве альтернативы к основному секрету

Предопределенная ссылка возврата (`redirect_uri`)

`https://auth.ws.dev5.on-premise.ru/api/v1/oauth2/sso/callback`

URL, на который по умолчанию будет переадресован пользователь после прохождения авторизации (`redirect_uri`)

Префиксы ссылок возврата

`https://auth.ws.dev5.on-premise.ru/api/v1/oauth2/sso/callback` x

Для добавления нового префикса введите его и нажмите Enter

Префикс используется для проверки ссылок возврата (`redirect_uri`). Если в запросе на аутентификацию указана ссылка возврата и она не соответствует ни одному из указанных префиксов, то в аутентификации будет отказано

Допустимые разрешения

x openid x profile x email

Разрешения (`scope`), которые будут доступны приложению.

Разрешения по умолчанию

x email x openid x profile

Разрешения (`scope`), которые будут по умолчанию выданы приложению после авторизации. Если значения по умолчанию не указаны, то в запросе необходимо явно прописать требуемые разрешения.

5. В поле **Допустимые grant type** укажите значения: `authorization_code` и `refresh_token`.
6. В поле **Допустимые response type** укажите значение: `code`.
7. В поле **Режим выдачи маркеров доступа по умолчанию** выберите значение: `offline`.

Допустимые grant type	<input type="checkbox"/> authorization_code <input type="checkbox"/> refresh_token
	Список grant type, которые будут доступны приложению. При пустом списке доступны все grant type
Допустимые response type	<input type="checkbox"/> code
	Список response type, которые будут доступны экземпляру приложения при обращении к URL авторизации (authorization endpoint). При пустом списке доступны все response type.
	<input type="checkbox"/> Добавлять в маркер доступа параметр rights с правами пользователя на данное приложение
Время жизни маркера доступа (access_token)	<input type="text"/>
	Задается количество секунд, через которое код доступа станет недействительным. Если не задан, то берется из общих настроек.
Режим выдачи маркеров доступа по умолчанию	<input type="text" value="offline"/>
	Режим выдачи маркеров доступа (access_token), если явно не указан в запросе. При online-режиме не выдается маркер обновления (refresh_token)

8. Нажмите кнопку **Сохранить**.

Шаг 2. Добавьте поставщика идентификации в Blitz

1. В левом меню перейдите в раздел **Поставщики идентификации**.
2. В списке поставщиков выберите **Blitz Identity Provider**.
3. Придумайте и задайте значения полей **Идентификатор поставщика** и **Название поставщика**.
4. Замените слово `DOMAIN` на ваш домен в значении следующих полей:
 - URL для авторизации.
 - URL для получения и обновления маркера.
 - URL для получения данных.
5. В поле **Запрашиваемые разрешения** укажите значения: openid, profile, email.

Безопасность

Для заполнения указанных параметров обратитесь к администратору внешнего поставщика идентификации Blitz Identity Provider. Необходимая подключаемого приложения (по протоколу OAuth 2.0). Также передайте администратору приведенные ниже URI перенаправления.

Предопределенные ссылки возврата (redirect_uri) `https://blitz.devel.vkwm.ru/blitz/login/externaldps/callback/blitz/blitz_1/false`
`https://blitz.devel.vkwm.ru/blitz/profile/social/externaldps/callbackPopup/blitz/blitz_1`

Эти ссылки должны быть прописаны в настройках поставщика идентификации для корректной обработки результатов аутентификации пользователя. Используйте схему `https`, если вы используете защищенное соединение.

URL для авторизации

URL для получения и обновления маркера

Запоминать маркеры

URL для получения данных

Идентификатор (client_id)

Секрет (client_secret) [Изменить значение](#)

Разрешения


Запрашиваемые разрешения

openid x profile x email x

Для добавления разрешения введите его имя и нажмите Enter

Укажите перечень разрешений (scope), которые должны быть получены при обращении к поставщику идентификации. Обратитесь к администратору внешнего поставщика идентификации

Шаг 3. Выполните настройку в установщике Диска VK Workspace

1. Откройте веб-интерфейс установщика `http://server-address:8888`.
2. Нажмите на кнопку  в правом верхнем углу, выберите пункт **Продукты**.
3. Включите компоненты **Интеграция с Kerberos (SSO-авторизация)** и **Внешняя web-авторизация через провайдера blitz**.

Интеграция с Kerberos (SSO-авторизация)

Keycloak внутри инсталляции v17.0.1

1 GB RAM, 1 vCPU

Интеграция с внешним Keycloak сервером

Внешняя web-авторизация через провайдера blitz

4. Нажмите на кнопку **Сохранить**.

5. Перейдите на вкладку **Настройки** → **Настройки компонентов** → **Авторизация**.

6. Нажмите кнопку редактирования .

7. Заполните поля:

- OAuth секрет клиента (Blitz) — значение поля **Секрет при настройке протокола** в панели администратора Blitz.
- OAuth id клиента авторизации (Blitz) — значение поля **Идентификатор при добавлении приложения** в панели администратора Blitz.
- Поля с URL нужно взять с шага [по добавлению поставщика идентификации](#).

OAuth секрет клиента (Blitz):
OAuth id клиента авторизации (Blitz):	ss-0191c6cc-3d67-72f6
URL для авторизации (Blitz):	https://blitz.domain.ru/blitz/oauth/ae
URL для получения и обновления маркера/токена (Blitz):	https://blitz.domain.ru/blitz/oauth/te
URL для получения данных о пользователе через провайдер (Blitz):	https://blitz.domain.ru/blitz/oauth/me
Список доменов для web-авторизации по oauth2	ad2013.on-premise.ru exch.on-premise.ru new.domain.ru

8. Добавьте домены, которые вы хотите авторизовывать через IDP Blitz.

9. Нажмите на кнопку **Сохранить**.

10. Найдите контейнер **swadb** и выполните шаг **add_sso_domains**.

11. Перейдите к списку контейнеров и выполните шаг **up_container** для контейнера **gofau**.

12. После настройки перейдите на страницу авторизации в Диске и введите свою почту, должен сработать редирект на IDP. Авторизуйтесь на странице IDP Blitz.

Если авторизация не прошла, проверьте, что домен добавлен в базу данных:

```
docker exec -it swadb1 mysql
use swa;
select * from sso_clients;
```

Примечание

Если редирект не сработал, то вероятнее всего gofau не успел увидеть изменения в БД. Перезапустите контейнер или снизьте интервал получения данных через переменную окружения gofau

`OAuth_SSO_CLIENTS_FETCHER_PULL_INTERVAL='5s'` и выполните шаг `up_container`.

🕒 27 апреля 2026 г.