Как настроить интеграцию с Blitz

Инструкция для администраторов

Портал с документацией: https://biz.mail.ru/docs/on-premises/

Оглавление

Что такое Blitz IDP?

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

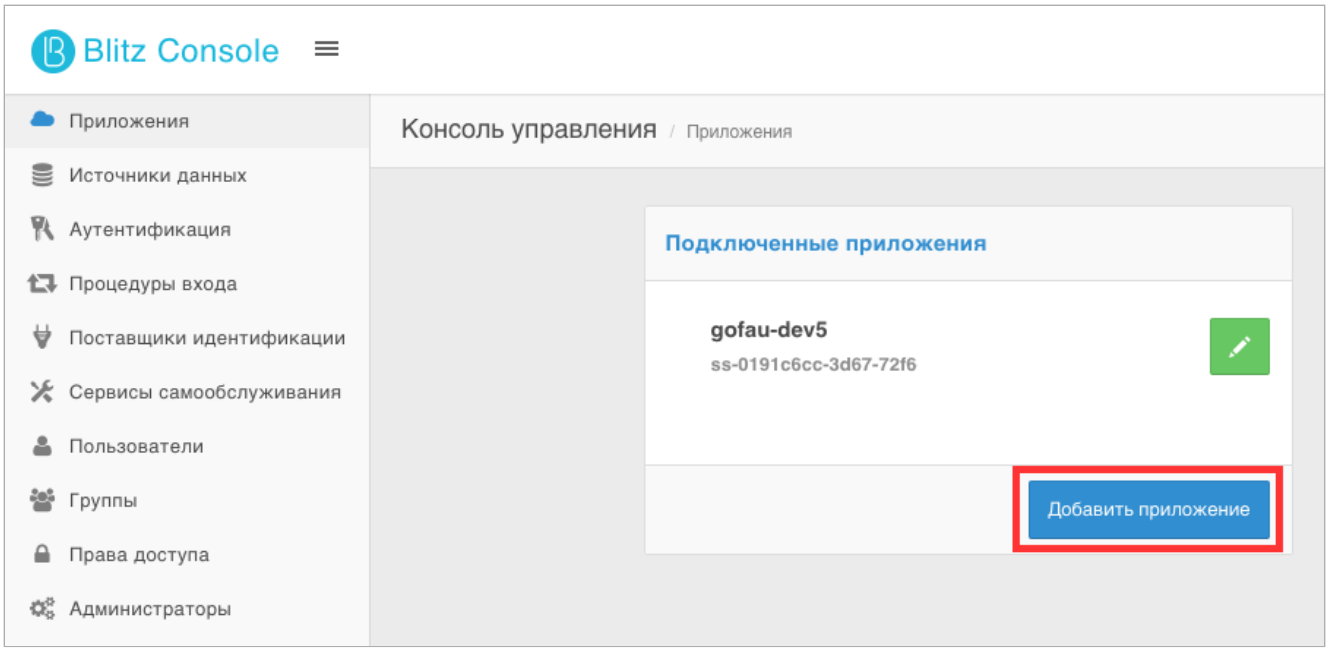
- Обеспечение единого сквозного входа пользователя в приложения (Single Sign-On).
- Конфигурируемый пользовательский интерфейс страниц входа, регистрации, восстановления доступа, управления учетной записью.
- Проверка прав доступа на вход пользователей в приложения.
- Проверка прав доступа пользователей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

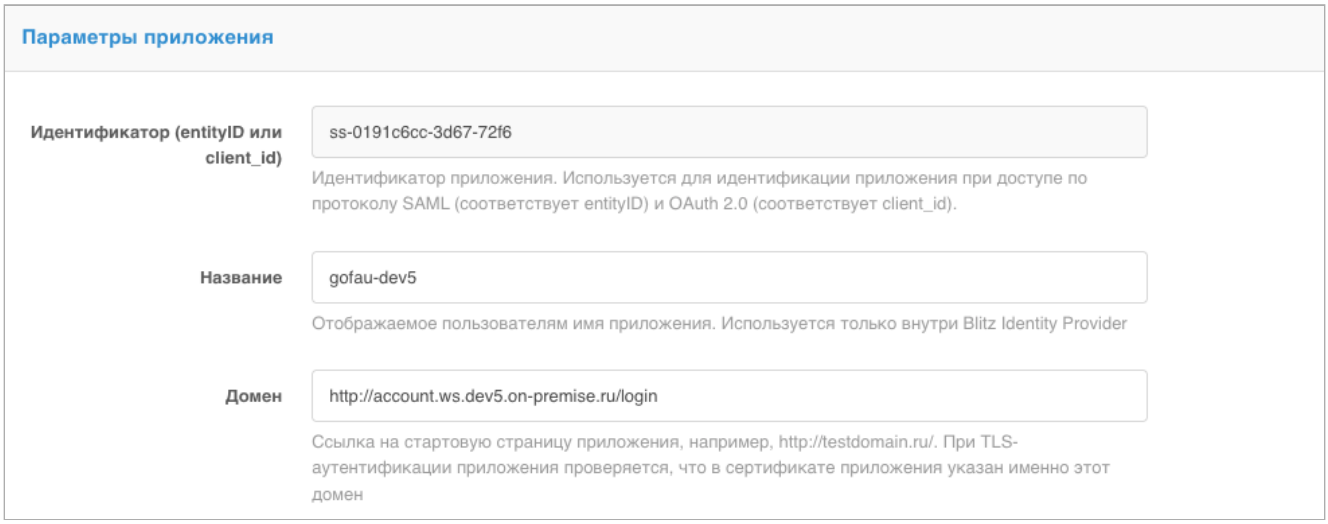
> **Внимание**
>
> Перед настройкой интеграции с Почтой обязательно настройте **Источники данных** в Blitz. В разделе **Пользователи** веб-интерфейса Blitz при поиске должны отображаться пользователи, которые синхронизируются из Active Directory.

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`.

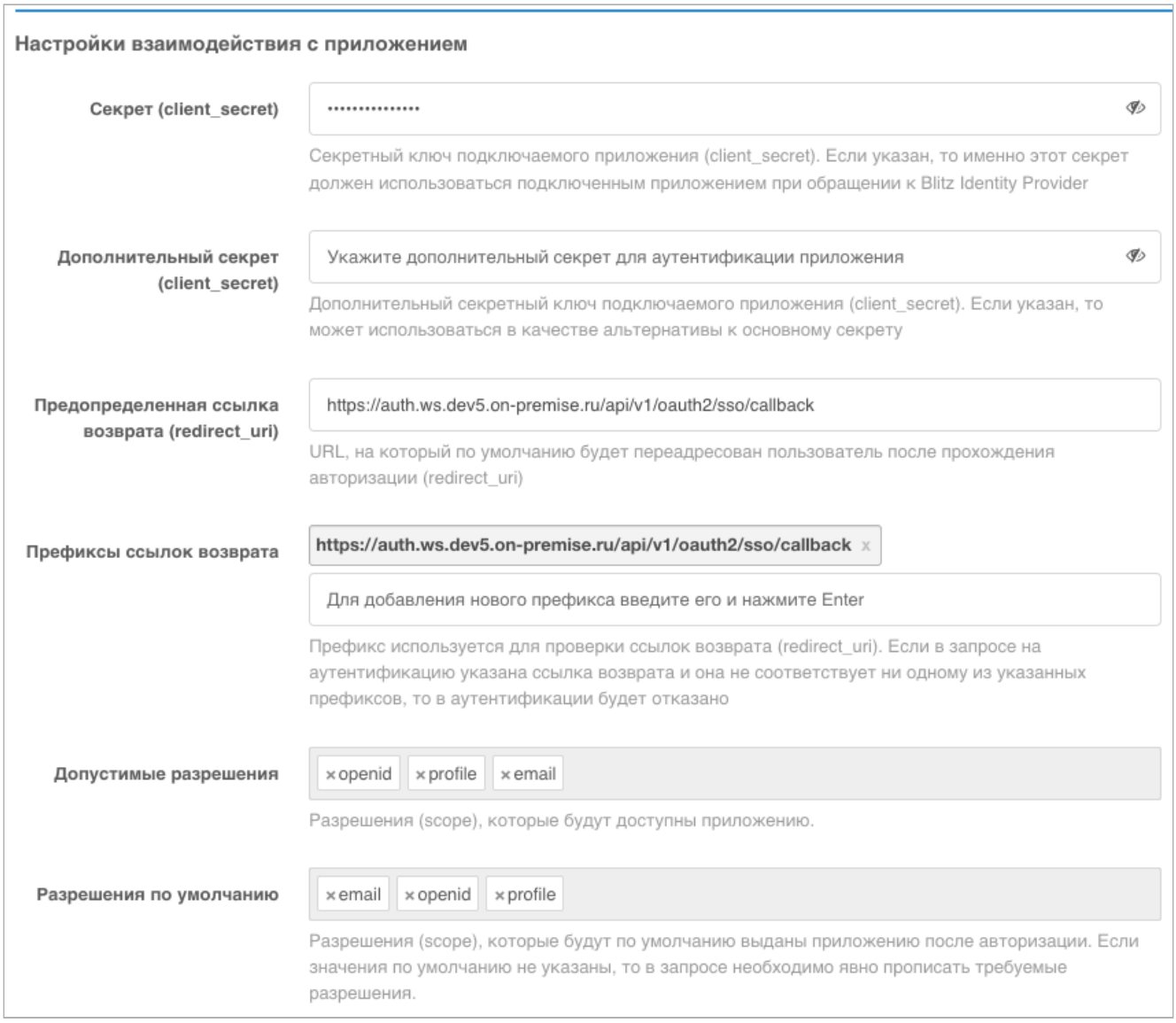


6. Нажмите кнопку **Сохранить**

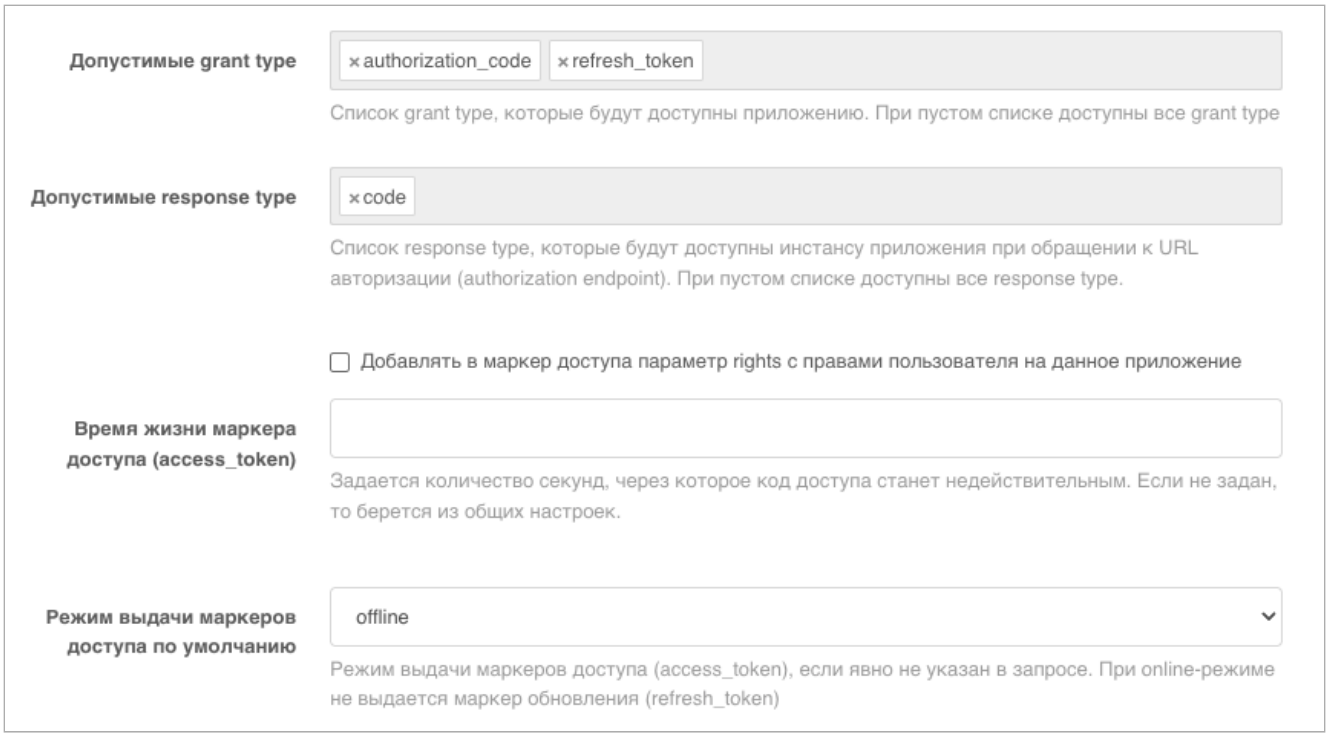
Настройте протокол OAuth 2.0 на той же странице:

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`.



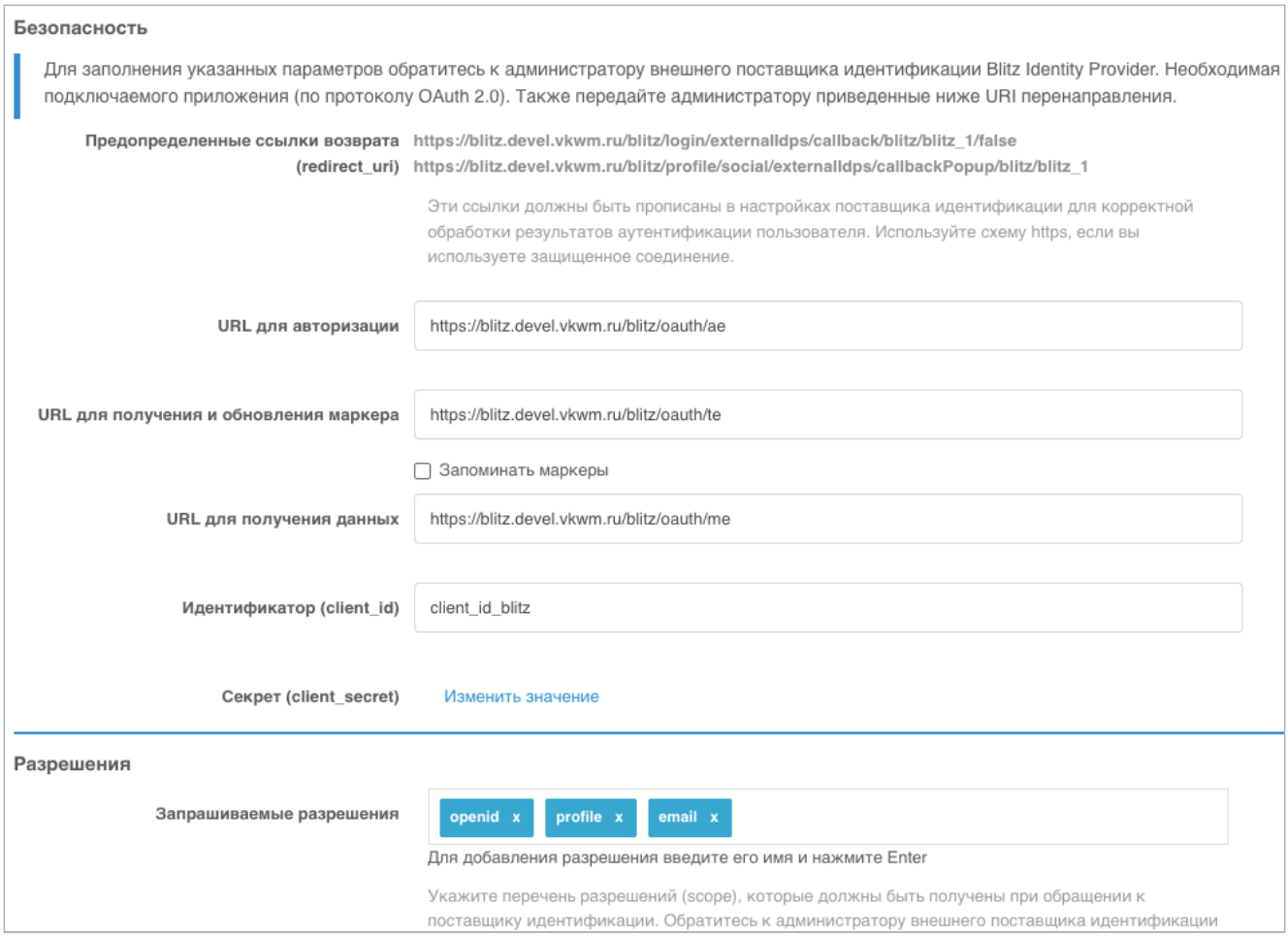
5. В поле **Допустимые grant type** укажите значения: authorization_code и refresh_token.
6. В поле **Допустимые reponse type** укажите значение: code.
7. В поле **Режим выдачи маркеров доступа по умолчанию** выберите значение: offline.



8. Нажмите кнопку **Сохранить**.

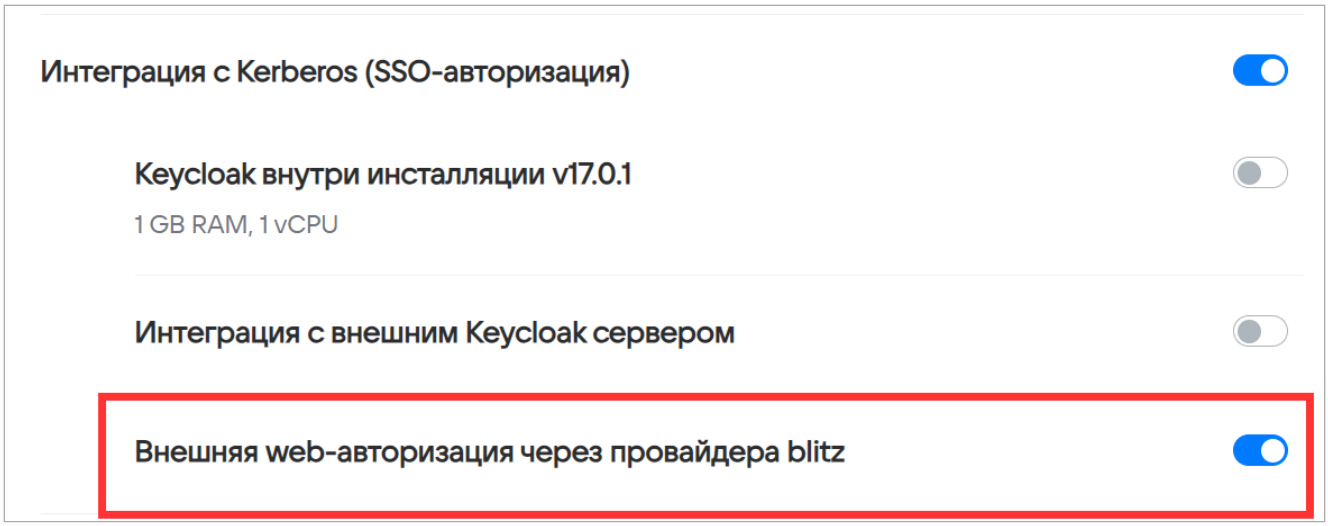
Шаг 2. Добавьте поставщика идентификации в Blitz

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.

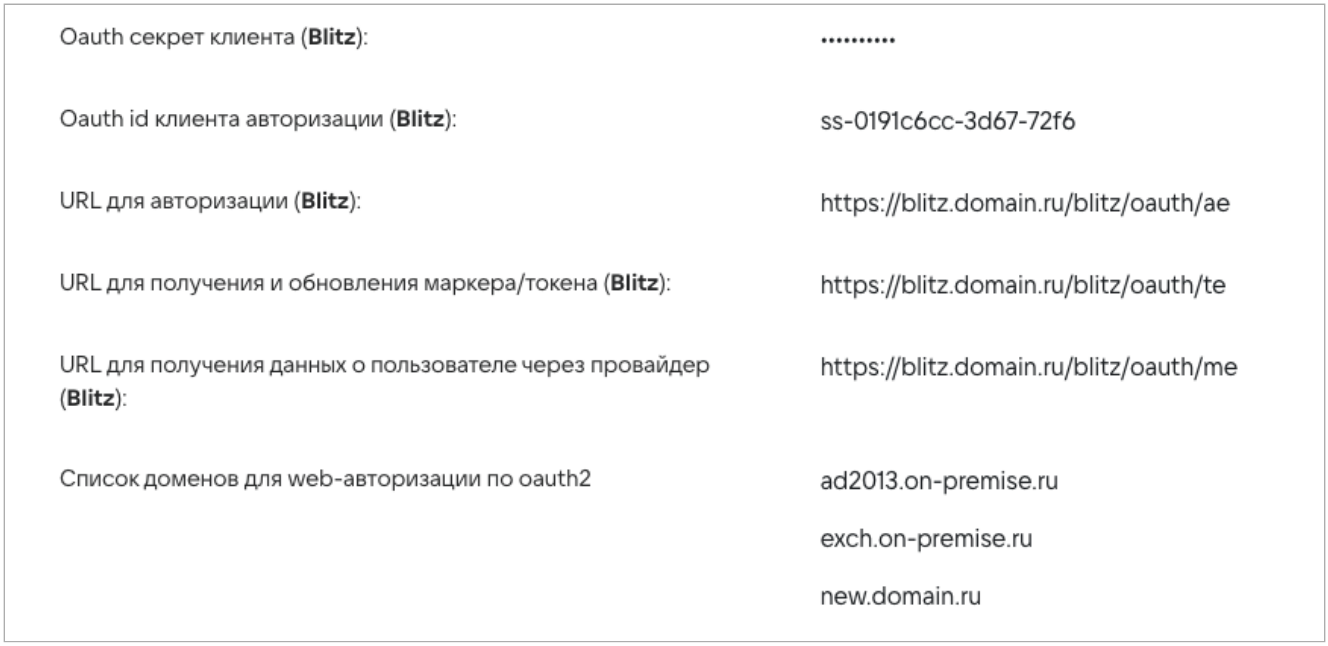


Шаг 3. Выполните настройку в установщике Почты VK Workspace

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



5. Нажмите на кнопку **Сохранить**.
6. Перейдите на вкладку **Настройки → Настройки компонентов → Авторизация**.
7. Нажмите кнопку редактирования .
8. 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.



9. Добавьте домены, которые вы хотите авторизовывать через IDP Blitz.
10. Нажмите на кнопку **Сохранить**.
11. Найдите контейнер **swadb** и выполните шаг **add_sso_domains**.
12. Перейдите к списку контейнеров и выполните шаг **up_container** для контейнера **gofau**.
13. После настройки перейдите на страницу авторизации в Почте 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.

16 марта 2026 г.