

Gitlab

GitLab (<https://gitlab.com>) — это веб-приложение для хранения и управления репозиториями программного кода для Git.

Подключение GitLab к Blitz Identity Provider выполняется по протоколу *OpenID Connect* и состоит из двух этапов:

- Этап 1. Настройки на стороне GitLab
- Этап 2. Настройки на стороне Blitz Identity Provider

Важно:

В инструкции для примера указано, что GitLab расположен на домене `https://gitlab.company.com`, а Blitz IDP установлен на домене `https://login.company.com`. Уточните ваши адреса перед применением инструкции.

Этап 1. Настройки на стороне GitLab

Выполните следующие действия:

1. Откройте для редактирования конфигурационный файл Gitlab: `gitlab.rb` (например, `/etc/gitlab/gitlab.rb`). **Отредактируйте** блок `gitlab_rails['omniauth_providers']`:
 - **label** - укажите название *Сервиса аутентификации*, понятное пользователям. Название будет отображаться на кнопке страницы аутентификации. Например, `Blitz`.
 - **name** - укажите название протокола `openid_connect`.
 - **scopes** - укажите необходимые разрешения для получения данных. Например, стандартный scope `profile`.
 - **response_type** - укажите тип ответа `code`.
 - **issuer** - укажите URL поставщика аутентификации. Например, `https://login.company.com/blitz`.
 - **discovery** - установите значение `true` для автоматического определения параметров клиента.
 - **client_auth_method** - укажите метод аутентификации клиента у поставщика. Например, `basic`.
 - **uid_field** - укажите значение `sub`.
 - **send_scope_to_token_endpoint** - укажите значение `false`.

- **identifier** - укажите уникальное название для идентификации приложения. Например, `gitlab`.
- **secret** - задайте секретный ключ для безопасной аутентификации приложения.
- **redirect_uri** - укажите URL, на который пользователь будет перенаправлен после успешного входа в систему. Например,
`https://login.company.com/gitlab/users/auth/openid_connect/callback`.

```
{
  name: "openid_connect",
  label: "Blitz",
  args: {
    name: "openid_connect",
    scope: ["openid", "profile"],
    response_type: "code",
    issuer: "https://login.company.com/blitz",
    discovery: true,
    client_auth_method: "basic",
    uid_field: "sub",
    send_scope_to_token_endpoint: "false",
    client_options: {
      identifier: "gitlab",
      secret: "eXa12m3PL45e",
      redirect_uri: "https://login.company.com/gitlab/users/auth/openid_connect/callback"
    }
  }
}
```

2. Сохраните файл.

Этап 2. Настройки на стороне Blitz Identity Provider

В консоли управления *Blitz Identity Provider* перейдите в раздел **Приложения** и выполните следующие действия:

1. **Создайте** новое приложение, задав его базовые настройки:
 - **Идентификатор (entityID или client_id)**: аналогичный `client_id`, который был прописан в `gitlab.rb`.
 - **Название**: имя приложения GitLab, которое будет отображаться на стороне Blitz IDP.

- **Домен:**

Новое приложение

Идентификатор (entityID или client_id)

Идентификатор приложения. Используется для идентификации приложения при доступе по протоколу SAML (соответствует entityID) и OAuth 2.0 (соответствует client_id).

Название

Отображаемое пользователям имя приложения. Используется только внутри Blitz Identity Provider.

Домен

Отмена

Сохранить

2. Нажмите **Сохранить**.

3. Далее нажмите кнопку **Параметры**  у предложения GitLab и отредактируйте параметры приложения:

- **Протоколы:** выберите и нажмите **Сконфигурировать**

Далее в параметрах укажите данные, как в .

- **Секрет (client_secret):** аналогичный client_secret, который был прописан в gitlab.rb
- **Префиксы ссылок возврата:**
- **Допустимые разрешения:**

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)

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

Предопределенная ссылка возврата (redirect_uri)

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

Префиксы ссылок возврата

x

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 profile

x openid

Разрешения (scope), которые будут доступны приложению.

4. Нажмите **Сохранить**.

Совет:

После прохождения всех шагов рекомендуем проверить корректность входа в GitLab:
<https://gitlab.company.com>

Версия #2

Admin создал 6 сентября 2024 08:24:56

Admin обновил 20 ноября 2024 14:11:19