

WordPress

WordPress (<https://wordpress.com>) - это система управления содержимым сайта.

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

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

Важно:

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

Этап 1. Настройки на стороне WordPress

Выполните следующие действия:

1. Для интеграции WordPress с Blitz Identity Provider войдите в WordPress под учетной записью администратора. Установите плагин OpenID Connect Generic и перейдите в его настройки.
2. Далее заполните следующие поля:
 - **Login Type** - выберите Auto `Login - SSO`.
 - **Client ID** - укажите уникальное название для идентификации приложения. Например, `Blitz`.
 - **Client Secret Key** - задайте секретный ключ для безопасной аутентификации приложения.
 - **OpenID Scope** - укажите необходимые разрешения для получения данных. Например, обязательный scope `openid` и стандартный scope `profile`. При указании нескольких разрешений разделите их пробелом.
 - **Login Endpoint URL** - укажите URL для авторизации. Например, `https://login.company.com/blitz/oauth/ae`.
 - **Userinfo Endpoint URL** - укажите URL сервиса получения данных пользователя. Например, `https://login.company.com/blitz/oauth/me`.

- **Token Validation Endpoint URL** - укажите URL для получения маркера доступа. Например, `https://login.company.com/blitz/oauth/te`.
- **End Session Endpoint URL** - укажите URL для выхода из приложения. Например, `https://login.company.com/blitz/login/logout`
- **Identity Key** - укажите в фигурных скобках ключ идентификации. Например, `{sub}`.
- **Nickname Key** - укажите в фигурных скобках ключ имени пользователя. Например, `{sub}`.
- **Email Formatting** - укажите в фигурных скобках формат электронной почты. Например, `{email}`.
- **Display Name Formatting** - укажите в фигурных скобках формат отображения имени. Например, `{family_name} {given_name}`.

Client Settings

Enter your OpenID Connect identity provider settings

Login Type

Auto Login - SSO

Select how the client (login form) should provide login options.

Client ID

Blitz

The ID this client will be recognized as when connecting the to identity provider server.
Example: `my-wordpress-client-id`

Client Secret Key

Arbitrary secret key the server expects from this client. Can be anything, but should be very unique.

OpenID Scope

openid profile

Space separated list of scopes this client should access.
Example: `email profile openid offline_access`

Login Endpoint URL

https://login.company.com/blitz/oauth/ae

Identify provider authorization endpoint.
Example: `https://example.com/oauth2/authorize`

Userinfo Endpoint URL

https://login.company.com/blitz/oauth/me

Identify provider User information endpoint.
Example: `https://example.com/oauth2/UserInfo`

Token Validation Endpoint URL

https://login.company.com/blitz/oauth/te

Identify provider token endpoint.
Example: `https://example.com/oauth2/token`

End Session Endpoint URL

https://login.company.com/blitz/login/logout

Identify provider logout endpoint.
Example: `https://example.com/oauth2/logout`

Identity Key

{sub}

Where in the user claim array to find the user's identification data. Possible standard values: `preferred_username`, `name`, or `sub`. If you're having trouble, use "sub".
Example: `preferred_username`

Disable SSL Verify

☐

Do not require SSL verification during authorization. The OAuth extension uses curl to make the request. By default CURL will generally verify the SSL certificate to see if its valid an issued by an accepted CA. This setting disabled that verification.
Not recommended for production sites.

HTTP Request Timeout

5

Set the timeout for requests made to the IDR. Default value is 5.
Example: `30`

Nickname Key

{sub}

Where in the user claim array to find the user's nickname. Possible standard values: `preferred_username`, `name`, or `sub`.
Example: `preferred_username`

Email Formatting

{email}

String from which the user's email address is built. Specify "{email}" as long as the user claim contains an email claim.
Example: `{email}`

Display Name Formatting

{family_name} {given_name}

String from which the user's display name is built.
Example: `{given_name} {family_name}`

3. Нажмите **Сохранить изменения**.

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 OpenID Connect Generic
- **Название:** имя приложения WordPress, 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 WordPress и отредактируйте параметры приложения:

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

Далее в параметрах укажите данные, как в *OpenID Connect Generic* и другие обязательные параметры:

- **Секрет (client_secret):** аналогичный client_secret, который был указан в настройках OpenID Connect Generic
- **Префиксы ссылок возврата:** `https://wp.company.com`
- **Допустимые разрешения:** `openid` `profile`
- **Метод аутентификации при обращении к сервису выдачи маркеров:** `client secret post`
- **Допустимые response type:** `code` `token`

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)

Введите предопределенный redirect_uri

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

Префиксы ссылок возврата

https://wp.company.com 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

Разрешения (scope), которые будут доступны приложению.

Разрешения по умолчанию

Для добавления нового scope введите его и нажмите Enter

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

☐ Не требовать от пользователя согласие на предоставление доступа к данным о себе
☐ Обязательное использование Proof Key for Code Exchange (RFC 7636) для Authorization code grant type

Метод аутентификации при обращении к сервису выдачи маркеров

Указанный метод аутентификации должен использоваться при обращении к сервису выдачи маркеров (token endpoint). При пустом значении доступны все методы

Допустимые grant type

x authorization_code x refresh_token

Список grant type, которые будут доступны приложению. При пустом списке доступны все grant type

Допустимые response type

x code x token

Список response type, которые будут доступны экземпляру приложения при обращении к URL авторизации (authorization endpoint). При пустом списке доступны все response type.

4. Нажмите **Сохранить**.

Совет:

После прохождения всех шагов рекомендуем проверить корректность входа в WordPress: `https://wp.company.com`