

# Jira

**Jira** (<https://www.atlassian.com/ru/software/jira>) — это веб-платформа управления проектами для планирования и отслеживания работы команд.

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

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

## Важно:

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

## Этап 1. Настройки на стороне Jira

### Примечание:

В Jira отсутствует встроенная поддержка одного подключения. Для этого нужно использовать плагин. Ниже в инструкции описано подключение на примере плагина Kantega SSO Enterprise.

Выполните следующие действия:

1. Установите плагин **Kantega SSO Enterprise**. Для этого в настройках Jira перейдите в **Manage Apps** и установите плагин.

## ATLASSIAN MARKETPLACE

Find new apps

Manage apps

## INTEGRATIONS

Kantega SSO Enterprise

## PROJECT CONFIGURATOR

Getting started

Manage Short Term Licenses

## Atlassian Marketplace for JIRA

Discover powerful apps compatible with your JIRA ver



2. В Kantega SSO Enterprise перейдите в раздел **Identity Providers**. Нажмите **Add new identity provider** и выберите **Other**.



Add-ons

# Kantega SSO Enterprise

Common

Identity Providers

Identity providers

Key management

Disable SAML / OIDC

## RESOURCES

Documentation [↗](#)

Add new identity provider ▾

AD FS (Active Directory Federation Services)

Auth0

AuthAnvil

AWS Cognito

Azure AD

Bitium

Centrify

Duo

GitHub

GitLab

Google GSuite

Keycloak

Okta

OneLogin

PingOne

Ping Federate

Salesforce

WSO2

Other

3. В открывшемся окне выберите **OpenID Connect** и нажмите **Next**.

## Add Identity Provider

Protocol

Users

Prepare

Import

Location

Secrets

Summary

### Select protocol for SSO integration

SSO protocol ☐ SAML ☒ OpenID Connect

What is the difference between SAML and OpenID Connect?

SAML and OpenID Connect (OIDC) are both identity federation technology. SAML is XML-based, while OIDC is built on top of OAuth 2.0 with JSON and REST. They are both mature and secure protocols for setting up SSO to JIRA, and work on both desktop clients and mobile apps.

[More info about SAML and OpenID Connect](#)

Discard

[Save draft](#)

Next

4. Выберите настройки по вашим потребностям. Например, **Create accounts on-the-fly**.  
Нажмите **Next**.

## Add Identity Provider

Protocol

Users

Prepare

Import

Location

Secrets

Summary

### User accounts

Users are matched with user accounts in JIRA when they log in

Will accounts pre-exist? ☐ Accounts already exist in JIRA when logging in  
This expects all users' accounts to be present in one of the configured [user directories](#).  
☒ Create accounts on-the-fly for non-existing users when they login  
Use Just-in-time provisioning to create a user account using the name and email address provided by the identity provider.

Default groups   
A comma-separated list of groups. Users will be assigned to the default groups when they do a login through Other.

Back

[Save draft](#)

Next

5. На следующем шаге формируется URL вашей Jira, который необходимо скопировать и добавить в Blitz IDP во втором этапе. Нажмите **Next**.

6. Далее введите **Discovery URL**. Например, `https://login.company.com/blitz/.well-known/openid-configuration`. Нажмите **Next**.

## Add Identity Provider

Protocol

Users

Prepare

**Import**

Location

Secrets

Summary

### Metadata import

Discovery URL:

OpenID server publishes metadata at a well-known discovery URL, returning a JSON listing of the OpenID/OAuth endpoints, supported scopes and claims, public keys used to sign the tokens, and other details.

**Discovery URL hint**

https://{identity server}/.well-known/openid-configuration

Back

Save draft

Next

7. Заполните следующие поля и нажмите **Next**:

- **Identity provider name:** укажите название Сервиса аутентификации, которое будет отображаться в настройках Jira. Например, `Blitz`.
- **Scopes:** укажите необходимые разрешения для получения данных. Например, обязательный scope `openid` и стандартный scope `profile`.

## Add Identity Provider

Protocol

Users

Prepare

Import

**Location**

Secrets

Summary

### SSO Integration

Identity provider name

Set a name for your identity provider (IdP). Typically the IdP organization name.

Scopes

Set scopes you want to request from your identity provider (IdP). If your desired scope is not in the list, start writing to add your own.

Back

Save draft

Next

8. На следующем шаге заполните поля и нажмите **Next**:

- **Client ID:** `jira.company.com`
- **Client Secret:** задайте секретный ключ для безопасной аутентификации приложения.

### Add Identity Provider

Protocol

Users

Prepare

Import

Location

Secrets

Summary

#### Credentials

Copy / paste client id and secret from the administration console of your identity provider into the fields below.

Client ID:

`jira.company.com`

Client Secret:

\*\*\*\*\*

Back

Save draft

Next

9. На следующем шаге проверьте введенные данные и нажмите **Finish**.

## 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):** укажите аналогичный `client_id`
  - **Название:** имя приложения Jira, которое будет отображаться на стороне Blitz IDP
  - **Домен:** `https://jira.company.com`

Новое приложение

Идентификатор (entityID или client\_id)

jira.company.com

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

Название

Jira

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

Домен

https://jira.company.com

Отмена

Сохранить

2. Нажмите **Сохранить**.

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

- **Протоколы:** выберите `OAuth 2.0` и нажмите **Сконфигурировать**

*Далее в параметрах укажите данные, как в учетных данных Jira:*

- **Секрет (client\_secret):** укажите аналогичный client\_secret
- **Префиксы ссылок возврата:** `https://jira.company.com`
- **Допустимые разрешения:** `profile` `openid`

#### Настройки взаимодействия с приложением

Секрет (client\_secret)

.....



Секретный ключ подключаемого приложения (client\_secret). Если указан, то именно этот секрет должен использоваться подключаемым 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

jira.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

client secret basic



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 client\_credentials

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

Допустимые response type

x code

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 Jira: <https://jira.company.com>

Версия #2

Admin создал 12 августа 2024 11:30:01

Admin обновил 20 ноября 2024 14:11:19