

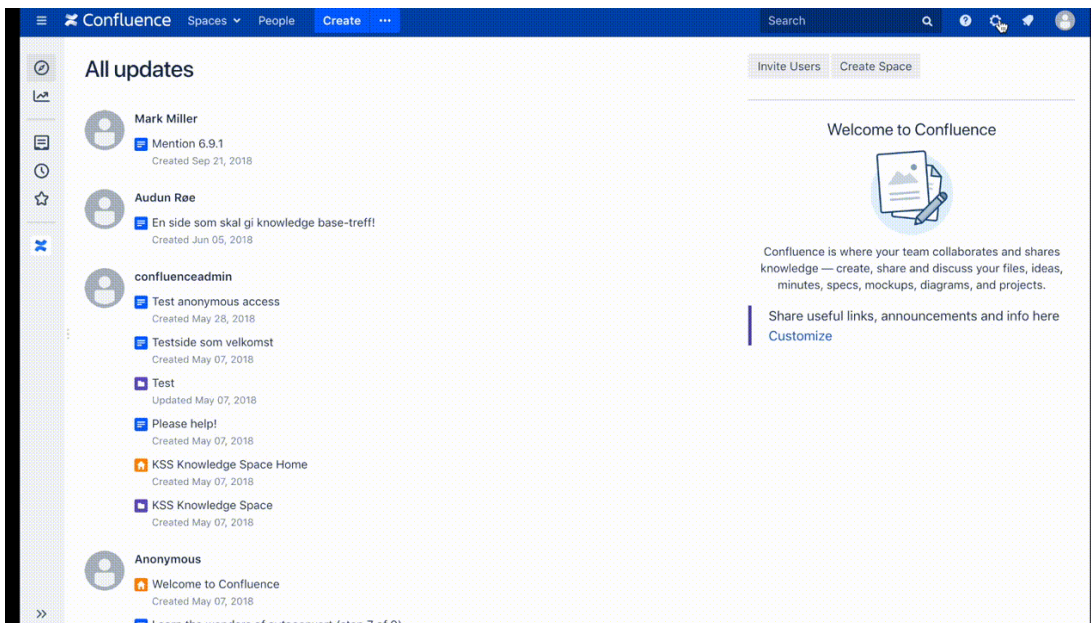
Auth0



Setup guide for adding Auth0 login to Atlassian server and datacenter products.

Context: This setup guides assumes that [Kantega SSO](#) is installed as an add-on to your Atlassian product ([Jira](#), [Confluence](#), [Bitbucket](#), [Bamboo](#), or [FeCru](#)).

The setup starts in the Configuration page of the Kantega SSO add-on. This configuration page can be found by pressing "**Configure**" on "Kantega Single Sign-On (SSO)" in list of installed add-ons.



1: Click "Add SAML identity provider" and select "**Auth0**"

Add SAML Identity Provider ▾

CLOUD

- Auth0
- AuthAnvil
- Azure Active Directory (Azure AD)
- Bitium
- Duo
- Google GSuite
- Okta
- OneLogin
- PingOne
- Salesforce
- WSO2

ON-PREMISE

- Active Directory Federation Services (AD FS)
- Keycloak
- Ping Federate

GENERAL

- Any other SAML 2.0 Identity Provider



Prepare

Copy the ACS URL/ Entity ID (the URLs are identical). They are used in a later step

Add Identity Provider

Prepare • Import • Location • Signature • Users • Summary

Preparing Auth0

Follow the step-by-step instructions [here](#) to setup JIRA SSO with Auth0.

The following information is needed by Auth0 to enable JIRA as a service provider / relying party:

ACS URL

URL where users return after signing in. Also known as "Assertion Consumer Service URL" or "Login URL"

Entity ID

Same value as the ACS URL above. Also known as "Destination" or "Receipient".

Next Save draft Discard

Add a new Client

In Auth0 navigate to Dashboard and select "New Client"


- Give the Client a name
- Select "Regular Web Applications"
- Press Create

Create Client

Name

You can change the client name later in the client settings.


Choose a client type



Native

Mobile or Desktop, apps that run natively in a device.


eg: iOS SDK



Single Page Web Applications

A JavaScript front-end app that uses an API.


eg: AngularJS + NodeJS



Regular Web Applications

Traditional web app (with refresh).

eg: Java ASP.NET



Non Interactive Clients

CLI, Daemons or Services running on your backend.

eg: Shell Script

CREATE

Addons












- Go to the Addons tab
- Select SAML 2.0

issues.example.com

[Quick Start](#) [Settings](#) [Addons](#) [Connections](#)

Client ID: nMsWgDwKf64xuAKKhNOVMe7hDjiyVT3l

Addons are plugins associated with an Application in Auth0. Usually, they are 3rd party APIs used by the client that Auth0 generates access tokens for (e.g. Salesforce, Azure Service Bus, Azure Mobile Services, SAP, etc).

 <input type="checkbox"/>	 Firebase <input type="checkbox"/>	 Layer <input type="checkbox"/>
 <input type="checkbox"/>	 <input type="checkbox"/>	 <input type="checkbox"/>
 <input type="checkbox"/>	 <input type="checkbox"/>	 <input type="checkbox"/>
 <input checked="" type="checkbox"/>	 <input type="checkbox"/>	

Application Callback URL

Paste the ACS URL from the Prepare step into Application Callback URL

Addon: SAML2 Web App ✕

[Settings](#) [Usage](#)

Application Callback URL

`https://issues.example.com/plugins/servlet/no.kantega.saml/sp/18nnk4zeno55r/login`

SAML Response will be POSTed to this URL.

Settings

- Add **audience** and **recipient** (Use the ACS URL from the Prepare step)
- Press Save, then close the Client setup

Settings

```
1 {  
2 "audience": "https://issues.example.com/plugins/servlet/no.ka  
3 "recipient": "https://issues.example.com/plugins/servlet/no.k
```

Federation Metadata

- Go to Settings
- Press "Show Advanced Settings"
- Press "Endpoints"
- Copy the SAML Metadata URL

Hide Advanced Settings

Advanced Settings

Application Metadata Mobile Settings OAuth Grant Types WS-Federation Certificates Endpoints

OAuth

OAuth Authorization URL	https://kantegasso.eu.auth0.com/authorize	📄
OAuth Token URL	https://kantegasso.eu.auth0.com/oauth/tok	📄
OAuth User Info URL	https://kantegasso.eu.auth0.com/userinfo	📄
OpenID Configuration	https://kantegasso.eu.auth0.com/well-know	📄
JSON Web Key Set	https://kantegasso.eu.auth0.com/well-know	📄

SAML

SAML Protocol URL	https://kantegasso.eu.auth0.com/samlp/nM	📄
SAML Metadata URL	https://kantegasso.eu.auth0.com/samlp/me	📄

Metadata import

- In Kantega Single Sign-on, go to the metadata import step
- Paste the metadata URL from the previous step
- Press Next

Add Identity Provider

Prepare Import Location Signature Users Summary

Metadata import

Import metadata using Metadata file published online

URL to metadata file

Metadata file on my computer

Paste metadata XML from clipboard

[Back](#) [Skip import](#)

Location

- Give the Identity Provider a name (This name is visible to end users)
- The SSO Redirect URL is automatically imported from the metadata
- Press Next

Add Identity Provider

Prepare Import Location Signature Users Summary

Name and SSO location

Identity provider name

Name of the organization providing the user's identity

SSO redirect URL

Imported from metadata

[Back](#)

Signature

- Review the imported signing certificate (This step is purely informational)
- Press Next.

Add Identity Provider

Prepare Import Location **Signature** Users Summary

Signature verification

Signing certificate

CN=kantegasso.eu.auth0.com

Valid from: Mon Jul 24 07:57:19 CEST 2017

Valid to: Wed Apr 02 07:57:19 CEST 2031

Sign. alg: SHA256withRSA (2048 bits)

Thumbprint: 36 D0 53 75 3A 80 D7 53 77 01 C1 31 FE 0B FF 2D 6C EC A4 A2 (SHA-1)

Certificate used to validate SAML messages issued by the identity provider

Next Back

Users

- Select whether users already exist, or if you wish to have users automatically created upon login
- Press Next

Add Identity Provider

Prepare Import Location Signature **Users** Summary

User accounts

When logging in SAML users, we must match them with accounts in JIRA

Will accounts pre-exist?

Accounts already exist in JIRA when logging in

Create accounts in JIRA's Internal Directory if needed

When no account is found, we'll create one using the name and email address provided in the SAML attributes

Next Back

Summary

- Review the Summary
- Press Finish

Add Identity Provider

Prepare Import Location Signature Users Summary

Summary

Display name: **Auth0** [Edit](#)

Endpoint location: <https://kantegasso.eu.auth0.com/samlp/nMsWgDWkf64xuAKKhNOVMe7hDjyVT3I> [Edit](#)

Signing certificate: CN=kantegasso.eu.auth0.com
[Edit](#)

JIRA users: Users will exist in JIRA when logging in.
[Edit](#)

Finish Cancel

Testing/configuring the identity provider

After finishing the wizard, you will be sent to the test pages for verification of your setup. Here, you may also perform the last configuration parts. [Follow this generic introduction to the test pages and final configuration.](#) AD FS is used as the example here.