

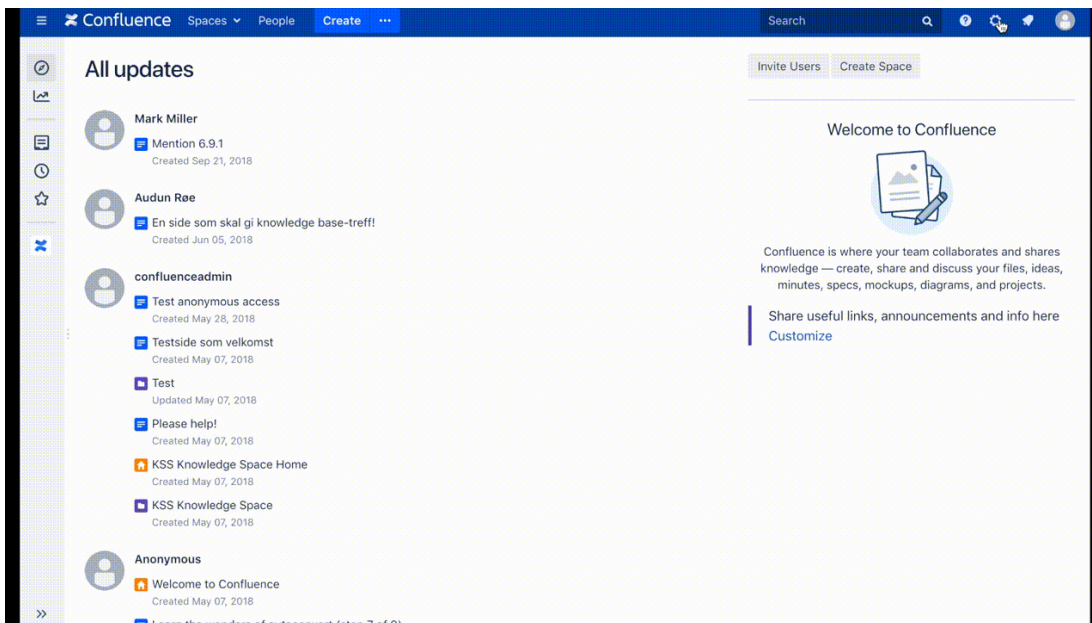
WSO2



Setup guide for adding WSO2 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](#)).

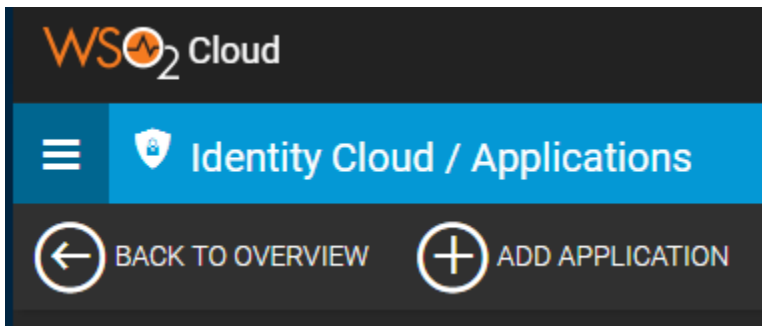
The setup starts in the Configuration page of the Kantega SSO add-on. This configuration page can be found by pressing "**Configure**" on "Kantega Single Sign-On (SSO)" in list of installed add-ons.



Add a new Application

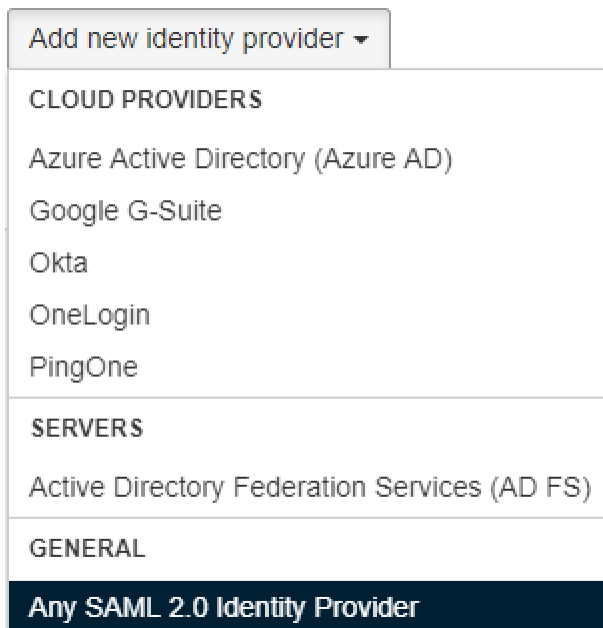
- Log into WSO2

- Select Add Application
- Choose Custom Application
- Enter an Application Name
- Select Add



Adding an identity provider

In Kantega Single Sign-on add an identity Provider of the type "Any SAML 2.0 Identity Provider".



Prepare

Copy the ACS URL. You will use this in the next step.

Add Identity Provider

Prepare Import Location Signature Users Summary

Adding a SAML 2.0 Identity Provider

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

ACS URL	<input type="text" value="https://issues.example.com/plugins/servlet/no.kantega.saml/sp/1maucgz5af2d€"/>	
	URL where users return after signing in. Also known as "Assertion Consumer Service URL" or "Login URL"	
Entity ID	<input type="text" value="https://issues.example.com/plugins/servlet/no.kantega.saml/sp/1maucgz5af2d€"/>	
	Same value as the ACS URL above. Also known as "Destination" or "Recipient".	

Configure the application

- Fill in the URL from the previous step into the following fields:
 - Issuer
 - Assertion Consumer URL's (Press Add)
 - Access URL
- Save



issues.example.com

Select App Type * ?

Standards-based Federation

The application should be able to generate standard SSO requests and process responses sent by the identity provider. The supported standards are SAML2 Web SSO, OpenID Connect, and WS-Federation (Passive). For more information, see the [documentation](#).

Proxy-based Federation

Shortcut

Select Security Protocol * ?

SAML2 Web SSO ▾

Configure Manually Upload SAML Metadata File

Issuer * ?

Assertion Consumer URLs* ?

Default	Assertion Consumer URL	Action
<input checked="" type="radio"/>	https://issues.example.com/plugins/servlet/no.kantega.saml/sp/hfsj68gn8gq/login	<input type="button" value="Delete"/>

Enable Response Signing

Claim Configuration

Configure User Claims

Add Local Claims Add Custom Claims

Store Configuration

Display Name * ?

issues.example.com

Access URL * ?

https://issues.example.com/plugins/servlet/no.kantega.saml/sp/hfsj6e8gn8gq/login

Download IDP Metadata

- Download the IDP metadata. You will use the metadata file in the next step.

The screenshot shows the WSO2 Cloud Identity Cloud / Applications interface. At the top, there is a navigation bar with the WSO2 Cloud logo, a search icon, and links for 'kantega', 'Documentation', and 'Support'. Below this is a blue header with a menu icon, the text 'Identity Cloud / Applications', and a 'Go to User Portal' link. A dark grey navigation bar contains three buttons: 'BACK TO OVERVIEW' (with a left arrow), 'ADD APPLICATION' (with a plus sign), and 'DOWNLOAD IDP METADATA' (with a download icon). The 'DOWNLOAD IDP METADATA' button is highlighted with a green border. Below the navigation bar, there is a large orange square containing a white globe icon. At the bottom of this square, the text 'issues.example.com' is displayed next to a vertical ellipsis menu icon.

Metadata Import

- In Kantega Single Sign-on, go to the metadata import step.
- Browse and select the downloaded metadata file 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



C=None, O="None L=None", OU=None, CN=kantega

Valid from: Wed Oct 25 13:55:10 CEST 2017

Valid to: Mon Nov 22 12:55:10 CET 2027

Sign. alg: MD5withRSA (1024 bits)

Thumbprint: 97 B9 97 6B CB ED 21 F2 12 2C 14 C5 08 43 73 74 FD 12 85 2B (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.
- Optionally assign a default group for new users.

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

A comma-separated list of groups that users will be added to when they first log in

Next Back

Summary

- Review the Summary.
- Press Finish.

Add Identity Provider

Prepare Import Location Signature Users Summary

Summary

Display name: WS02 [Edit](#)

Endpoint location <https://identity.cloud.wso2.com/identity/t/kantega> [Edit](#)

Signing certificate C=None, O="None L=None", OU=None, CN=kantega
[Edit](#)

JIRA users Create users in JIRA's Internal Directory if needed. (Default groups: jira-software-users)
[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](#).