

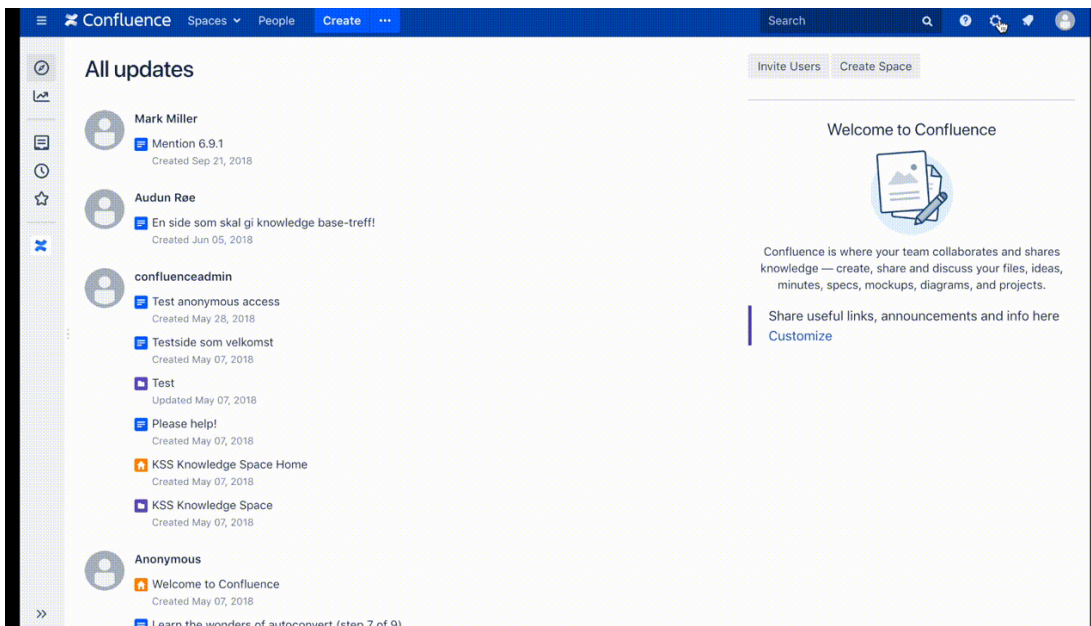
AuthAnvil



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

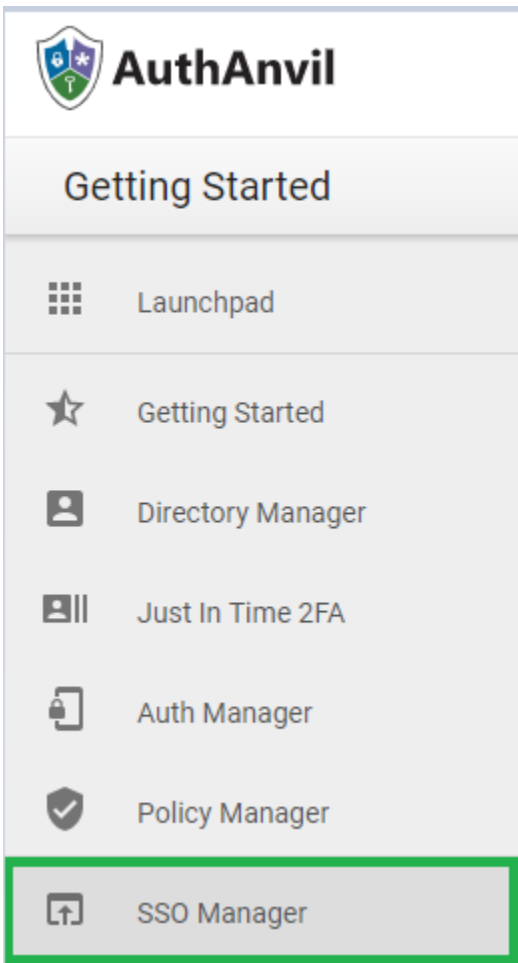
This setup guides assumes that [Kantega SSO](#) is installed as an add-on to your Atlassian product ([Jira](#), [Confluence](#), [Bitbucket](#), [Bamboo](#), or [FeCru](#)).

Context: This 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.

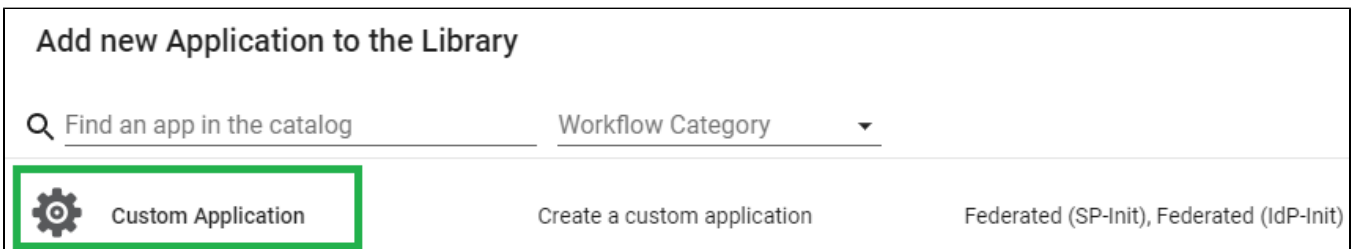


Add a new Application

Navigate to SSO Manager and press the green plus at the bottom right, then select the paper icon.



From the Library, add a Custom Application.

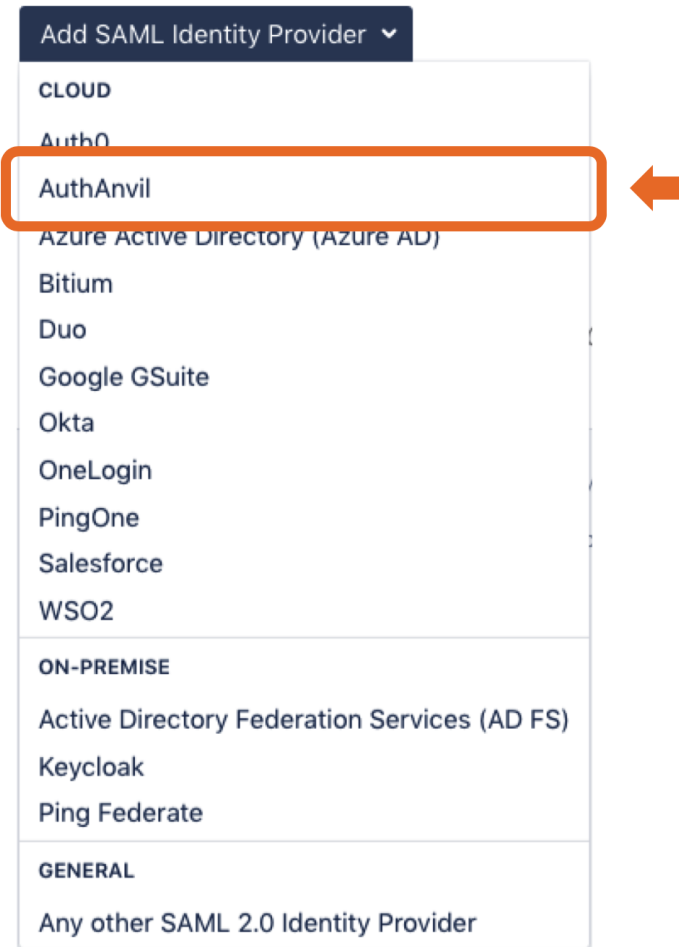


Application Configuration

- Start by giving your application a name.
- Select your preferred authentication policy.

Adding an identity provider

In Kantega Single Sign-on add an identity Provider of the type "AuthAnvil".



Prepare

Copy the ACS URL and Entity ID. These values are used in the next step.

Add Identity Provider

Prepare

Import

Location

Signature

Users

Summary

Preparing AuthAnvil

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

The following information is needed by AuthAnvil 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](#)

Protocol Setup

- In AuthAnvil, navigate to "Protocol Setup".
- Paste the values from the prepare step into the corresponding fields.
- Press "Add application".

Add new Application to the Library

Application Configuration

Protocol Setup

Protocol Type

SAML SP-Init

Assertion Consumer Service URL

<https://issues.example.com/plugins/servlet/no.kantega.sai>

Allow Multiple Audiences

Service Entity ID (Issuer)

<https://issues.example.com/plugins/servlet/no.kantega.sai>

Attribute Transformation

By default, AuthAnvil will only send the Name ID SAML attribute.

If you want automatic user creation, the attributes email and DisplayName must be added.

- In "Attribute Transformation" Press Add custom Attribute Map".
- Add your preferred attributes. (See example below.)
- Save the changes.

The screenshot shows the AuthAnvil SSO Manager interface for 'issues.example.com'. The 'Attribute Transformation' tab is active. It displays two radio button options: 'Just issue an attribute as the username' (unselected) and 'Specify custom attribute transform' (selected). Below these options is a table with columns 'Attribute Value' and 'Send As'. The table contains three rows of mappings, each with a 'REMOVE' button. At the bottom of the table is a blue button labeled 'ADD CUSTOM ATTRIBUTE MAP'.

Attribute Value	Send As	
{User.EmailAddress} =>	email	REMOVE
{User.DisplayName} =>	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	REMOVE
{User.PrincipalName} =>	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	REMOVE

Permissions

Select which users should be able to log into the SAML application.

- Navigate to Permissions.
- Press "Add Groups" to Assign permissions to the application.
- Select an already existing group or create a new one.
- Save the changes.

The screenshot shows the AuthAnvil SSO Manager interface for 'issues.example.com' with the 'Permissions' tab selected. The 'Permissions' tab is highlighted with a green box. The main content area is split into two sections: 'Group Access' and 'Application Permissions'. The 'Group Access' section has a heading 'Group Access' and a message 'There aren't any groups that have access to this application.' Below this message is a blue button labeled 'ADD GROUPS' with a green border. The 'Application Permissions' section has a heading 'Application Permissions' and a paragraph of text explaining that applications support group-based permissions for users.

Federation Metadata

- Go to Protocol Setup.
- Press "View Federation Metadata".
- Copy the metadata URL that opens and save it for the next step.

Launchpad	Application Configuration	Protocol Setup	Attribute Transformation
<ul style="list-style-type: none">Getting StartedDirectory ManagerJust In Time 2FAAuth ManagerPolicy ManagerSSO ManagerApplication LibraryWorkflow RequestsLicense Manager	<p>Protocol Type SAML SP-Init</p> <p>Assertion Consumer Service URL https://issues.example.com/plugins/servlet/no.kantega.sai</p> <p><input type="checkbox"/> Allow Multiple Audiences</p> <p>Service Entity ID (Issuer) https://issues.example.com/plugins/servlet/no.kantega.sai</p> <p>Identity Issuer https://kantegasso.my.authanvil.eu/trust</p> <p>Token Lifetime (Minutes) 60</p> <p>▶ Advanced Settings Configure advanced settings for this application</p> <p>< > VIEW FEDERATION METADATA</p>		

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

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

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 Signing Certificate

Valid from: Tue Nov 14 08:28:02 CET 2017

Valid to: Sun Nov 13 08:28:02 CET 2022

Sign. alg: SHA256withRSA (2048 bits)

Thumbprint: 24 19 E8 EC 51 CC B8 AD 09 C6 4D B4 DC 67 65 12 4D E7 5E B8 (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.
- Note that for users to be created, a name, username and an email must be sent in the SAML response. (See previous instructions.)
- 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: AuthAnvil [Edit](#)

Endpoint location <https://kantegasso.my.authanvil.eu/trust/launch> [Edit](#)

Signing certificate CN=kantegasso Signing Certificate
[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](#).