

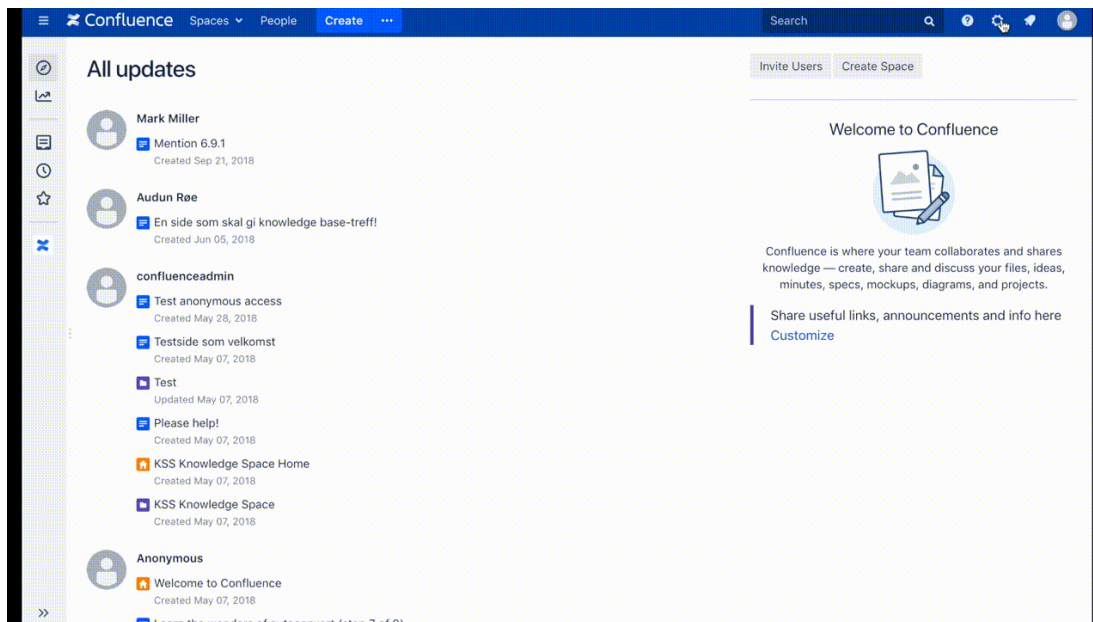
Bitium



Setup guide for adding Bitium login to Atlassian products.

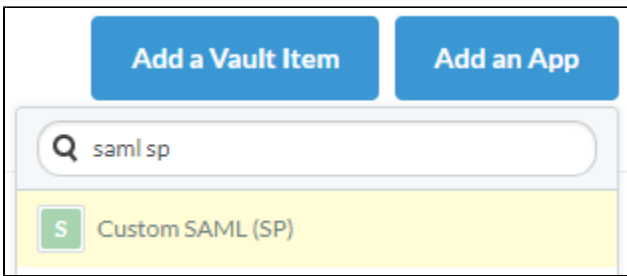
This setup guides assumes that [Kantega SSO](#) is installed as an add-on to your Atlassian product ([Jira](#), [Confluence](#), [Bitbucket](#), [Bamboo](#), or [FeCru](#)).

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 an App in Bitium

- Navigate to Apps, then select **Add an App**
- Search for and select **saml sp**



Naming the application

- Give your application a name.
- Select your preferred Type. E.g. Individual Account.
- Press Install App.



Custom SAML (SP)

Name

Custom name of the app

Type

Individual Account
Each user will enter his or her own username & password to configure this App.

Shared Account
Create a shared version of this App. All users given access will be logged in with the same username & password. Only users who enter the App password can view or change it and assign this App to others. For more information, [contact support](#).

Request Access
Ask someone from another company (e.g. customer, client, or consultant) to grant access to their account. After access is granted, users in your company with access to the installation will be able to login to the account. Only the person who enters the password and grants access to this App will be able to view or change the password. They can revoke access at any time. For more information, [contact support](#).

Assign Users (Subscribers)

- Select Assign Users.
- Select the preferred accounts.
- Choose a username for the selected accounts.
- Press Done.

The screenshot shows the 'Add Users' interface for 'issues.example.com'. The top bar includes a 'Cancel' button, a 'Users Selected: 1' indicator, and a 'Done' button. The main area is split into two panels. The left panel, titled 'Available Unsubscribed Users', contains a 'Filter by Group' dropdown and a search bar. Below the search bar, it says 'Showing 0 of 0 User'. The right panel, titled 'Users to add to issues.example.com', shows a list of users. One user, 'Mark Miller' with email 'mark.miller@kantega.no', is selected. Below the list, there is a 'Create a New User Account' section with a radio button selected. It prompts to 'Enter credentials to create a new account' and has a text input field for 'Username or Email' containing 'mark.miller@kantega.no'. A 'Save' button is located at the bottom of this section.

Adding an identity provider

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

The screenshot shows a dropdown menu titled 'Add SAML Identity Provider'. The menu is open, displaying a list of identity providers. The 'Bitium' option is highlighted with an orange box and an orange arrow pointing to it. The list is organized into three categories: 'CLOUD', 'ON-PREMISE', and 'GENERAL'. The 'Bitium' option is located under the 'CLOUD' category.

- 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.
- Press Next.

Add Identity Provider

Prepare Import Location Signature Users Summary

Preparing Bitium

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

The following information is needed by Bitium 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"

[Next](#) [Save draft](#) [Discard](#)

Configure the Single Sign-on App in Bitium

- In Apps Overview, select the App you just created.
- Select Single Sign-on.
- Paste the ACS URI from the previous step into SAML URL.

Select a Single Sign-On Provider

To set up Bitium to use an alternate sign on method for this application, select it below.

SAML Authentication ▼

Use a 3rd party identity provider (IdP)

SAML URL

This is the URL where Bitium will send SAML requests for Custom SAML (SP)

Download Bitium Metadata

- If your server has Internet access, **copy** the metadata URL. (Preferred)

- If the server does not have Internet access, **download** the metadata.

Metadata URL 

<https://www.bitium.com/kantega.no/saml/121779/metadata.xml>

[Download Metadata XML](#)

Metadata import

- Import the metadata using one of the options.
- Pres 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. (Depending on your redirect mode, this name may be visible to end users.)
- The SSO Redirect URL is automatically imported when using 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

Next 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=US, ST=CA, L=Los Angeles, O=Kantega, CN=kantega.no

Valid from: Wed Mar 08 09:14:43 CET 2017

Valid to: Mon Mar 08 09:14:43 CET 2027

Sign. alg: SHA1withRSA (2048 bits)

Thumbprint: BF 1B 24 9B D1 82 7F 33 9F E7 27 28 48 7C B6 8B 22 AF FC 23 (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.
- 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

Next Back

Summary

- Review the Summary.
- Press Finish.

Add Identity Provider

Prepare Import Location Signature Users Summary

Summary

Display name: Bitium [Edit](#)

Endpoint location: <https://www.bitium.com/kantega.no/saml/121779/auth> [Edit](#)

Signing certificate: C=US, ST=CA, L=Los Angeles, O=Kantega, CN=kantega.no
[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](#).