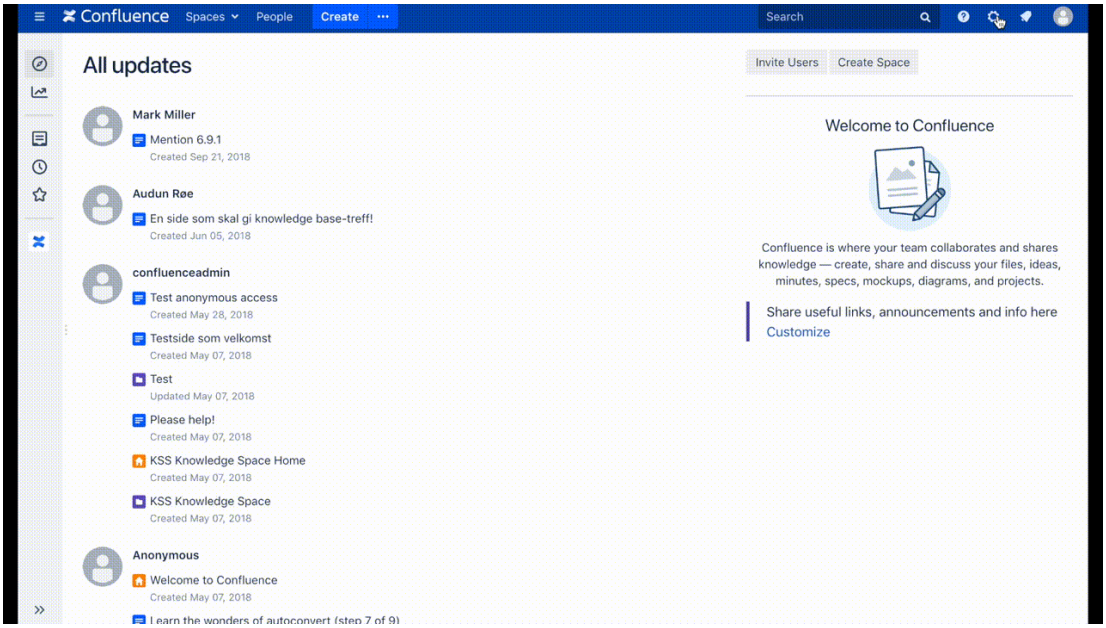
AuthAnvil

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

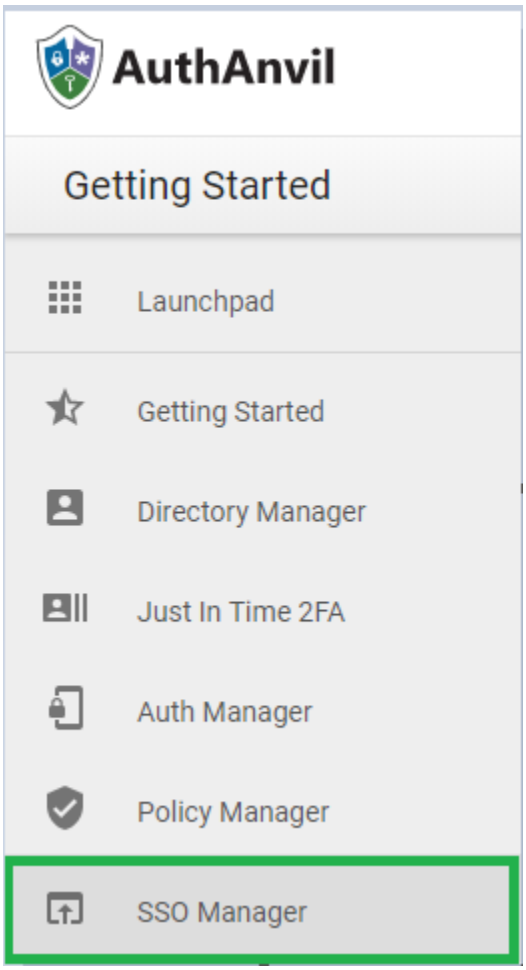
This setup guides assumes that Kantega SSO in installed as an add-on to your Atlassian product (Jira, Confluence, Bitbucket, Bamboo, or FeCru).

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.

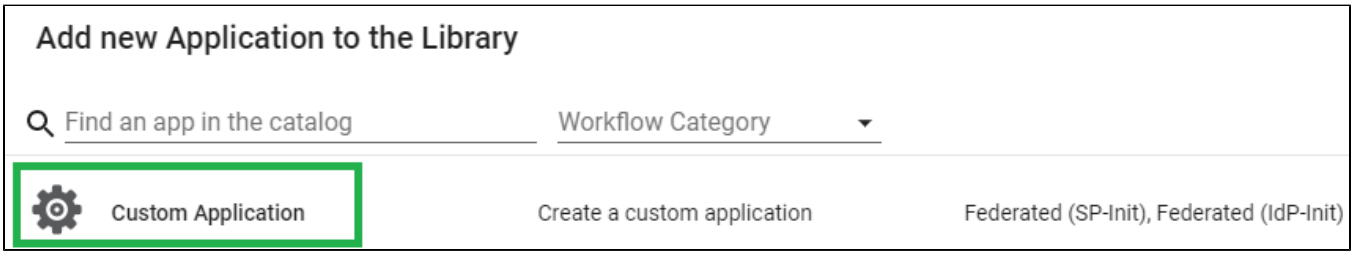


Add a new Application

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.

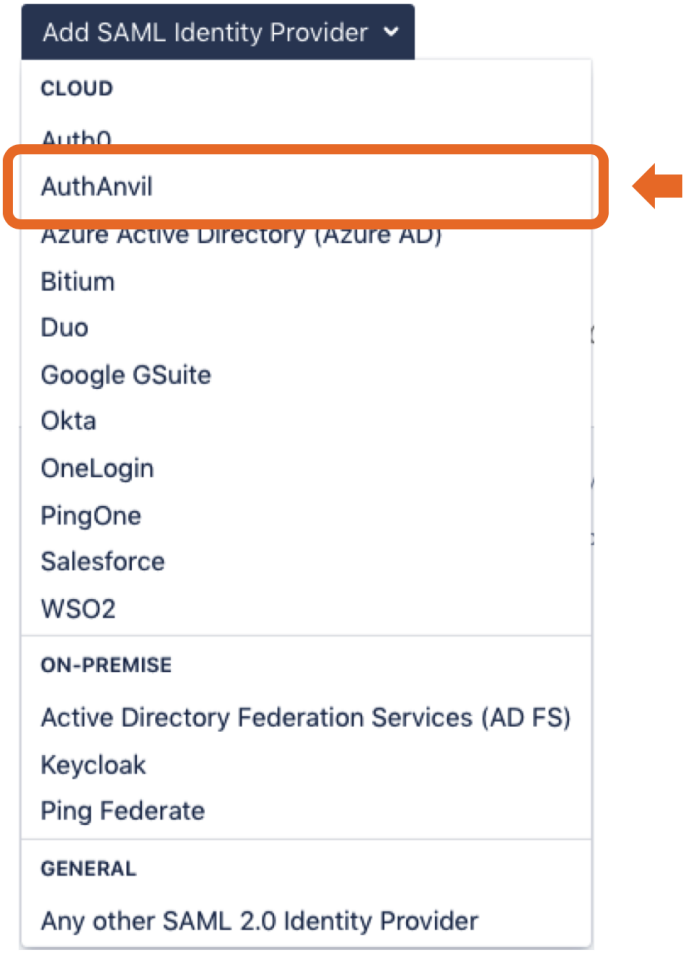


Application Configuration

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

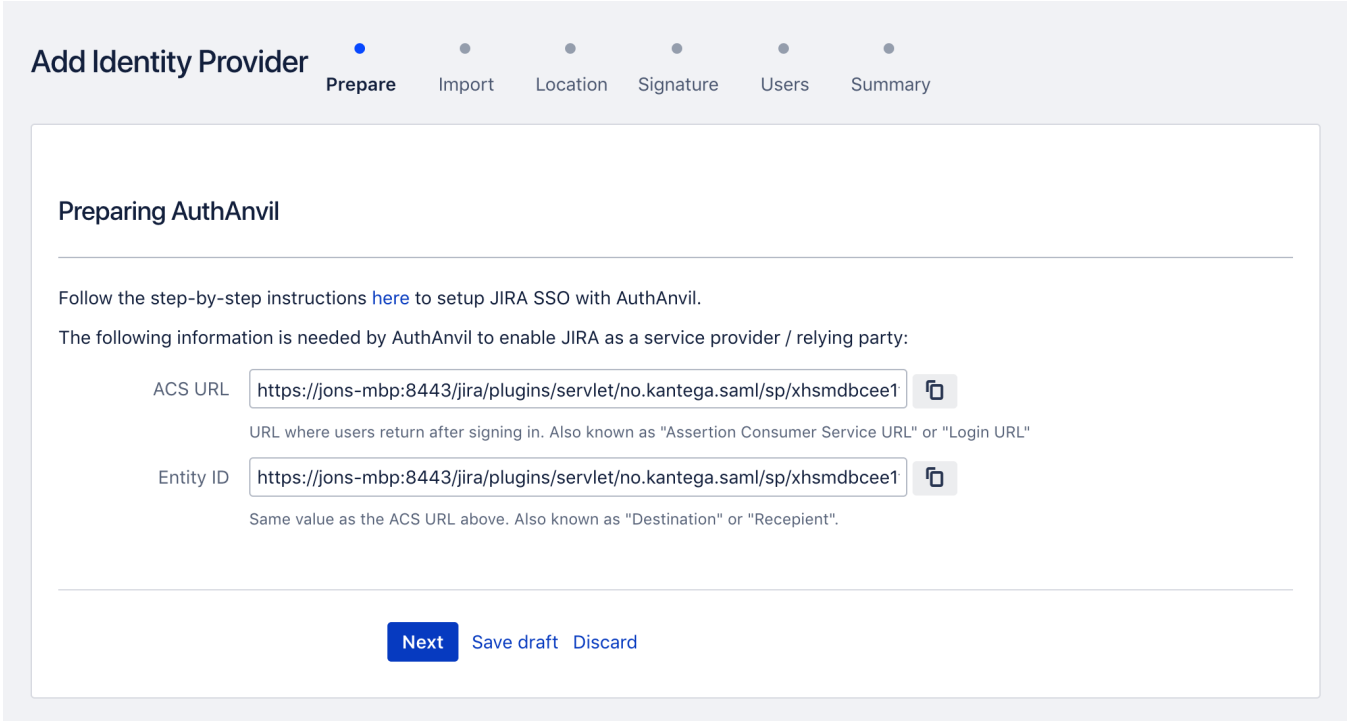
Adding an identity provider

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



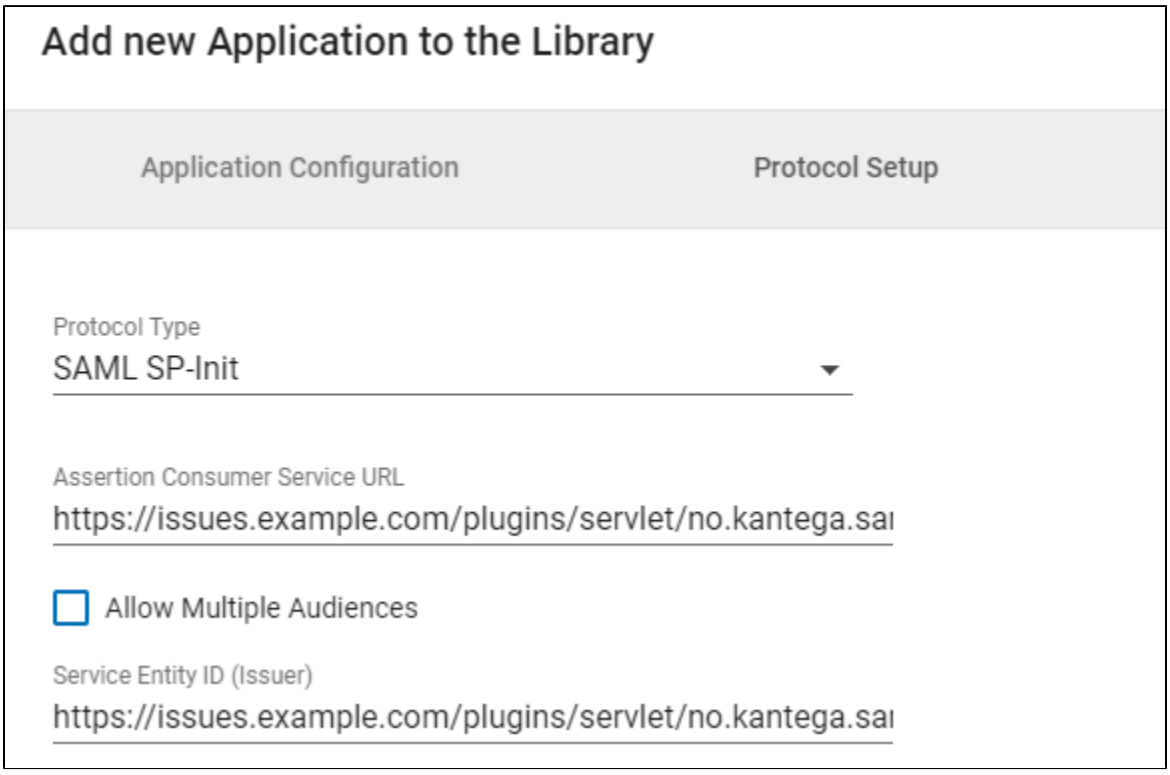
Prepare

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



Protocol Setup

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

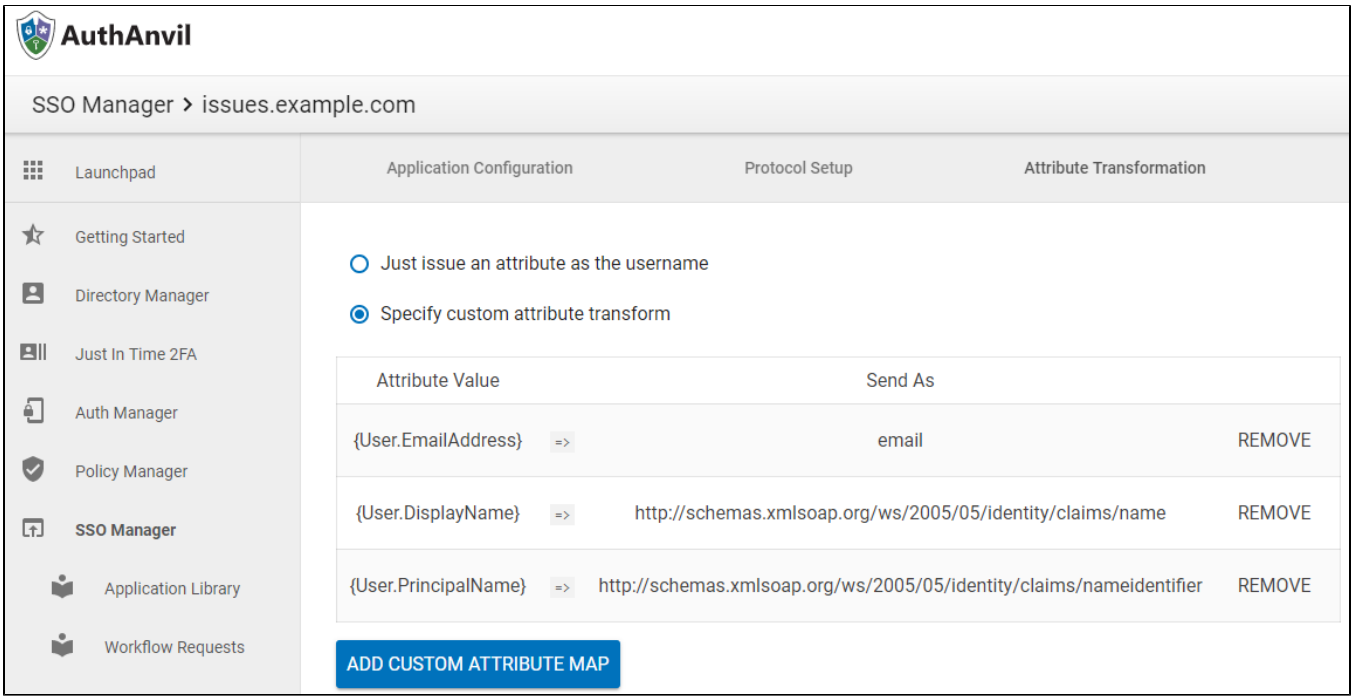


Attribute Transformation

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

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

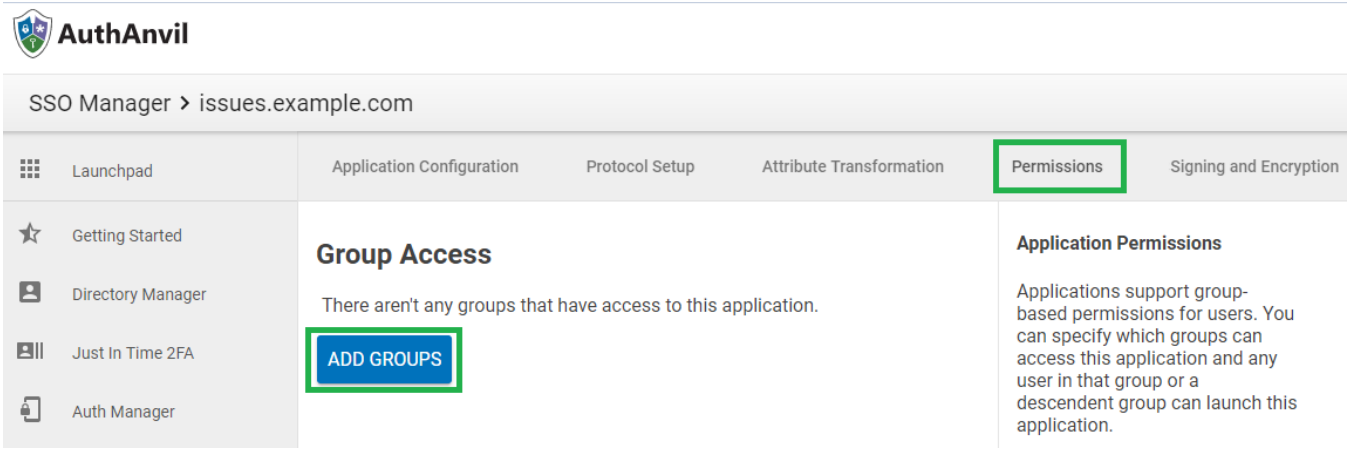
- In "Attribute Transformation" Press Add custom Attribute Map".
- Add your preferred attributes. (See example below.)
- Save the changes.



Permissions

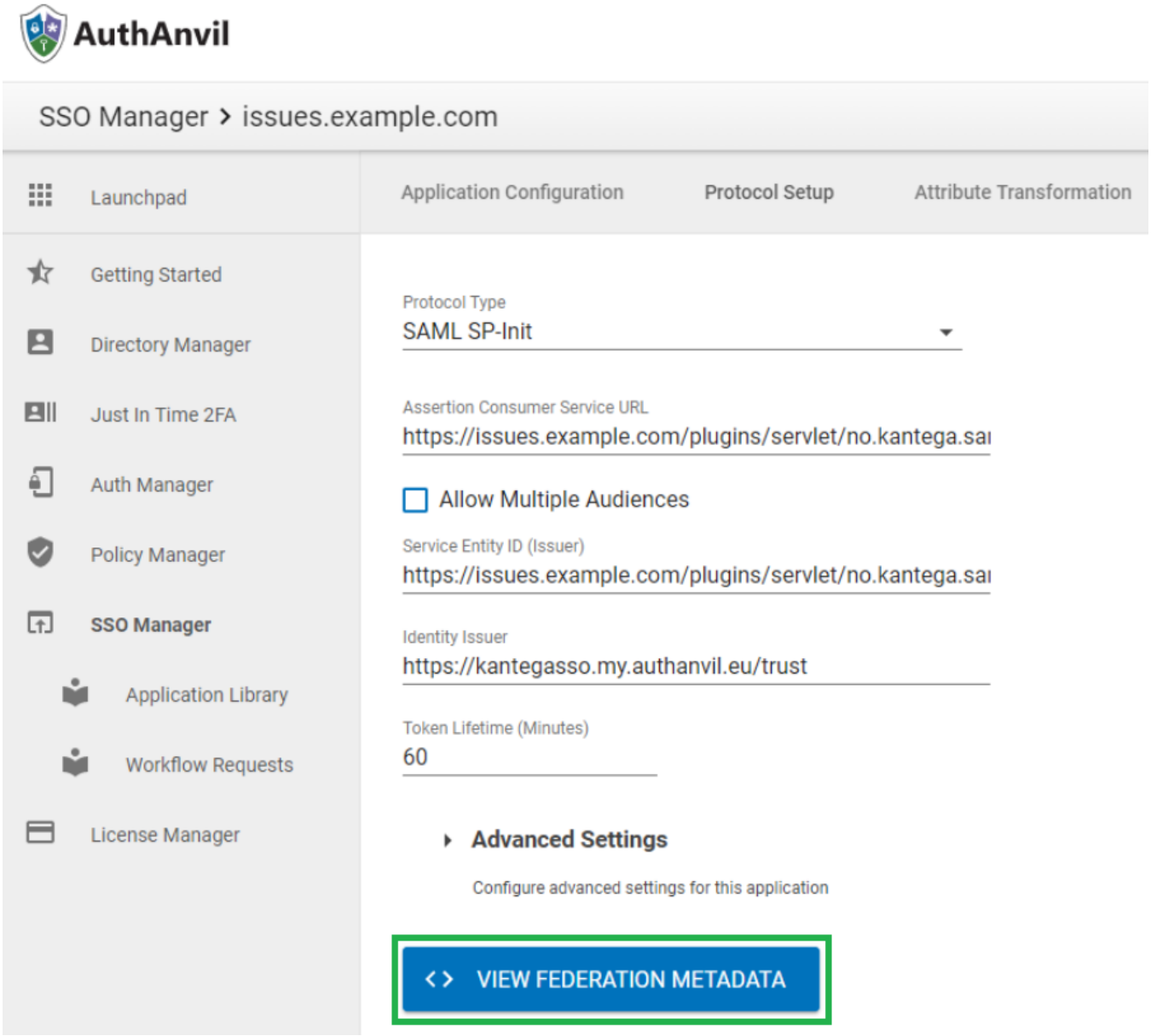
Select which users should be able to log into the SAML application.

- 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.



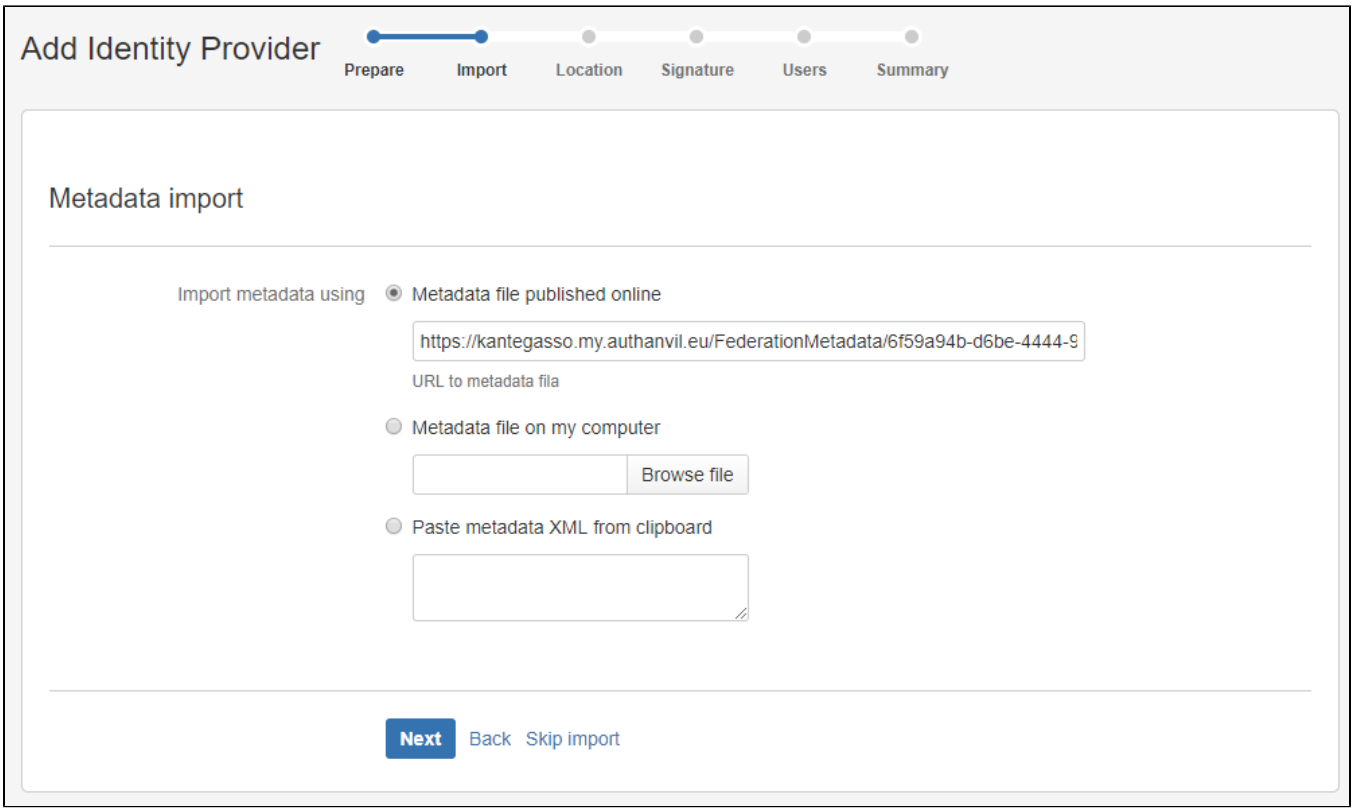
Federation Metadata

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



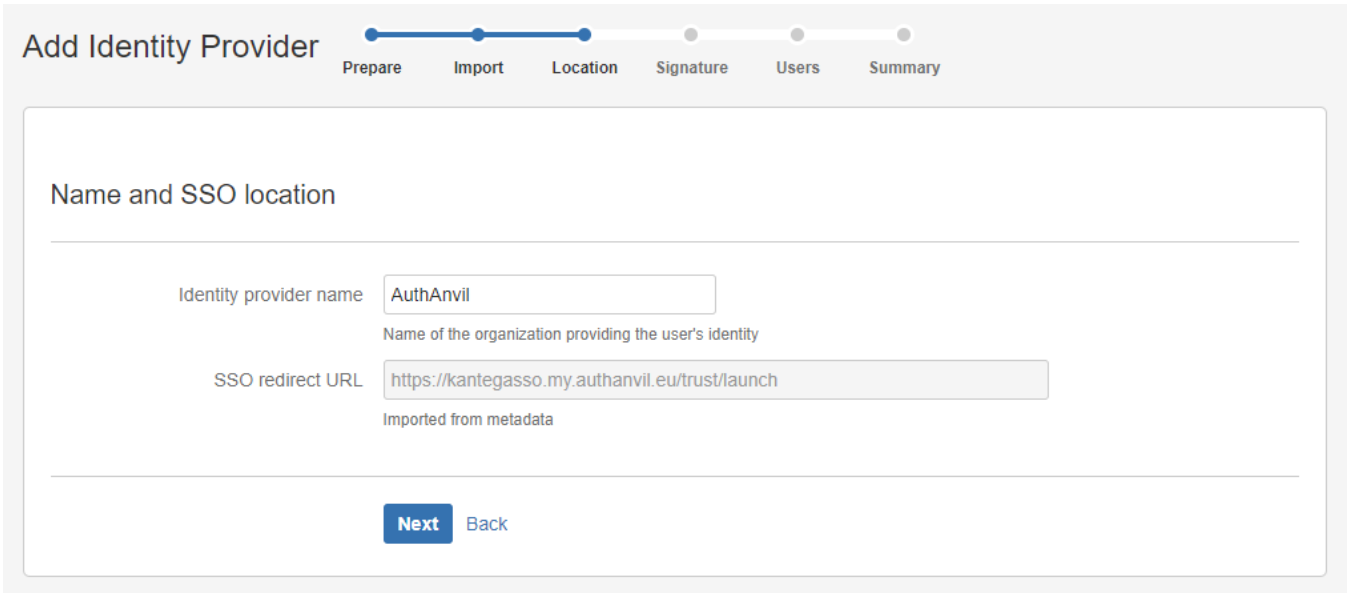
Metadata import

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



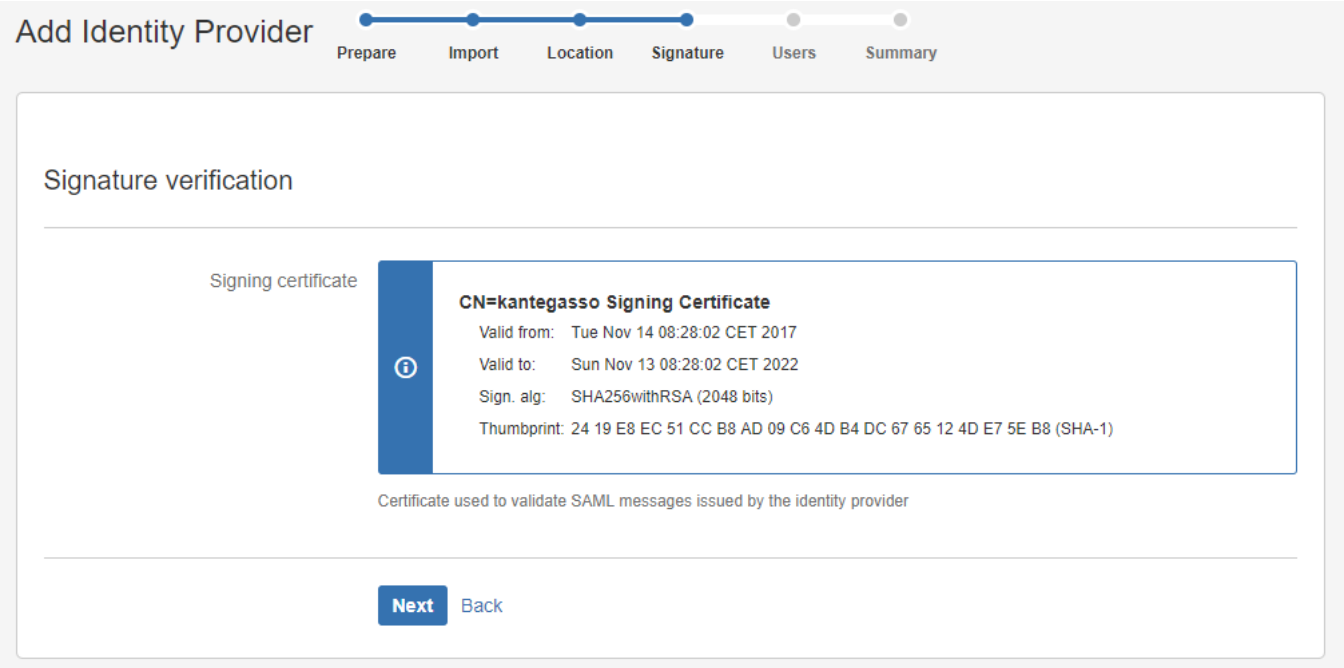
Location

- 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.



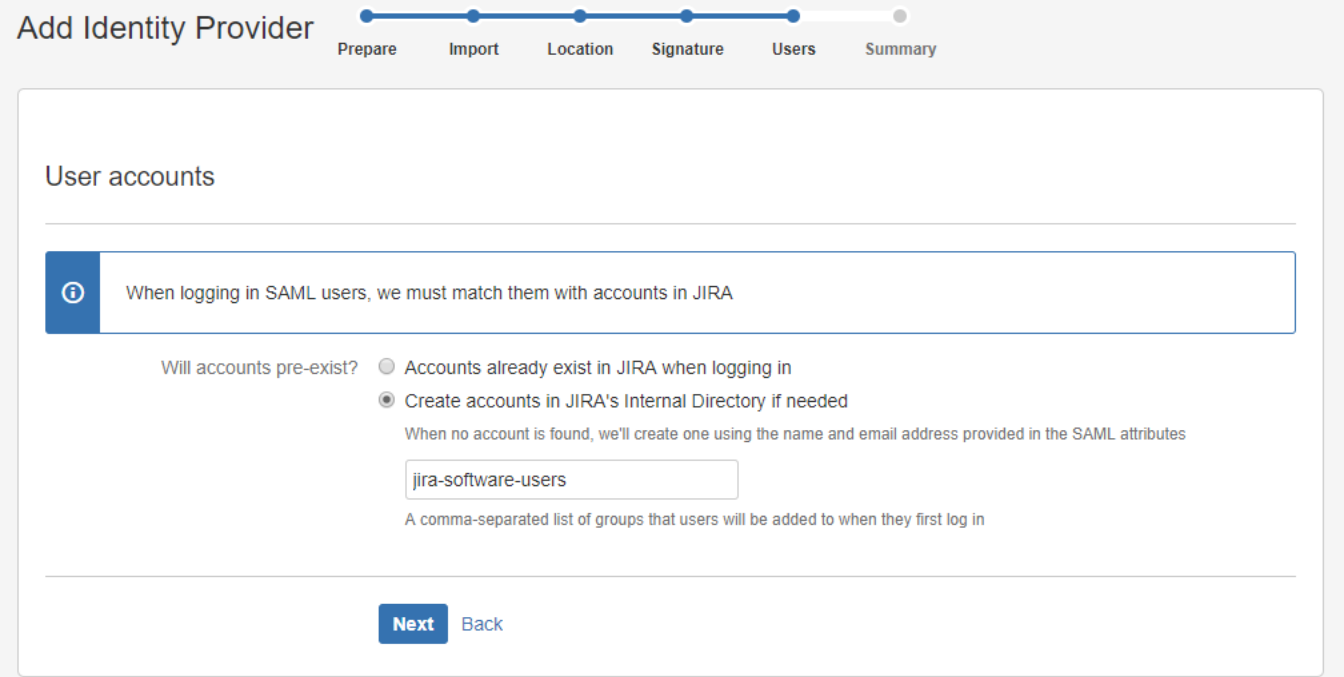
Signature

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



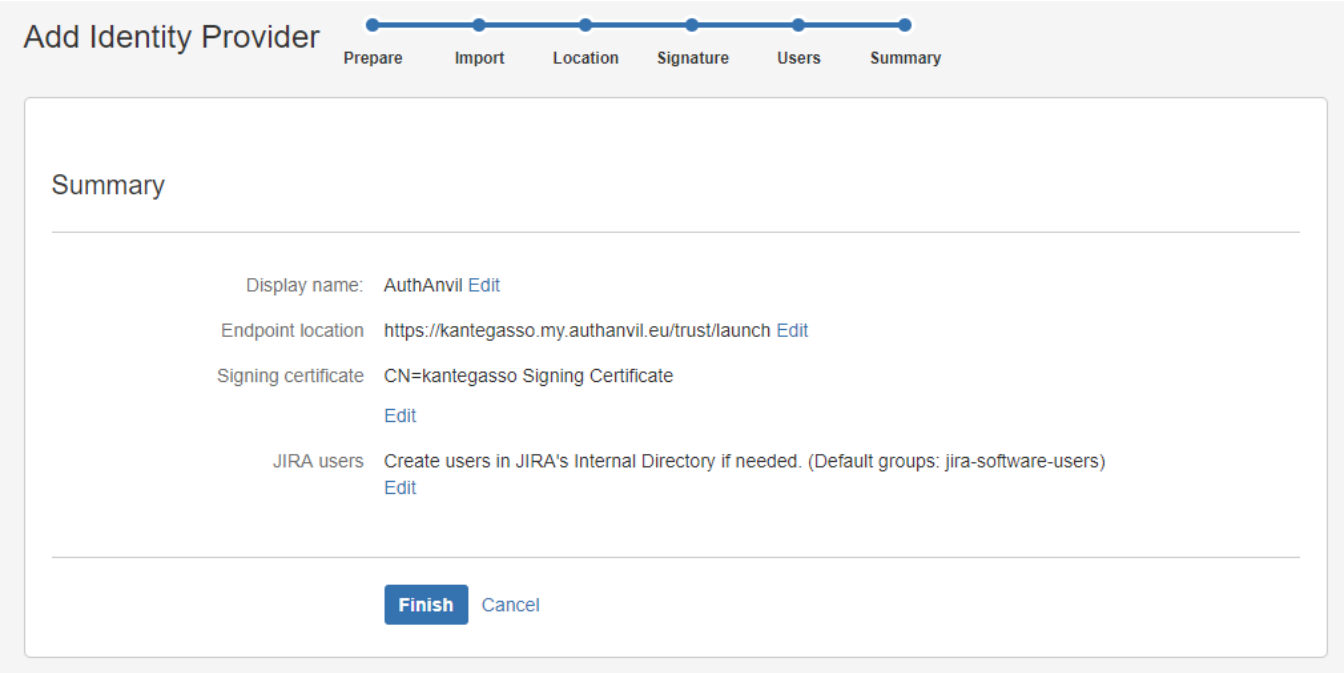
Users

- 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 insctrucions.)
- Optionally assign a default group for new users.



Summary

- Review the Summary.
- Press Finish.



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.