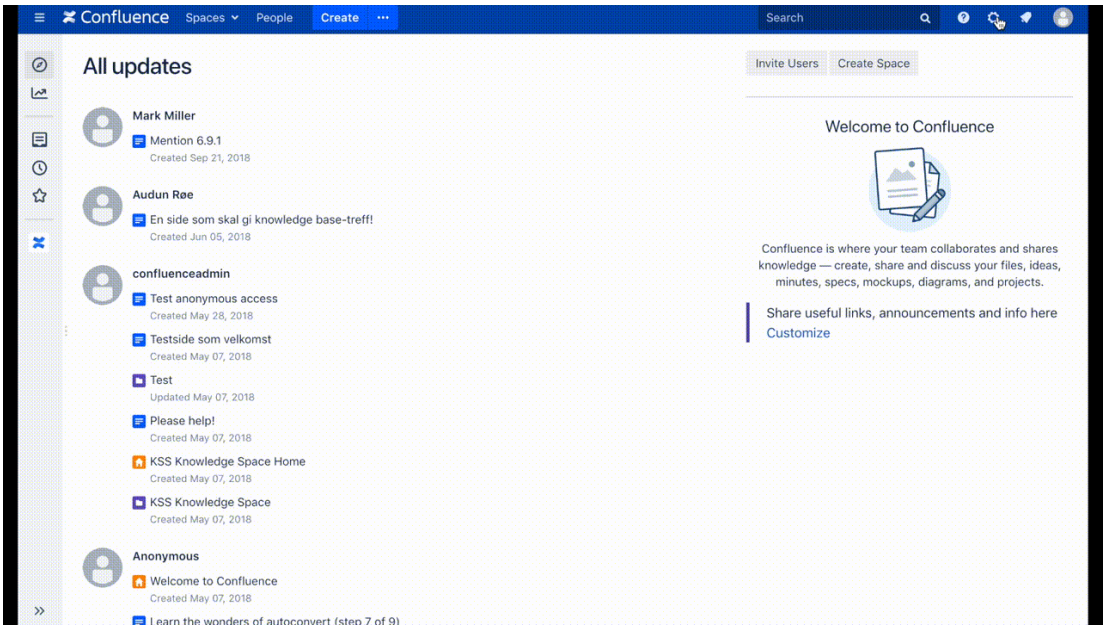
WSO2

Setup guide for adding WSO2 login to Atlassian server and datacenter products.

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

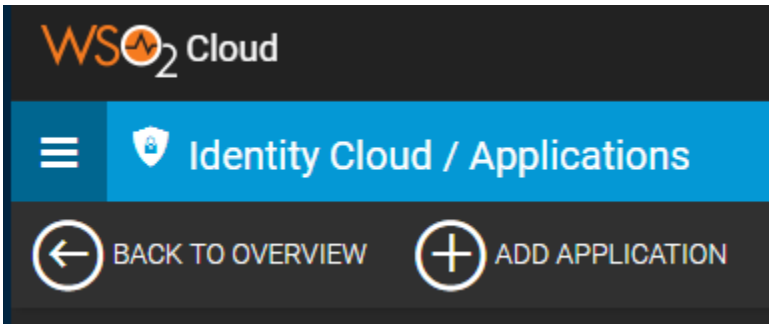
The setup starts in the Configuration page of the Kantega SSO add-on. This configuration page can be found by pressing "**Configure**" on "Kantega Single Sign-On (SSO)" in list of installed add-ons.



Add a new Application

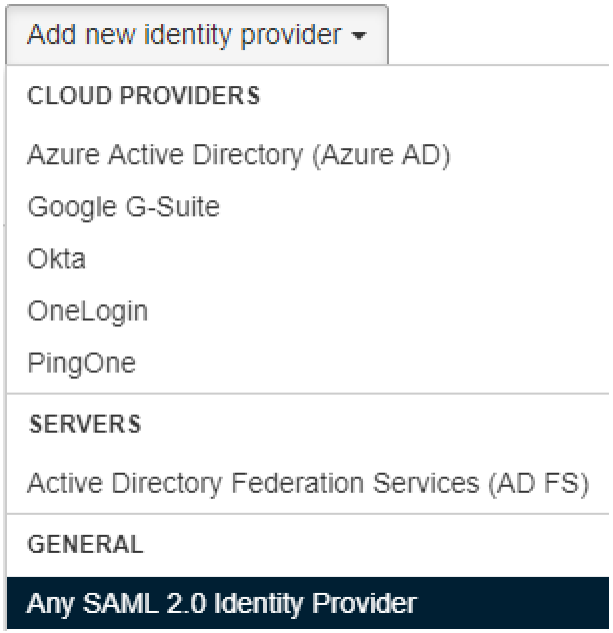
- Log into WS02

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



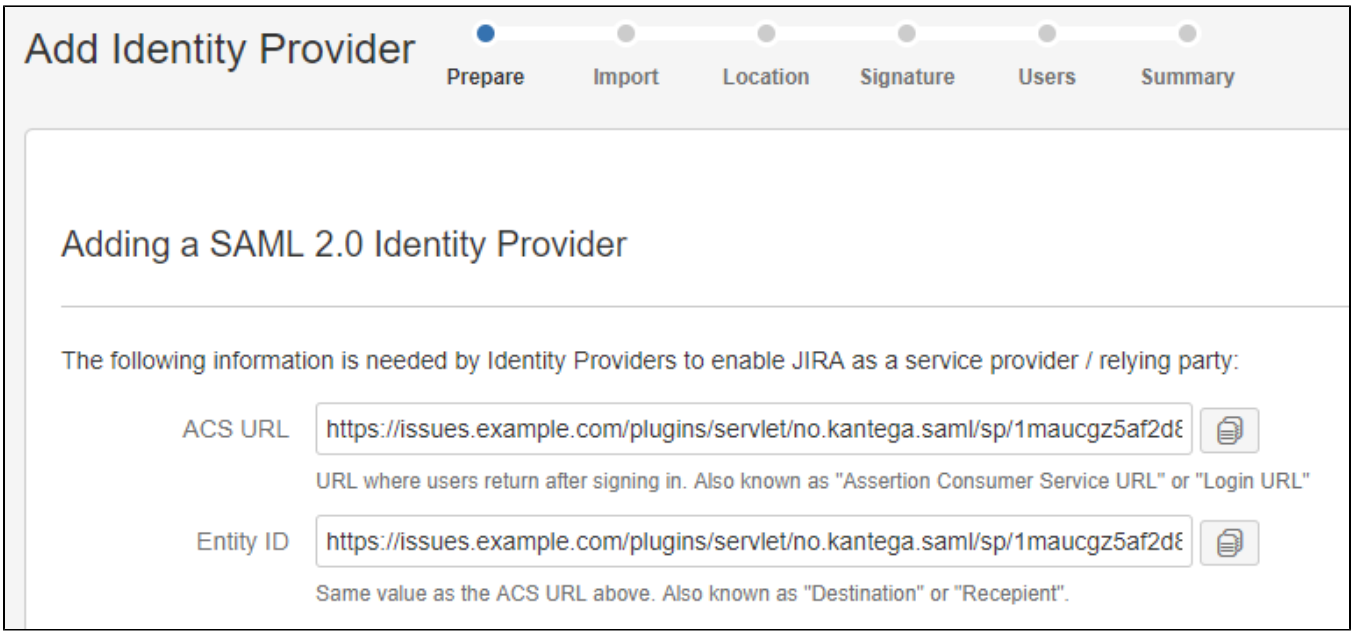
Adding an identity provider

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.



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 *

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

Assertion Consumer URLs*

Add

Default	Assertion Consumer URL	Action
(•)	https://issues.example.com/plugins/servlet/no.kantega.saml/sp/hfsj68gn8gq/login	Delete

[ ] Enable Response Signing

Show Advance Settings

Claim Configuration

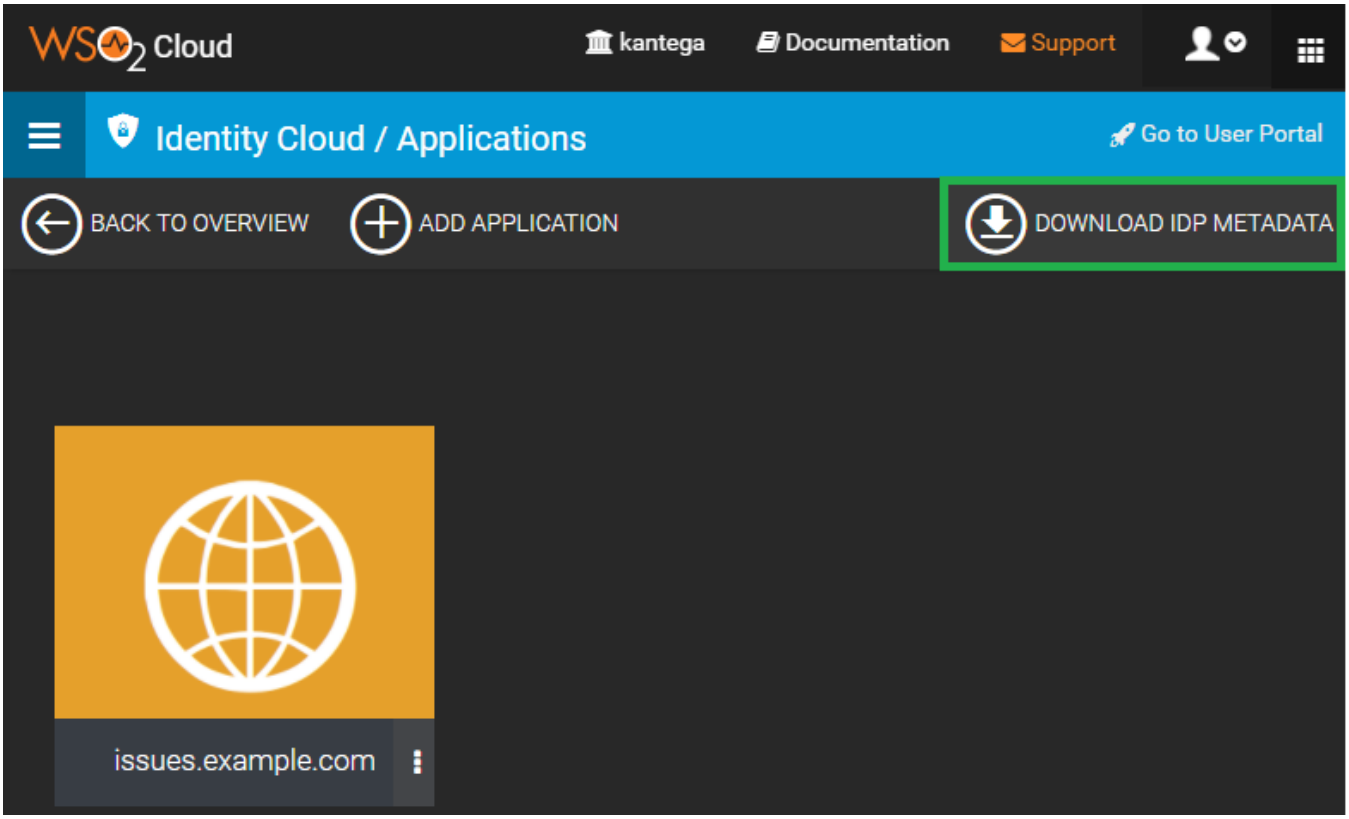
Configure User Claims

(•) Add Local Claims ( ) Add Custom Claims

http://wso2.org/claims/country ▾ Add Claim

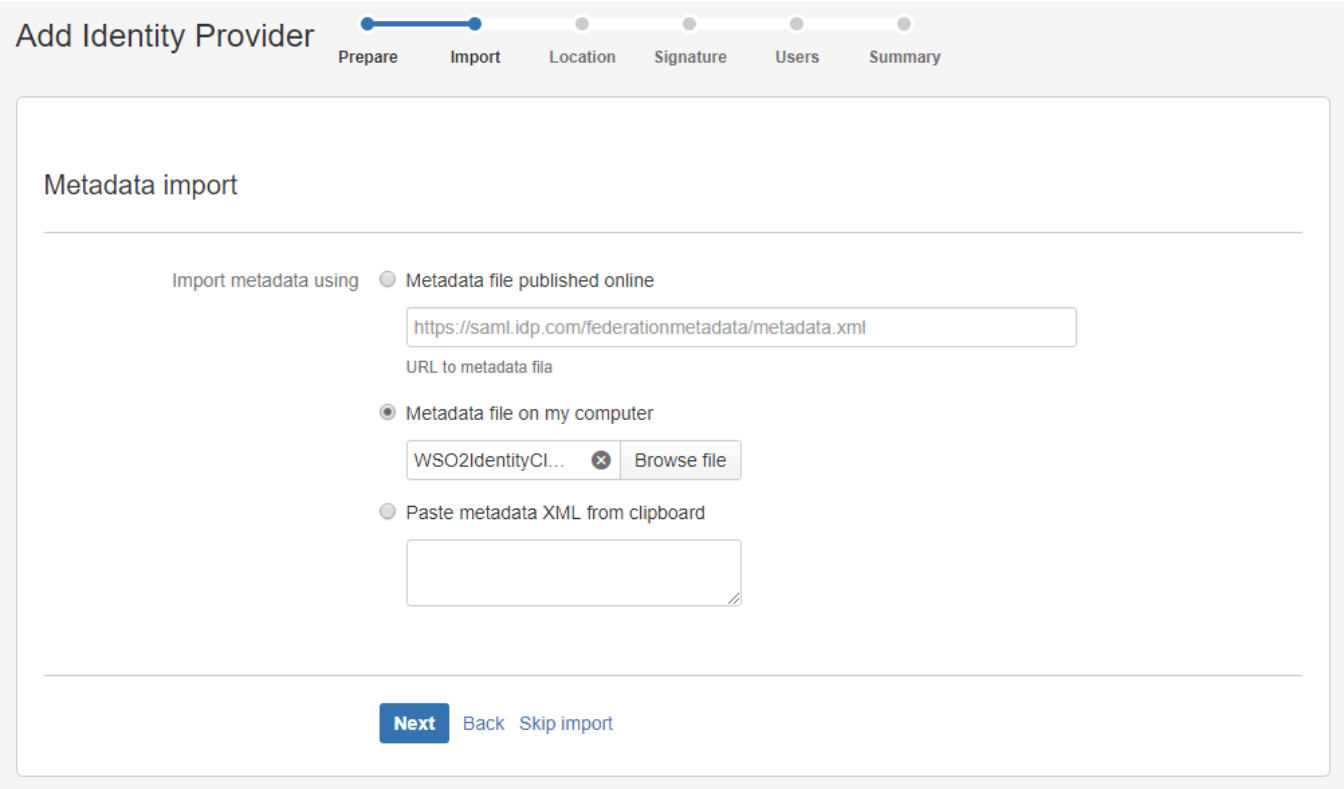
Download IDP Metadata

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



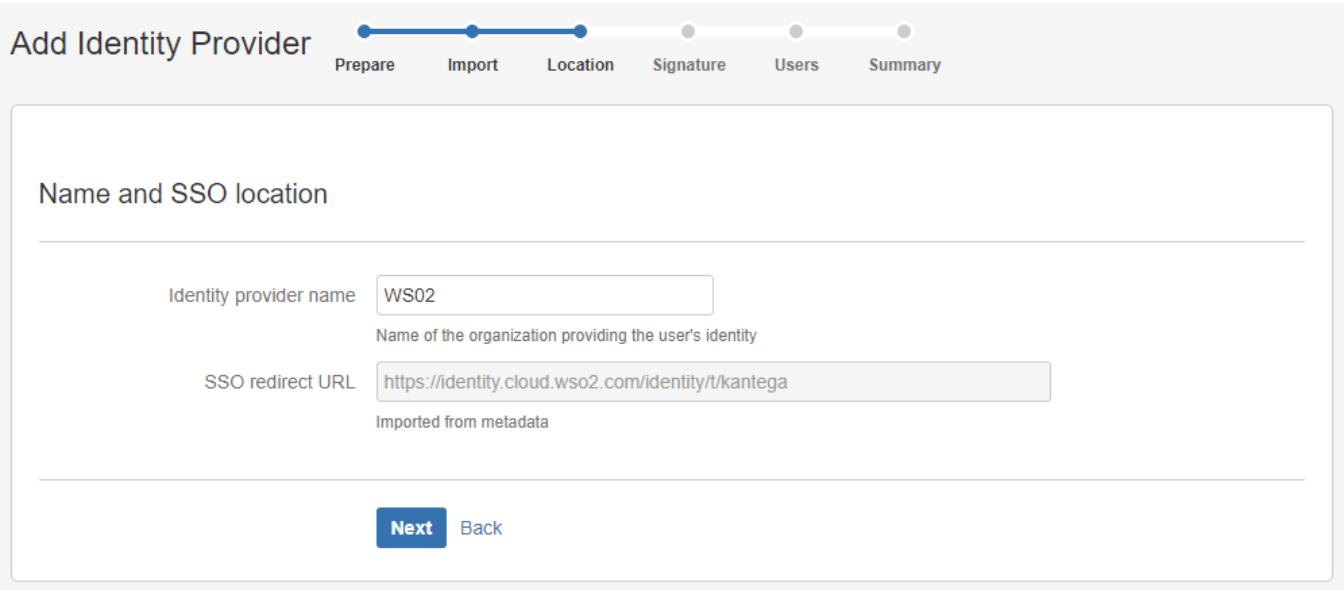
Metadata Import

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



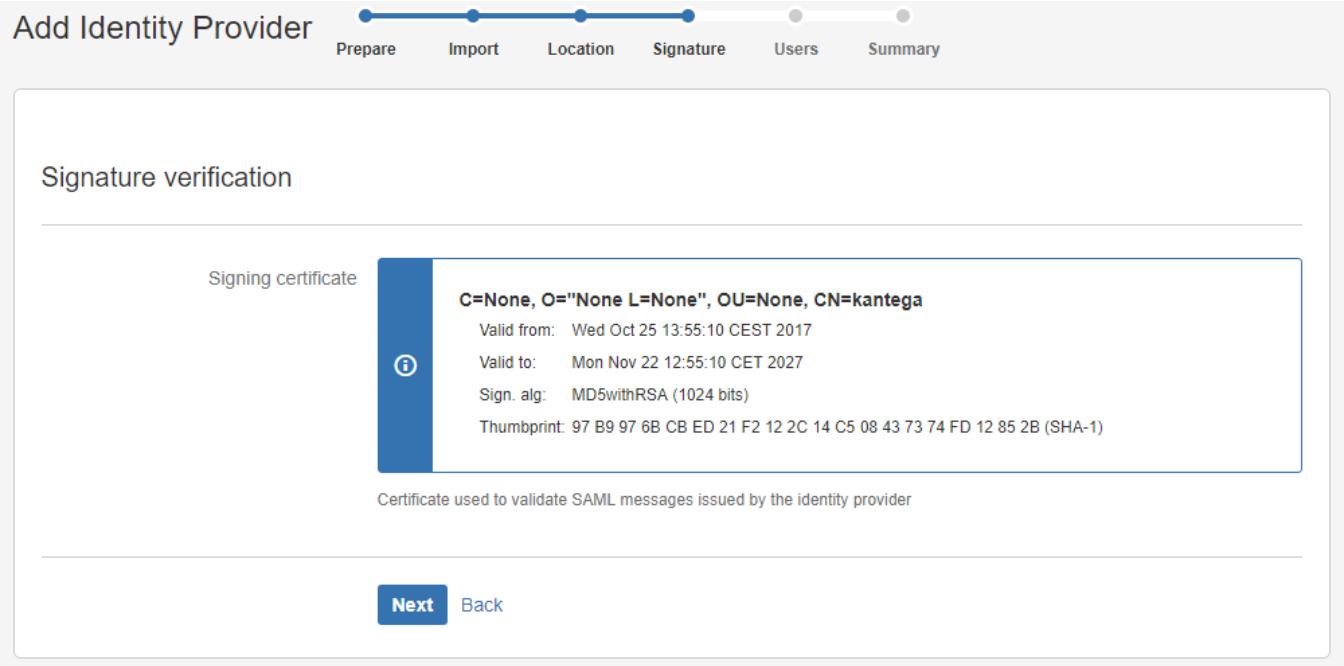
Location

- 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.



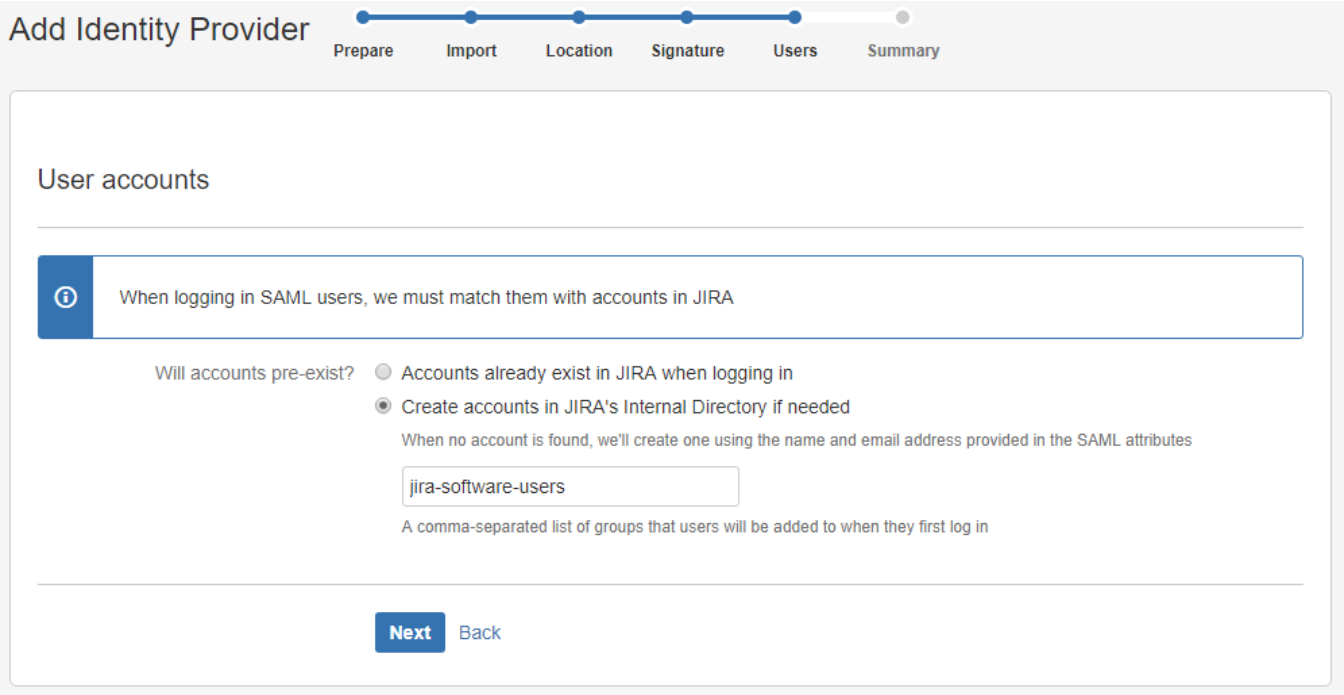
Signature

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



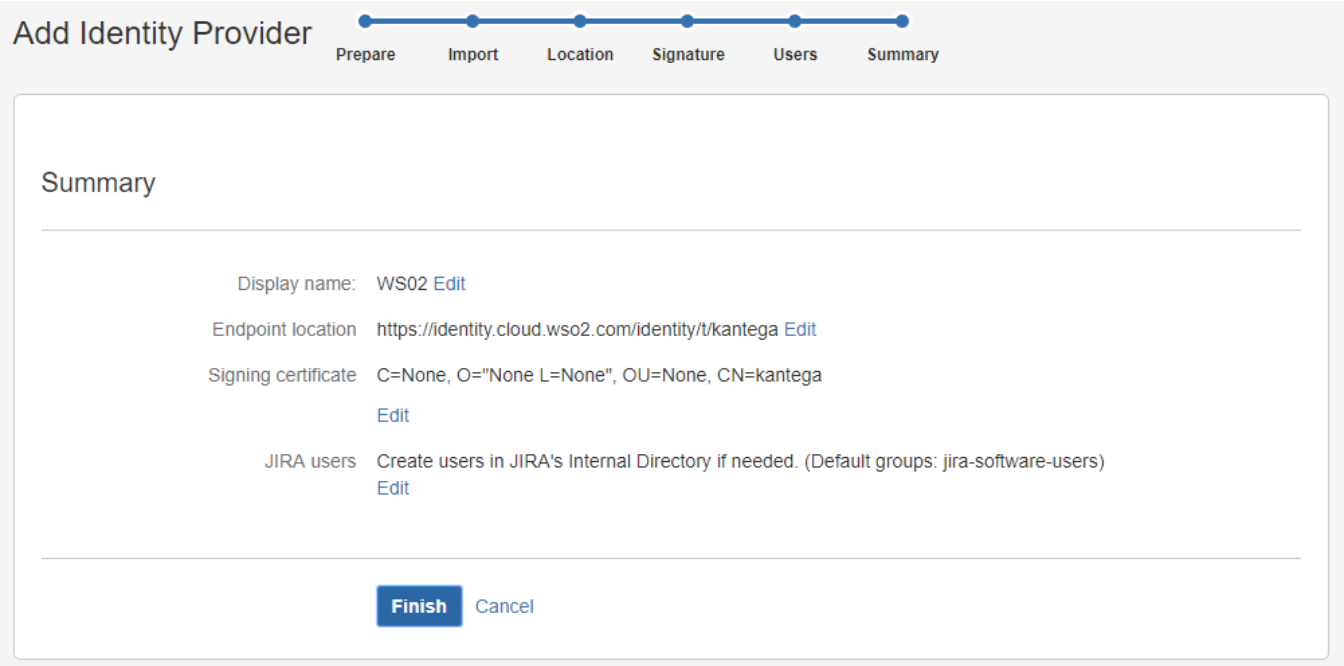
Users

- Select whether users already exist or if you wish to have users automatically created upon login.
- Optionally assign a default group for new users.



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.