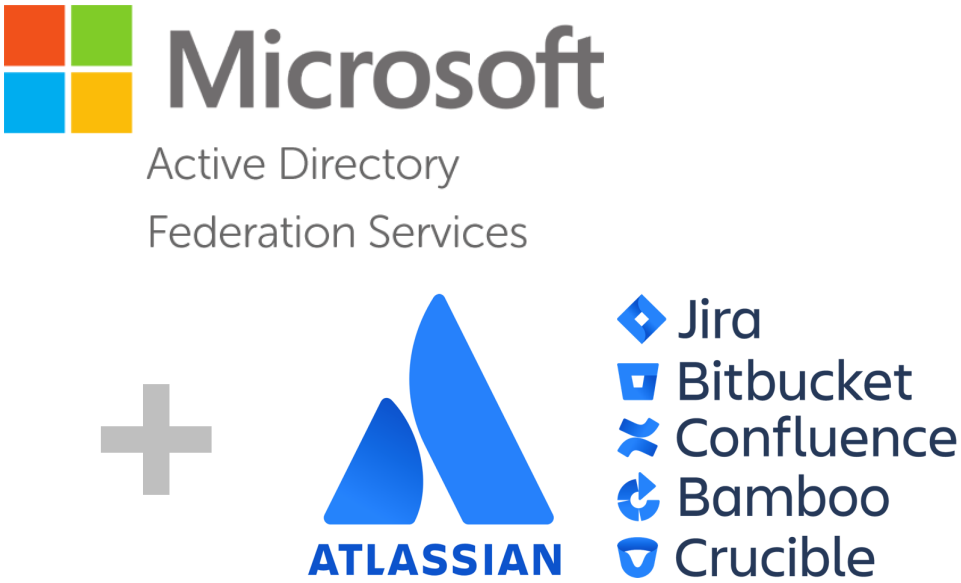
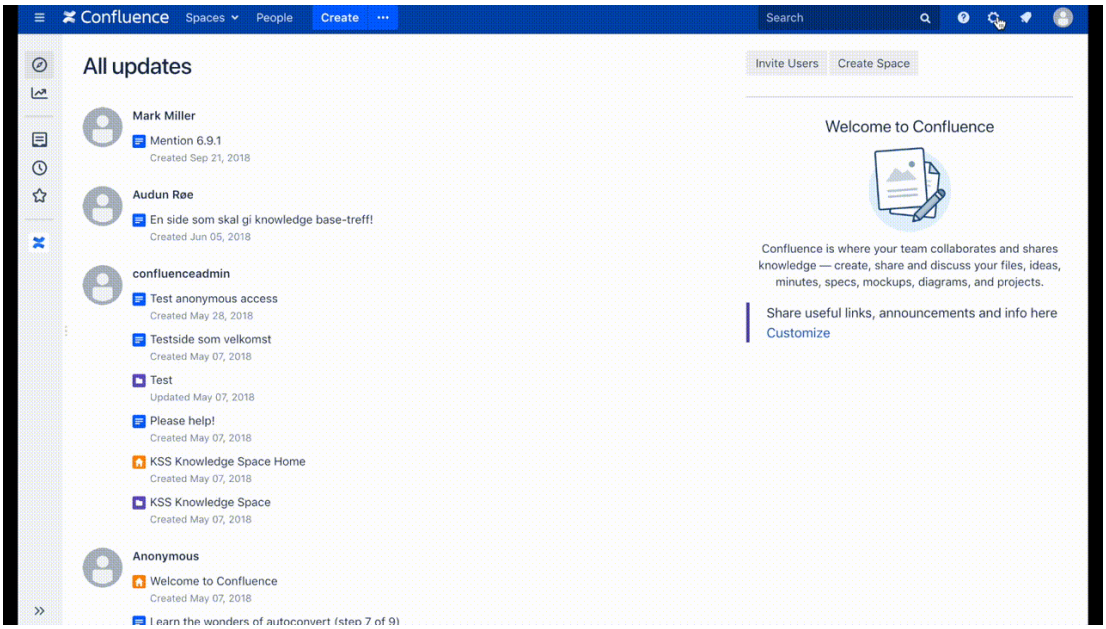
AD FS



Setup guide for adding Microsoft Active Directory Federation Services (AD FS) login to Atlassian server and datacenter products.

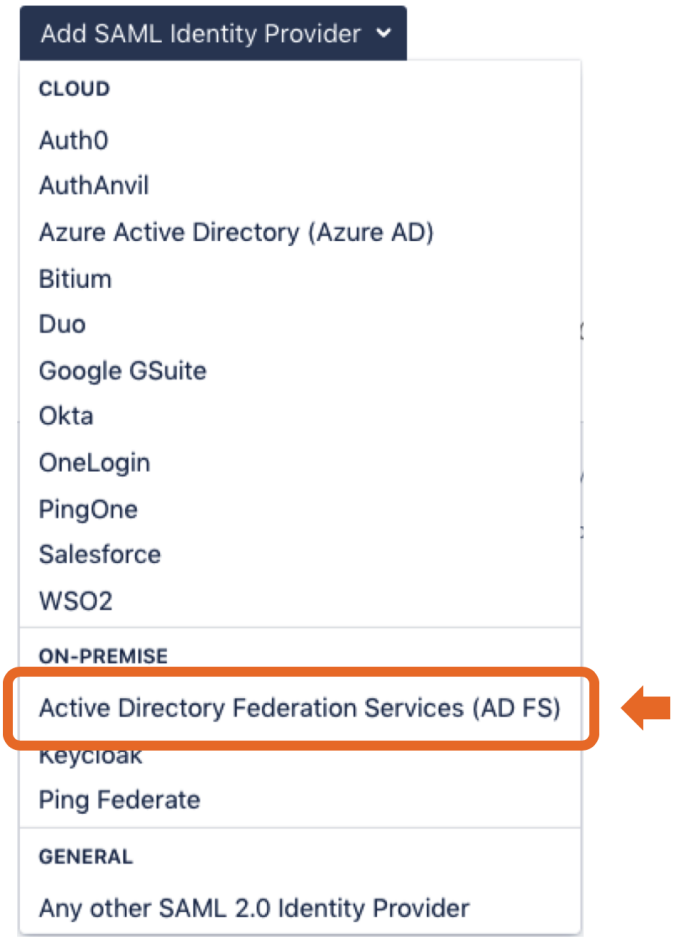
This setup guides assumes that Kantega SSO in installed as an add-on to your Atlassian product (Jira, Confluence, Bitbucket, Bamboo, or FeCru).

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.



1: Initiate setup

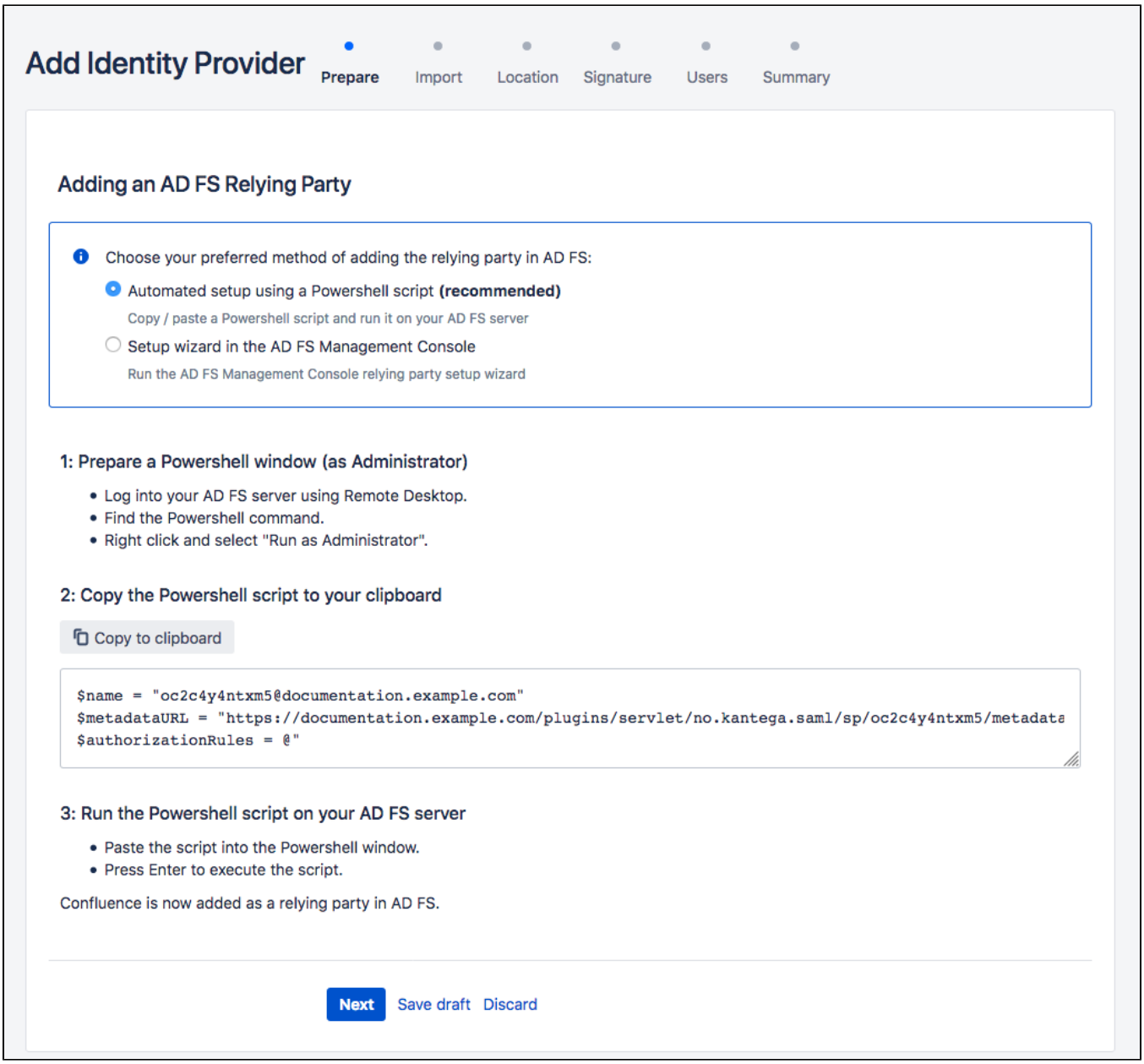
Click “Add SAML identity provider" and select "**Active Directory Federation Services (AD FS)**".



2: Prepare

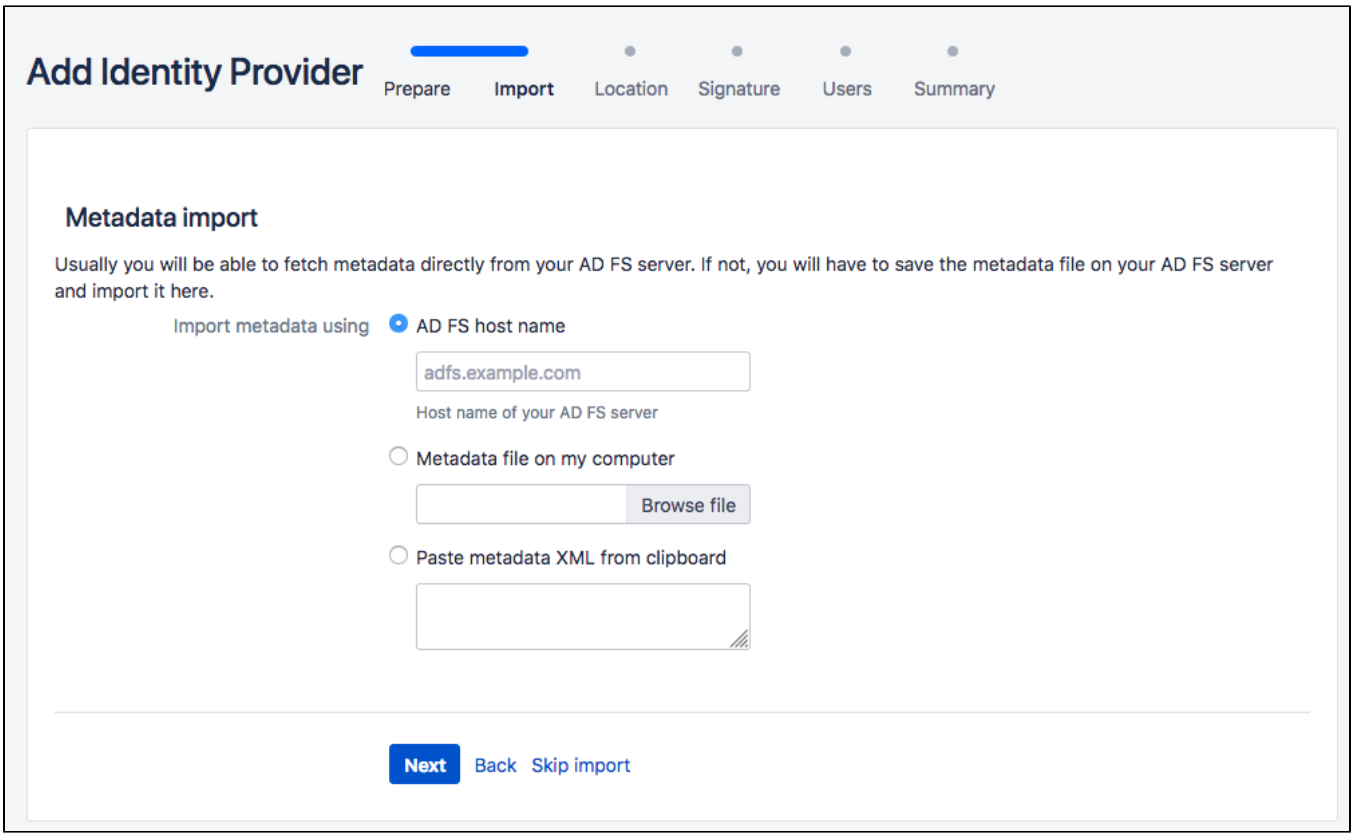
The easiest way to prepare AD FS is by using powershell. Simply copy the command and paste it into an elevated powershell window.

Make sure you are accessing the application using https.

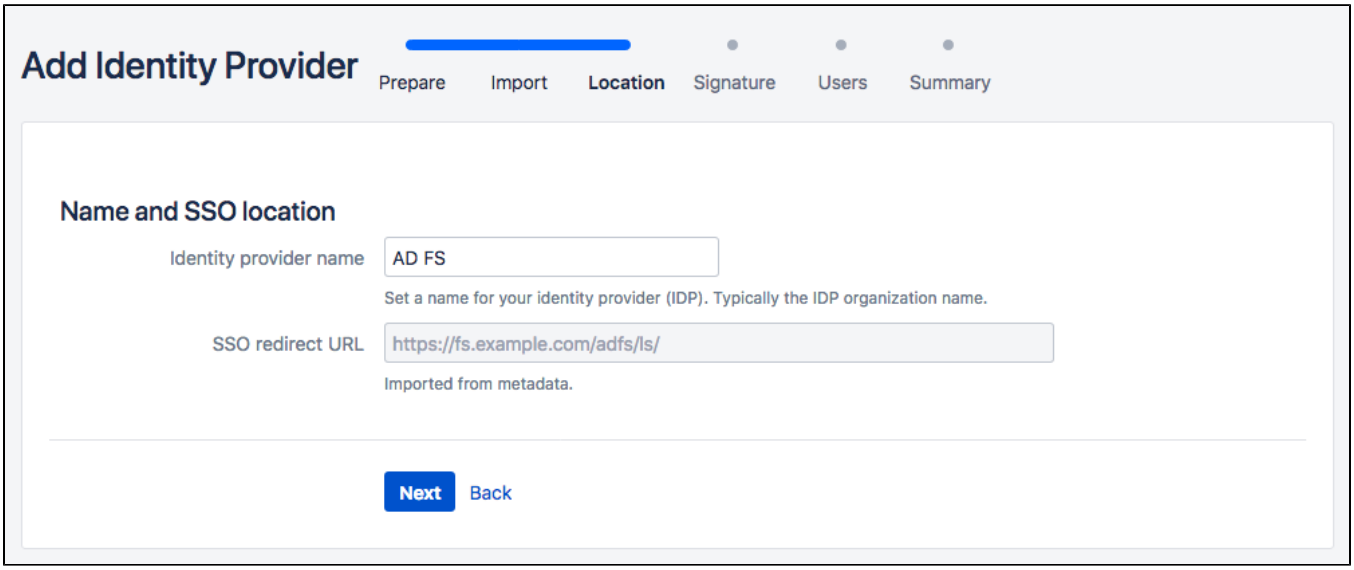


3: Import

Type the hostname of your AD FS server. Importing metadata by using the AD FS host name is recommended, as it allows for automatically updating certificates.

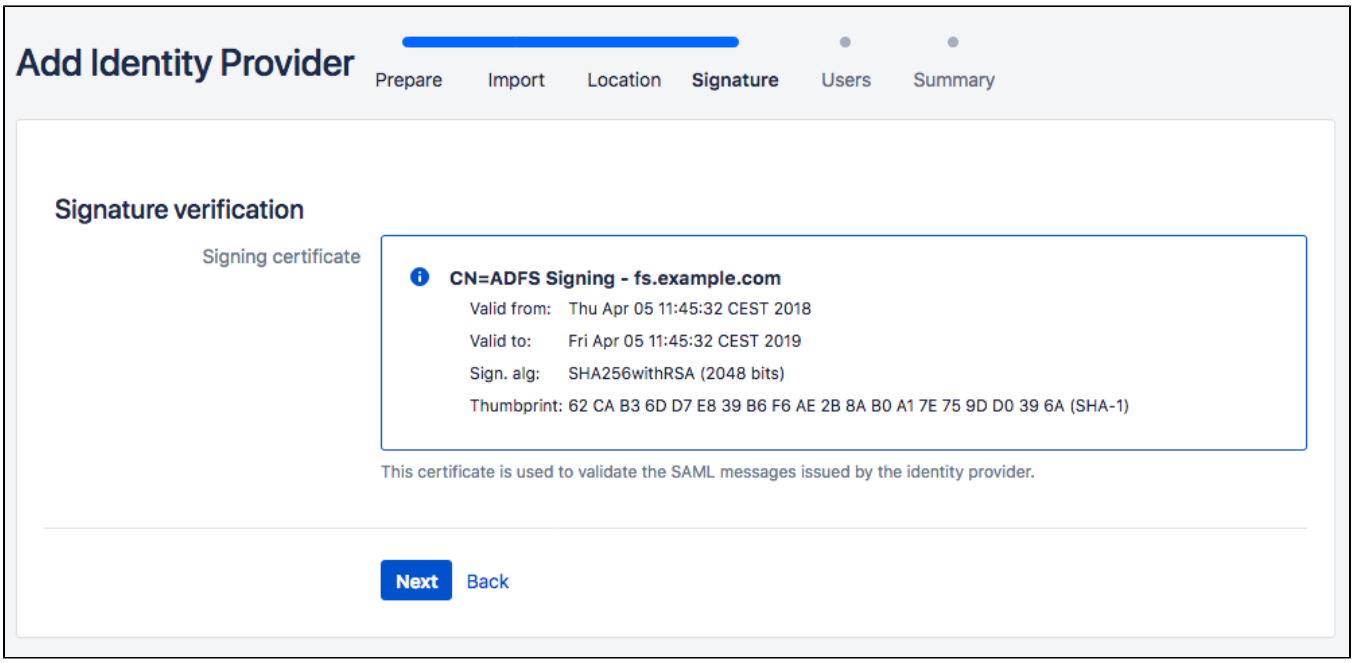


4: Give the SAML integration a name in the "Location" step.



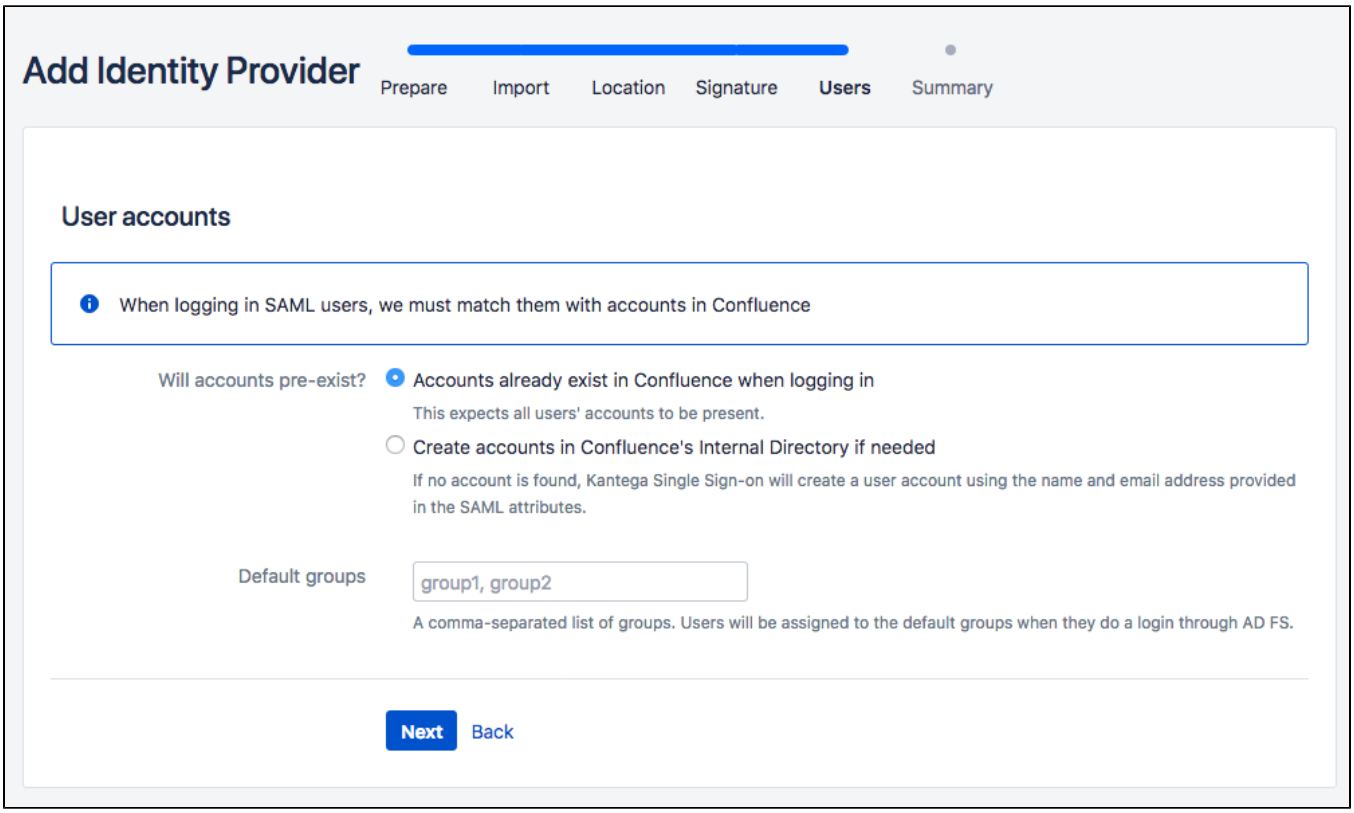
5: Verify signing certificate

The imported certificates from the AD FS server is presented.



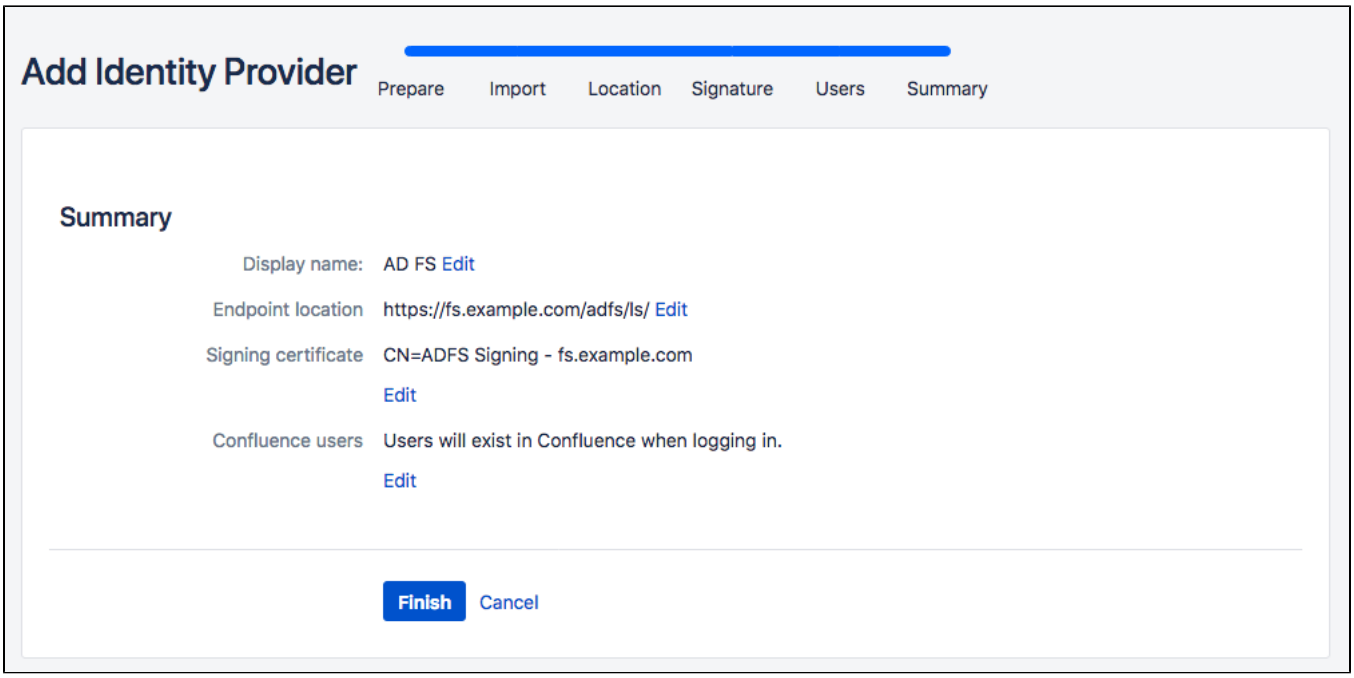
6: Specify whether authenticated users pre-exist or need to be created at login.

Here, you can also assign default group memberships to users at login. (Groups can also be assigned to individual users according to Group Claims in the SAML response during login. This is configured in the "Group membership" setting available after the setup wizard.



7: Summary

Review the IDP setup.



8: 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.