

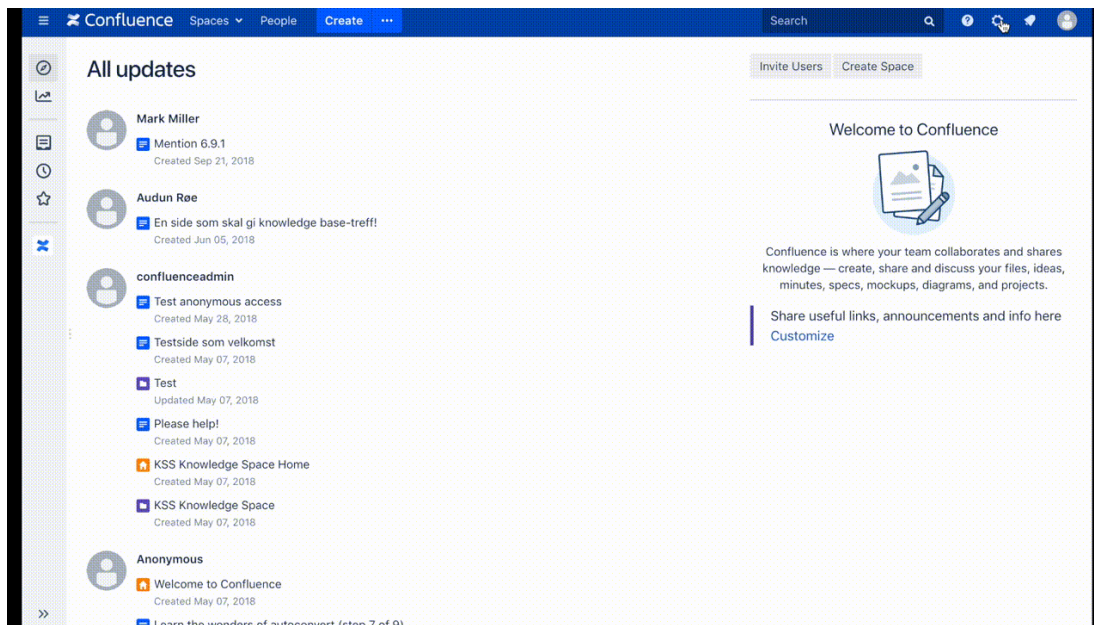
AD FS



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

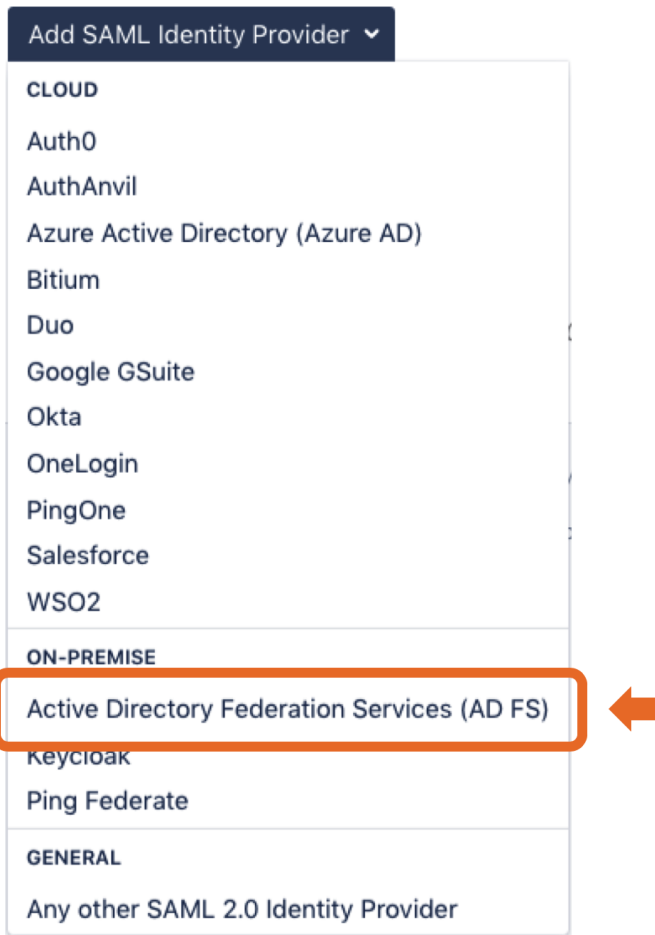
This setup guides assumes that [Kantega SSO](#) is installed as an add-on to your Atlassian product ([Jira](#), [Confluence](#), [Bitbucket](#), [Bamboo](#), or [FeCru](#)).

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.



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.

Add Identity Provider

Prepare

Import

Location

Signature

Users

Summary

Adding an AD FS Relying Party

Choose your preferred method of adding the relying party in AD FS:

Automated setup using a Powershell script (**recommended**)

Copy / paste a Powershell script and run it on your AD FS server

Setup wizard in the AD FS Management Console

Run the AD FS Management Console relying party setup wizard

1: Prepare a Powershell window (as Administrator)

- Log into your AD FS server using Remote Desktop.
- Find the Powershell command.
- Right click and select "Run as Administrator".

2: Copy the Powershell script to your clipboard

Copy to clipboard

```
$name = "oc2c4y4ntxm5@documentation.example.com"
$metadataURL = "https://documentation.example.com/plugins/servlet/no.kantega.saml/sp/oc2c4y4ntxm5/metadata"
$authorizationRules = @"
```

3: Run the Powershell script on your AD FS server

- Paste the script into the Powershell window.
- Press Enter to execute the script.

Confluence is now added as a relying party in AD FS.

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

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.

Add Identity Provider

Prepare Import Location Signature Users Summary

Metadata import

Usually you will be able to fetch metadata directly from your AD FS server. If not, you will have to save the metadata file on your AD FS server and import it here.

Import metadata using AD FS host name

Host name of your AD FS server

Metadata file on my computer

Paste metadata XML from clipboard

[Back](#) [Skip import](#)

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

Add Identity Provider

Prepare Import Location Signature Users Summary

Name and SSO location

Identity provider name

Set a name for your identity provider (IDP). Typically the IDP organization name.

SSO redirect URL

Imported from metadata.

[Back](#)

5: Verify signing certificate

The imported certificates from the AD FS server is presented.

Add Identity Provider

Prepare Import Location **Signature** Users Summary

Signature verification

Signing certificate

ⓘ CN=ADFS Signing - fs.example.com

Valid from: Thu Apr 05 11:45:32 CEST 2018

Valid to: Fri Apr 05 11:45:32 CEST 2019

Sign. alg: SHA256withRSA (2048 bits)

Thumbprint: 62 CA B3 6D D7 E8 39 B6 F6 AE 2B 8A B0 A1 7E 75 9D D0 39 6A (SHA-1)

This certificate is used to validate the SAML messages issued by the identity provider.

Next Back

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.

Add Identity Provider

Prepare Import Location Signature **Users** Summary

User accounts

ⓘ When logging in SAML users, we must match them with accounts in Confluence

Will accounts pre-exist?

Accounts already exist in Confluence when logging in
This expects all users' accounts to be present.

Create accounts in Confluence's Internal Directory if needed
If no account is found, Kantega Single Sign-on will create a user account using the name and email address provided in the SAML attributes.

Default groups
A comma-separated list of groups. Users will be assigned to the default groups when they do a login through AD FS.

Next Back

7: Summary

Review the IDP setup.

Add Identity Provider

Prepare Import Location Signature Users Summary

Summary

Display name: AD FS Edit

Endpoint location <https://fs.example.com/adfs/ls/> Edit

Signing certificate CN=ADFS Signing - fs.example.com
Edit

Confluence users Users will exist in Confluence when logging in.
Edit

Finish Cancel

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.