Setting up Single Sign On with ADFS

Last Modified on 06.08.2025

Single Sign-On is a convenient, yet secure way of authenticating a user. Most customers are already running an Identity Provider (IDP) that supports Single Sign-On through the SAML 2 protocol, e.g. Active Directory, OneLogin, or Okta.

Userlane can accept authentication via the SAML 2.0 Protocol.

Of the many implementations of this protocol, Microsoft Active Directory Federation Services (ADFS) is one of the most widespread. In this scenario, an ADFS server acts as the Identity Provider (IDP) and Userlane as the Service Provider (SP).

Requirements

- access to ADFS
- access to Userlane Portal

In order to configure the Single Sign-On for Userlane, follow these steps below:

1. Adding Userlane as a Service Provider (SP) to your IDP

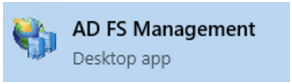
For the company's IDP to accept authentication requests by Userlane, the IT Admin must first register Userlane as a Service Provider (SP).

ℹ The Userlane Service Provider Metadata differs for each customer. Your Userlane SA will provide you with a .xml file to import into your ADFS Server.

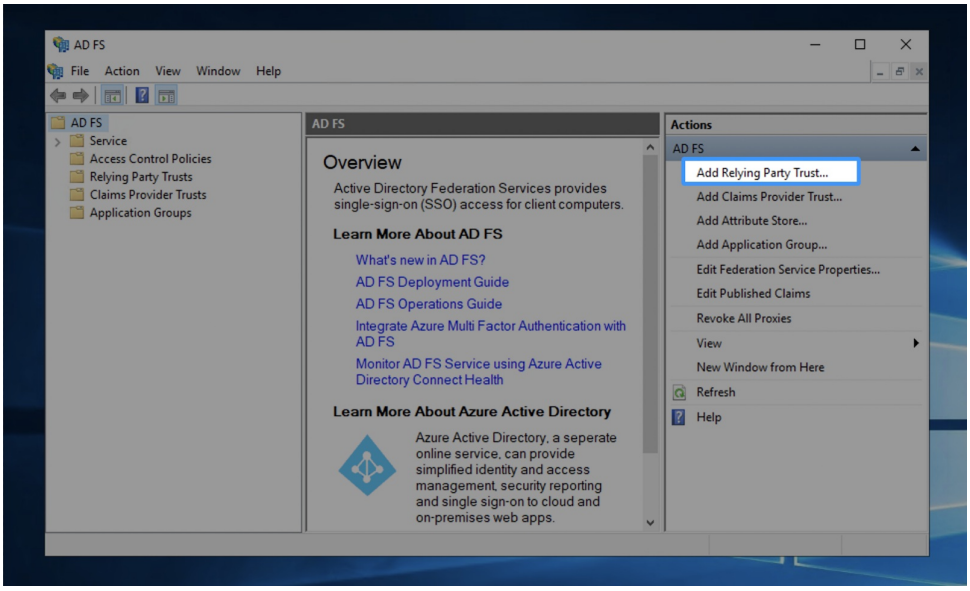
Registration steps:

1. Download the Metadata file onto your ADFS Server

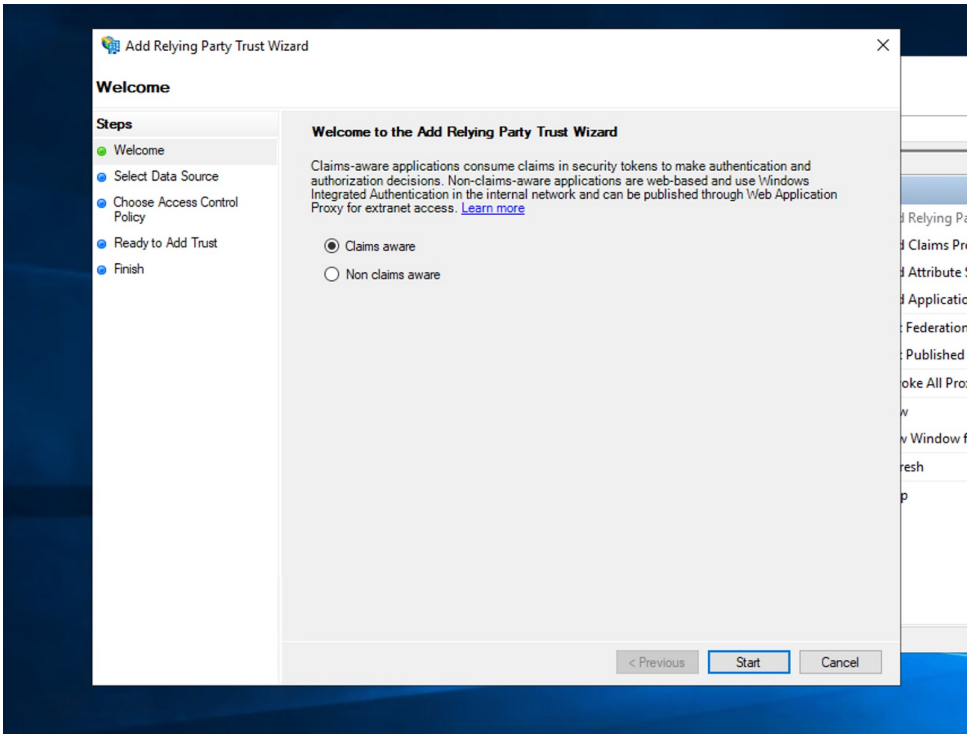
2. Open the "AD FS Management" app



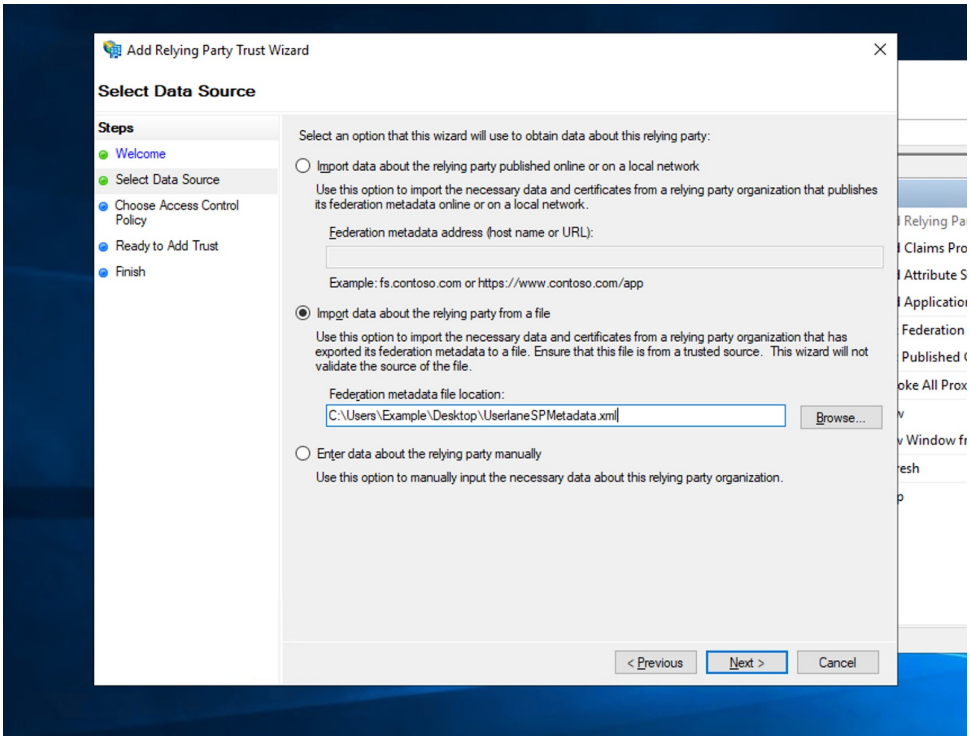
3. In the menu on the right, select "Add Relying Party Trust"



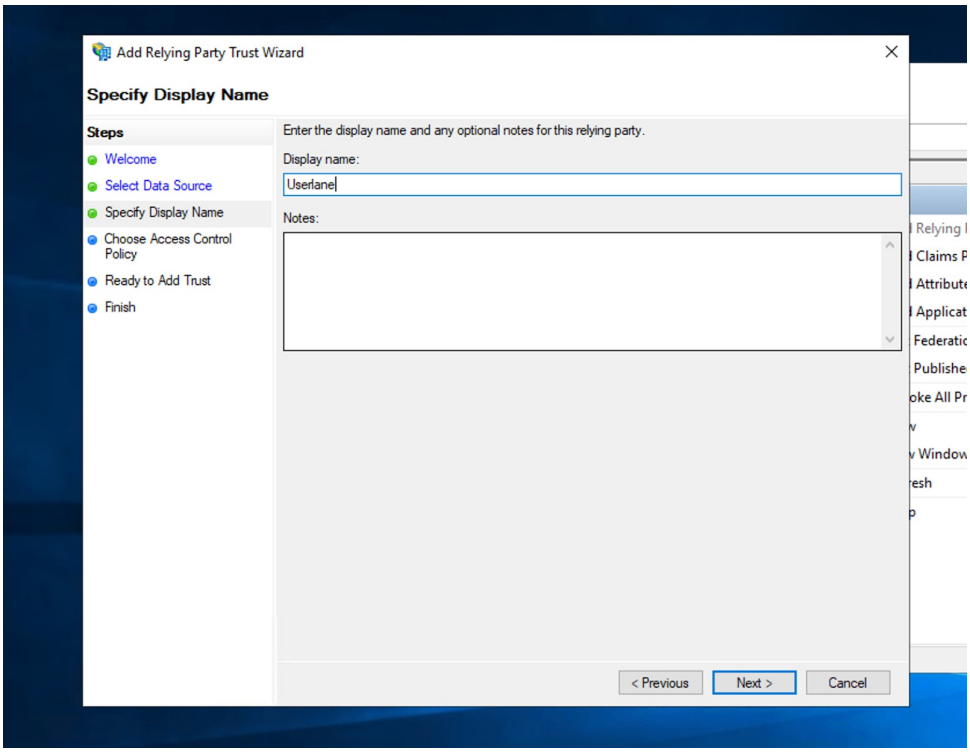
4. Select “Claims aware”



5. Select the Metadata file you’ve downloaded or follow the instructions for manual setup below



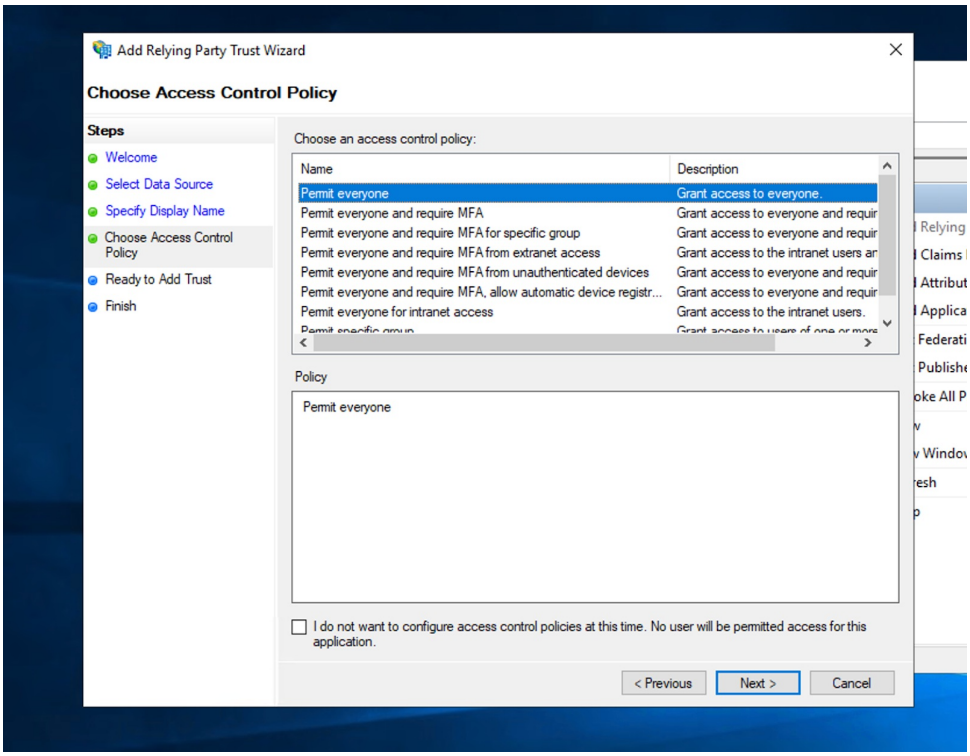
6. Specify any display name or description you like



7. It is essential to configure which employees are targeted for Userlane.
In general, any employee who has access to the connected application that uses Userlane for enablement purposes should also have access to the Userlane app. However, we recommend that App Owner confirms the target group after consulting with SA to avoid any misunderstanding.

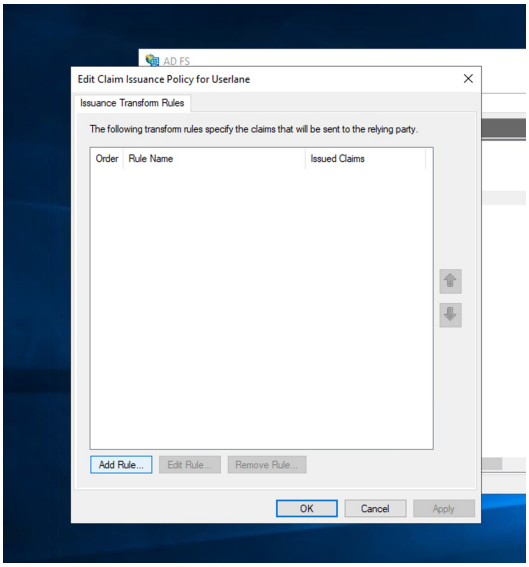
Note: Do not configure MFA (Multi-factor Authentication) as a requirement in order to make the sign-in easier

and seamless for your users.

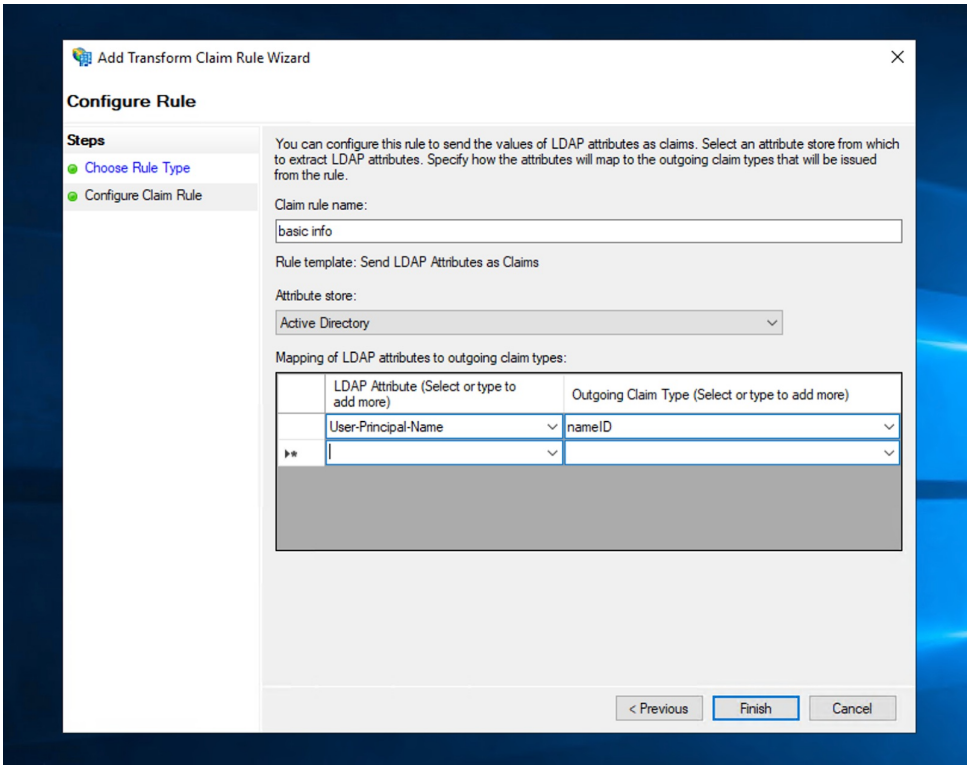


8. Confirm in order to add the Trust and continue with configuring a claims issuance policy for your application

8.1. Select “Add Rule”



8.2. Userlane requires a “nameID” (**please keep the exact letter-case form**) in the Outgoing Claim Type. This will be the unique identifier on Userlane level and it is the only mandatory attribute required. This ID must be unique for each user and is not meant to be changed over time in order to keep historical information clean.



Additional user information required by App Owner for improved targeting is explained in the article Expanding the Settings

Save and apply the Claim Rule.

2. Add information to Userlane Portal

Continue with step 3 from the article on setting up SSO for Userlane.