Configure TitanFile SSO with ADFS

Last updated: 2020-01-02

Overview

TitanFile can be configured to integrate with Active Directory (AD) to provide single sign-on (SSO) capability to users with AD credentials in your organization. TitanFile's SSO is supported through the Security Assertion Markup Language (SAML). A SAML-based identity federation service needs to run within your network. When your users attempt to login their requests are redirected to your Active Directory. The same SAML-based identity federation service can be used to provide SSO to multiple applications. If you already use such a service with another application, you can use the same service for TitanFile.

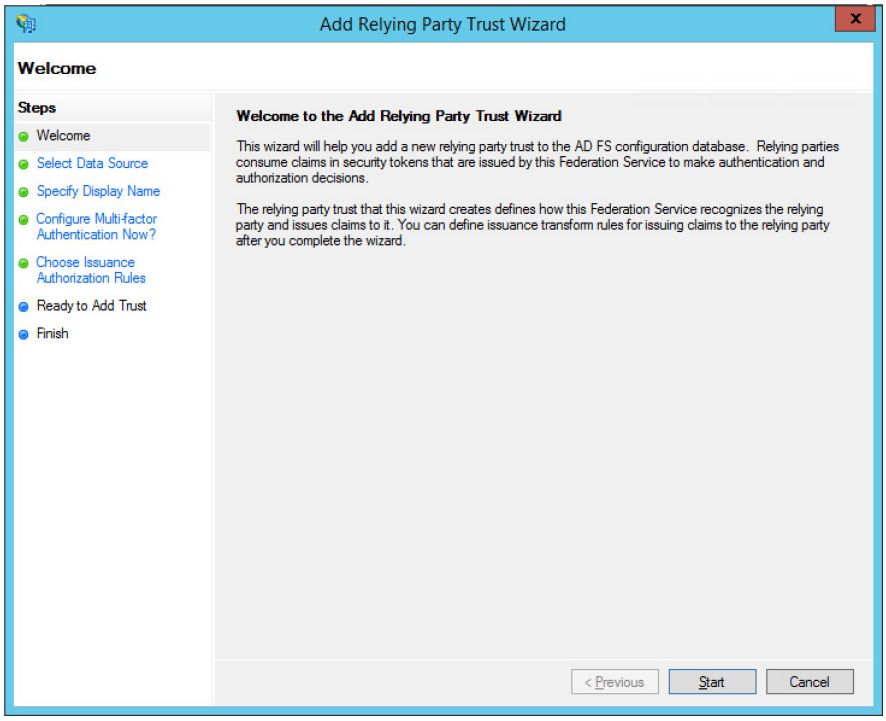
Configuring the SAML-based identity federation service

You will need the following information when configuring your SAML-based identity federation service:

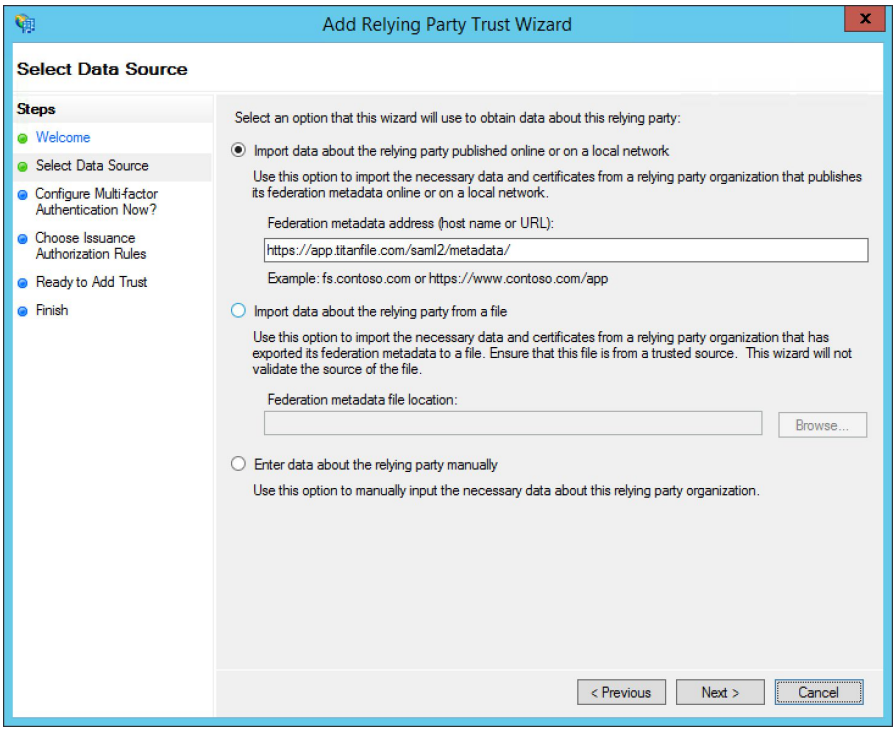
- Your TitanFile subdomain: subdomain.titanfile.com
- SAML assertion consumer service URL: https://subdomain.titanfile.com/saml2/acs/
- SAML single logout service URL: https://subdomain.titanfile.com/saml2/ls/ (optional)
- Application name: TitanFile

Here are the detailed steps to do this.

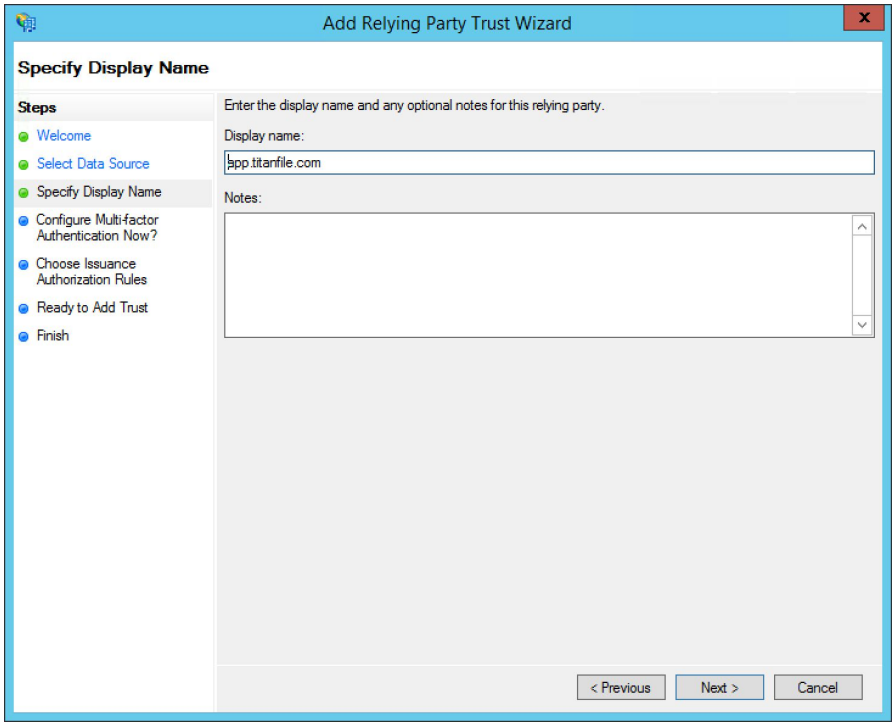
1. In the ADFS Management Console, expand “Trust Relationships”, go to “Relying Party Trusts” and select “Add Relying Party Trust…”



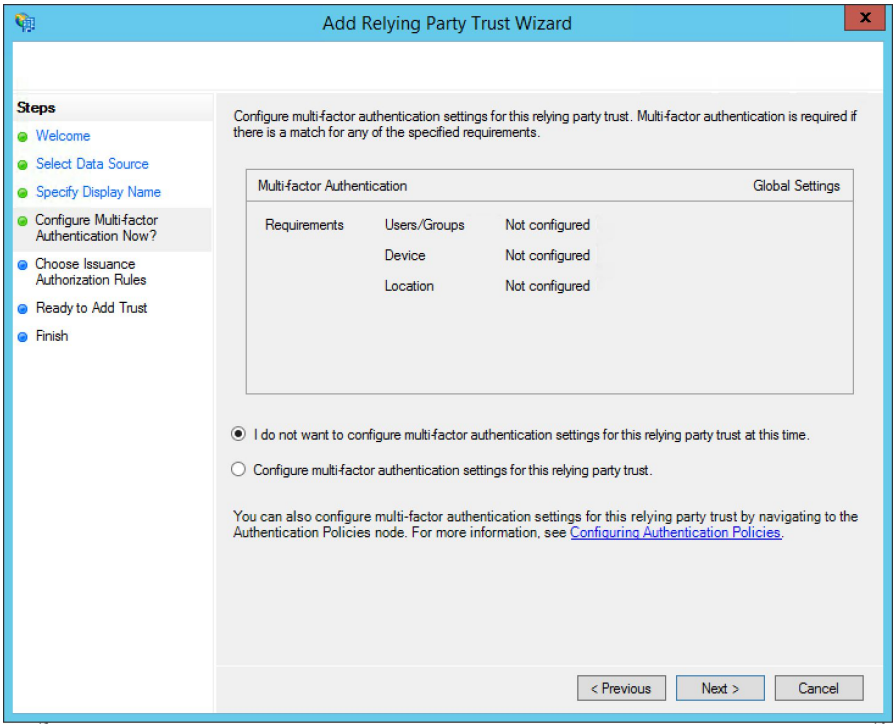
2. Press start and enter the TitanFile metadata URL: https://subdomain.titanfile.com/saml2/metadata/



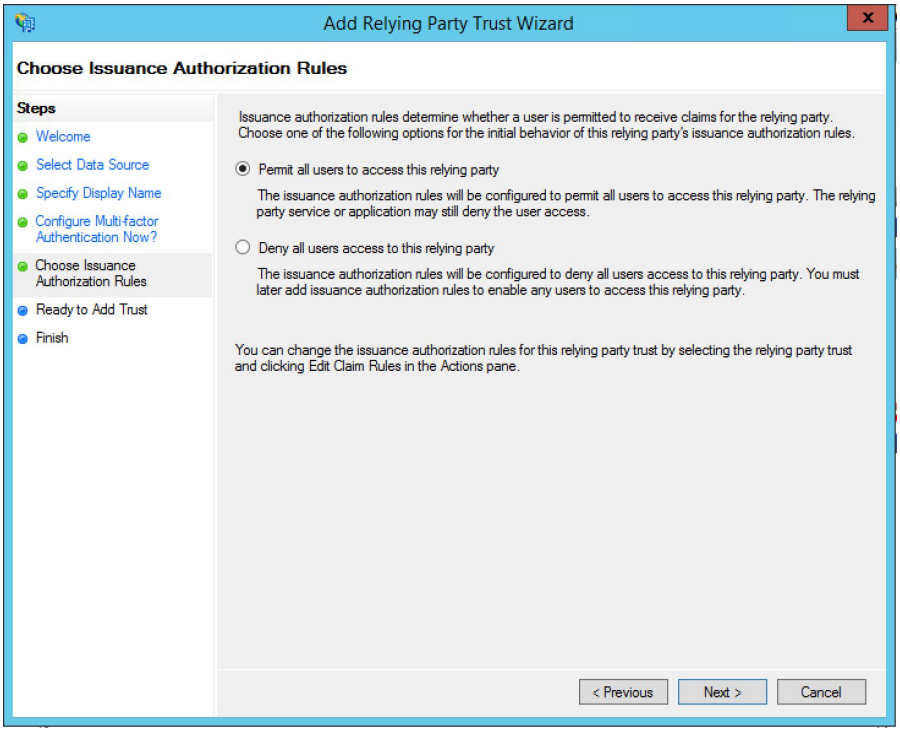
3. Specify a display name or keep the default.



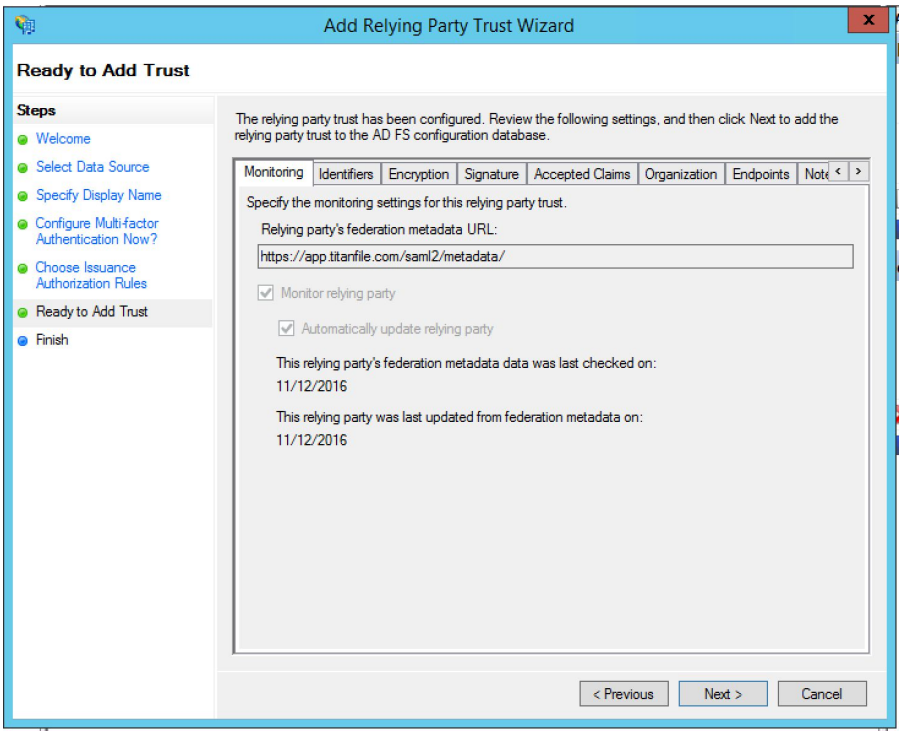
4. Keep default multi-factor authentication settings.



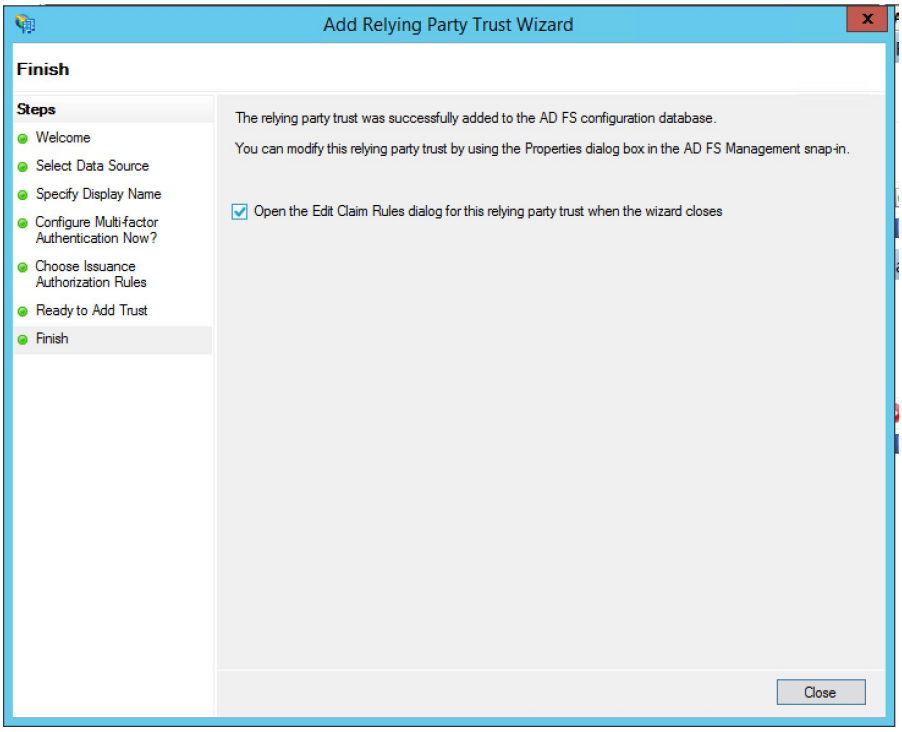
5. Set desired authorization rules. Either permit all user to access this relying party or configure permissions for each user/role separately.



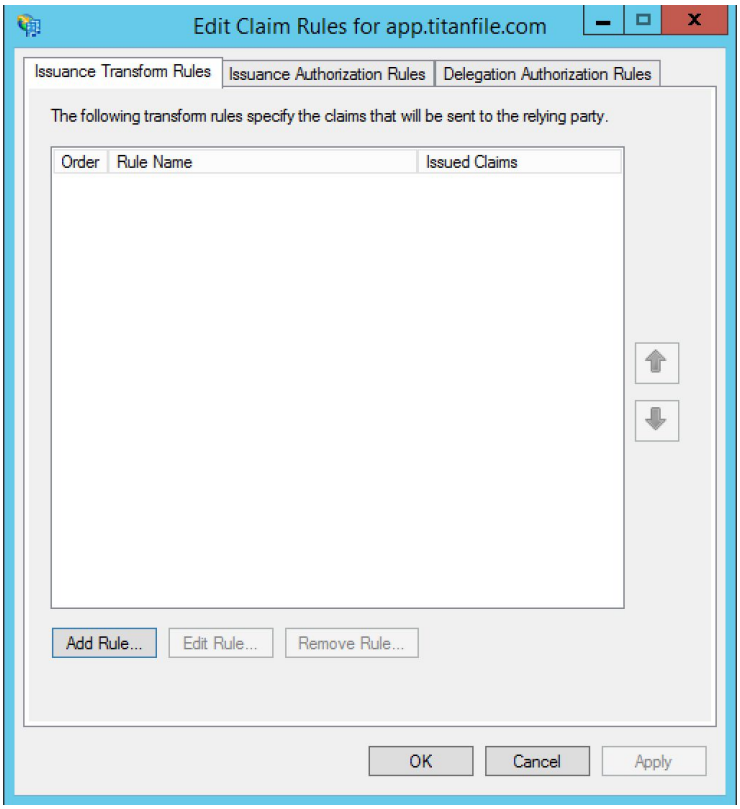
6. Review settings, go back to adjust if needed.



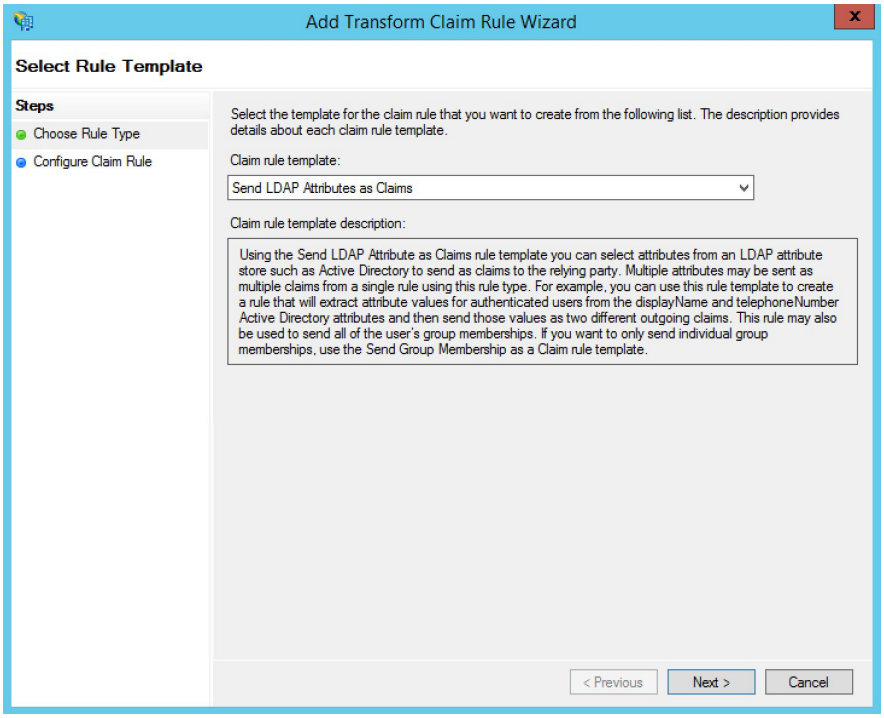
7. All set and ready to configure the Claim Rules.



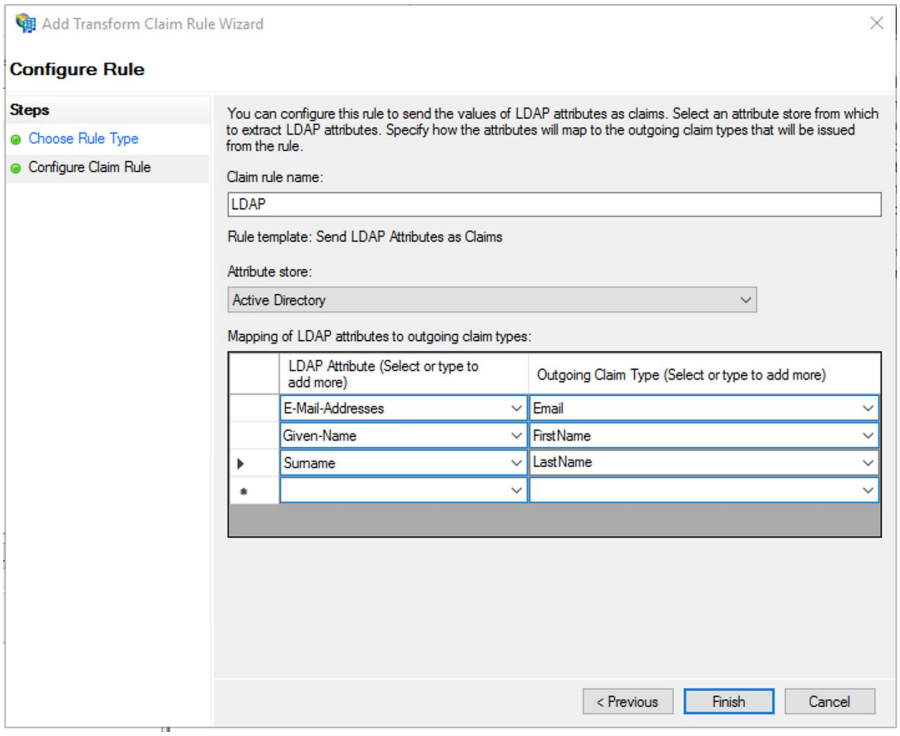
8. Here you add rules to map AD entities to TitanFile fields.



9. Add a claim rule using the LDAP template.



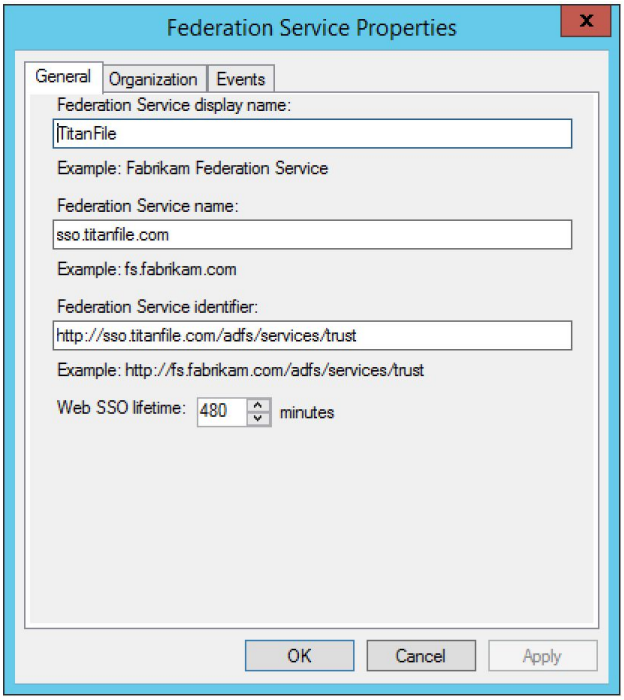
10. Populate the rule as per the screenshot below.



Information required by TitanFile

In order to establish a trust relationship between TitanFile and your identity federation service, TitanFile needs some information. All should be available in the configuration section of your federation service software:

- SAML entity ID
    - In ADFS Management Console, select “AD FS”, choose “Edit Federation Service Properties…”, and provide us with the value of “Federation Service Identifier” from the dialog box as in the screenshot below.



- SAML metadata XML file.
    - This can typically be downloaded from https://localhost/federationmetadata/2007-06/federationmetadata.xml where localhost is your ADFS server name. Please provide us with the XML file or the URL to download the XML file if it’s publicly accessible.

Final remarks

After both ends have been configured correctly - the identity federation (ADFS) end and the TitanFile service end - then the single sign on can be tested. Attempting to test intermediate configuration is not possible due to the way the SAML 2.0 protocol works.