

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.

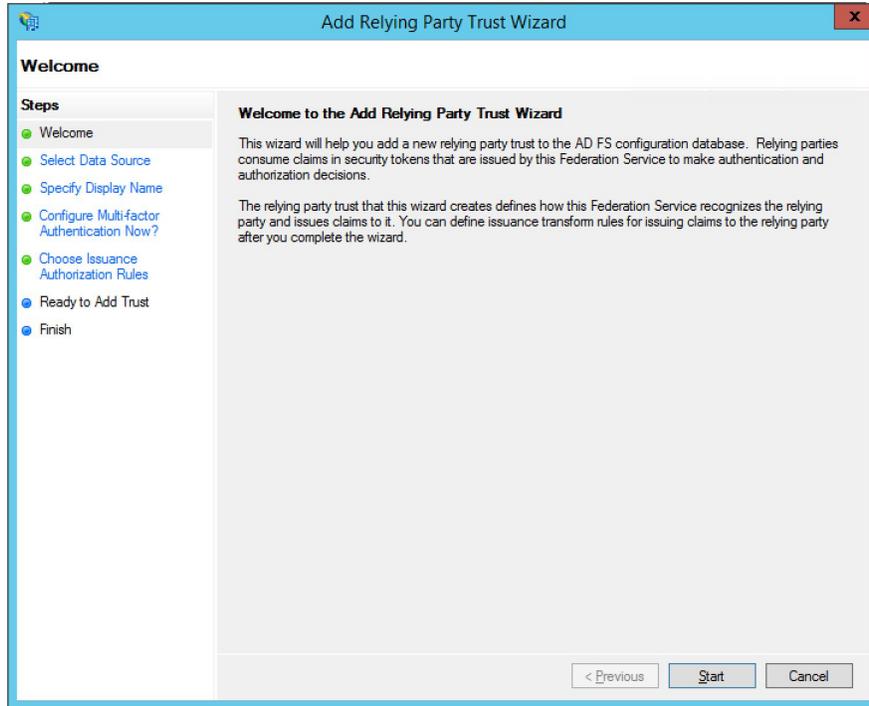
Configuring the SAML-based identity federation service

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

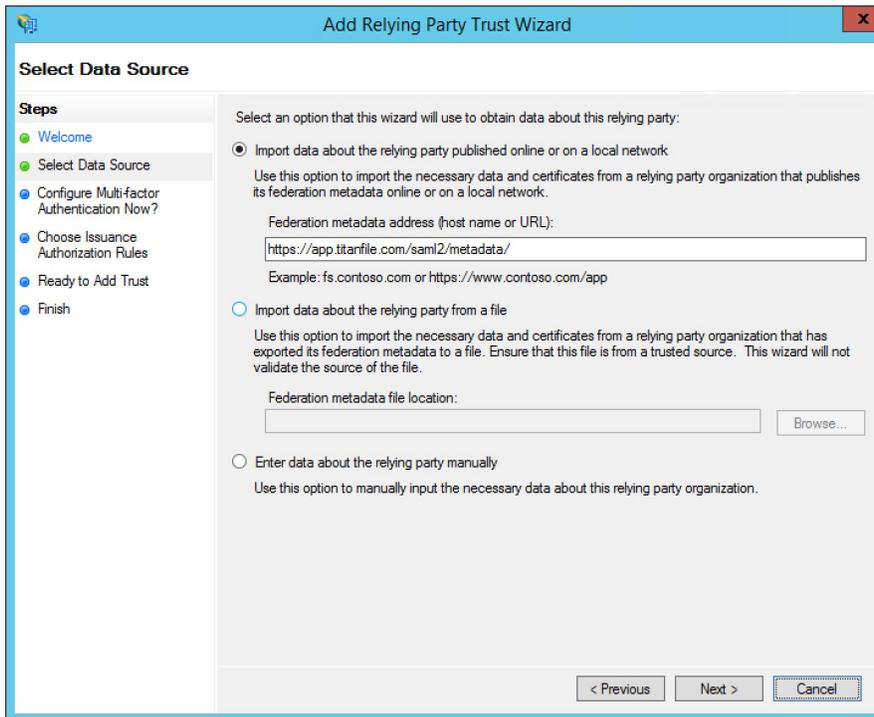
- Your TitanFile subdomain: subdomain.titanfile.com
- SAML assertion consumer service URL: <https://subdomain.titanfile.com/saml2/acs/>
- SAML single logout service URL: <https://subdomain.titanfile.com/saml2/ls/> (optional)
- Application name: TitanFile

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/>



- Specify a display name or keep the default.

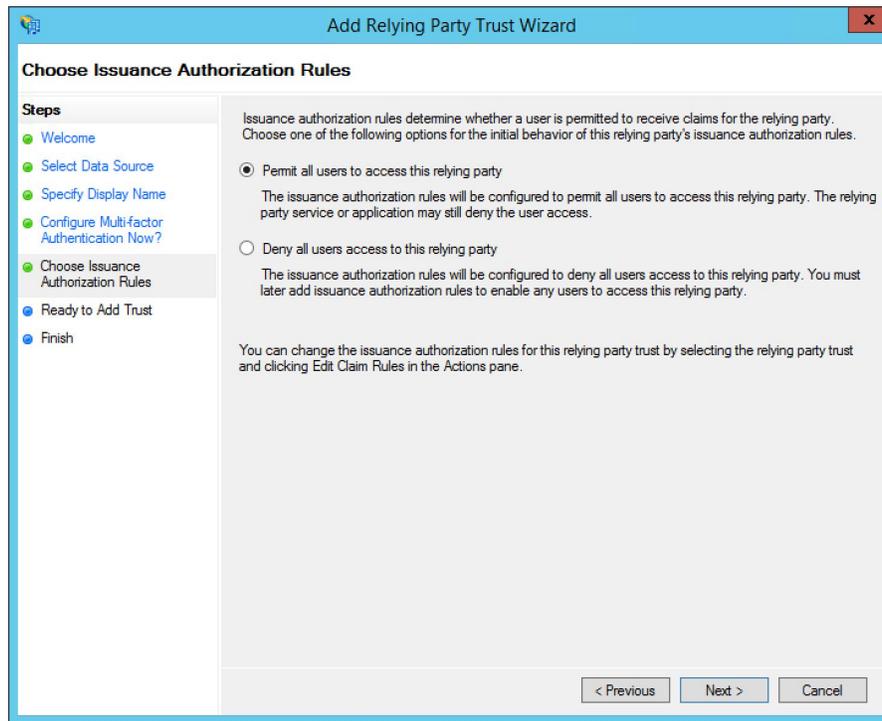
The screenshot shows the 'Add Relying Party Trust Wizard' dialog box. The title bar reads 'Add Relying Party Trust Wizard'. The main heading is 'Specify Display Name'. On the left, a 'Steps' pane lists the following steps: Welcome, Select Data Source, Specify Display Name (current step), Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area contains the instruction: 'Enter the display name and any optional notes for this relying party.' Below this, there is a 'Display name:' label followed by a text box containing 'app.titanfile.com'. Underneath is a 'Notes:' label followed by a large empty text area with scrollbars. At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

- Keep default multi-factor authentication settings.

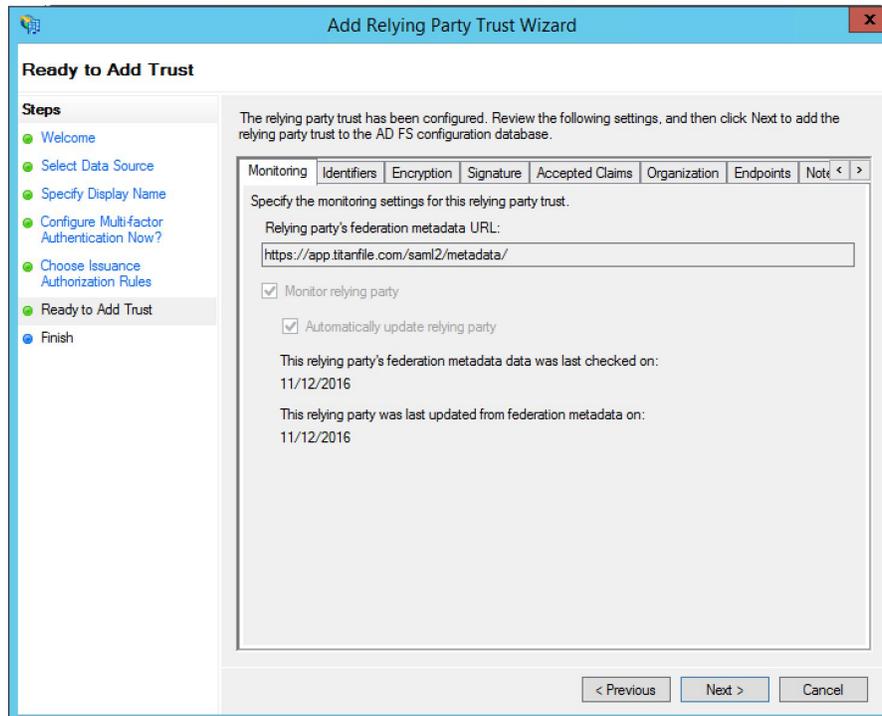
The screenshot shows the 'Add Relying Party Trust Wizard' dialog box. The title bar reads 'Add Relying Party Trust Wizard'. The main heading is 'Configure Multi-factor Authentication Now?'. On the left, the 'Steps' pane shows the current step 'Configure Multi-factor Authentication Now?' highlighted. The main area contains the instruction: 'Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required if there is a match for any of the specified requirements.' Below this is a table with two columns: 'Multi-factor Authentication' and 'Global Settings'. The table has three rows: 'Requirements', 'Users/Groups', and 'Device', all with 'Not configured' in the 'Global Settings' column. Below the table, there are two radio buttons: the first is selected and labeled 'I do not want to configure multi-factor authentication settings for this relying party trust at this time.', and the second is labeled 'Configure multi-factor authentication settings for this relying party trust.'. Below the radio buttons, there is a note: 'You can also configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see [Configuring Authentication Policies](#).' At the bottom right, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

Multi-factor Authentication	Global Settings
Requirements	Not configured
Users/Groups	Not configured
Device	Not configured
Location	Not configured

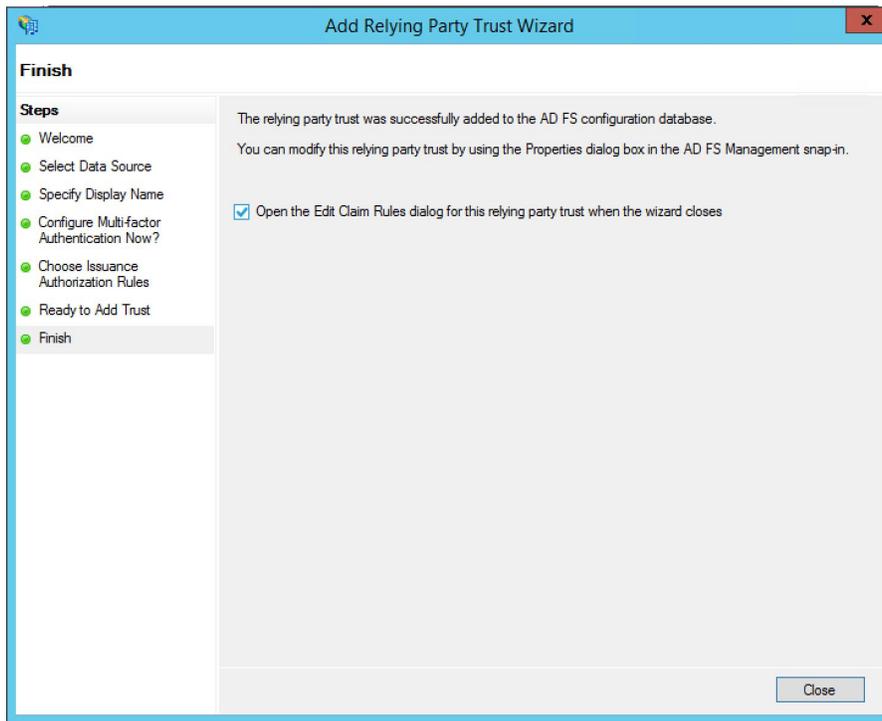
5. Set desired authorization rules. Either permit all user to access this relying party or configure permissions for each user/role separately.



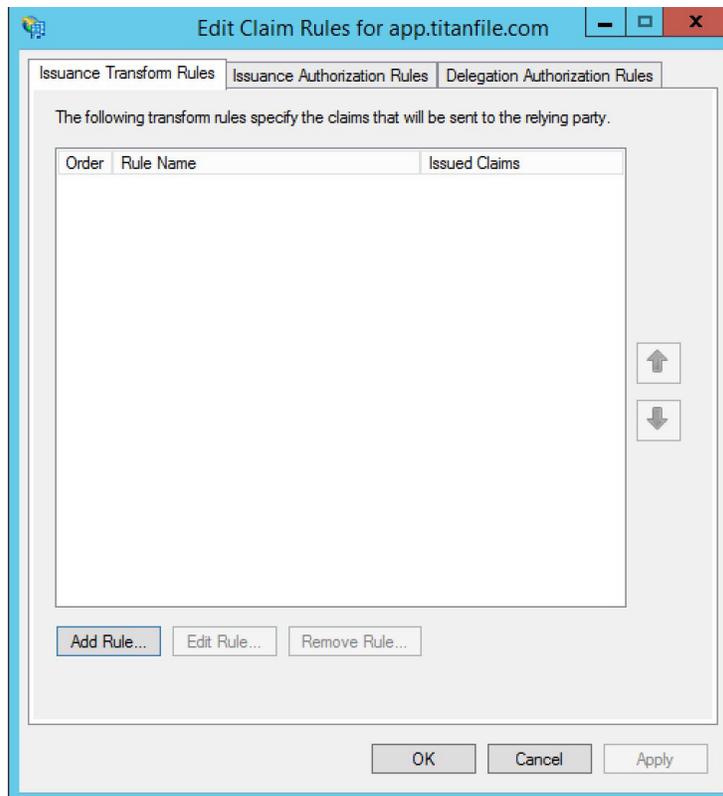
6. Review settings, go back to adjust if needed.



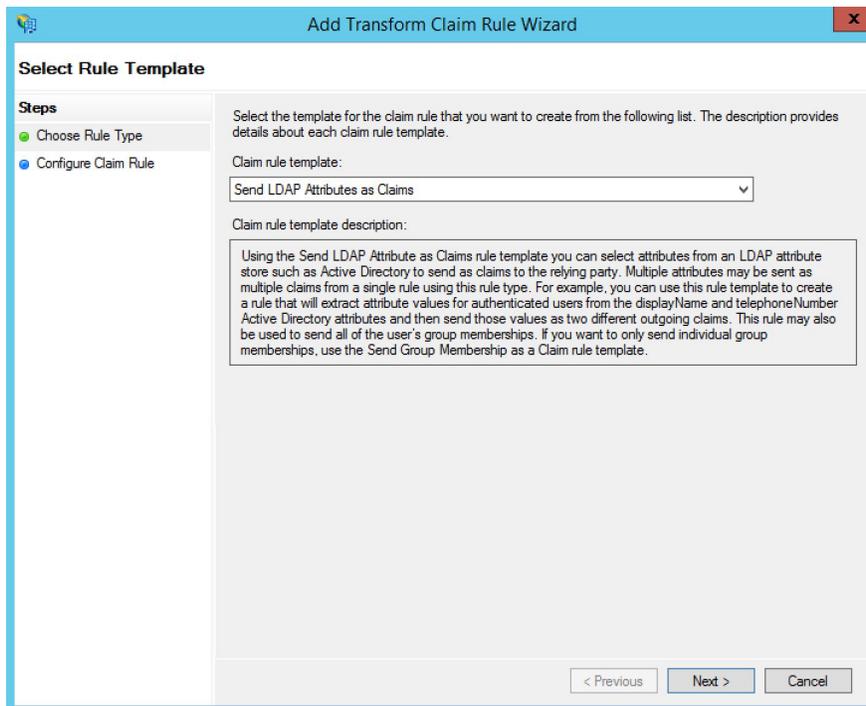
7. All set and ready to configure the Claim Rules.



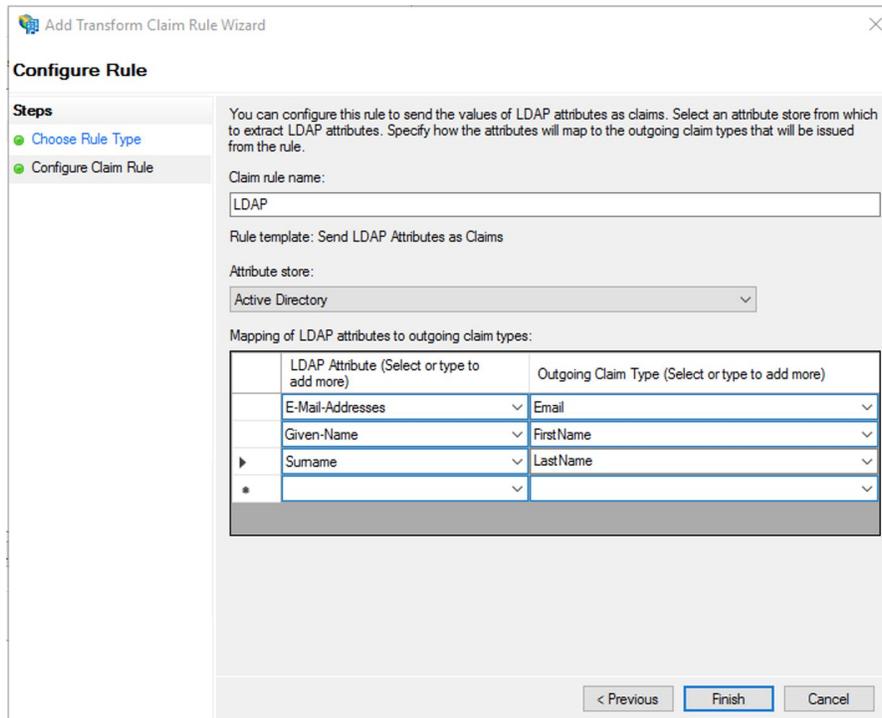
8. Here you add rules to map AD entities to TitanFile fields.



9. Add a claim rule using the LDAP template.



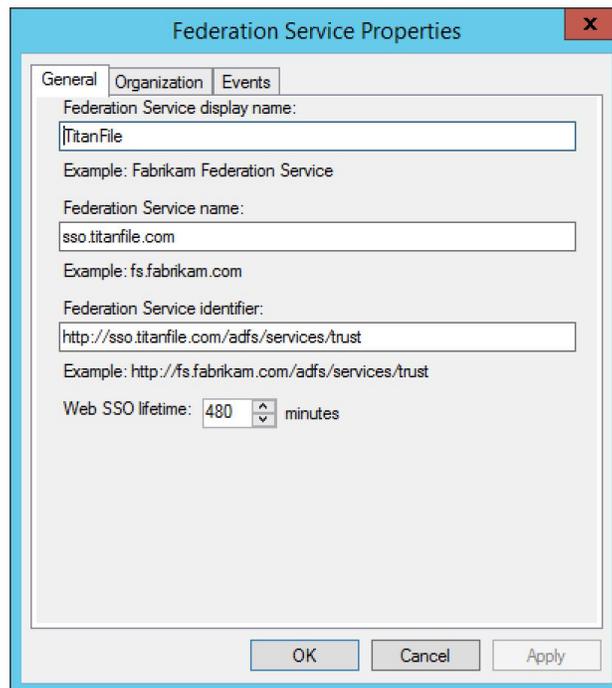
10. Populate the rule as per the screenshot below.



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.