



Knowledge base > API, SAML, integrations and general settings > How do you set up SSO with Active Directory using SAML?

How do you set up SSO with Active Directory using SAML?

Ester Andersson - 2024-02-19 - API, SAML, integrations and general settings

Step 1 -Contact Learnifier

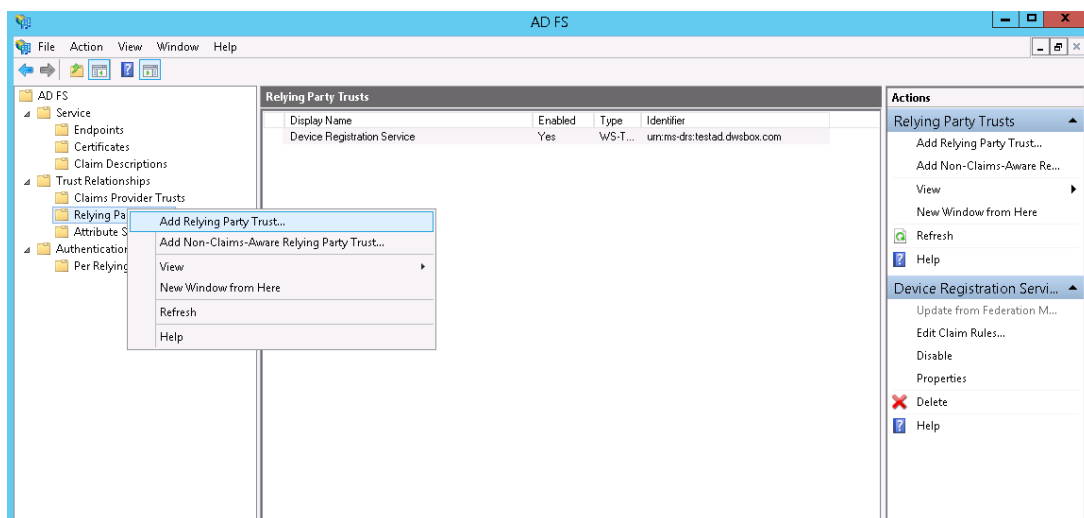
Contact support@learnifier.com and let us know that you want to set up SSO with Active Directory. We will then give you a customer-specific metadata URL for you to use.

OBS: We recommend that you use at least AD FS 3.0 (included in Windows 2012R2) or later.

Step 2 - Adding Learnifier as a Relying Party Trust in ADFS

Start the AD FS Management tool under Administrative Tools

Select the *Trust Relationships* folder and right click and select *Add Relying Party Trusts*



On the Welcome to the *Add Relying Party Trust Wizard* click *Start*

Make sure that the *Import data about the relying party published online or on a local network* button is selected.

Enter the **customer-specific metadata URL** you received from Learnifier. For example in this picture where you should enter

["https://service.learnifier.com/auth_saml/saml/metadata"](https://service.learnifier.com/auth_saml/saml/metadata) in the field.

Add Relying Party Trust Wizard

Select Data Source

Steps

- Welcome
- Select Data Source
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

Select an option that this wizard will use to obtain data about this relying party:

- Import data about the relying party published online or on a local network
Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.
Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app
- Import data about the relying party from a file
Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.
Federation metadata file location:
- Enter data about the relying party manually
Use this option to manually input the necessary data about this relying party organization.

< Previous Next > Cancel

Edit the display name and note if you like. When finished click Next

Add Relying Party Trust Wizard

Specify Display Name

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

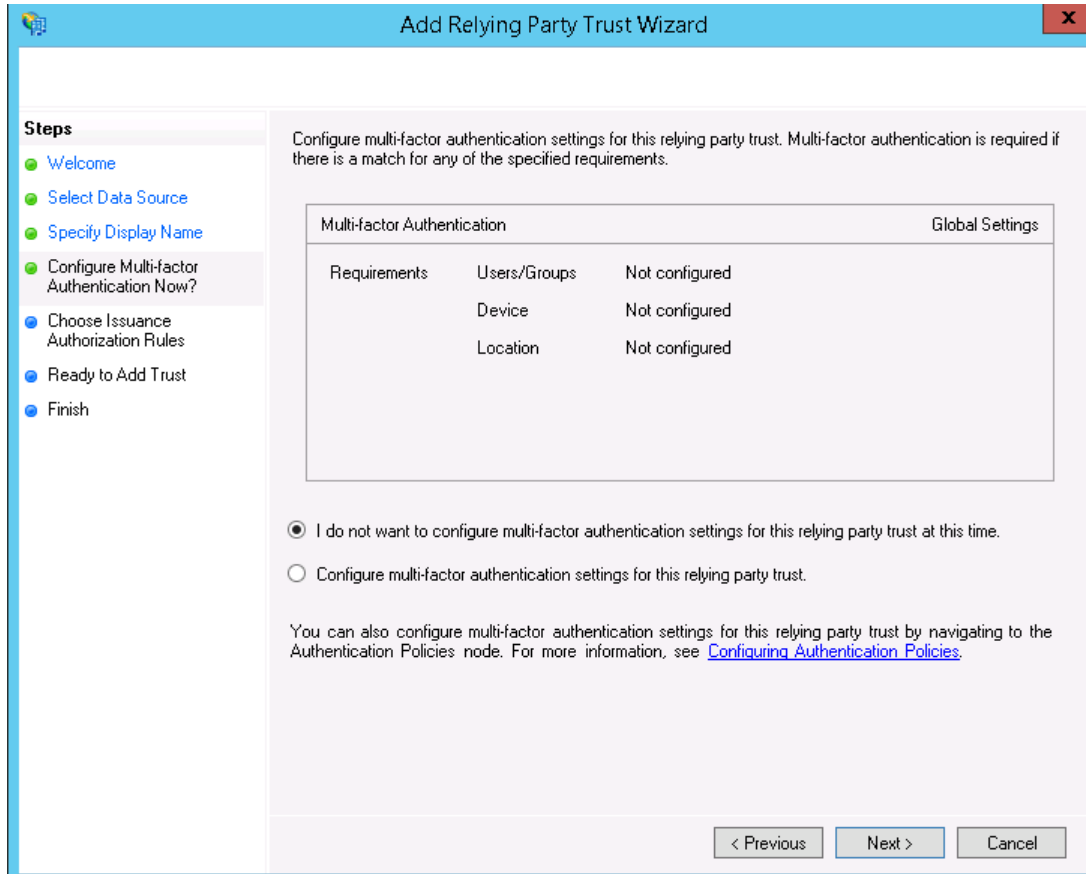
Enter the display name and any optional notes for this relying party.

Display name:

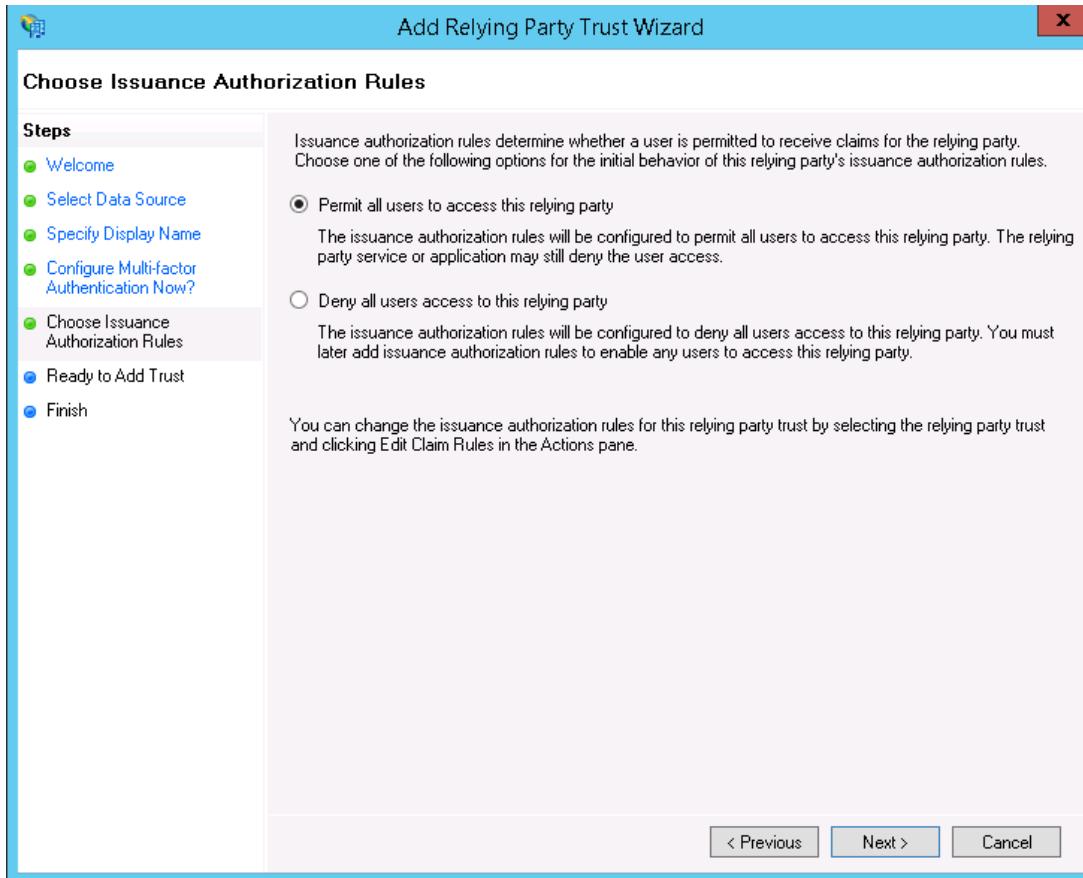
Notes:

< Previous Next > Cancel

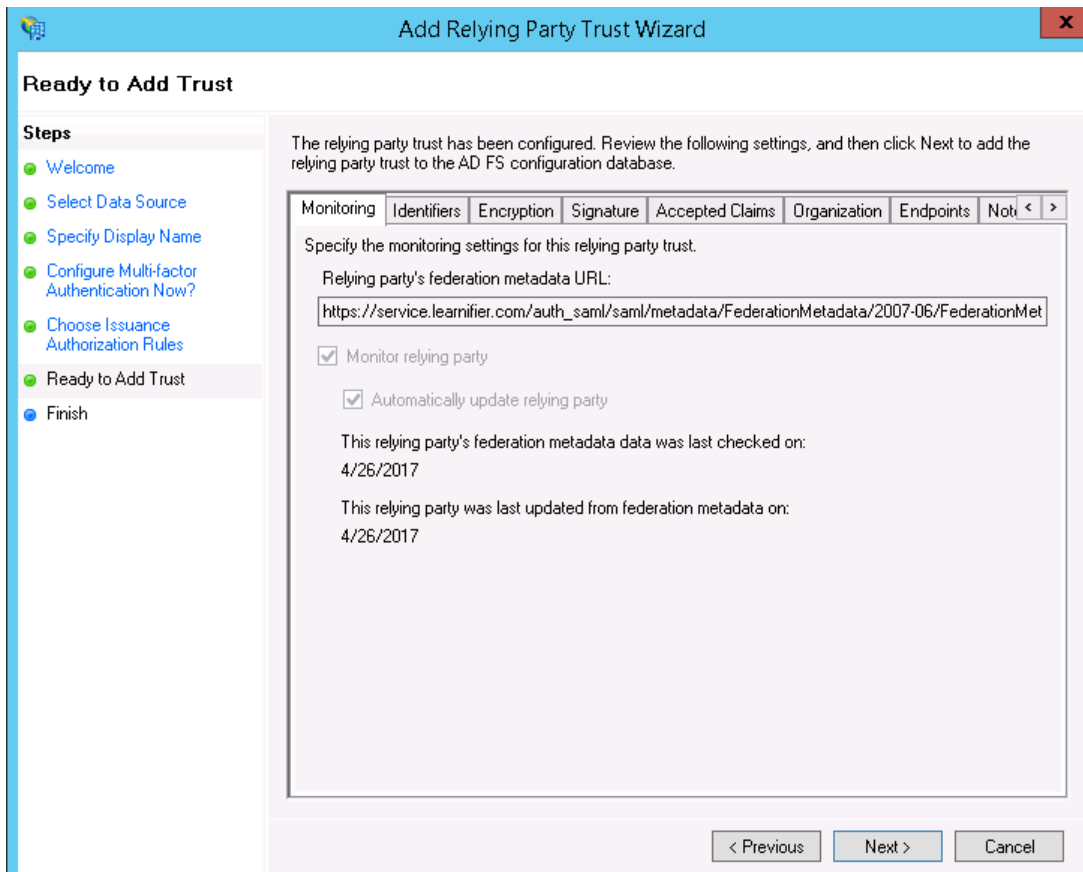
On this page, select to not use MFA.



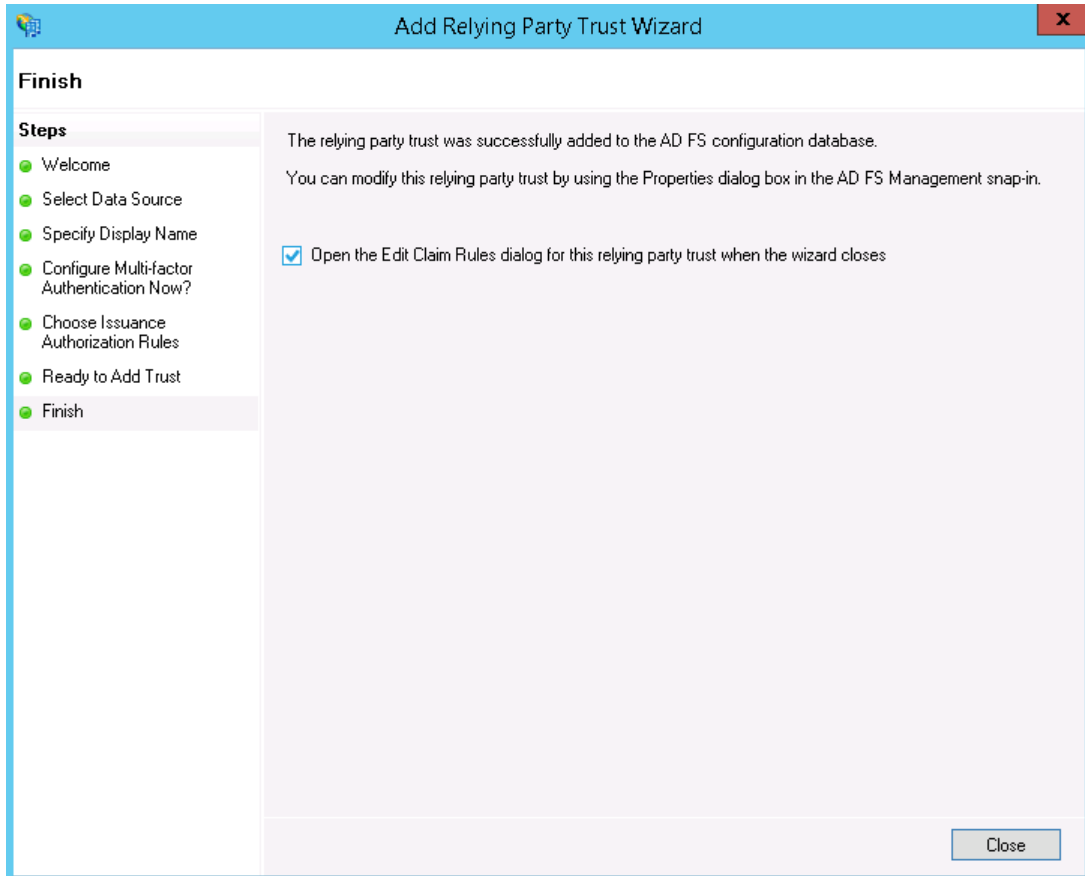
On this page, permit all users to access Learnifier



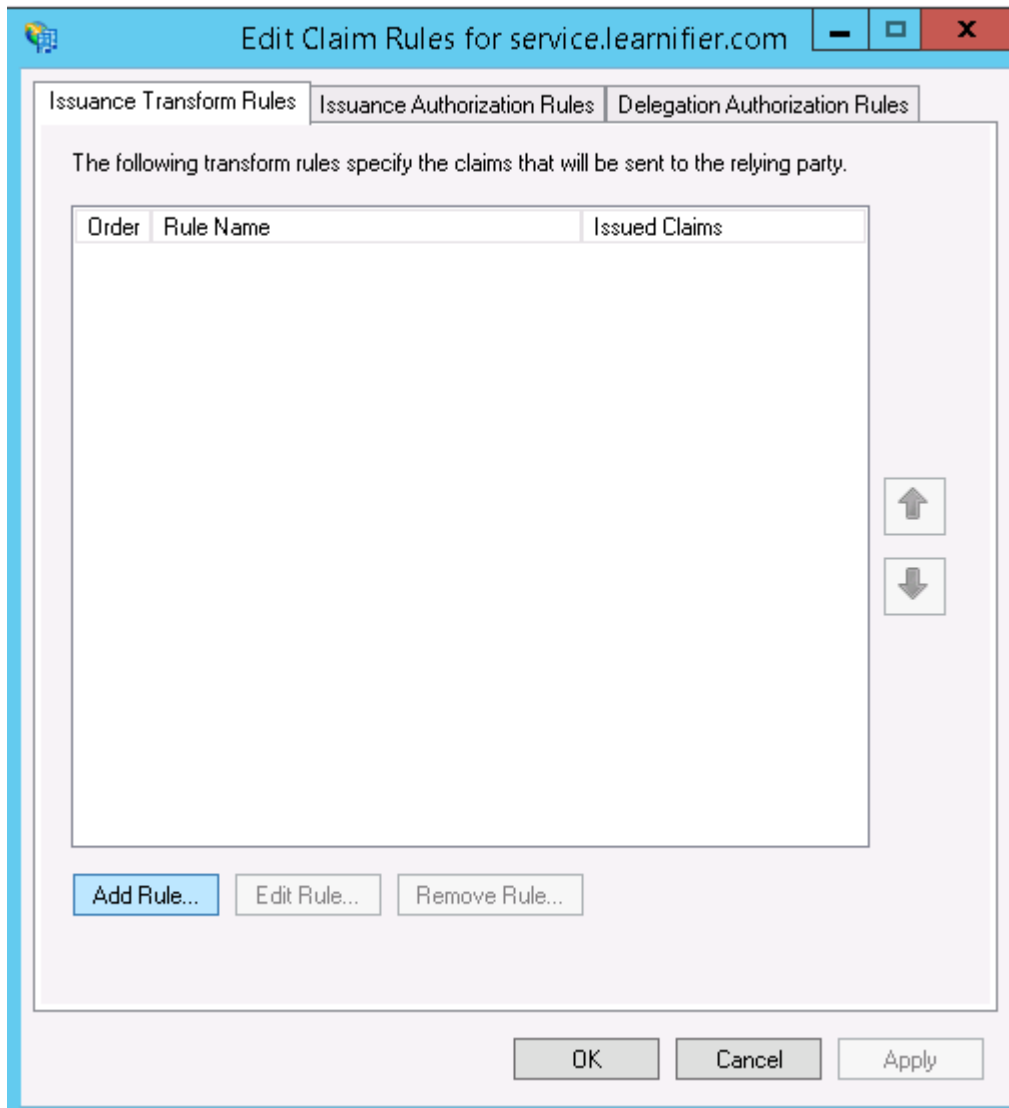
On this page, simply click Next



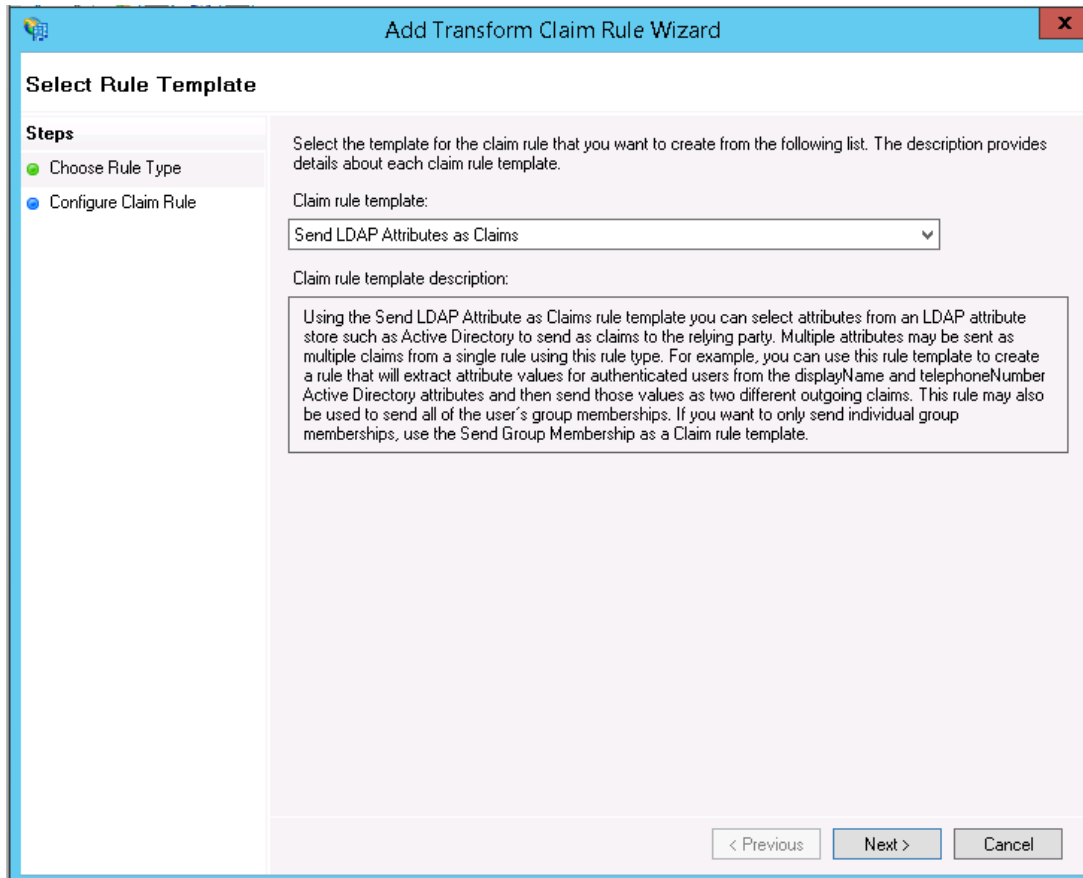
Make sure that the checkbox is marked and click close.



Click on "Add Rule"



Select to *Send LDAP Attributes as Claims*



Enter "Learnifier Claims" as the Claim rule name. Make sure that the Attribute Store is Active Directory and add the values according to the screenshot.

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Rule template: Send LDAP Attributes as Claims

Attribute store:

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)		Outgoing Claim Type (Select or type to add more)
	SAM-Account-Name	▼	Name ID
	Display-Name	▼	Name
	E-Mail-Addresses	▼	E-Mail Address
	Given-Name	▼	Given Name
▶	Surname	▼	Surname

< Previous Finish Cancel

Step 3 - Contact Learnifier

Contact your representative and provide him/her with the URL of the SAML metadata for your Active Directory Federation Services. If the login web server / AD FS is reachable under <https://login.example.com> the metadata is usually available at <https://login.example.com/FederationMetadata/2007-06/FederationMetadata.xml>. The link must be an HTTP link and the server must be reachable from the public internet.

You should receive a response shortly after that the connection is established.

Troubleshooting

Make sure that the Secure hash algorithm is set to SHA-256 (available under the Advanced tab) in the created Relying Party Trust.