



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

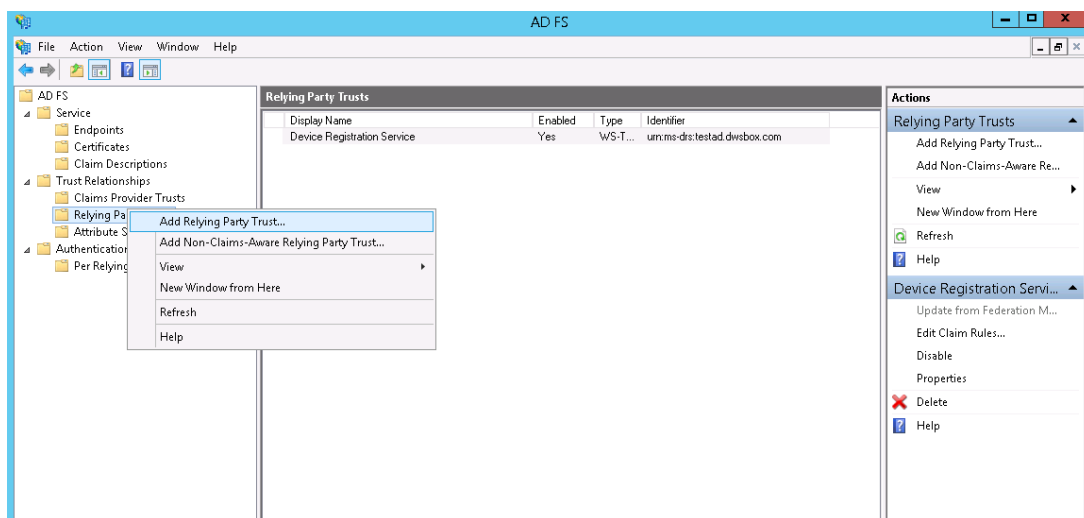
Contact support@learnifier.com and let us know that you want to set up SSO with Active Directory. We will then give you a customer-specific metadata URL for you to use.

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

Configuring Authentication Policies.' At the bottom right are three buttons: '< Previous', 'Next >', and 'Cancel'."/>

Steps

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

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.

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

☒ I do not want to configure multi-factor authentication settings for this relying party trust at this time.
 ☐ Configure multi-factor authentication settings for this relying party trust.

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](#).

< Previous
 Next >
 Cancel

On this page, permit all users to access Learnifier

Add Relying Party Trust Wizard

Choose Issuance Authorization Rules

Steps

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

Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.

☒ Permit all users to access this relying party

The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.

☐ Deny all users access to this relying party

The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party.

You can change the issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.

On this page, simply click Next

Add Relying Party Trust Wizard

Ready to Add Trust

Steps

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

The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.

Monitoring
Identifiers
Encryption
Signature
Accepted Claims
Organization
Endpoints
Not
<
>

Specify the monitoring settings for this relying party trust.

Relying party's federation metadata URL:

`https://service.learnifier.com/auth_saml/saml/metadata/FederationMetadata/2007-06/FederationMet`

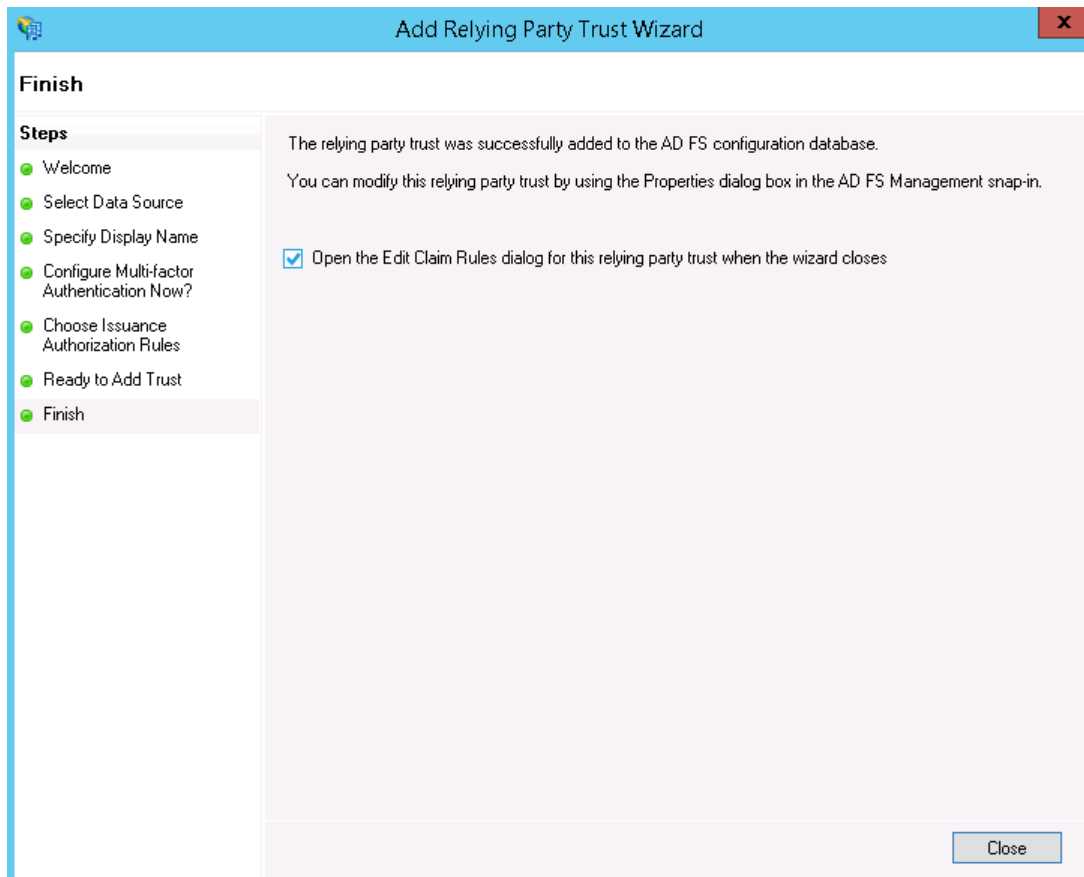
☒ Monitor relying party

☒ Automatically update relying party

This relying party's federation metadata data was last checked on:
4/26/2017

This relying party was last updated from federation metadata on:
4/26/2017

Make sure that the checkbox is marked and click close.



Click on "Add Rule"

Edit Claim Rules for service.learnifier.com

Issuance Transform Rules Issuance Authorization Rules Delegation Authorization Rules

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
-------	-----------	---------------

↑

↓

Add Rule... Edit Rule... Remove Rule...

OK Cancel Apply

Select to *Send LDAP Attributes as Claims*

The screenshot shows a Windows-style dialog box titled "Add Transform Claim Rule Wizard" with a close button (X) in the top right corner. The dialog is divided into two main sections. On the left, under the heading "Select Rule Template", there is a "Steps" sidebar with two items: "Choose Rule Type" (marked with a green dot) and "Configure Claim Rule" (marked with a blue dot). The main area on the right contains the following text: "Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template." Below this is a label "Claim rule template:" followed by a dropdown menu currently showing "Send LDAP Attributes as Claims". Underneath the dropdown is a label "Claim rule template description:" followed by a text box containing the following text: "Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template." At the bottom right of the dialog are three buttons: "< Previous", "Next >", and "Cancel".

Add Transform Claim Rule Wizard

Select Rule Template

Steps

- Choose Rule Type
- Configure Claim Rule

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

Send LDAP Attributes as Claims

Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

< Previous Next > Cancel

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

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.