

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 <u>support@learnifier.com</u> 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

_ 0 X AD FS 翰 File Action View Window Help _ 8 × (= e) 🖄 🖬 🚺 📋 AD FS Relying Party Trusts Actions ⊿ 📋 Service Relying Party Trusts Endpoints Enabled Type Identifier WS-T... urn:ms-drs:testad.dwsbox.com Device Registration Service Add Relying Party Trust... Claim Descriptions Add Non-Claims-Aware Re... Trust Relationships View New Window from Here Add Relying Party Trust... Refresh Add Non-Claims-Aware Relying Party Trust... ⊿ 📋 Authentication 👔 Help 📋 Per Relying View New Window from Her Device Registration Servi... 🔺 Refresh Edit Claim Rules... Help Disable Properties 🔀 Delete 👔 Help

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" in the field.

\$	Add Relying Party Trust Wizard	
Select Data Source		
Steps Velcome 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 address (host name or URL): https://service.learnifier.com/auth_saml/saml/metadata 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: Browse Browse 	
	< Previous Next > Cancel	

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

\$	Add Relying Party Trust Wizard	x
Specify Display Name		
Steps	Enter the display name and any optional notes for this relying party.	
Welcome	Display name:	
Select Data Source	service.learnifier.com	
Specify Display Name	Notes:	
 Configure Multi-factor Authentication Now? 		^
 Choose Issuance Authorization Rules 		
 Ready to Add Trust 		
Finish		\sim
		_
	< Previous Next > Cancel	

On this page, select to not use MFA.

Steps Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is requ
 Welcome Select Data Source Specify Display Name Configure Multi-factor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish Multi-factor Authentication multi-factor authentication settings for this relying party trust at this time. Configure multi-factor authentication settings for this relying party trust by navigating to Authentication Policies node. For more information, see <u>Configuring Authentication Policies</u>.

On this page, permit all users to access Learnifier

×	N Add Relying Party Tru
	Choose Issuance Authorization Rules
nitted to receive claims for the reluing partu.	Steps Issuance authorization rules determine wheth
this relying party's issuance authorization rules.	Welcome Choose one of the following options for the in
	Select Data Source Select Data Source Permit all users to access this relying party
nit all users to access this relying party. The relying	Specify Display Name The issuance authorization rules will be contracted by the instance of
	Configure Multi-factor Authentication Now? Denv all users access to this relving party
y all users access to this relying party. You must to access this relying party.	Choose Issuance Authorization Rules The issuance authorization rules will be con- later add issuance authorization rules to e
	Ready to Add Trust
g party trust by selecting the relying party trust	Finish You can change the issuance authorization ru and clicking Edit Claim Rules in the Actions particular to the actions particular to the actions particular to the actions of the action

On this page, simply click Next

🖗 🛛 🕹 Add Relying Party Trust Wizard		
Ready to Add Trust		
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/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 Understand Intervention Intervention Intervention	
	< Previous Next > Cancel	

Make sure that the checkbox is marked and click close.

🖗 🛛 Add Relying Party Trust Wizard 🗖 🎴		
Finish		
Steps	The relving party trust was successfully added to the AD FS configuration database.	
Welcome	You can modify this relating party trust by using the Properties dialog boy in the AD FS Management span-in	
🥃 Select Data Source		
🥥 Specify Display Name		
Configure Multi-factor Authentication Now?	Open the Edit Claim Rules dialog for this relying party trust when the wizard closes	
 Choose Issuance Authorization Rules 		
Ready to Add Trust		
🥃 Finish		
	Close	

Click on "Add Rule"

翰 Edit Claim Rules for service.learnifier.com 💶 🕻	x		
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 A	Apply		

Select to Send LDAP Attributes as Claims

\$	Add Transform Claim Rule Wizard	x
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 provide 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 template duess from the displayName and telephoneNumb Active Directory attributes and then send those values as two different outgoing claims. This rule may als 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.	25 2 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9
	< 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.

Ŷ	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: Learnifier Claims Rule template: Send LDAP Attributes as Claims Attribute store: Active Directory Mapping of LDAP attributes to outgoing claim types:		
	LDAP Attribute (Select or type to add more) Outgo	ing Claim Type (Select or type to add more)	
	Display-Name V Name	× =	
	E-Mail-Addresses V E-Mail	Address V	
	Luven-Name ✓ Luven ▶ Surname ✓ Surna	ne v	
		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 <u>https://login.example.com</u> the metadata is usually available at

<u>https://login.example.com/FederationMetadata/2007-06/FederationMetadata.xml</u>. 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.