Setting up Single Sign On with ADFS

Last Modified on 06.08.2025

Single Sign-On is a convenient, yet secure way of authenticating a user. Most customers are already running an Identity Provider (IDP) that supports Single Sign-On through the SAML 2 protocol, e.g. Active Directory, OneLogin, or Okta.

Userlane can accept authentication via the SAML 2.0 Protocol.

Of the many implementations of this protocol, Microsoft Active Directory Federation Services (ADFS) is one of the most widespread. In this scenario, an ADFS server acts as the Identity Provider (IDP) and Userlane as the Service Provider (SP).

Requirements

- access to ADFS
- access to Userlane Portal

In order to configure the Single Sign-On for Userlane, follow these steps below:

1. Adding Userlane as a Service Provider (SP) to your IDP

For the company's IDP to accept authentication requests by Userlane, the IT Admin must first register Userlane as a Service Provider (SP).

i The Userlane Service Provider Metadata differs for each customer. Your Userlane SA will provide you with a .xml file to import into your ADFS Server.

Registration steps:

1. Download the Metadata file onto your ADFS Server

2. Open the "AD FS Management" app



3. In the menu on the right, select "Add Relying Party Trust"



4. Select "Claims aware"



5. Select the Metadata file you've downloaded or follow the instructions for manual setup below

Steps Steps Select Data Source Choose Access Control Policy Ready to Add Trust Finish	Select an option that this wizard will use to obtain data about this relying party: () Ingoot 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. Ederation metadata address (host name or URL): Example: fs contoso com or https://www.contoso.com/app () Ingort 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: C:\Users\Example\Desktop\Userlane SPMetadata xml Browse () Enter data about the relying party manually Use this option to manually input the necessary data about this relying party organization.
--	---

6. Specify any display name or description you like

Add Kelying Party Trust	t wizard		
Specify Display Nam	e		
Steps	Enter the display name and any optional notes for this relying party.		
Welcome	Display name:		
Select Data Source	Userlane		
Specify Display Name	Notes:		
 Choose Access Control Policy 	,		
Beady to Add Trust			
Finish			
	< Previous Next > Cancel		

7. It is essential to configure which employees are targeted for Userlane.

In general, any employee who has access to the connected application that uses Userlane for enablement purposes should also have access to the Userlane app. However, we recommend that App Owner confirms the target group after consulting with SA to avoid any misunderstanding.

Note: Do not configure MFA (Multi-factor Authentication) as a requirement in order to make the sign-in easier

and seamless for your users.

Choose Access Control Policy					
Steps	Choose an access control policy:				
 Welcome Select Data Source Specify Display Name Choose Access Control Policy Ready to Add Trust Finish 	Name Permit everyone and require MFA Permit everyone and require MFA for specific group Permit everyone and require MFA form extranet access Permit everyone and require MFA, allow automatic device registr Permit everyone and require MFA, allow automatic device registr Permit everyone for intranet access Parmit everyone C Policy Permit everyone I do not want to configure access control policies at this time. No application.	Description Grant access to everyone and requir Grant access to everyone and requir Grant access to everyone and requir Grant access to the intranet users and Grant access to everyone and requir Grant access to the intranet users. Grant access to the intranet users. Grant access to user of one or more Very access to the or			

- 8. Confirm in order to add the Trust and continue with configuring a claims issuance policy for your application
- 8.1. Select "Add Rule"



8.2. Userlane requires a "nameID" (please keep the exact letter-case form) in the Outgoing Claim Type. This will be the unique identifier on Userlane level and it is the only mandatory attribute required. This ID must be unique for each user and is not meant to be changed over time in order to keep historical information clean.

Steps	You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from whi to extract LDAP attributes. Specify how the attributes will man to the outgoing claim types that will be issued					
Choose Rule Type	from the rule.					
 Configure Claim Rule 	Claim rule name:					
	basic i	basic info				
	Rule te	Rule template: Send LDAP Attributes as Claims				
	Attribut	e store:				
	Active Directory V					
	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)			
	▶ ₩	User-Principal-Name ~	nameID ~			
		l ~	·			

Additional user information required by App Owner for improved targeting is explained in the article Expanding the Settings

Save and apply the Claim Rule.

2. Add information to Userlane Portal

Continue with step 3 from the article on setting up SSO for Userlane.