Setting up Single Sign On with Azure Active Directory

Last Modified on 06.08.2025

Single Sign-On is a convenient, yet secure way of authenticating a user - without them having to set up a new password.

Requirements

- access to Azure Portal
- access to Userlane Portal

Set up SSO for Azure Active Directory

- 1. Open the Azure Portal and navigate to Azure Active Directory / Enterprise applications.
 - Administrative units
 - 🚸 Delegated admin partners
 - Enterprise applications
 - Devices
 - App registrations
- 2. Click on "New application"

) F

3. Click on "Create your own application"

Browse Azure AD Galler

```
+ Create your own application \bigcirc \bigtriangledown (
```

The Azure AD App Gallery is a catalog of tho you leverage prebuilt templates to connect y

4. Enter a name for your application. This can be whatever you like, for example "Userlane". Confirm the creation.

Create your own application

 \times

Rot feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

Userlane

What are you looking to do with your application?

- $\bigcirc\,$ Configure Application Proxy for secure remote access to an on-premises application
- O Register an application to integrate with Azure AD (App you're developing)
- Integrate any other application you don't find in the gallery (Non-gallery)
- 5. Open the "Properties" page from the menu on the left



6. Set the "Assignment required" option to "No". This allows all users to sign into Userlane if needed.

Assignment required?	(i) (i)	Yes	No

- 7. Open the "Single sign-on" page from the menu on the left
 - Users and groups
 - ➔ Single sign-on
 - Provisioning
- 8. Select "SAML" as the single sign-on method



9. Click "Edit" on the Basic SAML Configuration fields

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. Learn more.

Read the configuration guide \square for help integrating Userlane.

Basic SAML Configuration		Ø
Identifier (Entity ID)	Required	
Reply URL (Assertion Consumer Service URL)	Required	
Sign on URL	Optional	
Relay State (Optional)	Optional	
Logout Url (Optional)	Optional	

10. Now fill the Identifier and Reply URL with the value that you can find in the Userlane Portal under Account > Global settings > Single Sign-on. This typically looks like a URL starting with https://ssosaml.userlane.com/.. We tried to make this as easy as possible for you at Userlane, so this same value goes into both the Identifier and the Reply URL. Save these changes.

Basic SAML Configuration	×
☐ Save	
dentifier (Entity ID) * 💿	
The unique ID that identifies your application to Azure Active Directory. This value must be unique across all applications in your Azure Active Directory tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.	
Default	
https://sso-saml.userlane.com/c/12345/authenticate	
Add identifier	
Reply URL (Assertion Consumer Service URL) $* \oplus$ The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.	
Index Default	
https://sso-saml.userlane.com/c/16145/authenticate	
Add reply URL	

11. Optional step: If you want to segment users based on attributes in their profile, you can add "Attributes & Claims" in the second step of the "Set up Single Sign-On with SAML" page.

Typically we see that customers want to include attributes like country, department, or other organizational attributes to show the right training & enablement content to users.

Attributes & Claims		🖉 Edit
givenname	user.givenname	
surname	user.surname	
emailaddress	user.mail	
name	user.userprincipalname	
Unique User Identifier	user.userprincipalname	

12. This completes the setup on the side of Azure Active Directory. The remaining steps are about configuring Userlane to trust your Azure Active Directory and also need to be completed to enable Single Sign On. Scroll down to Step 4 of the "Set up Single Sign-On with SAML" page, and copy the Login URL.

Set up Userlane		
You'll need to configure the applica	tion to link with Azure AD.	Copy to clipboard
Login URL	https://login.microsoftonline.com	n/57c9244a-ce66 🗈
Azure AD Identifier	https://sts.windows.net/57c9244a	a-ce66-47fc-8010 🗈
Logout URL	https://login.microsoftonline.com	n/57c9244a-ce66 🗈

Paste this Login

URL into the "IDP Entrpoint URL" field in the Userlane Portal's SSO configuration page (Account > Global settings > Single Sign-on).

Configure SSO

3

IDP	ENTRYPOINT	URL	(FOR	SAML)
		OIL I		S And

https://login.microsoftonline.com/123467-abcdef/saml2

13. Back on the Azure Portal page, click on "Download" of the SAML Certificate in Base64 format in Step 3.

Token signing certificate		
Status	Active	6/ Eul
Thumbprint	8B55FE30B67EACB29CAF6A516A328A76A4FF1A81	
Expiration	3/3/2026, 5:27:19 PM	
Notification Email	felix@userlane.com	
App Federation Metadata Url	https://login.microsoftonline.com/57c9244a-ce66	2
Certificate (Base64)	<u>Download</u>	
Certificate (Raw)	Download	
Federation Metadata XML	Download	
Verification certificates (optional) (Pre	eview)	
Required	No	⊾ Eu
Active	0	
Expired	0	

 Open the downloaded .cer file in a Text Editor of your choice (e.g. Notepad by right-clicking on the file and then Open With) and copy the part inside of the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- part to your clipboard.

Userlane.cer - Notepad
File Edit Format View Help
BEGIN CERTIFICATE
MIIC8DCCAdigAwIBAgIQMeCWRxYkvYBGrWL3GfiYaDANBgkqhkiG9w0BAQsFADA0MTIwMAYDVQQD
Ey1NaWNyb3NvZnQgQXp1cmUgRmVkZXJhdGVkIFNTTyBDZXJ0aWZpY2F0ZTAeFw0yMzAzMDMxNjI3
MTlaFw0yNjAzMDMxNjI3MTlaMDQxMjAwBgNVBAMTKU1pY3Jvc29mdCBBenVyZSBGZWR1cmF0ZWQg
U1NPIEN1cnRpZmljYXR1MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA17vnyV6TJCos
oSbHXfnYVH5b/5wsNcb4UdyVwesTuDr97kyRHMHiaWWFV0eSTDm3fyXB0LugehxbQsRypye5YszZ
UeUoHfVxxwP1BgRrYgnDK40KUvz0S3b4Wh7Rm9KLxft6dIbChQ1TKo+PLI2N12qQwza+HMQShhT1
lJOBN4StZkC29e0Yz1/38dPvRydLWCmiGkk200mK6xE7ZTk1HCdtKhhxFnzQ7kM13hRZn2QmTthQ
hF6xCZdqPOV91QqN1nZmfQZ7Z1sLoXxKy23tVLrfLuZ1r8+LIxMIG45N8MUtmTAqB7EQ4FTQ+ZY1
j1jgmruJSbgu3PVAa5kxjYdokQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBUMIbpC639BcisHvpC
Lxa4SaNVWrdEF3D50mPq0r4XMFgxNAXLKqiSTx0FIw4/QaLKN8WWXEsgvmg30r1b/goxxesEqBZ5
pcUvHWFoUUIHzKuMQ1w/24d6Fxm3T20S/9FnV3zy4L7/kI1yzYxg9Pk91bj9DaNkss+WjSYZNqdG
IRZxBrPSAhRLIB64ewwcmzjBn0AxLqM7zN1zFJQ69vf+04v8w4aq61TWypRRVezICJ+i6ab/uhGB
U/wb5BDuX8eXaqamCCItWQROQsWs9xjhzco3nPjnM6Qdq3fg1kLBnBMGJSnPdiuY2ZHk1G/t8fxS
3hjwuryjQef8CeSJjevk
END CERTIFICATE

2. Add information to Userlane Portal

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