

Setting up Single Sign On with Azure Active Directory

Last Modified on 03.07.2023

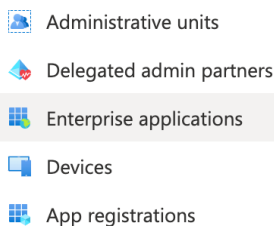
Single Sign-On is a convenient, yet secure way of authenticating a user - without them having to set up a new password.

Requirements

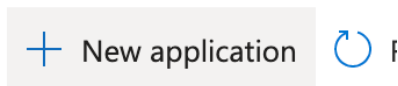
- access to Azure Portal
- access to Userlane Portal

Set up SSO for Azure Active Directory

1. Open the Azure Portal and navigate to Azure Active Directory / Enterprise applications.

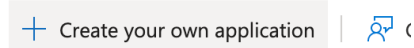


2. Click on “New application”



3. Click on “Create your own application”


Browse Azure AD Galler



The Azure AD App Gallery is a catalog of the 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 ×

 Got 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?


- Configure Application Proxy for secure remote access to an on-premises application
- 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

Manage

 Properties

 Owners

 Roles and administrators


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

Assignment required? ⓘ

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



SAML

Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

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](#) for help integrating Userlane.

1

Basic SAML Configuration Edit

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://sso-saml.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 | Got feedback?

Identifier (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

[Add identifier](#)

Reply URL (Assertion Consumer Service URL) * ⓘ
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

[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.

2

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.

4

Set up Userlane

You'll need to configure the application to link with Azure AD. Copy to clipboard

Login URL	https://login.microsoftonline.com/57c9244a-ce66-...
Azure AD Identifier	https://sts.windows.net/57c9244a-ce66-47fc-8010...
Logout URL	https://login.microsoftonline.com/57c9244a-ce66-...

Paste this Login

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

Configure SSO

IDP ENTRYPOINT URL (FOR SAML)

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

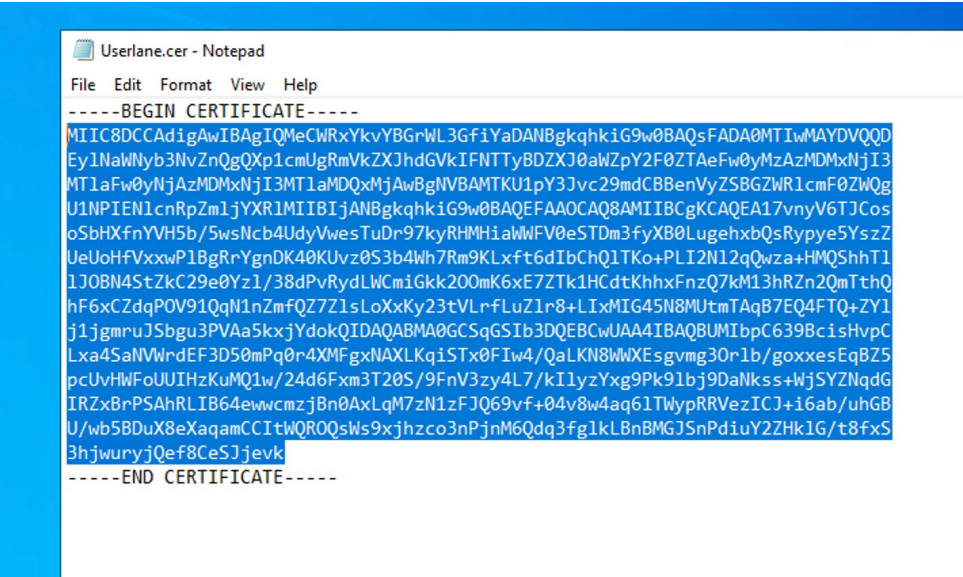
13. Back on the Azure Portal page, click on "Download" of the SAML Certificate in Base64 format in Step 3.

3

SAML Certificates

Token signing certificate		Edit
Status	Active	
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-...	
Certificate (Base64)	Download	
Certificate (Raw)	Download	
Federation Metadata XML	Download	
Verification certificates (optional) (Preview)		Edit
Required	No	
Active	0	
Expired	0	

14. 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.



15. Back in the Userlane Portal, paste this into the "IDP Certificate" field and save these changes.

IDP CERTIFICATE

```
IRZxBrPSAhRLIB64ewwcmzjBn0AxLqM7zN1zFJQ69vf+04v8  
w4aq6LTWypRRVezICJ+i6ab/uhGB  
U/wb5BDuX8eXaqamCCItWQROQsWs9xjhzco3nPjnM6Qdq3f  
gkLBnBMGJSnPdiuY2ZHKIG/t8fxS  
3hjwuryjQef8CeSJjevk
```

SAVE CHANGES

16. Now it's time to test the Single Sign On. You can do this by clicking on the "Test SSO" button on the Userlane Portal, or by opening the Entity ID URL used before in a new tab manually. The Single Sign On flow is working correctly if the tab closes automatically (after being redirected around a few times) and not showing any errors.

Test the SSO integration

TEST SSO