Setting up Single Sign On with Azure Active Directory

Last Modified on 06.08.2025

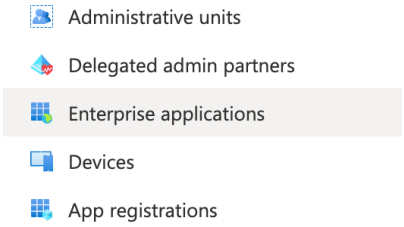
Single Sign-On is a convenient, yet secure way of authenticating a user - without them having to set up a new password.

Requirements

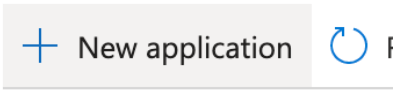
- access to Azure Portal
- access to Userlane Portal

Set up SSO for Azure Active Directory

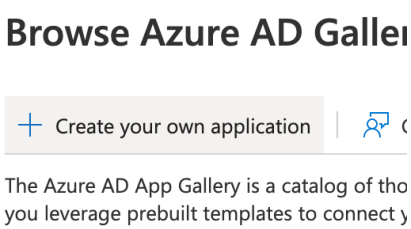
1. Open the Azure Portal and navigate to Azure Active Directory / Enterprise applications.



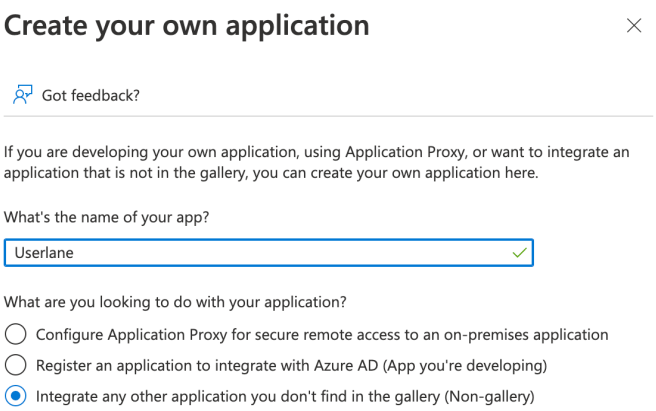
2. Click on “New application”



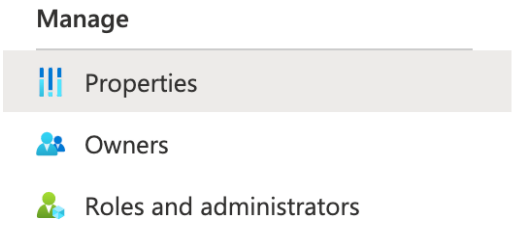
3. Click on “Create your own application”



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

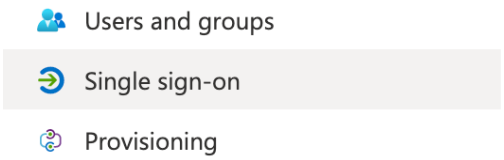


5. Open the “Properties” page from the menu on the left

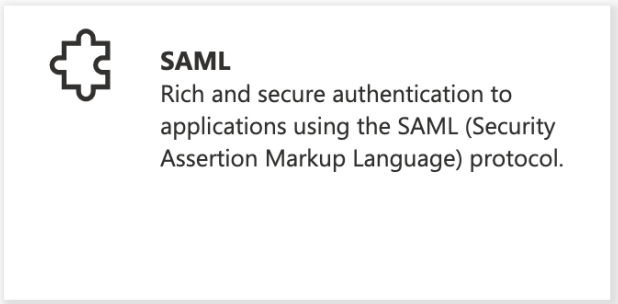


6. Set the “Assignment required” option to “No”. This allows all users to sign into Userlane if needed.

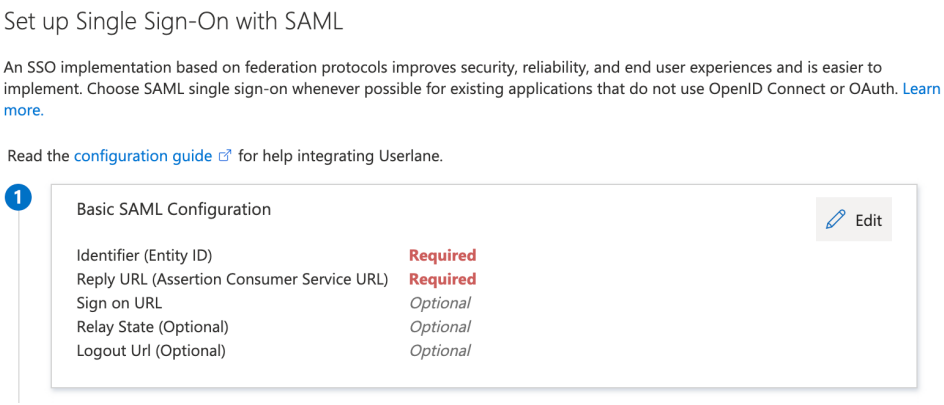
7. Open the “Single sign-on” page from the menu on the left



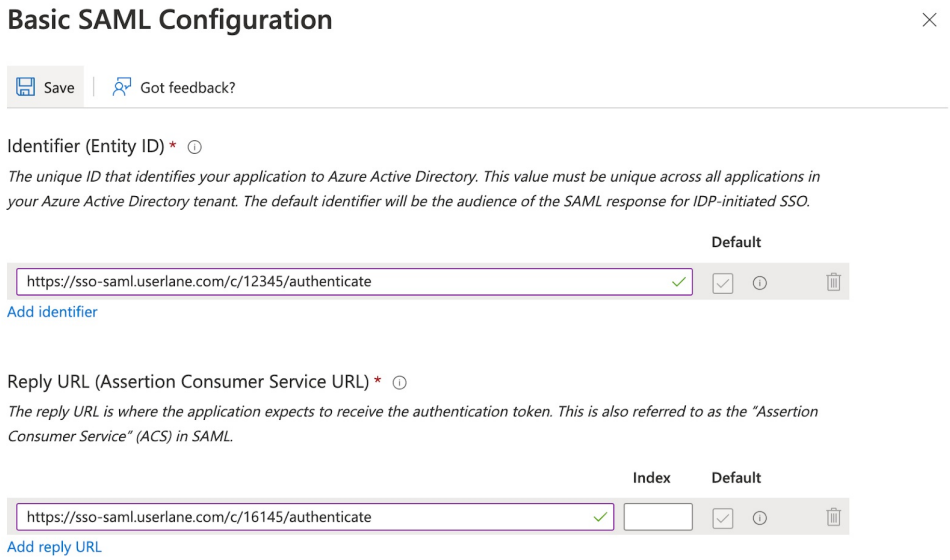
8. Select “SAML” as the single sign-on method



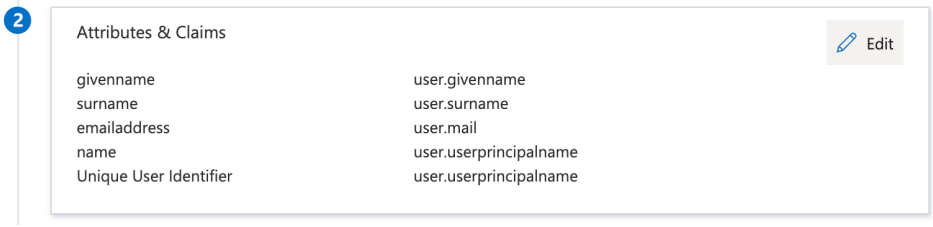
9. Click “Edit” on the Basic SAML Configuration fields



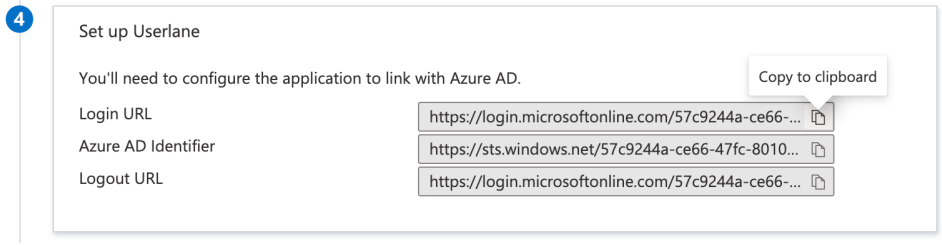
10. Now fill the Identifier and Reply URL with the value that you can find in the Userlane Portal under Account > Global settings > Single Sign-on. This typically looks like a URL starting with https://sso-saml.userlane.com/.. We tried to make this as easy as possible for you at Userlane, so this same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



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.

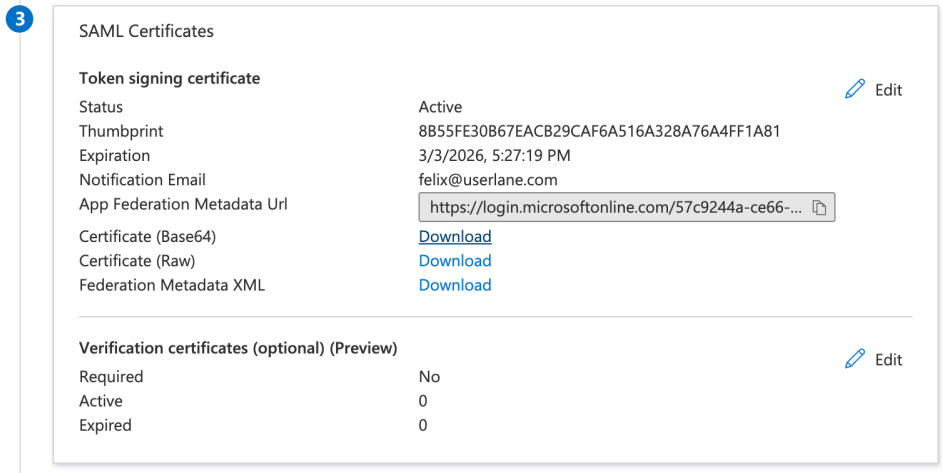


12. This completes the setup on the side of Azure Active Directory. The remaining steps are about configuring Userlane to trust your Azure Active Directory and also need to be completed to enable Single Sign On. Scroll down to Step 4 of the “Set up Single Sign-On with SAML” page, and copy the Login URL.

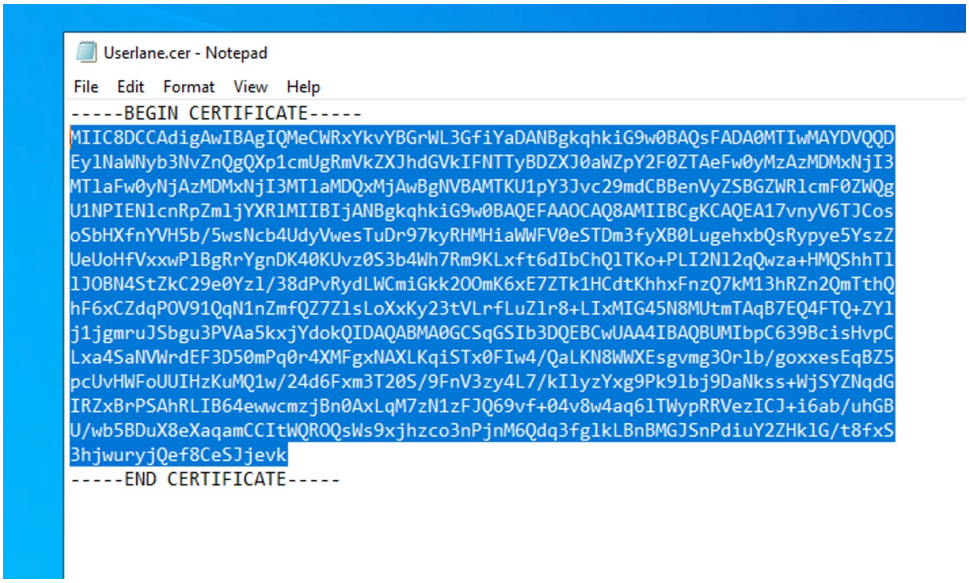


Paste this Login URL into the “IDP Entrpoint URL” field in the Userlane Portal’s SSO configuration page (Account > Global settings > Single Sign-on).

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



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.



2. Add information to Userlane Portal

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