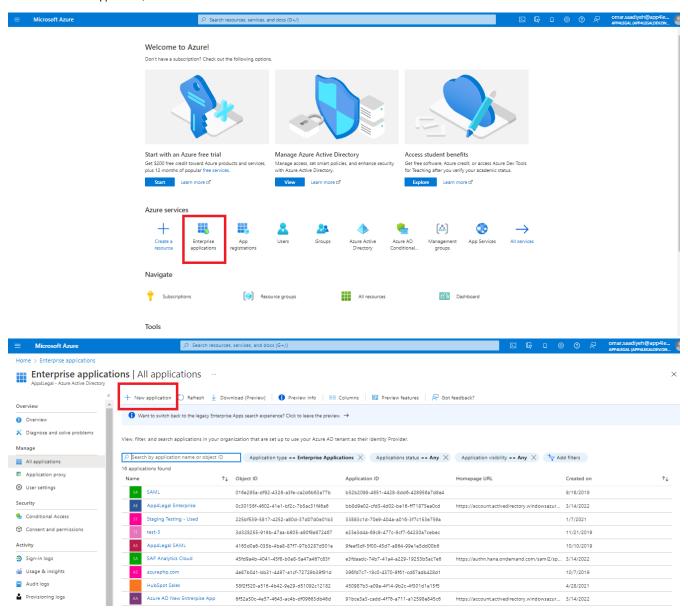# SSO Integration with Azure Active Directory
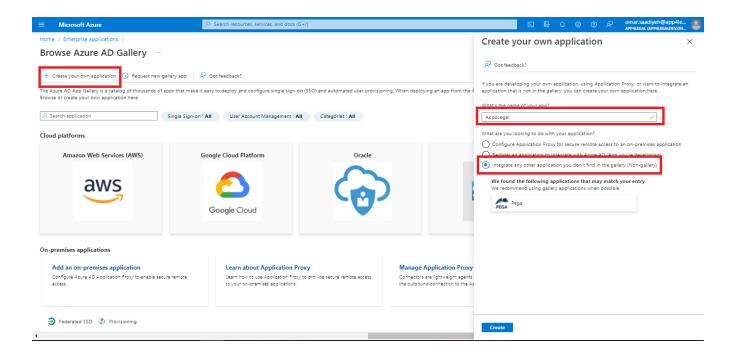
Configure Azure Active Directory as SAML Identity Provider:

Add an enterprise application

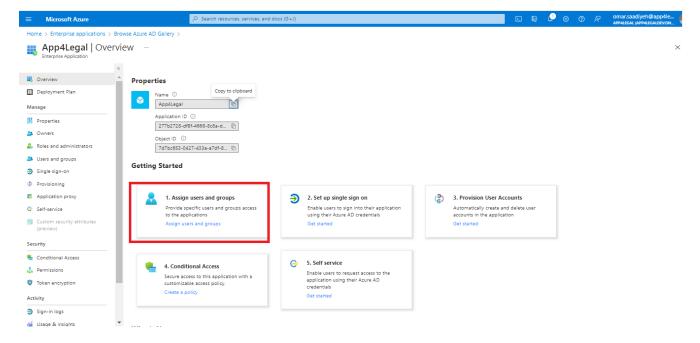To add an enterprise application to your tenant:

1. Sign in to your Azure Account through the Azure portal.
2. Select **Azure Active Directory**.
3. Select **Enterprise applications**.
4. Select **New application**.
5. Select **Create your own application.**
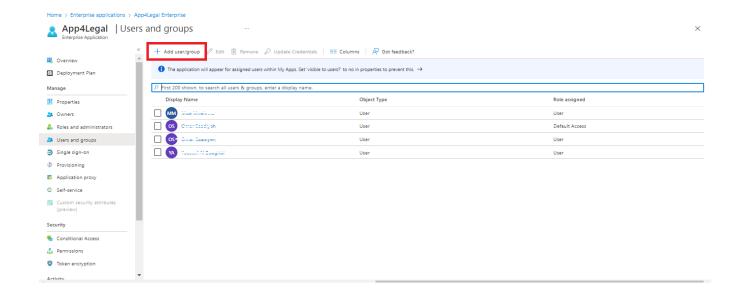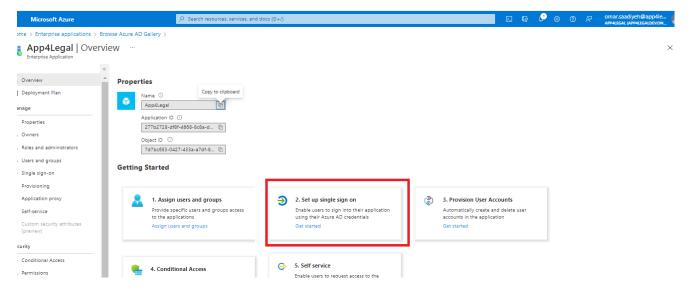6. Name the application, and Create.

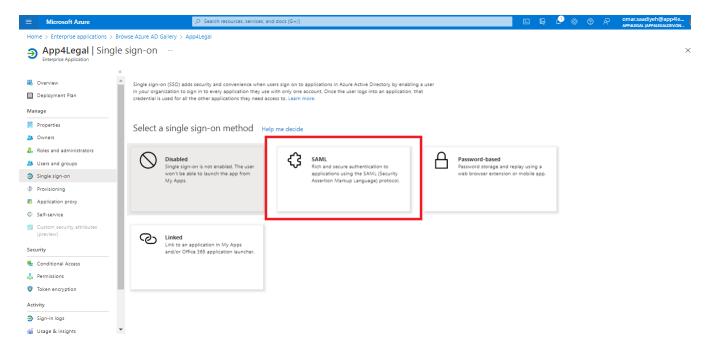## Assign users and groups

Only the assigned users/groups will be able to sign in to this application.

Setup Single sign-on

Basic SAML Configuration

1. Select **Edit**.
2. Setup the below and Save.

Identifier (Entity ID)	`https://site.app4legal.com/xxxx/`
Reply URL (Assertion Consumer Service URL)	`https://site.app4legal.com/xxxx/saml/www/module.php/saml/sp/saml2-acs.php/app4legal-azure_ad`
Sign on URL	`https://site.app4legal.com/xxxx/users/login_idps/azure_ad/`

Obtain Federation Metadata XML

1. Go to **SAML Signing Certificate.**
2. Download **Federation Metadata XML** *(to be imported as Metadata File at LEXZUR)*.

Obtain Client ID & Client Secret

1. From **App registrations** in Azure AD, select your application.
2. Select **Overview**.
3. Copy **Application (client) ID** *(to be pasted as Client ID at LEXZUR)*.
4. Select **Certificates & secrets**.
5. Select **Client secrets New client secret**.
6. Provide a description of the secret, and a duration. When done, select **Add**.
7. After saving the client secret, the value of the client secret is displayed. **Copy this value because you won't be able to retrieve the key later** *(to be pasted as Client Secret at LEXZUR).*

Client Secret

blocked URL

API Permissions

1. Select **API Permissions.**

2. Select **Add a permission Microsoft Graph**.
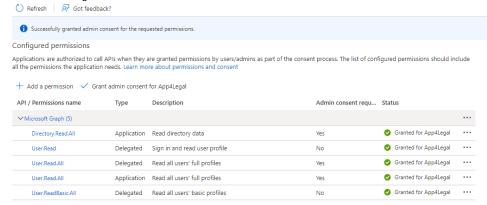3. Add the Following Permission.

Refresh | Got feedback?

ℹ Successfully granted admin consent for the requested permissions.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

+ Add a permission ✓ Grant admin consent for App4Legal

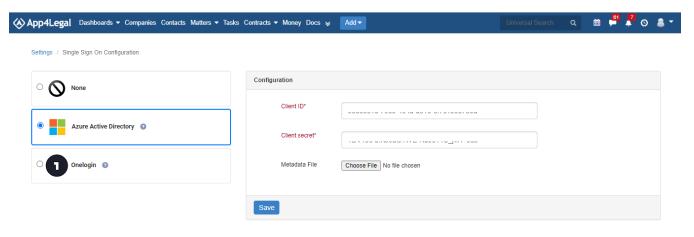| API / Permissions name	Type	Description	Admin consent requ...	Status	
⌄ Microsoft Graph (5)					...
Directory.Read.All	Application	Read directory data	Yes	✓ Granted for App4Legal	...
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for App4Legal	...
User.Read.All	Delegated	Read all users' full profiles	Yes	✓ Granted for App4Legal	...
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for App4Legal	...
User.ReadBasic.All	Delegated	Read all users' basic profiles	No	✓ Granted for App4Legal	...

4. Don't forget to grant admin consent for these permissions.

Configure LEXZUR as SAML Service Provider
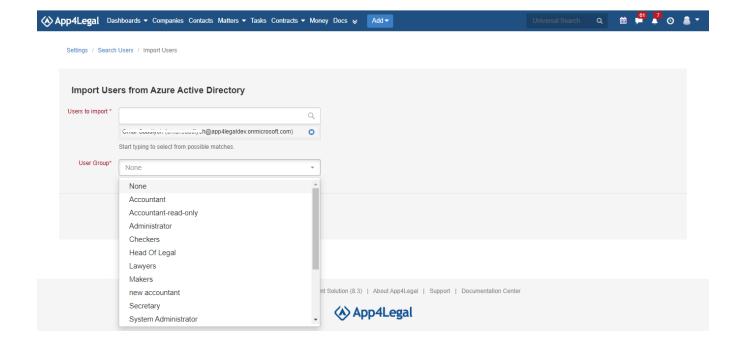
Enable SSO in LEXZUR

1. Sign in to your LEXZUR instance LEXZUR.
2. Go to the **Settings Single Sign On Setup** .
3. Select **Azure Active Directory**
4. Paste **Client ID** & **Client Secret** *(copied before from Azure AD)*.
5. Upload **Metadata File** *(downloaded before from Azure AD)*.
6. Click Save

Import Users from Azure AD to LEXZUR

1. Go to the **Settings Users & Permissions Import Users from Azure Active Directory**.
2. Look up the users and choose the appropriate User Group.

For more information about LEXZUR, kindly reach out to us at help@lexzur.com.

Thank you!