

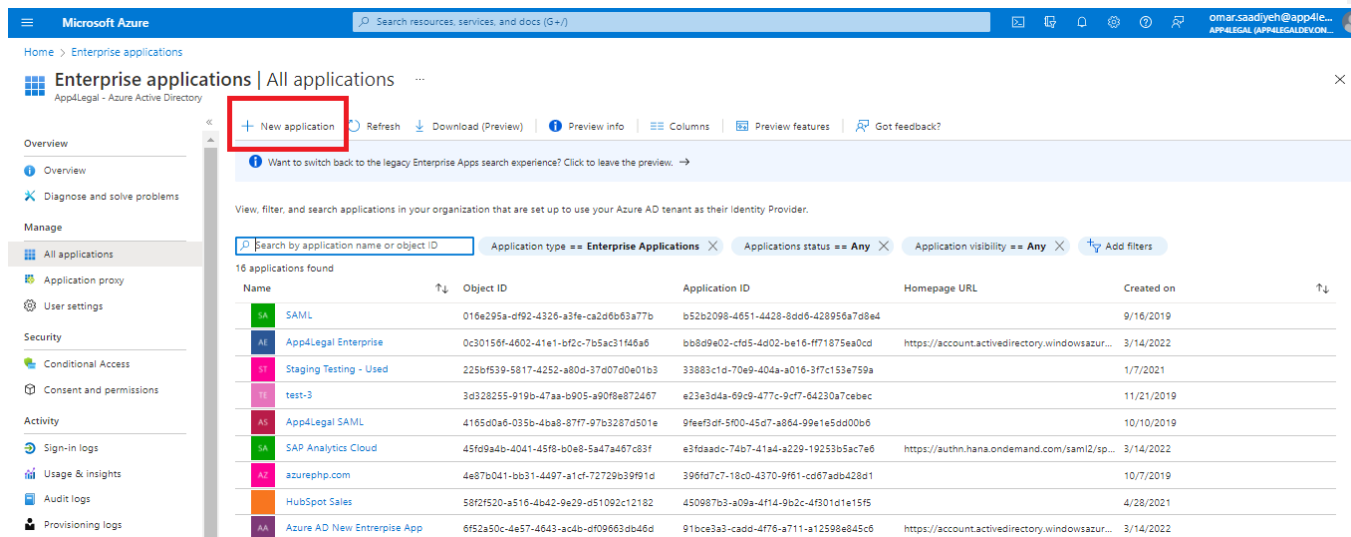
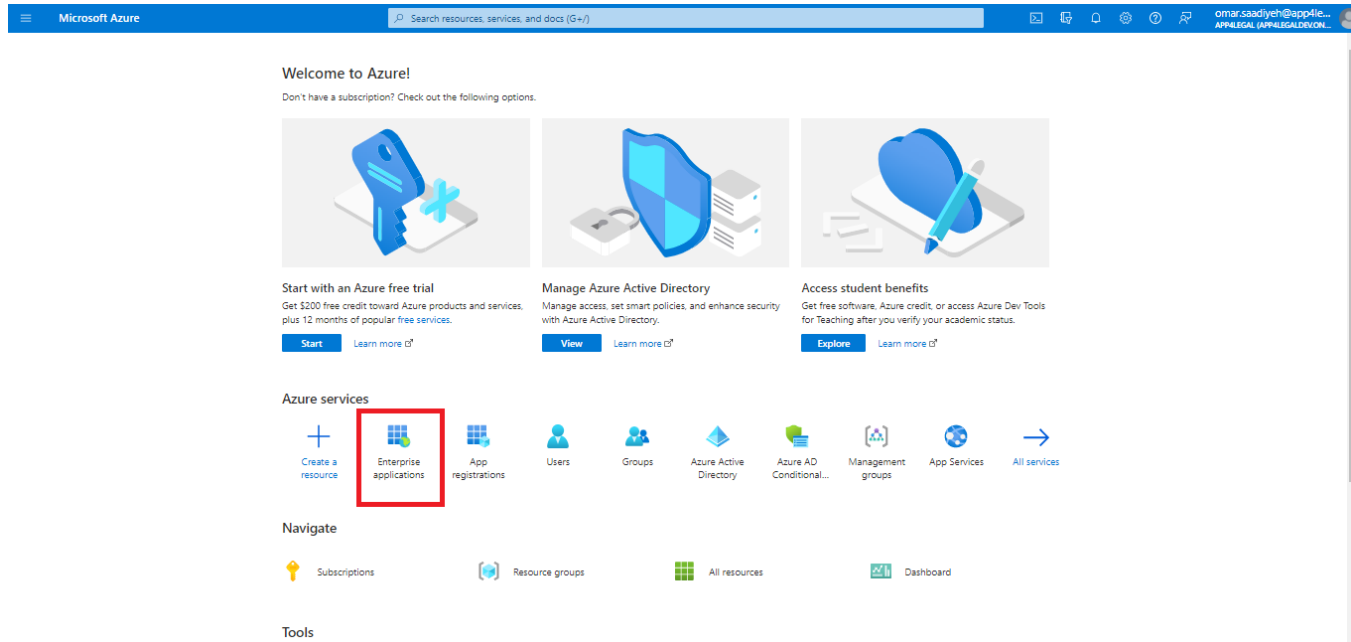
Azure Active Directory SSO Integration

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.



Microsoft Azure

Home > Enterprise applications > Browse Azure AD Gallery

+ Create your own application | Request new gallery app | Got feedback?

The Azure AD App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from the gallery, you can create your own application here.

Search application

Single Sign-on: All | User Account Management: All | Categories: All

Cloud platforms

Amazon Web Services (AWS)

Google Cloud Platform

Oracle

On-premises applications

Add an on-premises application

Learn about Application Proxy

Manage Application Proxy

Federated SSO | Provisioning

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?

App4Legal

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-owners: developers)

Integrate any other application you don't find in the gallery (Non-gallery)

We found the following applications that may match your entry

We recommend using gallery applications when possible.

PEGA

Create

Assign users and groups

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

Microsoft Azure

Home > Enterprise applications > Browse Azure AD Gallery > App4Legal | Overview

Overview

Deployment Plan

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Custom security attributes (preview)

Security

Conditional Access

Permissions

Token encryption

Activity

Sign-in logs

Usage & Insights

Properties

Name

App4Legal

Copy to clipboard

Application ID

277b2728-df8f-4668-8c8a-d...

Object ID

7d7bc653-0427-433a-a7df-8...

Getting Started

1. Assign users and groups

Provide specific users and groups access to the applications

Assign users and groups

2. Set up single sign on

Enable users to sign into their application using their Azure AD credentials

Get started

3. Provision User Accounts

Automatically create and delete user accounts in the application

Get started

4. Conditional Access

Secure access to this application with a customizable access policy.

Create a policy

5. Self service

Enable users to request access to the application using their Azure AD credentials

Get started

Home > Enterprise applications > App4Legal Enterprise

App4Legal | Users and groups

Overview | Deployment Plan | Manage | Properties | Owners | Roles and administrators | Users and groups | Single sign-on | Provisioning | Application proxy | Self-service | Custom security attributes (preview) | Security | Conditional Access | Permissions | Token encryption

+ Add user/group | Edit | Remove | Update Credentials | Columns | Got feedback?

The application will appear for assigned users within My Apps. Set 'Visible to users?' to no in properties to prevent this. →

First 200 shown, to search all users & groups, enter a display name.

	Display Name	Object Type	Role assigned
☐	MM Mike M...@m...@m...	User	User
☐	OS Omar Saadiyeh	User	Default Access
☐	OS Omar Saadiyeh	User	User
☐	YA Youssef A. Saadiyeh	User	User

Setup Single sign-on

Microsoft Azure | Search resources, services, and docs (G+I)

Home > Enterprise applications > Browse Azure AD Gallery >

App4Legal | Overview

Overview | Deployment Plan | Manage | Properties | Owners | Roles and administrators | Users and groups | Single sign-on | Provisioning | Application proxy | Self-service | Custom security attributes (preview) | Security | Conditional Access | Permissions

Properties

Name App4Legal [Copy to clipboard](#)

Application ID 277b2728-df8f-4668-8c8a-d...

Object ID 7d7bc693-0427-433a-a7df-8...

Getting Started

- 1. Assign users and groups**
Provide specific users and groups access to the applications
[Assign users and groups](#)
- 2. Set up single sign on**
Enable users to sign into their application using their Azure AD credentials
[Get started](#)
- 3. Provision User Accounts**
Automatically create and delete user accounts in the application
[Get started](#)
- 4. Conditional Access**
- 5. Self service**
Enable users to request access to the

Microsoft Azure

Home > Enterprise applications > Browse Azure AD Gallery > App4Legal

App4Legal | Single sign-on

Overview

Deployment Plan

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Custom security attributes (preview)

Security

Conditional Access

Permissions

Token encryption

Activity

Sign-in logs

Usage & insights

Select a single sign-on method [Help me decide](#)

Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

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

Password-based
Password storage and replay using a web browser extension or mobile app.

Linked
Link to an application in My Apps and/or Office 365 application launcher.

Basic SAML Configuration

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

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

Microsoft Azure

Home > Enterprise applications > Browse Azure AD Gallery > App4Legal

App4Legal | SAML-based Sign-on

Overview

Deployment Plan

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Custom security attributes (preview)

Security

Conditional Access

Permissions

Token encryption

Activity

Sign-in logs

Usage & insights

Audit logs

Provisioning logs

Access reviews

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 App4Legal.

1 [Edit](#)

Basic SAML Configuration

Identifier (Entity ID)

Reply URL (Assertion Consumer Service URL)

Sign on URL (Optional)

Relay State (Optional)

Logout URL (Optional)

Attributes & Claims

Fill out required fields in Step 1

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

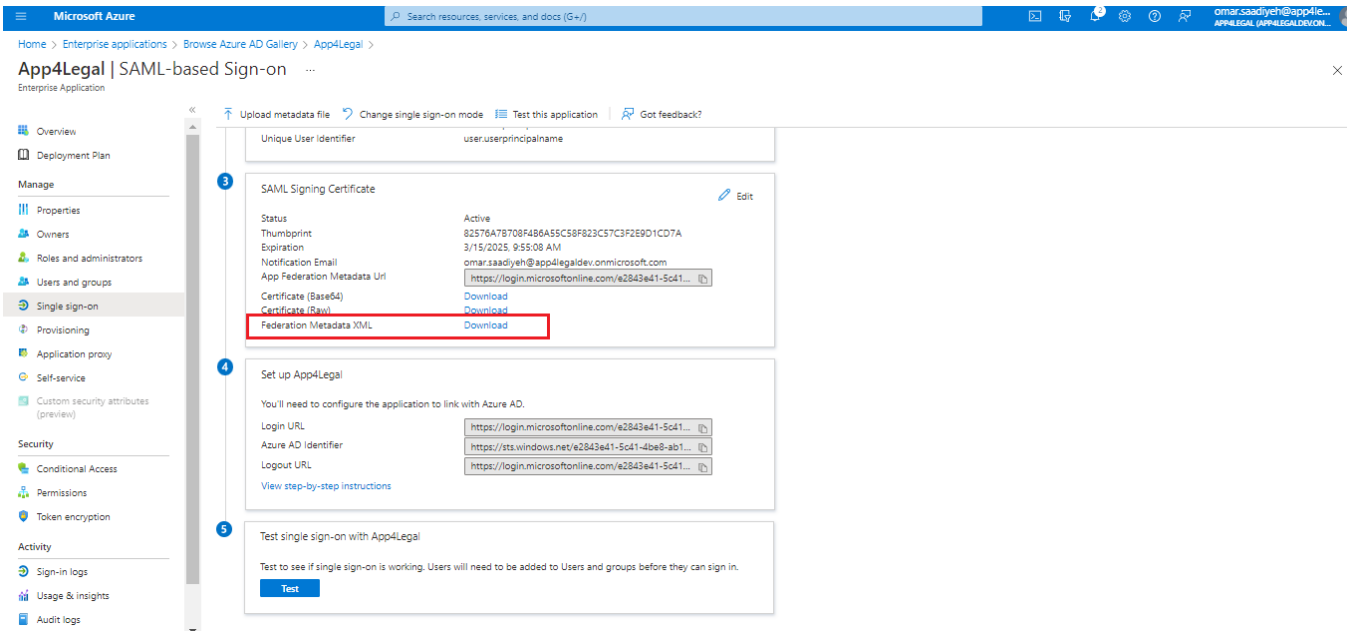
SAML Signing Certificate

Fill out required fields in Step 1

Status	Active
Thumbprint	8D2D57A353960E3FF9DAF6F18D82F40ED96CC7
Expiration	1/31/2027, 1:06:14 AM
Notification Email	omar.saadiyeh@app4legaldev.onmicrosoft.com
App Federation Metadata URL	https://login.microsoftonline.com/62843e41-5c41-4b4a-b0e0-000000000000/...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

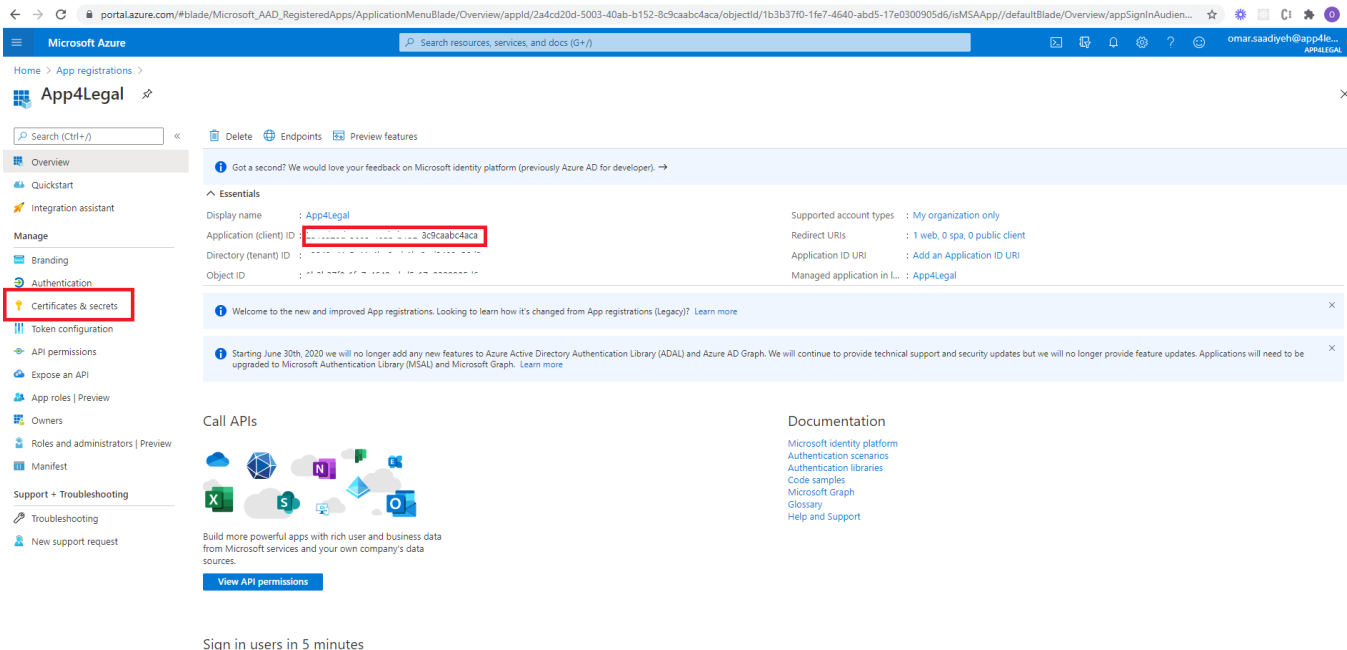
Obtain Federation Metadata XML

1. Go to **SAML Signing Certificate**.
2. Download **Federation Metadata XML** (to be imported as Metadata File at App4Legal).



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 App4Legal).
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 App4Legal).



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 App4Legal as SAML Service Provider

Enable SSO in App4Legal

1. Sign in to your App4Legal instance [App4Legal](#).
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

App4Legal
Dashboards ▾
Companies
Contacts
Matters ▾
Tasks
Contracts ▾
Money
Docs ▾
Add ▾
Universal Search
61
7

Settings / Single Sign On Configuration

☐ None

☒ Azure Active Directory ⓘ
☐ OneLogin ⓘ

Configuration

Client ID*

Client secret*

Metadata File
 No file chosen

Import Users from Azure AD to App4Legal

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

Import Users from Azure Active Directory

Users to import *

Crane Search (crane@app4legaldev.onmicrosoft.com)

Start typing to select from possible matches.

User Group*

None

None

Accountant

Accountant-read-only

Administrator

Checkers

Head Of Legal

Lawyers

Makers

new accountant

Secretary

System Administrator