

# SSO against MS-Azure Active Directory

This article describes how to configure your Microsoft Azure Active Directory to enable Imagicle users to login to web portal, gadgets and Attendant Console with Single Sign-on using the Azure credentials.

Instructions are provided for both SAML and OpenID Connect SSO protocols.

## Prerequisites

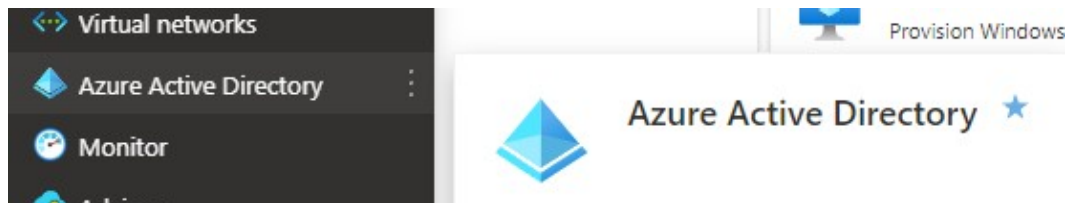
In order to successfully configure your Azure AD, you should have the following data:

- **User Pool ID (SAML only)**
- **Redirect URI**

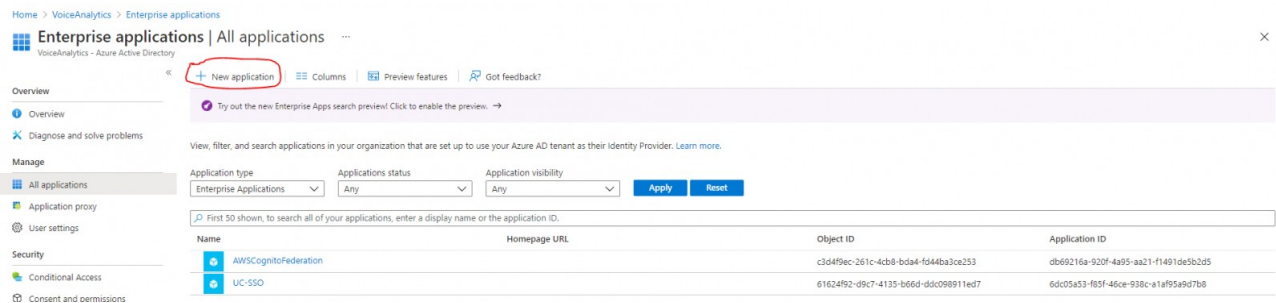
More details are available [here](#).

## Procedure for SAML-based SSO

1. Login to Azure web portal as Administrator
2. Select **Azure Active Directory**



3. Select **"Enterprise Applications"** from the left menu panel
4. Click on **"New Application"** on the top command bar



5. Click on **"Create your own application"**
6. Insert a name and select the option **"Integrate any other application you don't find in the gallery (Non-gallery)"**

# 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?

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)

- 7. Hit **"Create"** and wait for the app creation
- 8. Once the app creation is accomplished, you are redirected to the app properties
- 9. Select **"Single Sign-on"** from the left menu panel

Imagicle SSO | Overview  
Enterprise Application

Overview  
Deployment Plan

Manage

Properties  
Owners  
Roles and administrators (Preview)  
Users and groups  
Single sign-on  
Provisioning

Propert


- 10. Select **"SAML"** sign-on method
- 11. Within "Basic SAML configuration" section, click **"Edit"** link

## 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 Imgicle SSO.

1

Basic SAML Configuration		 Edit
Identifier (Entity ID)	<b>Required</b>	
Reply URL (Assertion Consumer Service URL)	<b>Required</b>	
Sign on URL	Optional	
Relay State	Optional	
Logout Url	Optional	

12. In **Identifier (Entity ID)** field, please enter the **User Pool ID**

13. In **Reply URL** field, please enter the **Redirect URI**

14. In "**User Attribute & Claims**" section, please set the "Emailaddress" attribute to **user.mail**

User Attributes & Claims		 Edit
givenname	user.givenname	
surname	user.surname	
<b>emailaddress</b>	<b>user.mail</b>	
name	user.userprincipalname	
Unique User Identifier	user.userprincipalname	
Group	user.groups	

15. Hit Save. See below sample:

## Basic SAML Configuration

Save | Got feedback?

Identifier (Entity ID) \* ⓘ

The default identifier will be the audience of the SAML response for IDP-initiated SSO

	Default
<input checked="" type="checkbox"/> <input type="text" value="http://adapplicationregistry.onmicrosoft.com/customappsso/primary"/>	<input checked="" type="checkbox"/> ⓘ
<input checked="" type="checkbox"/> <input type="text" value="urn:amazon:cognito:sp:eu-central-1_yBFmhxxxx"/>	<input type="checkbox"/> ⓘ
<input type="text"/>	

Reply URL (Assertion Consumer Service URL) \* ⓘ

The default reply URL will be the destination in the SAML response for IDP-initiated SSO

	Default
<input checked="" type="checkbox"/> <input type="text" value="https://sso.acme.imagicle.cloud/saml2/idpresponse"/>	<input checked="" type="checkbox"/> ⓘ
<input type="text"/>	

16. From "SAML Signing Certificate" section, please download **"Federation Metadata XML"**:

**3**

### SAML Signing Certificate Edit

Status	Active
Thumbprint	32BE7E01489B7C18A2ECD7758C179B6B16E85D6D
Expiration	10/24/2026, 7:45:56 PM
Notification Email	marco.cerri@imagicle.com
App Federation Metadata Url	<input type="text" value="https://login.microsoftonline.com/969d5b92-bc05..."/>
Certificate (Base64)	<a href="#">Download</a>
Certificate (Raw)	<a href="#">Download</a>
Federation Metadata XML	<a href="#">Download</a>

17. Send the file to **Imagicle Team** to complete the SSO federation.

### Enable users and groups to Single Sign-on authentication to Imagicle Apps

1. Open the Enterprise application above created in step #5
2. Select "Users and Groups" on the left menu panel
3. Click on "Add user/group" item on the top command bar
4. Select all the users or groups you want to grant the access through SSO

### Procedure for OpenID-based SSO

1. Login to Azure web portal as Administrator
2. Select **Azure Active Directory**

## Azure services



3. Select **App registrations** item in the left menu panel
4. Click on **New registration** button

The screenshot shows the 'App registrations' page in the Azure Active Directory portal. The top navigation bar includes 'Microsoft Azure' and a search bar. The breadcrumb trail is 'Home > imagicleucdev'. The page title is 'imagicleucdev | App registrations'. The left-hand navigation pane lists various management options, with 'App registrations' selected. The main content area features a '+ New registration' button circled in red, along with 'Endpoints', 'Troubleshooting', 'Refresh', 'Download', 'Preview features', and 'Got feedback?' links. A notification banner at the top of the main area states: 'Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more'. Below this, there are tabs for 'All applications', 'Owned applications' (selected), and 'Deleted applications'. A search bar prompts 'Start typing a display name to filter these results'. A filter button shows 'Application (client) ID starts with' and an 'Add filters' button. The results section shows '2 applications found' and a table with columns 'Display name' and 'Application (client) ID'.

Display name	Application (client) ID
DI DigitalFaxRum	da34af4b-b01f-47e4-bfac-2f9fc
TE TestSsoOpenId	b6d8ecc1-1371-49de-acde-6c8

5. Fill the mask field as following screenshot (**Redirect URI** provided by Imagicle) and click on **Register** button:

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

Home > imagicleucdev >

## Register an application

The user-facing display name for this application (this can be changed later).

Imagicle SSO ✓

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (imagicleucdev only - Single tenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web  ✓

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

**Register**

6. After app registration is accomplished, please take note of Client ID and Tenant ID values.

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

Home > imagicleucdev >

## Imagicle SSO

Search (Ctrl+/) Delete Endpoints Preview features

- Overview
- Quickstart
- Integration assistant
- Manage
  - Branding
  - Authentication
  - Certificates & secrets
  - Token configuration
  - API permissions

**Essentials**

Display name	: Imagicle SSO	Client credentials	: Add a certificate or secret
Application (client) ID	: c8253dfb-8b0b-4d5e-ad6a-fc73f2658a9f	Redirect URIs	: 1 web, 0 spa, 0 public client
Object ID	: b89ad344-52bd-491b-899b-31b96cfd0d9f	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: 8f8ccdec-23bd-4452-bdb3-bec80c415a99	Managed application in l...	: Imagicle SSO

Supported account types : My organization only

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)

7. Now click on "Certificates and secrets" and then on "Client secrets"

Search

- Overview
- Quickstart
- Integration assistant
- Manage
  - Branding & properties
  - Authentication
  - Certificates & secrets**
  - Token configuration
  - API permissions
  - Expose an API
  - App roles
  - Owners
  - Roles and administrators
  - Manifest
- Support + Troubleshooting
  - Troubleshooting
  - New support request

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (1)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
imgicle SSO	11/10/2023	qZD*****	9132a19d-b82f-4b8d-a922-480444263835

8. Create a new client secret with a description and set an expiration (at the expiration, this procedure must be done again, so put an expiration as long as possible)

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (1)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
Imgicle SSO	11/10/2023	qZD*****	9132a19d-b82f-4b8d-a922-480444263835

### Add a client secret

Description:

Expires:

9. After the creation, copy and save the Client Secret Value, highlighted in the below screenshot sample. This must be saved immediately, otherwise, it can't be recovered later and the secret would need to be created from scratch.

Certificates (0) **Client secrets (2)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
.		qZD*****	9132a19d-b82f-4b8d-a922-480444263835
imgicle SSO	14/10/2023	<b>xKc8Q~Z7V0kdgvVKwkPITu0GQMycalK...</b>	2556d6c6-7772-42ae-99f4-...

## imagicle

10. Send to **Imagicle Team** the following data:

- ◆ **Client ID:** previously noted in step #6
- ◆ **Client Secret Value:** previously noted in step #8
- ◆ **Issuer URL:** <https://login.microsoftonline.com/<app-tenant-id>/v2.0> (Tenant ID noted on step #6)