## 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

Home > VoiceAnalytics > Enterprise a Enterprise application VoiceAnalytics - Azure Active Directory	ons   All applications					×
« Overview Overview	New application     E Column     Try out the new Enterprise Apps see	s Preview features	$\mathcal{R}$ Got feedback? eview. $\rightarrow$			
X Diagnose and solve problems Manage	View, filter, and search applications in ye Application type A	our organization that are set up Applications status	to use your Azure AD tenant a Application visibility	as their Identity Provider. Learn more.		
All applications	Enterprise Applications	Any 🗸	Any	✓ Apply Reset		
Application proxy	O first 50 shows to south all of source	linting dislation	and another appellantian in			
User settings	Name	applications, enter a display har	Homepage URL		Object ID	Application ID
Security	AWSCognitoFederation				c3d4f9ec-261c-4cb8-bda4-fd44ba3ce253	db69216a-920f-4a95-aa21-f1491de5b2d5
<ul> <li>Conditional Access</li> <li>Consent and permissions</li> </ul>	o uc-sso				61624f92-d9c7-4135-b66d-ddc098911ed7	6dc05a53-f85f-46ce-938c-a1af95a9d7b8

#### 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

Sot 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?

Imagicle SSO

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   Over	rview
«	
Uverview	Prope
Deployment Plan	8
Manage	
Properties	
A Owners	
& Roles and administrators (Preview)	
Users and groups	Cattin
Single sign-on	Gettin
Provisioning	
10. Select " <b>SAML</b> " sign-on method	

11. Within "Basic SAML configuration" section, click "Edit" link

X

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. Lear more.

Read the configuration guide 🗗 for help integrating Imagicle SSO.

basic SAME Configuration		C Edi
Identifier (Entity ID)	Required	
Reply URL (Assertion Consumer Service URL)	Required	
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	
emailaddress	user.mail	
name	user.userprincipalname	
Unique User Identifier	user.userprincipalname	
Group	user.groups	

15. Hit Save. See below sample:

## **Basic SAML Configuration**

Save Save Got feedback?

#### Identifier (Entity ID) \* 🕕

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

		Defa	ult	
http://adapplicationregistry.onmicrosoft.com/customappsso/primary		$\checkmark$	(i)	Î
urn:amazon:cognito:sp:eu-central-1_yBFmhxxxxx	~		0	Û

#### Reply URL (Assertion Consumer Service URL) \* ①

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

	Def	ault	
https://sso.acme.imagicle.cloud/saml2/idpresponse		0	Î

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

SAME signing Certificate	0 E
Status	Active
Thumbprint	32BE7E01489B7C18A2ECD7758C179B6B16E85D6D
Expiration	10/24/2026, 7:45:56 PM
Notification Email	marco.cerri@imagicle.com
App Federation Metadata Url	https://login.microsoftonline.com/969d5b92-bc05
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

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

+		+	2		2	•	۲		$\rightarrow$
Create a resource	Azure Active Directory	Subscriptions	Users	Bot Services	Quickstart Center	Virtual machines	App Services	Storage accounts	All services

#### 3. Select App registrations item in the left menu panel

4. Click on New registration button

Microsoft Azure	${\cal P}$ Search resources, services, and docs (G+/)	
Home > imagicleucdev		
Azure Active Directory	p registrations 🛷 …	
Overview	+ New registration 🕀 Endpoints 🖉 Troubleshooting 🖒 Refresh 🞍 Download 🖾 Preview features	₽ Got feedback?
<ul> <li>Preview features</li> <li>X Diagnose and solve problems</li> </ul>	Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and N	and Azure AD Graph. We will cont ficrosoft Graph. Learn more
Manage		
🚨 Users	All applications Owned applications Deleted applications	
🎎 Groups	Start typing a display name to filter these results Application (client) ID starts with	$\times$ + Add filters
External Identities		
🎄 Roles and administrators	2 applications found	Application (client) ID
Administrative units	DinitalEavRum	da24af4b b01f 47a4 bfaa 2f0fr
Enterprise applications	TechScoOpenid	649acc1 1271 40da acda 6c0
Devices	Te readoopend	b608ecc1-13/1-49de-acde-6c8
App registrations		
Identity Governance		
Application proxy		

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

	ch resources, services, and docs (G+/)		<b>&gt;</b> 1	} Q	۲	0	ନ
Home > imagicleucdev >							
Register an application							
5							
The user-facing display name for this application (this can be o	hanged later).						
Imagicle SSO		$\checkmark$					
Supported account types							
Who can use this application or access this API?							
Accounts in this organizational directory only (imagicleuc	dev only - Single tenant)						
O Accounts in any organizational directory (Any Azure AD d	rectory - Multitenant)						
O Accounts in any organizational directory (Any Azure AD d	rectory - Multitenant) and personal Microsoft accounts (e.g. Skype	Xbox)					
O Personal Microsoft accounts only							
Help me choose							
Redirect URI (optional)							
We'll return the authentication response to this URI after succe changed later, but a value is required for most authentication	ssfully authenticating the user. Providing this now is optional and i scenarios.	can be					
Web	maidp.auth.eu-central-1.amazoncognito.com/o						
Register an app you're working on here. Integrate gallery apps	and other apps from outside your organization by adding from En	terprise 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.

		es, services, and docs (G+/)		D 🖟 🗘 🍈 Ø R
Home > imagicleucdev >				
🔣 Imagicle SSO	\$			
✓ Search (Ctrl+/)	🔍 📋 Delete 🌐 Endpoin	ts 💀 Preview features		
Uverview	Got a second? We wo	uld love your feedback on Microsoft identity platform (previously Azur	e AD for developer). →	
📣 Quickstart				
🚀 Integration assistant	∧ Essentials			
Manage	Display name	: Imagicle SSO	Client credentials	: Add a certificate or secret
Branding	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
J Authentication	Directory (tenant) ID	: 8f8ccdec-23bd-4452-bdb3-bec80c415a99	Managed application in	I : Imagicle SSO
📍 Certificates & secrets	Supported account typ	es : My organization only		
Token configuration				
API permissions	Welcome to the n	ew 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"

Home > VoiceAnalytics   App registrations >				
👪 Imagicle SSO 👒 …				
₽ Search «				
Overview				
🝊 Quickstart				~
🚀 Integration assistant	Application registration certificates, secret	ts and federated credentia	ils can be found in the tabs below.	~
Manage	Cartificates (0) Client secrets (1)	adarated gradantials ((		
Branding & properties	Certificates (0) Cilent secrets (1)	ederated credentials (t	ŋ	
Authentication	A secret string that the application uses to p	rove its identity when re	equesting a token. Also can be referred to as	application password.
📍 Certificates & secrets	+ New client secret			
Token configuration	Description	Expires	Value 🕕	Secret ID
API permissions	Imagicle SSO	11/10/2023	qZD***********	9132a19d-b82f-4b8d-a922-480444263835 🗅 🣋
🔷 Expose an API				
App roles				
A Owners				
Boles and administrators				
11 Manifest				
Support + Troubleshooting				
Troubleshooting				
New support request				

# 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)

<ul> <li>Application registration certificates,</li> </ul>	secrets and federated credent	ials can be found in the tabs below.	×
Certificates (0) Client secrets (1)	Federated credentials	(0)	
A secret string that the application use	s to prove its identity when	requesting a token. Also can be refer	red to as application password.
+ New client secret			
Description	Expires	Value ①	Secret ID
Imagicle SSO	11/10/2023	qZD*************	9132a19d-b82f-4b8d-a922-4804 3835 🗅 🧯
Add a d	lient secret		×
Description		Imagicle SSO	
Expires		Recommended: 180 days (6 mor	nths) V
9. After the creation, co saved immediately, Certificates (0) <u>Client secrets (2)</u>	opy and save the Clie otherwise, it can't be Federated credentials (0)	ent Secret Value, highlighte e recovered later and the se	d in the below screenshot sample. This must be ecret would need to be created from scratch.
A secret string that the application uses t	o prove its identity when rec	questing a token. Also can be referred	to as application password.
+ New client secret			
Description	Expires	Value 🛈	Secret ID
X		qZD**************	9132a19d-b82f-4b8d-a922 😳 53835 🗅 📋
Imagicle SSO	14/10/2023	xKc8Q~Z7V0kdgvVKwkPITu0GQM	YcaLk 🗅 2556d6c62-42ae-99f4 🗈 🧻

- 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)