

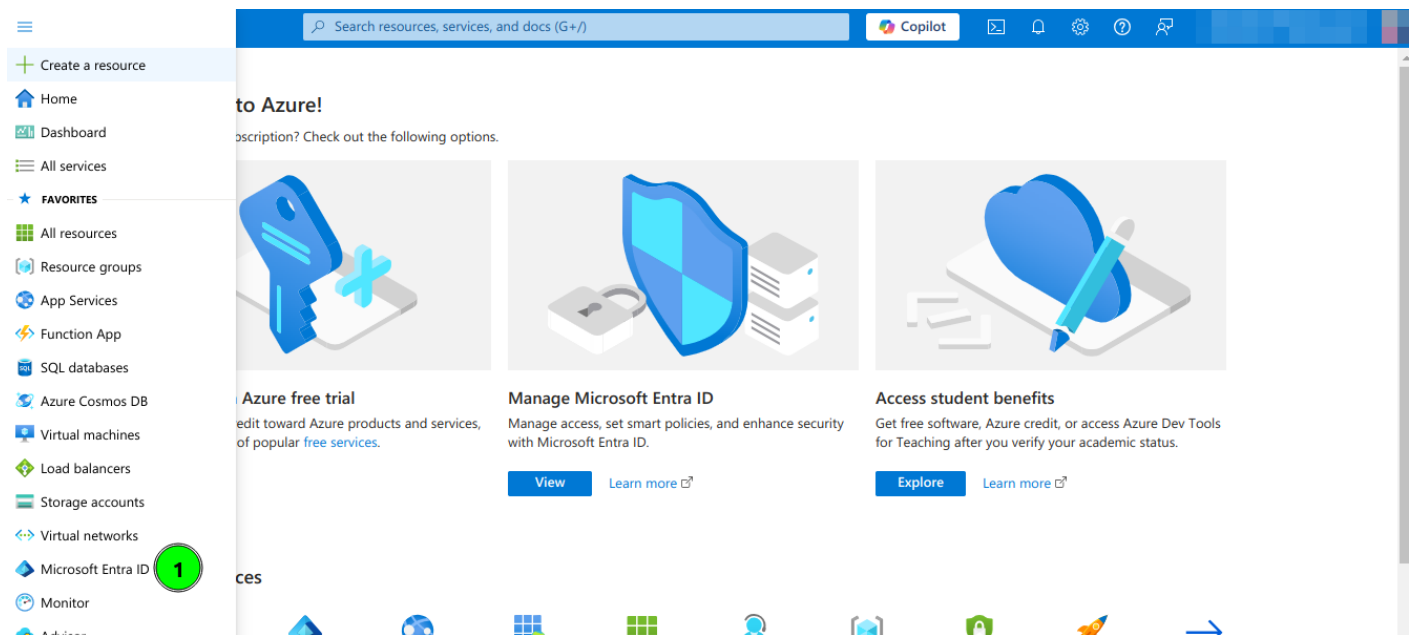
Office 365 as External SAML identity provider

Introduction

Steps to configure Office 365 as External SAML identity provider.

Step-by-Step

1. Open a <https://portal.azure.com>
2. Open **Microsoft Entra ID** and then select **Enterprise applications** option



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

Home > Soffid IAM, S.L. | Overview

Overview Manage tenants What's new Preview features Got feedback?

Overview

Microsoft Entra has a simpler, integrated experience for managing all your Identity and Access Management needs. Try the new Microsoft Entra admin center!

Overview Monitoring Properties Recommendations Setup guides

Search your tenant

Basic information

| | | | |
|----------------|--------------------------------------|--------------|----|
| Name | Soffid IAM, S.L. | Users | 10 |
| Tenant ID | 25bc9848-d3c2-423f-93f1-cf465332a68d | Groups | 5 |
| Primary domain | soffidcom.onmicrosoft.com | Applications | 10 |
| License | Microsoft Entra ID Free | Devices | 1 |

Alerts

Migrate to the converged Authentication methods policy
Please migrate your authentication methods off the legacy MFA and SSPR policies by September 2025 to avoid any service impact

Enterprise applications

3. Select **All applications** and click **New Application**

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

Home > Enterprise applications

Enterprise applications | All applications

New application Refresh Download (Export) Preview info Columns Preview features Got feedback?

Overview

Manage

All applications

Private Network connectors

User settings

App launchers

Custom authentication extensions

Security

Activity

Troubleshooting + Support

View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenant as their Identity Provider.

The list of applications that are maintained by your organization are in [application registrations](#).

Search by application name or object ID Application type == Enterprise Applications Application ID starts with Add filters

11 applications found

| Name | Object ID | Application ID | Homepage URL | Created on | Certificate Expir... | Active Certificat. |
|------|-----------|----------------|--------------|------------|----------------------|--------------------|
| GE | | | | /12/2020 | - | - |
| S | | | | 0/23/2024 | Current | 10/23/2027 |
| SC | | | | /20/2020 | - | - |
| O | | | | /25/2022 | - | - |
| | | | | 0/23/2024 | - | - |
| PA | | | | /29/2020 | - | - |
| TS | | | | 1/28/2023 | - | - |
| AL | | | | /10/2020 | - | - |

4. Select Create your own application

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

Home > Enterprise applications | All applications >

Browse Microsoft Entra Gallery

+ Create your own application | Got feedback?


The Microsoft Entra 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 App Gallery, you leverage prebuilt templates to connect your users more securely to their apps. Browse or create your own application here. If you are wanting to publish an application you have developed into the Microsoft Entra Gallery for other organizations to discover and use, you can file a request using the process described in [this article](#).

Search application


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

Cloud platforms


Amazon Web Services (AWS)



Google Cloud Platform



Oracle



SAP

5. Type the name of your app and select the "Integrate any other application you don't find in the gallery (Non-gallery)" option

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?

pat.soffid.lab 

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 Microsoft Entra ID (App you're developing)
- ☒ Integrate any other application you don't find in the gallery (Non-gallery)

Create

6. Click on **Set up single sign on**

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

Home > Enterprise applications | All applications > Browse Microsoft Entra Gallery >

pat.soffid.lab | Overview Enterprise Application

Overview

- Deployment Plan
- Diagnose and solve problems
- Manage
 - Properties
 - Owners
 - Roles and administrators
 - Users and groups
 - Single sign-on
 - Provisioning
 - Application proxy
 - Self-service
 - Custom security attributes
- Security
- Activity

Properties

Name pat.soffid.lab

Application ID 6bb554ed-b96d-4631-9204-...

Object ID 76afac14-c10f-4dde-94f7-8d...

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 Microsoft Entra credentials
[Get started](#)
- 3. Provision User Accounts**
- 4. Conditional Access**

7. Click the **SAML** option

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

Home > Enterprise applications | All applications > Browse Microsoft Entra Gallery > pat.soffid.lab

pat.soffid.lab | Single sign-on Enterprise Application

Overview

- Deployment Plan
- Diagnose and solve problems
- Manage
 - Properties
 - Owners
 - Roles and administrators
 - Users and groups
 - Single sign-on
 - Provisioning
 - Application proxy
 - Self-service
 - Custom security attributes
- Security
- Activity

Single sign-on (SSO) adds security and convenience when users sign on to applications in Microsoft Entra ID by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. [Learn more.](#)

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.

8. Enter the **Basic SAML Configuration** and Save:

- **Identifier:** https://<YOUR-SERVER>/soffid-iam-console

- **Reply URL:** https://<YOUR-SERVER>/soffid/saml/log/post
- **Sign on URL:** https://<YOUR-SERVER>/soffid/
- **Logout URL:** https://<YOUR-SERVER>/soffid/saml/slo/post

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home > Enterprise applications | All applications > soffid.pat.lab

soffid.pat.lab | SAML-based Sign-on

Enterprise Application

Upload metadata file | Change single sign-on mode | Test this application | Got feedback?

Overview

Deployment Plan

Diagnose and solve problems

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups
- Single sign-on**
- Provisioning
- Application proxy
- Self-service
- Custom security attributes

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 soffid.pat.lab.

1

Basic SAML Configuration

| | |
|--|--|
| Identifier (Entity ID) | https://pat.soffid.lab:8443/soffid-iam-console |
| Reply URL (Assertion Consumer Service URL) | https://pat.soffid.lab:8443/soffid/saml/log/post |
| Sign on URL | https://pat.soffid.lab:8443/soffid/ |
| Relay State (Optional) | Optional |
| Logout Url (Optional) | https://pat.soffid.lab:8443/soffid/saml/slo/post |

1 Edit

2

Attributes & Claims

| | |
|-----------|----------------|
| givenname | user.givenname |
|-----------|----------------|

Edit

Basic SAML Configuration



Save



Got feedback?

Identifier (Entity ID) * ⓘ

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Default

| | | | | |
|---|-------------------------------------|--------------------------|--------------------------------|----------------------------------|
| <input type="text" value="https://pat.soffid.lab:8443/soffid-iam-console"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="text" value="i"/> | <input type="button" value="🗑"/> |
|---|-------------------------------------|--------------------------|--------------------------------|----------------------------------|

[Add identifier](#)

Reply URL (Assertion Consumer Service URL) * ⓘ

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

| | Index | Default |
|---|--------------------------|-------------------------------------|
| <input type="text" value="https://pat.soffid.lab:8443/soffid/saml/log/post"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

[Add reply URL](#)

Sign on URL (Optional)

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

| | |
|--|-------------------------------------|
| <input type="text" value="https://pat.soffid.lab:8443/soffid/"/> | <input checked="" type="checkbox"/> |
|--|-------------------------------------|

Relay State (Optional) ⓘ

The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URI or URI path that takes users to a specific location within the application

9. Configure **Attributes & Claims** and change the attributes and claims to send the mailnickname as the user identifier (nameid)

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home > Enterprise applications | All applications > soffid.pat.lab

soffid.pat.lab | SAML-based Sign-on

Enterprise Application

Upload metadata file

Change single sign-on mode

Test this application

Got feedback?

Overview

Deployment Plan

Diagnose and solve problems

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups
- Single sign-on
- Provisioning
- Application proxy
- Self-service
- Custom security attributes

Security

Activity

Troubleshooting + Support

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 soffid.pat.lab.

1

Basic SAML Configuration

Identifier (Entity ID)

Reply URL (Assertion Consumer Service URL)

Sign on URL

Relay State (Optional)

Logout Url (Optional)

https://pat.soffid.lab:8443/soffid-iam-console

https://pat.soffid.lab:8443/soffid/saml/log/post

https://pat.soffid.lab:8443/soffid/

Optional

https://pat.soffid.lab:8443/soffid/saml/slo/post

Edit

2

Attributes & Claims

givenname

surname

emailaddress

name

Unique User Identifier

user.givenname

user.surname

user.mail

user.userprincipalname

user.mailnickname

Edit

3

SAML Certificates

Attributes & Claims

+ Add new claim

+ Add a group claim

Columns

Got feedback?

Required claim

| Claim name | Type | Value |
|----------------------------------|------|--|
| Unique User Identifier (Name ID) | SAML | <div>1</div> user.mailnickname [nam... *** |

Additional claims

| Claim name | Type | Value |
|---|------|----------------------------|
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd... | SAML | user.mail *** |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname | SAML | user.givenname *** |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name | SAML | user.userprincipalname *** |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname | SAML | user.surname *** |

Advanced settings

10. Copy the App Federation Metadata Url

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

Home > soffid.pat.lab

soffid.pat.lab | SAML-based Sign-on

Enterprise Application

Upload metadata file Change single sign-on mode Test this application Got feedback?

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
 - Properties
 - Owners
 - Roles and administrators
 - Users and groups
 - Single sign-on**
 - Provisioning
 - Application proxy
 - Self-service
 - Custom security attributes
- Security
- Activity
- Troubleshooting + Support

| | |
|------------------------|------------------------|
| givenname | user.givenname |
| surname | user.surname |
| emailaddress | user.mail |
| name | user.userprincipalname |
| Unique User Identifier | user.mainnickname |

SAML Certificates

Token signing certificate [Edit](#)

Status: Active

Thumbprint: 560B064826325CB89FOCE229BDBDEE3A20E64587

Expiration: 10/23/2027, 4:14:18 PM

Notification Email: admin@soffidcom.onmicrosoft.com

App Federation Metadata Url: <https://login.microsoftonline.com/25bc9848-d3c2-423f-93f1-cf465332a68d/> [Download](#)

Certificate (Base64): [Download](#)

Certificate (Raw): [Download](#)

Federation Metadata XML: [Download](#)

Verification certificates (optional) [Edit](#)

| | |
|----------|----|
| Required | No |
| Active | 0 |
| Expired | 0 |

11. Configure the **External SAML identity Provider** in the Soffid Console Authentication page

soffid Search ?

Main Menu > Administration > Configuration > Security settings > Authentication **1**

Global status

☒ Maintenance mode (only administrators can log in)

Message to display before logging in:

Session timeout in minutes:

Username and password

☒ Enabled

☒ Forward authentication requests to trusted target sytems

External SAML identity provider

☒ Enabled **2**

Soffid server host name: **3**

SAML federation metadata URL: **3**

Cache limit (seconds):

Identity provider: **4**

SAML attribute containing user name:

☒ Enable SAML debug log

12. Optional, **enable any user to login**

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home > soffid.pat.lab

soffid.pat.lab | Properties

Enterprise Application

Save Discard Delete Got feedback?

Overview

Deployment Plan

Diagnose and solve problems

Manage

- Properties 1
- Owners
- Roles and administrators
- Users and groups
- Single sign-on
- Provisioning
- Application proxy
- Self-service
- Custom security attributes

Security

Activity

Troubleshooting + Support

View and manage application settings for your organization. Editing properties like display information, user sign-in settings, and user visibility settings requires Global Administrator, Cloud Application Administrator, Application Administrator roles. [Learn more.](#)

If this application resides in your tenant, you can manage additional properties on the [application registration](#).

Enabled for users to sign-in?

Yes No

Name *

soffid.pat.lab

Homepage URL

https://account.activedirectory.windowsazure.com:444/applications/de...

Logo

Select a file

User access URL

https://launcher.myapps.microsoft.com/api/signin/b17d8844-4fac-4f2...

Application ID

b17d8844-4fac-4f2c-863a-59d8be7781f5

Object ID

38283f52-d45b-4306-bef5-1ea73fc7e7ef

Terms of Service Url

Publisher did not provide this information

Privacy Statement Url

Publisher did not provide this information

Reply URL

https://pat.soffid.lab:8443/soffid/saml/log/post

Assignment required?

Yes No 2

Visible to users?

Yes No

Notes

Revision #7

Created 23 October 2024 15:05:19 by pgarcia@soffid.com

Updated 28 October 2024 07:03:14 by pgarcia@soffid.com