Use Case

This folder will contain information about different use cases

- Office 365 as External SAML identity provider

Office 365 as External SAML identity provider

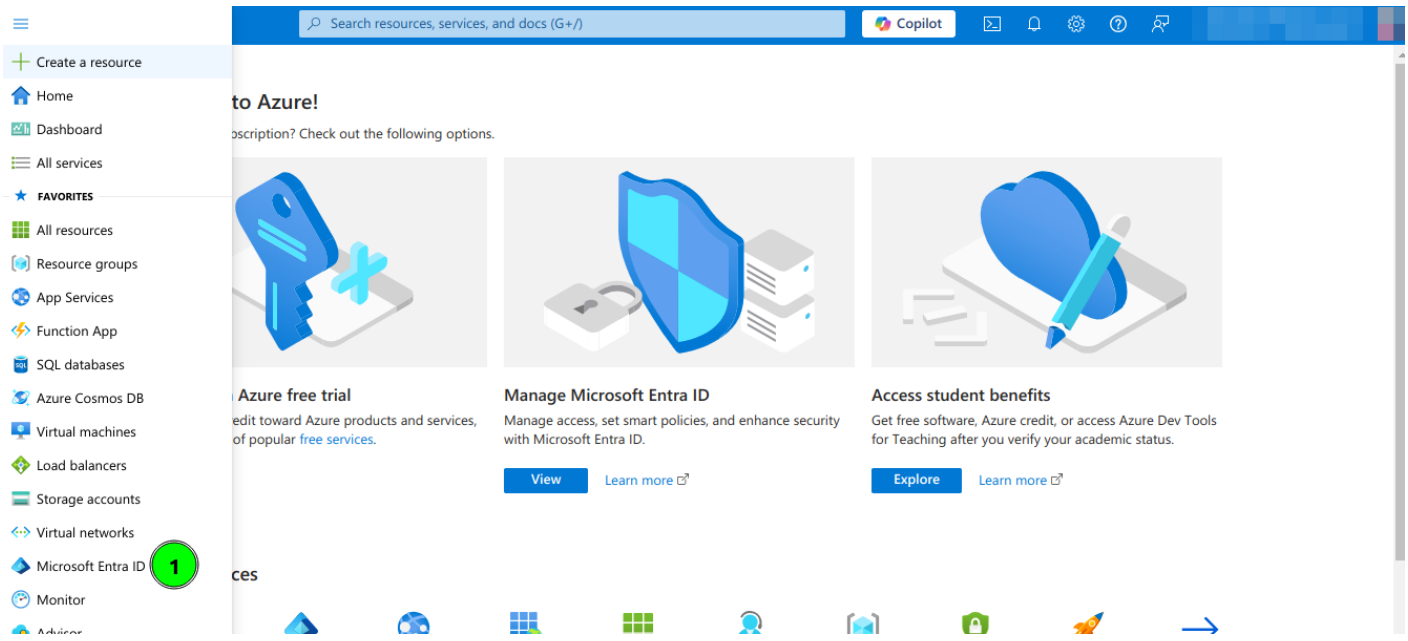
Introduction

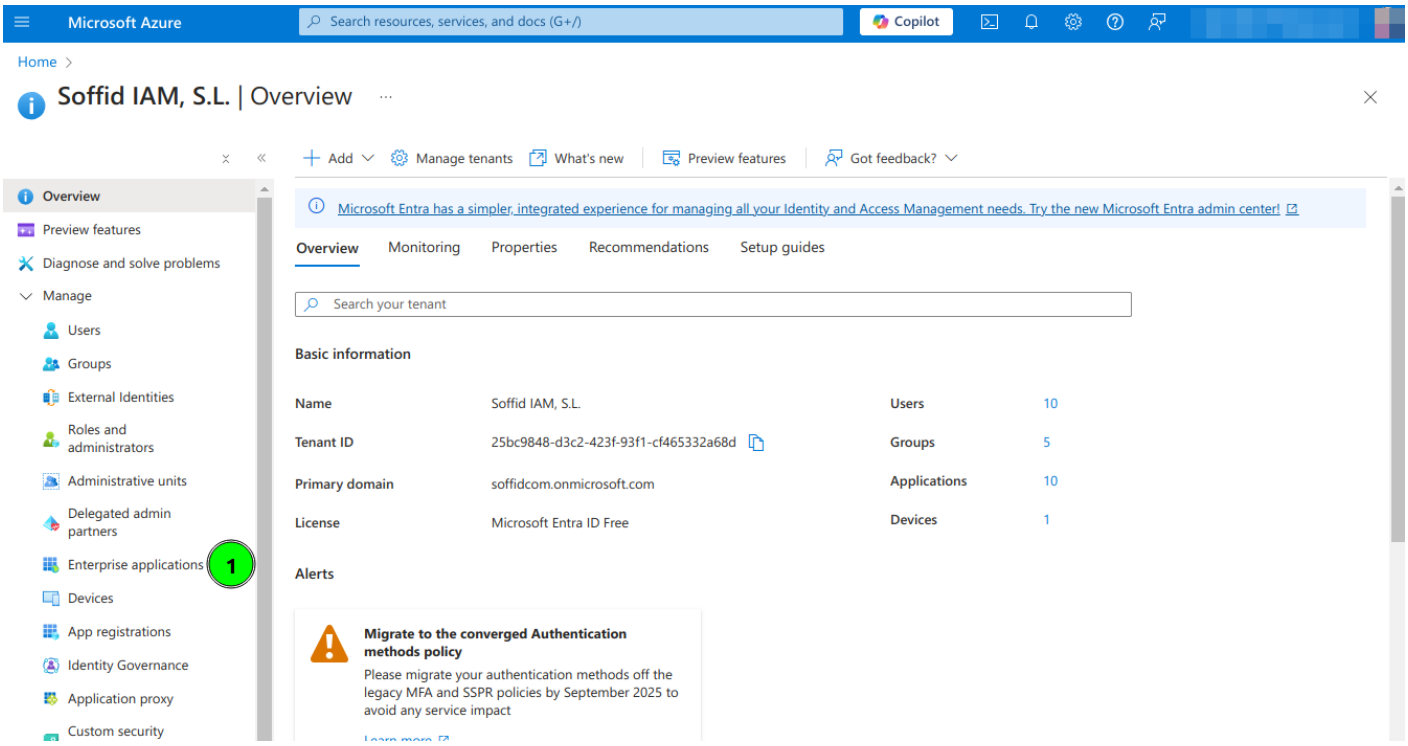
Steps to configure Office 365 as External SAML identity provider.

Step-by-Step

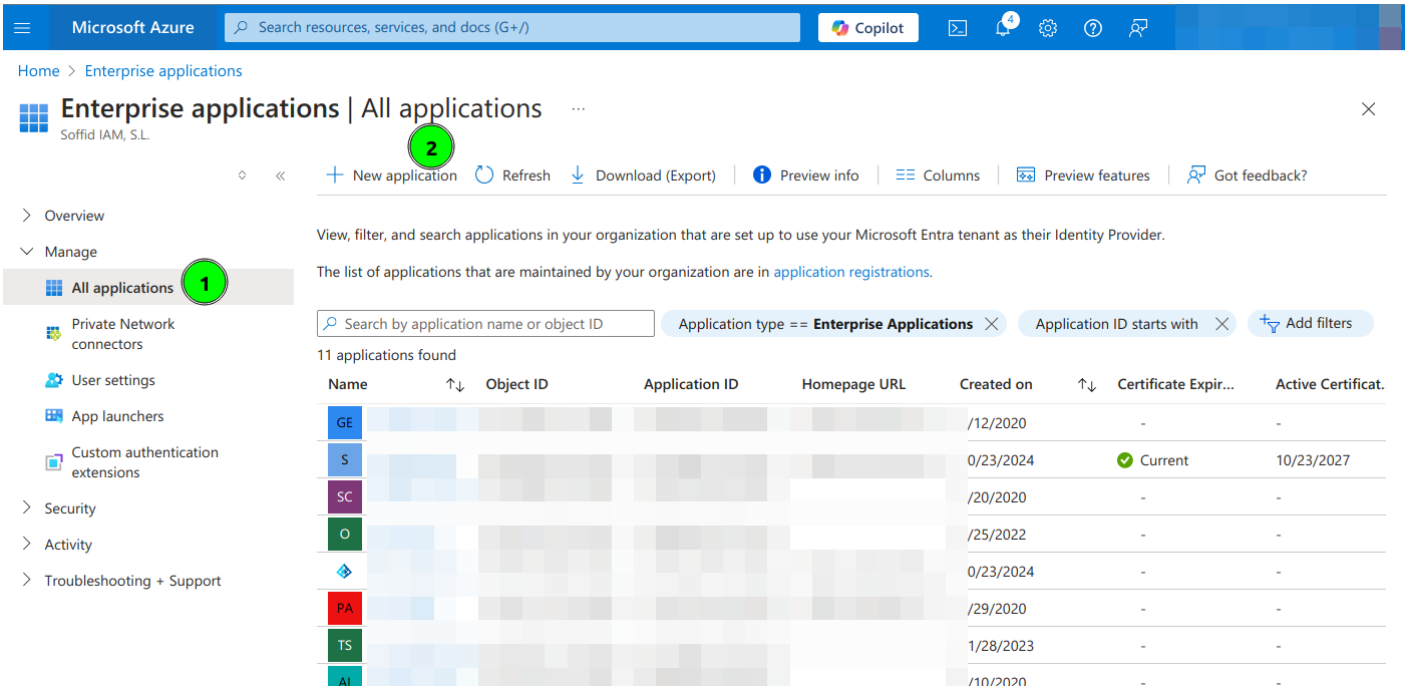
1. Open a https://portal.azure.com

2. Open **Microsoft Entra ID** and then select **Enterprise applications** option

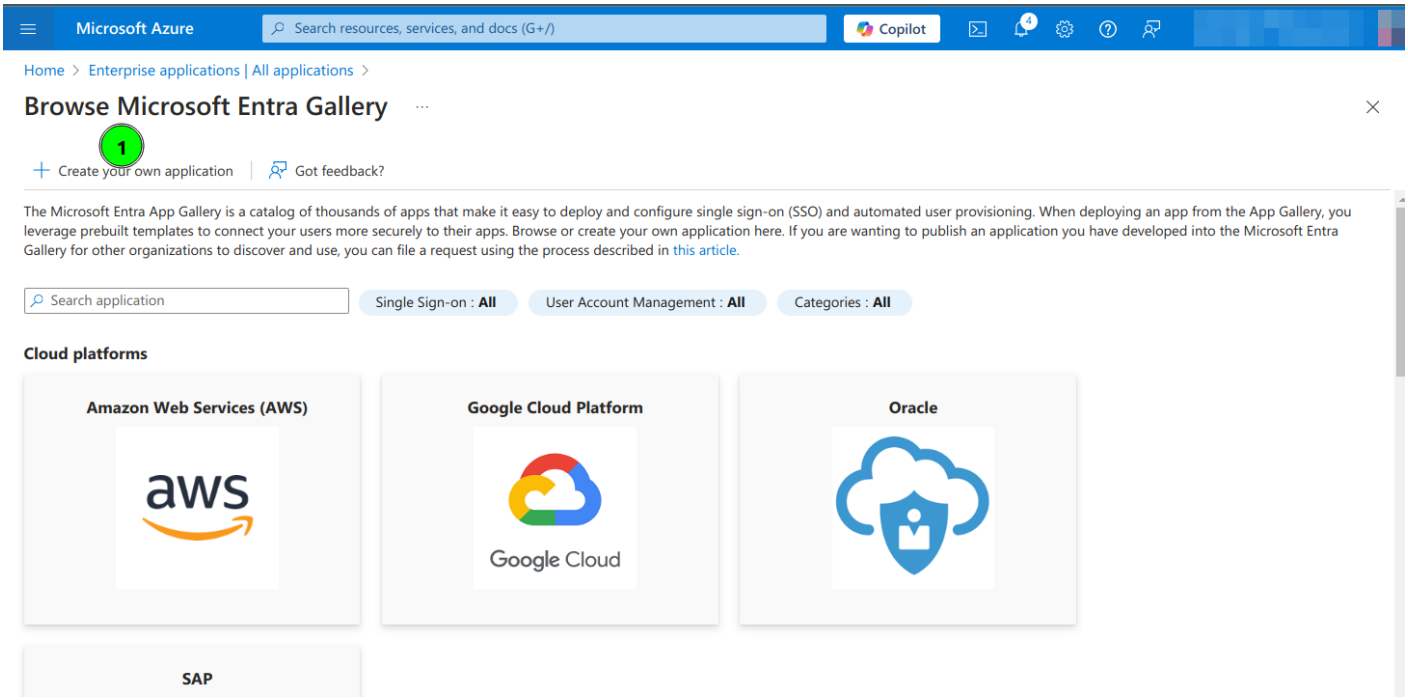




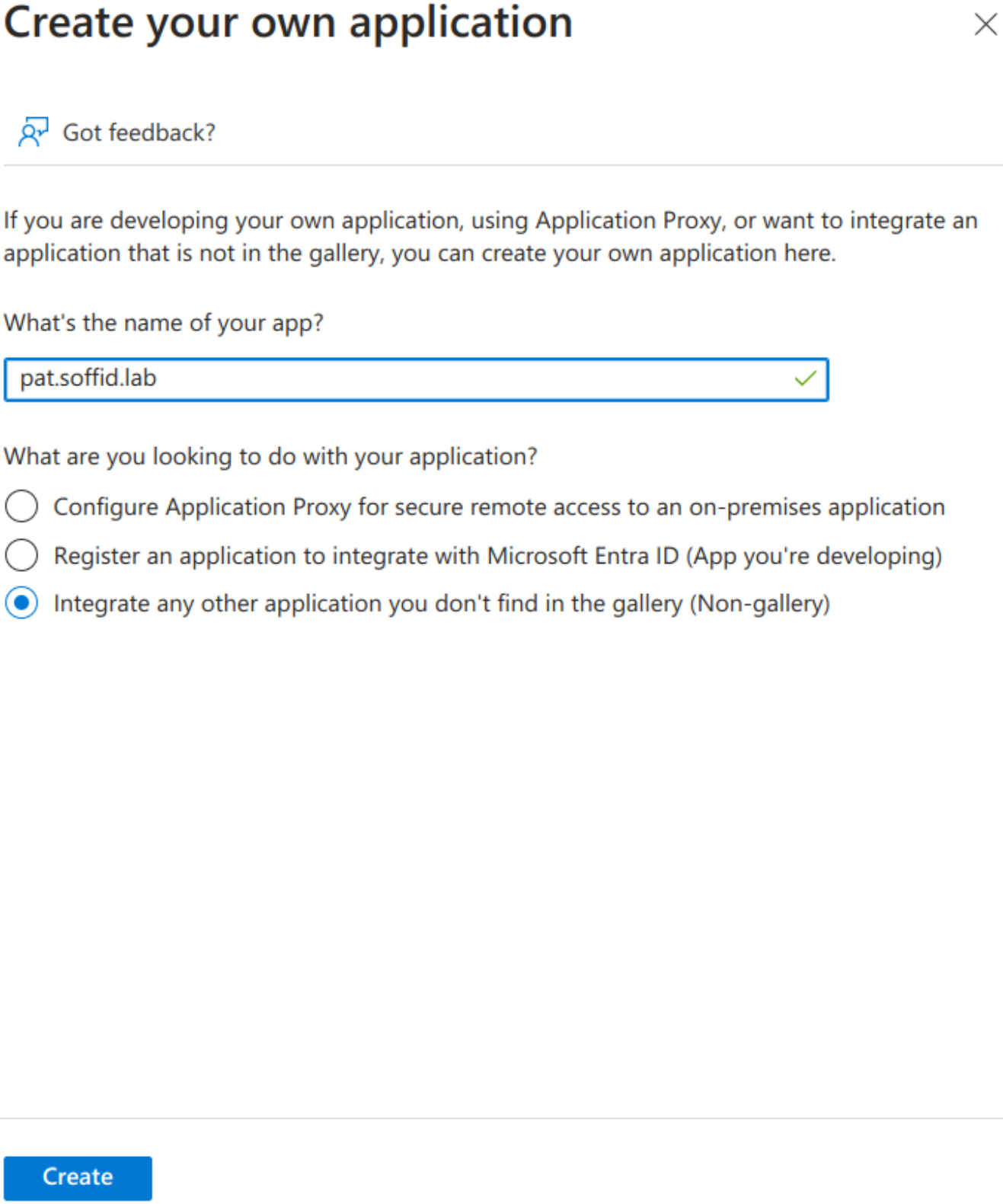
3. Select **All applications** and click **New Application**



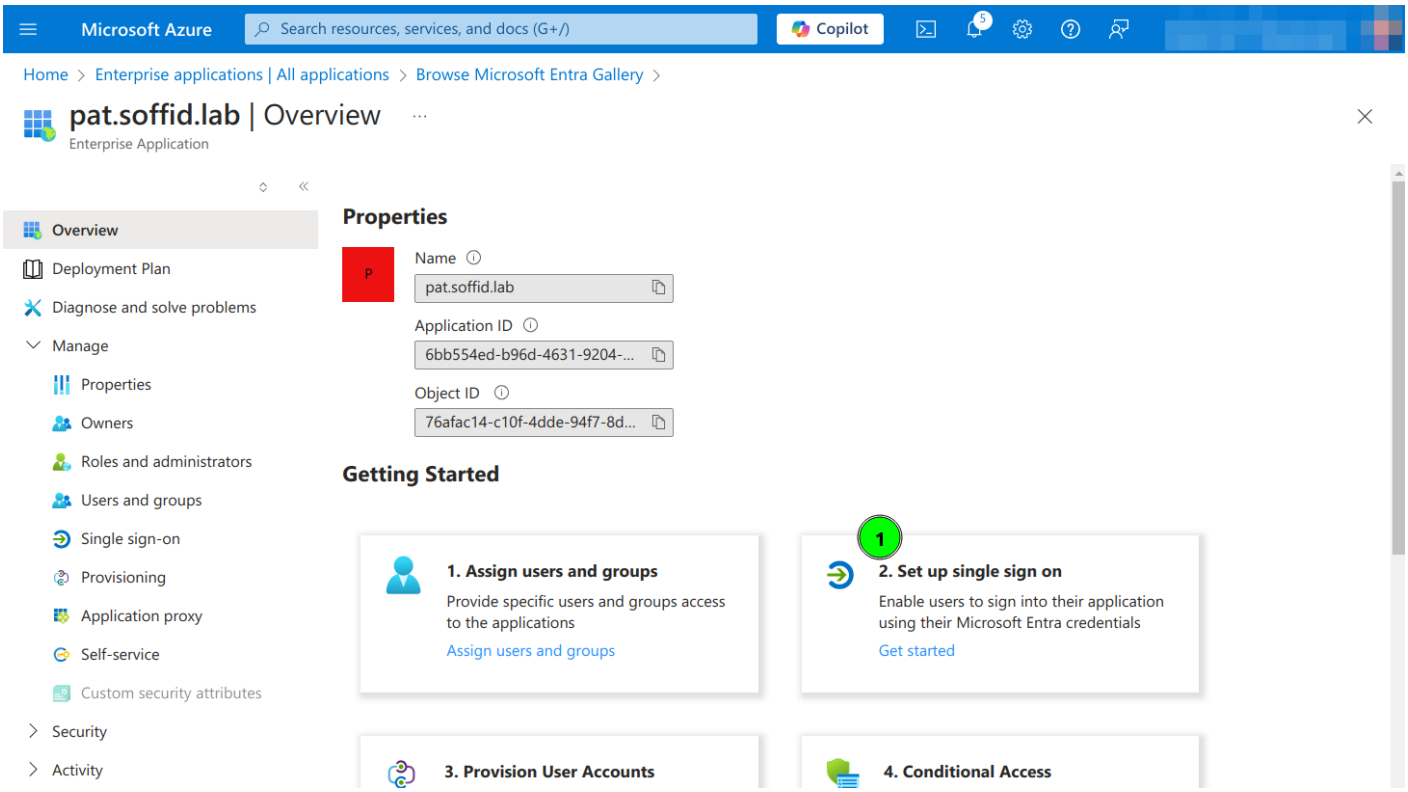
4. Select Create your own application



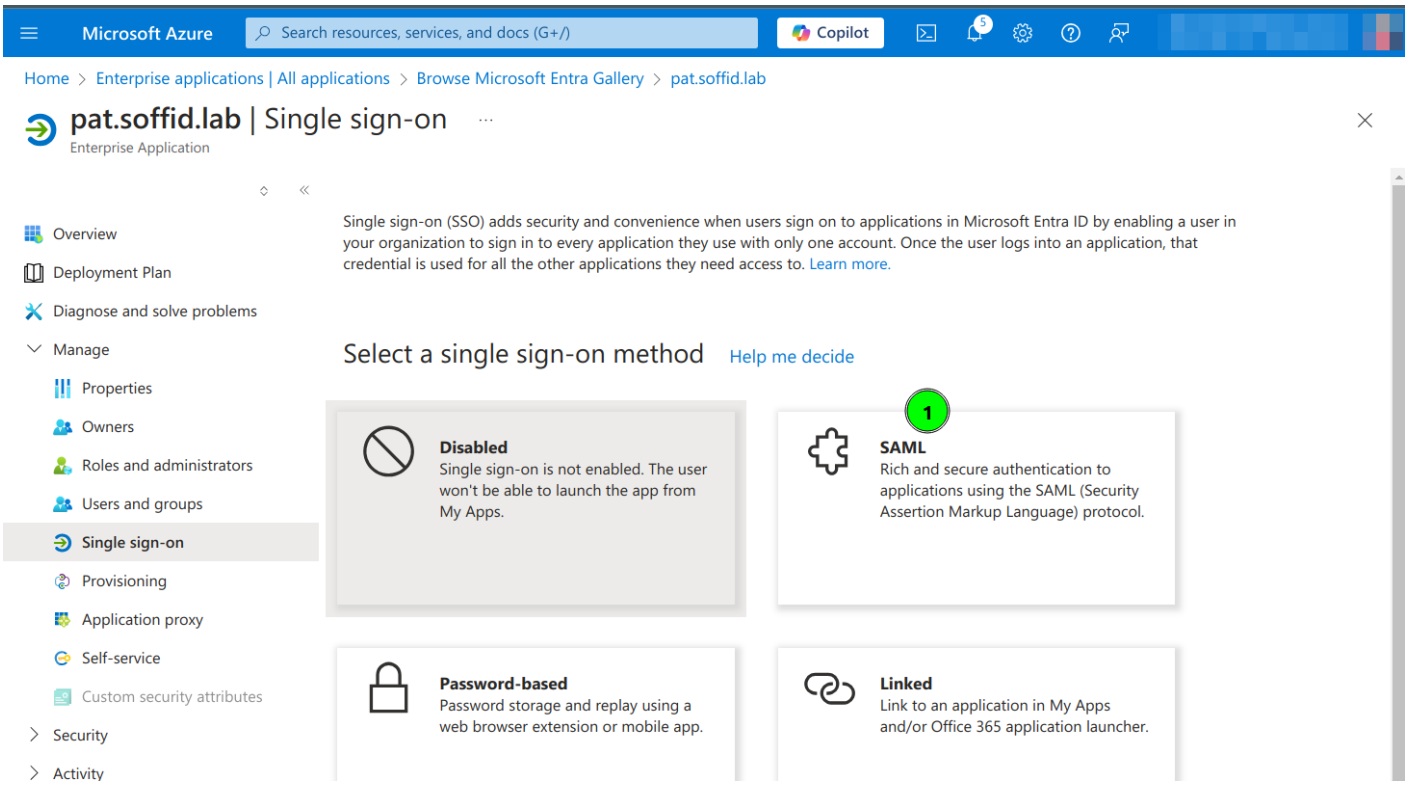
5. Type the name of your app and select the "Integrate any other application you don't find in the gallery (Non-gallery)" option



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



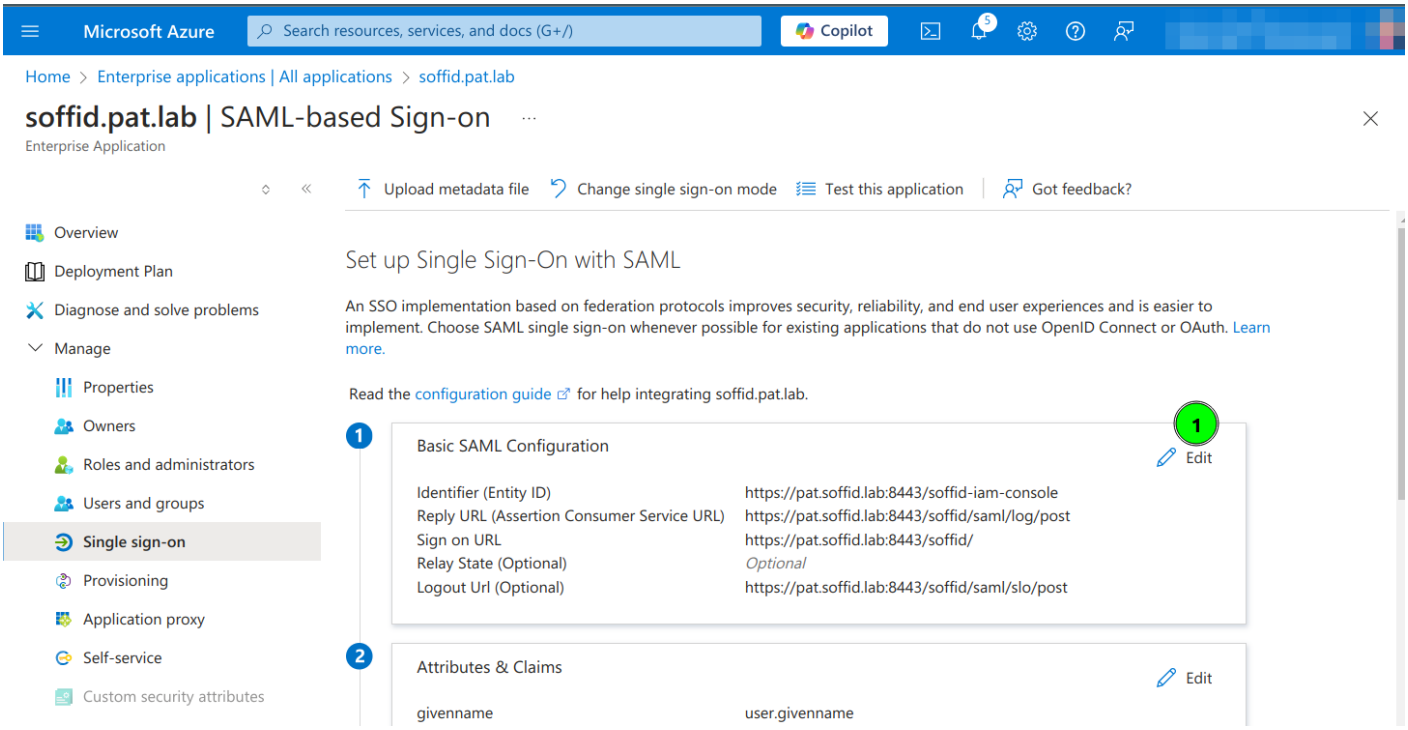
7. Click the **SAML** option

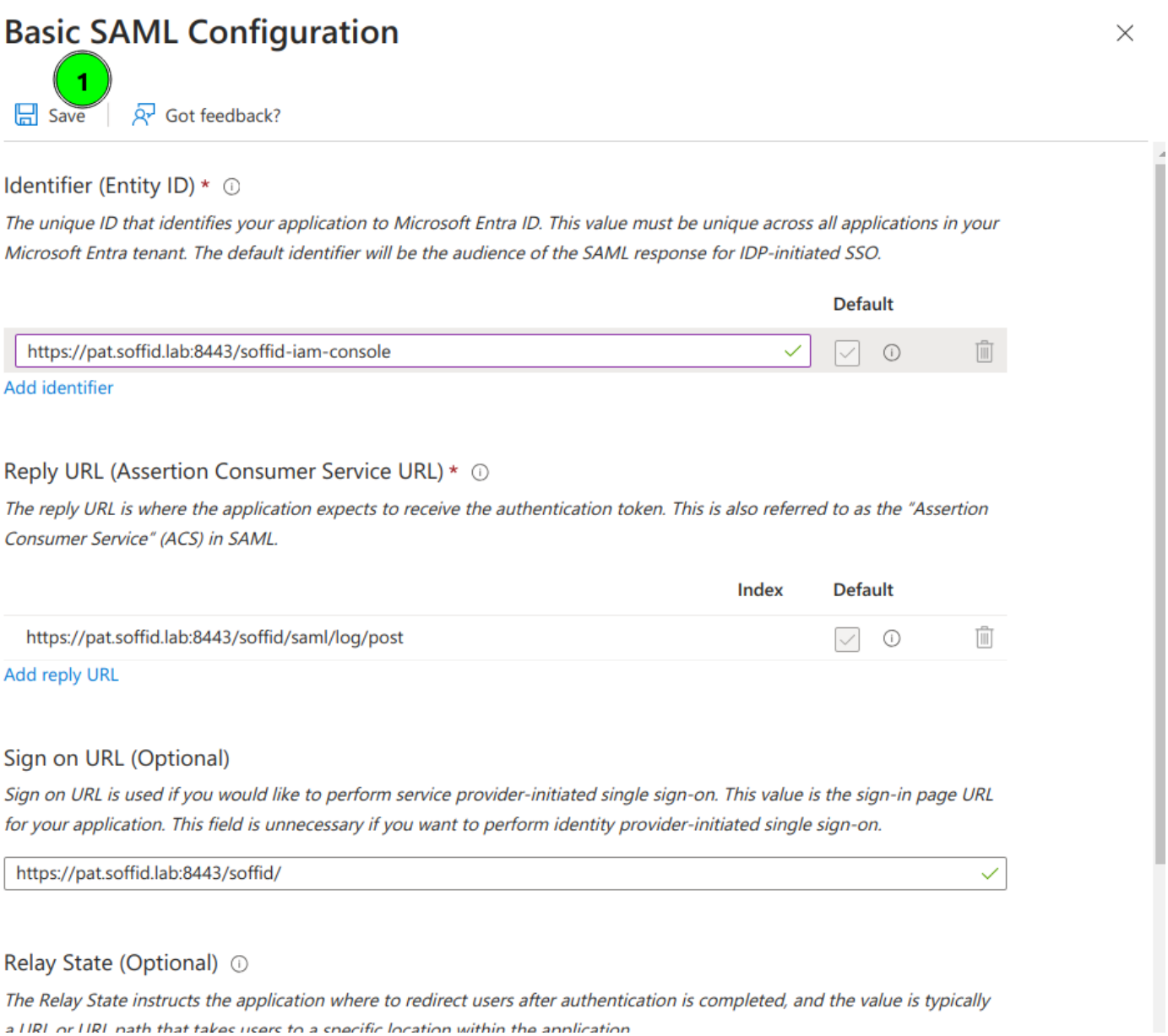


8. Enter the **Basic SAML Configuration** and Save:

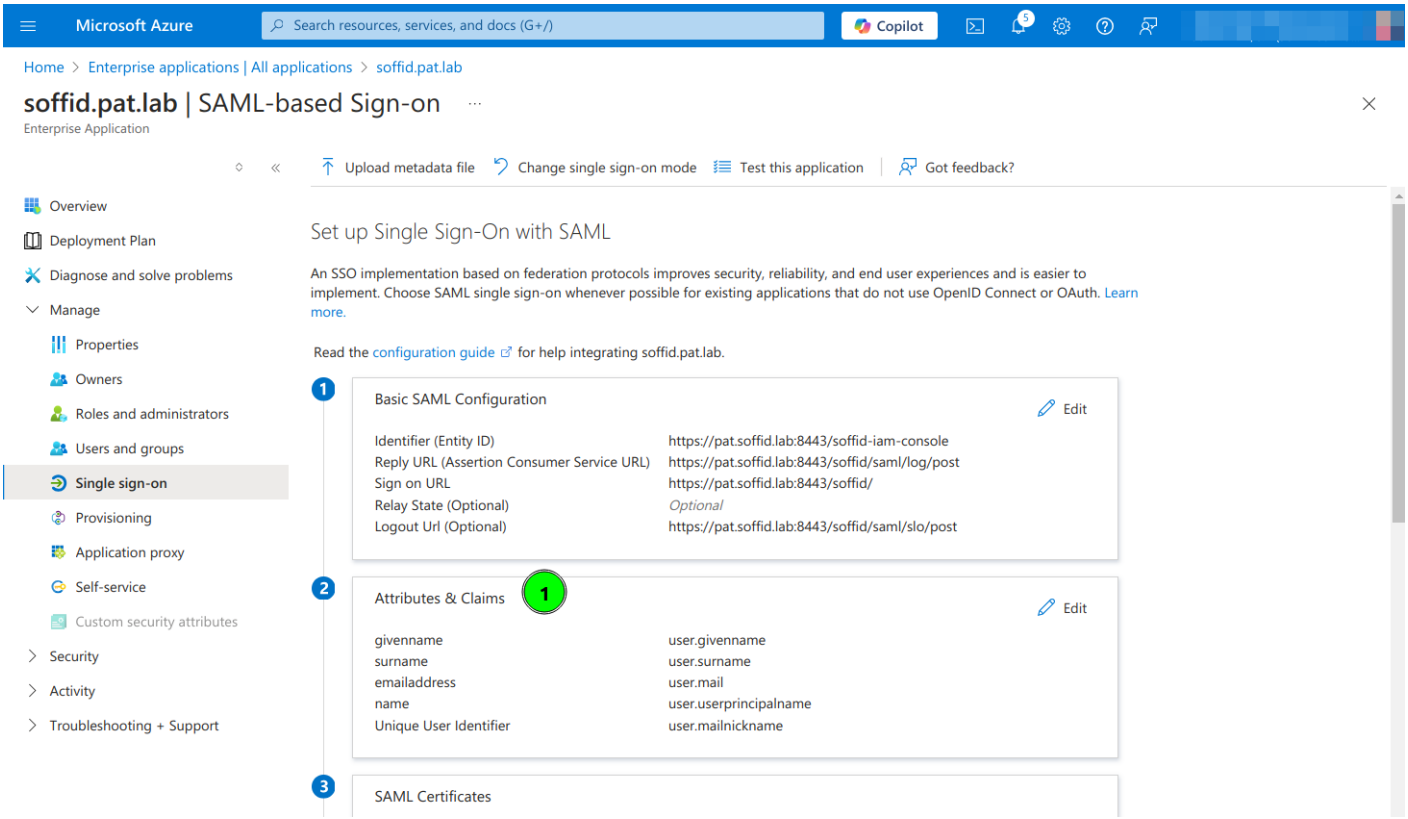
- **Identifier**: https://<YOUR-SERVER>/soffid-iam-console

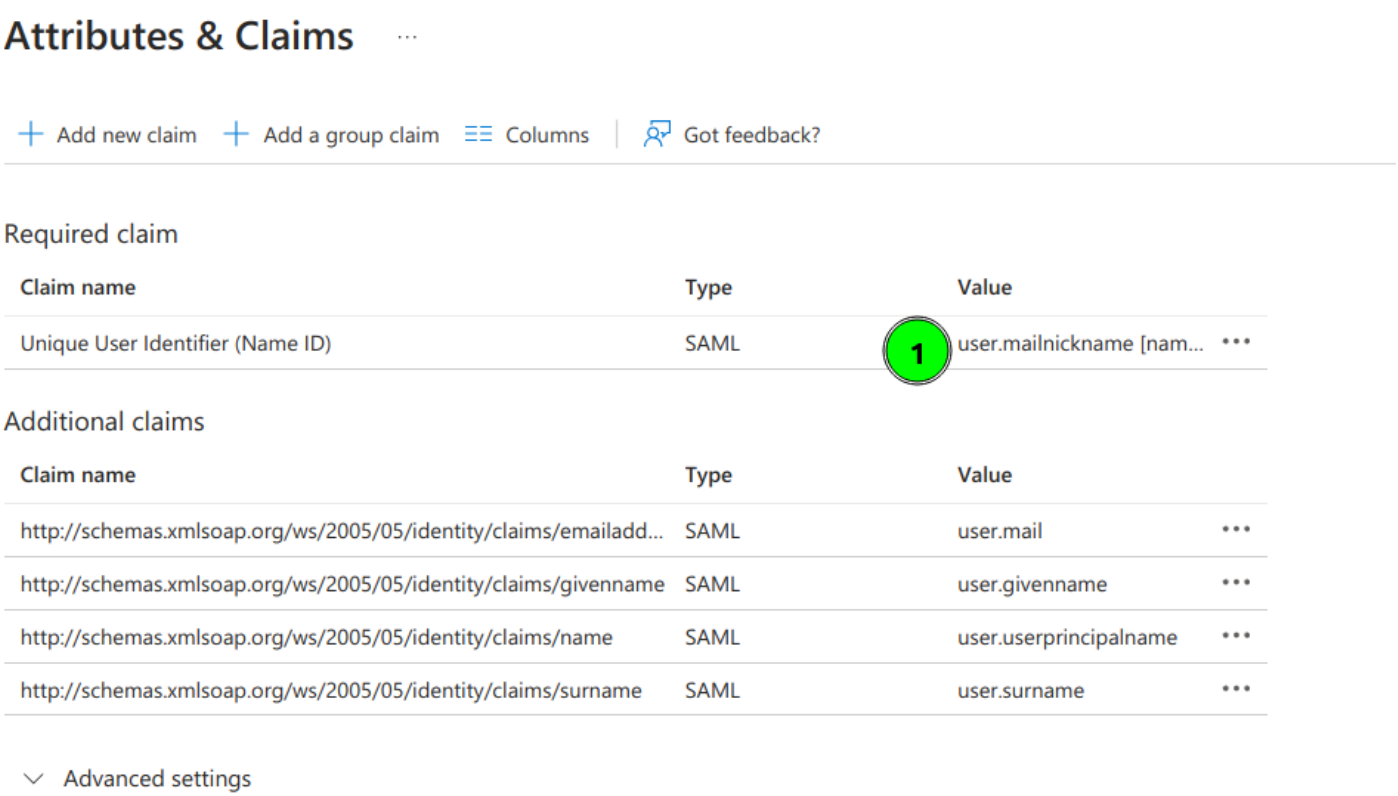
- **Reply URL**: https://<YOUR-SERVER>/soffid/saml/log/post
- **Sign on URL**: https://<YOUR-SERVER>/soffid/
- **Logout URL**: https://<YOUR-SERVER>/soffid/saml/slo/post



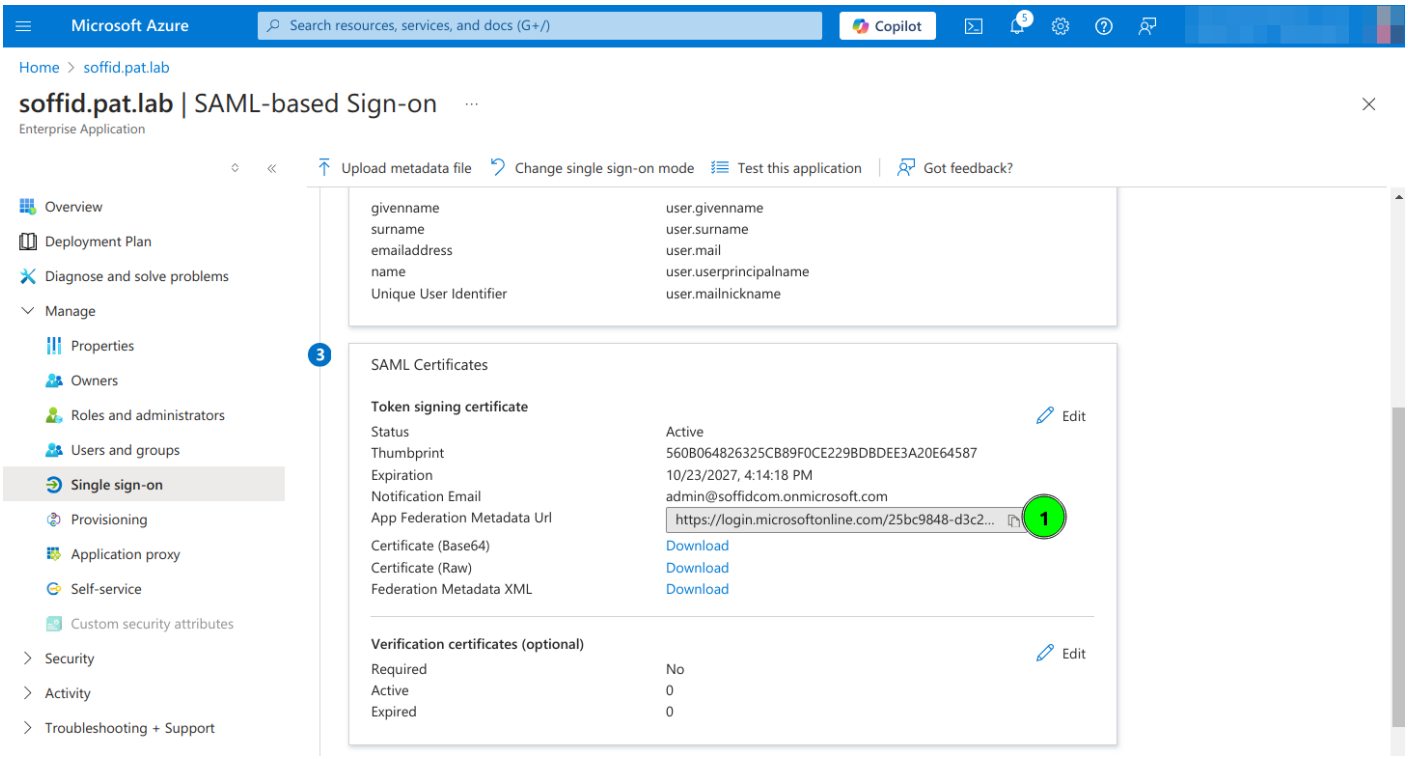


9. Configure **Attributes & Claims** and change the attributes and claims to send the mailnickname as the user identifier (nameid)

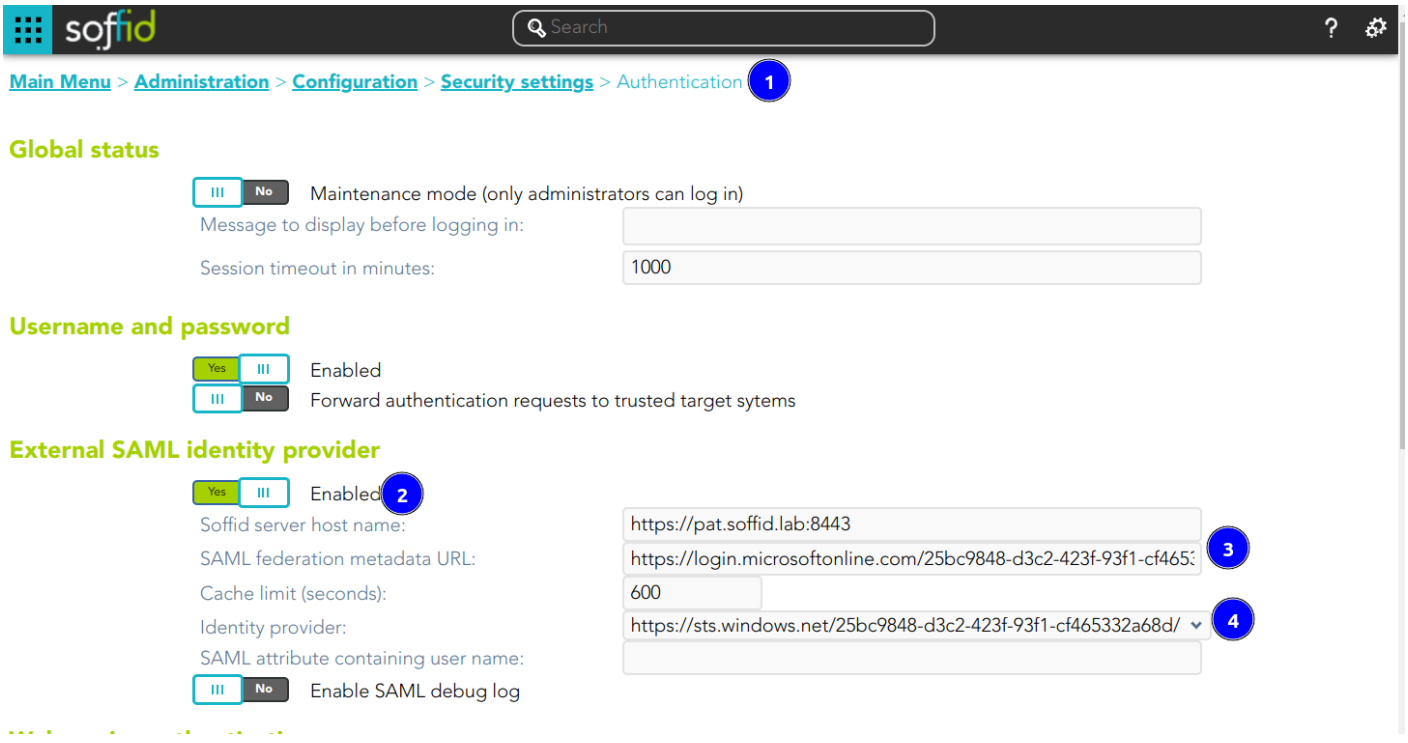




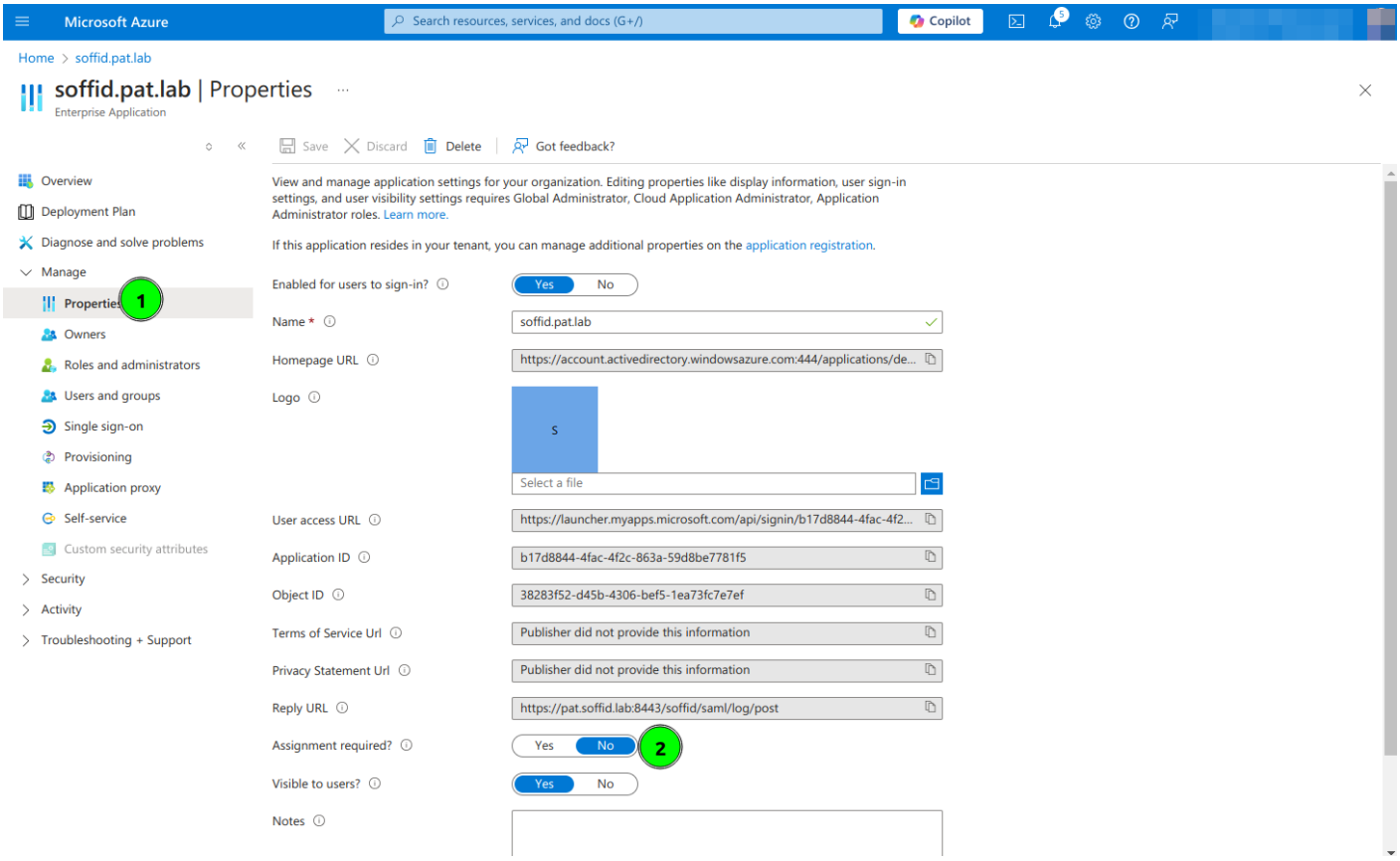
10. Copy the App Federation Metadata Url



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



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
s
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