

CONFIGURATION – SSO

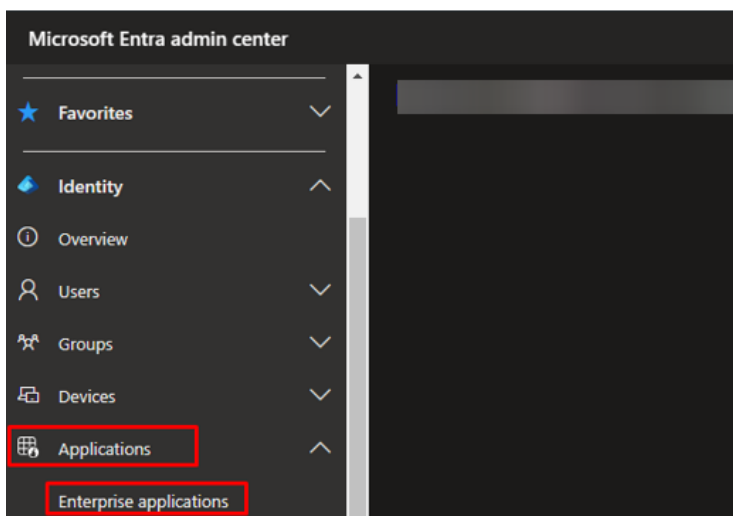
Purpose: The purpose of this document is to detail the configuration of a Single Sign On procedure for an application in Microsoft Entra Admin Center.

There are three components to this configuration

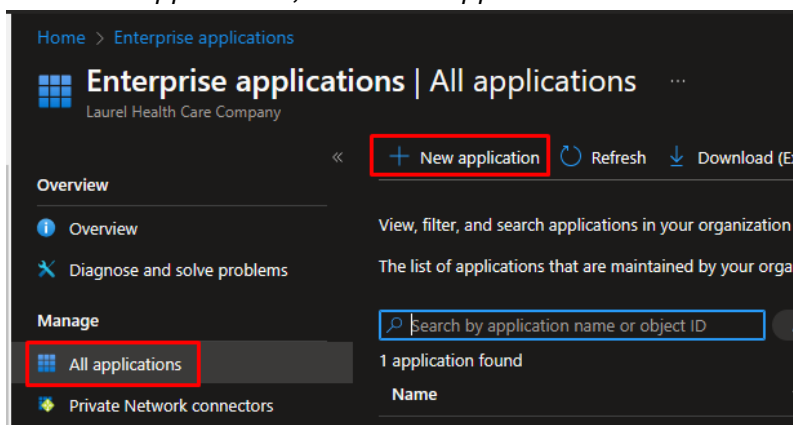
1. Single Sign on Configuration
2. Conditional Access Policy (For this specific Application)
3. Add user to a security group (For App_SSO Application)

The instruction below is how to configure SSO for Ethico Application

- Navigate to <https://portal.office.com/Adminportal/Home/#/homepage>
- Sign in using your M365 Admin account
- Select “Identity”, then you should be redirected to Microsoft Entra Admin Center.
- Expand “Application”, and select “Enterprise Application”



- Under “All application”, click “New application”



- Then, proceed to “*Create your own application*”. Name your application and keep the same default settings (Integrate any other application you don’t find in the gallery (Non-gallery)).

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 securely to their apps. Browse or create your own application here.

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

- The next step is to configure the SSO part. Click on “Single sign on”, and choose SAML.

MyCm | 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

Single sign-on (SSO) adds security and convenience when users sign on to applications in Microsoft Entra ID by enabling a single credential 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.

- In this step, we are going to need Entity ID, ACS URL and Sign On URL from the application that you are adding.

- Entity ID: <https://sso.AppName.com/auth/realms/CIprod>
- ACS URL: <https://sso.AppName.com/auth/realms/CIprod/broker/KodeSaml/endpoint>
- Sign On URL: <https://app.compliancemanagement.com/redirect?cid=Kode>

➤ We will fill this information into the “Basic SAML Configuration” by clicking on “Edit”.

Set up Single Sign-On with SAML

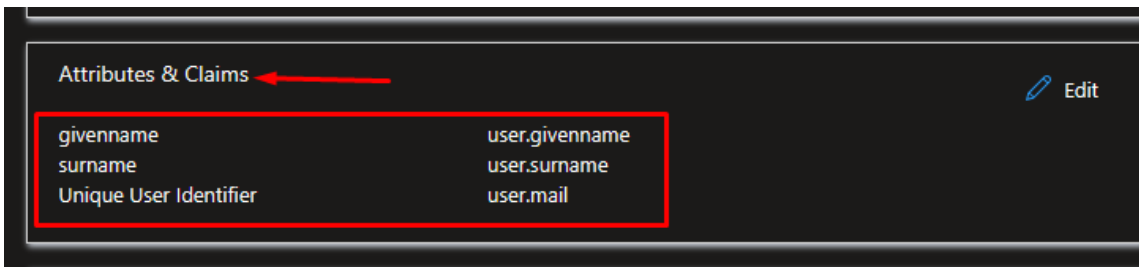
An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth 2.0.

Read the [configuration guide](#) for help integrating Ethico MyCm.

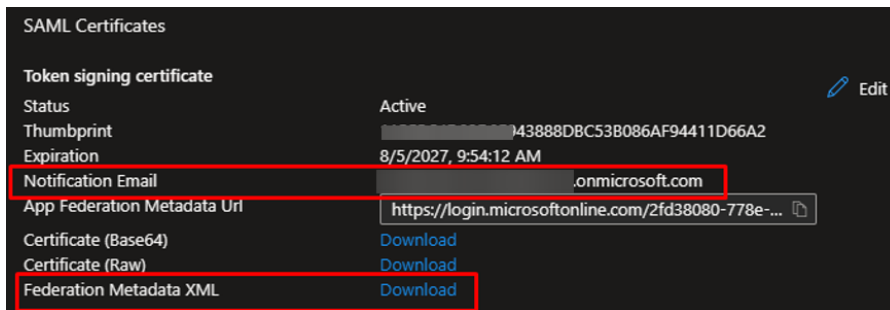
1 Basic SAML Configuration [Edit](#)

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State (Optional)	Optional
Logout URL (Optional)	Optional

After finishing this step, make sure that “Attributes & Claims” are set to these values below:



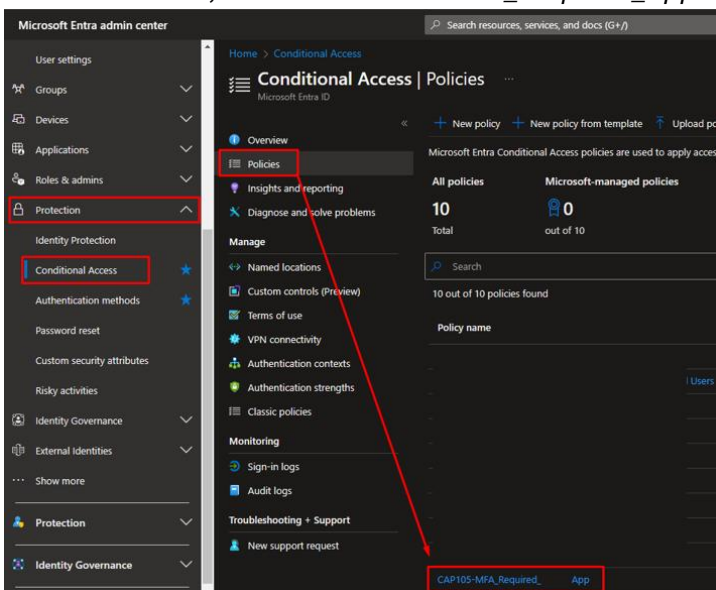
- The last part is to download “Federation Metadata XML” and give it to Application side company so that they can take that XML file to configure it on their backend.



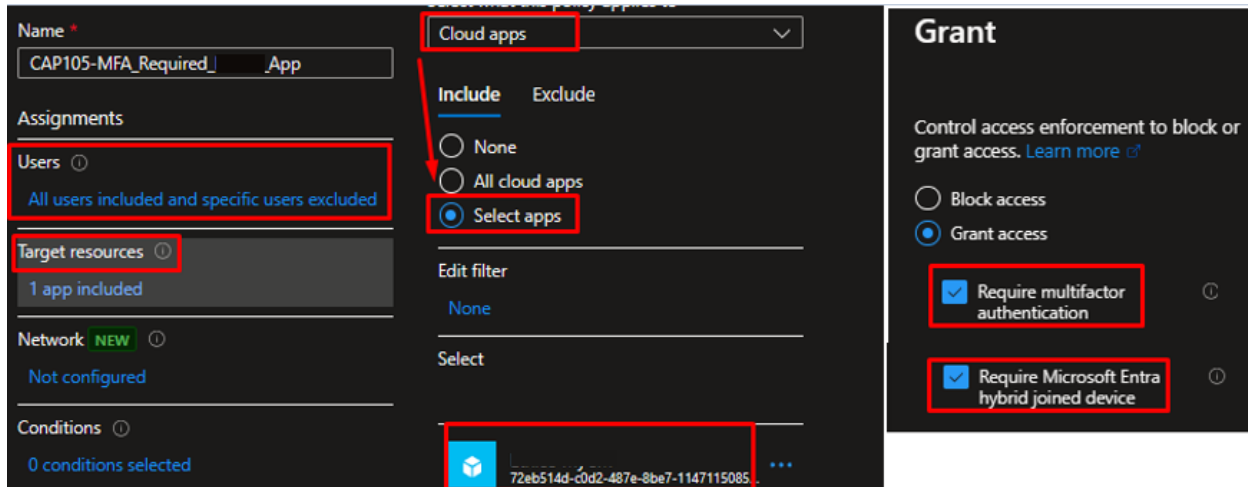
Finally change the “Notification Email” to any distributed email address as you desire for the alerts.

This is a Conditional Access Policy Configuration Part for App_SSO

- Navigate to <https://portal.office.com/Adminportal/Home/#/homepage>
- Sign in using your M365 Admin account
- Go to “Protection” and select “Conditional Access”.
- Under “Policies”, click on “CAP105-MFA_Required_App”



- In this step, there are the settings we set up for the App.
 - Users: All users
 - Target resources: Clouds App > App Name
 - Grant: Required multifactor authenticator and Require Microsoft Entra hybrid joined device
 - Session: Sign-In frequency – Every time
- Keep everything else from the default.

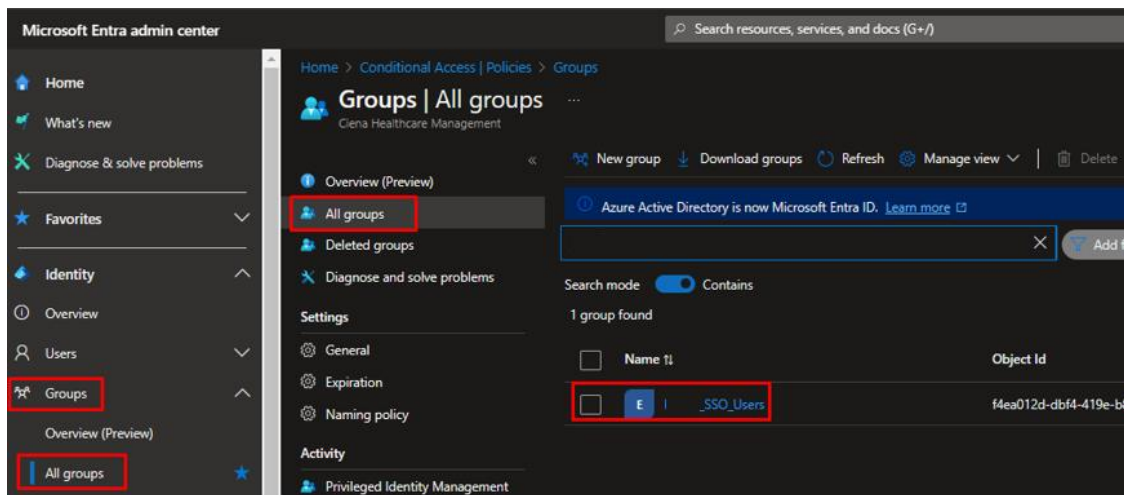


- Lastly, save the policy as “report-only”, after testing everything and working as expect, you can switch the policy to “On”.

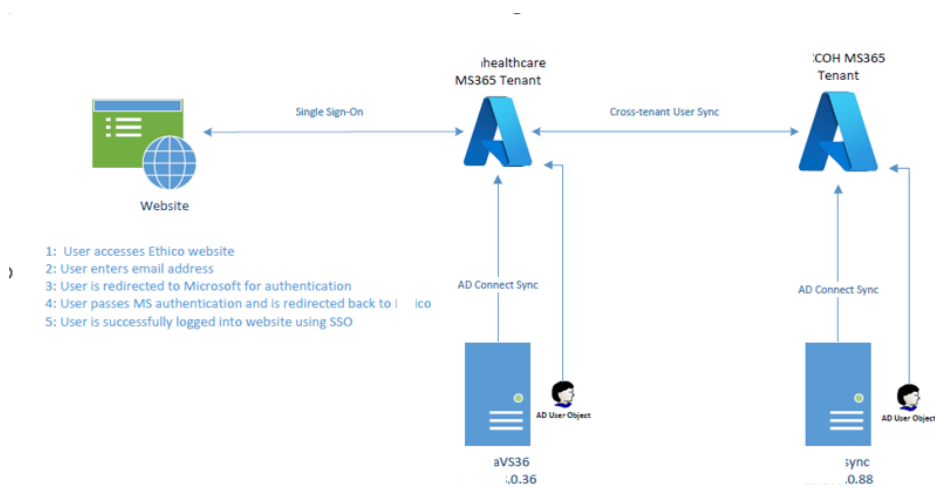
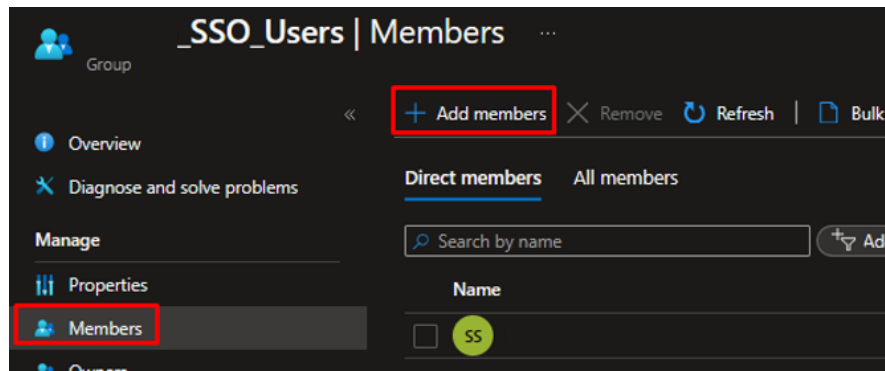
This is how to do add the users to the SSO_User security group

NOTE: Please make sure that the user (First name, Last name, Email address) that being created on the Application side matches on the Active Directory attributes on your company side.

- Navigate to <https://portal.office.com/Adminportal/Home/#/homepage>
- Sign in using your M365 Admin account
- Expand “Groups” and select “All groups> SSO_Users”



- Go to “Members” and “Add members”



Revision

1.0	08/08/2024	Soklim Seang		Initial document creation.
-----	------------	--------------	--	----------------------------