

# Single Sign On (SSO) for Business and Contact Center Systems

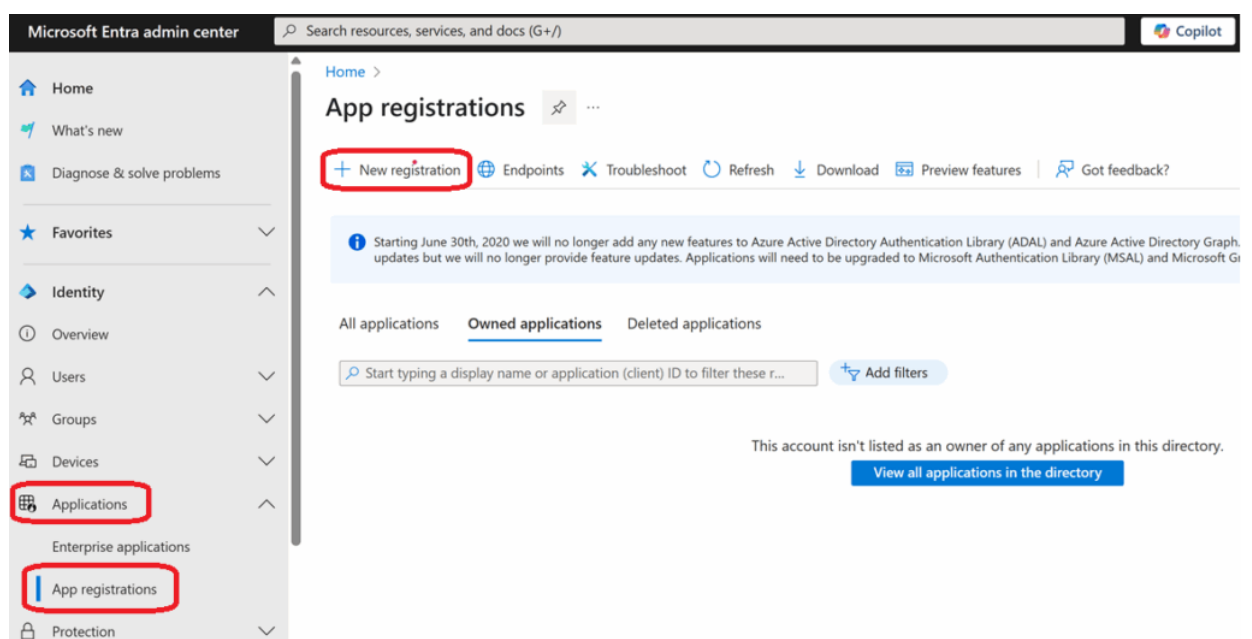
Single Sign-On (SSO) is a feature that allows users to access multiple applications or websites with just one set of login credentials. It simplifies the authentication process, reduces the need to manage multiple usernames and passwords, and improves user experience by eliminating the need to log in repeatedly.

For SSO to work your PBX system must be able to access <https://login.microsoftonline.com> .

## Microsoft Entra Setup

To setup an OAuth 2.0 client with Microsoft you must first register the application in the [Microsoft Entra Admin Center](#)

1. Select Applications
2. App registrations
3. Click New Registration



4. **Name:** Enter a name for the Application
5. **Supported account types:** Select Accounting in any organizational directory (any Microsoft Entra ID tenant – Multitenant) and personal Microsoft accounts (r.g. Skype, Xbox)
6. **Redirect URI:** Web  
https://pbx\_domain\_name/auth/azurereadv2/callback
7. Click Register

Microsoft Entra admin center

Search resources, services, and docs (G+/)

Copilot

Home

What's new

Diagnose & solve problems

Favorites

Identity

Overview

Users

Groups

Devices

Applications

Enterprise applications

App registrations

Protection

Identity Governance

External Identities

Show more

Learn & support

Register an application

Name

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

My\_SSO\_App

Supported account types

Who can use this application or access this API?

☐ Accounts in this organizational directory only (Fireline Network Solutions, Inc. only - Single tenant)

☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

☒ Accounts in any organizational directory (Any Microsoft Entra ID tenant - 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

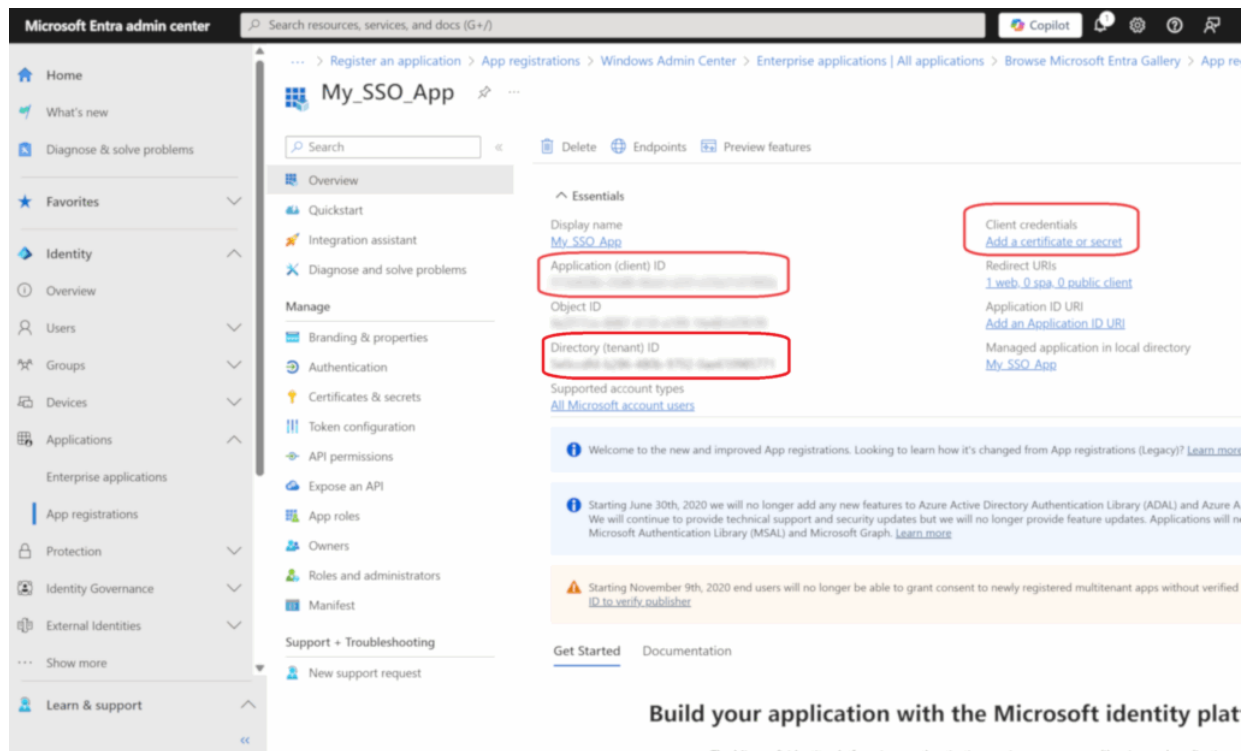
https://mydomain.com/auth/azurereadv2/callback

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

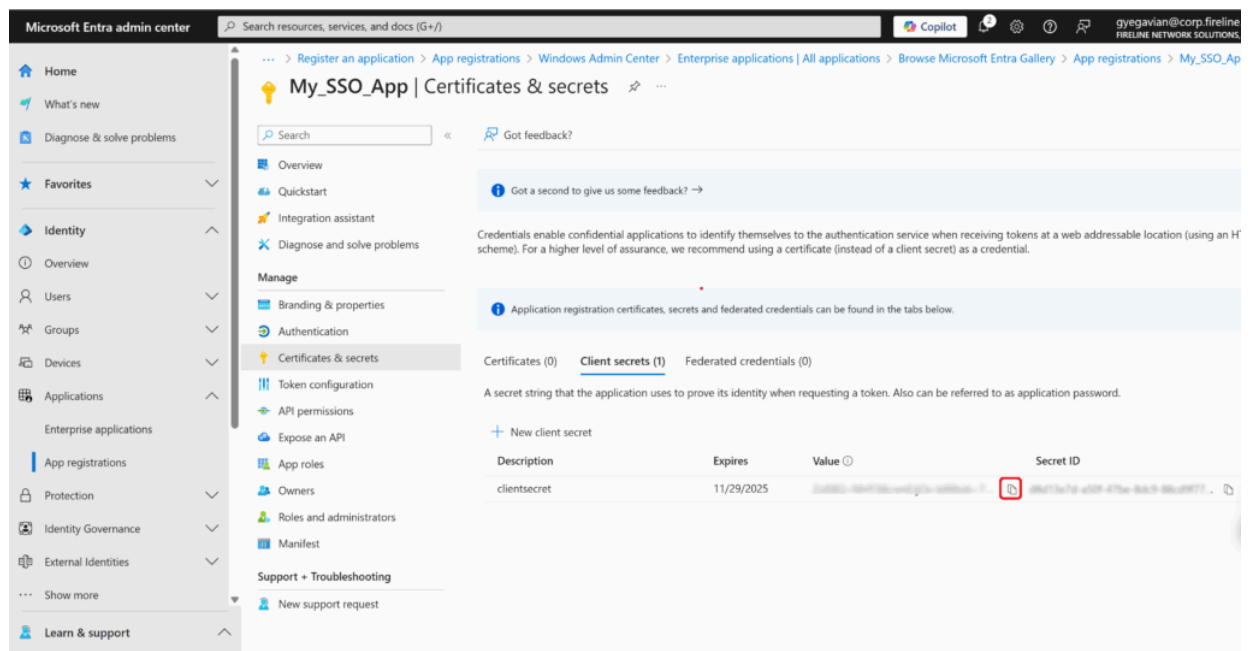
By proceeding, you agree to the Microsoft Platform Policies

Register

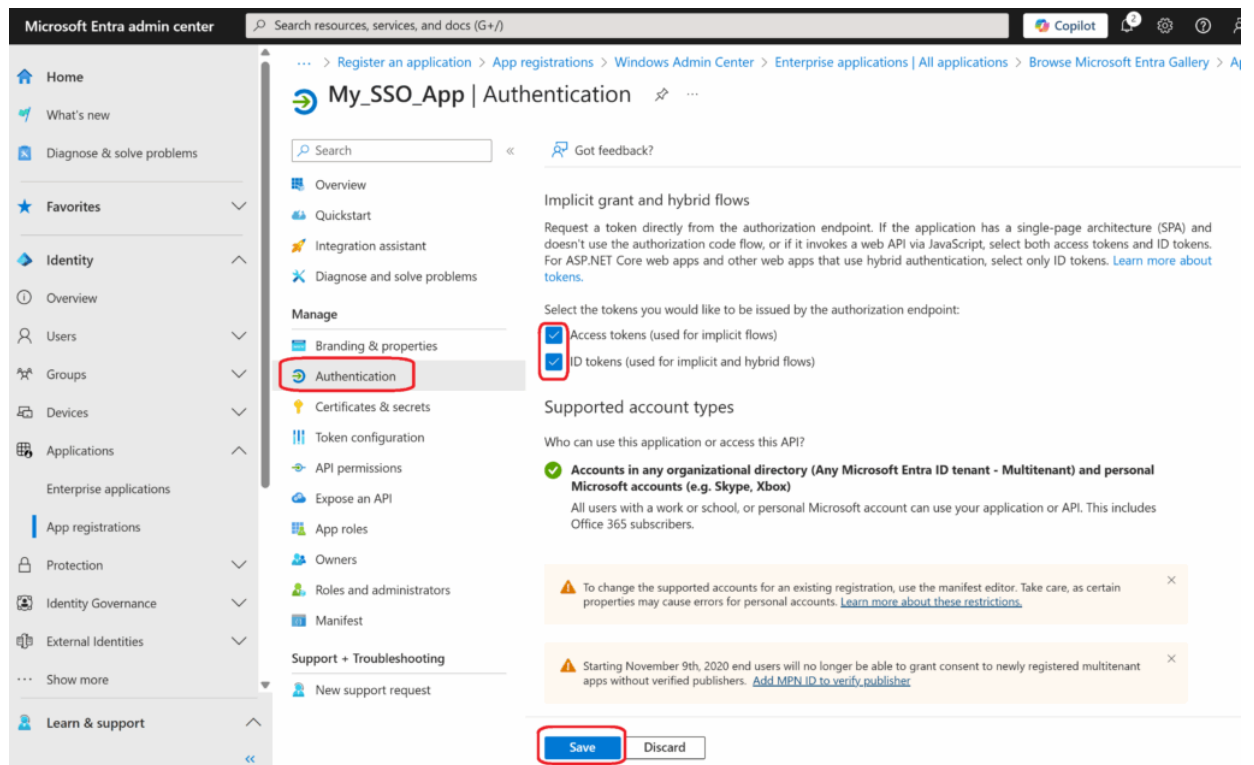
8. Copy the Application ID to a safe location, this will be needed later.
9. Copy the Directory (tenant) ID to a safe location. This is an optional field and can be used to restrict SSO access to members of this tenant only.
10. Under Client credentials, click Add a certificate or secret.



11. Copy the Value from the Client secret and save it with the Application ID.

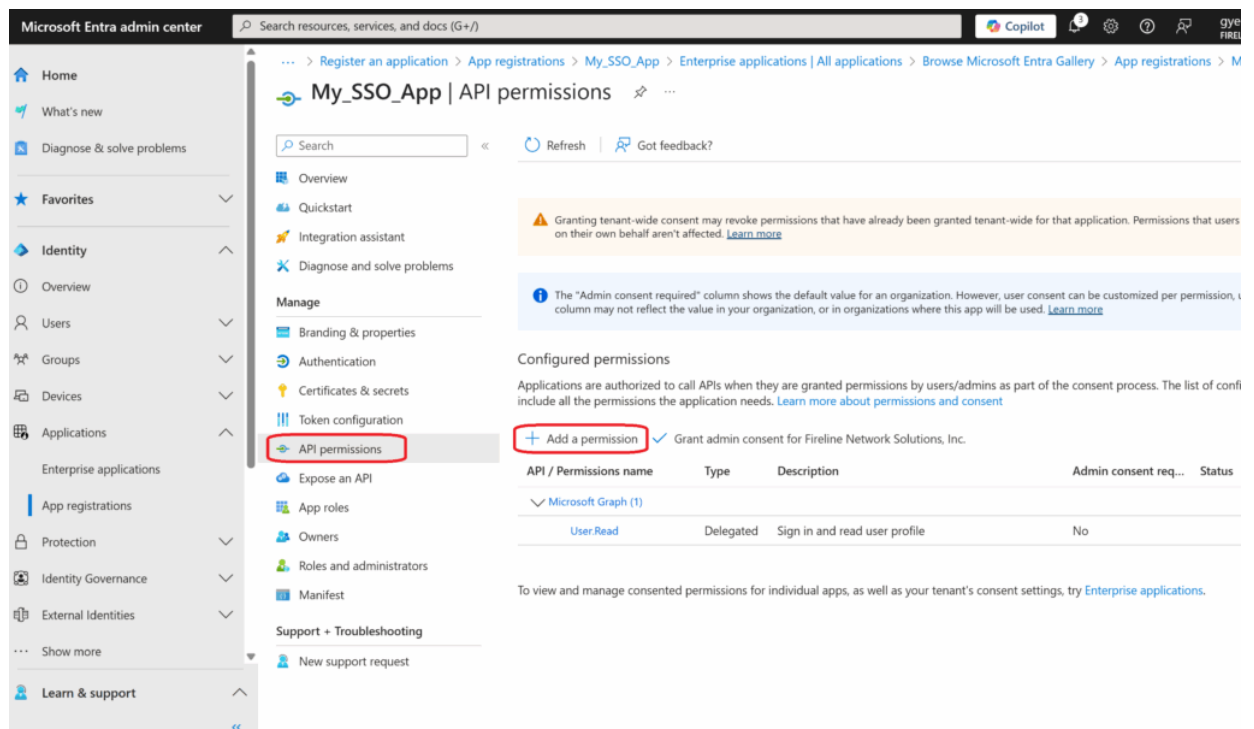


12. Select Authentication Menu Item
13. Place a check mark in both Access tokens (used for implicit flows) & ID tokens (used for implicit and hybrid flows)
14. Click Save

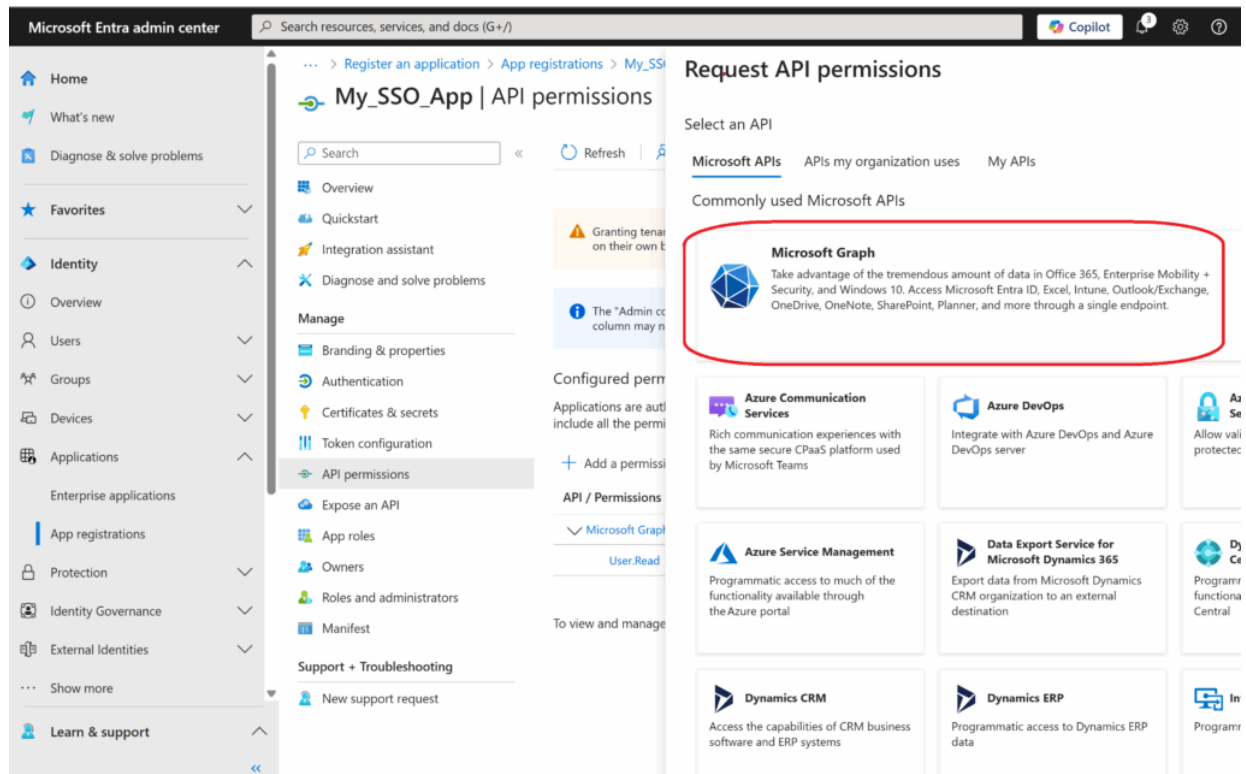


15. Select API permissions

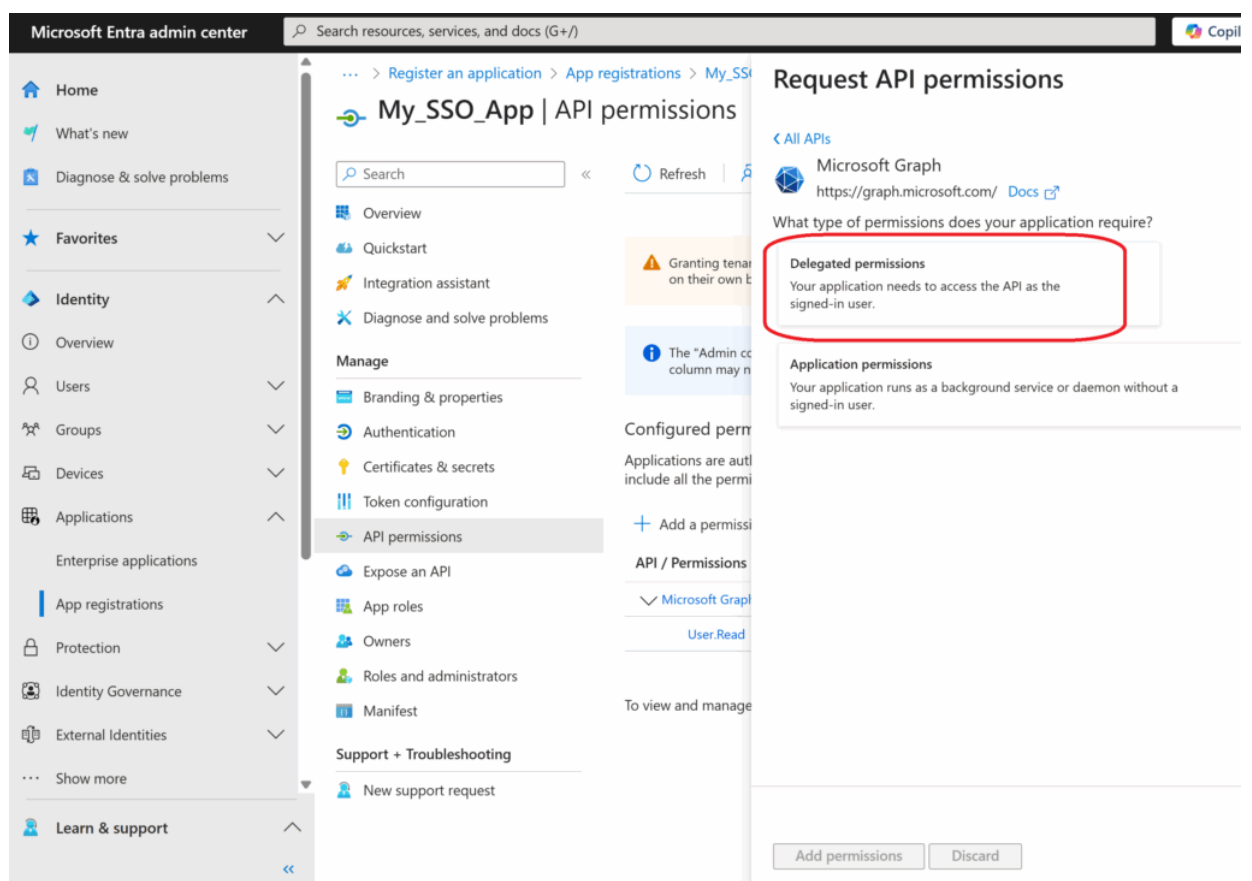
16. Click Add a permission



17. Under Request API permissions select Microsoft Graph



## 18. Select Delegated permissions



19. Under Select Permissions type o to pull up the OpenID permissions

20. Expand OpenID and select the following

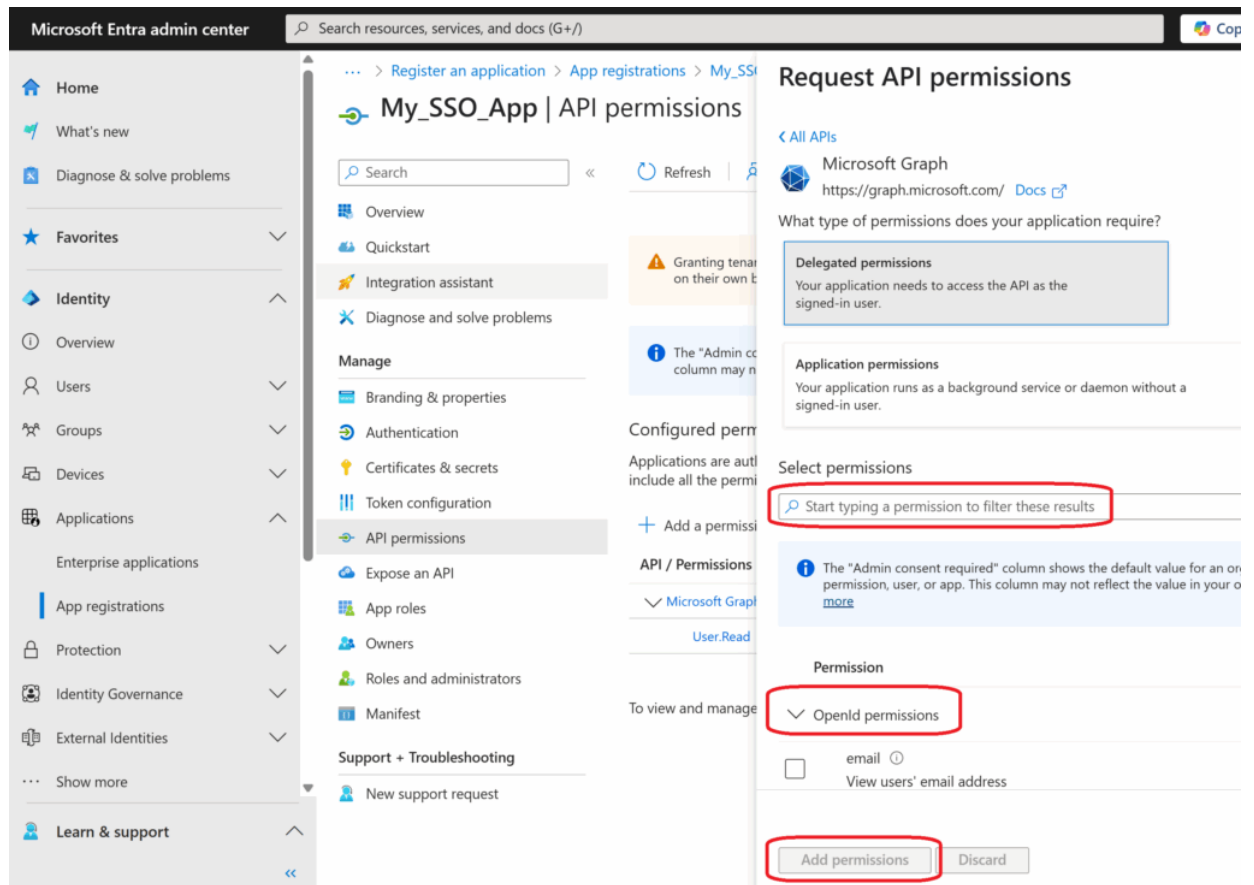
1. email

2. offline\_access

3. openid

4. profile

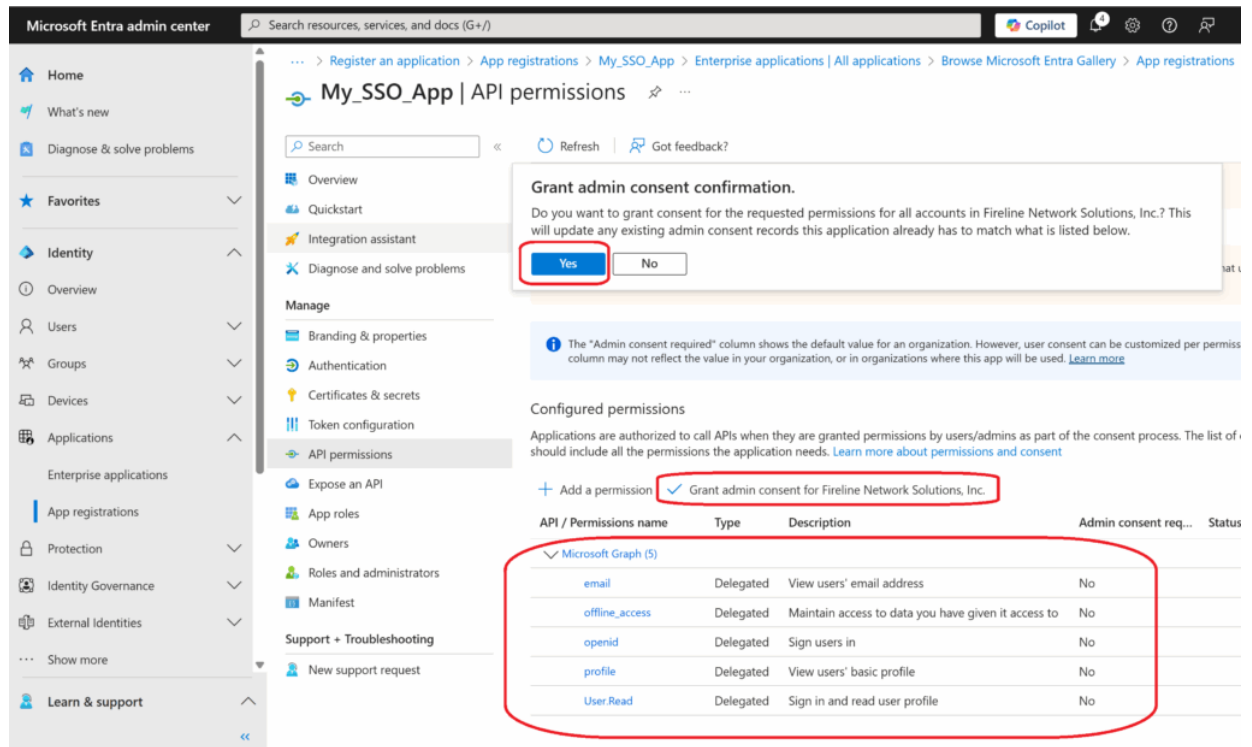
21. Once selected click add permissions



22. Review all items are listed under Microsoft Graph including User.Read which should have been selected by default.

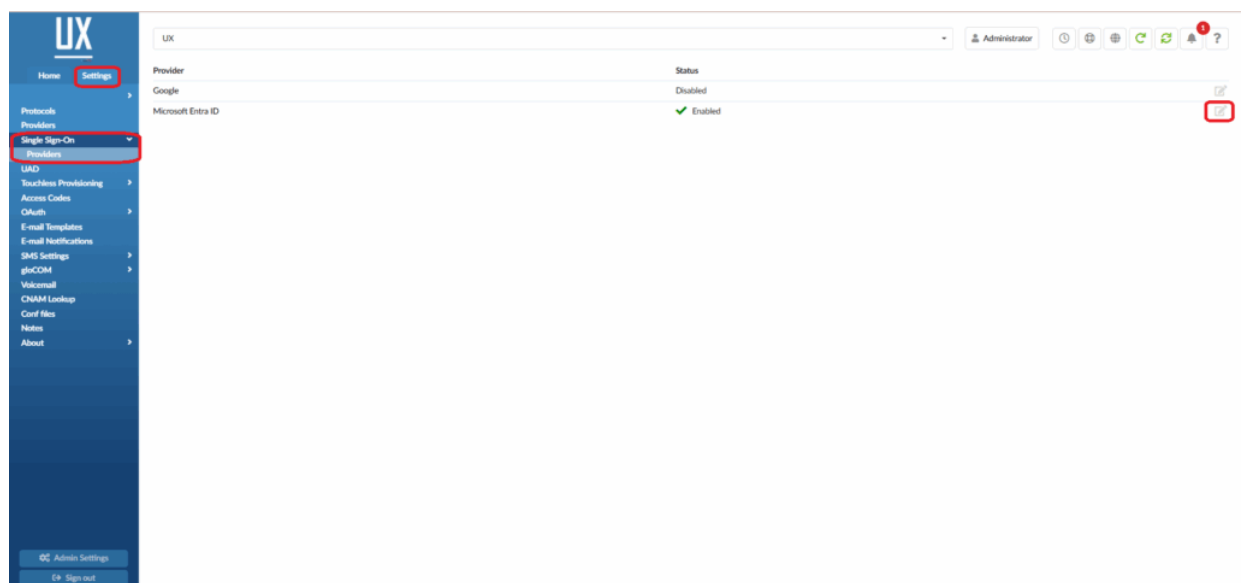
23. Click on Grant admin consent

24. Click Yes to the Grant admin consent confirmation, pop up.



## PBX Setup

1. to your PBX system
2. Select the Settings tab
3. Select Single Sign On
4. Select the Edit button to the right of the Microsoft Entra ID option



5. Select Yes to enable the Entra Client

6. Copy the Application ID you saved earlier, and paste it into the Client ID field
7. Copy the Value of the Client Secret saved earlier, and paste it into the Client Secret field.
8. The Tenant ID can be left empty, allowing users from any Microsoft Entra ID tenant to authenticate or populated to restrict to single Microsoft tenant only.
9. Save

The screenshot displays the UX Admin Settings interface. On the left is a dark blue sidebar with a 'UX' logo at the top. Below the logo are tabs for 'Home' and 'Settings'. The 'Settings' tab is active, and a dropdown menu is open, showing options like 'Protocols', 'Providers', 'Single Sign-On', 'UAD', 'Touchless Provisioning', 'Access Codes', 'OAuth', 'E-mail Templates', 'E-mail Notifications', 'SMS Settings', 'gloCOM', 'Voicemail', 'CNAM Lookup', 'Conf files', 'Notes', and 'About'. The 'Single Sign-On' option is selected. The main content area shows the 'Single Sign-On Provider > Microsoft Entra ID' configuration. Under the 'Client' section, there is an 'Enable' toggle set to 'Yes'. Below this, the 'Client ID' and 'Client Secret' fields are filled with values and marked with green checkmarks. The 'Tenant ID' field is empty. A 'Save' button is at the bottom right.

10. Select Servers
11. Move to the Authentication section and select Yes to Enforce SSO Auth, accross the system. Select No if you want to manage SSO per extension.
12. Select the number of months, (1-3), that you would like the SSO token to expire.



Authentication

2FA Expiry Time: 1 day

2FA Max Inactivity Time: 1 Year

**Enforce SSO Auth:** Yes No

SSO Token Expiry Time: 1 Month

13. Select Save

## Per Extension Settings

1. From the Home tab open Extensions
2. Chose the extension you would like to enforce SSO on.
3. Go to Autentication section and select Yes to SSO Enabled.
4. Save extension.

201 - 201-Test Account

Administrator

Extensions > Edit

General

Extension Number: Title: Name: Communicator User E-mail: SMS Number: UAD: glvCOM UAD Location: Remote Check for UAD SIP headers: Label: Line Number: Location: Language: Extension Timezone: System default Department: None X User Type: friend DTMF Mode: rfc2833 Context: t-201

Authentication

Username: LDAP username: Authname: Auth: Secret: User Password: Password is encrypted. Incoming IP addresses (new line separated): Insecure: Please select ... 2FA Expiry Time: 1 day 2FA Max Inactivity Time: 1 Month SSO Enabled: Yes No PIN:

Permissions

Destinations Enhanced Services Notes Editions & Modules

Save Save & E-mail Copy As New Go back

5. SSO will be enforced for this specific extension only.

