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

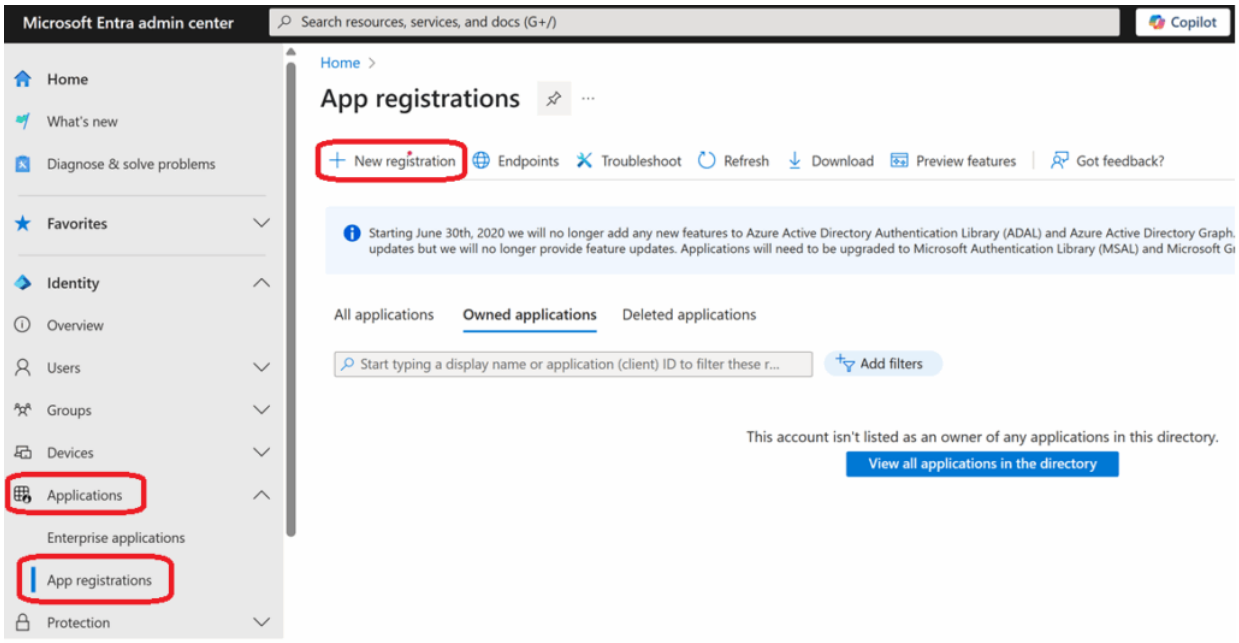
Single Sign-On (SSO) is a feature that allows users to access multiple applications or websites with just one set of login credentials. It simplifies the authentication process, reduces the need to manage multiple usernames and passwords, and improves user experience by eliminating the need to log in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

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

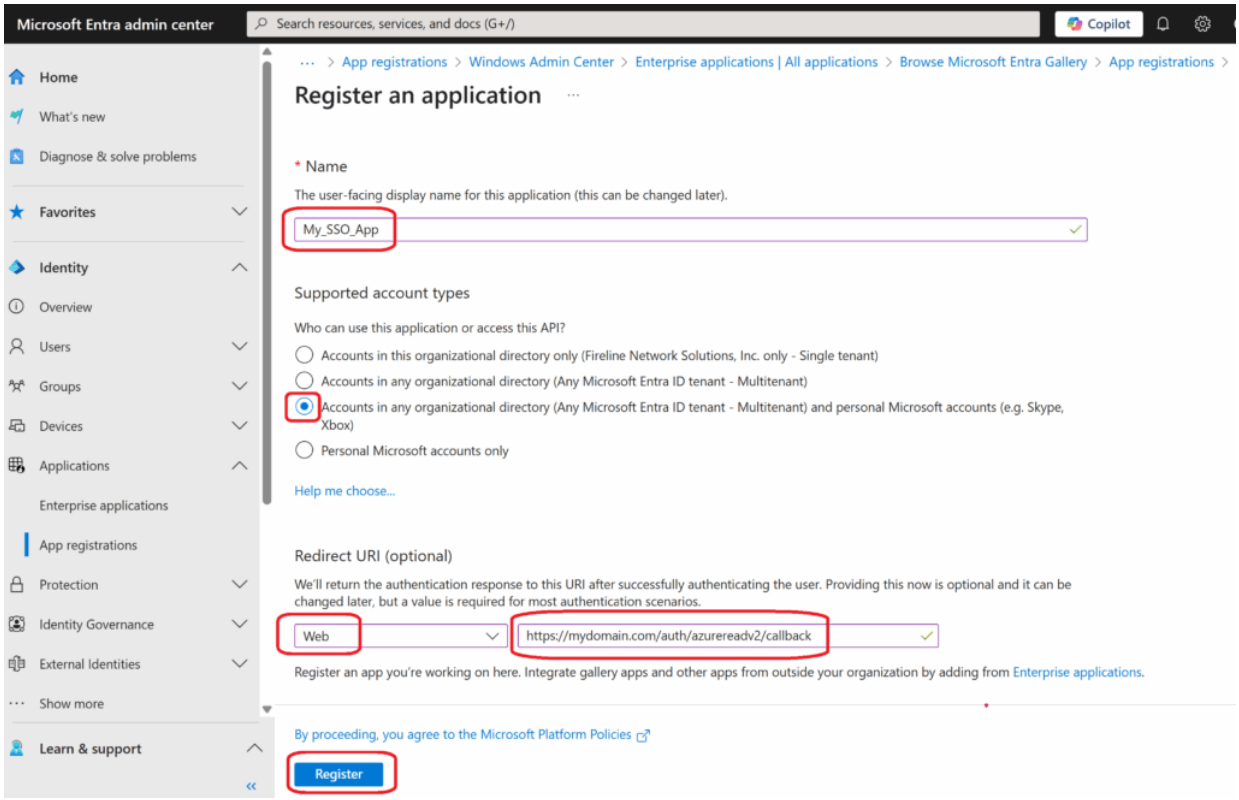
Microsoft Entra Setup

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

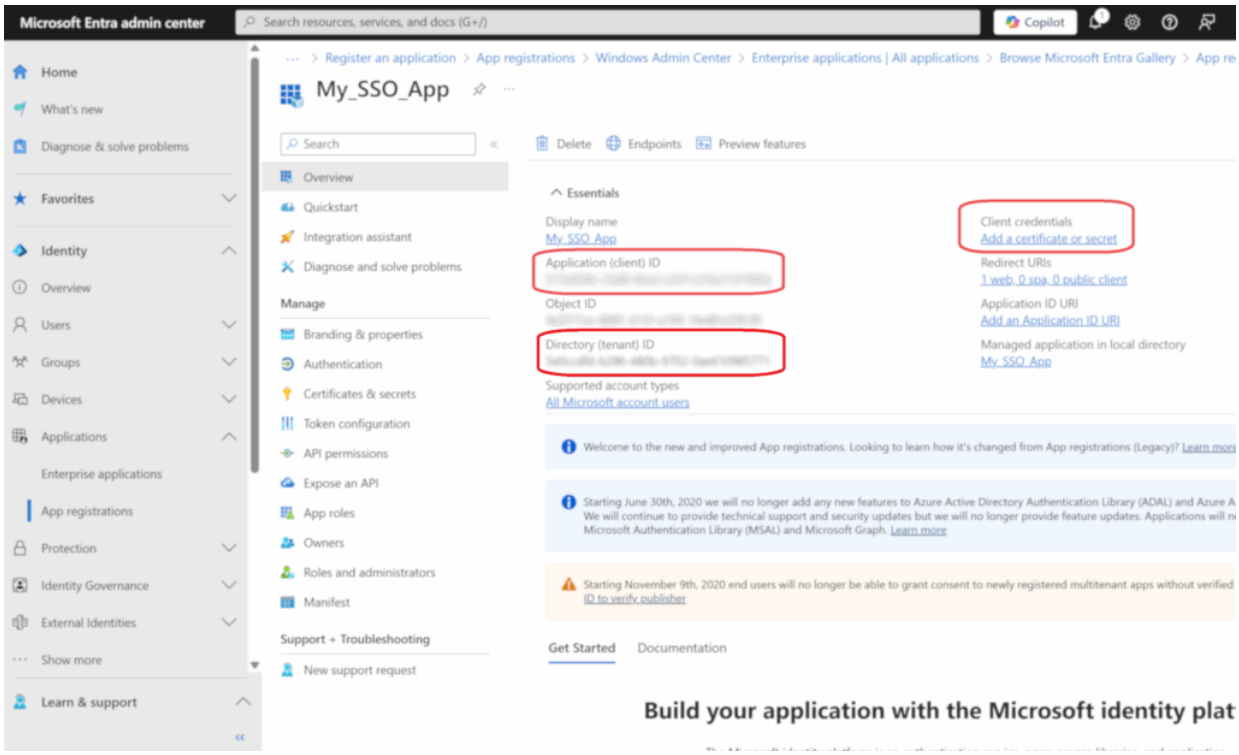
1. Select Applications
2. App registrations
3. Click New Registration



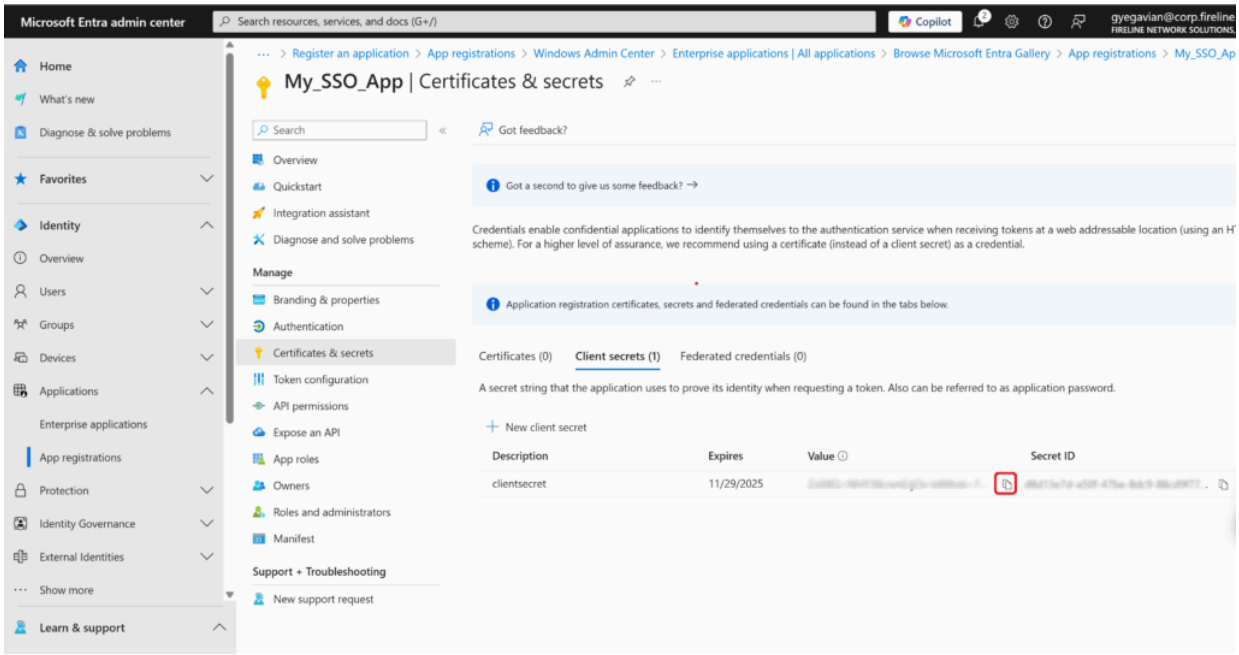
4. **Name:** Enter a name for the Application
5. **Supported account types:** Select Accounting in any organizational directory (any Microsoft Entra ID tenant – Multitenant) and personal Microsoft accounts (r.g. Skype, Xbox)
6. **Redirect URI:** Web https://pbx_domain_name/auth/azureadv2/callback
7. Click Register



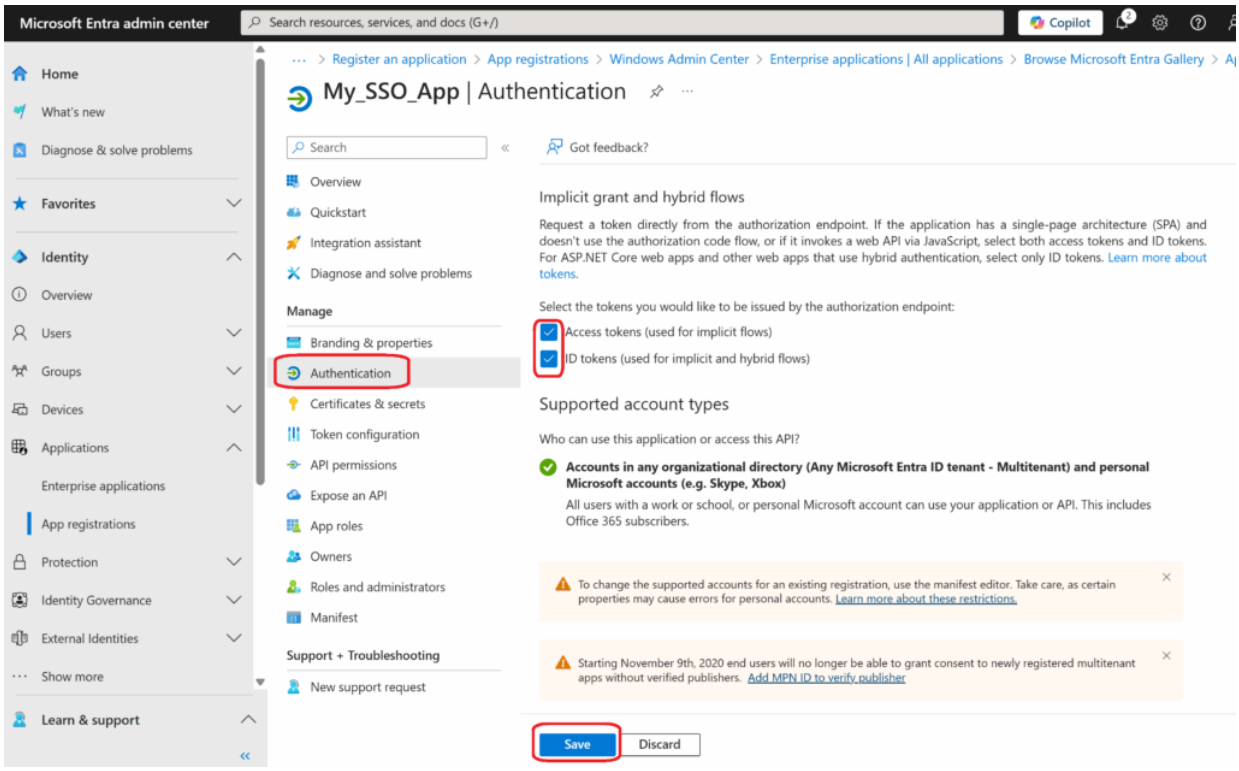
8. Copy the Application ID to a safe location, this will be needed later.
9. Copy the Directory (tenant) ID to a safe location. This is an optional field and can be used to restrict SSO access to members of this tenant only.
10. Under Client credentials, click Add a certificate or secret.



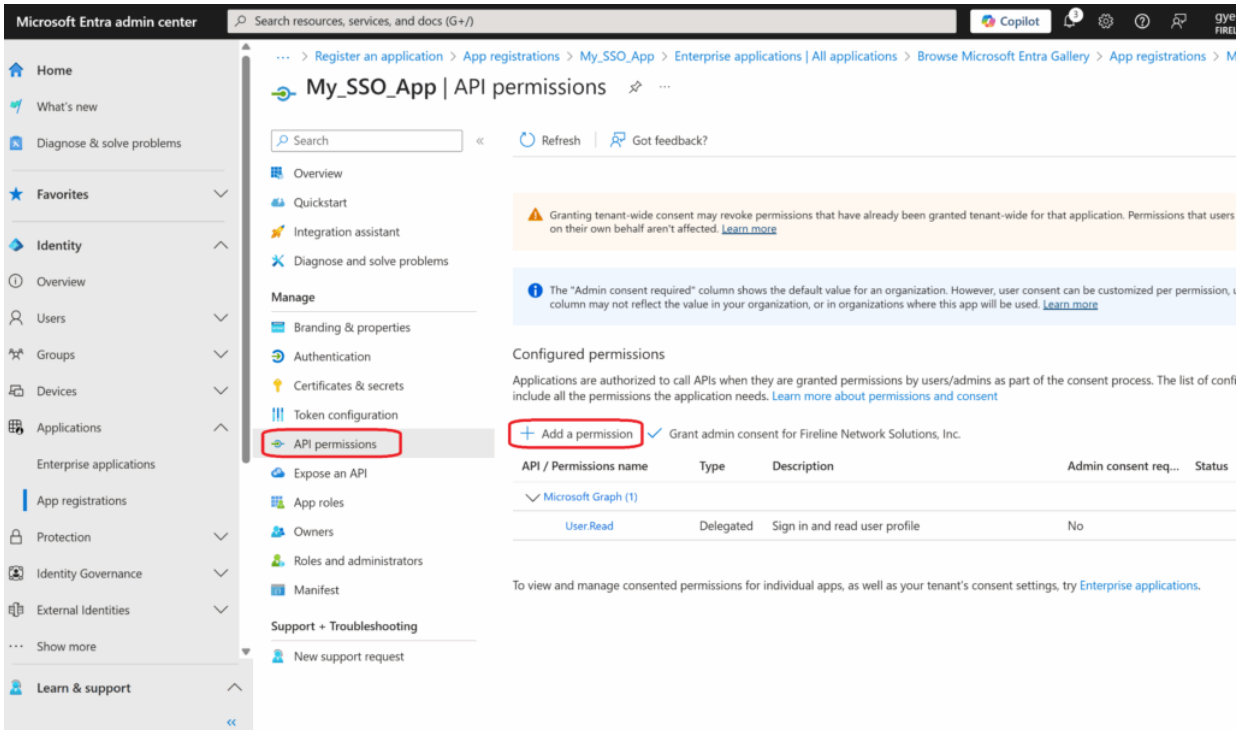
11. Copy the Value from the Client secret and save it with the Application ID.



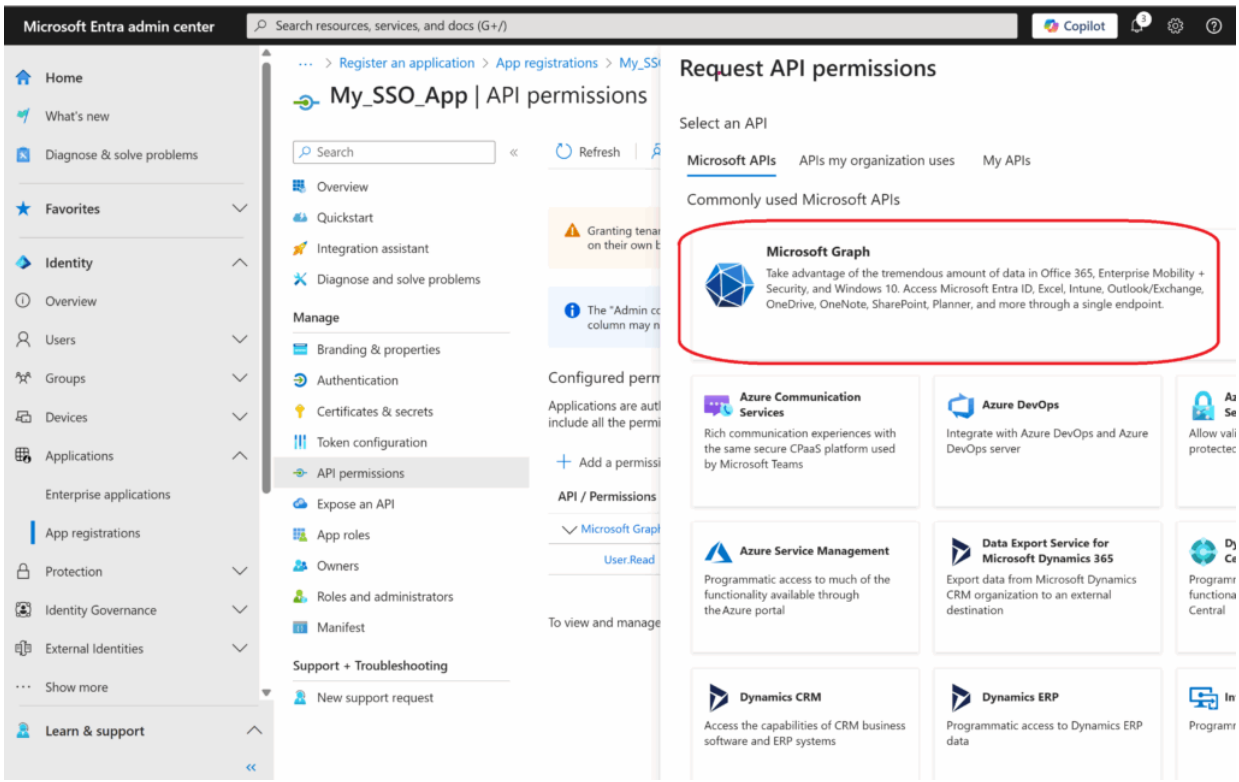
12. Select Authentication Menu Item
13. Place a check mark in both Access tokens (used for implicit flows) & ID tokens (used for implicit and hybrid fows)
14. Click Save



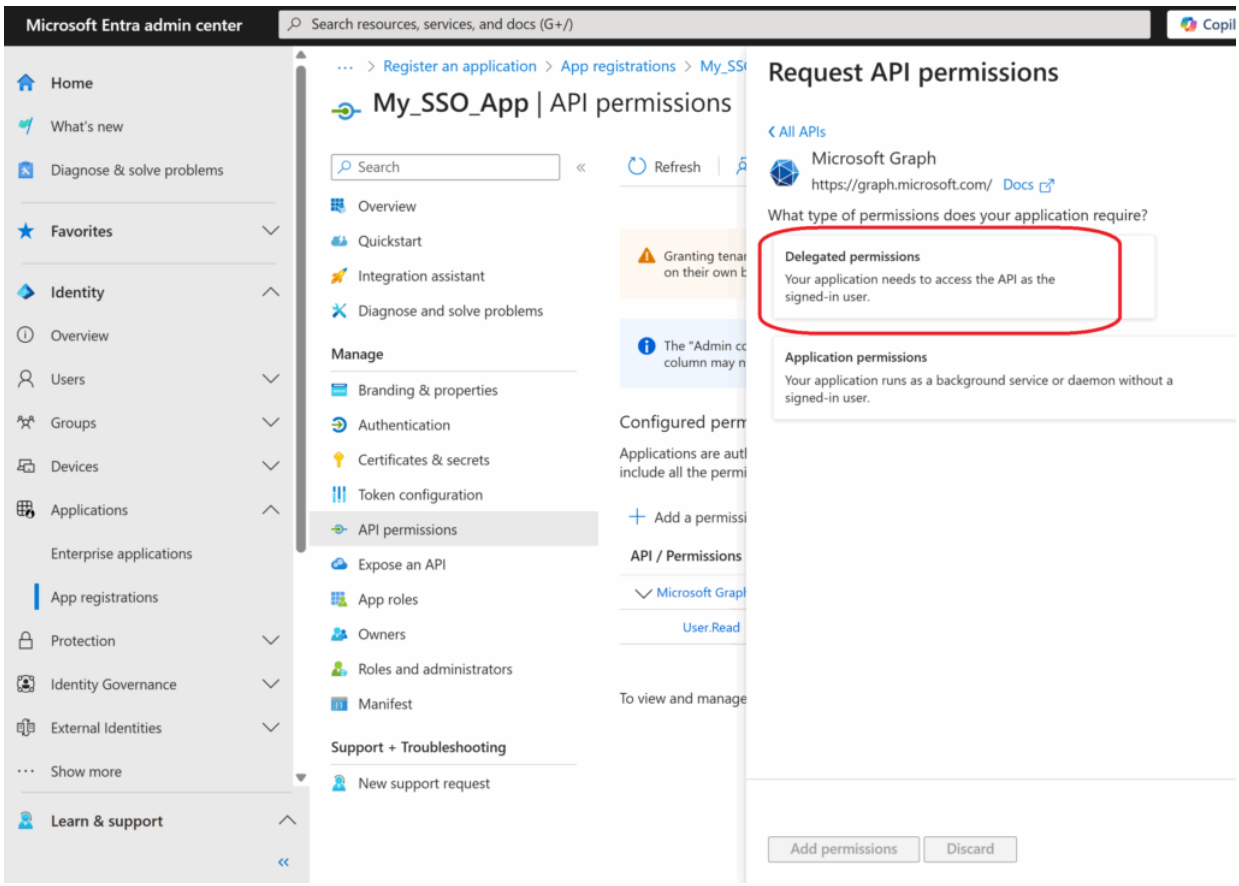
15. Select API permissions
16. Click Add a permission



17. Under Request API permissions select Microsoft Graph



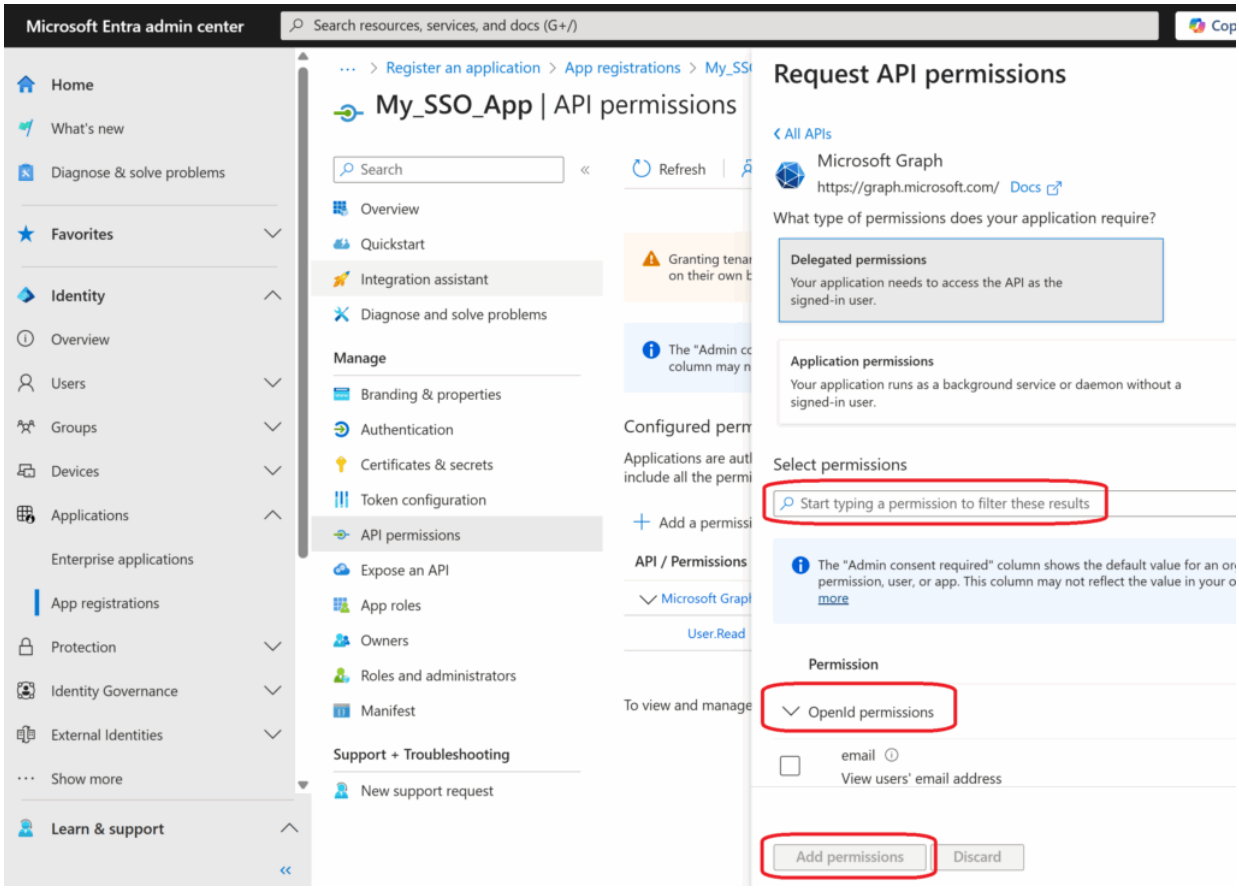
18. Select Delegated permissions



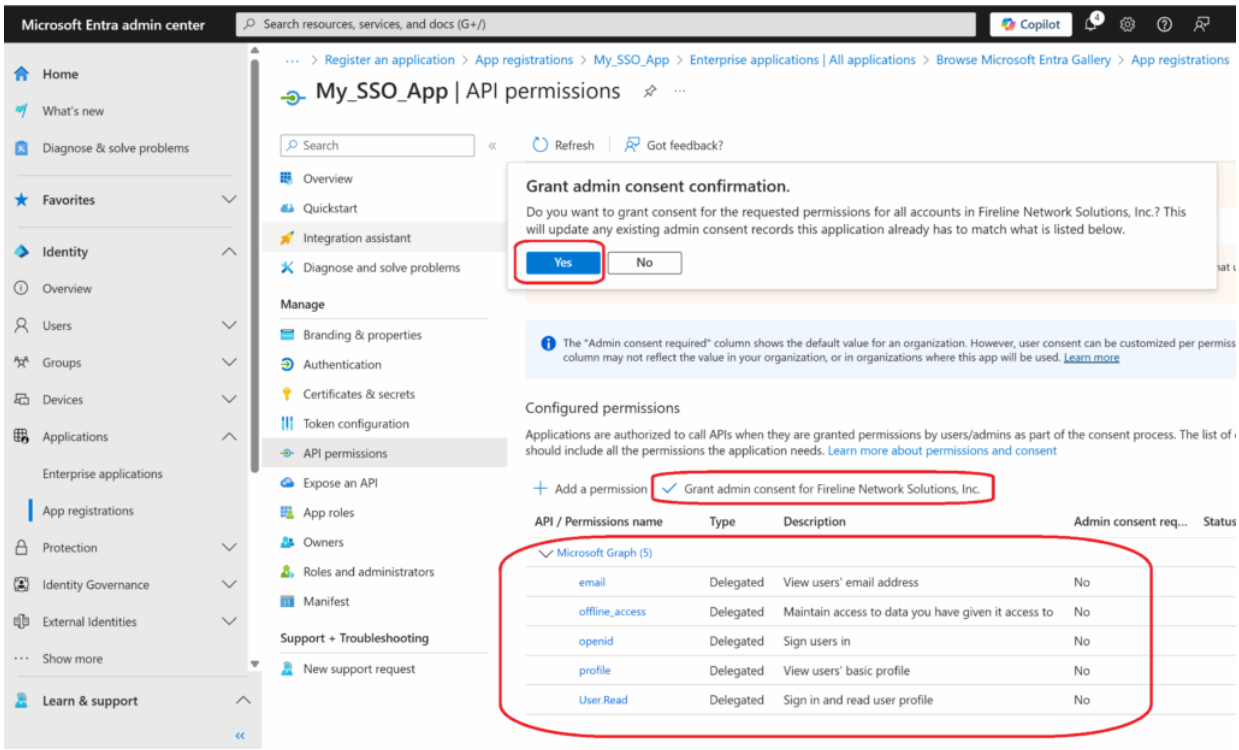
19. Under Select Permissions type o to pull up the OpenID permissions
20. Expand OpenID and select the following
    1. email

2. offline_access
3. openid
4. profile

21. Once selected click add permissions

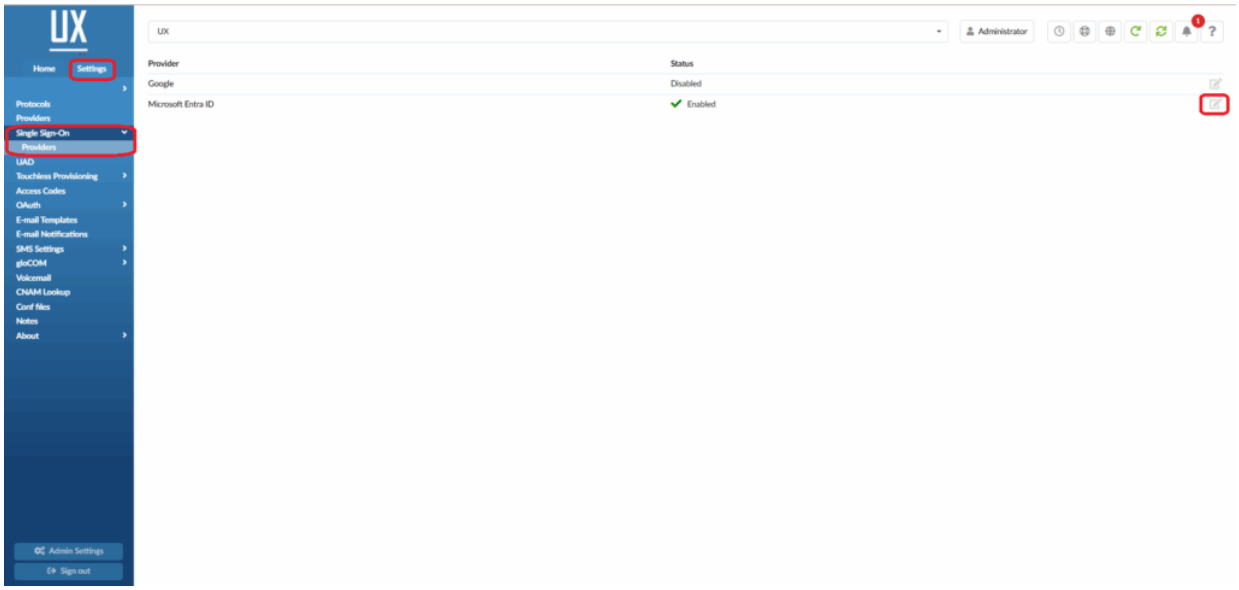


22. Review all items are listed under Microsoft Graph including User.Read which should have been selected by default.
23. Click on Grant admin consent
24. Click Yes to the Grant admin consent confirmation, pop up.



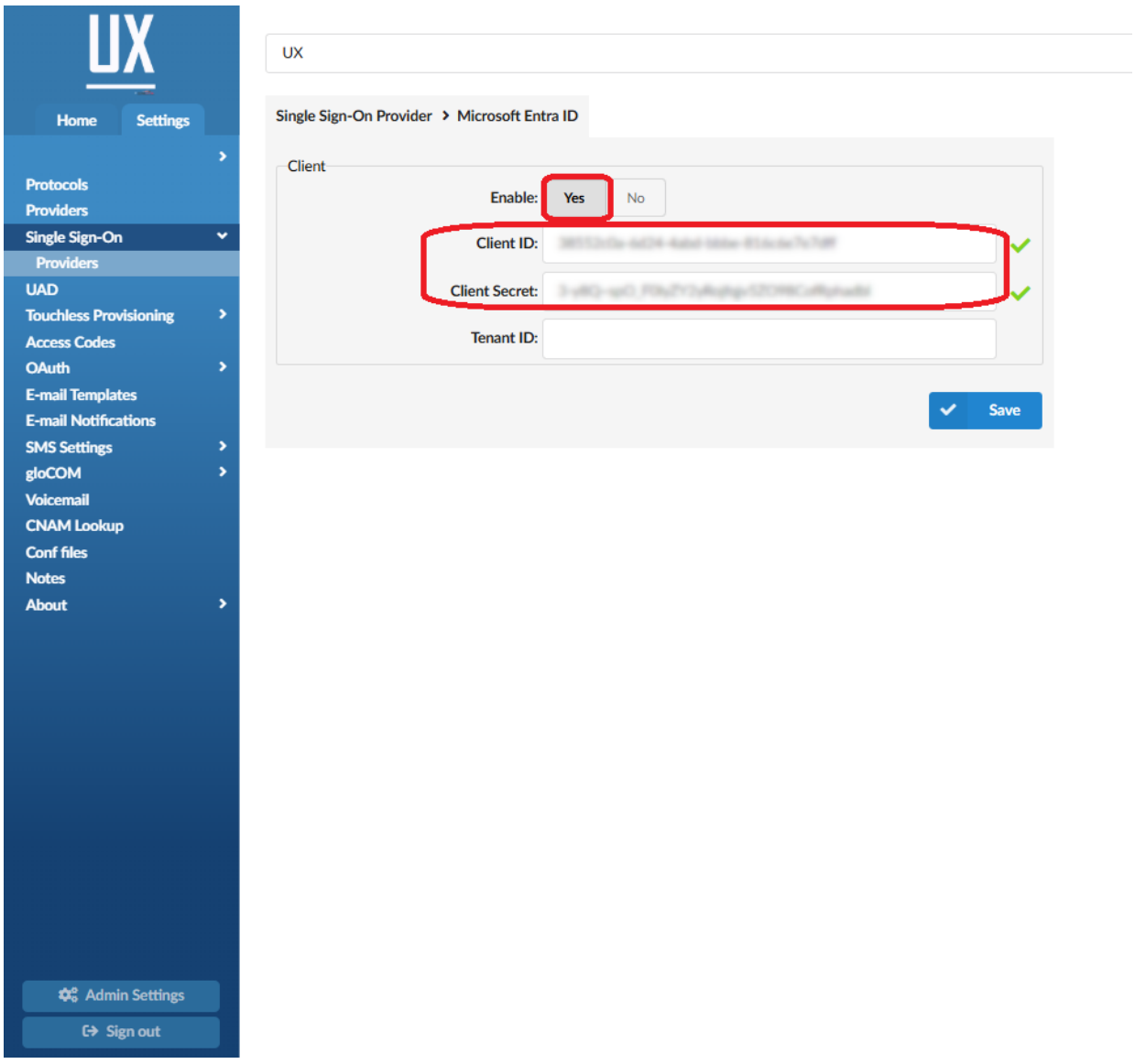
PBX Setup

1. to your PBX system
2. Select the Settings tab
3. Select Sigle 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 Micrososft tenant only.
9. Save

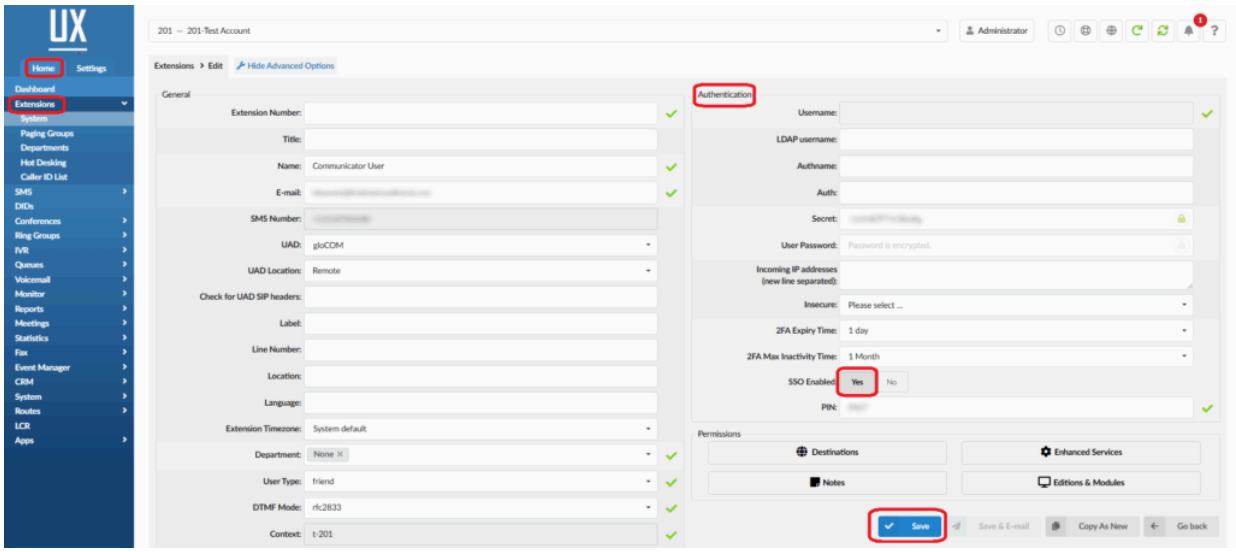


10. Select Servers
11. Move to the Autehntication section and select Yes to Enforce SSO Auth, accross the system. Select No if you want to manage SSO per extension.
12. Select the number of months, (1-3), that you would like the SSO token to expire.

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.



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