POWERFLEET®
People Powered AIoT

Version 1.1

Federated Authentication (SSO) Setup Guide

Connecting to Keycloak from Azure / Microsoft Entra ID

This guide explains how a customer sets up single sign-on (SSO) between their Azure / Entra ID tenant and the Powerfleet Keycloak identity platform. Two protocols are supported: **OpenID Connect 1.0** and **SAML 2.0**. Follow either Option A or Option B, not both.

Table of Contents

1 Process Overview 3

2 What to include in the support case 3

3 Option A: Connect with OpenID Connect 4

3.1 Register the application 4

3.2 Copy the metadata URL 7

3.3 Configure the redirect URL 8

3.4 Create a client secret 9

4 Option B: Connect with SAML 11

4.1 Create the enterprise application 11

4.2 Configure SAML single sign-on 13

4.3 Grant access 15

1 Process Overview

1. The customer configures an application in Azure / Entra ID using OpenID or SAML, following the steps in this guide.
2. The customer contacts Support and includes the details listed in section 2 (including the subject line). A case is created in Salesforce.
3. The case is routed to Advanced Support, where a Service Request is created for the Auth team.
4. The Auth team creates the Keycloak client, adds the customer's email domain(s) so they are discovered for SSO, and handles the Jira updates.
5. The Support team notifies the customer that SSO has been set up. Support manages all communication with the customer throughout the request.
6. SSO is now active. The customer's users sign in with SSO from their next login.

2 What to include in the support case

Use one of these subject lines so the case can be identified and routed correctly:

- **SSO Enable** – to enable SSO
- **SSO Update** – to update the SSO client secret

Collect these details while you complete the setup steps, then include them in the support case:

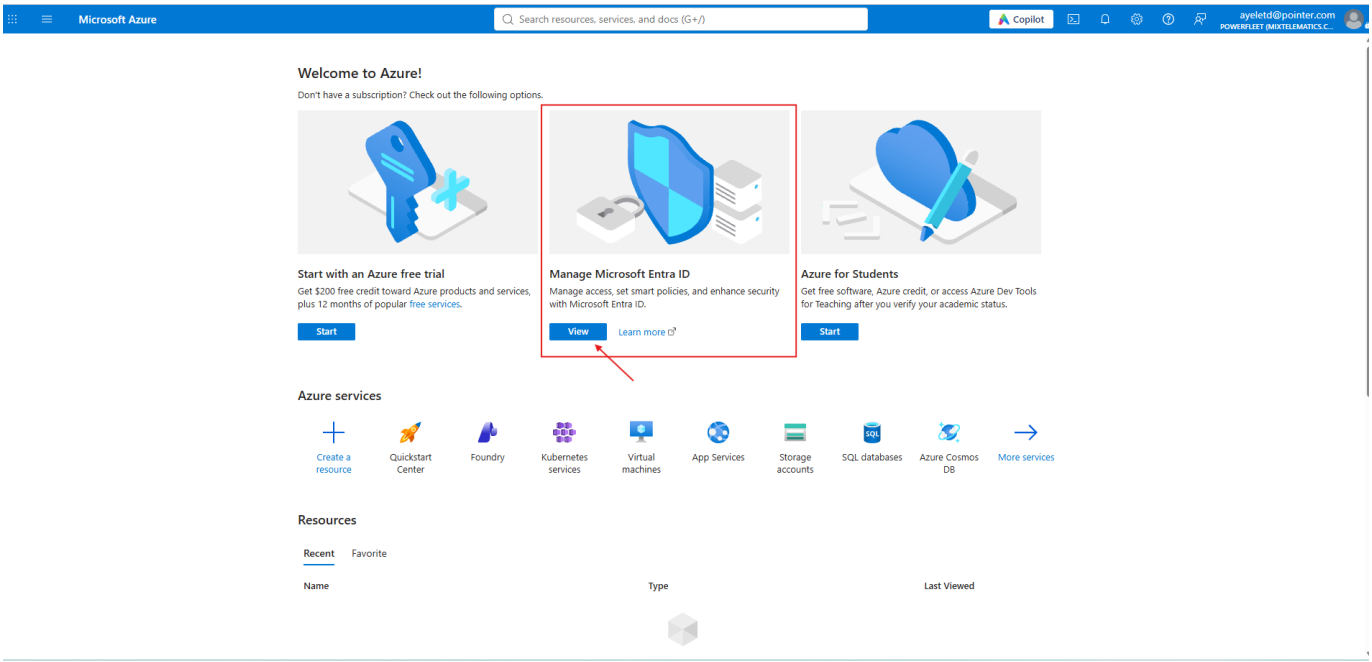
Detail	OpenID	SAML	Where to find it
Company email domain(s)	✓	✓	Your IT team
Display name (app name)	✓	✓	Azure app Overview page
Application (Client) ID	✓		Azure app Overview page
OpenID Connect metadata document URL	✓		Endpoints tab (Option A, step 9)
Client secret value	✓		Certificates & secrets (Option A, step 15)
App Federation Metadata URL		✓	SAML-based Sign-on page (Option B, step 11)

Security: The client secret is a password for your application. Share it only through the support case, never by email or chat, and note its expiry date. Before the current secret expires, create a new one and open a support case with the subject line SSO Update, or SSO will stop working.

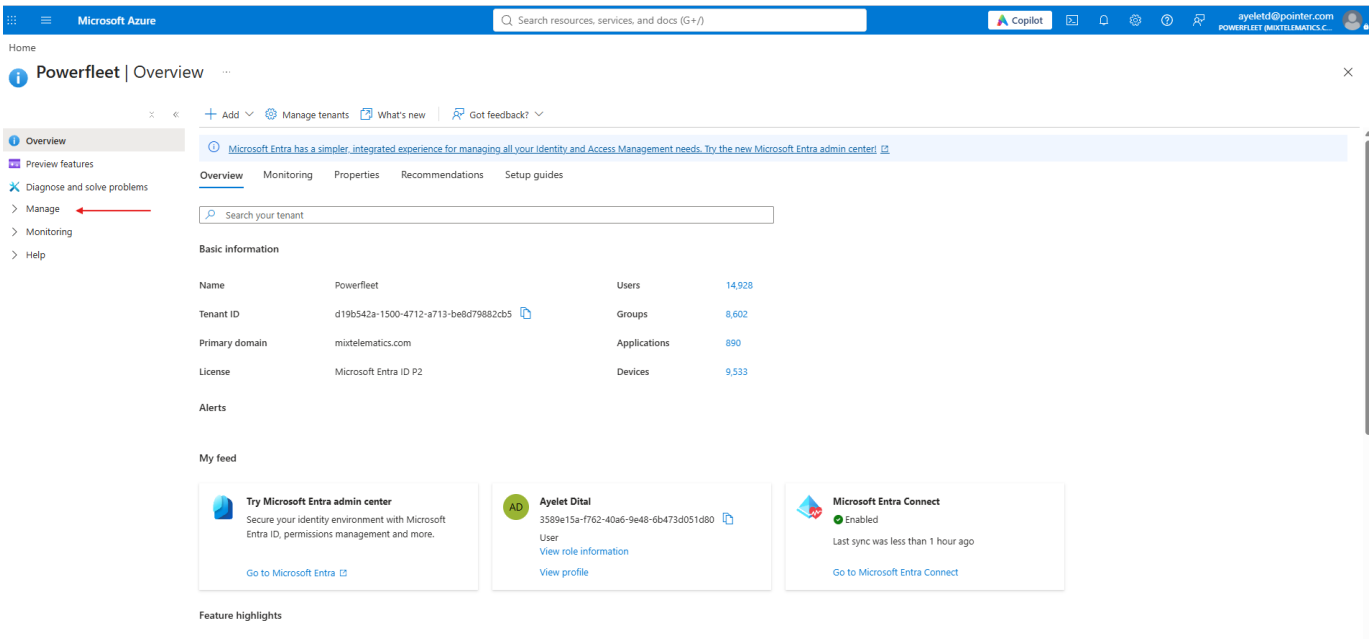
3 Option A: Connect with OpenID Connect

3.1 Register the application

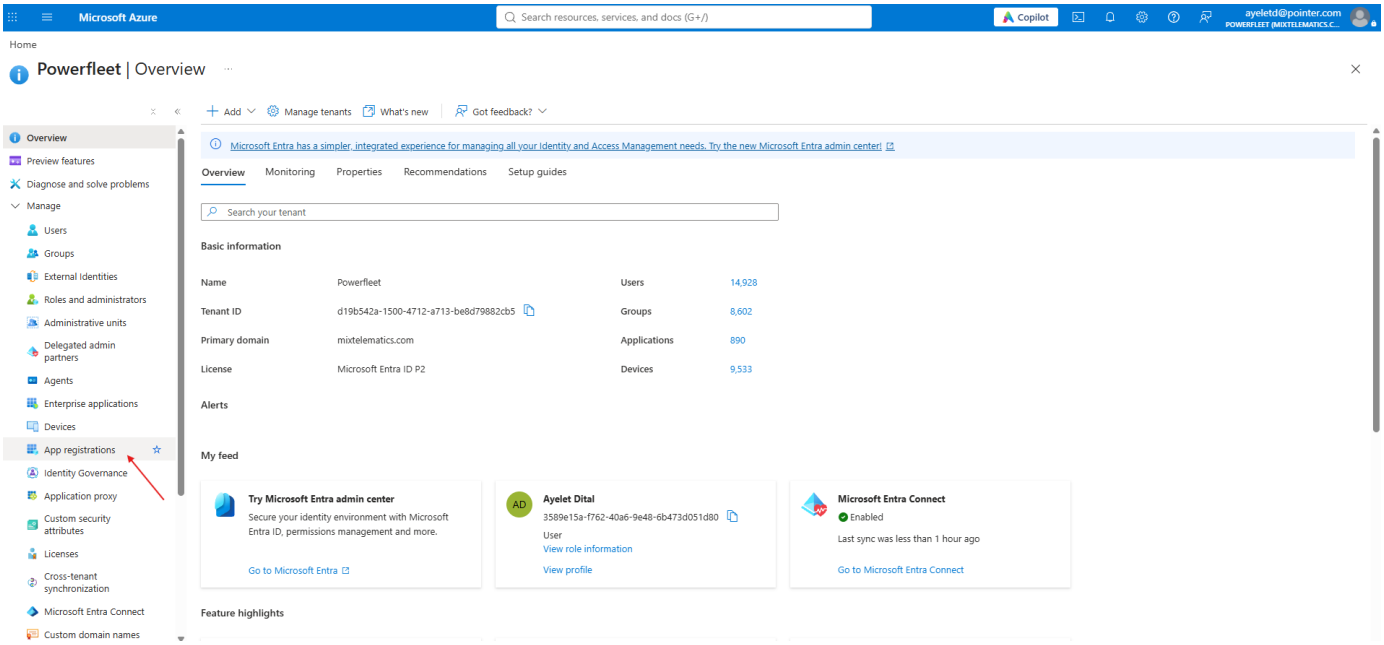
1. Sign in to the Azure portal: https://portal.azure.com/#home
2. Under **Manage Microsoft Entra ID**, click **View**.



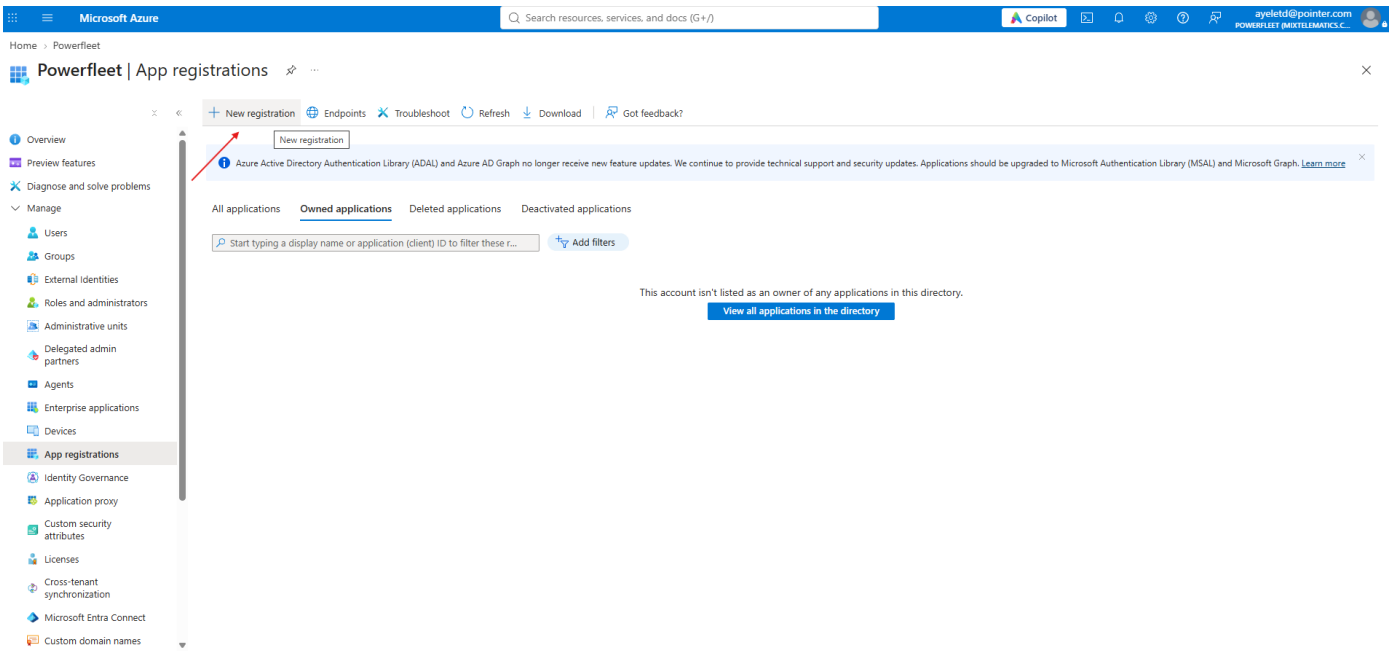
3. In the side menu, expand **Manage**.



4. Select **App registrations**.

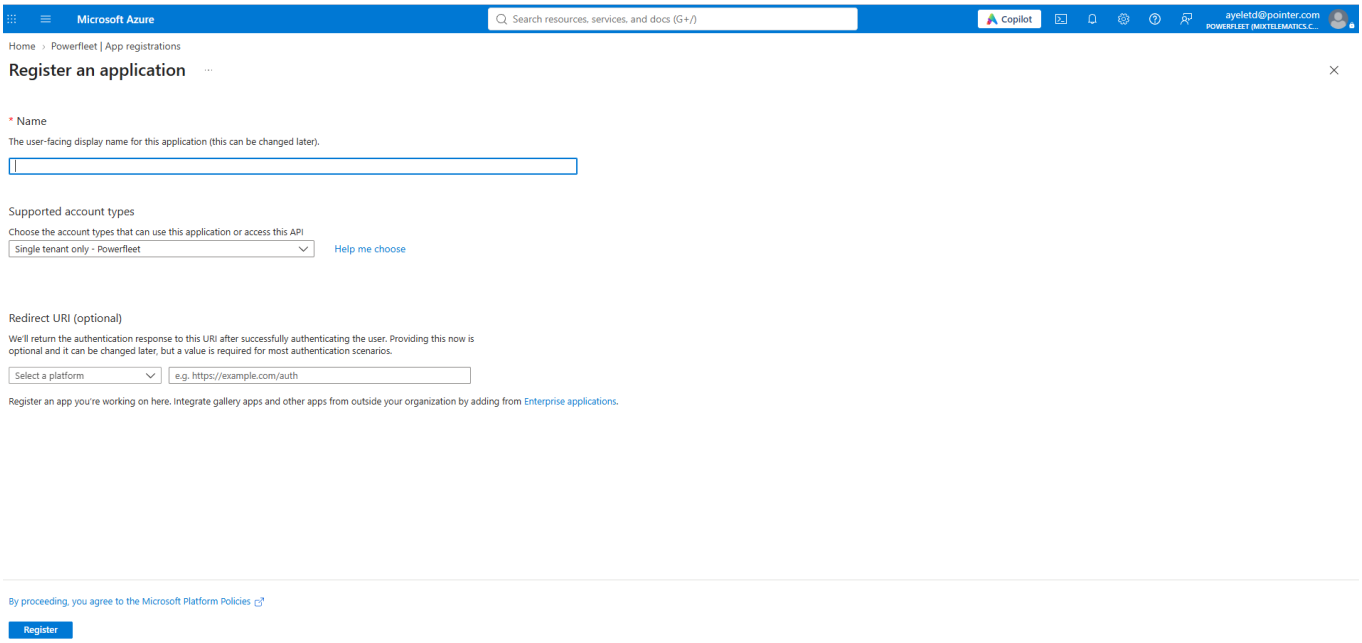


5. Click **New registration**.

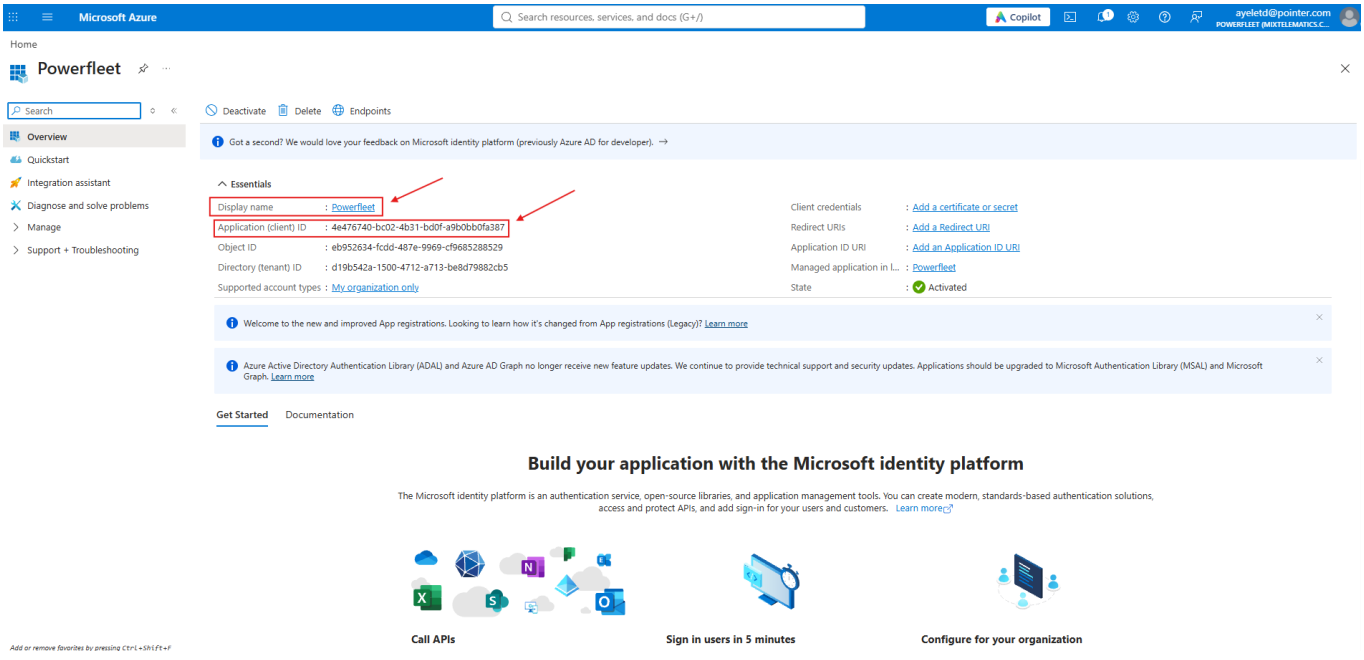


Already have an app? If your company already has an application registered in Azure / Entra ID, select it from the list and skip to step 7.

6. Fill in the required fields to register an application for your company, then click **Register**.

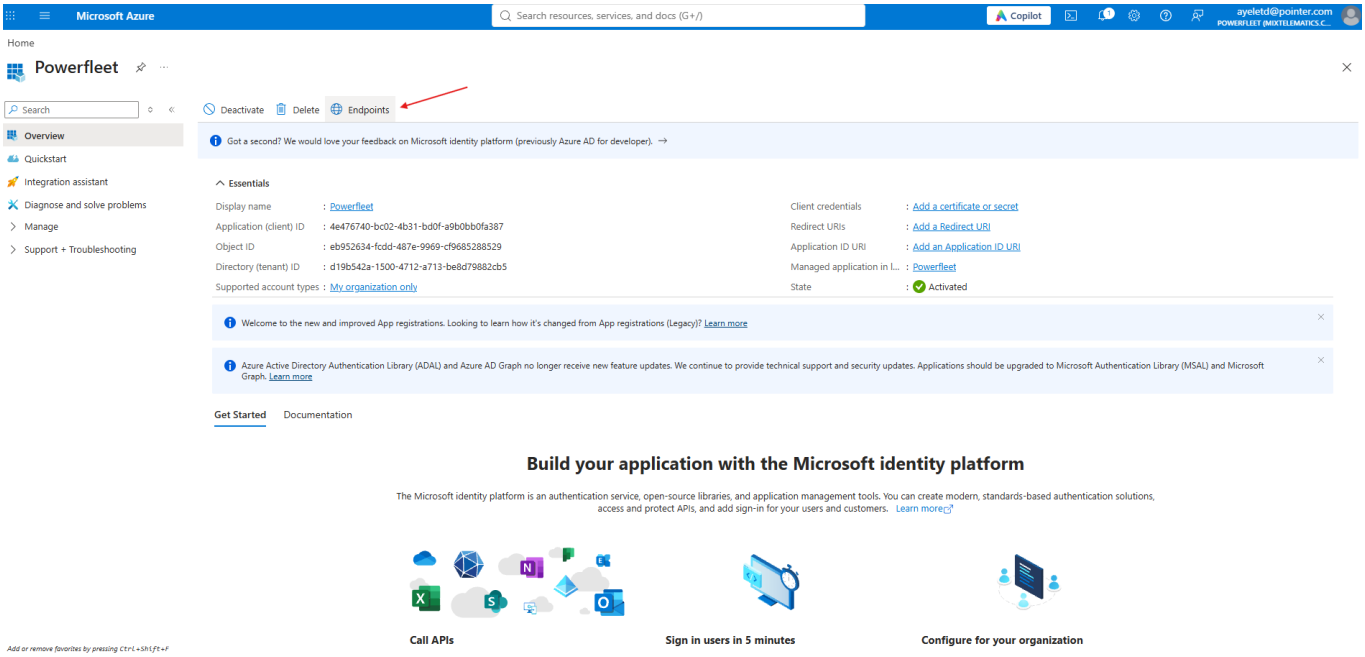


7. On the app's Overview page, copy the following for the support case:
   - **Display name**
   - **Application (client) ID**

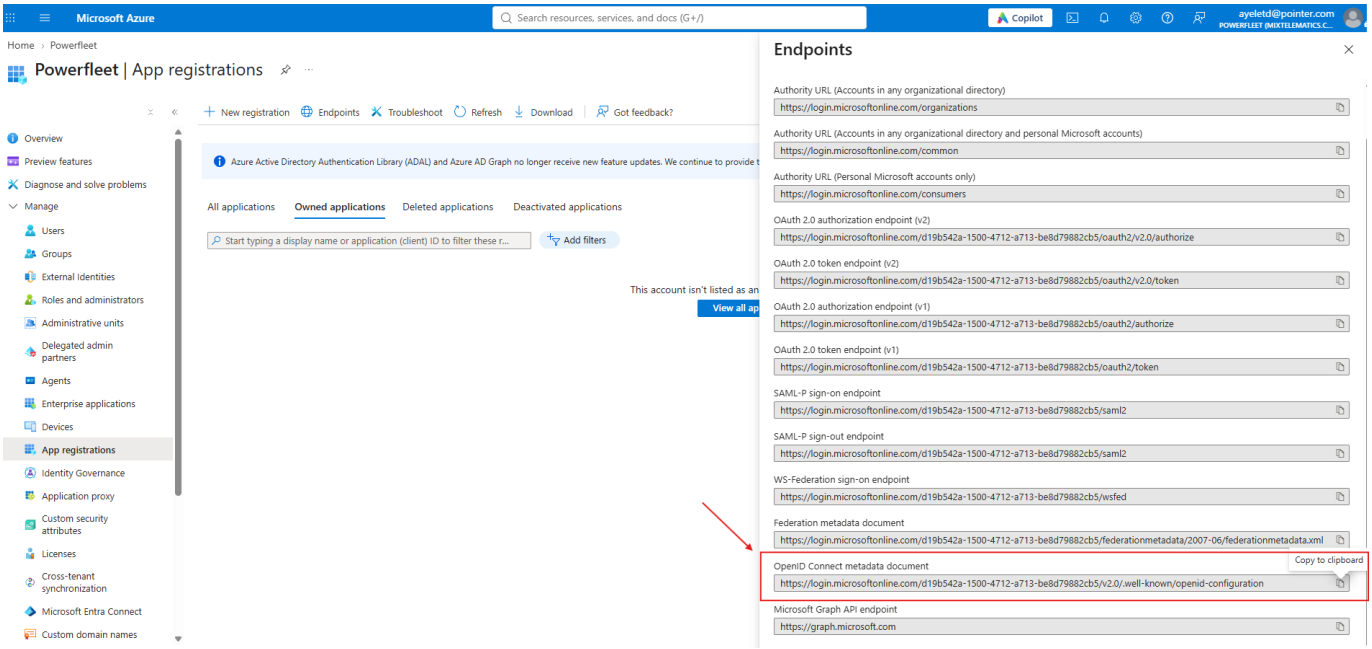


3.2 Copy the metadata URL

8. Select the **Endpoints tab**.

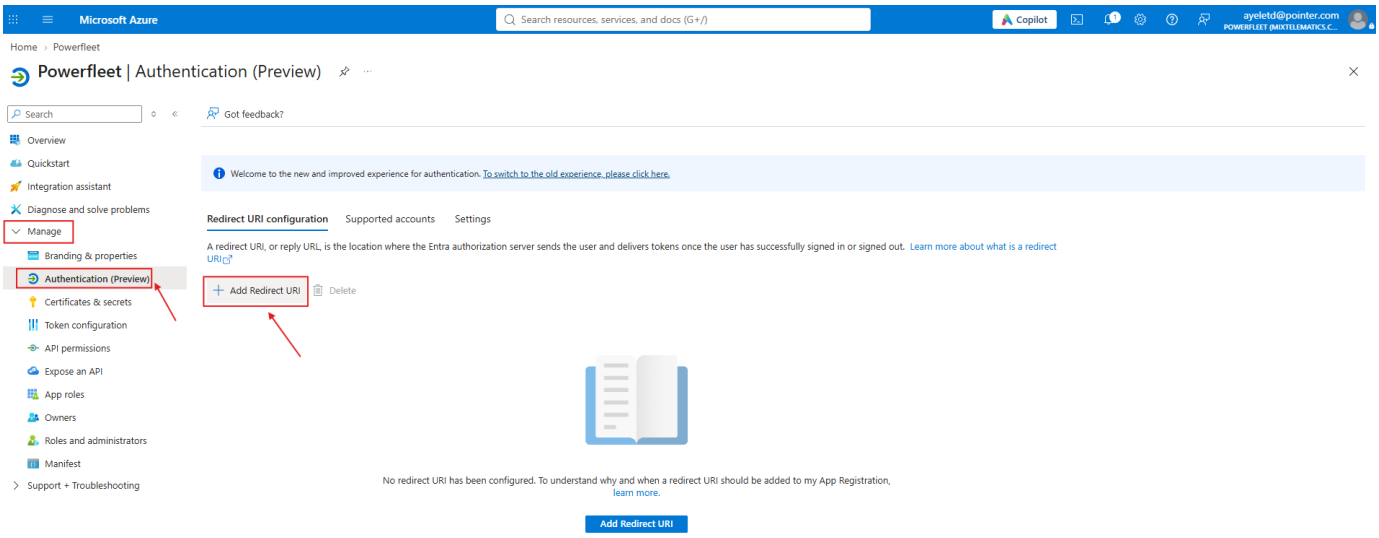


9. Copy the **OpenID Connect metadata document URL** for the support case.

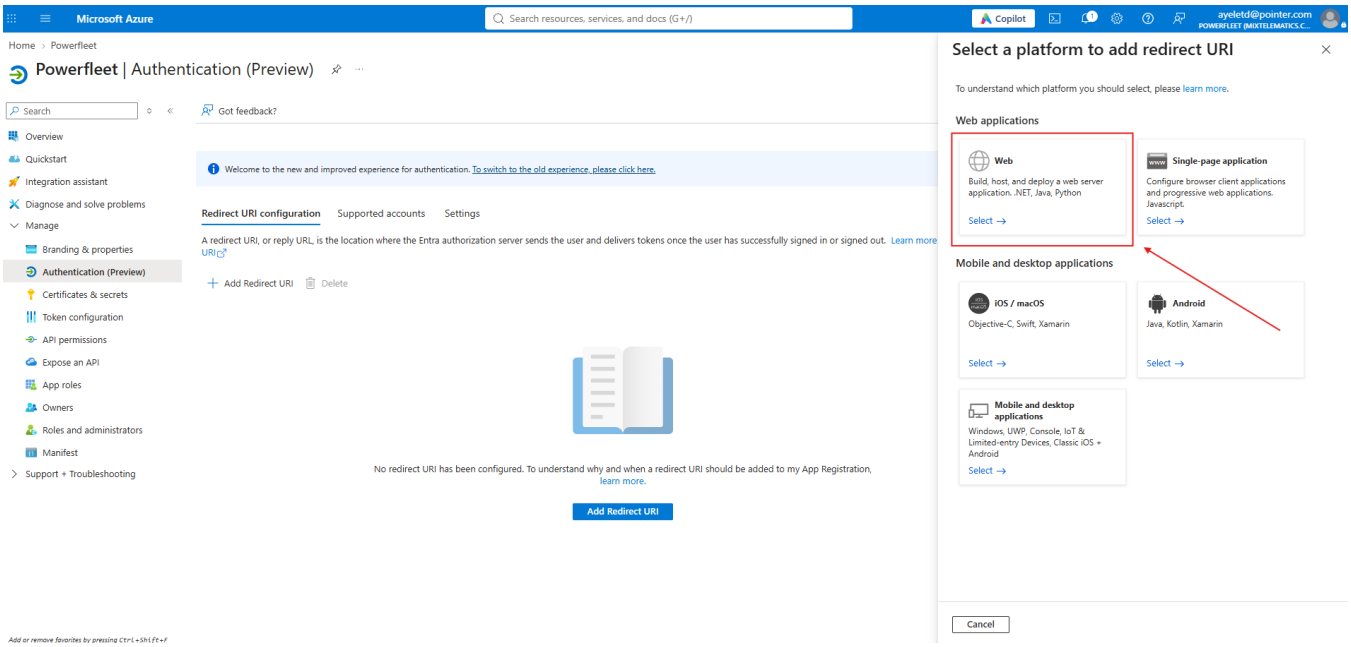


3.3 Configure the redirect URL

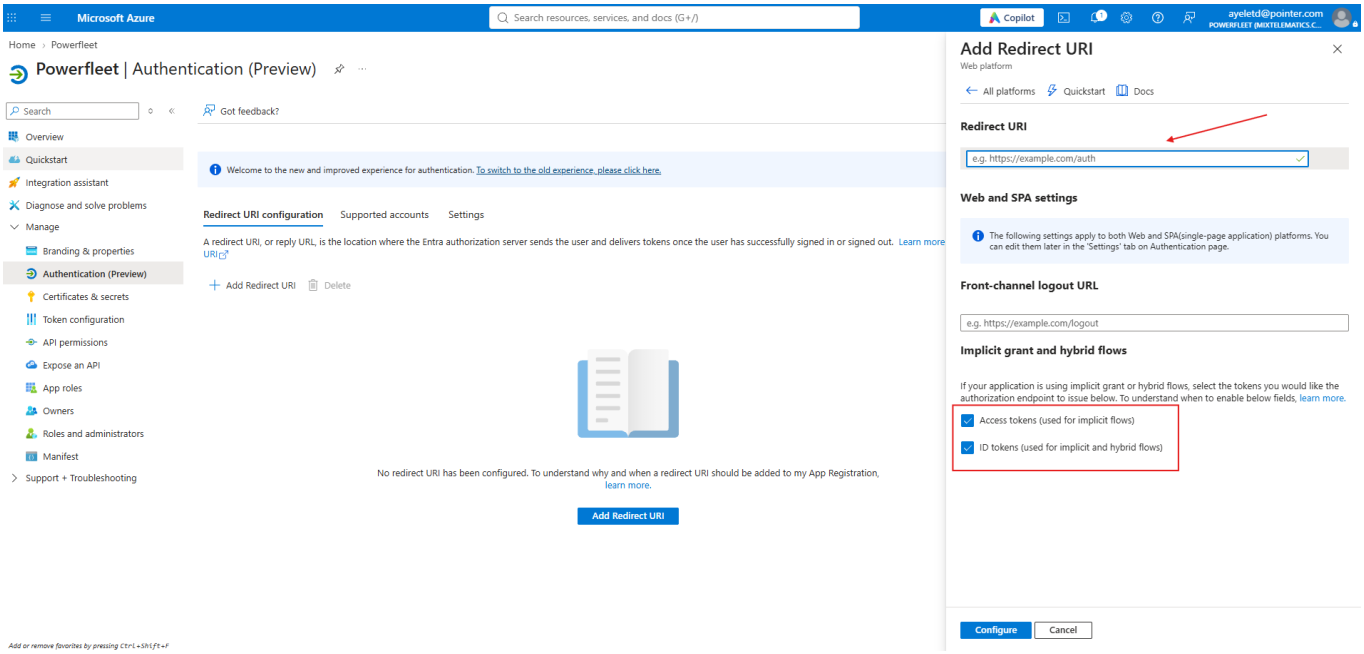
10. In the side menu, select **Authentication (Preview)**, then click **Add Redirect URL**.



11. Select **Web**.

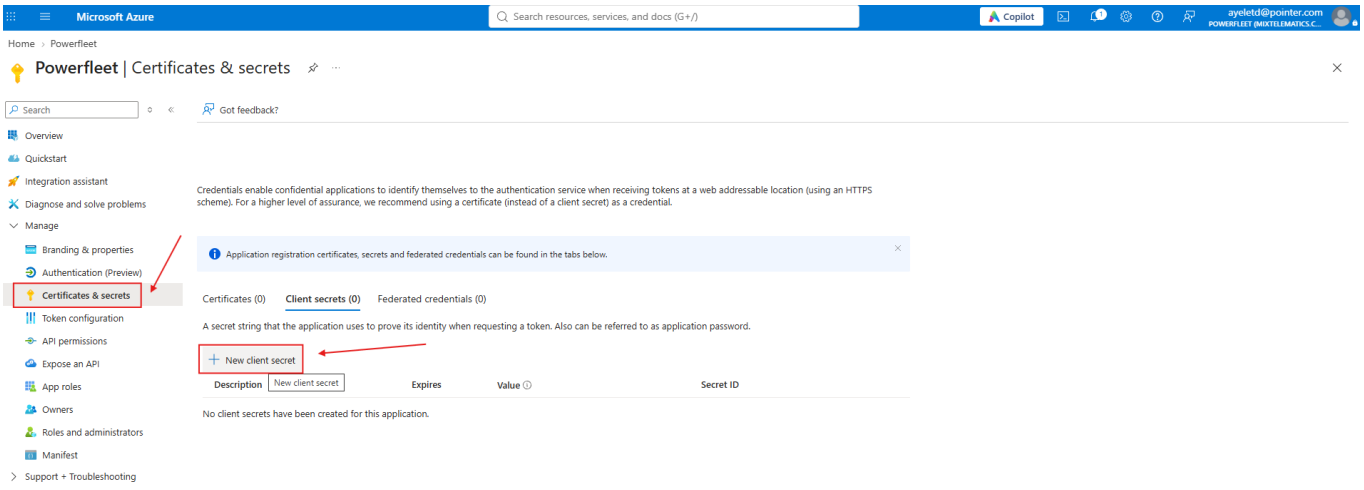


12. Configure the web platform:
    - In the **Redirect URL** field, enter the URL below, replacing **[App Name]** with your app's display name:
    - https://auth.fleetcomplete.com/auth/realms/fleetcomplete/broker/**[App Name]**/endpoint
    - Enable both **Access tokens** and **ID tokens**.
    - Click **Configure.**

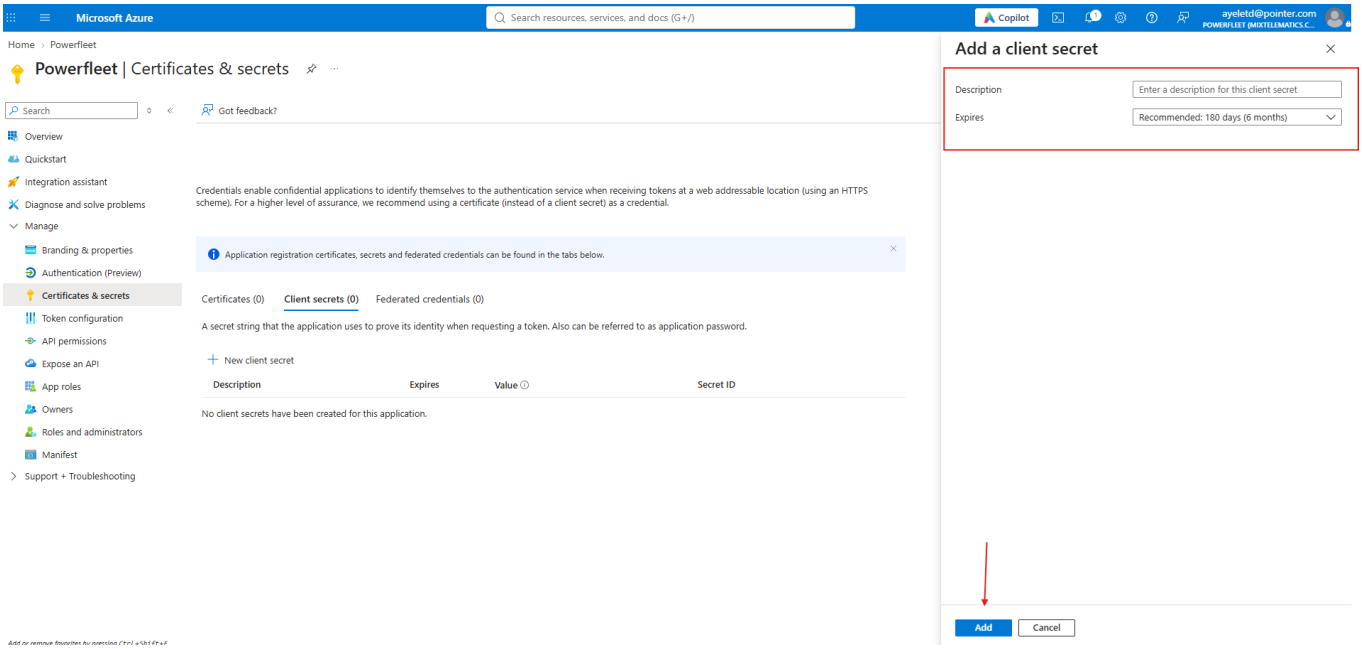


3.4 Create a client secret

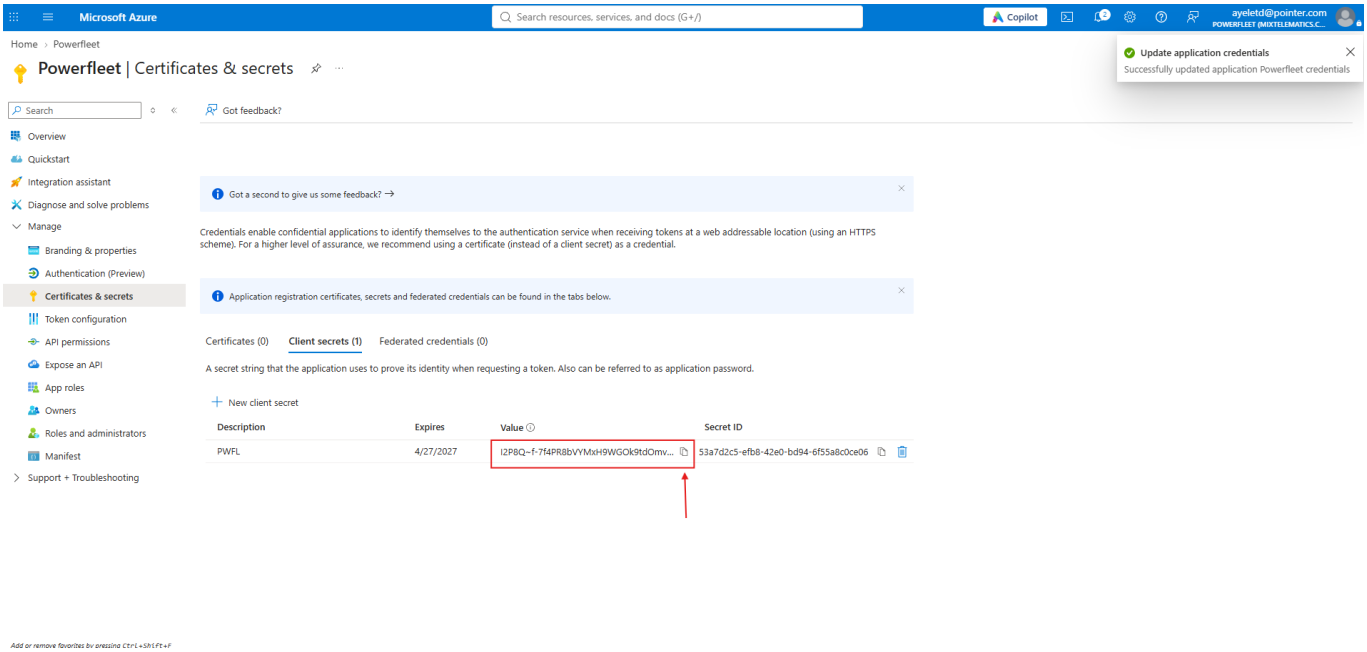
13. In the side menu, select **Certificates & secrets**, then click **New client secret**.



14. Enter a description, choose an expiry period, and click **Add**.



15. Copy the secret **Value** right away and add it to the support case.



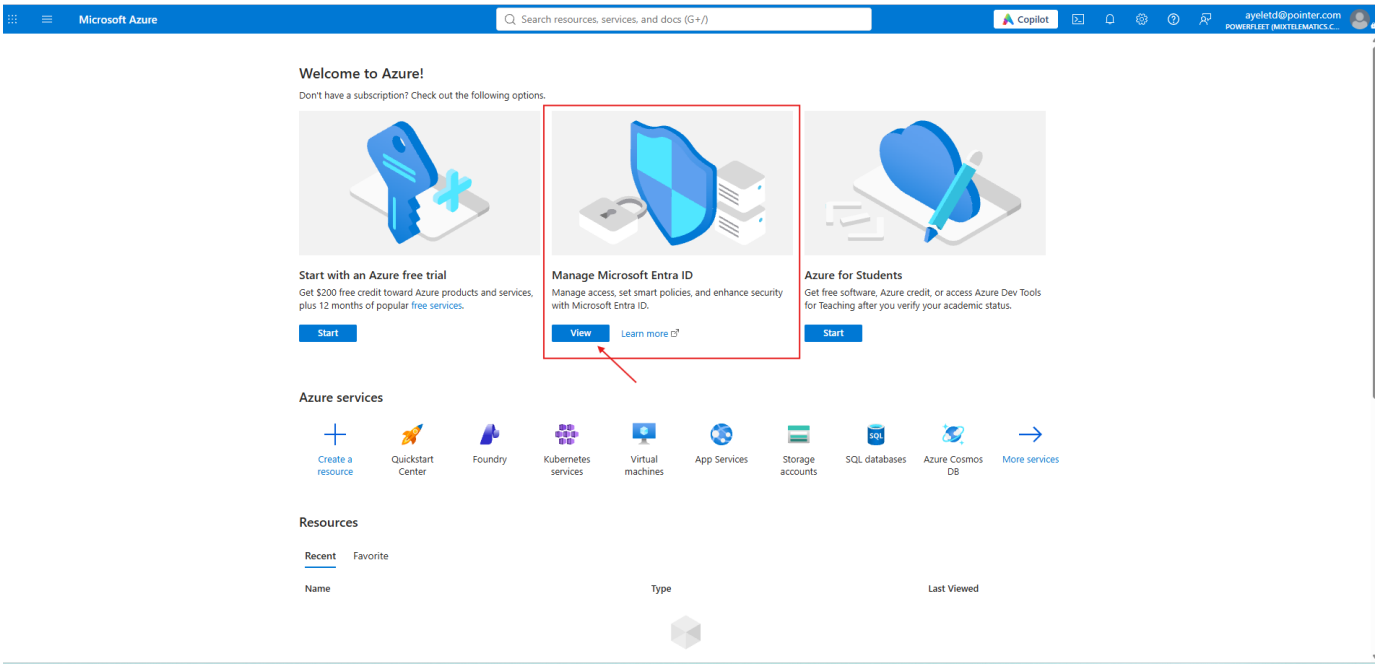
Important: Azure shows the secret value only once. If you leave the page before copying it, you must create a new secret.

16. Confirm with your IT team that the relevant Azure users have access to the new application.

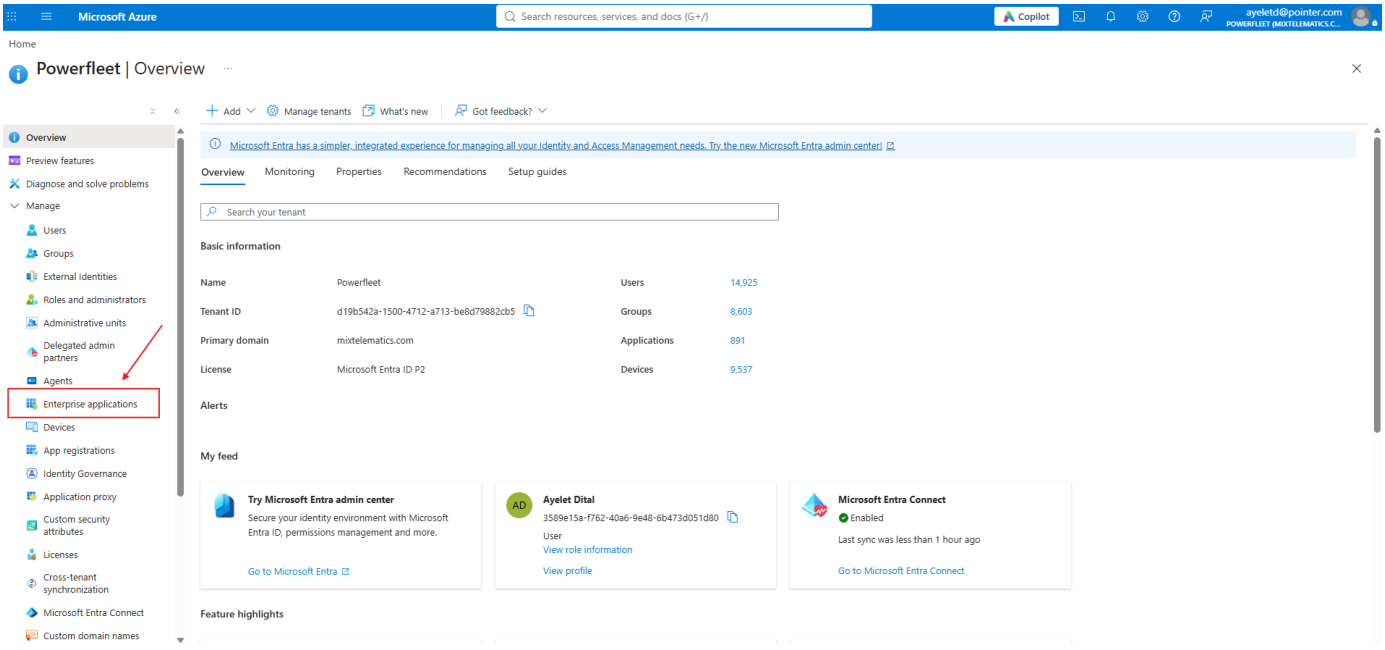
4 Option B: Connect with SAML

4.1 Create the enterprise application

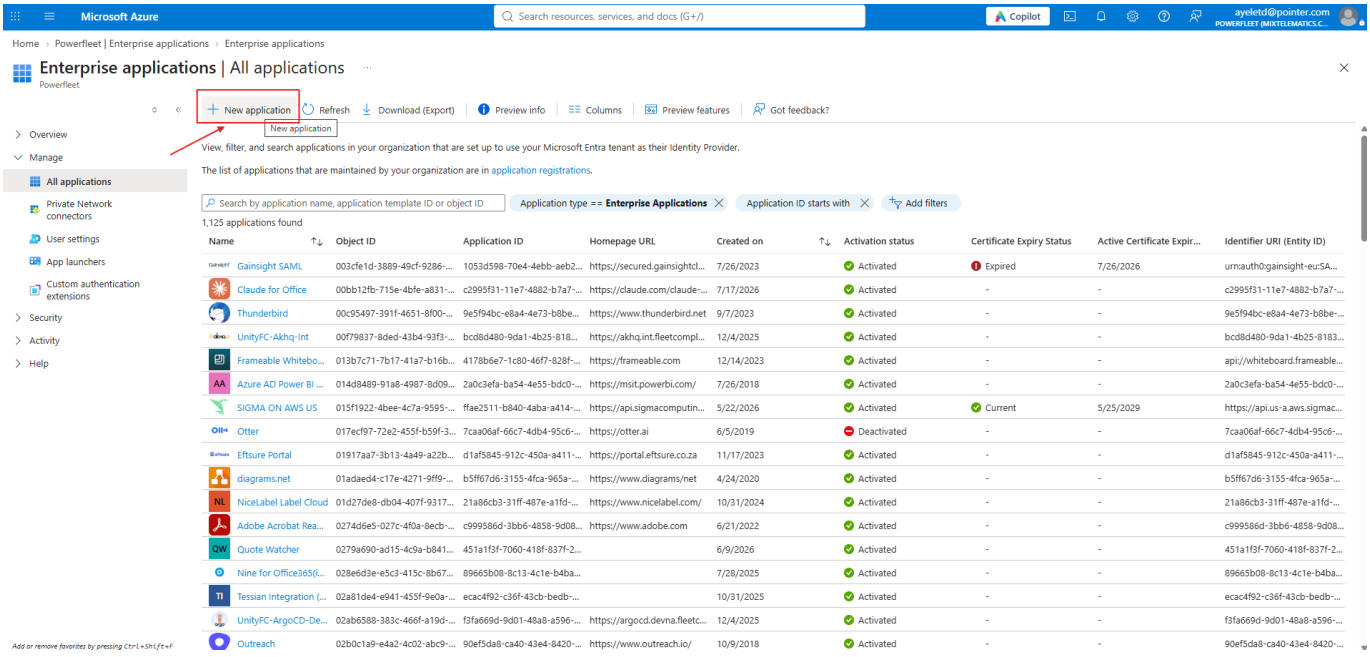
1. Sign in to the Azure portal: https://portal.azure.com/#home
2. Under **Manage Microsoft Entra ID**, click **View**.



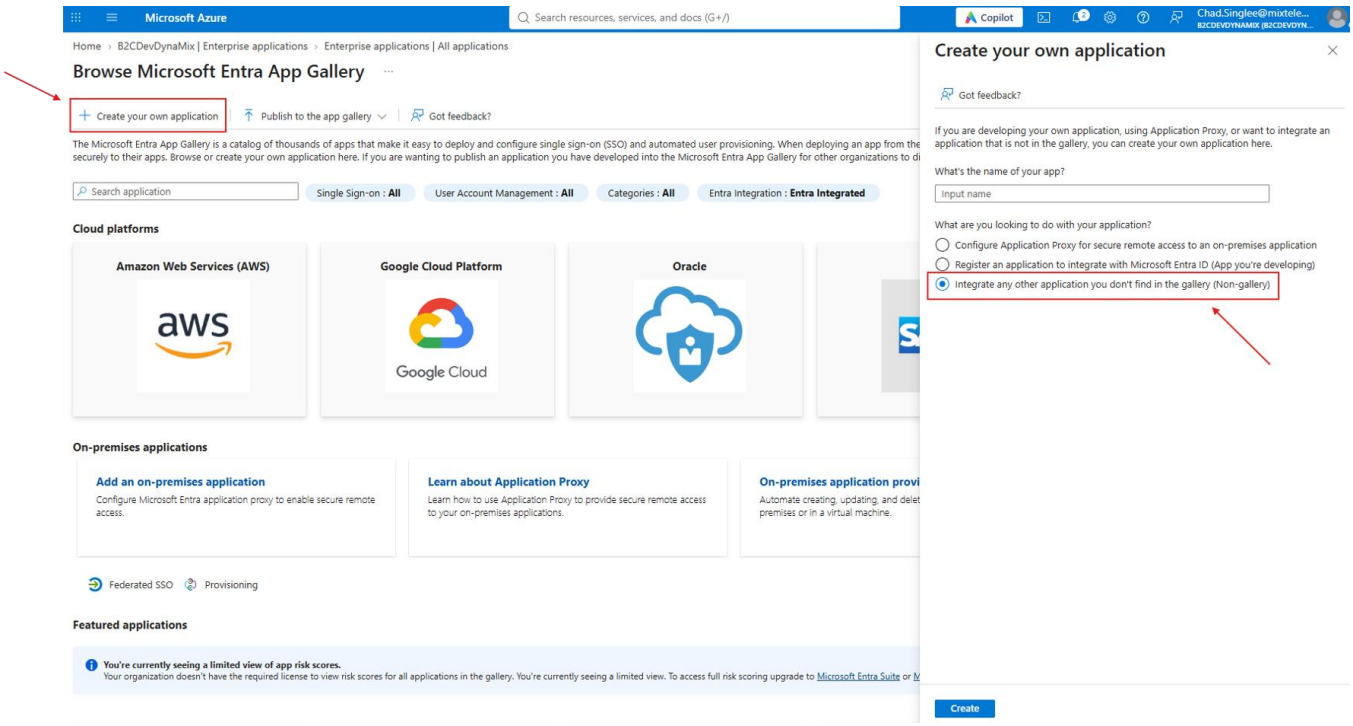
3. Select **Enterprise applications**.



4. Click **New application**.

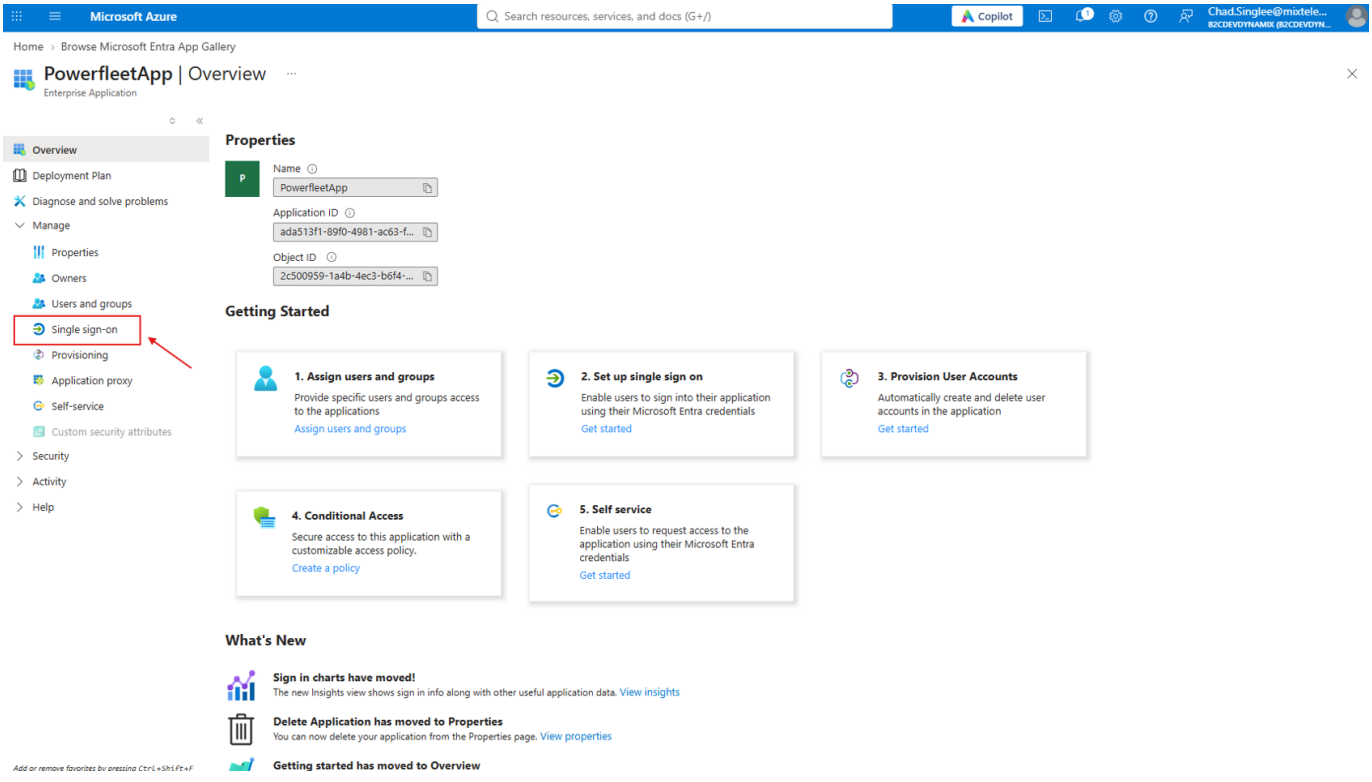


5. Click **Create your own application**, enter a name, **select Integrate any other application you don't find in the gallery (Non-gallery)**, and click **Create**.

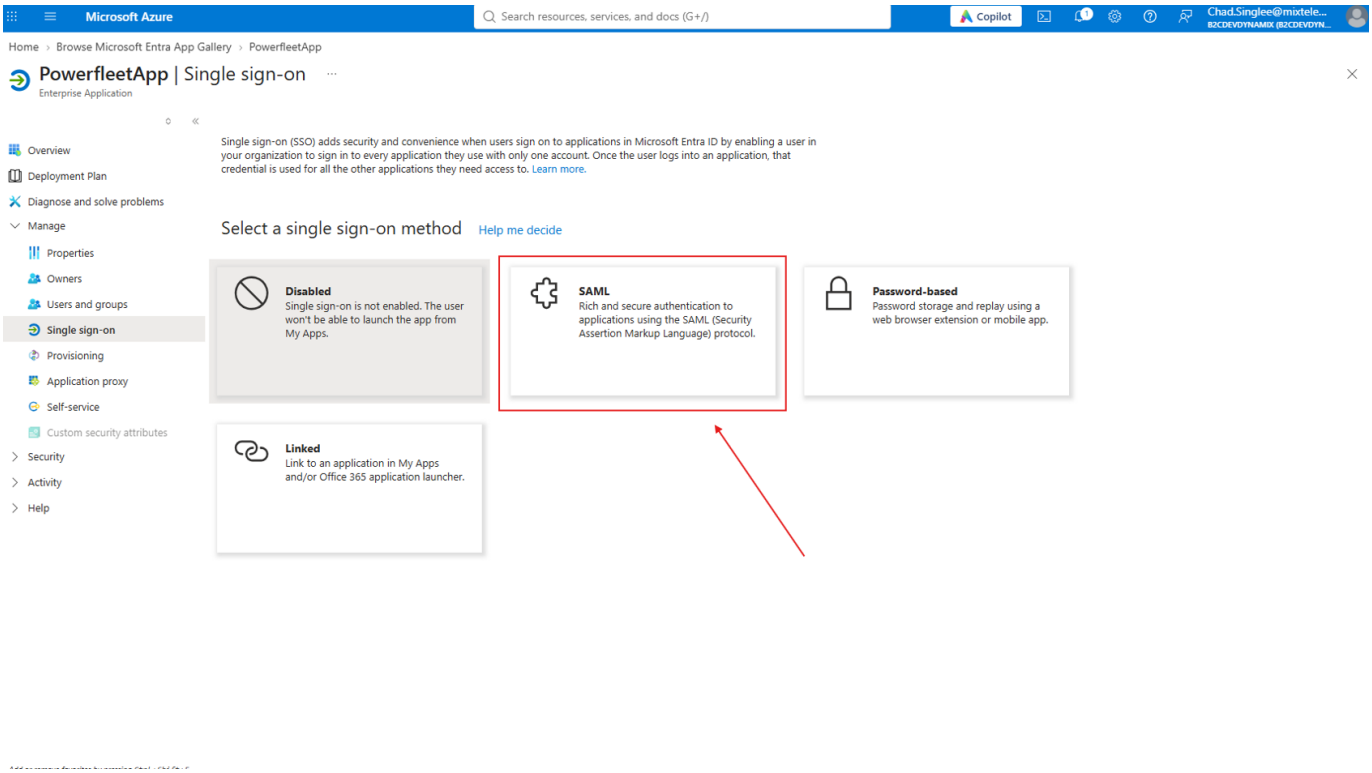


4.2 Configure SAML single sign-on

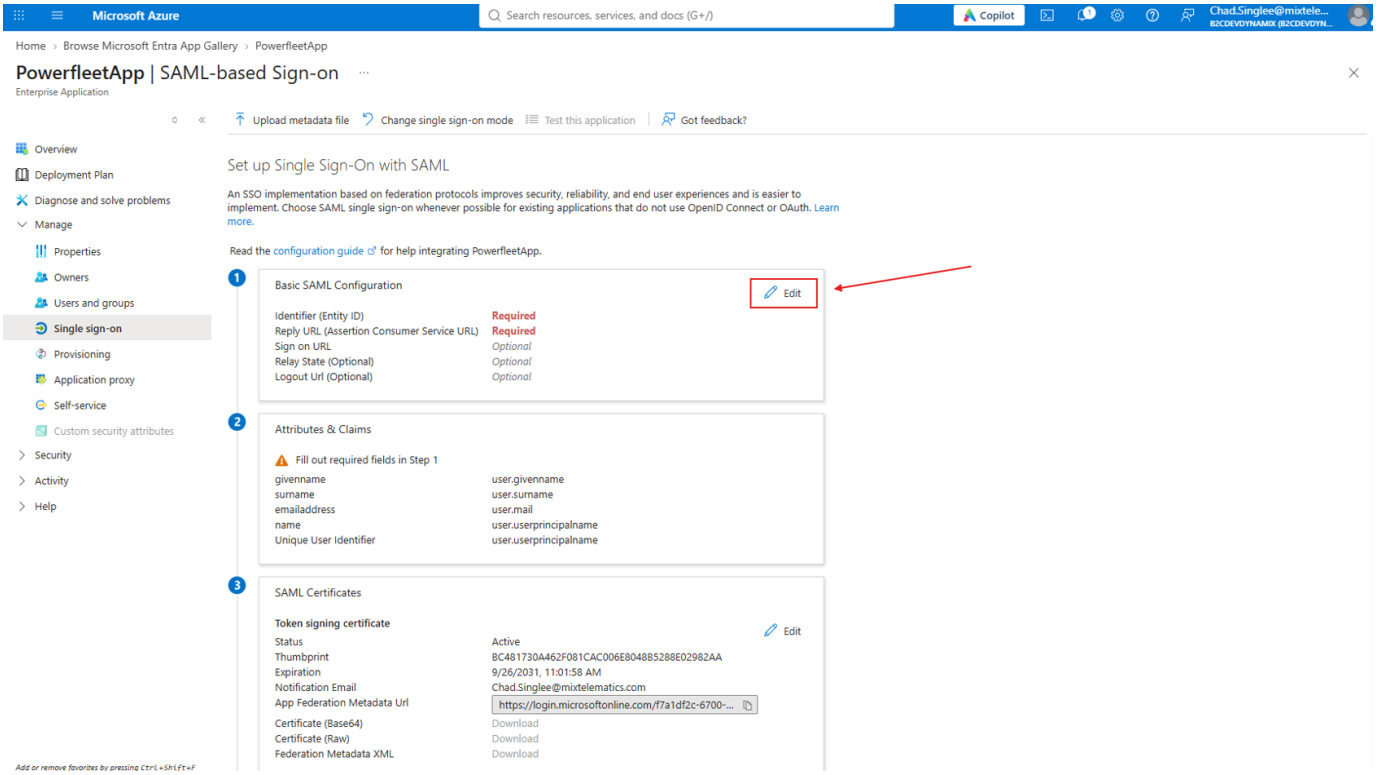
6. In the side menu, select **Single sign-on**.



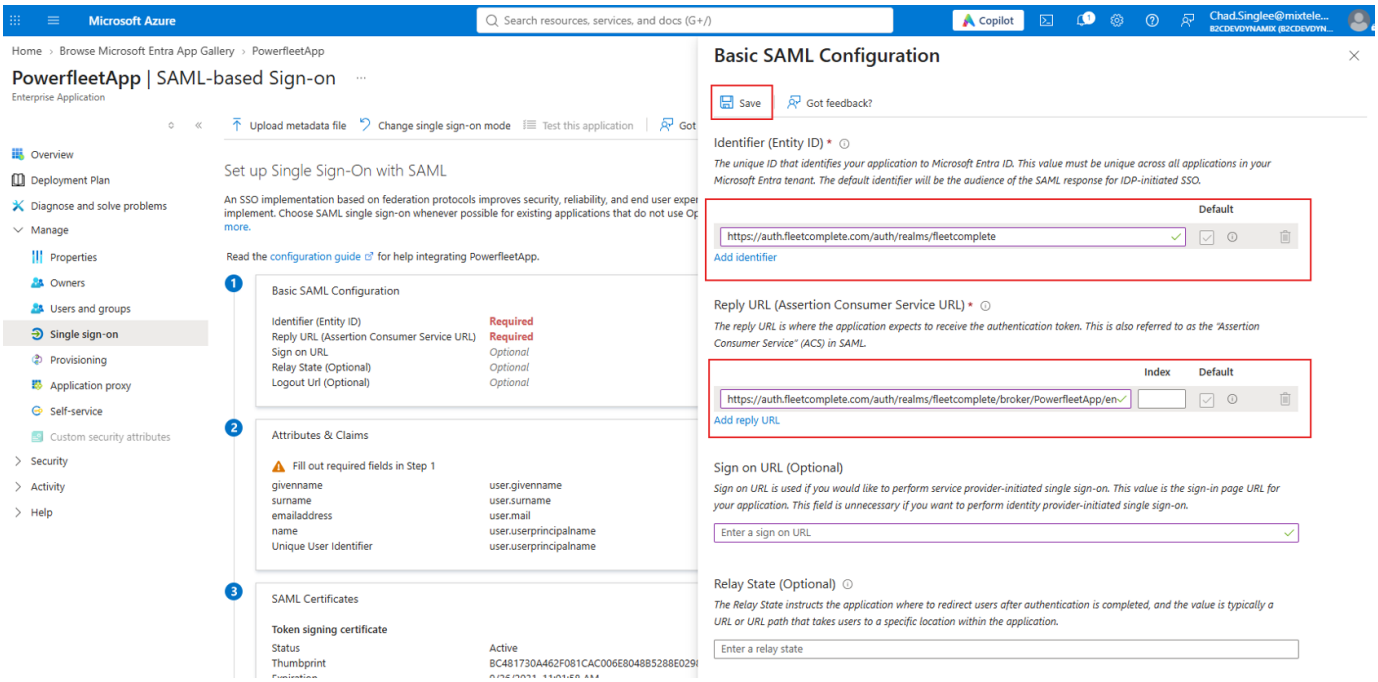
7. Select **SAML**.



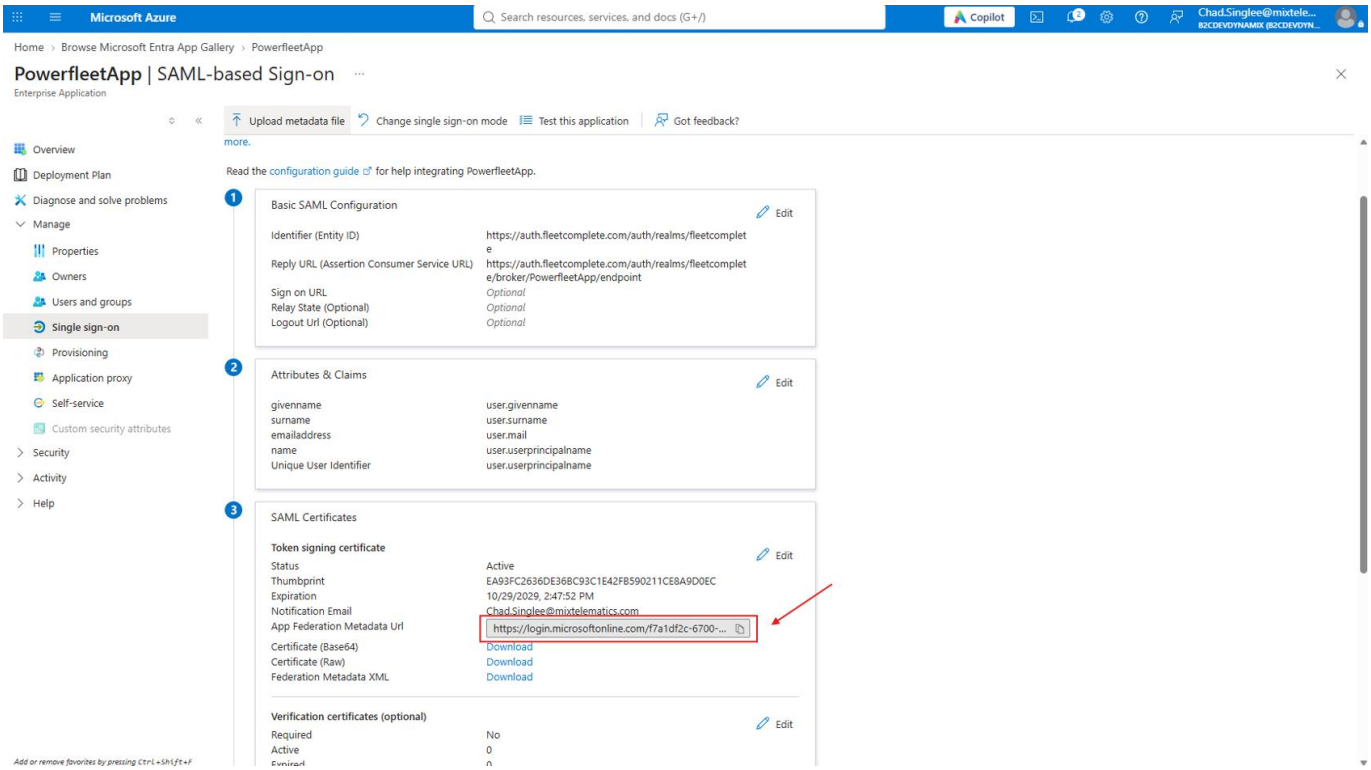
8. In the **Basic SAML Configuration** section, click **Edit**.



9. Enter the following values, replacing **[App Name]** with your application name:
   - Identifier (Entity ID): https://auth.fleetcomplete.com/auth/realms/fleetcomplete
   - Reply URL: https://auth.fleetcomplete.com/auth/realms/fleetcomplete/broker/**[App Name]**/endpoint



10. Click **Save**.
11. Copy the **App Federation Metadata Url** and **add** it to the support case.



4.3 Grant access

12. Assign the relevant users or groups to the new application (under **Users and groups**) so they can sign in with SSO.