

Entra App Registration Setup Guide

Step-by-step guide for "Xero M365 OAuth Service"

"Xero M365 OAuth Service"



Introduction

This guide provides clear, step-by-step instructions for creating an App Registration in Entra ID (Azure Active Directory) called Xero M365 OAuth Service.

Step 1: Login to Azure Portal

- Go to <https://entra.microsoft.com/> and sign in with an account that has any of the following roles.
 - Application Administrator
 - Cloud Application Administrator
 - Global Administrator

Step 2: Register a New Application

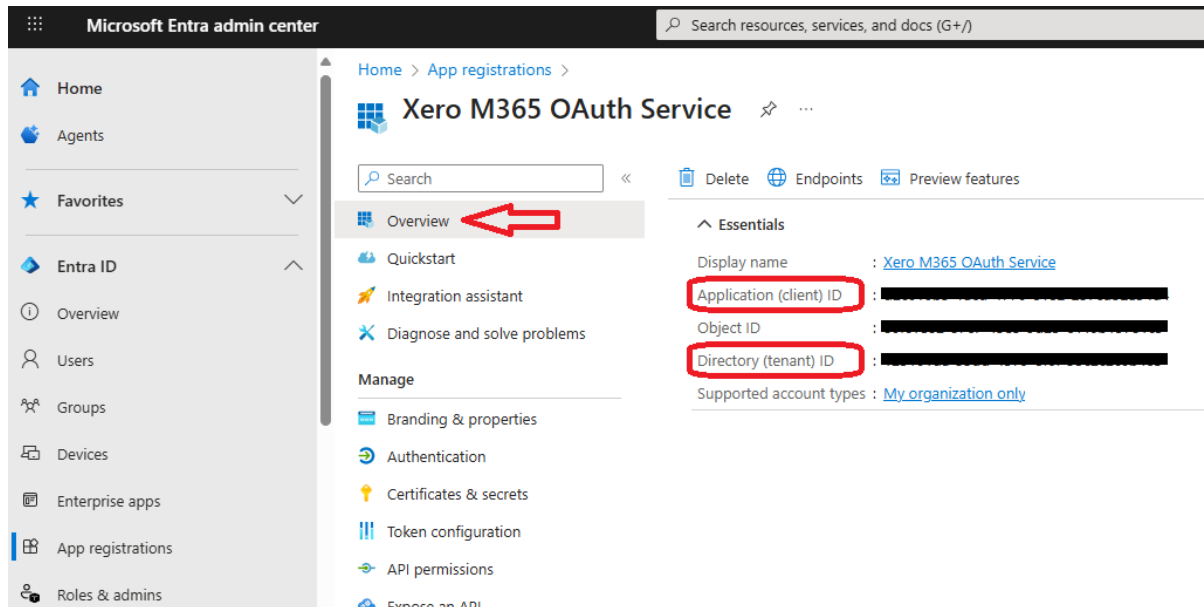
- In the left sidebar, click on App registrations.
- Click + New registration at the top.
- Enter the following details:
- Name: **Xero M365 OAuth Service**
- Supported account types: Select "Accounts in this organizational directory only (Single tenant)" unless you have a specific need for other options.
- Redirect URI: (Optional; can be filled in later if needed.)

Click Register.

The screenshot shows the Microsoft Entra admin center interface. The left sidebar contains a navigation menu with items like Home, Agents, Favorites, Entra ID, Overview, Users, Groups, Devices, Enterprise apps, App registrations, Roles & admins, Delegated admin partners, Domain services, Conditional Access, Multifactor authentication, Identity Secure Score, and Authentication methods. A red arrow points to 'App registrations'. The main content area is titled 'Register an application'. It includes a 'Name' field with the value 'Xero M365 OAuth Service' and a red arrow pointing to it. Below this is the 'Supported account types' section with three radio button options: 'Accounts in this organizational directory only (Single tenant)' (selected), 'Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)', and 'Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)'. A red arrow points to the first option. At the bottom, there is a 'Redirect URI (optional)' section and a 'Register' button, both with red arrows pointing to them. The 'Register' button is a blue button with white text.

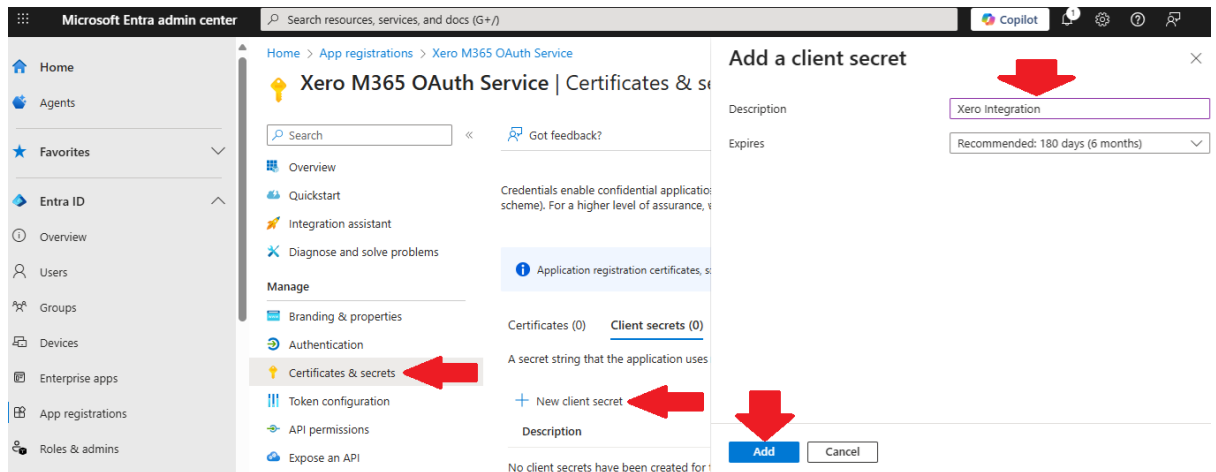
Step 3: Record Directory (tenant) ID and Application (client) ID

- After registration, you will be redirected to the application's Overview page.
- Copy and save the following information (you'll need it later):
- Directory (tenant) ID
- Application (client) ID

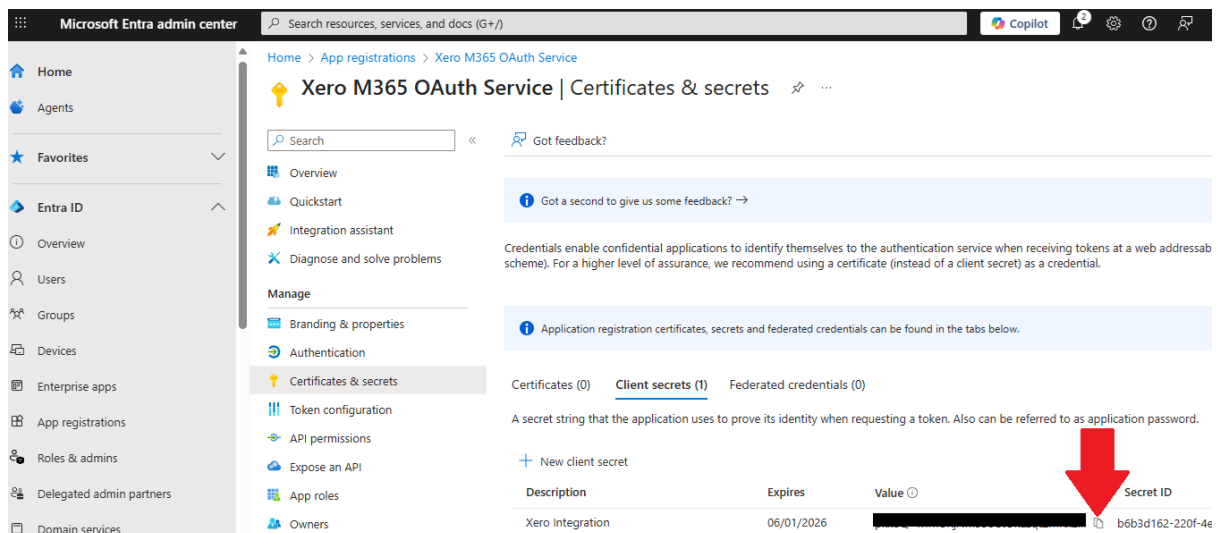


Step 4: Create a Client Secret

- In the left menu under Manage, select Certificates & secrets.
- In the Client secrets section, click + New client secret.
- Enter a description (e.g., "Xero Integration") and choose the desired expiration period.
- Click Add.

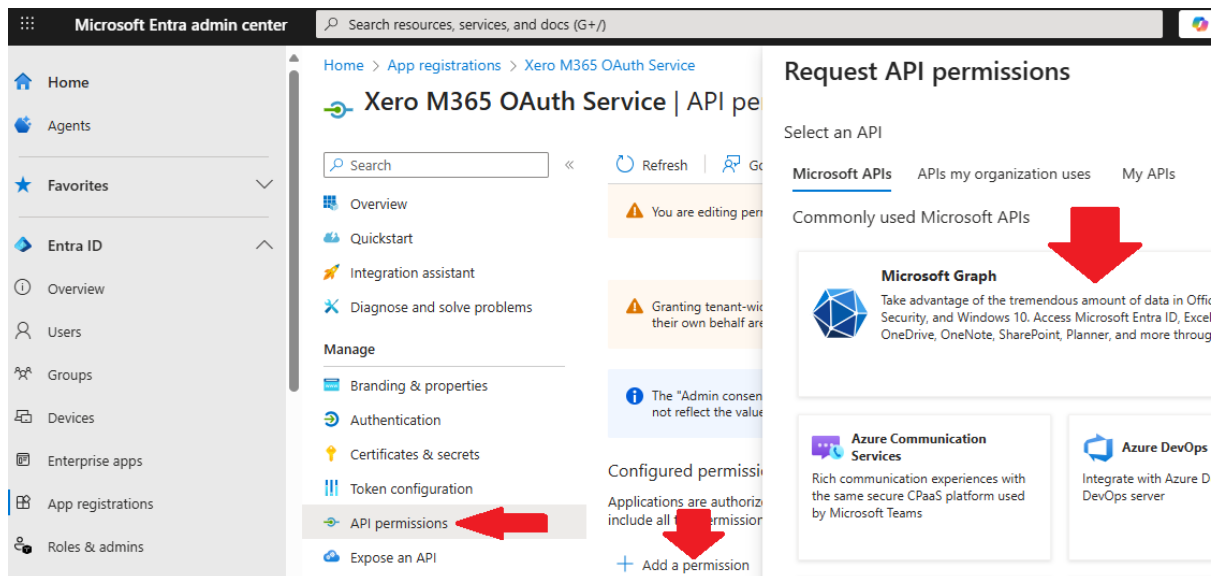


- **IMPORTANT:** Immediately after creation, copy the Value of the client secret and save it securely. You will not be able to retrieve it again later.

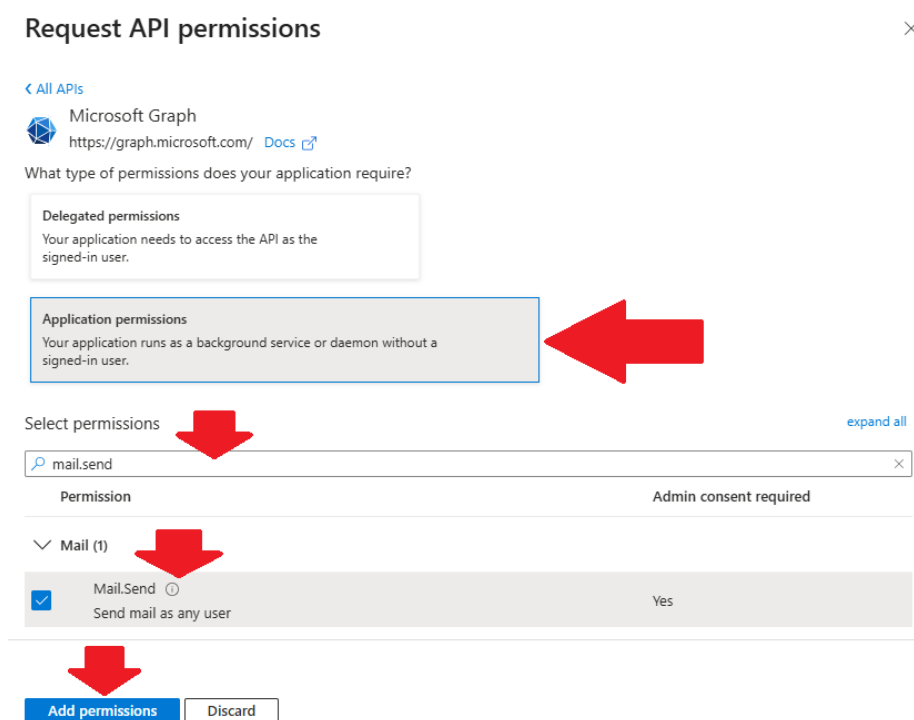


Step 5: Add Microsoft Graph API Permission (Mail.Send)

- In the left menu, select API permissions.
- Click + Add a permission.
- Select Microsoft Graph.

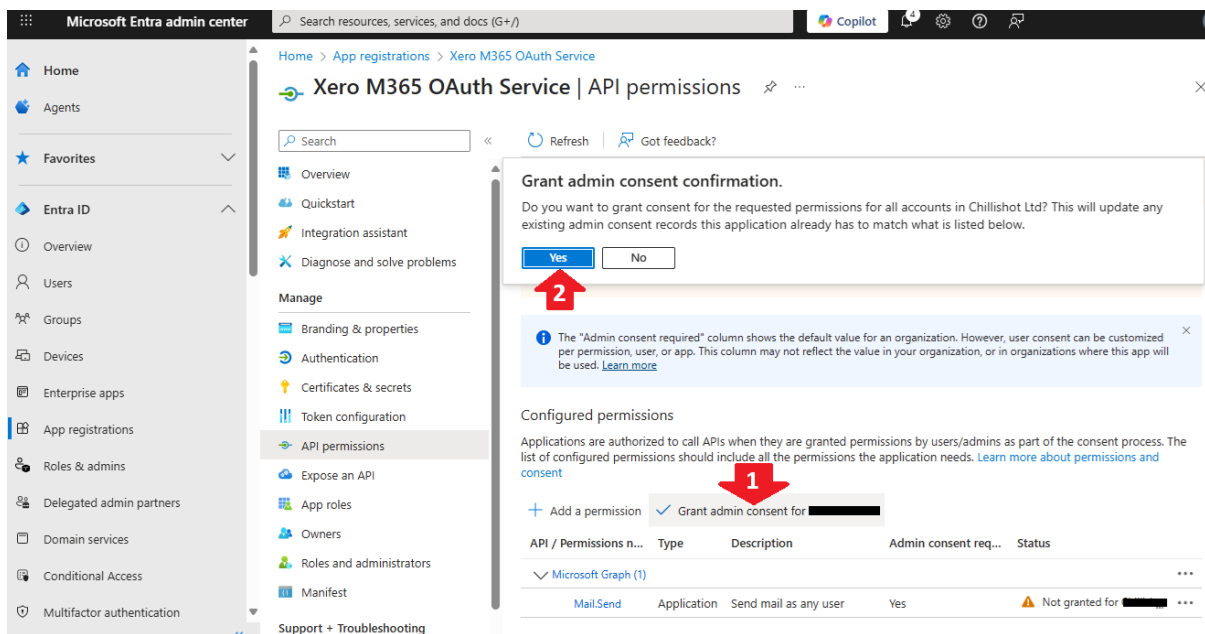


- Choose Application permissions (not Delegated permissions).
- In the search box, type "Mail.Send".
- Tick the checkbox for Mail.Send.
- Click Add permissions.



Step 6: Grant Admin Consent

- After adding the permission, you'll see it listed in the API permissions page, ensure Mail.Send is the only one listed, remove all others. Click the Grant admin consent for [Your Tenant Name] button.
- Confirm the prompt to grant consent.
To grant Admin Consent you will need to be assigned the **Global Administrator** role, or the **Privileged Role Administrator** role.
- The status should update to show that admin consent has been granted.



Step 7: Enter the following in appsettings.json

- Directory (tenant) ID: Found on the App Registration's Overview page.
- Application (client) ID: Found on the same Overview page.
- Client Secret Value: Found only at the moment of creation in the Certificates & secrets section. Store it securely.
- Shared Mailbox: This is the mailbox you wish to send emails from.
This can be a User or Shared Mailbox, but the email address MUST exist.