App Registration & Microsoft Graph Authentication – Entra ID (Free Tier)

Mini Company Directory – Project 2

by Boyon Dey Shipon

Date: August 2025

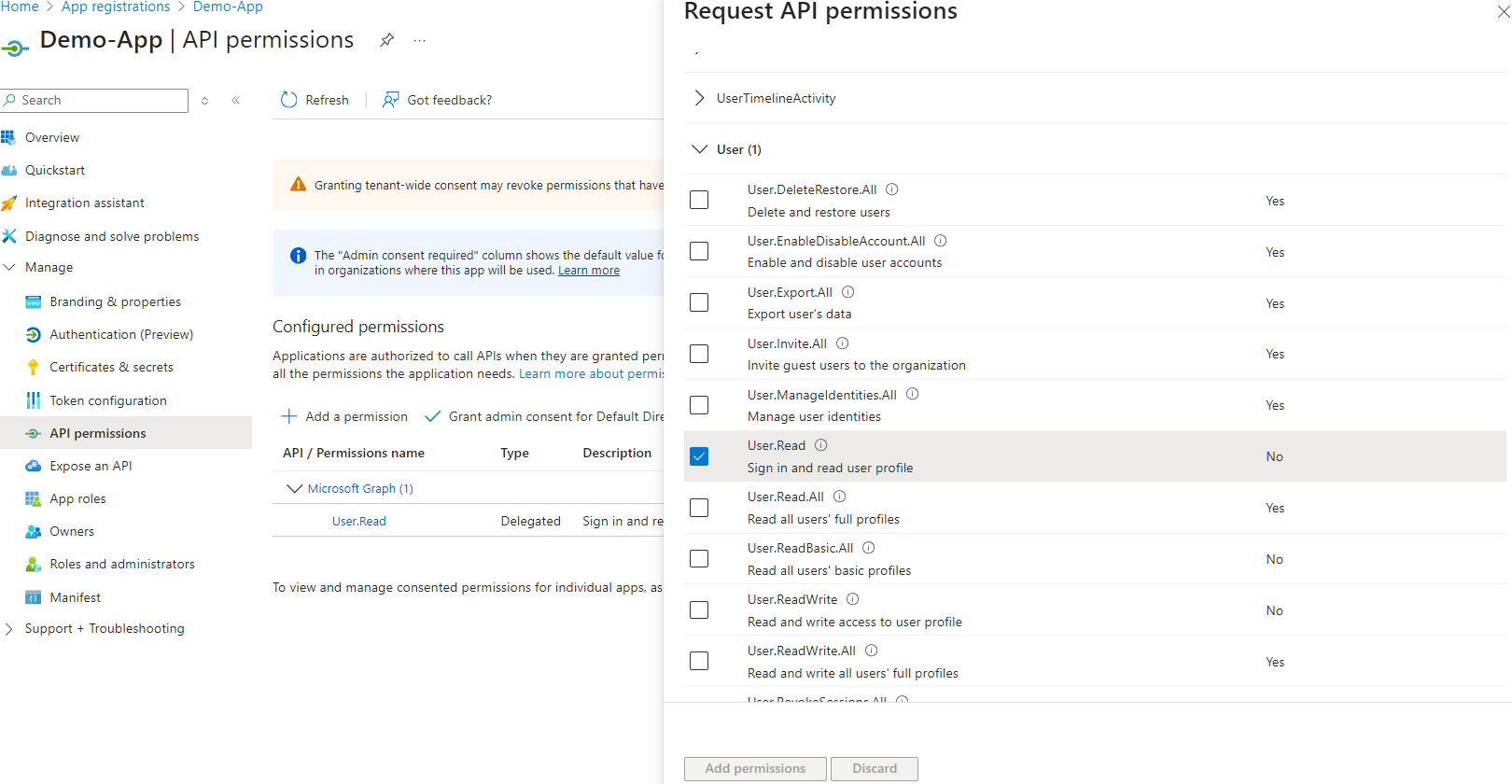
# Introduction

This case study demonstrates how to integrate an application with Microsoft Entra ID using the free-tier (Azure for Students) tenant. The project goal was to register an application, configure delegated permissions, and authenticate against Microsoft Graph using the Device Code Flow.  
  
The exercise highlights the fundamentals of app integration with Entra ID and Graph API, while also documenting the limitations of the free/student licensing model where directory-wide API queries are blocked.

# Implementation

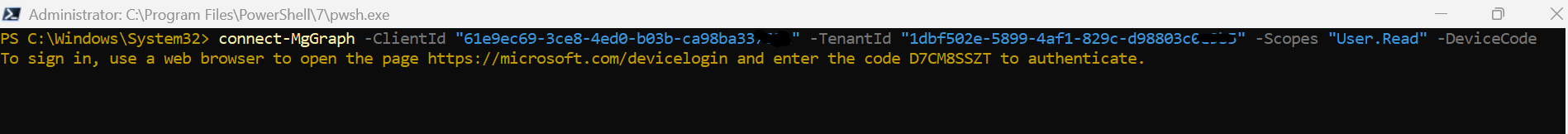
## A. Application Registration

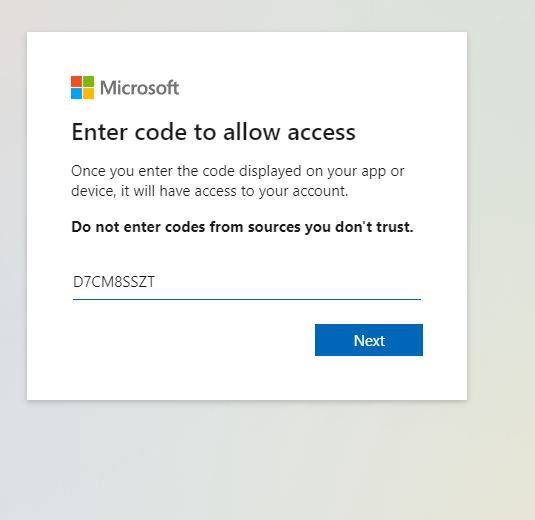
A new application, Demo-App, was registered in Entra ID. It was configured as a single-tenant app. The Application (client) ID and Directory (tenant) ID were captured for authentication.  
  
The User.Read delegated permission was added to allow the app to sign in and read the profile of the authenticated user.

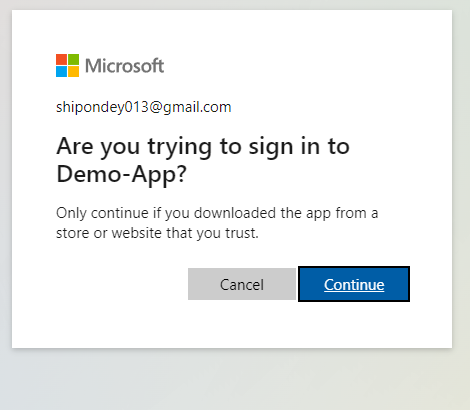


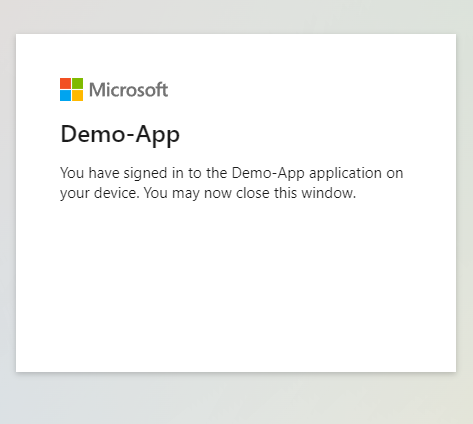
## B. Authentication with Device Code Flow

PowerShell was used to connect to Microsoft Graph via the Device Code Flow. The process generated a device login code, which was entered at https://microsoft.com/devicelogin. The user was then prompted to confirm access to the Demo-App.



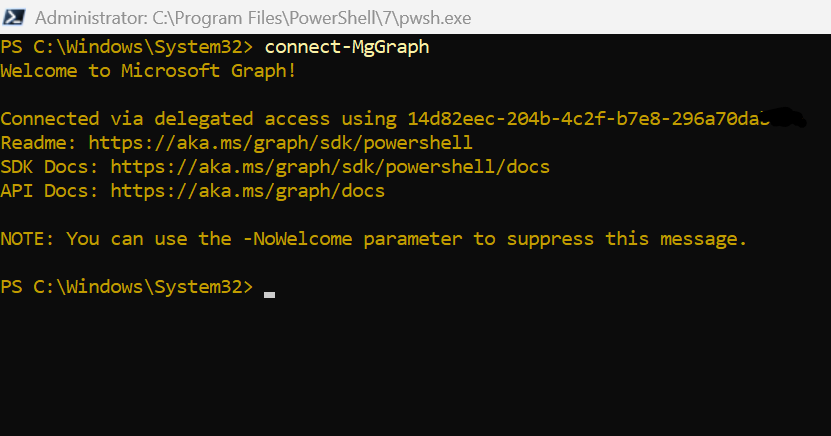


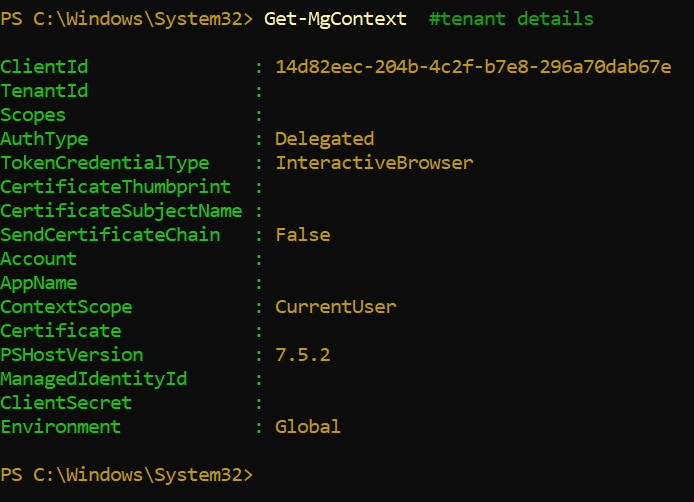




## C. Graph SDK Connection Context

After successful login, Microsoft Graph SDK confirmed the delegated connection. Although user profile queries returned 403 Forbidden due to tenant restrictions, the connection context showed authenticated account, tenant, and client information.





# Limitations

- In free/student tenants, Microsoft Graph API calls (Get-MgUser, Get-MgUser -UserId me) return 403 Forbidden.  
- Higher-level delegated or application permissions such as Directory.Read.All cannot be granted.  
- The project is limited to authenticating the session and showing Graph context, without directory-wide data retrieval.

# Conclusion

This project successfully demonstrated how to register an app, assign delegated permissions, and authenticate against Microsoft Graph using the Device Code Flow. While limited by licensing constraints, the implementation illustrates core identity integration concepts that scale to enterprise environments with Azure AD Premium.  
  
In a licensed environment, this workflow could be extended to retrieve user profiles, manage groups, and enable conditional access policies.