Identity & Access Management in Microsoft Entra ID (Free Tier)

Mini Company Directory Project

by Boyon Dey Shipon

Date: August 2025

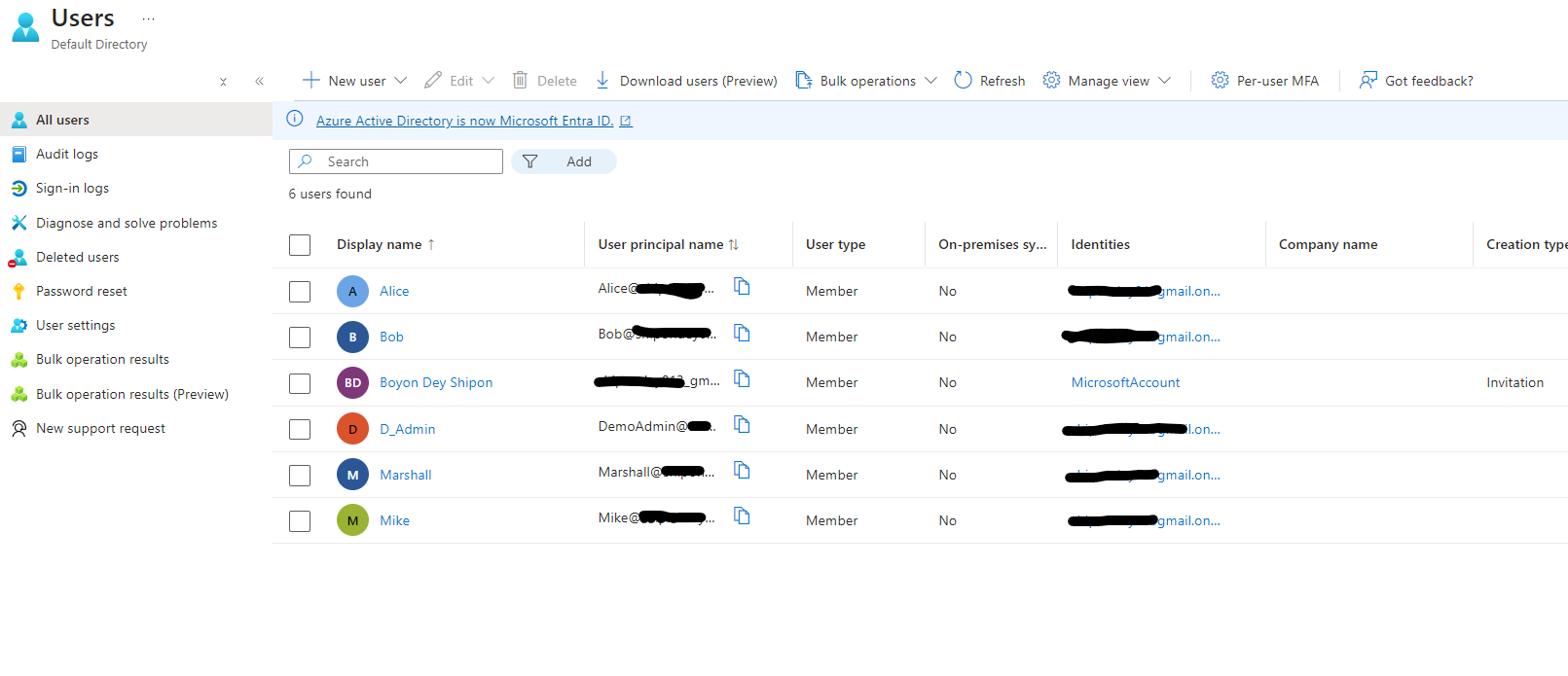
# Introduction

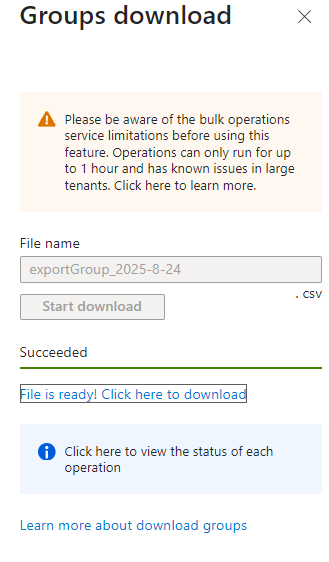
Identity and Access Management (IAM) is a critical part of cloud security, ensuring that the right people have the right access to the right resources at the right time. In cloud environments, where services and users scale quickly, proper IAM practices prevent unauthorized access, reduce security risks, and support compliance.  
  
In this project, a small company directory was simulated using Microsoft Entra ID Free (Azure for Students). The implementation covered the essentials of IAM, including:  
- Creating and managing users  
- Organizing users into groups  
- Assigning roles using RBAC (Role-Based Access Control)  
- Exporting directory information (users and groups) via the portal  
- Simulating admin tasks such as password resets and group membership changes  
- Registering an application in Entra ID and assigning permissions  
  
This demonstrates IAM fundamentals and shows how a free-tier tenant can still be used to build a professional portfolio project that mirrors enterprise scenarios.

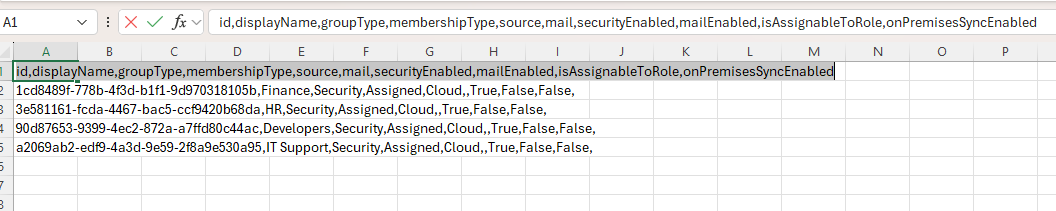
# Implementation

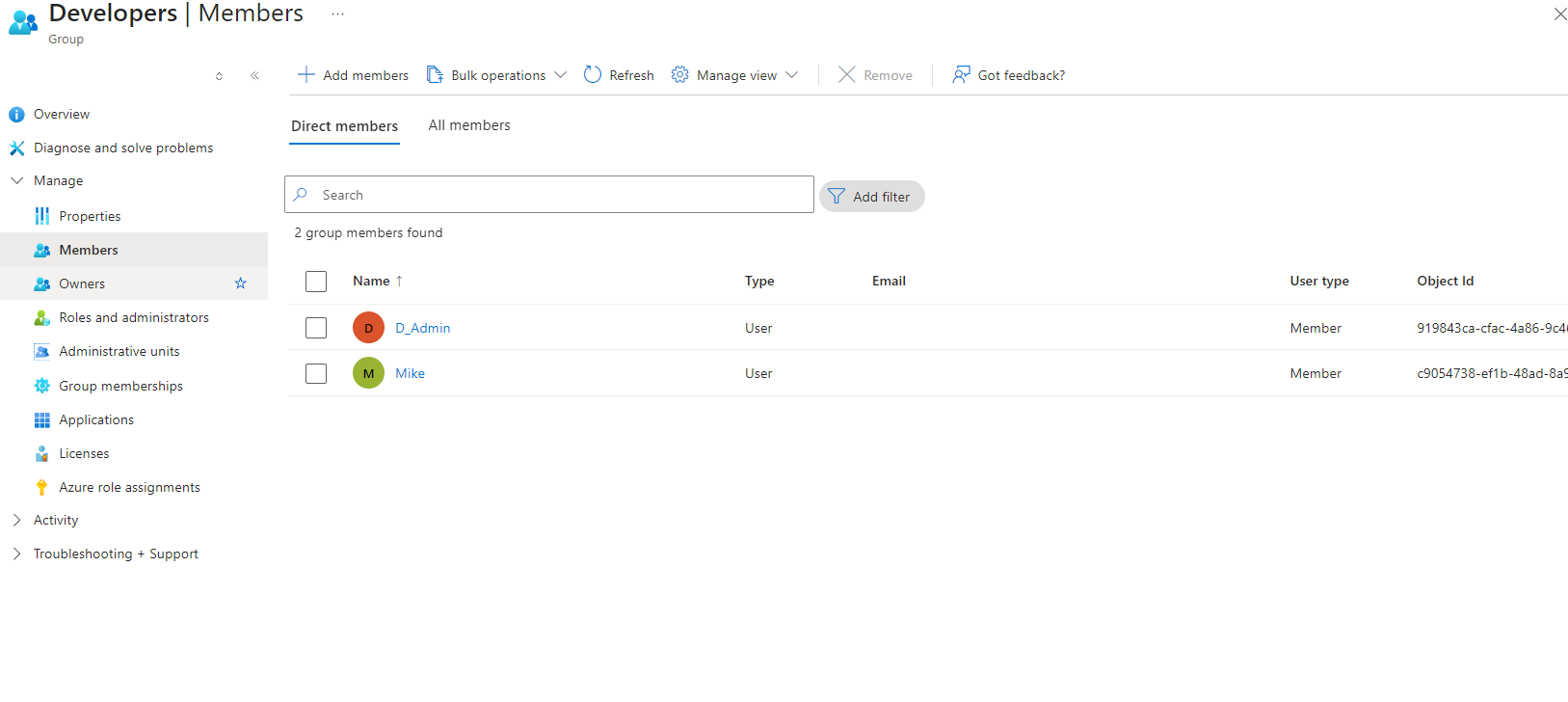
## A. User & Group Management

Users created: Alice (HR), Bob (IT), Mike (Finance), Marshall (Developers), D\_Admin (Admin).  
Groups created: HR, IT Support, Finance, Developers.  
Users were added to their respective groups as shown below.



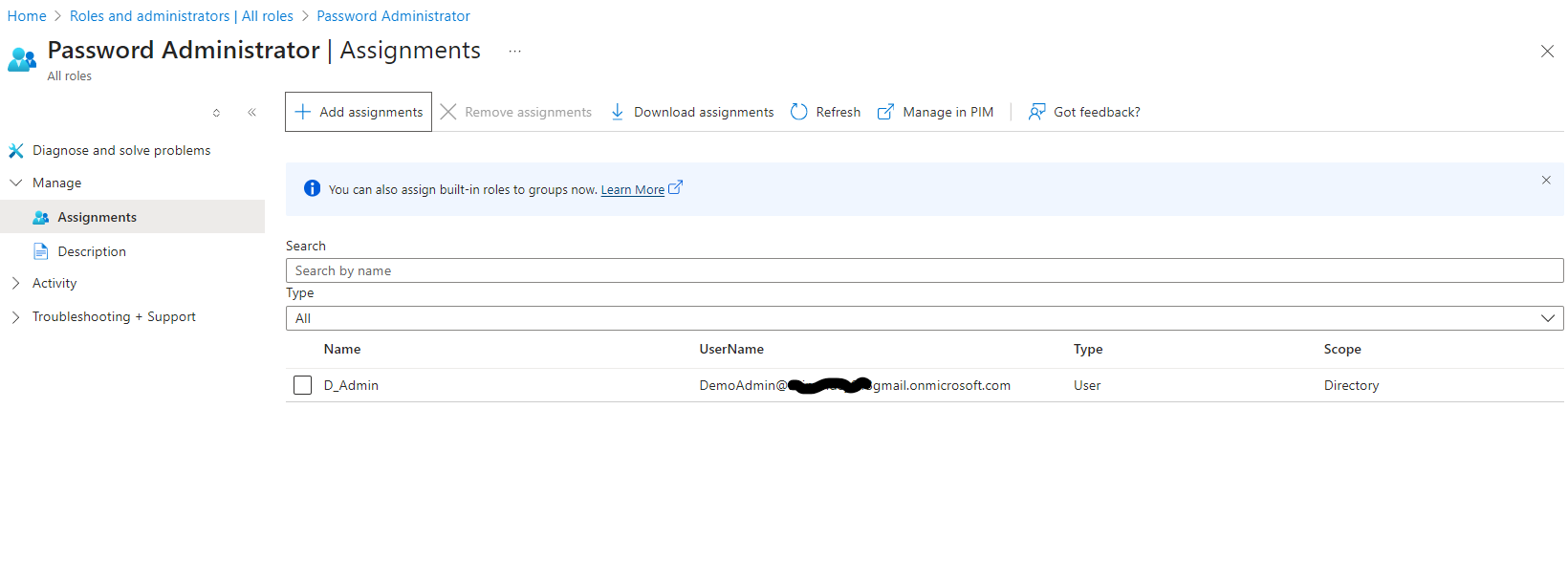






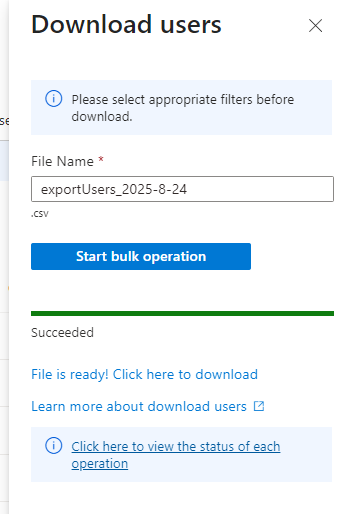
## B. Role Assignment

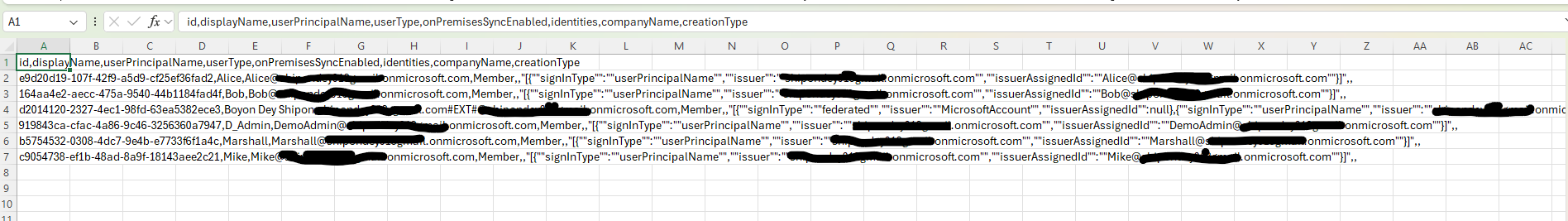
To enforce least privilege, the D\_Admin account was assigned the 'Password Administrator' role. This allows limited administrative capabilities, such as resetting user passwords, without granting full control.



## C. Directory Export

Since Microsoft Graph directory API access is restricted in free-tier tenants, directory exports were performed via the Entra ID portal. Both user and group information were downloaded in CSV format for documentation.





# Limitations

- Microsoft Graph API calls like Get-MgUser and Get-MgGroup return 403 Forbidden in free-tier tenants.  
- Conditional Access, Self-Service Password Reset (per user/group), and Identity Protection are Premium features and unavailable in Azure for Students.  
- As a workaround, directory exports were completed through the portal and documented.

# Conclusion

This project demonstrated IAM fundamentals in Microsoft Entra ID Free. The tasks included creating users, organizing groups, assigning RBAC roles, exporting directories, and simulating admin tasks. While limited compared to enterprise P1/P2 licenses, this exercise successfully mirrors real-world identity management practices and is suitable for a portfolio showcase.