Azure Portfolio Projects

Each project in this 5-project portfolio is designed to demonstrate my hands-on experience with Azure and cloud technologies. The projects cover core aspects such as compute and identity management, networking and storage, monitoring, backup and recovery, identity integration, and app service deployment.

**Project 4**Entra ID Integration and Identity Management

# 📝 Project Summary

Topics Covered: Entra ID, User and Group Management, App Registration, Conditional Access, MFA

This project demonstrates integrating applications with Entra ID, managing users and groups, setting up conditional access policies, enabling MFA, and monitoring authentication activity.

# 📘 Scenario

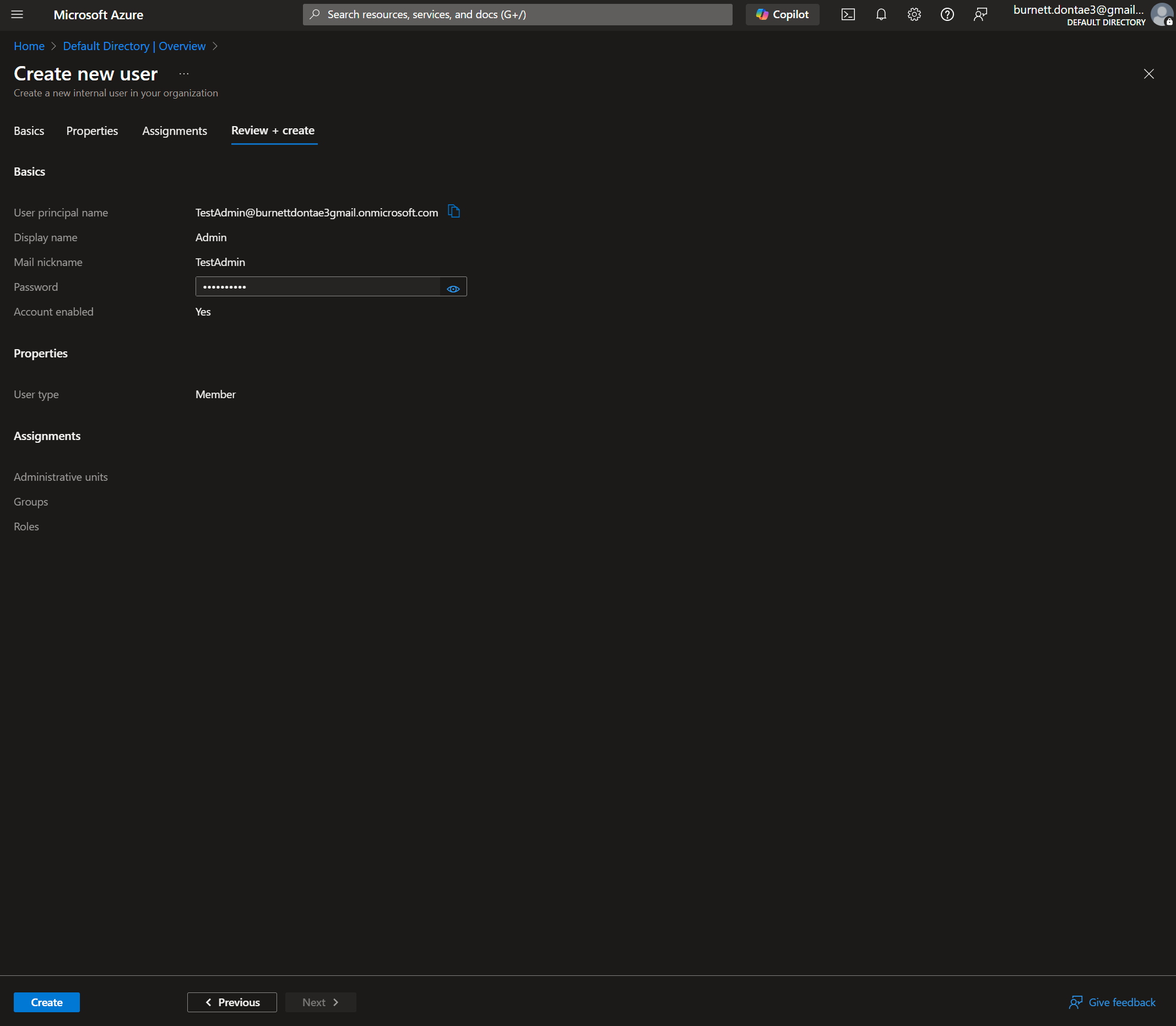
A company wants to integrate their web application with Entra ID for authentication, manage user and group permissions, enforce conditional access policies, and enable multi-factor authentication (MFA) for added security.

# 🚀 Project Tasks

## Task 1: Create Users and Groups in Entra ID

* Go to Entra ID > Users > Create User
* Create multiple users with roles such as Admin, Developer, and Reader
* Go to Groups > Create Group > Add users to respective groups

Admin Account



Developer Account

A screenshot of a computer

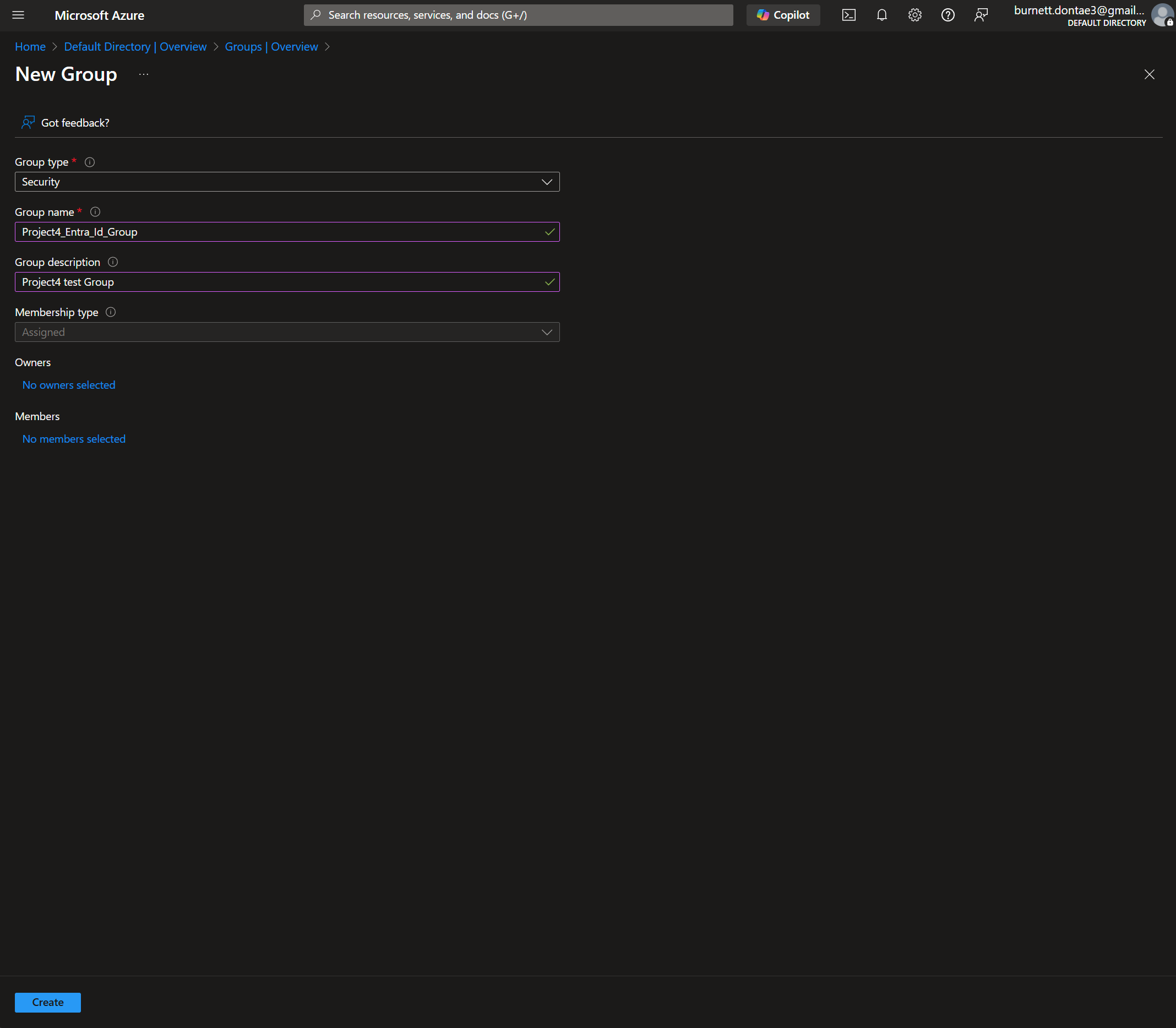
AI-generated content may be incorrect.

Directory Reader

A screenshot of a computer

AI-generated content may be incorrect.

Creation of the Group For the Project Entra ID



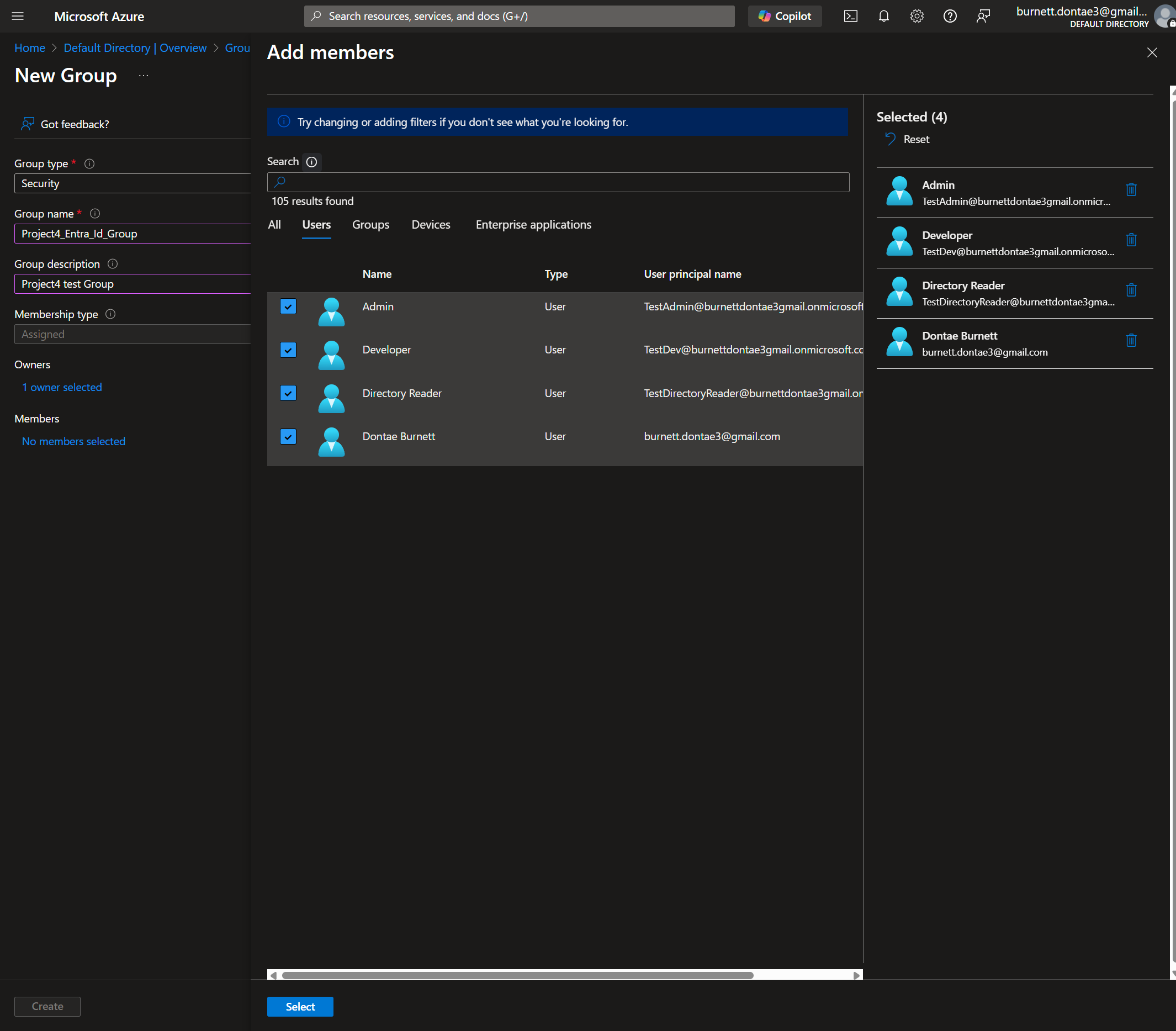
Making myself the owner of the Group

A screenshot of a computer

AI-generated content may be incorrect.

Adding the members By sorting by users for this demonstration

Adding myself as a member in addition to being the owner so I can have access to the group’s resources instead of only having the ability to manage the group properties, setting and user access



A screenshot of a computer

AI-generated content may be incorrect.

## Task 2: Register an Application in Entra ID

* Go to App Registrations > New Registration
* Provide name, account types, and redirect URI (web)
* Under API Permissions, add Microsoft Graph > User.Read
* Go to Certificates & Secrets > Create a client secret

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

## Task 3: Assign Users and Groups to the Application

* Go to Enterprise Applications > Select the app
* Navigate to Users and Groups > Add User/Group
* Assign the previously created groups to the app

A screenshot of a computer

AI-generated content may be incorrect.

Due to my free trial, I could not select a group, I can only select users

A screenshot of a computer

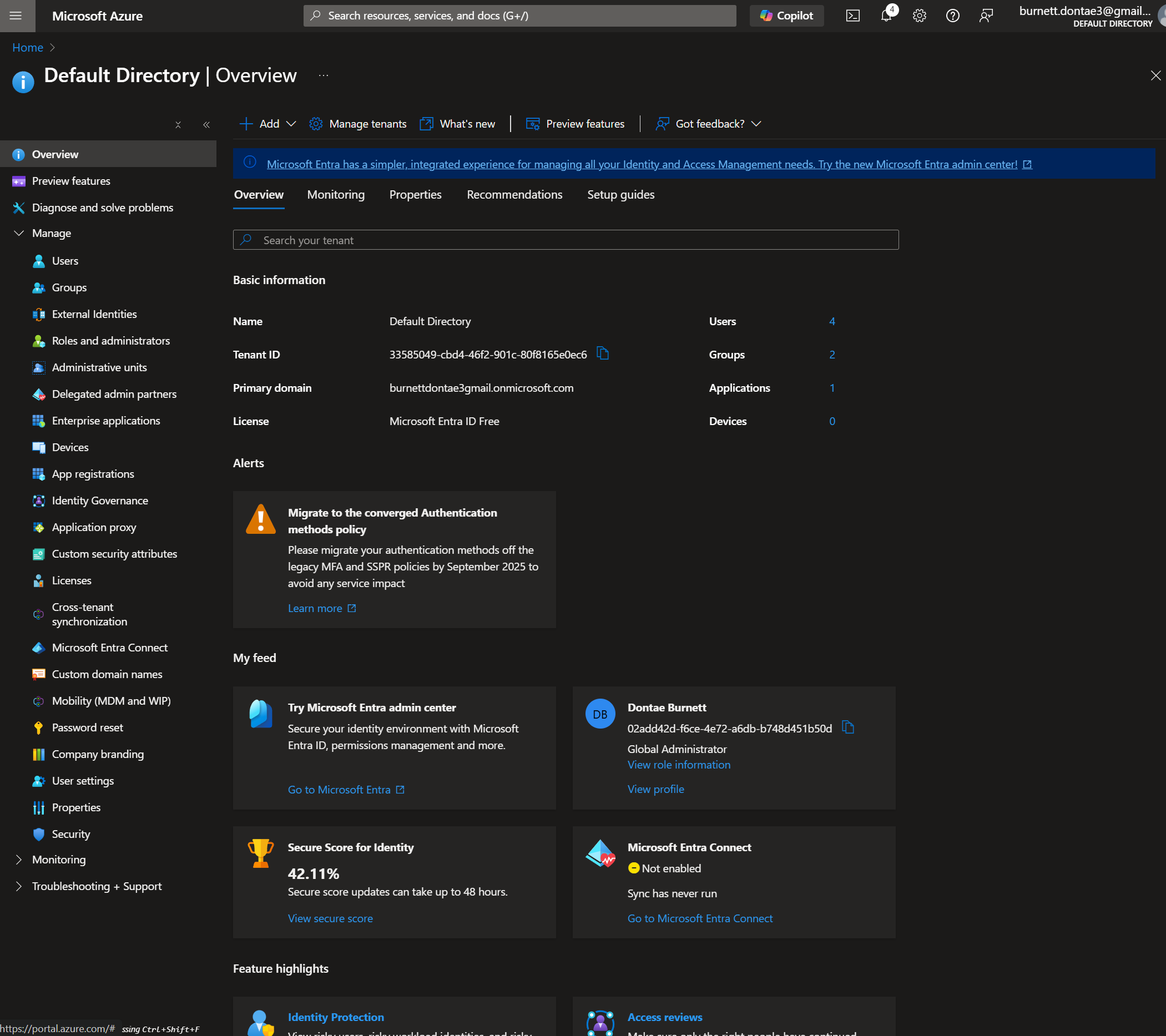
AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

## Task 4: Configure Conditional Access

* Go to Entra ID > Security > Conditional Access
* Create a new policy to require MFA
* Configure conditions (e.g., location, device compliance)
* Enable the policy and test user access



Since I’m not using an Entra ID premium I can’t show the last step but from here I could set a policy to require MFA and set Location based Access

A screenshot of a computer

AI-generated content may be incorrect.

## Task 5: Enable Multi-Factor Authentication (MFA)

* Go to Entra ID > Users > Multi-Factor Authentication
* Enable MFA for selected users

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

## Task 6: Monitor Sign-In Activity

* Go to Entra ID > Sign-ins
* Review logs for successful and failed authentication attempts

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.