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

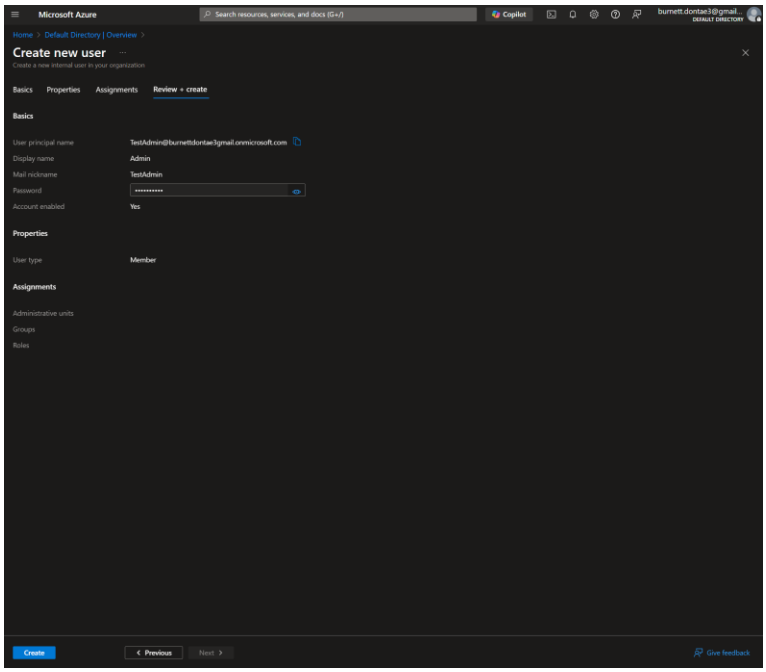
A company wants to integrate their web application with Entra ID for authentication, manage user and group permissions, enforce conditional access policies, and enable multi-factor authentication (MFA) for added security.

Project Tasks

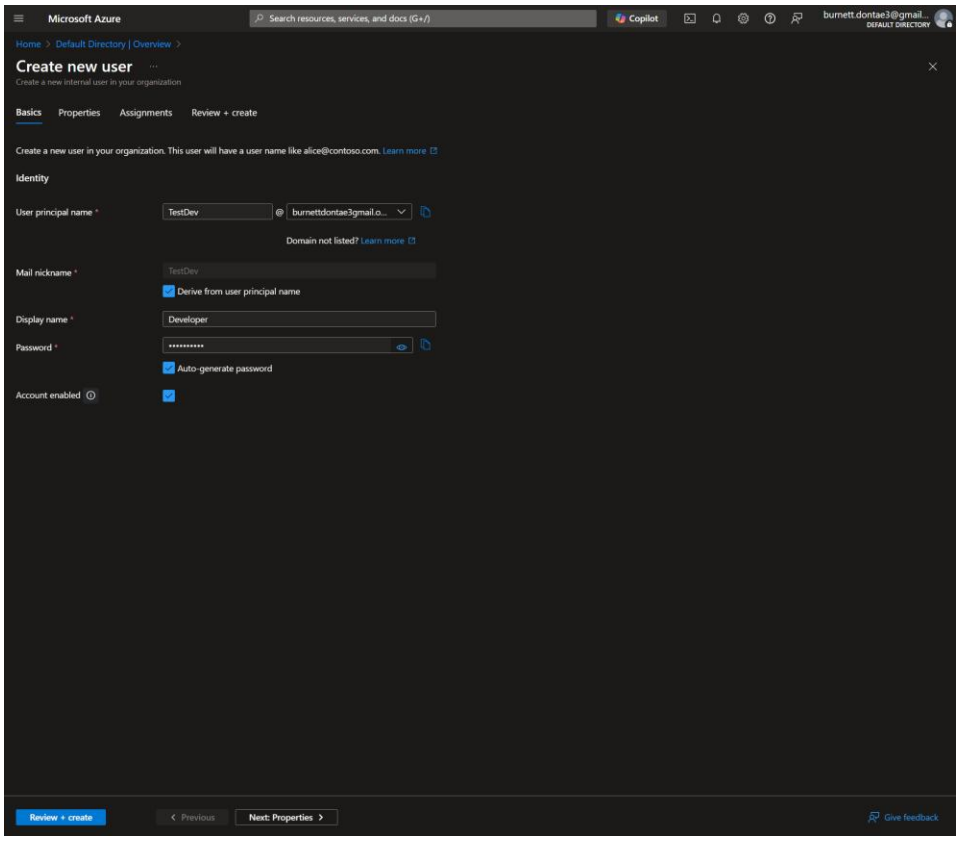
Task 1: Create Users and Groups in Entra ID

- 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

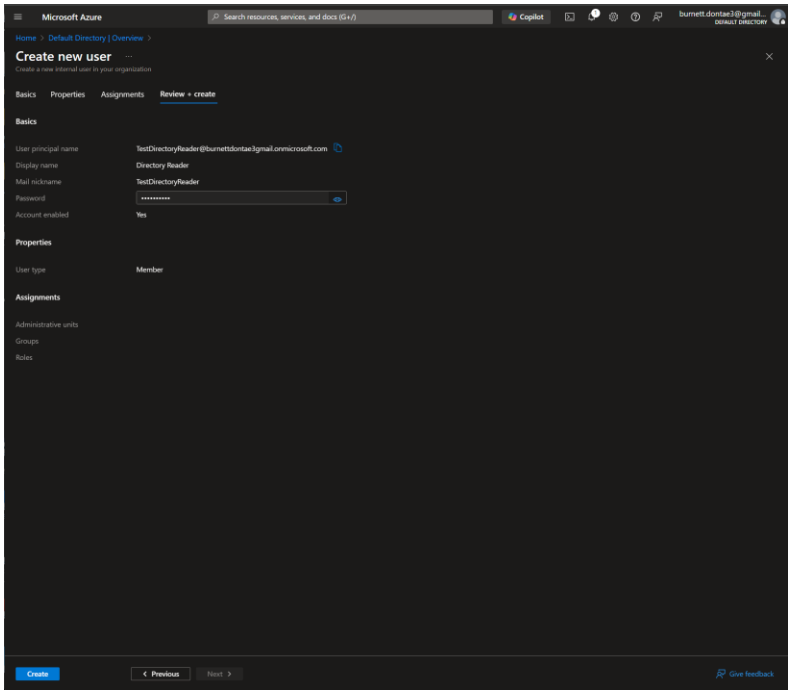
Admin Account



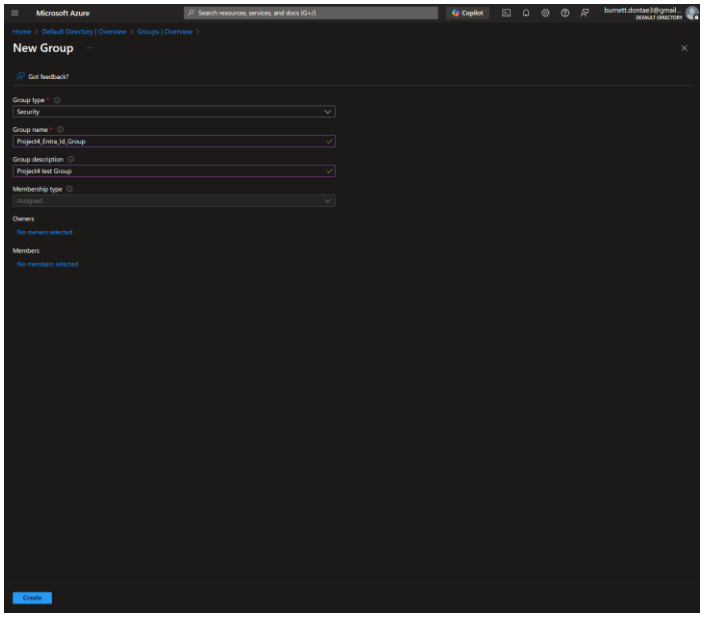
Developer Account



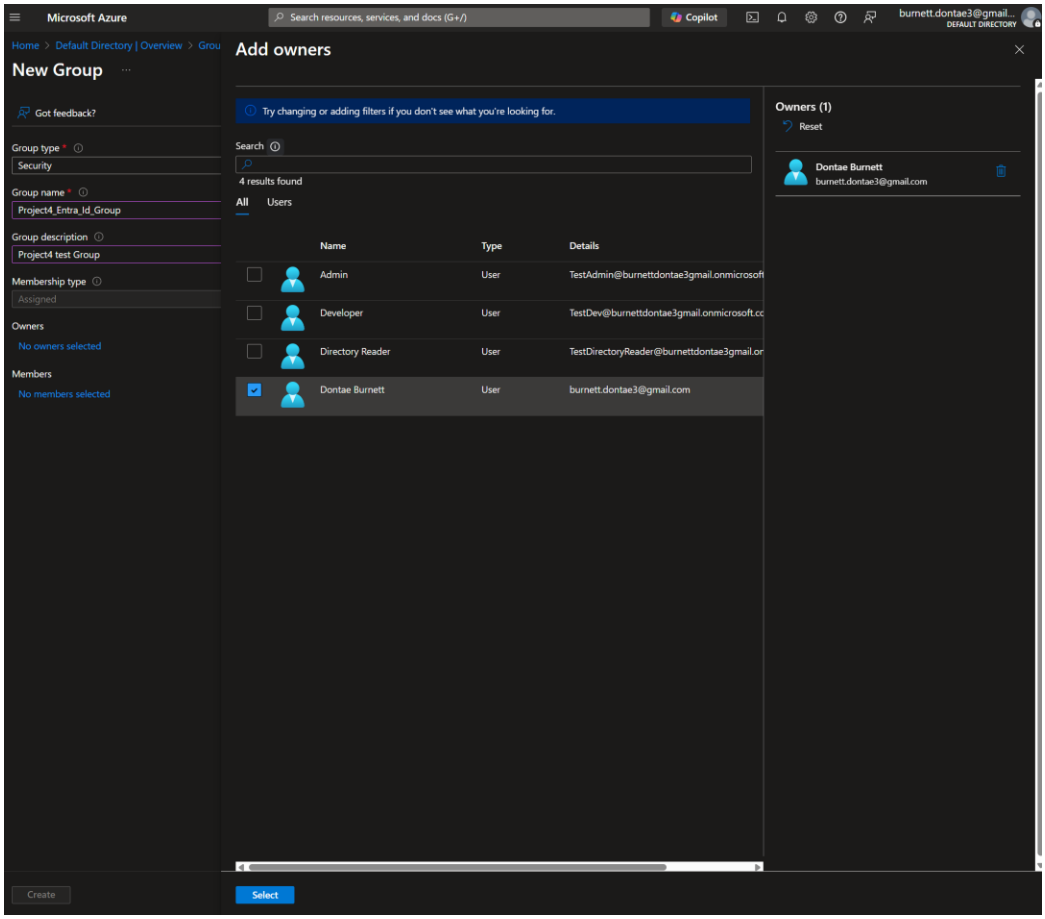
Directory Reader



Creation of the Group For the Project Entra ID

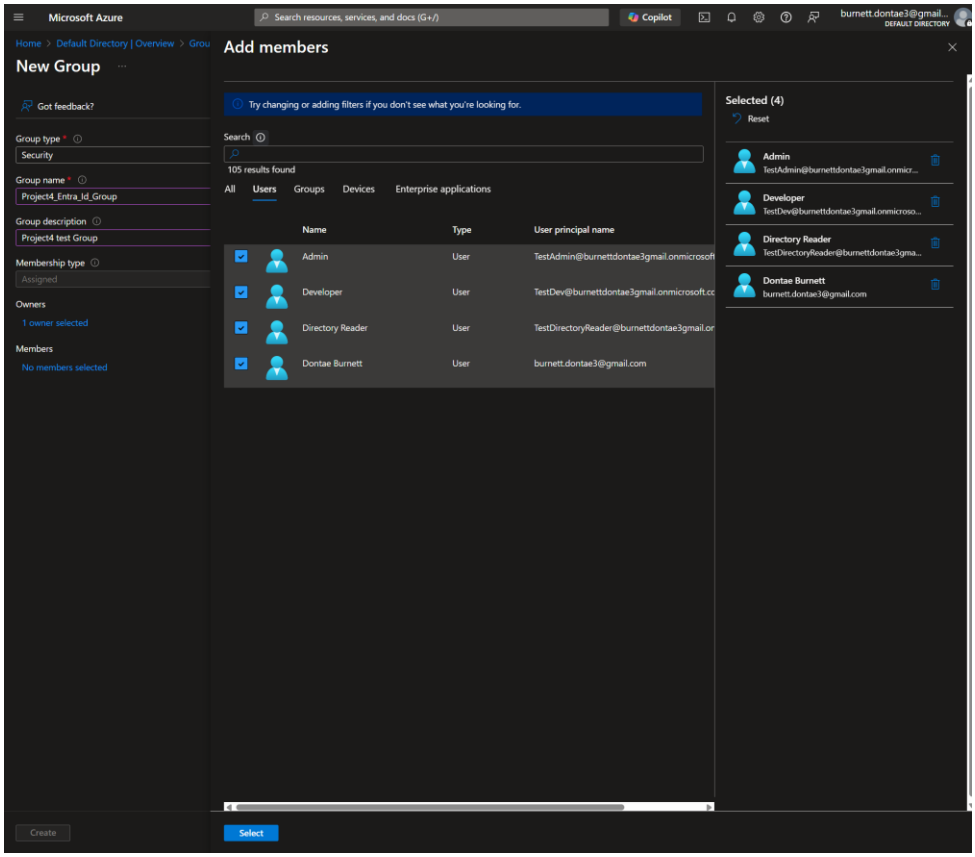


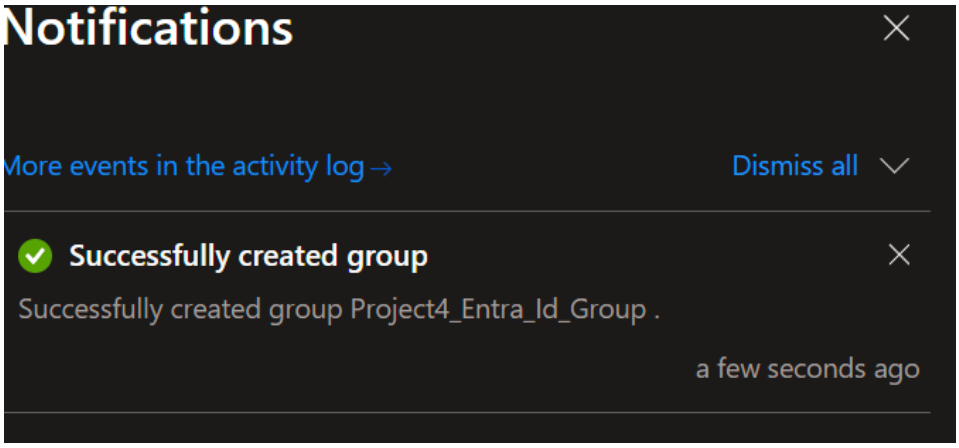
Making myself the owner of the Group



Adding the members By sorting by users for this demonstration

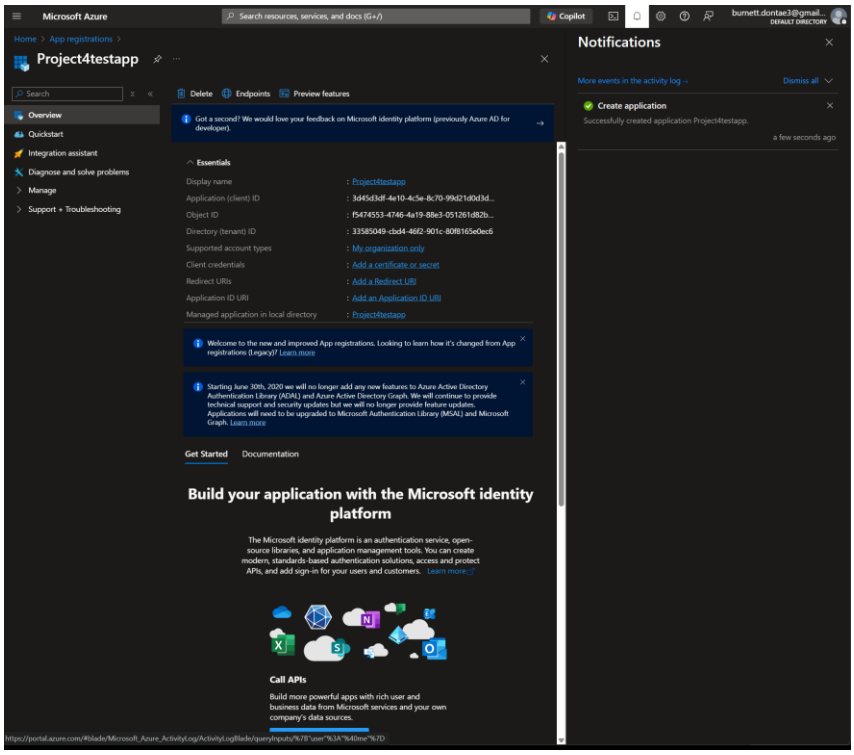
Adding myself as a member in addition to being the owner so I can have access to the group's resources instead of only having the ability to manage the group properties, setting and user access

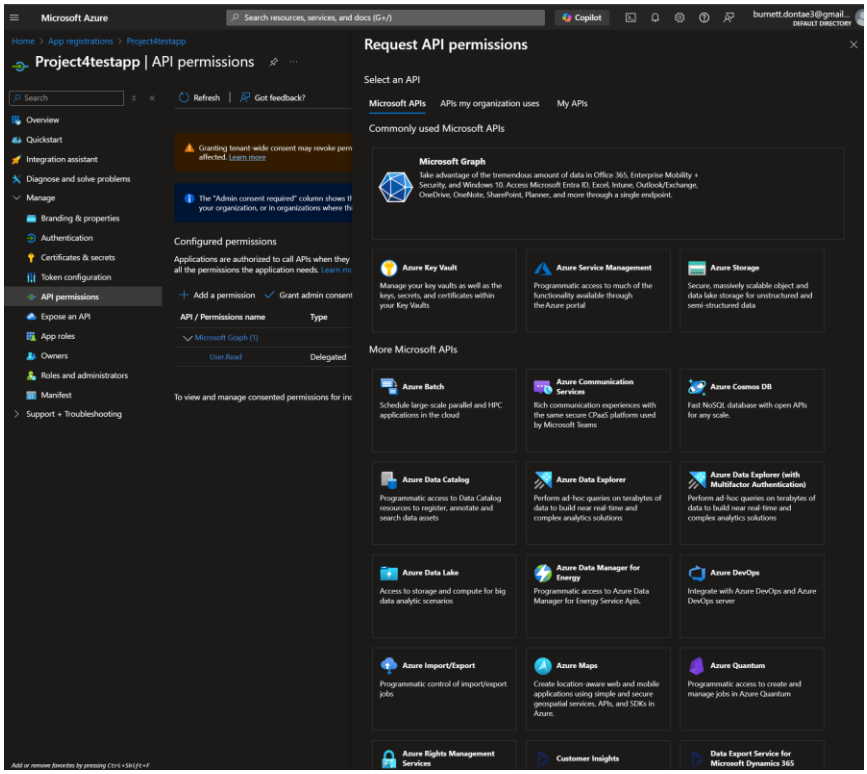


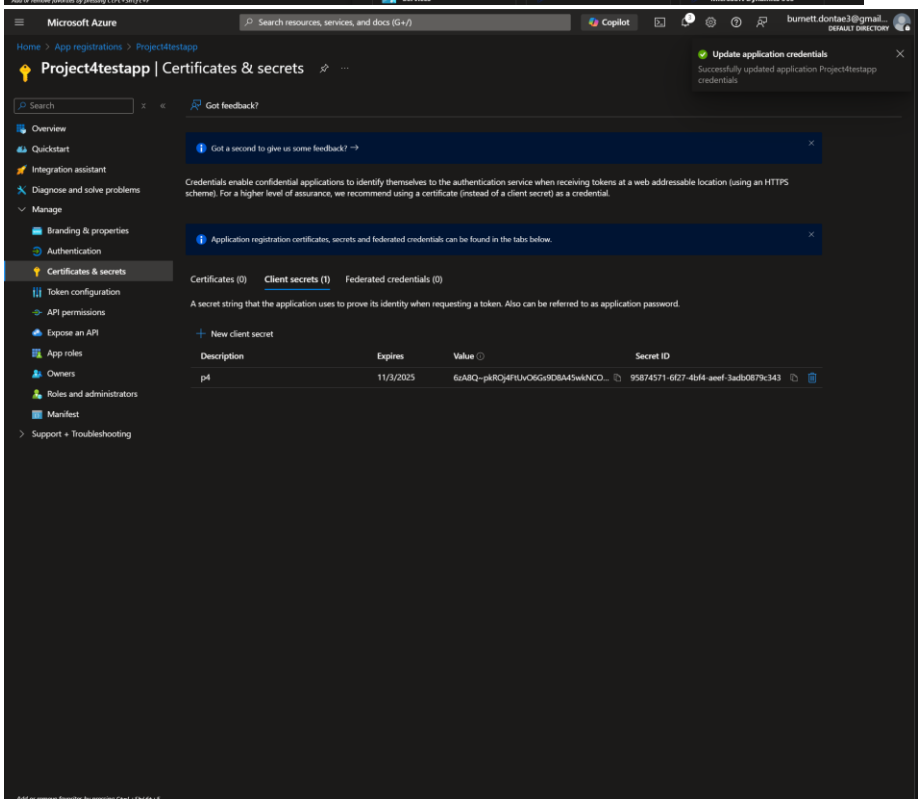


Task 2: Register an Application in Entra ID

- 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

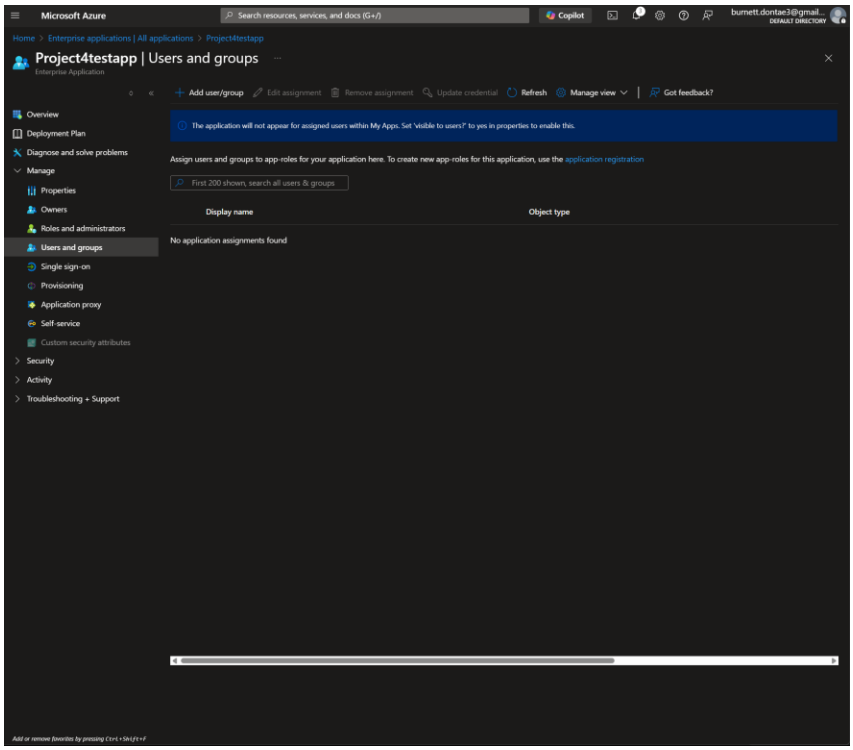



Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
burnett.dontae3@gmail...
DEFAULT DIRECTORY
Home > App registrations > Project4testapp
Project4testapp | API permissions
Search
Refresh
Got feedback?
Overview
Quickstart
Integration assistant
Diagnose and solve problems
Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest
Support + Troubleshooting
Granting tenant-wide consent may revoke perm
affected. Learn more
The "Admin consent required" column shows th
your organization, or in organizations where th
Configured permissions
Applications are authorized to call APIs when they
all the permissions the application needs. Learn mo
Add a permission
Grant admin consent
API / Permissions name
Type
Microsoft Graph (1)
User.Read
Delegated
To view and manage consented permissions for inc
Request API permissions
Select an API
Microsoft APIs
APIs my organization uses
My APIs
Commonly used Microsoft APIs
Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Microsoft Entra ID, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.
Azure Key Vault
Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults
Azure Service Management
Programmatic access to much of the functionality available through the Azure portal
Azure Storage
Secure, massively scalable object and data lake storage for unstructured and semi-structured data
More Microsoft APIs
Azure Batch
Schedule large-scale parallel and HPC applications in the cloud
Azure Communication Services
Rich communication experiences with the same secure CPaaS platform used by Microsoft Teams
Azure Cosmos DB
Fast NoSQL database with open APIs for any scale.
Azure Data Catalog
Programmatic access to Data Catalog resources to register, annotate and search data assets
Azure Data Explorer
Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions
Azure Data Explorer (with Multifactor Authentication)
Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions
Azure Data Lake
Access to storage and compute for big data analytic scenarios
Azure Data Manager for Energy
Programmatic access to Azure Data Manager for Energy Service Apis.
Azure DevOps
Integrate with Azure DevOps and Azure DevOps server
Azure Import/Export
Programmatic control of import/export jobs
Azure Maps
Create location-aware web and mobile applications using simple and secure geospatial services, APIs, and SDKs in Azure.
Azure Quantum
Programmatic access to create and manage jobs in Azure Quantum
Azure Rights Management Services
Customer Insights
Data Export Service for Microsoft Dynamics 365

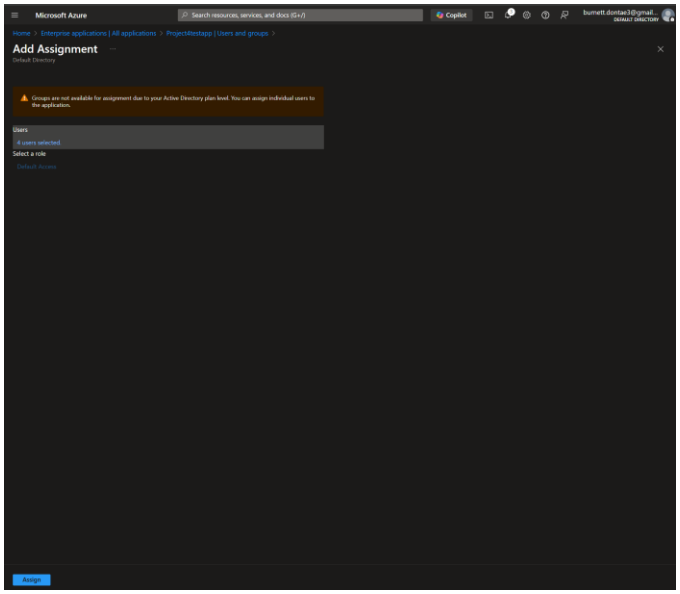

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
burnett.dontae3@gmail...
DEFAULT DIRECTORY
Home > App registrations > Project4testapp
Project4testapp | Certificates & secrets
Update application credentials
Successfully updated application Project4testapp credentials
Search
Got feedback?
Overview
Quickstart
Integration assistant
Diagnose and solve problems
Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest
Support + Troubleshooting
Got a second to give us some feedback? →
Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.
Application registration certificates, secrets and federated credentials can be found in the tabs below.
Certificates (0)
Client secrets (1)
Federated credentials (0)
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.
New client secret
Description
Expires
Value
Secret ID
p4
11/3/2025
6zA8Q~pkROj4FtUvO6Gs9D8A45wkNCO...
95874571-6f27-4bf4-aeef-3adb0879c343

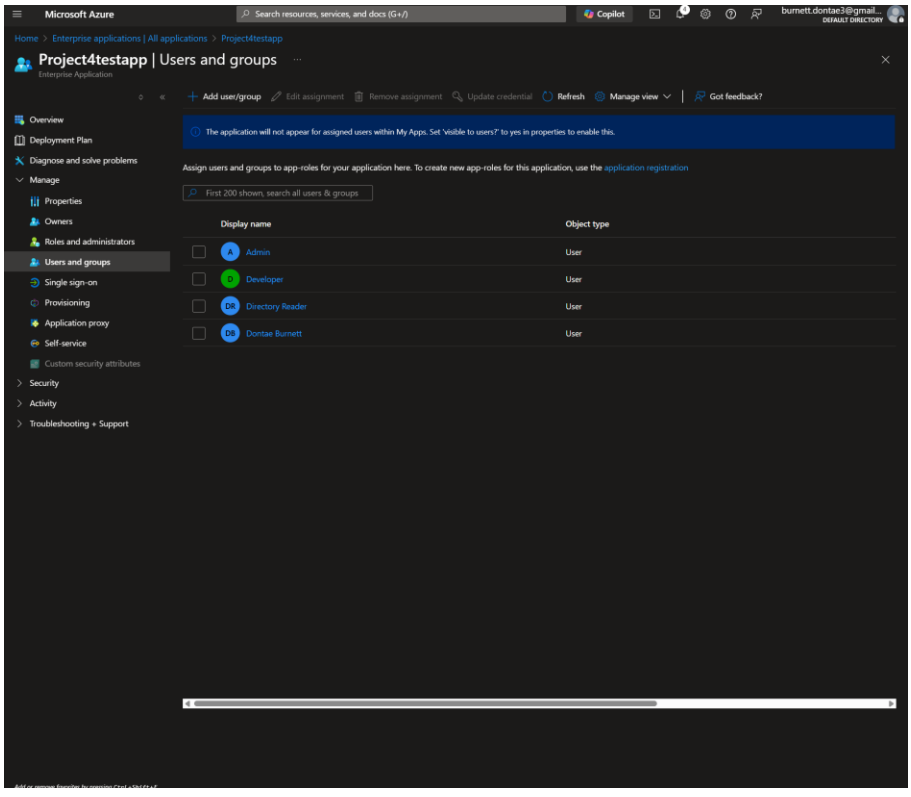
Task 3: Assign Users and Groups to the Application

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



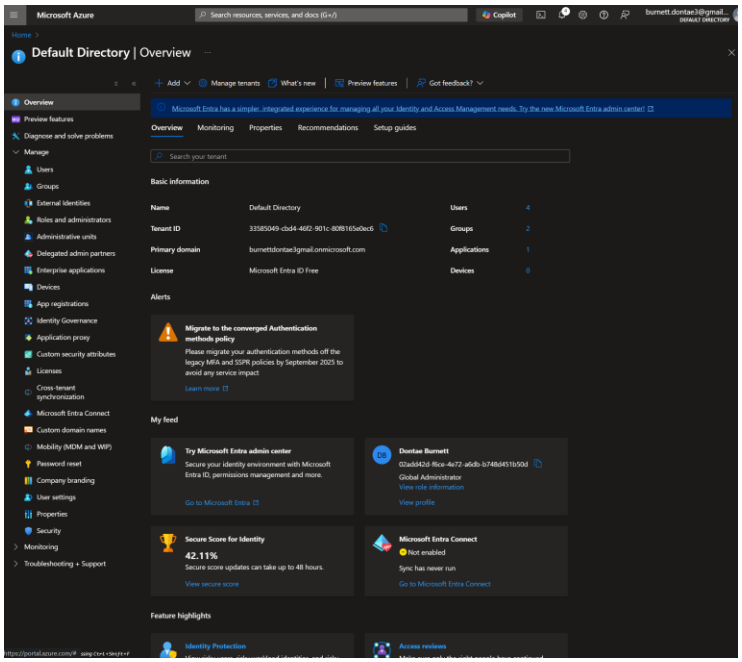
Due to my free trial, I could not select a group, I can only select users


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
burnett.dontae3@gmail...
DEFAULT DIRECTORY
Home > Enterprise applications | All applications > Project4testapp | Users and groups >
Add Assignment
Default Directory
Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application.
Users
4 users selected.
Select a role
Default Access
Assign

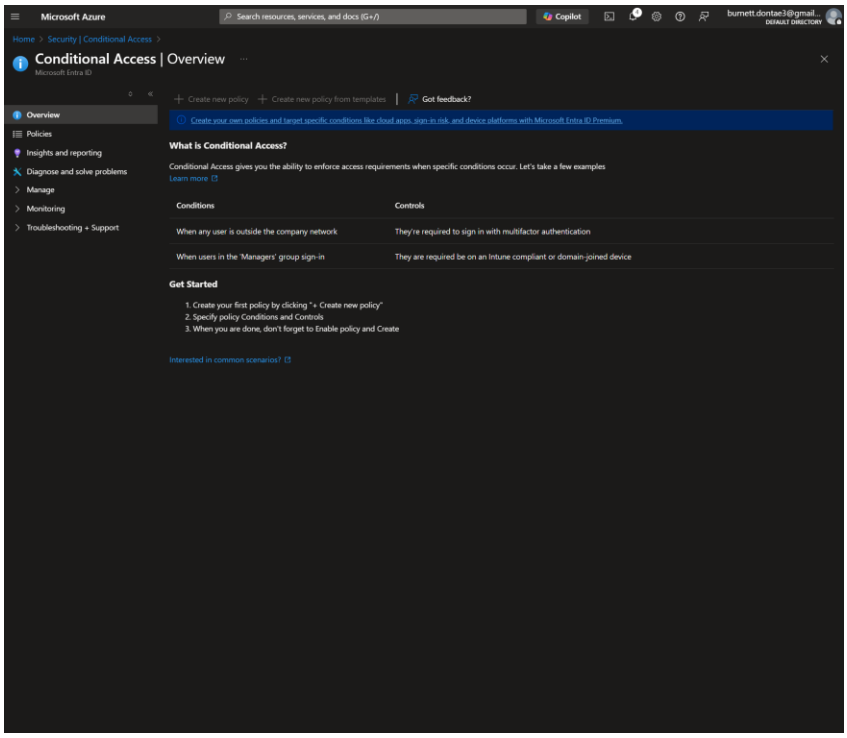

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
burnett.dontae3@gmail...
DEFAULT DIRECTORY
Home > Enterprise applications | All applications > Project4testapp
Project4testapp | Users and groups
Enterprise Application
Add user/group
Edit assignment
Remove assignment
Update credential
Refresh
Manage view
Got feedback?
Overview
Deployment Plan
Diagnose and solve problems
Manage
Properties
Owners
Roles and administrators
Users and groups
Single sign-on
Provisioning
Application proxy
Self-service
Custom security attributes
Security
Activity
Troubleshooting + Support
The application will not appear for assigned users within My Apps. Set 'visible to users?' to yes in properties to enable this.
Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the application registration
First 200 shown, search all users & groups
Display name
Object type
Admin
User
Developer
User
Directory Reader
User
Dontae Burnett
User

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

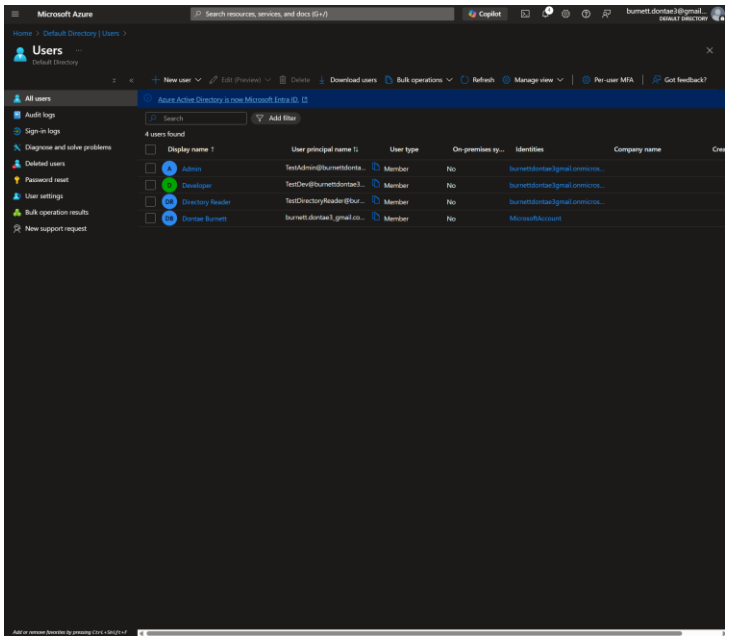


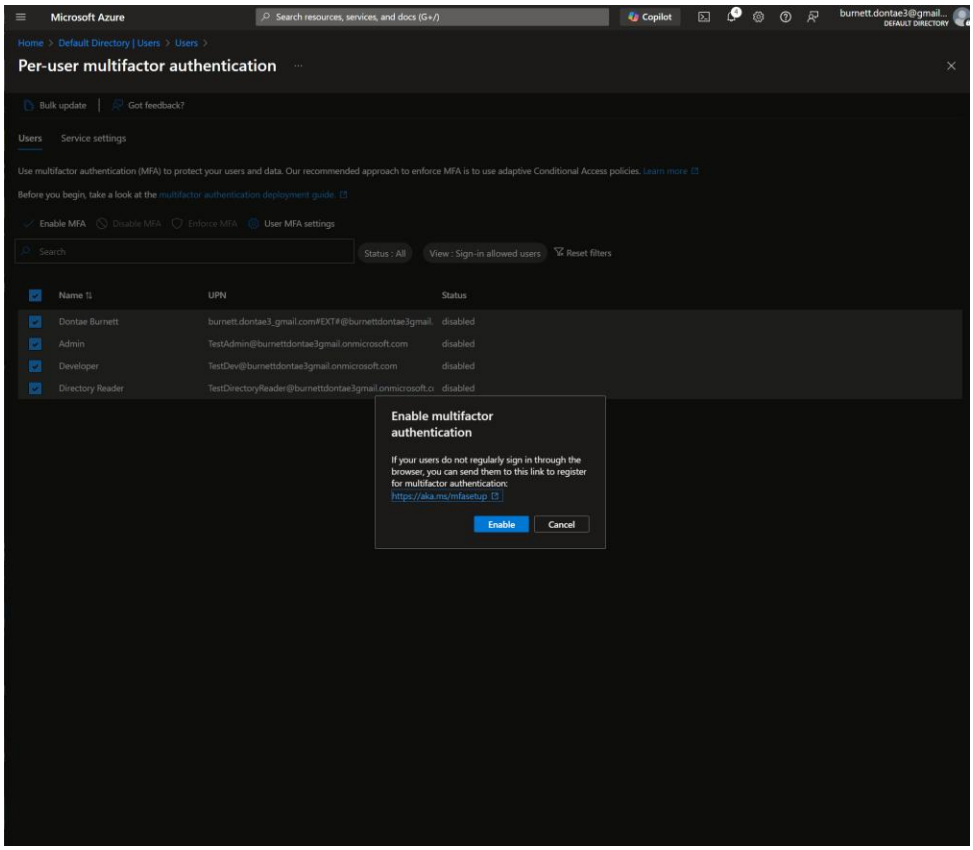
Since I'm not using an Entra ID premium I can't show the last step but from here I could set a policy to require MFA and set Location based Access

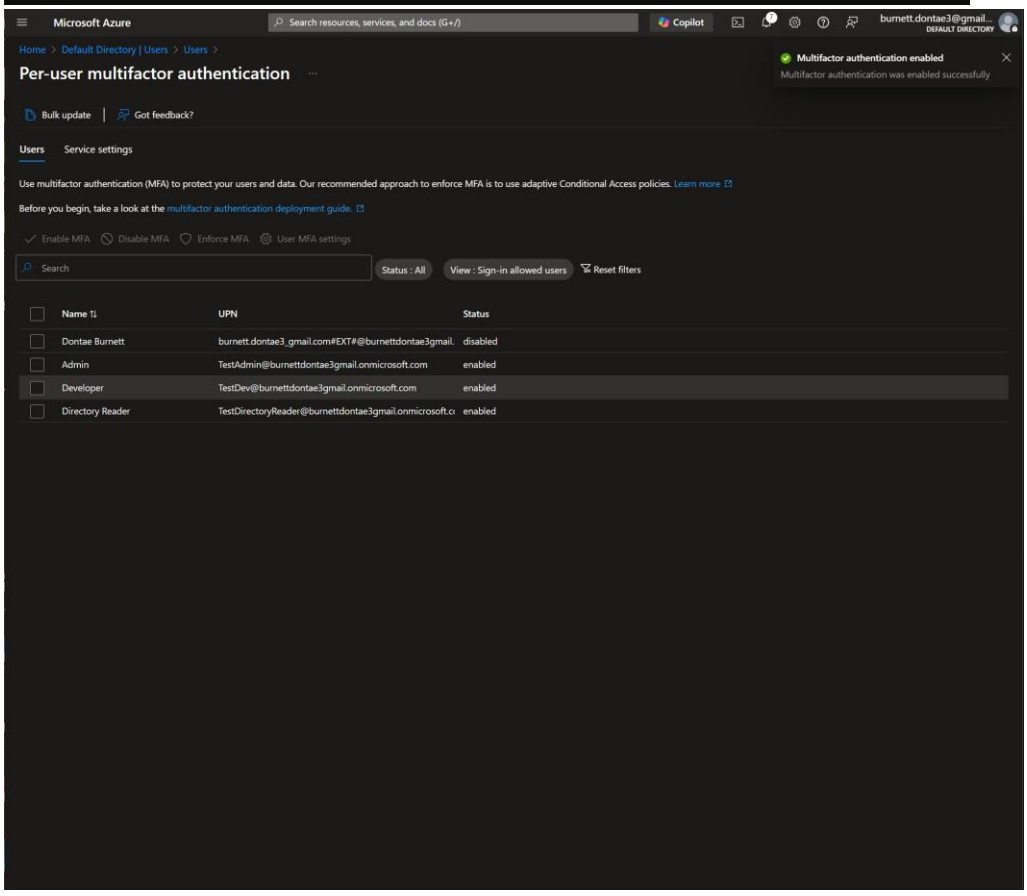


Task 5: Enable Multi-Factor Authentication (MFA)

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

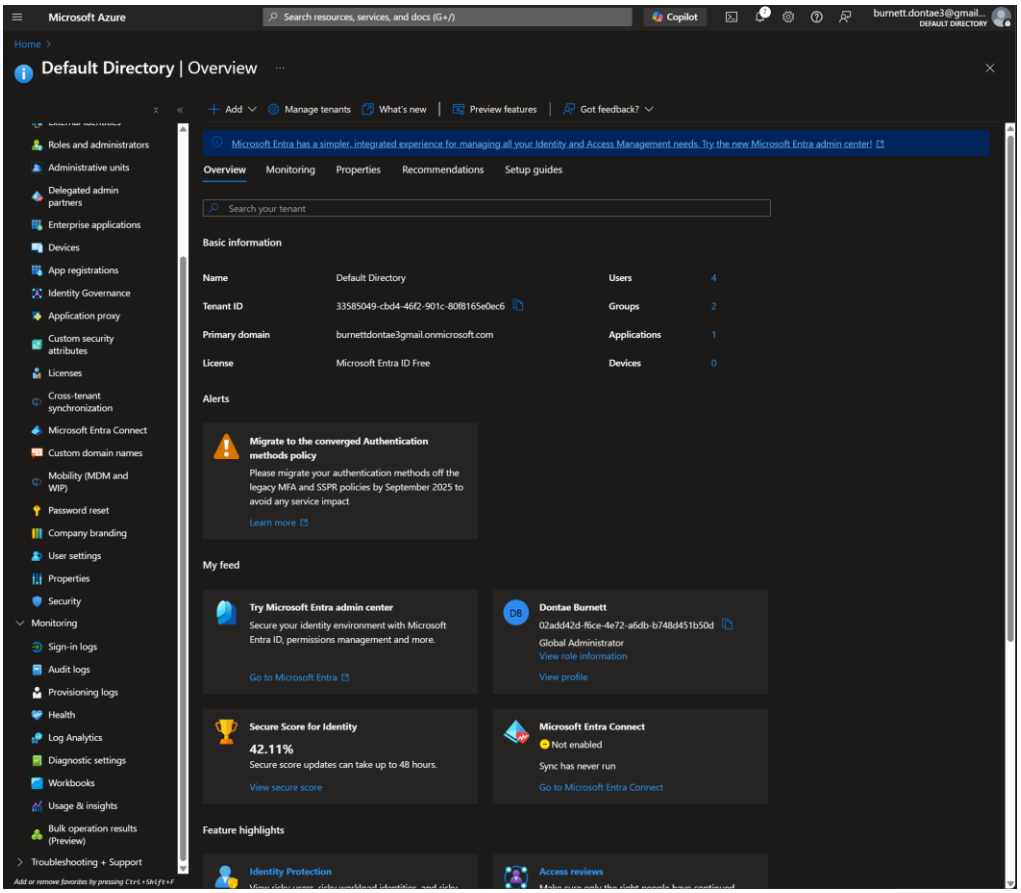


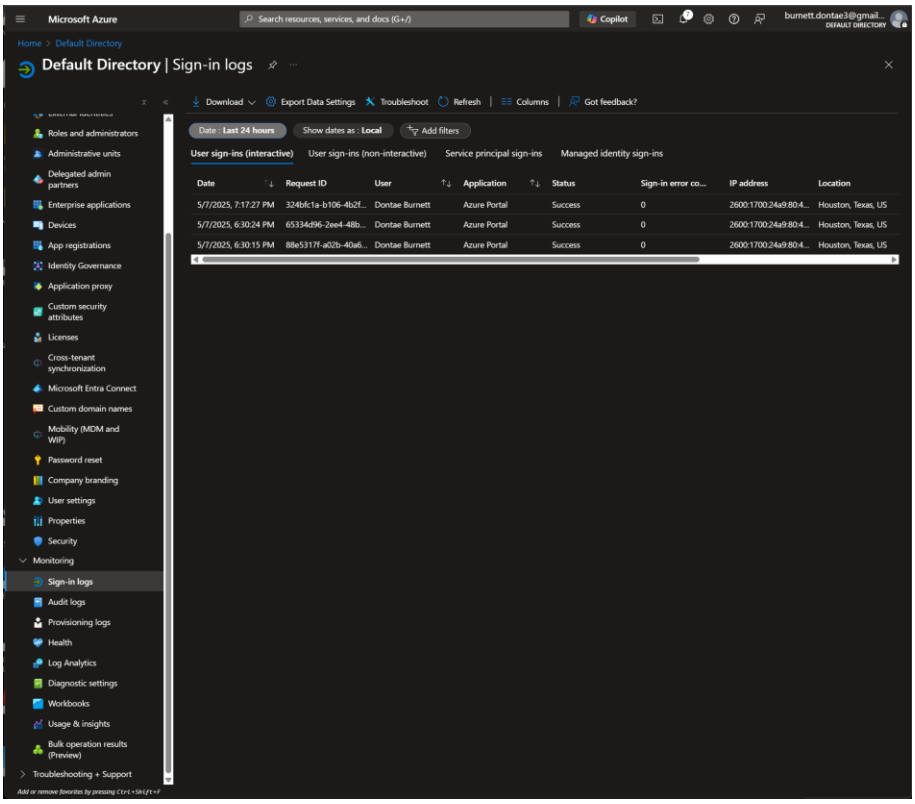

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
burnett.dontae3@gmail...
DEFAULT DIRECTORY
Home > Default Directory | Users > Users >
Per-user multifactor authentication
Bulk update
Got feedback?
Users
Service settings
Use multifactor authentication (MFA) to protect your users and data. Our recommended approach to enforce MFA is to use adaptive Conditional Access policies. Learn more
Before you begin, take a look at the multifactor authentication deployment guide.
Enable MFA
Disable MFA
Enforce MFA
User MFA settings
Search
Status : All
View : Sign-in allowed users
Reset filters
Name
UPN
Status
Dontae Burnett
burnett.dontae3_gmail.com#EXT#@burnettdontae3gmail.
disabled
Admin
TestAdmin@burnettdontae3gmail.onmicrosoft.com
disabled
Developer
TestDev@burnettdontae3gmail.onmicrosoft.com
disabled
Directory Reader
TestDirectoryReader@burnettdontae3gmail.onmicrosoft.c
disabled
Enable multifactor authentication
If your users do not regularly sign in through the browser, you can send them to this link to register for multifactor authentication:
https://aka.ms/mfasetup
Enable
Cancel


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
burnett.dontae3@gmail...
DEFAULT DIRECTORY
Home > Default Directory | Users > Users >
Per-user multifactor authentication
Multifactor authentication enabled
Multifactor authentication was enabled successfully
Bulk update
Got feedback?
Users
Service settings
Use multifactor authentication (MFA) to protect your users and data. Our recommended approach to enforce MFA is to use adaptive Conditional Access policies. Learn more
Before you begin, take a look at the multifactor authentication deployment guide.
Enable MFA
Disable MFA
Enforce MFA
User MFA settings
Search
Status : All
View : Sign-in allowed users
Reset filters
Name
UPN
Status
Dontae Burnett
burnett.dontae3_gmail.com#EXT#@burnettdontae3gmail.
disabled
Admin
TestAdmin@burnettdontae3gmail.onmicrosoft.com
enabled
Developer
TestDev@burnettdontae3gmail.onmicrosoft.com
enabled
Directory Reader
TestDirectoryReader@burnettdontae3gmail.onmicrosoft.c
enabled

Task 6: Monitor Sign-In Activity

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




Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
burnett.dontae3@gmail...
DEFAULT DIRECTORY
Home > Default Directory
Default Directory | Sign-in logs
Download
Export Data Settings
Troubleshoot
Refresh
Columns
Got feedback?
Roles and administrators
Administrative units
Delegated admin partners
Enterprise applications
Devices
App registrations
Identity Governance
Application proxy
Custom security attributes
Licenses
Cross-tenant synchronization
Microsoft Entra Connect
Custom domain names
Mobility (MDM and WIP)
Password reset
Company branding
User settings
Properties
Security
Monitoring
Sign-in logs
Audit logs
Provisioning logs
Health
Log Analytics
Diagnostic settings
Workbooks
Usage & insights
Bulk operation results (Preview)
Troubleshooting + Support
Add or remove favorites by pressing Ctrl+Shift+F
Date : Last 24 hours
Show dates as : Local
Add filters
User sign-ins (interactive)
User sign-ins (non-interactive)
Service principal sign-ins
Managed identity sign-ins
Date
Request ID
User
Application
Status
Sign-in error co...
IP address
Location
5/7/2025, 7:17:27 PM
324bfc1a-b106-4b2f...
Dontae Burnett
Azure Portal
Success
0
2600:1700:24a9:80:4...
Houston, Texas, US
5/7/2025, 6:30:24 PM
65334d96-2ee4-48b...
Dontae Burnett
Azure Portal
Success
0
2600:1700:24a9:80:4...
Houston, Texas, US
5/7/2025, 6:30:15 PM
88e5317f-a02b-40a6...
Dontae Burnett
Azure Portal
Success
0
2600:1700:24a9:80:4...
Houston, Texas, US