

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

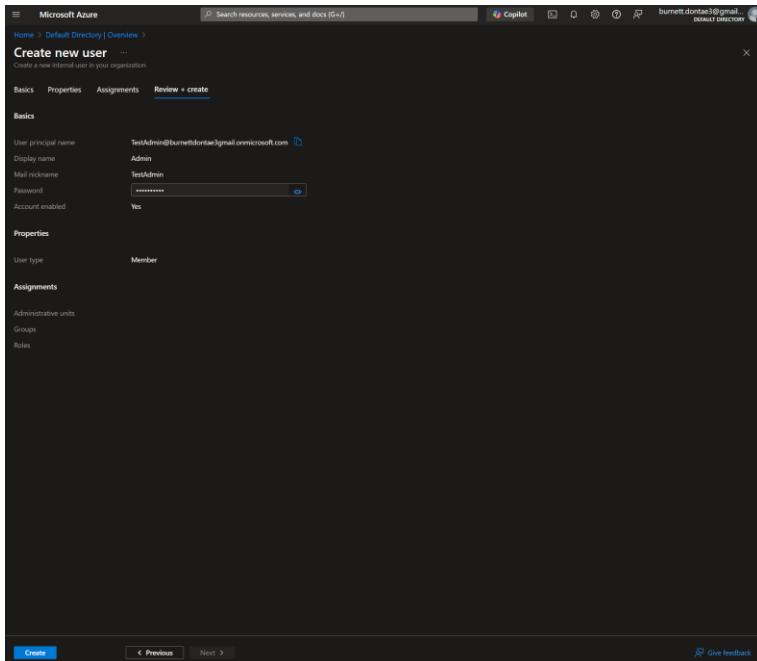
A company wants to integrate their web application with Entra ID for authentication, manage user and group permissions, enforce conditional access policies, and enable multi-factor authentication (MFA) for added security.

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

The screenshot shows the Microsoft Azure portal interface for creating a new user. The top navigation bar includes 'Microsoft Azure', 'Search resources, services, and docs (G+)', 'Copilot', and the user's email 'burnett.donate3@gmail.com'. The main title is 'Create new user ...' with a subtitle 'Create a new internal user in your organization'. Below this, there are tabs for 'Basics', 'Properties', 'Assignments', and 'Review + create'. The 'Basics' tab is selected. The form fields include:

- User principal name: TestDev
- Domain: burnett.donate3@gmail.com (selected)
- Mail nickname: TestDev (checkbox checked: 'Derive from user principal name')
- Display name: Developer
- Password: (redacted)
- Auto-generate password: (checkbox checked)
- Account enabled: (checkbox checked)

At the bottom of the form are buttons for 'Review + create', '< Previous', 'Next: Properties >', and 'Give feedback'.

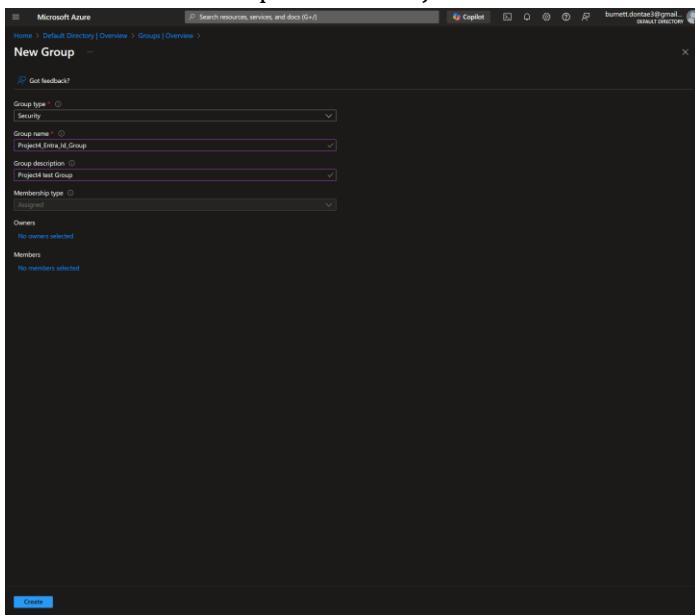
Directory Reader

The screenshot shows the Microsoft Azure portal interface for creating a new user. The top navigation bar includes 'Microsoft Azure', 'Search resources, services, and docs (G+)', 'Copilot', and the user's email 'burnett.donate3@gmail.com'. The main title is 'Create new user ...' with a subtitle 'Create a new internal user in your organization'. Below this, there are tabs for 'Basics', 'Properties', 'Assignments', and 'Review + create'. The 'Basics' tab is selected. The form fields include:

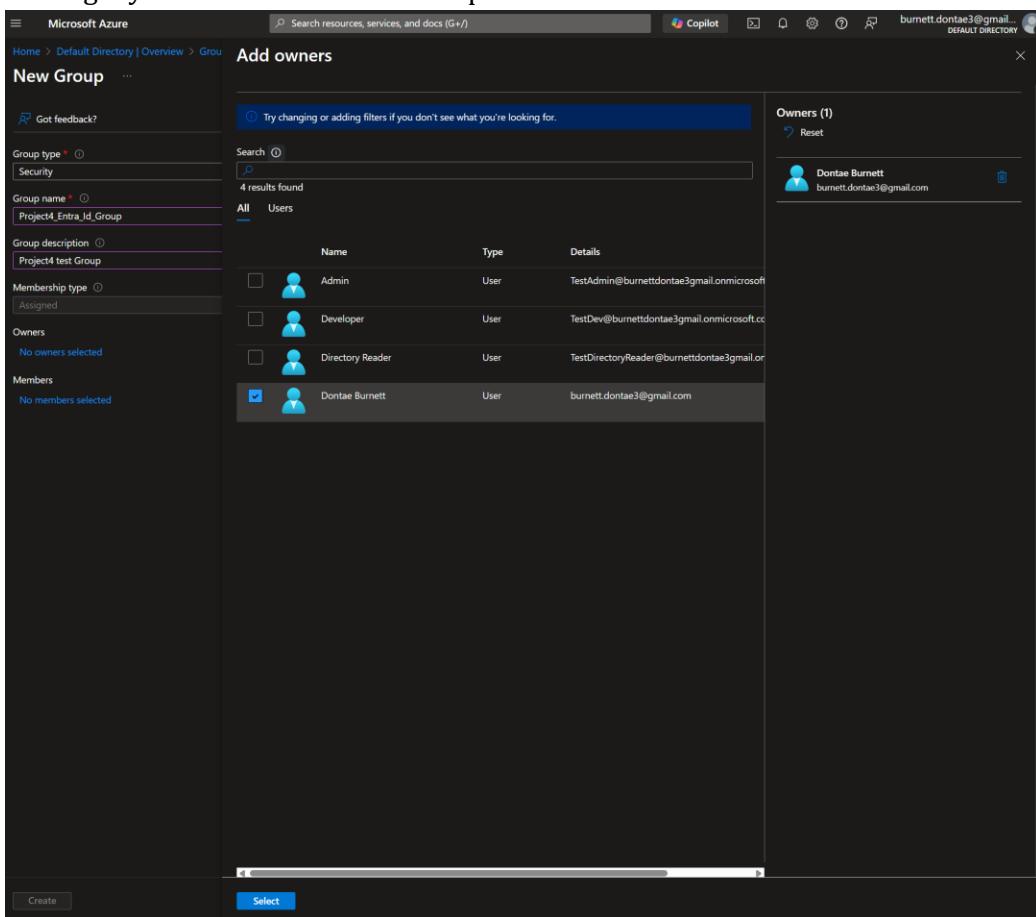
- User principal name: TestDirectoryReader@burnettdonate3@gmail.onmicrosoft.com
- Display name: Directory Reader
- Mail nickname: TestDirectoryReader
- Password: (redacted)
- Account enabled: Yes

Below the 'Basics' section, there are sections for 'Properties' (User type: Member) and 'Assignments' (Administrative units, Groups, Roles). At the bottom of the form are buttons for 'Create', '< Previous', 'Next >', and 'Give feedback'.

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

The screenshot shows the 'Add members' dialog in the Microsoft Azure portal. On the left, there is a sidebar with group configuration options like Group type (Security), Group name (Project4_Entra_Id_Group), Group description (Project4 test Group), and Membership type (Assigned). The 'Owners' section shows '1 owner selected'. The 'Members' section shows 'No members selected'. The main area has a search bar and tabs for All, Users, Groups, Devices, and Enterprise applications. Under the 'Users' tab, a list of 105 results is shown, with four users selected: Admin, Developer, Directory Reader, and Doniae Burnett. Each user has a checkbox next to their name and a small profile icon. The 'Selected (4)' section on the right lists these users with their names and email addresses. At the bottom, there are 'Create' and 'Select' buttons.

Notifications

[More events in the activity log →](#)

[Dismiss all](#)

Successfully created group



Successfully created group Project4_Entra_Id_Group .

a few seconds ago

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

The screenshot shows the Microsoft Azure portal interface for managing app registrations. The main area displays the 'Overview' blade for the application 'Project4testapp'. Key details shown include:

- Display name: Project4testapp
- Application (client) ID: 3d45d3df-4e10-4c5e-8c70-99d21d0xd3d...
- Object ID: 5474553-4746-462-901c-808165e0ec6...
- Directory (tenant) ID: 33585049-cb44-462-901c-808165e0ec6...
- Supported account types: My organization only
- Client credentials: Add a certificate or secret
- Redirect URIs: Add a Redirect URI
- Application ID URI: Add an Application ID URI
- Managed application in local directory: Project4testapp

A notification bar at the top right of the blade indicates: "Successfully created application Project4testapp." Below the blade, there are two informational cards:

- "Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more"
- "Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Applications (Azure AD). We will continue to provide technical support and security updates, but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more."

At the bottom of the page, there is a section titled "Build your application with the Microsoft identity platform" which provides information about the Microsoft identity platform and links to documentation.

Microsoft Azure | Microsoft Graph

Home > App registrations > Project4testapp

Project4testapp | API permissions

Search resources, services, and docs (G+)

Granting tenant-wide consent may invoke permission affected. Learn more

The "Admin consent required" column shows if your organization, or in organizations where this app is installed, requires admin consent before users can consent to this permission.

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

Configured permissions

API / Permissions name Type User Read Delegated

To view and manage consented permissions for this application, click here.

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.

Configured permissions

API / Permissions name Type

Microsoft Graph (1)

User Read Delegated

Add a permission Grant admin consent

Microsoft 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 experience 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 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 API

Azure DevOps Integrate with Azure DevOps and Azure DevTest Labs

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 Rights Management Programmatic access to create and manage jobs in Azure Quantum

Azure Customer Insights

Data Export Service for Microsoft Dynamics 365

Add or remove favorites by pressing Ctrl+Shift+F

Microsoft Azure | Microsoft Graph

Home > App registrations > Project4testapp

Project4testapp | Certificates & secrets

Search resources, services, and docs (G+)

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 | 6z@Q-pkRQj4fUvO6G9D8a45wNCO... | 95874571-6f27-4b44-aef-3ad80879c343 |

Successfully updated application Project4testapp credentials

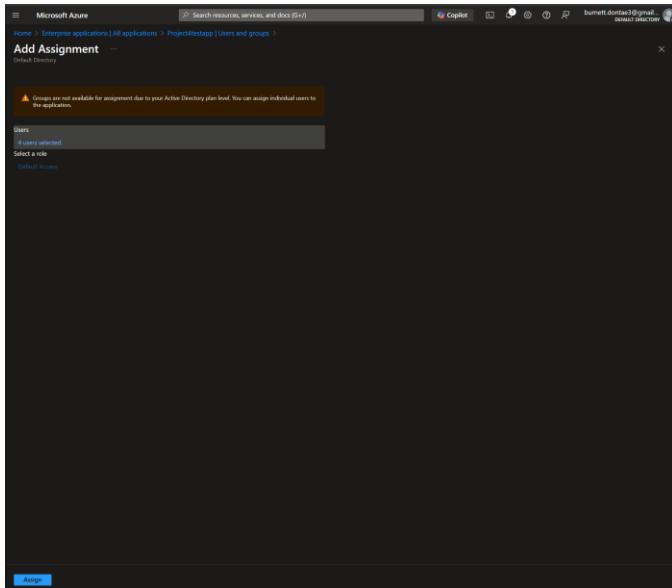
Task 3: Assign Users and Groups to the Application

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

The application will not appear for assigned users within My Apps. Set 'Visible to users?' to yes in properties to enable this.

| Display name | Object type |
|----------------------------------|-------------|
| No application assignments found | |

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



Microsoft Azure

Home > Enterprise applications | All applications > Project4testapp

Project4testapp | Users and groups

Enterprise Application

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 App. 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

Find 200+ users, search all users & groups

| Display name | Object type |
|------------------|-------------|
| Admin | User |
| Developer | User |
| Directory Reader | User |
| Doniae 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

The screenshot shows the Microsoft Azure portal's Default Directory Overview page. The left sidebar contains navigation links for Overview, Preview features, Diagnostic and solve problems, Manage (with sub-links for Users, Groups, External identities, 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 MAM), Company branding, User settings, Properties, Security, Monitoring, Troubleshooting + Support), and Feature highlights (Identity Protection, Access review). The main content area displays basic information about the tenant, including Name (Default Directory), Tenant ID (3358049-cd44-46c2-901c-80881650ec6), Primary domain (burnettdonate@gmail.onmicrosoft.com), License (Microsoft Entra ID Free), and Alerts. A prominent alert message encourages migrating to converged authentication methods by September 2025. Below the alerts, there is a "My feed" section with cards for "try Microsoft Entra admin center", "Secure Score for Identity" (42.119), and "Microsoft Entra Connect". At the bottom, there are links for "Identity Protection" and "Access review".

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

The screenshot shows the Microsoft Azure Conditional Access Overview page. The left sidebar includes links for Policies, Insights and reporting, Diagnose and solve problems, Manage, Monitoring, Troubleshooting + Support, and a Create new policy button. The main content area explains what Conditional Access is and provides examples of conditions and controls. It also includes a Get Started section with three steps: Create your first policy by clicking 'Create new policy', Specify policy Conditions and Controls, and When you are done, don't forget to Enable policy and Create.

Task 5: Enable Multi-Factor Authentication (MFA)

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

The screenshot shows the Microsoft Entra ID Users page. The left sidebar lists All users, Audit logs, Sign-in logs, Diagnose and solve problems, Deleted users, Password reset, User settings, Bulk operation results, and New support request. The main content area displays a table of users with columns for Display name, User principal name, User type, On-premises sync status, Identities, Company name, and Created date. Four users are listed: Admin, Developer, Directory Reader, and Daniel Burnett.

| Display name | User principal name | User type | On-premises sync | Identities | Company name | Created |
|------------------|---|-----------|------------------|----------------------------|--------------|----------------------|
| Admin | TestAdmin@burnettontest.onmicrosoft.com | Member | No | burnettontest@gmail.com#mc | | 2023-09-01T12:00:00Z |
| Developer | TestDeveloper@burnettontest.onmicrosoft.com | Member | No | burnettontest@gmail.com#mc | | 2023-09-01T12:00:00Z |
| Directory Reader | TestDirectoryReader@burnettontest.onmicrosoft.com | Member | No | burnettontest@gmail.com#mc | | 2023-09-01T12:00:00Z |
| Daniel Burnett | burnett.donate3@gmail.com | Member | No | MicrosoftAccount | | 2023-09-01T12:00:00Z |

Microsoft Azure

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#@burnettdontae3@gmail | disabled |
| Admin | TestAdmin@burnettdontae3@gmail.onmicrosoft.com | disabled |
| Developer | TestDev@burnettdontae3@gmail.onmicrosoft.com | disabled |
| Directory Reader | TestDirectoryReader@burnettdontae3@gmail.onmicrosoft.co | 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

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#@burnettdontae3@gmail | disabled |
| Admin | TestAdmin@burnettdontae3@gmail.onmicrosoft.com | enabled |
| Developer | TestDev@burnettdontae3@gmail.onmicrosoft.com | enabled |
| Directory Reader | TestDirectoryReader@burnettdontae3@gmail.onmicrosoft.co | enabled |

Multifactor authentication enabled

Multifactor authentication was enabled successfully

Task 6: Monitor Sign-In Activity

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

The screenshot shows the Microsoft Azure portal interface for the 'Default Directory' overview. The left sidebar contains navigation links for Roles and administrators, 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 VIP), 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), and Troubleshooting + Support. The main content area displays basic information about the directory, including Name (Default Directory), Tenant ID (33585049-cbd4-46f2-901c-808f165e0ec6), Primary domain (burnett.dontae3@gmail.onmicrosoft.com), License (Microsoft Entra ID Free), and user statistics (Users: 4, Groups: 2, Applications: 1, Devices: 0). A prominent alert box titled 'Migrate to the converged Authentication methods policy' encourages users to migrate from legacy MFA and SSPR policies by September 2025. Below the alert, the 'My feed' section shows a card for 'Try Microsoft Entra admin center' and a user profile for 'Dontae Burnett'. The 'Feature highlights' section includes cards for 'Secure Score for Identity' (42.11%) and 'Microsoft Entra Connect' (Sync has never run). At the bottom, there are sections for 'Identity Protection' and 'Access reviews'.

Microsoft Azure

Home > Default Directory

Default Directory | Sign-in logs

Download Export Data Settings Troubleshoot Refresh Columns Got feedback?

Date: Last 24 hours Show 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 | 324bf1ca-b106-4b2f... | Dontae Burnett | Azure Portal | Success | 0 | 2600:1700:24d9:804... | Houston, Texas, US |
| 5/7/2025, 8:30:24 PM | 65334d96-2ee4-4b8... | Dontae Burnett | Azure Portal | Success | 0 | 2600:1700:24d9:804... | Houston, Texas, US |
| 5/7/2025, 8:30:15 PM | 88e5317f-a02b-406f... | Dontae Burnett | Azure Portal | Success | 0 | 2600:1700:24d9:804... | Houston, Texas, US |

Identity Governance Application proxy Custom security attributes Licenses Cross-tenant synchronization Microsoft Entra Connect Custom domain names Mobility (MDM and Wi-Fi) 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)

Add or remove favorites by pressing Ctrl+Shift+F4

The screenshot shows the Microsoft Azure portal interface for the 'Default Directory'. The left sidebar contains a navigation menu with various options like 'Roles and administrators', '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 Wi-Fi)', 'Password reset', 'Company branding', 'User settings', 'Properties', 'Security', 'Monitoring', 'Sign-in logs' (which is currently selected and highlighted in blue), 'Audit logs', 'Provisioning logs', 'Health', 'Log Analytics', 'Diagnostic settings', 'Workbooks', 'Usage & insights', and 'Bulk operation results (Preview)'. The main content area is titled 'Default Directory | Sign-in logs' and displays a table of sign-in logs. The table has columns for Date, Request ID, User, Application, Status, Sign-in error count, IP address, and Location. There are three entries listed, all showing a success status and an IP address starting with 2600:1700. The location for all entries is Houston, Texas, US. The first two entries occurred at 7:17:27 PM and 8:30:24 PM on 5/7/2025, while the third entry occurred at 8:30:15 PM. The application for all entries was the Azure Portal.

| Date | Request ID | User | Application | Status | Sign-in error co... | IP address | Location |
|----------------------|-----------------------|----------------|--------------|---------|---------------------|-----------------------|--------------------|
| 5/7/2025, 7:17:27 PM | 324bf1ca-b106-4b2f... | Dontae Burnett | Azure Portal | Success | 0 | 2600:1700:24d9:804... | Houston, Texas, US |
| 5/7/2025, 8:30:24 PM | 65334d96-2ee4-4b8... | Dontae Burnett | Azure Portal | Success | 0 | 2600:1700:24d9:804... | Houston, Texas, US |
| 5/7/2025, 8:30:15 PM | 88e5317f-a02b-406f... | Dontae Burnett | Azure Portal | Success | 0 | 2600:1700:24d9:804... | Houston, Texas, US |