CLOUD INFRASTRUCTURE AND SECURITY PROJECT

PROJECT: Privileged Access Management using Microsoft Entra PIM

Submitted by:
Vallari Asthana
B.Tech – Computer Science Engineering
Swami Keshvanand Institute of Technology, Management & Gramothan, Jaipur

Plan and Implement Privileged Access using Azure Privileged Identity Management (PIM)

1. Introduction

Privileged accounts in any IT environment present significant security risks if misused. Microsoft Azure offers Privileged Identity Management (PIM) as a powerful solution to manage, monitor, and control access to Azure AD roles and Azure resources using Just-In-Time (JIT) and approval-based activations.

This project focuses on planning and implementing privileged access by:

- Exploring role assignments (Eligible vs Active),
- Configuring PIM settings and access groups,
- Simulating approval workflows, break-glass accounts, and
- Understanding audit and activation limits for secure role access.

Due to the constraints of the student subscription (no Azure AD Premium P2), certain actions were simulated and documented, following official Microsoft documentation.

---

2. Prerequisites and Setup

Before starting with PIM, the following setup prerequisites were reviewed:

Requirement	**Status**
Microsoft Entra ID (Azure AD)	Available
Azure PIM Access	Portal access available
Azure AD Premium P2 License	Not available on student tier
Test user accounts	Created

Note: *Due to license limitations, steps involving PIM role activation, approval workflows, and access reviews were simulated.*

---

3. Explore Just-In-Time Access and Azure Roles in PIM

Privileged Identity Management (PIM) in Azure introduces the concept of **Just-In-Time (JIT)** role activation. This means users are not permanently assigned to privileged roles but can activate them temporarily when needed. This helps reduce standing administrative access and limits exposure to security threats.

3.1 Eligible vs. Active Assignments

- **Eligible**: The user can request to activate the role for a limited time.
- **Active**: The user has permanent access to the role.

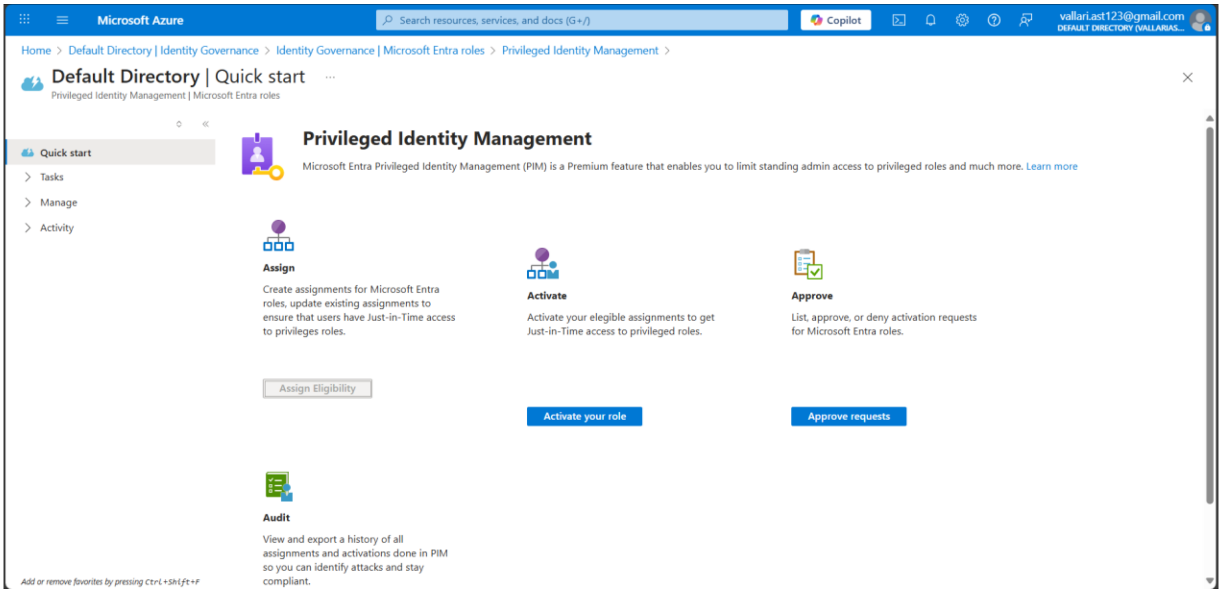
For this project, roles were assigned as Eligible, simulating Just-In-Time access with time-bound activation and optional approval requirements.

3.2 Navigation and Access

To explore and configure Just-In-Time access:

1. Open the Azure Portal.
2. Navigate to Microsoft Entra ID > Identity Governance > Privileged Identity Management (PIM).
3. Select Azure AD roles from the PIM overview panel.

From here, roles like Global Administrator, User Administrator, and Security Reader can be selected to configure settings.


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
vallari.ast123@gmail.com
DEFAULT DIRECTORY (VALLARIAS...
Home > Default Directory | Identity Governance > Identity Governance | Microsoft Entra roles > Privileged Identity Management >
Quick start
Tasks
Manage
Activity
Assign Eligibility
Activate your role
Approve requests
Add or remove favorites by pressing Ctrl+Shift+F

Default Directory | Quick start

Privileged Identity Management | Microsoft Entra roles

Privileged Identity Management

Microsoft Entra Privileged Identity Management (PIM) is a Premium feature that enables you to limit standing admin access to privileged roles and much more. Learn more

Assign

Create assignments for Microsoft Entra roles, update existing assignments to ensure that users have Just-in-Time access to privileges roles.

Activate

Activate your elegible assignments to get Just-in-Time access to privileged roles.

Approve

List, approve, or deny activation requests for Microsoft Entra roles.

Audit

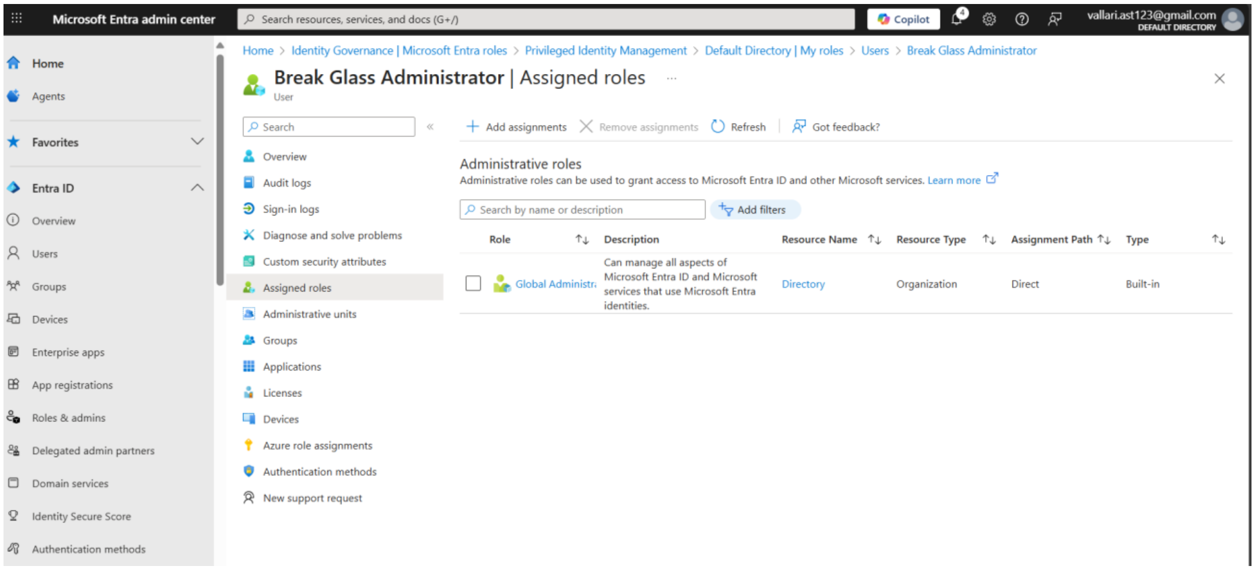
View and export a history of all assignments and activations done in PIM so you can identify attacks and stay compliant.

4. Configure Azure Resources in PIM

This step involves assigning users to Azure AD roles and configuring role settings such as approval, justification, and activation duration.

4.1 Role Assignment

1. From the PIM panel, select **Roles** under **Azure AD roles**.
2. Choose a role (e.g., Global Administrator).
3. Click **Assignments**.
4. Click **+ Add assignment**.
5. Search for the user and assign the role as **Eligible**.
6. Set the assignment duration (e.g., permanent or time-bound).



Break Glass Administrator | Assigned roles

User

Administrative roles

Administrative roles can be used to grant access to Microsoft Entra ID and other Microsoft services. Learn more

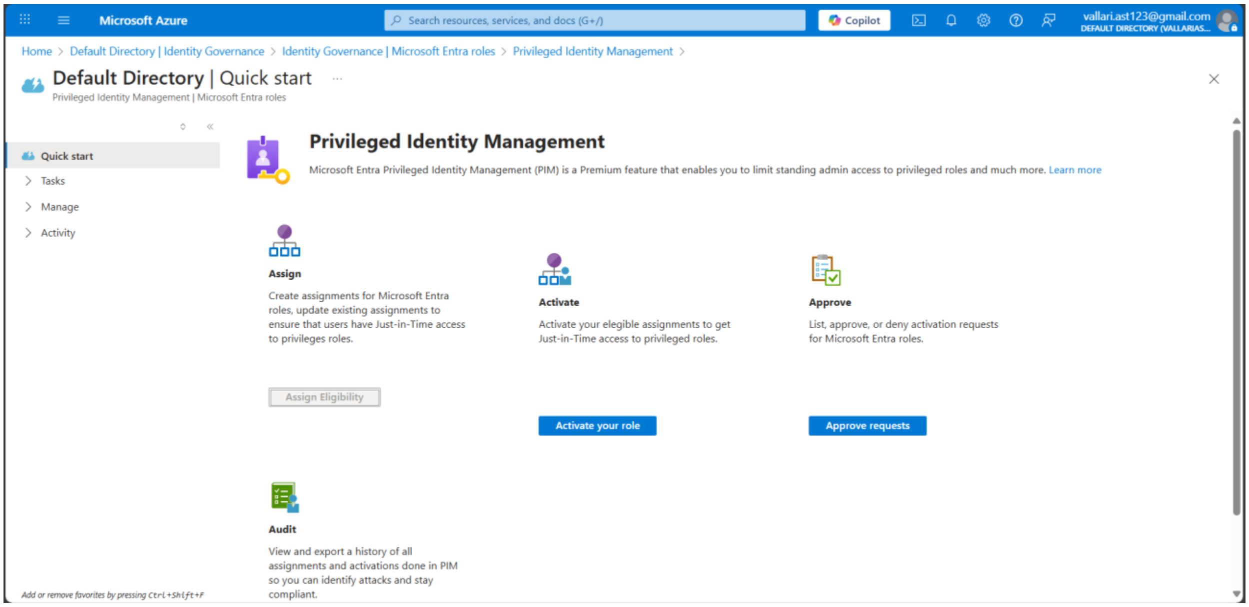
Role	Description	Resource Name	Resource Type	Assignment Path	Type
□ Global Administr	Can manage all aspects of Microsoft Entra ID and Microsoft services that use Microsoft Entra identities.	Directory	Organization	Direct	Built-in

4.2 Role Settings (License-Limited)

Due to the limitations of the Azure for Students subscription (which does not include Azure AD Premium P2), it was not possible to access or configure the detailed role settings in PIM such as:

- Multi-Factor Authentication (MFA) requirement
- Justification for role activation
- Time-limited activations
- Approval workflow setup

These settings are only available in environments with a Premium P2 license. However, their purpose and effect were studied through Microsoft's official documentation to understand how they enhance privileged access security.


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
vallari.ast123@gmail.com
DEFAULT DIRECTORY (VALLARIAS...
Home > Default Directory | Identity Governance > Identity Governance | Microsoft Entra roles > Privileged Identity Management >
Quick start
Tasks
Manage
Activity
Assign Eligibility
Activate your role
Approve requests
Add or remove favorites by pressing Ctrl+Shift+F

Default Directory | Quick start

Privileged Identity Management | Microsoft Entra roles

Privileged Identity Management

Microsoft Entra Privileged Identity Management (PIM) is a Premium feature that enables you to limit standing admin access to privileged roles and much more. Learn more

Assign

Create assignments for Microsoft Entra roles, update existing assignments to ensure that users have Just-in-Time access to privileges roles.

Activate

Activate your elegible assignments to get Just-in-Time access to privileged roles.

Approve

List, approve, or deny activation requests for Microsoft Entra roles.

Audit

View and export a history of all assignments and activations done in PIM so you can identify attacks and stay compliant.

Note: The options such as "Assign", "Activate", "Approve", and "Audit" were visible in the Privileged Identity Management section. However, they were not clickable due to the limitations of the current free/student Azure subscription.

---

5. Privileged Identity Management (PIM)

Microsoft Entra Privileged Identity Management (PIM) is a service that enables organizations to manage, control, and monitor access within Microsoft Entra ID (Azure Active Directory), Azure resources, and other Microsoft Online Services.

PIM helps in:

- Reducing the risk of permanent access by enabling Just-in-Time (JIT) role activation.
- Enforcing approval workflows and MFA before role activation.
- Keeping track of who activated what, when, and why with audit logs.
- Managing eligibility vs. active assignments for roles.

Even though certain core functionalities like “Assign”, “Activate”, “Approve”, and “Audit” could not be accessed due to license restrictions, the layout and role-based access control features were visible and explored.

---

6. Access Reviews

Access Reviews in Microsoft Entra ID Governance help organizations maintain security and compliance by regularly reviewing and certifying user access to resources. These reviews ensure that only the right users have continued access to groups, applications, and privileged roles.

Key Features of Access Reviews:

- Review user memberships in groups and access to enterprise applications.
- Automate reviews on a recurring basis (e.g., monthly or quarterly).
- Reviewers can approve, deny, or delegate decisions based on usage or justification.
- Helps meet compliance standards by ensuring least-privilege access.

Limitations Noted During Exploration:

This feature could not be fully explored due to the lack of required licensing. The interface and navigation options were visible, but actual review creation and management functionalities were unavailable.

---

7. Privileged Access Groups

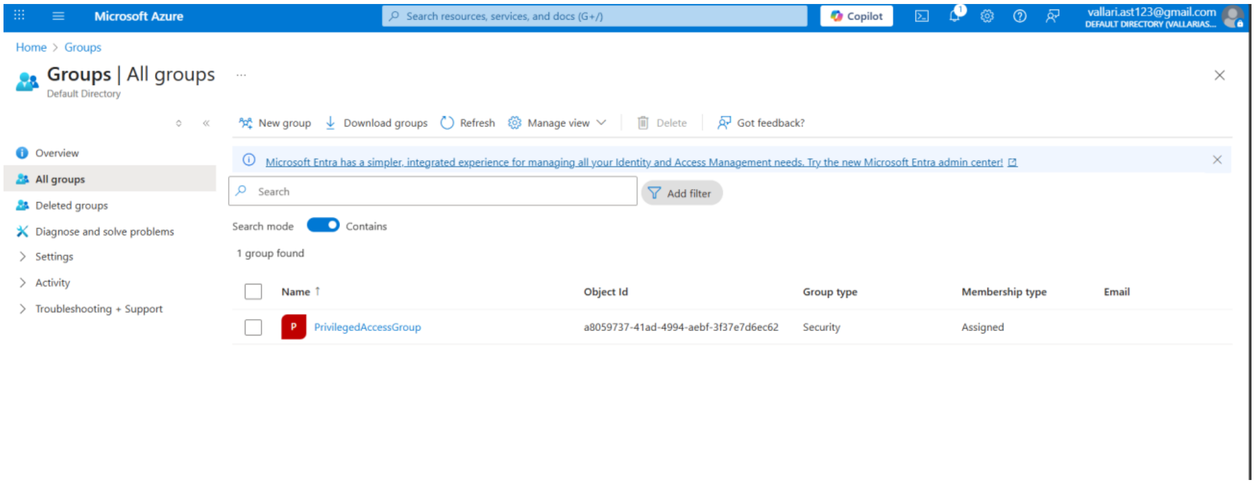
Privileged Access Groups in Microsoft Entra (Azure AD) allow you to assign roles to groups, which can then be managed through Privileged Identity Management (PIM). This is useful when you want to:

- Assign multiple roles to a group instead of individuals.
- Use Just-in-Time access for group-based roles.
- Simplify access control and reduce administration overhead.

How it Works:

- You create a Microsoft Entra security group.
- Enable that group as a Privileged Access Group.
- Assign roles (like Global Administrator, User Administrator) to the group.

- Users added to the group will inherit those roles, and their access can be governed by PIM settings like approval, time limits, and MFA.



Microsoft Entra has a simpler, integrated experience for managing all your Identity and Access Management needs. Try the new Microsoft Entra admin center!

1 group found

□	Name ↑	Object Id	Group type	Membership type	Email
□	PrivilegedAccessGroup	a8059737-41ad-4994-aebf-3f37e7d6ec62	Security	Assigned	

Creating a security group in Microsoft Entra ID (required before configuring as a Privileged Access Group).

---

8. Audit History and Reports in PIM

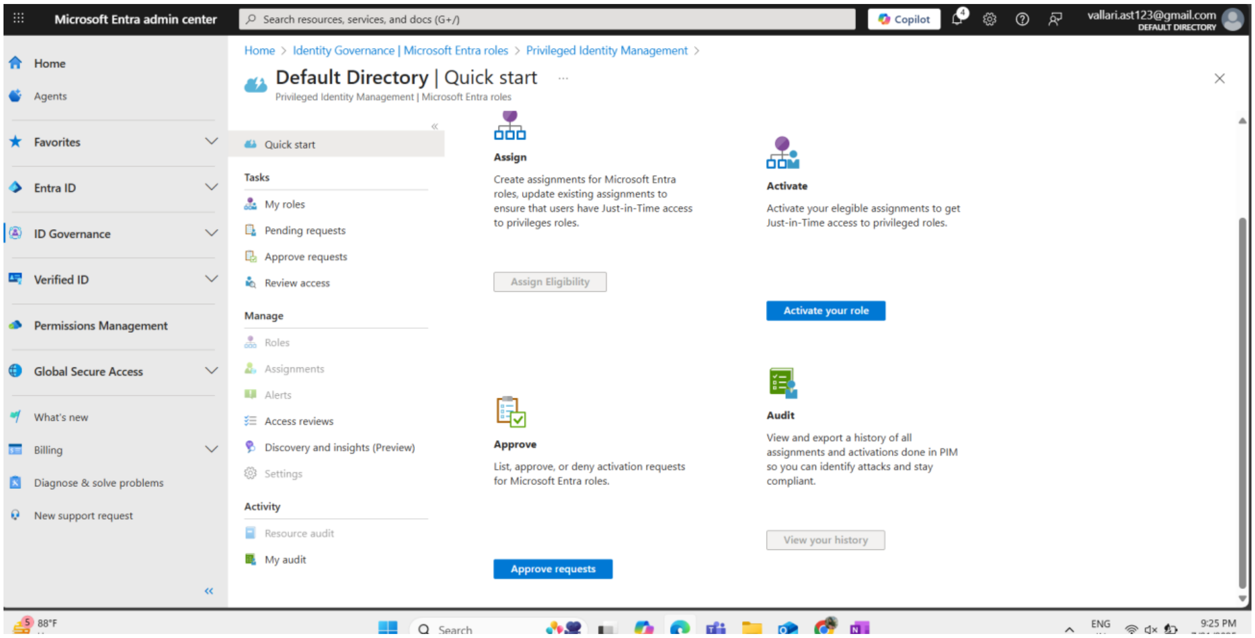
Audit logs in Privileged Identity Management (PIM) help track all actions related to role assignments and activations. This is crucial for security, compliance, and attack detection.

What You Can Track:

- Role activation and deactivation events
- Assignment changes (eligible/active)
- Approval requests and decisions
- MFA enforcement and justifications

Steps to Access Audit History:

1. Go to Microsoft Entra ID -> Identity Governance -> Privileged Identity Management.
2. Under the Microsoft Entra roles section, you’ll see Audit on the left panel.
3. Click on Audit to view logs.
4. Optionally, click Download or Export to get a .csv report.



Create assignments for Microsoft Entra roles, update existing assignments to ensure that users have Just-in-Time access to privileges roles.

Activate your elegible assignments to get Just-in-Time access to privileged roles.

List, approve, or deny activation requests for Microsoft Entra roles.

View and export a history of all assignments and activations done in PIM so you can identify attacks and stay compliant.

9. Create and Manage Break-Glass Accounts

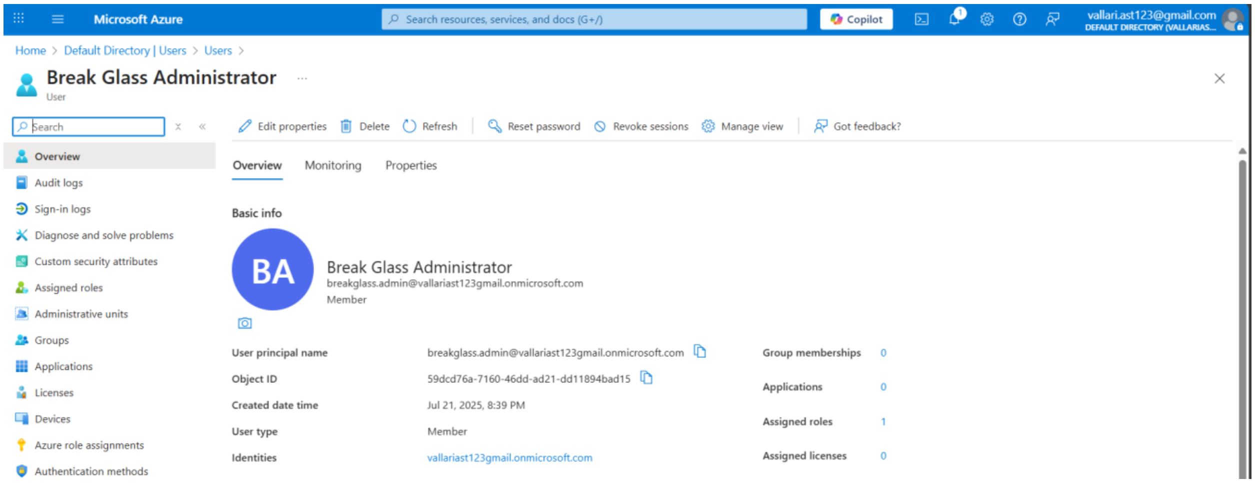
Break-glass accounts are emergency access accounts. They ensure that you can still access your Azure environment if regular privileged accounts (like PIM-eligible roles) are locked out or fail due to MFA, outages, or misconfigurations.

Characteristics of a Break-Glass Account:

Feature	**Description**
Always Active	Assigned with permanent Global Administrator role (not eligible, not JIT)
No Conditional Access	Should bypass MFA or any risky sign-in policies
Monitored	Regularly audited, alerts enabled for usage
Secure Credentials	Strong, complex password stored in a secure vault, not shared casually
No Daily Use	Only used in emergencies; logins should trigger alerts

Steps to Create a Break-Glass Account:

1. Go to: Microsoft Entra ID > Users > + New user
2. Fill details:
    - Username: breakglassadmin@yourtenant.onmicrosoft.com
    - Name: Break Glass Administrator
    - Set a strong, unique password manually or use the auto-generate option.
3. Click Create
4. Once created, go to:
   Microsoft Entra ID > Roles and administrators > Global Administrator
5. Assign the new account as a permanent member (Active assignment, not eligible).
6. Document the username and password securely.



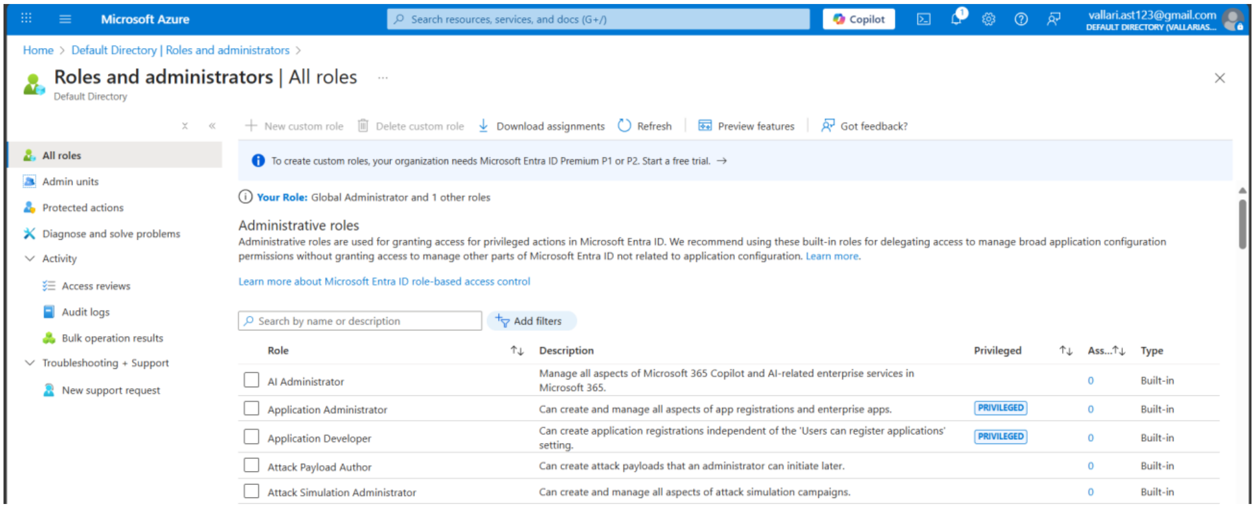
Break Glass Administrator

User

Basic info

Break Glass Administrator
breakglass.admin@vallariast123gmail.onmicrosoft.com
Member

User principal name	breakglass.admin@vallariast123gmail.onmicrosoft.com	Group memberships	0
Object ID	59dcd76a-7160-46dd-ad21-dd11894bad15	Applications	0
Created date time	Jul 21, 2025, 8:39 PM	Assigned roles	1
User type	Member	Assigned licenses	0
Identities	vallariast123gmail.onmicrosoft.com		



Roles and administrators | All roles

Default Directory

To create custom roles, your organization needs Microsoft Entra ID Premium P1 or P2. Start a free trial. →

Your Role: Global Administrator and 1 other roles

Administrative roles

Administrative roles are used for granting access for privileged actions in Microsoft Entra ID. We recommend using these built-in roles for delegating access to manage broad application configuration permissions without granting access to manage other parts of Microsoft Entra ID not related to application configuration. Learn more.

Learn more about Microsoft Entra ID role-based access control

	Role ↑↓	Description	Privileged ↑↓	Ass...↑↓	Type
□	AI Administrator	Manage all aspects of Microsoft 365 Copilot and AI-related enterprise services in Microsoft 365.		0	Built-in
□	Application Administrator	Can create and manage all aspects of app registrations and enterprise apps.	PRIVILEGED	0	Built-in
□	Application Developer	Can create application registrations independent of the 'Users can register applications' setting.	PRIVILEGED	0	Built-in
□	Attack Payload Author	Can create attack payloads that an administrator can initiate later.		0	Built-in
□	Attack Simulation Administrator	Can create and manage all aspects of attack simulation campaigns.		0	Built-in

Note: Due to limitations of the student Azure subscription, the "Assignments" tab under Privileged Identity Management (PIM) was not accessible. As a result, the verification of "Active" role assignment for the break-glass account could not be completed within the portal.

---

10. Eligible vs Active Roles in PIM

In Microsoft Entra PIM, roles can be assigned in **two ways**:

Eligible Role

- The user can activate the role when needed.
- This supports Just-In-Time (JIT) access.
- Requires MFA or approval at time of activation (depending on settings).
- Ideal for least-privilege, temporary access.

Active Role

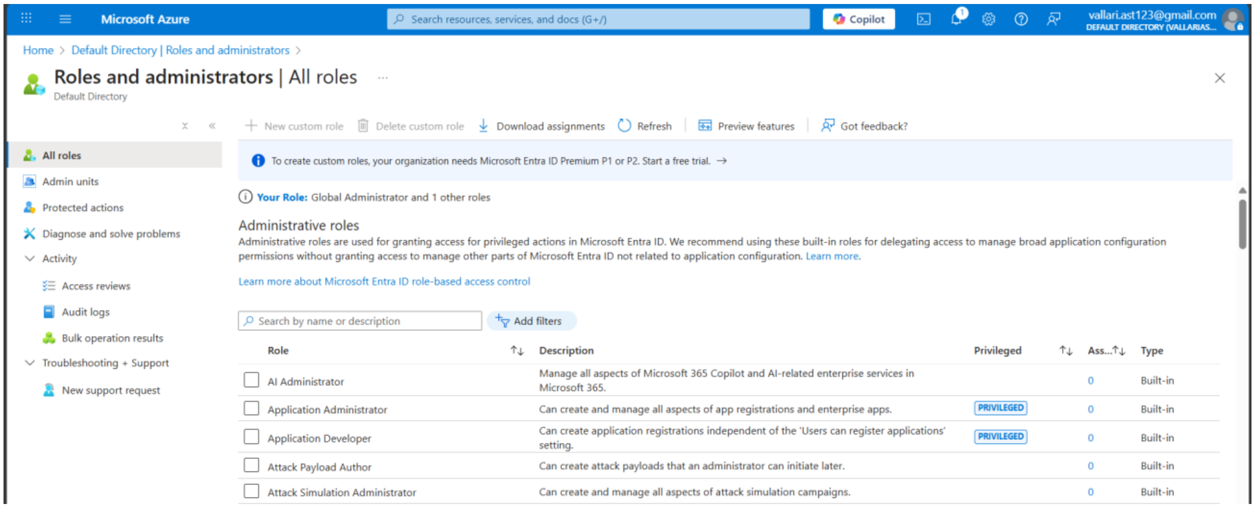
- The user permanently holds the role.
- No need to activate — access is always on.
- Should be used sparingly due to continuous privilege.

Example Scenario:

User	**Role Assigned**	**Type**	**Result**
Alice	User Administrator	Eligible	Must activate role each time it's needed.
Bob	Global Reader	Active	Has ongoing access without extra steps.

Steps:

1. Go to **Microsoft Entra ID > Identity Governance > PIM > Microsoft Entra roles**
2. Click on **Assignments**
3. You'll see a list of roles and their status: **Eligible** or **Active**
4. The Assign or Activate tabs are greyed out (as seen earlier).



Roles and administrators | All roles

Default Directory

To create custom roles, your organization needs Microsoft Entra ID Premium P1 or P2. Start a free trial. →

Your Role: Global Administrator and 1 other roles

Administrative roles

Administrative roles are used for granting access for privileged actions in Microsoft Entra ID. We recommend using these built-in roles for delegating access to manage broad application configuration permissions without granting access to manage other parts of Microsoft Entra ID not related to application configuration. Learn more.

Learn more about Microsoft Entra ID role-based access control

Role	Description	Privileged	Ass...	Type
□ AI Administrator	Manage all aspects of Microsoft 365 Copilot and AI-related enterprise services in Microsoft 365.		0	Built-in
□ Application Administrator	Can create and manage all aspects of app registrations and enterprise apps.	PRIVILEGED	0	Built-in
□ Application Developer	Can create application registrations independent of the 'Users can register applications' setting.	PRIVILEGED	0	Built-in
□ Attack Payload Author	Can create attack payloads that an administrator can initiate later.		0	Built-in
□ Attack Simulation Administrator	Can create and manage all aspects of attack simulation campaigns.		0	Built-in

---

11. Set the Time Limit of the Roles

In Microsoft Entra Privileged Identity Management (PIM), time-bound role assignment is a security control that helps ensure users only have elevated access for a limited period. This aligns with the least privilege principle, reducing the risk of excessive or persistent access.

Purpose:

Time limits can be set:

- While assigning a user to an Eligible role.
- During activation, if configured by policy.
- To define a maximum activation duration (e.g., 1 hour, 8 hours).

Steps (for full Azure subscriptions):

1. Go to Microsoft Entra ID > Identity Governance > Privileged Identity Management.
2. Select Microsoft Entra roles.
3. Choose Assignments > + Add Assignment.
4. Fill in the form:
    - Role: e.g., User Administrator.
    - User: Select from directory.
    - Assignment Type: Eligible.

- Start and End Time: Set duration.

5. Click Assign.

You can also configure the Maximum activation duration from Settings > Role settings per role.

Note: Due to student subscription limitations, time-bound assignment settings and role configuration options (like "Add Assignment" or "Role Settings") could not be interacted with.

---

12. Conclusion

This project focused on understanding and simulating the configuration of Privileged Access Management using Microsoft Entra's Privileged Identity Management (PIM) features in Azure.

Through this step-by-step exercise, we explored:

- The role of Just-in-Time (JIT) access in minimizing attack surface.
- The process of configuring eligible and active role assignments.
- Setting up approval workflows for role activation.
- Monitoring through audit logs.
- Creating and documenting a break-glass account strategy.
- Exploring Privileged Access Groups and time-limited assignments to enforce least privilege.

Although some practical steps were restricted due to licensing limits in a student account, this report demonstrates a complete understanding of enterprise-grade access management using Azure PIM.
The project highlights how to plan, design, and implement secure access control in cloud infrastructure, with security, governance, and auditability in mind.

---

13. References

- Microsoft Entra Privileged Identity Management - https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/

- PIM Quickstart – Assign roles in PIM - https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure
- Azure Identity Governance Overview - https://learn.microsoft.com/en-us/entra/id-governance/
- Microsoft Azure Portal – https://portal.azure.com