Step 3: Configure Microsoft Entra Roles in PIM

Objective

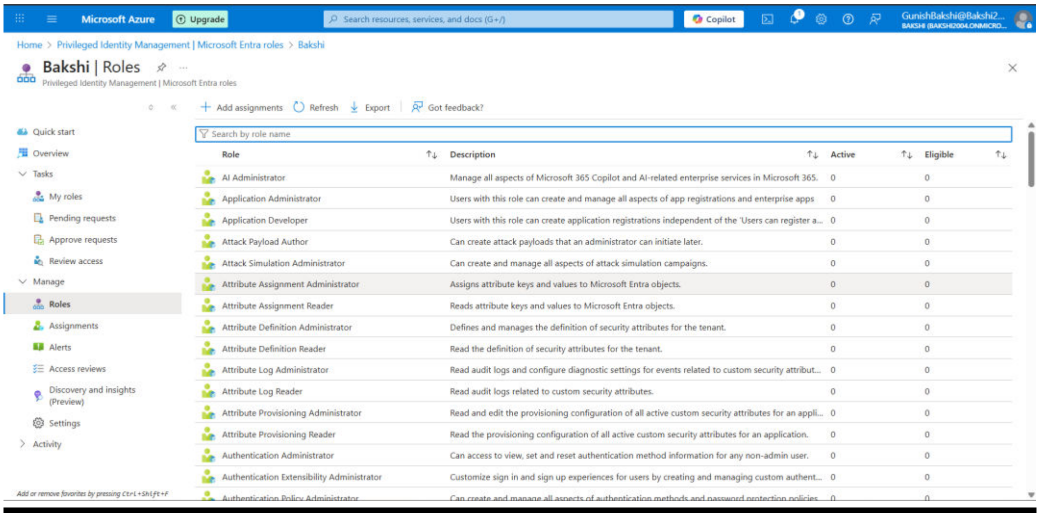
Assign users to Microsoft Entra roles as eligible (not permanent) and configure role settings such as activation requirements (MFA, approval, justification, etc.).

1. What Are Microsoft Entra Roles?

Microsoft Entra roles (previously Azure AD roles) are built-in roles that control access to identity-related features and resources. Common roles include:

- Global Administrator
- Privileged Role Administrator
- Security Administrator
- User Administrator

With PIM, users can be made eligible for these roles instead of being permanently assigned.

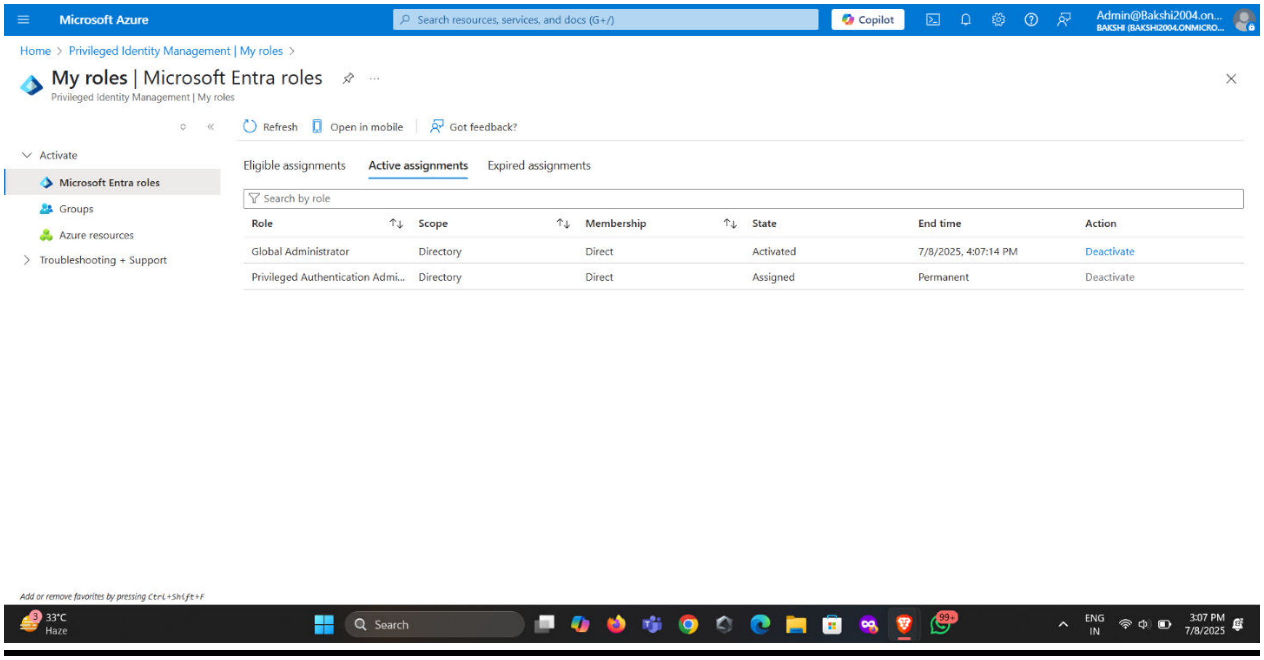

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
GunishBakshi@Bakshi2...
BAKSHI (BAKSHI2004.ONMICRO...
Home > Privileged Identity Management | Microsoft Entra roles > Bakshi
Bakshi | Roles
Privileged Identity Management | Microsoft Entra roles
Add assignments
Refresh
Export
Got feedback?
Quick start
Overview
Tasks
My roles
Pending requests
Approve requests
Review access
Manage
Roles
Assignments
Alerts
Access reviews
Discovery and insights (Preview)
Settings
Activity
Add or remove favorites by pressing Ctrl+Shift+F
Search by role name

Role	Description	Active	Eligible
AI Administrator	Manage all aspects of Microsoft 365 Copilot and AI-related enterprise services in Microsoft 365.	0	0
Application Administrator	Users with this role can create and manage all aspects of app registrations and enterprise apps	0	0
Application Developer	Users with this role can create application registrations independent of the 'Users can register a...	0	0
Attack Payload Author	Can create attack payloads that an administrator can initiate later.	0	0
Attack Simulation Administrator	Can create and manage all aspects of attack simulation campaigns.	0	0
Attribute Assignment Administrator	Assigns attribute keys and values to Microsoft Entra objects.	0	0
Attribute Assignment Reader	Reads attribute keys and values to Microsoft Entra objects.	0	0
Attribute Definition Administrator	Defines and manages the definition of security attributes for the tenant.	0	0
Attribute Definition Reader	Read the definition of security attributes for the tenant.	0	0
Attribute Log Administrator	Read audit logs and configure diagnostic settings for events related to custom security attribut...	0	0
Attribute Log Reader	Read audit logs related to custom security attributes.	0	0
Attribute Provisioning Administrator	Read and edit the provisioning configuration of all active custom security attributes for an appli...	0	0
Attribute Provisioning Reader	Read the provisioning configuration of all active custom security attributes for an application.	0	0
Authentication Administrator	Can access to view, set and reset authentication method information for any non-admin user.	0	0
Authentication Extensibility Administrator	Customize sign in and sign up experiences for users by creating and managing custom authent...	0	0
Authentication Policy Administrator	Can create and manage all aspects of authentication methods and password protection policies.	0	0

2. Configure Role Settings

Steps:

1. Go to: Microsoft Entra ID → Identity Governance → Privileged Identity Management
2. Click: Microsoft Entra Roles → Roles
3. Select a role (e.g., owner)
4. Click: Settings → Edit
5. Set the following:
    - Activation maximum duration (e.g., 1 hour)
    - Require MFA: Yes
    - Require justification: Yes
    - Require approval: Optional (select approver if Yes)
    - Enable notifications: Yes
6. Click Update to apply the settings


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Admin@Bakshi2004.on...
BAKSHI (BAKSHI2004.ONMICRO...
Home > Privileged Identity Management | My roles >
Refresh
Open in mobile
Got feedback?
Activate
Microsoft Entra roles
Groups
Azure resources
Troubleshooting + Support
Add or remove favorites by pressing Ctrl+Shift+F
33°C
Haze
Search
ENG
IN
3:07 PM
7/8/2025

My roles | Microsoft Entra roles

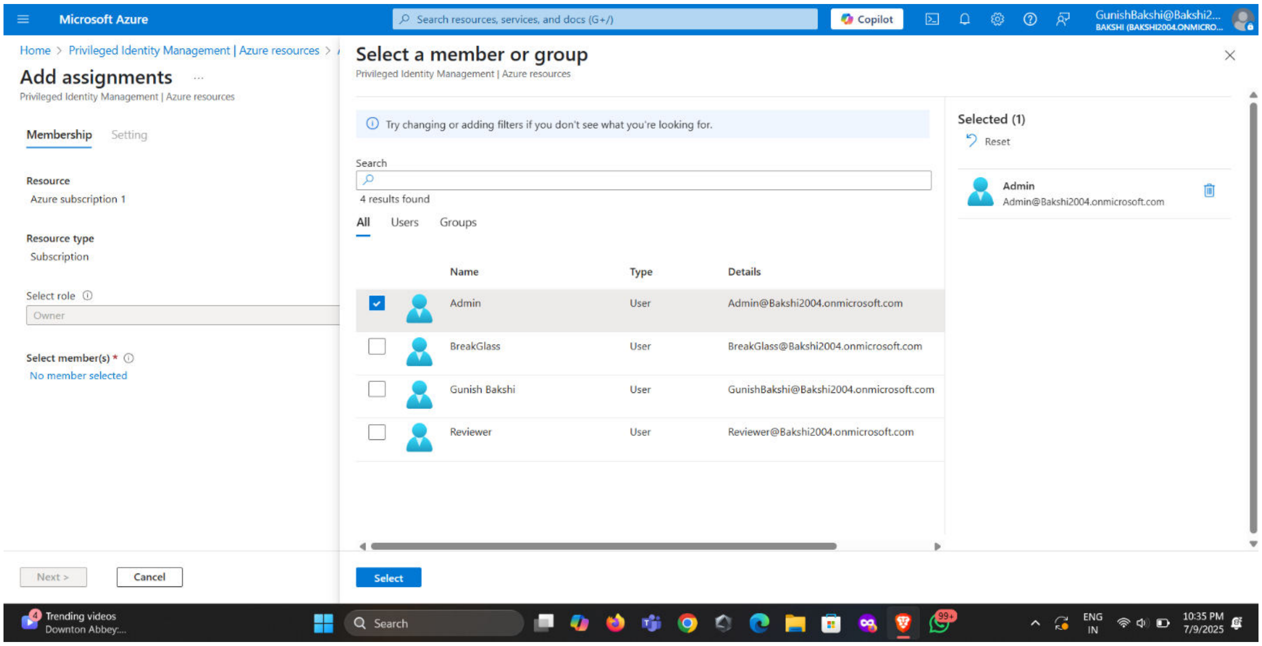
Privileged Identity Management | My roles

Eligible assignments | **Active assignments** | Expired assignments

Search by role

Role	Scope	Membership	State	End time	Action
Global Administrator	Directory	Direct	Activated	7/8/2025, 4:07:14 PM	Deactivate
Privileged Authentication Admi...	Directory	Direct	Assigned	Permanent	Deactivate

- Microsoft Entra roles



Add assignments

Privileged Identity Management | Azure resources

Resource: Azure subscription 1

Resource type: Subscription

Select role: Owner

Select member(s) *: No member selected

Select a member or group

Privileged Identity Management | Azure resources

Try changing or adding filters if you don't see what you're looking for.

Search

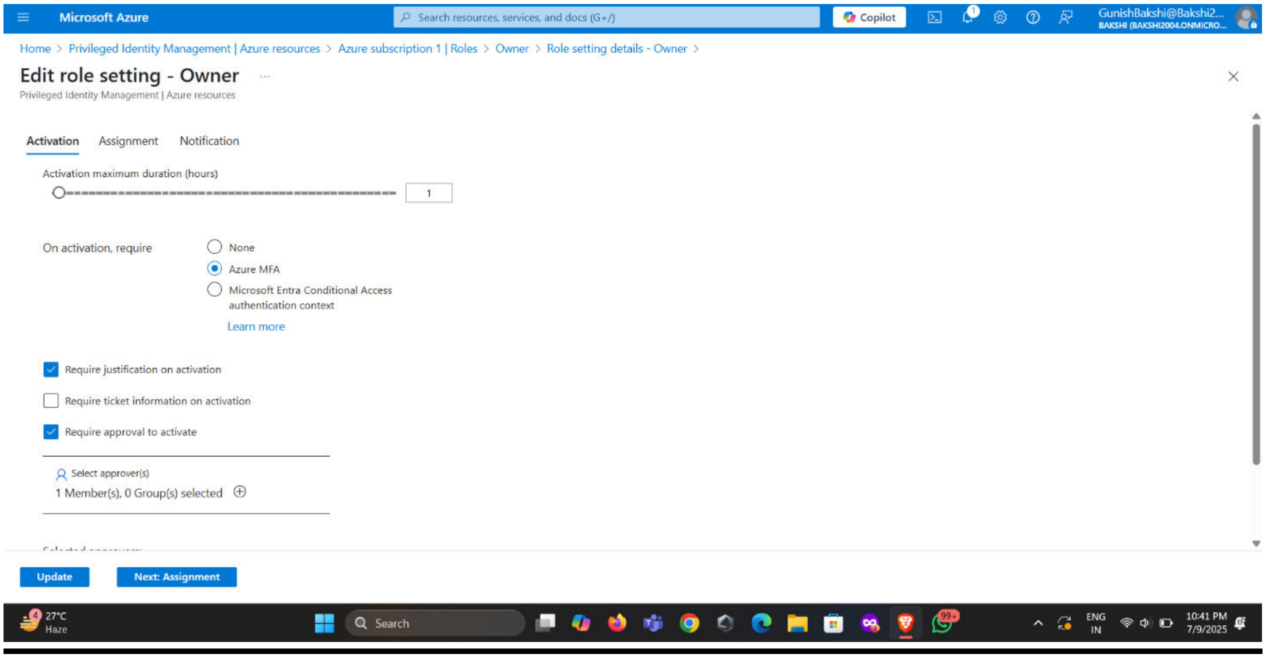
4 results found

	Name	Type	Details
☑	Admin	User	Admin@Bakshi2004.onmicrosoft.com
□	BreakGlass	User	BreakGlass@Bakshi2004.onmicrosoft.com
□	Gunish Bakshi	User	GunishBakshi@Bakshi2004.onmicrosoft.com
□	Reviewer	User	Reviewer@Bakshi2004.onmicrosoft.com

Selected (1)

Admin
Admin@Bakshi2004.onmicrosoft.com

- Selecting the role (Owner) and the Member(Admin) to give the role to.



Home > Privileged Identity Management | Azure resources > Azure subscription 1 | Roles > Owner > Role setting details - Owner >

Edit role setting - Owner

Privileged Identity Management | Azure resources

Activation | Assignment | Notification

Activation maximum duration (hours): 1

On activation, require
○ None
● Azure MFA
○ Microsoft Entra Conditional Access authentication context
Learn more

☑ Require justification on activation

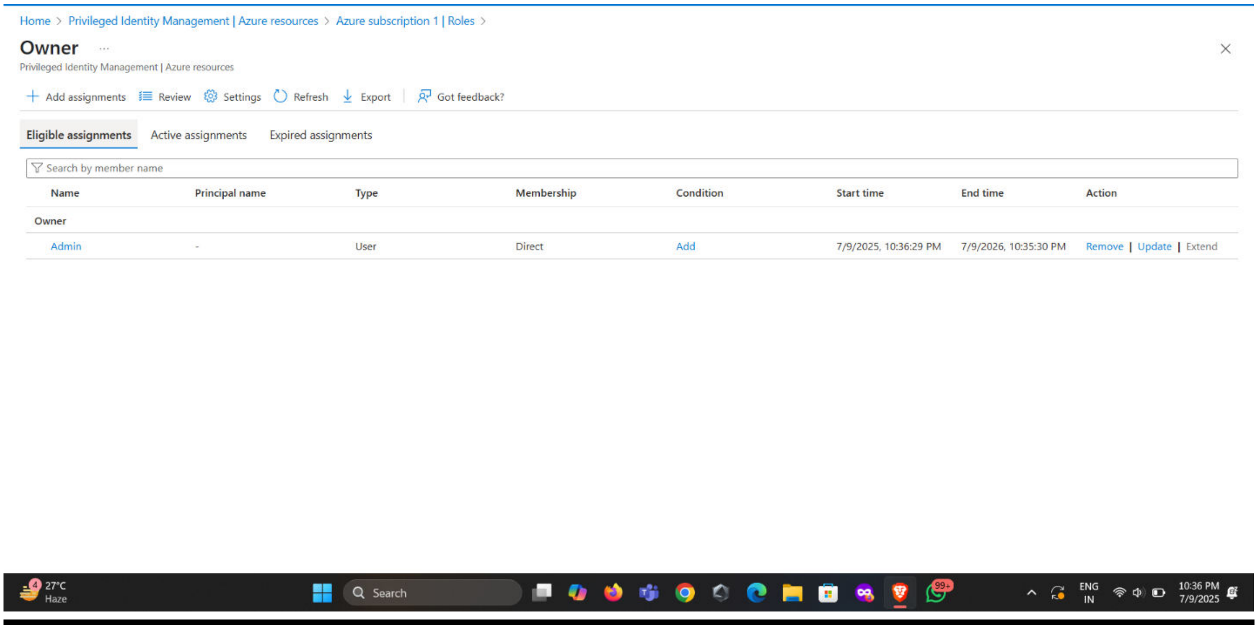
☐ Require ticket information on activation

☑ Require approval to activate

Select approver(s)
1 Member(s), 0 Group(s) selected

Update | Next: Assignment

- Editing role settings such as MFA and enable notifications.



Home > Privileged Identity Management | Azure resources > Azure subscription 1 | Roles >

Owner

Privileged Identity Management | Azure resources

+ Add assignments | Review | Settings | Refresh | Export | Got feedback?

Eligible assignments | Active assignments | Expired assignments

Search by member name

Name	Principal name	Type	Membership	Condition	Start time	End time	Action
Owner							
Admin	-	User	Direct	Add	7/9/2025, 10:36:29 PM	7/9/2026, 10:35:30 PM	Remove | Update | Extend

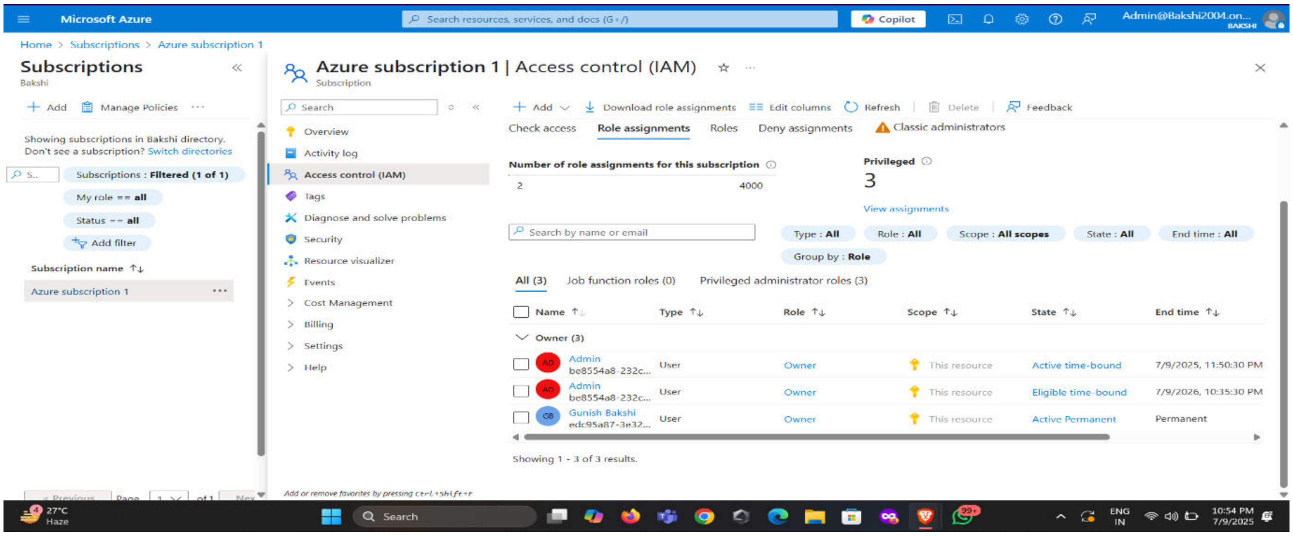
- The admin is now the owner.

3. Assign Users as Eligible for Roles

Account	Role Assigned	Assignment Type
GunishBakshi@Bakshi2004.onmicrosoft.com	Global Administrator	Permanent
admin@Bakshi2004.onmicrosoft.com	Application Administrator	Eligible
reviewer@Bakshi2004.onmicrosoft.com	Privileged Role Admin	Eligible
breakglass@Bakshi2004.onmicrosoft.com	Global Administrator	Permanent

Steps:

1. In PIM, go to: **Microsoft Entra Roles → Roles**
2. Select the role
3. Click: **Add assignments**
4. Choose the **user**, **assignment type** (Eligible or Active), and **duration**
5. Review and confirm



Number of role assignments for this subscription

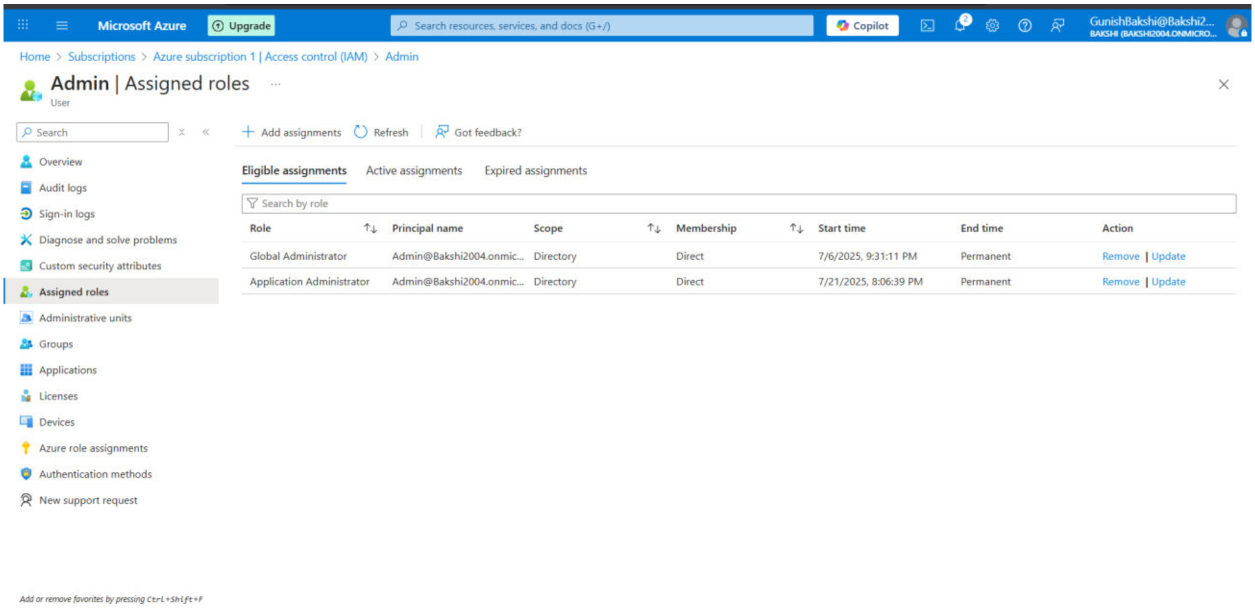
2 4000

Privileged

3

□ Name ↑↓	Type ↑↓	Role ↑↓	Scope ↑↓	State ↑↓	End time ↑↓
Owner (3)					
□ Admin be8554a8-232c...	User	Owner	This resource	Active time-bound	7/9/2025, 11:50:30 PM
□ Admin be8554a8-232c...	User	Owner	This resource	Eligible time-bound	7/9/2026, 10:35:30 PM
□ Gunish Bakshi edc95a87-3e32...	User	Owner	This resource	Active Permanent	Permanent

Showing 1 - 3 of 3 results.



Role ↑↓	Principal name	Scope ↑↓	Membership ↑↓	Start time	End time	Action
Global Administrator	Admin@Bakshi2004.onmic...	Directory	Direct	7/6/2025, 9:31:11 PM	Permanent	Remove | Update
Application Administrator	Admin@Bakshi2004.onmic...	Directory	Direct	7/21/2025, 8:06:39 PM	Permanent	Remove | Update

Summary of This Step

- Entra role settings configured for JIT activation
- Users assigned as **eligible** to different roles
- Permanent access only granted to break-glass accounts