

# Step 4: Configure Azure Resources in PIM

## Objective

Enable PIM for **Azure resource roles** such as Virtual Machine Contributor, Network Contributor, etc., and assign eligible users with role activation settings similar to Entra roles.

## 1. What Are Azure Resource Roles?

Azure resource roles (RBAC roles) control access to Azure resources like:

- Virtual Machines
- Resource Groups
- Storage Accounts
- Virtual Networks

With PIM, you can make these role assignments **Just-In-Time** by configuring them as **eligible** and requiring activation.

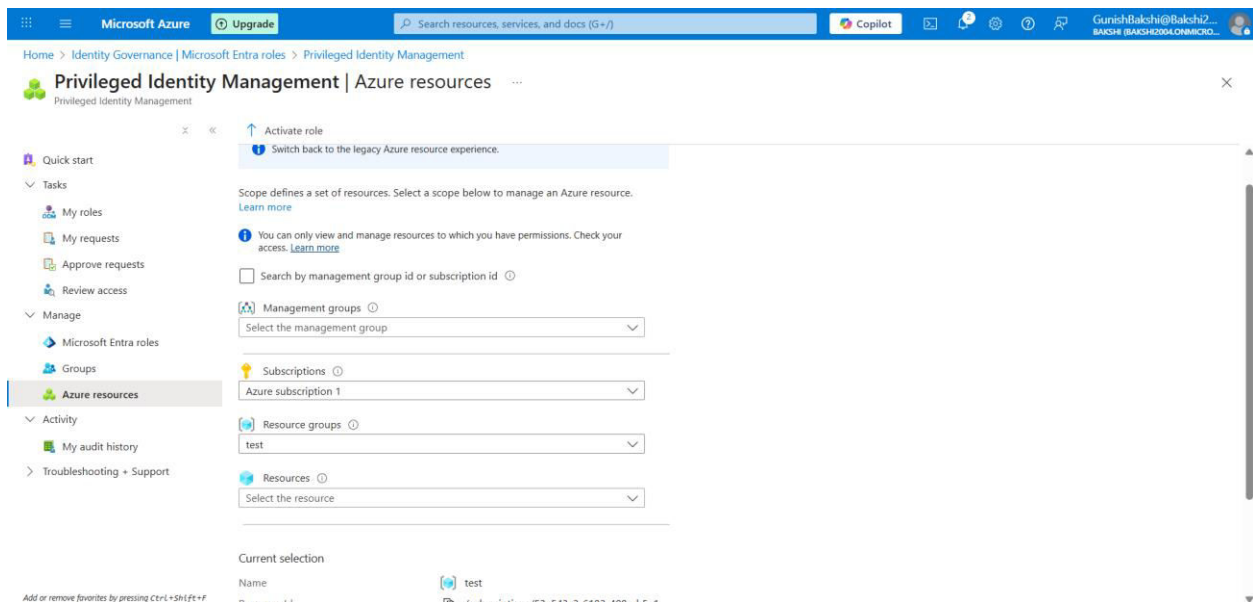
A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)

All   Job function roles   Privileged administrator roles					
Search by role name, description, permission, or ID					
		Type : All	Category : All		
<input type="checkbox"/> Name ↑↓	Description ↑↓	Type ↑↓	Category ↑↓	Details	
<input type="checkbox"/> Owner	Grants full access to manage all resources, including the ability to assign roles in Azur...	BuiltInRole	General	<a href="#">View</a>	***
<input type="checkbox"/> Contributor	Grants full access to manage all resources, but does not allow you to assign roles in A...	BuiltInRole	General	<a href="#">View</a>	***
<input type="checkbox"/> Reader	View all resources, but does not allow you to make any changes.	BuiltInRole	General	<a href="#">View</a>	***
<input type="checkbox"/> Access Review Operator Service ...	Lets you grant Access Review System app permissions to discover and revoke access ...	BuiltInRole	None	<a href="#">View</a>	***
<input type="checkbox"/> AcrDelete	acr delete	BuiltInRole	Containers	<a href="#">View</a>	***
<input type="checkbox"/> AcrImageSigner	acr image signer	BuiltInRole	Containers	<a href="#">View</a>	***
<input type="checkbox"/> AcrPull	acr pull	BuiltInRole	Containers	<a href="#">View</a>	***
<input type="checkbox"/> AcrPush	acr push	BuiltInRole	Containers	<a href="#">View</a>	***
<input type="checkbox"/> AcrQuarantineReader	acr quarantine data reader	BuiltInRole	Containers	<a href="#">View</a>	***
<input type="checkbox"/> AcrQuarantineWriter	acr quarantine data writer	BuiltInRole	Containers	<a href="#">View</a>	***

## 2. Enable PIM for an Azure Subscription

### Steps:

1. Go to: **Azure Portal** → **Microsoft Entra ID** → **Identity Governance** → **PIM**
2. Click: **Azure Resources**
3. If prompted, click **Discover Resources**
4. Select the **Subscription** where you want to enable PIM
5. Click **Manage Resource** → **Enable PIM**

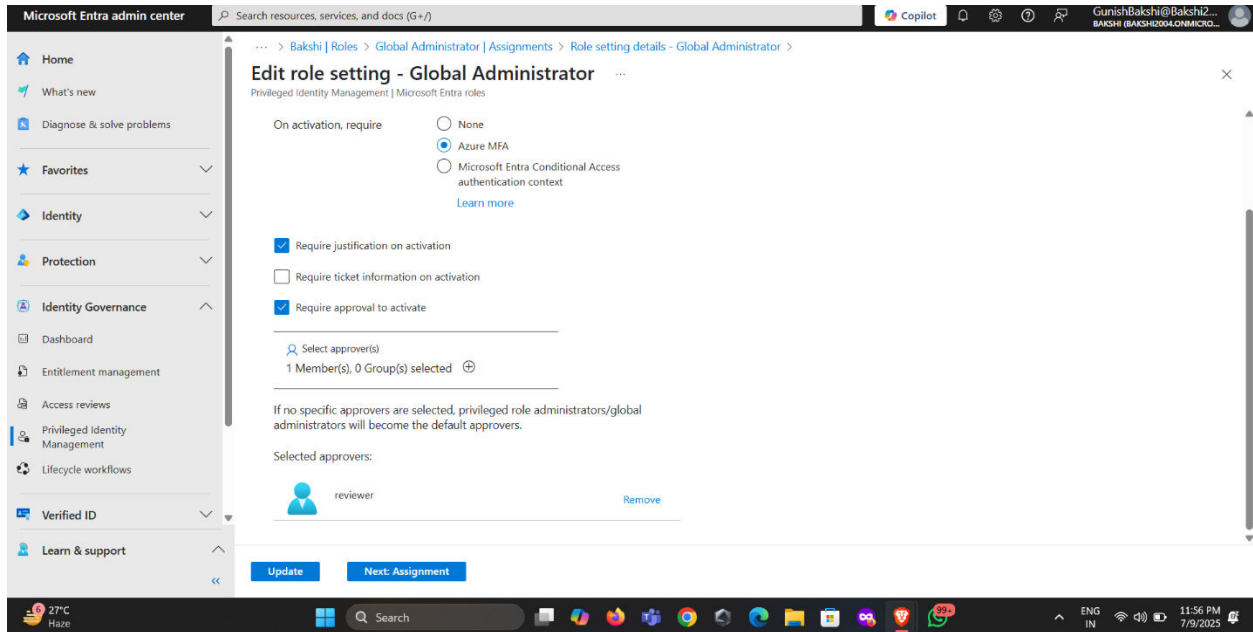


## 3. Configure Role Settings

1. After enabling PIM, select the **Subscription**
2. Click **Roles**
3. Choose a role
4. Click **Settings** → **Edit**
5. Configure:
  - **Activation duration** (e.g., 1 hour)

- **MFA requirement:** Yes
- **Approval required:** Yes/No
- **Justification required:** Yes

## 6. Save settings



## 4. Assign Eligible Resource Roles

### Steps:

1. In the PIM dashboard under Azure Resources, click **Roles**
2. Choose a role
3. Click **Add Assignment**
4. Select:
  - **User** (e.g., admin@Bakshi2004.onmicrosoft.com)
  - **Assignment type:** Eligible
  - **Scope:** Subscription or Resource Group
5. Click **Assign**

Microsoft Azure Upgrade Search resources, services, and docs (G+/) Copilot GunishBakshi@Bakshi2004.onmicrosoft.com

Home > Subscriptions > Azure subscription 1 | Access control (IAM) >

## Add role assignment

Role Members Conditions Assignment type Review + assign

**Selected role** Reader

**Assign access to** ☒ User, group, or service principal ☐ Managed identity

**Members** + Select members

Name	Object ID	Type
No members selected		

**Description** Optional

Review + assign Previous Next

Select members

Search by name or email address

- Admin Admin@Bakshi2004.onmicrosoft.com
- BreakGlass BreakGlass@Bakshi2004.onmicrosoft.com
- Gunish Bakshi GunishBakshi@Bakshi2004.onmicrosoft.com
- Privileged-BAKSHI-Group 3a49f545-fb61-4ac7-867b-38712376af1c
- Reviewer Reviewer@Bakshi2004.onmicrosoft.com

Selected members:

- Reviewer Reviewer@Bakshi2004.onmicrosoft.com

Select Close

If you have Microsoft Entra Privileged Identity Management (PIM), you can use eligible assignments to provide just-in-time access to role. Users with eligible and/or time-bound assignments must have a valid license. [Learn more](#)

**Selected role** Reader

**Assignment type** ☒ Eligible (Recommended) Member must activate to use this role for a limited period of time. ☐ Active Member can use this role at any time.

**Assignment duration** ☐ Permanent Assignment has no end date or time. ☒ Time bound Assignment has an end date and time.

**Start date and time\*** 07/21/2025 8:25 PM

**End date and time\*** 07/21/2026 8:25 PM

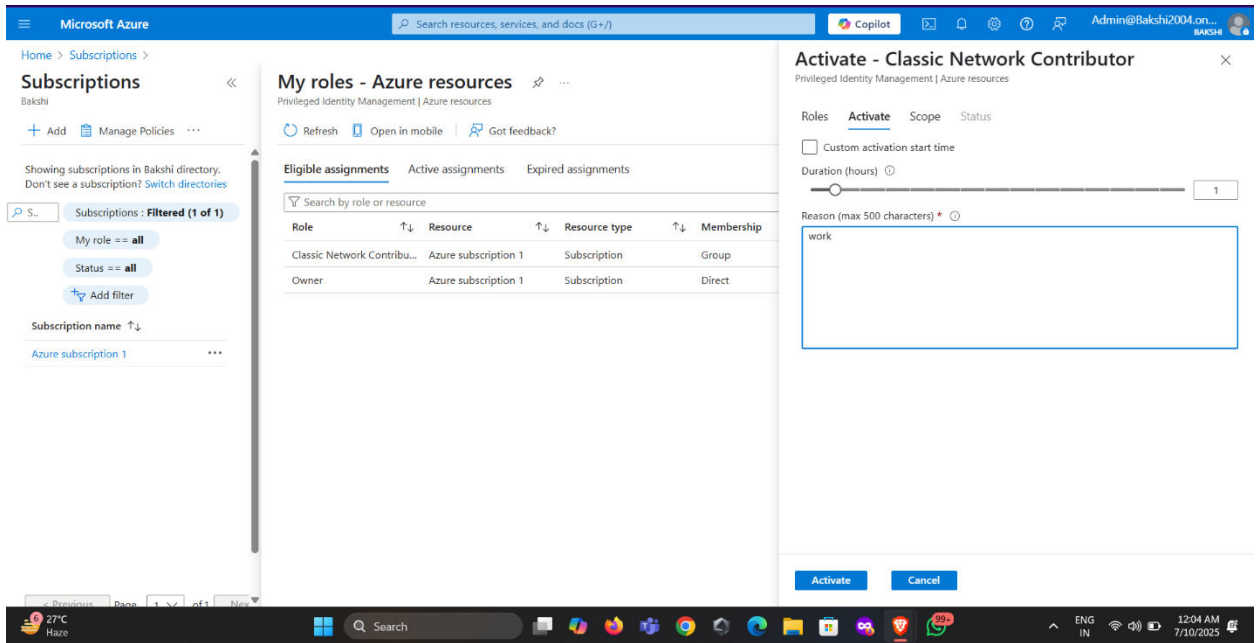
Configure Privileged Identity Management (PIM) policy

Privileged Identity Management (PIM) Policy defines whether permanent assignments can be created, maximum duration of time-bound assignments, roles activation requirements (approval, multifactor authentication, or Conditional Access authentication context), and other settings.

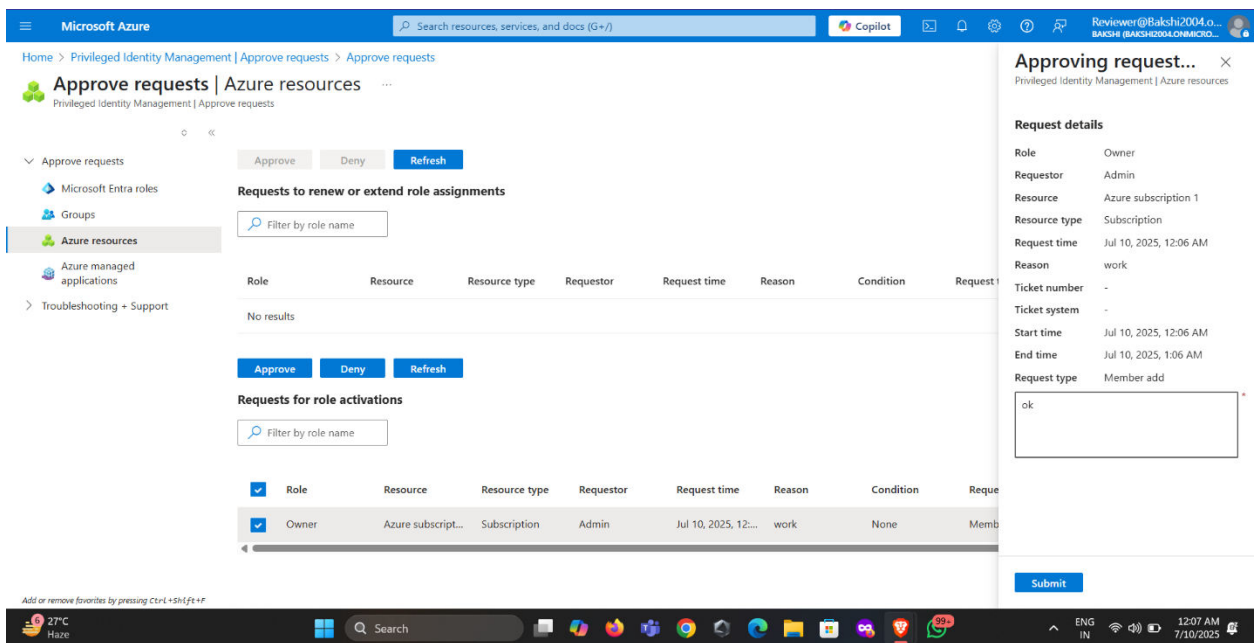
## Test Role Activation

You can test this just like Entra roles:

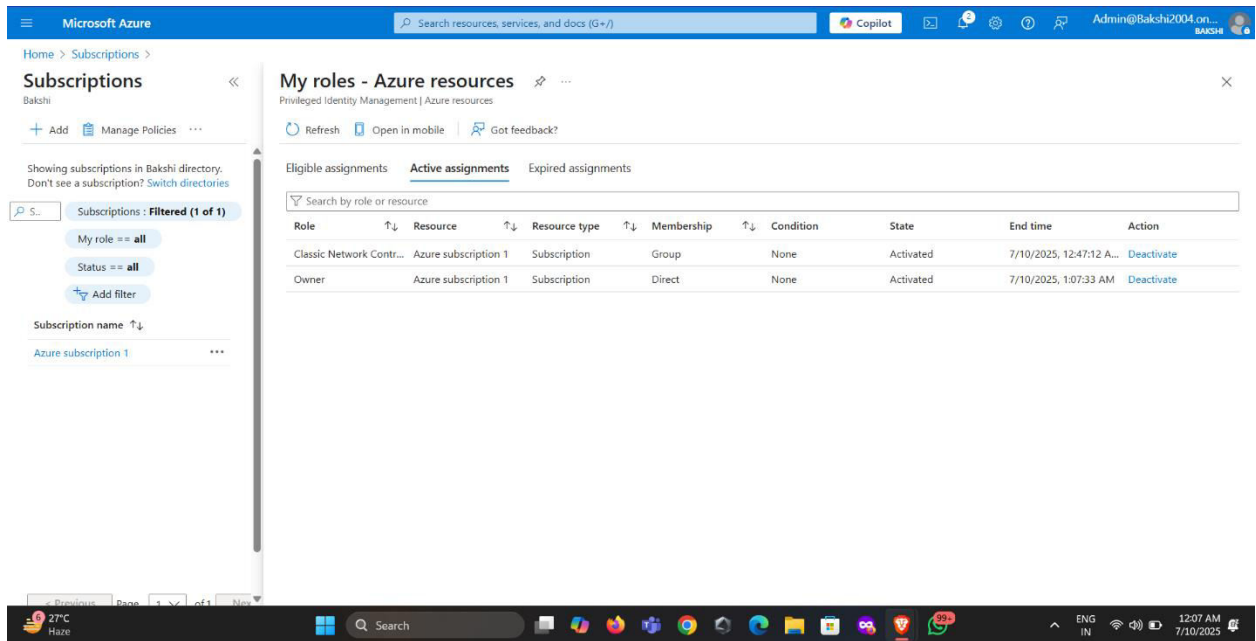
1. Sign in as the eligible user
2. Navigate to **PIM** → **My Roles**
3. Activate the assigned Azure role
4. Provide justification and complete MFA if required



- Admin Request to activate the JIT role.



- Reviewer activating the role



- The activated role for the admin.

## Summary of This Step

- PIM enabled for Azure subscription and resources
- Roles configured for Just-In-Time activation
- Users assigned as eligible for Azure RBAC roles