Step 4: Configure Azure Resources in PIM

Objective

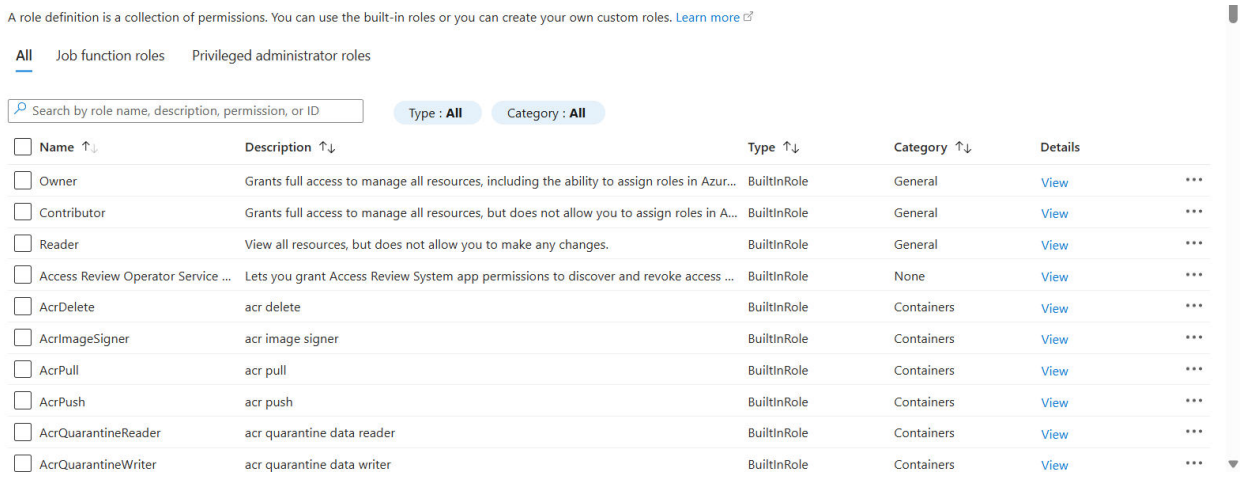
Enable PIM for **Azure resource roles** such as Virtual Machine Contributor, Network Contributor, etc., and assign eligible users with role activation settings similar to Entra roles.

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

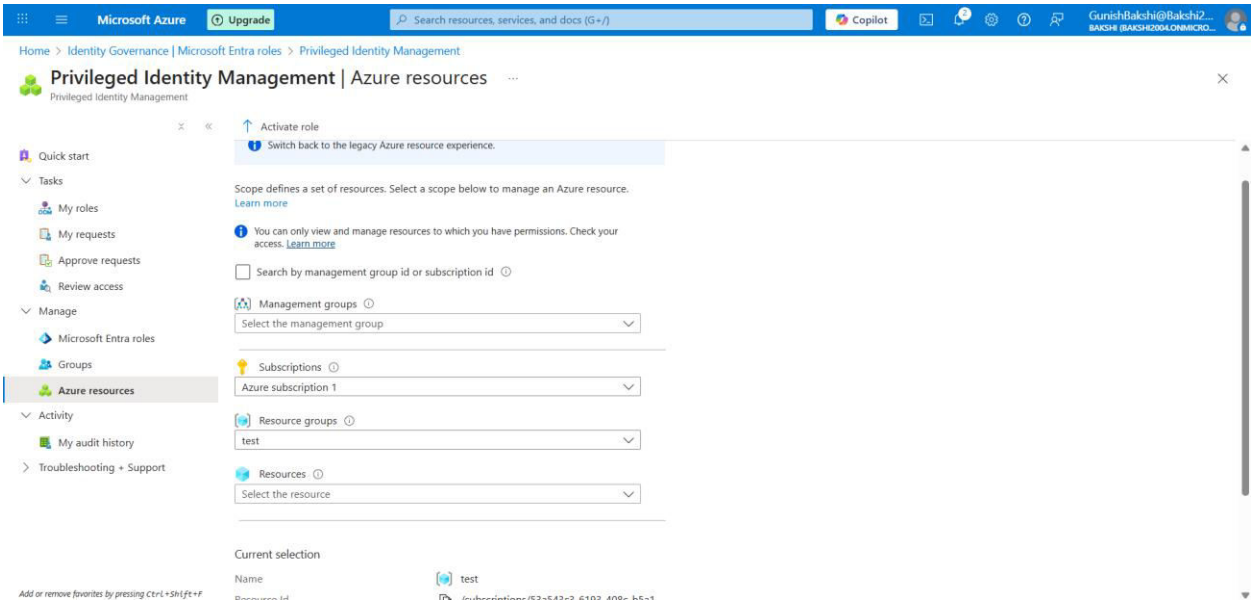
With PIM, you can make these role assignments **Just-In-Time** by configuring them as **eligible** and requiring activation.



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**

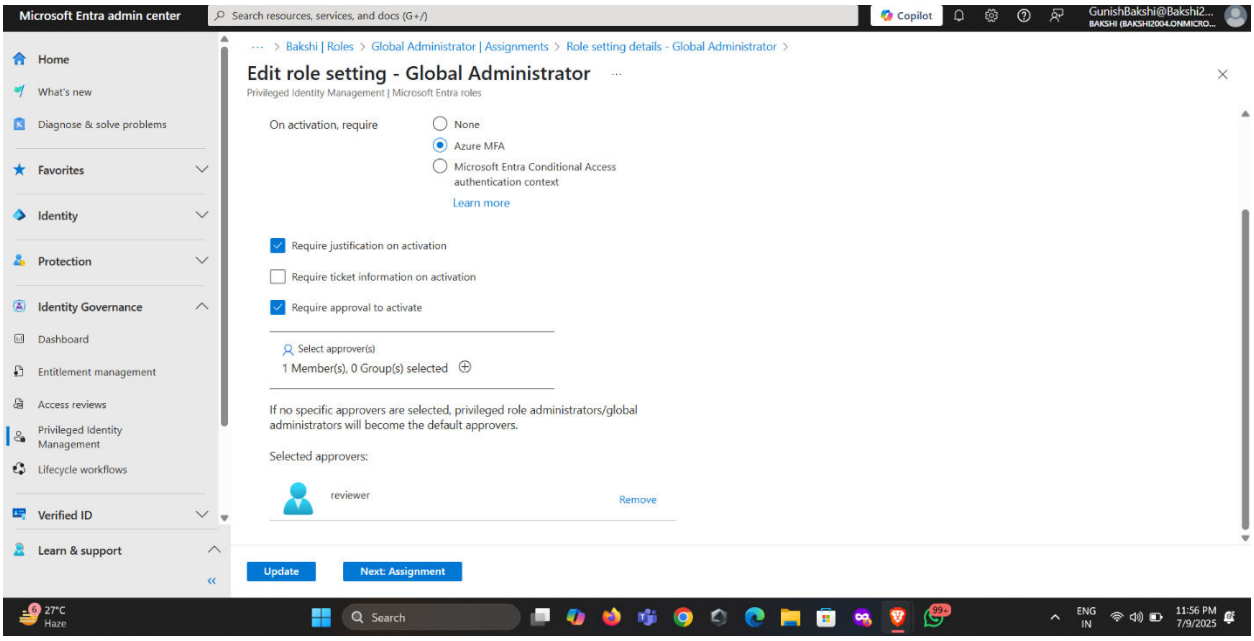


3. Configure Role Settings

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

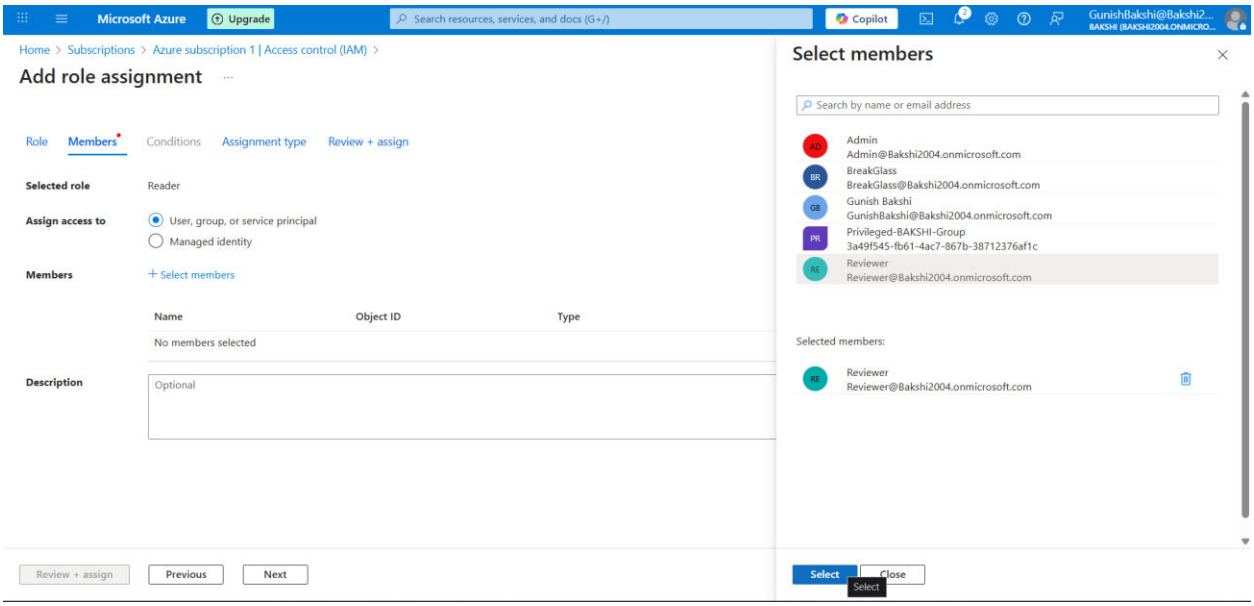
6. Save settings

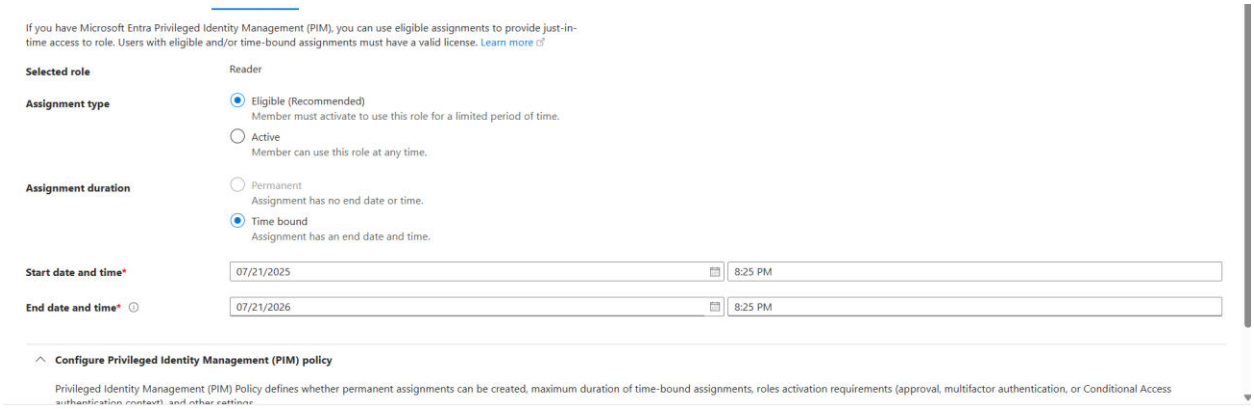


4. Assign Eligible Resource Roles

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**

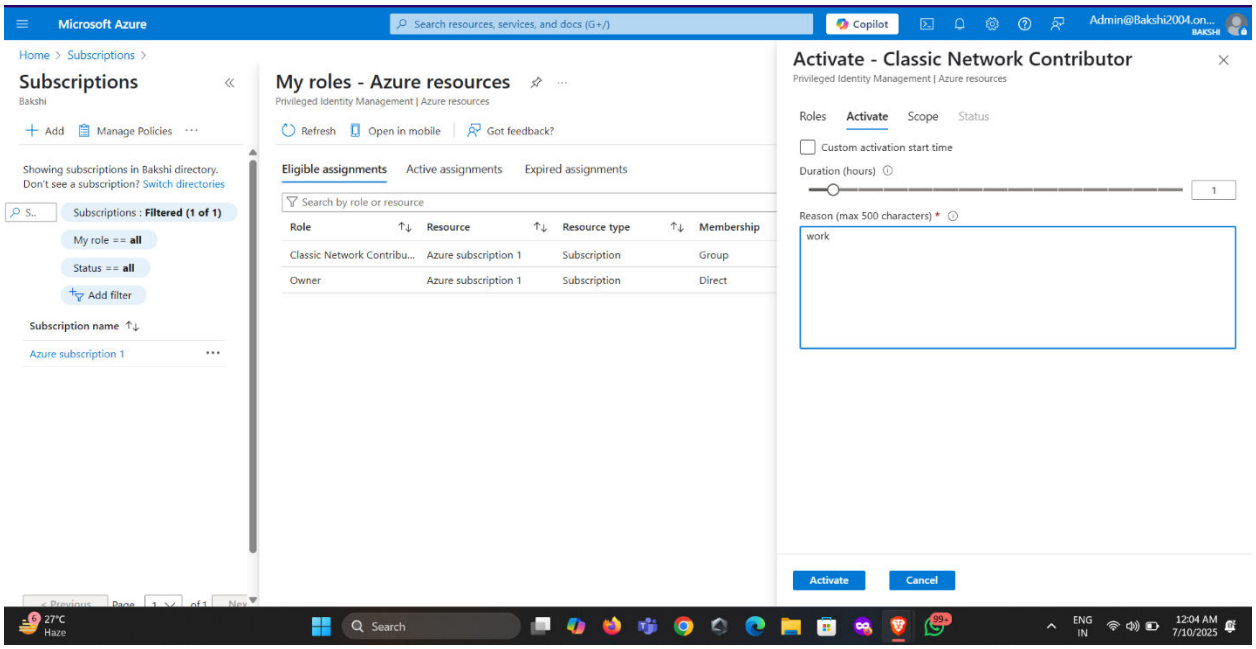




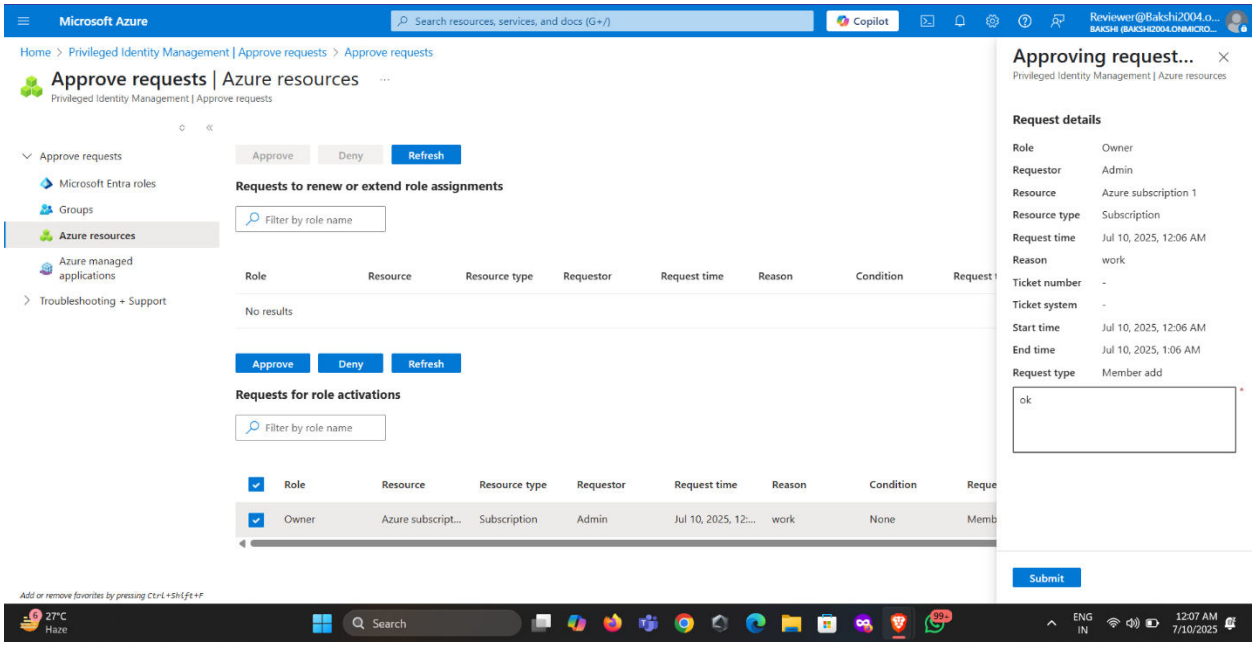
Test Role Activation

You can test this just like Entra roles:

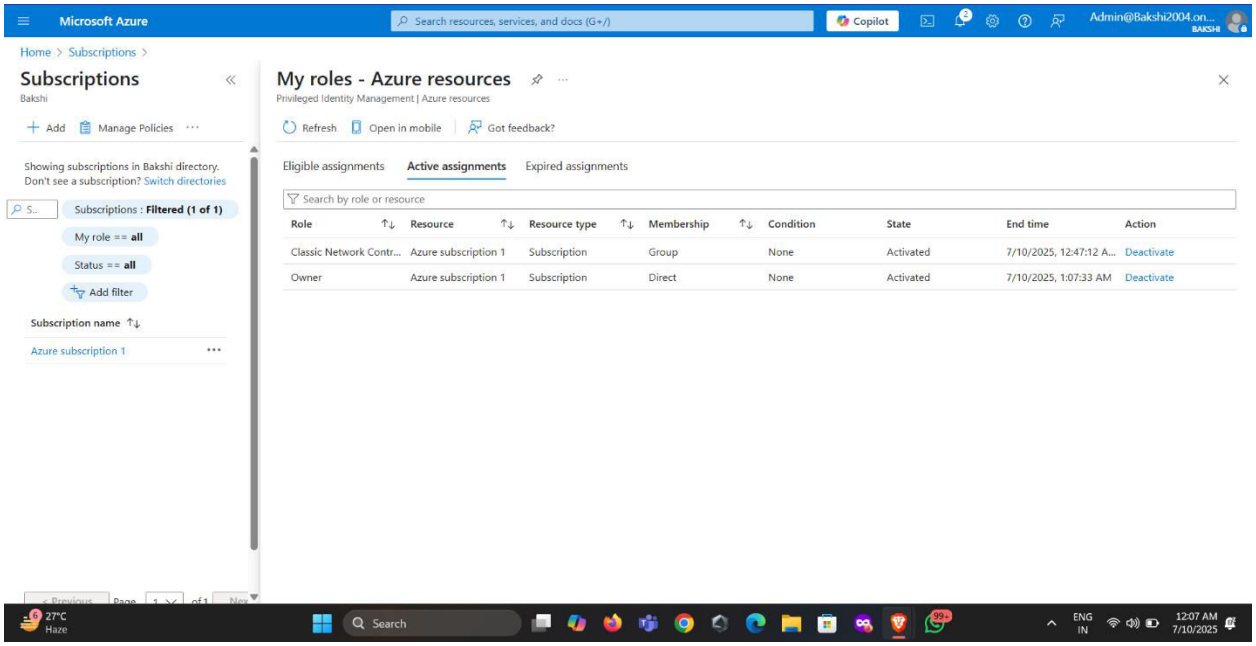
1. Sign in as the eligible user
2. Navigate to **PIM → My Roles**
3. Activate the assigned Azure role
4. Provide justification and complete MFA if required



- 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