

Step 5: Configure Privileged Access Groups

Objective

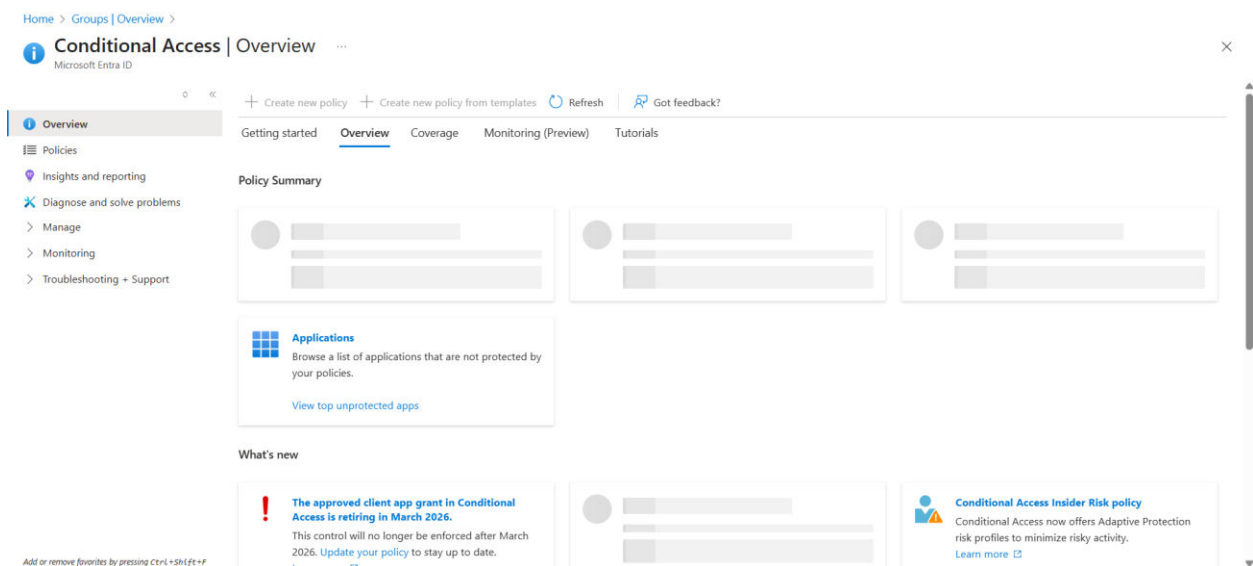
Create and configure **Privileged Access Groups** in Microsoft Entra ID to manage multiple role assignments as a single unit and enable Just-In-Time access for groups.

1. What Are Privileged Access Groups?

Privileged Access Groups allow you to:

- Assign users to **multiple Entra roles** through a single group membership.
- Make group **membership eligible**, requiring activation.
- Apply PIM policies like approval, MFA, and justification to group membership.

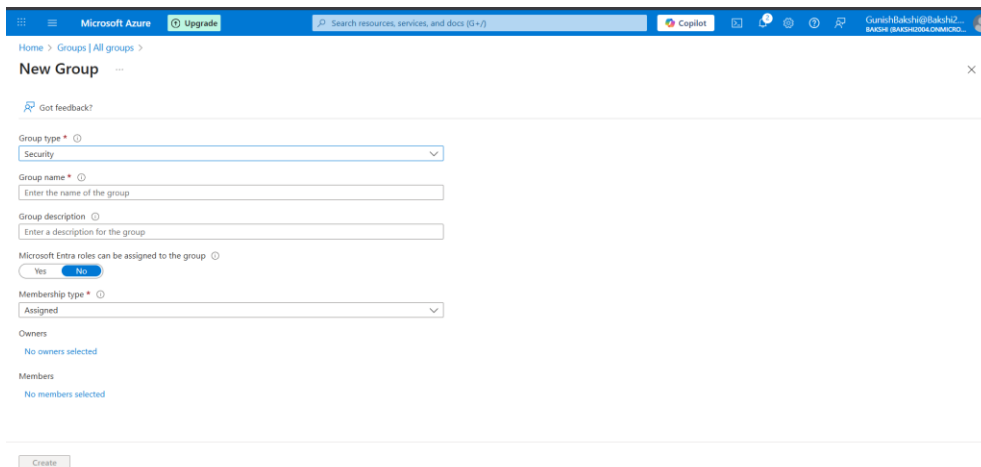
These are highly useful when many users need the same set of privileged roles temporarily.



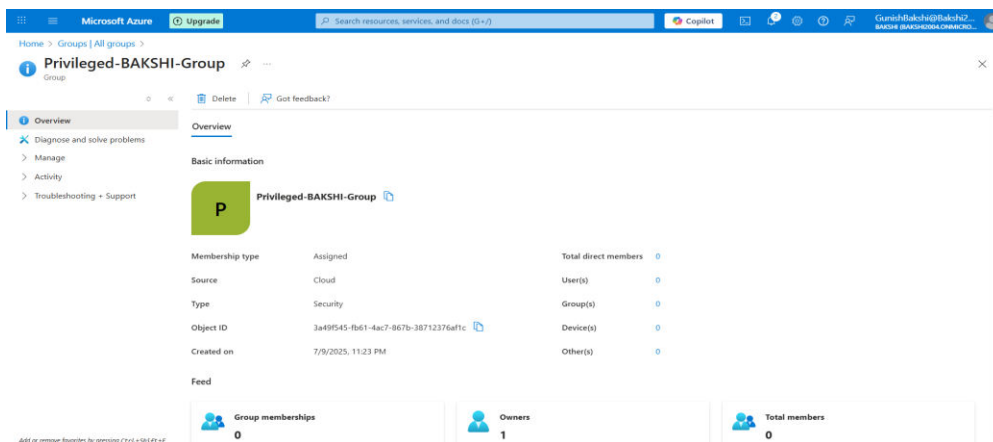
2. Create a Microsoft Entra Security Group

Steps:

1. Go to: Microsoft Entra ID → Groups
2. Click + New group
3. Set the following:
 - Group type: Security
 - Group name: e.g., PrivilegedSupportGroup
 - Membership type: Assigned
 - Azure AD roles can be assigned to the group: Yes
4. Click Create



The screenshot shows the 'New Group' form in the Microsoft Azure portal. The form is titled 'New Group' and includes a 'Got feedback?' link. The 'Group type' dropdown is set to 'Security'. The 'Group name' field is empty, with a placeholder 'Enter the name of the group'. The 'Group description' field is also empty, with a placeholder 'Enter a description for the group'. The 'Microsoft Entra roles can be assigned to the group' toggle is set to 'Yes'. The 'Membership type' dropdown is set to 'Assigned'. Below these fields, there are sections for 'Owners' and 'Members', both showing 'No owners selected' and 'No members selected' respectively. At the bottom, there is a 'Create' button.



The screenshot shows the 'Privileged-BAKSHI-Group' overview page in the Microsoft Azure portal. The page has a left sidebar with navigation links: 'Overview', 'Diagnose and solve problems', 'Manage', 'Activity', and 'Troubleshooting + Support'. The main content area is titled 'Privileged-BAKSHI-Group' and includes a 'Basic information' section. This section displays the group's details in a table-like format:

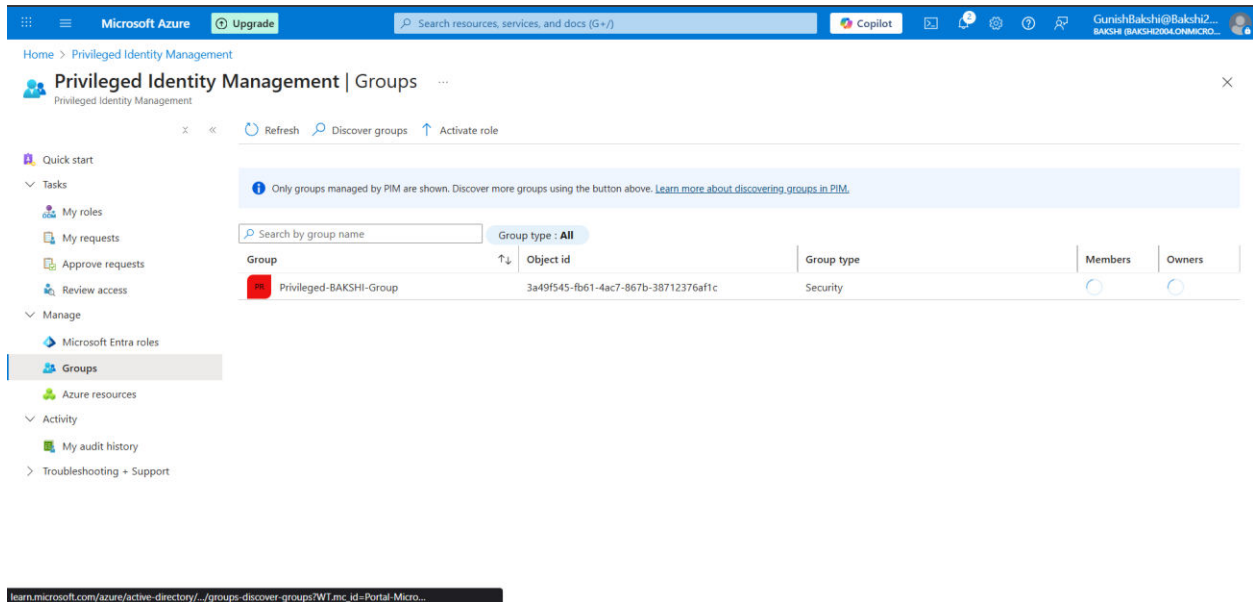
Basic information	
Membership type	Assigned
Source	Cloud
Type	Security
Object ID	3a49f545-fb61-4ac7-867b-38712376affc
Created on	7/9/2025, 11:23 PM
Total direct members	0
User(s)	0
Group(s)	0
Device(s)	0
Other(s)	0

Below the 'Basic information' section, there is a 'Feed' section with three cards: 'Group memberships' (0), 'Owners' (1), and 'Total members' (0). At the bottom, there is a note: 'Add or remove favorites by pressing Ctrl + Shift + F'.

3. Enable the Group for PIM

Steps:

1. Go to: PIM → Groups
2. Click Discover Groups
3. Select the group you created (e.g., PrivilegedSupportGroup)
4. Click Enable PIM

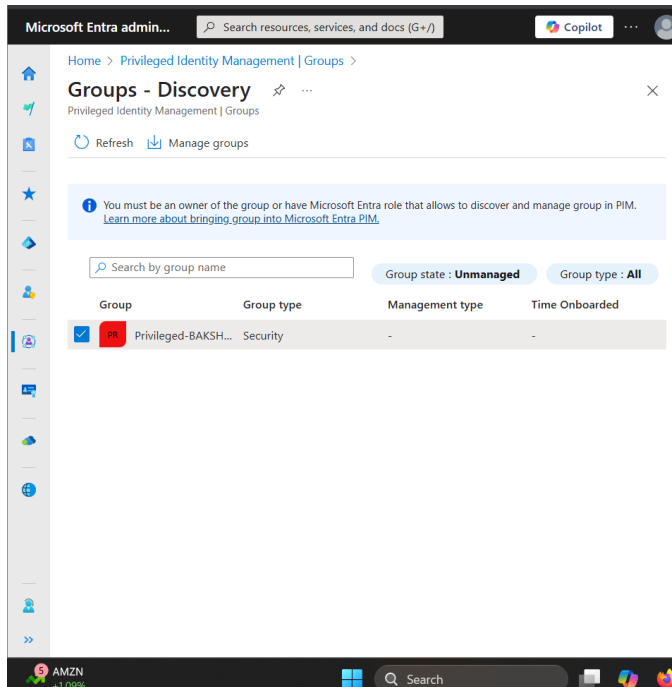


The screenshot displays the Microsoft Azure Privileged Identity Management (PIM) Groups page. The page header shows the Microsoft Azure logo and the 'Upgrade' button. The main title is 'Privileged Identity Management | Groups'. Below the title, there are buttons for 'Refresh', 'Discover groups', and 'Activate role'. A message states: 'Only groups managed by PIM are shown. Discover more groups using the button above. [Learn more about discovering groups in PIM.](#)'

The page includes a search bar labeled 'Search by group name' and a dropdown menu for 'Group type' set to 'All'. Below this is a table with the following columns: Group, Object id, Group type, Members, and Owners. The table contains one entry: 'Privileged-BAKSHI-Group' with Object id '3a49f545-fb61-4ac7-867b-38712376af1c' and Group type 'Security'. The 'Members' and 'Owners' columns show empty circles.

The left sidebar contains a 'Quick start' section with links to 'My roles', 'My requests', 'Approve requests', and 'Review access'. Below this is a 'Manage' section with links to 'Microsoft Entra roles', 'Groups' (selected), 'Azure resources', 'Activity', 'My audit history', and 'Troubleshooting + Support'.

The URL bar at the bottom shows: learn.microsoft.com/azure/active-directory/privileged-identity-management/pim-groups-discover-groups?WT.mc_id=Portal-Microsoft-Azure-Active-Directory



4. Configure Group Membership Settings

1. In PIM under **Groups**, select the group
2. Click **Settings**
3. Configure:
 - **Require justification:** Yes
 - **Require approval:** Optional (add reviewer@Bakshi2004.onmicrosoft.com)
 - **MFA required:** Yes
 - **Activation duration:** e.g., 1 hour
4. Click **Update**

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

GunishBakshi@Bakshi2...
BAKSHI (BAKSHI2004.0NMICRO...

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

Add role assignment

RoleMembersConditionsAssignment typeReview + assign

Role

Classic Network Contributor

Scope

/subscriptions/53a543c3-6193-408c-b5a1-497b526968ef

Members

Name	Object ID	Type
Privileged-BAKSHI-Group	3a49f545-fb61-4ac7-867b-38712376af1c	Group

Description

No description

Assignment type

Eligible

Assignment duration

Time bound

Start date and time

7/9/2025, 11:37:46 PM

End date and time

7/9/2026, 11:37:46 PM

Users with eligible and/or time-bound assignments must have a valid license.

Review + assign

Previous

Next

Feedback

Microsoft Azure

Upgrade

Search resources, services, and docs (G+)

Copilot

GunishBakshi@Bakshi2...
BAKSHI (BAKSHI2004.0NMICRO...

Home > Privileged Identity Management | Groups > Privileged-BAKSHI-Group | Settings > Role setting details - Member >

Edit role setting - Member

Privileged Identity Management | Groups

ActivationAssignmentNotification

Activation maximum duration (hours)

0-----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)

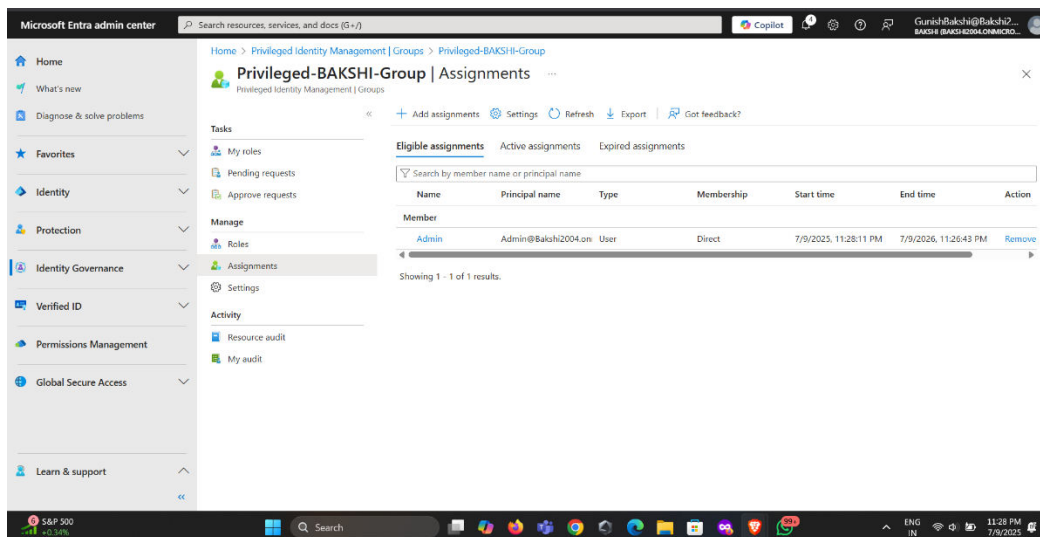
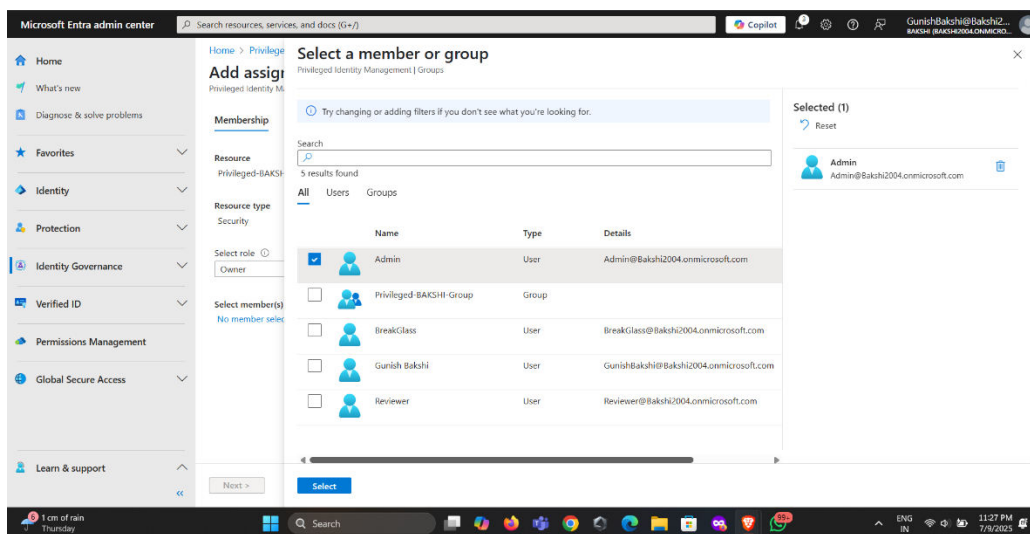
1 Member(s), 0 Group(s) selected

Update

Next: Assignment

5. Assign Eligible Group Members

1. In PIM → Groups → Select your group
2. Click Add assignments
3. Choose:
 - User (e.g., admin@Bakshi2004.onmicrosoft.com)
 - Assignment type: Eligible



Summary of This Step

- Privileged Access Group created and PIM-enabled
- Just-In-Time membership settings configured
- Group assigned to Microsoft Entra roles
- Eligible user added to group