

Step 6: Set Up PIM Requests and Approval Process

Objective

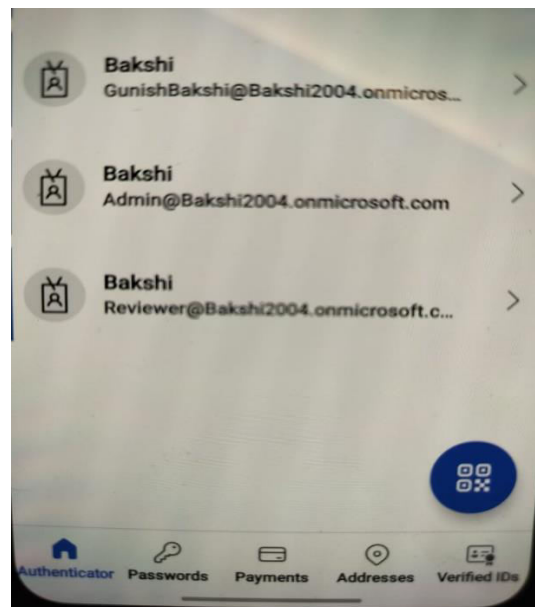
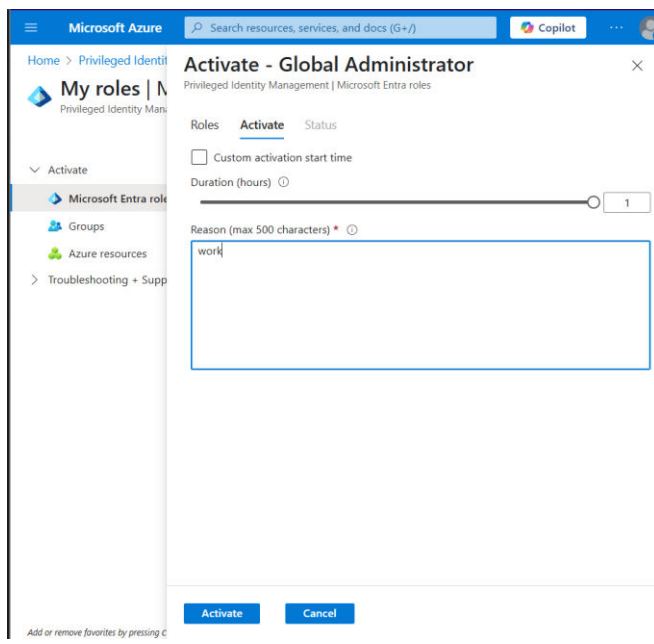
Test and configure the approval workflow for role and group activations in Microsoft Entra Privileged Identity Management (PIM).

1. Role Activation Workflow in PIM

When a user is assigned an eligible role or group, they must request activation. You can configure:

- MFA requirements
- Justification
- Approval workflow

This ensures users activate privileges only when needed and under control.

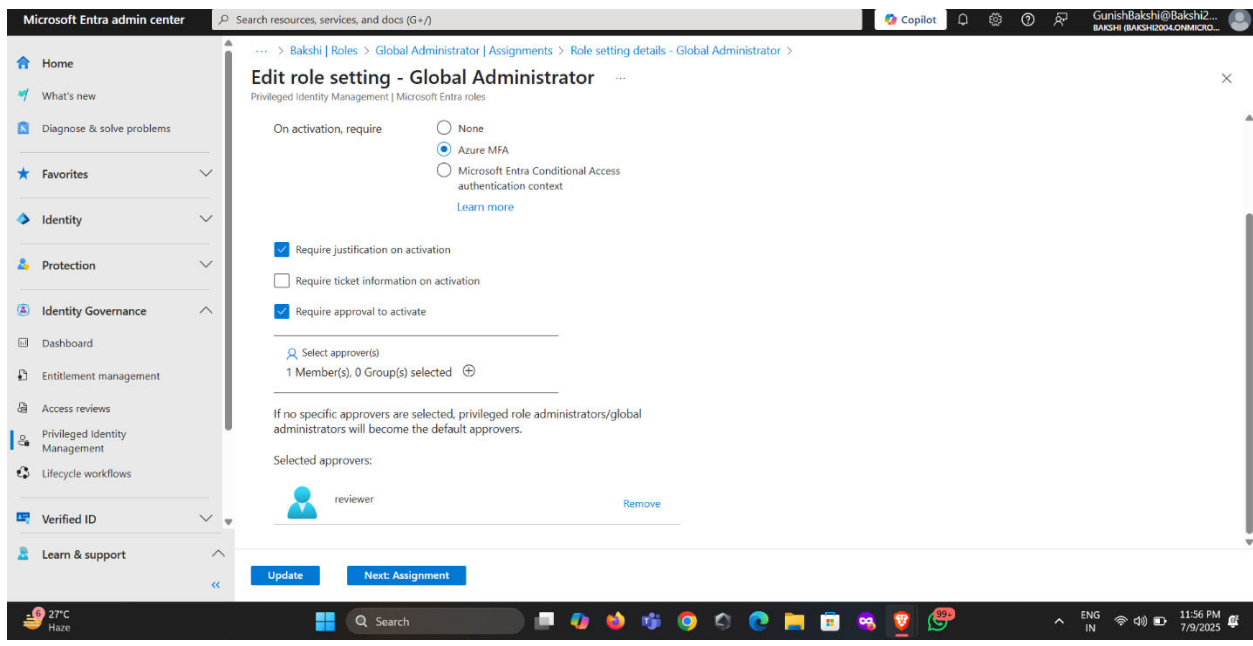


2. Set Up Approvers for Roles and Groups

Steps:

1. Go to PIM → Microsoft Entra roles (or PIM → Groups)
2. Select the role or group you want to configure
3. Click Settings → Edit
4. Enable:
 - Require approval to activate → Yes
 - Select approvers → Add
reviewer@Bakshi2004.onmicrosoft.com
 - Require justification → Yes
 - Require MFA to activate → Yes
5. Click Update

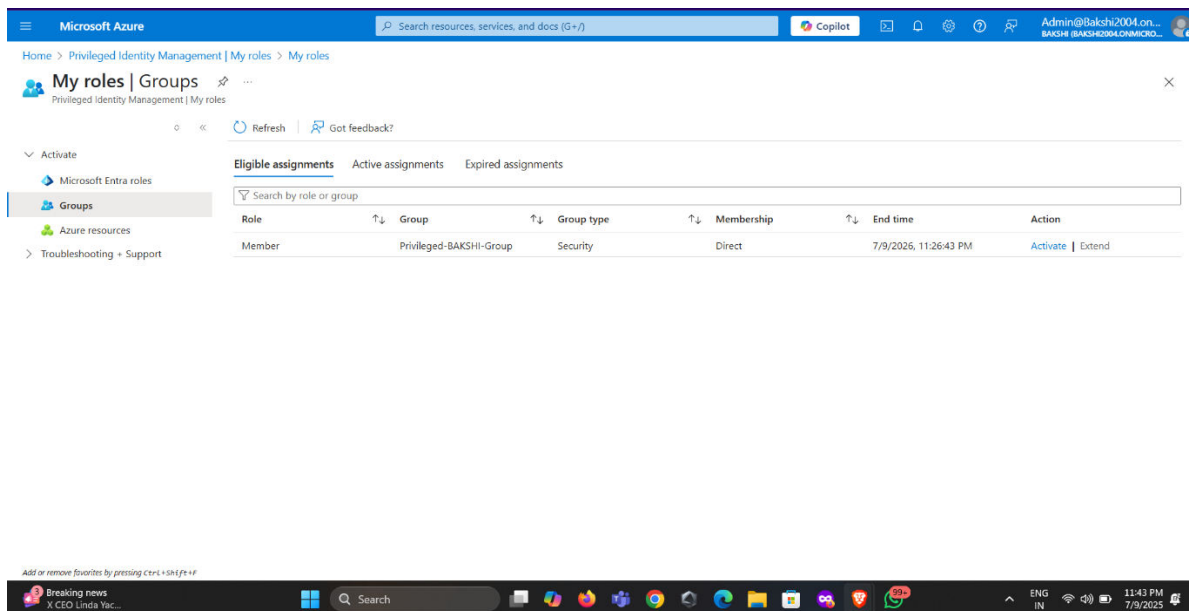
Repeat for each role/group that should require approval.



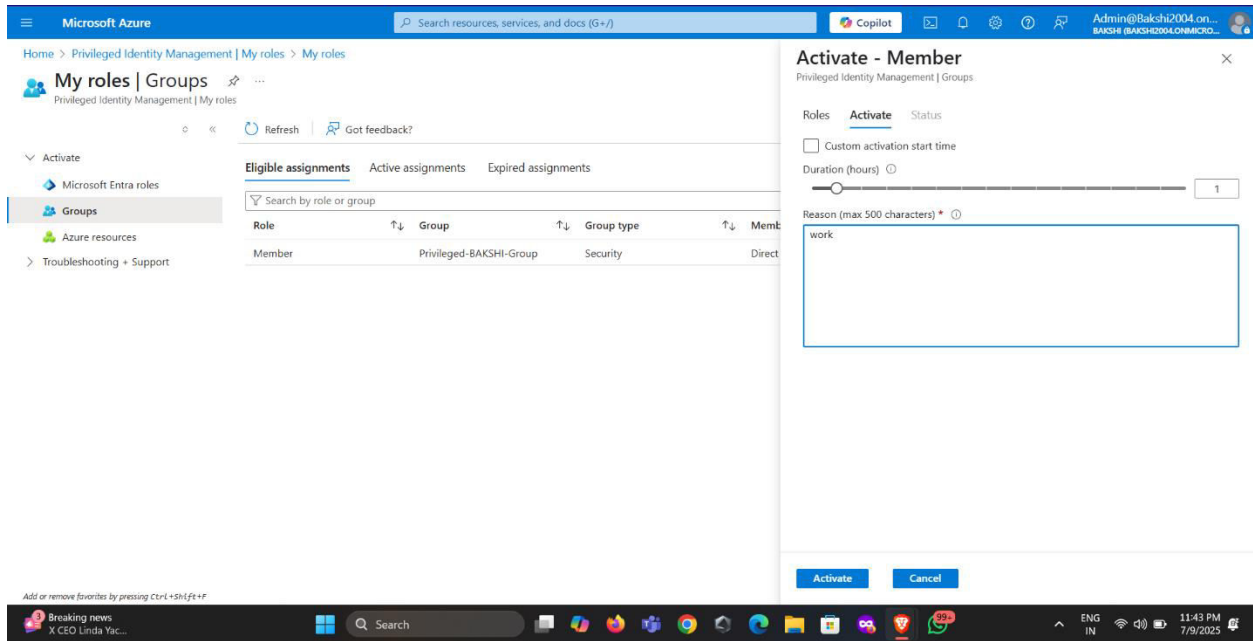
3. Request Activation (as eligible user)

Steps:

1. Sign in as admin@Bakshi2004.onmicrosoft.com (eligible user)
2. Go to: **PIM** → **My Roles** or **PIM** → **My Groups**
3. Click **Activate** next to an eligible role or group
4. Provide:
 - Justification
 - Complete MFA
5. Submit the activation request



- Selecting an eligible role (member of the privileged group)



- Sending an activation request.

4. Approve or Deny Requests (as reviewer)

Steps:

1. Sign in as reviewer@Bakshi2004.onmicrosoft.com
2. Go to: **PIM** → **Approvals**
3. View pending requests
4. Click:
 - Approve or Deny
 - Optionally add a reason

The requesting user will be notified upon approval.

Microsoft Azure

Home > Privileged Identity Management | Approve requests > Approve requests

Approve requests | Azure resources

Privileged Identity Management | Approve requests

Approve requests

- Microsoft Entra roles
- Groups
- Azure resources**
- Azure managed applications
- Troubleshooting + Support

Approve Deny Refresh

Requests to renew or extend role assignments

Filter by role name

Role	Resource	Resource type	Requestor	Request time	Reason	Condition	Request
No results							

Approve Deny Refresh

Requests for role activations

Filter by role name

Role	Resource	Resource type	Requestor	Request time	Reason	Condition	Request
Owner	Azure subscript...	Subscription	Admin	Jul 10, 2025, 12...	work	None	Memb

Approving request...

Privileged Identity Management | Azure resources

Request details

Role	Owner
Requestor	Admin
Resource	Azure subscription 1
Resource type	Subscription
Request time	Jul 10, 2025, 12:06 AM
Reason	work
Ticket number	-
Ticket system	-
Start time	Jul 10, 2025, 12:06 AM
End time	Jul 10, 2025, 1:06 AM
Request type	Member add

ok

Submit

27°C
Haze

Search

12:07 AM
7/10/2025

- Reviewer approves

Microsoft Azure

Home > Privileged Identity Management > My roles

My roles | Groups

Privileged Identity Management | My roles

Refresh Got feedback?

Activate

- Microsoft Entra roles
- Groups
- Azure resources
- Troubleshooting + Support

Eligible assignments Active assignments Expired assignments

Search by role or group

Role	Group	Group type	Membership	State	End time	Action
Member	Privileged-BAKSHI-Group	Security	Direct	Activated	7/10/2025, 12:43:36 AM	Deactivate

AMZN
+1.53%

Search

11:45 PM
7/10/2025

- The group role is activated.

Admin activated the Owner role for the Azure subscription 1 subscription

View the activation history for this user in the Privileged Identity Management (PIM) portal.

[View history >](#)

Settings	Value
User or Group	Admin
Role	Owner
Resource	Azure subscription 1
Resource type	subscription
Activated by	Admin
Start	July 9, 2025 17:20 UTC
End	July 9, 2025 18:20 UTC
Justification	work

- Emails are also sent to the main setup account so that everything is accounted for

Summary of This Step

- Approval workflow configured for roles and groups
- Just-In-Time activations now require approval and MFA
- Roles tested with user and reviewer accounts