



Privileged Identity Management (PIM): Just-in-Time Access in Action

In a Zero Trust environment, even administrators must be challenged. Microsoft Entra PIM provides *time-bound*, *approval-based*, and *auditable* access to privileged roles — replacing standing permissions with on-demand elevation.

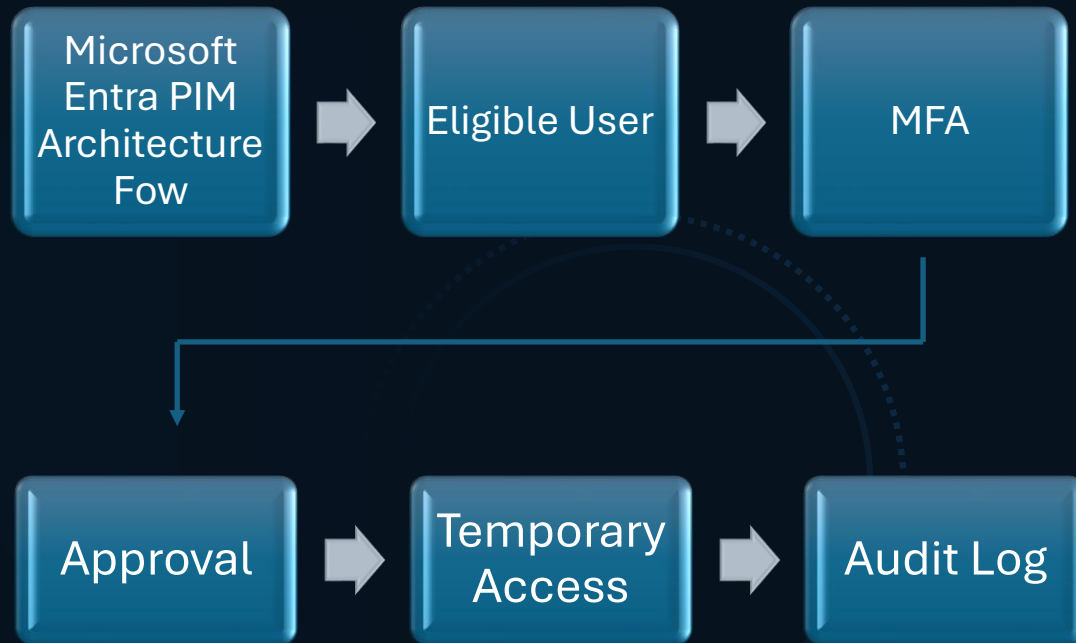
Key Concepts

- ✓ **Principle of Least Privilege** – Grant only what's required
- ✓ **Privilege Bracketing** – Access expires automatically
- ✓ **Just-in-Time Access** – Admins activate roles temporarily
- ✓ **Approval Workflow** – Another admin must approve
- ✓ **MFA & Justification** – Every activation is verified and logged

How PIM Works

- 1 Admin is marked *Eligible* for a role
- 2 User requests activation
- 3 MFA + justification + (optional) approval
- 4 Role becomes Active for set duration
- 5 Access auto-revoked & audited

Architecture Diagram



Microsoft Entra Privileged Identity Management (PIM)



Business Value

- ✓ **Stops** lateral movement
- ✓ **Enables** Zero Trust identity governance
- ✓ **Delivers** audit readiness and compliance

Assign an Admin Role with Just-in-Time Access

- Here we assign a user to the **User Administrator** role using Microsoft Entra PIM.
- The role is marked as **Eligible**, meaning the user must manually activate it when needed — ensuring that privileged access is temporary and intentional.

Microsoft Azure

Search resources, services, and doc

Home > Privileged Identity Management | Microsoft Entra roles > Perparims Cloud Solutions | Roles >

Add assignments

Privileged Identity Management | Microsoft Entra roles

Membership Setting

Assignment type ⓘ

☒ Eligible

☐ Active

Maximum allowed eligible duration is permanent.

☒ Permanently eligible

Assignment starts

Assignment ends

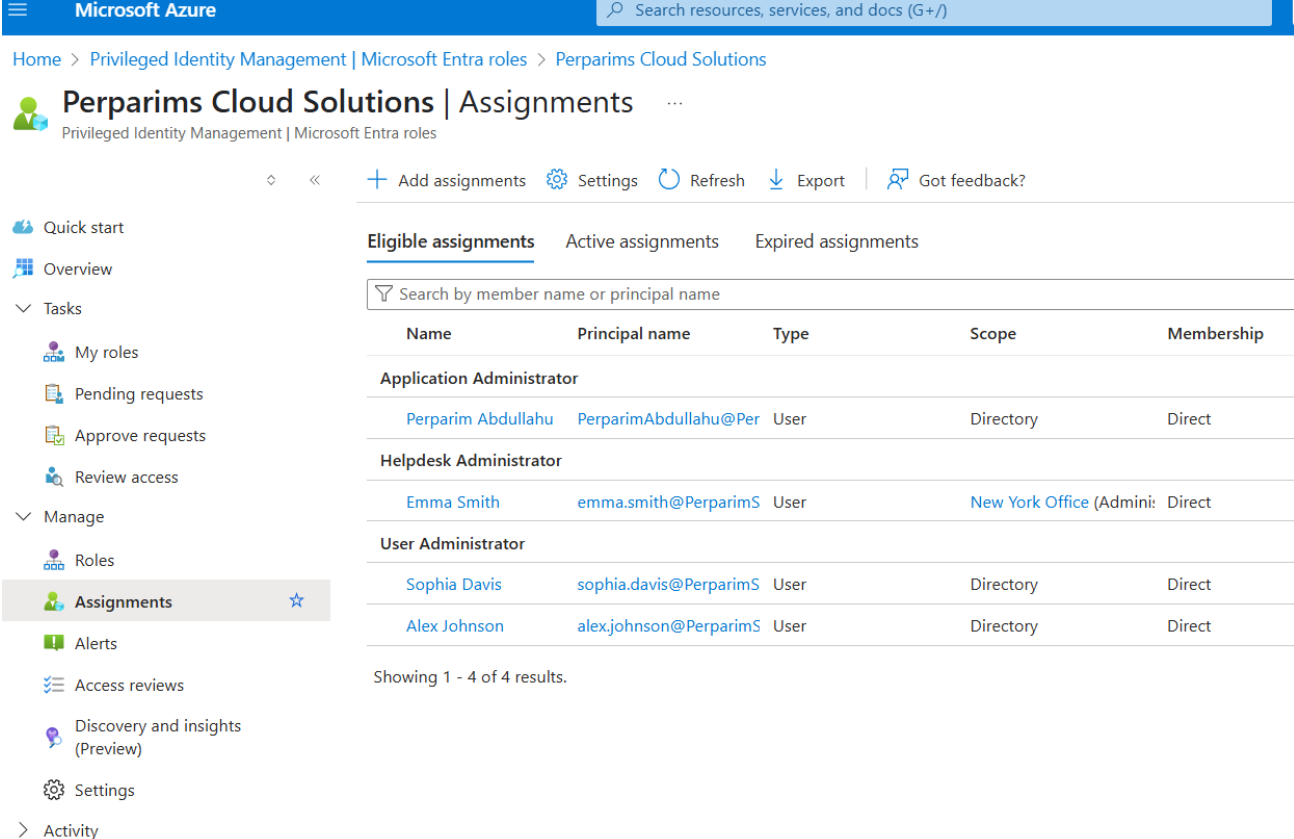
Tip: For higher control, you can configure a specific start and end window instead of permanently eligible.



(Permanently eligible shown for demo — time-bound options available)

How the User Activates Their Role in PIM

- Eligible users can view their roles in **Privileged Identity Management** under *My Roles* or *Assignments*.
- To gain access, they must click **Activate**, provide justification, and confirm their **MFA challenge**.
- Access is granted only for the configured time window — and everything is logged for audit.



Microsoft Azure

Search resources, services, and docs (G+/)

Home > Privileged Identity Management | Microsoft Entra roles > Perparims Cloud Solutions

Perparims Cloud Solutions | Assignments

Privileged Identity Management | Microsoft Entra roles

+ Add assignments Settings Refresh Export Got feedback?

Quick start Overview Tasks Manage

- My roles
- Pending requests
- Approve requests
- Review access
- Roles
- Assignments**
- Alerts
- Access reviews
- Discovery and insights (Preview)
- Settings
- Activity

Eligible assignments Active assignments Expired assignments


Search by member name or principal name

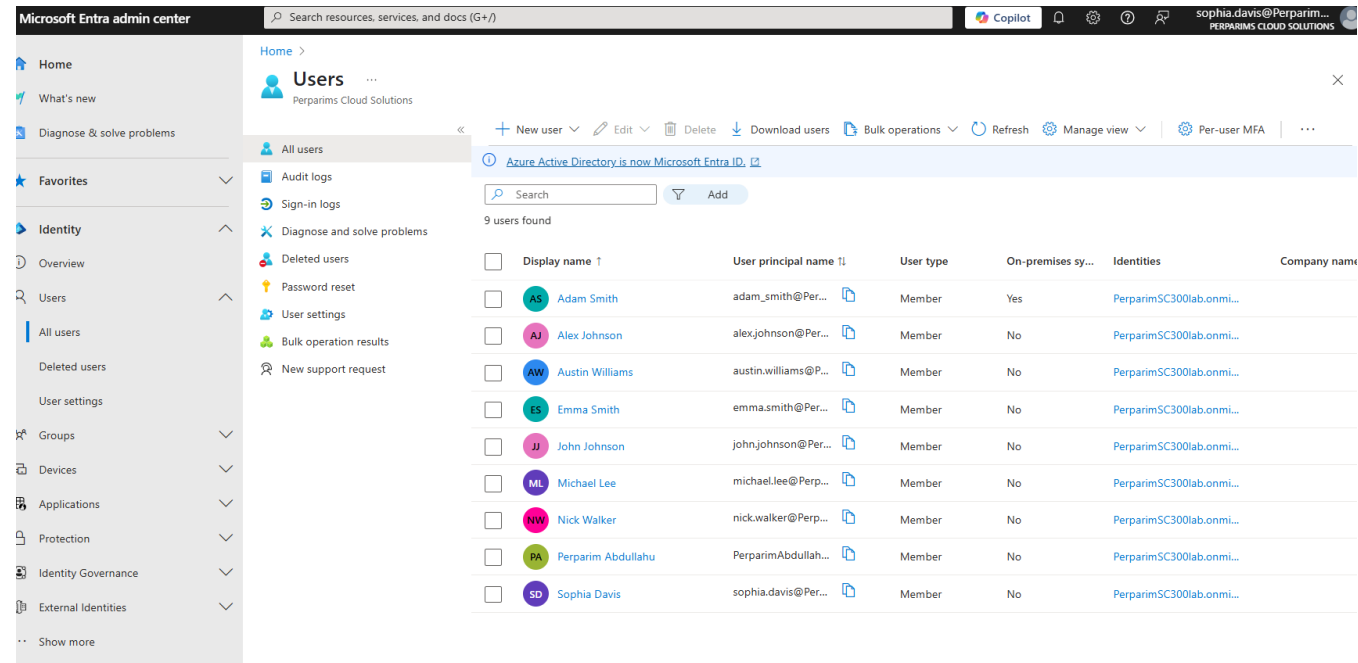
Name	Principal name	Type	Scope	Membership
Application Administrator				
Perparim Abdullahu	PerparimAbdullahu@Per	User	Directory	Direct
Helpdesk Administrator				
Emma Smith	emma.smith@PerparimS	User	New York Office (Admini:	Direct
User Administrator				
Sophia Davis	sophia.davis@PerparimS	User	Directory	Direct
Alex Johnson	alex.johnson@PerparimS	User	Directory	Direct

Showing 1 - 4 of 4 results.

Temporary Admin Access in Action

- After activating the *User Administrator* role, Sophia Davis can now see the **+ New user** option — something not available before.
- This confirms the role is active and privileges are granted — but only for the approved time window.

 Just-in-time access in action — secure, temporary, and auditable.



Secure Admin Access with Confidence

- ✅ Eliminate standing admin privileges
- 🔄 Grant temporary access only when needed
- 🔒 Enforce MFA, justification & time limits
- 🧠 Everything is logged for audit & compliance
- 📉 Reduces insider risk and accidental exposure

Start using Microsoft Entra PIM to protect your privileged roles — especially in hybrid or high-security environments. Add PIM to your Zero Trust and compliance strategy — and sleep easier.

With Microsoft Entra PIM, organizations can move from static admin rights to dynamic Just-in-Time access — achieving least privilege without losing agility.

