

# *Grant Just-in-Time Admin Access with Microsoft Entra PIM*

---

Enforce least privilege. Secure your environment.  
Maintain audit readiness.



# Why Use Privileged Identity Management (PIM)?

- 🔑 **Standing admin access = constant risk**
- 🕒 **JIT (Just-in-Time) access reduces attack surface**
- 🔒 Enforces **least privilege** by default
- ✅ Ensures admin rights are **temporary, approved, and auditable**
- 🛡️ Critical for **Zero Trust** and compliance readiness

No one should have permanent admin access — even admins.

# How Just-in-Time Access Works with PIM

---

 **Assign Role (Eligible)**

---

 **User Requests Activation**

---

 **Optional Approval Step**

---

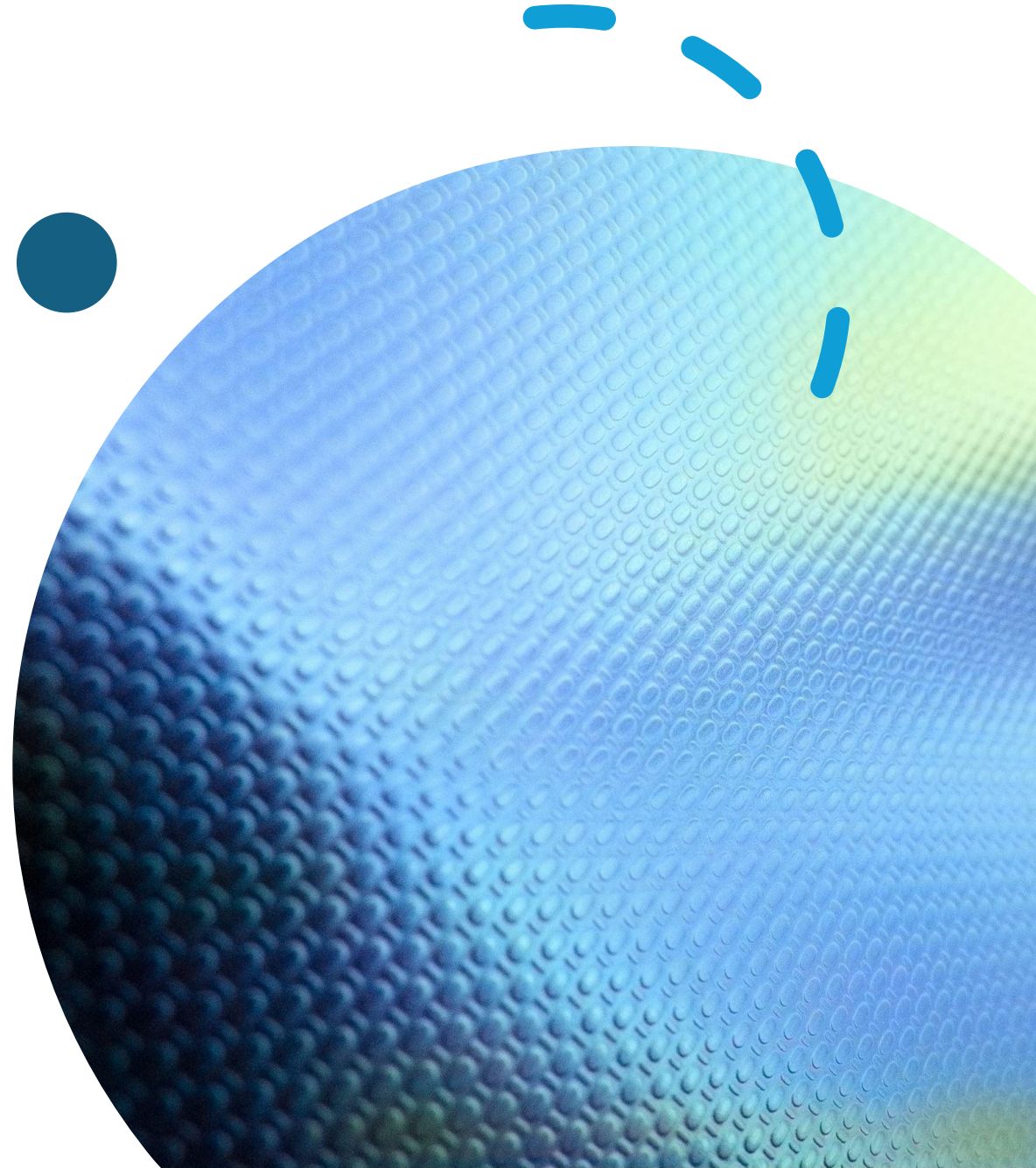
 **MFA & Justification (If enabled)**

---

 **Temporary Access Granted**

---


 **Access Expires Automatically**

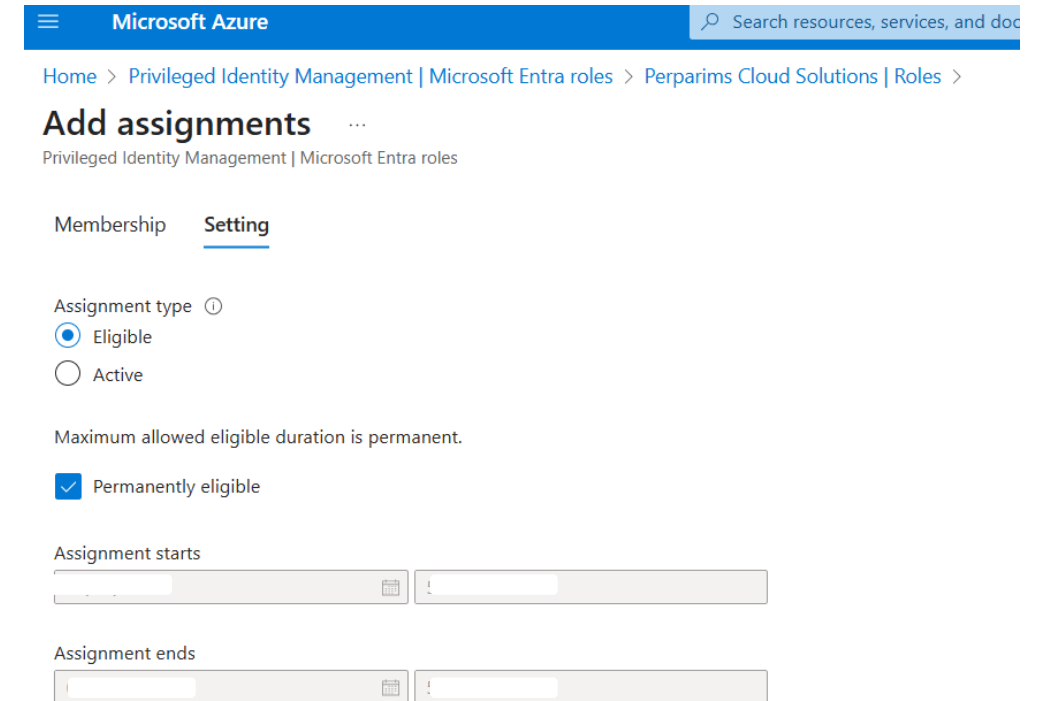


# Assign an Admin Role with Just-in-Time Access

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.

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



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

(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

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 My roles Pending requests Approve requests Review access Manage 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
<b>Application Administrator</b>				
Perparim Abdullahu	PerparimAbdullahu@Per	User	Directory	Direct
<b>Helpdesk Administrator</b>				
Emma Smith	emma.smith@PerparimS	User	New York Office (Admini	Direct
<b>User Administrator</b>				
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.

Microsoft Entra admin center

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

Copilot

sophia.davis@Perparim...  
PERPARIMS CLOUD SOLUTIONS

Home

What's new

Diagnose & solve problems

Favorites

Identity

Overview

Users

All users

Deleted users

User settings

Groups

Devices

Applications

Protection

Identity Governance

External Identities

Show more

Home >

Users ...  
Perparims Cloud Solutions

All users

Audit logs

Sign-in logs

Diagnose and solve problems

Deleted users

Password reset

User settings

Bulk operation results

New support request

+ New user

Edit

Delete

Download users

Bulk operations

Refresh

Manage view

Per-user MFA

Azure Active Directory is now Microsoft Entra ID.

Search

Add

9 users found

	Display name ↑	User principal name ↑	User type	On-premises sy...	Identities	Company name
<input type="checkbox"/>	AS Adam Smith	adam.smith@Per...	Member	Yes	PerparimSC300lab.onmi...	
<input type="checkbox"/>	AJ Alex Johnson	alex.johnson@Per...	Member	No	PerparimSC300lab.onmi...	
<input type="checkbox"/>	AW Austin Williams	austin.williams@P...	Member	No	PerparimSC300lab.onmi...	
<input type="checkbox"/>	ES Emma Smith	emma.smith@Per...	Member	No	PerparimSC300lab.onmi...	
<input type="checkbox"/>	JJ John Johnson	john.johnson@Per...	Member	No	PerparimSC300lab.onmi...	
<input type="checkbox"/>	ML Michael Lee	michael.lee@Perp...	Member	No	PerparimSC300lab.onmi...	
<input type="checkbox"/>	NW Nick Walker	nick.walker@Perp...	Member	No	PerparimSC300lab.onmi...	
<input type="checkbox"/>	PA Perparim Abdullahu	PerparimAbdullah...	Member	No	PerparimSC300lab.onmi...	
<input type="checkbox"/>	SD Sophia Davis	sophia.davis@Per...	Member	No	PerparimSC300lab.onmi...	



# 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.