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.

PerparimLabs

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

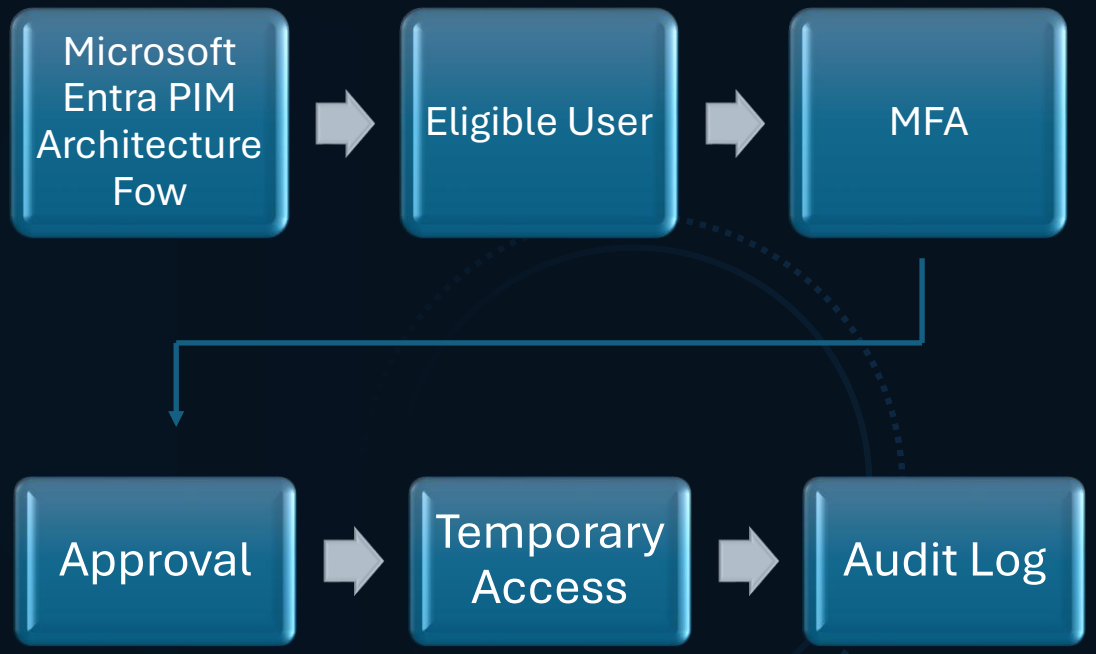
PerparimLabs

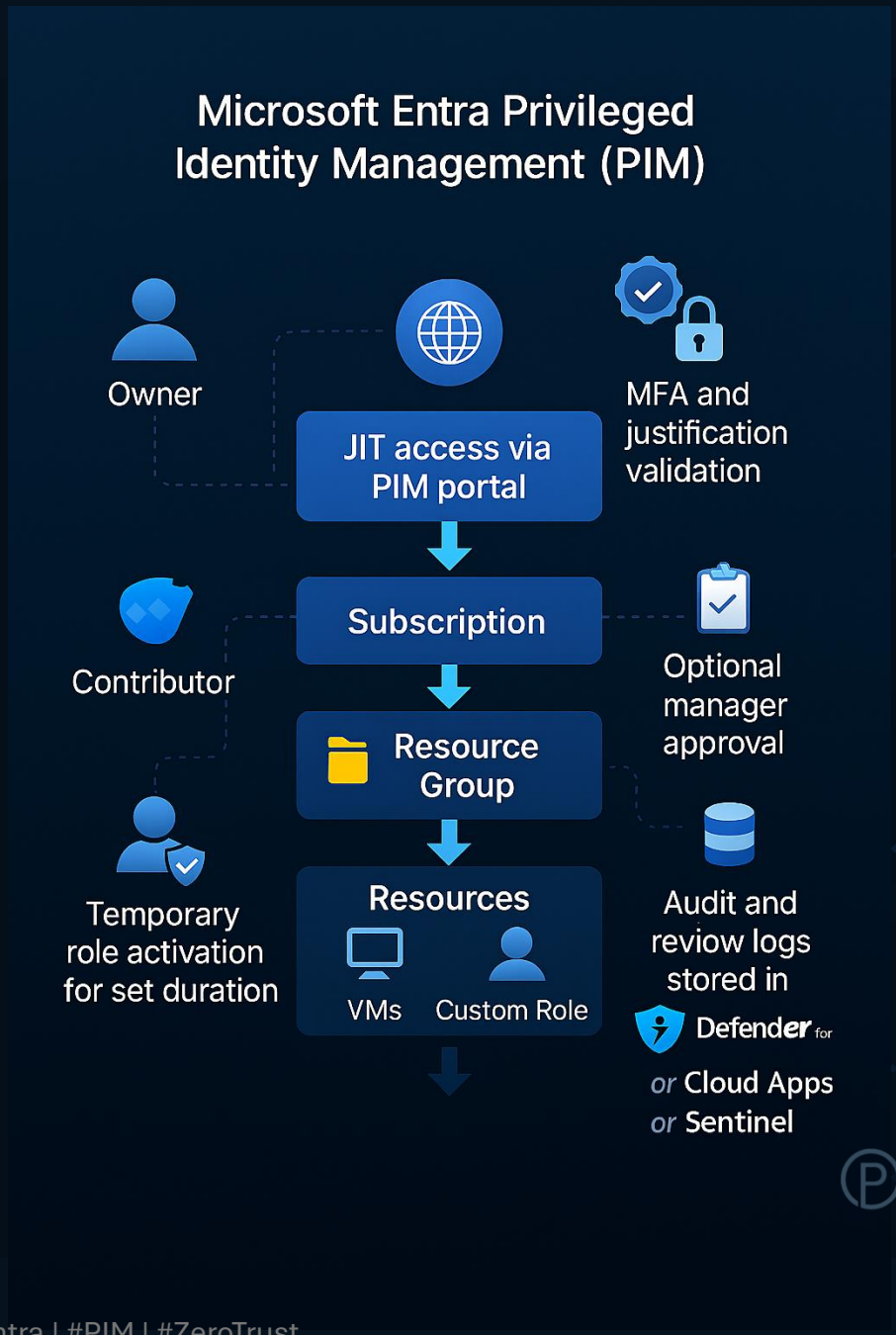
How PIM Works

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

PerparimLabs

Architecture Diagram





Business Value

✅ **Stops** lateral movement

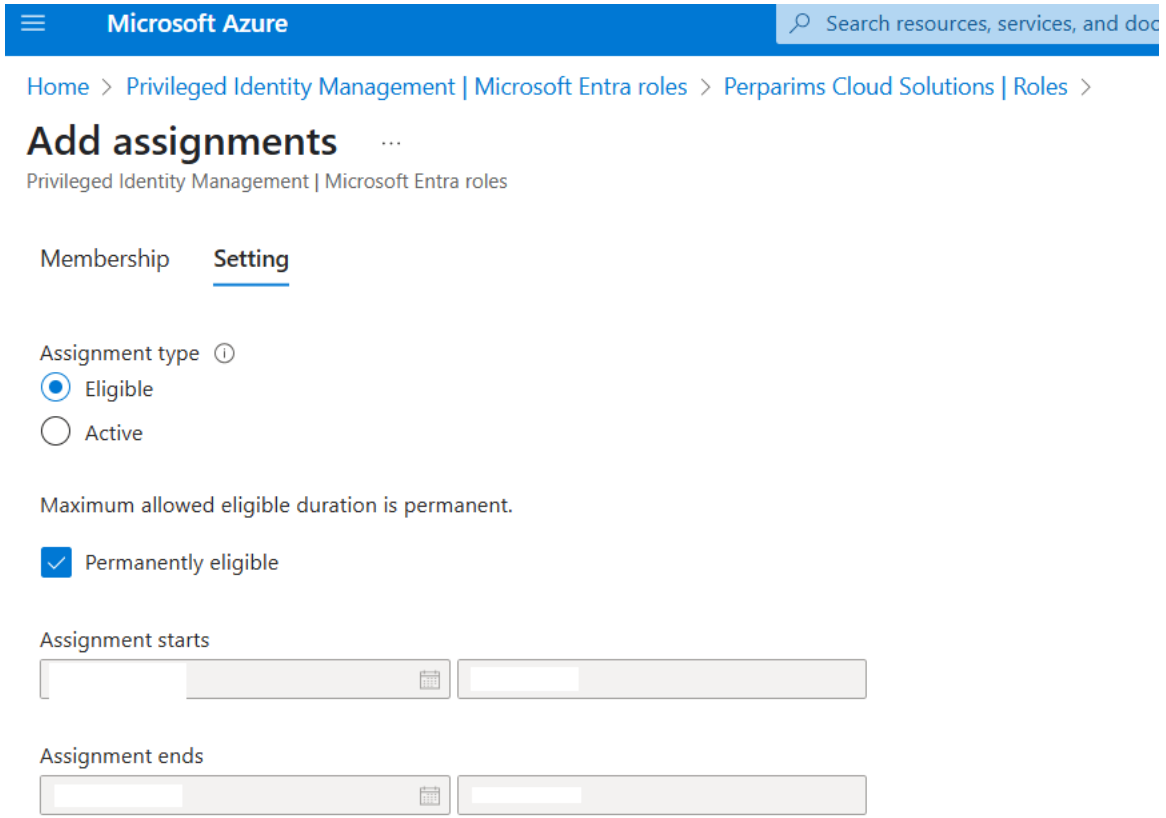
✅ **Enables** Zero Trust identity governance

✅ **Delivers** audit readiness and compliance

PerparimLabs

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.



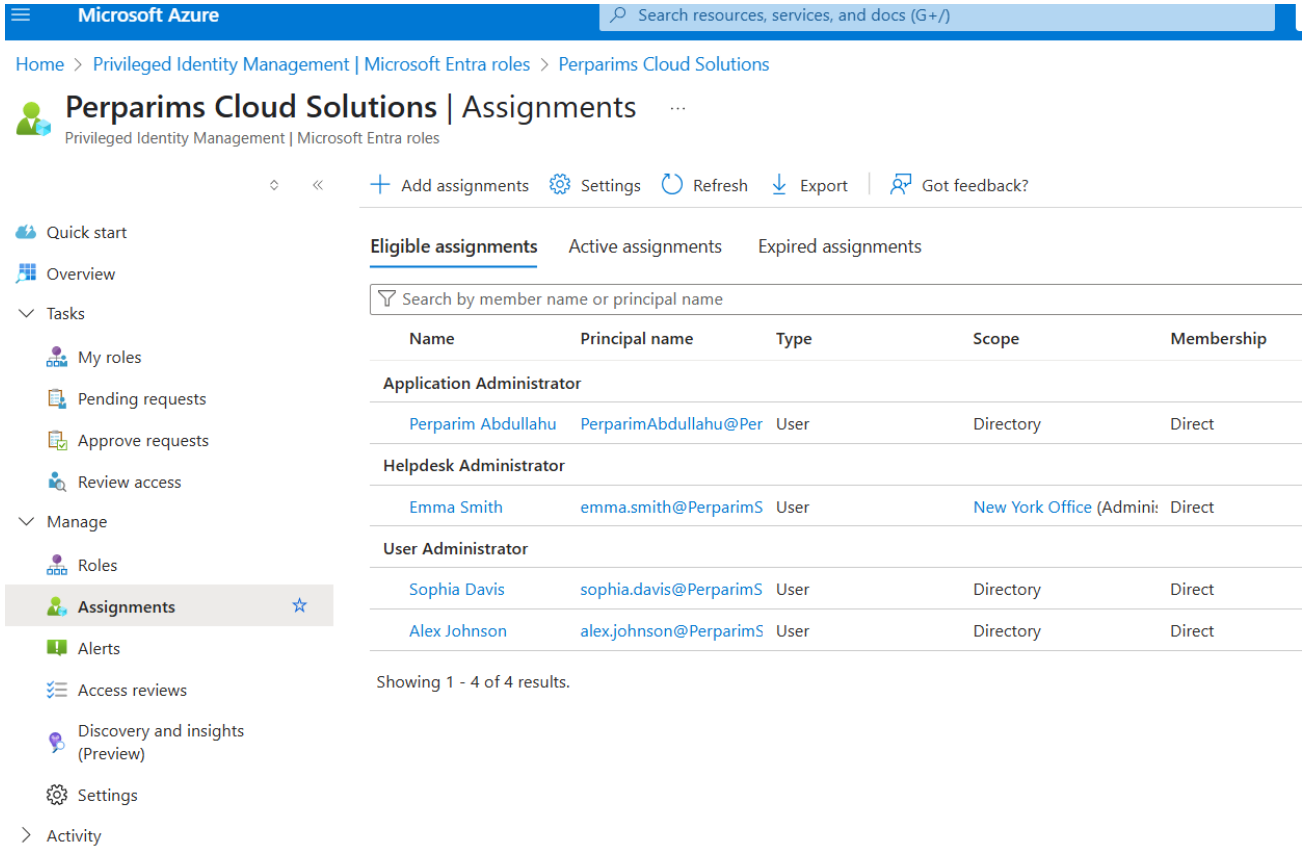
Tip: For higher control, you can configure a specific start and end window instead of permanently eligible.

PerparimLabs

(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.

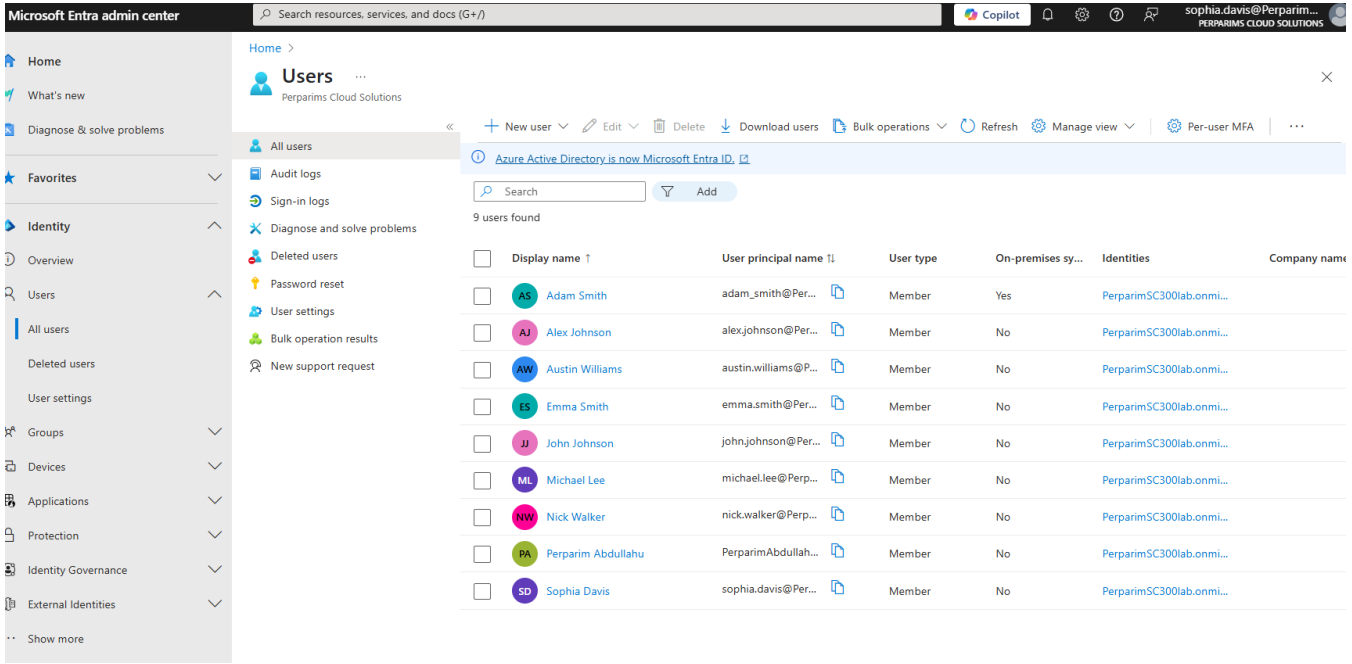


PerparimLabs

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.



PerparimLabs

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.

PerparimLabs