







Strengthen Your Security with Privileged Identity Management

Microsoft Entra PIM Configuration TechNet UC

What You'll Gain

-  Approval workflows and MFA for elevated roles
-  Just in time access enforcement
-  Real-time auditing and alerts
-  A fully configured Privileged Identity Management

“By definition [privileged users], they possess a range of capabilities that pose a far greater security risk than the capabilities routinely granted to standard users.”*

...operationalizing your Zero Trust strategy, and rolling out new capabilities.”

How confident are you that your organization can detect and prevent the misuse of privileged access before it becomes a breach?

Take Control with Microsoft Entra Privileged Identity Management

In today's hybrid and cloud-first world, privileged access is a top target for attackers—and one of the most overlooked risks in identity security. Microsoft Entra Privileged Identity Management (PIM) empowers organizations to enforce least privilege access, reduce standing permissions, and gain full visibility into who has access to what—and when.

Our PIM Configuration engagement helps you operationalize Microsoft Entra PIM with precision and speed. We align your privileged access strategy with Microsoft's Zero Trust model, ensuring that elevated roles are only activated when needed, with the right controls in place.



Why Configure PIM?

Configuring PIM is a strategic move for organizations seeking to strengthen their security posture and align with Microsoft's Zero Trust principles. PIM enables secure, scalable control over privileged access to critical resources by enforcing least privilege access, just-in-time role activation, and comprehensive auditing.

Eliminate standing admin rights with just-in-time access

Enforce MFA and approval for sensitive role activations

Audit privileged activity with real-time alerts and logs

Assign secure access with role-based controls

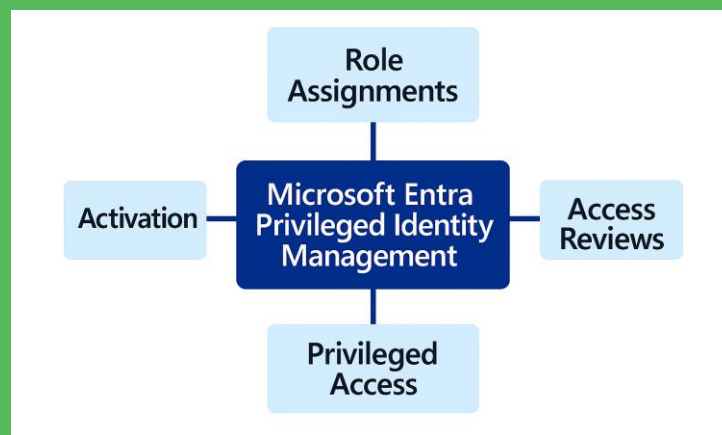
What to expect

Our PIM Configuration engagement is more than a technical setup—it's a strategic foundation for identity governance. TechNet UC's certified experts work closely with your team to deploy, tune, and document Microsoft Entra PIM to meet your organization's unique needs.

We'll work with you to:

- Review Azure AD roles and access policies
- Configure PIM for eligible assignments and just-in-time access
- Set up approval workflows, MFA, and Conditional Access
- Deliver documentation, runbooks, and knowledge transfer

We'll work with you to ensure all aspects of PIM are configured to your needs



Who should be interested

The engagement is intended for security decision-makers such as:

- Chief Information Security Officer (CISO)
- Chief Information Officer (CIO)
- Chief Security Officer (CSO)
- Endpoint & Device Management owners/ decision makers
- Application business owners
- IT Security
- IT Operations
- Security Architect
- Security Engineers

Why TechNet UC?

When it comes to security you need an experienced partner.

We have helped hundreds of customers with their security environment. Let us help you too.



TechNet UC