Access Security Privileged Identity Management

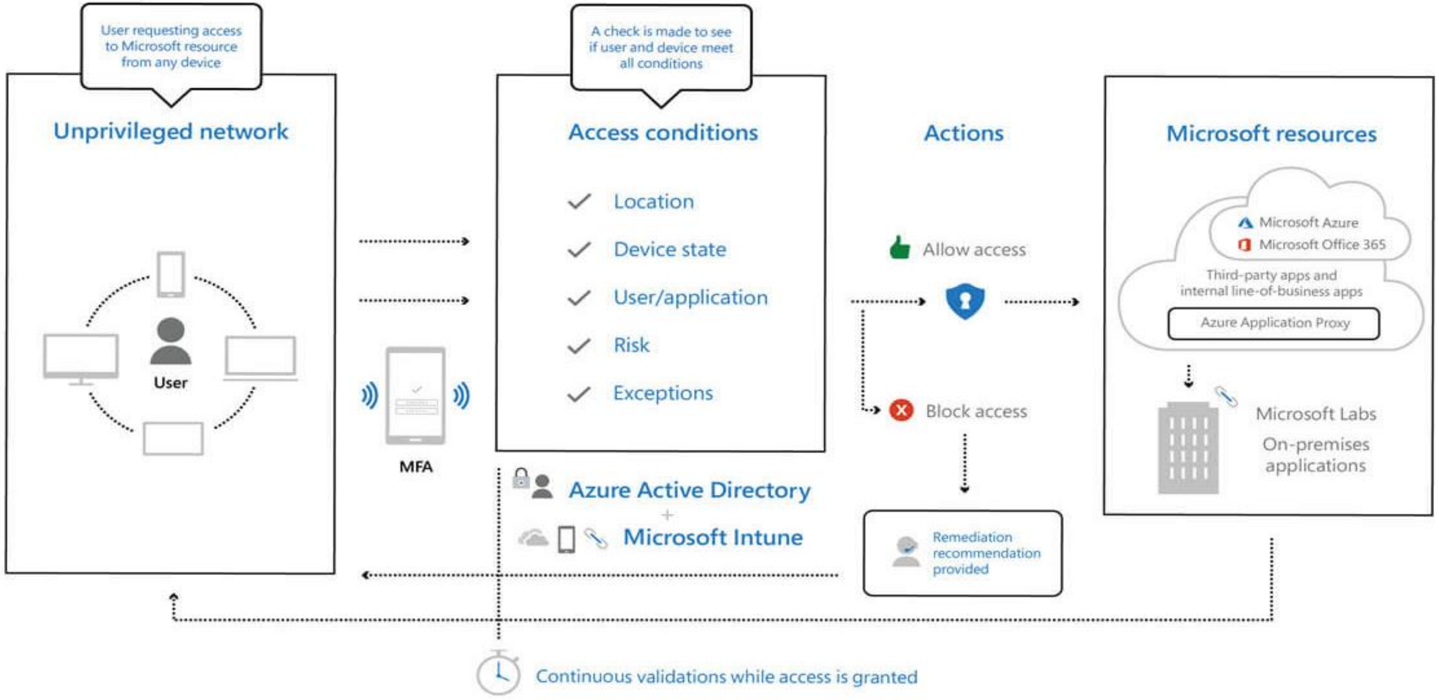
Hello!

I am Eng Teong Cheah

Microsoft MVP

Privileged Identity Management

Microsoft's Zero Trust Model



Microsoft Identity Management Evolution

Traditional	Advanced	Optimal
On-premises identity provider is in use	Cloud identity federates with on-premises system	Password less authentication is enabled
No SSO is present between cloud and on-premises apps	Conditional access policies gate access and provide remediation actions	User, device, location and behavior is analyzed in real time to determine risk and deliver ongoing protection
Visibility into identity risk is very limited	Analytics improve visibility	MFA is enforced

Azure AD Privileged Identity Management (PIM)

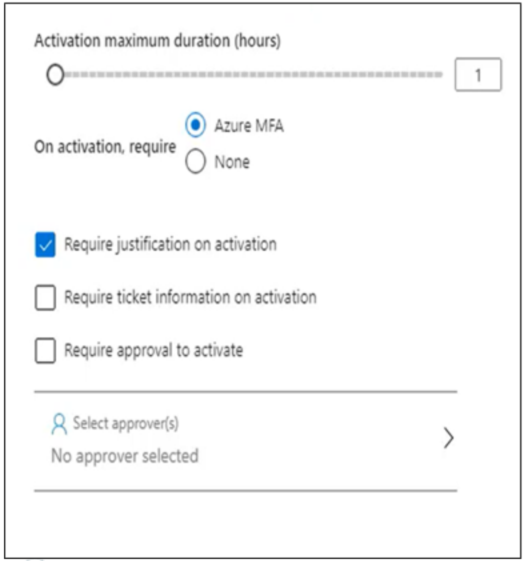
- Provide just-in-time privileged access to Azure AD and Azure Resources
- Assign time-bound access to resources using start and end dates
- Require approval to activate privileged roles
- Enforce multi-factor authentication to activate any role
- Use justification to understand why users activate
- Get notifications when privileged roles are activated
- Conduct access reviews to ensure users still need roles
- Download audit history for internal or external audit

PIM Onboarding

- Azure AD Premium P2, Enterprise Mobility + Security (EMS) E5, or Microsoft 365 M5 license
- The Global administrator (first user) who enables PIM gets write access
- The first user can assign others to the Privileged Role Administrator
- Global administrators (not first user), Security administrators, and Security readers have read-only access
- Ensure there are always at least two Privileged Role Administrators

PIM Confiuration Settings

Activation



Activation maximum duration (hours) 1

On activation, require ● Azure MFA ○ None

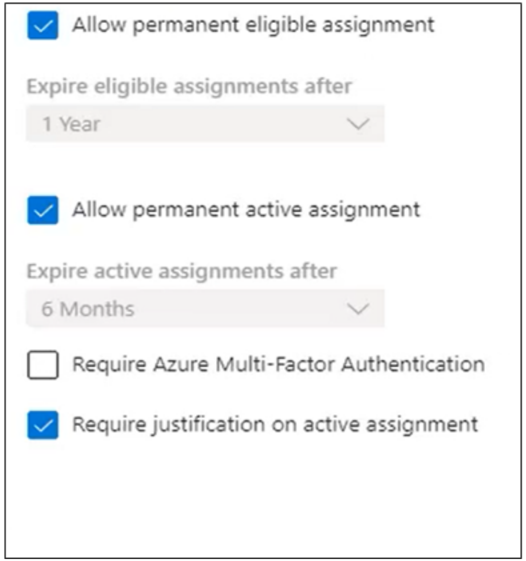
☑ Require justification on activation

□ Require ticket information on activation

□ Require approval to activate

Select approver(s)
No approver selected

Assignment



☑ Allow permanent eligible assignment

Expire eligible assignments after
1 Year

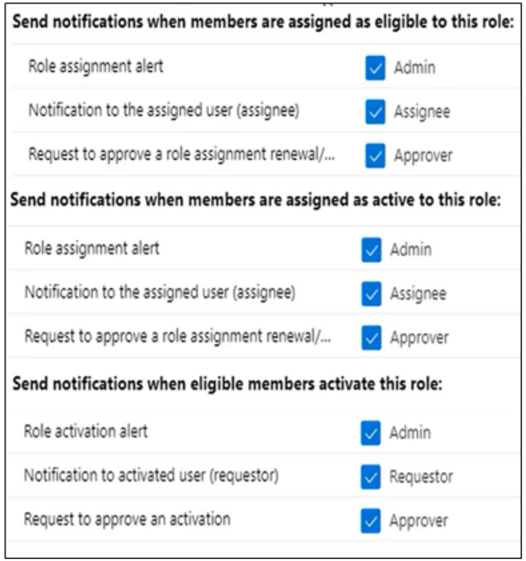
☑ Allow permanent active assignment

Expire active assignments after
6 Months

□ Require Azure Multi-Factor Authentication

☑ Require justification on active assignment

Notifications



Send notifications when members are assigned as eligible to this role:

Role assignment alert	☑ Admin
Notification to the assigned user (assignee)	☑ Assignee
Request to approve a role assignment renewal/...	☑ Approver

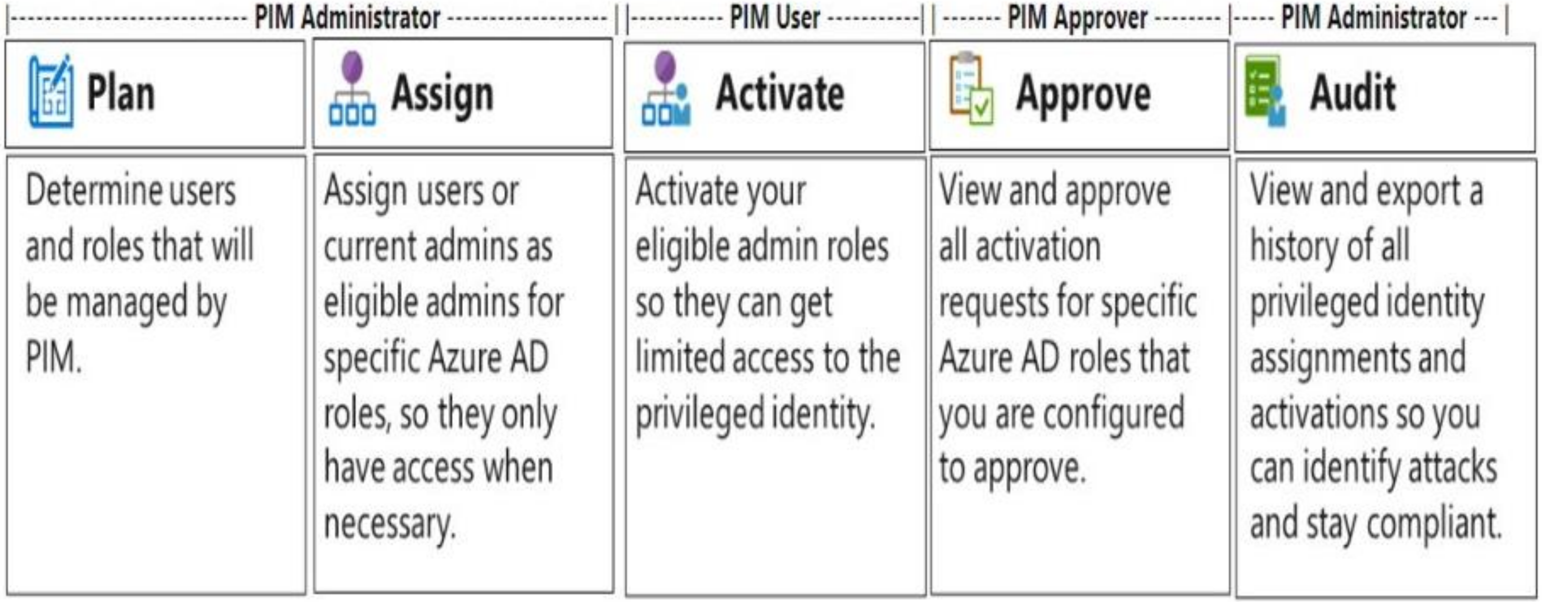
Send notifications when members are assigned as active to this role:

Role assignment alert	☑ Admin
Notification to the assigned user (assignee)	☑ Assignee
Request to approve a role assignment renewal/...	☑ Approver

Send notifications when eligible members activate this role:

Role activation alert	☑ Admin
Notification to activated user (requestor)	☑ Requestor
Request to approve an activation	☑ Approver

PIM Workflow



PIM Administrator		PIM User	PIM Approver	PIM Administrator
Plan	Assign	Activate	Approve	Audit
Determine users and roles that will be managed by PIM.	Assign users or current admins as eligible admins for specific Azure AD roles, so they only have access when necessary.	Activate your eligible admin roles so they can get limited access to the privileged identity.	View and approve all activation requests for specific Azure AD roles that you are configured to approve.	View and export a history of all privileged identity assignments and activations so you can identify attacks and stay compliant.

Demostrations

MFA, Conditional Access and AAD Identity Protection

Thanks!

Any questions?

You can find me at:

@walkercet

References

- https://docs.microsoft.com/en-us/