4 Steps to Configure Azure AD PIM for Groups

By: Shehan Perera | MVP - Enterprise Mobility
https://linktr.ee/shehanjp

Challenge

You have a protected resource to which you need to provide access to a group of users only for a specific time period, you need to make sure they explicitly elevate access when needed and that elevation is going through a verification process before accessing the resource and elevation is available only for 2 months time.

Solution

With Azure Active Directory (Azure AD), part of Microsoft Entra, you can provide users just-in-time membership in the group and just-in-time ownership of the group using the Azure AD Privileged Identity Management for Groups feature. These groups can be used to govern access to various scenarios that include Azure AD roles, Azure roles, as well as Azure SQL, Azure Key Vault, Intune, other application roles, and third party applications. ~Microsoft Learn

Licensing Requirement

- Azure AD Premium P2 - Users with eligible and/or time-bound assignments as members or owners of PIM for Groups
- Azure AD Premium P2 - Users able to approve or reject activation requests in PIM
- Azure AD Premium P2 - Users assigned to an access review
- Azure AD Premium P2 - Users who perform access reviews
- No licenses are required for users who set up PIM, configure policies, receive alerts, and set up access reviews.

More Info

https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/concept-pim-for-groups

1 Create the Azure AD Group

2 Onboard the group for PIM

Click on the "Privileged Identity Management" section under Activity and select Enable Azure AD PIM for this group

3 Add PIM Assignments

This is where you select who are the group owners and/ or members for this group.

Role type ⟶ Owner/ Member

Assignment Type ⟶ Eligible/ Active

Assignment Start Date and End date

4 Setup Role Settings

Add additional Member or Owner related settings.

Activation - On Activation, require MFA?/ AAD CA Auth Context
Require Justification?
Require Ticket Info?
Require Approval?

Assignment
Expire eligible and active assignments after what date?

Notification
Send email notifications to admins during the activation process

User Activtaion

User login to Entra Portal ⟶ Identity Governance ⟶ Privileged Identity Management ⟶ Groups ⟶ Select the Group ⟶ Eligible Assignments ⟶ Activate

shehanperera.com
https://www.linkedin.com/in/shehanperera85/
https://github.com/shehanperera85
https://twitter.com/Shehanperera85