Microsoft Security

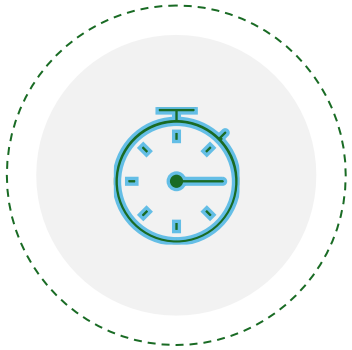
Identity Governance and Administration Proof of concept

Govern privileged identities and their access

Introduction

Privileged Identity Management (PIM) is a service in Microsoft Entra ID that enables you to manage, control, and monitor access to important resources in your organization. These resources include resources in Microsoft Entra ID, Azure, and other Microsoft Online Services such as Microsoft 365 or Microsoft Intune

Microsoft Entra ID Privileged Identity Management



Just in Time Access

Just Enough Access

Privileged Admin Workflow

Audit-ready

Protect and control privileged access to your organization

Privileged Identity Management (PIM)

Manage and audit admin roles across Azure, Microsoft Entra ID and Microsoft 365

See which users are assigned privileged roles.

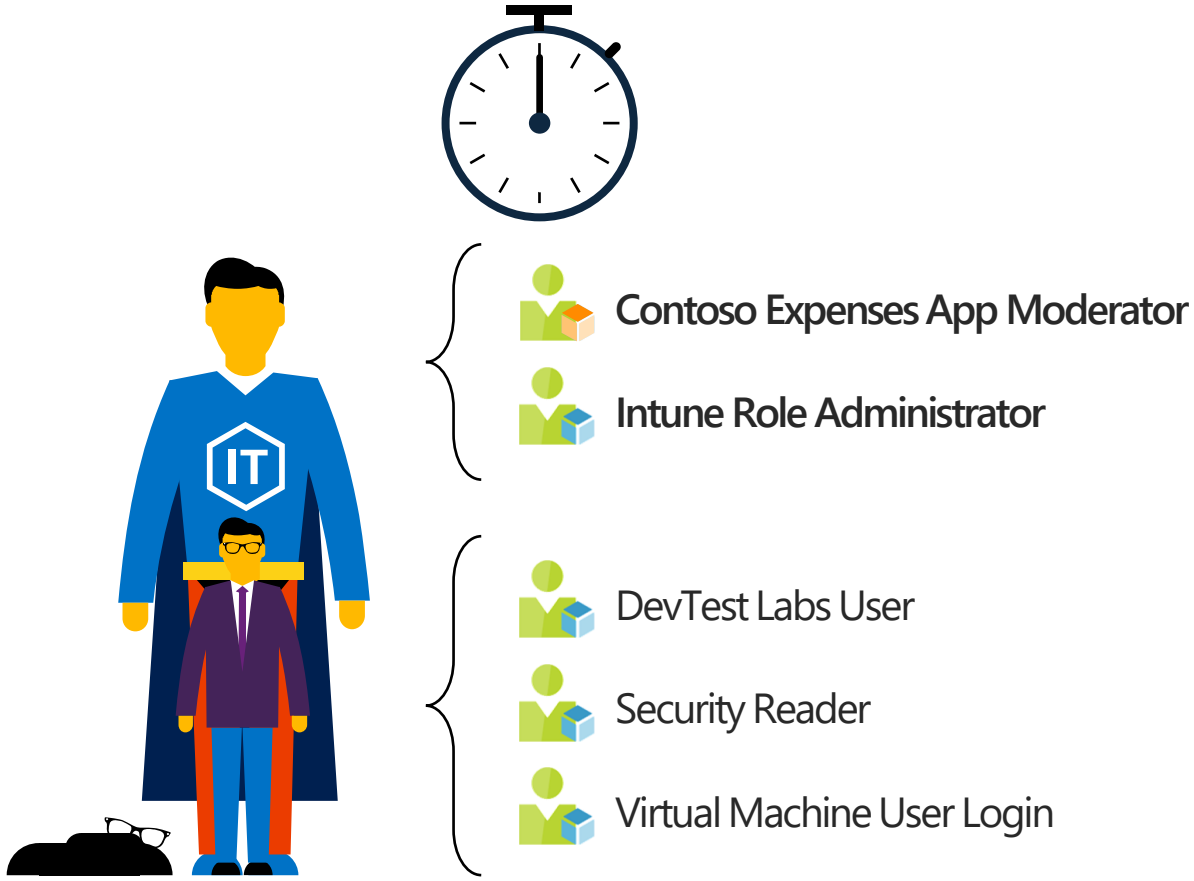
Enable on-demand, "just in time" administrative access.

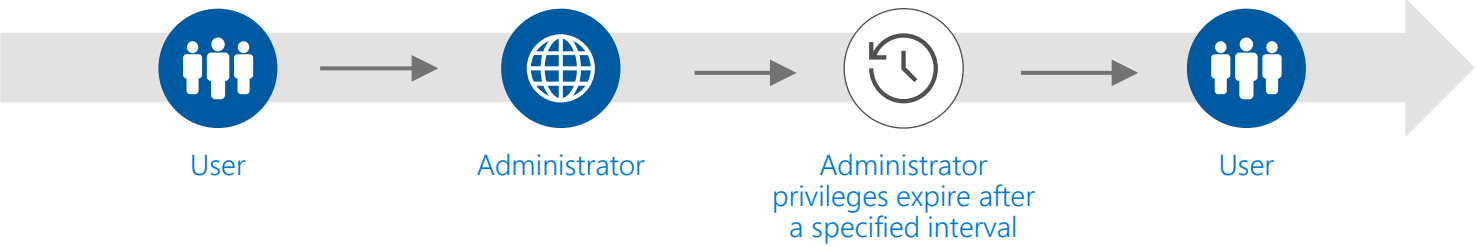
Set up approval flows for privilege activation.

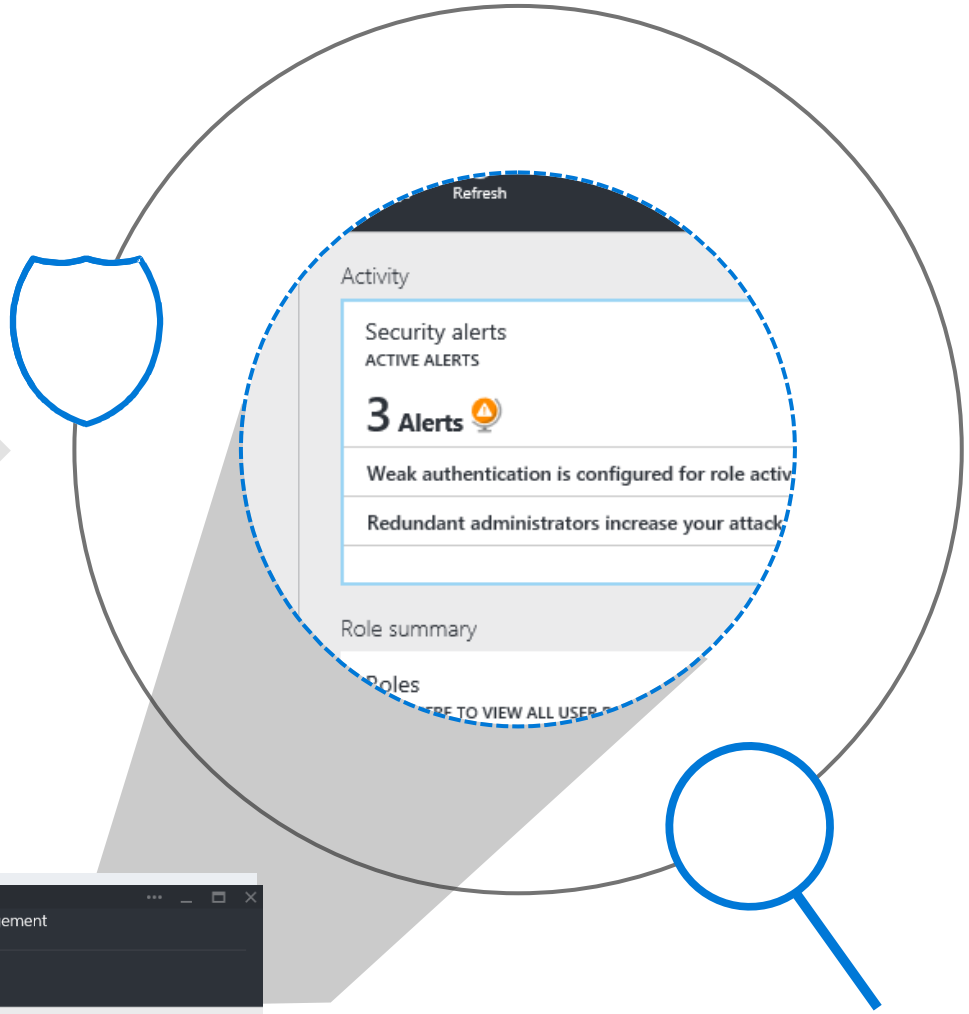
Get alerts and view a history of administrator activation and actions.

Works for:

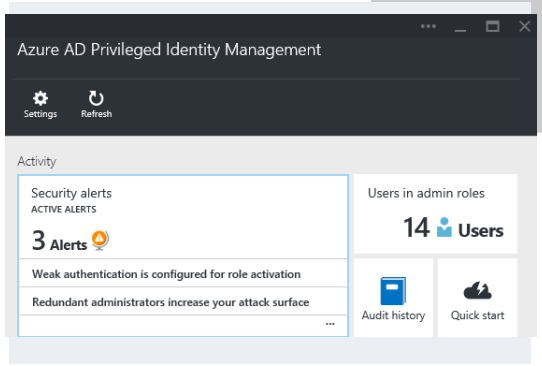
- Microsoft Entra ID directory roles
- Azure Resource roles
- Privileged Access Groups (Public Preview)







- Enforce on-demand, just-in-time administrative access when needed
- Ensure policies are met with alerts, audit reports and access reviews
- Manage admins access in Microsoft Entra ID and also in Azure RBAC



What you can manage in PIM

Azure Roles

Microsoft Entra ID Roles

Groups

What you can manage in PIM

Azure Roles

The role-based access control (RBAC) roles in Azure that grants access to management groups, subscriptions, resource groups, and resources.

Microsoft Entra ID Roles

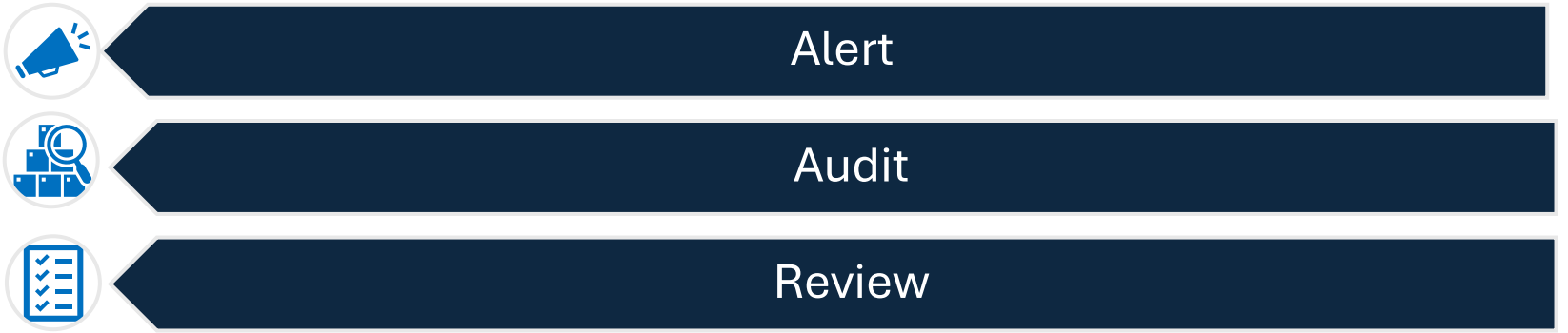
Privileged Roles include built-in and custom roles to manage Microsoft Entra ID and other Microsoft 365 online services.

Groups

PIM for groups allows you to setup just-in-time access to member and owner role of an Microsoft Entra ID security group, alternatively you can use these groups for Microsoft Entra ID roles and Azure roles assignments and other permissions within Microsoft online services

Privileged Identity Management high level flow

Bring under management	Set role settings	Assign	Activate	Approve / Reject	Extend or renew
• Applicable for Azure roles and Groups	• Define assignment process and requirements	• Eligible or permanent	• If eligible, follow process to activate the role	• For roles that require approval	• When assignment end approaches



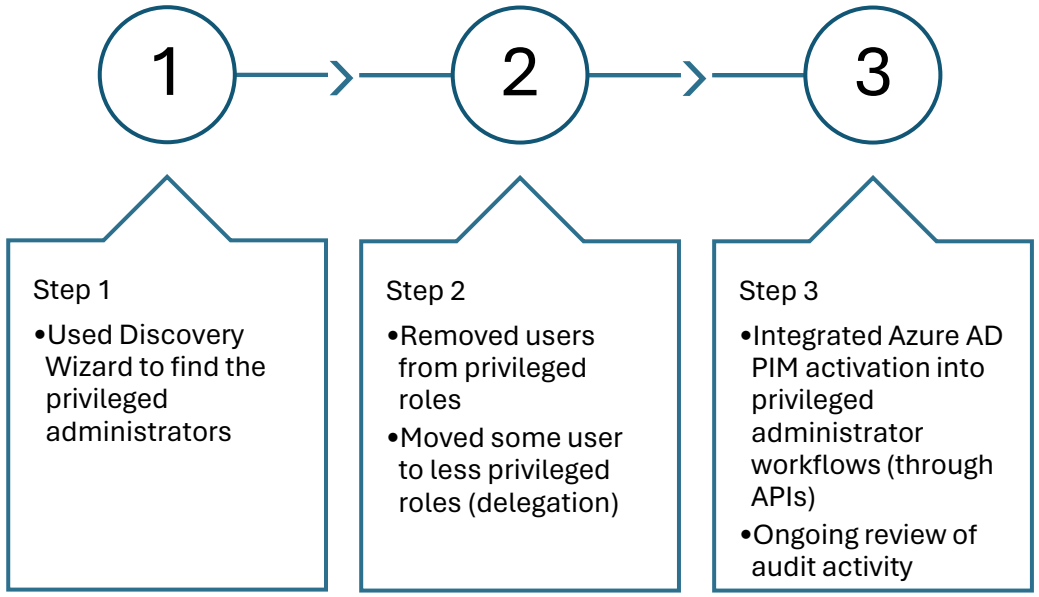
Microsoft Entra ID PIM assignment types

·**Eligible assignments:** require the member to activate the role before using it. Administrator may require role member to perform certain actions before role activation which might include performing a multi-factor authentication (MFA) check, providing a business justification, or requesting approval from designated approvers.

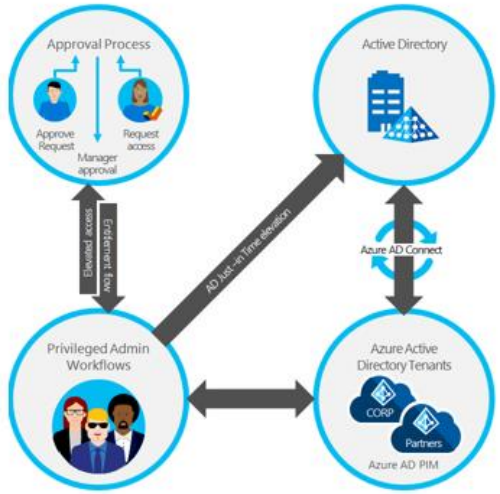
·**Active assignments:** don't require the member to activate the role before usage. Members assigned as active have the privileges assigned ready to use. This type of assignment is also available to customers that don't use Microsoft Entra ID PIM.

Deploying Privileged Identity Management

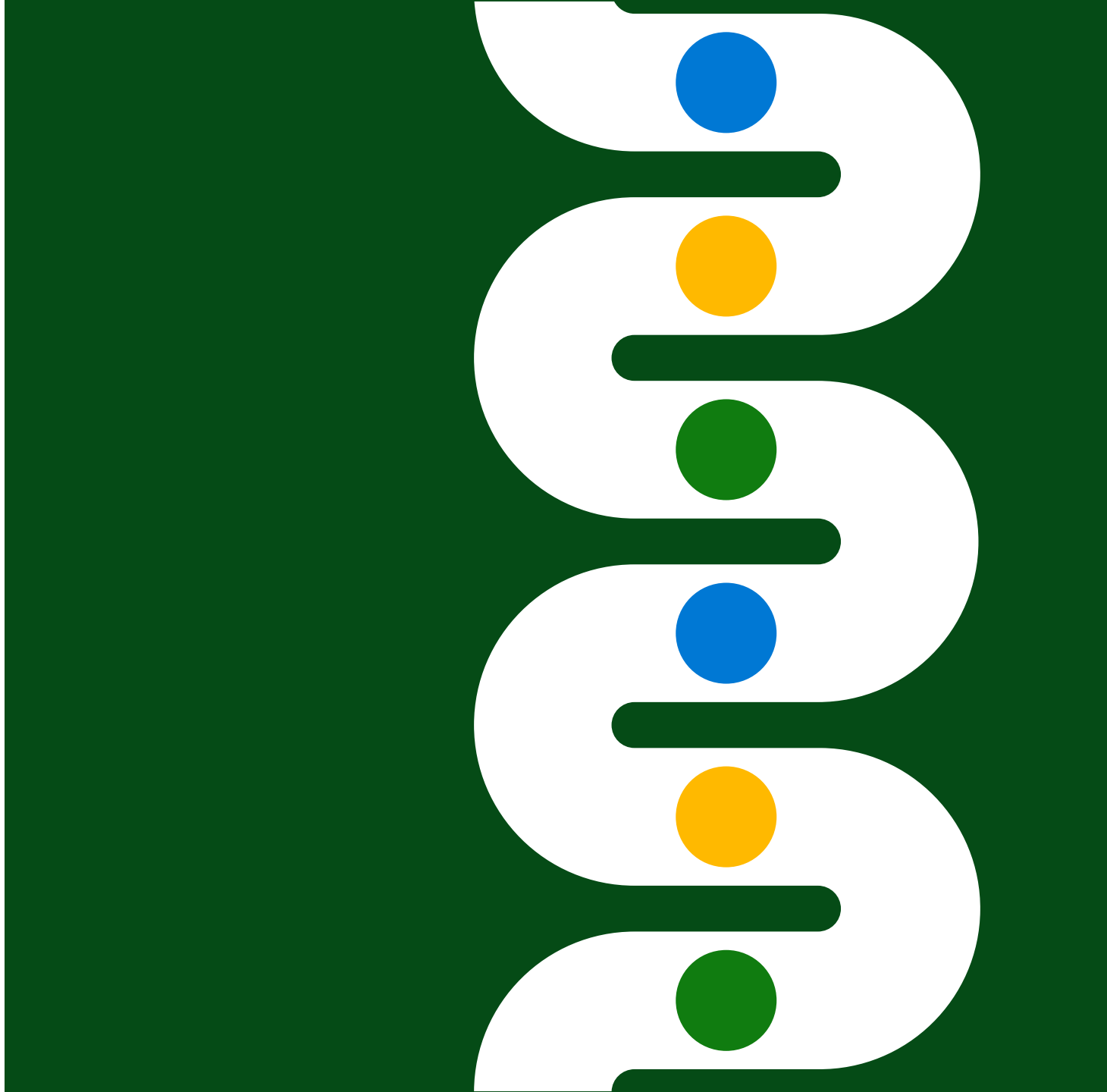
Discovery, delegation, automation



Role	Eligible	Persistent	% reduction
Global Administrator	93	2	97.89%
Password Administrator	5	0	100.00%
Service Administrator	71	14	83.53%
User Administrator	126	6	95.45%

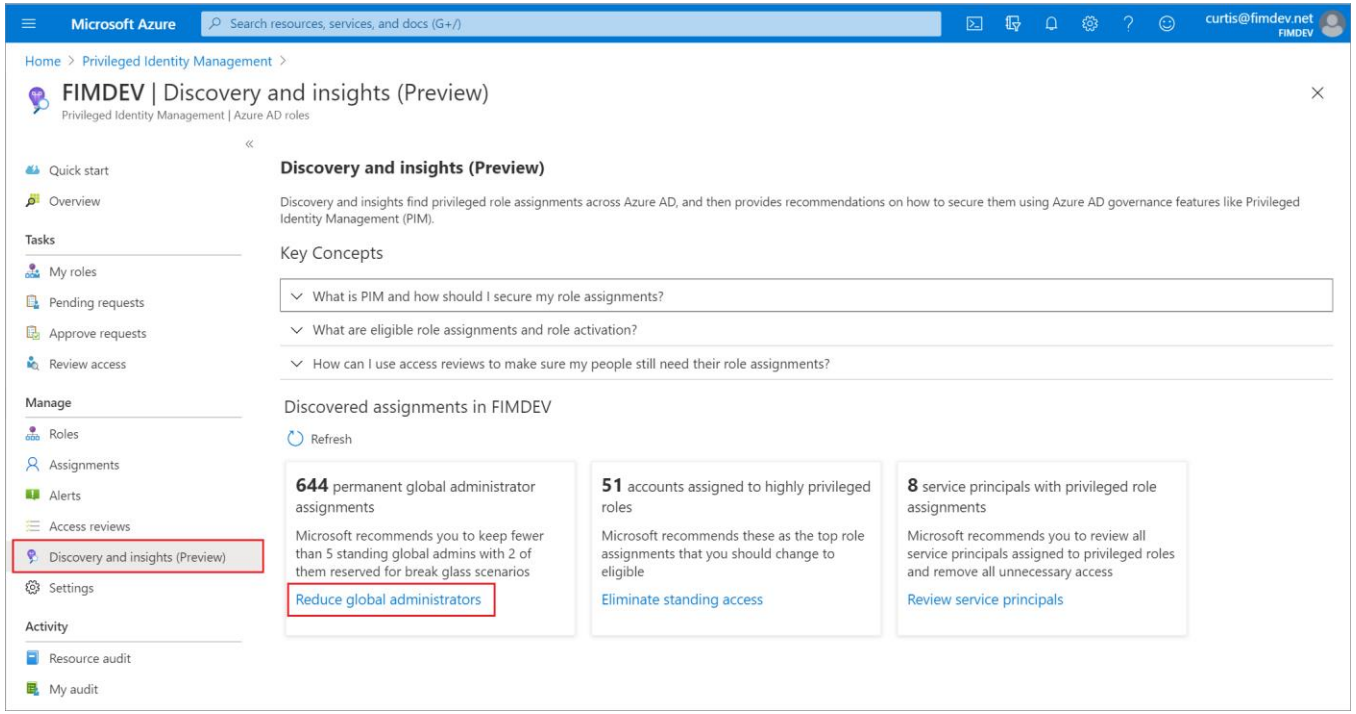


Discovery and Insights (Preview)

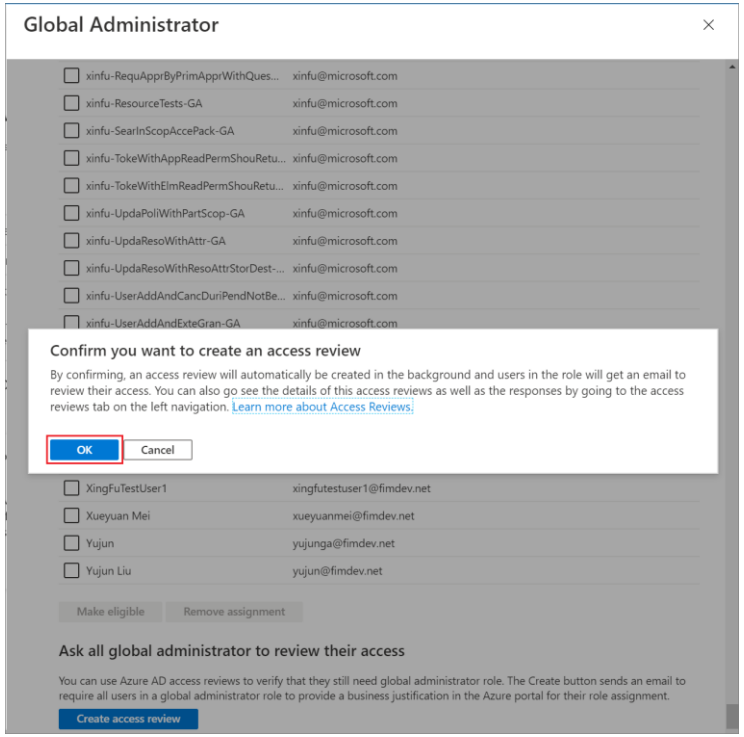


Discovery and Insights (Preview)

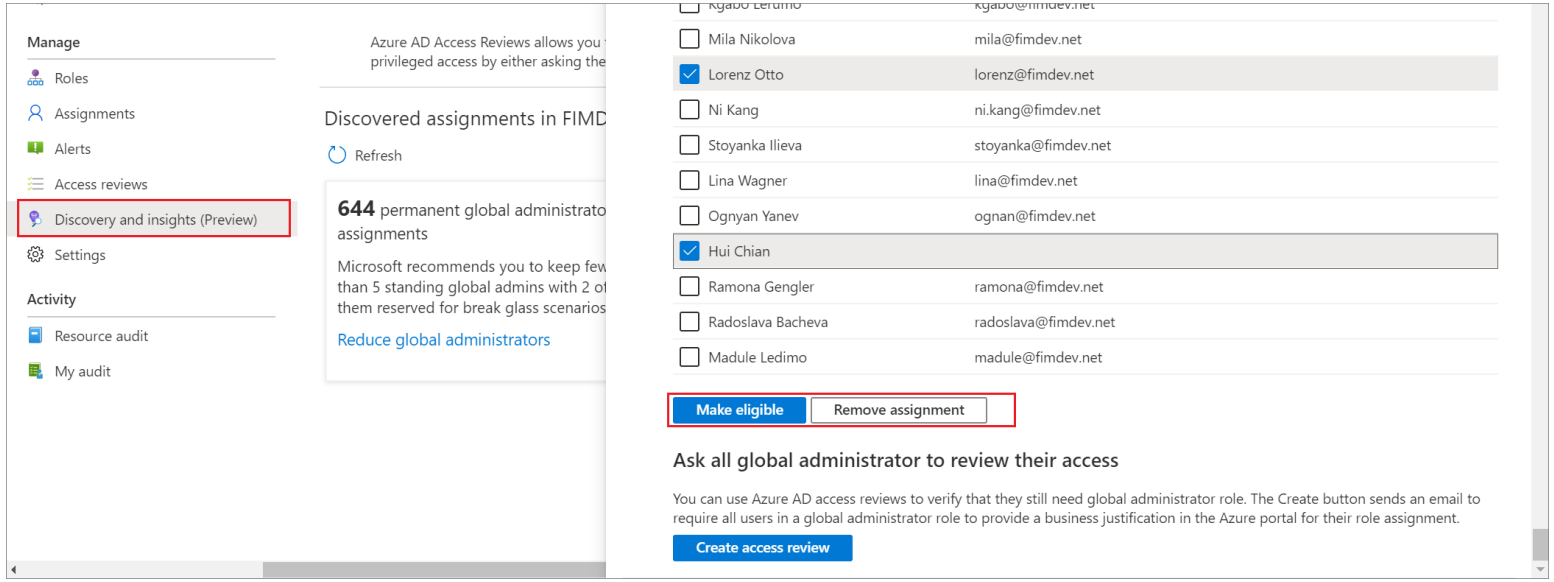
- Lists all privileged roles and how many users are currently holding those roles
- Learn more about the assigned users if one or more of them are unfamiliar.
- Move users to eligible status or just remove them from the role completely
- Create Access reviews for global admins



Discovery and Insights (Preview)



Create Access Review



Remove assignment or Make user eligible for the role

PIM for Microsoft Entra ID roles

How to use PIM for Microsoft Entra ID roles

Microsoft Entra ID Roles

Configure Microsoft Entra ID roles

- Select the resource you want to manage
- Review settings and PIM policies
- Configure settings like:
  - ✓Activation max duration
  - ✓MFA on activation
  - ✓Require conditional access authentication context
  - ✓Require justification
  - ✓Require ticket information
  - ✓Require approval
  - ✓Assignment duration

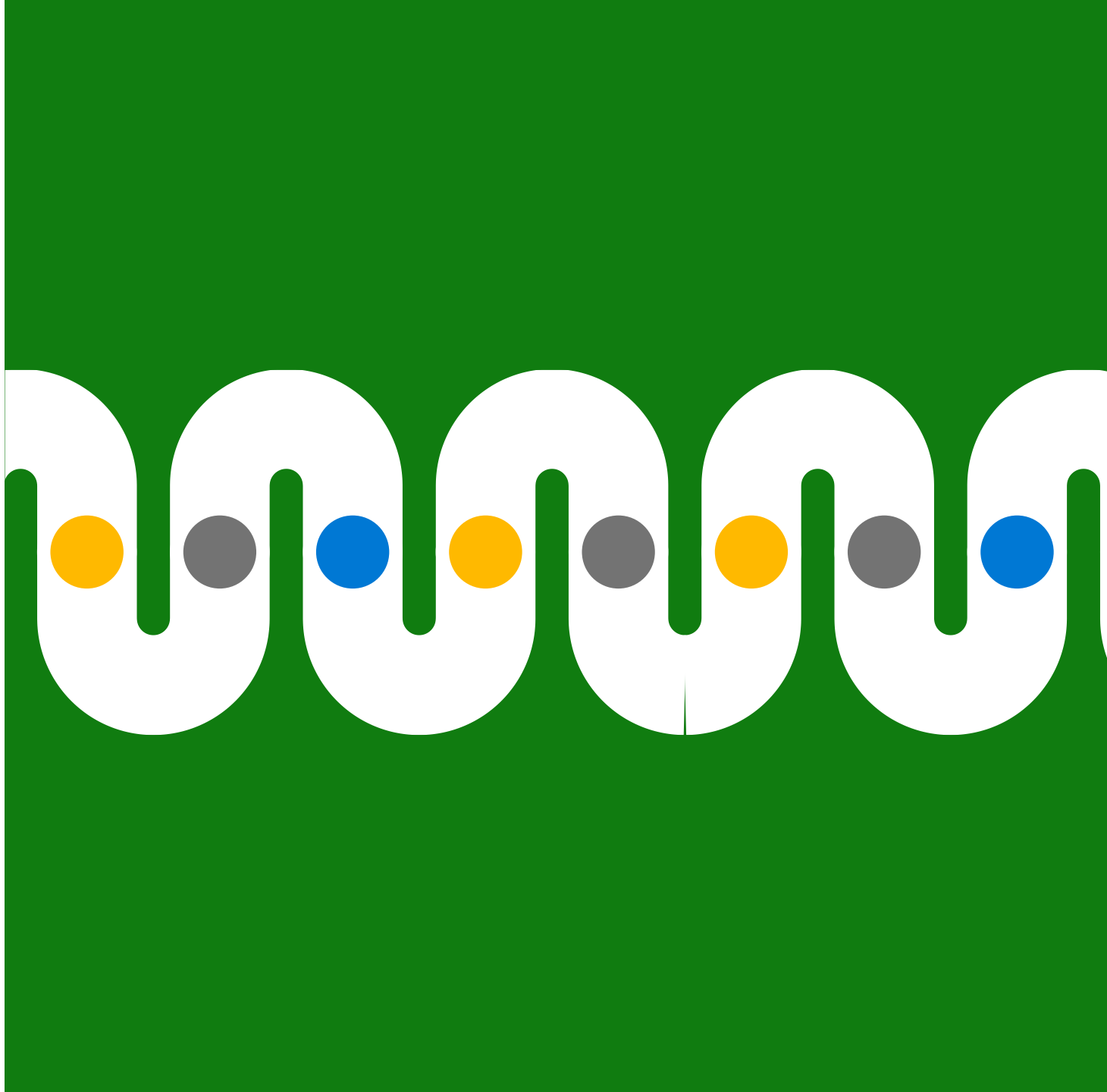
Give eligible assignments

- For those who may require to elevate to a privileged Microsoft Entra ID role

Allow eligible users to activate their Azure roles just-in-time

- Users can activate their eligible roles through Microsoft Entra portal -> My roles

PIM for Azure Roles



How to use PIM for Azure roles

Azure Roles

Discover Azure resources

- If this is the first time , go to **Entra portal -> PIM -> Azure resources -> Discover resources**
- After discovery is complete , select any unmanaged resource that you wish to manage under PIM

Configure Azure role settings

- Select the resource you want to manage
- Review settings and PIM policies
- Configure settings like:
  - ✓Activation max duration
  - ✓MFA on activation
  - ✓Require conditional access authentication context
  - ✓Require justification
  - ✓Require ticket information
  - ✓Require approval
  - ✓Assignment duration

How to use PIM for Azure roles (cont'd)

Azure Roles

Give eligible assignments

- For those who may require to elevate to a privileged role

Allow eligible users to activate their Azure roles just-in-time

- Users can activate their eligible roles through Microsoft Entra portal -> My roles

Tutorial : Prepare PIM for Azure roles

PIM for Groups

How to use PIM for Groups

Groups

Identify Groups to Manage

Use the discovery process to bring groups to management

Assign eligibility for a group through PIM

- Select the users who are eligible for member or owner roles

Allow Eligible users to activate group membership or ownership

- Users can activate their eligible roles through Microsoft Entra portal -> My roles

Tutorial : PIM for groups

PIM for Groups: Role-assignable vs non-role assignable

Groups

Role-Assignable

Only the Global Administrator, Privileged Role Administrator, or the group Owner can manage the group

For security reasons, No other users can change the credentials of active members, this prevents elevation without approval

Non-role-assignable

More Microsoft Entra ID roles can manage group

Various Roles can change the credentials of active members

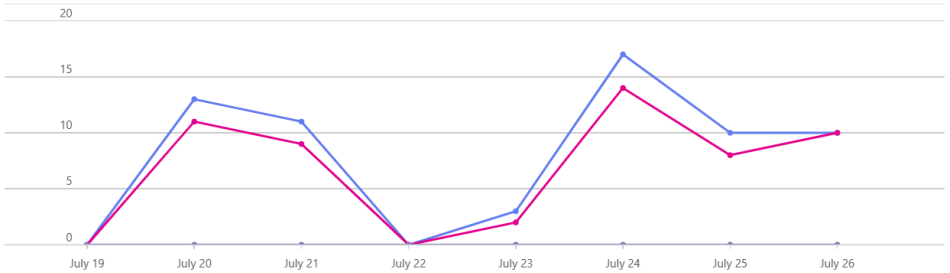
PIM for Groups considerations

- Role-assignable groups can’t have other groups nested
- Groups must be an Azure AD security group or a Microsoft 365 group
- One group can be an eligible member of another group, even if one of those groups is role-assignable
- If a user is an active member of Group A, and Group A is an eligible member of Group B, the user can activate their membership in Group B. This activation will be only for the user that requested the activation for, it does not mean that the entire Group A becomes an active member of Group B

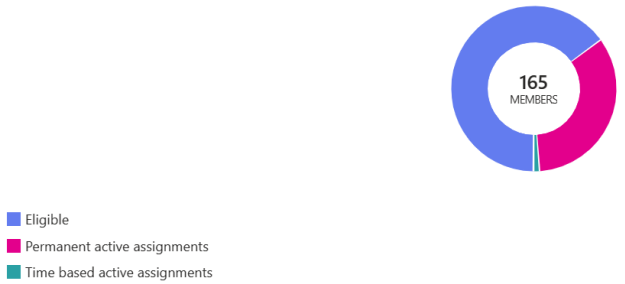
PIM dashboard

ghts (Preview)

Role activations in last 7 days



Role assignment distribution



PIM Activities in last 30 days

Title	Count
Members with new eligible assignments	142
Members assigned as active	6

Alert

Alert	Count	Risk level
Roles don't require multi-factor authentication for activation	35	Medium
Eligible administrators aren't activating their privileged role	629	Low
Potential stale accounts in a privileged role	385	Medium

Roles by assignment (descending)

Role	Eligible	Active
Global Reader	1	744
Attribute Definition Reader	674	1
Global Administrator	443	31
Application Administrator	11	7
Cloud Device Administrator	0	13
Attribute Definition Administrator	5	6
Compliance Administrator	4	6
Directory Readers	1	9
Security Administrator	5	3
Attribute Assignment Administrator	5	3

Access Reviews in PIM

How does Access Reviews work?

Administrator

- **1. Select resource**

Team/Group
SaaS application
Privileged role
Access Package

2. Select scope

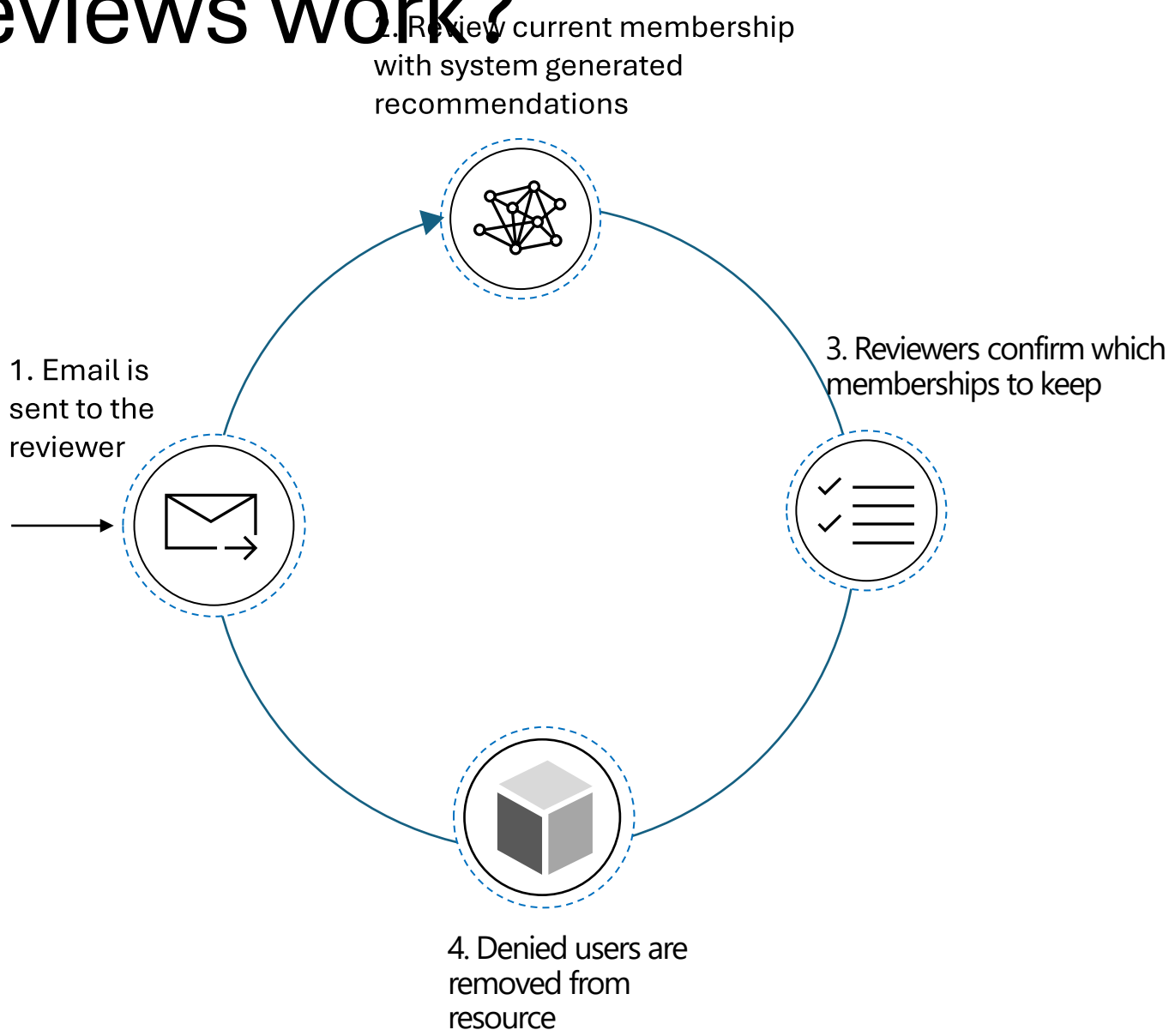
Guests
Employees
Everyone

3. Select reviewer

Team/Group owner
Manager*
Specific user(s)
Users' self review

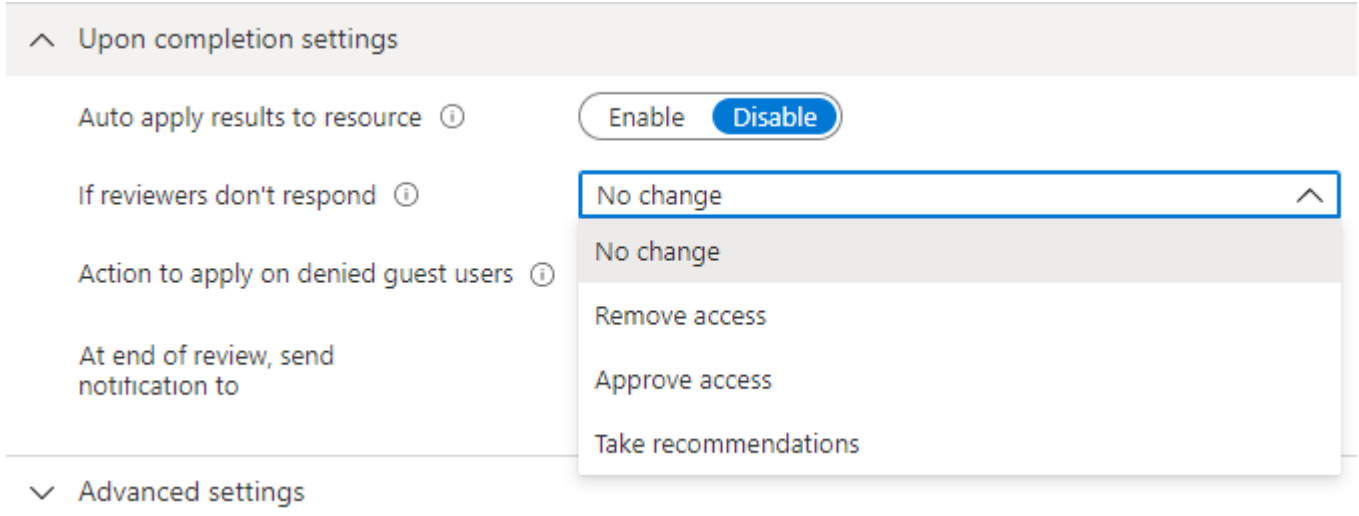
4. Select frequency

Weekly
Monthly
Quarterly
Annually



Access reviews in PIM

- Used to Automate the discovery of stale roles assignments
- Azure Roles and Microsoft Entra ID roles
- Optionally, you can automatically remove the users from the role upon completion of the Access Review

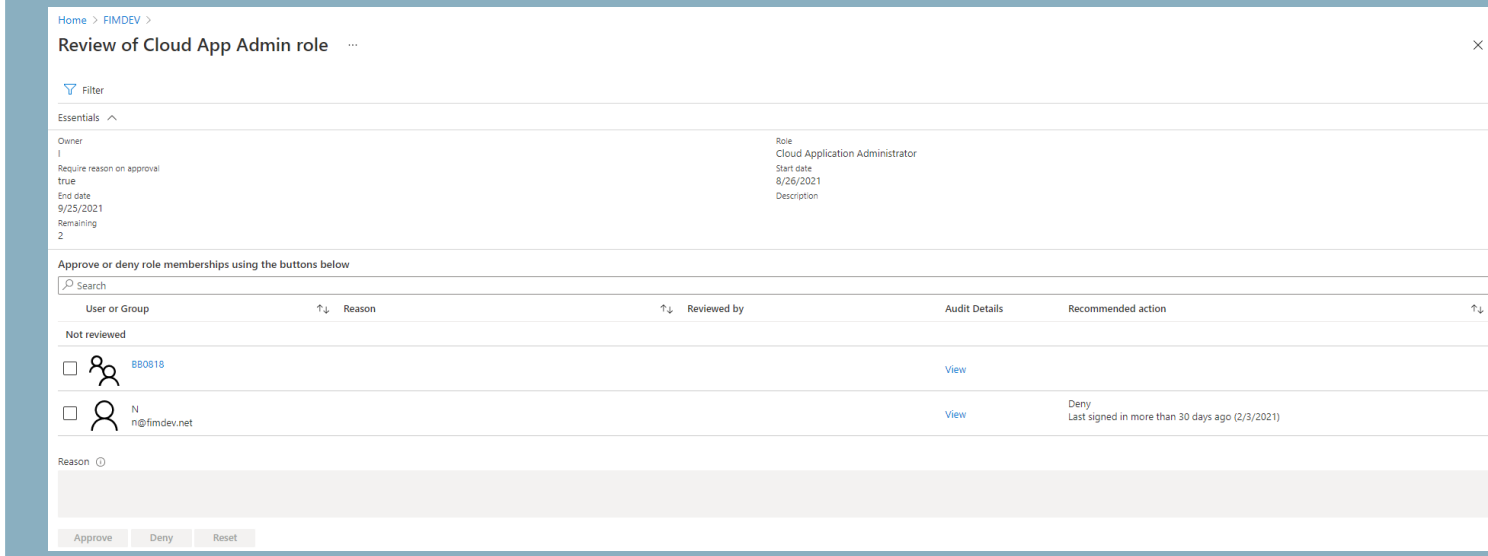


Perform and complete an Access review

You can approve or deny access based on whether the user still needs access to the role.

Choose Approve if you want them to stay in the role, or Deny if they do not need the access anymore.

The users' assignment status will not change until the review closes and the administrator applies the results



PIM + CA Integration

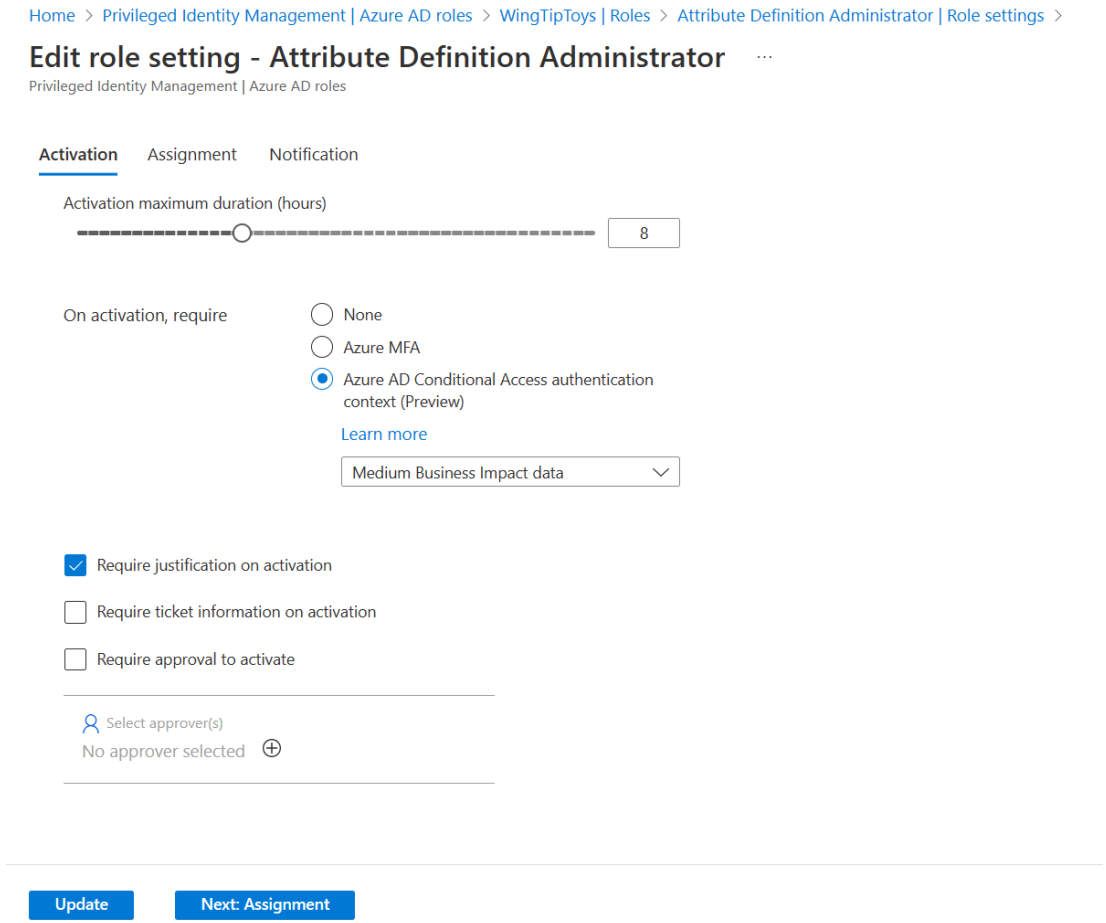
You can require users who are eligible for a role to satisfy conditional access policy requirements on elevation using Microsoft Entra ID Conditional Access Authentication Context.

This Allows administrators to add other security requirements through conditional access policies like:

- Require elevation only from Intune-compliant device
- Enforce specific strong authentication method like phishing resistant on role elevation

PIM + CA Integration

- Create Authentication Context
- Create CA policy with requirements using the authentication context
- Edit Role settings to require the CA policy on Activation



Join Entra ID Governance Advisors - Customer Community

What is Entra ID Governance Advisors

- Entra ID Governance Advisors is a community that consists of selected customers and partners who collaborate via virtual small/large group discussions, content reviews, digital forum and more

Benefits of Joining the Entra ID Governance Advisors:

- Members benefit by participating in the following ways:
- Direct engagement with Microsoft Product Groups
- Dedicated sessions focused on upcoming features and deep-dives
- Early access to Private Preview and Roadmap access
- Valuable inputs from Microsoft and other customers all under NDA
- Learn and interact with other customers across verticals, sizes, and segments\

- Please fill out the survey here if interested in joining: **https://aka.ms/MicrosoftEntraAdvisors/**

POC Deployment - Privileged Identity Management

Title	Link
Bring under Management	Azure Resources → Discover Azure resources to manage in PIM Groups → Bring groups into Privileged Identity Management
Set role settings	Azure AD Roles → Role settings for Azure AD roles Azure Resources → Role settings for Azure resource Roles Groups → Group settings for PIM
Assign	Azure AD Roles → Assign Azure AD roles in PIM Azure Resources → Assign Azure resources in PIM Groups → Assign Groups in PIM
Activate	Azure AD Roles → Activate Azure AD roles in PIM Azure Resources → Activate Azure resources in PIM Groups → Activate Groups in PIM
Approve	Azure AD Roles → Approve Azure AD roles in PIM Azure Resources → Approve Azure resources in PIM Groups → Approve Groups in PIM
Extend or Renew	Azure AD Roles → Extend Azure AD roles in PIM Azure Resources → Extend Azure resources in PIM Groups → Extend Groups in PIM
Review Access	Create Access Review → Create an access review Perform Access Review → Perform an access review Complete Access Review → Complete an access review
PIM + CA	Require Azure AD conditional access authentication context

Next Steps

Give us feedback, let us know your comments:
aka.ms/idnacat/igapocsurvey

Are you ready for deployment?


Thank you