**Research and Development Document**

**ON**

**Privileged Identity Management**

**as**

**Internship Project**

****

****

**By**

**Anirudh Sharma**

**(CT\_CSI\_CI\_66)**

**Under**

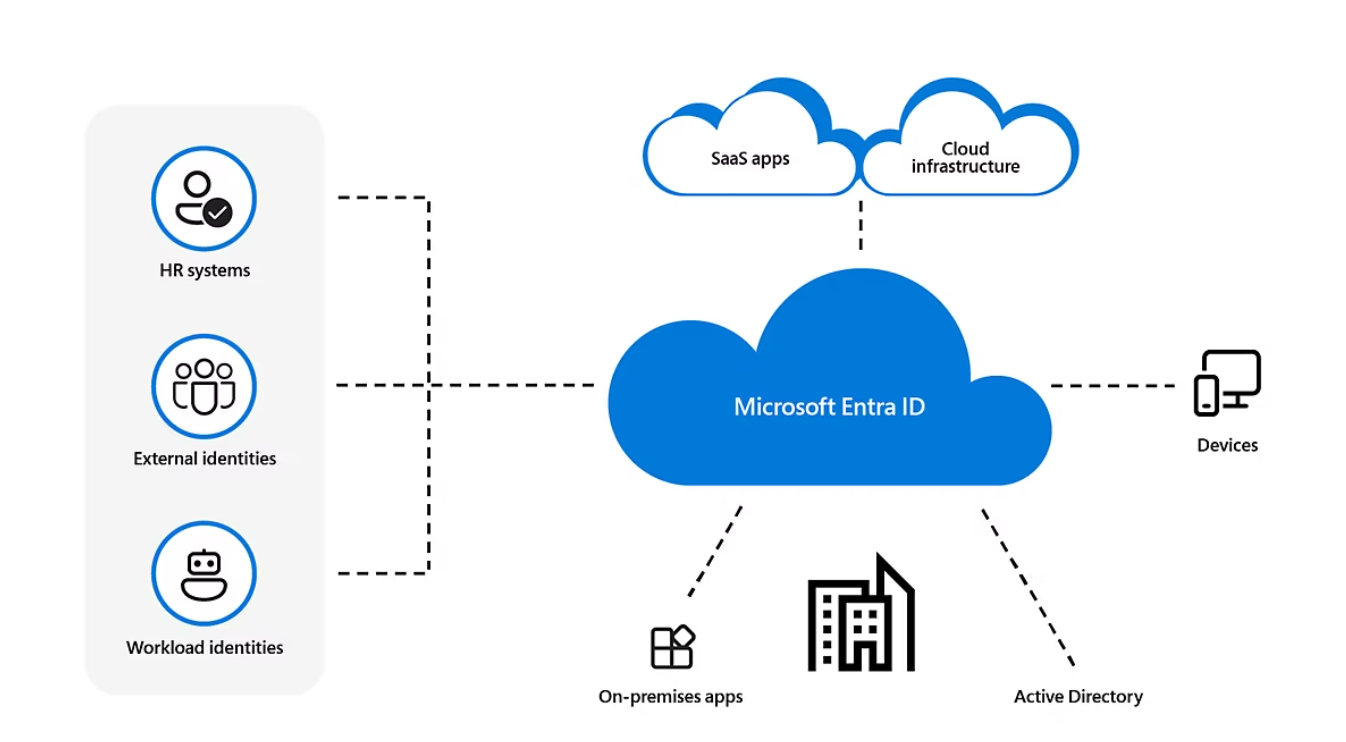
**Celebal Summer Internship**

**in**

**Cloud Infra & Security**

**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.**

**Microsoft Entra ID –** also known as **Azure Active Directory (AD),** is a cloud-based identity and access management service that helps organizations secure and manage user identities and access to resources



**Use of Azure Active Directory**

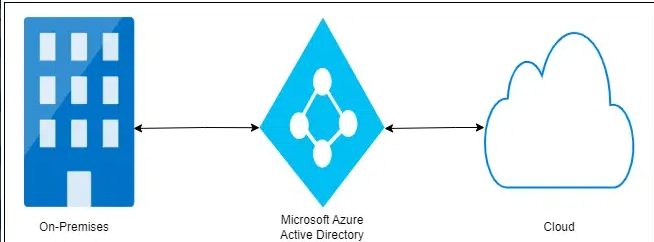
Suppose you have a large organization with a lot of developers. Some Azure services must be available to all developers for them to perform their responsibilities. When the administrator gives them a unique username and password for each service, they can access services like databases, virtual machines, or Azure storage services. It might be challenging for administrators and employees to manage many user logins at once.

Azure Active Directory (AD) enters the scene in this situation. Administrators can easily manage numerous user logins with Azure AD. To access each service, administrators must provide a single login and password in Azure. It is used by:

* Administrators
* Developers
* Users

**Structure of Azure AD/ Microsoft Entra ID:**

Azure Active Directory (Azure AD) is structured as a cloud-based directory and identity management service with a flat hierarchy. It organizes resources into tenants, where each tenant represents a dedicated and isolated instance of Azure AD. Within a tenant, **users**, **groups**, and **applications** are managed**. Users are individual accounts**, **groups are collections of users**, and **applications are registered entities that Azure AD can authenticate**. Additionally, administrators can set up roles and permissions to control access and enforce policies across these resources.



**Working of Azure AD/Microsoft Entra ID:**

Azure Active Directory (Azure AD) simplifies identity and access management in the cloud. Users authenticate with Azure AD credentials, enabling secure access to applications and services. Single sign-on (SSO) streamlines user experience by allowing access to multiple resources with one login. Robust security features like multifactor authentication (MFA) and access policies ensure secure access control. Azure AD Connect facilitates seamless integration between on-premises and cloud environments for unified identity management.

**Licensing of Microsoft Entra ID:**

**Licenses of Entra ID are:**

* **Microsoft Entra ID Free:**Provides user and group management, on-premises directory synchronization, basic reports, self-service password change for cloud users, and single sign-on across Azure, Microsoft 365, and many popular SaaS apps.
* **Microsoft Entra ID P1**: In addition to the Free features, P1 also lets your hybrid users access both on-premises and cloud resources. It also supports advanced administration, such as dynamic membership groups, self-service group management, Microsoft Identity Manager, and cloud write-back capabilities, which allow self-service password to reset for your on-premises users.
* **Microsoft Entra ID P2**: includes features in addition to the features included in Free and P1. P2 includes Microsoft Entra ID Protection to help provide risk-based Conditional Access to your apps and critical company data and Privileged Identity Management to help discover, restrict, monitor administrators, their access to resources and to provide just-in-time access when needed.

**In addition to Microsoft Entra ID licenses, you can enable additional identity management capabilities with licenses for other Microsoft Entra products, including:**

* **Microsoft Entra ID Governance. Microsoft Entra ID Governance is an advanced set of identity governance capabilities for Microsoft Entra ID P1 and P2 customers.**
* **"Pay as you go" feature licenses. You can also get licenses for features such as Microsoft Entra Domain Services, and Microsoft Entra customer identity and access management solution (CIAM). CIAM can help you provide identity and access management solutions for your customer-facing apps. For more information, see our next-generation solution for external identities, Microsoft Entra External ID.**

**Basic Terminology of Entra ID:**

* **Identity:** A thing that can get authenticated. An identity can be a user with a username and password. Identities also include applications or other servers that might require authentication through secret keys or certificates.
* **Account:** An identity that has data associated with it. You can’t have an account without an identity.
* **Microsoft Entra account:** An identity created through Microsoft Entra ID or another Microsoft cloud service, such as Microsoft 365. Identities are stored in Microsoft Entra ID and accessible to your organization's cloud service subscriptions. This account is also sometimes called a Work or school account.
* **Tenant:** A dedicated and trusted instance of Microsoft Entra ID. The tenant is automatically created when your organization signs up for a Microsoft cloud service subscription. These subscriptions include Microsoft Azure, Microsoft Intune, or Microsoft 365. This tenant represents a single organization and is intended for managing your employees, business apps, and other internal resources.

**Identity and Access Management**

**Identity and access management ensures that the right people, machines, and software components get access to the right resources at the right time. First, the person, machine, or software component proves they're who or what they claim to be. Then, the person, machine, or software component is allowed or denied access to or use of certain resources.**

**Identity**: A digital identity is a collection of unique identifiers or attributes that represent a human, software component, machine, asset, or resource in a computer system. An identifier can be:

* An email address
* Sign-in credentials (username/password)
* MAC address or IP address

**Identities are used to authenticate and authorize access to resources, communicate with other humans, conduct transactions, and other purposes.**

**there are three types of identities:**

* **Human identities**represent people such as employees (internal workers and frontline workers) and external users (customers, consultants, vendors, and partners).
* **Workload identities**represent software workloads such as an application, service, script, or container.
* **Device identities**represent devices such as desktop computers, mobile phones, IoT sensors, and IoT managed devices. Device identities are distinct from human identities.

**Authentication**

**Authentication is the process of challenging a person, software component, or hardware device for credentials to verify their identity or prove they're who or what they claim to be. Authentication typically requires the use of credentials**

**Multifactor authentication (MFA)** is a security measure that requires users to provide more than one piece of evidence to verify their identities, such as:

* Something they know, for example a password.
* **Something they are, like a biometric (fingerprint or face).**

**Single sign-on (SSO)** allows users to authenticate their identity once and then later silently authenticate when accessing various resources that rely on the same identity. Once authenticated, the IAM system acts as the source of identity truth for the other resources available to the user. It removes the need for signing on to multiple, separate target systems.

**Authorization: Authorization validates that the user, machine, or software component has been granted access to certain resources.**

**Authentication vs. authorization**

**The terms authentication and authorization are sometimes used interchangeably, because they often seem like a single experience to users. They're two separate processes:**

* Authentication proves the identity of a user, machine, or software component.
* Authorization grants or denies the user, machine, or software component access to certain resources.

**Identity provider:** identity provider creates, maintains, and manages

| **Authentication** | **Authorization** |
| --- | --- |
| * **Can be thought of as a gatekeeper, allowing access only to those entities who provide valid credentials.** | * **Can be thought of as a guard, ensuring that only those entities with the proper clearance can enter certain areas.** |
| * **Verifies whether a user, machine, or software is who or what they claim to be.** | * **Determines if the user, machine, or software is allowed to access a particular resource.** |
| * **Challenges the user, machine, or software for verifiable credentials (for example, passwords, biometric identifiers, or certificates).** | * **Determines what level of access a user, machine, or software has.** |
| * **Done before authorization.** | * **Done after successful authentication.** |
| * **Information is transferred in an ID token.** | * **Information is transferred in an access token.** |

identity information while offering authentication, authorization, and auditing services.

**Working of Identity and Access Management (IAM):**

* **Identity management -** The process of creating, storing, and managing identity information. **Identity providers** are software solutions that are used to track and manage user identities, as well as the permissions and access levels associated with those identities.
* **Provisioning and deprovisioning of users -** The process of creating and managing user accounts, which includes specifying which users have access to which resources and assigning permissions and access levels.
* **Authentication of users**- Authenticate a user, machine, or software component by confirming that they're who or what they say they are. **You can**
* **Authorization of users -** Authorization ensures a user is granted the exact level and type of access to a tool that they're entitled to. Users can also be portioned into groups or roles so large cohorts of users can be granted the same privileges.
* **Access control -** The process of determining who or what has access to which resources. This includes defining user roles and permissions, as well as setting up authentication and authorization mechanisms. Access controls regulate access to systems and data**.**
* **Reports and monitoring -** Generate reports after actions taken on the platform (like sign-in time, systems accessed, and type of authentication) to ensure compliance and assess security risks. Gain insights into the security and usage patterns of your environment.

**Authenticating, authorizing, and accessing resources:**

Suppose you have an application that signs in a user and then accesses a protected resource.

**A screenshot of a computer

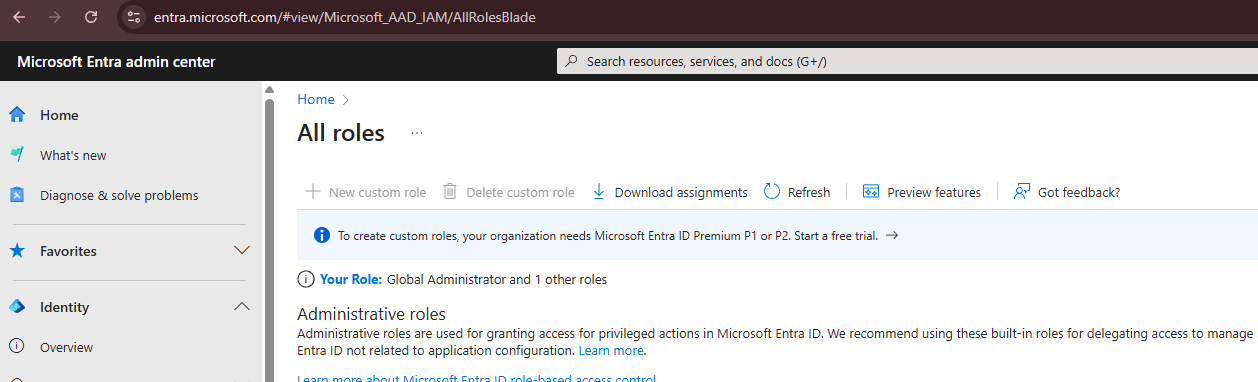
AI-generated content may be incorrect.**

1. The user (resource owner) initiates an authentication request with the identity provider/authorization server from the client application.
2. If the credentials are valid, the identity provider/authorization server first sends an ID token containing information about the user back to the client application.
3. The identity provider/authorization server also obtains end-user consent and grants the client application authorization to access the protected resource. Authorization is provided in an access token, which is also sent back to the client application.
4. The access token is attached to subsequent requests made to the protected resource server from the client application.
5. The identity provider/authorization server validates the access token. If successful the request for protected resources is granted, and a response is sent back to the client application.

**1.Setting up Pre-Requisites for Roles and Licences**

**Pre-Requisites for Privileged Identity Management are :**

* **Configured Entra ID**
* **P2 License**
* **Just In Time Access**

****

***A computer screen with text

AI-generated content may be incorrect.***

***Steps:***

1. ***Verify License***
   * ***Go to: Azure AD > Licenses > Overview***
   * ***Ensure Azure AD Premium P2 is assigned to users and admins.***
2. ***Check Required Roles***
   * ***You must be either:***
     + ***Global Administrator***
     + ***Privileged Role Administrator***
3. ***Consent to PIM***
   * ***Go to: Azure AD > Privileged Identity Management***
   * ***Click Consent to PIM if prompted.***
4. ***Enable PIM for Azure AD Roles***
   * ***Go to: PIM > Azure AD roles > Manage > Roles***
   * ***Click Discover roles > Select > Click Enable PIM.***
5. ***Enable PIM for Azure Resources (Subscriptions, Resource Groups)***
   * ***Go to: PIM > Azure resources***
   * ***Select the subscription > Click Manage resource>Enable PIM***

**2. Just In Time Access**

Just-In-Time Access is a security principle that ensures users get temporary privileged access only when they need it, for a limited duration and with justification and auditing. In Azure, JIT is implemented via Privileged Identity Management (PIM).

Instead of giving permanent admin roles, JIT ensures that:

* Privileged roles are assigned as eligible (not active).
* Users activate roles only when needed.
* Roles are time-limited and may require approval, MFA, and justification.

**Working of JIT:**

**Role Lifecycle in JIT**

1. **Assign Role as “Eligible”**
   * Role is not active by default.
   * User can request to activate when needed.
2. **User Requests Activation**
   * Go to Azure Portal > PIM > My roles
   * Click on an eligible role → Activate
3. **Activation Settings Are Checked**
   * MFA Prompt
   * Justification Field
   * Ticket ID (Optional)
   * Approval Workflow (Optional)
4. **Role Becomes Active for Limited Time**
   * E.g., 1 hour, 4 hours (configurable)
5. **Automatic Expiration**
   * After the time limit, access is revoked automatically.

**Automation Features**

* **Approval Workflow:**
  + Use internal or external approvers.
  + Useful for separation of duties.
* **Justification & Ticketing**:
  + Integrate with ITSM tools (e.g., ServiceNow).
  + Add custom fields for request tracking.
* **Notifications:**
  + Email alerts on activation, approval, expiration.
  + Forward to SOC/SIEM systems.
* **Access Reviews:**
  + Regularly review who has eligible roles.
  + Clean up unused eligibility.

***Steps:***

1. *Assign a user to a role as “Eligible”*
   * *Go to: PIM > Azure AD roles > Roles > [Select Role]*
   * *Click Add assignment*
   * *Choose Eligible > Select user > Set duration.*
2. *Test JIT Activation*
   * *Have the user go to: My roles in PIM*
   * *Click Activate > Provide justification*
   * *Perform MFA if prompted.*
3. *Set activation time limit*
   * *From the role settings (see step 10 below), configure max activation duration (e.g., 1 hour).*

**3.Configure Azure roles in Privileged Identity Management (PIM)**

**Privileged Identity Management support both built-in and custom Azure roles.**

**Role assignment conditions**

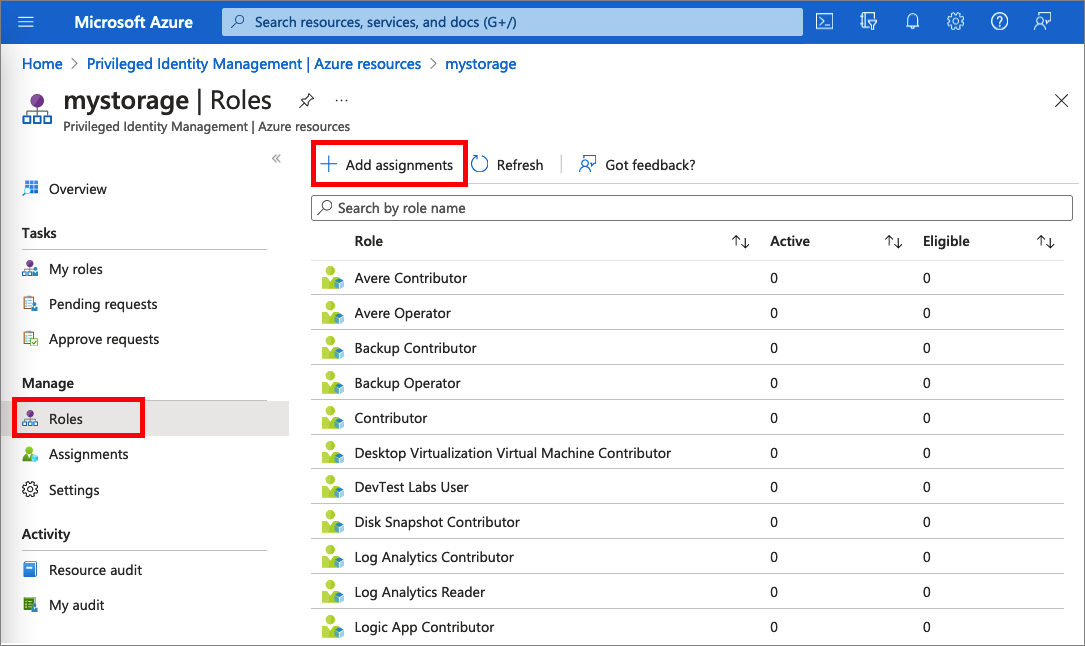
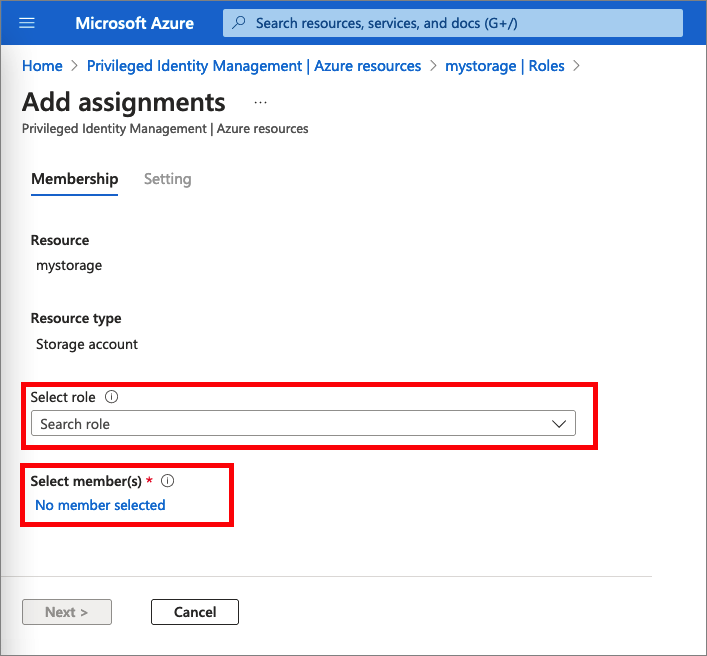
You can use the Azure attribute-based access control (Azure ABAC) to add conditions on eligible role assignments using Microsoft Entra PIM for Azure resources. With Microsoft Entra PIM, your end users must activate an eligible role assignment to get permission to perform certain actions. Using conditions in Microsoft Entra PIM enables you not only to limit a user's role permissions to a resource using fine-grained conditions, but also to use Microsoft Entra PIM to secure the role assignment with a time-bound setting, approval workflow, audit trail, and so on.

Note: When a role is assigned, the assignment:

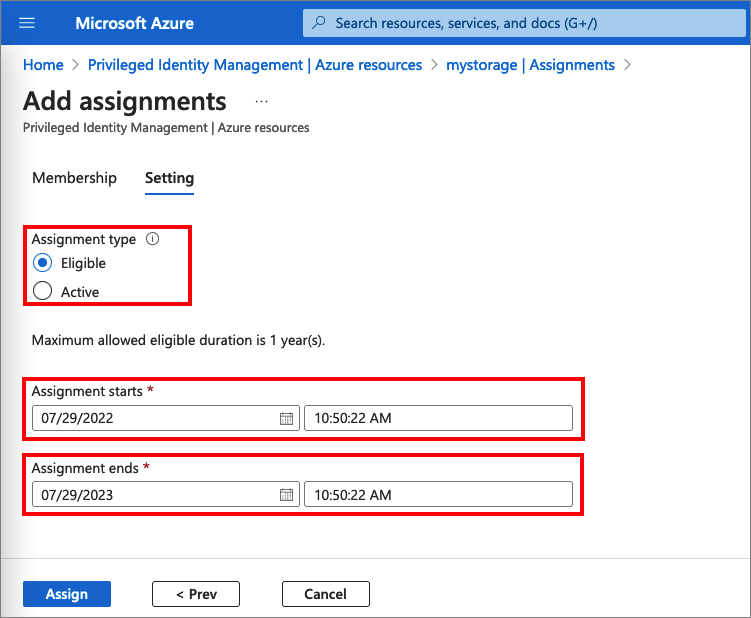
* Can't be assigned for a duration of less than five minutes
* Can't be removed within five minutes of it being assigned

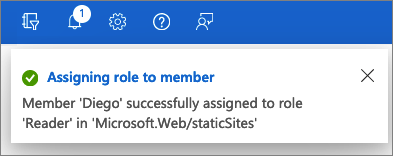
**Assigning a role**

1. Sign in to the Microsoft Entra admin center as at least a User Access Administrator.
2. Browse to ID Governance > Privileged Identity Management > Azure resources.
3. Select the resource type you want to manage. Start at either the Management group dropdown or the Subscriptions dropdown, and then further select Resource groups or Resources as needed. Select the Select button for the resource you want to manage to open its overview page.
4. Under Manage, select Roles to see the list of roles for Azure resources.
5. Select Add assignments to open the Add assignments pane.
6. Select a Role you want to assign.
7. Select No member selected link to open the Select a member or group pane.



1. Select a member or group you want to assign to the role and then choose Select.
2. On the Settings tab, in the Assignment type list, select Eligible or Active.
3. To specify a specific assignment duration, change the start and end dates and times.
4. If the role has been defined with actions that permit assignments to that role with conditions, then you can select Add condition to add a condition based on the principal user and resource attributes that are part of the assignment.



1. When finished, select Assign.
2. After the new role assignment is created, a status notification is displayed. 

Microsoft Entra PIM for Azure resources provide two distinct 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 multifactor 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 PIM.

**Update or remove an existing role assignment:**

1. Open Microsoft Entra Privileged Identity Management.
2. Select Azure resources.
3. Select the resource type you want to manage. Start at either the Management group dropdown or the Subscriptions dropdown, and then further select Resource groups or Resources as needed. Select the Select button for the resource you want to manage to open its overview page.
4. Under Manage, select Roles to list the roles for Azure resources. The following screenshot lists the roles of an Azure Storage account. Select the role that you want to update or remove.
5. Find the role assignment on the Eligible roles or Active roles tabs.
6. To add or update a condition to refine Azure resource access, select Add or View/Edit in the Condition column for the role assignment.
7. Select Add expression or delete to update the expression. You can also select Add condition to add a new condition to your role.

***Steps:***

1. *Go to: PIM > Azure AD Roles > Roles*
2. *Select a role (e.g., Global Administrator)*
3. *Click Add assignment*
4. *Choose:*
   * *Eligible for JIT access*
   * *Active for permanent access (not recommended)*
5. *Set:*
   * *Start/End Time*
   * *Require MFA*
   * *Justification*
6. *Click Assign*

**4. Configure Azure resources in PIM, including settings and assignments.**

Role settings define role assignment properties. These properties include multifactor authentication and approval requirements for activation, assignment maximum duration, and notification settings. This article shows you how to configure role settings and set up the approval workflow to specify who can approve or deny requests to elevate privilege.

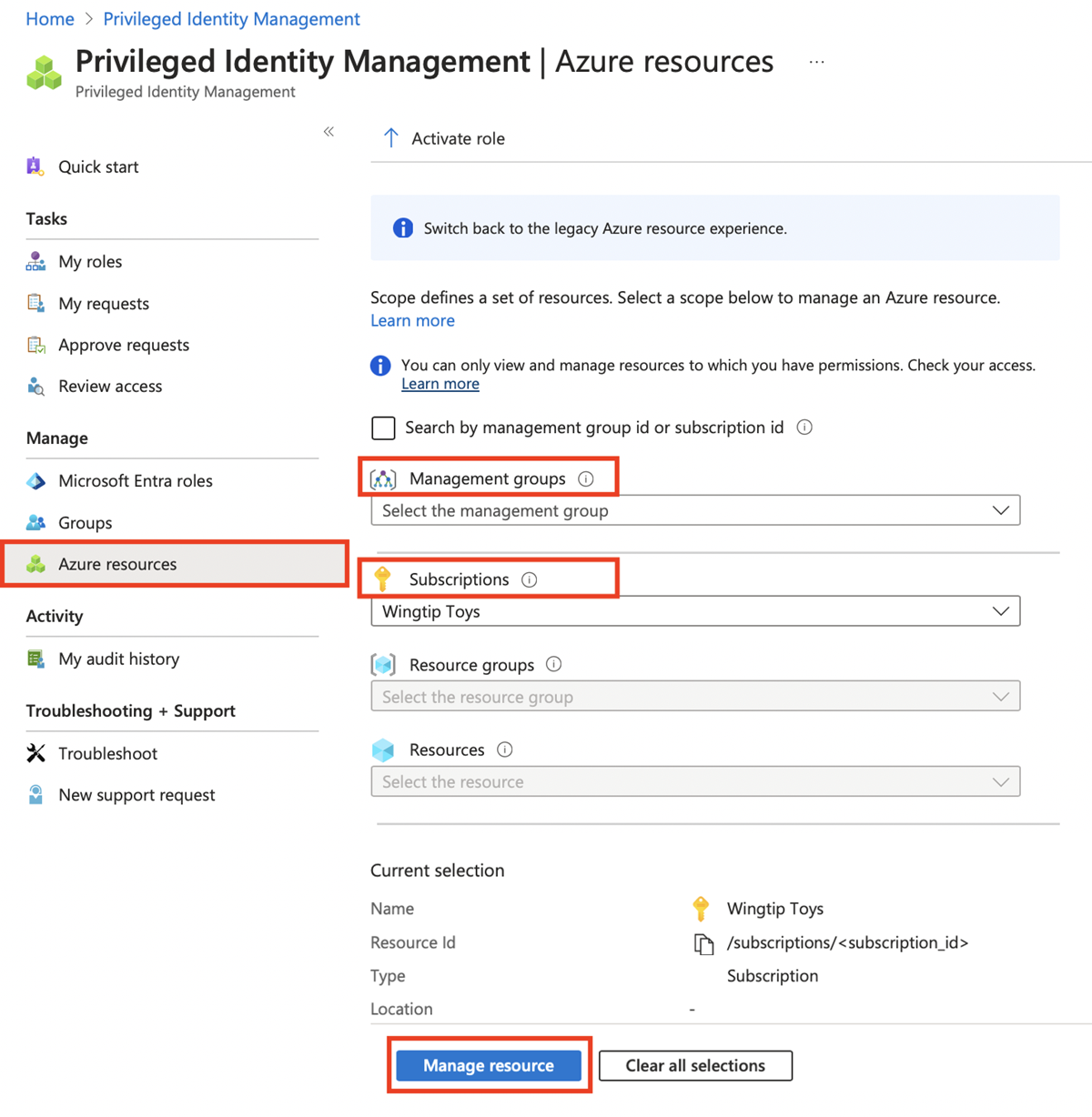
Role settings are defined per role and per resource. All assignments for the same role follow the same role settings. Role settings of one role are independent from role settings of another role. Role settings of one resource are independent from role settings of another resource. Role settings configured on a higher level, such as **Subscription**, for example, aren't inherited on a lower level, such as **Resource Group**.

PIM role settings are also known as PIM policies.

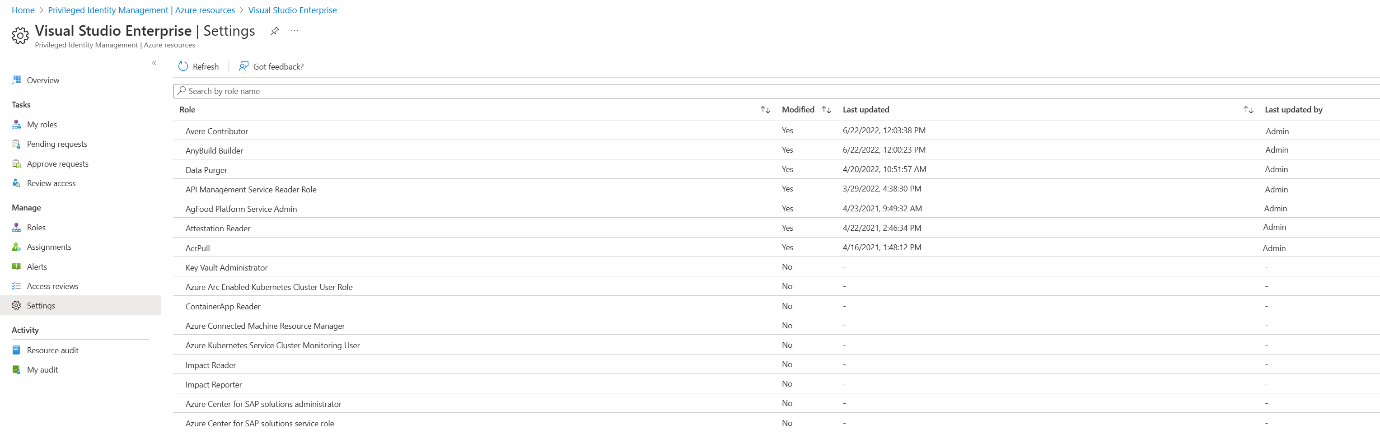
**Open role settings**

To open the settings for an Azure resource role:

1. Sign in to the Microsoft Entra admin center.
2. Browse to **ID Governance** > **Privileged Identity Management** > **Azure Resources**. You can select the **resource type** you want to manage. Start at either the Management group dropdown or the Subscriptions dropdown, and then select **Resource groups** or **Resources** as needed.

[](https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/media/pim-resource-roles-configure-role-settings/resources-list.png#lightbox)

1. Select the resource for which you need to configure PIM role settings.
2. Select **Settings**. View a list of PIM policies for a selected resource.

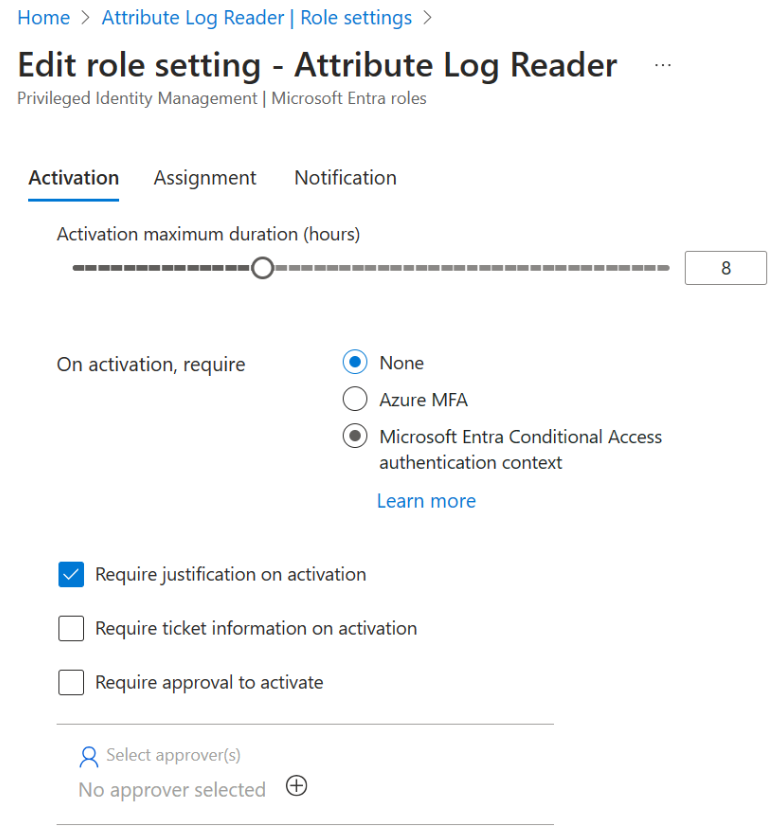
[](https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/media/pim-resource-roles-configure-role-settings/resources-role-settings.png#lightbox)

1. Select the role or policy that you want to configure.
2. Select **Edit** to update role settings.
3. Select **Update**.

**Activation maximum duration**

Use the Activation maximum duration slider to set the maximum time, in hours, that an activation request for a role assignment remains active before it expires. This value can be from 1 to 24 hours.

* **On activation, require multifactor authentication:** You can require users who are eligible for a role to prove who they are by using the multifactor authentication feature in Microsoft Entra ID before they can activate. Multifactor authentication helps safeguard access to data and applications. It provides another layer of security by using a second form of authentication.
* **On activation, require Microsoft Entra Conditional Access authentication context**: You can require users who are eligible for a role to satisfy Conditional Access policy requirements. For example, you can require users to use a specific authentication method enforced through Authentication Strengths, elevate the role from an Intune-compliant device, and comply with terms of use.
* Require justification on activation: You can require users to enter a business justification when they activate the eligible assignment.
* Require ticket information on activation: You can require users to enter a support ticket number when they activate the eligible assignment. This option is an information-only field. Correlation with information in any ticketing system isn't enforced.
* Require approval to activate: You can require approval for activation of an eligible assignment. The approver doesn't have to have any roles. When you use this option, you must select at least one approver.



***Steps:***

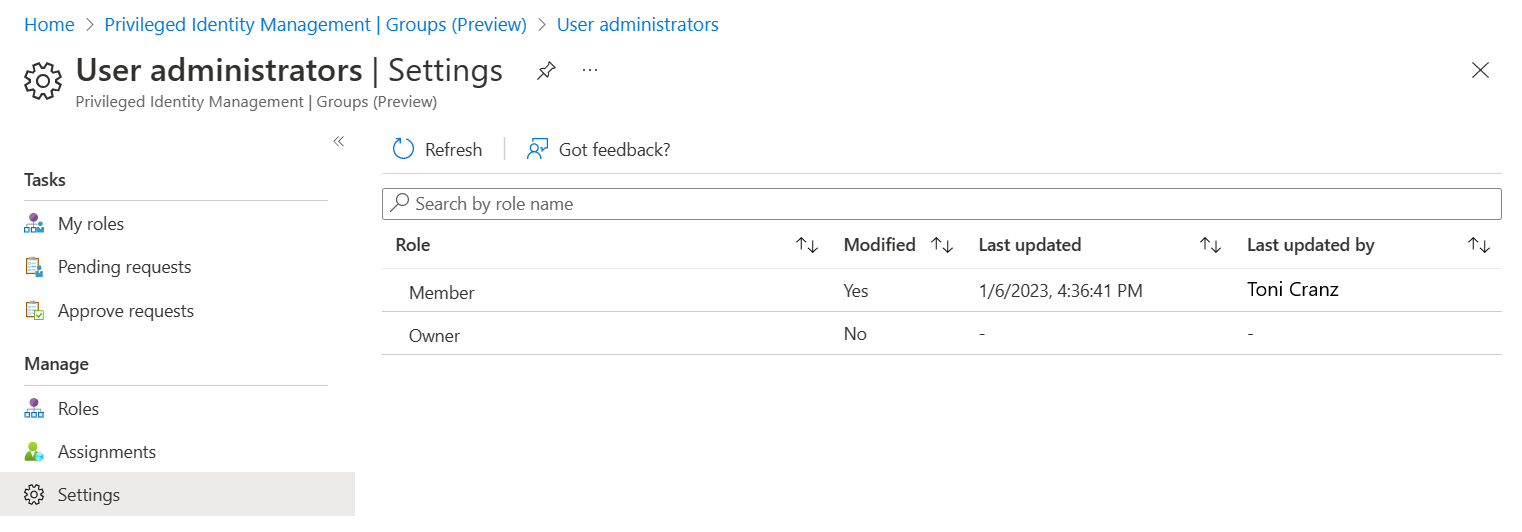
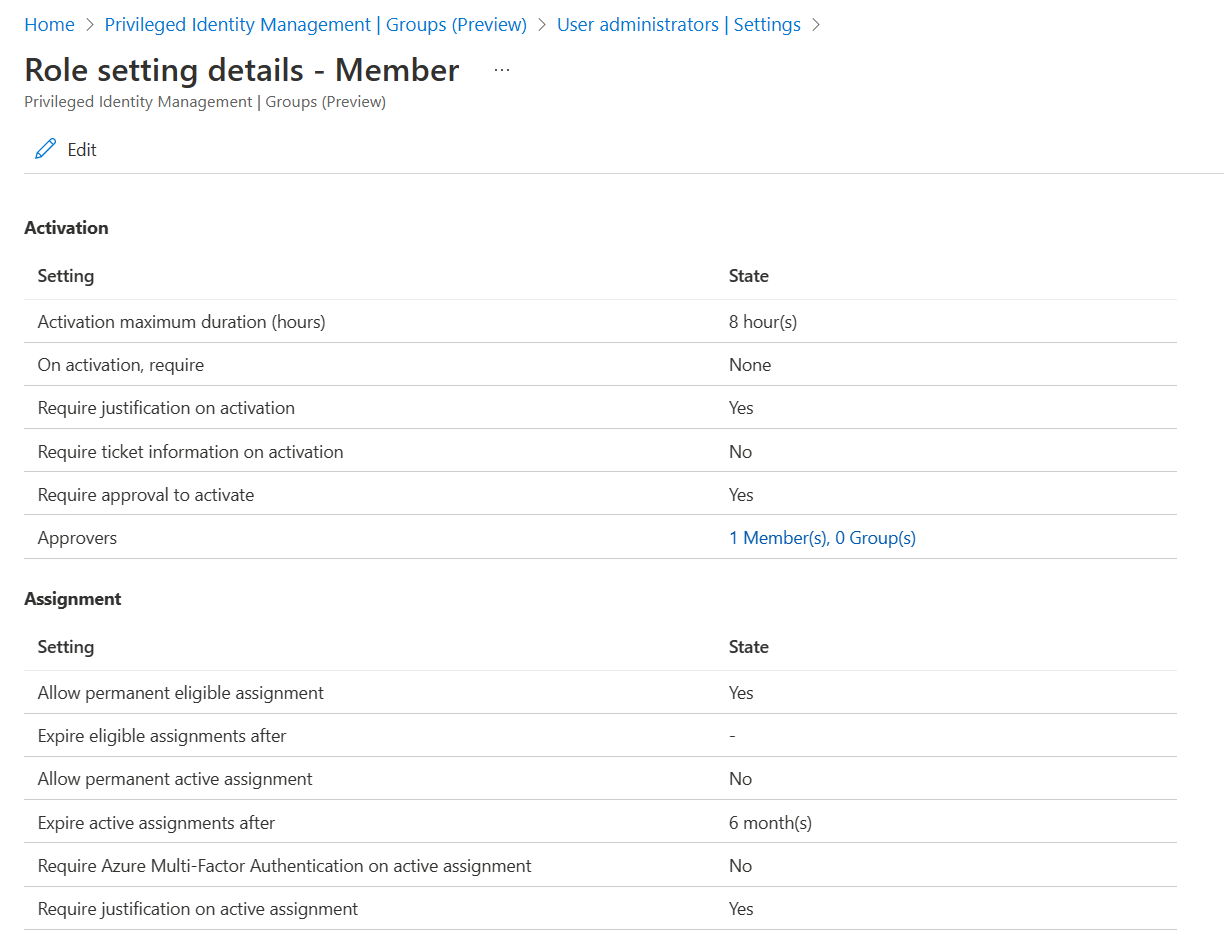
1. *Go to: PIM > Azure Resources*
2. *Select your* ***Subscription/Resource Group***
3. *Click* ***Manage resource*** *> Click* ***Enable PIM***
4. *Go to* ***Roles*** *> Select a role (e.g., Contributor)*
5. *Click* ***Add assignment***
6. *Choose:*
   * ***Eligible***
   * ***User or Group***
   * *Set* ***duration****,* ***MFA****,* ***approval****, etc.*

**5.Configure Privileged Access groups.**

**Assign an owner or member of a group:**

You need permissions to manage groups. For role-assignable groups, you need to be at least a Privileged Role Administrator role or be an Owner of the group. For non-role-assignable groups, you need to be at least a Directory Writer, Groups Administrator, or Identity Governance Administrator, User Administrator role, or be an Owner of the group. Role assignments for administrators should be scoped at directory level (not administrative unit level).

1. Sign in to the Microsoft Entra admin center
2. Browse to ID Governance > Privileged Identity Management > Groups.
3. Here you can view groups that are already enabled for PIM for Groups.
4. Select the group you need to manage.
5. Select Assignments.
6. Use Eligible assignments and Active assignments blades to review existing membership or ownership assignments for selected group.
7. Select Add assignments.
8. Under Select role, choose between Member and Owner to assign membership or ownership.
9. Select the members or owners you want to make eligible for the group.
10. Select Next.
11. In the Assignment type list, select Eligible or Active. Privileged Identity Management provides two distinct assignment types:
    * Eligible assignment requires member or owner to perform an activation to use the role. Activations may also require providing a multifactor authentication (MFA), providing a business justification, or requesting approval from designated approvers.
12. If the assignment should be permanent (permanently eligible or permanently assigned), select the Permanently checkbox. Depending on the group's settings, the check box might not appear or might not be editable. For more information, check out the Configure PIM for Groups settings in Privileged Identity Management article.



***Steps:***

1. ***Go to: Azure AD > Groups > New Group***
2. ***Create a Security Group***
   * ***Enable "Azure AD roles can be assigned to the group"***
3. ***Go to: PIM > Groups***
4. ***Select your group > Click Enable PIM***
5. ***Assign users as:***
   * ***Eligible Members (for JIT group membership)***
   * ***Set approval/MFA rules***
6. ***Assign roles to the group via:  
   Azure AD > Roles > [Select Role] > Assign to Group***

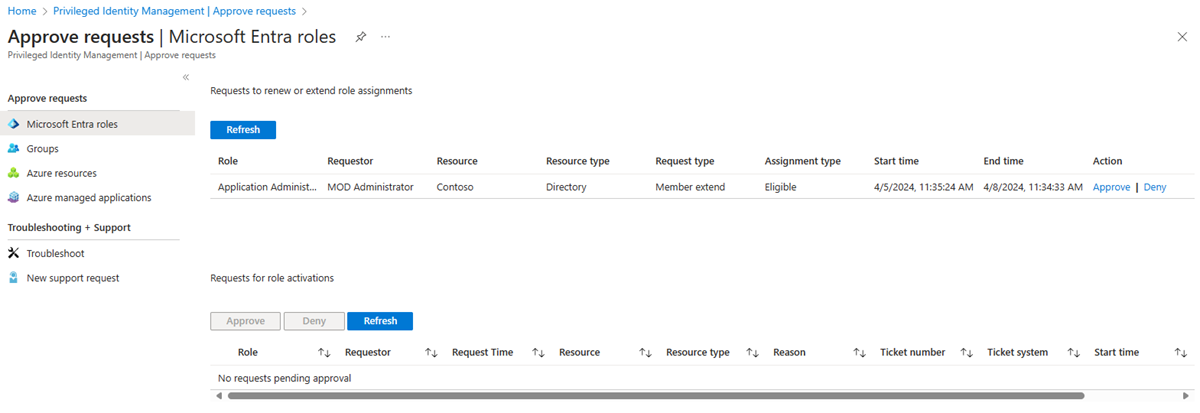
**6. Setting up PIM requests and approval process.**

**Azure resource roles in Privileged Identity Management**

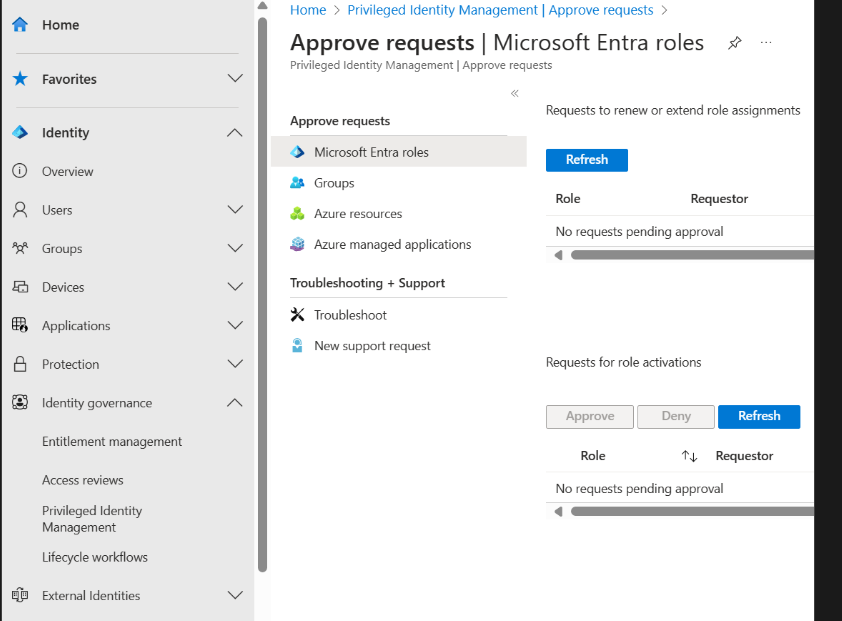
Microsoft Entra Privileged Identity Management (PIM) enables you to configure roles so that they require approval for activation and choose users or groups from your Microsoft Entra organization as delegated approvers. We recommend selecting two or more approvers for each role to reduce workload for the Privileged Role Administrator. Delegated approvers have 24 hours to approve requests. If a request isn't approved within 24 hours, then the eligible user must resubmit a new request. The 24-hour approval time window isn't configurable.

As a delegated approver, you receive an email notification when an Azure resource role request is pending your approval. You can view these pending requests in Privileged Identity Management.

1. Sign in to the Microsoft Entra admin center as at least a Privileged Role Administrator.
2. Browse to ID Governance > Privileged Identity Management > Approve requests.



In the Requests for role activations section, you see a list of requests pending your approval.



**Approve requests**

1. Find and select the request that you want to approve. An approve or deny page appears.
2. In the Justification box, enter the business justification.
3. Select Approve. You receive an Azure notification of your approval.

Deny requests

1. Find and select the request that you want to approve. An approve or deny page appears.
2. In the Justification box, enter the business justification.
3. Select Deny. A notification appears with your denial.

**Workflow notifications**

* Approvers are notified by email when a request for a role is pending their review. Email notifications include a direct link to the request, where the approver can approve or deny.
* Requests are resolved by the first approver who approves or denies.
* When an approver responds to the request, all approvers are notified of the action.
* Resource administrators are notified when an approved user becomes active in their role.

***Steps:***

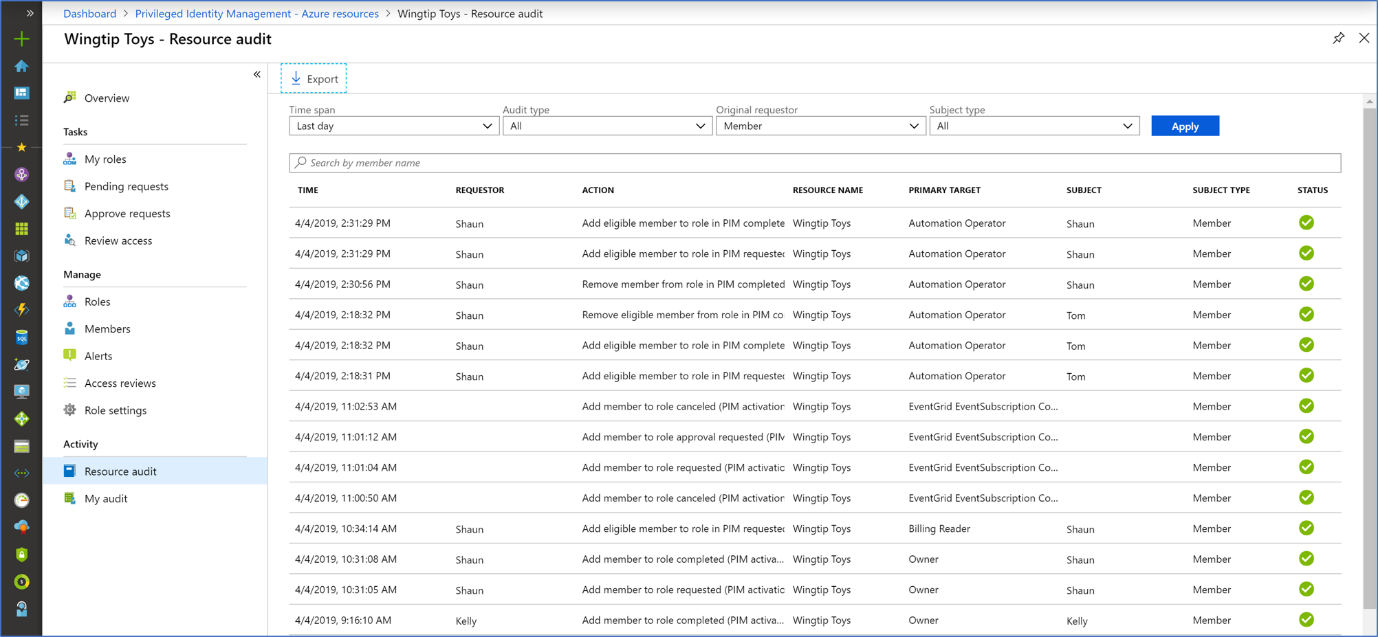
1. *Go to: PIM > Azure AD Roles > Roles > [Select Role]*
2. *Click* ***Settings***
3. *Under* ***Require approval to activate****, select* ***Yes***
4. *Add one or more* ***Approvers***
5. *Configure:*
   * ***Require MFA***
   * ***Justification***
   * ***Ticketing system ID (optional)***
6. *Click* ***Save***

**7.Analyze PIM audit history and reports**

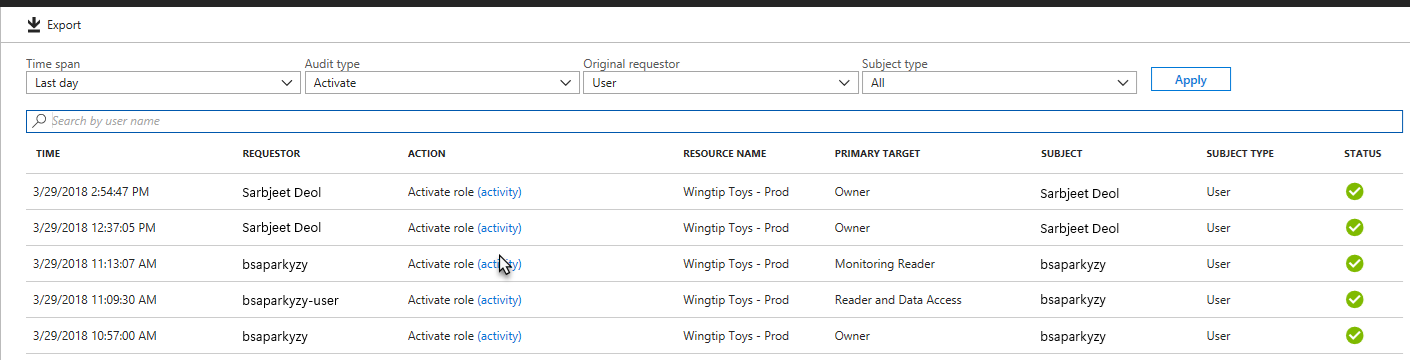
**View resource audit history**

Resource audit gives you a view of all role activity for a resource.

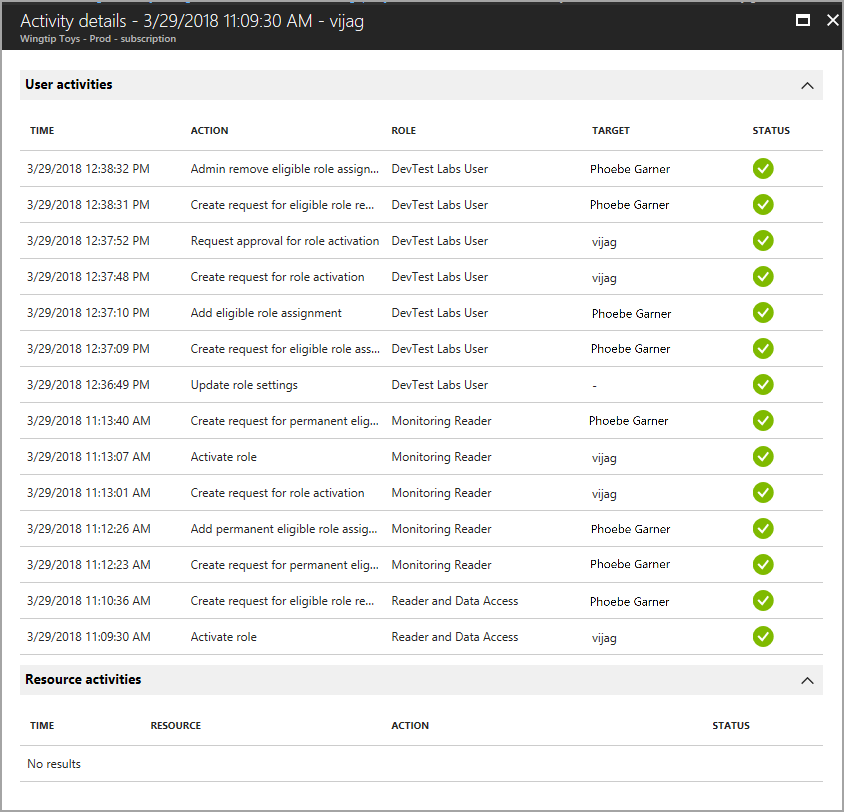
1. Sign in to the Microsoft Entra admin center as at least a Privileged Role Administrator.
2. Browse to **ID Governance** > **Privileged Identity Management** > **Azure resources**.
3. Select the resource you want to view audit history for.
4. Select **Resource audit**.
5. Filter the history using a predefined date or custom range.



1. For **Audit type**, select **Activate (Assigned + Activated)**.



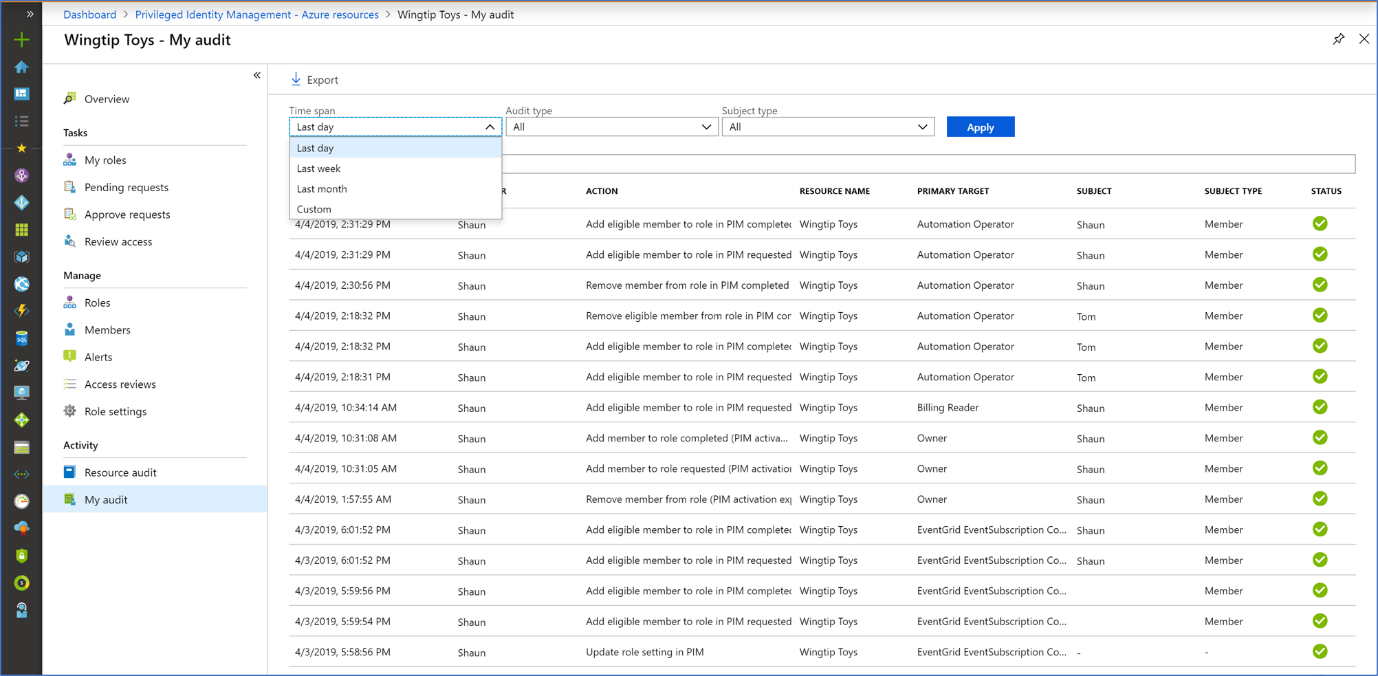
1. Under **Action**, select **(activity)** for a user to see that user's activity detail in Azure resources.



**View my audit**

My audit enables you to view your personal role activity.

1. Sign in to the Microsoft Entra admin center as at least a Privileged Role Administrator.
2. Browse to **ID Governance** > **Privileged Identity Management** > **Azure resources**.
3. Select the resource you want to view audit history for.
4. Select **My audit**.
5. Filter the history using a predefined date or custom range.



***Steps:***

1. *Go to: PIM > Audit History*
2. *Filter by:*
   * *Role*
   * *User*
   * *Activation status*
   * *Time range*
3. *Export audit logs as CSV*
4. *(Optional) Integrate with* ***Log Analytics****:*
   * *Go to: Azure Monitor > Diagnostic settings*
   * *Enable PIM logs to Log Analytics*
5. **Create and manage break-glass accounts**

**Break Glass Accounts:**

Break-glass accounts, also known as emergency access accounts, are crucial for maintaining access to systems and resources during emergencies **when standard access methods are unavailable**. These accounts should be carefully created and managed with strict security protocols to ensure they are only used when necessary. The term “break glass” originates from breaking the glass in an emergency to access a fire alarm.

Break-glass accounts are designed to provide a temporary, highly privileged means of access when standard administrative accounts are compromised or unavailable due to system outages, security breaches, or other unforeseen circumstances.

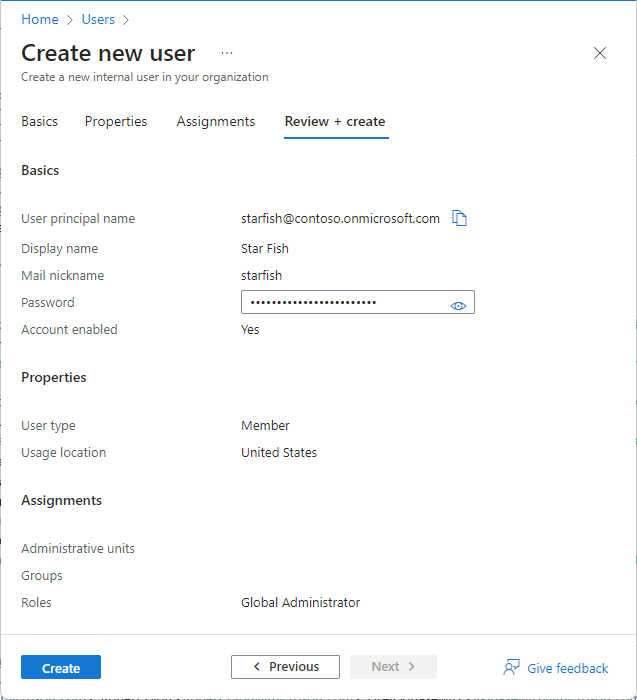
**When should we use a break glass account:**

* System Outages
* Network Failures
* Federation Service Failures
* Administrative Lockouts
* Cyberattacks
* Natural Disasters

**Creating emergency access accounts**

Create two or more emergency access accounts. These accounts should be cloud-only accounts that use the \*.onmicrosoft.com domain and that aren't federated or synchronized from an on-premises environment.

1. Find your existing emergency access accounts or create new accounts with the Global Administrator role.

[](https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/media/security-emergency-access/create-emergency-access-account.png#lightbox)

1. Select one of these passwords less authentication methods for your emergency access accounts. These methods satisfy the mandatory multifactor authentication requirements.
   * Passkey (FIDO2) (Recommended)
   * Certificate-based authentication if your organization already has a Public Key Infrastructure (PKI) setup
2. Configure your emergency access accounts to use password less authentication.
   * Enable passkeys (FIDO2) for your organization
   * Register a passkey (FIDO2)
   * Configure certificate-based authentication
3. Require phishing-resistant multifactor authentication for all your emergency accounts.
4. Store account credentials safely.
5. Monitor sign-in and audit logs.
6. Validate accounts regularly.

**Configuration requirements**

When you configure these accounts, the following requirements must be met:

* **Not tied to individuals**

Accounts shouldn't belong to specific users.

Credentials should be stored securely and accessible to multiple admins.

* **Alternatively: Individual accounts allowed**

You *can* assign personal emergency accounts to admins for accountability and remote access.

* **Use different strong authentication**

Don’t use the same MFA method as regular admin accounts.

* **Avoid expiring or auto-cleanup risks**

Credentials must not expire or get deleted due to inactivity.

* **Make role assignments permanent**

In PIM, assign the **Global Administrator role as permanently active** (not eligible).

* **Use secure devices only**

**Monitoring Emergency Account Activity:**

1. Sign in to the Azure portal with a user administrator role.
2. Select Azure Active Directory.
3. From the menu on the left, select Users.
4. Find the emergency account and select the user’s name.
5. Copy and save the Object ID attribute for future use.
6. Repeat the above steps for the second emergency account.

**Creating the Alert Log**

1. Sign in with an Azure Portal account assigned to the Monitoring Contributor role in Azure Monitor.
2. In the portal, click on All Services. In the search, type, Log Analytics.
3. Select Log Analytics workspaces and then select a workspace\*\*. \*\*
4. In the workspace, select Alerts, then click on New Alert Rule.
5. Check under Resource that the subscription is the one you are associating with the alert rule. Under Condition, select Add.
6. Under Signal Name, select Custom Log Search.
7. Search Query, enter the information
8. Under Alert Logic, enter the information, as shown below

on: Number of results Operator: Greater than Threshold value: 0

1. Under Evaluated Based On, select the Period (in minutes) on the desired length of time the query will run and the Frequency (in minutes) for how often it should run. The frequency should be less than or equal to the period.

10.Click on Done. The estimated monthly cost of the alert is now viewable.

**Creating an Action Group**

The next step is to select an action group of users who will receive alert notifications. If not previously complete, action groups configure as follows:

1. Select **Create an**
2. **Action Group. A set of fields to complete will appear.**
3. **Under Action Group Name,** enter the full description of the group, such as who is notified. Under **Short Name**, give a shorter name to describe the group.
4. Verify the information in the **Subscription** and **Resource Group** fields is correct.
5. For **Action Type**, select **Email/SMS/Push/Voice.** For **Action Name,** enter the event, such as Notify global admin\*\*.\*\*
6. Under **Edit Details**, enter the notification method, along with the necessary contact information. Click on **OK** to save this information.
7. With additional actions, enter the information before selecting **OK**.

**Customizing Notifications**

1. After the creation and selection of the action group, the notification actions can be set up under **Customize Actions**. Under **Alert Details**, specify the alert rule name. Add an optional description here.
2. Set the event’s **Severity Level**. Microsoft recommends using Critical (Sev 0).
3. Under **Enable Rule Upon Creation,** this should be set to **Yes.**
4. The **Suppress Alerts** checkbox can be checked to turn off the alerts. Enter the duration of time before the next alert event and select **Save**.

**9.Exploring Active and Eligible Roles**

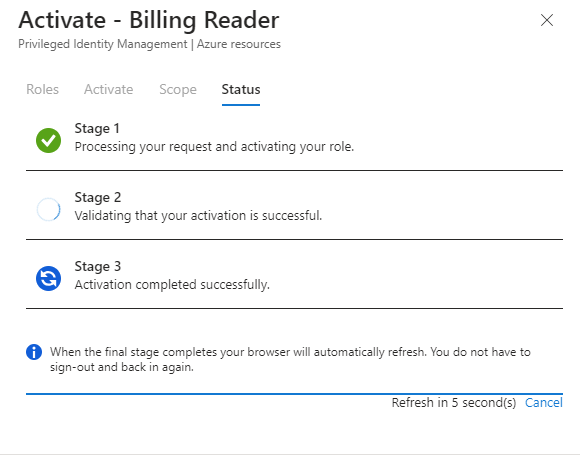
In Azure's Privileged Identity Management (PIM), roles can be assigned as either eligible or active. Eligible roles require users to activate the role when they need to perform privileged tasks, often requiring multi-factor authentication or justification. Active roles grant users immediate and continuous access to the role's privileges.

**Eligible Roles:**

* **Just-in-time access:** Users are not permanently assigned to the role and must activate it when needed.
* **Activation process:** Activation may involve MFA, justification, or approval from designated approvers.
* **Time-bound:** Can be configured with start and end dates for activation.

**Example:** A user might be eligible for the "Global Administrator" role, requiring them to activate it before making changes to tenant-wide settings.

**Active Roles:**

* **Permanent access:** Users are immediately granted the role's privileges without activation.
* **Continuous access:** Privileges are always available without any activation steps.
* **Time-bound:** Can be configured with start and end dates for the assignment.
* **Example:** A user might be actively assigned the "Reader" role, allowing them to view resources without needing to activate anything. 

|  |  |  |
| --- | --- | --- |
| **Feature** | **Eligible Roles** | **Active Roles** |
| Activation Required | Yes | No |
| Access Type | Just-in-time | Continuous |
| Security Benefit | Reduced risk by limiting access | Simplified access for frequently used roles |
| Use Case | Privileged tasks requiring review and approval | Frequent access to resources with defined scope |

**10.Setting up time bounds for Roles**

**Control how long a user stays in a privileged role.**

In Azure, you can set time limits for role assignments using Privileged Identity Management (PIM) for Azure resources. This allows you to configure the maximum duration an active role assignment can last before expiring and also manage the duration for which a user is eligible to activate a role.

*Steps:*

1. *Go to: PIM > Azure AD roles > Roles*
2. *Click Settings*
3. *Set:*
   * *Activation maximum duration (e.g., 1 or 4 hours)*
   * *Start/End dates (in assignment)*
4. *Save the settings*

**NOTE: Max duration can range from 0.5 to 24 hours**

**References**

* + **Microsoft Documentation**
  + **Medium**
  + **John Savill’s Videos**
  + **Geeks for Geeks**
  + **AgileIT**
  + **AZ-900 Certification Modules**