

Privileged identity management (Task)

Contents :-

- 1) Objective of the task
- 2) What is PIM
- 3) Key Features of PIM
- 4) Practical Implementation of the task
- 5) Conclusion
- 6) References

Objective of the task

Perform a privileged identity management task and assign users roles on subscription and AD (Active Directory). Users must request the roles that are assigned to it and the role is approved by the specific approver.

What is PIM

Privileged Identity Management (PIM) in Azure is a service that helps organizations manage, control, and monitor access to important resources within their Azure environment. It focuses on securing privileged identities, such as administrators and other high-level users, who have access to critical Azure resources and configurations. By using PIM, organizations can minimize the risk of unauthorized access, potential

misuse of privileges, and better adhere to security and compliance requirements.

Key Features of PIM

Just-In-Time (JIT) Access: PIM allows administrators to assign time-bound, on-demand access to specific Azure roles. This means that users won't have constant privileged access but can activate it for a defined period when needed, reducing the attack surface.

Time-Bound Access: Instead of having constant privileged access, users can be granted elevated permissions for a limited time. After the specified time expires, their privileges are automatically revoked until they request access again.

Approval Workflow: For certain high-privileged roles, PIM can enforce an approval process. When a user requests access to a privileged role, an assigned approver must review and approve the request before the user gains the elevated permissions.

Privileged Role Auditing: PIM provides detailed auditing and logging capabilities, allowing organizations to track who activated privileged roles,

when, and for what purposes. This helps in monitoring and identifying potential security risks.

Privileged Role Auditing: PIM provides detailed auditing and logging capabilities, allowing organizations to track who activated privileged roles, when, and for what purposes. This helps in monitoring and identifying potential security risks.

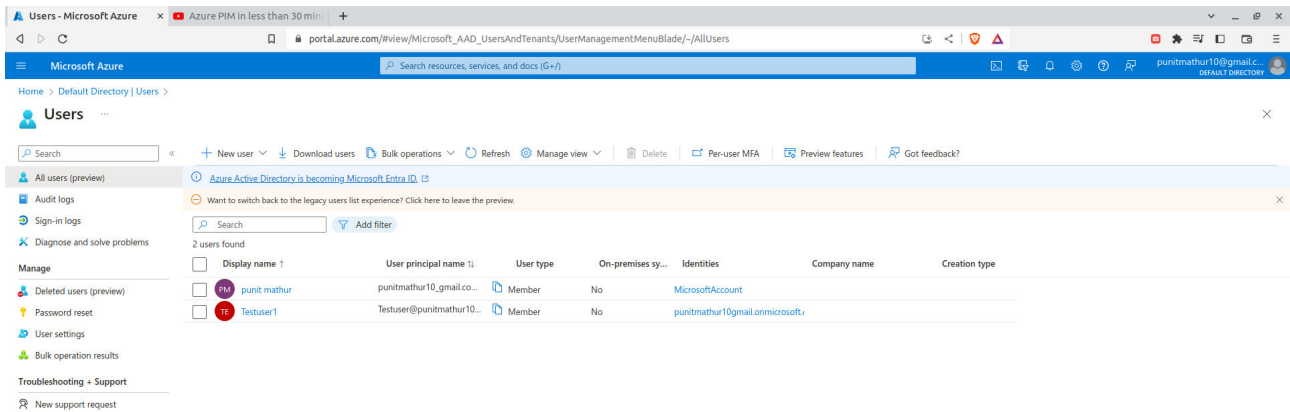
Just-Enough-Administration (JEA): PIM helps enforce the principle of least privilege by limiting the scope of administrative actions to only what is necessary for users to perform their specific tasks.

Security Reports and Alerts: The service provides security reports and alerts to notify administrators of any suspicious or potentially risky activities related to privileged roles.

Azure AD Integration: PIM seamlessly integrates with Azure Active Directory (Azure AD), which is the identity and access management service for Azure. It builds upon the existing Azure AD roles and enhances them with privileged access management features.

Practical Implementation of the task

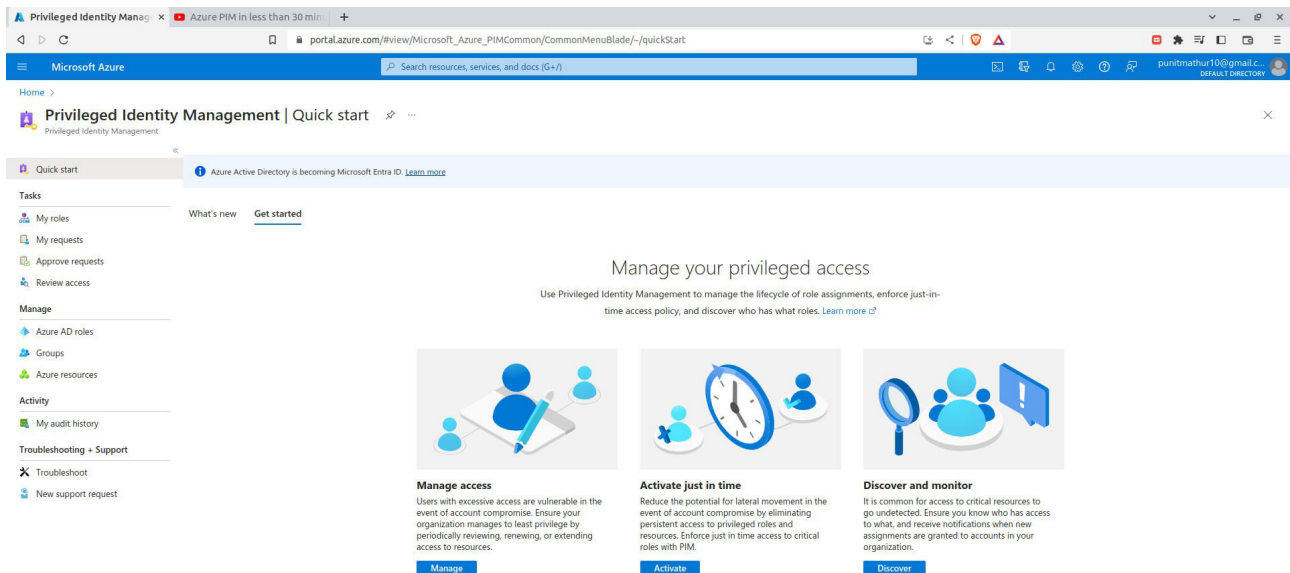
Create a user



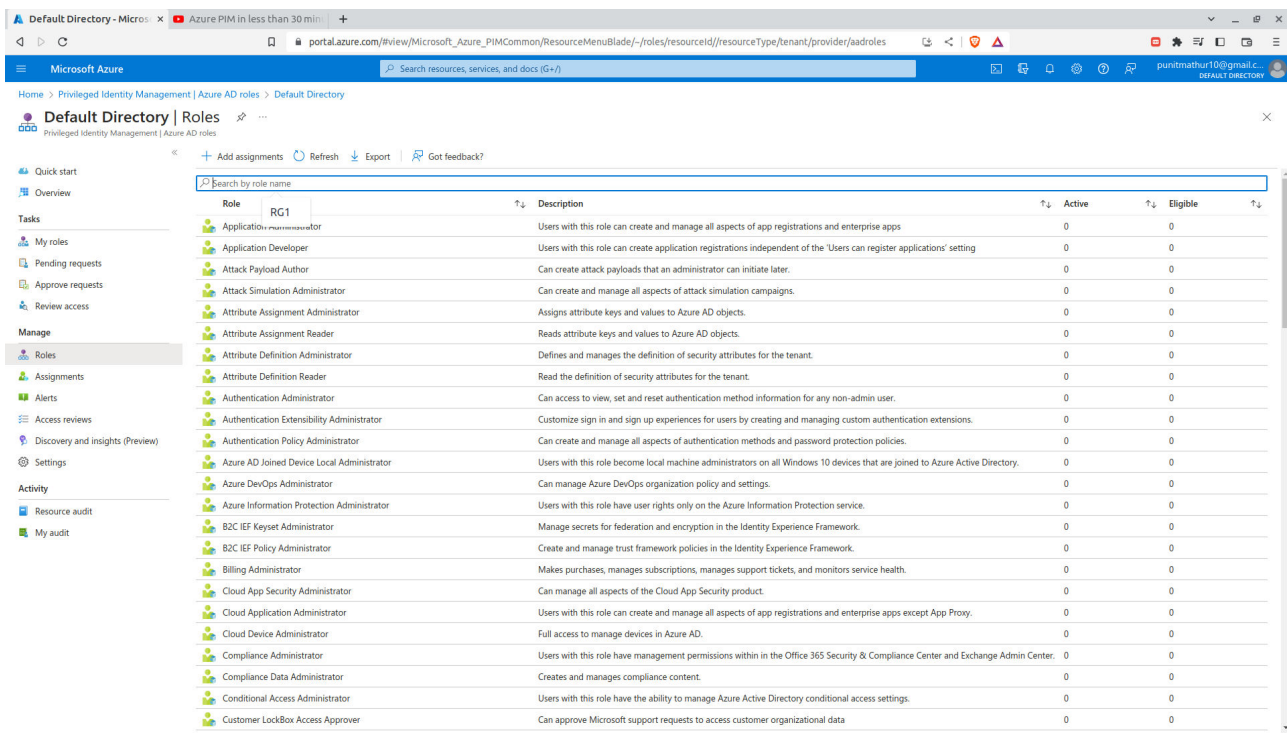
The screenshot shows the Microsoft Azure portal's 'Users' management page. The interface includes a left-hand navigation menu with options like 'All users (preview)', 'Audit logs', 'Sign-in logs', 'Diagnose and solve problems', 'Manage', 'Deleted users (preview)', 'Password reset', 'User settings', 'Bulk operation results', 'Troubleshooting + Support', and 'New support request'. The main content area displays a table of users with columns for 'Display name', 'User principal name', 'User type', 'On-premises sy...', 'Identities', 'Company name', and 'Creation type'. Two users are listed: 'punit mathur' and 'Testuser1'. A notification banner at the top indicates 'Azure Active Directory is becoming Microsoft Entra ID'. A search bar and various action buttons (New user, Download users, Bulk operations, Refresh, Manage view, Delete, Per-user MFA, Preview features, Got feedback?) are located at the top of the main content area.

| Display name ↑ | User principal name ↑ | User type | On-premises sy... | Identities | Company name | Creation type |
|----------------|----------------------------|-----------|-------------------|-----------------------------------|--------------|---------------|
| punit mathur | punitmathur10_gmail.co... | Member | No | MicrosoftAccount | | |
| Testuser1 | Testuser1@punitmathur10... | Member | No | punitmathur10gmail.onmicrosoft... | | |

After creating a user go to Privileged identity management. You can directly search for PIM in search bar of azure portal.



Now Go to Roles in PIM (Home > PIM | Azure AD Roles > Default Directory)



Assign roles as you wish (Here for use case we've chosen User Administrator)

Home > PIM | Azure AD Roles > Default Directory | Roles > User Administrator | Assignments

Add assignments

Privileged Identity Management | Azure AD roles

Membership | Setting

You can also assign roles to groups now. [Learn more](#)

Resource
Default Directory

Resource type
Directory

Select role
User Administrator

Scope type
Directory

Select member(s)
1 Member(s) selected

Selected member(s)
Testuser1
Testuser1@punitmathur10@gmail.onmicrosoft.com

[Remove](#)

[Next >](#) [Cancel](#)

Now click on edit in role settings

User Administrator | Role settings

Privileged Identity Management | Azure AD roles

[Edit](#)

Manage

- Assignments
- Description
- Role settings**

Activation

| Setting | State |
|--|-----------|
| Activation maximum duration (hours) | 8 hour(s) |
| On activation, require | Azure MFA |
| Require justification on activation | Yes |
| Require ticket information on activation | No |
| Require approval to activate | No |
| Approvers | None |

Assignment

| Setting | State |
|--|-------|
| Allow permanent eligible assignment | Yes |
| Expire eligible assignments after | - |
| Allow permanent active assignment | Yes |
| Expire active assignments after | - |
| Require Azure Multi-Factor Authentication on active assignment | No |
| Require justification on active assignment | Yes |

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

| Type | Default recipients | Additional recipients | Critical emails only |
|--|--------------------|-----------------------|----------------------|
| Role assignment alert | Admin | None | False |
| Notification to the assigned user (assignee) | Assignee | None | False |
| Request to approve a role assignment renewal/extension | Approver | None | False |

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

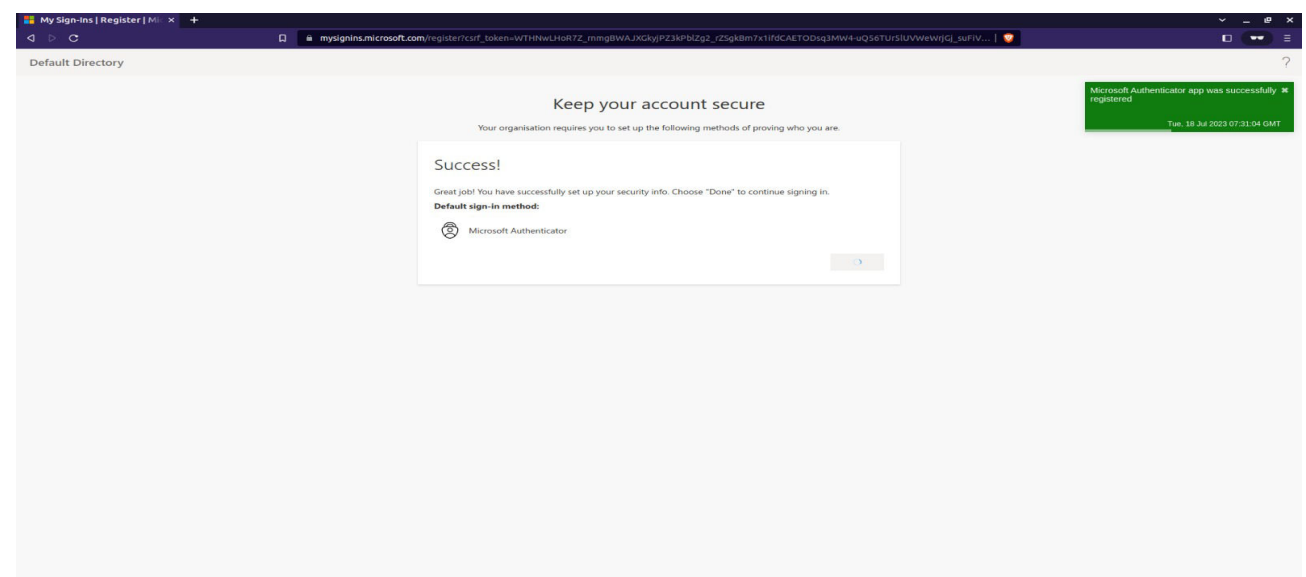
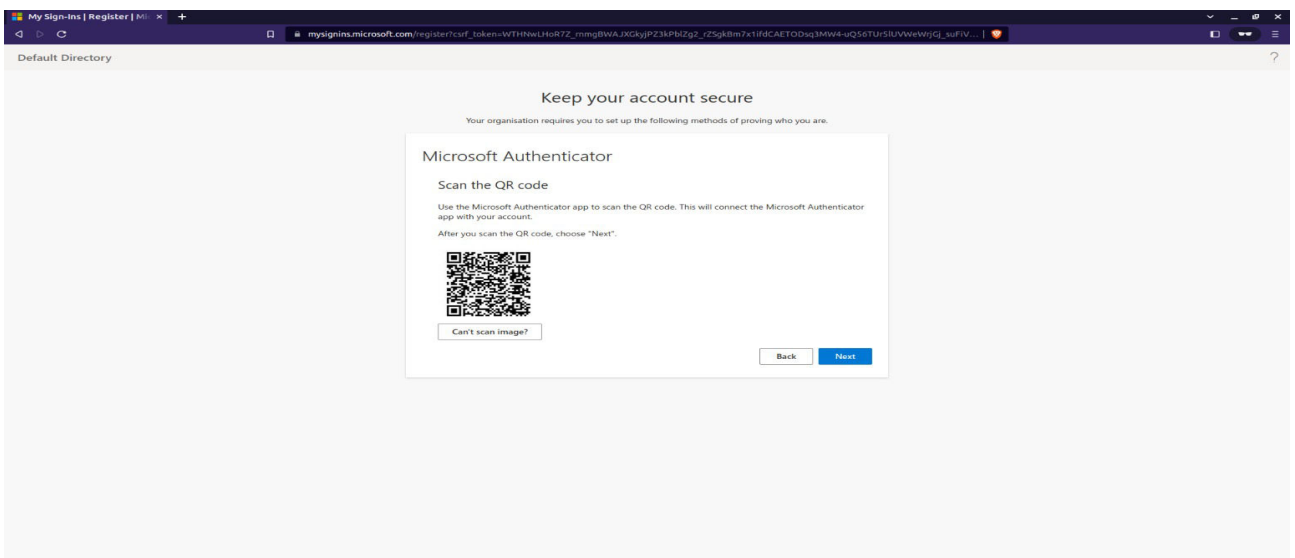
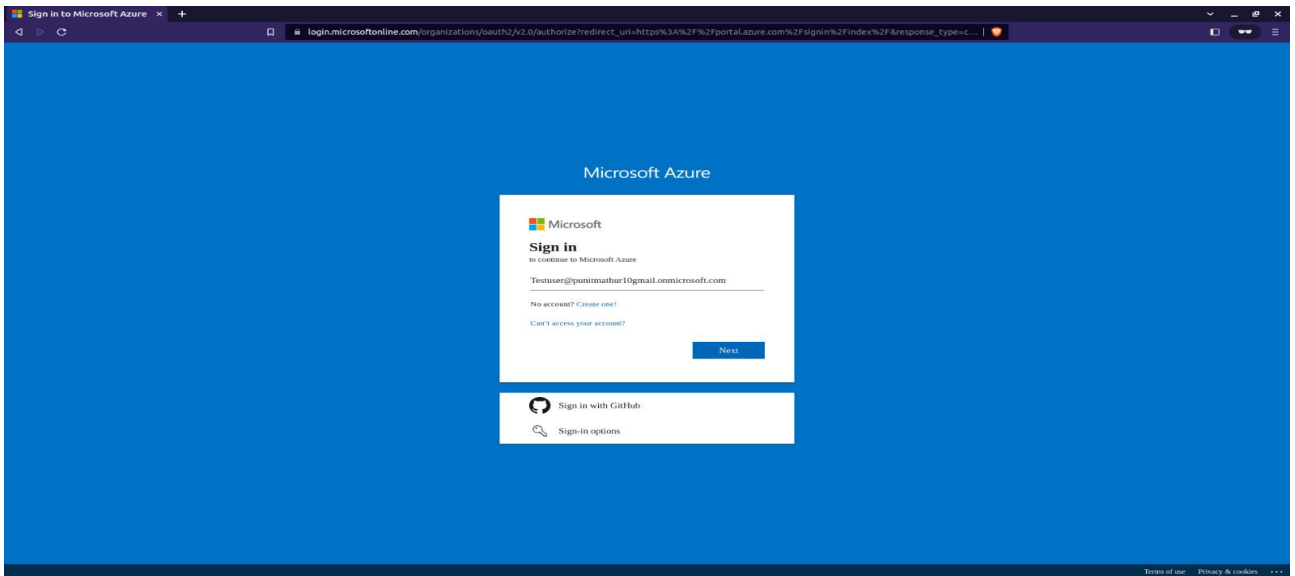
| Type | Default recipients | Additional recipients | Critical emails only |
|-----------------------|--------------------|-----------------------|----------------------|
| Role assignment alert | Admin | None | False |

Now Click on Require approval to activate. Adding this feature will make sure that anytime a request comes from user end , it first gets approval from global admin. For extra security enable Multi Factor Authentication (Azure MFA). Now click on update.

The screenshot shows the Microsoft Azure portal interface. On the left, the 'Edit role setting - User Administrator' page is visible, with the 'Activation' tab selected. Under 'On activation, require', the 'Azure MFA' option is selected. The 'Require approval to activate' checkbox is checked. A 'Select a member' dialog is open on the right, showing a list of users and groups. The user 'punit mathur' is selected. The dialog also shows a search bar and a 'Selected (1)' section.

| Name | Type | Details |
|--|-------|---|
| <input checked="" type="checkbox"/> punit mathur | User | punitmathur10@gmail.com |
| <input type="checkbox"/> TestGroup | Group | |
| <input type="checkbox"/> TestGroup2 | Group | |
| <input type="checkbox"/> Testuser1 | User | Testuser@punitmathur10gmail.onmicrosoft.com |

Now login to your Test User account using MFA. The first time MFA will make you scan a QR code and make sure that the right user is logged in it do this by using Microsoft Authenticator app. Enabling MFA increases the security and maintain a certain level of integrity in the child users.

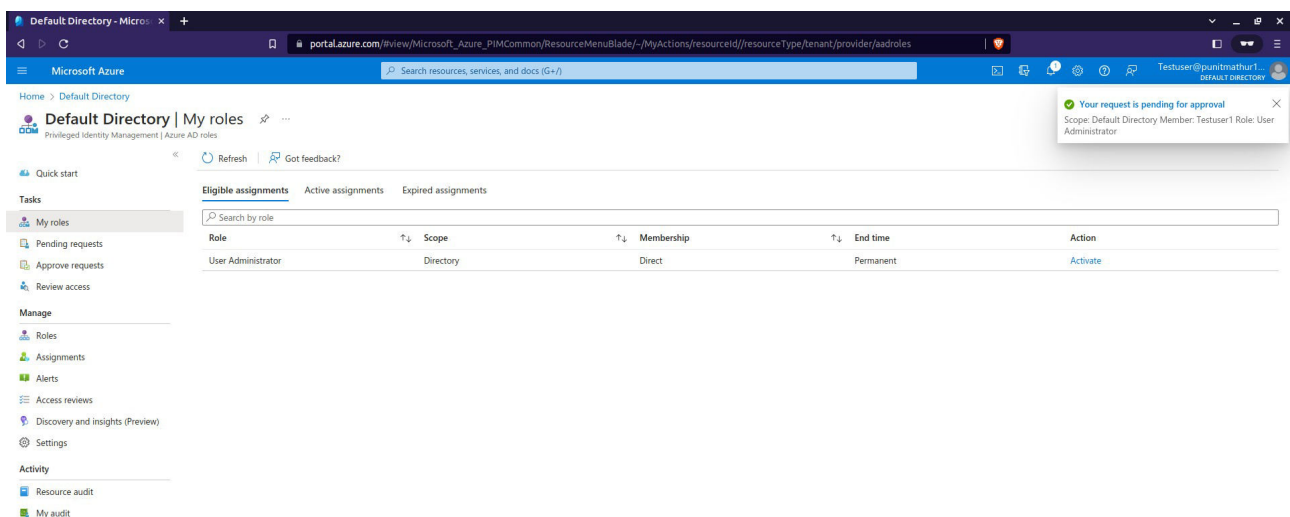
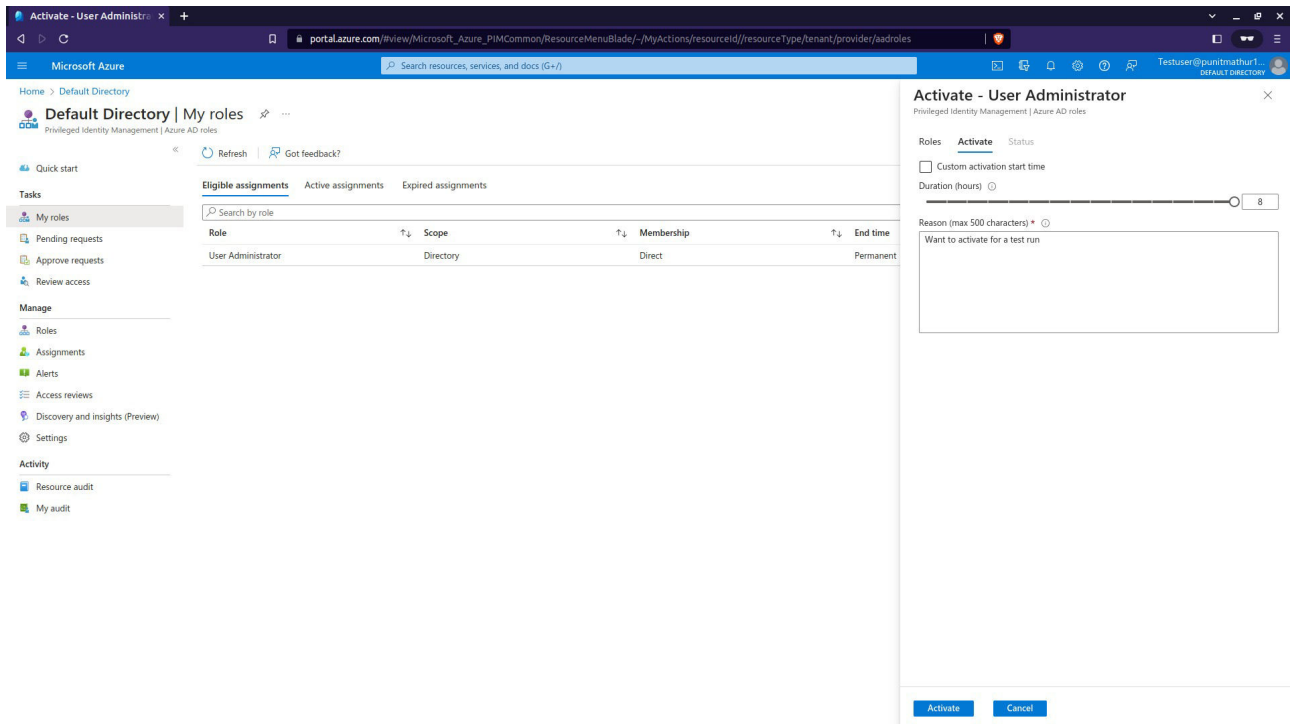


Now after login into test user, go to my roles to check that if this user have eligible assignments. Here eligible assignments basically means that the assignment eligible for request to global administrator. In eligible assignment we can clearly see that the test user have shown user administrator role.

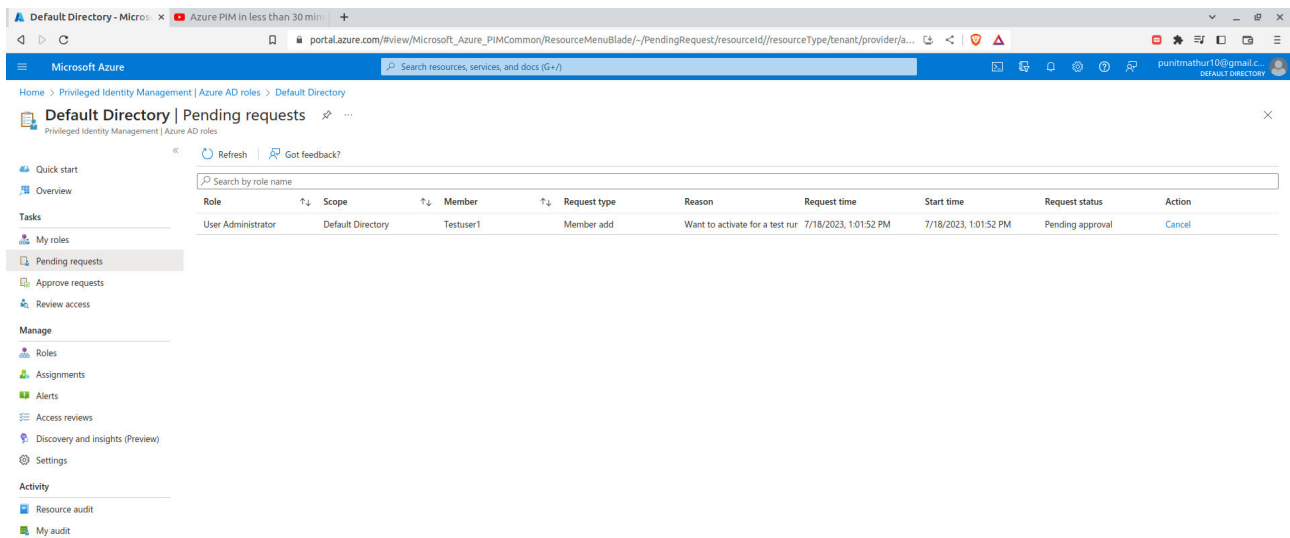
The screenshot shows the Microsoft Azure portal interface. The breadcrumb navigation at the top indicates the path: Home > Default Directory. The main heading is 'Default Directory | My roles', with a subheading 'Privileged Identity Management | Azure AD roles'. On the left sidebar, under the 'Tasks' section, 'My roles' is selected. Below this, there are links for 'Pending requests', 'Approve requests', and 'Review access'. Under the 'Manage' section, there are links for 'Roles', 'Assignments', 'Alerts', 'Access reviews', 'Discovery and insights (Preview)', and 'Settings'. Under the 'Activity' section, there are links for 'Resource audit' and 'My audit'. The main content area has tabs for 'Eligible assignments', 'Active assignments', and 'Expired assignments'. The 'Eligible assignments' tab is active and contains a search bar 'Search by role'. Below the search bar is a table with the following data:

| Role | Scope | Membership | End time | Action |
|--------------------|-----------|------------|-----------|--------------------------|
| User Administrator | Directory | Direct | Permanent | Activate |

Now click on Activate in action section. The use of this feature is after clicking it, the test user will send an approval request to the global administrator so that the test user can use the assigned role.



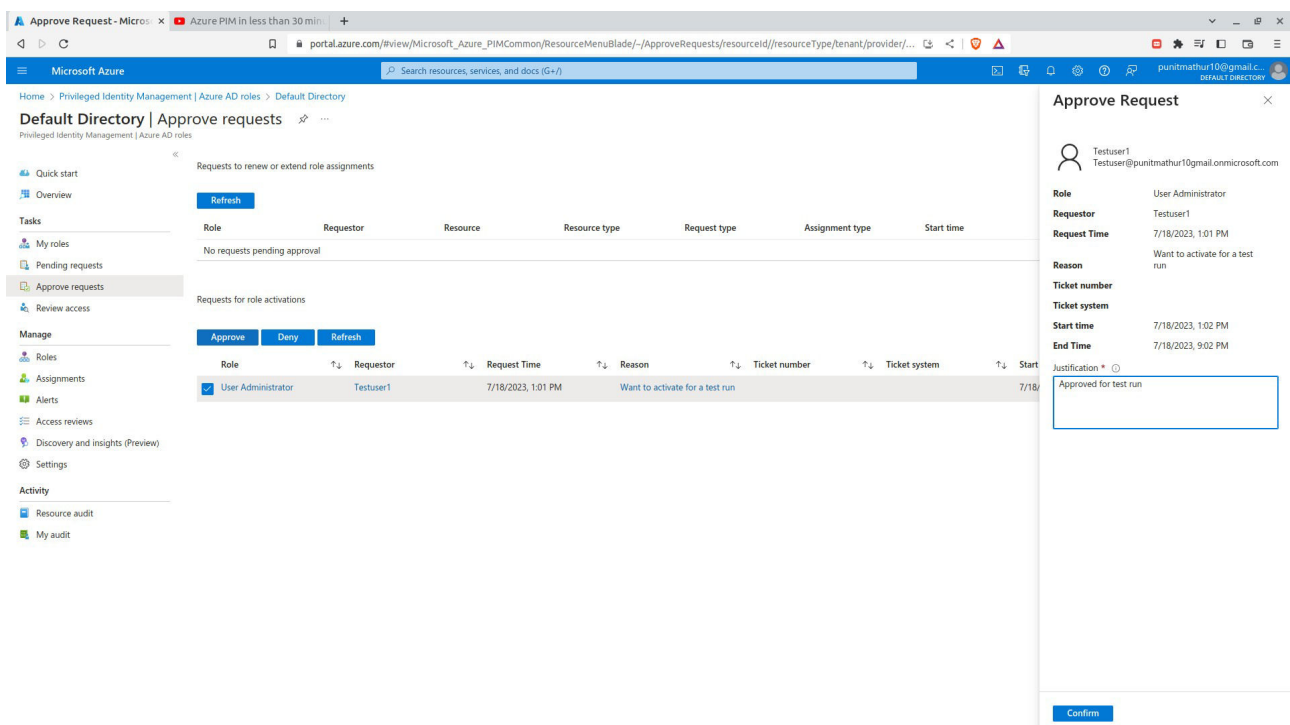
Now go and check in your Global admin account, a pending request will be there in PIM section.



The screenshot shows the Microsoft Azure portal interface. The breadcrumb navigation is 'Home > Privileged Identity Management | Azure AD roles > Default Directory'. The page title is 'Default Directory | Pending requests'. The left sidebar shows the 'Tasks' section with 'Pending requests' selected. The main content area displays a table of pending requests.

| Role | Scope | Member | Request type | Reason | Request time | Start time | Request status | Action |
|--------------------|-------------------|-----------|--------------|---------------------------------|-----------------------|-----------------------|------------------|--------|
| User Administrator | Default Directory | Testuser1 | Member add | Want to activate for a test run | 7/18/2023, 1:01:52 PM | 7/18/2023, 1:01:52 PM | Pending approval | Cancel |

Now Check in Approve requests section, select the user administrator and click on approve and then confirm.



The screenshot shows the Microsoft Azure portal interface. The breadcrumb navigation is 'Home > Privileged Identity Management | Azure AD roles > Default Directory'. The page title is 'Default Directory | Approve requests'. The left sidebar shows the 'Tasks' section with 'Approve requests' selected. The main content area displays a table of requests for role activations. A modal window titled 'Approve Request' is open on the right side of the screen.

| Role | Requestor | Request Time | Reason | Ticket number | Ticket system | Start |
|--------------------|-----------|--------------------|---------------------------------|---------------|---------------|--------------------|
| User Administrator | Testuser1 | 7/18/2023, 1:01 PM | Want to activate for a test run | | | 7/18/2023, 1:02 PM |

Approve Request

Testuser1
Testuser@punitmathur10gmail.onmicrosoft.com

Role: User Administrator
Requestor: Testuser1
Request Time: 7/18/2023, 1:01 PM
Reason: Want to activate for a test run
Ticket number:
Ticket system:
Start time: 7/18/2023, 1:02 PM
End Time: 7/18/2023, 9:02 PM
Justification: Approved for test run

Confirm

Now go check in your test user that the user administrator role has been shifted from eligible assignment to active assignment. So our main objective is completed.

The screenshot shows the Microsoft Azure portal interface. The breadcrumb navigation indicates the path: Home > Privileged Identity Management | My roles. The page title is 'My roles | Azure AD roles'. On the left, there is a sidebar with options: 'Activate', 'Azure AD roles' (selected), 'Groups', 'Azure resources', and 'Troubleshooting + Support'. The main content area has three tabs: 'Eligible assignments', 'Active assignments' (selected), and 'Expired assignments'. Below the tabs is a search bar 'Search by role'. A table displays the active assignments with the following data:

| Role | Scope | Membership | State | End time | Action |
|--------------------|-----------|------------|-----------|-----------------------|----------------------------|
| User Administrator | Directory | Direct | Activated | 7/18/2023, 9:02:48 PM | Deactivate |

Conclusion :-

So basically what we really wanted to do was we wanted that every user created on our root subscription, when assigned roles then they should get approvals first from global administrator and then only the users can use the assigned roles on their end. This was done with the help of privileged identity management in azure portal.

References :-

- 1) <https://chat.openai.com> – For writing the keyfeatures part of this document.
- 2) <https://www.youtube.com> – For Learning about some major implentation of this task.
- 3) <https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-assign-roles> - For learning purpose of Previledged Identity Management.
- 4) Celebal Technologies COE Training – For Learning the key concepts and basic understanding of azure portal.