😊 Privilege Identity Management

Privileged Identity Management (PIM) in Azure is a security feature in **Microsoft Entra ID (formerly Azure AD)** that helps manage, control, and monitor access to important resources. It allows organizations to enforce **just-in-time (JIT) access** and apply **role-based access control (RBAC)** to limit unnecessary permanent privileges.

Key Features of Azure PIM:

1. **Just-in-Time (JIT) Access** – Users and admins can activate privileges only when needed, reducing exposure to risks.
2. **Role Assignment with Expiry** – Assign privileged roles for a limited time instead of permanent access.
3. **Approval Workflow** – Requires approval before activating certain roles.
4. **Access Reviews** – Regularly review and validate role assignments.
5. **MFA Enforcement** – Multi-Factor Authentication (MFA) is required for activating high-privilege roles.
6. **Activity Logging & Alerts** – Tracks and notifies admins about role activations and suspicious activities.
7. **Time-bound Assignments** – Set expiration dates for privileged role assignments.

Common Use Cases:

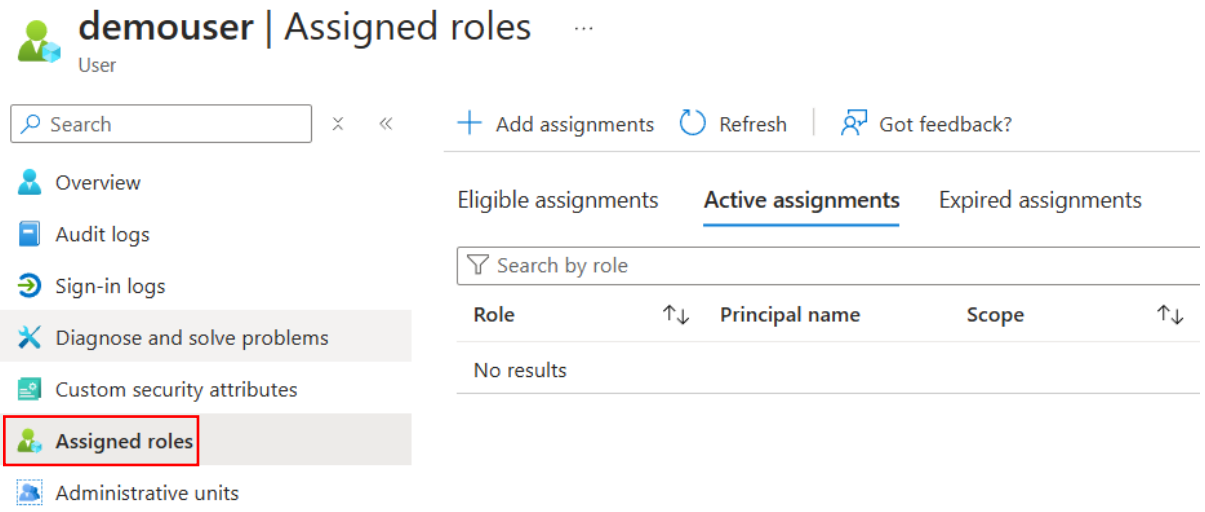
- **Managing Admin Roles:** Assigning temporary global admin roles for IT teams.
- **Securing Azure Resources:** Controlling access to Azure subscriptions, resource groups, and VMs.
- **Reducing Attack Surface:** Preventing overprivileged accounts from being exploited.

The process of Privileged Identity Management (PIM) in Azure involves assigning just-in-time (JIT) access to a user without granting permanent admin privileges. First, a demo user is created in Microsoft Entra ID with no roles assigned. The main account assigns the User Administrator role using PIM, making it an eligible assignment rather than an active one. The demo user must request activation through Microsoft Entra PIM under My Roles and can activate it for up to 8 hours. Once activated, the demo user gains admin rights, such as creating new users. The goal is to enhance security by minimizing standing privileges.

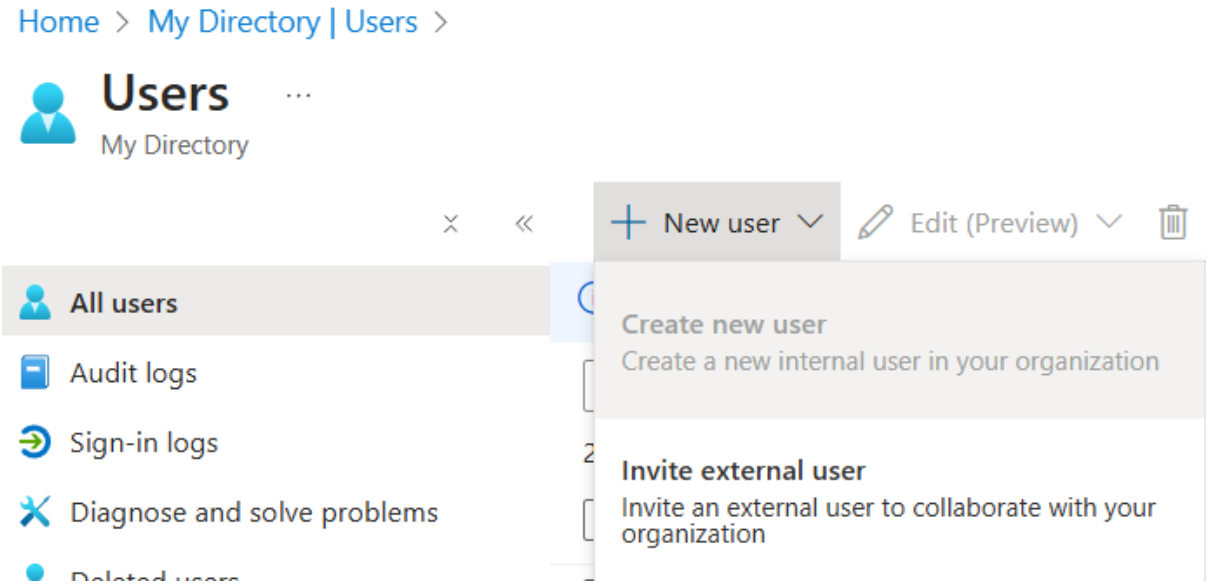
😄 To begin with the Lab:

😁 Configuring an Eligible Role:

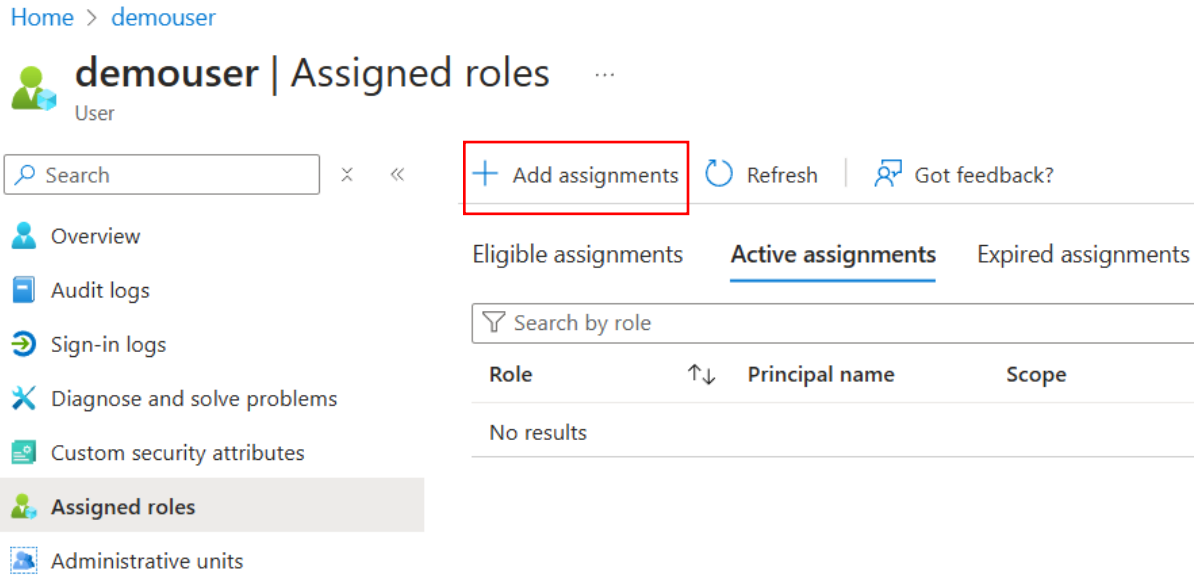
1. You should have a User in place, and you should have logged in to the user account.
2. Now in your main account in the Microsoft Entra ID open the demo user you have and go to Assigned roles you will see that it has no role assigned.



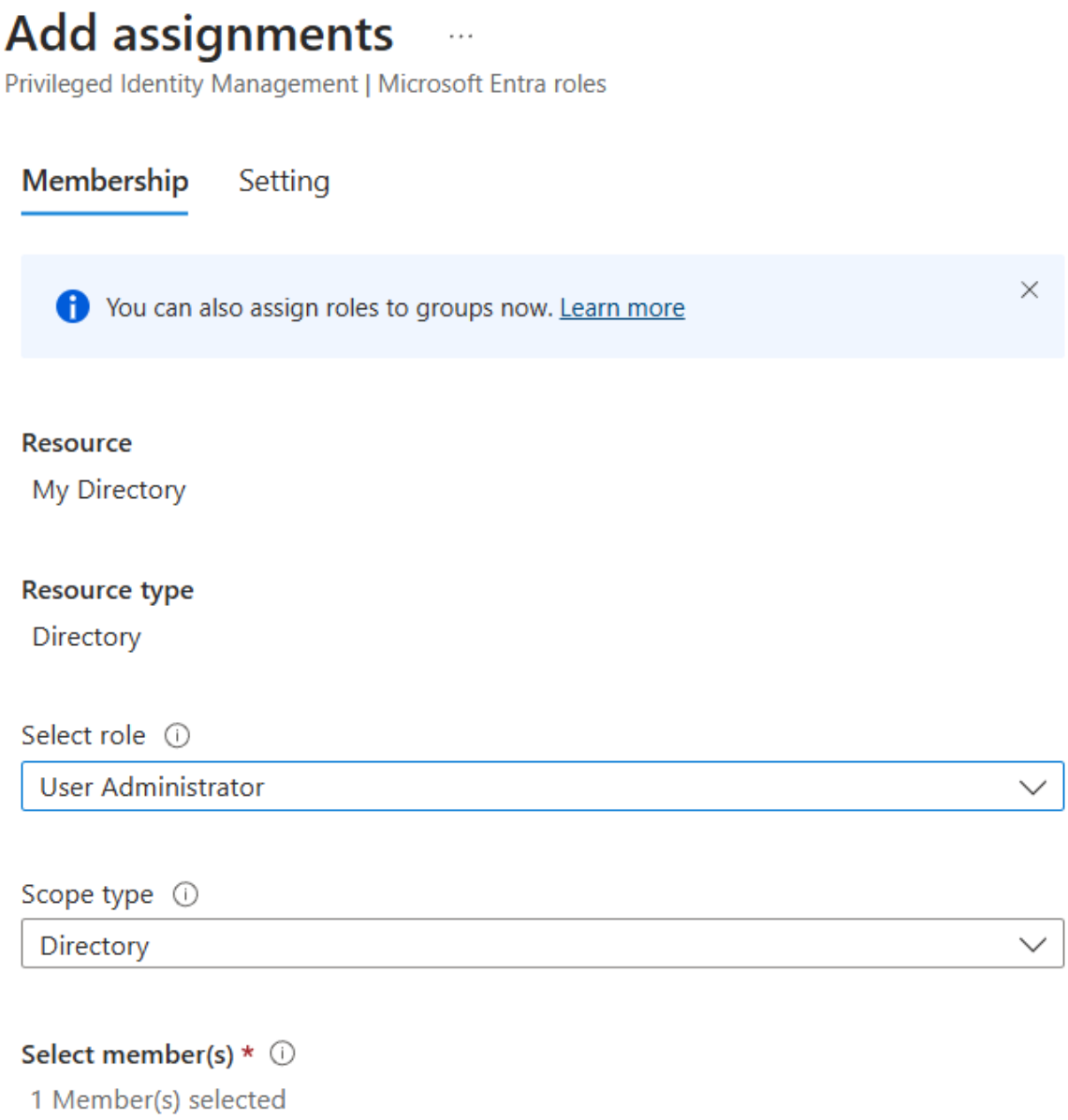
3. And if you go to the Microsoft Entra ID of the demo user, here you will see that you don't have any right to create a new user from it.



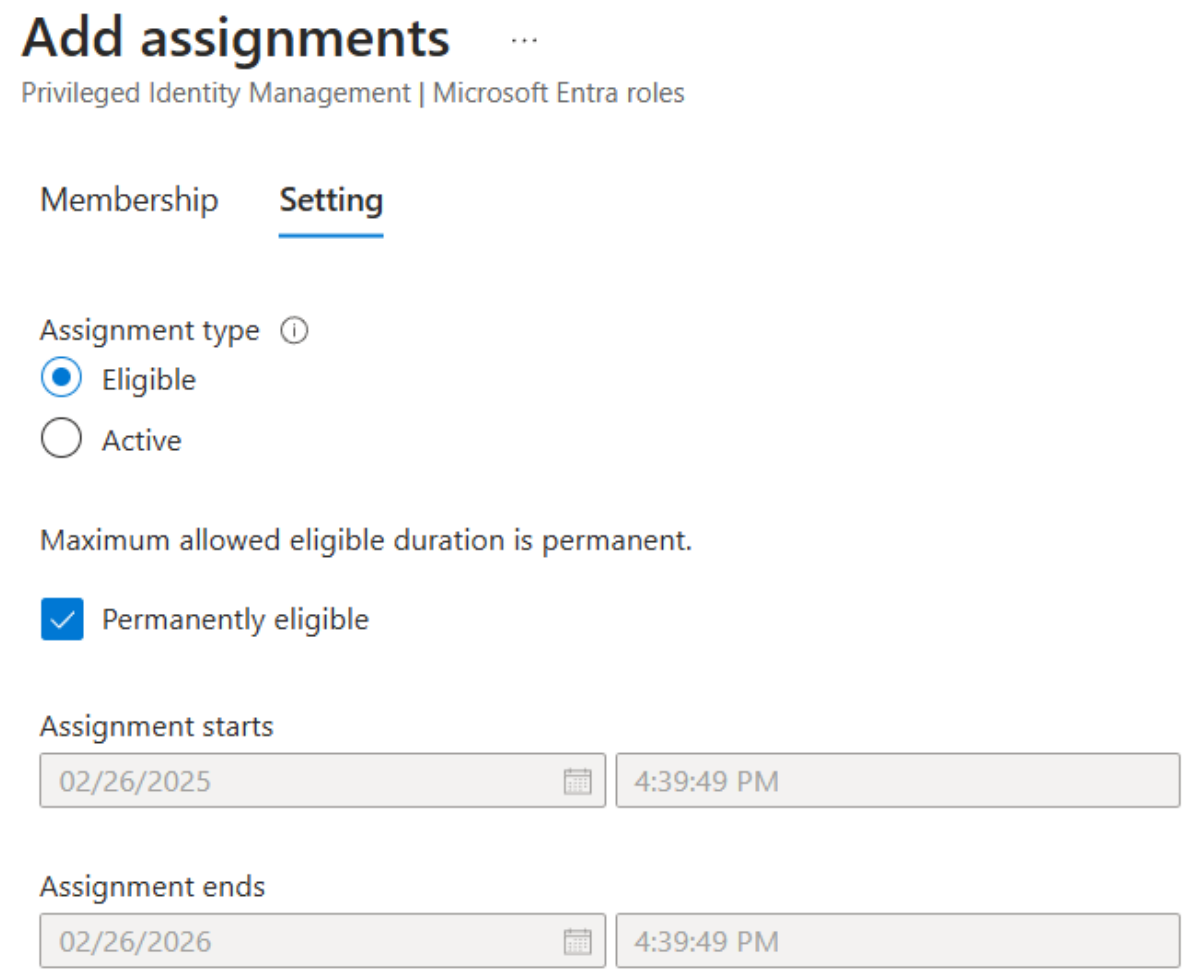
4. Now come back to the demo user in the main account and click on add assignment to add a new role but this time we will use the Privilege Identity Management.



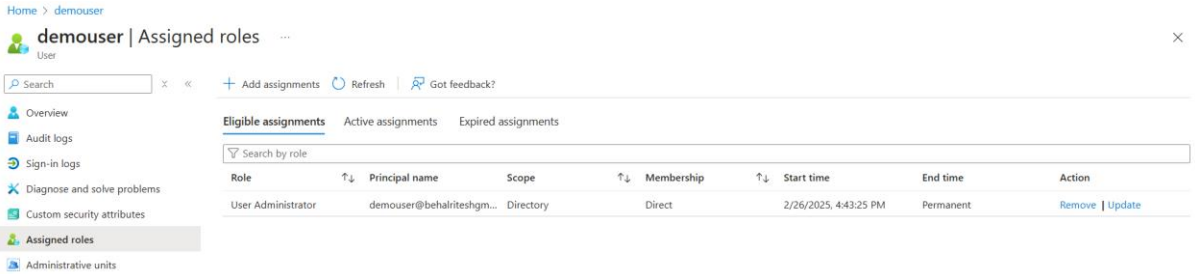
5. Here you have to select a role and select User Administrator Role, click on Next.



6. Then in the setting leave it to default and create your role assignment.

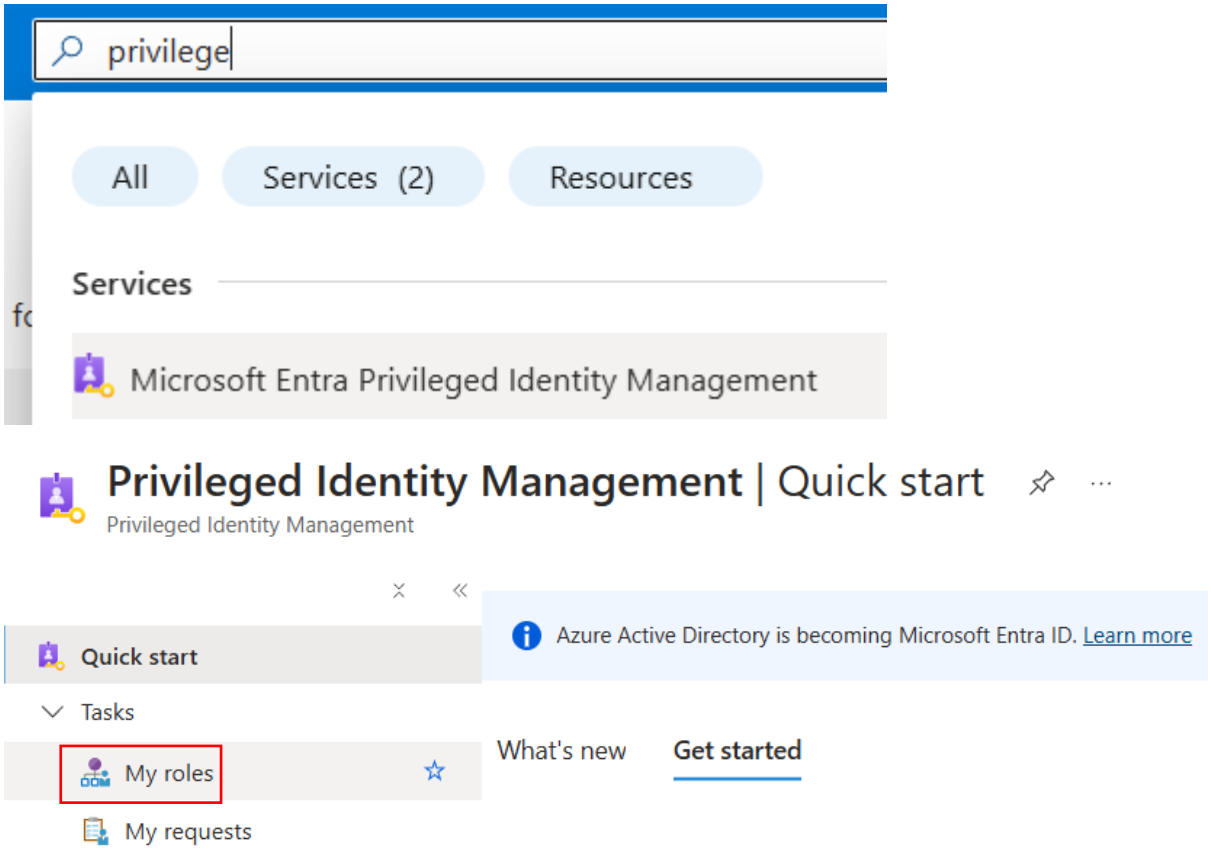


7. Now you can see the role has been assigned to the user but this is not an Active assignment this is just an Eligible assignment which means that the user is eligible to take up the role but the role is not directly assigned to the user.
8. The user has to go ahead and request now to take up the role and that is the entire concept of privilege identity management.
9. Now as the demo user we have to request the role from the administrator.

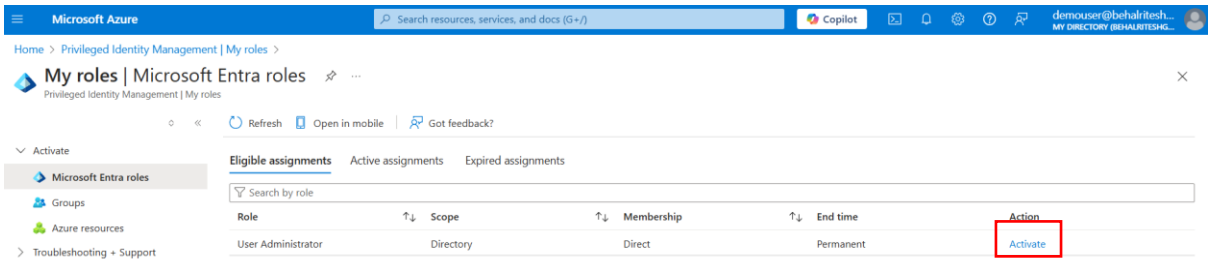


😁 Activating the Role

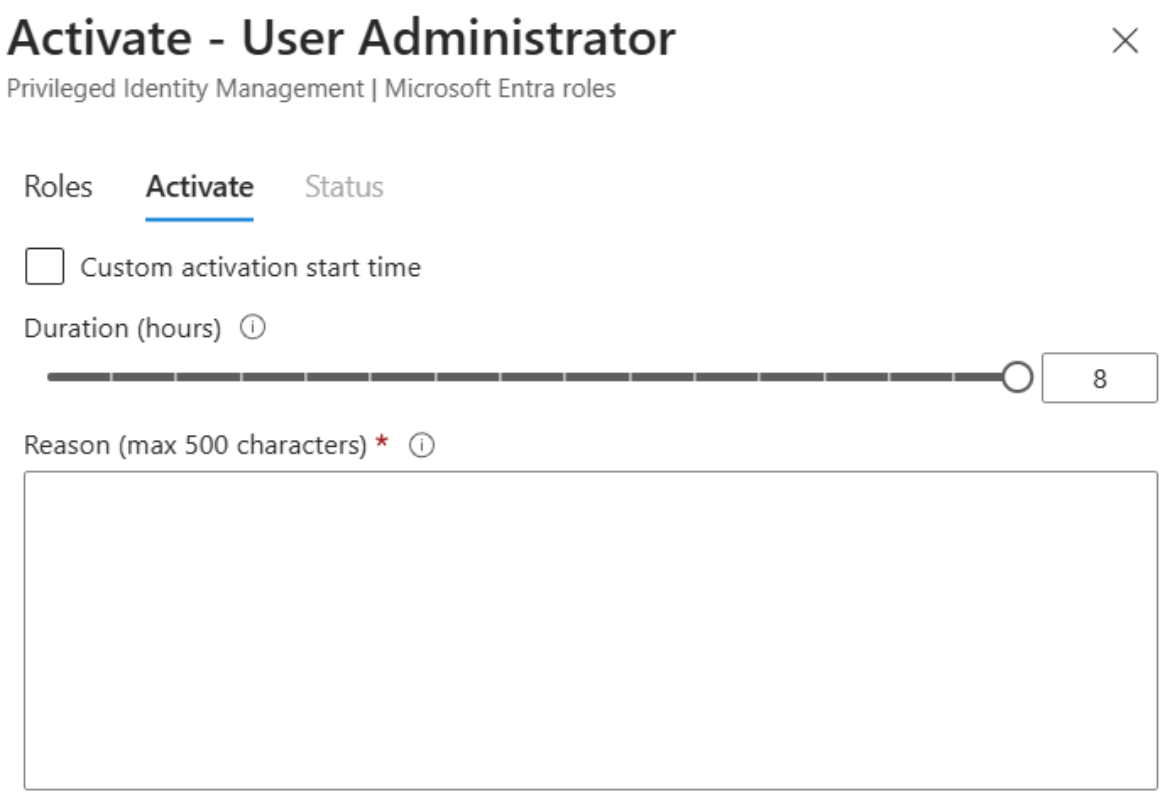
10. So, now from the demo user account we have to search for Microsoft Entra Privilege Identity Management and go to it, and then we have to go to My Roles.



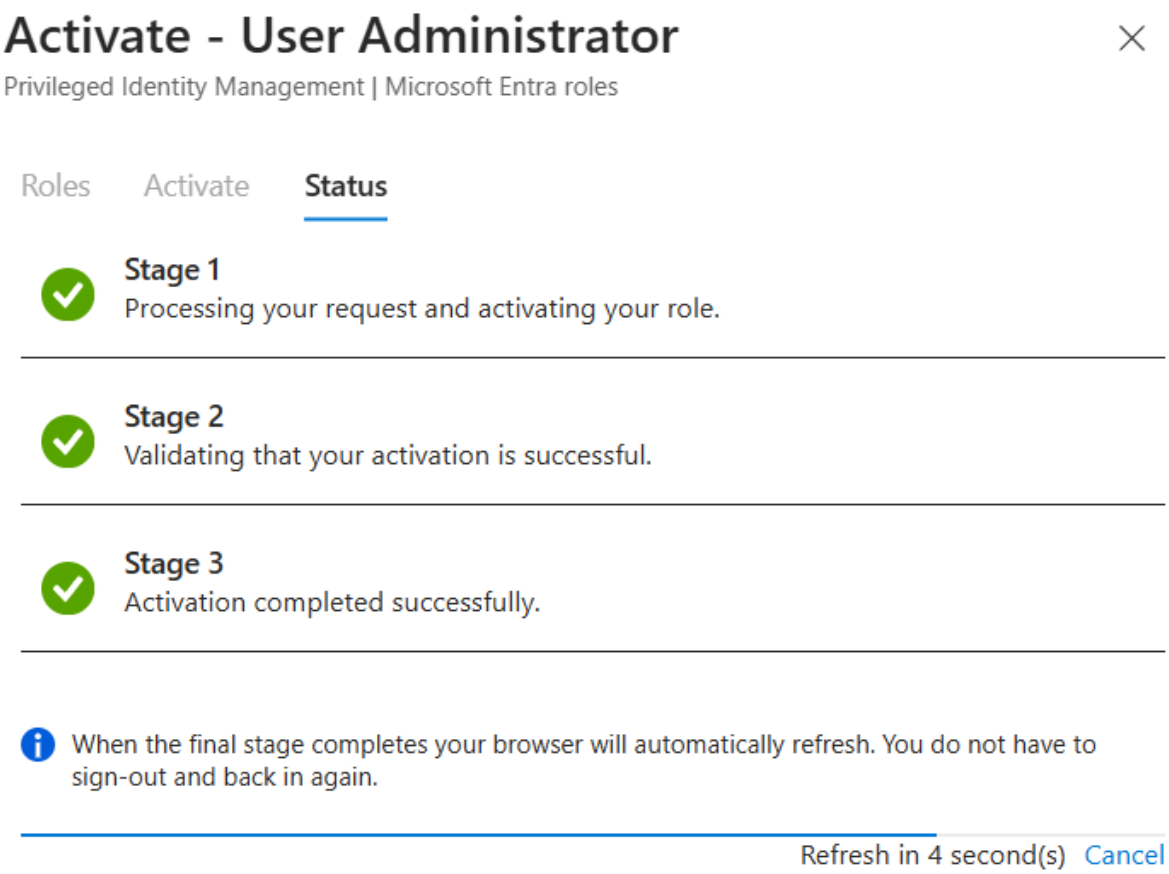
11. Here you can see that we have the eligible assignment for the user administrator role, which is ready to be activated.



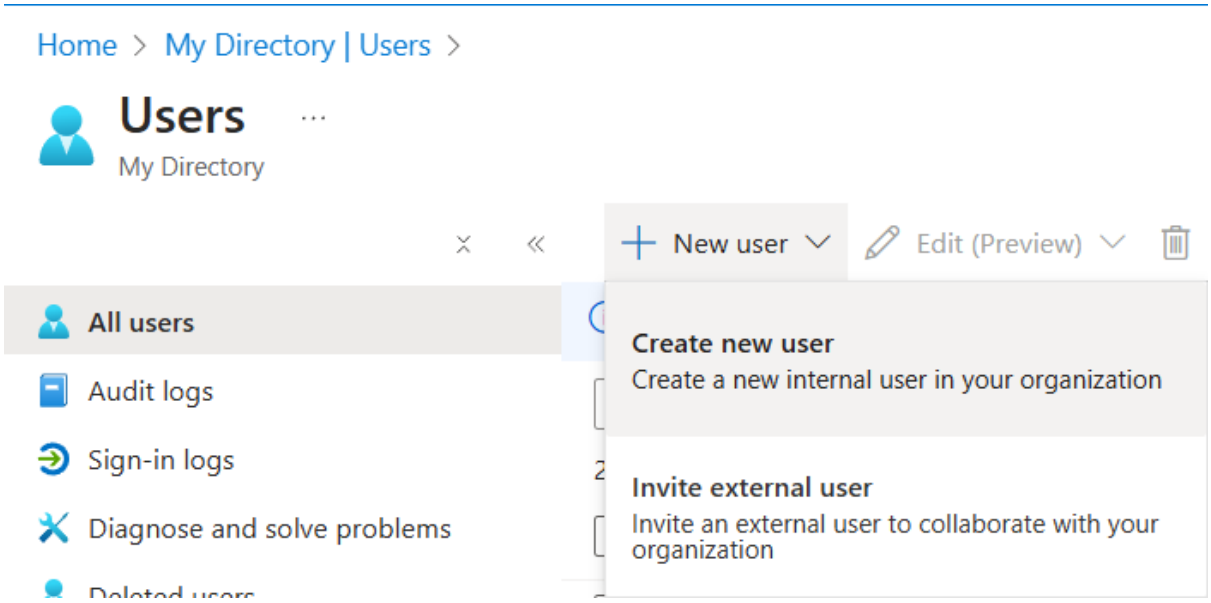
12. Here you can see that we can activate this role for a maximum of 8 hours. Click on Activate.



13. You can see that your role has been activated for the demo user.



14. In the end you can verify that your demo user is now able to create a new user by itself.


Home > My Directory | Users >
Users
My Directory
New user
Edit (Preview)
All users
Audit logs
Sign-in logs
Diagnose and solve problems
Create new user
Create a new internal user in your organization
Invite external user
Invite an external user to collaborate with your organization