😊 User Groups

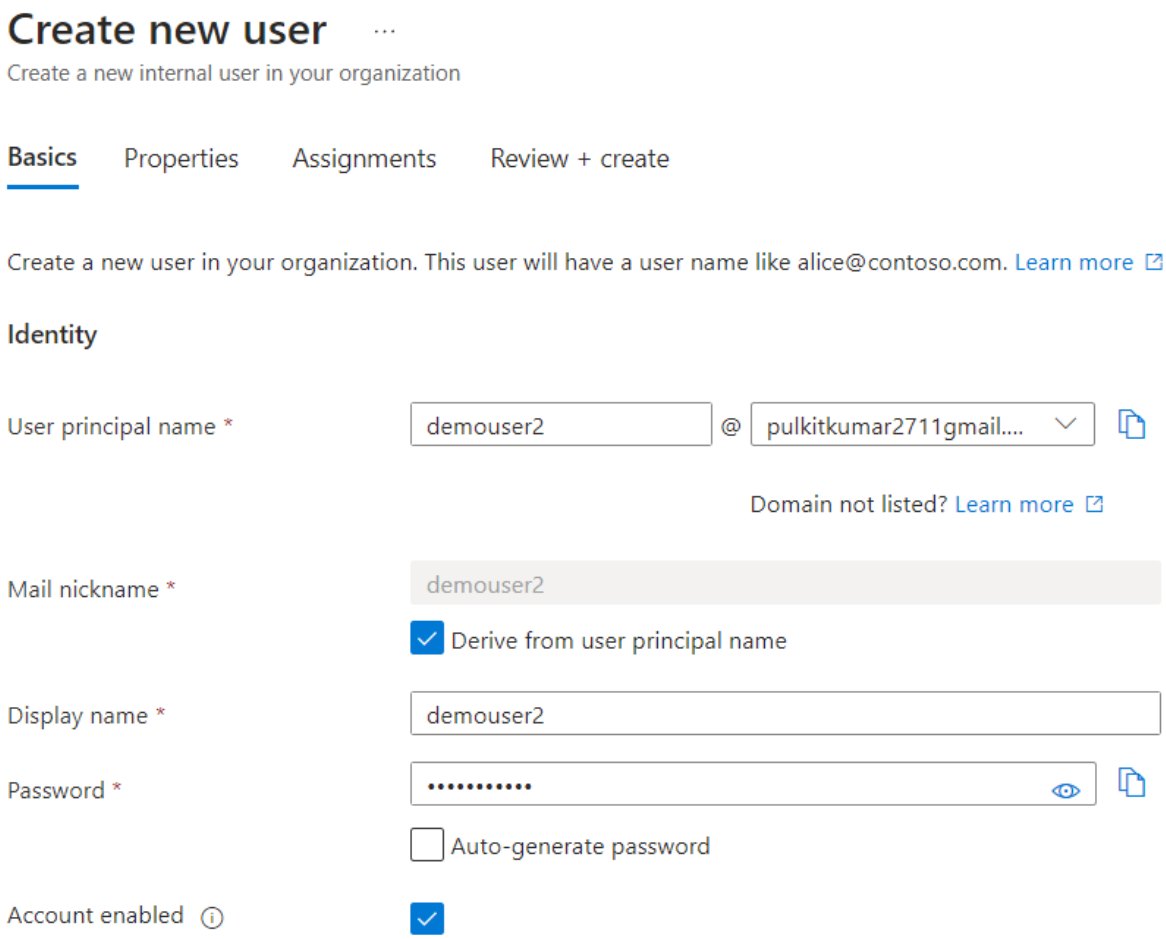
In Azure Active Directory (Azure AD), user groups are collections of user accounts. These groups serve several purposes, primarily related to access management and collaboration:

1. **Access Management:** User groups help streamline access management by allowing administrators to grant permissions to a group of users rather than individual accounts. For example, you can assign permissions to access resources like Azure subscriptions, applications, or SharePoint sites to a user group. This simplifies administration and makes it easier to manage access control.
2. **Role Assignment:** User groups can be assigned to roles within Azure AD or other Azure services. For example, you can assign a user group the role of "Contributor" on a resource in Azure, granting all members of the group the ability to manage that resource.
3. **License Assignment:** Azure AD user groups can also be used to assign licenses to multiple users simultaneously. Instead of assigning licenses individually, you can assign licenses to a group, and all members of the group will receive the assigned licenses automatically.
4. **Group-Based Licensing:** With Azure AD group-based licensing, you can automatically assign licenses to users based on their group membership. When users are added to or removed from a group, their licensing status is updated accordingly, which helps streamline license management.
5. **Collaboration and Sharing:** User groups can be used for collaboration and sharing within Microsoft 365 services like SharePoint, Teams, and Exchange. For example, you can create a Microsoft 365 group (formerly Office 365 group) for a project team, and all members of the group will have access to shared resources such as a shared mailbox, calendar, SharePoint site, and Teams channel.

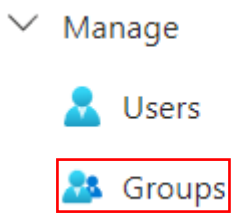
In this walkthrough, we are setting up user groups in Azure Active Directory (Azure AD) and demonstrating their usage for access management and collaboration within the Azure environment. The end goal is to streamline access control by assigning permissions to groups of users rather than individual accounts, thereby simplifying administration and improving efficiency.

😄 To begin with the Lab:

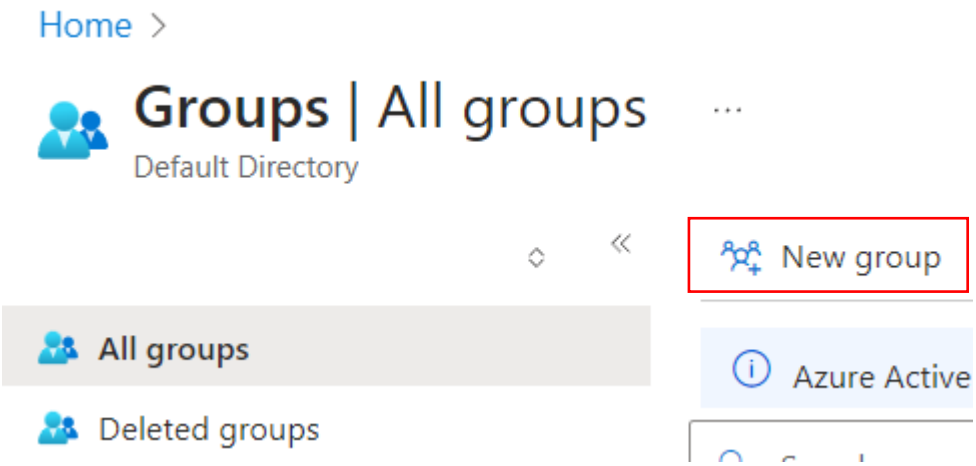
1. Until now in our Azure Active Directory or say Microsoft Entra ID we just have one user which demo user1.
2. Now we are going to create another user. For that navigate to Entra ID then to users. Then you'll be at all users page from there choose to create a new user.



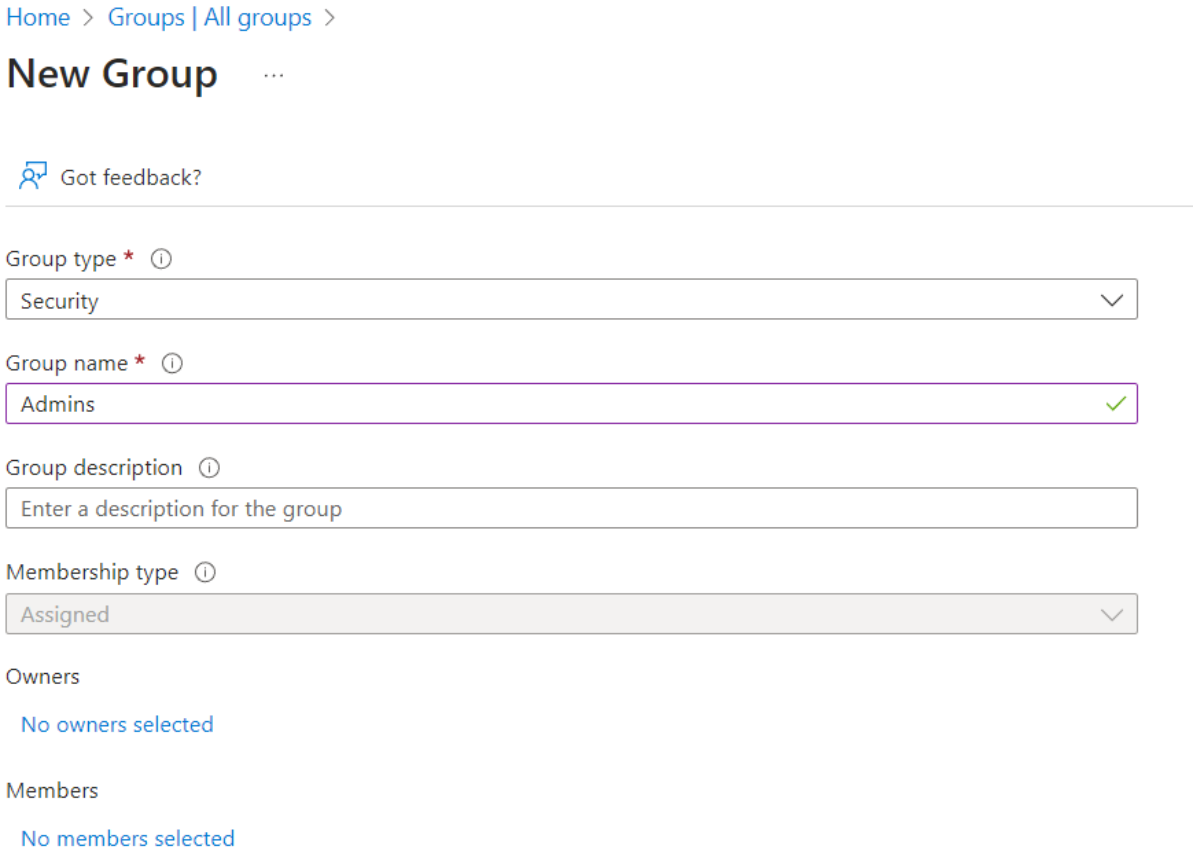
3. Once your user is created then go back to the default directory and this time choose Groups.



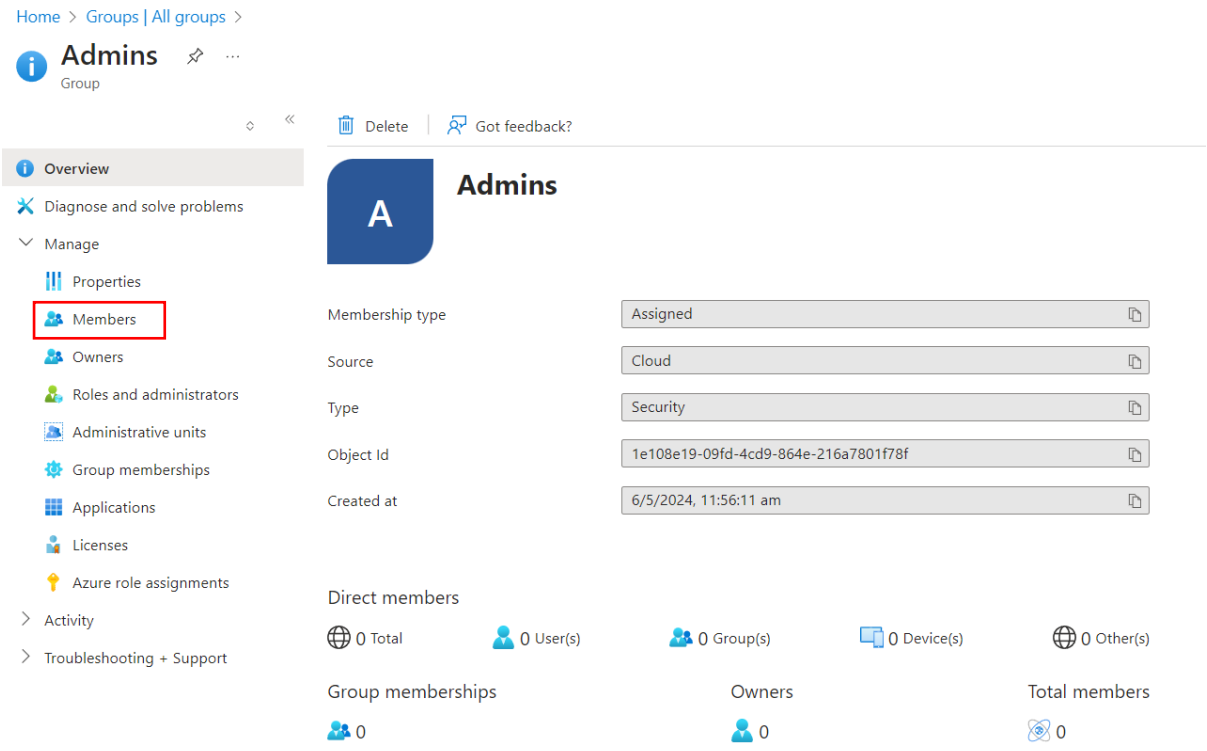
4. Here from all groups section, you need to choose New group.



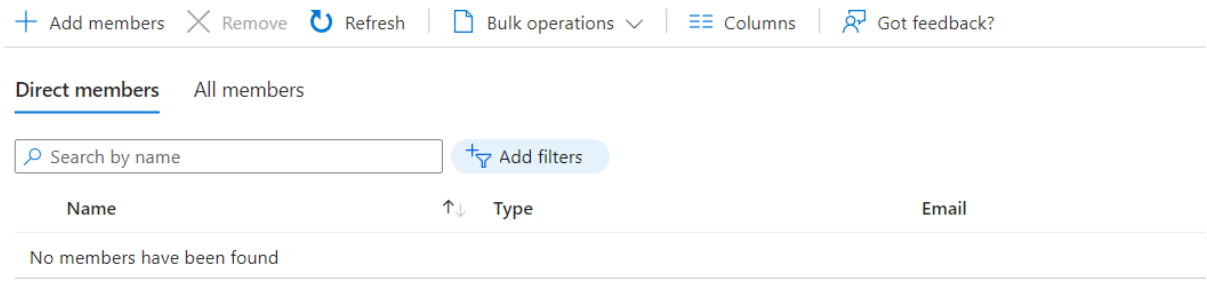
5. While creating your group choose the group type as security and then give it a name then just create your group.



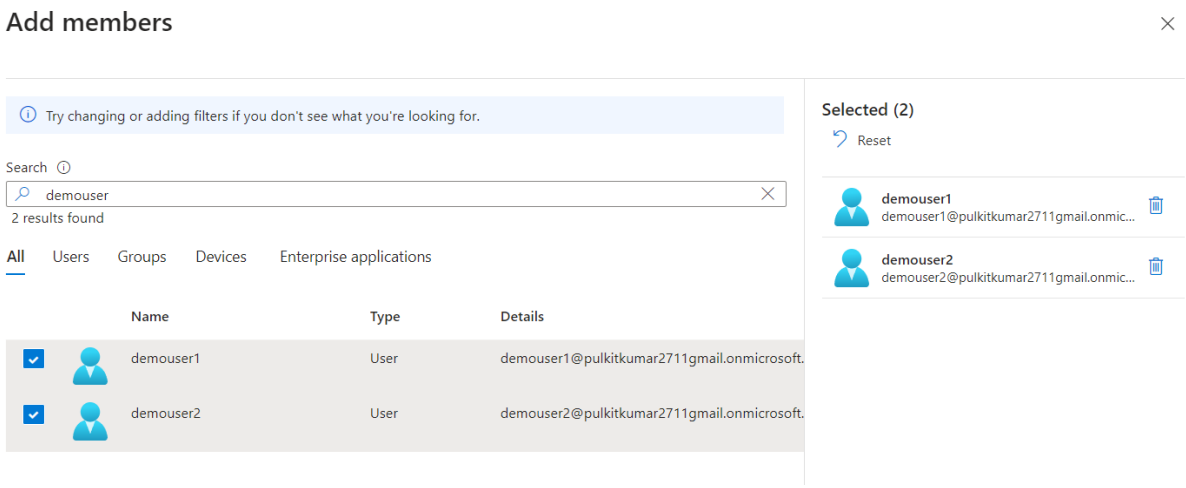
6. Once your group is created then go inside of it and from its dashboard expand the Manage tab and navigate to Members.



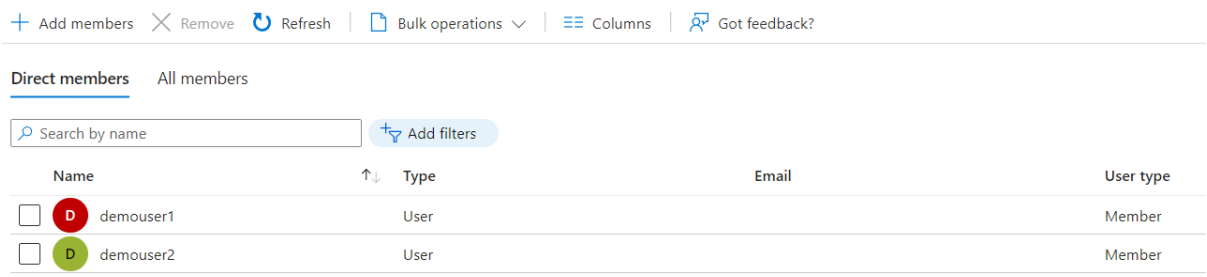
7. Then click on Add members and add demo user1 and 2 here.



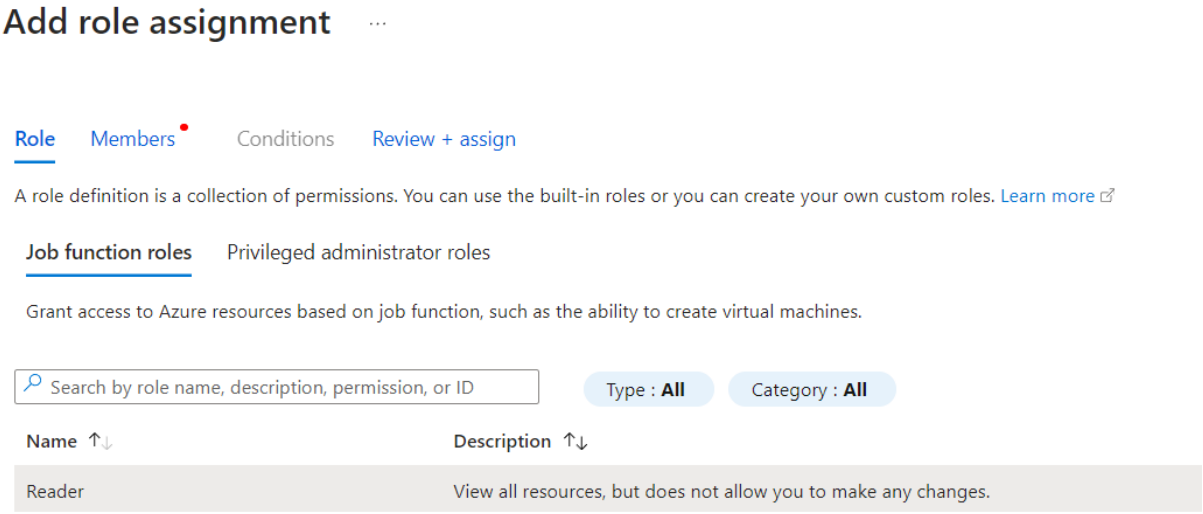
8. Choose both your user and click on select.



9. Then after sometime you will be able to see your members in place.



10. Now while adding a role assignment you can directly use this group instead of adding both the members separately.
11. To verify that you can go to IAM of your resource group then choose add Role assignment.
12. After that choose the reader role.



13. Then while selecting your member you can choose your group. After that move to Review and assign page.