

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.

Create new user ...

Create a new internal user in your organization

Basics Properties Assignments Review + create

Create a new user in your organization. This user will have a user name like alice@contoso.com. [Learn more](#)

Identity

User principal name * demouser2 @ pulkitkumar2711gmail....

Domain not listed? [Learn more](#)

Mail nickname *

demouser2

☒ Derive from user principal name

Display name *

demouser2

Password *

.....

☐ Auto-generate password


Account enabled ⓘ



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

✓ Manage

 Users

 Groups

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

[Home](#) >



Groups | All groups ...

Default Directory



New group



All groups



Deleted groups



Azure Active

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

[Home](#) > [Groups | All groups](#) >

New Group ...



Got feedback?

Group type * ⓘ

Security



Group name * ⓘ

Admins



Group description ⓘ

Enter a description for the group

Membership type ⓘ

Assigned



Owners

No owners selected

Members

No members selected

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


Home > Groups | All groups >

Admins ...

Group


 Delete |  Got feedback?

Overview


 Diagnose and solve problems

Manage

 Properties


 **Members**

 Owners


 Roles and administrators

 Administrative units

 Group memberships

 Applications

 Licenses






 Azure role assignments

> Activity



> Troubleshooting + Support



Admins

Membership type	Assigned 
Source	Cloud 
Type	Security 
Object Id	1e108e19-09fd-4cd9-864e-216a7801f78f 
Created at	6/5/2024, 11:56:11 am 

Direct members

 0 Total  0 User(s)  0 Group(s)  0 Device(s)  0 Other(s)

Group memberships

 0








Owners

 0

Total members


 0


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

 Add members  Remove  Refresh |  Bulk operations  |  Columns |  Got feedback?


Direct members

All members

 Search by name

 Add filters

Name


 Type

Email


No members have been found

8. Choose both your user and click on select.

Add members



 Try changing or adding filters if you don't see what you're looking for.

Search 

 demouser


2 results found


All Users Groups Devices Enterprise applications

	Name	Type	Details
<input checked="" type="checkbox"/>	 demouser1	User	demouser1@pulkitkumar2711gmail.onmicrosoft.
<input checked="" type="checkbox"/>	 demouser2	User	demouser2@pulkitkumar2711gmail.onmicrosoft.

Selected (2)

 Reset



 **demouser1**
demouser1@pulkitkumar2711gmail.onmic...

 **demouser2**
demouser2@pulkitkumar2711gmail.onmic...

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

+ Add members ✕ Remove ↻ Refresh | 📄 Bulk operations ▾ | ☰ Columns | 🗨️ Got feedback?

Direct members All members

	Name	↑↓ Type	Email	User type
<input type="checkbox"/>	 demouser1	User		Member
<input type="checkbox"/>	 demouser2	User		Member


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.

Add role assignment ...

Role **Members** [•] Conditions [Review + assign](#)

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#) 

Job function roles Privileged administrator roles

Grant access to Azure resources based on job function, such as the ability to create virtual machines.

🔍 Search by role name, description, permission, or ID		Type : All	Category : All
Name ↑↓	Description ↑↓		
Reader	View all resources, but does not allow you to make any changes.		

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

Select members



Select ⓘ

admins



Admins