Secure Access with Azure Active Directory(Microsoft Entra ID)

In this project, you will demonstrate your ability to perform the following tasks in Azure Active Directory (Microsoft Entra ID):

- Create and manage users and groups
- Manage authentication

The activities include:

- Creating users
- Creating groups
- Assigning users to groups
- Enabling and testing self-service password reset
- Enabling and verifying multifactor authentication

These tasks align with the typical responsibilities of Azure security engineers and administrators within an organization.

Project scenario

In this project, you will go through the typical activities that an Azure security engineer would perform in an organization.

Imagine you have recently joined a large organization as an Azure security engineer. You have been assigned the responsibility for the following:

- The organization has created a new department called DevSupport. Three new employees, John, Dave, and Jeff, have joined as part of the new department. You are responsible for creating user accounts for these employees on Azure Active Directory (Microsoft Entra ID.) You should also create a group for the department and assign the users to the new group.

- The organization's employees regularly call the support team to reset their passwords. This adds to the workload of support teams and delays employees in their duties. You are responsible for enabling self-service password reset so that users of the organization can self-authenticate with Azure AD to reset their own passwords.
- The organization has decided to enhance the security of its systems and data. You have been assigned to enable and configure multifactor authentication for the new employees to facilitate this.

You will perform these tasks in the Azure platform

- Task 1: Add new users in Azure AD based on the requirements of the scenario.
- Task 2: Create a group and add members to this group.
- Task 3: Select a group and enable self-service password reset for this group.
- Task 4: Sign in as a non-administrator user to test whether users can reset their own passwords.
- Task 5: Enable and configure multifactor authentication for a user.

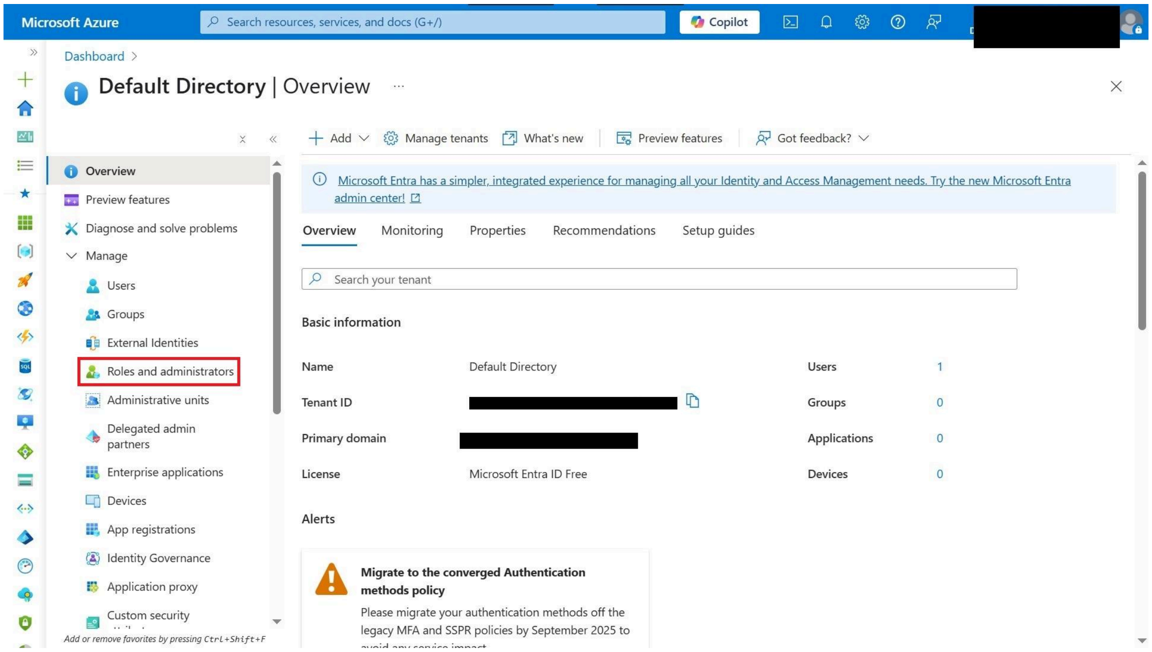
Setting up the system

This project consists of tasks you should complete on the Azure platform itself. Before you begin, you must have the following:

- Access to an Azure Active Directory instance as a Global Administrator

Task 1: Add a new user

1. Sign in to the Azure portal with your login credentials. Navigate to the Azure Active directory. Select **Roles and administrators** under the Manage blade.



Microsoft Entra has a simpler, integrated experience for managing all your Identity and Access Management needs. Try the new Microsoft Entra admin center!

Basic information

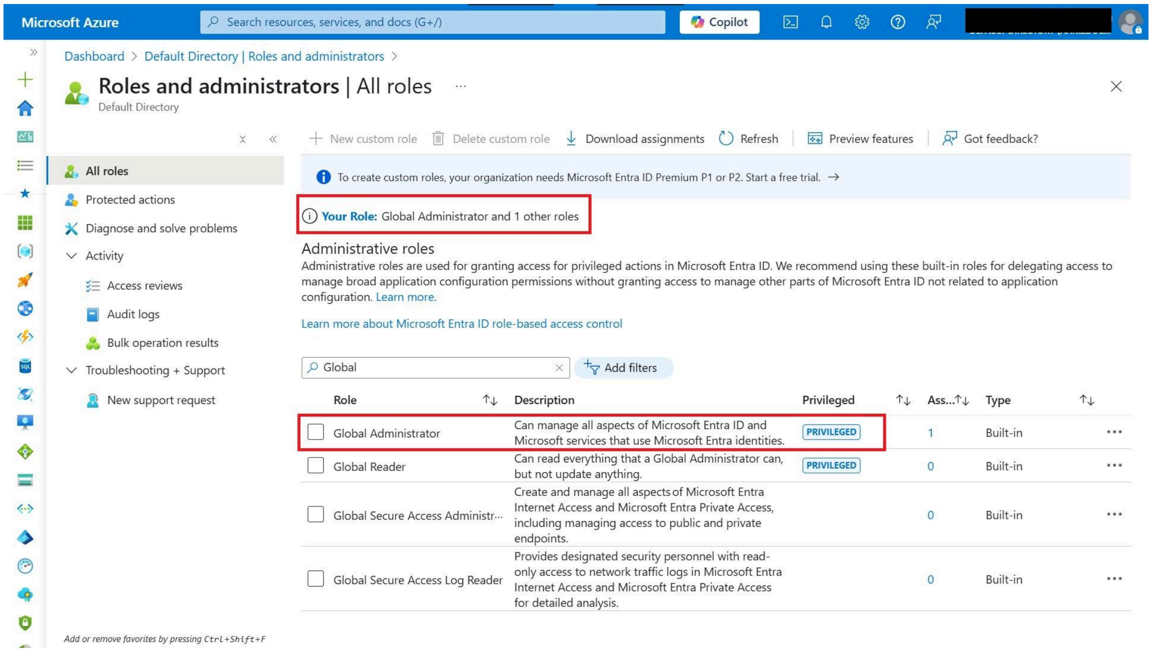
Name	Default Directory	Users	1
Tenant ID	[redacted]	Groups	0
Primary domain	[redacted]	Applications	0
License	Microsoft Entra ID Free	Devices	0

Alerts

Migrate to the converged Authentication methods policy

Please migrate your authentication methods off the legacy MFA and SSPR policies by September 2025 to avoid any service impact.

2. To create a user, check your role. If your role is Global Administrator, you can manage all aspects of Azure AD.



To create custom roles, your organization needs Microsoft Entra ID Premium P1 or P2. Start a free trial. →

Your Role: Global Administrator and 1 other roles

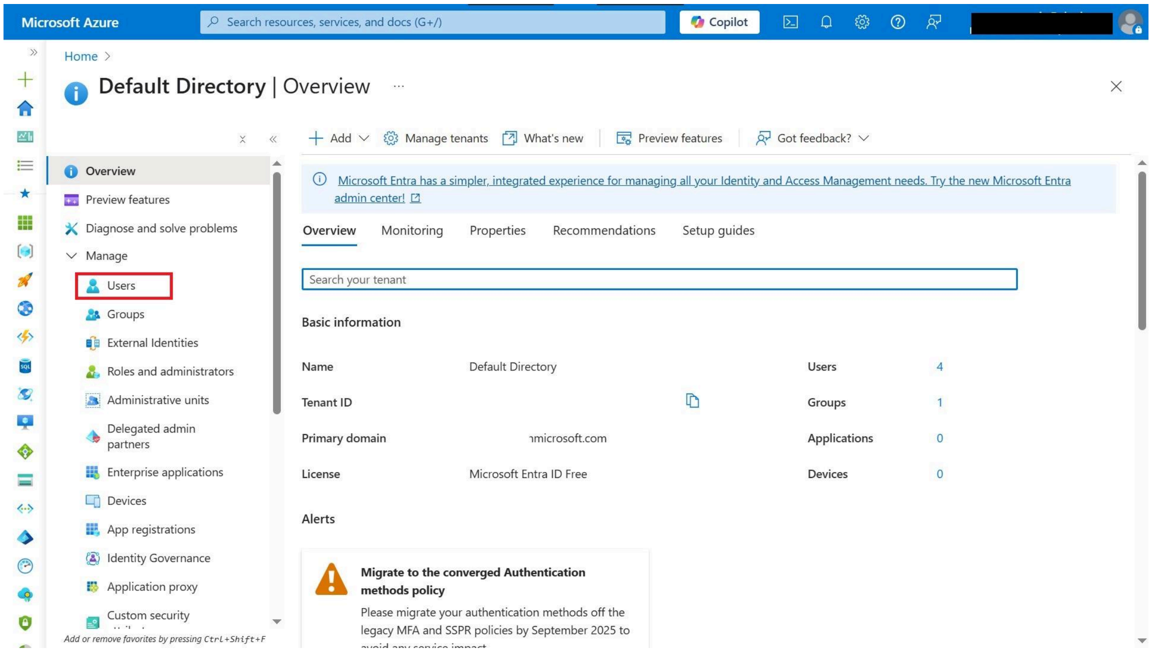
Administrative roles

Administrative roles are used for granting access for privileged actions in Microsoft Entra ID. We recommend using these built-in roles for delegating access to manage broad application configuration permissions without granting access to manage other parts of Microsoft Entra ID not related to application configuration. Learn more.

Learn more about Microsoft Entra ID role-based access control

Role	Description	Privileged	Ass...	Type
□ Global Administrator	Can manage all aspects of Microsoft Entra ID and Microsoft services that use Microsoft Entra identities.	PRIVILEGED	1	Built-in
□ Global Reader	Can read everything that a Global Administrator can, but not update anything.	PRIVILEGED	0	Built-in
□ Global Secure Access Administr...	Create and manage all aspects of Microsoft Entra Internet Access and Microsoft Entra Private Access, including managing access to public and private endpoints.		0	Built-in
□ Global Secure Access Log Reader	Provides designated security personnel with read-only access to network traffic logs in Microsoft Entra Internet Access and Microsoft Entra Private Access for detailed analysis.		0	Built-in

3. Go to **Azure Active Directory**, then select **Users**.



Microsoft Entra has a simpler, integrated experience for managing all your Identity and Access Management needs. Try the new Microsoft Entra admin center!

Basic information

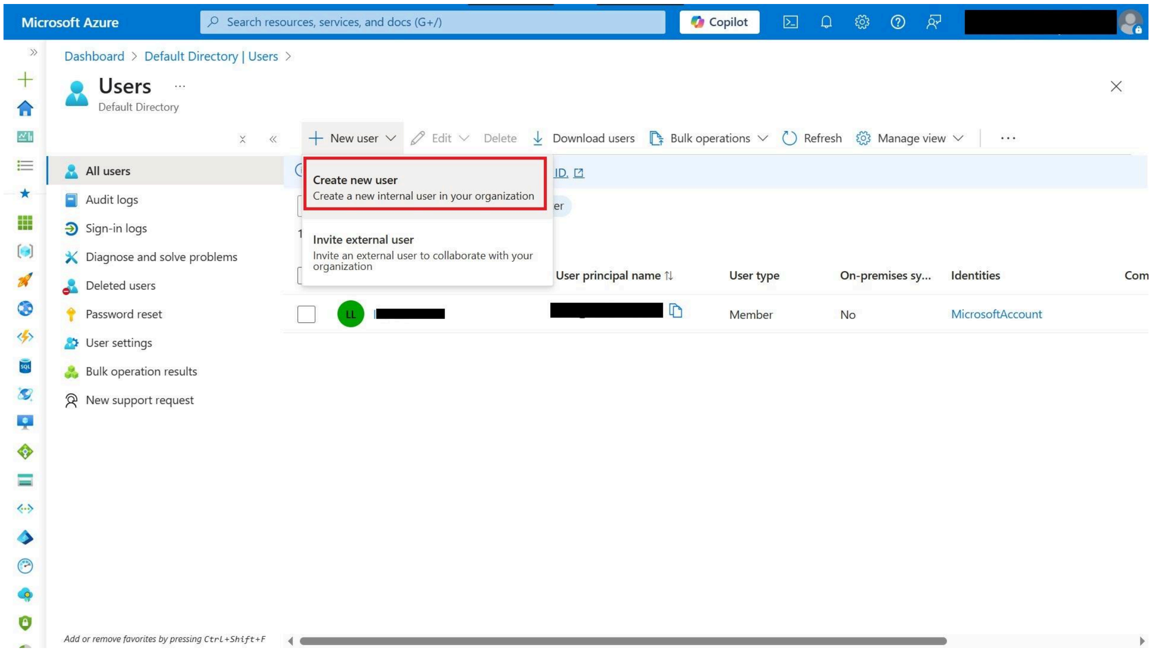
Name	Default Directory	Users	4
Tenant ID		Groups	1
Primary domain	ımicrosoft.com	Applications	0
License	Microsoft Entra ID Free	Devices	0

Alerts

Migrate to the converged Authentication methods policy

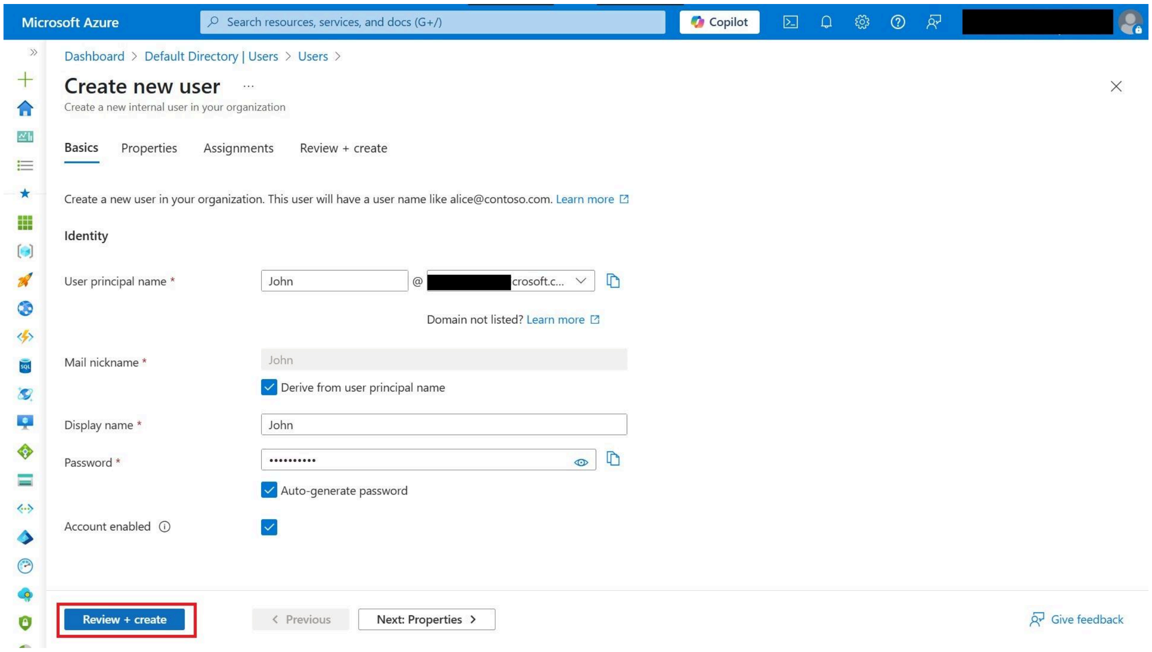
Please migrate your authentication methods off the legacy MFA and SSPR policies by September 2025 to avoid any service impact.

4. Click **Add**, then choose **Create new user**.



	User principal name	User type	On-premises sy...	Identities	Com
LL [redacted]	[redacted]	Member	No	MicrosoftAccount	

5. Enter the user details and click **Review + Create**.



Create new user

Create a new internal user in your organization

Create a new user in your organization. This user will have a user name like alice@contoso.com. Learn more

Identity

User principal name * John @ [redacted] crosoft.c...

Domain not listed? Learn more

Mail nickname * John

☑ Derive from user principal name

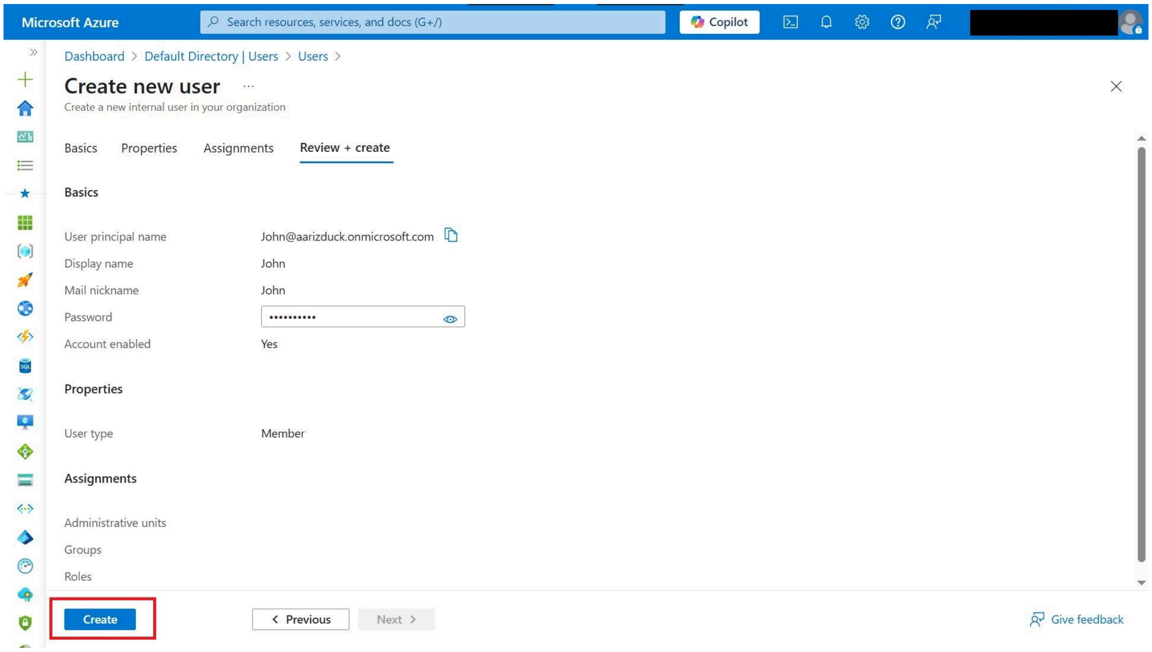
Display name * John

Password * ••••••••••

☑ Auto-generate password

Account enabled ☑

6. Click **Create** to finalize.



Create new user

Create a new internal user in your organization

Basics

User principal name John@aarizduck.onmicrosoft.com

Display name John

Mail nickname John

Password ••••••••••

Account enabled Yes

Properties

User type Member

Assignments

Administrative units

Groups

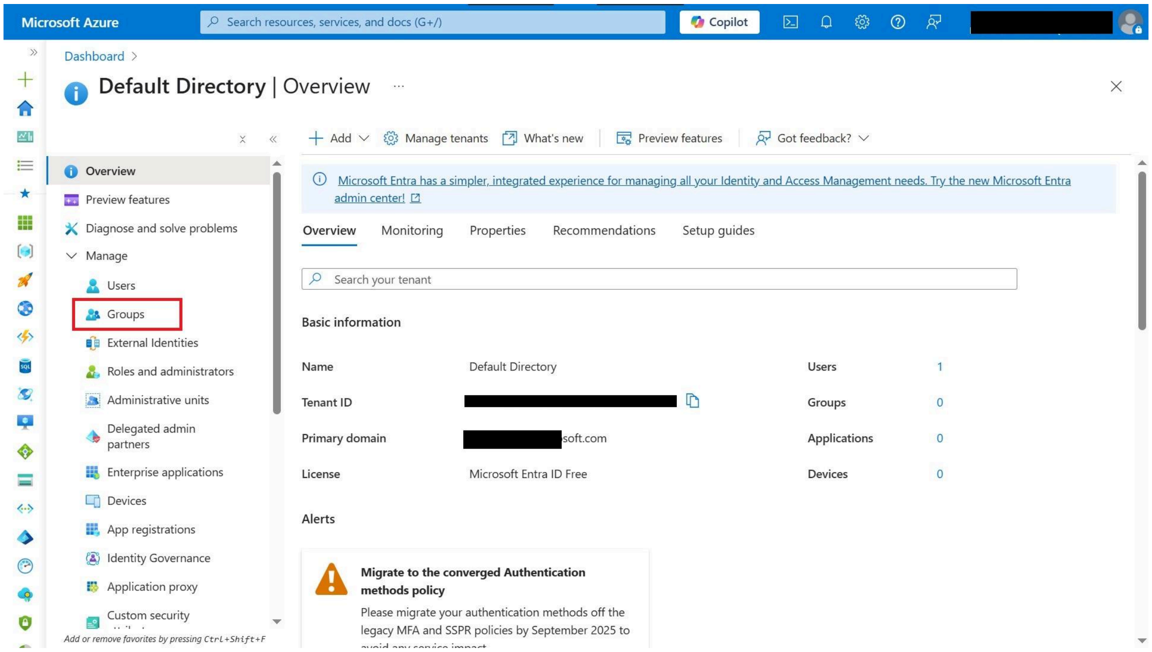
Roles

7. The new user will now be created.
8. Repeat these steps to add any additional users.

Task 2: Create a group called DevSupport and add members

To create a group in Azure Active Directory:

1. Sign in to the **Microsoft Azure portal** and navigate to **Groups** under **Azure Active Directory**.



Microsoft Entra has a simpler, integrated experience for managing all your Identity and Access Management needs. Try the new Microsoft Entra admin center!

Basic information

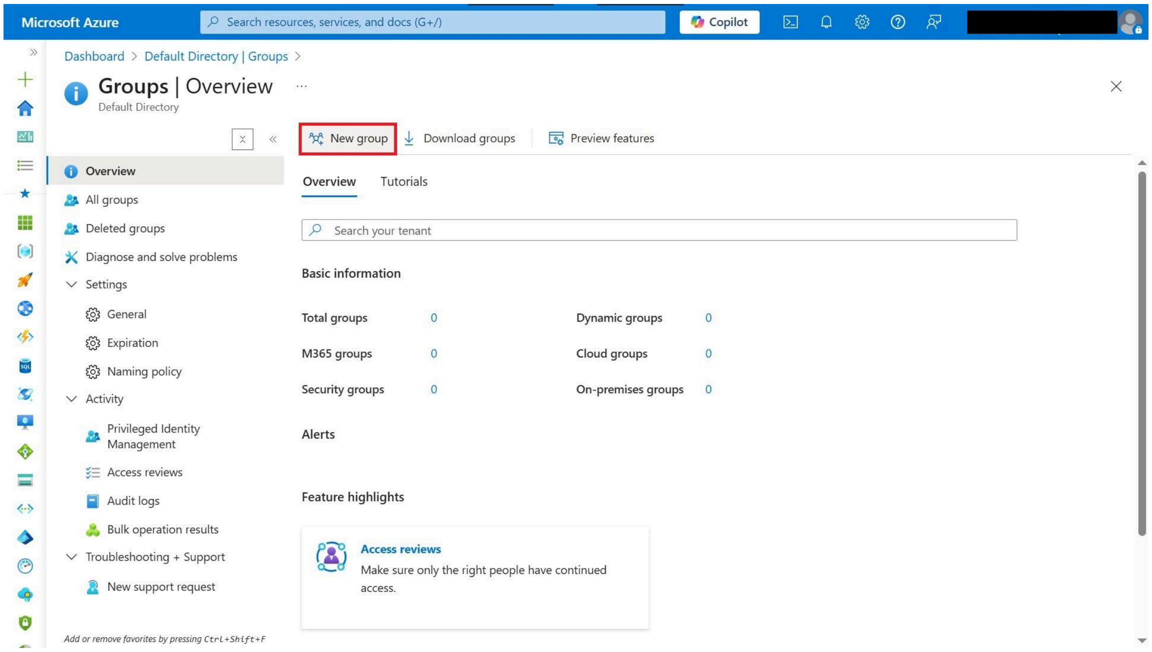
Name	Default Directory	Users	1
Tenant ID	[redacted]	Groups	0
Primary domain	[redacted]soft.com	Applications	0
License	Microsoft Entra ID Free	Devices	0

Alerts

Migrate to the converged Authentication methods policy

Please migrate your authentication methods off the legacy MFA and SSPR policies by September 2025 to avoid any service impact

2. On the **Groups** page, click **New Group**.



Basic information

Total groups	0	Dynamic groups	0
M365 groups	0	Cloud groups	0
Security groups	0	On-premises groups	0

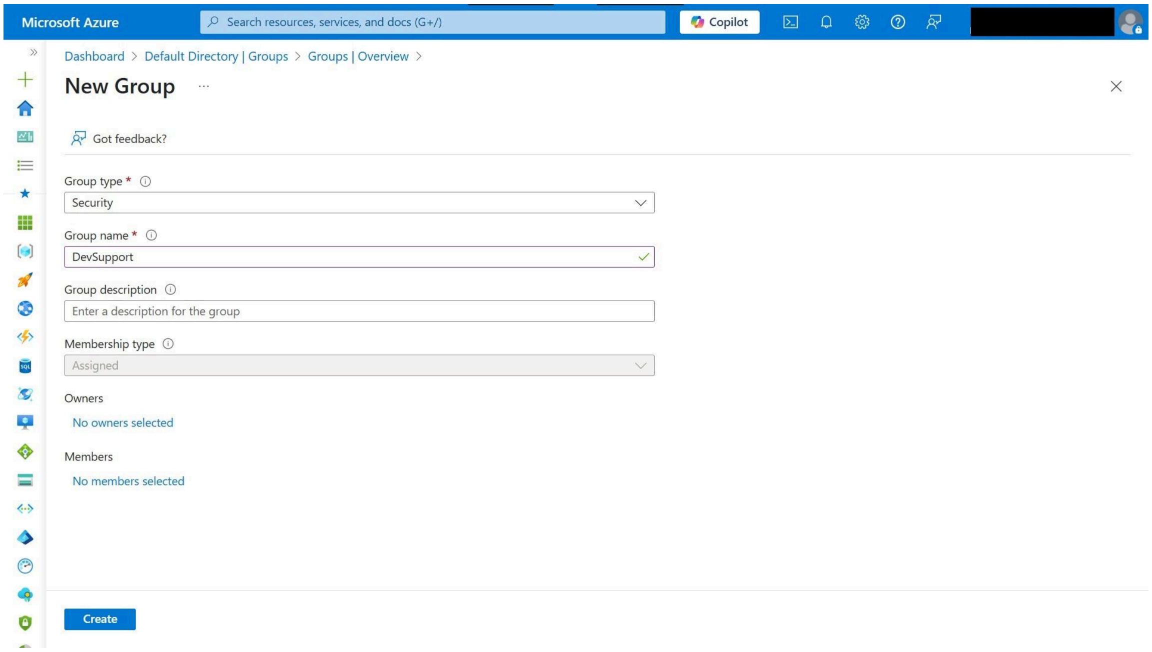
Alerts

Feature highlights

Access reviews

Make sure only the right people have continued access.

3. On the **New Group** page, choose the desired **Group type**, fill in the required details, and click **Create**.


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Dashboard > Default Directory | Groups > Groups | Overview >
Got feedback?
Create

[redacted]

New Group

Group type * Security

Group name * DevSupport

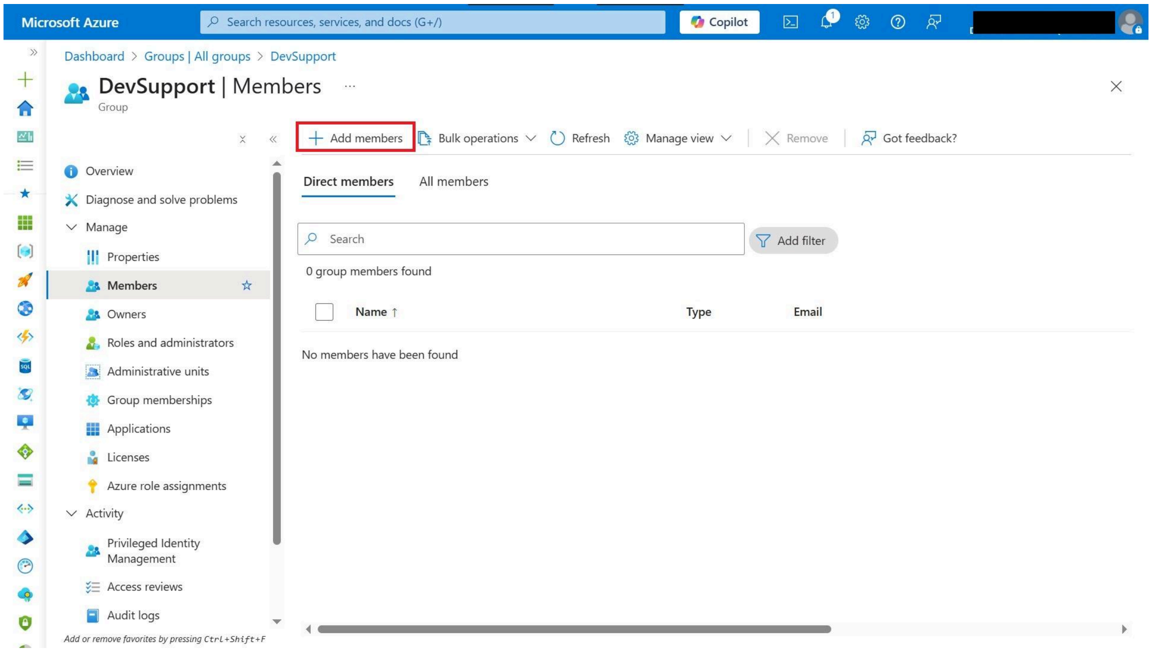
Group description Enter a description for the group

Membership type Assigned

Owners
No owners selected

Members
No members selected

4. To add members, go to **All Groups**, select the group you just created, then go to **Members** and click **Add Members**.



[redacted]

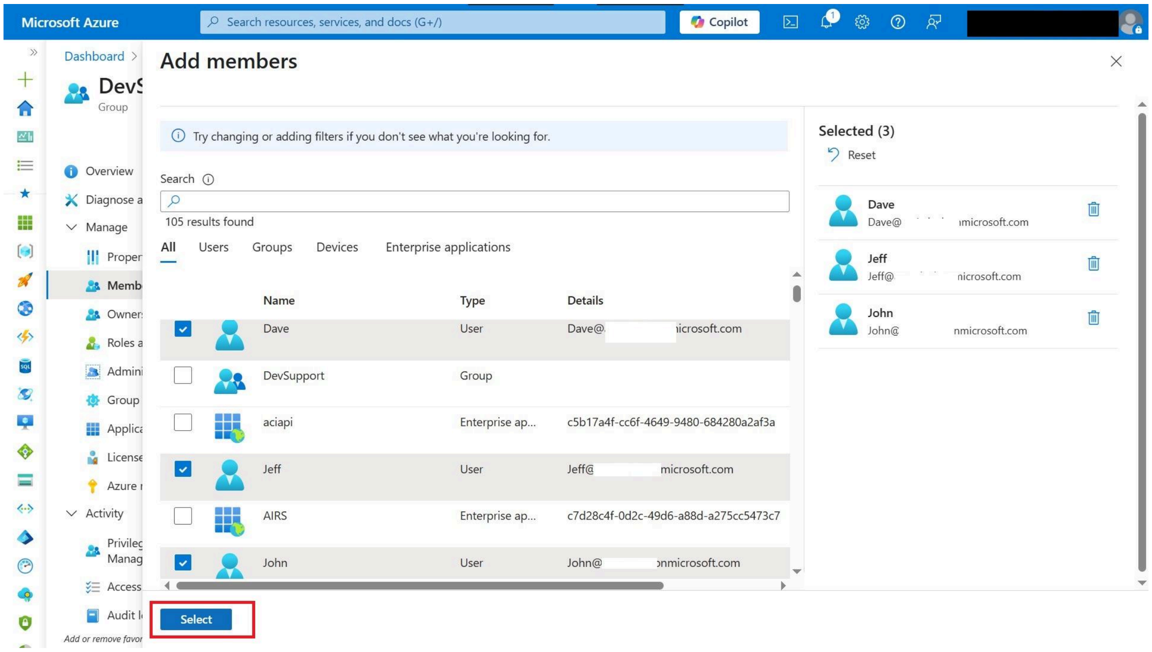
DevSupport | Members

0 group members found

Name ↑	Type	Email

No members have been found

5. Select the users you want to add, then confirm your selection.



Add members

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

Search

105 results found

All | Users | Groups | Devices | Enterprise applications

	Name	Type	Details
☑	Dave	User	Dave@ icrosoft.com
□	DevSupport	Group	
□	aciapi	Enterprise ap...	c5b17a4f-cc6f-4649-9480-684280a2af3a
☑	Jeff	User	Jeff@ microsoft.com
□	AIRS	Enterprise ap...	c7d28c4f-0d2c-49d6-a88d-a275cc5473c7
☑	John	User	John@ onmicrosoft.com

Selected (3)

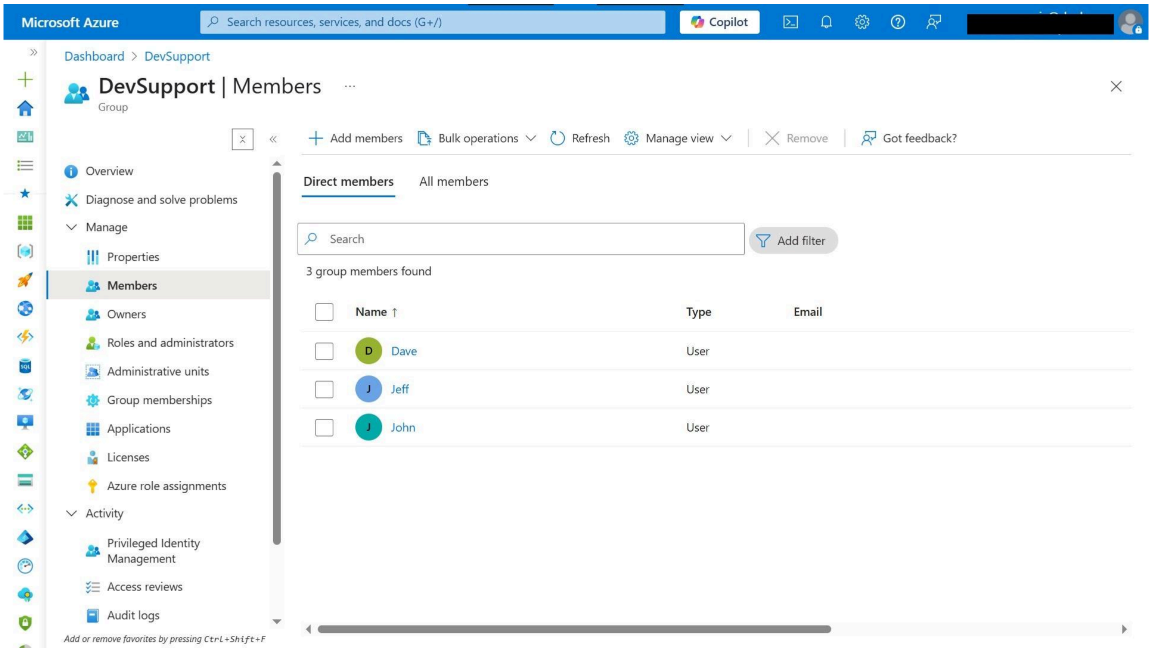
Reset

Dave
Dave@ ımicrosoft.com

Jeff
Jeff@ nicrosoft.com

John
John@ nmicrosoft.com

6. After refreshing the page, you will see the newly added members.



DevSupport | Members

3 group members found

	Name ↑	Type	Email
□	D Dave	User	
□	J Jeff	User	
□	J John	User	

Task 3: Enable self-service password reset

A P1 license is required for this task.

Task 4: Test self-service password reset

A P1 license is required for this task.

Task 5: Enable and configure multifactor authentication for a user

A P1 license is required for this task.