



Administrative Units

In Azure Active Directory (Azure AD), an administrative unit is a container within which you can delegate administrative responsibilities for managing directory objects. This feature allows you to grant specific administrative permissions to a subset of users or groups in your organization, rather than providing full administrative access to the entire directory. Administrative units help in organizing and securing the management of directory objects such as users, groups, and devices. They are particularly useful in large organizations where different departments or teams require autonomy over certain aspects of directory management.



Use cases of Administrative Units:

Administrative units in Azure AD are beneficial in various scenarios, including:

1. **Departmental Segregation:** In large organizations with multiple departments, administrative units can be used to delegate administrative control to departmental IT teams. For example, the HR department might have control over user management for their staff, while the IT department retains control over broader directory settings.
2. **Geographical Segmentation:** Companies with a global presence can use administrative units to assign administrative privileges based on geographical regions. This ensures that local IT teams have control over user accounts, groups, and resources specific to their region while maintaining centralized oversight.
3. **Project-based Access Control:** For organizations working on multiple projects concurrently, administrative units can be created for each project. This allows project managers to have administrative control over the resources and users associated with their projects without interfering with other projects' configurations.
4. **Delegated Administration for Partners or Customers:** In scenarios where external partners or customers need access to certain resources within your Azure AD environment, administrative units can be utilized to delegate administrative control selectively. This ensures that partners or customers have the necessary permissions without compromising the security of other parts of the directory.
5. **Compliance and Security:** Administrative units can help enforce compliance and security policies by limiting administrative privileges to only the necessary individuals or teams. This reduces the risk of unauthorized access to sensitive data or configurations within the directory.
6. **Organizational Restructuring:** During organizational restructuring or mergers/acquisitions, administrative units can facilitate the transition by allowing for the segregation of administrative responsibilities based on the new organizational structure.

In this lab exercise, the goal is to explore the functionalities of administrative units in Azure Active Directory (Azure AD) and understand their practical applications. The steps outlined involve creating users and groups, assigning administrative roles within specific units, and demonstrating how administrative permissions are applied based on unit membership. The

end goal is to gain hands-on experience in utilizing administrative units to delegate administrative responsibilities, organize directory management, and enforce security policies effectively within an organization's Azure AD environment.

😊 To begin with the Lab:

1. The prerequisites for this lab, you should delete all the user and groups and which we had created so far.
2. Then we are going to create users using Bulk Operations. For that you are going to use a CSV file which has the set of users.
3. You can get this file from GitHub.

A	B	C	D
1 version:v1.0			
2 Name [displayName] Required	User name [userPrincipalName] Required	Initial password [passwordProfile] Required	Block sign
3 UserA	UserA@CloudFreaks.onmicrosoft.com	Azure@123	No
4 UserB	UserB@CloudFreaks.onmicrosoft.com	Azure@123	No
5 UserC	UserC@CloudFreaks.onmicrosoft.com	Azure@123	No
6 UserD	UserD@CloudFreaks.onmicrosoft.com	Azure@123	No
7 UserE	UserE@CloudFreaks.onmicrosoft.com	Azure@123	No
8 UserF	UserF@CloudFreaks.onmicrosoft.com	Azure@123	No
9 UserG	UserG@CloudFreaks.onmicrosoft.com	Azure@123	No
10 UserH	UserH@CloudFreaks.onmicrosoft.com	Azure@123	No
11 AdminA	AdminA@CloudFreaks.onmicrosoft.com	Azure@123	No
12 AdminB	AdminB@CloudFreaks.onmicrosoft.com	Azure@123	No
13			

4. Now click on Bulk Operation then choose Bulk Create, after that upload your CSV file, and click on Create.

Bulk create users



1. Download csv template (optional)

[Download](#)

2. Edit your csv file

3. Upload your csv file

"UserCreateTemplate.csv"



File uploaded successfully

[Learn more about bulk import users](#)

5. Once you get the message that it succeeded, then refresh the users list and you will all your users in place.

<input type="checkbox"/>	Display name ↑	User principal name ↑	User type	On-premises sync...	Identities	Company name
<input type="checkbox"/>	A AdminA	AdminA@CloudFreaks.on...	Member	No	CloudFreaks.onmicrosoft.com	
<input type="checkbox"/>	A AdminB	AdminB@CloudFreaks.on...	Member	No	CloudFreaks.onmicrosoft.com	
<input type="checkbox"/>	PK Pukit Kumar	PukitKumar@CloudFreek...	Member	No	CloudFreaks.onmicrosoft.com	
<input type="checkbox"/>	U UserA	UserA@CloudFreaks.onmi...	Member	No	CloudFreaks.onmicrosoft.com	
<input type="checkbox"/>	U UserB	UserB@CloudFreaks.onmi...	Member	No	CloudFreaks.onmicrosoft.com	
<input type="checkbox"/>	U UserC	UserC@CloudFreaks.onmi...	Member	No	CloudFreaks.onmicrosoft.com	
<input type="checkbox"/>	U UserD	UserD@CloudFreaks.onmi...	Member	No	CloudFreaks.onmicrosoft.com	
<input type="checkbox"/>	U UserE	UserE@CloudFreaks.onmi...	Member	No	CloudFreaks.onmicrosoft.com	
<input type="checkbox"/>	U UserF	UserF@CloudFreaks.onmi...	Member	No	CloudFreaks.onmicrosoft.com	
<input type="checkbox"/>	U UserG	UserG@CloudFreaks.onmi...	Member	No	CloudFreaks.onmicrosoft.com	
<input type="checkbox"/>	U UserH	UserH@CloudFreaks.onmi...	Member	No	CloudFreaks.onmicrosoft.com	

6. Now you are going to create groups and add the users accordingly.
7. After that go to the groups and create a new group. Give it a name then choose two members User C and D.

New Group

[Got feedback?](#)

Group type * ⓘ

Group name * ⓘ

Group description ⓘ

Microsoft Entra roles can be assigned to the group ⓘ

Yes No

Membership type * ⓘ

Owners

No owners selected

Members

2 members selected

Selected (2)

↻ Reset



UserC



UserD



8. Then again you are going to create a new group and add 2 users in it which are User G and H.

New Group

...

👤 Got feedback?

Group type * ⓘ

Security



Group name * ⓘ

General-group



Group description ⓘ

Enter a description for the group

Microsoft Entra roles can be assigned to the group ⓘ

Yes

No

Membership type * ⓘ

Assigned



Owners

No owners selected

Members

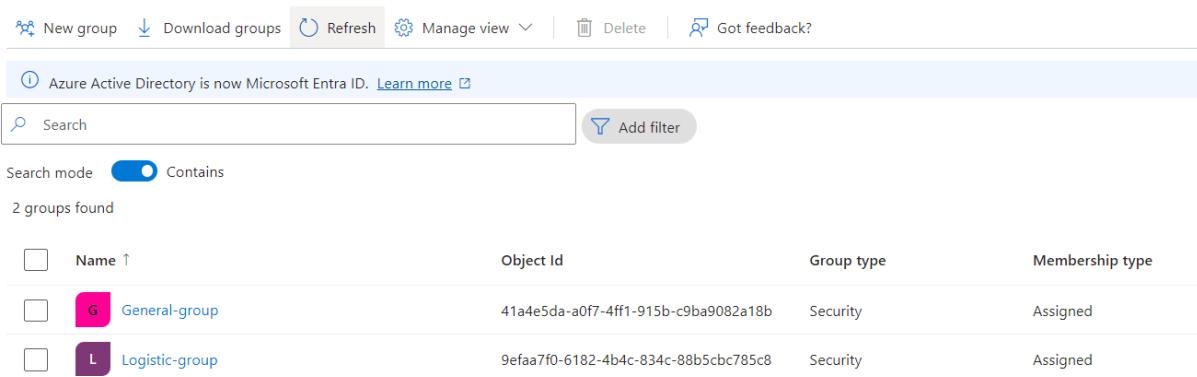
2 members selected

Selected (2)

↶ Reset

	UserH	
	UserG	

9. Currently you can see that we have two groups in place as of now.



Azure Active Directory is now Microsoft Entra ID. Learn more ↗

New group Download groups Refresh Manage view Delete Got feedback?

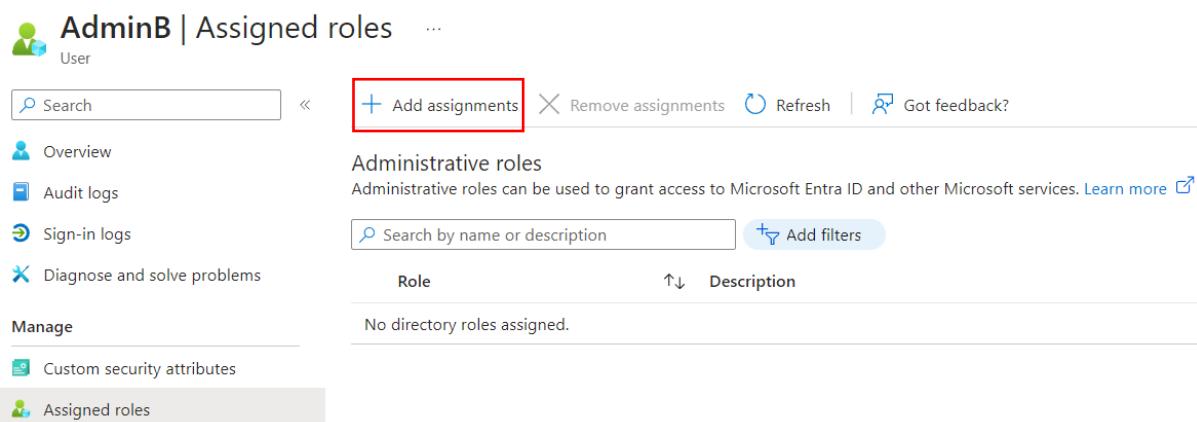
Search mode Contains

2 groups found

	Name ↑	Object Id	Group type	Membership type
<input type="checkbox"/>	G General-group	41a4e5da-a0f7-4ff1-915b-c9ba9082a18b	Security	Assigned
<input type="checkbox"/>	L Logistic-group	9efaa7f0-6182-4b4c-834c-88b5cbc785c8	Security	Assigned

10. Now we are going to Users, from there go inside Admin B and go onto the assigned roles.

11. Now we are going to add an active assignment. Click on it.



AdminB | Assigned roles

User

+ Add assignments

Remove assignments Refresh Got feedback?

Overview Audit logs Sign-in logs Diagnose and solve problems

Custom security attributes Assigned roles

Administrative roles

Administrative roles can be used to grant access to Microsoft Entra ID and other Microsoft services. Learn more ↗

Search by name or description Add filters

Role	↑↓	Description
No directory roles assigned.		

12. Then search for the user administrator role and add it to user Admin B.

Directory roles

X

Choose admin roles that you want to assign to this user. [Learn more](#)

Role	Description
<input type="checkbox"/> Extended Directory User Administrator	Manage all aspects of external user profiles in the extended directory for Teams.
<input checked="" type="checkbox"/> User Administrator	Can manage all aspects of users and groups, including resetting passwords for limited admins.

13. Once it is done then come back to the default directory and move to administrative units.
14. Now click on add to create a new unit.

[Home](#) > [CloudFreaks](#)

CloudFreaks | Administrative units

Learn more Add Delete Refresh Preview features

Search administrative units

Administrative units

Roles and administrators

Delegated admin partners

Enterprise applications

Name Description

No administrative units found.

15. Just give a name to your unit and move onto the next.

Properties Assign roles Review + create

Name *

 ✓

Description

Enter the description of the administrative unit

Restricted management administrative unit ⓘ

Yes No

16. Now on the next page you have to choose User Administrator role.

Add administrative unit

 Got feedback?

Administrative roles

Administrative roles can be used to grant access to Microsoft Entra ID and other Microsoft services. [Learn more](#)

Role ↑↓	Description	Type
 Authentication Administrator	Can access to view, set and reset authentication method info...	Built-in
 Cloud Device Administrator	Limited access to manage devices in Microsoft Entra ID.	Built-in
 Groups Administrator	Members of this role can create/manage groups, create/man...	Built-in
 Helpdesk Administrator	Can reset passwords for non-administrators and Helpdesk A...	Built-in
 License Administrator	Can manage product licenses on users and groups.	Built-in
 Password Administrator	Can reset passwords for non-administrators and Password A...	Built-in
 Printer Administrator	Can manage all aspects of printers and printer connectors.	Built-in
 Privileged Authentication Administrator	Can access to view, set and reset authentication method info...	Built-in
 SharePoint Administrator	Can manage all aspects of the SharePoint service.	Built-in
 Teams Administrator	Can manage the Microsoft Teams service.	Built-in
 Teams Devices Administrator	Can perform management related tasks on Teams certified d...	Built-in
 User Administrator	Can manage all aspects of users and groups, including resett...	Built-in

17. And then choose Admin A as your user when it asks you.

Selected (1)

 Reset



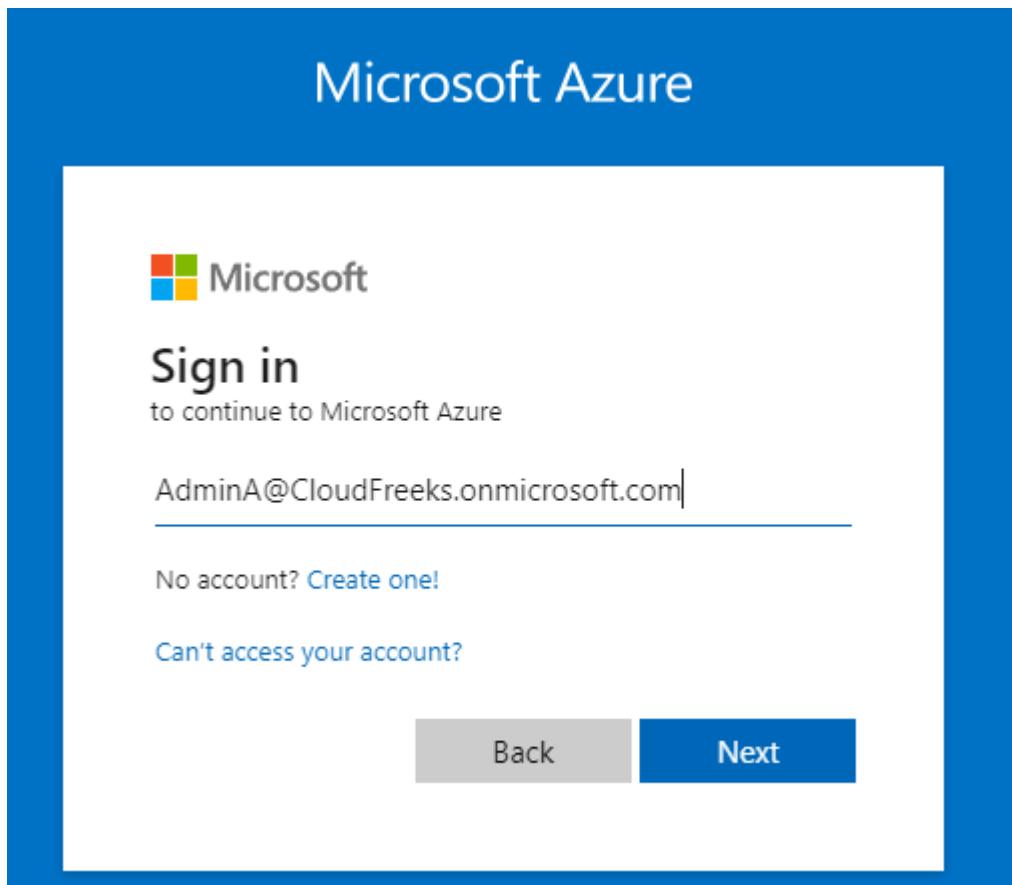
AdminA

AdminA@CloudFreaks.onmicrosoft.com



18. Then move on to review and create and create your administrative unit.

19. Then go to users and login to Admin A user.



20. Then enter the password and because we are logging in for the first time we need to change the password.
21. Now you need to login with Admin B user simultaneously.
22. Then open Microsoft Entra ID for both of the users.
23. Now from your Admin B user you need to go to Users and then from all users open User E.
24. Here for user E we can edit the properties and reset the password.
25. Because remember, this particular administrator has the user admin role when it comes to Azure AD as a whole, when it comes to the entire directory.

A screenshot of the Microsoft Entra ID user properties page for "UserE". The top navigation bar includes a search bar, a back arrow, and several action buttons: "Edit properties" (highlighted with a red box), "Delete", "Refresh", "Reset password", "Revoke sessions", "Manage view", and "Got feedback?". The main content area shows the "Overview" tab selected, with other tabs for "Audit logs" and "Sign-in logs". Below the tabs, there are sections for "Basic info" and "Advanced info".

26. Even for user A you can you are able to edit the properties and reset password.

The screenshot shows the Microsoft Azure portal's user management interface. On the left, a sidebar for 'UserA' lists options like Overview, Audit logs, Sign-in logs, Diagnose and solve problems, Manage (with sub-options for Custom security attributes and Assigned roles), and a large 'U' icon. The main area is titled 'Basic info' and displays the user details: 'UserA', 'UserA@CloudFreaks.onmicrosoft.com', and 'Member'. At the top, there are buttons for Edit properties, Delete, Refresh, Reset password, and Revoke sessions.

27. But for Admin A user if you go to user E, then here you will see that you cannot edit the properties and even you cannot reset the password.

The screenshot shows the Microsoft Azure portal's user management interface for 'UserE'. The sidebar is identical to the UserA page. The main area shows 'Basic info' for 'UserE', 'UserE@CloudFreaks.onmicrosoft.com', and 'Member'. The 'Reset password' button is visible in the top navigation bar but is greyed out, indicating it cannot be used for this user.

28. If you look carefully then you have the ability to click on reset password but if you do that then you'll get the error.
29. Because Admin A user is only the admin, the user administrator of this particular admin unit, and user E is not part of the admin unit.

A modal dialog box titled 'Reset password' is shown. It contains the message: 'The password can not be reset. This may be due to an incorrect level of administrative privilege or if trying to reset your own password.' There is a close button 'X' in the top right corner.

30. Let's go to User A who is the part of admin unit and here also you can see that we can change the properties.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes 'Microsoft Azure', a search bar, and user information 'AdminA@CloudFreaks... CLOUDFREEKS (CLOUDFREEKS.O...)'. Below the navigation bar, the URL 'Home > CloudFreaks | Users > Users > UserA' is visible. The main content area displays 'UserA' with a blue 'U' icon. A sidebar on the left lists 'Overview', 'Audit logs', 'Sign-in logs', 'Diagnose and solve problems', 'Manage', 'Custom security attributes', and 'Assigned roles'. The 'Overview' tab is selected. The 'Basic info' section shows 'UserA@CloudFreaks.onmicrosoft.com' and 'Member' status.

31. Even though we've added admin A as the admin for the admin unit, we have not added the users of user A and user B onto the admin unit, and we haven't added the logistics GRP Azure AD group that contains user C and user D.
32. Now go to administrative unit and open department A

The screenshot shows the 'CloudFreaks | Administrative units' page. The left sidebar has a 'Delegated admin partners' section with 'Administrative units' highlighted and surrounded by a red box. Other items in the sidebar include 'Enterprise applications', 'Devices', and 'App registrations'. The main content area shows a table with columns 'Name', 'Description', 'Restricted management', and 'Membership type'. One row is visible: 'DepartmentA' with 'No' under 'Restricted management' and 'Assigned' under 'Membership type'. The 'Add' button is highlighted with a red box.

33. In users click on add members then select user A and B.

The screenshot shows the 'DepartmentA | Users' page. The left sidebar includes 'Properties (Preview)', 'Users' (highlighted with a red box), 'Groups', 'Devices', and 'Roles and administrators'. The main content area shows a table with columns 'Display name', 'User principal name', 'User type', 'On-premises syn...', 'Identities', and 'Com...'. A note at the top says 'Azure Active Directory is now Microsoft Entra ID'. The 'Add member' button is highlighted with a red box.

Selected (2)

Reset

The screenshot shows a list of selected users: 'UserA' (UserA@CloudFreaks.onmicrosoft.com) and 'UserB' (UserB@CloudFreaks.onmicrosoft.com). Each user entry includes a blue person icon, the user name, the email address, and a blue trash can icon for deletion.

34. Then go to groups, click on add. Then choose your logistic group.

DepartmentA | Groups

CloudFreaks

Search New group Add Remove Delete Refresh Columns Got feedback?

Manage

Properties (Preview)

Users

Groups

Devices

Roles and administrators

Activity

Bulk operation results

Name	Object Id	Group Type	Membership Type
No groups found			

Selected groups (1)

 Reset

 Logistic-group 

35. Now in department A go to roles and administrators. From there choose user administrator.

DepartmentA |

CloudFreaks

Search

Manage

Properties (Preview)

Users

Groups

Devices

Roles and administrators

36. Here you will see that Admin A is the admin of this department A group.

Name	UserName	Type	Scope
AdminA	AdminA@CloudFreaks.onmicrosoft.com	User	This resource
AdminB	AdminB@CloudFreaks.onmicrosoft.com	User	Directory (Inherited)

37. Now in the other tab login back to Admin A user and open Microsoft Entra ID and go to User A here you will see that now we are able to edit the properties and reset password accordingly.

38. But if you go to User C then you are not able to do anything because you can only do that to the users which are added directly as users not to the users which have been added via a group.

39. Now once you are done clean up everything.