😊 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

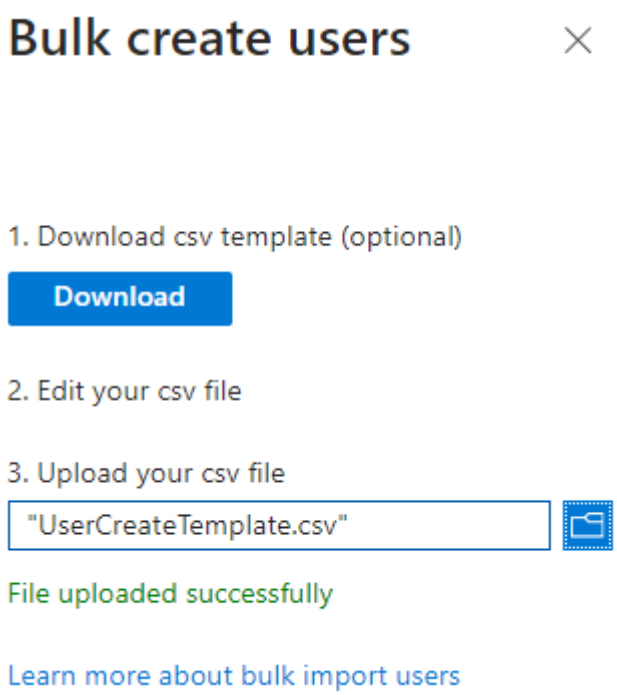
end goal is to gain hands-on experience in utilizing administrative units to delegate administrative responsibilities, organize directory management, and enforce security policies effectively within an organization's Azure AD environment.

😄 To begin with the Lab:

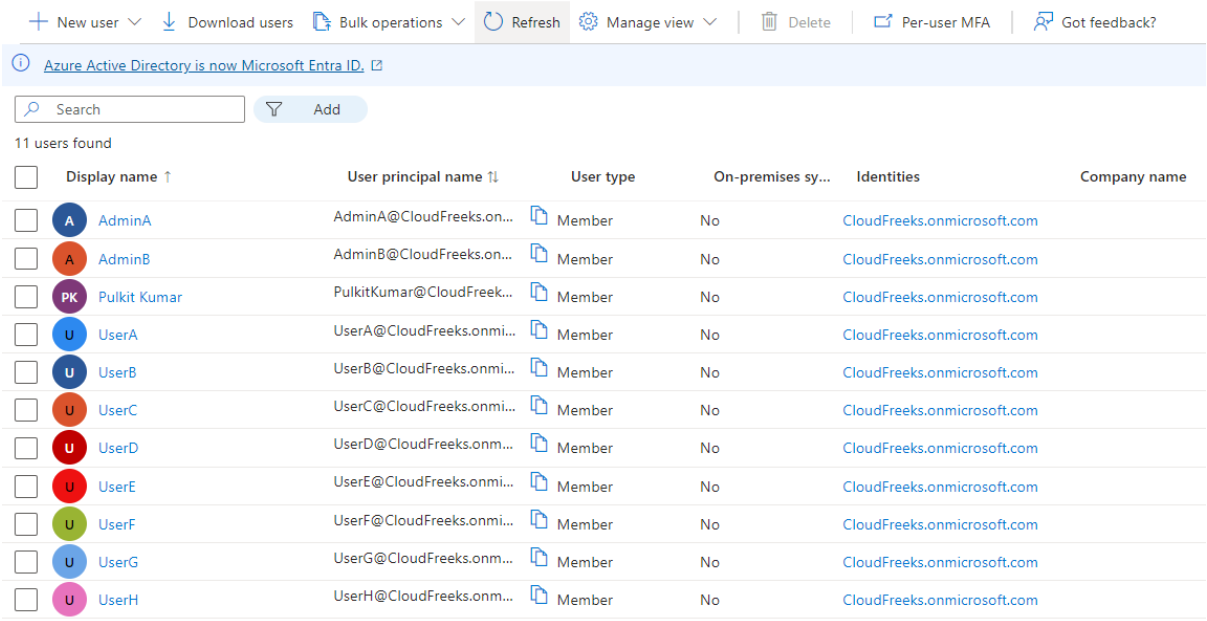
1. The prerequisites for this lab, you should delete all the user and groups and which we had created so far.
2. Then we are going to create users using Bulk Operations. For that you are going to use a CSV file which has the set of users.
3. You can get this file from GitHub.

	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@CloudFreeks.onmicrosoft.com	Azure@123	No
4	UserB	UserB@CloudFreeks.onmicrosoft.com	Azure@123	No
5	UserC	UserC@CloudFreeks.onmicrosoft.com	Azure@123	No
6	UserD	UserD@CloudFreeks.onmicrosoft.com	Azure@123	No
7	UserE	UserE@CloudFreeks.onmicrosoft.com	Azure@123	No
8	UserF	UserF@CloudFreeks.onmicrosoft.com	Azure@123	No
9	UserG	UserG@CloudFreeks.onmicrosoft.com	Azure@123	No
10	UserH	UserH@CloudFreeks.onmicrosoft.com	Azure@123	No
11	AdminA	AdminA@CloudFreeks.onmicrosoft.com	Azure@123	No
12	AdminB	AdminB@CloudFreeks.onmicrosoft.com	Azure@123	No
13				

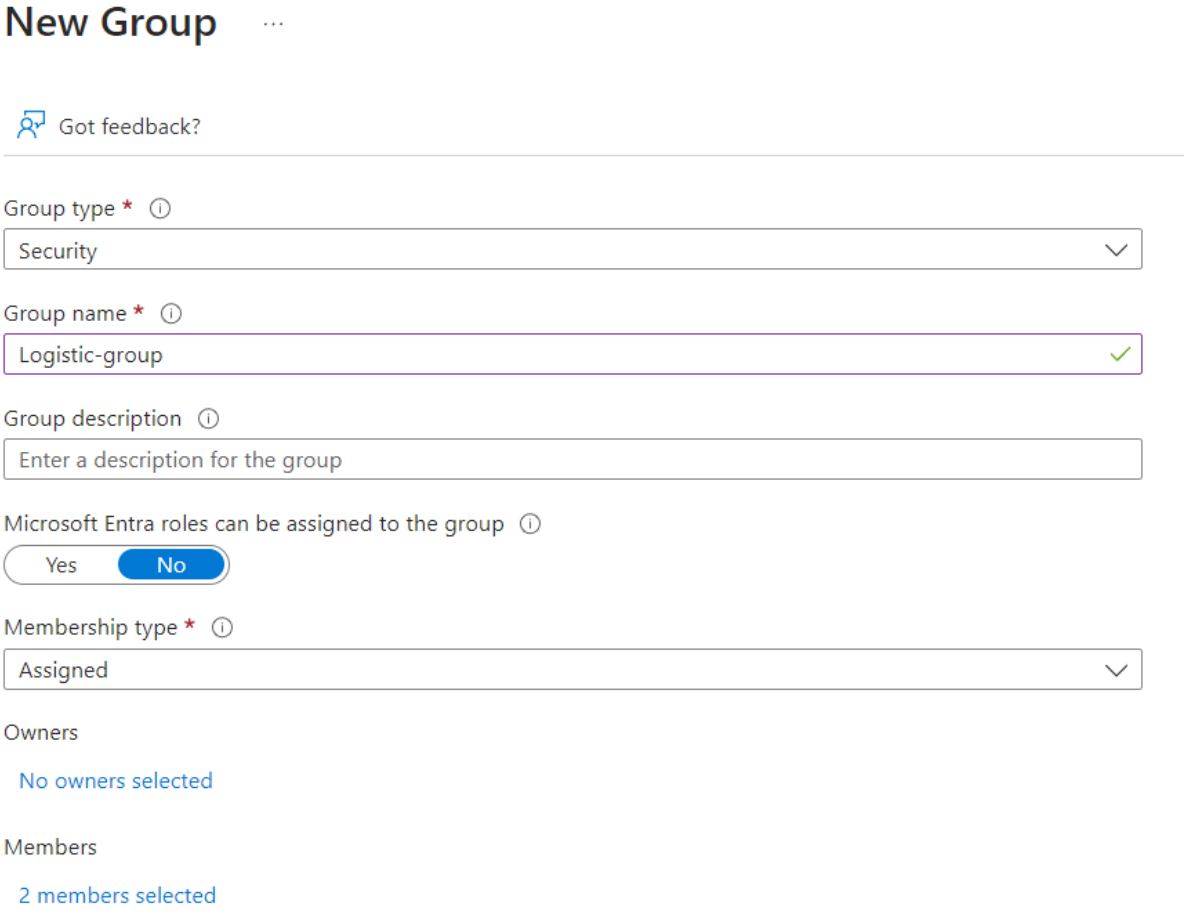
4. Now click on Bulk Operation then choose Bulk Create, after that upload your CSV file, and click on Create.

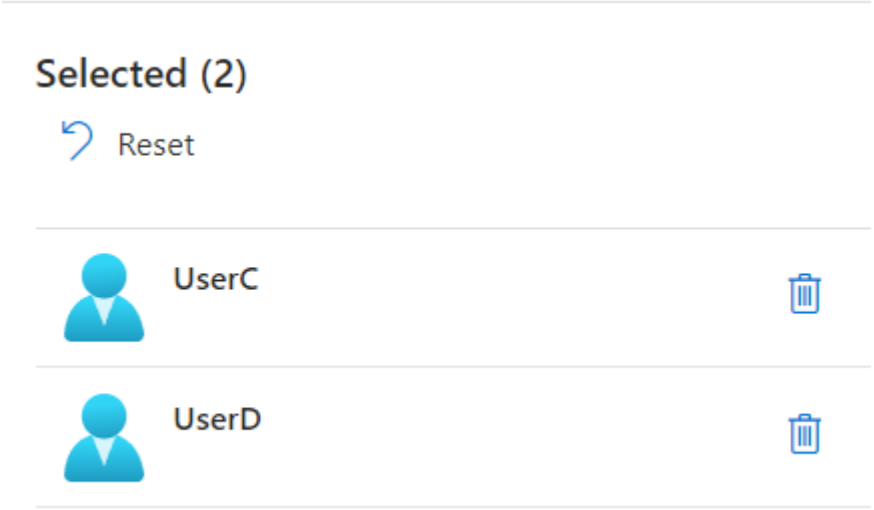


5. Once you get the message that it succeeded, then refresh the users list and you will all your users in place.

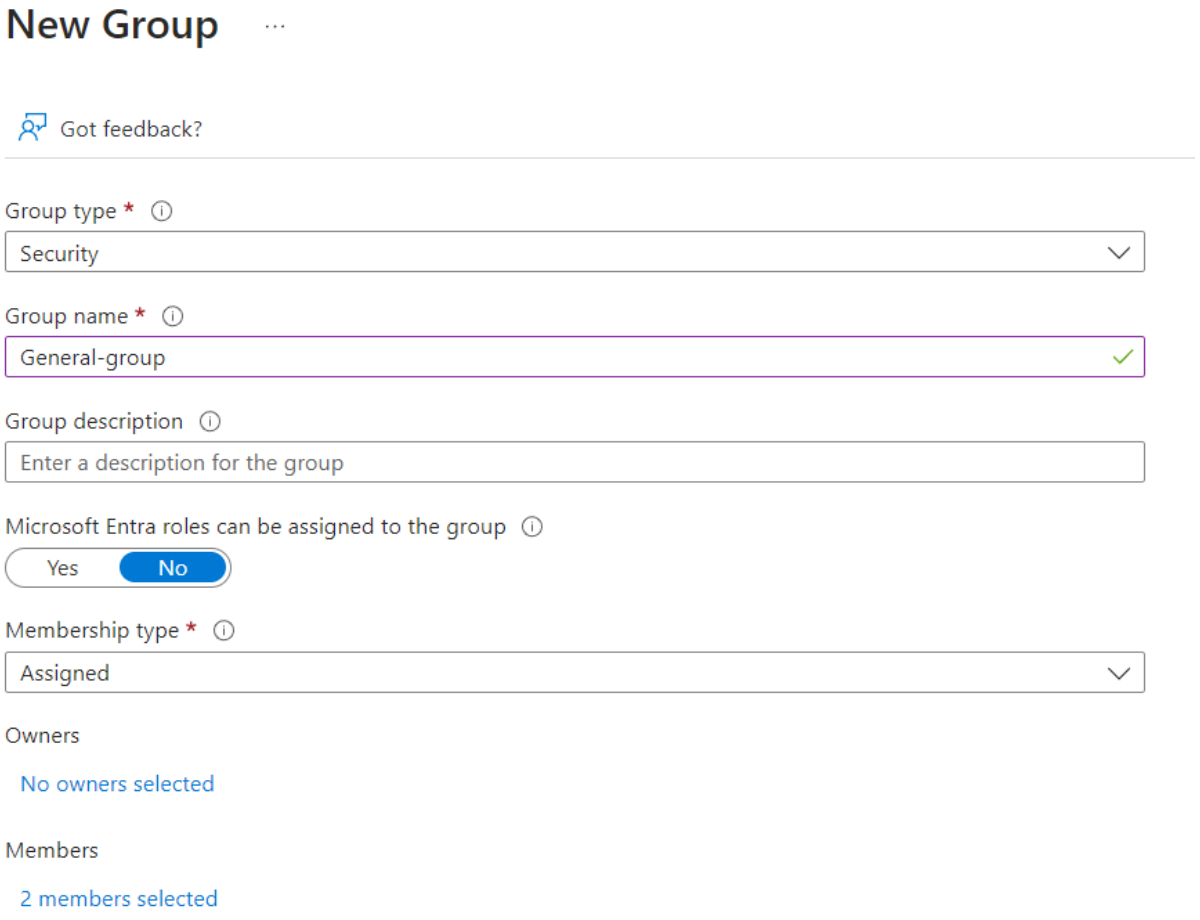


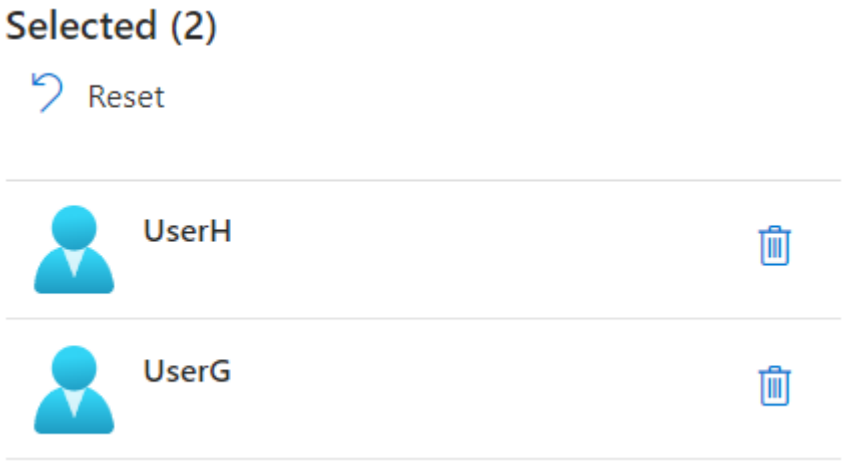
6. Now you are going to create groups and add the users accordingly.
7. After that go to the groups and create a new group. Give it a name then choose two members User C and D.



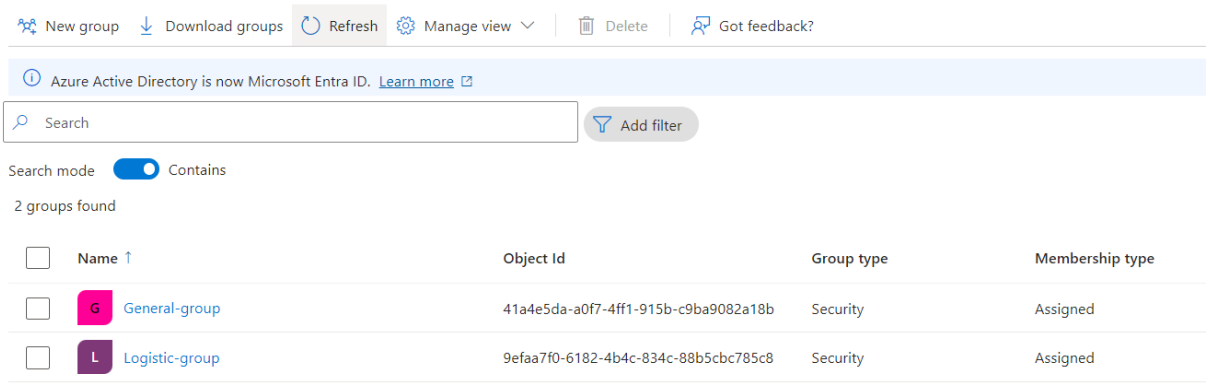


8. Then again you are going to create a new group and add 2 users in it which are User G and H.

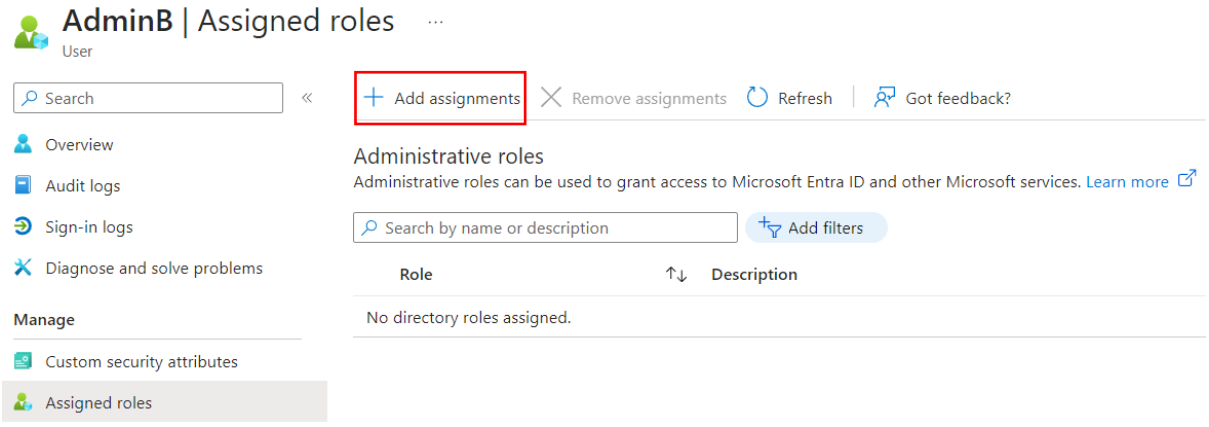




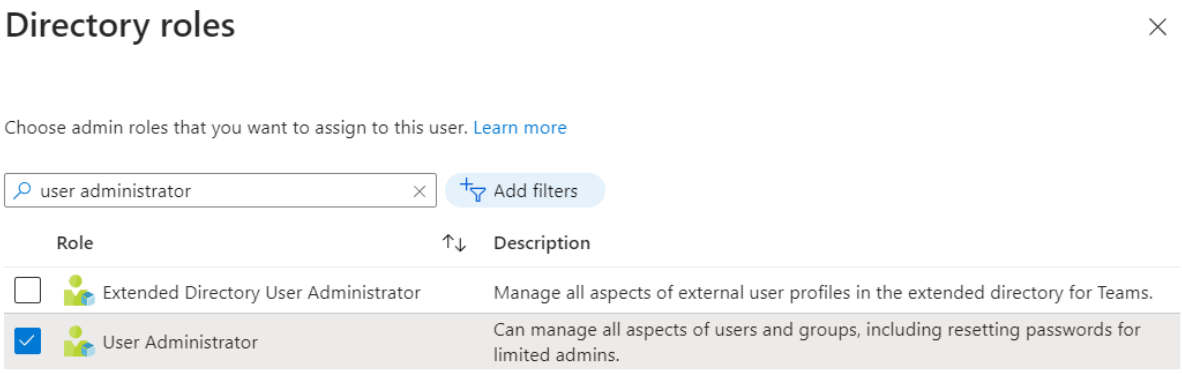
9. Currently you can see that we have two groups in place as of now.



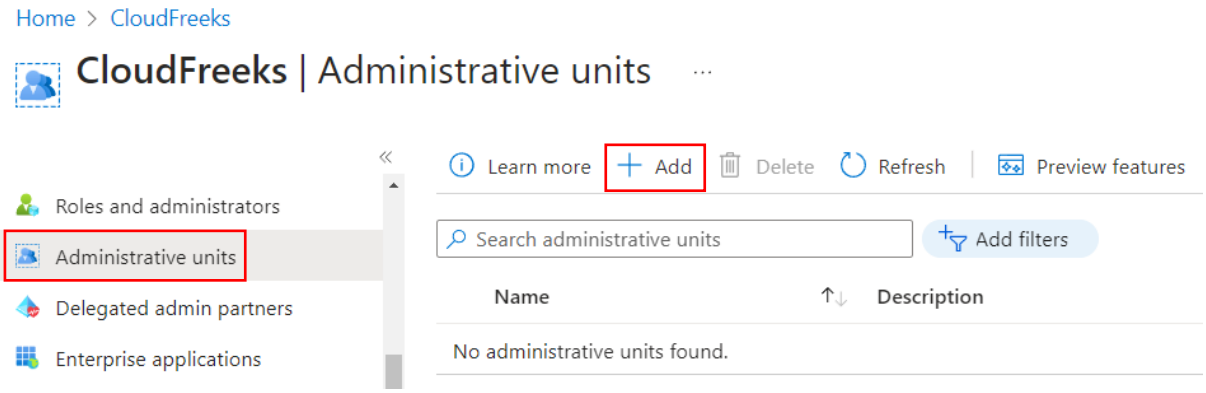
10. Now we are going to Users, from there go inside Admin B and go onto the assigned roles.
11. Now we are going to add an active assignment. Click on it.



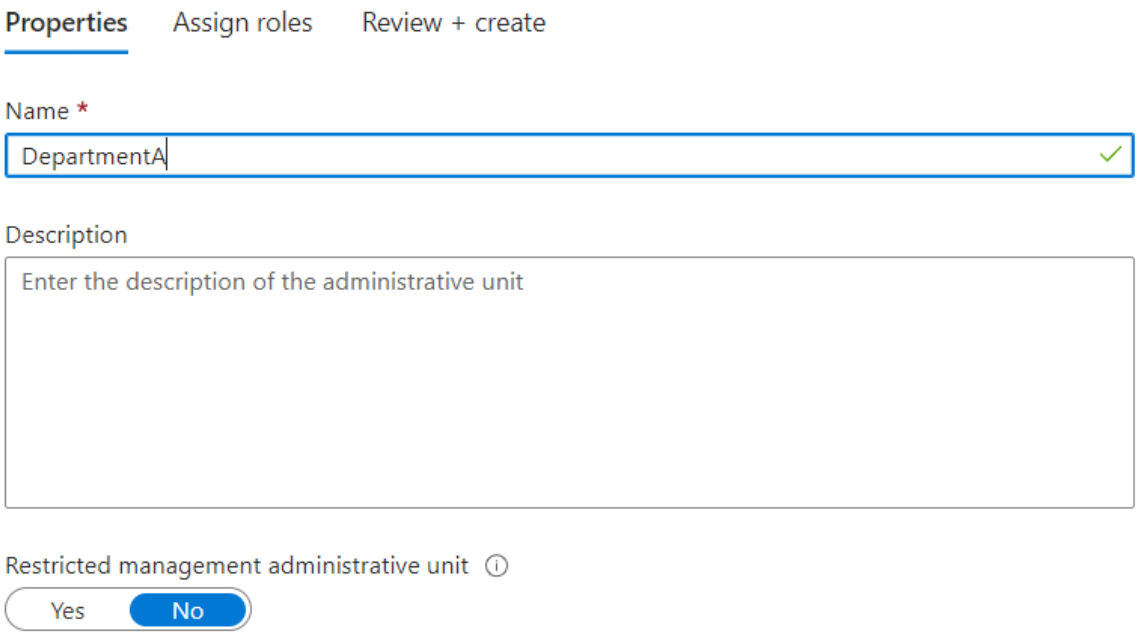
12. Then search for the user administrator role and add it to user Admin B.



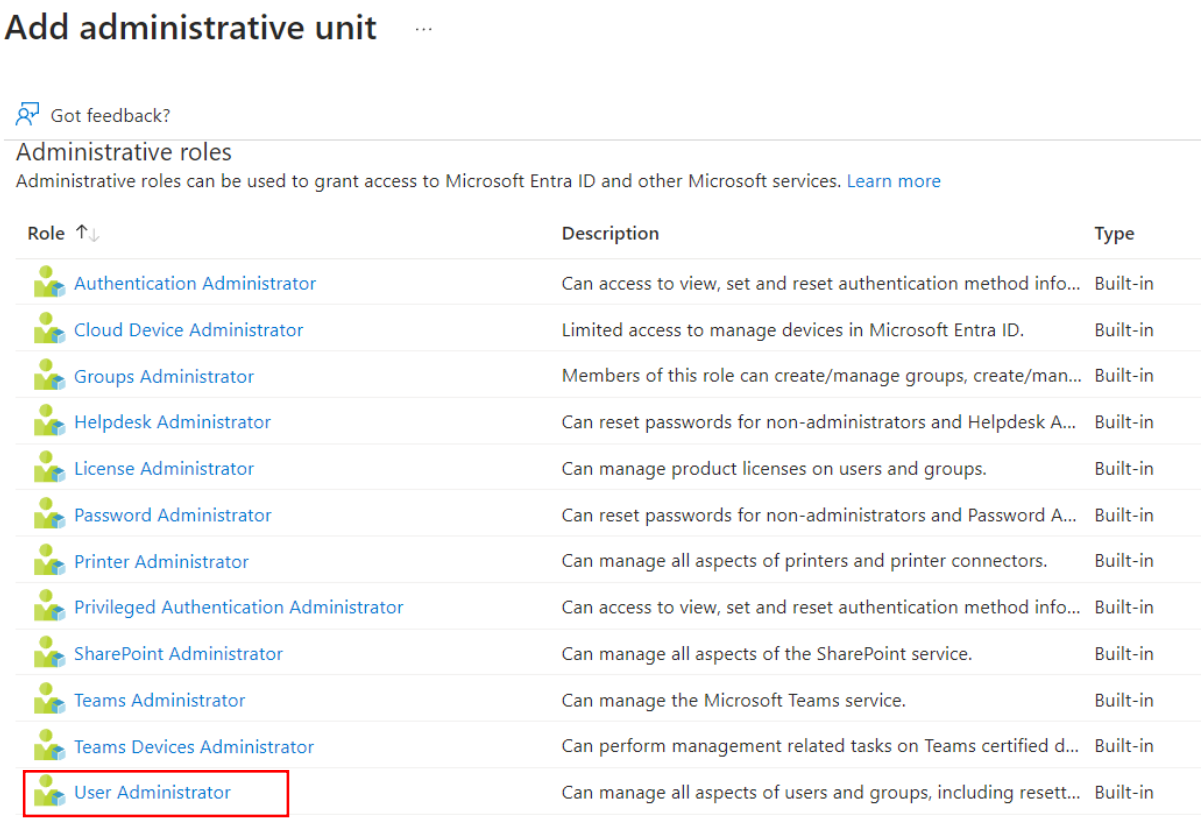
13. Once it is done then come back to the default directory and move to administrative units.
14. Now click on add to create a new unit.



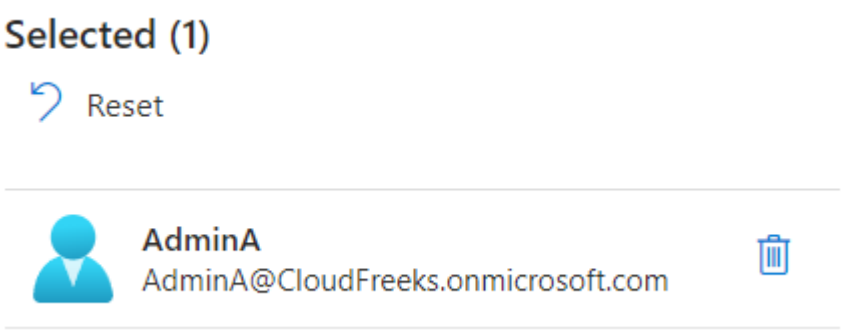
15. Just give a name to your unit and move onto the next.



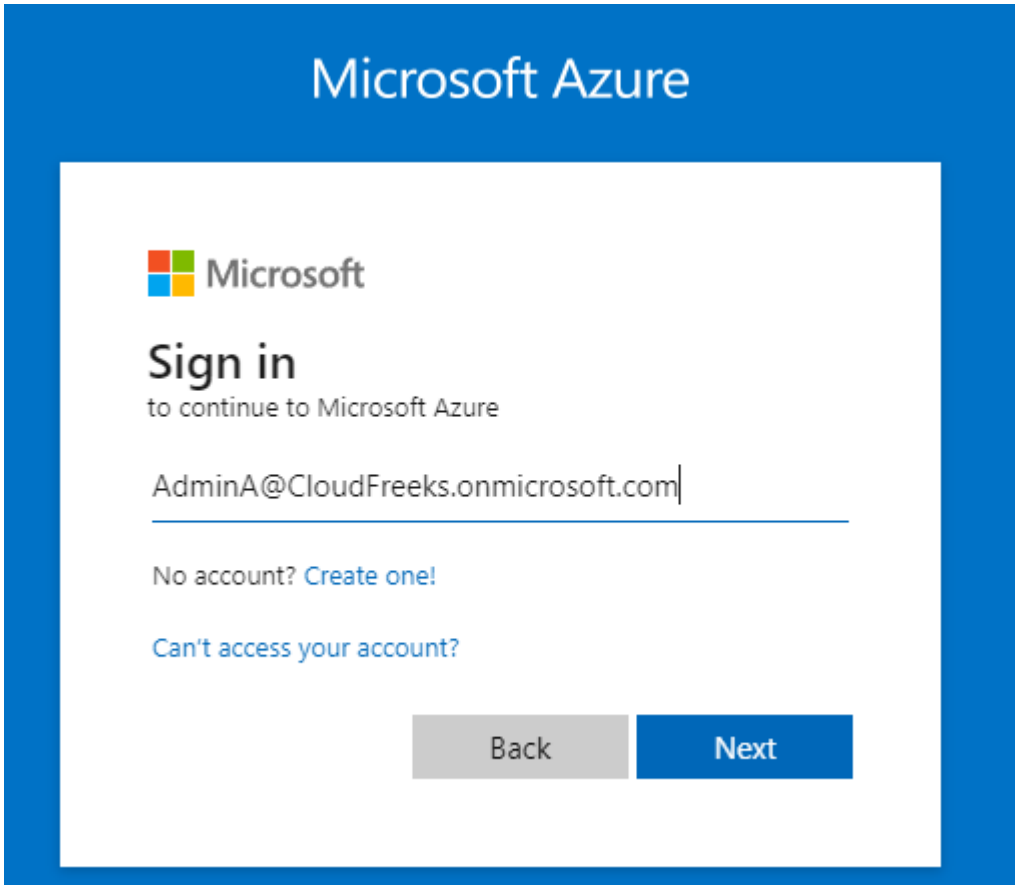
16. Now on the next page you have to choose User Administrator role.



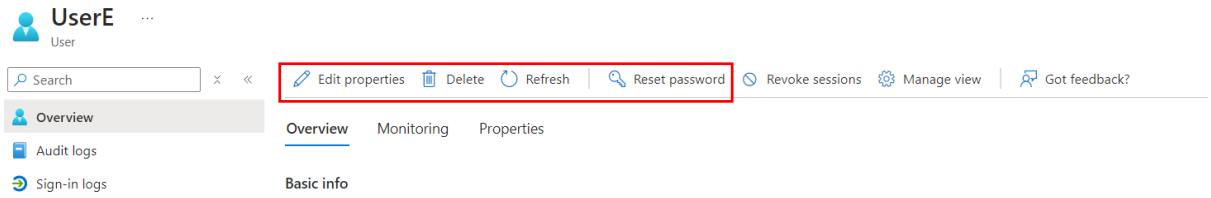
17. And then choose Admin A as your user when it asks you.



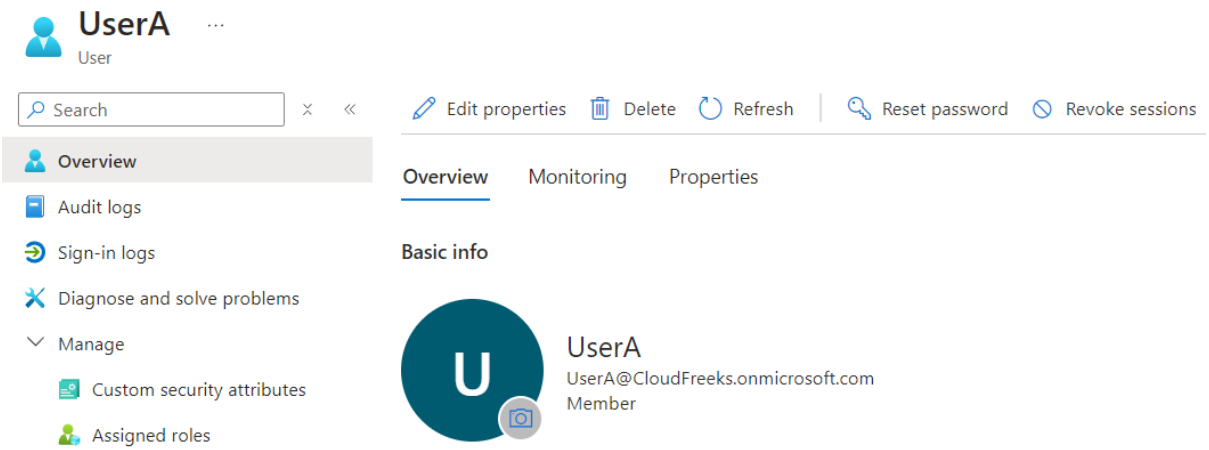
18. Then move on to review and create and create your administrative unit.
19. Then go to users and login to Admin A user.



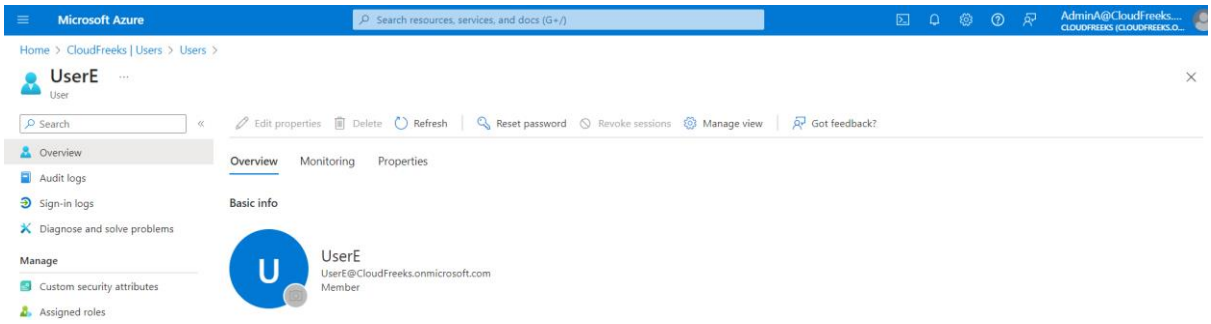
20. Then enter the password and because we are logging in for the first time we need to change the password.
21. Now you need to login with Admin B user simultaneously.
22. Then open Microsoft Entra ID for both of the users.
23. Now from your Admin B user you need to go to Users and then from all users 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.



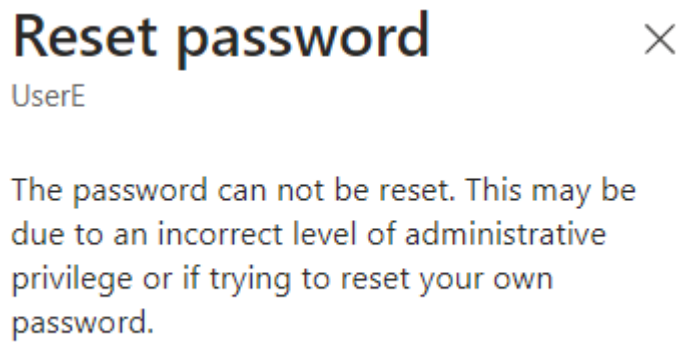
26. Even for user A you can you are able to edit the properties and reset password.



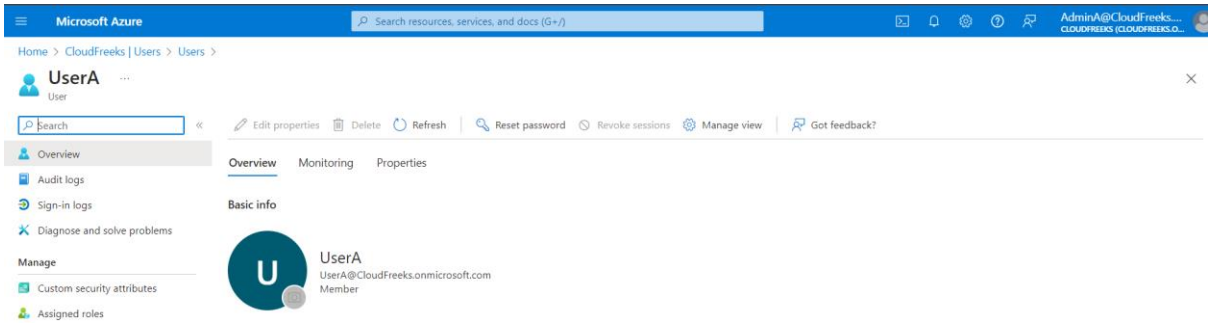
27. But for Admin A user if you go to user E, then here you will see that you cannot edit the properties and even you cannot reset the password.



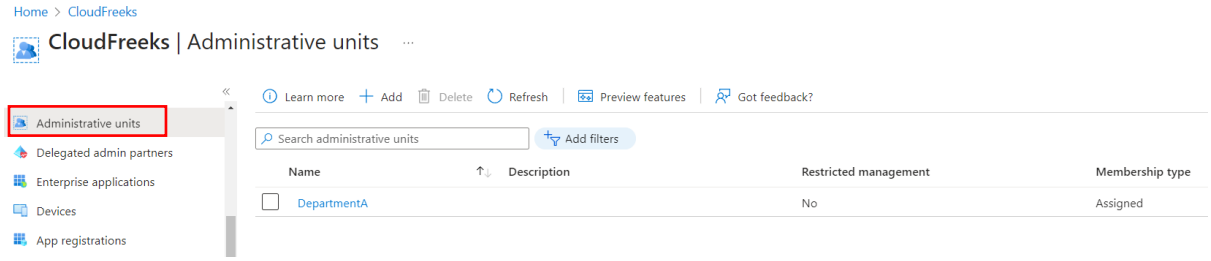
28. If you look carefully then you have the ability to click on reset password but if you do that then you'll get the error.
29. Because Admin A user is only the admin, the user administrator of this particular admin unit, and user E is not part of the admin unit.



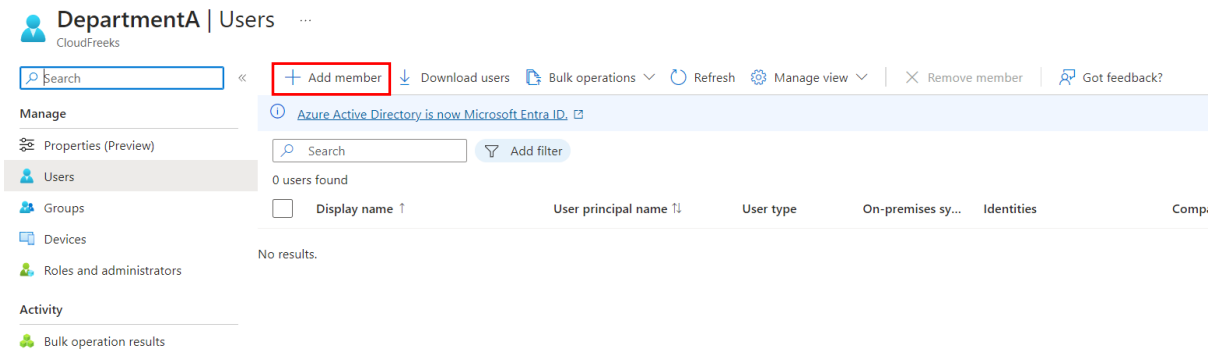
30. Let's go to User A who is the part of admin unit and here also you can see that we can change the properties.

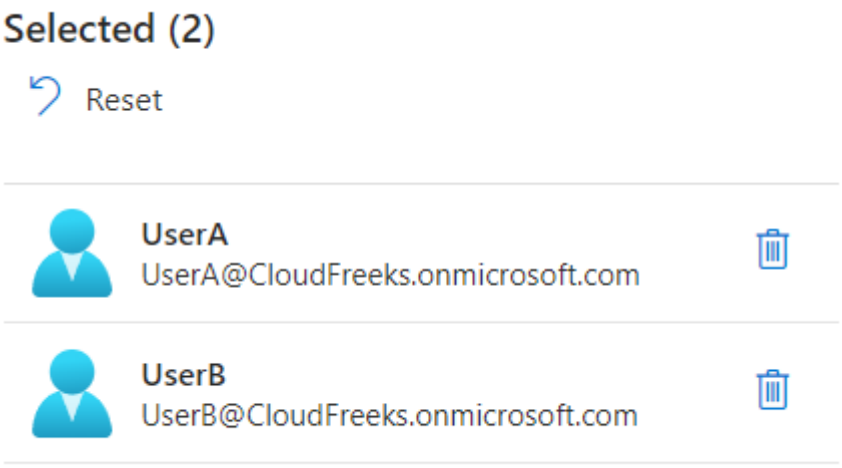


31. Even though we've added admin A as the admin for the admin unit, we have not added the users of user A and user B onto the admin unit, and we haven't added the logistics GRP Azure AD group that contains user C and user D.
32. Now go to administrative unit and open department A

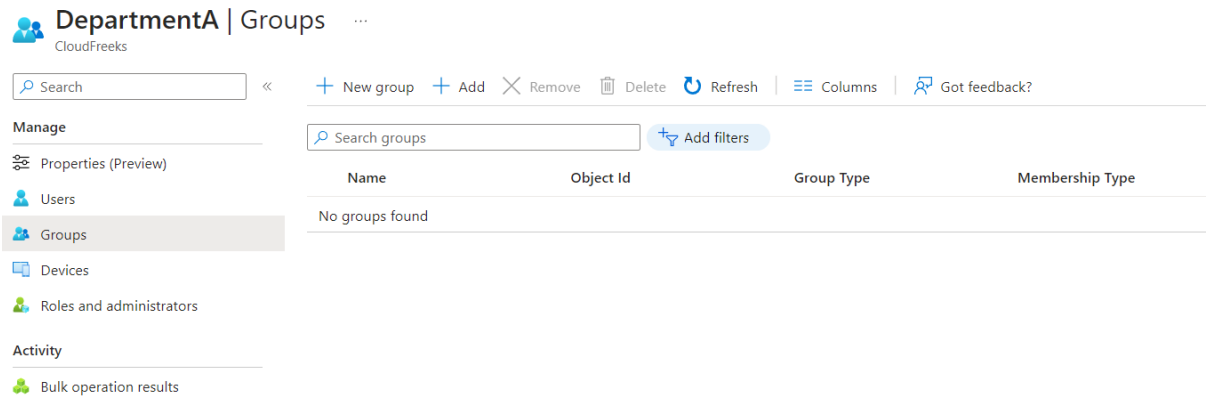


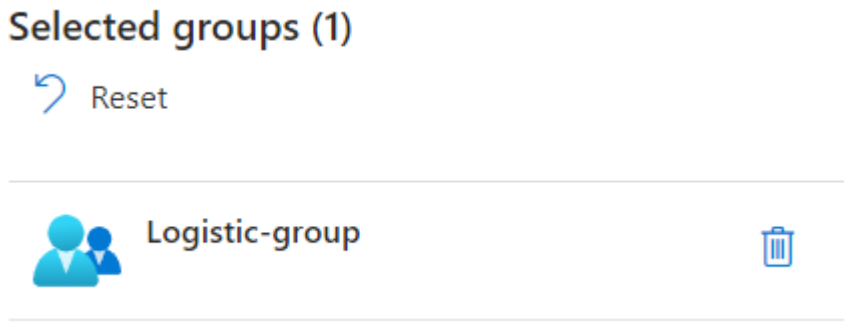
33. In users click on add members then select user A and B.



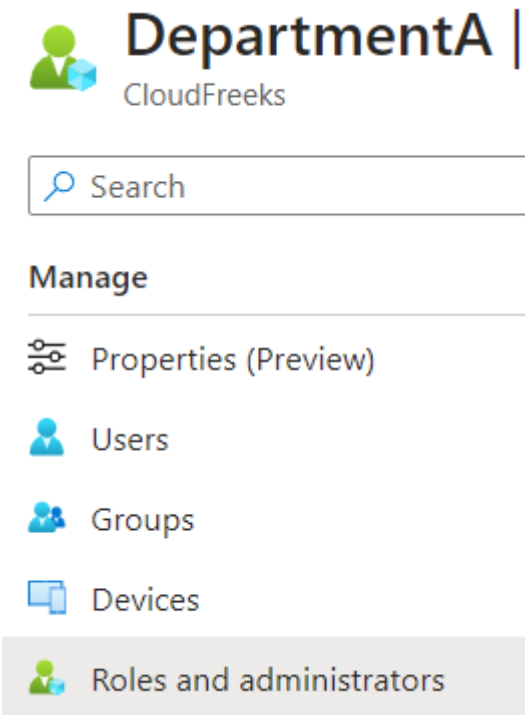


34. Then go to groups, click on add. Then choose your logistic group.

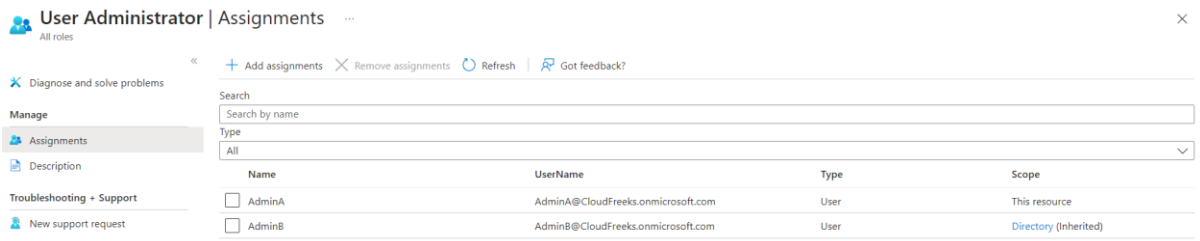




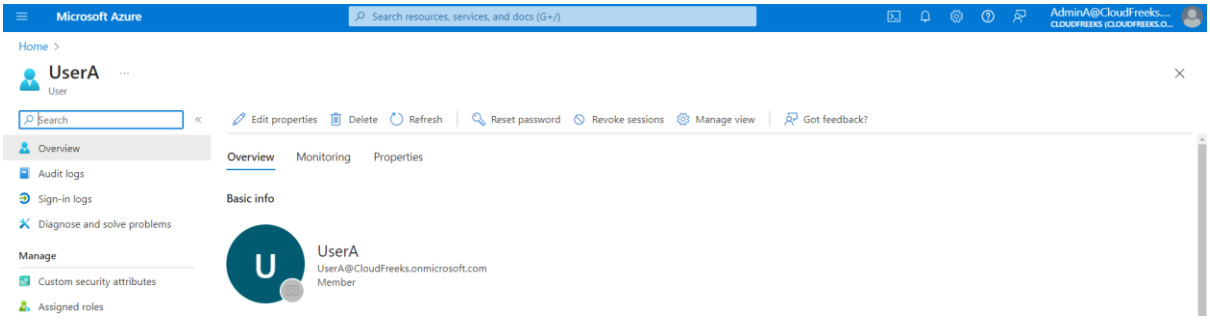
35. Now in department A go to roles and administrators. From there choose user administrator.



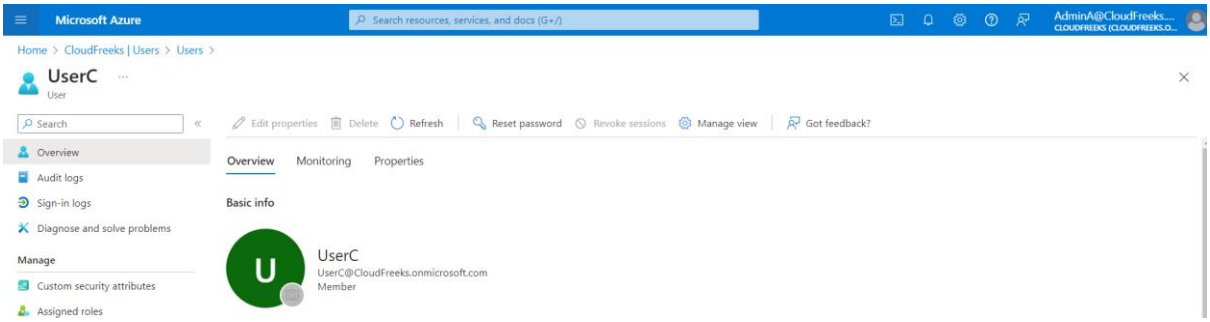
36. Here you will see that Admin A is the admin of this department A group.



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.