

Dynamic groups in Azure AD are special types of groups whose membership is automatically managed based on rules or criteria defined by administrators. Unlike traditional groups where membership is manually added or removed, dynamic groups dynamically update their membership as users or objects within Azure AD match or no longer match the defined criteria.

Here's a summary of dynamic groups in Azure AD:

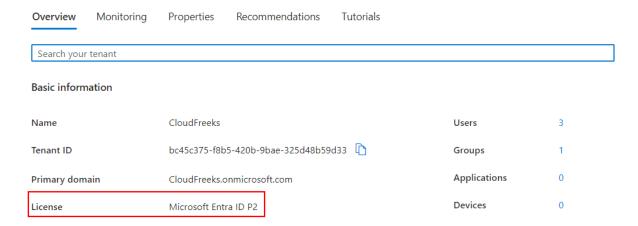
- 1. **Automated Membership:** Dynamic groups automatically add or remove members based on predefined rules or attributes. This eliminates the need for manual management of group membership.
- 2. **Rule-Based Membership:** Administrators can define rules or criteria based on user attributes such as department, job title, location, or other custom attributes. Objects that meet these criteria are dynamically added to the group.
- 3. **Real-Time Updates:** Membership in dynamic groups is continuously evaluated and updated in real-time as changes occur in Azure AD, such as user attribute updates or object creations.
- 4. **Scalability and Efficiency:** Dynamic groups offer scalability and efficiency by automating the process of managing group membership, particularly in large or dynamic environments with frequent user attribute changes.
- 5. **Use Cases:** Dynamic groups are commonly used for scenarios such as role-based access control (RBAC), application assignment, license assignment, and targeted policy enforcement based on user attributes.
- 6. **Integration with Conditional Access:** Dynamic groups can be integrated with Azure AD Conditional Access policies to apply access controls or security policies based on group membership dynamically.

Overall, dynamic groups in Azure AD provide a powerful mechanism for automating group membership management, improving operational efficiency, and ensuring that access controls and policies remain up-to-date in dynamic IT environments.

In this lab, we're setting up a dynamic group in Azure AD and configuring it to automatically manage its membership based on predefined criteria, such as user attributes like city. The end goal is to demonstrate how dynamic groups can automate the process of adding and removing members, improving operational efficiency, and ensuring that access controls remain up-to-date in Azure AD. This allows organizations to dynamically manage group membership without manual intervention, enhancing scalability and reducing administrative overhead.

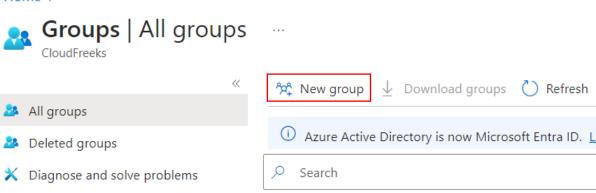
To begin with the Lab:

1. The prerequisite for this lab is that you should have a Microsoft Entra ID P2 license.



- 2. For this lab you should have two users in Azure AD.
- 3. Now go to groups in Azure AD and click on New Group.

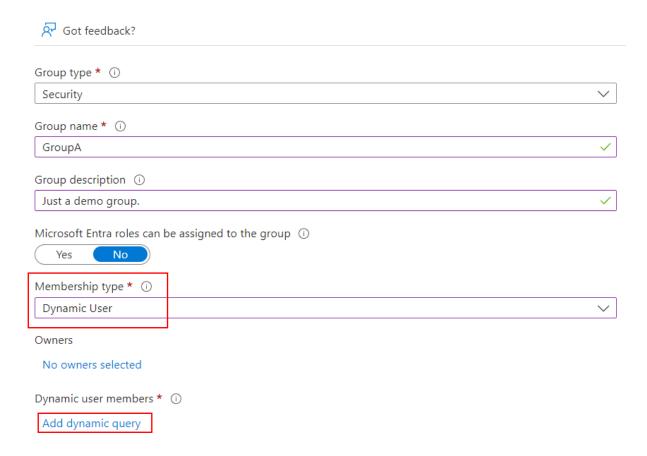
Home >



- 4. Now while creating a group you need to give it a name and then choose the membership type as Dynamic User. This option will allow Azure AD to add user itself to the group based on the query.
- 5. Now click on add dynamic query.

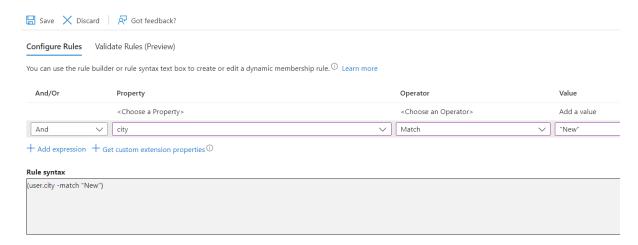
Home > Groups | All groups >

New Group

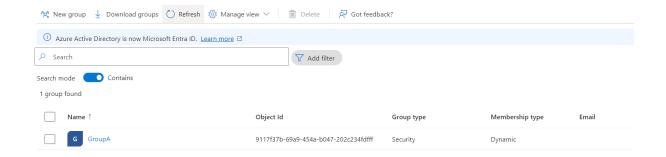


6. Then in your query first you need to click on add expression then choose the property type, after that choose the operator then the value as you can see down below. Choose save.

Dynamic membership rules ---



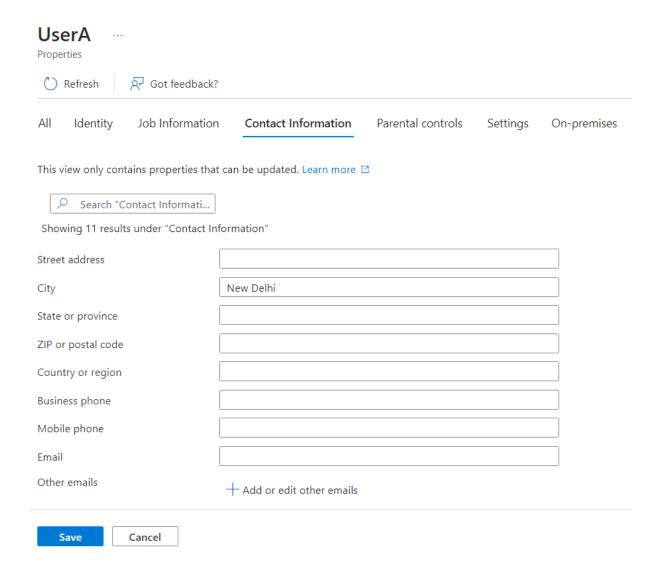
7. After that create your group. Then after some time you will be able to see your group.



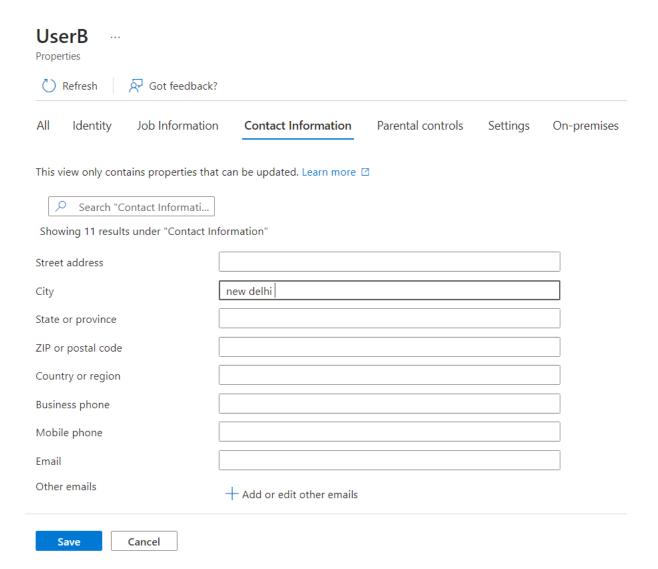
- 8. Once this is done then come back to default directory and go to users.
- 9. Open your User A, click on edit properties.



10. Then go to contact information and in the city type the city of your choices which has a word new in it.

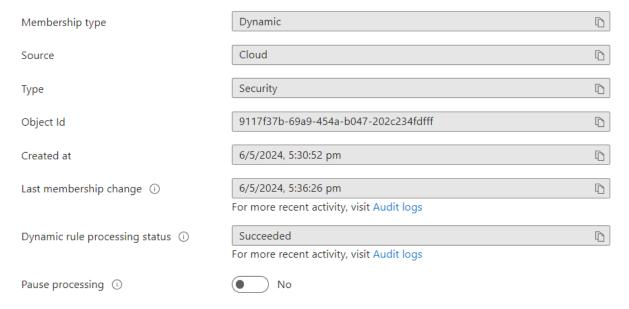


11. After that you need to do the same for User B also.



12. Now you have to wait for some time. Then go to your group and open it. Here you can see the basic information about it like it is a dynamic group.

G GroupA



13. Now from the left pane, go to members and you will see that both of the users has been added to it based on the properties we defined.

