😊 Performing Azure Access Review

Azure Access Review is a feature in Microsoft Azure that allows administrators to periodically review and update access permissions for users and groups within Azure Active Directory (Azure AD). This feature helps organizations ensure that access to resources remains appropriate and up-to-date, reducing the risk of unauthorized access.

With Azure Access Review, administrators can define review schedules, specify the scope of the review (such as specific groups or applications), and select reviewers who will be responsible for evaluating access permissions. Reviewers are typically managers or other individuals who are familiar with the access needs of the users or groups being reviewed.

During the access review process, reviewers are presented with a list of users or groups and their associated access permissions. Reviewers can then either approve the access permissions as they are or request changes, such as revoking access for a user who no longer requires it or granting additional permissions to a user who needs them.

Once the review is complete, administrators can view the results and take appropriate actions based on the feedback provided by reviewers. This may include updating access permissions, removing users or groups that no longer require access, or escalating access issues to higher-level administrators for further review.

😄 Use cases:

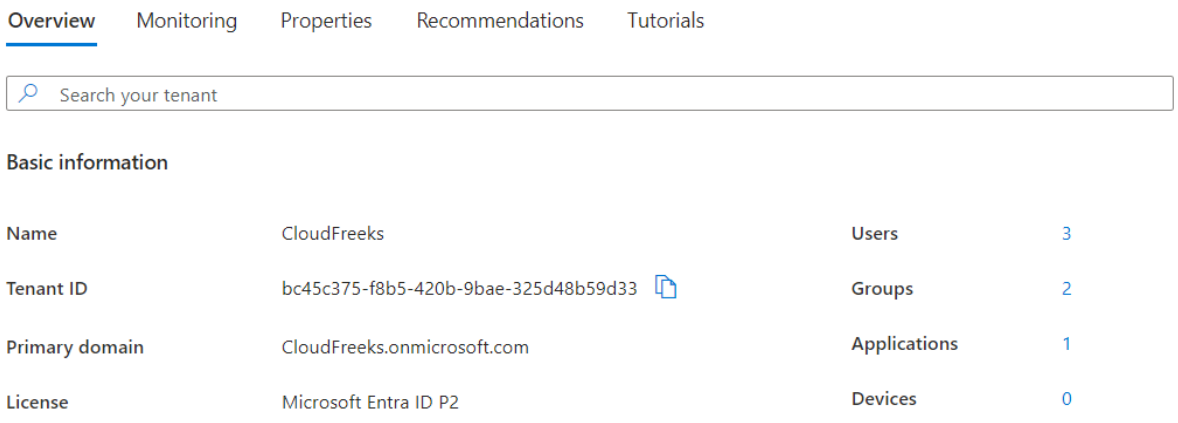
1. **Regular Access Reviews:** Organizations often need to periodically review access permissions to ensure they are aligned with business needs and security policies. Azure Access Review allows administrators to schedule regular reviews of user and group access to resources, helping to identify and address any access permissions that are no longer necessary or appropriate.
2. **Role Changes or Transitions:** When employees change roles within an organization or leave the company, their access requirements may change. Azure Access Review can be used to quickly update access permissions for users and groups to reflect these changes, ensuring that employees have the appropriate level of access to resources based on their current role.
3. **Compliance Audits:** Many industries and regulatory frameworks require organizations to regularly review and audit access permissions to ensure compliance with security and privacy requirements. Azure Access Review provides a centralized platform for conducting these audits, documenting access reviews, and demonstrating compliance to auditors.
4. **External Collaboration:** When collaborating with external partners or vendors, organizations need to carefully manage access to sensitive resources. Azure Access Review can be used to review and approve access permissions for external users, helping to ensure that only authorized individuals have access to confidential data or systems.

5. **Temporary Access:** In some cases, users may require temporary access to resources for a specific project or task. Azure Access Review allows administrators to grant temporary access permissions to users or groups and schedule a review to ensure that access is revoked once it is no longer needed.
6. **Emergency Access Reviews:** In the event of a security breach or other emergency situation, organizations need to quickly assess and revoke access permissions to limit the impact of the incident. Azure Access Review provides a rapid way to review and revoke access for users and groups, helping to mitigate the risk of further unauthorized access.

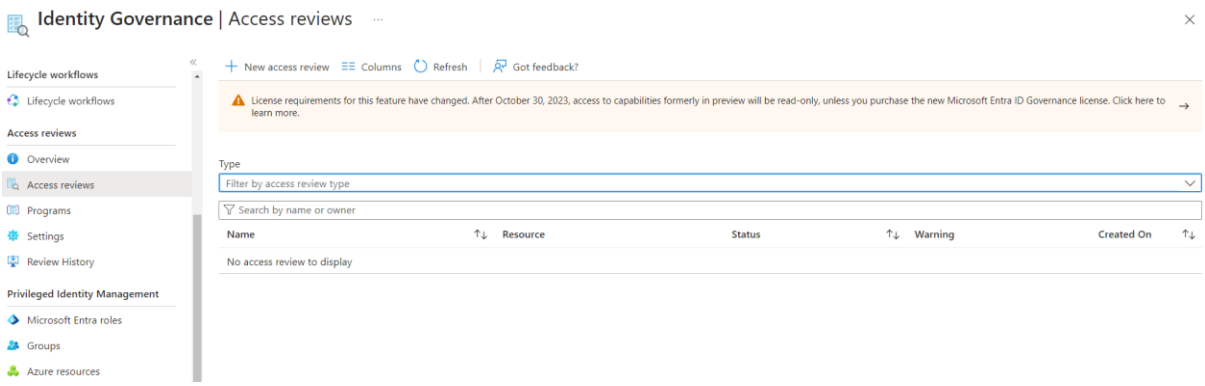
We are carrying out an Azure Access Review in this lab, which entails routinely checking and changing user and group access rights within Azure Active Directory. In order to lower the danger of illegal access, the ultimate objective is to guarantee that access to resources is still suitable and current. Through regular evaluation and modification of access rights in accordance with business requirements and roles within the organization, this process assists companies in maintaining security, compliance, and efficiency.

😄 To begin with this Lab:

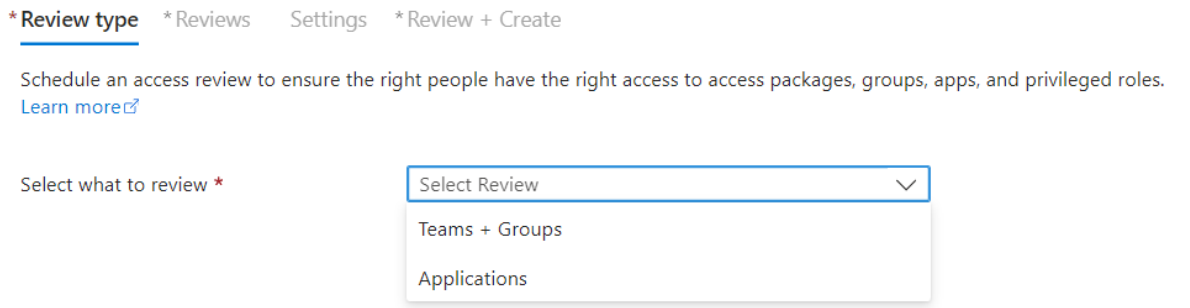
1. Before you begin this lab, there is a requirement that you should have Azure Premium P1 or P2 license with you. As you can see below, we have this P2 license which you can also see in your Microsoft Entra ID formally known as Azure active directory.
2. Also you need to create an User in your Microsoft Entra ID, if you don't have any users in place.



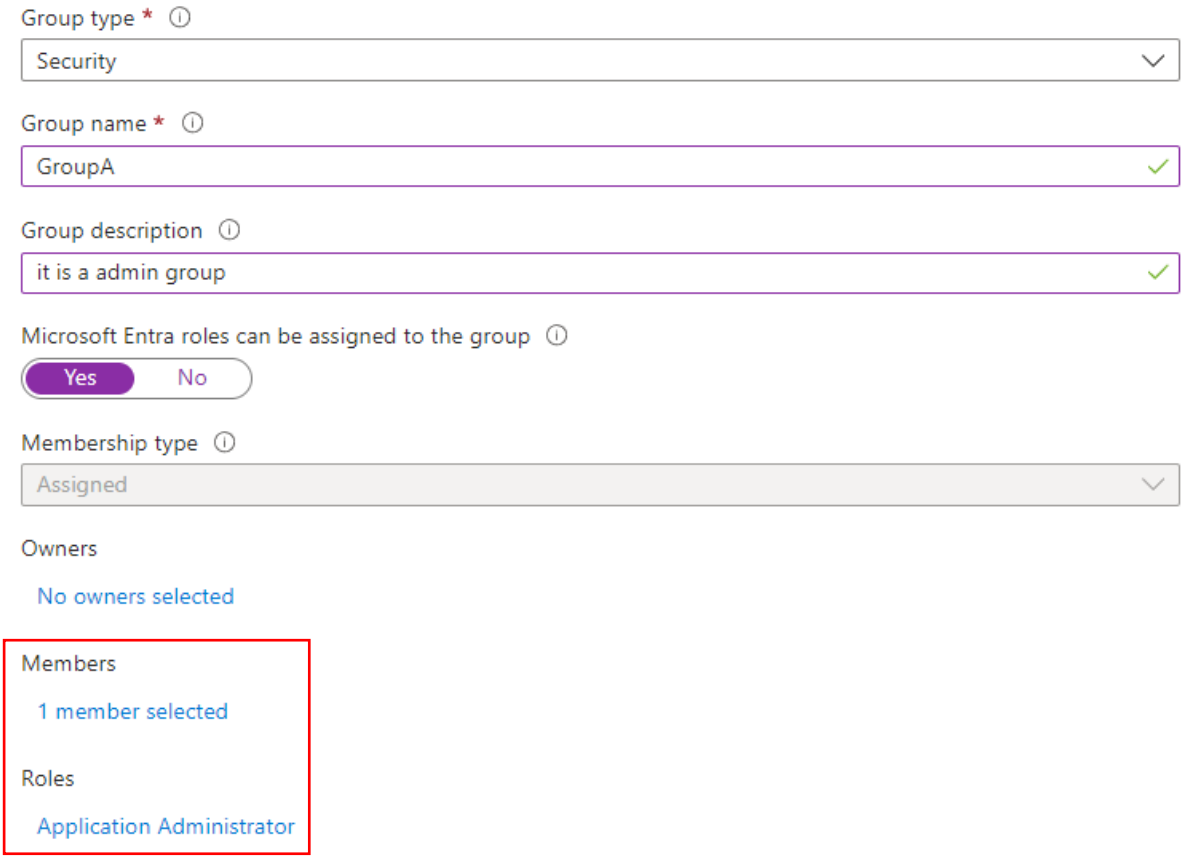
3. Now you need to search Identity Governance and navigate towards this service. Here, you can work with many other services, but we will work with access reviews. Click on new access review to create one.



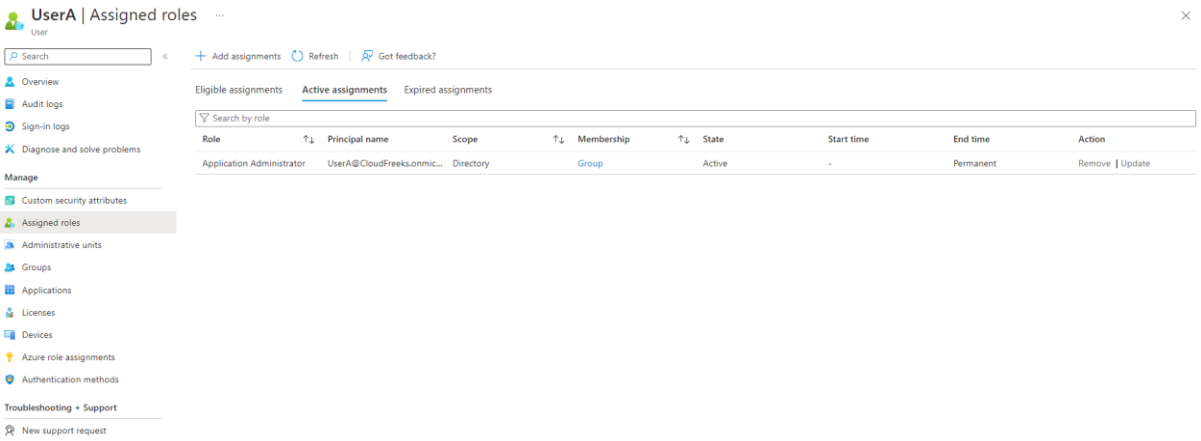
4. So, now in the review type we only have two options as you can see below. So, we need to create a group in order to create a review.



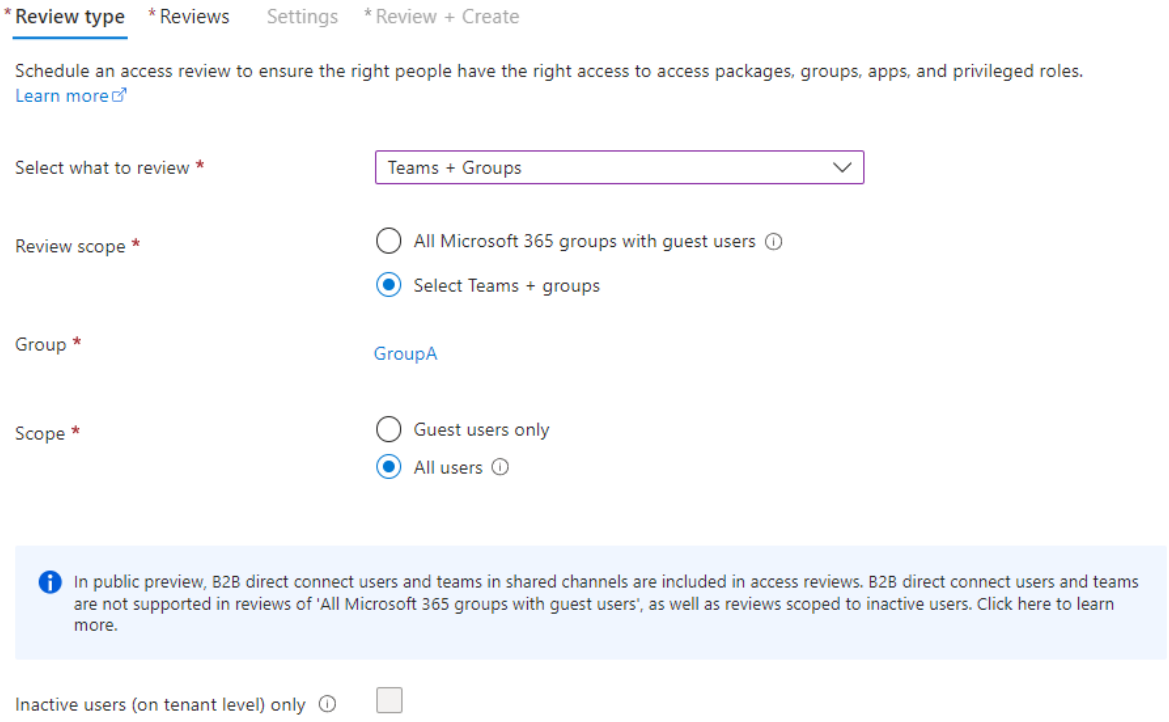
5. For that navigate to Microsoft Entra ID then to groups and create a new group. Now you need to choose group type as security and give your group a name then choose yes for Microsoft Entra roles.
6. After that you need to choose a user from the members and for the roles choose application administrator.
7. Then just create your group.



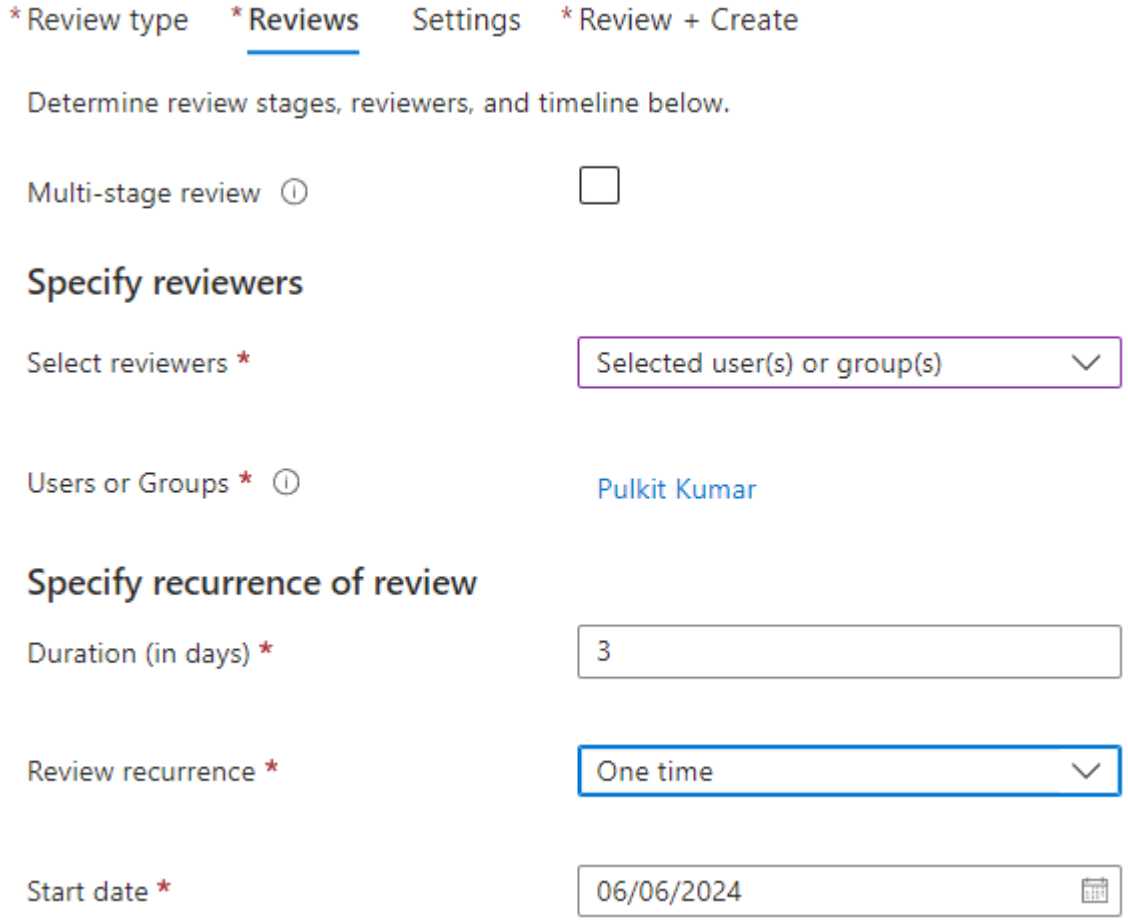
8. Now if you go to user in Microsoft Entra ID and then navigate to assigned roles you will see that the application administrator role has been assigned to this user as well because it a part of a group now.



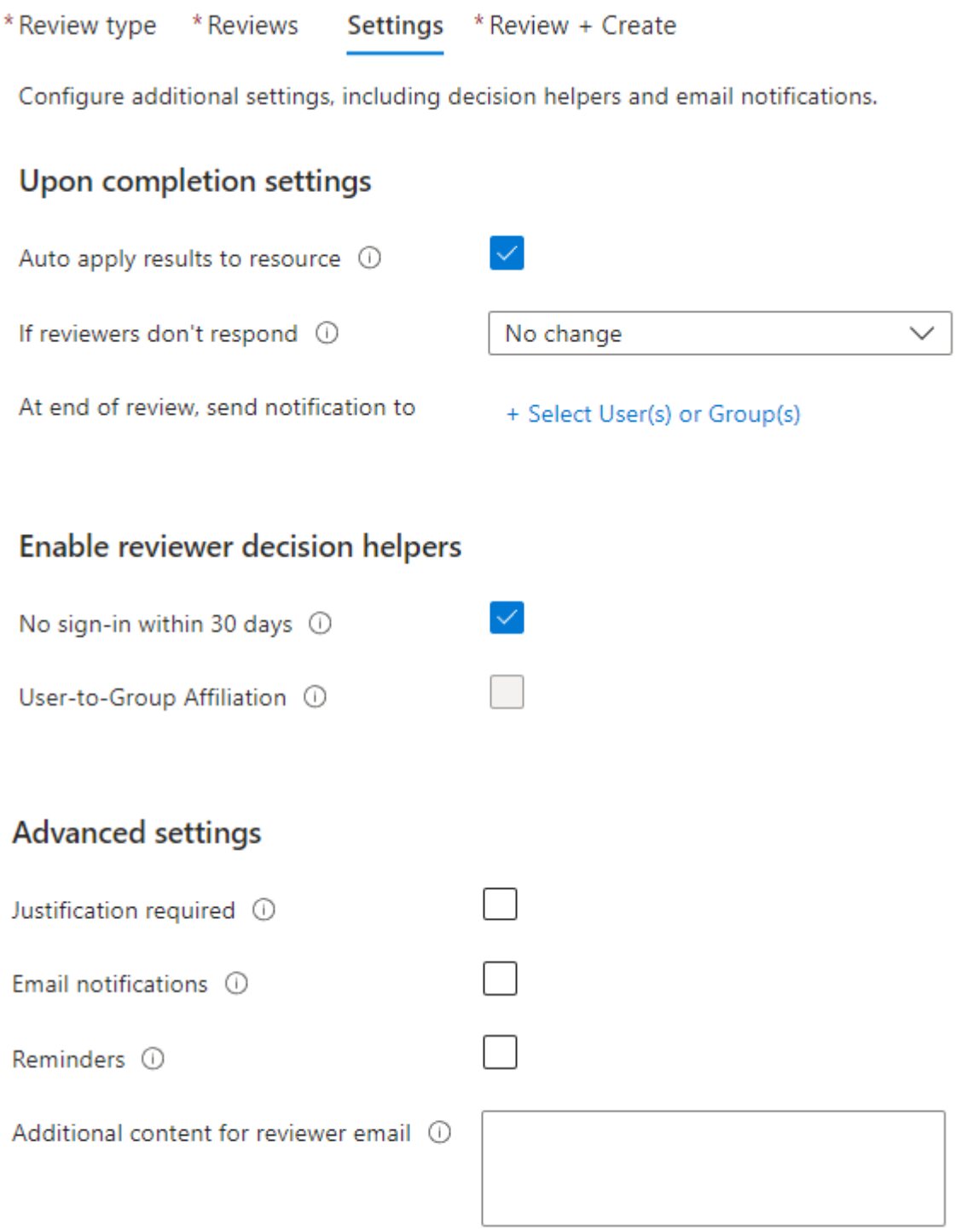
9. Now go back to identity governance and start creating your access review. So, you need to choose teams and groups, then choose Teams + Groups.
10. After that you need to choose your group and, in the scope, choose all users.



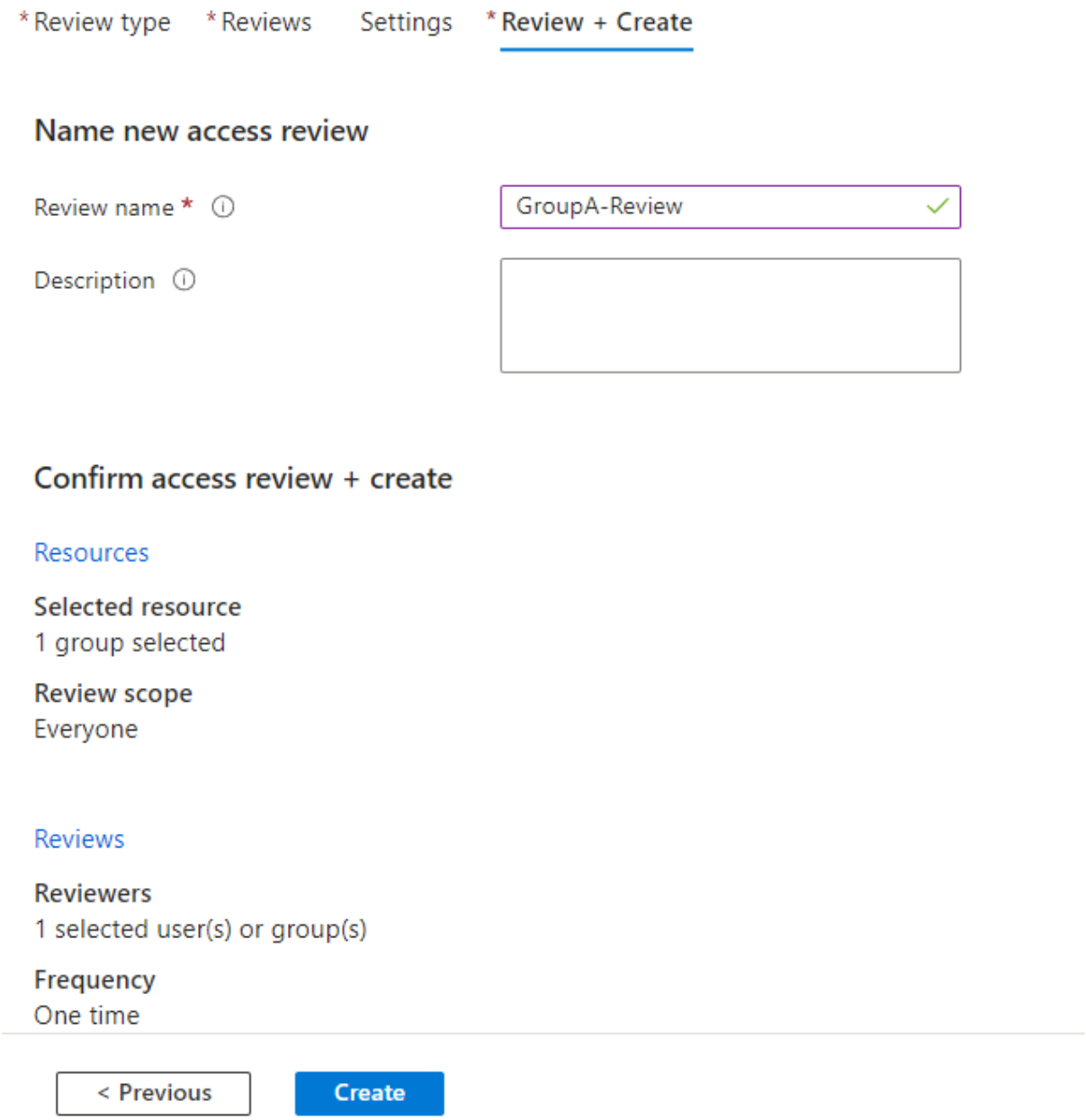
11. Then in the reviews you need to choose the Selected user and group then you need to choose yourself as a user who will review the things.
12. Then you need to choose review occurrence as one time.



13. Now for settings we need to check the box for auto-apply results to resource, and in the advanced settings, you need to turn off everything.



14. Then in the review and create page you need to give a review name and choose to create it.

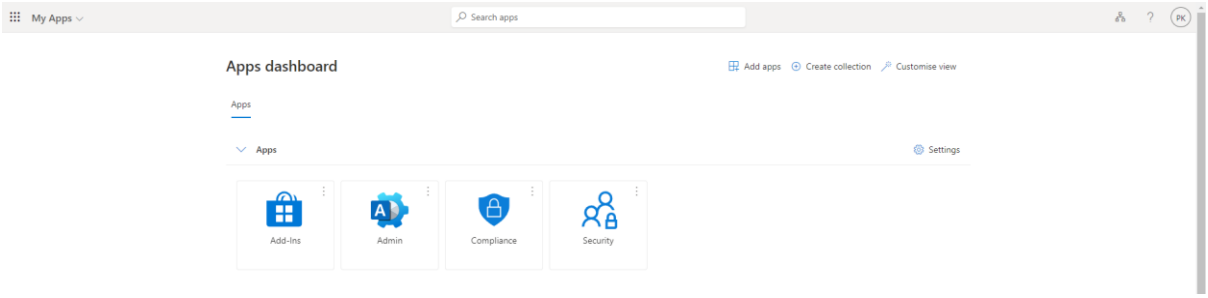


15. Below you can see that your review is created.

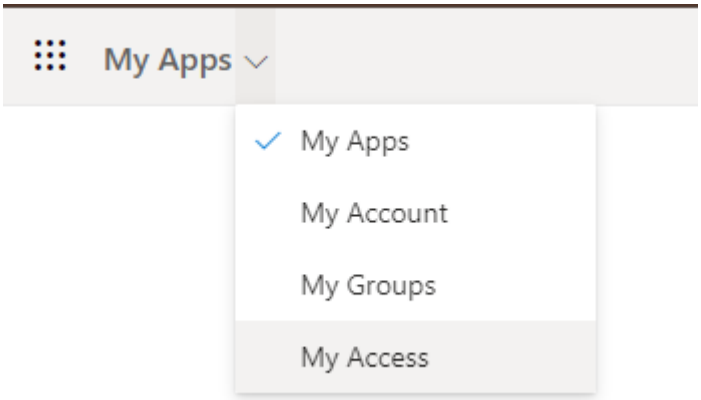
16. Now to review this group we need to go something known as an access panel. To visit the access panel, you can use the link below and sign in with your account.

    https://myapps.microsoft.com/

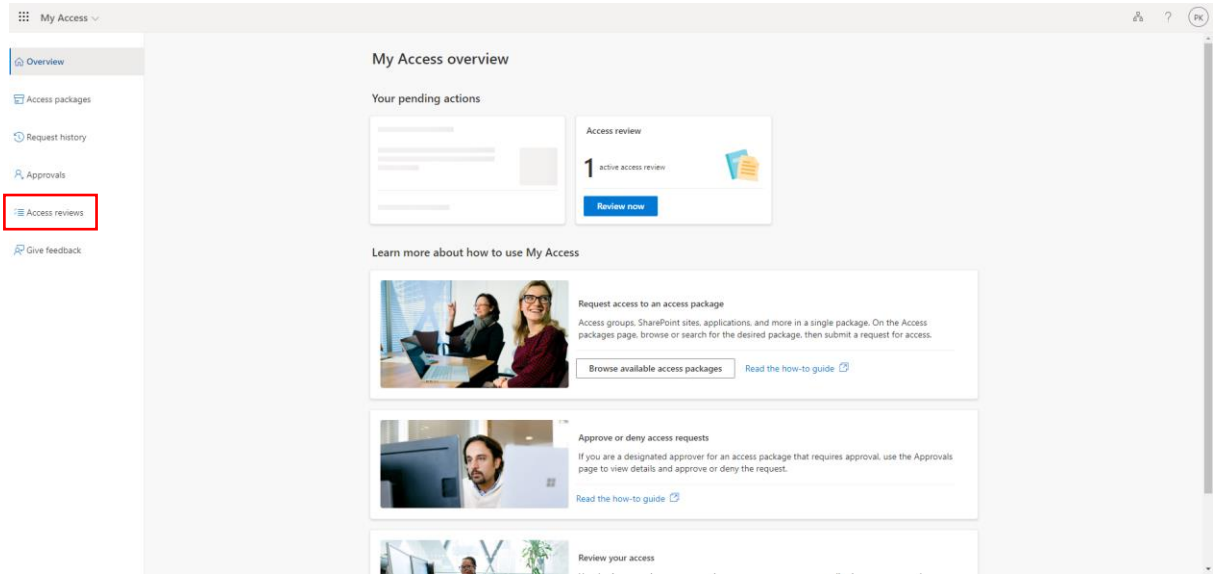
17. Below is the access panel.



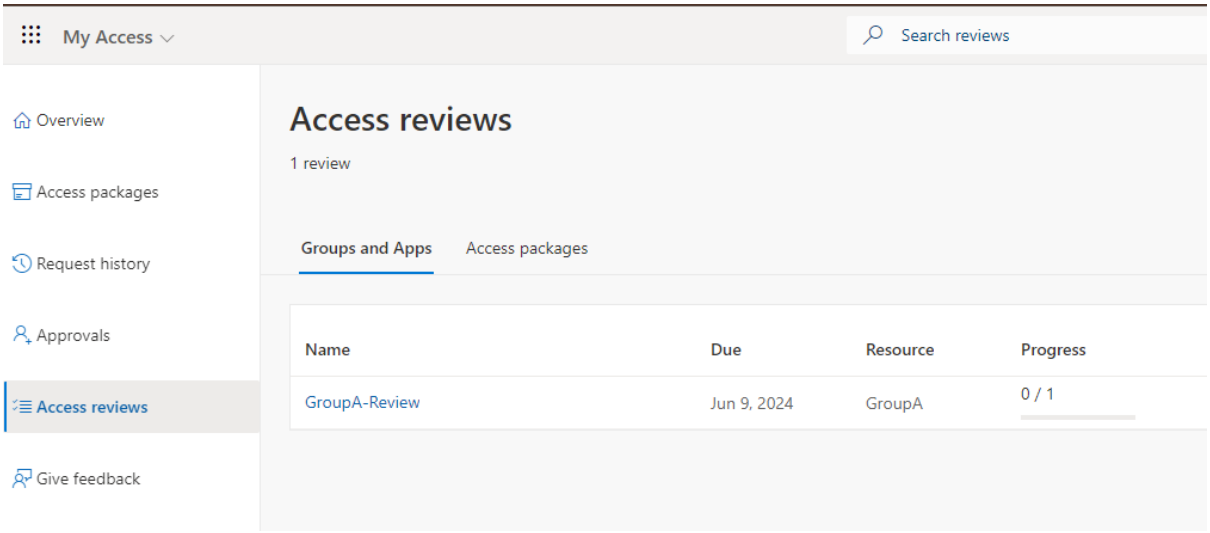
18. Now from the top right corner open the menu and choose My access.



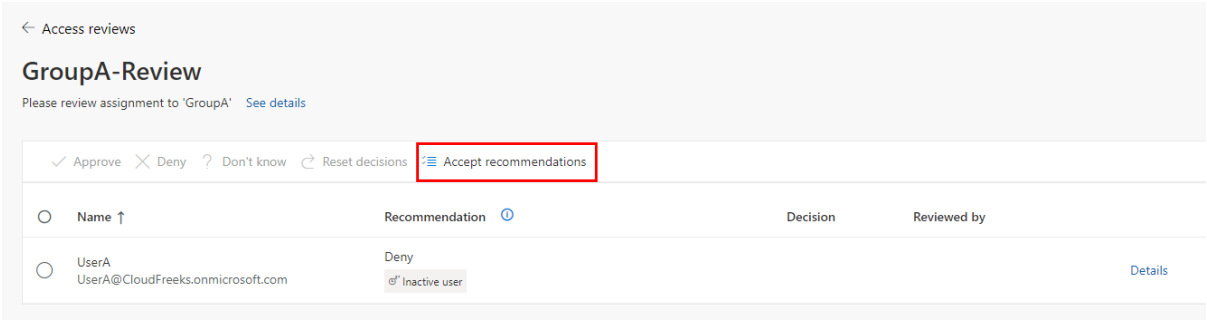
19. From the dashboard of My access go to Access reviews.



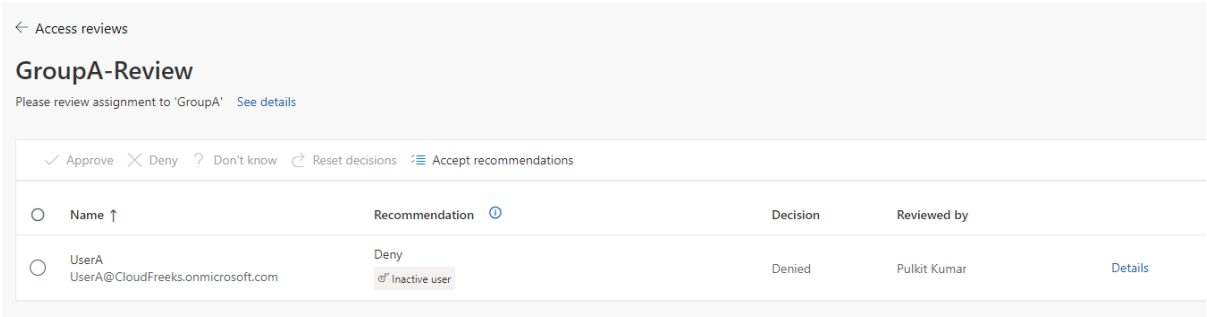
20. And here you can see your group A review.



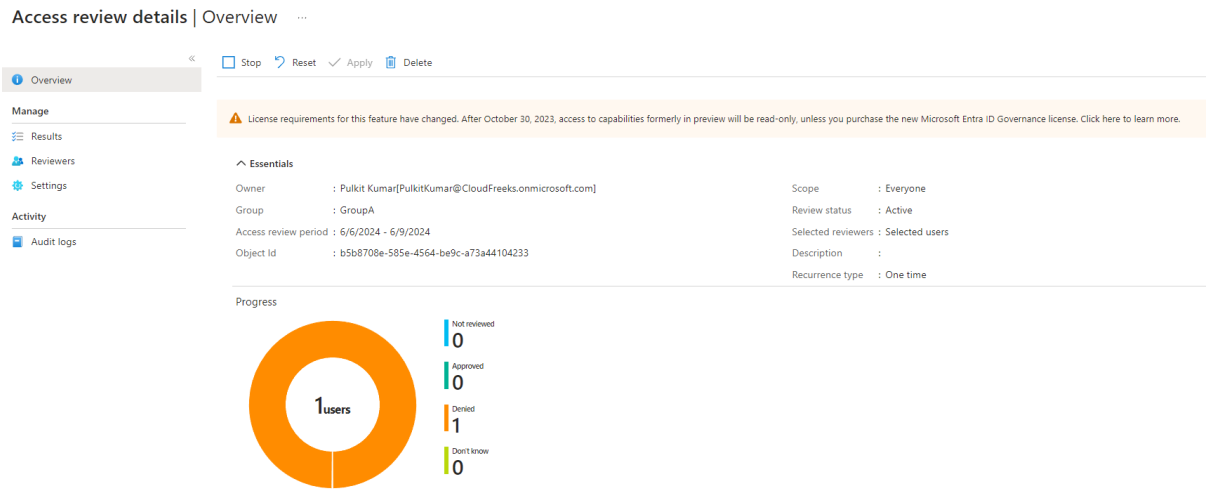
21. Now in the recommendation you can see that it is telling us that it is an inactive user. So, you have to accept the recommendations.



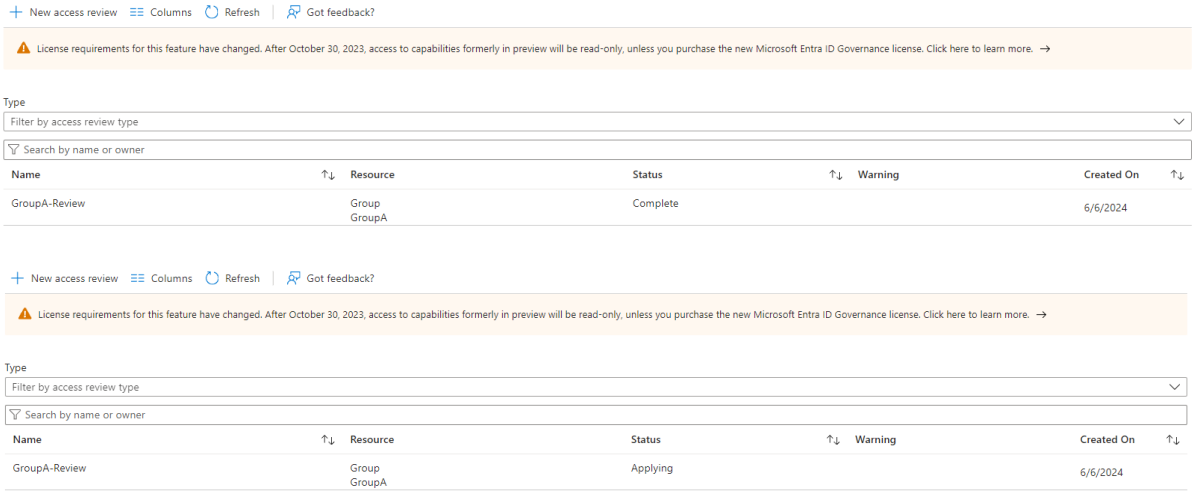
22. Then you will see that our decision was denied so, it is reflecting here and it is also telling us that it is reviewed by the Admin.



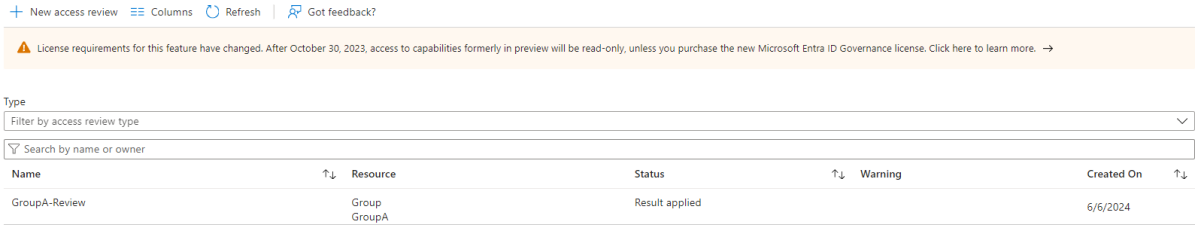
23. Now if you go back to Identity governance and go to access review and open it, then you will see that the review is working and we have denied one user as you can see in the snapshot.
24. Now just manually stop the review.



25. After stopping the review if you come outside, it and check for the status you will see the status says completed now. After sometime it changed to applying which means that it is applying the changes.



26. And after some more time you can see that the result has been applied.



27. After that if you go to Microsoft Entra ID and then go to Groups and check for your members, then you will see that the member was removed from your group based on the access review policy.
28. Also, a point to note is that if you don't have Premium licensing on your account then the effect won't take place.