**Azure AD PIM Explained**

**What is Azure Active Directory PIM ?**

Microsoft’s definition of Privileged Identity Managment is that it is a service in Azure Active Directory that enables you to manage, control, and monitor access to important resources in your organization

What it really is in plain english, it’s a service that ‘s similar to PAM where you strip all admin rights, and you have to elevate to use them. This elevation process could include any combination of logging, approved/not approved by peers owners, mfa etc.

**How does it work?**

In a nutshell short high level answer would be PIM Groups are assigned RBAC Roles and are give permission to different Azure resources. In the group configuration properties you can configure length of elevation time, mfa, etc that you want to configure for security purposes. Admins gets added to these groups for elevation. Once elevated they are granted the RBAC role permissions to the Azure Resource.

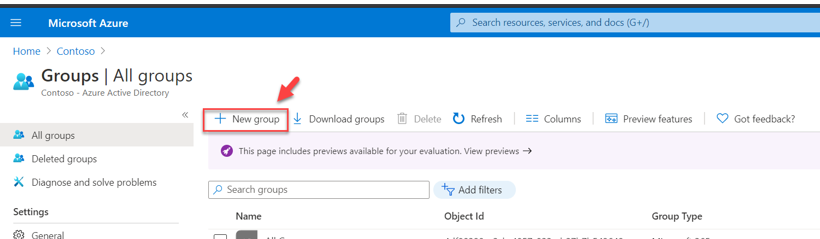
**How to configure a PIM Group? See below for steps**

Create A Role-Assignable Group aka Cloud Group, this group must have the “Azure AD roles can be assigned to the group” option turned on

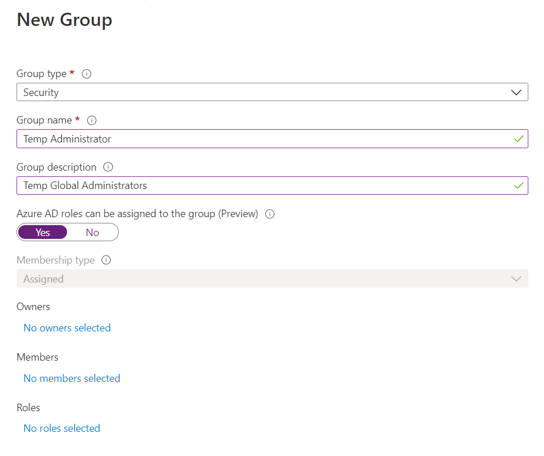
1. Log in to Azure Portal as Global Administrator

2. Search for Azure Active Directory and click on it

3. Go to Groups and click on + New group



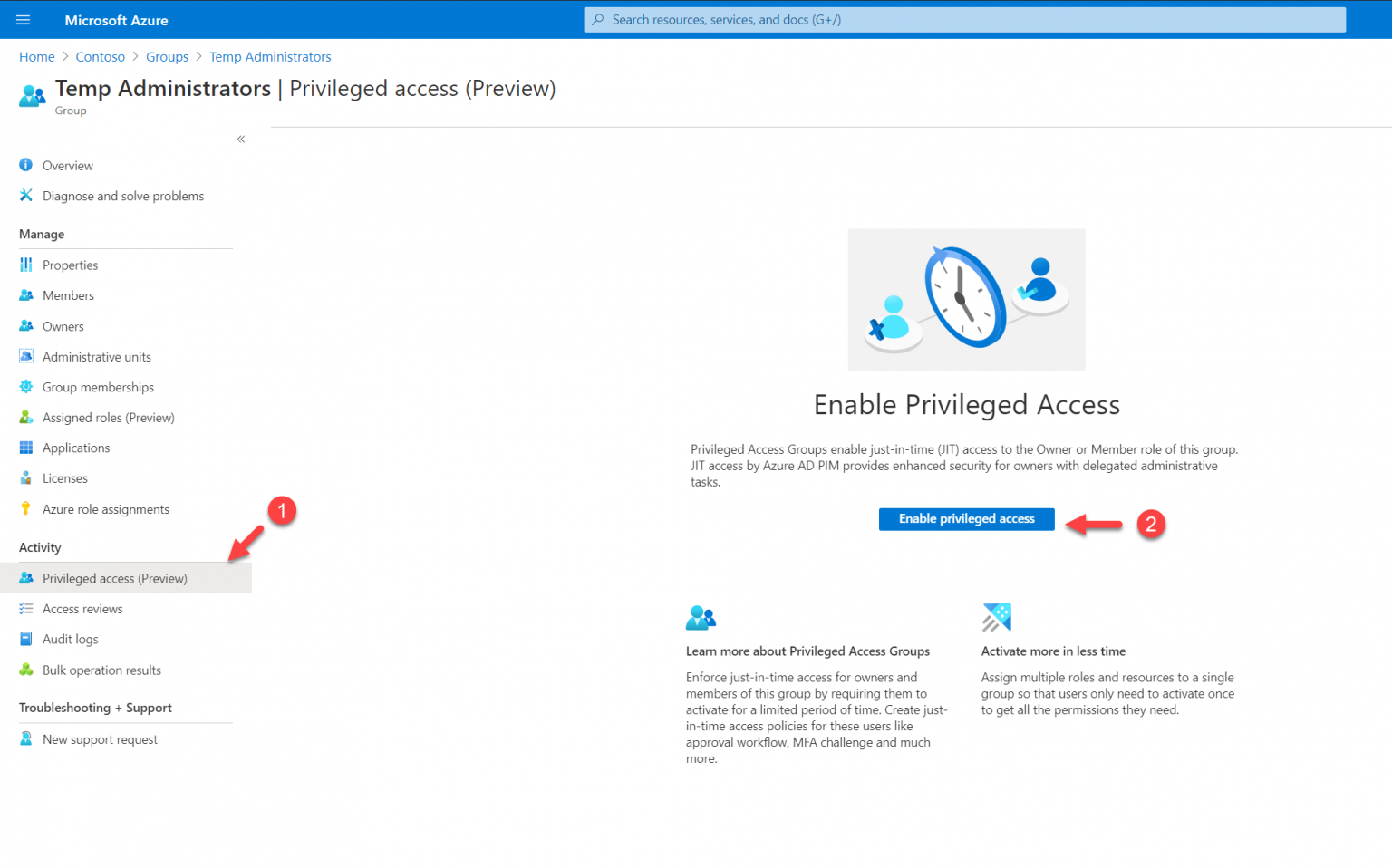
4. In the new window, set Group type to Security, provide a name and description for the group, set Azure AD roles can be assigned to the group option to Yes. After, click ok create to complete the group setup process



Enable Privileged Access For A Group - the next step of the configuration is to enable privileged access for the newly created group.

1. Go to Azure Active Directory home page

2. Then go to Groups and click on the group we created in the previous section. On the group properties page, click on Privileged access (preview). Next, click on Enable privileged access button.

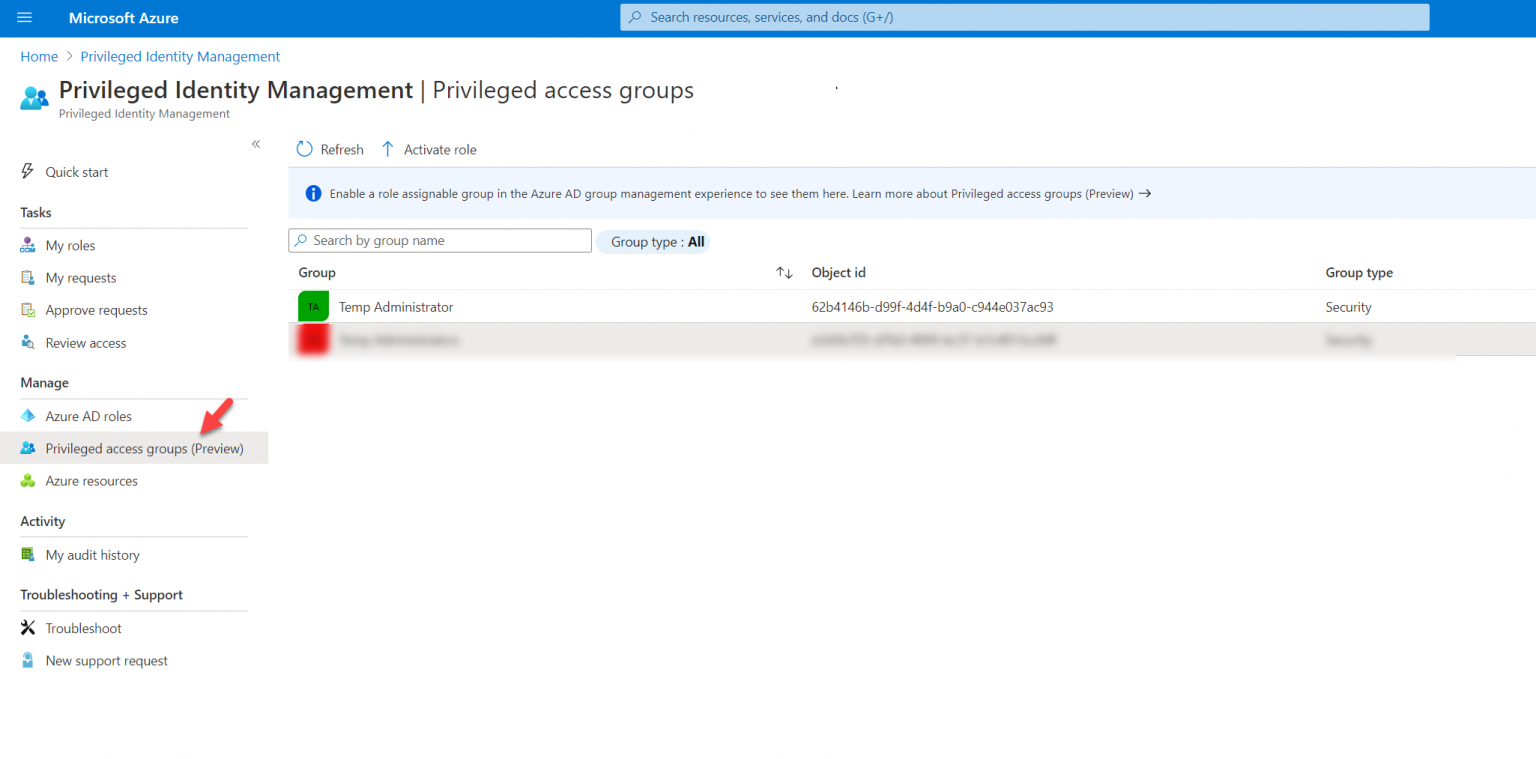


Configure Role Settings - configure the role settings of the group

1. Log in to Azure Portal

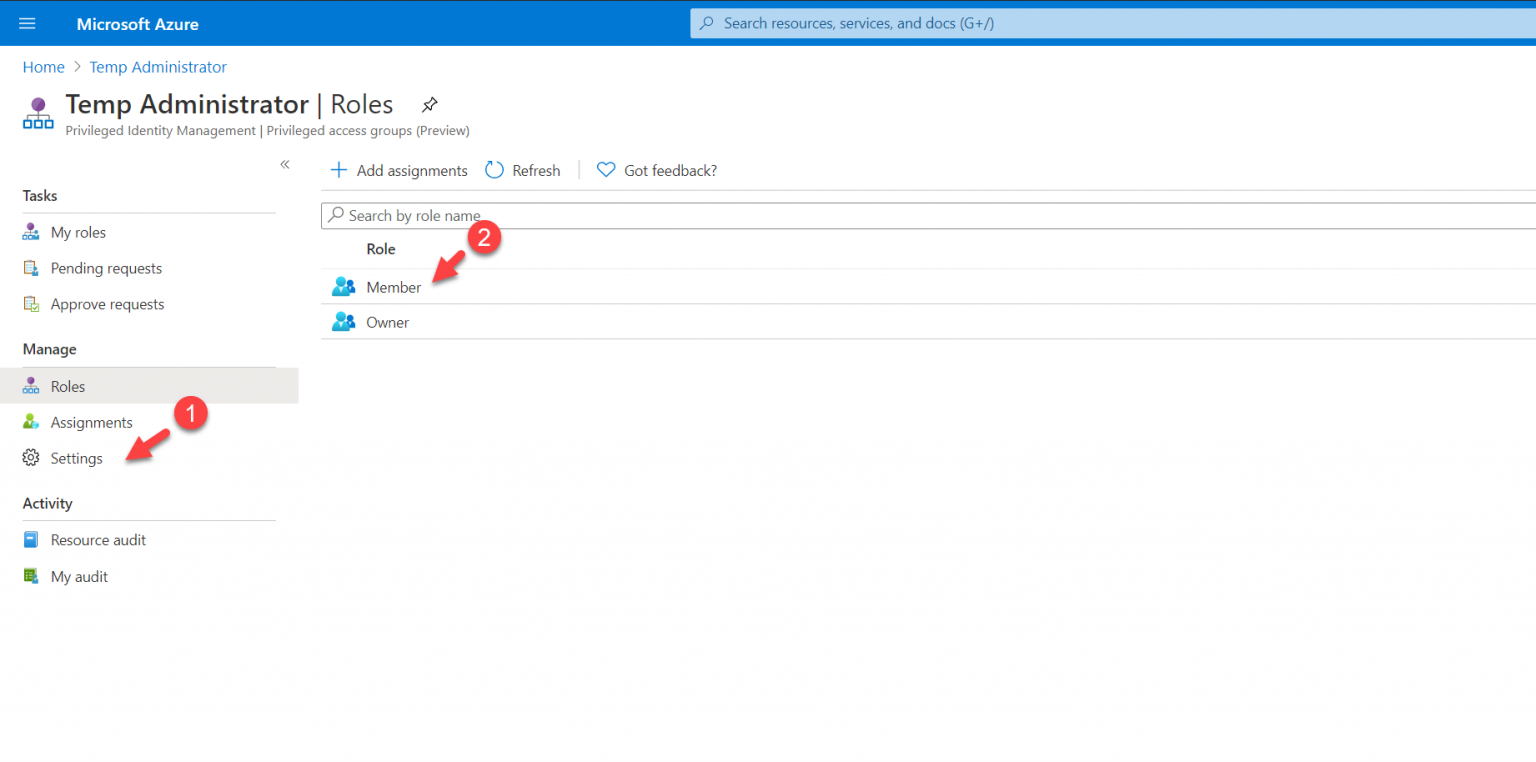
2. Search for Azure AD Privileged Identity Management and click on it

3. Then click on Privileged access groups

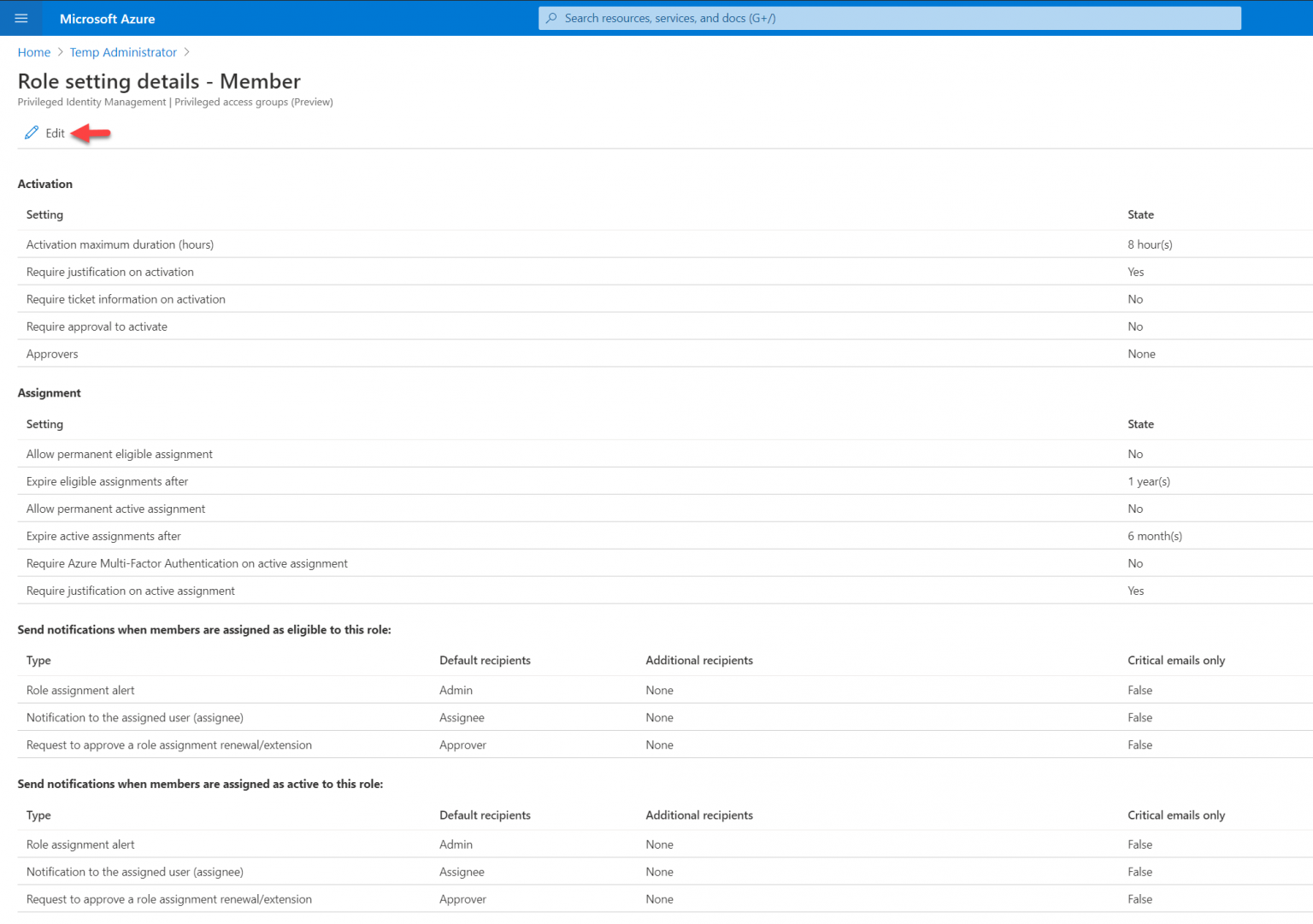


4. In there, we should be able to see the group we just created. Click on it.

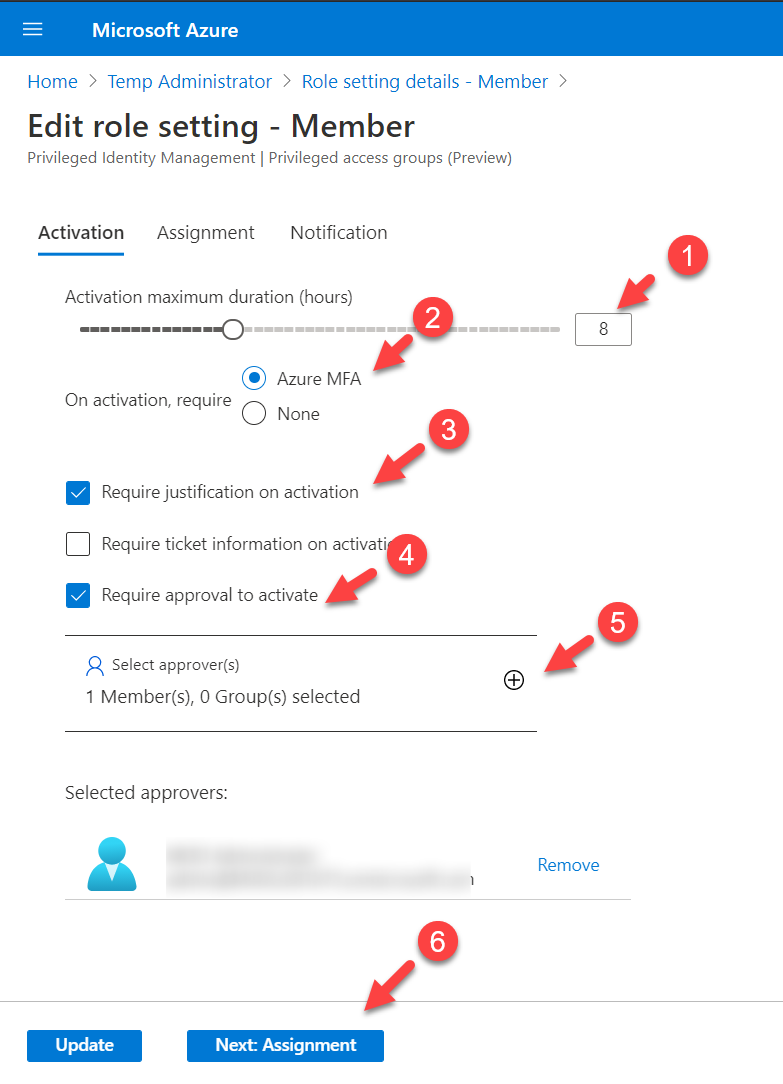
5. Then in the properties page, click on Settings | Member



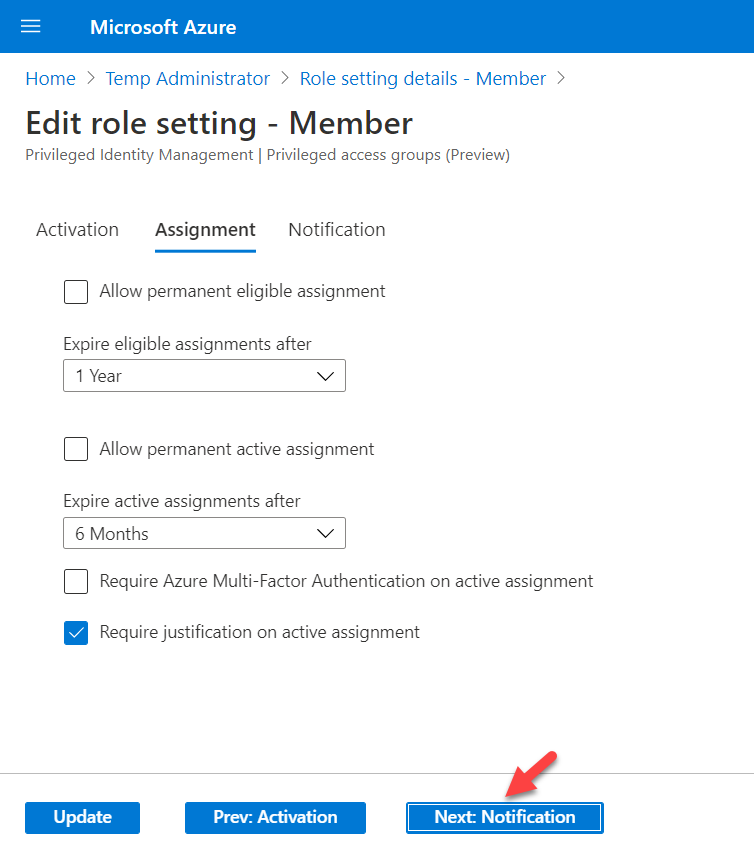
6. Next, click on Edit



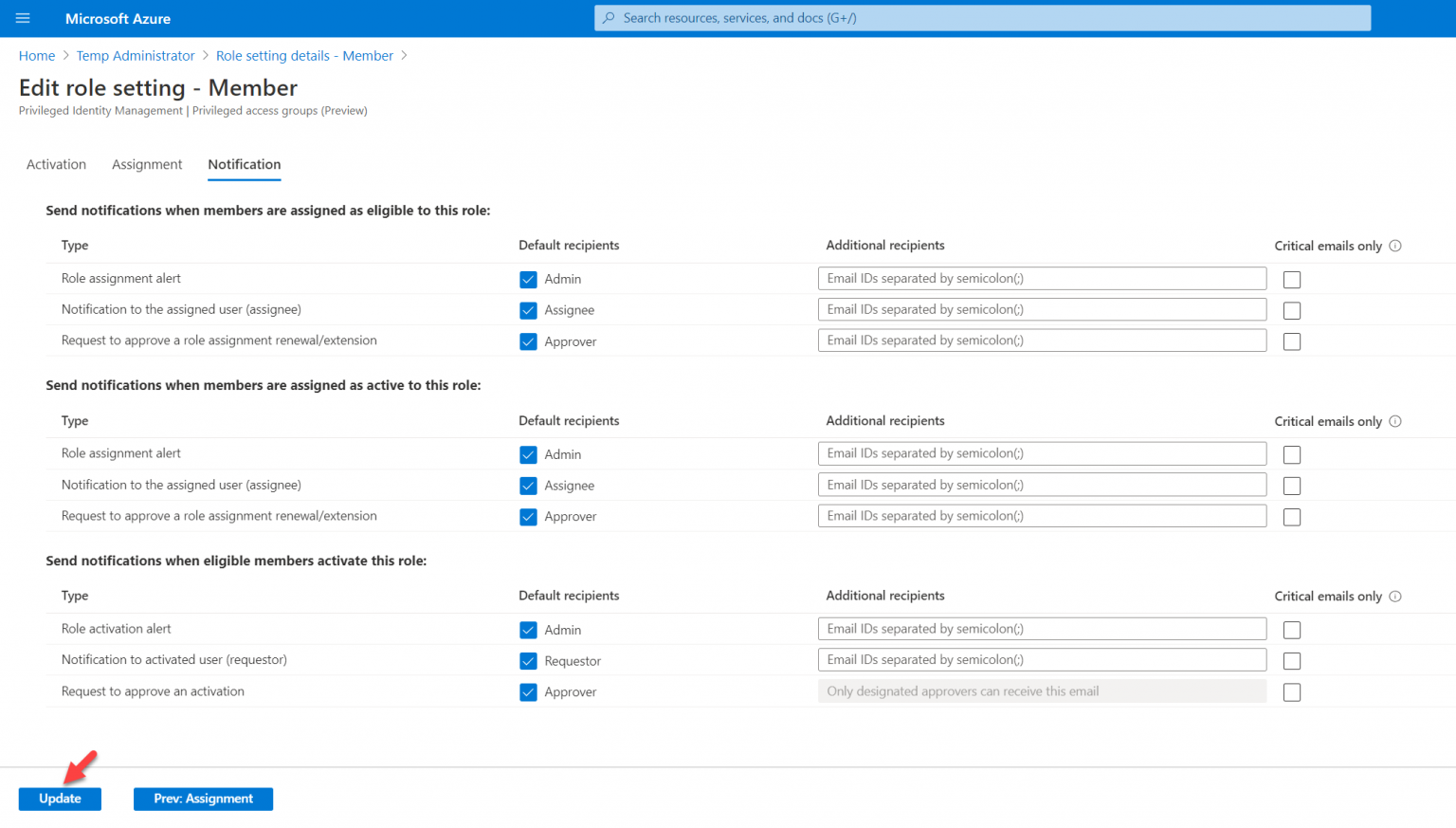
7. In there we can start changing settings for the role as per requirements. In this demo, I am going to keep Activation maximum duration (hours) to 8. On activation, I also want to verify Azure MFA. I also like the user to justify the request. Also, the request must be approved by an approver. Once the above settings are in place, I click on the select approvers option and define an approver. At the end, I click on Next: Assignment



8. In the Assignment page, I will keep default settings and click on Next: Notifications



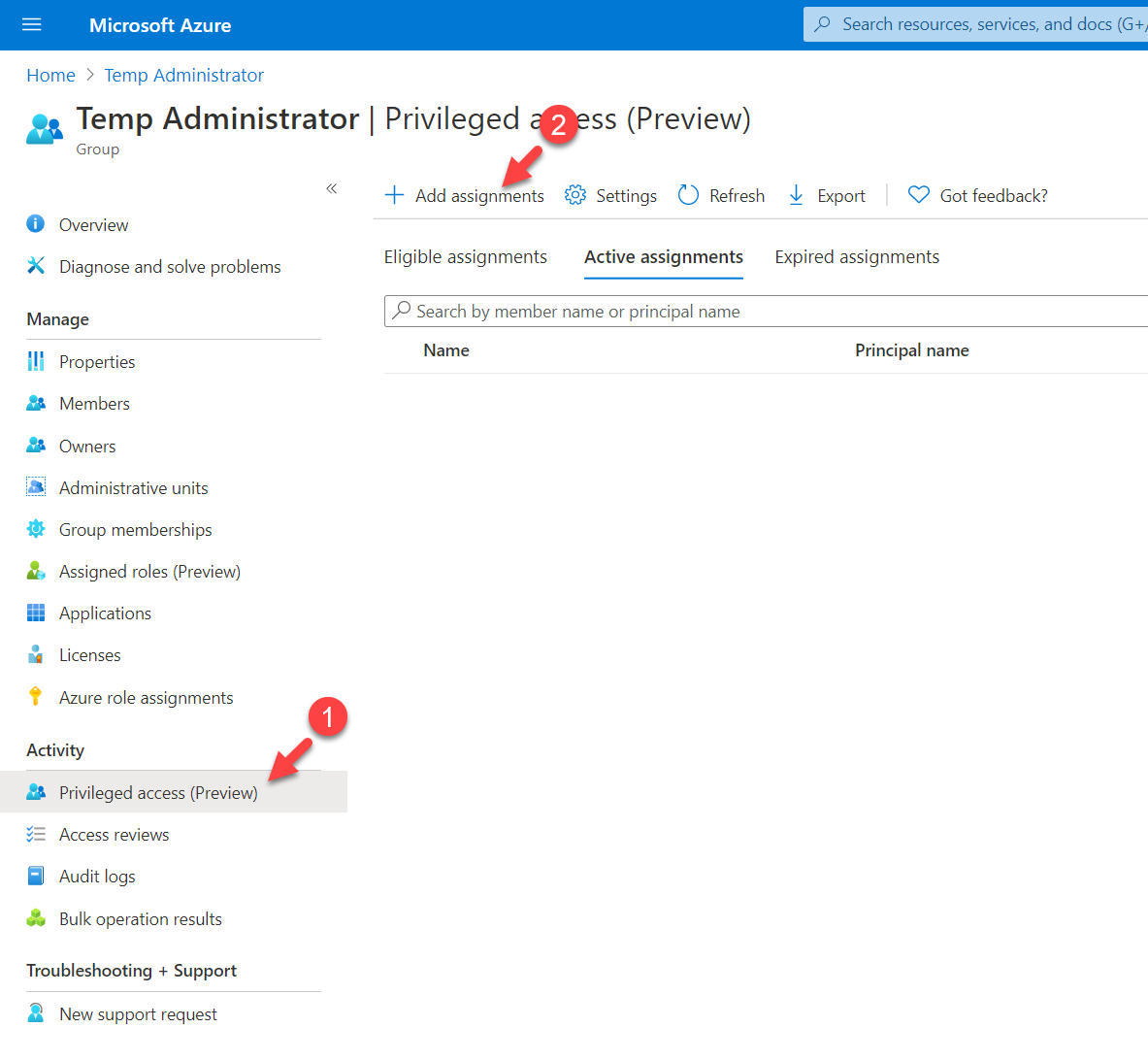
9. In the notification page, we can define who will be notified of different actions. For this demo, I am going to keep the default settings and click on Update to apply the changes.



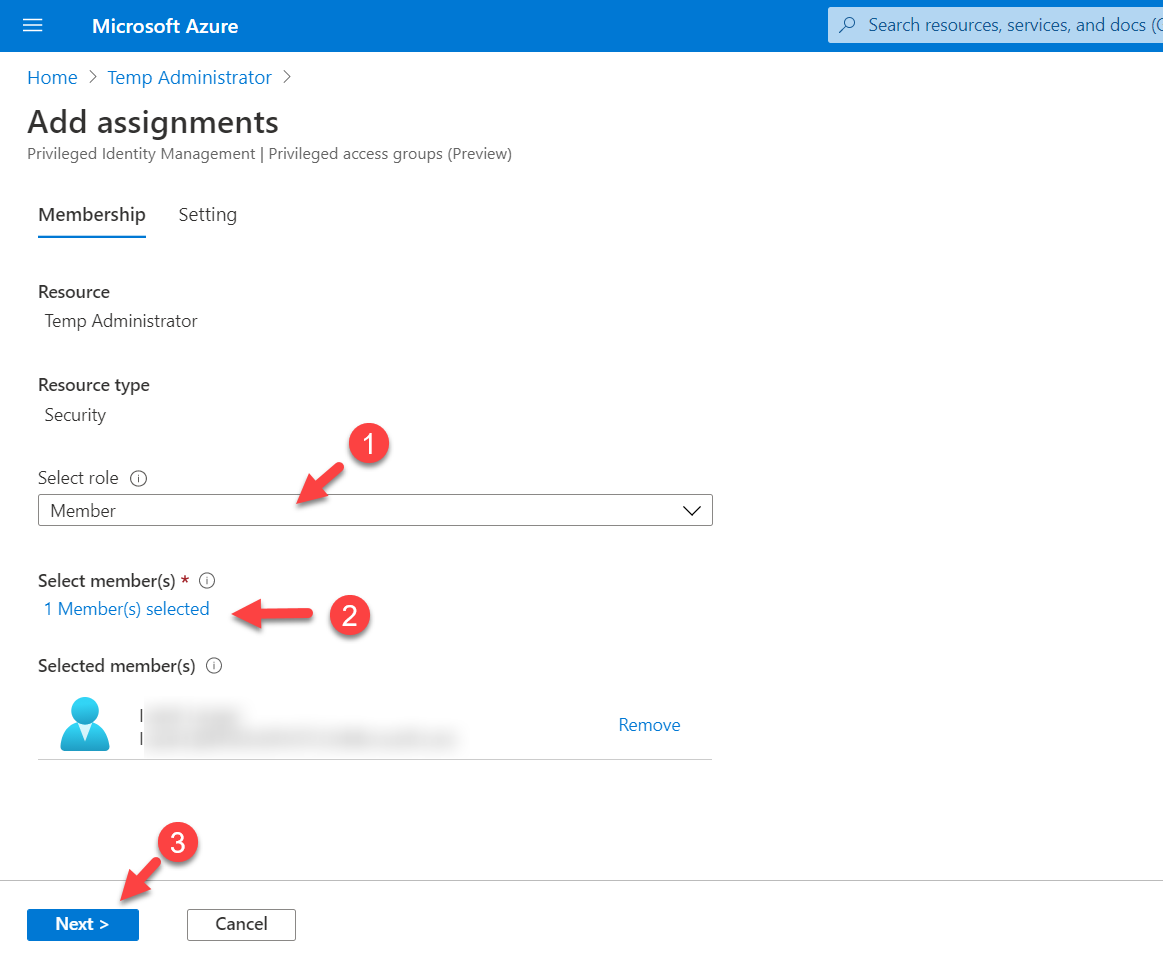
Make User Eligible For The Membership - we need to decide who is going to be eligible for the group membership.

1. Go to the Azure AD group we previously created

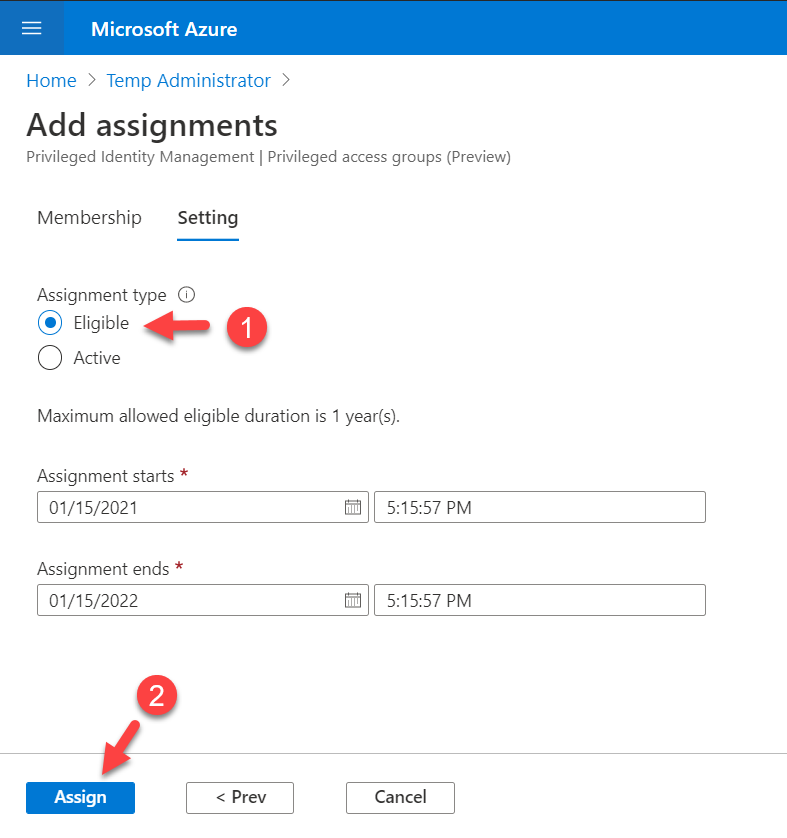
2. Click on Privileged access (preview) | + Add assignments



3. On the next page select Member under the Select role option. Then click on the No member selected link under Select member(s) and select the eligible user(s). Once settings are in place click on Next.



4. Then make the user eligible and click on Assign.

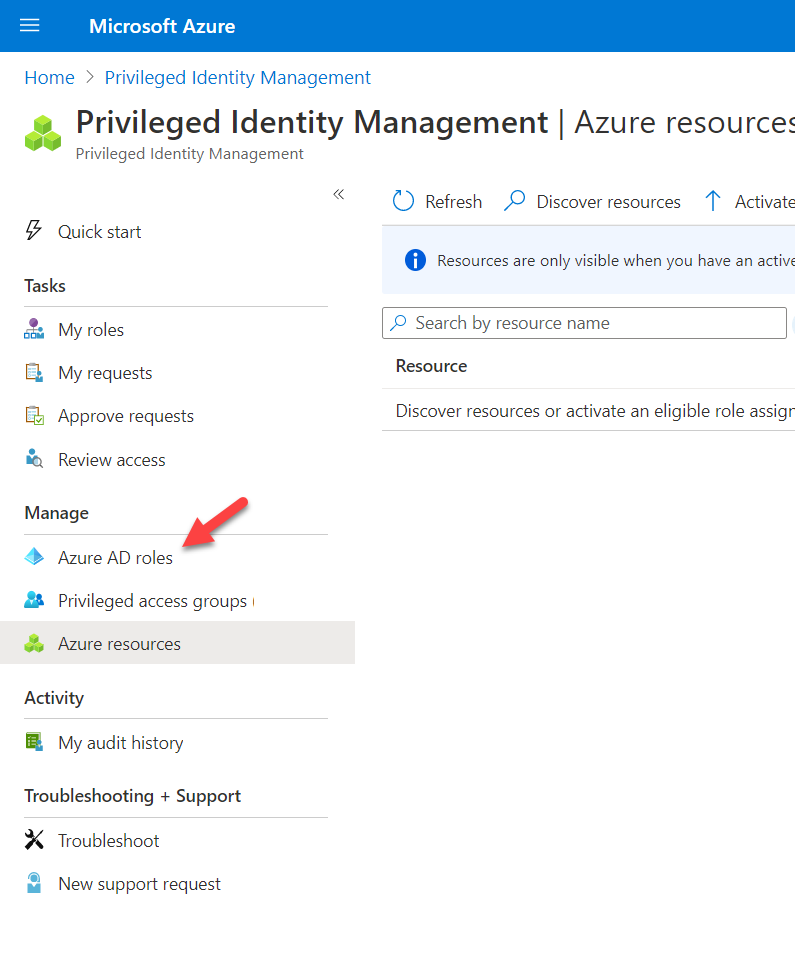


Assign Global Administrator Role To The Privileged Group - The final step of the configuration is to assign Global Administrator role to the group we created by using Azure AD PIM.

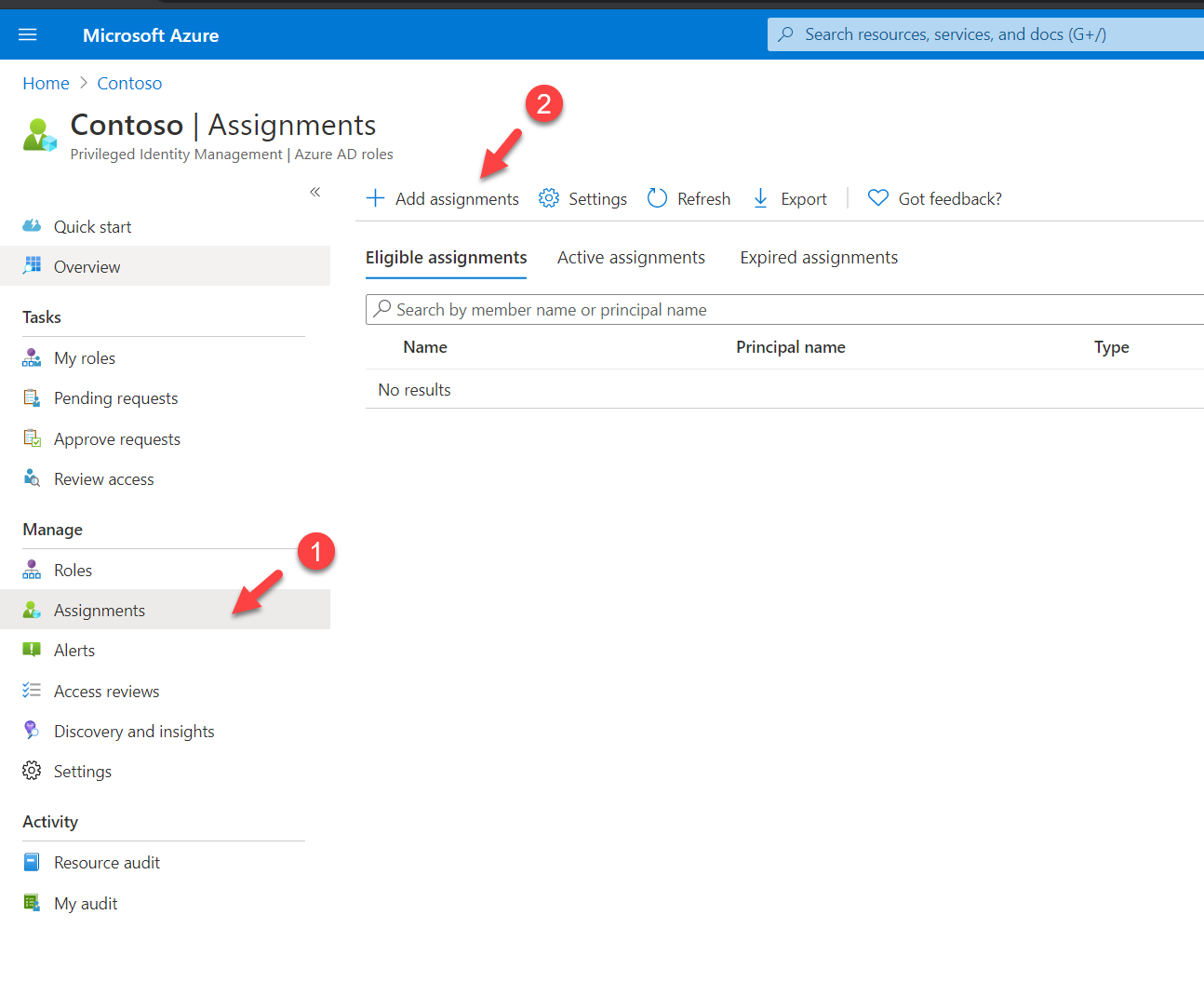
1. Log in to Azure Portal

2. Search for Azure AD Privileged Identity Management and click on it

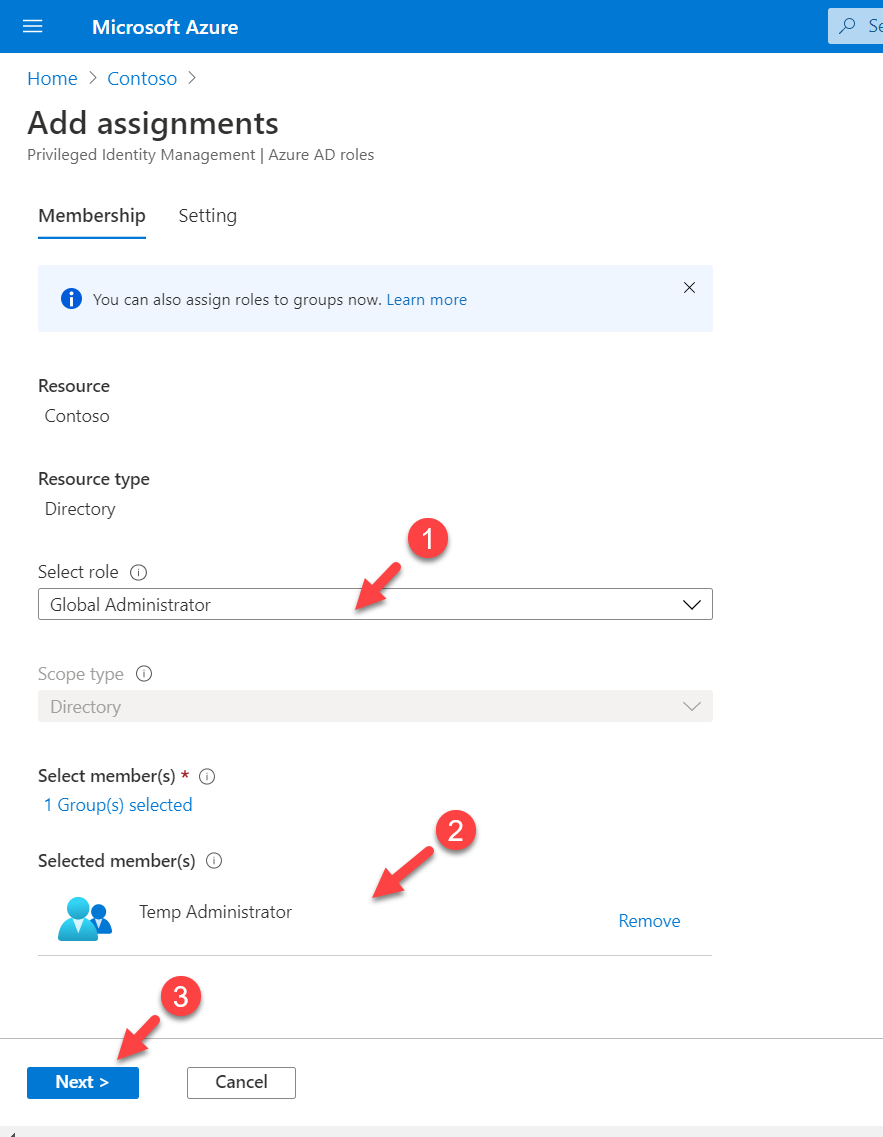
3. Then click on Azure AD roles



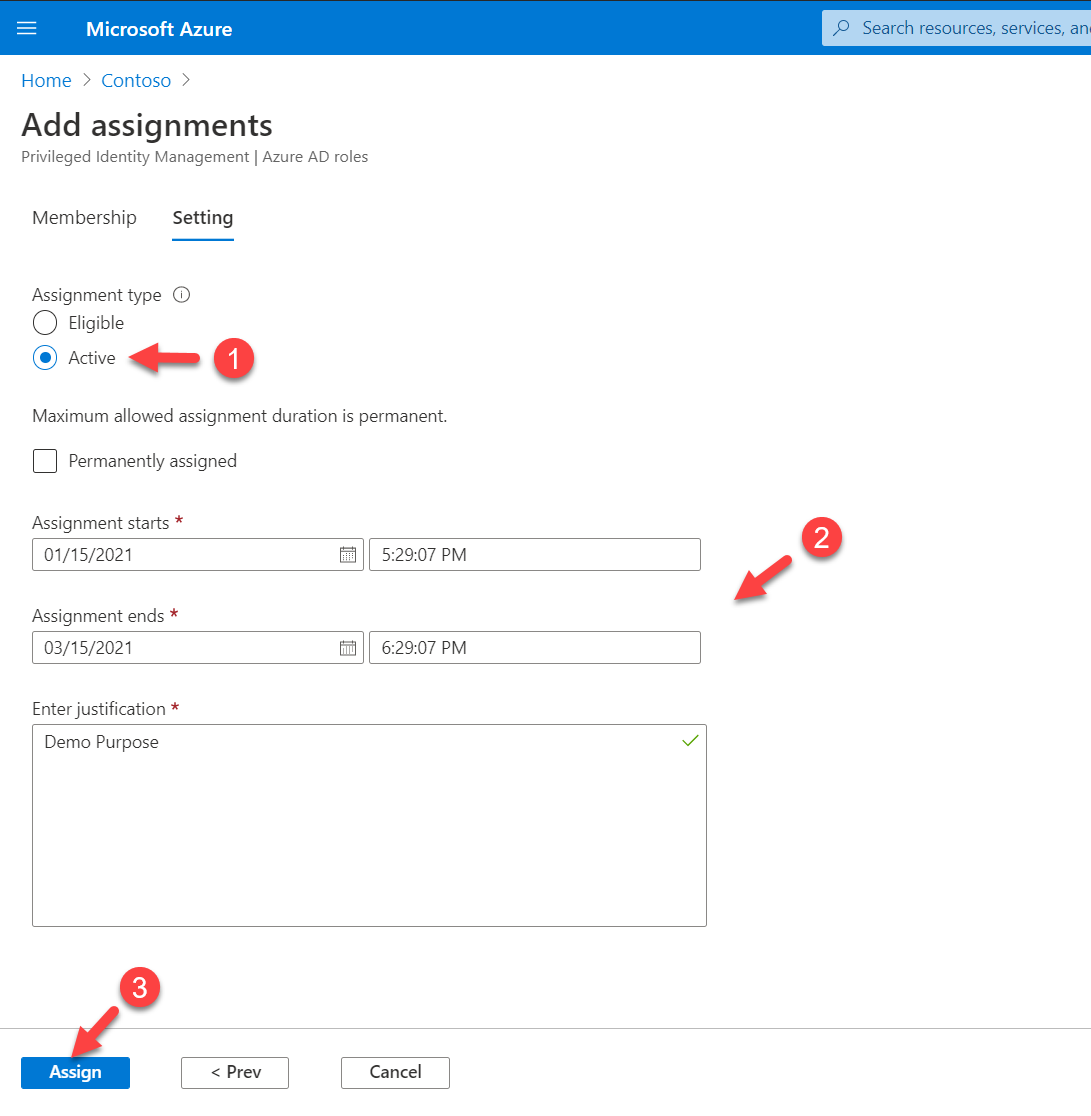
4. In the next page click on Assignments | + Add assignment

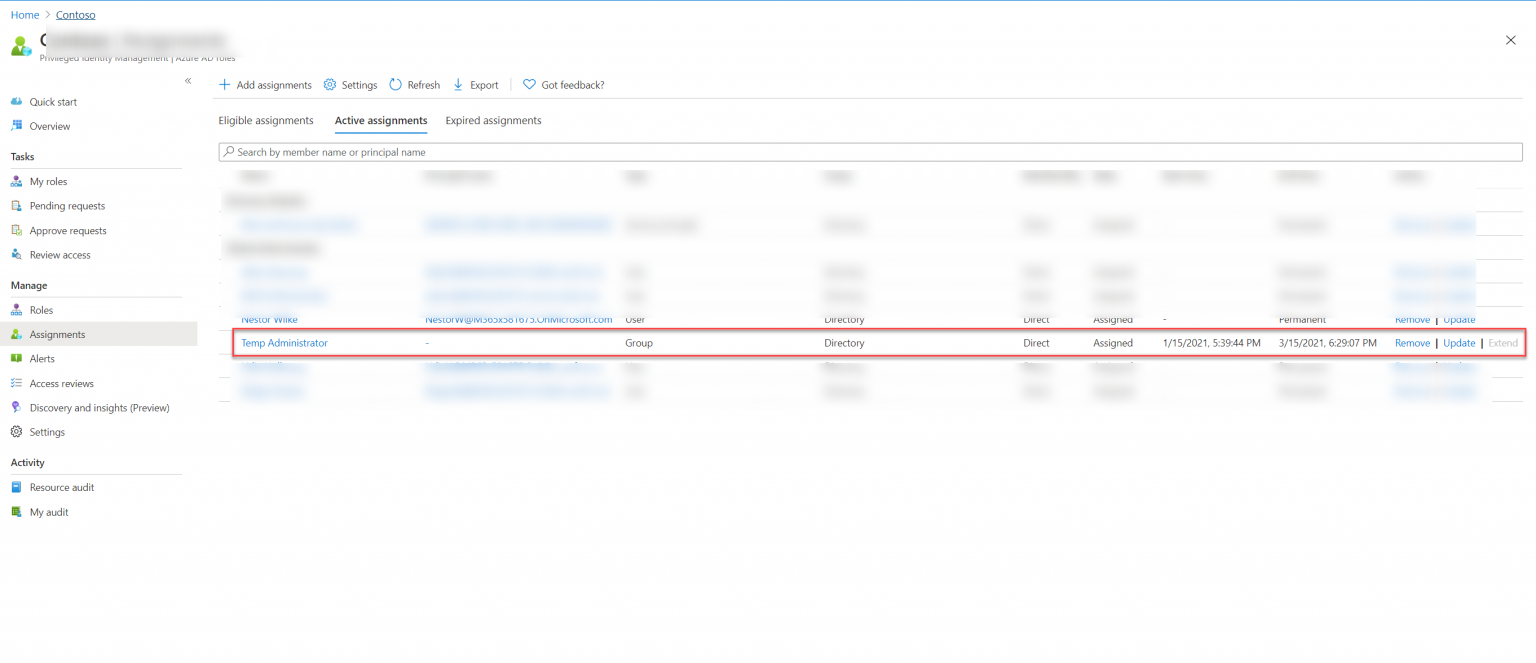


5. Then, select Global Administrators under the Select role. Then assign “Temp Administrators” group to the members and click on Next.

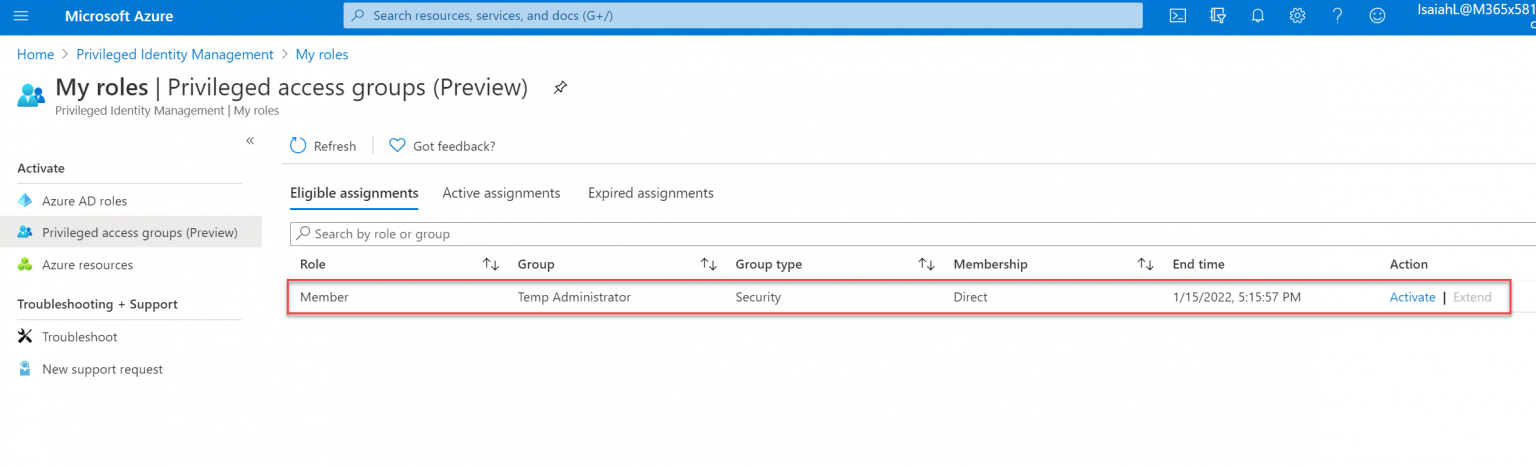


6. On the next page, select Active under assignment type. Then select the assignment start date and assignment end date. In this demo, I am setting it up for 3 months. Once settings are in place click on assign to complete the configuration process.

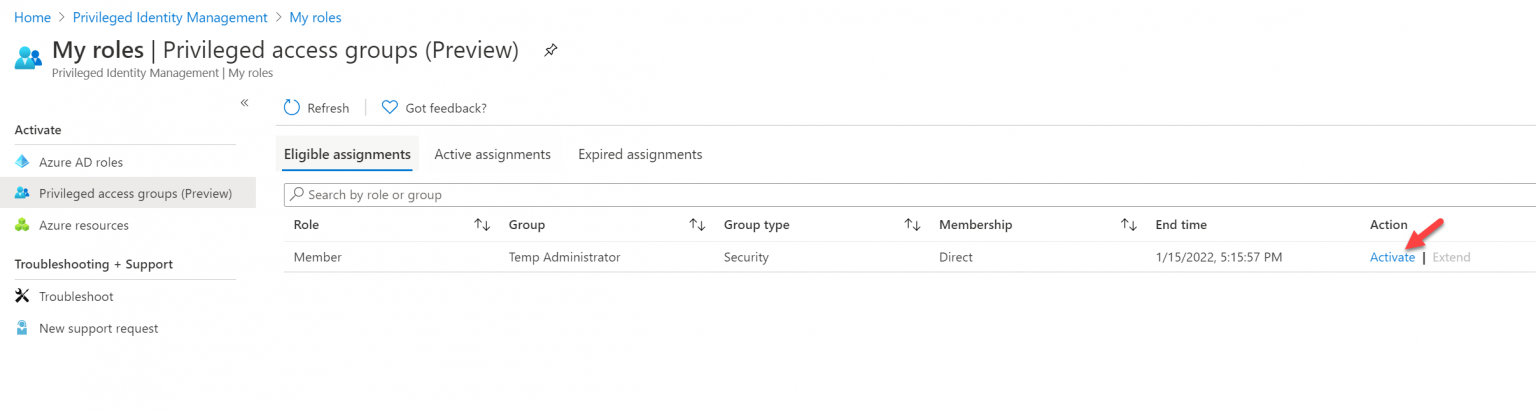




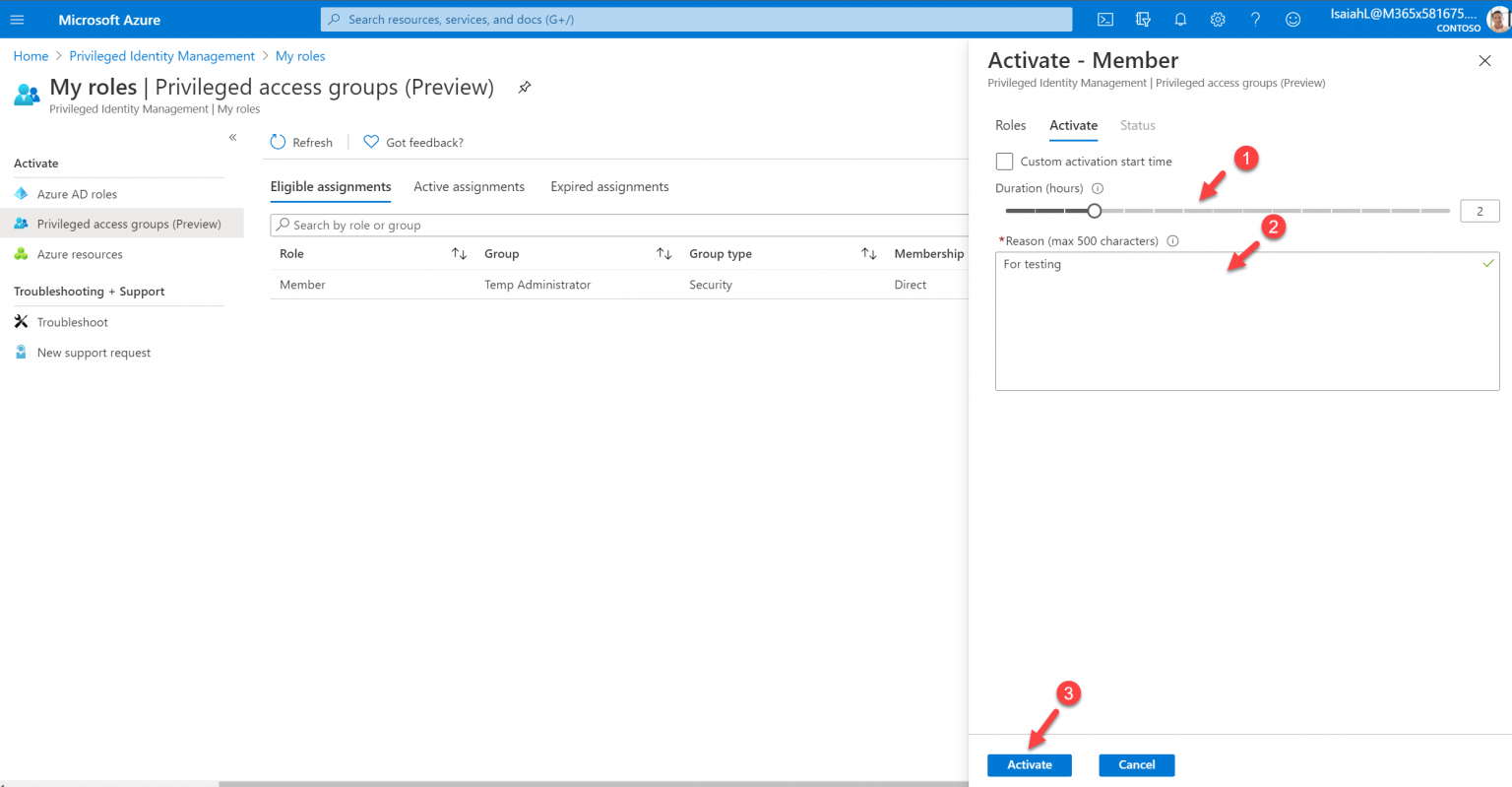
Testing - To test the configuration, I log in to the Azure portal as privileged user. Then I went to Azure AD Privileged Identity Management | My roles | Privileged access groups. In there we can see the eligible group membership.



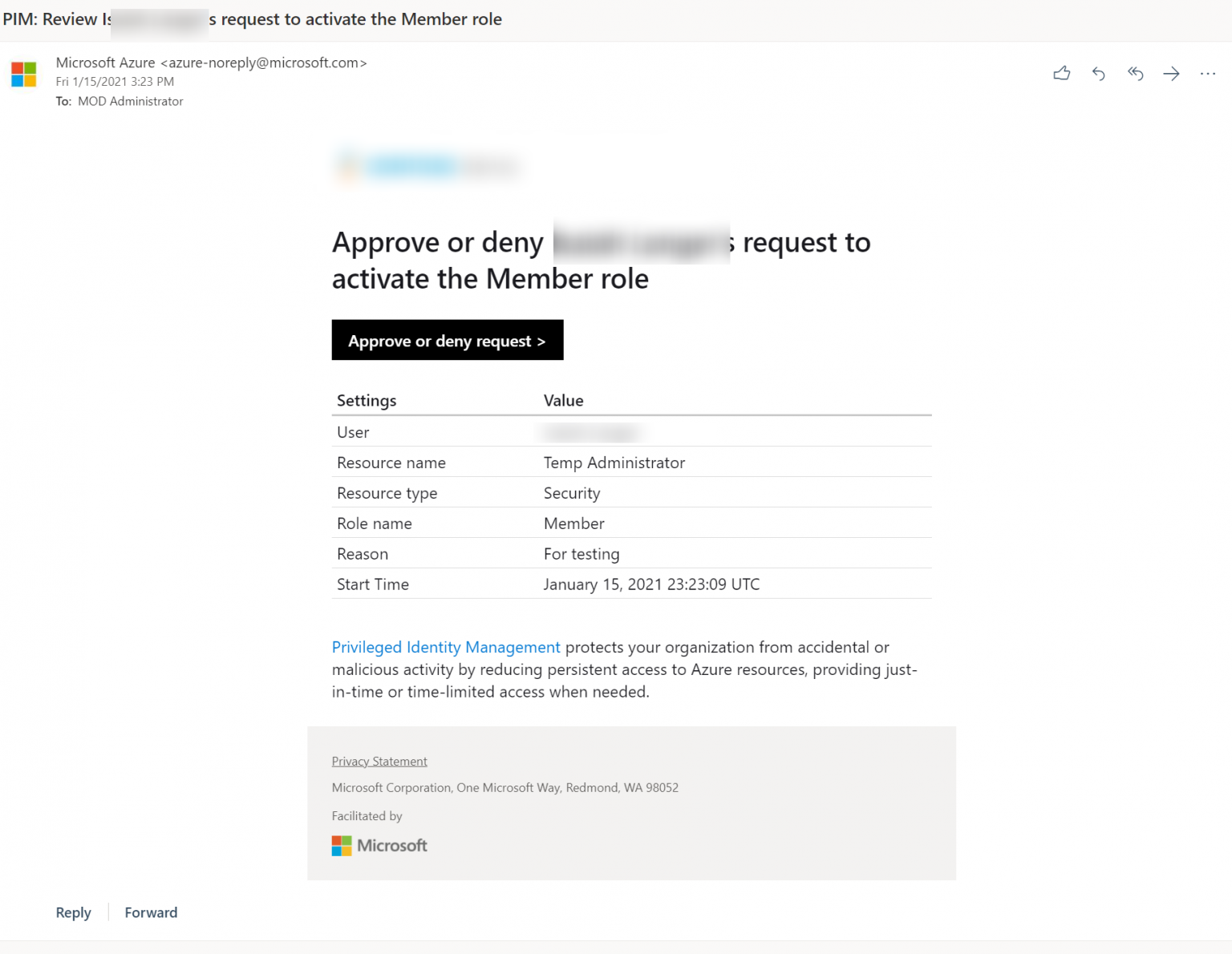
1. To proceed further with testing, click on Activate.



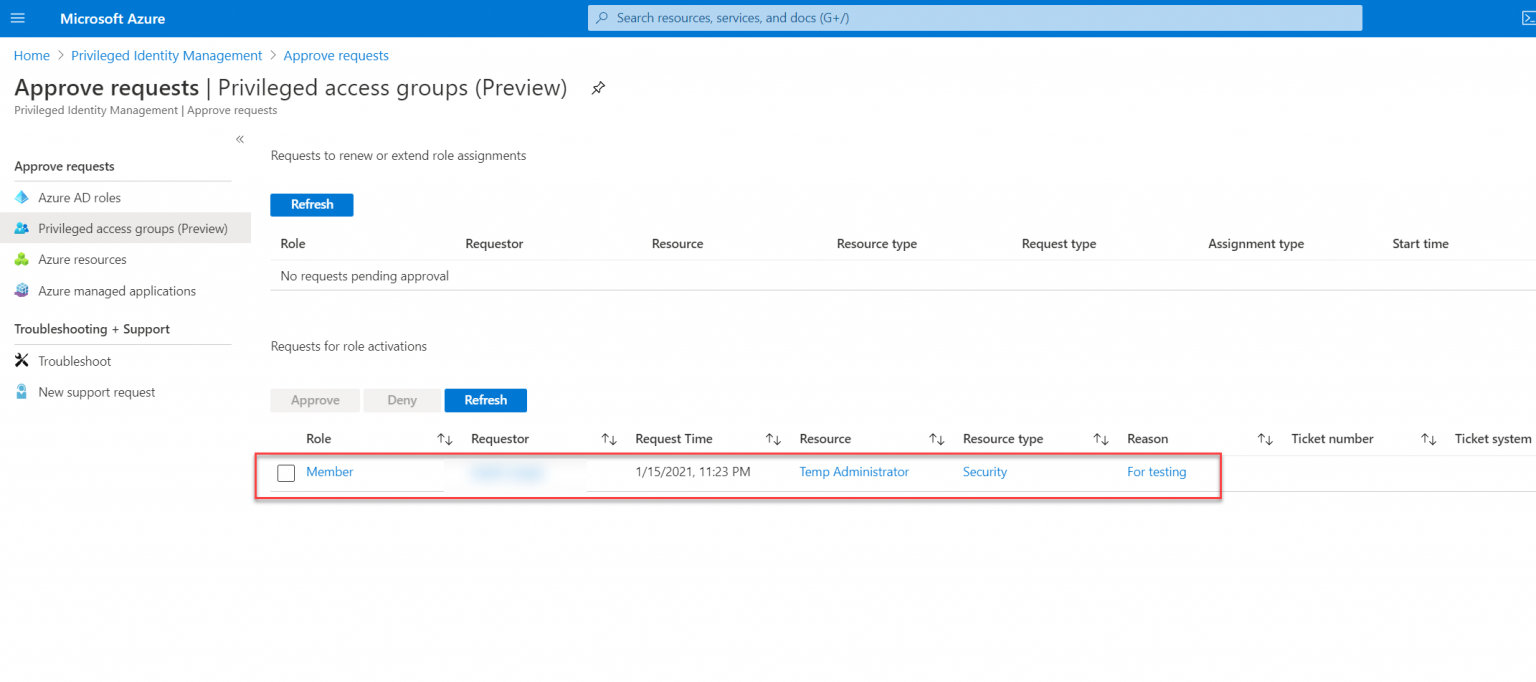
2. Then in the new window, I am requesting to activate membership for 2 hours. I also provide a reason as it is mandatory.



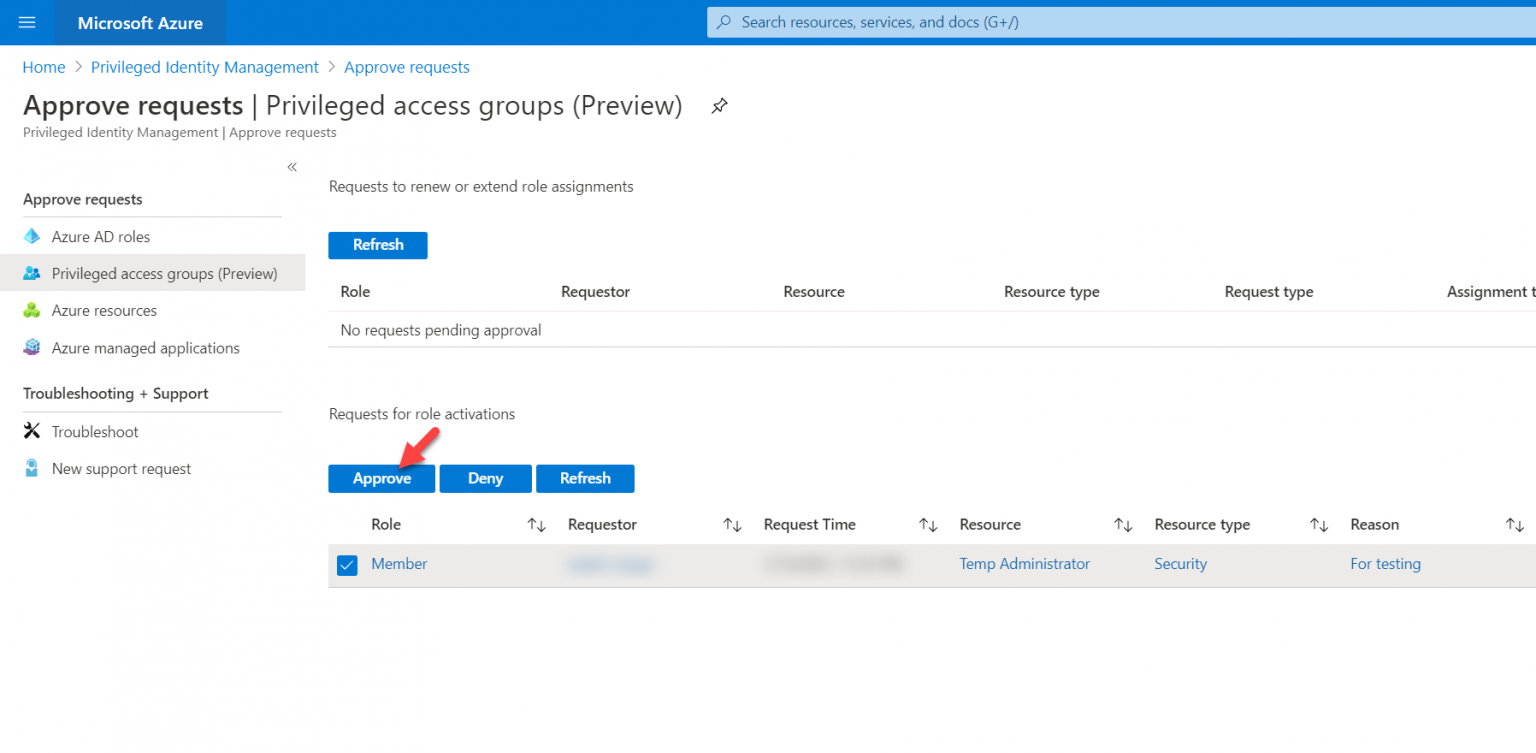
3. After I click on Activate, the approver received an email notification regarding the request.

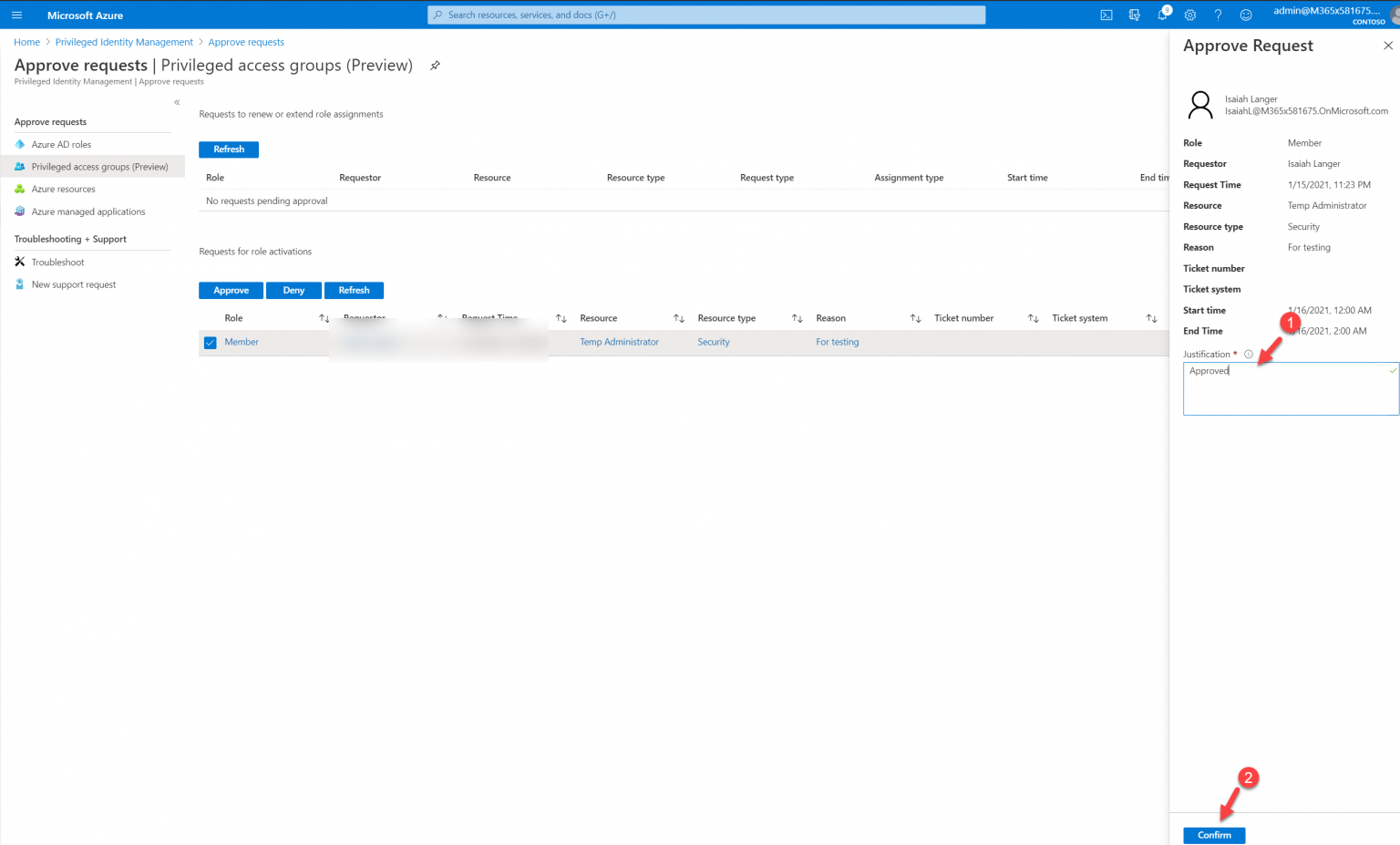


4. Then I log in to the Azure portal as approver and went to Azure AD Privileged Identity Management| Approve requests | Privileged access groups. As expected, I can see the request from privileged user.

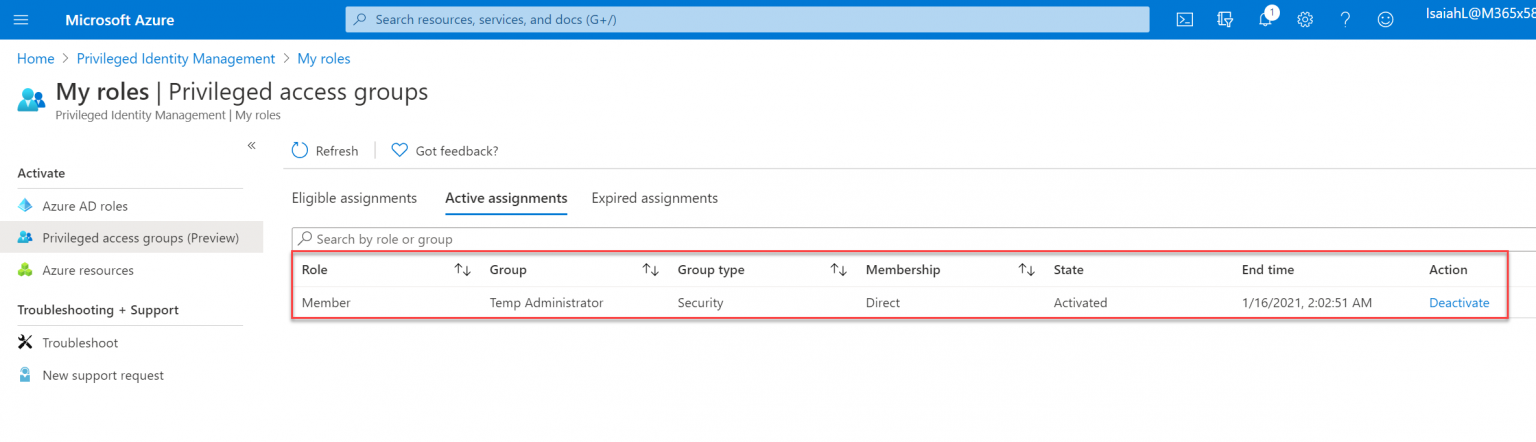


5. To approve the request, select the request first and then click on Approve.





6. Once it is approved, I went back to the user and check. Now I can see he got an active assignment.



As expected, the user the privileged user will have Global Administrator rights for 2 hours. After two hours, he will be removed from the “Temp Administrators” group automatically.