

Configuring Microsoft Entra ID

In this lab, I will configure a Microsoft Entra account. Entra is a cloud-based IAM system used with Azure. I will configure new user and group identity settings. Also I will set new password and MFA requirements.

ADDING NEW USERS

- The first step is to expand out the users column on the left and click “All Users” to view all users for the organization. Then click “New User” to add a new account.

The screenshot shows the Microsoft Entra ID 'Users' page. The left sidebar has 'Users' selected under the 'Identity' section. The main area shows a list of users with the following columns: Name, User principal name, User type, On-premises sync, and Identities. A 'New user' button is visible at the top of the list.

| Name | User principal name | User type | On-premises sync | Identities |
|-------------------|-----------------------------|-----------|------------------|--------------------------|
| Admin | admin@demoso.com | Member | No | mydemoso.onmicrosoft.com |
| Ailene McDott | ailene.mcdott@demoso.com | Member | No | mydemoso.onmicrosoft.com |
| Arnold Rickshaw | arnold.rickshaw@demoso.com | Member | No | mydemoso.onmicrosoft.com |
| Bryan Li | bryan.li@demoso.com | Member | No | mydemoso.onmicrosoft.com |
| Dustin Liverton | dustin.liverton@demoso.com | Member | No | mydemoso.onmicrosoft.com |
| Guestspeaker Jane | guestspeaker.jane@gmail.com | Guest | No | mail |
| Henry Twill | henry.twill@demoso.com | Member | No | mydemoso.onmicrosoft.com |
| Jerome Donaldson | jerome.donaldson@demoso.com | Member | No | mydemoso.onmicrosoft.com |
| Kristiann Ngu | kristiann.ngu@demoso.com | Member | No | mydemoso.onmicrosoft.com |
| Morgan King | morgan.king@demoso.com | Member | No | mydemoso.onmicrosoft.com |
| Peyton Farbain | peyton.farbain@demoso.com | Member | No | mydemoso.onmicrosoft.com |
| Tracy Westbay | tracy.westbay@demoso.com | Member | No | mydemoso.onmicrosoft.com |

EDIT GROUPS

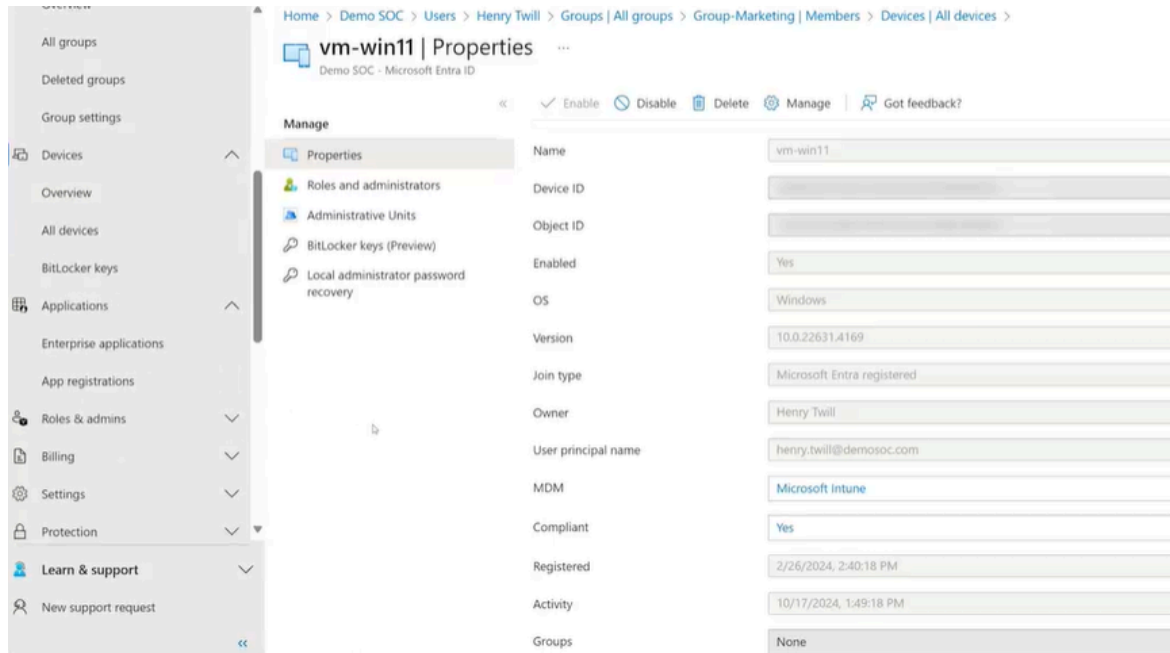
- To edit members, expand the Groups column on the left and click “All Groups”.
- Next select the group to edit. In this case, I want to add the newly created member. In the Group, I then add new members

The screenshot shows the Microsoft Entra ID 'Group-Marketing | Members' page. The left sidebar has 'Groups' selected under the 'Identity' section. The main area shows a list of group members with the following columns: Name, Type, Email, and User type. A 'Add members' button is visible at the top of the list.

| Name | Type | Email | User type |
|---------------|------|--------------------------|-----------|
| Henry Twill | User | henry.twill@demoso.com | Member |
| Morgan King | User | morgan.king@demoso.com | Member |
| Tracy Westbay | User | tracy.westbay@demoso.com | Member |

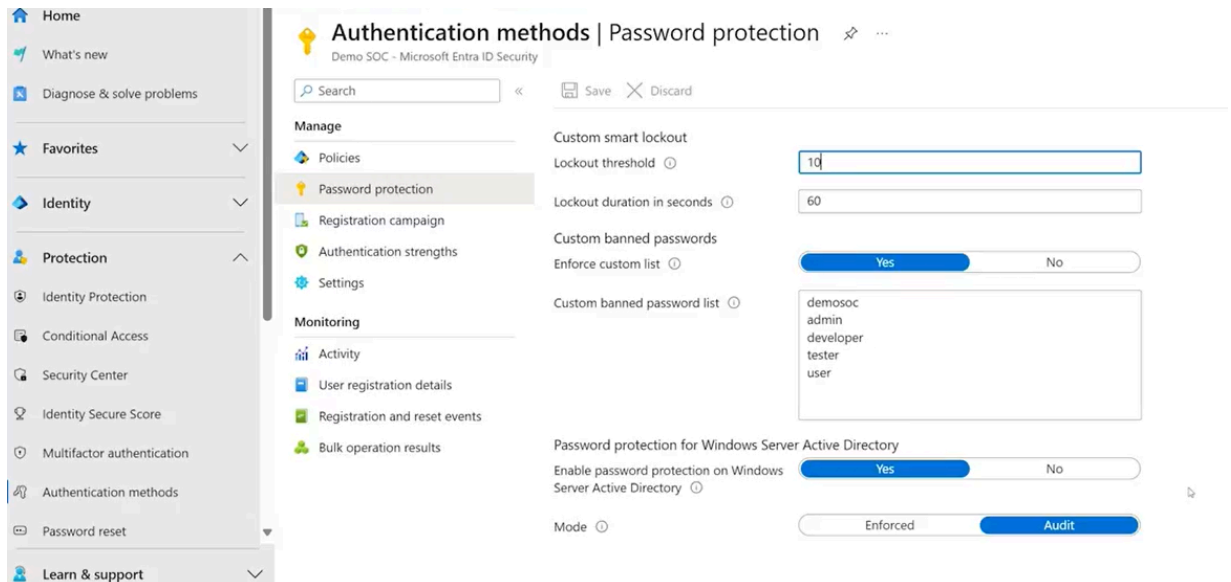
MANAGE DEVICES

- Next, I need to manage the BYOD to delete access to resources for a previous employee. Select “Devices” on the left, and All Devices to navigate to the device. Once I select the device, I can choose to disable from the companies account.

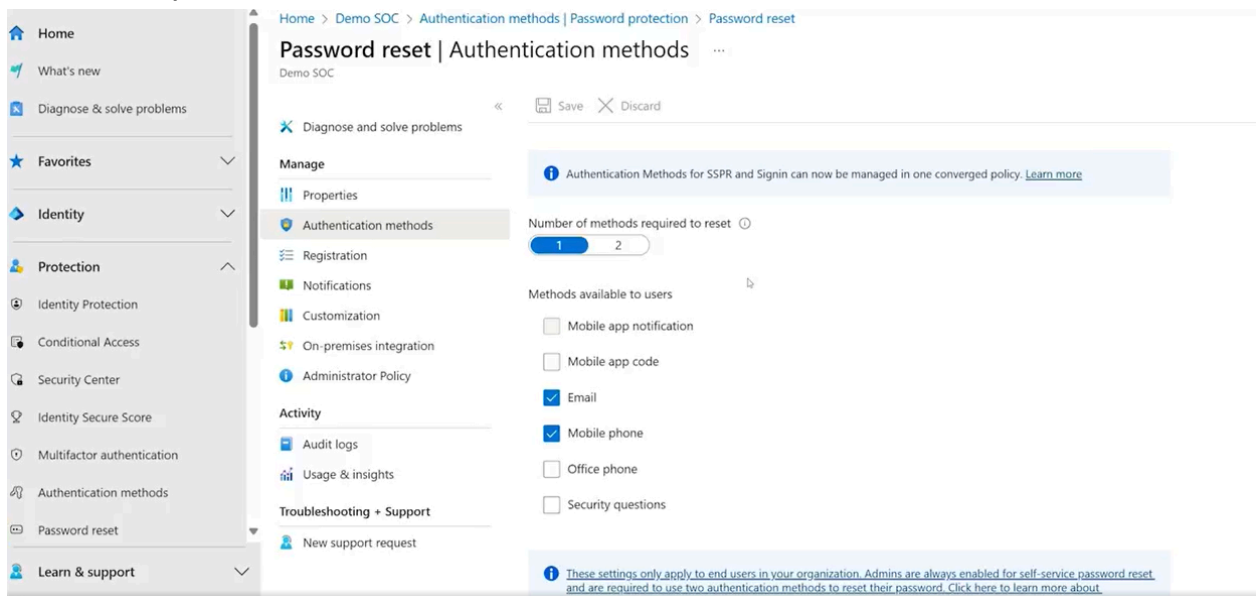


PASSWORD ACCOUNT SETTINGS

- To change the lock out count for failed password attempts, click on “Authentication Methods” and “Password Protection”. Set the number from 10 to 5.

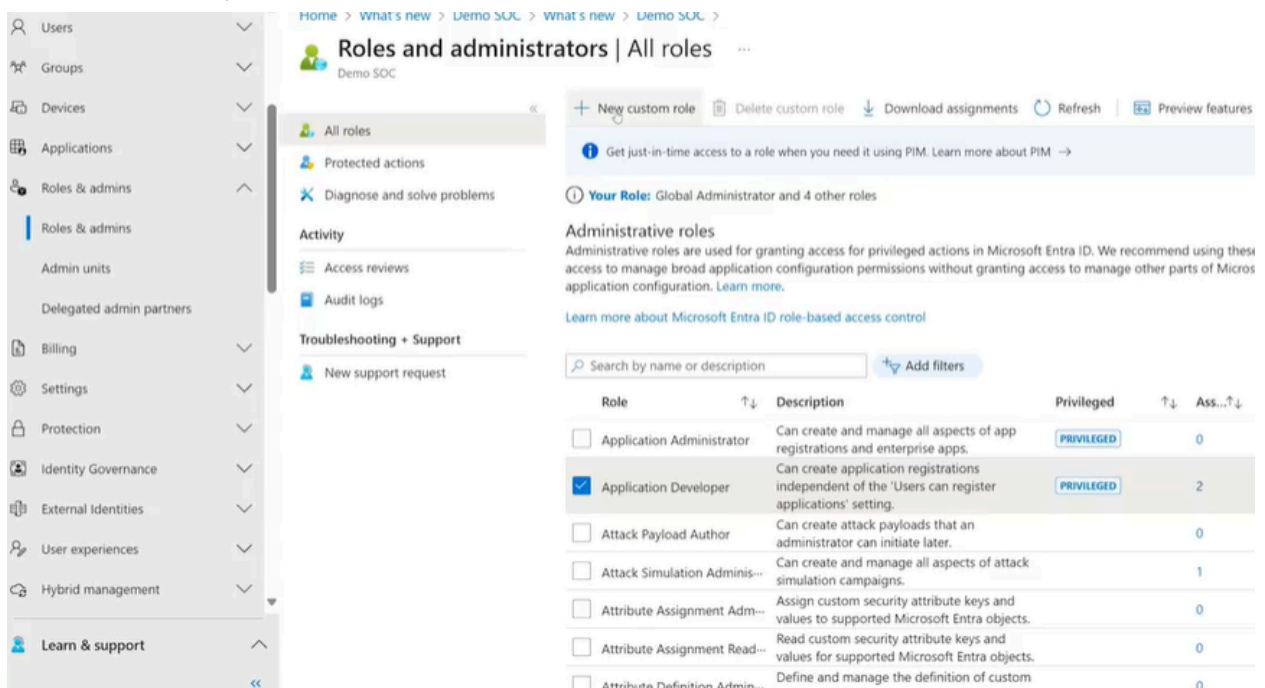


- Next, to allow users to reset their own password, click on “Password Reset” and “Authentication Methods” to set the policy to require 2 methods of authentication to reset the password.

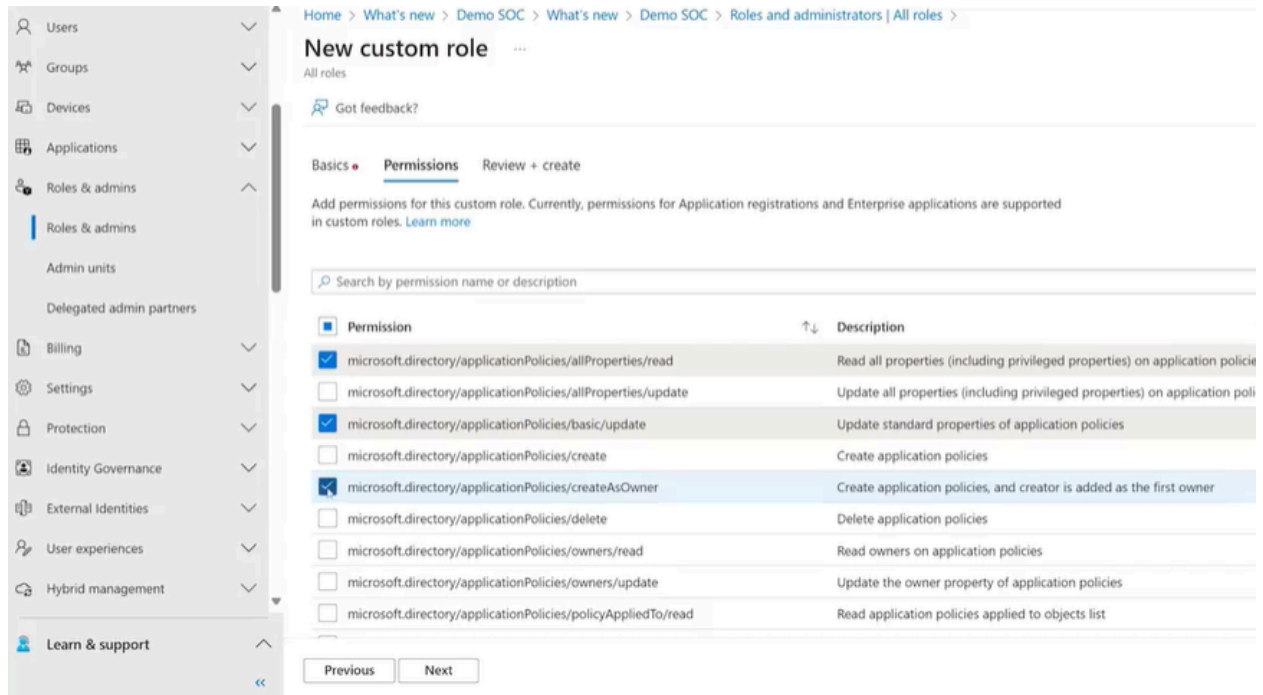


ADDING RBAC

- To add a RBAC, click on “Roles and Admins” and “New Custom Role”

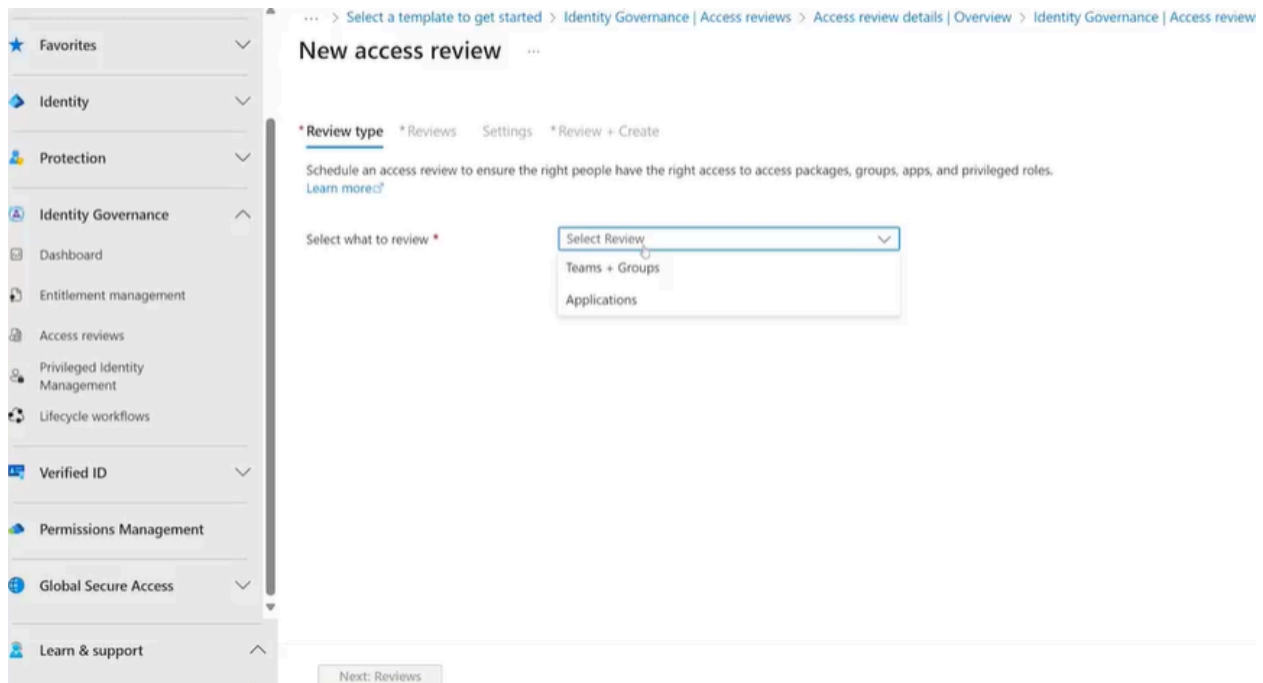


- Add a new name for the role. Then select the permissions to add for the role

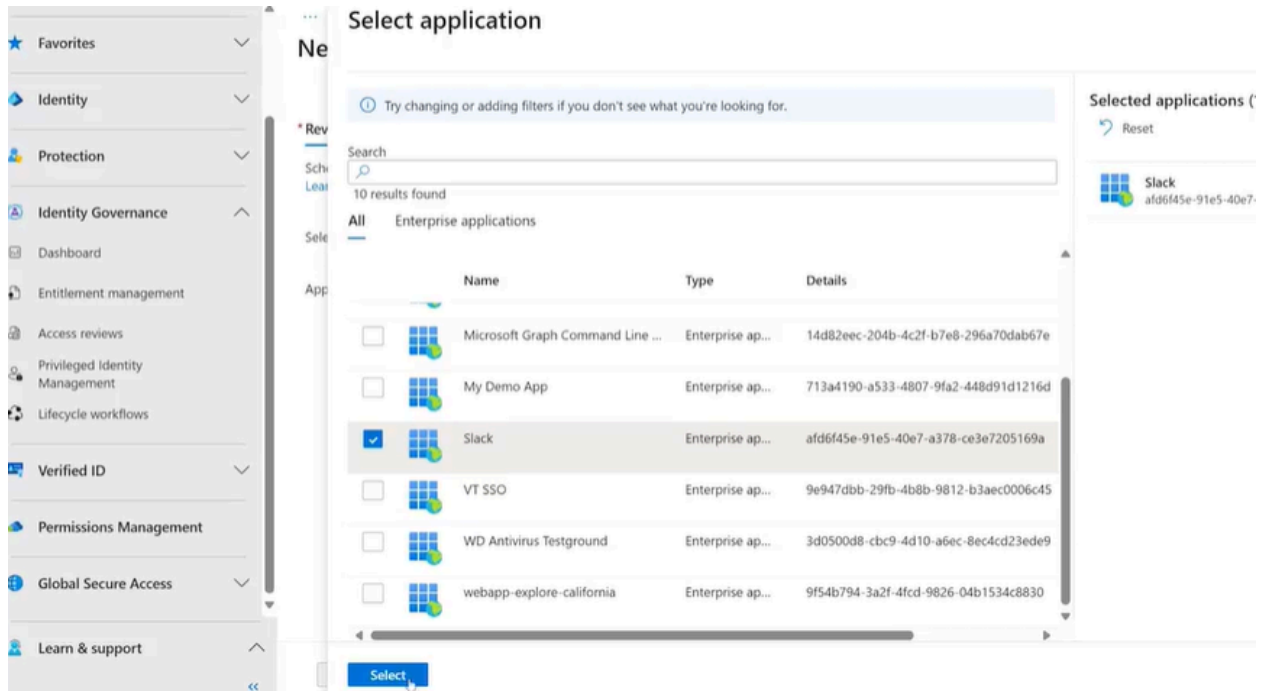


SETTING ACCESS REVIEWS

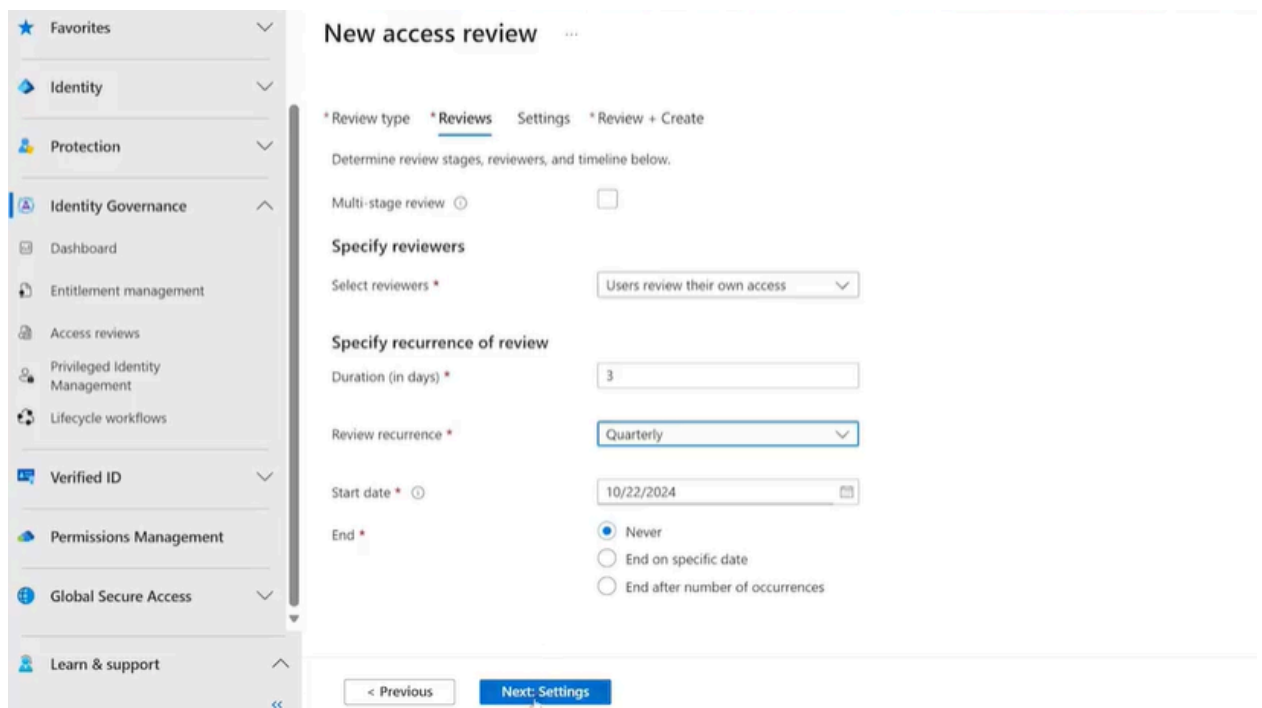
- Access reviews can be used to schedule permissions reviews to make sure only the proper accounts have the access they need.
- Click “Identity Governance” in the left column, then “Access Reviews”. Then “New Access Review”



- Select “Applications” and Slack



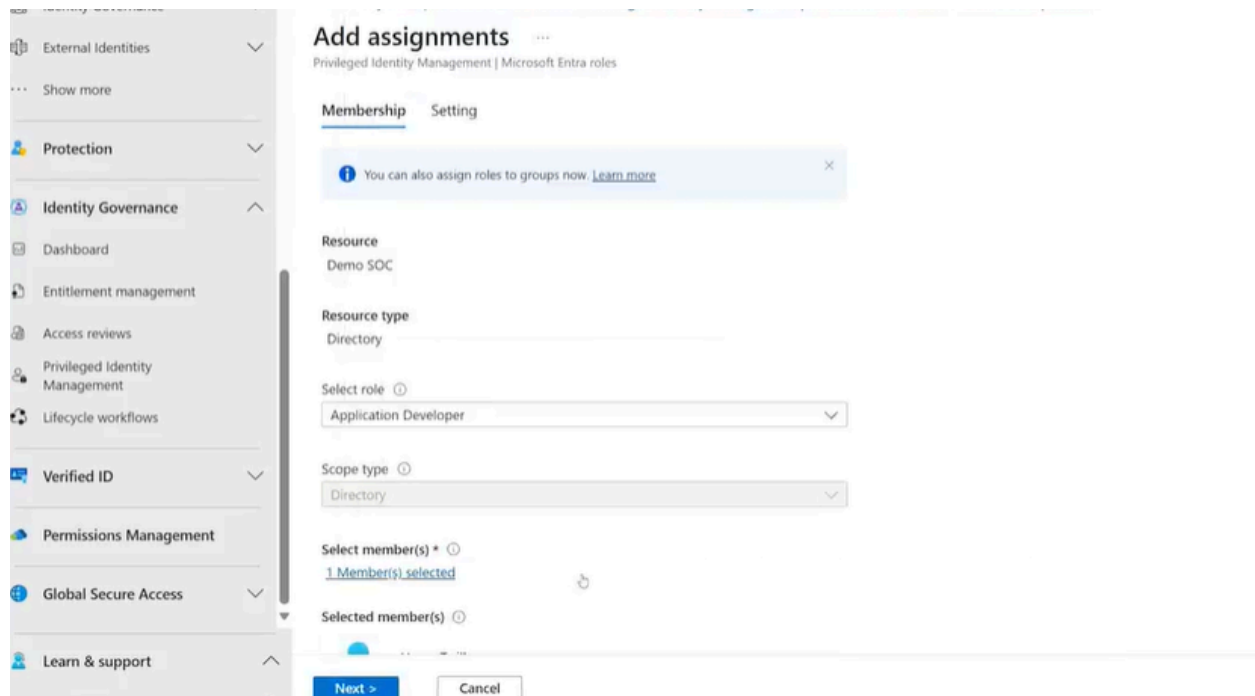
- Next select “All Users” and “Users Review Their own Access”



- Select “Next Settings” and select “Remove Access” if the reviewer does not respond
- Select “Next” and “Create”

PRIVILEGED IDENTITY MANAGEMENT

- PIM is used to give admin rights to users
- Select “Identity Governance” and “Privileged Identity Management”. Click “Assign Eligibility” and “Add Assignments”
- Then select the “Application Developer” role. And assign it to “Henry Twill”



-Then click “Next” and set the start and end dates for the role.

In this lab, I created a new user and added them to a group. I added RBAC and Access Review rules to ensure only the correct accounts stay active. Next I created and added a PIM policy to give admin rights to Henry Twill.