Microsoft 365 Identity and Services II – Enterprise Administration

~~~~~~

Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

~~~~~~

Lab Activity 1: Implementing and Managing Identity and Access

Objective: To understand and implement identity and access management in Microsoft 365.

Tasks:

1. **Set up and Configure Entra ID (Azure Active Directory)**
   - Navigate to the admin center and access the Entra ID.``
   - Add a new user to your directory.
   - Assign the user to a specific group.
   - Verify the user's group membership.
2. **Configure and Implement Multi-Factor Authentication (MFA)**
   - Enable MFA for a user in your Azure AD.
   - Configure the MFA settings to use a phone number for verification.
   - Simulate a sign-in attempt and verify that MFA is required.
   - Review the sign-in logs to confirm MFA usage.
3. **Create and Manage Conditional Access Policies**
   - Access the protection section in the Entra admin and go to Conditional Access.
   - Create a new conditional access policy for a specific group of users.
   - Set conditions that require MFA when accessing a sensitive application.
   - Test the policy by attempting to access the application from a user account.
4. **Assign and Manage User Roles**
   - Assign an administrative role to a user (e.g., Global Administrator).
   - Verify the user's permissions and access levels.
   - Remove the administrative role from the user.
   - Confirm that the user's access rights have been reduced.

~~~~~~~
Paste your screenshots here
~~~~~~~

~~~~~~

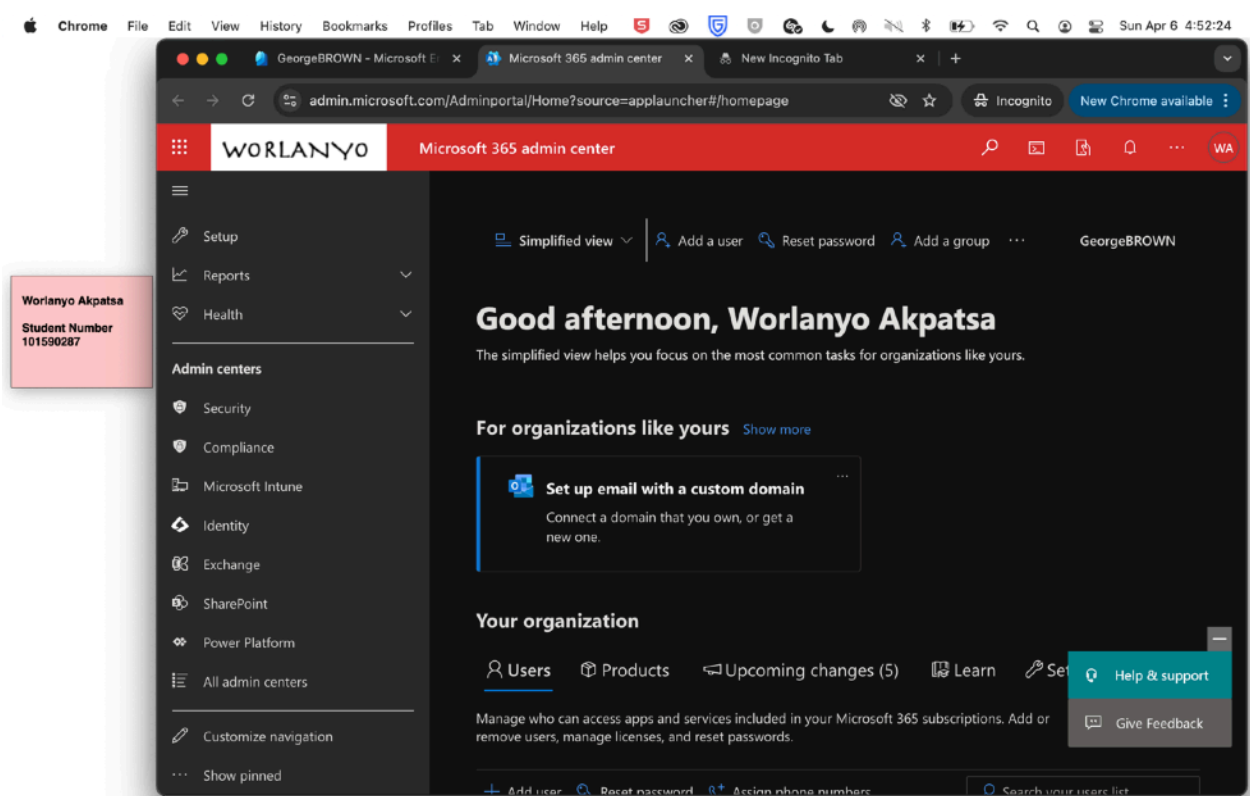
Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

~~~~~~

TASK 1: SET UP AND CONFIGURE ENTRA ID (AZURE ACTIVE DIRECTORY)

1.1: Navigate to the admin center and access the Entra ID

A: Navigating to Microsoft 365 Admin Center Homepage



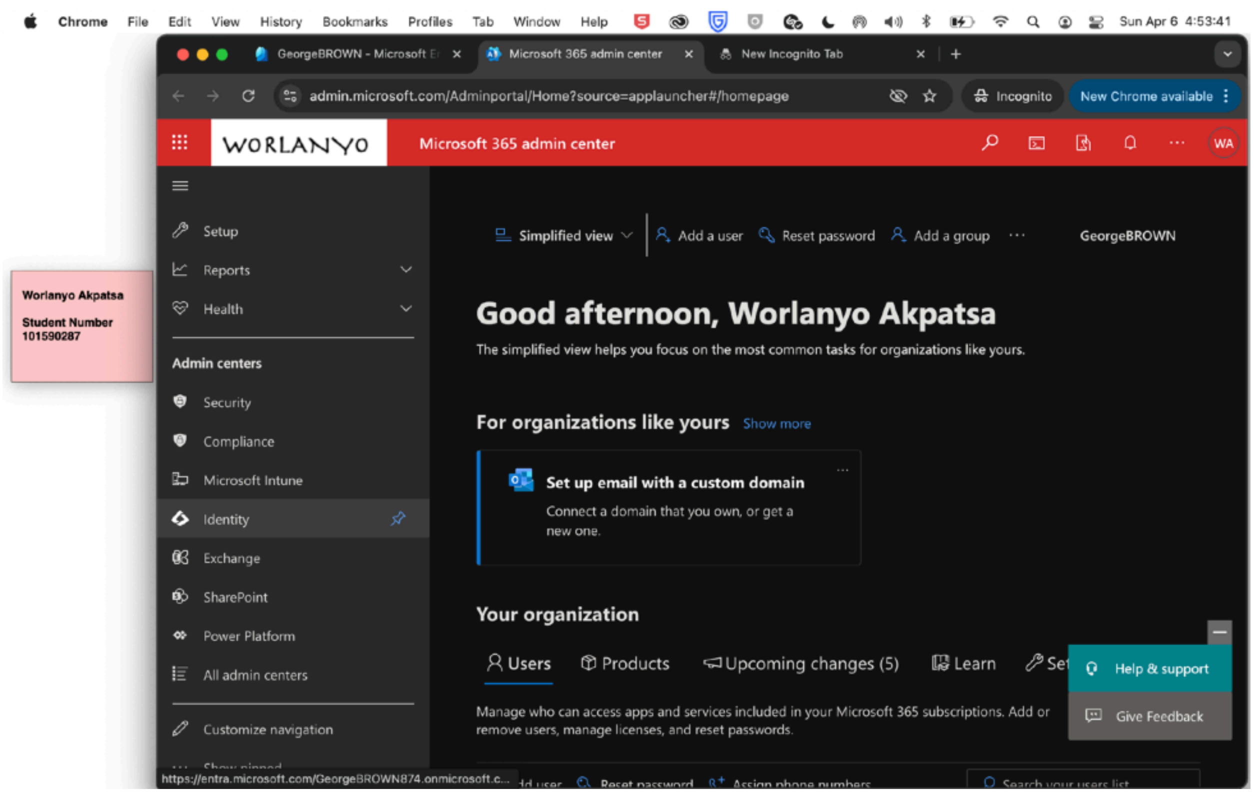
~~~~~~

Student Name: Worlanyo Akpatsa
Student ID: 101590287

Term: Winter 2025

~~~~~~

B: Scrolling down on the left panel and clicking Identity to reach Entra Homepage

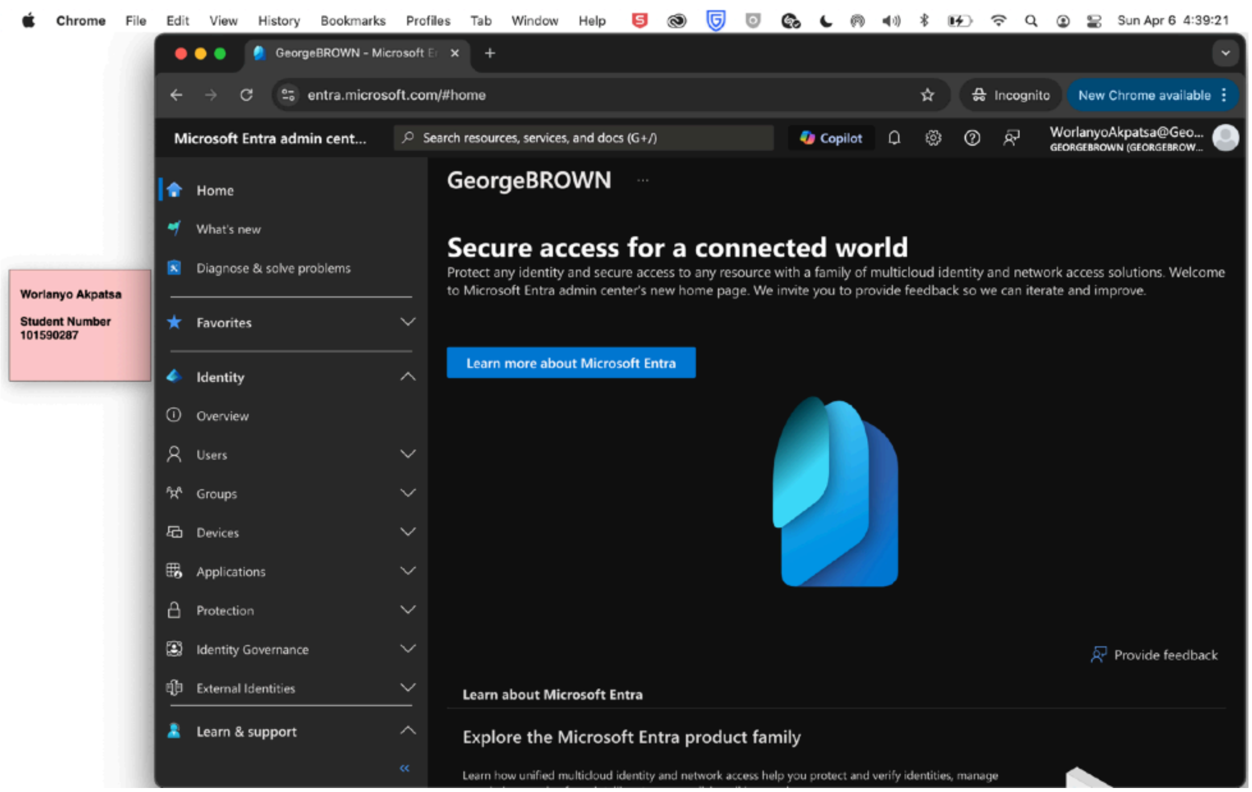


~~~~~~

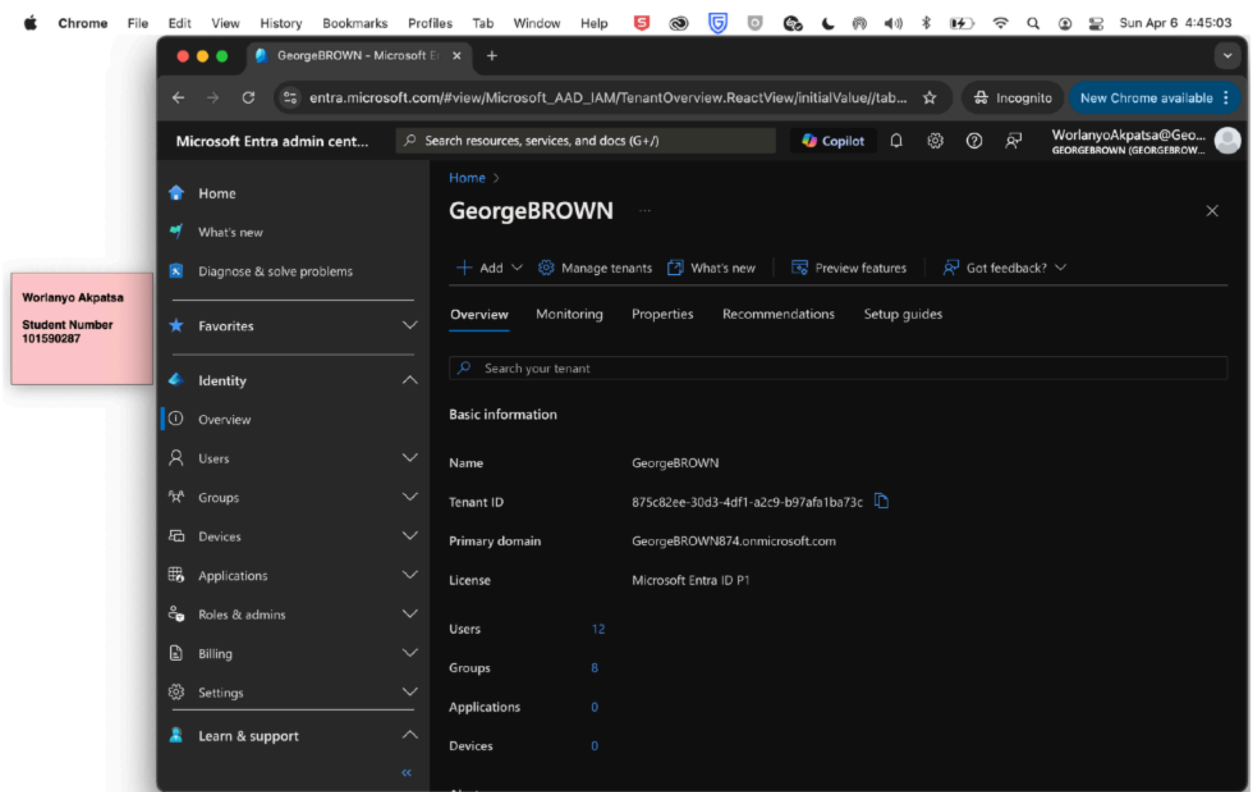
Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

~~~~~~

C: Entra Homepage



D: Clicking on identity->Overview in the left pane to view directory overview and access the Entra ID



~~~~~~

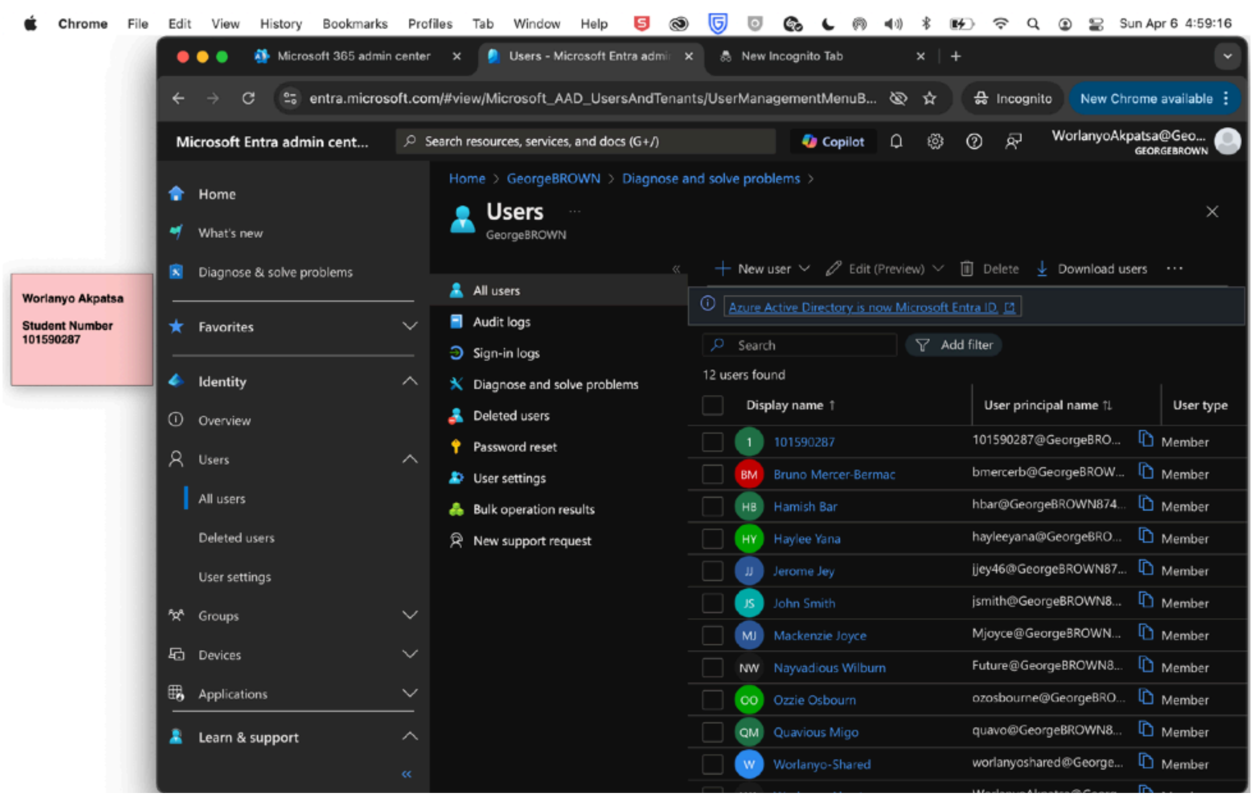
Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

~~~~~~

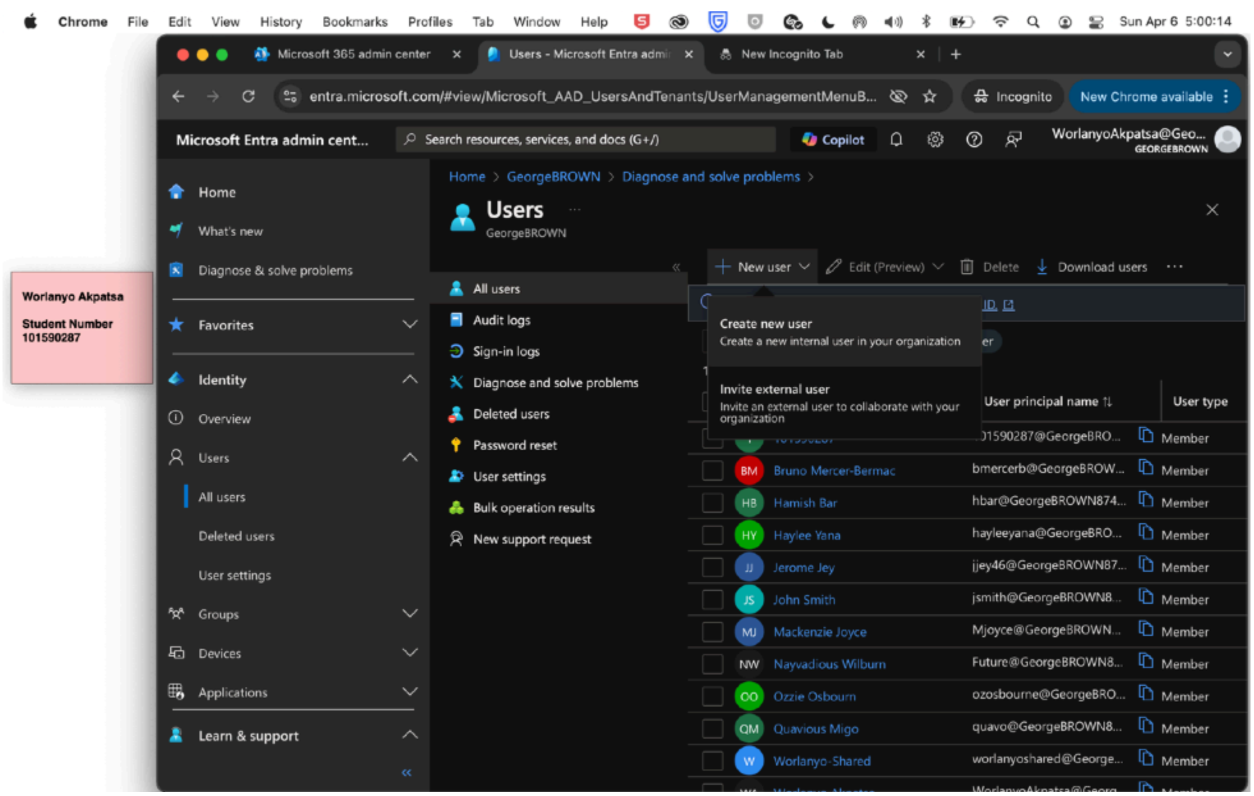
1.2: Add a new user to your directory

1.3: Assign the user to a specific group

A: Navigate to identity->users->all users



B: Clicking on "New user" then "create new user" to add a user to the directory

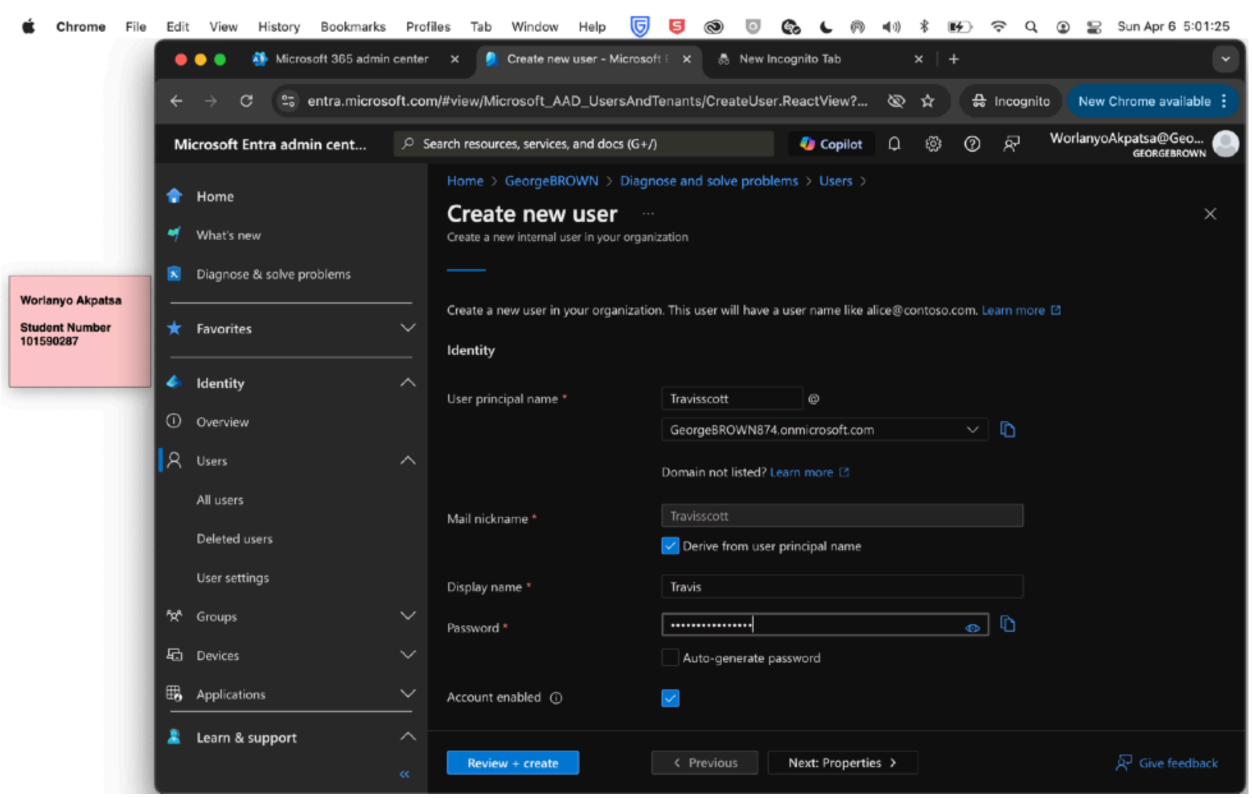


~~~~~~

Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

~~~~~~

C: User Creation Process (Basics)

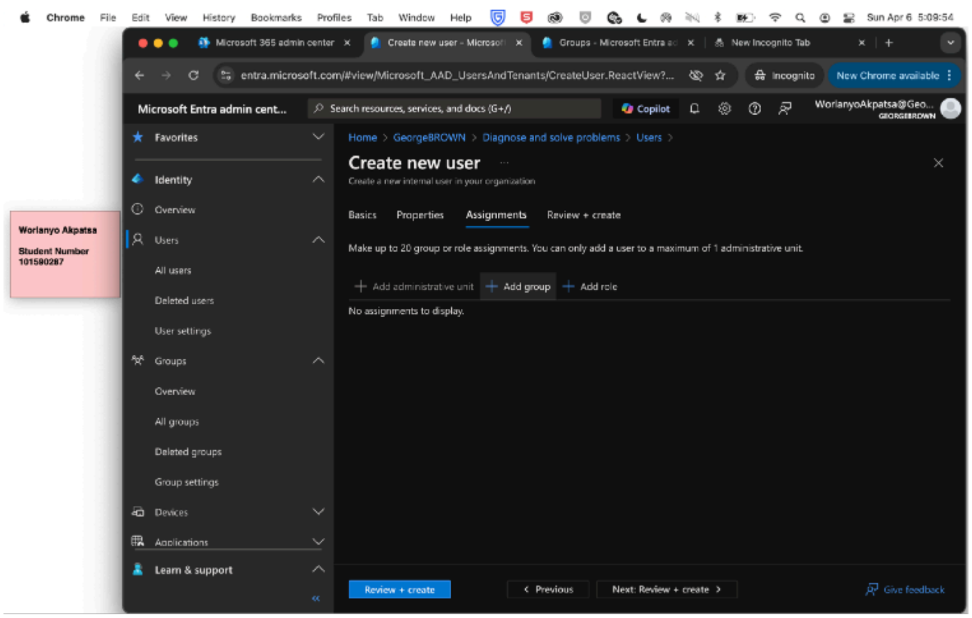


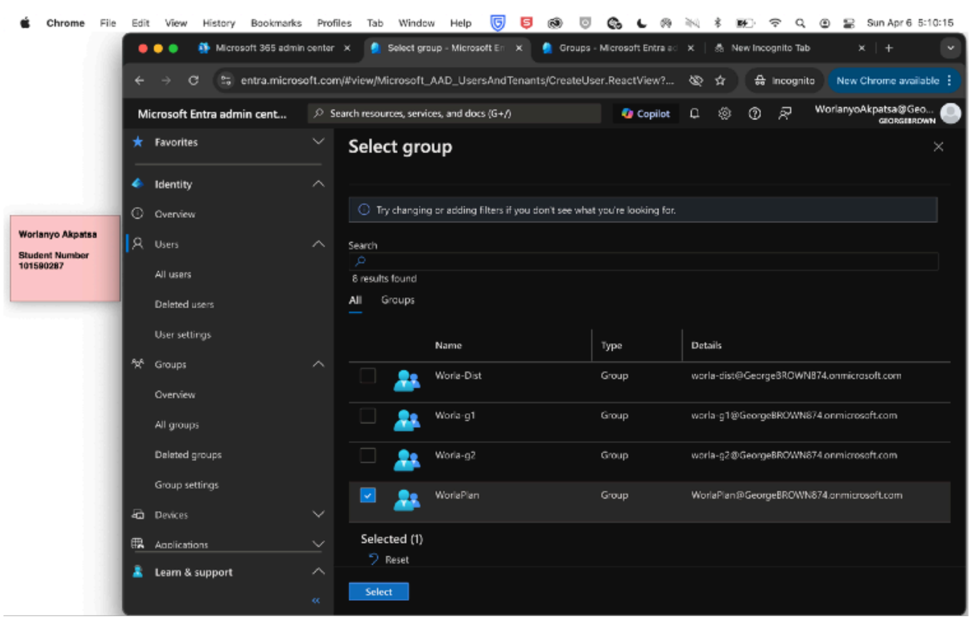
~~~~~~
~~~~

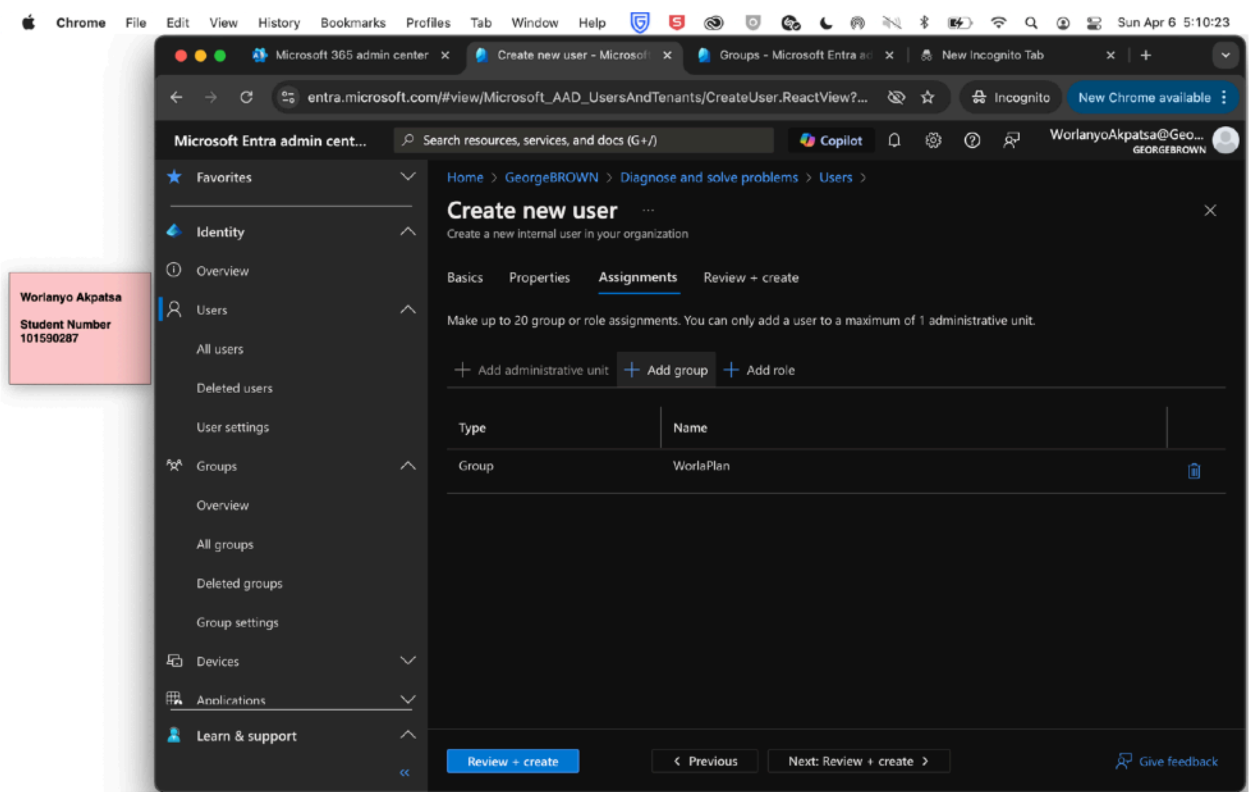
Student Name: Worlanyo Akpatsa	Term: Winter 2025
Student ID: 101590287

~~~~~~
~~~~

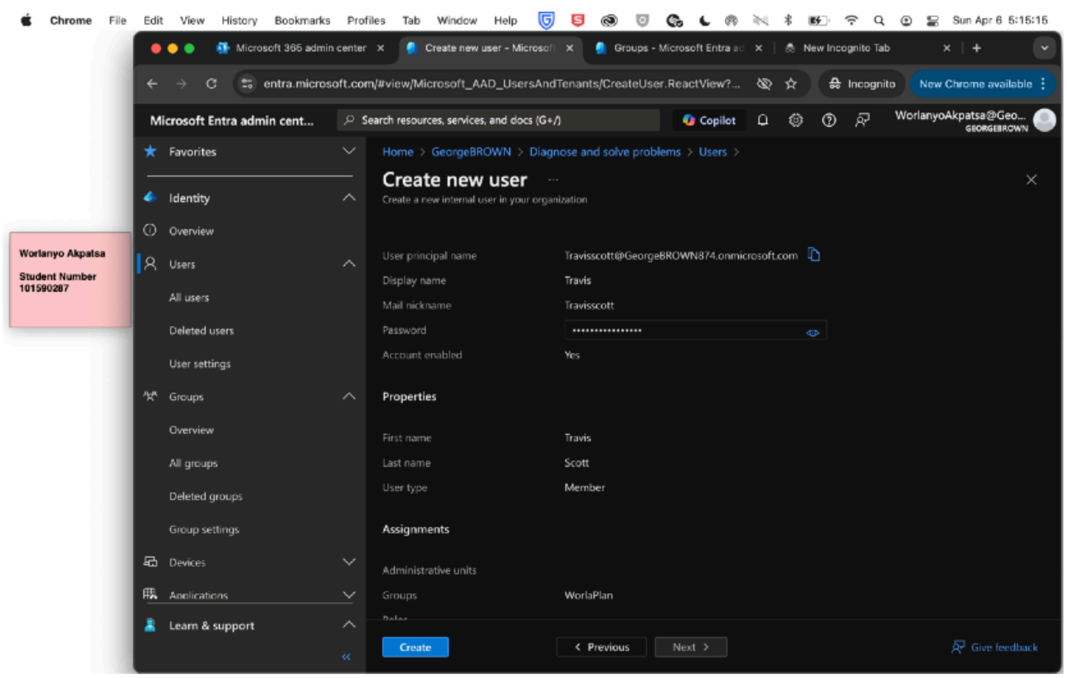
D: User Creation Process (Assignments=Assigning user Travis Scott to the group Worla Plan)





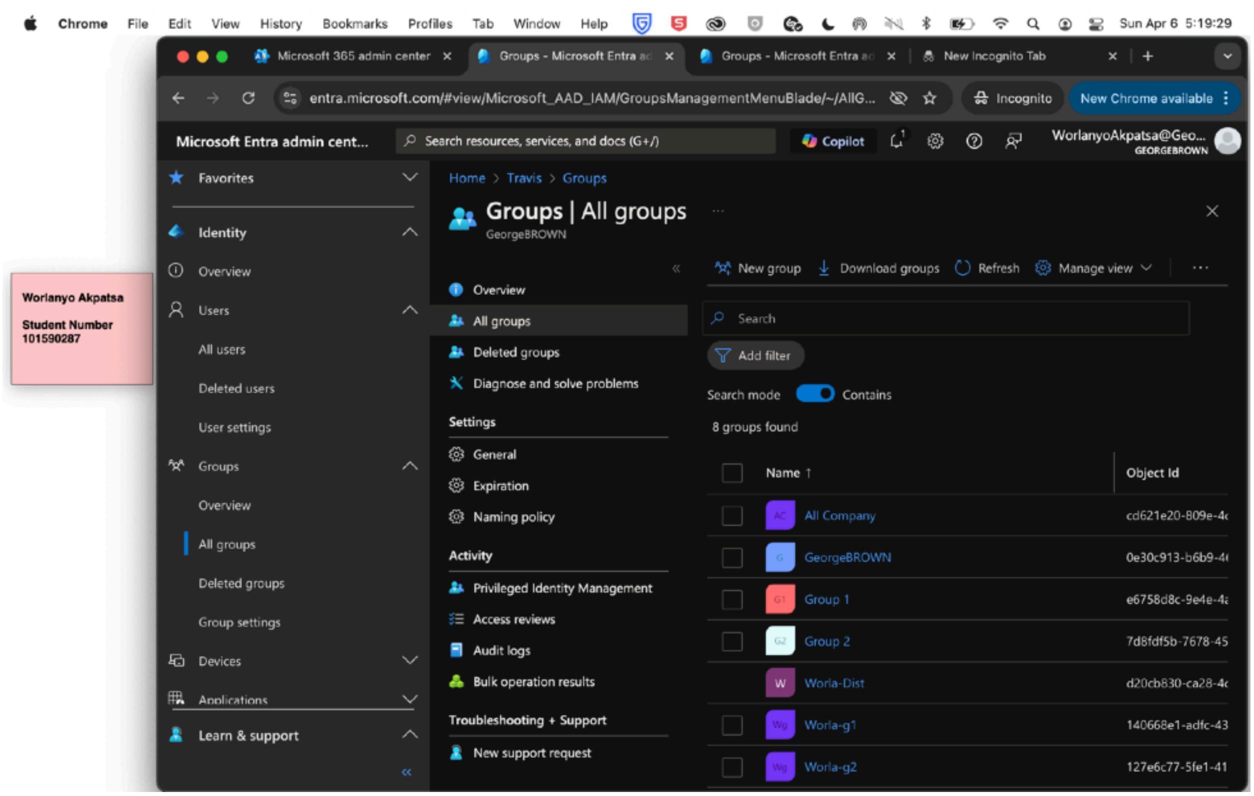

Worlanyo Akpatsa
Student Number 101590287
entra.microsoft.com/#view/Microsoft_AAD_UsersAndTenants/CreateUser.ReactView?...
Microsoft Entra admin cent...
Home > GeorgeBROWN > Diagnose and solve problems > Users >
Create new user
Create a new internal user in your organization
Basics
Properties
Assignments
Review + create
Make up to 20 group or role assignments. You can only add a user to a maximum of 1 administrative unit.
Add administrative unit
Add group
Add role
Type
Name
Group
WorlaPlan
Review + create
Previous
Next: Review + create
Give feedback

E: Review and finish creating user



1.4: Verify the user's group membership

A: Navigate to Groups->All groups on the left pane

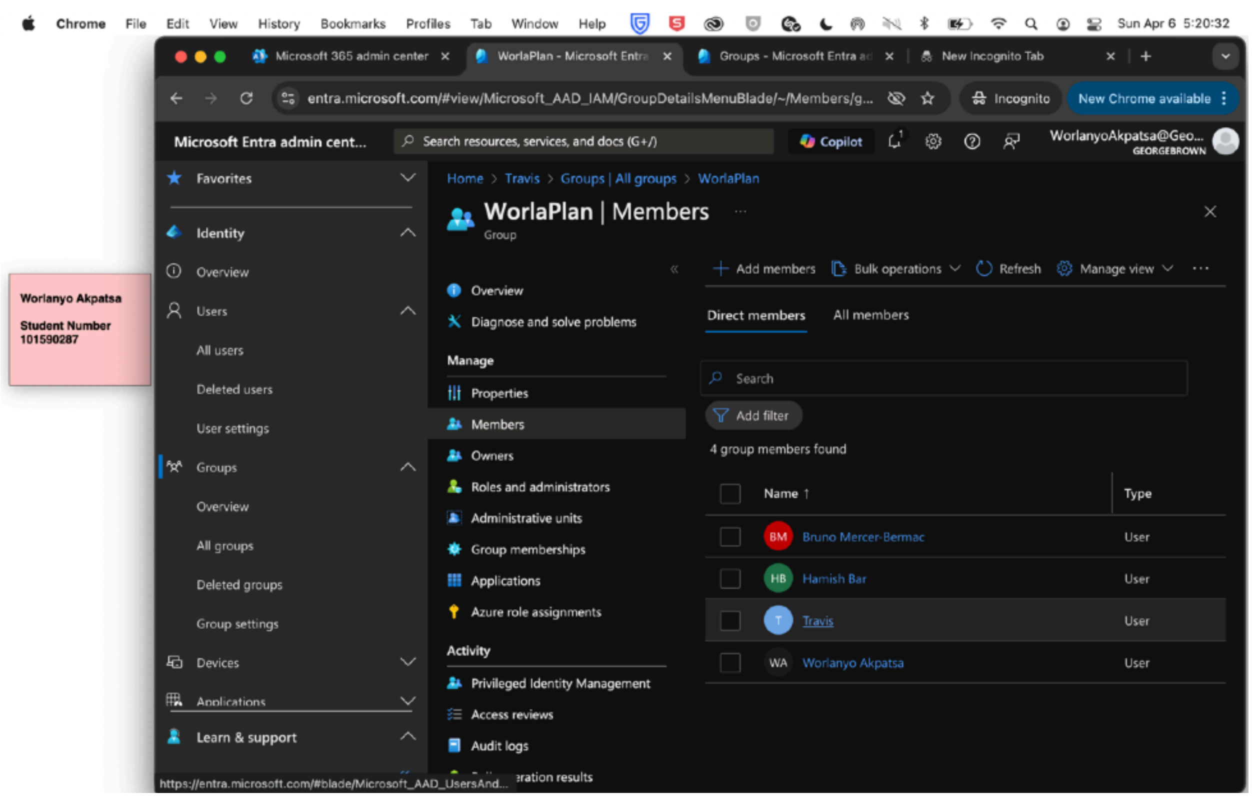


~~~~~~
~~~~

Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

~~~~~~
~~~~

B: Open WorlaPlan group and observe new user Travis as a member



Task 1 Summary

Task 1 was rather easy to do I must admit because most of the things asked of us were already covered in the first Microsoft 365 class.

To be really honest, the most confusing part of this assignment was accessing the Entra Homepage which shows how easy the task was. Luckily for me, I learnt different ways to access it.

To explain, while on your 365 Admin Center Homepage, if you scroll down the left pane you are supposed to see all the other types of Admin Centers (exchange, sharepoint, etc) but it does not explicitly say “Entra” so I had to google to see how to access it.

Google suggested I navigate to “entra.microsoft.com” which isn’t a bad option. However, with this, I have to log in with all my credentials.

The better way is to use the 365 Admin Center. Just like all the other admin centers, you have to scroll down on the left pane and you will see “Identity”. If you click on this, it takes you to your Entra Homepage without having to now sign in. I think this is the advantageous option obviously.

After logging in, the task asked to access the Entra ID. Similar to other admin centers, the navigation is really simple and easy to figure out. All I had to do was click on Identity in the left pane and click Overview. This shows the name of the directory, Tenant ID, domain name, licenses, users, groups, etc. Basically it shows an overview of your directory.

Next task was to create a new user and assign them a group which because I have done several times, was a breeze. I clicked on users->all users in the left pane and when that page opened, I clicked new user and began filling in the info for my new user. While creating user, there is an Assignments page where you can assign groups and roles. I assigned this new user to a group I had already created called WorlaPlan. After, I reviewed and created the user.

To verify that my user was in this group, I chose to open the group and see its members. To do this, I clicked on groups->all groups in the left pane and selected my group, WorlaPlan.

Here, there are a number of tabs containing information about the group. These tabs include overview, owners, members, etc. To verify that my user Travis was in the group, I clicked on members and saw his name. This shows that he was successfully added to the group.

~~~~~~

Student Name: Worlanyo Akpatsa
Student ID: 101590287

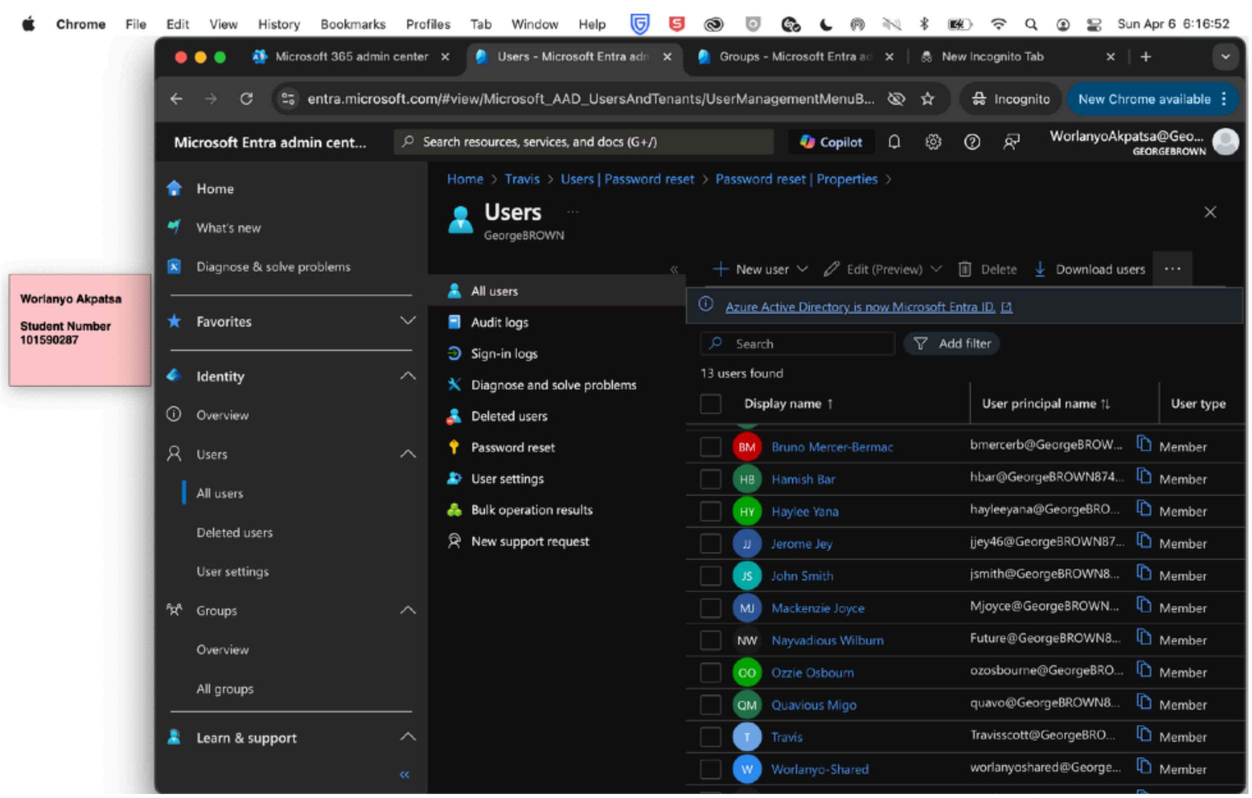
Term: Winter 2025

~~~~~~

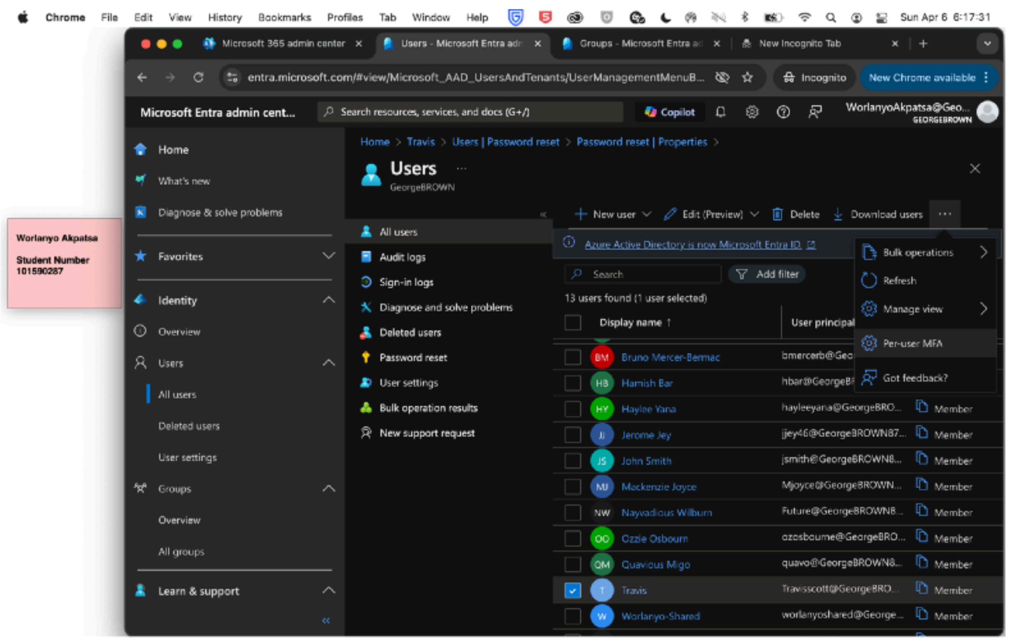
TASK 2: CONFIGURE AND IMPLEMENT MULTI-FACTOR AUTHENTICATION (MFA)

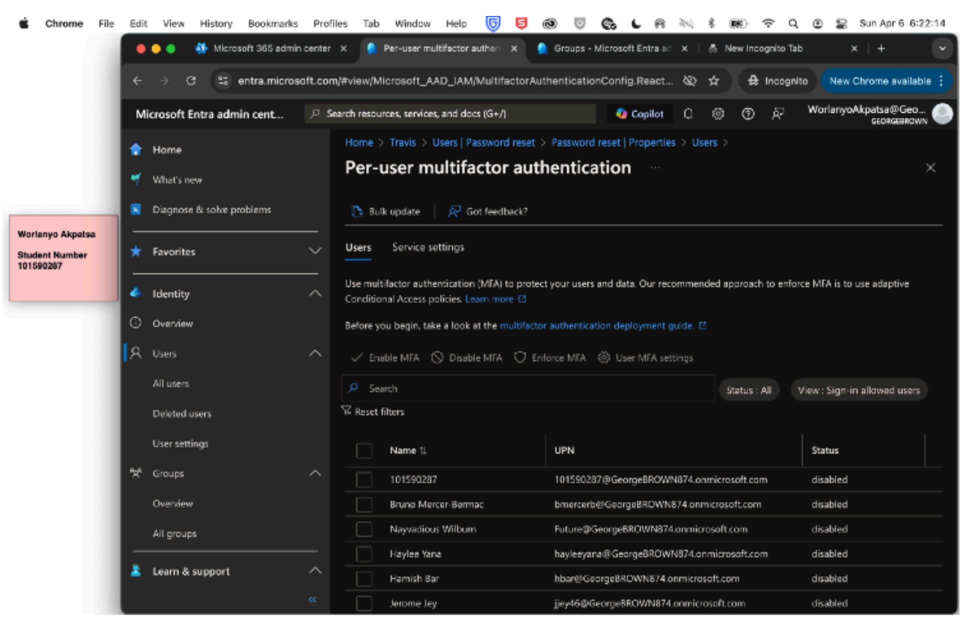
2.1: Enable MFA for a user in your Azure AD

A: Navigate to All Users

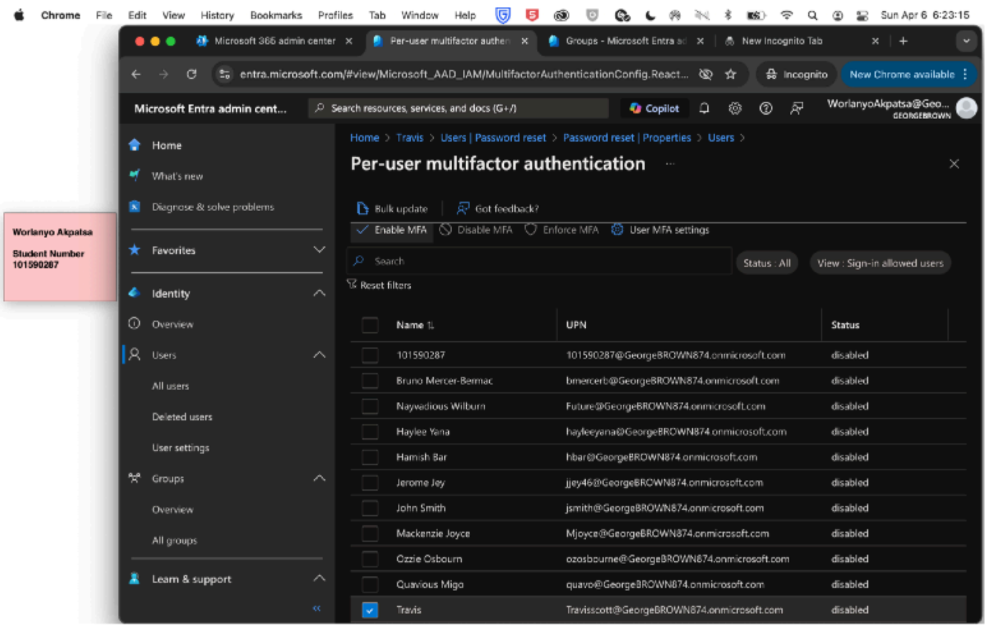


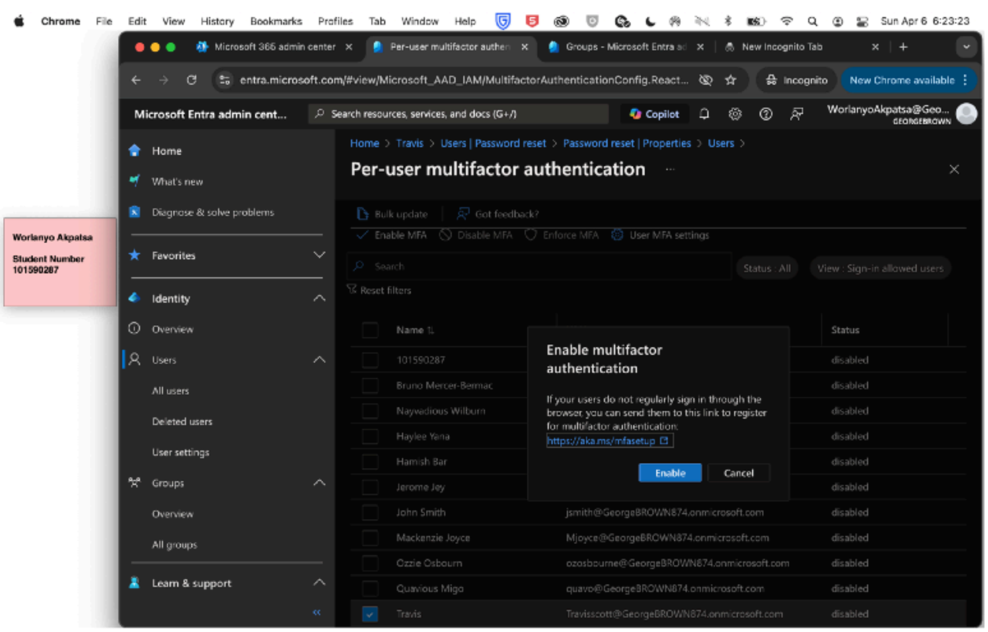
B: Clicking on the three dots at the top and selecting "Per-user MFA"





C: Clicking on the checkmark beside user created in task 1 and clicking “Enable MFA”



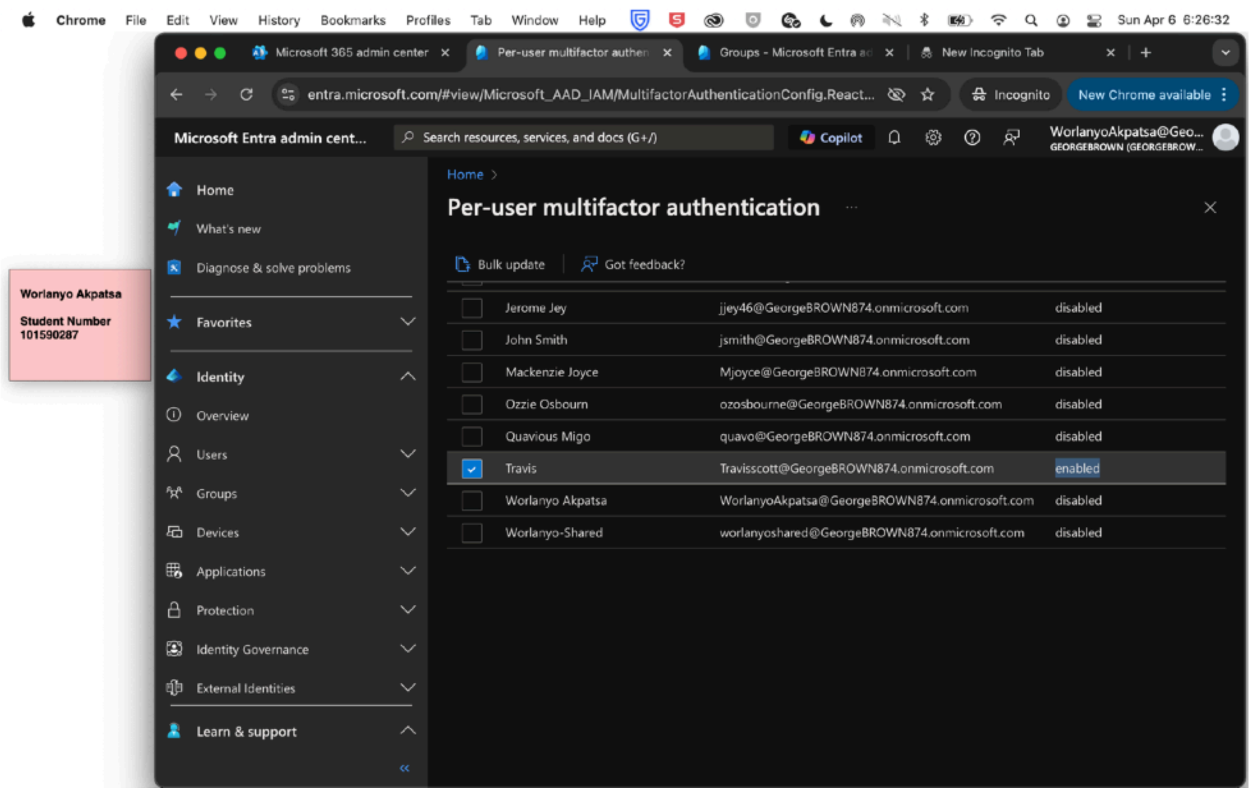


~~~~~~

Student Name: Worlanyo Akpatsa
Student ID: 101590287
Term: Winter 2025

~~~~~~

D: MFA enabled for user Travis



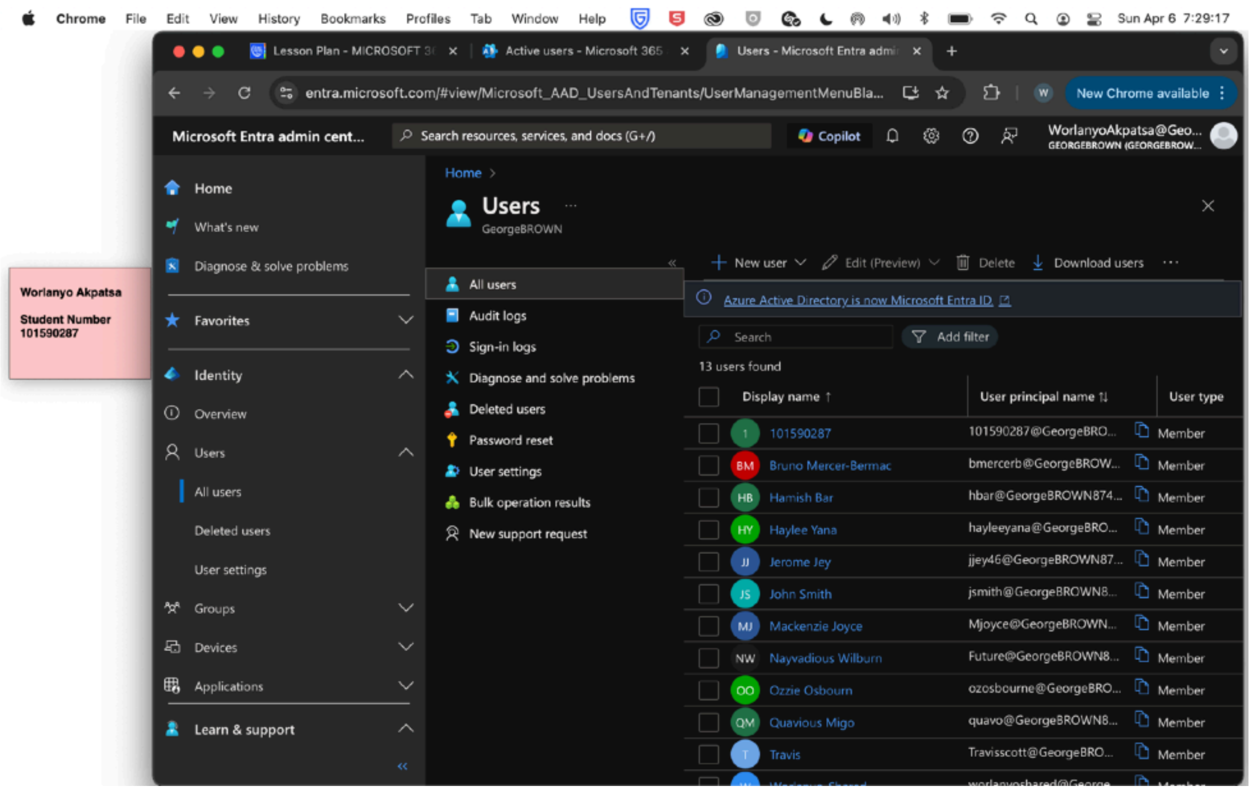
~~~~~~

Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

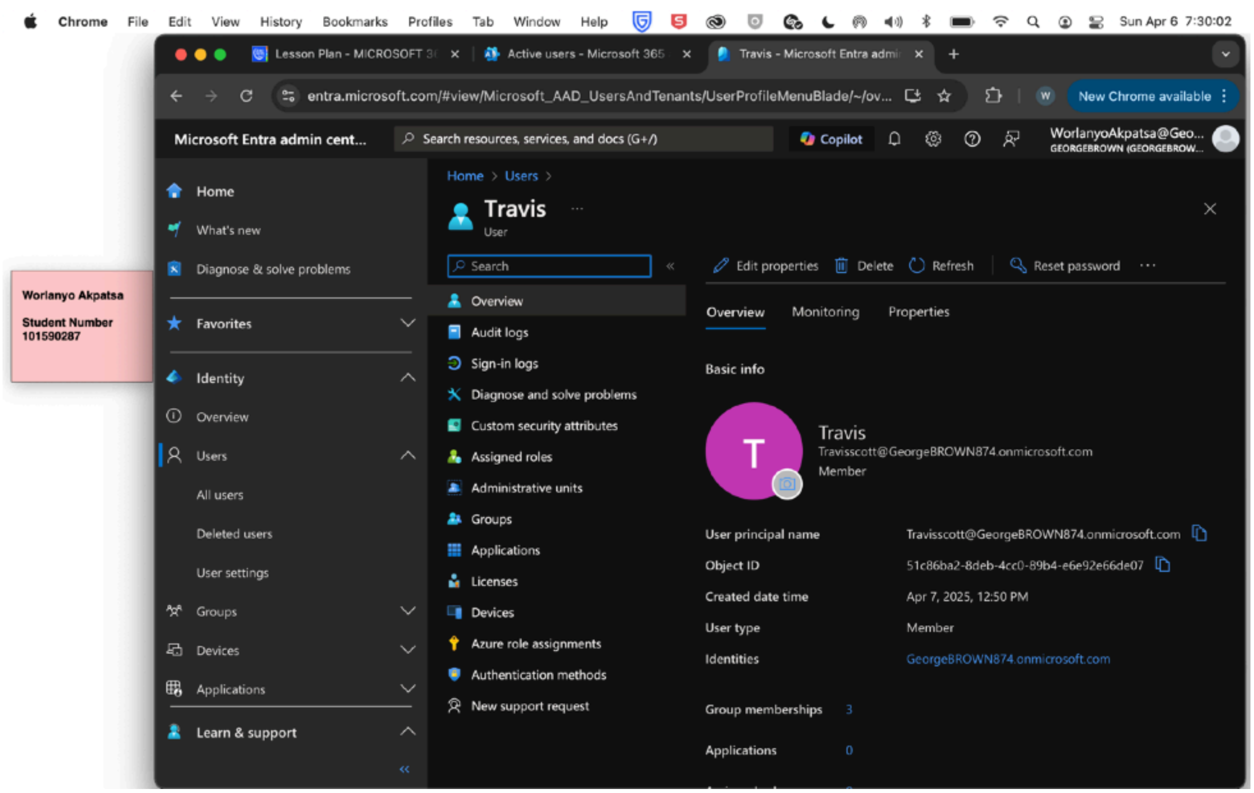
~~~~~~

2.2: Configure the MFA settings to use a phone number for verification

A: Navigate to users->all users

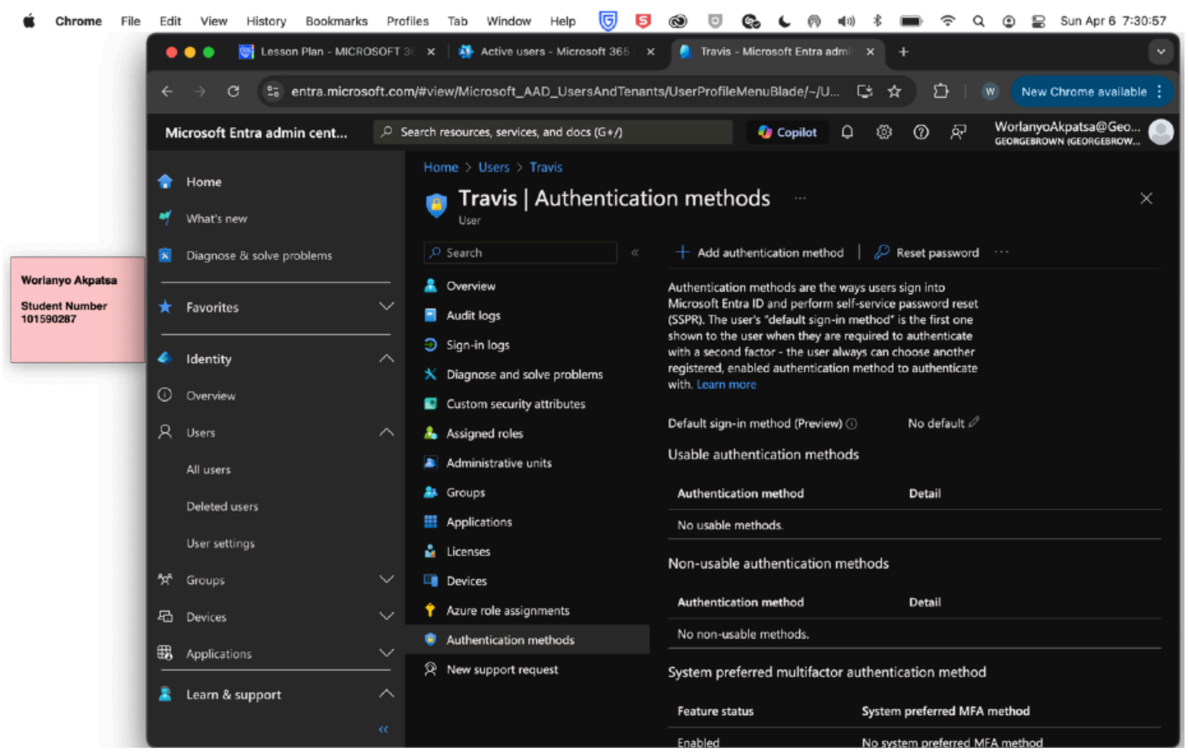


B: Select new user (travis)



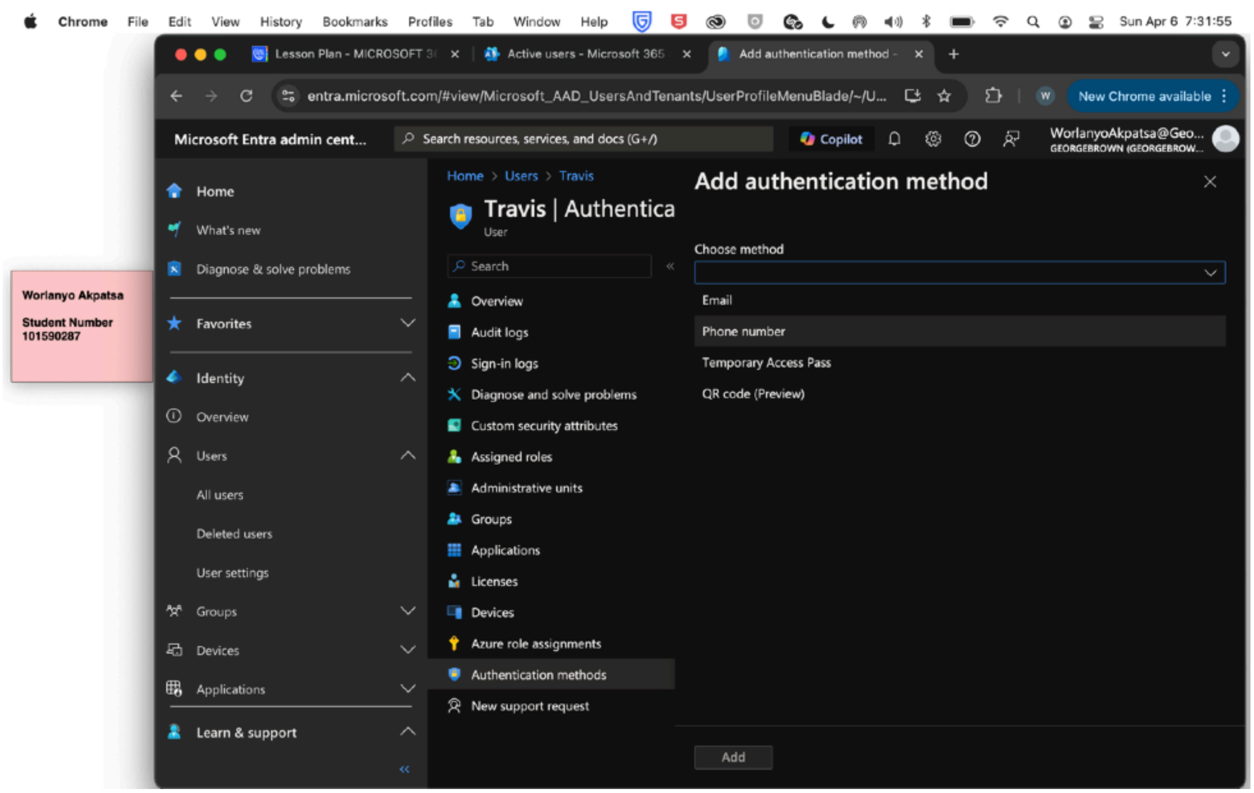
Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

C: Choose Authentication Methods under Travis Profile

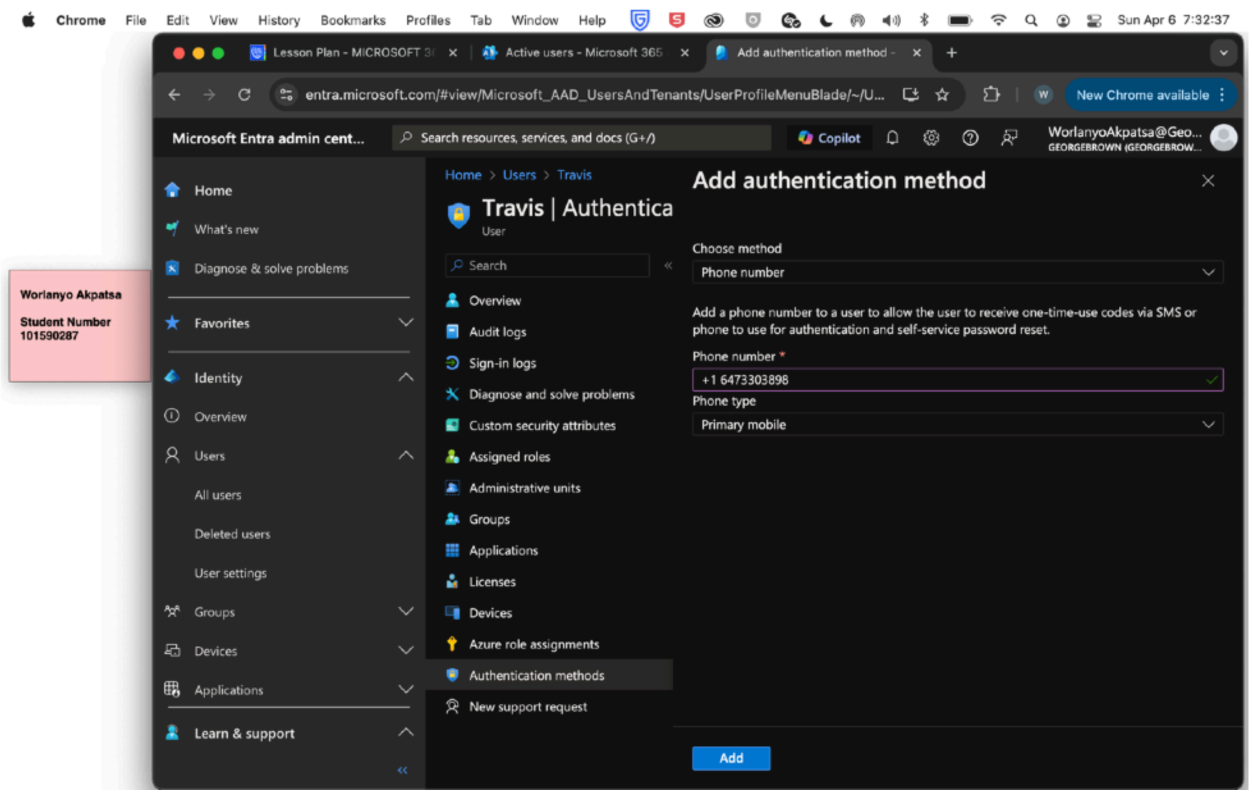


Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

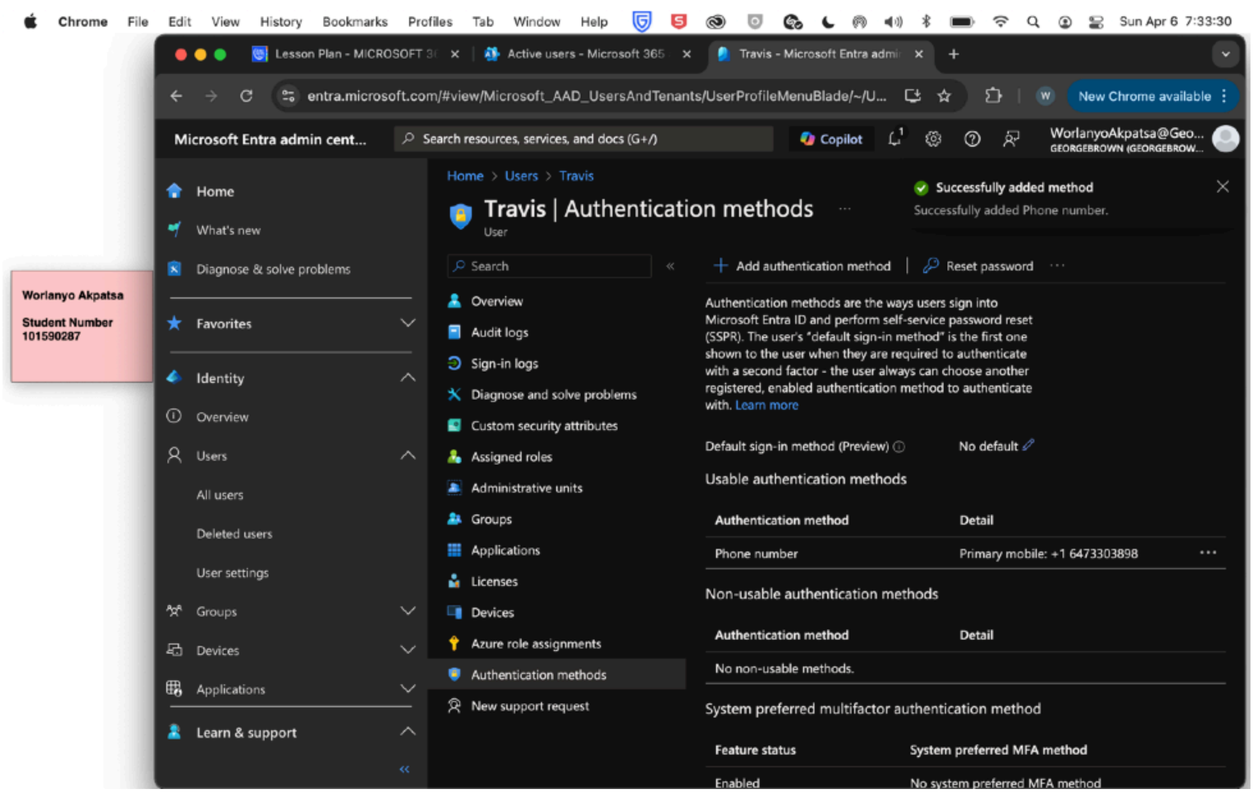
D: Click Add Authentication Method and Select Phone Number



E: Add phone details



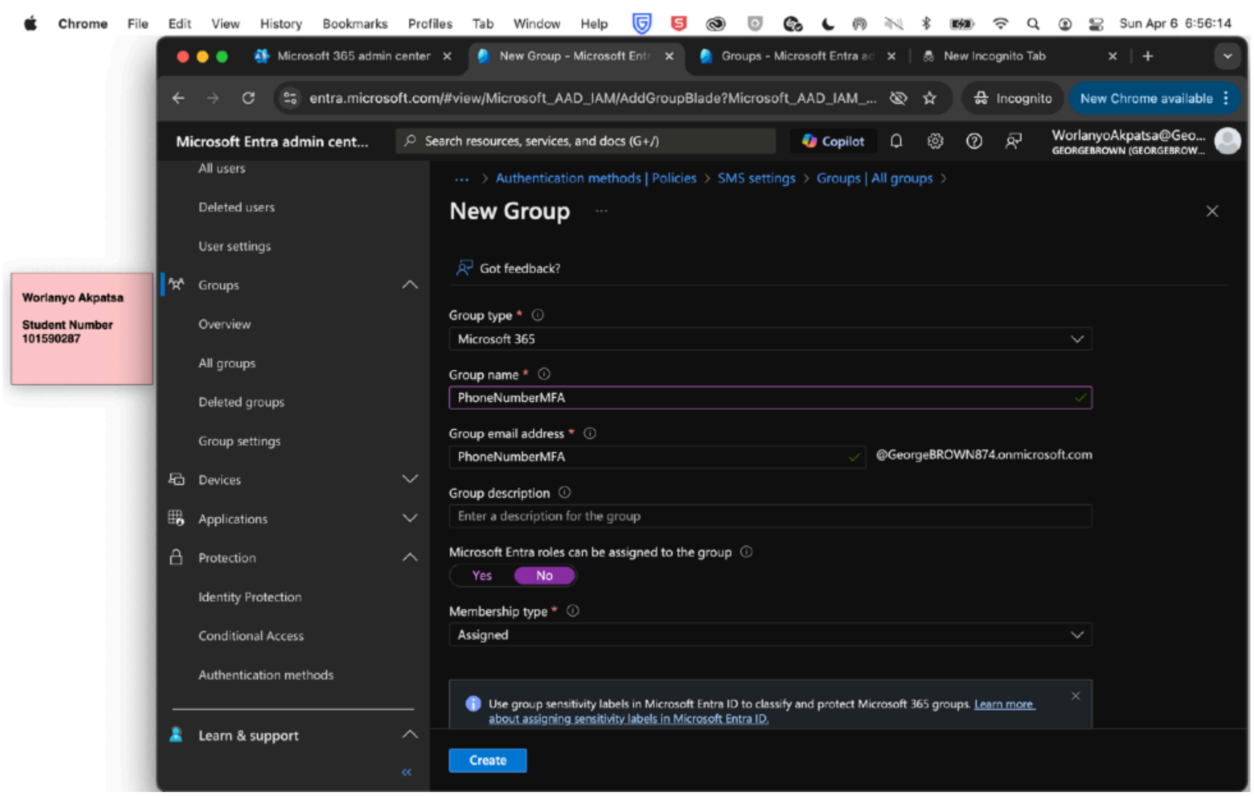
F: Successfully Added Method of Authentication (Phone Number)



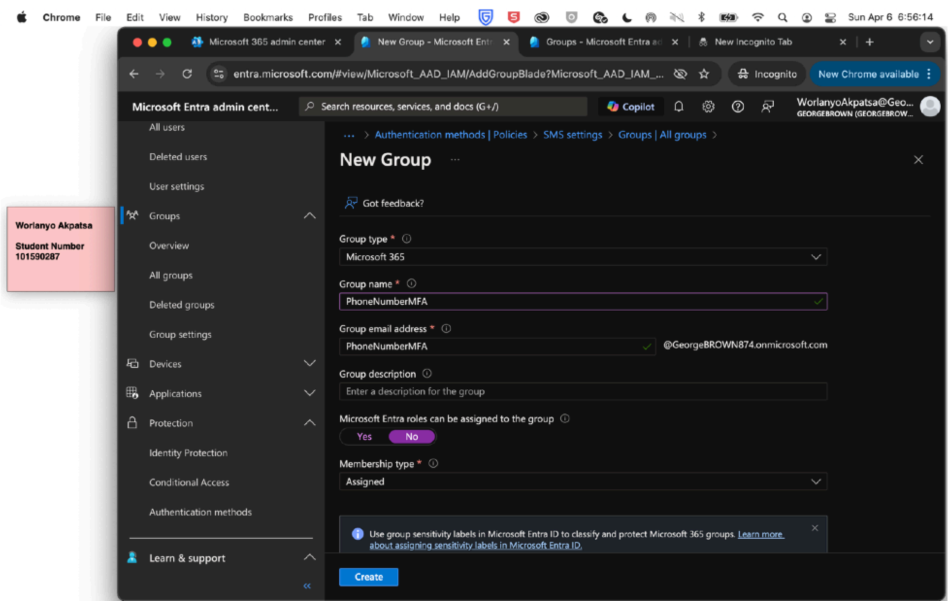
Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

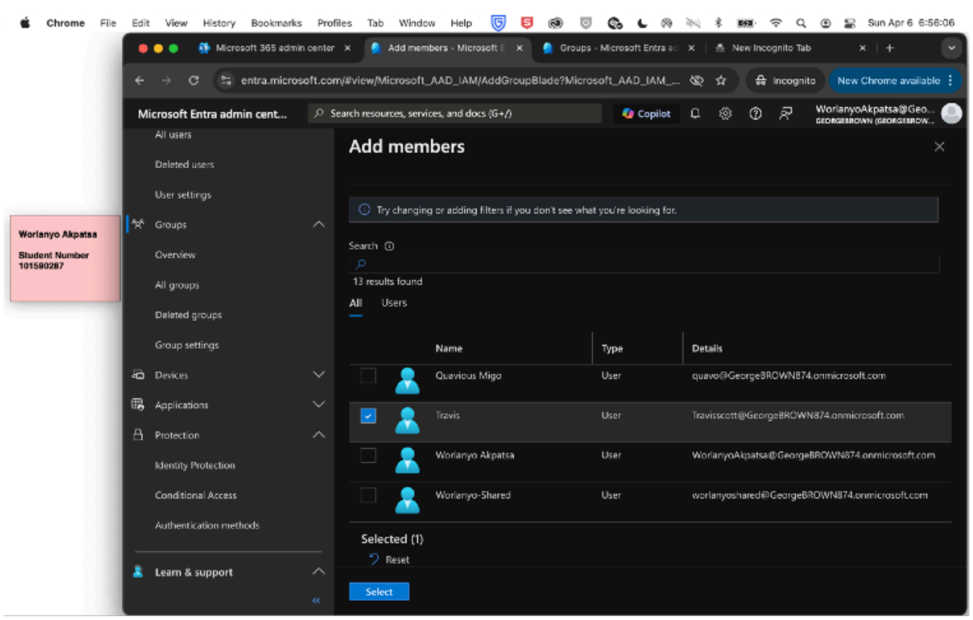
I learnt that you can also set custom Authentication settings for specific groups which also involve their phone number. For example, getting SMS messages. I underwent this process below as an extra Authentication feature.

A: Create group called Phone Number MFA and add user Travis to it

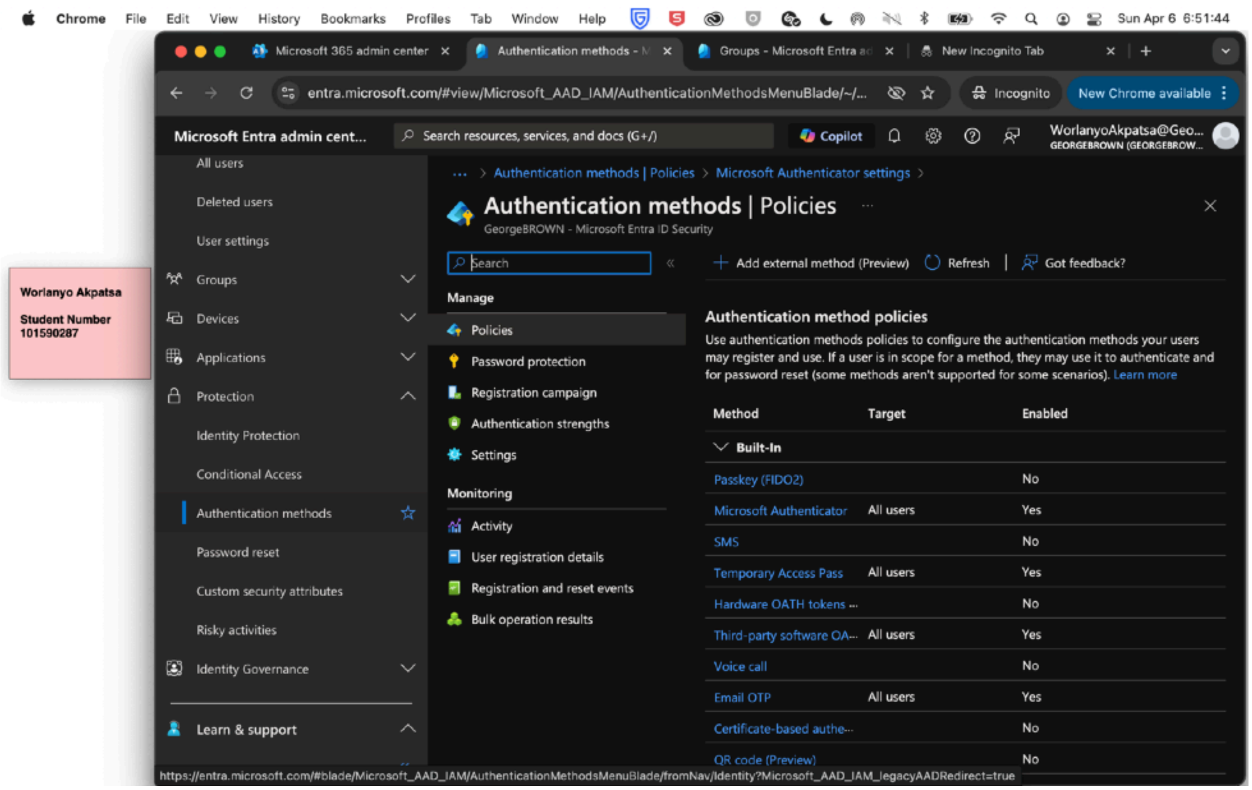


A: Create group called Phone Number MFA and add user Travis to it



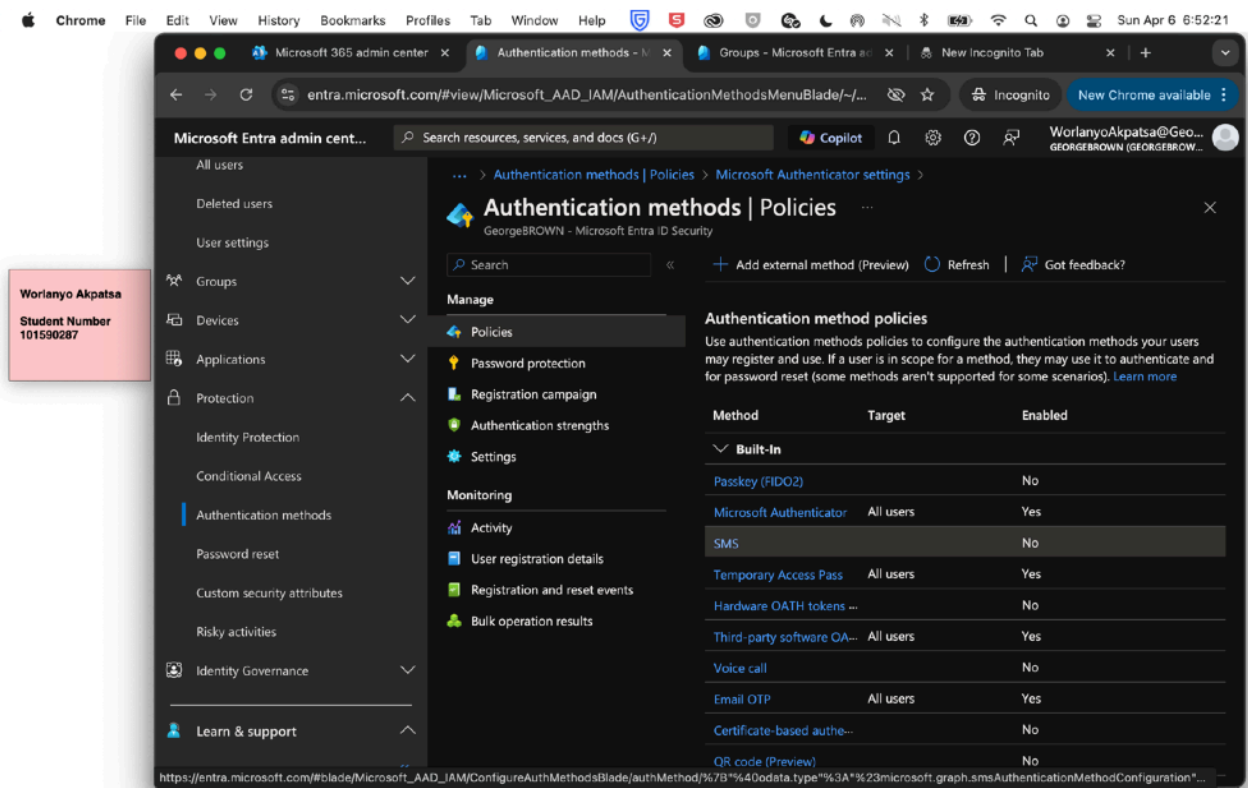


B: Navigate to Protection->Authentication Methods on the left pane



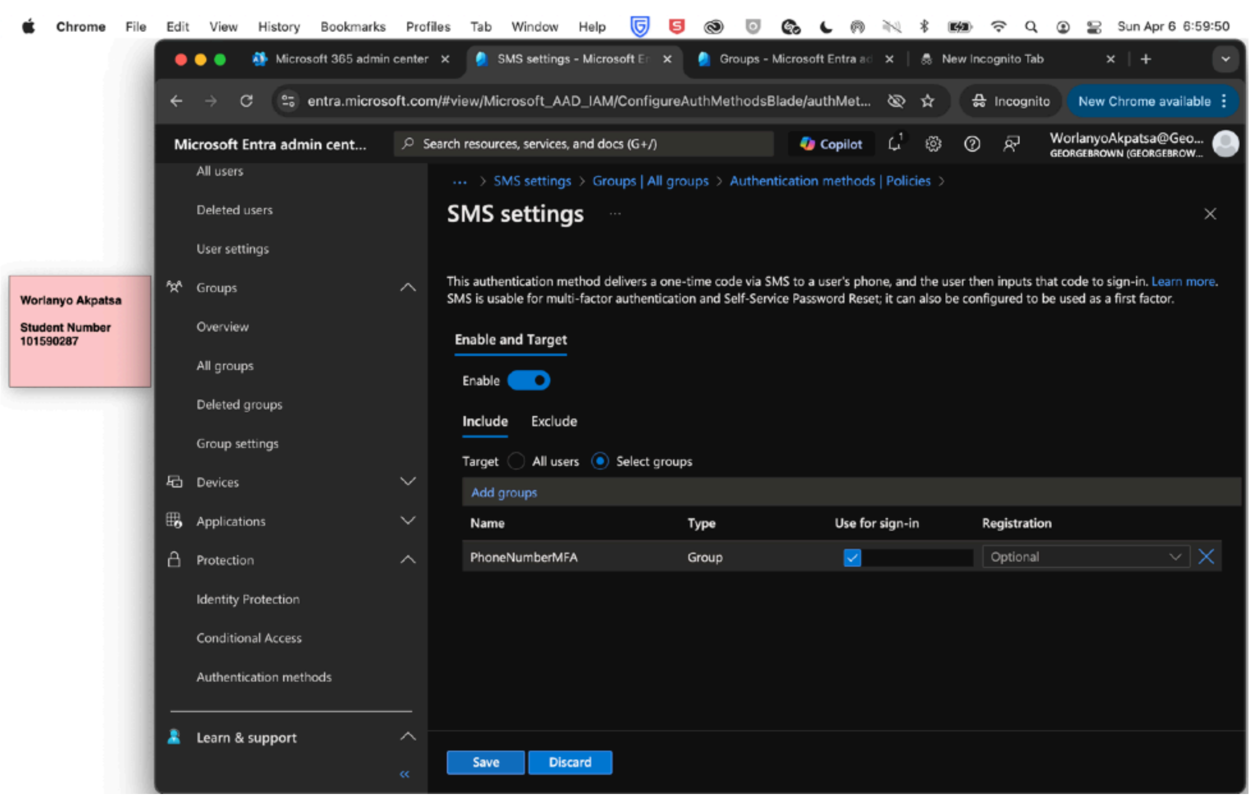
Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

C: Under Policies, Open SMS



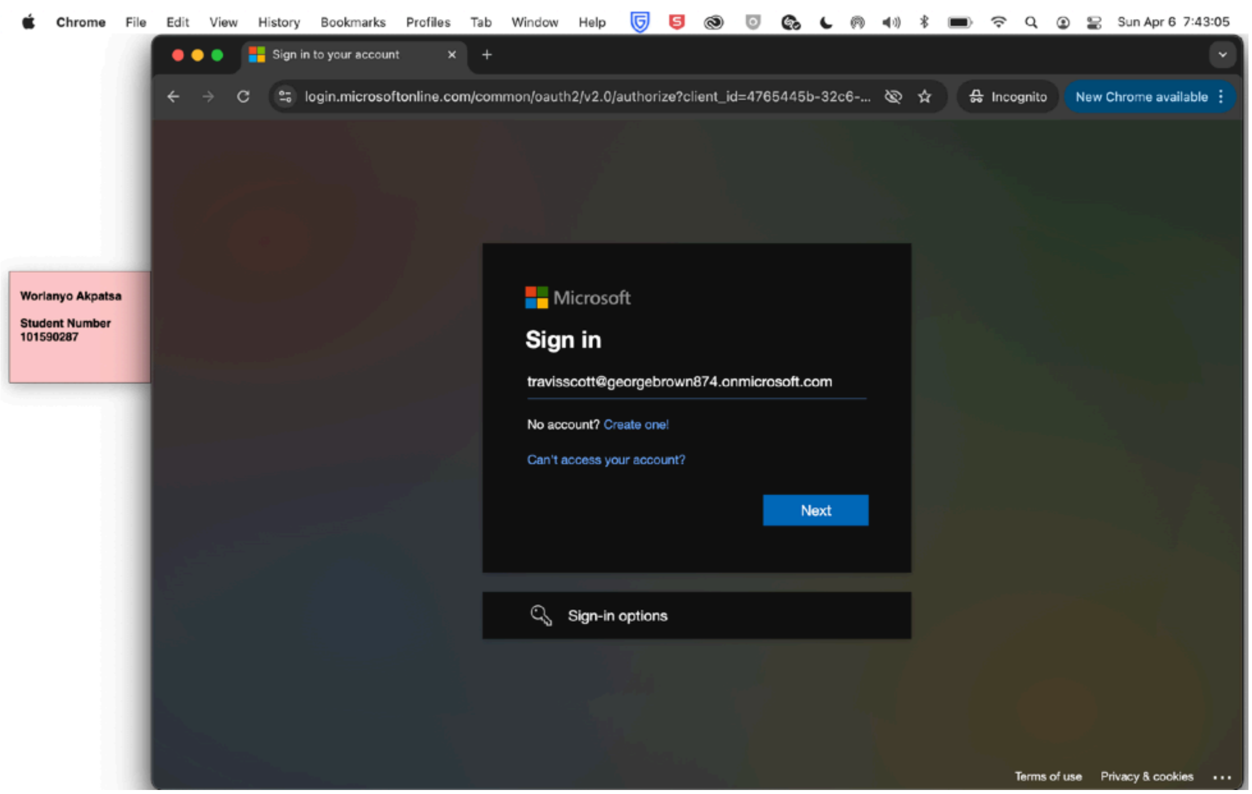
Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

D: Enable and Target SMS to new group, Phone Number MFA



2.3: Simulate a sign-in attempt and verify that MFA is required

A: Navigating to Microsoft and attempting to sign in using new user credentials



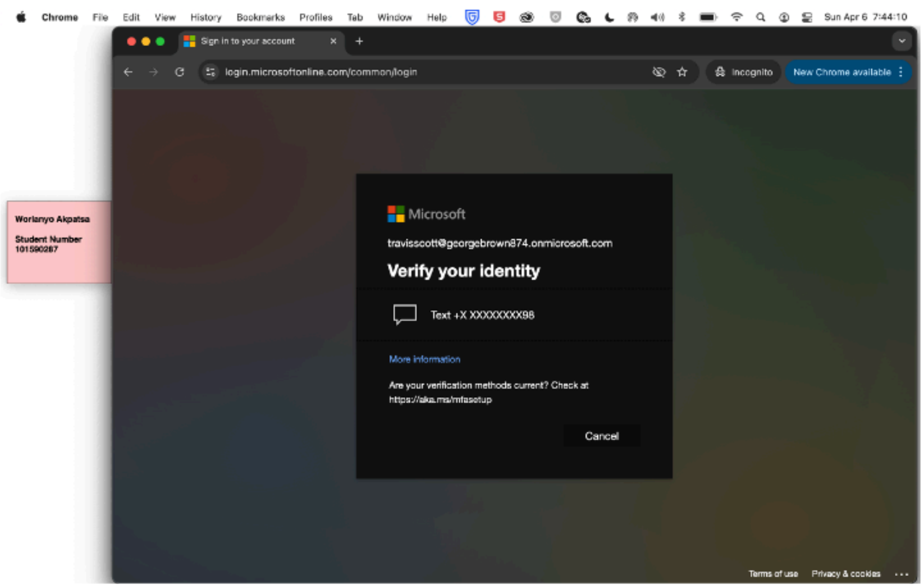
~~~~~~

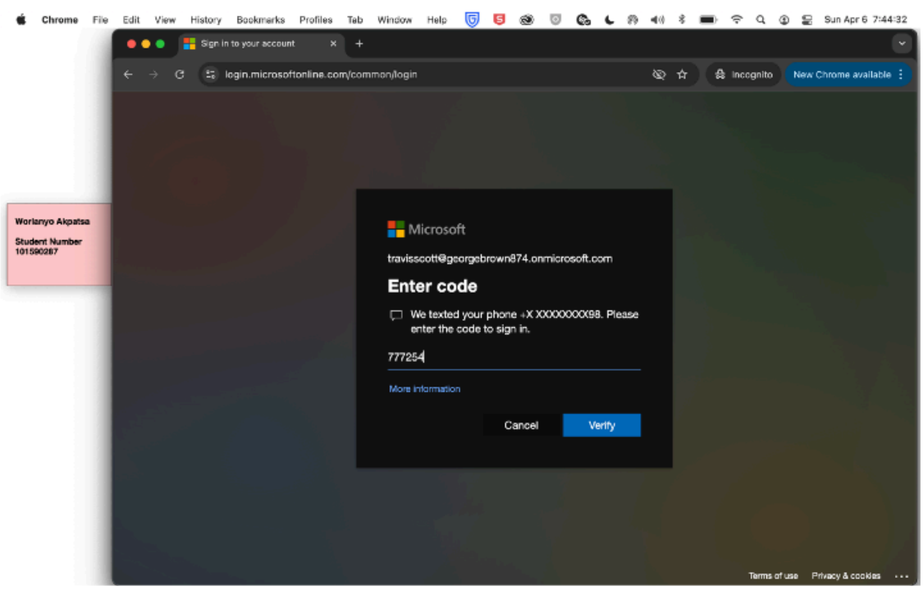
Student Name: Worlanyo Akpatsa
Student ID: 101590287

Term: Winter 2025

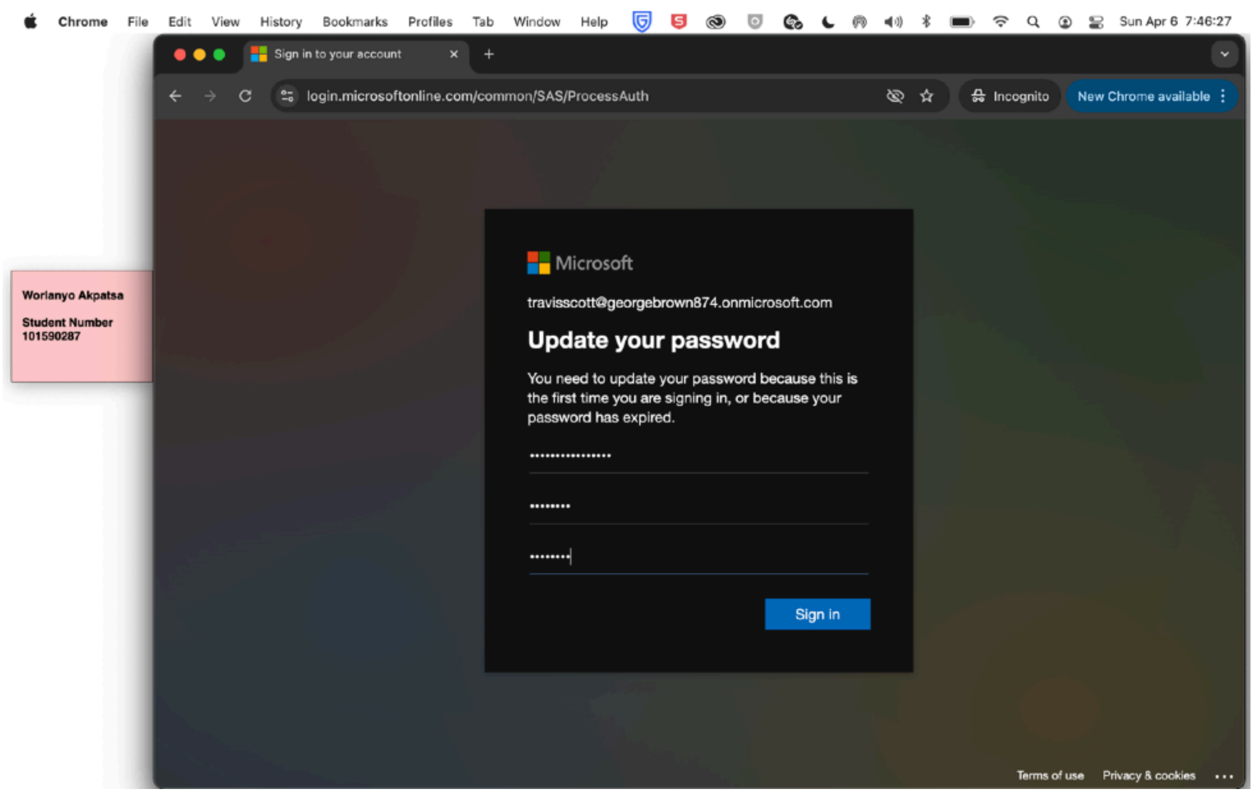
~~~~~~

B: Multi Factor Verification and confirming with code sent to number





C: Updating Password

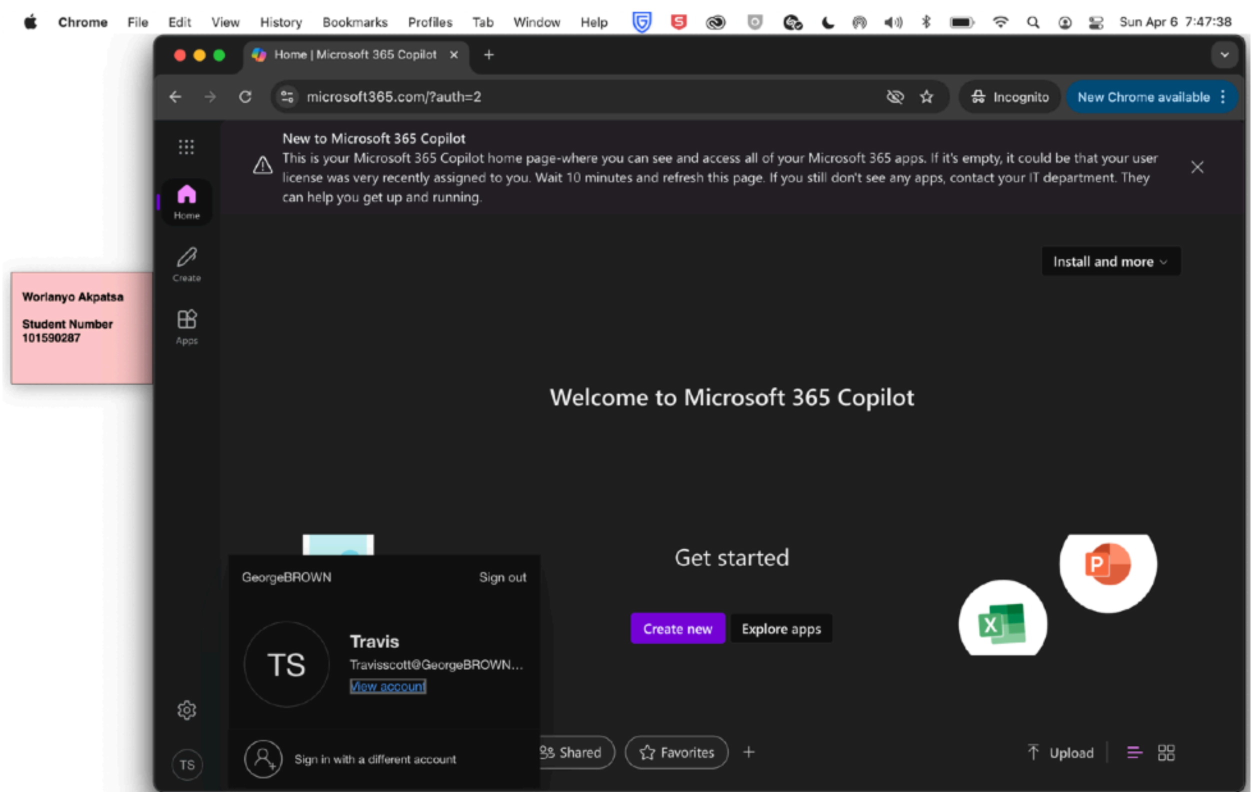


~~~~~~

Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

~~~~~~

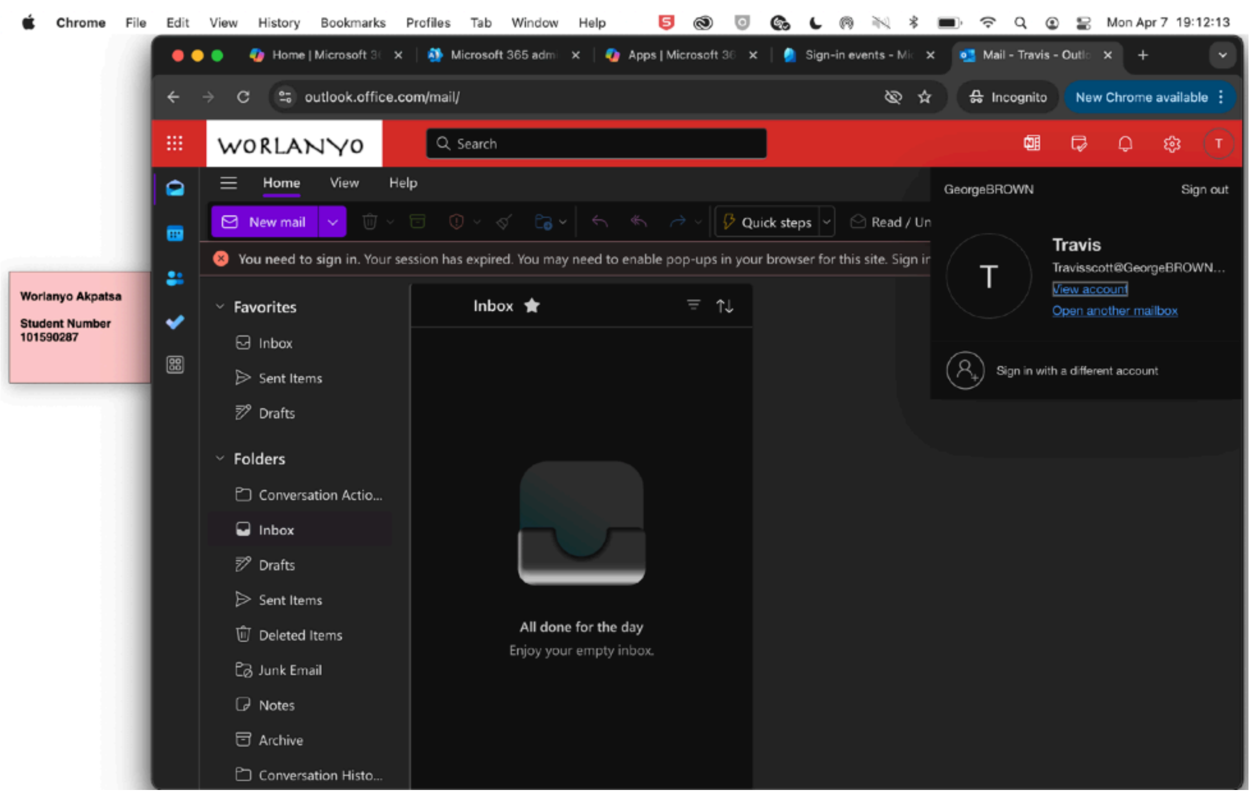
D: Signed in to new user account



Student Name: Worlanyo Akpatsa
Student ID: 101590287

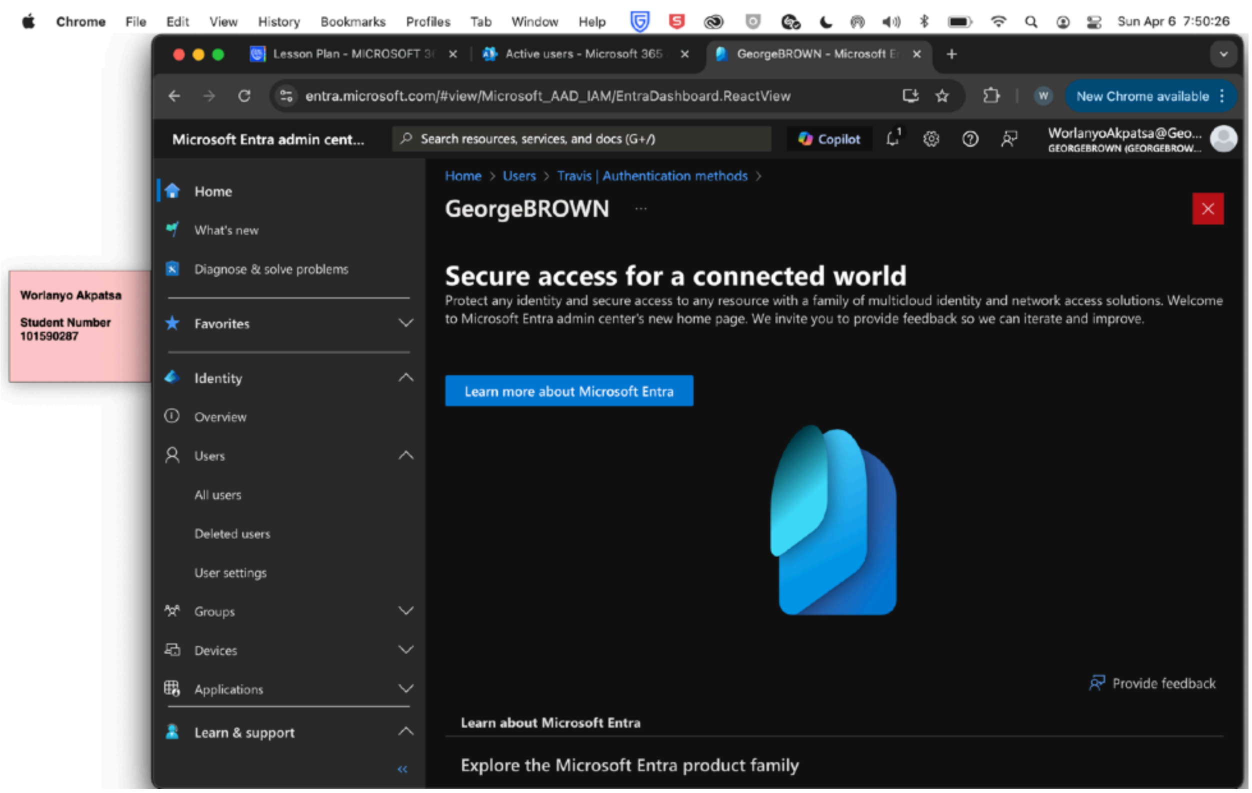
Term: Winter 2025

E: Open Outlook for new user (just to view in sign-in logs)



2.4: Review the sign-in logs to confirm MFA usage

A: Navigate to Entra Admin Homepage

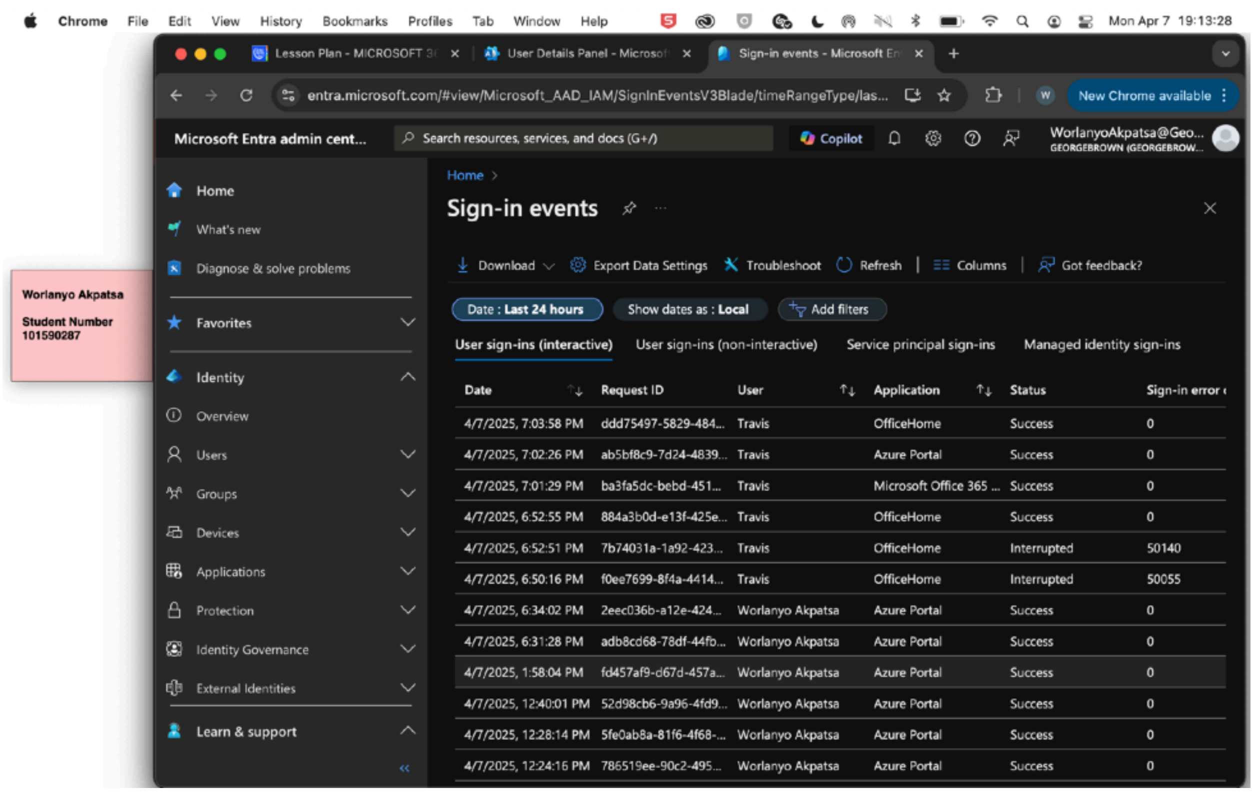


~~~~~~

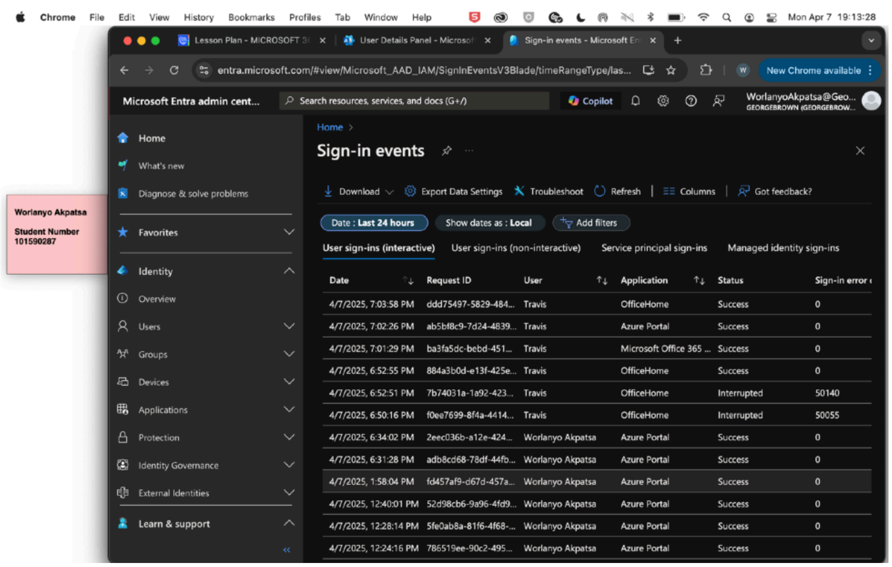
Student Name: Worlanyo Akpatsa
Student ID: 101590287
Term: Winter 2025

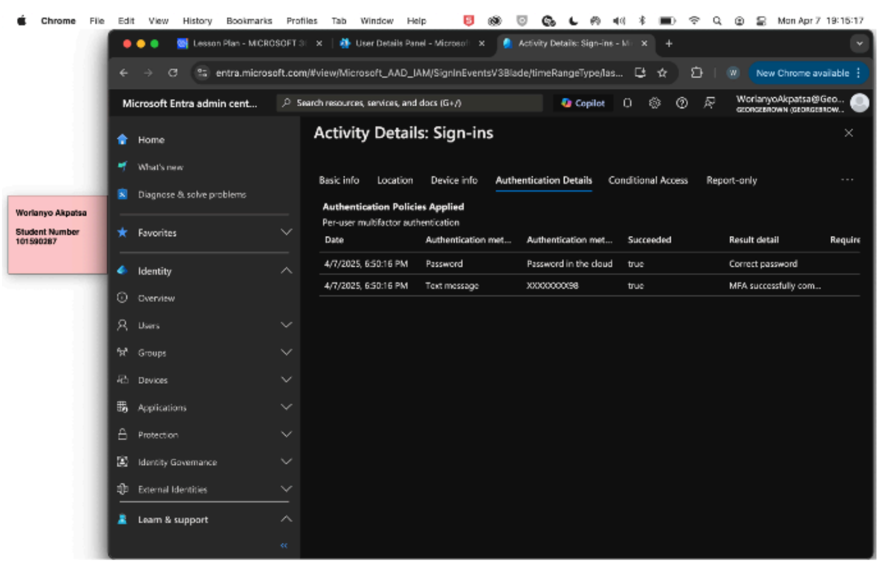
~~~~~~

B: Navigate to “Monitoring & Health -> Sign-in Logs” on left pane



C: Confirming Authentication for new user sign-in (clicking on their first sign in and clicking authentication details)





Task 2 Summary

I must admit I enjoyed doing this task very much because this was the first time in Microsoft Entra that I had to do something we hadn't yet done in any of the admin centers; Multi Factor Authentication.

In everyday life, there are many instances where we use Multi Factor Authentication (MFA) but I have never thought about how it is set up and the various specifications which could be added to it but thankfully, I was able to learn it.

To begin, I had to enable MFA fora user in my Azure AD. To do this, I had to first navigate to All users on the left pane and then click on the three dots (…) in the right side of the header. This opens a drop down box where I chose Per-User MFA.

When this window opens, all the users are listed. I clicked the checkmark beside the user created in task 1 and clicked enable MFA to enable it for that user.

Next I had to configure the MFA settings to use a phone number for verification which made me learn a lot about the verification system and the types that could be used.

To start, I navigated to all users and selected my task 1 created user. This opens a window with his name (Travis) as the main header. Under this, there are several subheaders. I clicked on the "Authentication methods" header for him and chose to add a new authentication methods. When you click this, a drop down header comes and I selected phone number. After this, I added the phone details and successfully added his number as a method of authentication.

This was really fascinating to do so it got me eager and I went to google to try to find other authentication settings. As seen above in my work, I added my user to a group and named it Phone Number MFA. Next, I navigated to protection on the left pane and chose authentication methods. Under this, I clicked on policies and then was met with several modes of authentication.

In this instance, I chose SMS and targeted this to the group I created which has my user.

As a result, when it was time to sign in to Microsoft using the new user, I was prompted with MFA which sent a text message to the number I provided showing that my MFA configuration worked.

Finally; the tasked asked to view the sign-in logs to confirm MFA usage which I found really fascinating because you can see every users log ins.

To begin, I navigated to Monitoring & Health on the left pane and chose Sign-in Logs. Here, it is a page full of the different sign ins which have taken place by each user on the directory.

I clicked on the recent sign in that I did for the created user. It opens a window where I then chose Authentication Details. Here, the MFA for my recent sign in is showed and labelled successful.

This was a very entertaining task to do and I'm glad I learnt a lot about MFA.

~~~~~~

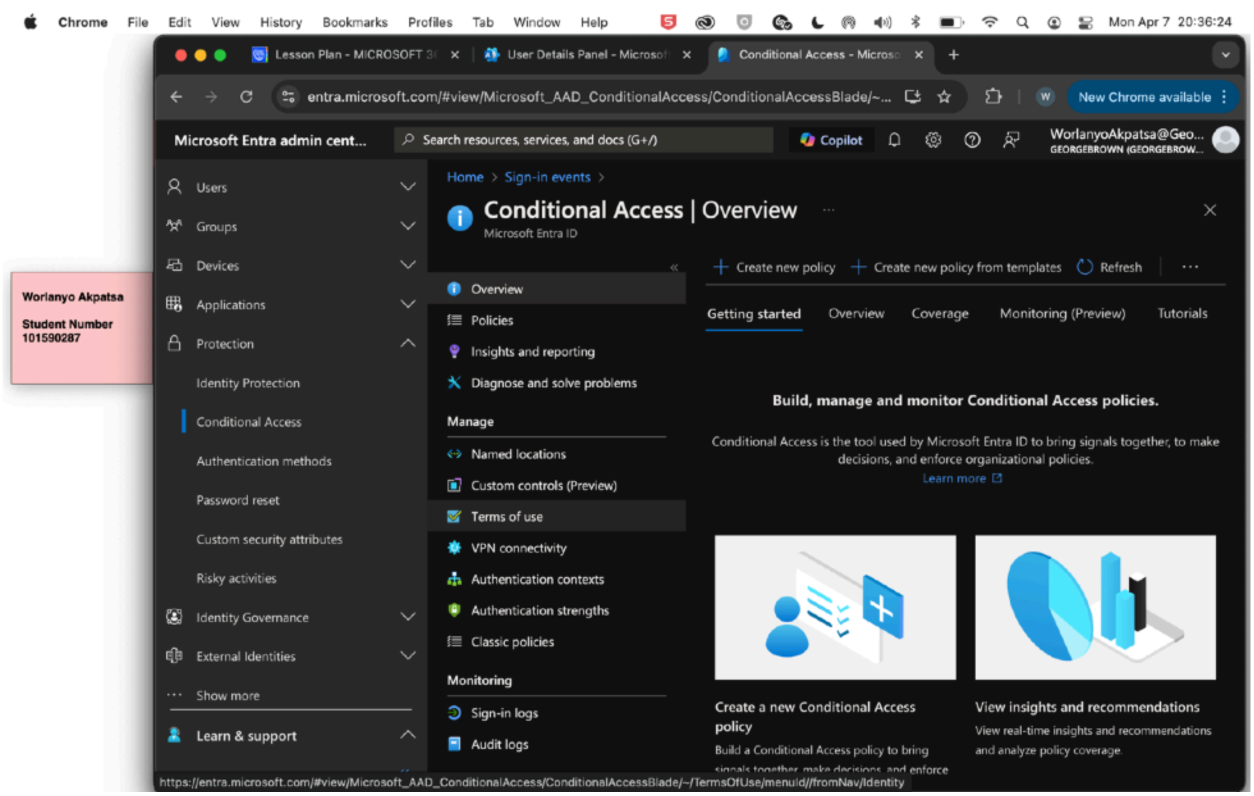
Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

~~~~~~

TASK 3: CREATE AND MANAGE CONDITIONAL ACCESS POLICIES

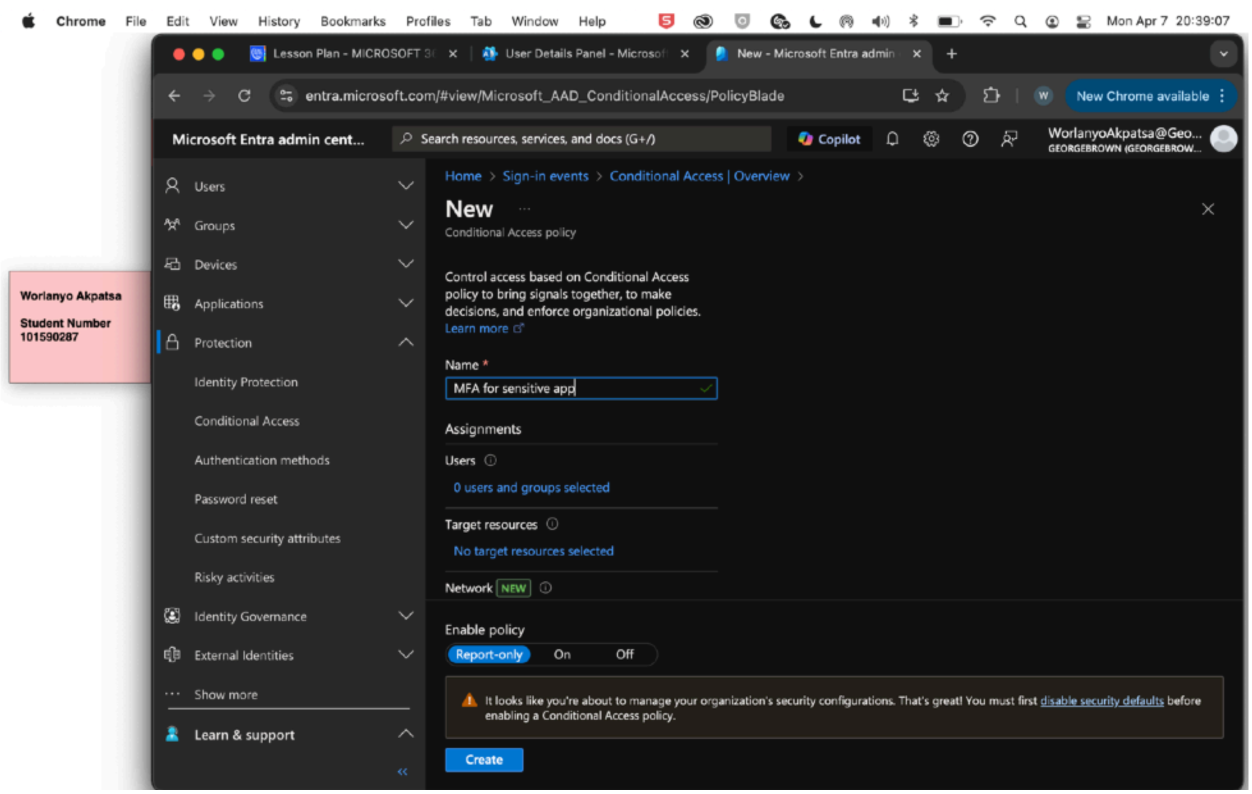
3.1: Access the protection section in the Entra admin and go to Conditional Access

A: Navigate to protection on the left pane and choose Conditional Access

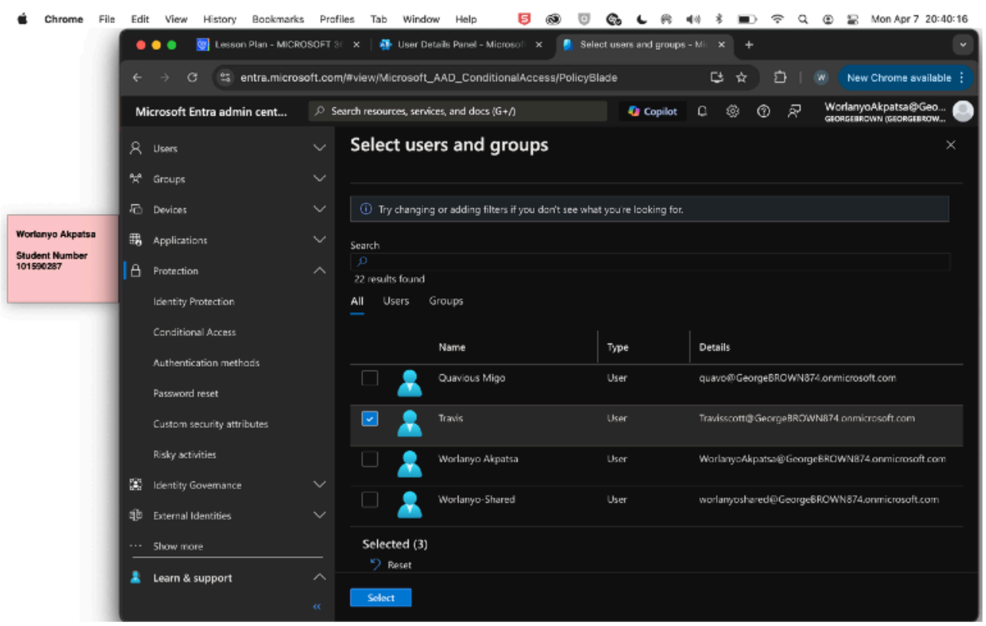


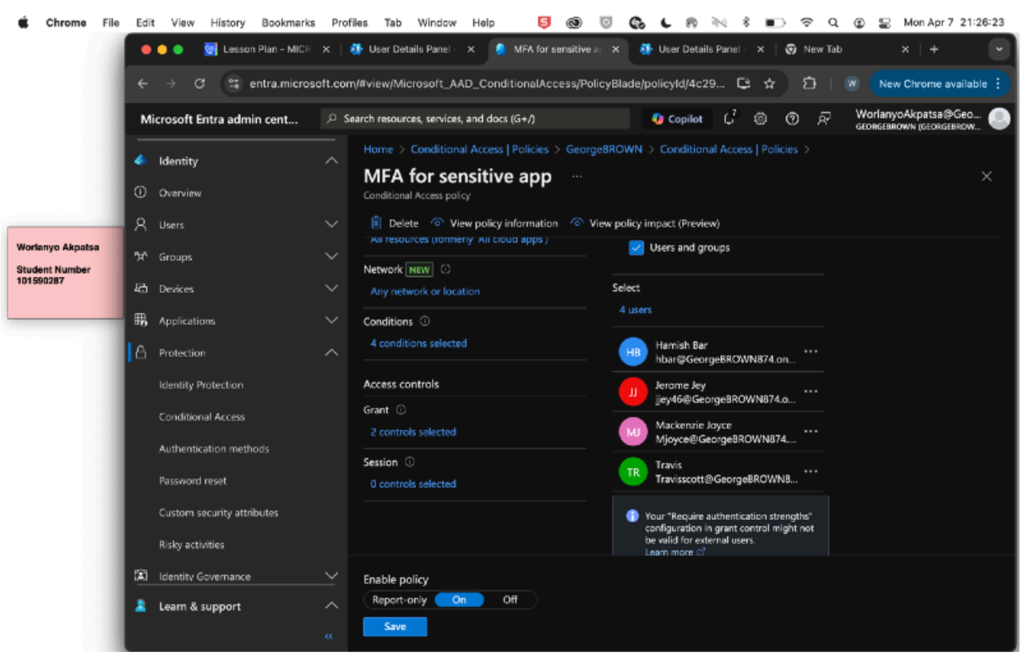
3.2: Create a new conditional access policy for a specific group of users

A: Click new policy and name it

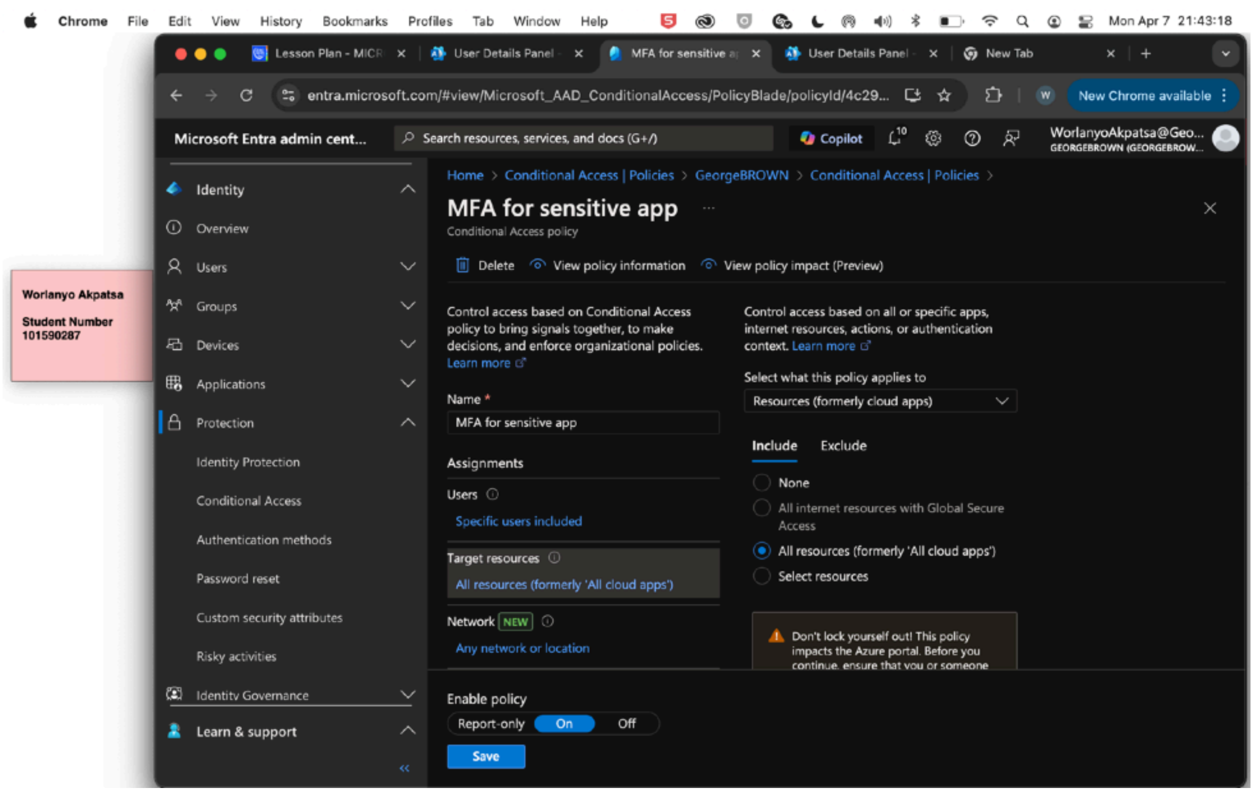


B: Assign policy to specific users





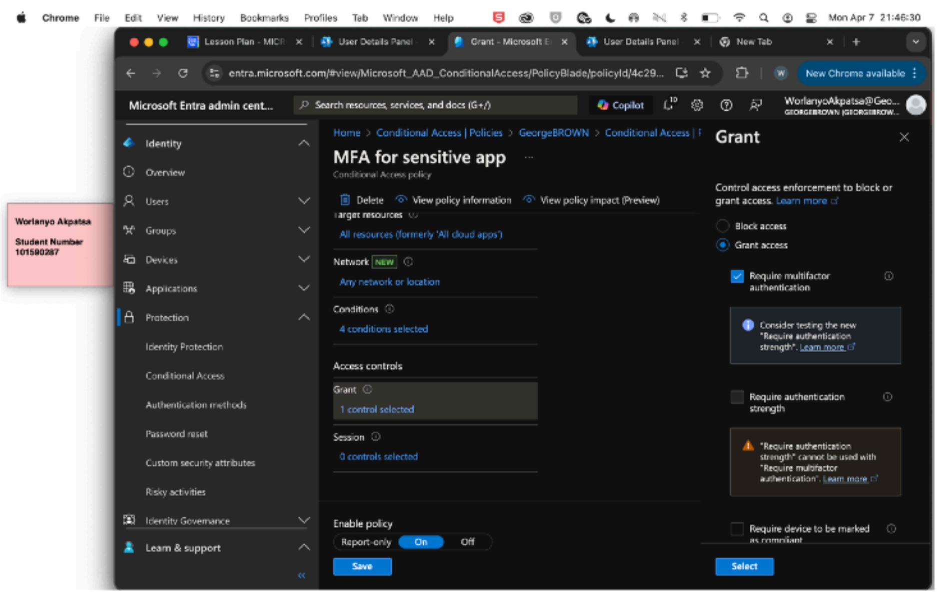
C: Selecting target resources (All Cloud Apps) by clicking on “No target resources selected”

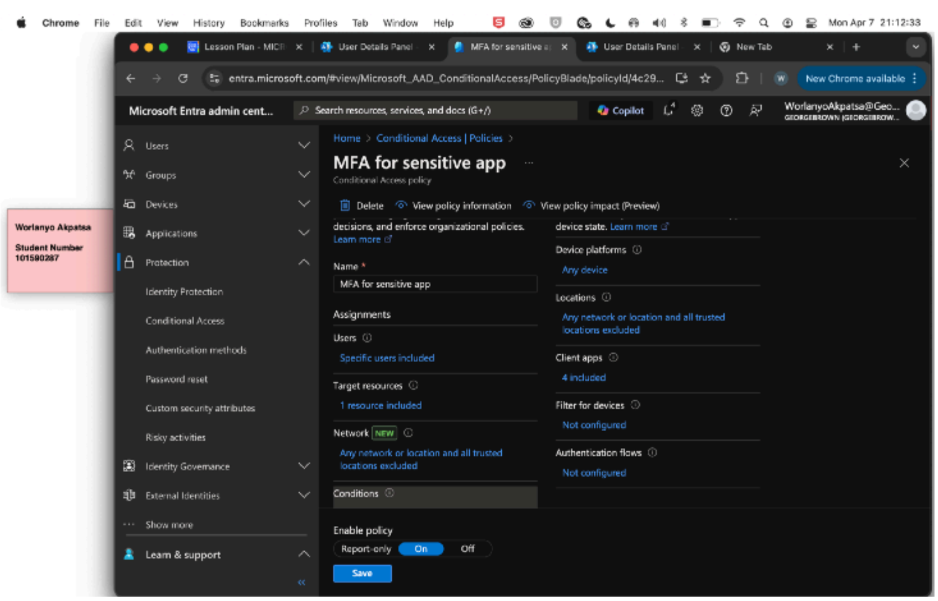


Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

3.3: Set conditions that require MFA when accessing a sensitive application

D: Editing Access Controls to require Multi-Factor Authentication

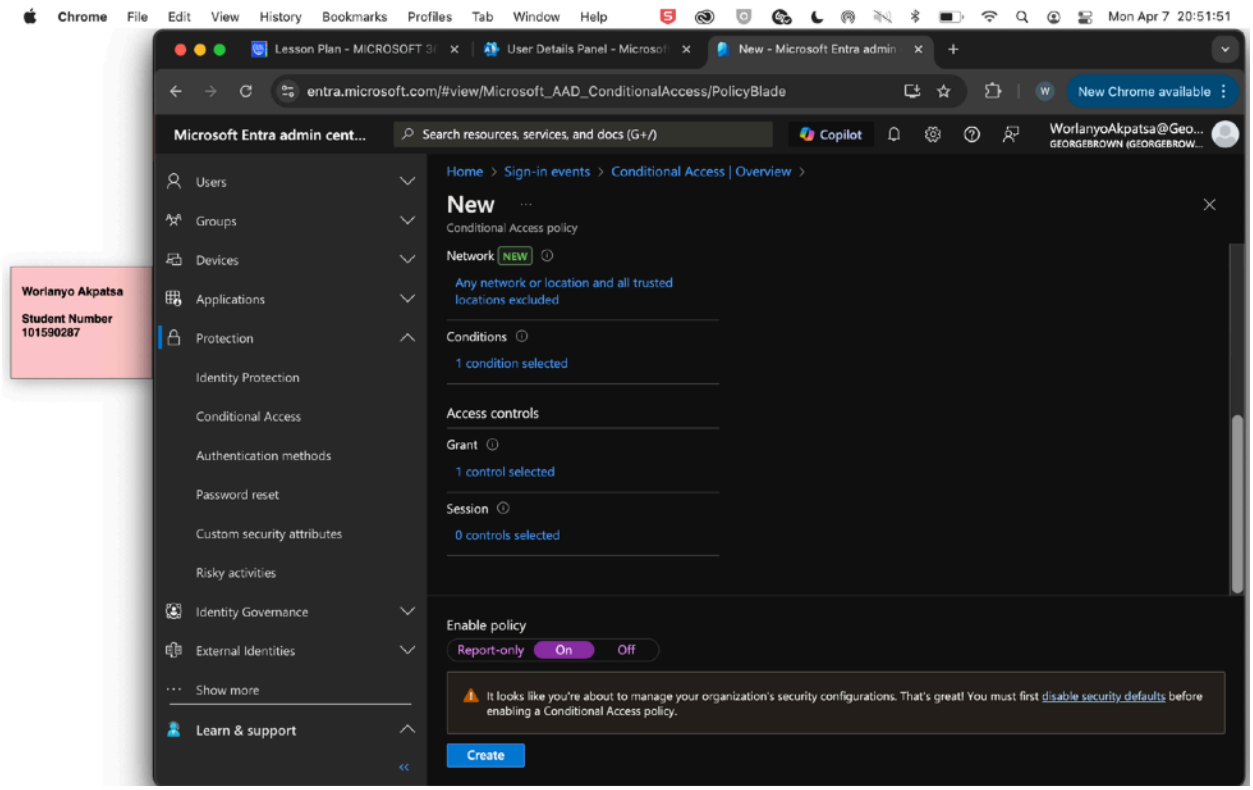




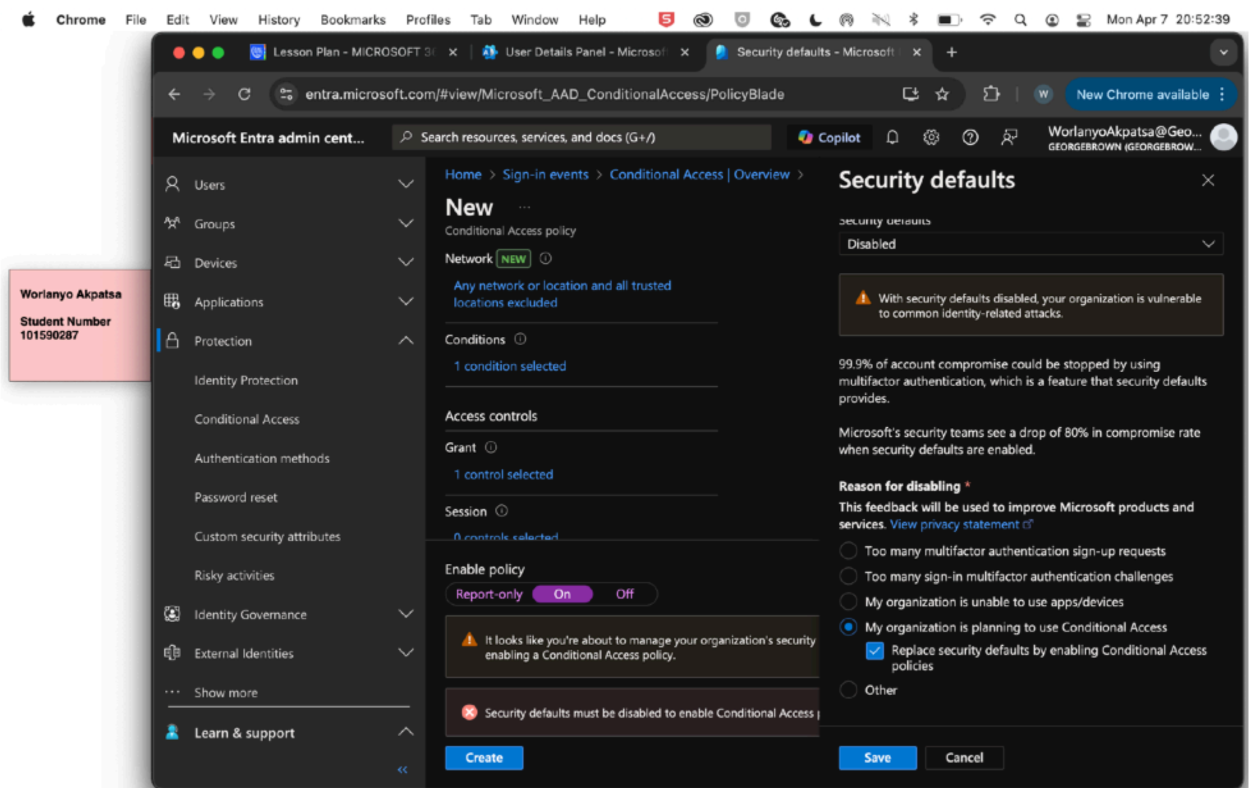
Student Name: Worlanyo Akpatsa
Student ID: 101590287

Term: Winter 2025

E: Toggling Enable Policy to “On”



F: Disabling Security Defaults for Organization to enable Conditional Access

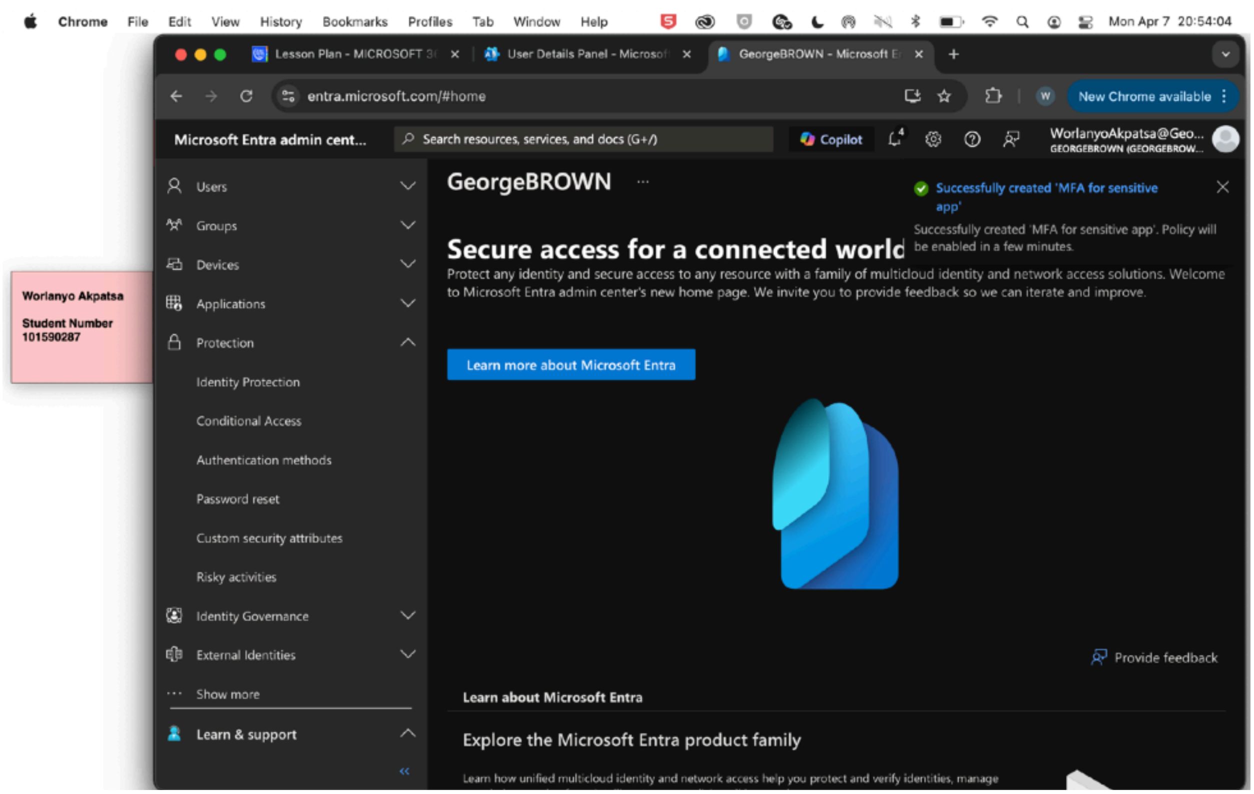


~~~~~~

Student Name: Worlanyo Akpatsa   Term: Winter 2025
Student ID: 101590287

~~~~~~

G: Successfully created Conditional Access Policy “MFA for sensitive app”

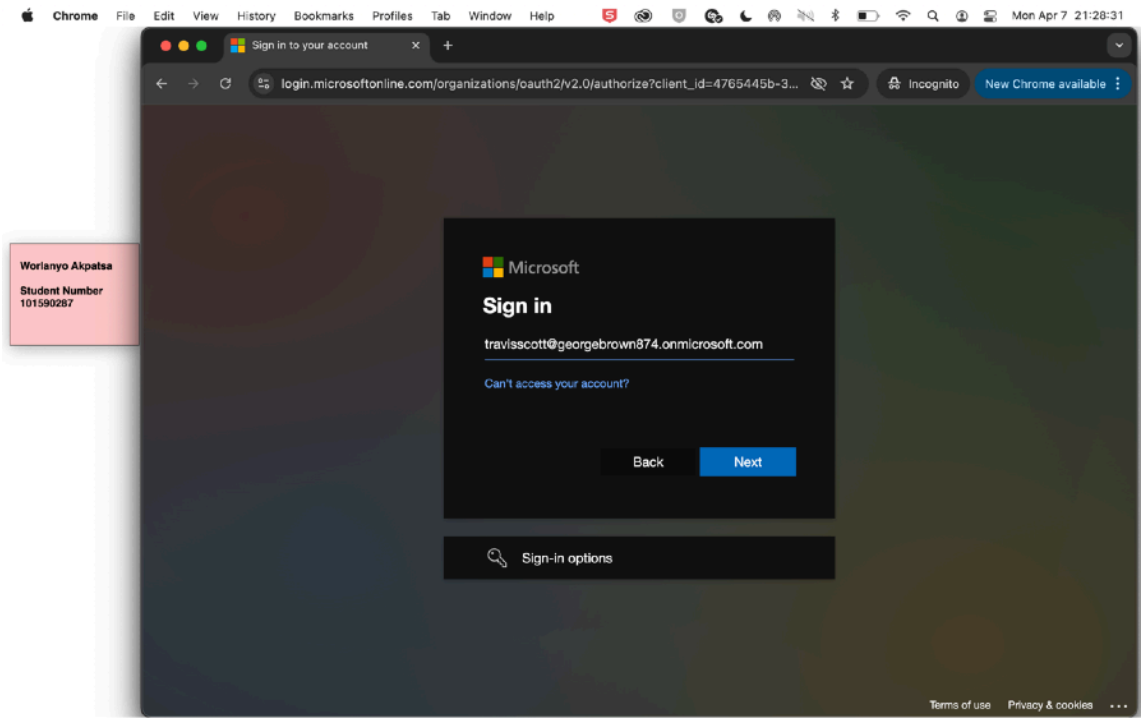


Student Name: Worlanyo Akpatsa
Student ID: 101590287

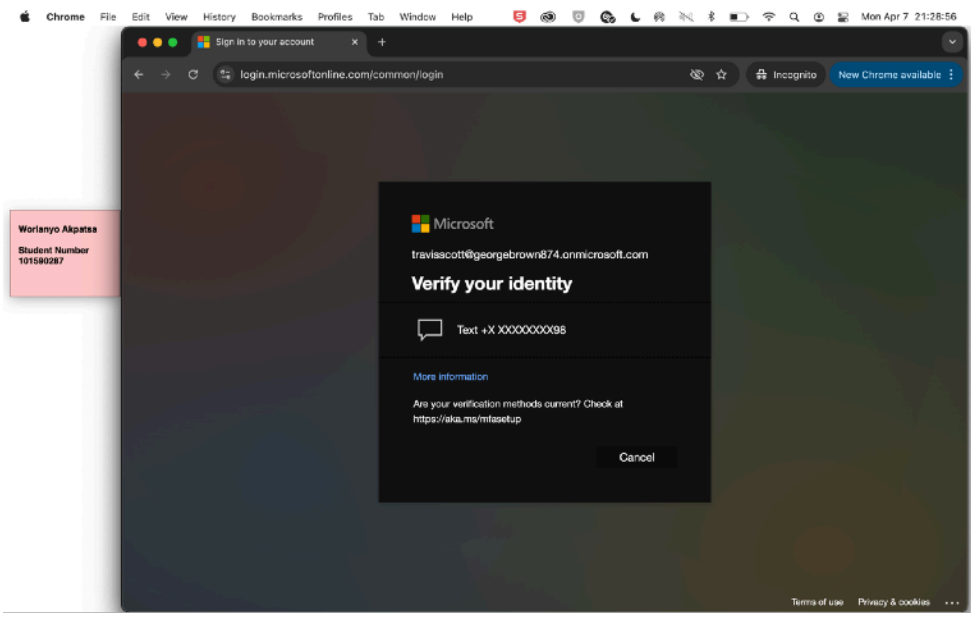
Term: Winter 2025

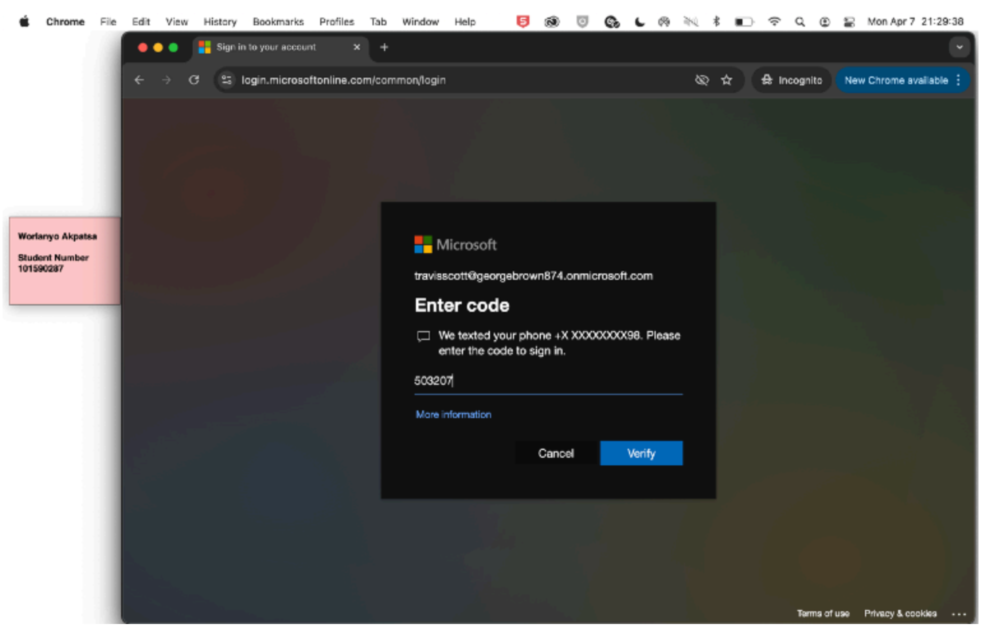
3.4: Test the policy by attempting to access the application from a user account

A: Logging in as one of the users into Microsoft 365



B: MFA


Chrome File Edit View History Bookmarks Profiles Tab Window Help
Mon Apr 7 21:28:56
Sign in to your account
login.microsoftonline.com/common/login
Incognito
New Chrome available
Worlanyo Akpatsa
Student Number
101590287
Microsoft
travisscott@georgebrown874.onmicrosoft.com
Verify your identity
Text +X XXXXXXXX98
More information
Are your verification methods current? Check at https://aka.ms/mfasetup
Cancel
Terms of use
Privacy & cookies

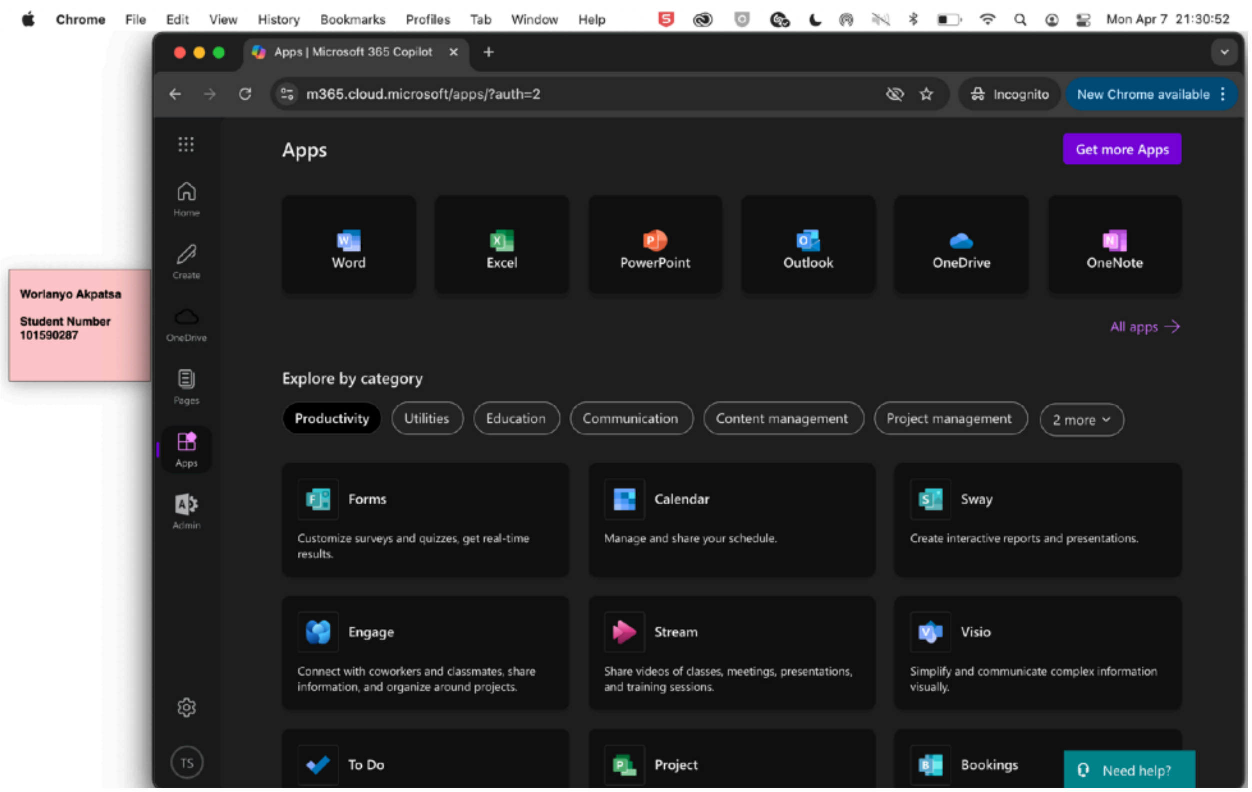

Chrome File Edit View History Bookmarks Profiles Tab Window Help
Mon Apr 7 21:29:38
Sign in to your account
login.microsoftonline.com/common/login
Incognito
New Chrome available
Worlanyo Akpatsa
Student Number
101590287
Microsoft
travisscott@georgebrown874.onmicrosoft.com
Enter code
We texted your phone +X XXXXXXXX98. Please enter the code to sign in.
503207
More information
Cancel
Verify
Terms of use
Privacy & cookies

~~~~~~

Student Name: Worlanyo Akpatsa　　　　Term: Winter 2025
Student ID: 101590287

~~~~~~

C: Apps



Task 3 Summary

Task 3 took me into the policy creation process where I had to create a conditional policy to enable MFA for apps.

To start, I had to navigate on the left pane to protection and under it, choose conditional access. Then in this window, I chose "create new policy".

I named my policy MFA for sensitive apps.

Next thing was the assignment where I had to choose the users who this policy would affect. After this, I selected the target resources this policy was going to affect. Just for the sake of the lab, I chose Microsoft Admin Portals as we have been accessing them all this time.

Next thing to do in configuration is explore the access controls. Under grant, I chose Require Multifactor Authentication.

I then toggled enable policy to on and saved it.

By the way, before I was able to toggle it to on, I had to disable security defaults to allow my conditional access policy to function.

Then I logged in to Microsoft as one of the selected users for my conditional policy and before I could even use an app, it was asking for Multi Factor authentication showing that my policy was successful.

~~~~~~

Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

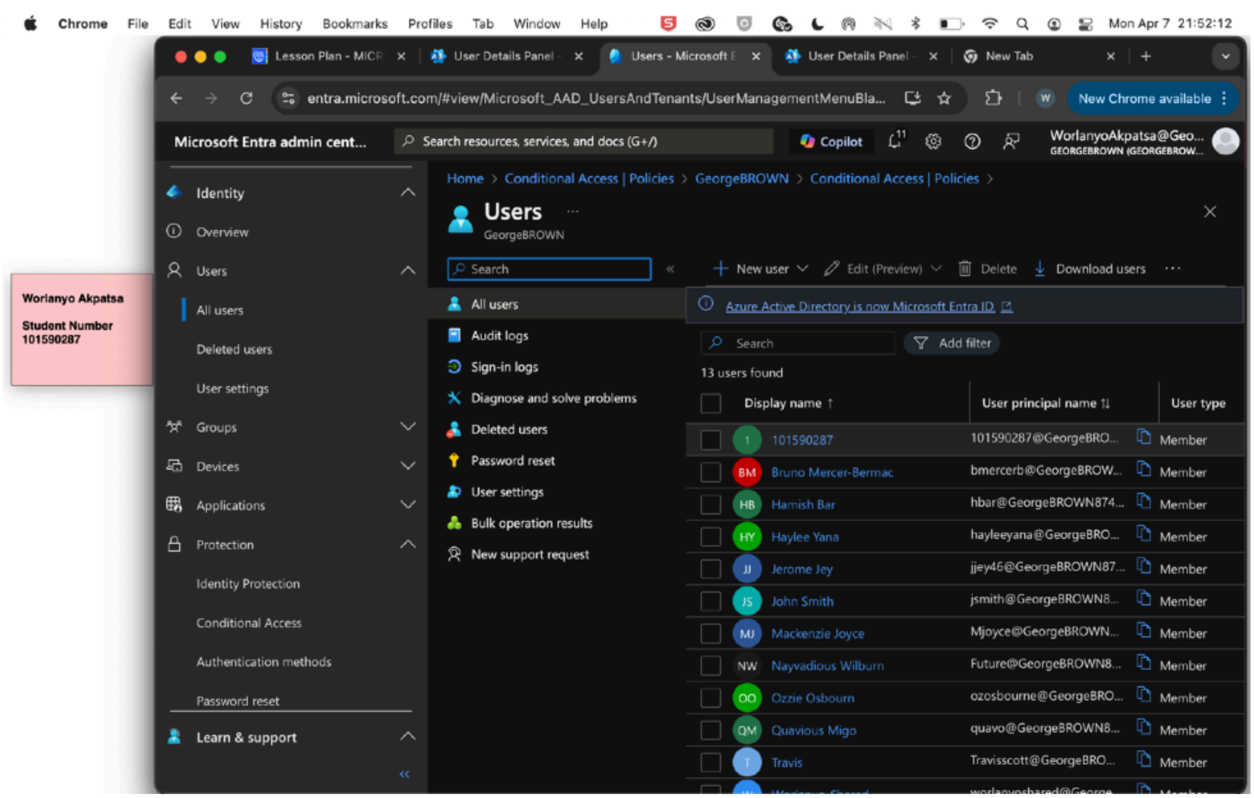
~~~~~~

TASK 4: ASSIGN AND MANAGE USER ROLES

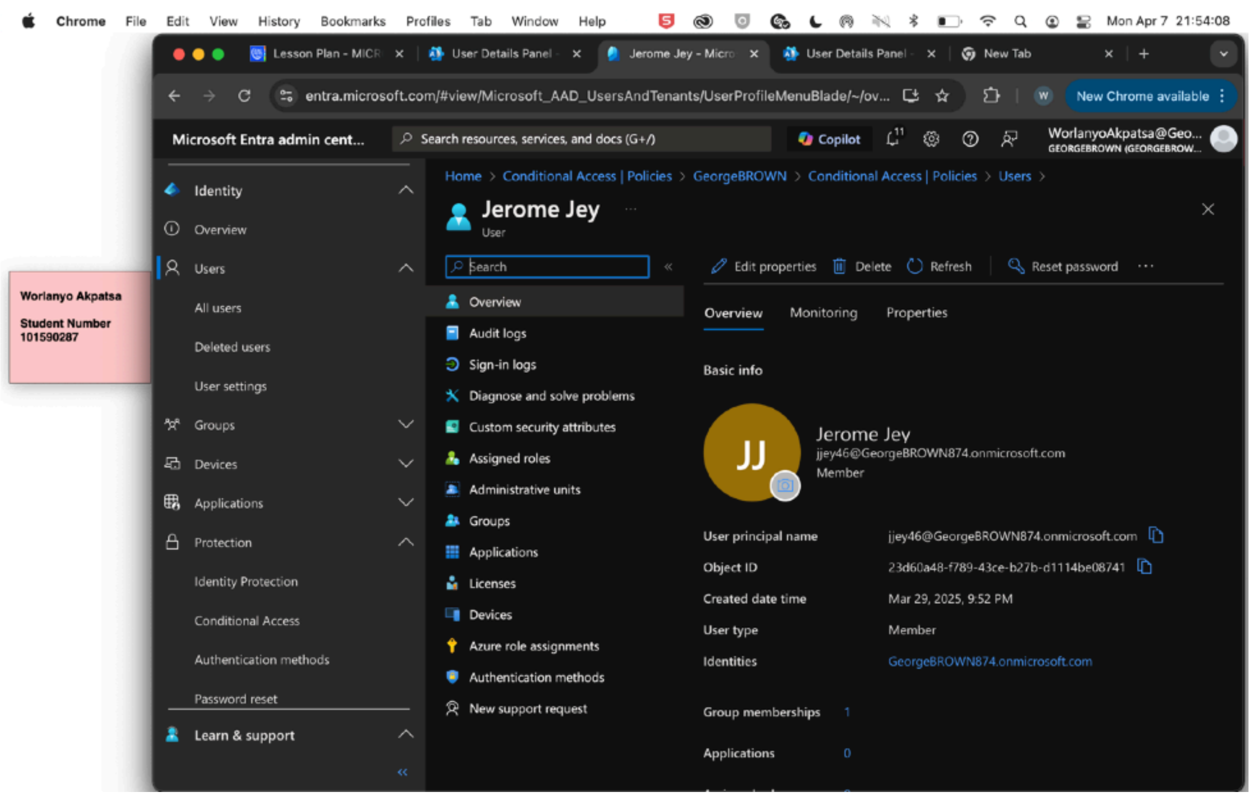
4.1: Assign an admin role to a user

4.2: Verifying the user's permissions and access levels

A: Navigate to users->all users



B: Select a user (Jerome Jey who is a regular user with no admin rights)

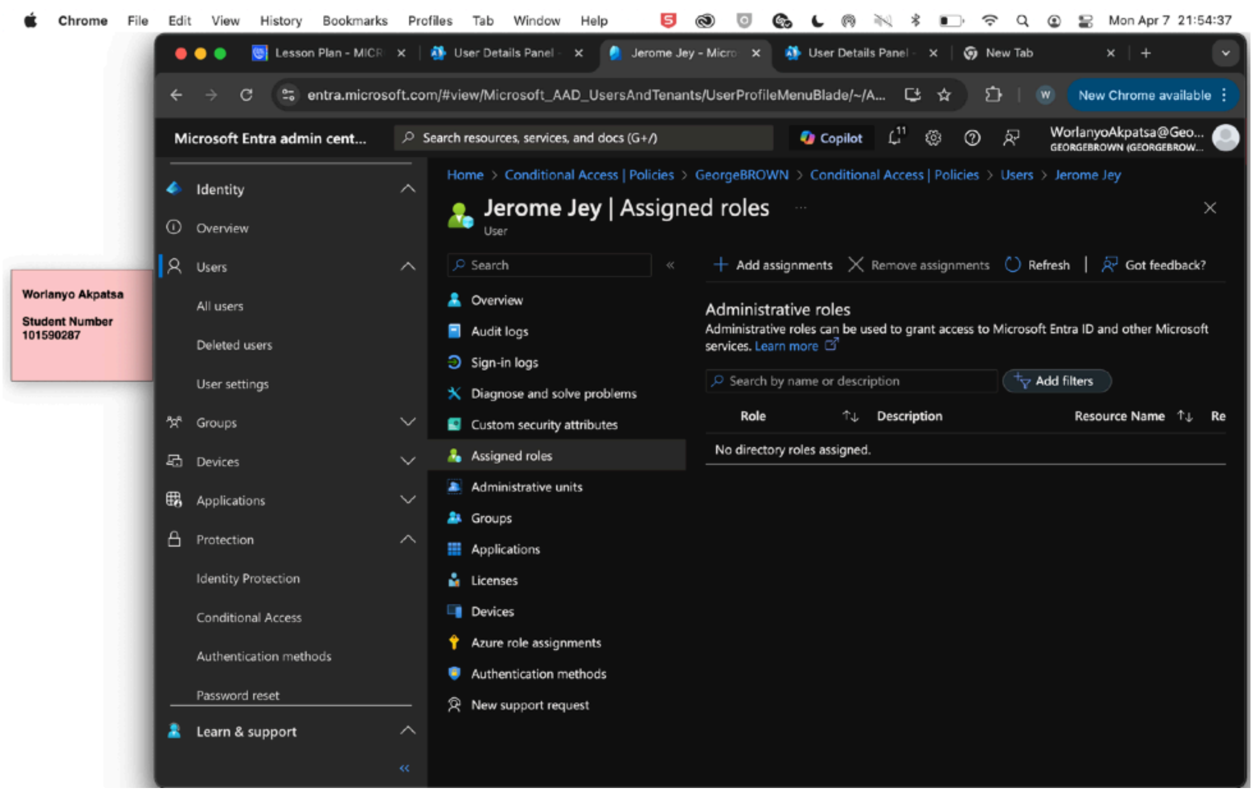


~~~~~~

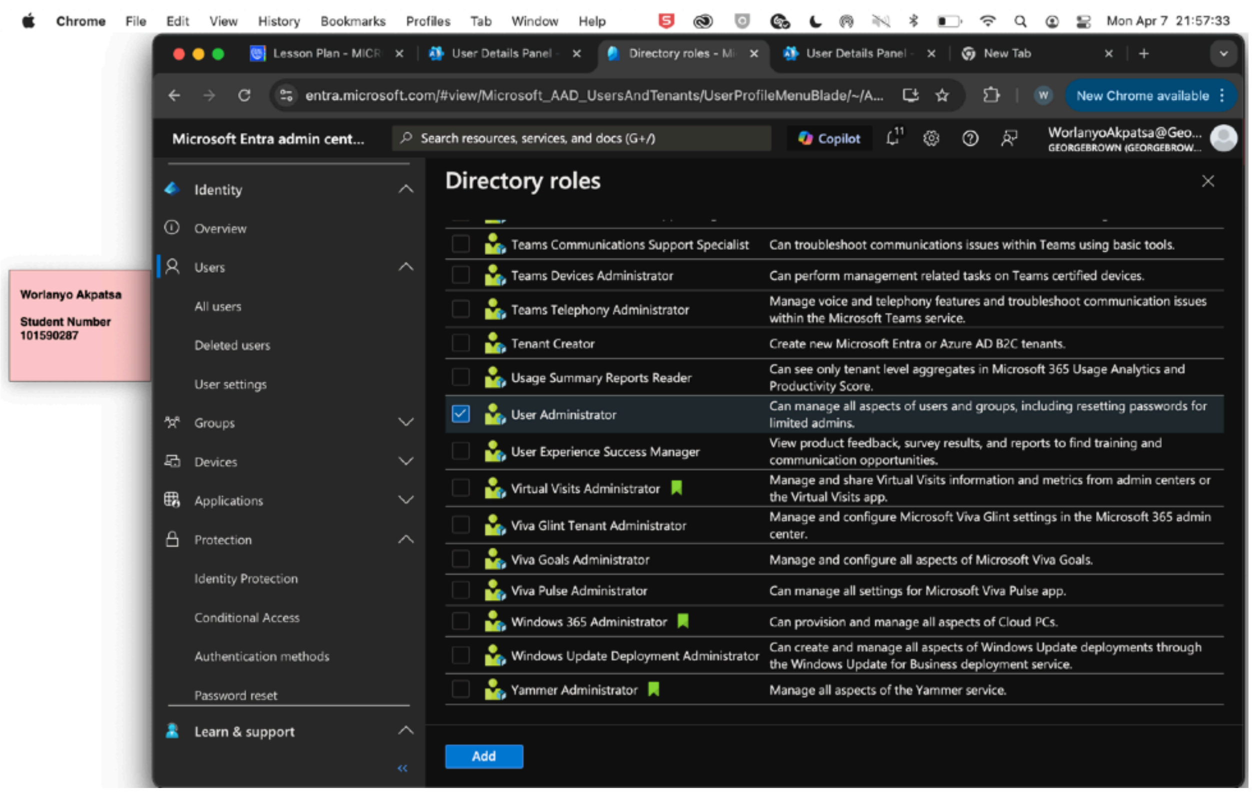
Student Name: Worlanyo Akpatsa Term: Winter 2025
Student ID: 101590287

~~~~~~

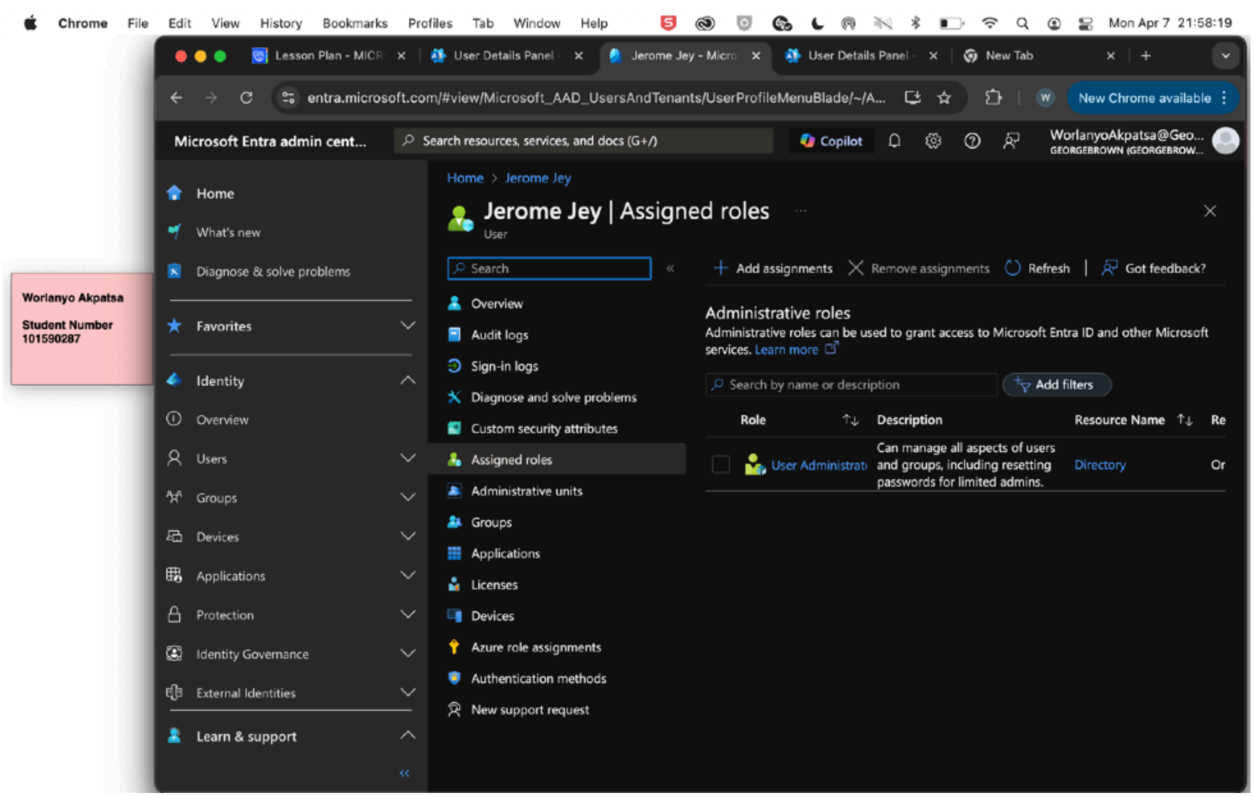
C: Navigate to Assigned Roles



D: Add role assignment (user Administrator)



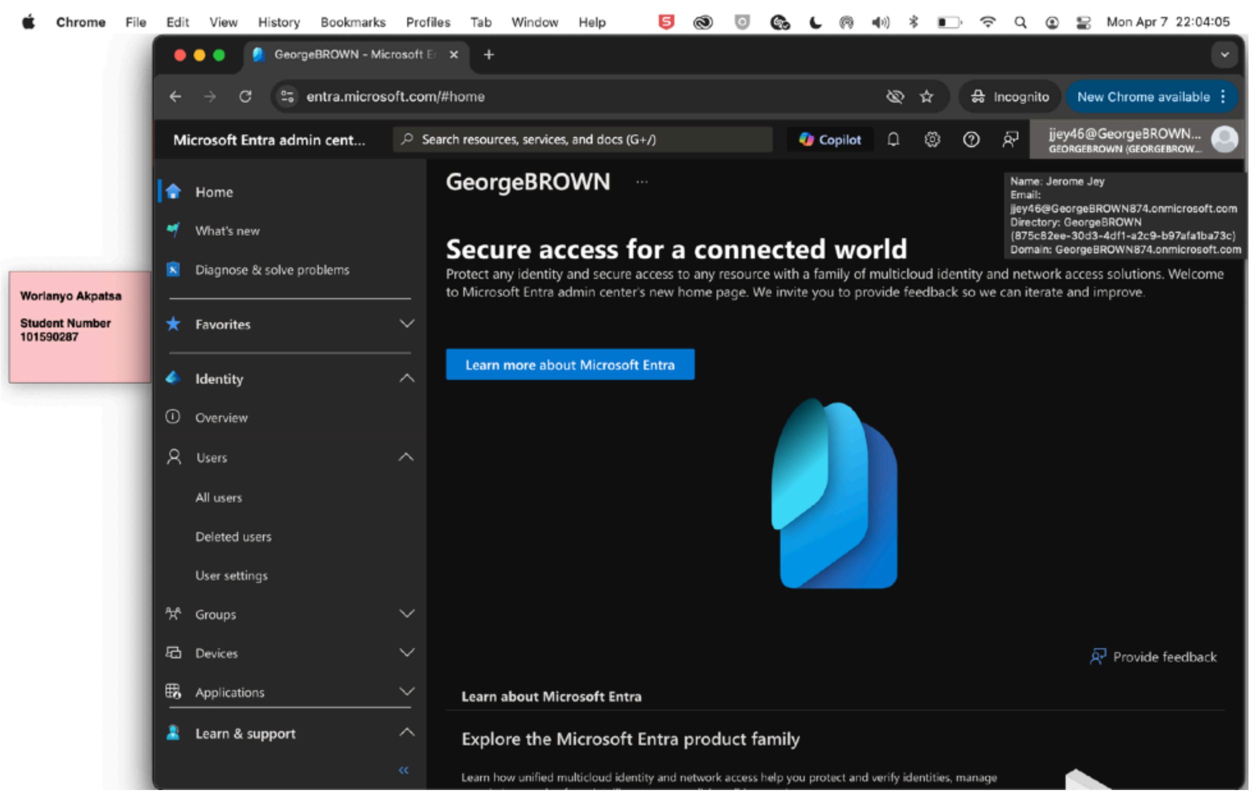
E: Confirmed Assigned Role



Now I will prove that this admin role works by signing in to entra on another browser using the user's credentials. As he is a user administrator, he will be able to create and edit users on entra.

After, I will remove the assigned role and sign in to entra again. I am very sure I will not be able to use this user's account to do any user administrator activity.

A: Sign in to entra of user admin Jey (his homepage)



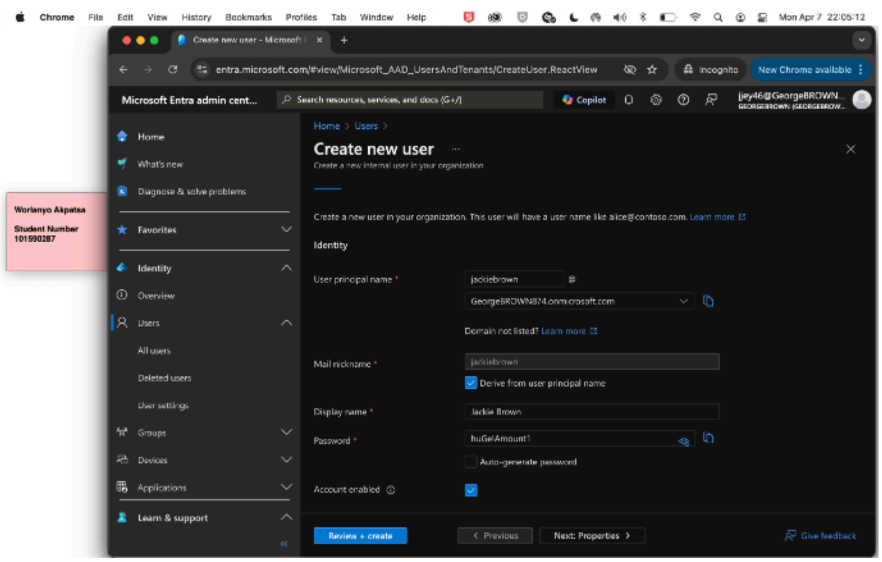
~~~~~~

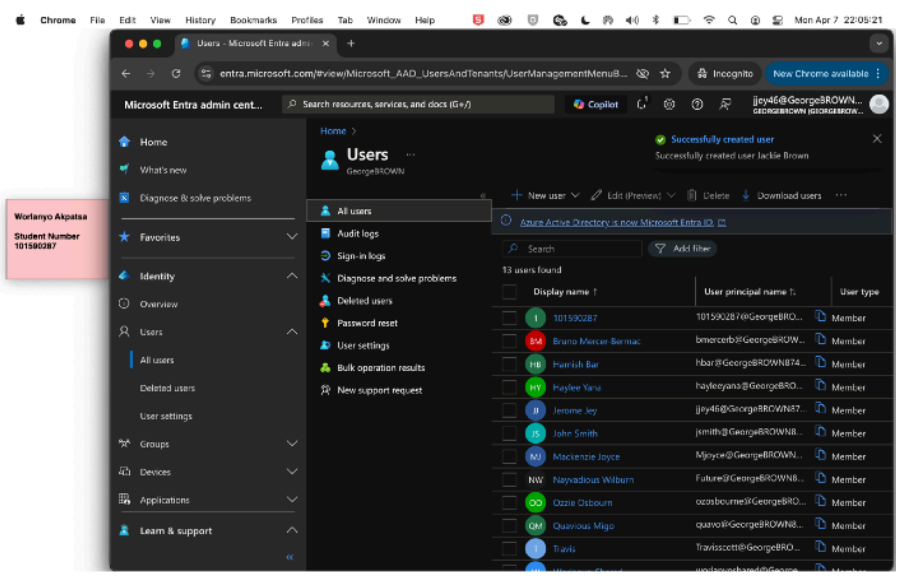
Student Name: Worlanyo Akpatsa
Student ID: 101590287

Term: Winter 2025

~~~~~~

B: Create user using Jey's entra admin account



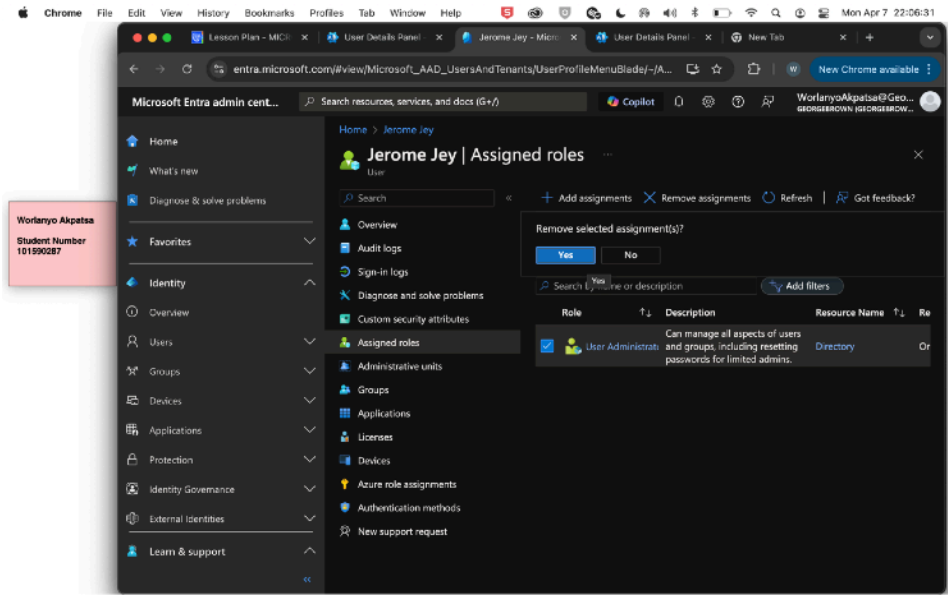


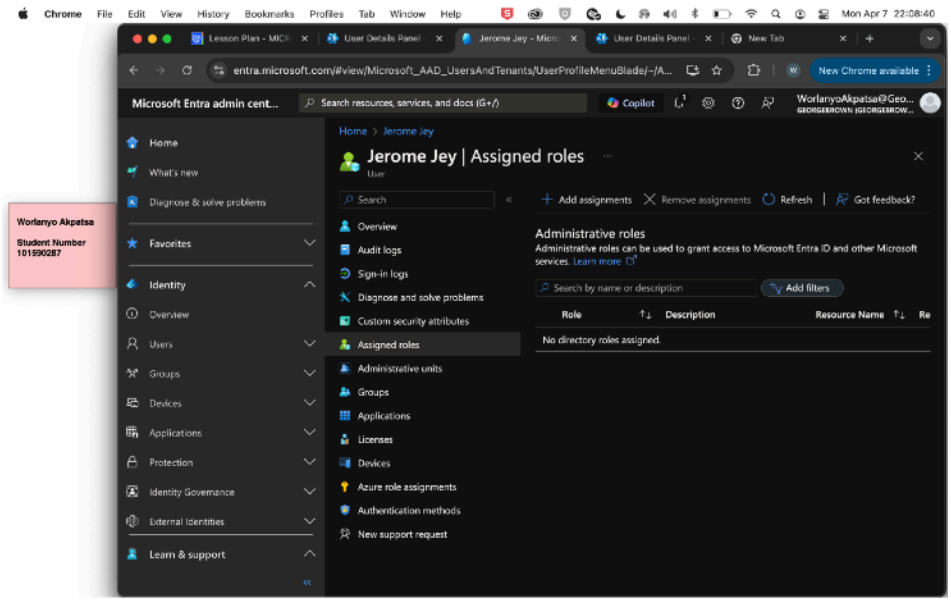
Student Name: Worlanyo Akpatsa
Student ID: 101590287

Term: Winter 2025

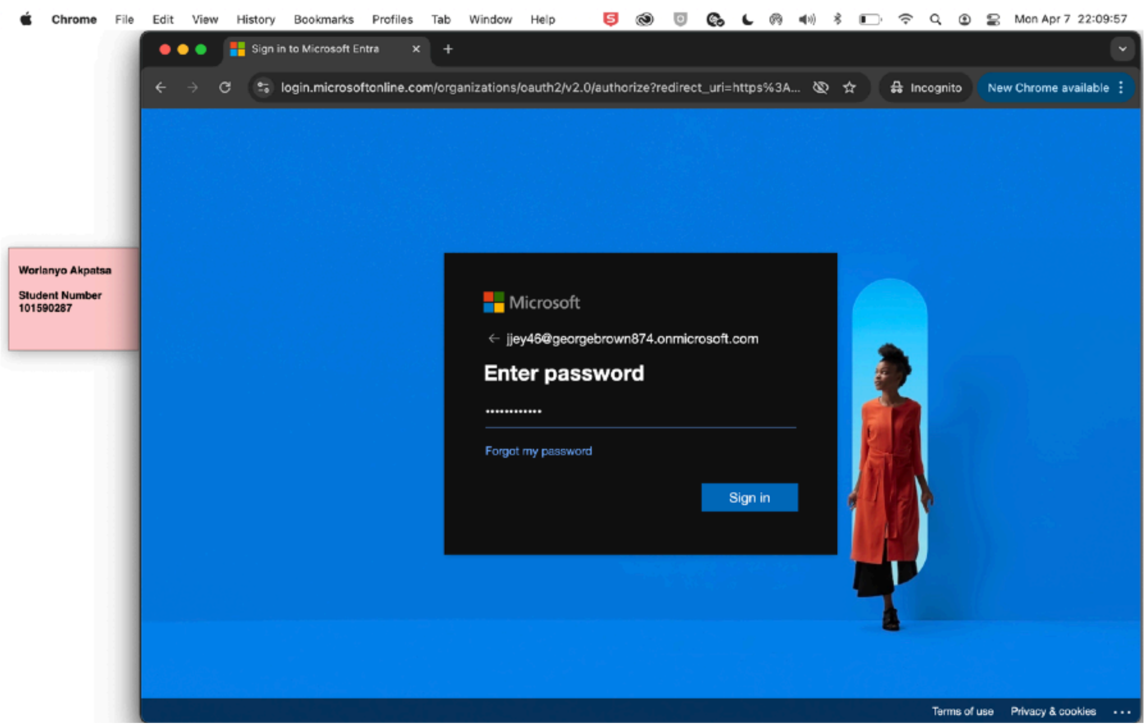
4.3: Removing the administrative role from the user

A: Removing Assigned Role from Jey

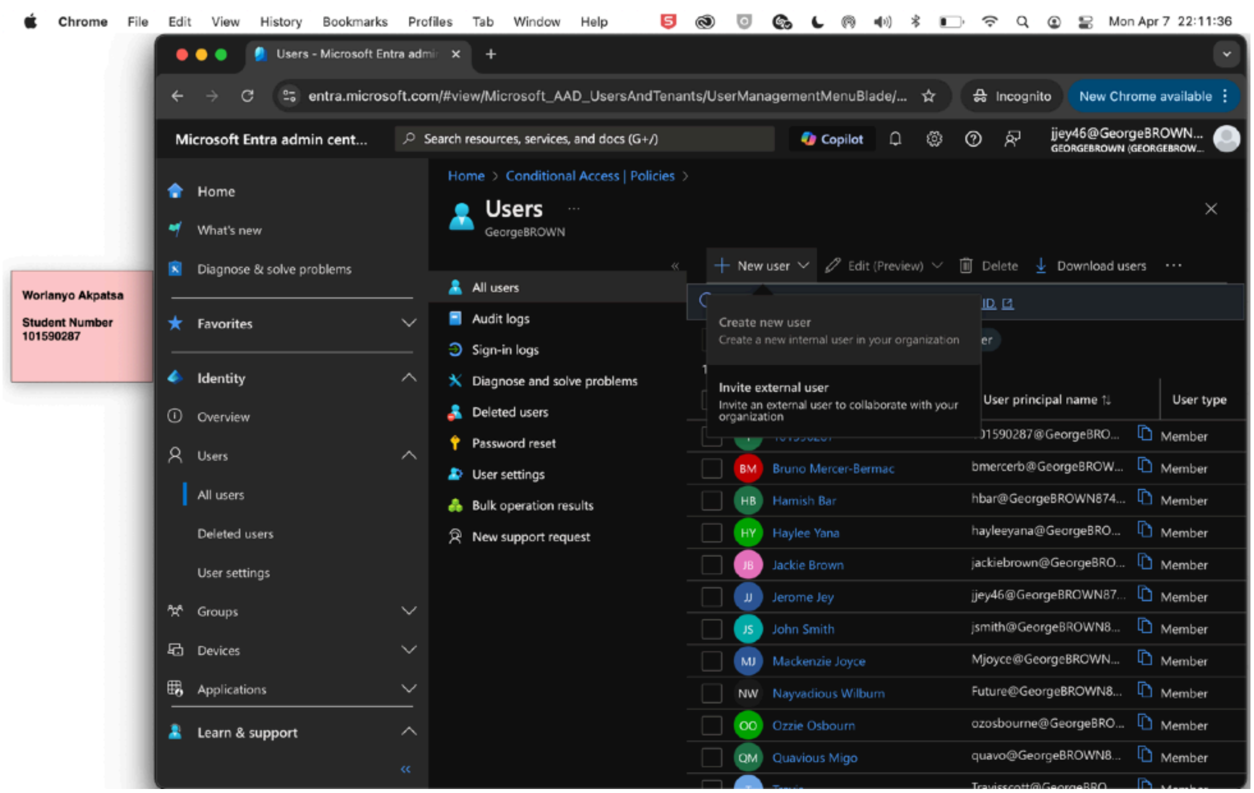




B: Signing in to entra admin using Jey's Account



C: Attempting to create user after admin role has been removed (user cannot create users anymore)

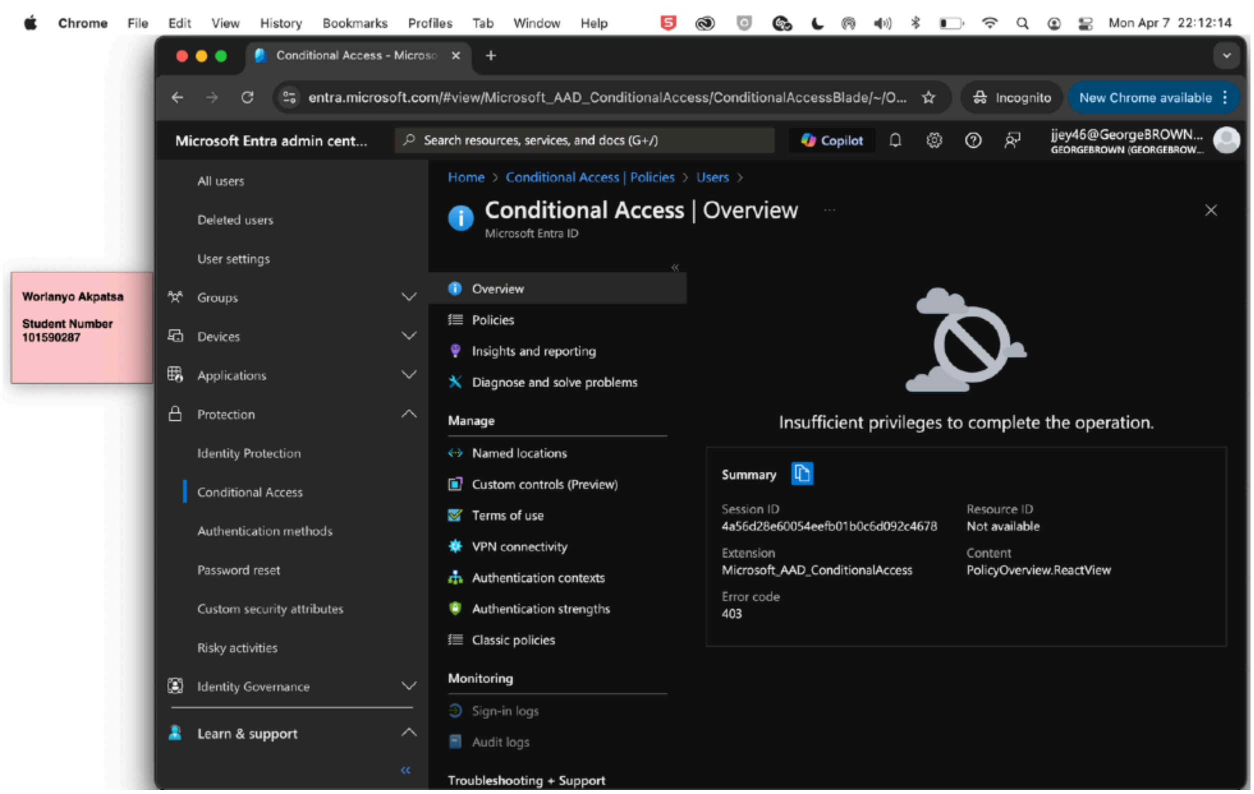


~ ~

Student Name: Worlanyo Akpatsa — Term: Winter 2025
Student ID: 101590287

~ ~

Also cannot view conditional Access details and policies



Task 4 Summary

Luckily for me, this last lab ended just how it started: with a simple task to do. The general overview of this task was to see how assigned admin roles affect a user's capability.

To begin, I had to assign an admin role to a user so I picked a user in my organization that had zero assigned roles. To do this, I had to navigate to users->all users and then click on the name of this user I had in mind.

A new page pops up with all his details and several sub headers to choose from. I chose the Assigned roles header and clicked add assignments. I decided to assign the role of a user administrator who I learnt can manage all aspects of users and groups.

As a result, I decided that to test this role out I would create a new user on entra admin using the selected users credentials.

I logged in to entra admin using his credentials and unsurprisingly, I was able to create a new user.

Then I unassigned this user admin role from him and decided to try and create a user again.

Unfortunately, I couldn't as he was not an admin anymore.

This showed that I was able to assign and unassign roles to this user successfully.