

Student Name: Worlanyo Akpatsa
Student ID: 101590287

Term: Winter 2025

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  
Student ID: 101590287

Term: Winter 2025

### 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

The screenshot shows the Microsoft 365 Admin Center homepage in a web browser. The URL is [admin.microsoft.com/Adminportal/Home?source=applauncher#/homepage](https://admin.microsoft.com/Adminportal/Home?source=applauncher#/homepage). The page has a red header bar with the title "Microsoft 365 admin center". On the left, there is a navigation sidebar with a user profile for "Worlanyo Akpatsa" (Student Number 101590287) and a list of admin centers including Security, Compliance, Microsoft Intune, Identity, Exchange, SharePoint, Power Platform, and All admin centers. The main content area features a greeting "Good afternoon, Worlanyo Akpatsa" and a section titled "For organizations like yours" with a button to "Set up email with a custom domain". Below this, there is a "Your organization" section with tabs for Users, Products, Upcoming changes (5), Learn, Set, Help & support, and Give Feedback. At the bottom, there are buttons for Add user, Reset password, Assign phone numbers, and a search bar.

## Microsoft 365 Identity and Services II – Enterprise Administration

---

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

The screenshot shows the Microsoft 365 admin center interface. On the left, there is a navigation sidebar with a user profile section for "WORLANYO" and "GeorgeBROWN". The sidebar includes sections for "Setup", "Reports", "Health", "Admin centers" (with "Identity" highlighted), "Exchange", "SharePoint", "Power Platform", and "Customize navigation". The main content area displays a message: "Good afternoon, Worlanyo Akpatsa" followed by a subtitle "The simplified view helps you focus on the most common tasks for organizations like yours." Below this, there is a callout box titled "Set up email with a custom domain" with the sub-instruction "Connect a domain that you own, or get a new one.". At the bottom of the main content, there is a section titled "Your organization" with links for "Users", "Products", "Upcoming changes (5)", "Learn", "Set", "Help & support", and "Give Feedback". The URL in the browser bar is <https://entra.microsoft.com/GeorgeBROWN874.onmicrosoft.com>.

## Microsoft 365 Identity and Services II – Enterprise Administration

---

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### C: Entra Homepage

The screenshot shows a Chrome browser window displaying the Microsoft Entra admin center at [entra.microsoft.com/#home](https://entra.microsoft.com/#home). The page has a dark theme. On the left, there's a navigation sidebar with a user profile for "Worlanyo Akpatsa" (Student Number 101590287) and a sidebar menu including Home, What's new, Diagnose & solve problems, Favorites, Identity (Overview, Users, Groups, Devices, Applications, Protection, Identity Governance, External Identities), Learn & support, and Learn more about Microsoft Entra.

The main content area features the Microsoft logo and the tagline "Secure access for a connected world". It includes a call-to-action button "Learn more about Microsoft Entra", a "Provide feedback" link, and sections for "Learn about Microsoft Entra" and "Explore the Microsoft Entra product family". A footer note states: "Learn how unified multicloud identity and network access help you protect and verify identities, manage".

## Microsoft 365 Identity and Services II – Enterprise Administration

---

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

The screenshot shows a Chrome browser window with the Microsoft Entra admin center URL: [entra.microsoft.com/#view/Microsoft\\_AAD\\_IAM/TenantOverview.ReactView/initialValue/tab...](https://entra.microsoft.com/#view/Microsoft_AAD_IAM/TenantOverview.ReactView/initialValue/tab...). The page displays basic information about the tenant "GeorgeBROWN".

**Basic Information:**

| Name           | GeorgeBROWN                          |
|----------------|--------------------------------------|
| Tenant ID      | 875c82ee-30d3-4df1-a2c9-b97afa1ba73c |
| Primary domain | GeorgeBROWN874.onmicrosoft.com       |
| License        | Microsoft Entra ID P1                |
| Users          | 12                                   |
| Groups         | 8                                    |
| Applications   | 0                                    |
| Devices        | 0                                    |

**User Profile (highlighted in pink):**

Worlanyo Akpatsa  
Student Number  
101590287

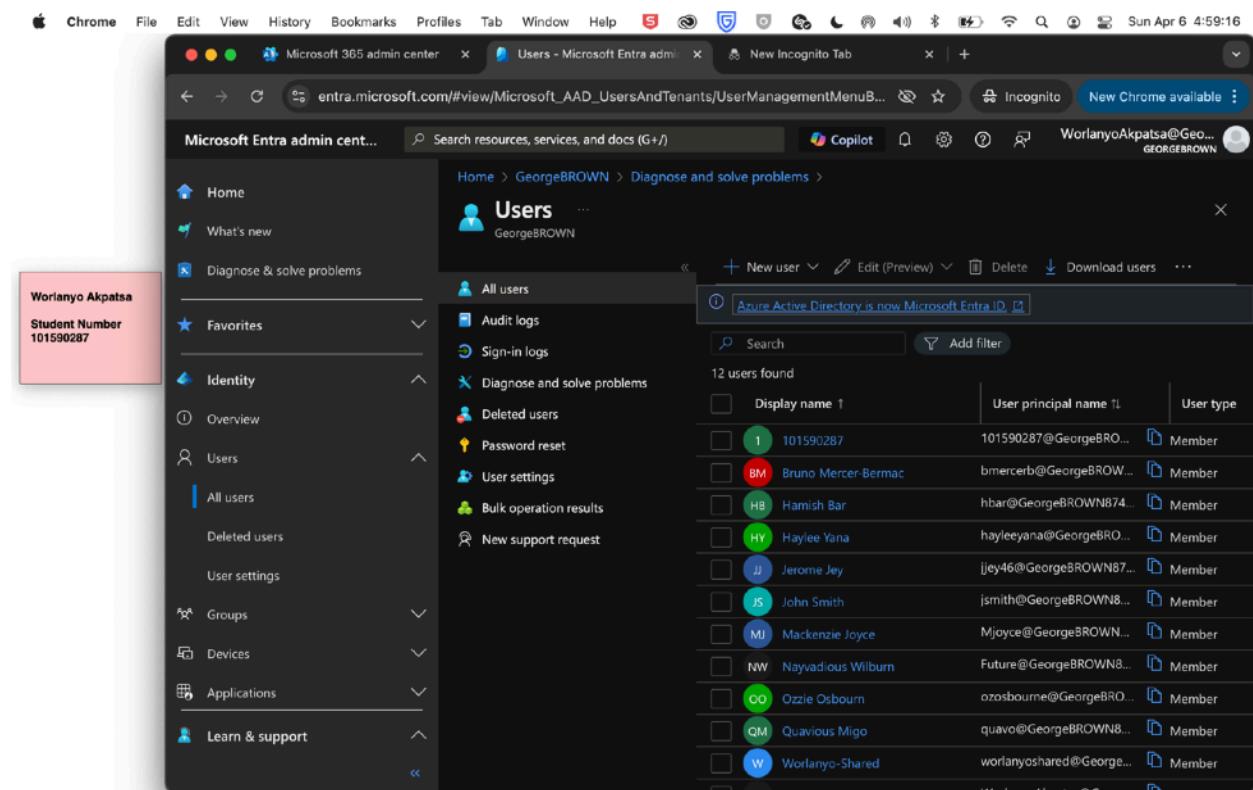
Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### 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



The screenshot shows the Microsoft Entra admin center interface. On the left, there is a navigation sidebar with the following sections:

- Home
- What's new
- Diagnose & solve problems
- Favorites
- Identity
  - Overview
  - Users
    - All users
    - Deleted users
    - User settings
  - Groups
  - Devices
  - Applications
- Learn & support

The 'Users' section is currently selected. In the main content area, the title is 'Users' under 'GeorgeBROWN'. Below it, there is a search bar and a button to 'New user'. A message indicates 'Azure Active Directory is now Microsoft Entra ID'. The table lists 12 users found:

| Display name | User principal name      | User type |
|--------------|--------------------------|-----------|
| 101590287    | 101590287@GeorgeBRO...   | Member    |
| BM           | bmercerb@GeorgeBROW...   | Member    |
| HB           | hbar@GeorgeBROWN87...    | Member    |
| HY           | hayleeyana@GeorgeBRO...  | Member    |
| JJ           | jjey46@GeorgeBROWN87...  | Member    |
| JS           | jsmith@GeorgeBROWN8...   | Member    |
| MJ           | Mjoyce@GeorgeBROWN...    | Member    |
| NW           | Future@GeorgeBROWN8...   | Member    |
| OO           | ozosbourne@GeorgeBRO...  | Member    |
| QM           | quavo@GeorgeBROWN8...    | Member    |
| W            | worlanyoshared@George... | Member    |

## Microsoft 365 Identity and Services II – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

The screenshot shows the Microsoft 365 admin center interface. On the left, there's a sidebar with navigation links like Home, What's new, Diagnose & solve problems, Favorites, Identity, Overview, Users (selected), Groups, Devices, Applications, and Learn & support. A pink box highlights the 'Worlanyo Akpatsa' and 'Student Number 101590287' information in the sidebar.

The main content area is titled 'Users' under 'GeorgeBROWN'. It shows a list of users with columns for 'User principal name', 'User type', and 'Last sign-in'. A 'Create new user' dialog is open, prompting the user to 'Create a new internal user in your organization'. The dialog includes fields for 'User principal name' (containing 'er') and 'User type' (set to 'Member').

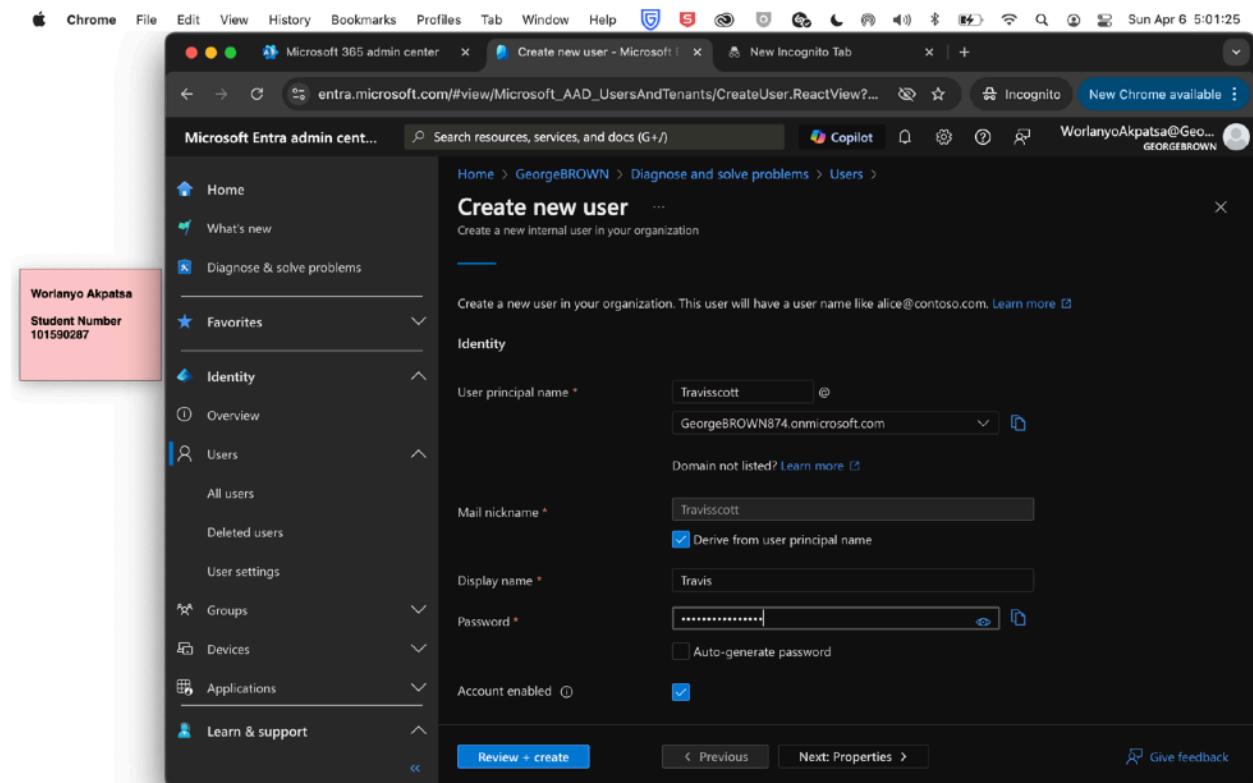
| User principal name     | User type                |
|-------------------------|--------------------------|
| 101590287@GeorgeBROW... | Member                   |
| BM Bruno Mercer-Bermac  | bmerc...                 |
| HB Hamish Bar           | hbar@GeorgeBROWN874...   |
| HY Haylee Yana          | hayleeyana@GeorgeBRO...  |
| JJ Jerome Jey           | jjey46@GeorgeBROWN87...  |
| JS John Smith           | jsmith@GeorgeBROWN8...   |
| MU Mackenzie Joyce      | Mjoyce@GeorgeBROWN...    |
| NW Nayadius Wilburn     | Future@GeorgeBROWN8...   |
| OO Ozzie Osbourn        | ozosbourne@GeorgeBRO...  |
| QM Quavious Migo        | quavo@GeorgeBROWN8...    |
| W Worlanyo-Shared       | worlanyoshared@George... |
| Worlanyo-Akpatsa@Geo... | Member                   |

## Microsoft 365 Identity and Services II – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### C: User Creation Process (Basics)



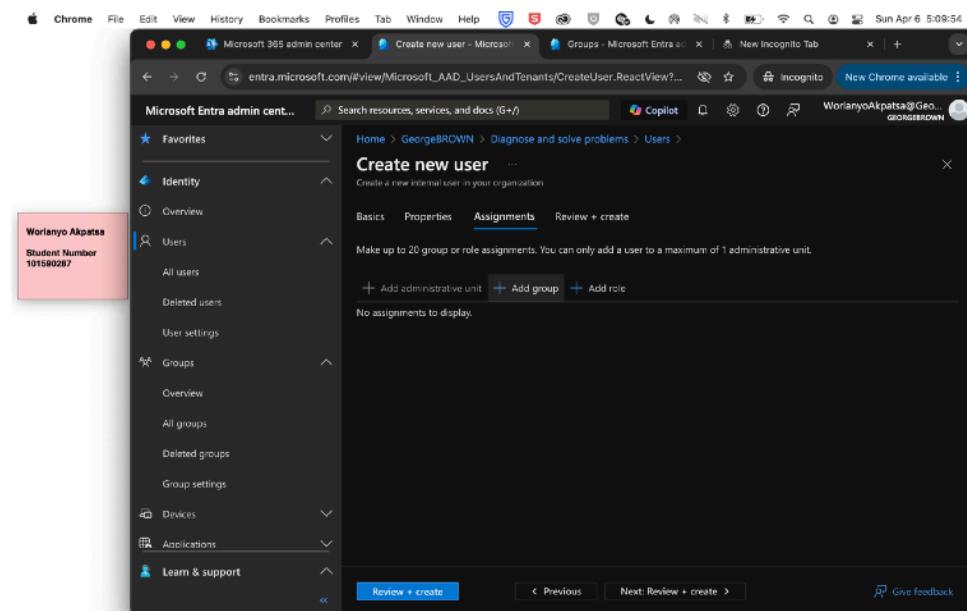
The screenshot shows the Microsoft 365 admin center interface. On the left, there is a sidebar with navigation links such as Home, What's new, Diagnose & solve problems, Favorites, Identity, Overview, Users (All users, Deleted users, User settings), Groups, Devices, Applications, Learn & support, and Help. A red box highlights the 'Worlanyo Akpatsa' section under 'Identity'. The main content area is titled 'Create new user' and contains fields for User principal name (Travisscott @ GeorgeBROWN874.onmicrosoft.com), Mail nickname (Travisscott), Display name (Travis), Password (redacted), and Account enabled (checked). Buttons at the bottom include 'Review + create' (highlighted in blue), 'Previous', 'Next: Properties', and 'Give feedback'.

## Microsoft 365 Identity and Services II – Enterprise Administration

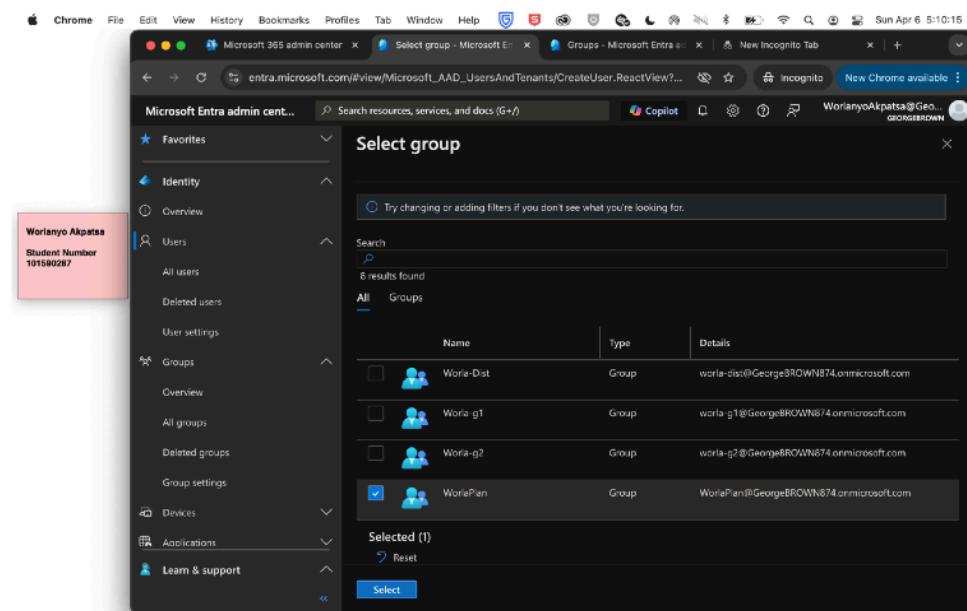
Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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



The screenshot shows the 'Create new user' interface in the Microsoft Entra admin center. The 'Assignments' tab is active. A red box highlights the user profile on the left, which includes the name 'Worlanyo Akpatsa' and 'Student Number 101590287'. The main pane displays a message stating 'No assignments to display.'



The screenshot shows the 'Select group' dialog in the Microsoft Entra admin center. A red box highlights the user profile on the left. The dialog lists four groups: 'Worla-Dst', 'Worla\_g1', 'Worla\_g2', and 'WorlaPlan'. The 'WorlaPlan' group is selected, indicated by a blue checkmark icon.

| Name      | Type  | Details                                  |
|-----------|-------|------------------------------------------|
| Worla-Dst | Group | worla-dst@GeorgeBROWN874.onmicrosoft.com |
| Worla_g1  | Group | worla_g1@GeorgeBROWN874.onmicrosoft.com  |
| Worla_g2  | Group | worla_g2@GeorgeBROWN874.onmicrosoft.com  |
| WorlaPlan | Group | WorlaPlan@GeorgeBROWN874.onmicrosoft.com |

## Microsoft 365 Identity and Services II – Enterprise Administration

---

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

The screenshot shows the Microsoft 365 Admin Center interface. On the left, there is a navigation sidebar with sections like Favorites, Identity, Overview, Users (with All users, Deleted users, User settings), Groups (with Overview, All groups, Deleted groups, Group settings), Devices, Applications, and Learn & support. A red box highlights the 'Worlanyo Akpatsa' and 'Student Number 101590287' information in the user profile section. The main content area is titled 'Create new user' and shows a 'Assignments' tab selected. It prompts to 'Create a new internal user in your organization'. Below this, it says 'Make up to 20 group or role assignments. You can only add a user to a maximum of 1 administrative unit.' There are three buttons: '+ Add administrative unit', '+ Add group' (which is highlighted in blue), and '+ Add role'. A table below shows one entry: Type 'Group' and Name 'WorlaPlan'. At the bottom, there are buttons for 'Review + create', 'Previous', 'Next: Review + create >', and 'Give feedback'.

## Microsoft 365 Identity and Services II – Enterprise Administration

---

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### E: Review and finish creating user

The screenshot shows the Microsoft 365 Admin Center interface. On the left, there is a navigation sidebar with sections like Favorites, Identity, Overview, Users (which is selected and highlighted in pink), Groups, Devices, Applications, and Learn & support. The main content area is titled 'Create new user' and contains fields for User principal name (Travisscott@GeorgeBROWN874.onmicrosoft.com), Display name (Travis), Mail nickname (Travisscott), Password (redacted), and Account enabled (Yes). Below these are 'Properties' (First name: Travis, Last name: Scott, User type: Member) and 'Assignments' (Administrative units: WorldPlan, Groups: WorldPlan). At the bottom, there are 'Create' and 'Next >' buttons, along with a 'Give feedback' link.

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### 1.4: Verify the user's group membership

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

The screenshot shows the Microsoft 365 admin center interface. On the left, there is a navigation sidebar with a red box highlighting the user information: "Worlanyo Akpatsa" and "Student Number 101590287". The main content area is titled "Groups | All groups" under "Identity". The "All groups" option is selected in the left-hand menu. The right side displays a list of 8 groups found, each with a checkbox, a small icon, the group name, and its object ID. The groups listed are: All Company (cd621e20-809e-4c), GeorgeBROWN (0e30c913-b6b9-4f), Group 1 (e6758d8c-9e4e-4c), Group 2 (7d8dff5b-7678-45), Worla-Dist (d20cb830-ca28-4c), Worla-g1 (140668e1-adfc-43), and Worla-g2 (127e6c77-5fe1-41).

| Name        | Object Id        |
|-------------|------------------|
| All Company | cd621e20-809e-4c |
| GeorgeBROWN | 0e30c913-b6b9-4f |
| Group 1     | e6758d8c-9e4e-4c |
| Group 2     | 7d8dff5b-7678-45 |
| Worla-Dist  | d20cb830-ca28-4c |
| Worla-g1    | 140668e1-adfc-43 |
| Worla-g2    | 127e6c77-5fe1-41 |

## Microsoft 365 Identity and Services II – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

The screenshot shows the Microsoft Entra admin center interface. On the left, there is a navigation sidebar with sections like Favorites, Identity, Users, Groups, Devices, Applications, and Learn & support. A pink box highlights the 'Worlanyo Akpatsa' profile in the 'Users' section. The main content area shows the 'WorlaPlan | Members' page. At the top, there are buttons for 'Add members', 'Bulk operations', 'Refresh', and 'Manage view'. Below this, a table lists four group members:

| Name                   | Type |
|------------------------|------|
| BM Bruno Mercer-Bermac | User |
| HB Hamish Bar          | User |
| Travis                 | User |
| WA Worlanyo Akpatsa    | User |

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### *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.

## **Microsoft 365 Identity and Services II – Enterprise Administration**

---

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

~~~~~  
~~~~~  
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

The screenshot shows the Microsoft Entra admin center interface. On the left, there is a navigation sidebar with the following structure:

- Home
- What's new
- Diagnose & solve problems
- Favorites
- Identity
  - Overview
  - Users
    - All users
    - Deleted users
    - User settings
  - Groups
    - Overview
    - All groups
  - Learn & support

A pink rectangular box highlights the "All users" link under the "Users" section. The main content area is titled "Users" and shows the "All users" list. The list includes the following columns: "Display name", "User principal name", and "User type". The list contains 13 entries, each with a small profile icon and initials. The entries are:

| Display name | User principal name                          | User type |
|--------------|----------------------------------------------|-----------|
| BM           | bmercer@GeorgeBROW...<br>Bruno Mercer-Bermac | Member    |
| HB           | hbar@GeorgeBROWN874...<br>Hamish Bar         | Member    |
| HY           | hayleeyana@GeorgeBRO...<br>Haylee Yana       | Member    |
| JJ           | jhey46@GeorgeBROWN87...<br>Jerome Jey        | Member    |
| JS           | jsmith@GeorgeBROWN8...<br>John Smith         | Member    |
| MJ           | Mjoyce@GeorgeBROWN...<br>Mackenzie Joyce     | Member    |
| NW           | Future@GeorgeBROWN8...<br>Nayvadious Wilburn | Member    |
| OO           | ozosbourne@GeorgeBRO...<br>Ozzie Osbourn     | Member    |
| QM           | quavo@GeorgeBROWN8...<br>Quavious Migo       | Member    |
| T            | Travisscott@GeorgeBRO...<br>Travis           | Member    |
| W            | worlanyoshared@George...<br>Worlanyo-Shared  | Member    |

## Microsoft 365 Identity and Services II – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

The screenshot shows the Microsoft 365 admin center interface. On the left, there's a sidebar with navigation links like Home, Favorites, Identity, Overview, Users, Groups, Learn & support, and more. The main area is titled 'Users' and shows a list of 13 users found. The user 'Bruno Mercer-Berma' (bm...@georgebrown.onmicrosoft.com) is selected. A context menu is open over this user, listing various actions: New user..., Edit (Preview)..., Delete, Download users..., Bulk operations..., Refresh, Manage view..., and Per-user MFA. The 'Per-user MFA' option is circled in red.

The screenshot shows the 'Per-user multifactor authentication' configuration page. The left sidebar is identical to the previous screenshot. The main content area is titled 'Per-user multifactor authentication' and includes a sub-header 'Before you begin, take a look at the [multifactor authentication deployment guide](#)'. Below this, there are four checkboxes: 'Enable MFA' (checked), 'Disable MFA', 'Enforce MFA', and 'User MFA settings'. A table lists users with their names, UPNs, and status. The table has columns for 'Name', 'UPN', and 'Status'. All users listed (101590287, Bruno Mercer-Berma, Nayadious Wilburn, Haylee Yana, Hamish Bar, Jerome Jey) have the status 'disabled'. There are also 'Bulk update' and 'Got feedback?' buttons at the top of the table.

## Microsoft 365 Identity and Services II – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a sidebar with a red box highlighting 'Worlanyo Akpatsa' and 'Student Number 101590287'. The main area is titled 'Per-user multifactor authentication'. At the top, there are four checkboxes: 'Enable MFA' (which is checked), 'Disable MFA', 'Enforce MFA', and 'User MFA settings'. Below this is a search bar and a 'Status' dropdown set to 'All'. A 'Reset filters' button is also present. The main table lists users with columns for 'Name', 'UPN', and 'Status'. The user 'Travis' is selected, indicated by a blue checkmark icon next to their name. The status for Travis is 'disabled'.

This screenshot shows the same Microsoft Entra admin center interface as the previous one, but with a modal dialog box open over the user list. The dialog is titled 'Enable multifactor authentication'. It contains a message: 'If your users do not regularly sign in through the browser, you can send them to this link to register for multifactor authentication.' followed by a link 'https://aka.ms/mfasetup'. At the bottom of the dialog are two buttons: 'Enable' (highlighted with a red box) and 'Cancel'.

## Microsoft 365 Identity and Services II – Enterprise Administration

---

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

D: MFA enabled for user Travis

The screenshot shows the Microsoft 365 admin center interface. On the left, there is a sidebar with the user's name and student number highlighted in pink. The main content area is titled "Per-user multifactor authentication". It lists several users with their email addresses and current MFA status. The user "Travis" is highlighted with a blue selection bar, indicating that MFA is enabled for them.

| User             | Email Address                                  | MFA Status |
|------------------|------------------------------------------------|------------|
| Jerome Jey       | jjey46@GeorgeBROWN874.onmicrosoft.com          | disabled   |
| John Smith       | jsmith@GeorgeBROWN874.onmicrosoft.com          | disabled   |
| Mackenzie Joyce  | Mjoyce@GeorgeBROWN874.onmicrosoft.com          | disabled   |
| Ozzie Osbourn    | ozosbourne@GeorgeBROWN874.onmicrosoft.com      | disabled   |
| Quavious Migo    | quavo@GeorgeBROWN874.onmicrosoft.com           | disabled   |
| Travis           | Traviscott@GeorgeBROWN874.onmicrosoft.com      | enabled    |
| Worlanyo Akpatsa | WorlanyoAkpatsa@GeorgeBROWN874.onmicrosoft.com | disabled   |
| Worlanyo-Shared  | worlanyoshared@GeorgeBROWN874.onmicrosoft.com  | disabled   |

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

A: Navigate to users->all users

The screenshot shows the Microsoft Entra admin center interface. On the left, there is a navigation sidebar with the user's name (Worlanyo Akpatsa) and student number (101590287) highlighted in pink. The main area shows the 'Users' section with the 'All users' tab selected. A message at the top right states 'Azure Active Directory is now Microsoft Entra ID'. Below this, there is a search bar and a list of 13 users found. The columns in the user list are 'Display name', 'User principal name', and 'User type'. Each user entry includes a small profile icon and a download link.

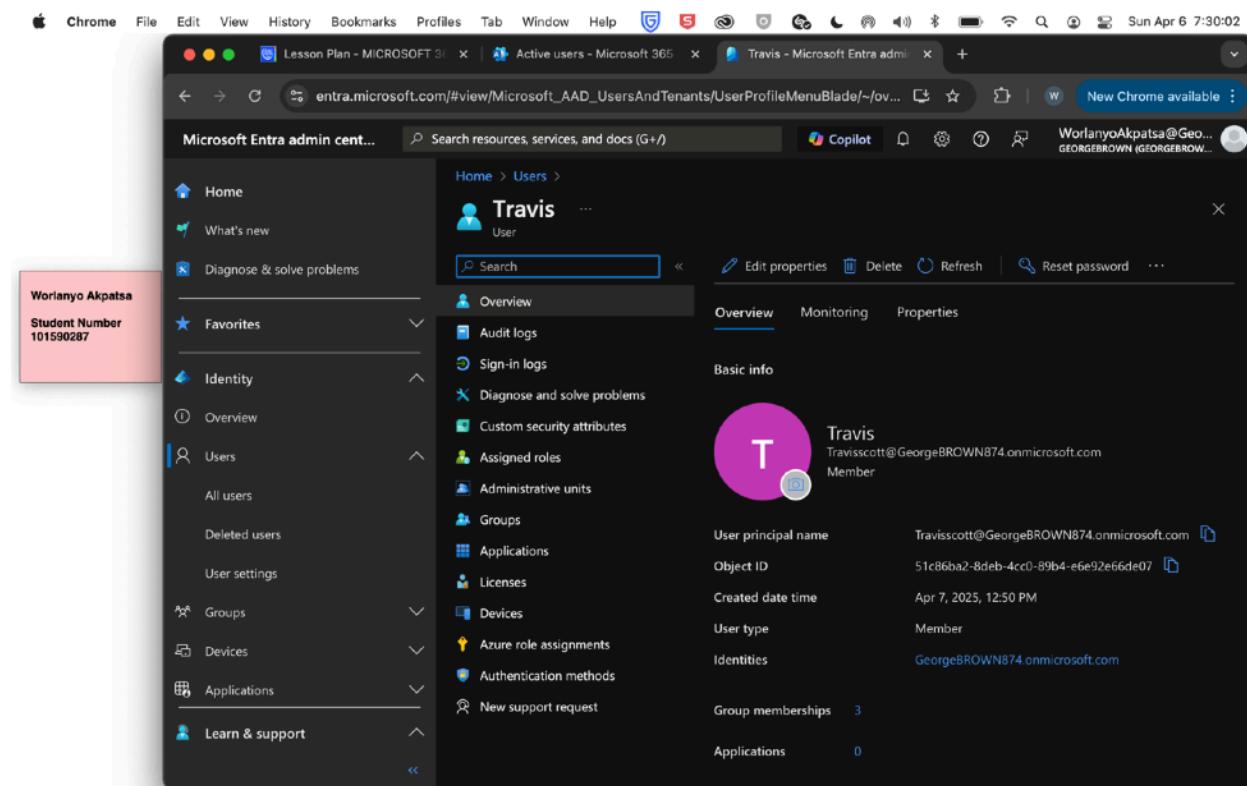
| Display name        | User principal name        | User type |
|---------------------|----------------------------|-----------|
| 101590287           | 101590287@GeorgeBRO...     | Member    |
| Bruno Mercer-Bermac | bmercerb@GeorgeBROW...     | Member    |
| Hamish Bar          | hbar@GeorgeBROWN874...     | Member    |
| Haylee Yana         | hayleeyana@GeorgeBRO...    | Member    |
| Jerome Jey          | jjey46@GeorgeBROWN87...    | Member    |
| John Smith          | jsmith@GeorgeBROWN8...     | Member    |
| Mackenzie Joyce     | Mjoyce@GeorgeBROWN...      | Member    |
| Nayvadios Wilburn   | Future@GeorgeBROWN8...     | Member    |
| Ozzie Osbourn       | ozosburne@GeorgeBRO...     | Member    |
| Quavious Migo       | quavo@GeorgeBROWN8...      | Member    |
| Travis              | Travisscott@GeorgeBRO...   | Member    |
| Worlanyo Akpatsa    | worlanyo.akpatsa@George... | Member    |

## Microsoft 365 Identity and Services II – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

B: Select new user (travis)



The screenshot shows the Microsoft Entra admin center interface. On the left, there is a sidebar with a red box highlighting the user 'Worlanyo Akpatsa' and their student number '101590287'. The main content area shows the user profile for 'Travis'. The profile includes a purple circular icon with a white 'T', the name 'Travis', the email 'Travisscott@GeorgeBROWN874.onmicrosoft.com', and the status 'Member'. Below the profile, there is a table with basic user information:

| User principal name | Travisscott@GeorgeBROWN874.onmicrosoft.com |
|---------------------|--------------------------------------------|
| Object ID           | 51c86ba2-8deb-4cc0-89b4-e6e92e66de07       |
| Created date time   | Apr 7, 2025, 12:50 PM                      |
| User type           | Member                                     |
| Identities          | GeorgeBROWN874.onmicrosoft.com             |
| Group memberships   | 3                                          |
| Applications        | 0                                          |

## Microsoft 365 Identity and Services II – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### C: Choose Authentication Methods under Travis Profile

The screenshot shows the Microsoft Entra admin center interface. On the left, there is a navigation sidebar with the following sections:

- Home
- What's new
- Diagnose & solve problems
- Favorites
- Identity (selected)
- Overview
- Users
  - All users
  - Deleted users
  - User settings
- Groups
- Devices
- Applications
- Learn & support

A red box highlights the "Identity" section in the sidebar.

The main content area shows the "Travis | Authentication methods" page. The URL in the address bar is `entra.microsoft.com/#view/Microsoft_AAD_UsersAndTenants/UserProfileMenuBlade/-/JU...`. The page includes the following elements:

- Search bar:** Search resources, services, and docs (G+)
- Add authentication method** button
- Reset password** button
- Overview:** Authentication methods are the ways users sign into Microsoft Entra ID and perform self-service password reset (SSPR). The user's "default sign-in method" is the first one shown to the user when they are required to authenticate with a second factor - the user always can choose another registered, enabled authentication method to authenticate with. [Learn more](#)
- Default sign-in method (Preview):** No default
- Usable authentication methods:** Authentication method: Detail. No usable methods.
- Non-usuable authentication methods:** Authentication method: Detail. No non-usuable methods.
- System preferred multifactor authentication method:** Feature status: Enabled. System preferred MFA method: No system preferred MFA method.

## Microsoft 365 Identity and Services II – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

D: Click Add Authentication Method and Select Phone Number

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a sidebar with navigation links like Home, What's new, Diagnose & solve problems, Favorites, Identity (Overview, Users, Groups, Devices, Applications), Learn & support, and a user profile section for 'Worlanyo Akpatsa' with 'Student Number 101590287'. The main content area is titled 'Travis | Authentication' and shows the 'Add authentication method' page. A dropdown menu titled 'Choose method' is open, listing several options: Email, Phone number, Temporary Access Pass, QR code (Preview), Custom security attributes, Assigned roles, Administrative units, Groups, Applications, Licenses, Devices, Azure role assignments, and Authentication methods. The 'Authentication methods' option is highlighted with a blue selection bar. At the bottom right of the main content area, there's a large 'Add' button.

## Microsoft 365 Identity and Services II – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### E: Add phone details

The screenshot shows the Microsoft Entra admin center interface. On the left, there is a sidebar with navigation links such as Home, Favorites, Identity, Overview, Users, Groups, Devices, Applications, Learn & support, and a pink-highlighted section for 'Worlanyo Akpatsa' with the student number '101590287'. The main content area is titled 'Add authentication method' for a user named 'Travis | Authentica'. It has a search bar and a dropdown menu for 'Choose method'. Under 'Phone number', the field contains '+1 6473303898' and 'Primary mobile' is selected under 'Phone type'. A blue 'Add' button is at the bottom right.

## Microsoft 365 Identity and Services II – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### F: Successfully Added Method of Authentication (Phone Number)

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a sidebar with navigation links like Home, What's new, Diagnose & solve problems, Favorites, Identity, Overview, Users, Groups, Devices, Applications, Learn & support, and New support request. A red box highlights the 'Worlanyo Akpatsa' user profile in the sidebar, which includes the student number '101590287'. The main content area shows the 'Travis | Authentication methods' page for the 'Travis' user. At the top right, a green checkmark icon and the message 'Successfully added method' are displayed, along with the note 'Successfully added Phone number.' Below this, there's a search bar and buttons for 'Add authentication method' and 'Reset password'. The 'Authentication methods' section lists 'Default sign-in method (Preview)' as 'No default' and 'Usable authentication methods' as 'Phone number' (Primary mobile: +1 6473303898). The 'Non-usable authentication methods' section shows 'No non-usuable methods.' The 'System preferred multifactor authentication method' section indicates 'Enabled' and 'No system preferred MFA method'.

## Microsoft 365 Identity and Services II – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

The screenshot shows the Microsoft 365 Admin Center interface. On the left, there's a sidebar with navigation links like All users, Deleted users, User settings, Groups, Overview, All groups, Deleted groups, Group settings, Devices, Applications, Protection, Identity Protection, Conditional Access, and Authentication methods. A pink box highlights the 'Groups' link. The main content area is titled 'New Group' and shows the following fields:

- Group type: Microsoft 365
- Group name: PhoneNumberMFA
- Group email address: PhoneNumberMFA @GeorgeBROWN874.onmicrosoft.com
- Group description: Enter a description for the group
- Microsft Entra roles can be assigned to the group: Yes (selected)
- Membership type: Assigned

A tooltip at the bottom left of the form area says: "Use group sensitivity labels in Microsoft Entra ID to classify and protect Microsoft 365 groups. Learn more about assigning sensitivity labels in Microsoft Entra ID." At the bottom right of the form is a blue 'Create' button.

## Microsoft 365 Identity and Services II – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

The screenshot shows the Microsoft 365 admin center interface. On the left, there's a sidebar with navigation links like All users, Groups, Overview, All groups, Deleted groups, Group settings, Devices, Applications, Protection, Identity Protection, Conditional Access, Authentication methods, and Learn & support. A red box highlights the 'Groups' link. The main content area is titled 'New Group' and contains fields for Group type (set to Microsoft 365), Group name (set to 'PhoneNumberMFA'), Group email address (set to 'PhoneNumberMFA @GeorgeBROWN874.onmicrosoft.com'), Group description (empty), Microsoft Entra roles can be assigned to the group (Yes selected), Membership type (Assigned selected), and a note about using group sensitivity labels. At the bottom is a blue 'Create' button.

The screenshot shows the Microsoft 365 admin center interface. The sidebar is identical to the previous screenshot. The main content area is titled 'Add members' and lists users found by search. It shows four users: Quievous Migo, Travis, Worlanyo Akpatsa, and Worlanyo-Shared. The 'Travis' user is selected, indicated by a checked checkbox next to their name. Below the list, there's a 'Selected (1)' section with a 'Select' button. The status bar at the bottom indicates the date as Sun Apr 6 6:56:06.

## Microsoft 365 Identity and Services II – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

The screenshot shows the Microsoft 365 Admin Center interface. On the left, there is a navigation sidebar with the following sections:

- All users
- Deleted users
- User settings
- Groups
- Devices
- Applications
- Protection
  - Identity Protection
  - Conditional Access
  - Authentication methods
- Password reset
- Custom security attributes
- Risky activities
- Identity Governance
- Learn & support

The "Authentication methods" section is highlighted with a blue star icon. A red box highlights the "Student Number 101590287" entry in the user profile area.

The main content area is titled "Authentication methods | Policies". It shows a list of authentication methods under the "Manage" section:

- Policies
  - >Password protection
  - Registration campaign
  - Authentication strengths
  - Settings
- Monitoring
  - Activity
  - User registration details
  - Registration and reset events
  - Bulk operation results

Below this, there is a section titled "Authentication method policies" with a brief description and a table:

| Method                     | Target    | Enabled |
|----------------------------|-----------|---------|
| Passkey (FIDO2)            | All users | No      |
| Microsoft Authenticator    | All users | Yes     |
| SMS                        | All users | No      |
| Temporary Access Pass      | All users | Yes     |
| Hardware OATH tokens       | All users | No      |
| Third-party software OA... | All users | Yes     |
| Voice call                 | All users | No      |
| Email OTP                  | All users | Yes     |
| Certificate-based auth...  | All users | No      |
| QR code (Preview)          | All users | No      |

The URL in the browser's address bar is [https://entra.microsoft.com/#blade/Microsoft\\_AAD\\_IAM/AuthenticationMethodsMenuBlade/fromNav/Identity?Microsoft\\_AAD\\_IAM\\_legacyAADRedirect=true](https://entra.microsoft.com/#blade/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/fromNav/Identity?Microsoft_AAD_IAM_legacyAADRedirect=true).

## Microsoft 365 Identity and Services II – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### C: Under Policies, Open SMS

The screenshot shows the Microsoft 365 admin center interface. On the left, there is a navigation sidebar with various categories like All users, Groups, Applications, Protection, and Authentication methods. A red box highlights the 'Worlanyo Akpatsa' section in the sidebar, which includes the student number '101590287'. The main content area is titled 'Authentication methods | Policies' and shows a list of authentication methods. One method, 'SMS', is highlighted with a red box. The table below lists the methods, their targets, and whether they are enabled.

| Method                     | Target    | Enabled |
|----------------------------|-----------|---------|
| Passkey (FIDO2)            | All users | No      |
| Microsoft Authenticator    | All users | Yes     |
| <b>SMS</b>                 | All users | No      |
| Temporary Access Pass      | All users | Yes     |
| Hardware OATH tokens ...   | All users | No      |
| Third-party software OA... | All users | Yes     |
| Voice call                 | All users | No      |
| Email OTP                  | All users | Yes     |
| Certificate-based auth...  | All users | No      |
| QR code (Preview)          | All users | No      |

## Microsoft 365 Identity and Services II – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

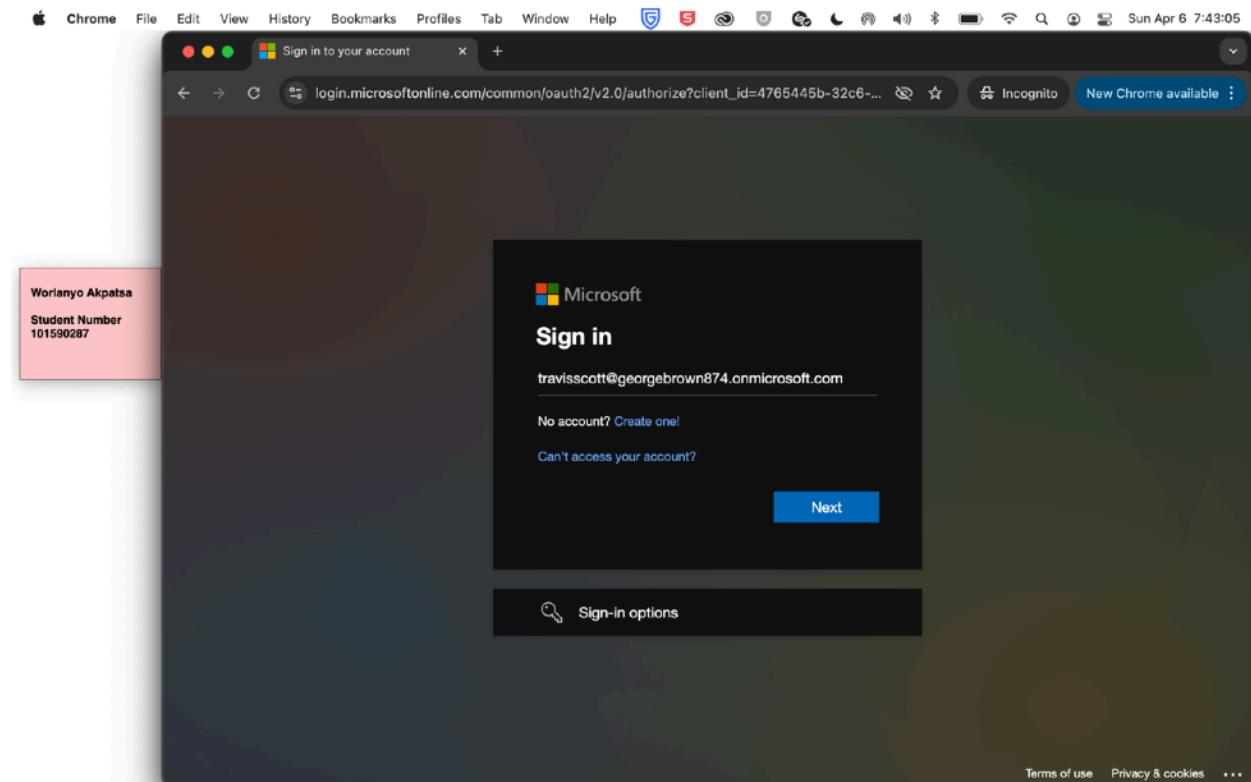
The screenshot shows the Microsoft 365 admin center interface. On the left, there is a navigation sidebar with the user's name (Worlanyo Akpatsa) and student number (101590287) highlighted. The main content area is titled "SMS settings" and shows the "Enable and Target" configuration. The "Enable" toggle switch is turned on. Under the "Target" section, the "Select groups" radio button is selected. A table below lists a single group named "PhoneNumberMFA" with the "Type" set to "Group". The "Use for sign-in" checkbox is checked, and the "Registration" dropdown is set to "Optional". At the bottom of the page are "Save" and "Discard" buttons.

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### 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

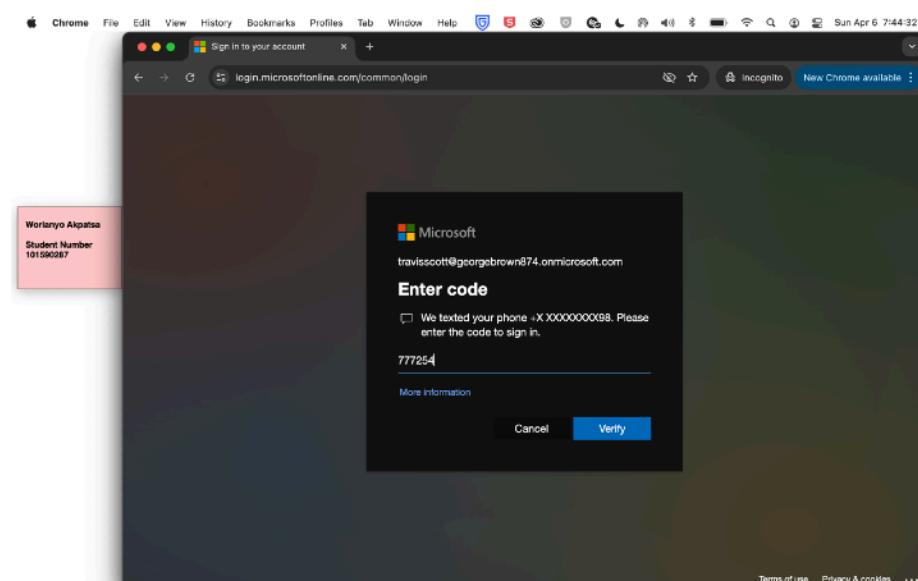
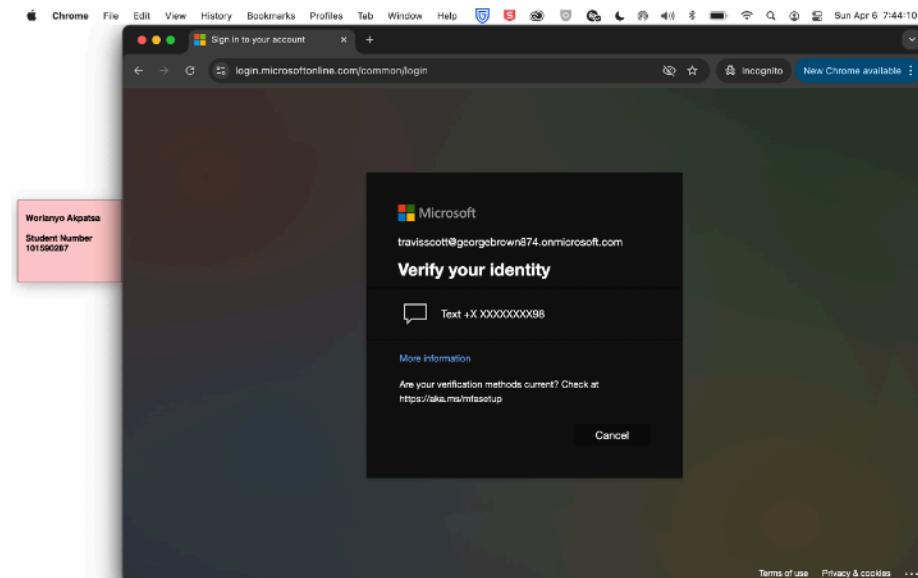


## Microsoft 365 Identity and Services II – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

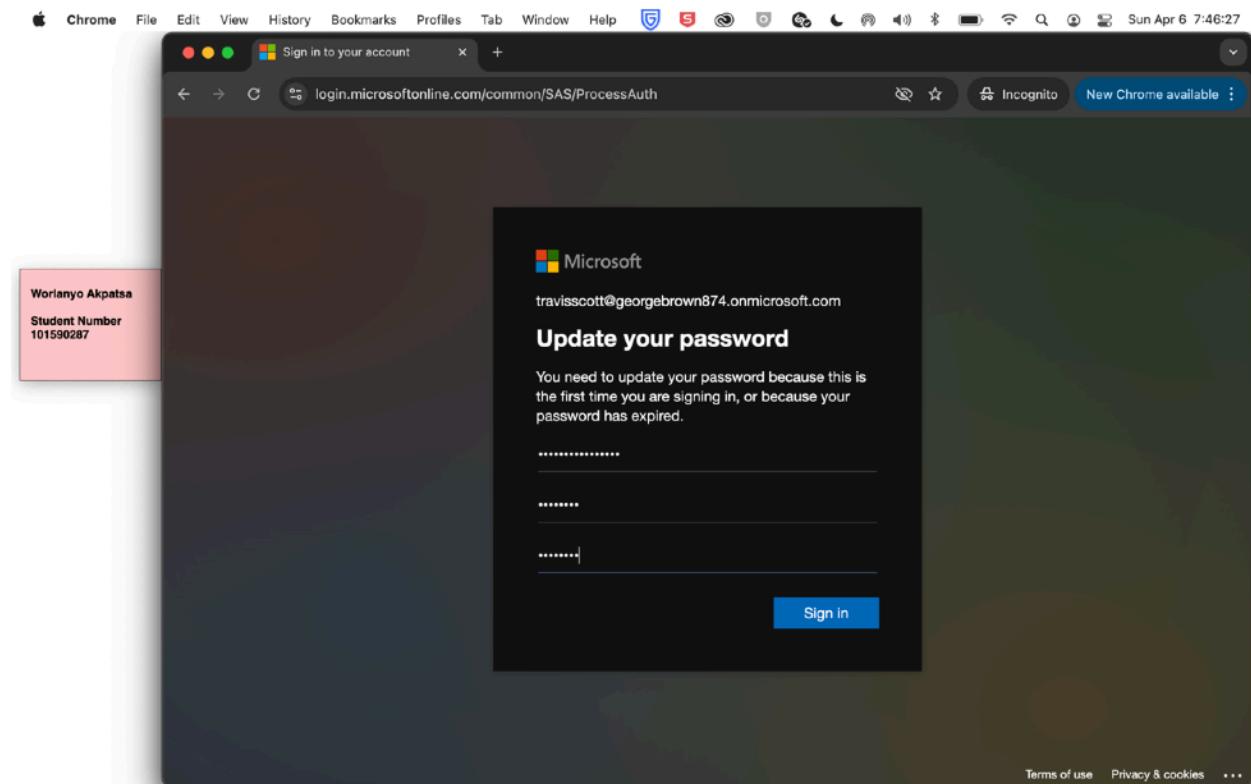
### B: Multi Factor Verification and confirming with code sent to number



Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### C: Updating Password



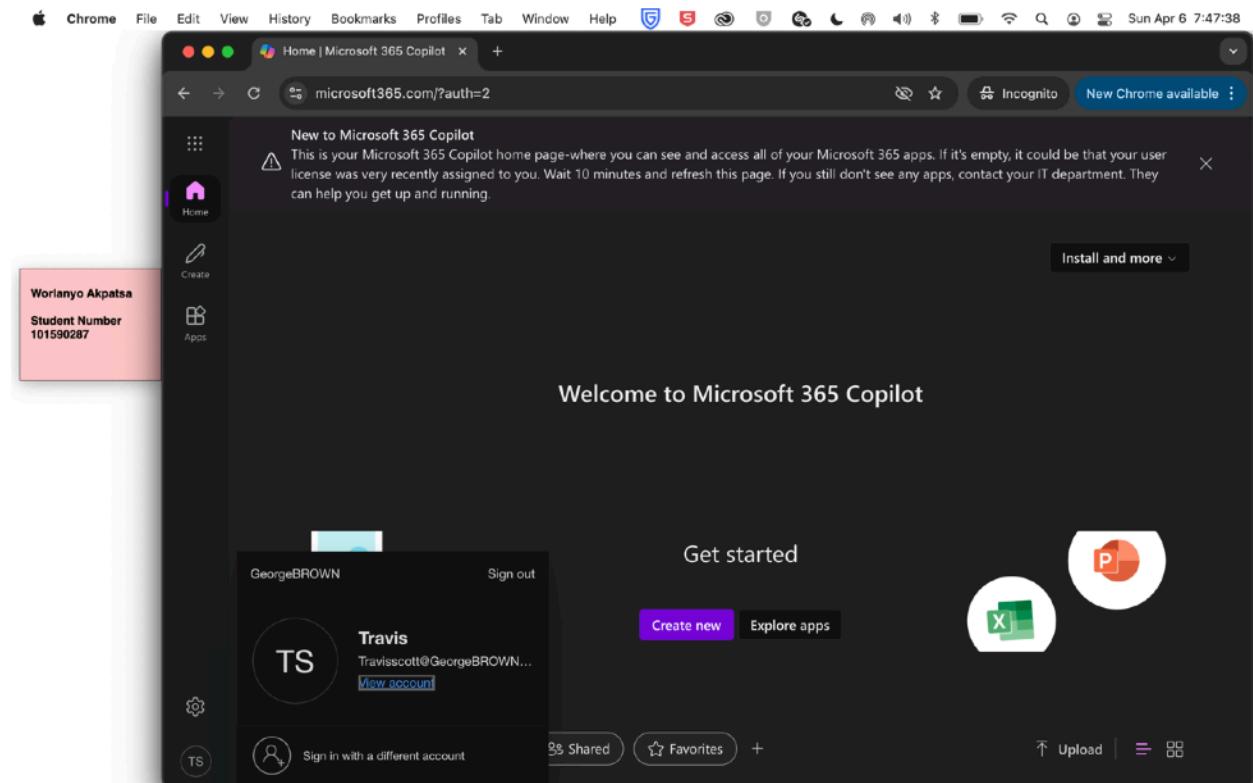
## Microsoft 365 Identity and Services II – Enterprise Administration

---

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

D: Signed in to new user account



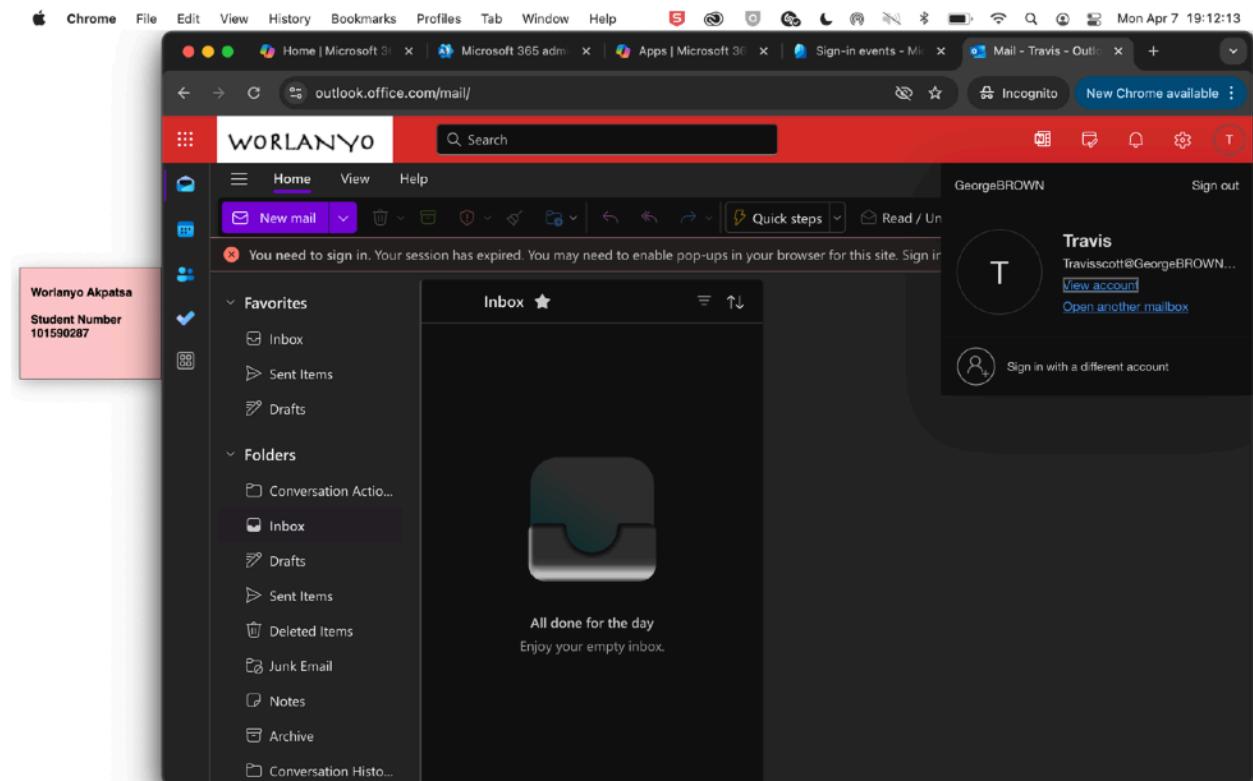
## Microsoft 365 Identity and Services II – Enterprise Administration

---

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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



Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

A: Navigate to Entra Admin Homepage

The screenshot shows the Microsoft Entra Admin Center interface. On the left, there is a navigation sidebar with the user's name (Worlanyo Akpatsa) and student number (101590287) at the top. Below this, the sidebar includes sections for Home, What's new, Diagnose & solve problems, Favorites, Identity (Overview, Users, Groups, Devices, Applications), Learn & support, and Learn about Microsoft Entra. The main content area features a large blue 'Secure access for a connected world' banner with a subtext about protecting identities and securing access. It also includes links to 'Learn more about Microsoft Entra', 'Provide feedback', and 'Explore the Microsoft Entra product family'. The top right corner shows the user's email (WorlanyoAkpatsa@Geo...), name (GEORGEBROWN), and a Copilot icon.

## Microsoft 365 Identity and Services II – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

The screenshot shows the Microsoft Entra admin center interface. On the left, there is a navigation sidebar with a pink header bar containing the user's name and student number. The sidebar includes sections for Home, What's new, Diagnose & solve problems, Favorites (with a star icon), Identity (with a blue triangle icon), Overview, Users, Groups, Devices, Applications, Protection, Identity Governance, External Identities, Learn & support, and Help & feedback. The main content area is titled "Sign-in events" and displays a table of sign-in logs. The table has columns for Date, Request ID, User, Application, Status, and Sign-in errors. The table shows several successful sign-ins for the user "Worlanyo Akpatsa" from various applications like OfficeHome, Azure Portal, and Microsoft Office 365. One entry is highlighted in dark grey.

| Date                  | Request ID            | User             | Application              | Status      | Sign-in errors |
|-----------------------|-----------------------|------------------|--------------------------|-------------|----------------|
| 4/7/2025, 7:03:58 PM  | ddd75497-5829-484...  | Travis           | OfficeHome               | Success     | 0              |
| 4/7/2025, 7:02:26 PM  | ab5bf8c9-7d24-4839... | Travis           | Azure Portal             | Success     | 0              |
| 4/7/2025, 7:01:29 PM  | ba3fa5dc-bebd-451...  | Travis           | Microsoft Office 365 ... | Success     | 0              |
| 4/7/2025, 6:52:55 PM  | 884a3b0d-e13f-425e... | Travis           | OfficeHome               | Success     | 0              |
| 4/7/2025, 6:52:51 PM  | 7b74031a-1a92-423...  | Travis           | OfficeHome               | Interrupted | 50140          |
| 4/7/2025, 6:50:16 PM  | f0ee7699-8f4a-4414... | Travis           | OfficeHome               | Interrupted | 50055          |
| 4/7/2025, 6:34:02 PM  | 2eec036b-a12e-424...  | Worlanyo Akpatsa | Azure Portal             | Success     | 0              |
| 4/7/2025, 6:31:28 PM  | adb8cc68-78df-44fb... | Worlanyo Akpatsa | Azure Portal             | Success     | 0              |
| 4/7/2025, 1:58:04 PM  | fd457af9-c67d-457a... | Worlanyo Akpatsa | Azure Portal             | Success     | 0              |
| 4/7/2025, 12:40:01 PM | 52d98cb6-9a96-4fd9... | Worlanyo Akpatsa | Azure Portal             | Success     | 0              |
| 4/7/2025, 12:28:14 PM | 5fe0ab8a-81f6-4f68... | Worlanyo Akpatsa | Azure Portal             | Success     | 0              |
| 4/7/2025, 12:24:16 PM | 786519ee-90c2-495...  | Worlanyo Akpatsa | Azure Portal             | Success     | 0              |

## Microsoft 365 Identity and Services II – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

This screenshot shows the Microsoft Entra admin center interface. On the left, the navigation menu is visible with a red box highlighting the user's name and student number. The main pane displays the 'Sign-in events' section. A table lists various sign-in attempts, with the first one highlighted in yellow. The columns include Date, Request ID, User, Application, Status, and Sign-in error. The first entry is for 'Travis' on 4/7/2025 at 7:03:58 PM.

| Date                  | Request ID            | User             | Application              | Status      | Sign-in error |
|-----------------------|-----------------------|------------------|--------------------------|-------------|---------------|
| 4/7/2025, 7:03:58 PM  | dddf75497-5829-484... | Travis           | OfficeHome               | Success     | 0             |
| 4/7/2025, 7:02:26 PM  | ab5fb89-7fd24-4839... | Travis           | Azure Portal             | Success     | 0             |
| 4/7/2025, 7:01:29 PM  | ba3f95dc-bebd-451...  | Travis           | Microsoft Office 365 ... | Success     | 0             |
| 4/7/2025, 6:52:55 PM  | 884ab30d-a131-425e... | Travis           | OfficeHome               | Success     | 0             |
| 4/7/2025, 6:52:51 PM  | 7b74031a-1a92-423...  | Travis           | OfficeHome               | Interrupted | 50140         |
| 4/7/2025, 6:50:16 PM  | 10ee7699-84fa-4414... | Travis           | OfficeHome               | Interrupted | 50055         |
| 4/7/2025, 6:34:02 PM  | 2ee036b-a12e-424...   | Worlanyo Akpatsa | Azure Portal             | Success     | 0             |
| 4/7/2025, 6:31:28 PM  | adb8cd68-78d1-4ff...  | Worlanyo Akpatsa | Azure Portal             | Success     | 0             |
| 4/7/2025, 1:58:04 PM  | d4d57a99-d67d-457...  | Worlanyo Akpatsa | Azure Portal             | Success     | 0             |
| 4/7/2025, 12:40:01 PM | 52d98cb6-9a96-4ff9... | Worlanyo Akpatsa | Azure Portal             | Success     | 0             |
| 4/7/2025, 12:28:14 PM | 5feabb8a-8116-4ff8... | Worlanyo Akpatsa | Azure Portal             | Success     | 0             |
| 4/7/2025, 12:24:16 PM | 786519ee-90c2-495...  | Worlanyo Akpatsa | Azure Portal             | Success     | 0             |

This screenshot shows the 'Activity Details: Sign-ins' page. The left sidebar has a red box around the user information. The main area shows tabs for Basic info, Location, Device info, Authentication Details (which is selected), Conditional Access, and Report-only. Under 'Authentication Policies Applied', it lists 'Per-user multi-factor authentication'. Two entries are shown in the table:

| Date                 | Authentication met... | Authentication met... | Succeeded | Result detail           | Require |
|----------------------|-----------------------|-----------------------|-----------|-------------------------|---------|
| 4/7/2025, 6:50:16 PM | Password              | Password in the cloud | true      | Correct password        |         |
| 4/7/2025, 6:50:16 PM | Text message          | xx000000098           | true      | MFA successfully com... |         |

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### *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 for a 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 method. 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.

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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  
Student ID: 101590287

Term: Winter 2025

### 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

The screenshot shows the Microsoft Entra admin center interface. On the left, there is a navigation sidebar with several categories: Users, Groups, Devices, Applications, Protection, Identity Protection, Conditional Access (which is selected and highlighted in blue), Authentication methods, Password reset, Custom security attributes, Risky activities, Identity Governance, External Identities, and Learn & support. A red box highlights the 'Protection' category. The main content area is titled 'Conditional Access | Overview' under 'Microsoft Entra ID'. It features a sub-menu with 'Overview', 'Policies', 'Insights and reporting', and 'Diagnose and solve problems'. Below this is a 'Manage' section with 'Named locations', 'Custom controls (Preview)', 'Terms of use' (which is selected and highlighted in blue), 'VPN connectivity', 'Authentication contexts', 'Authentication strengths', and 'Classic policies'. There are also 'Monitoring' sections for 'Sign-in logs' and 'Audit logs'. Two large callout boxes are present: one for 'Create a new Conditional Access policy' and another for 'View insights and recommendations'. The URL in the browser bar is [https://entra.microsoft.com/#view/Microsoft\\_AAD\\_ConditionalAccess/ConditionalAccessBlade/-/TermsOfUse/menuid/ffromNav/Identity](https://entra.microsoft.com/#view/Microsoft_AAD_ConditionalAccess/ConditionalAccessBlade/-/TermsOfUse/menuid/ffromNav/Identity).

## Microsoft 365 Identity and Services II – Enterprise Administration

---

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

A: Click new policy and name it

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a sidebar with navigation links like Users, Groups, Devices, Applications, Protection, Identity Protection, Conditional Access, Authentication methods, Password reset, Custom security attributes, Risky activities, Identity Governance, External Identities, and Learn & support. A red box highlights the 'Worlanyo Akpatsa' user card, which includes the text 'Student Number 101590287'. The main content area is titled 'New - Conditional Access policy'. It has sections for 'Name' (containing 'MFA for sensitive app'), 'Assignments' (with 'Users' and '0 users and groups selected'), 'Target resources' (with 'No target resources selected'), and 'Network' (with a 'NEW' button). Under 'Enable policy', the 'Report-only' option is selected. A warning message at the bottom says, 'It looks like you're about to manage your organization's security configurations. That's great! You must first [disable security defaults](#) before enabling a Conditional Access policy.' A blue 'Create' button is at the bottom.

## Microsoft 365 Identity and Services II – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### B: Assign policy to specific users

Microsoft Entra admin center

Select users and groups

Try changing or adding filters if you don't see what you're looking for.

Search

22 results found

All Users Groups

| Name             | Type | Details                                        |
|------------------|------|------------------------------------------------|
| Quavious Migo    | User | quavio@GeorgeBROWN874.onmicrosoft.com          |
| Travis           | User | TravisScott@GeorgeBROWN874.onmicrosoft.com     |
| Worlanyo Akpatsa | User | WorlanyoAkpatsa@GeorgeBROWN874.onmicrosoft.com |
| Worlanyo-Shared  | User | worlanyoshared@GeorgeBROWN874.onmicrosoft.com  |

Selected (3)

Select

Microsoft Entra admin center

MFA for sensitive app

Conditional Access policy

View policy information View policy impact (Preview)

Any network or location

Conditions 4 conditions selected

Access controls

Grant 2 controls selected

Session 0 controls selected

Enable policy Report-only On Off

Save

Your "Require authentication strengths" configuration in grant control might not be valid for external users.

## Microsoft 365 Identity and Services II – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a sidebar with navigation links like Identity, Users, Groups, Devices, Applications, Protection, Identity Governance, and Learn & support. A red box highlights the user profile information: "Worlanyo Akpatsa" and "Student Number 101590287". The main content area is titled "MFA for sensitive app" and shows a "Conditional Access policy". It includes sections for "Name" (MFA for sensitive app), "Assignments" (Users, Specific users included), "Target resources" (set to "All resources (formerly 'All cloud apps'))", "Network" (Any network or location), and "Enable policy" (Report-only, On). A warning message at the bottom right says: "⚠️ Don't lock yourself out! This policy impacts the Azure portal. Before you continue, ensure that you or someone".

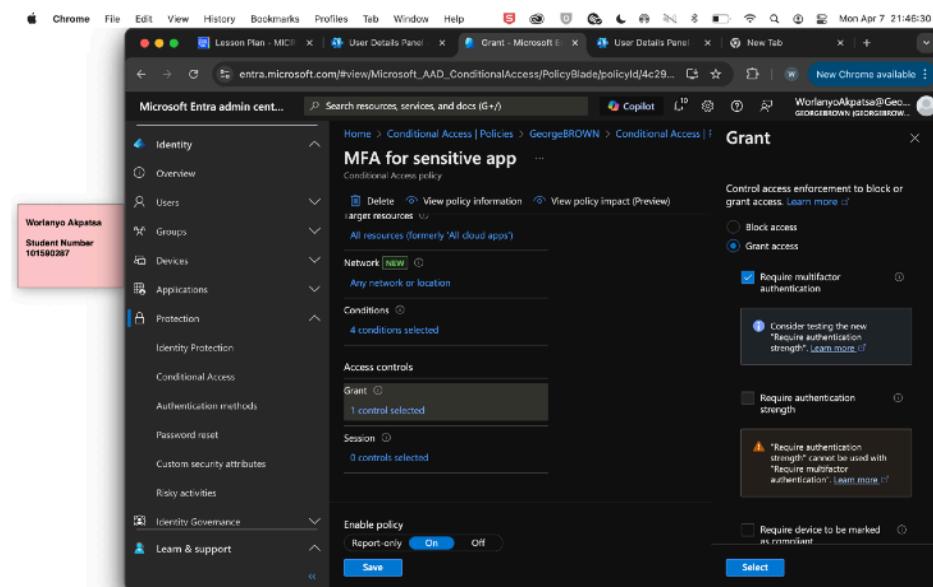
## Microsoft 365 Identity and Services II – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

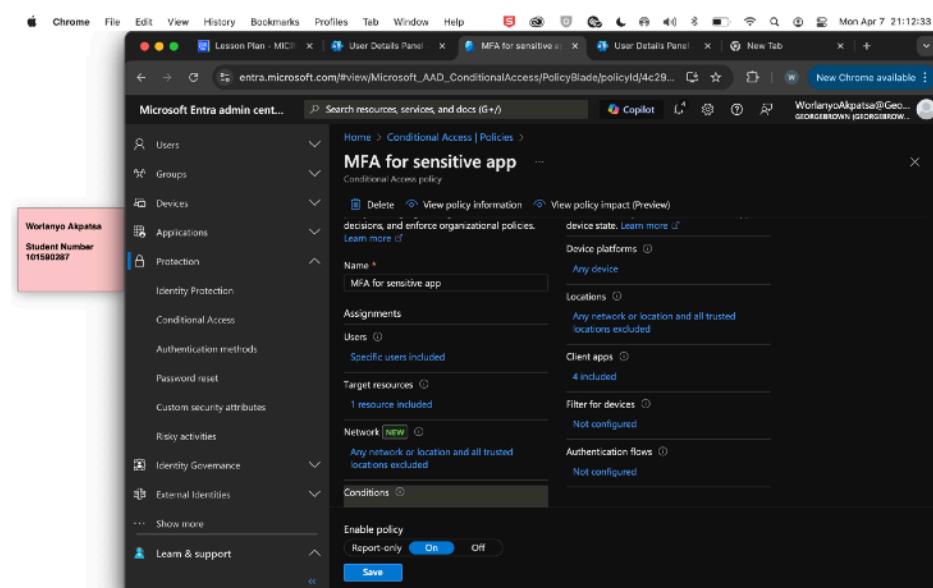
Term: Winter 2025

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

D: Editing Access Controls to require Multi-Factor Authentication



The screenshot shows the Microsoft Entra admin center interface. On the left, there's a sidebar with navigation links like Identity, Overview, Users, Groups, Devices, Applications, Protection, and more. The main area is titled 'Grant' under 'Conditional Access | Policies'. It shows a policy named 'MFA for sensitive app'. Under 'Access controls', the 'Grant' control is selected. A note says: "'Require authentication strength' cannot be used with 'Require multifactor authentication'. Learn more." The 'Enable policy' section has 'Report only' set to 'On'. At the bottom right, there's a 'Select' button.



The screenshot shows the 'MFA for sensitive app' policy configuration page. The 'Name' field is set to 'MFA for sensitive app'. In the 'Assignments' section, 'Users' are specified as 'Specific users included'. 'Target resources' include '1 resource included'. 'Network' settings are 'Any network or location and all trusted locations excluded'. 'Conditions' are set to '4 conditions selected'. The 'Enable policy' section has 'Report only' set to 'On'. At the bottom right, there's a 'Save' button.

## Microsoft 365 Identity and Services II – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### E: Toggling Enable Policy to “On”

The screenshot shows a Microsoft Entra admin center page titled "New - Microsoft Entra admin". The URL is [entra.microsoft.com/#view/Microsoft\\_AAD\\_ConditionalAccess/PolicyBlade](https://entra.microsoft.com/#view/Microsoft_AAD_ConditionalAccess/PolicyBlade). The left sidebar has a red box highlighting the user "Worlanyo Akpatsa" and "Student Number 101590287". The main content area shows a "New" blade for creating a Conditional Access policy. It includes sections for "Network" (Any network or location and all trusted locations excluded), "Conditions" (1 condition selected), "Access controls" (Grant 1 control selected), and "Session" (0 controls selected). At the bottom, there is an "Enable policy" section with a radio button set to "On". A warning message states: "⚠️ It looks like you're about to manage your organization's security configurations. That's great! You must first [disable security defaults](#) before enabling a Conditional Access policy." A blue "Create" button is at the bottom.

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### F: Disabling Security Defaults for Organization to enable Conditional Access

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with options like Users, Groups, Devices, Applications, Protection (Identity Protection, Conditional Access, Authentication methods, Password reset, Custom security attributes, Risky activities), Identity Governance, External Identities, and Learn & support. A red box highlights the 'Worlanyo Akpatsa' and 'Student Number 101590287' information in the sidebar.

The main content area is titled 'Conditional Access | Overview'. It shows a 'New' button for creating a 'Conditional Access policy'. Under 'Network', it says 'Any network or location and all trusted locations excluded'. There are sections for 'Conditions' (1 condition selected) and 'Access controls' (Grant, Session). Under 'Enable policy', the 'Report-only' option is selected. A warning message states: 'It looks like you're about to manage your organization's security enabling a Conditional Access policy.' Another message says: 'Security defaults must be disabled to enable Conditional Access.' At the bottom right are 'Create', 'Save', and 'Cancel' buttons.

On the right side of the screen, there's a 'Security defaults' section with a dropdown set to 'Disabled'. A note says: 'With security defaults disabled, your organization is vulnerable to common identity-related attacks.' Below that, it says: '99.9% of account compromise could be stopped by using multifactor authentication, which is a feature that security defaults provides.' Another note says: 'Microsoft's security teams see a drop of 80% in compromise rate when security defaults are enabled.'

A 'Reason for disabling' section includes a note: 'This feedback will be used to improve Microsoft products and services. [View privacy statement](#)' and several radio button options:

- Too many multifactor authentication sign-up requests
- Too many sign-in multifactor authentication challenges
- My organization is unable to use apps/devices
- My organization is planning to use Conditional Access
- Replace security defaults by enabling Conditional Access policies
- Other

## Microsoft 365 Identity and Services II – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

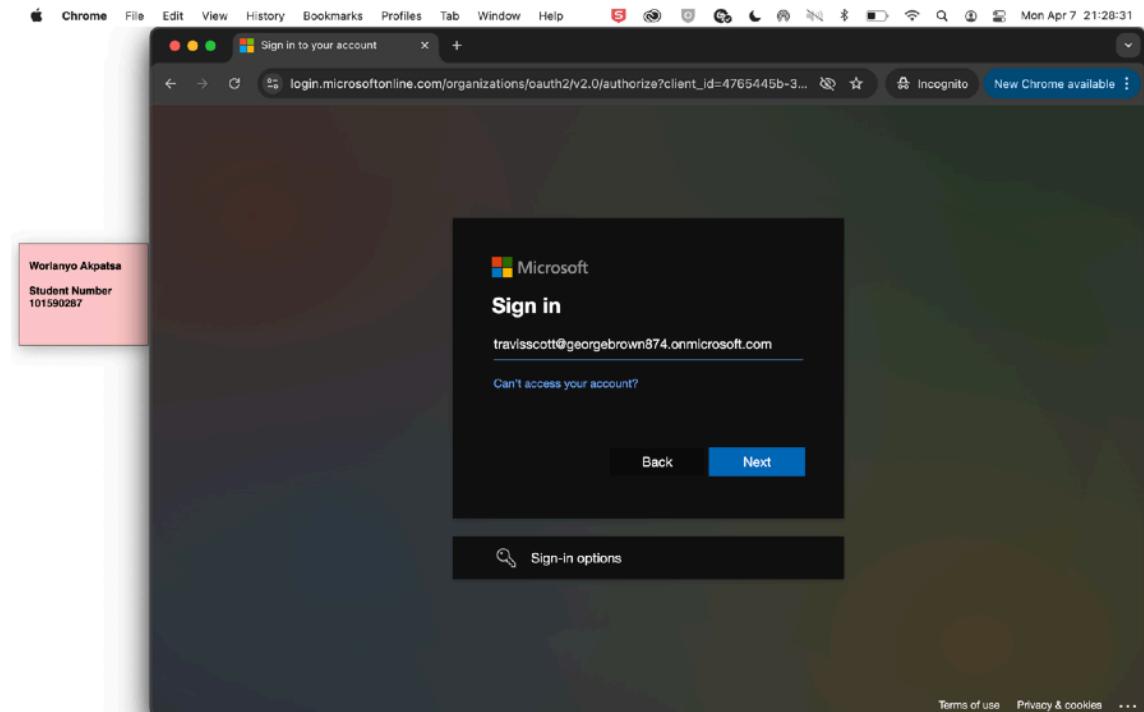
The screenshot shows a Microsoft Chrome browser window with three tabs open: "Lesson Plan - MICROSOFT 365", "User Details Panel - Microsoft", and "GeorgeBROWN - Microsoft Entra". The main content area is the Microsoft Entra admin center home page. On the left, there's a sidebar with navigation links like Users, Groups, Devices, Applications, Protection, Identity Governance, External Identities, and Learn & support. A red box highlights the "Worlanyo Akpatsa" and "Student Number 101590287" information in the sidebar. The main content area features a large blue "Secure access for a connected world" logo. To the right of the logo, a success message is displayed: "Successfully created 'MFA for sensitive app'". Below this message, a note says "Successfully created 'MFA for sensitive app'. Policy will be enabled in a few minutes." At the bottom of the page, there are links to "Learn about Microsoft Entra" and "Explore the Microsoft Entra product family".

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

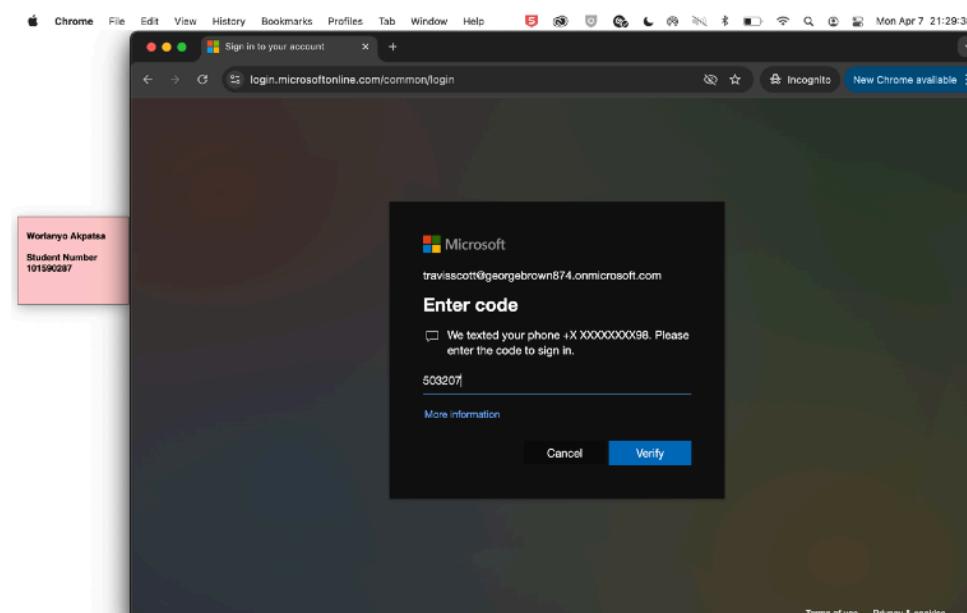
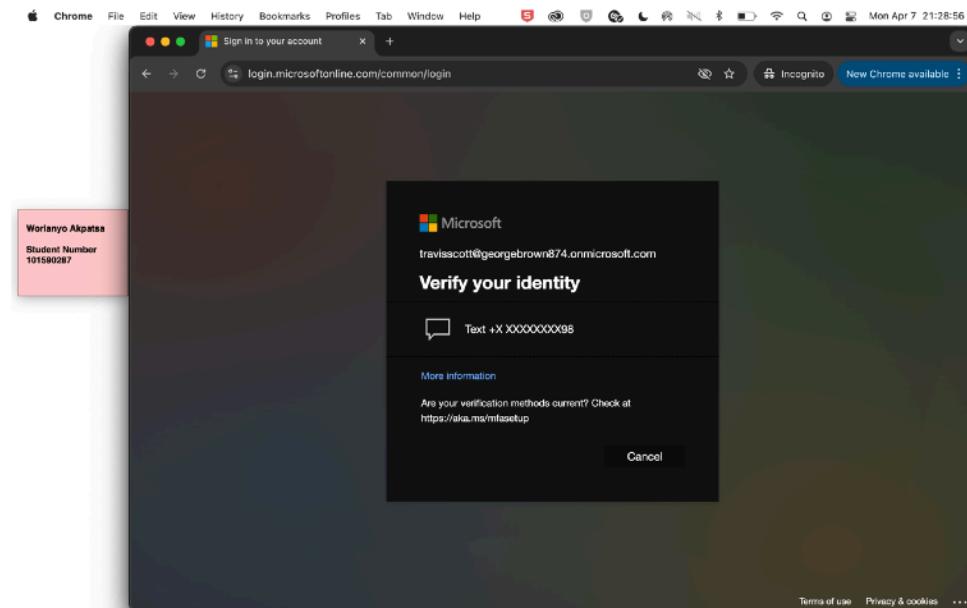


## Microsoft 365 Identity and Services II – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### B: MFA



## Microsoft 365 Identity and Services II – Enterprise Administration

---

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### C: Apps

The screenshot shows the Microsoft 365 Copilot Apps interface. At the top, there's a navigation bar with links for Home, Create, Pages, Apps (which is highlighted), and Admin. On the left, a sidebar displays the user's name (Worlanyo Akpatsa) and student number (101590287). The main area is titled "Apps" and features a grid of six large tiles: Word, Excel, PowerPoint, Outlook, OneDrive, and OneNote. Below this, there's a section titled "Explore by category" with several smaller tiles representing different Microsoft services: Forms, Calendar, Sway, Engage, Stream, Visio, To Do, and Project. A "Need help?" button is located at the bottom right of the explore section. The browser status bar at the bottom indicates it's a Monday at 21:30:52.

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### ***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  
Student ID: 101590287

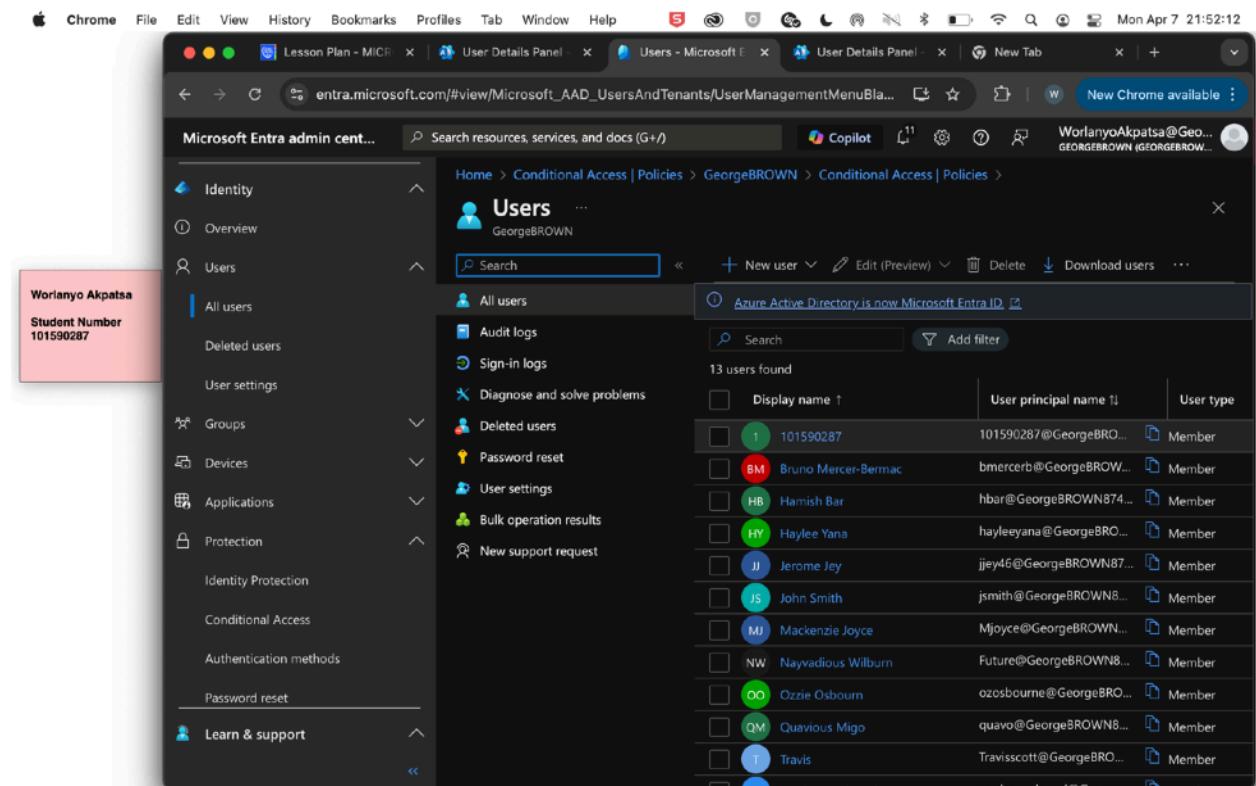
Term: Winter 2025

### 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



The screenshot shows the Microsoft Entra admin center interface. On the left, there is a navigation sidebar with the following sections:

- Identity**: Overview, Users (highlighted), Groups, Devices, Applications, Protection.
- Learn & support**.

The main content area displays the "Users" page for "GeorgeBROWN". It includes a search bar and buttons for "New user", "Edit (Preview)", "Delete", and "Download users". A message at the top right states "Azure Active Directory is now Microsoft Entra ID".

The "All users" table lists 13 users found:

| Display name        | User principal name       | User type |
|---------------------|---------------------------|-----------|
| 101590287           | 101590287@GeorgeBRO...    | Member    |
| Bruno Mercer-Bermac | bmercerb@GeorgeBROW...    | Member    |
| Hamish Bar          | hbar@GeorgeBROWN874...    | Member    |
| Haylee Yana         | hayleeyana@GeorgeBRO...   | Member    |
| Jerome Jey          | jjey46@GeorgeBROWN87...   | Member    |
| John Smith          | jsmith@GeorgeBROWN8...    | Member    |
| Mackenzie Joyce     | Mjoyce@GeorgeBROWN8...    | Member    |
| Nayvadious Wilburn  | Future@GeorgeBROWN8...    | Member    |
| Ozzie Osbourne      | ozosbourne@GeorgeBRO...   | Member    |
| Quavious Migo       | quavo@GeorgeBROWN8...     | Member    |
| Travis              | Travisscott@GeorgeBRO...  | Member    |
| Worlanyo Akpatsa    | worlanyoakpatsa@George... | Member    |

## Microsoft 365 Identity and Services II – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

The screenshot shows the Microsoft Entra admin center interface. On the left, there is a navigation sidebar with the following sections:

- Identity**:
  - Overview
  - Users
    - All users
    - Deleted users
    - User settings
  - Groups
  - Devices
  - Applications
  - Protection
    - Identity Protection
    - Conditional Access
    - Authentication methods
    - Password reset
  - Learn & support

A pink box highlights the "User settings" under the "Users" section.

In the main content area, the user **Jerome Jey** is selected. The URL in the browser bar is `entra.microsoft.com/#view/Microsoft_AAD_UsersAndTenants/UserProfileMenuBlade/~/ov...`. The user's profile picture is a yellow circle with "JJ". The basic info table includes:

| User principal name | jiej46@GeorgeBROWN874.onmicrosoft.com |
|---------------------|---------------------------------------|
| Object ID           | 23d60a48-f789-43ce-b27b-d1114be08741  |
| Created date time   | Mar 29, 2025, 9:52 PM                 |
| User type           | Member                                |
| Identities          | GeorgeBROWN874.onmicrosoft.com        |
| Group memberships   | 1                                     |
| Applications        | 0                                     |

## Microsoft 365 Identity and Services II – Enterprise Administration

---

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### C: Navigate to Assigned Roles

The screenshot shows the Microsoft Entra admin center interface. On the left, there is a navigation sidebar with the following sections:

- Identity**: Overview, Users (All users, Deleted users, User settings), Groups, Devices, Applications, Protection (Identity Protection, Conditional Access, Authentication methods), Password reset.
- Learn & support**

A pink box highlights the "Worlanyo Akpatsa" and "Student Number 101590287" information in the sidebar.

The main content area shows the user profile for **Jerome Jey | Assigned roles**. The "Assigned roles" section is selected in the left sidebar. The right pane displays the "Administrative roles" section, which includes a search bar, filter buttons, and a table header for "Role", "Description", and "Resource Name". The table body states "No directory roles assigned."

## Microsoft 365 Identity and Services II – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

D: Add role assignment (user Administrator)

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a sidebar with navigation links like Identity, Overview, Users, Groups, Devices, Applications, Protection, Learn & support, and a user profile section for 'Worlanyo Akpatsa' with 'Student Number 101590287'. The main content area is titled 'Directory roles' and lists various administrator roles with their descriptions. The 'User Administrator' role is selected, indicated by a checked checkbox. At the bottom of the list is an 'Add' button.

| Role                                    | Description                                                                                                                 |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Teams Communications Support Specialist | Can troubleshoot communications issues within Teams using basic tools.                                                      |
| Teams Devices Administrator             | Can perform management related tasks on Teams certified devices.                                                            |
| Teams Telephony Administrator           | Manage voice and telephony features and troubleshoot communication issues within the Microsoft Teams service.               |
| Tenant Creator                          | Create new Microsoft Entra or Azure AD B2C tenants.                                                                         |
| Usage Summary Reports Reader            | Can see only tenant level aggregates in Microsoft 365 Usage Analytics and Productivity Score.                               |
| <b>User Administrator</b>               | <b>Can manage all aspects of users and groups, including resetting passwords for limited admins.</b>                        |
| User Experience Success Manager         | View product feedback, survey results, and reports to find training and communication opportunities.                        |
| Virtual Visits Administrator            | Manage and share Virtual Visits information and metrics from admin centers or the Virtual Visits app.                       |
| Viva Glint Tenant Administrator         | Manage and configure Microsoft Viva Glint settings in the Microsoft 365 admin center.                                       |
| Viva Goals Administrator                | Manage and configure all aspects of Microsoft Viva Goals.                                                                   |
| Viva Pulse Administrator                | Can manage all settings for Microsoft Viva Pulse app.                                                                       |
| Windows 365 Administrator               | Can provision and manage all aspects of Cloud PCs.                                                                          |
| Windows Update Deployment Administrator | Can create and manage all aspects of Windows Update deployments through the Windows Update for Business deployment service. |
| Yammer Administrator                    | Manage all aspects of the Yammer service.                                                                                   |

## Microsoft 365 Identity and Services II – Enterprise Administration

---

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

E: Confirmed Assigned Role

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with a red box highlighting the user information: "Worlanyo Akpatsa" and "Student Number 101590287". The main content area is titled "Jerome Jey | Assigned roles". It shows a list of administrative roles with one item listed:

| Role               | Description                                                                                   |
|--------------------|-----------------------------------------------------------------------------------------------|
| User Administrator | Can manage all aspects of users and groups, including resetting passwords for limited admins. |

## Microsoft 365 Identity and Services II – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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)

The screenshot shows the Microsoft Entra admin center homepage. On the left, there is a navigation sidebar with the following sections:

- Home
- What's new
- Diagnose & solve problems
- Favorites
- Identity
  - Overview
  - Users
    - All users
    - Deleted users
    - User settings
  - Groups
  - Devices
  - Applications
- Learn & support

A red box highlights the "Worlanyo Akpatsa" and "Student Number 101590287" information in the sidebar. The main content area displays the user "GeorgeBROWN" (Jerome Jey) with their profile picture and contact information. A large blue "A" icon is prominently displayed. Below the user info, there are links for "Learn more about Microsoft Entra", "Provide feedback", and "Explore the Microsoft Entra product family".

## Microsoft 365 Identity and Services II – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

### B: Create user using Jey's entra admin account

The screenshot shows the Microsoft Entra Admin Center interface. On the left, there is a sidebar with the following navigation items:

- Home
- What's new
- Diagnose & solve problems
- Identity** (selected)
- Overview
- Users
  - All users
  - Deleted users
  - User settings
- Groups
- Devices
- Applications
- Learn & support

A red box highlights the "Identity" item in the sidebar.

The main content area is titled "Create new user" and contains the following fields:

- User principal name: jackiebrown (dropdown menu shows "GeorgeBROWN@contoso.com")
- Mail nickname: JackieBrown
- Display name: Jackie Brown
- Password: HuGelAumnt!
- Account enabled:

At the bottom, there are "Review + create" and "Next: Properties" buttons.

The screenshot shows the Microsoft Entra Admin Center interface. On the left, there is a sidebar with the following navigation items:

- Home
- What's new
- Diagnose & solve problems
- Identity** (selected)
- Overview
- Users
  - All users
  - Deleted users
  - User settings
- Groups
- Devices
- Applications
- Learn & support

A red box highlights the "Identity" item in the sidebar.

The main content area is titled "Users" and displays a list of users. At the top, it says "Successfully created user" and "Successfully created user Jackie Brown".

| Display name        | User principal name     | User type |
|---------------------|-------------------------|-----------|
| 101590287           | 101590287@GeorgeBRO...  | Member    |
| Bruno Mercer-Bernac | bmercerb@GeorgeBROW...  | Member    |
| Hannah Bar          | hb@#GeorgeBROWNB...     | Member    |
| Hayley Yara         | hayleyana@GeorgeBRO...  | Member    |
| Jerome Jey          | jjey46@GeorgeBRCWN87... | Member    |
| John Smith          | jsmith@GeorgeBROWNB...  | Member    |
| Kassandra Joyce     | mjoyce@GeorgeBROWNB...  | Member    |
| Nayvadious Wilburn  | future@GeorgeBROWNB...  | Member    |
| Ozzie Osborne       | osbourne@GeorgeBRO...   | Member    |
| Quavious Mingo      | quavo@GeorgeBROWNB...   | Member    |
| Travis Scott        | traviscott@GeorgeBRO... | Member    |

## Microsoft 365 Identity and Services II – Enterprise Administration

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

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with a red box highlighting the user 'Worlanyo Akpatsa' and 'Student Number 101590287'. The main content area is titled 'Jerome Jey | Assigned roles'. It shows a list of assigned roles under 'Administrative units'. One role is selected: 'User Administrator' (checked). A modal dialog box is open, asking 'Remove selected assignment(s)?' with 'Yes' and 'No' buttons. Below the modal, there's a search bar and a 'Add filters' button. The table headers are 'Role', 'Description', and 'Resource Name'. The row for 'User Administrator' has a tooltip: 'Can manage all aspects of users and groups, including resetting passwords for limited admins.'

This screenshot shows the same Microsoft Entra admin center interface as the previous one, but the 'User Administrator' role has been removed. The main content area now displays a message: 'No directory roles assigned.' The rest of the interface, including the sidebar and the list of other roles like 'Groups', 'Applications', and 'Devices', remains the same.

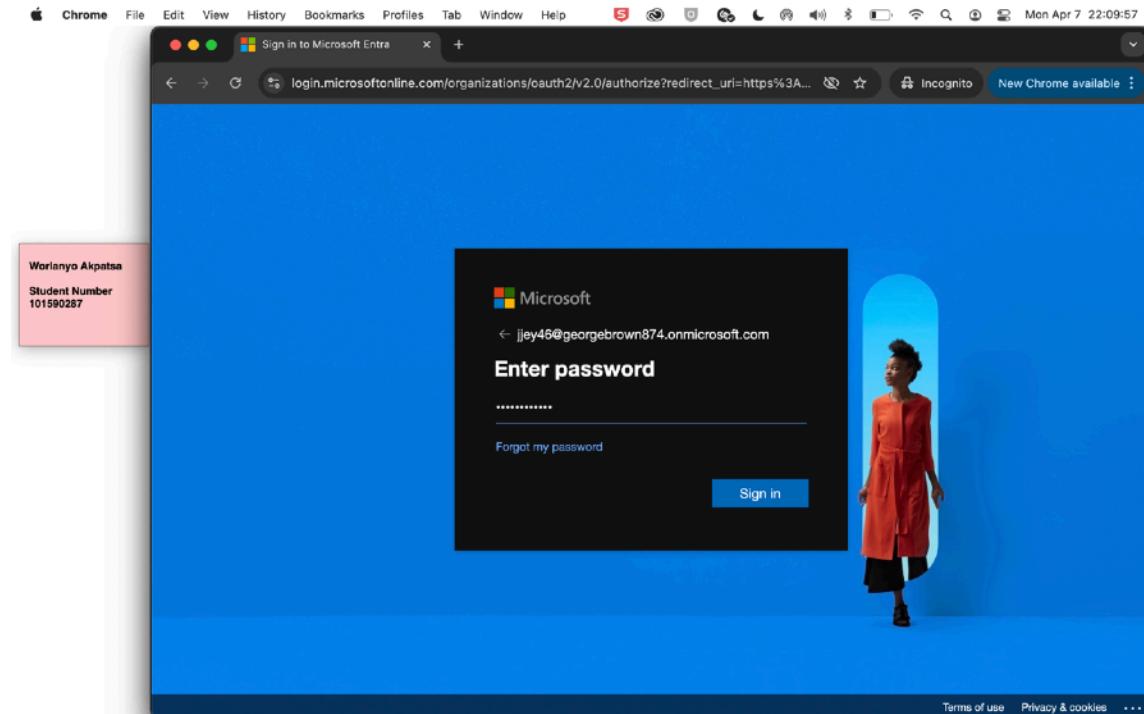
## Microsoft 365 Identity and Services II – Enterprise Administration

---

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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

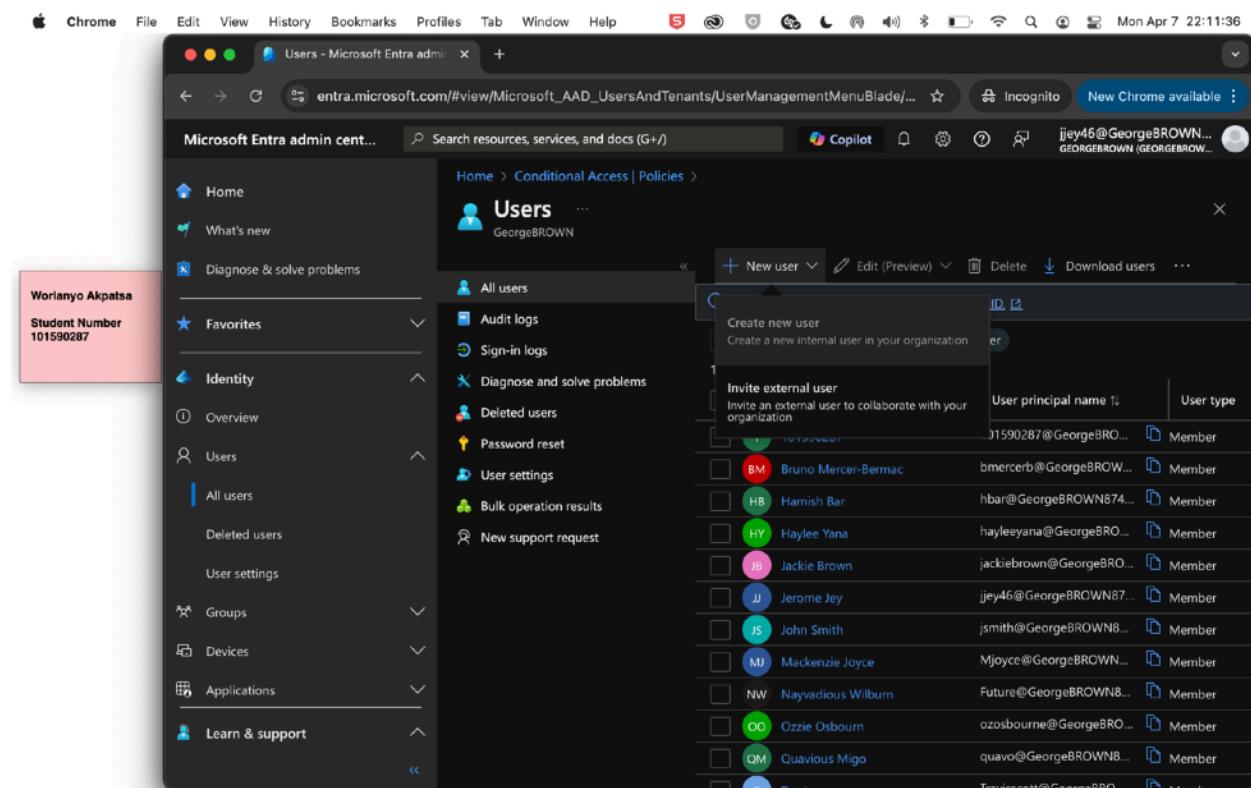


## Microsoft 365 Identity and Services II – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

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



The screenshot shows the Microsoft Entra admin center interface. The left sidebar is collapsed, and the main area displays the 'Users' page under 'Conditional Access | Policies'. The 'All users' section is selected, showing a list of users. A red box highlights the user 'Worlanyo Akpatsa' in the sidebar. The user list includes:

| User principal name    | User type |
|------------------------|-----------|
| 101590287@GeorgeBRO... | Member    |
| BM Bruno Mercer-Bermac | Member    |
| HB Hamish Bar          | Member    |
| HY Haylee Yana         | Member    |
| JB Jackie Brown        | Member    |
| JJ Jerome Jey          | Member    |
| JS John Smith          | Member    |
| MJ Mackenzie Joyce     | Member    |
| NW Nayadious Wilbum    | Future    |
| OO Ozzie Osbourn       | Member    |
| QM Quavious Migo       | Member    |
| TW Travisscott         | Member    |

## Microsoft 365 Identity and Services II – Enterprise Administration

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

Also cannot view conditional Access details and policies

The screenshot shows a Chrome browser window with the Microsoft Entra admin center URL: [entra.microsoft.com/#view/Microsoft\\_AAD\\_ConditionalAccess/ConditionalAccessBlade/~/O...](https://entra.microsoft.com/#view/Microsoft_AAD_ConditionalAccess/ConditionalAccessBlade/~/O...). The user is signed in as `jjey46@GeorgeBROWN...` with a GEORGEBROWN (GEORGEBROW...).

The left sidebar shows the user profile: **Worlanyo Akpatsa** and **Student Number 101590287**. The navigation menu includes: All users, Deleted users, User settings, Groups, Devices, Applications, Protection (Identity Protection, Conditional Access, Authentication methods, Password reset, Custom security attributes, Risky activities), Identity Governance, Learn & support.

The main content area is titled "Conditional Access | Overview". It displays the "Overview" section with a "Policies" card. A large error message "Insufficient privileges to complete the operation." is displayed, along with a "Summary" table:

| Session ID                        | Resource ID                     |
|-----------------------------------|---------------------------------|
| 4a56d28e60054eeefb01b0c6d092c4678 | Not available                   |
| Extension                         | Microsoft_AAD_ConditionalAccess |
| Error code                        | 403                             |
| Content                           | PolicyOverview.ReactView        |

Student Name: Worlanyo Akpatsa  
Student ID: 101590287

Term: Winter 2025

*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.