

Microsoft 365 Administration Portfolio - Task Documentation

This document outlines the tasks performed as part of a Microsoft 365 administration project, demonstrating key skills in user management, security, and data handling within an M365 environment.

Project Overview

As an IT administrator, I was tasked by HR personnel to onboard new employees into the organization's Microsoft 365 environment. This involved creating user accounts, assigning roles, configuring security policies, and managing user access to organizational resources and applications. The project also included tasks related to user offboarding and email management.

Organizational Policies & Requirements

The following organizational policies and requirements guided the execution of these tasks:

- **User Group Membership:** All employees must belong to the "Employees" group.
- **Microsoft Teams Integration:** A Teams channel must be provisioned for the "Employees" group to facilitate seamless information dissemination.
- **Entra ID (Azure AD) Integration:** User creation and management must be performed using Entra ID. Users must have access to organizational data and applications.
- **Self-Service Password Reset (SSPR):** Users must be able to reset their passwords without administrative support.
- **Multi-Factor Authentication (MFA):** MFA must be configured for users with a periodic authentication requirement of 14 days.
- **Password Policy Restrictions:** Users are restricted from using the following words in their passwords: "passwords", "user", "organization", "Microsoft".
- **Role-Based Access Control (RBAC):**
 - HR Managers are required to have the **User Administrator** role.
 - Finance Analysts are required to have the **Billing Administrator** role.
- **Email Management (Offboarding):** Upon an employee's departure, their email must be handed over to their manager.

Task Breakdown & Deliverables

The following tasks were executed, with corresponding screenshots provided as evidence:

1. **User Provisioning:**
 - Screenshot of **all created users** in Entra ID.
2. **Application Access & Teams Integration Verification:**
 - Screenshots verifying that **two random users** can access the organization's applications.
 - Screenshots verifying that the "Employees" group is **enabled in Teams** for the users.
3. **Self-Service Password Reset (SSPR) Verification:**
 - Screenshot of the **SSPR reset** for "Chika" and "Ayo" from the audit log.
4. **Security Policy Configuration:**
 - Screenshot of the **MFA policy** demonstrating the 90-day periodic re-authentication requirement.
 - Screenshot of the **password policy** enforcing the specified word restrictions.
5. **Role-Based Access Control (RBAC) Implementation:**
 - Screenshots of the **Entra ID roles** assigned to the specified users (HR Managers as User Administrators, Finance Analysts as Billing Administrators).
6. **Email Handover (Offboarding Scenario):**
 - Screenshot verifying that **Henry's mail is visible in his manager's inbox**.

Microsoft 365 Administration Portfolio - Task Report

Executive Summary

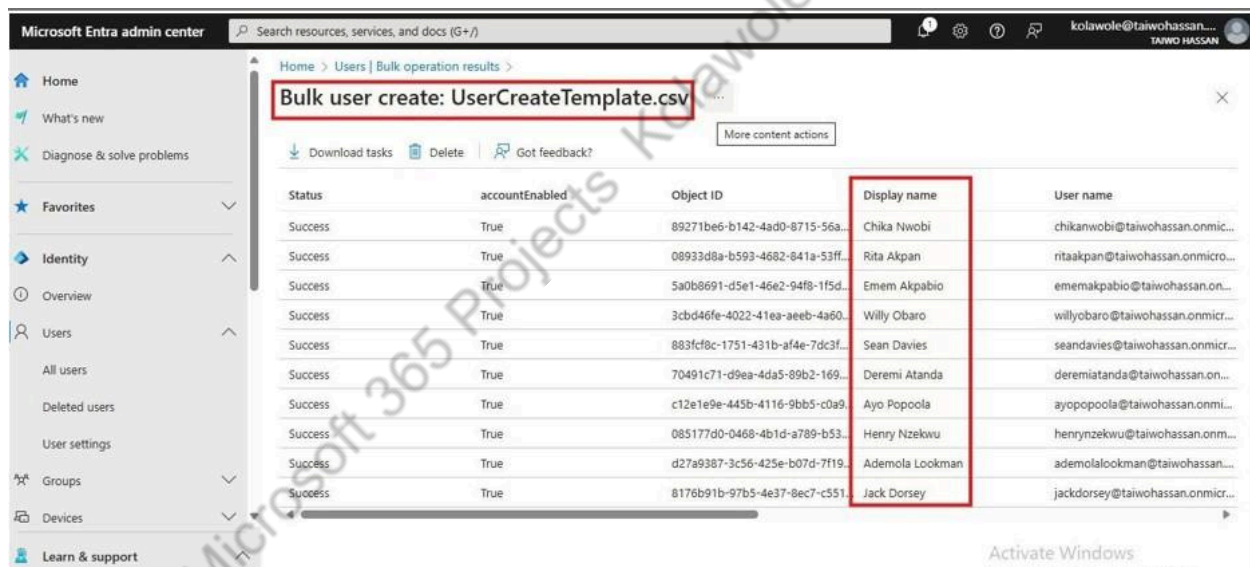
This report details the execution of various Microsoft 365 administration tasks, as outlined by organizational policies and requirements. The objective was to demonstrate proficiency in user management, security policy configuration, role-based access control, and email management within an M365 environment. Each task's process and the corresponding deliverable are documented with supporting explanations.

Key Project Users and Roles

List of the users and their specific roles or functions as used in this Microsoft 365 administration project:

- **Rita Akpan:** User Administrator
- **Willy Obaro:** Billing Administrator
- **Chika Nwobi:** General User (involved in Self-Service Password Reset)
- **Ayo Popoola:** General User / Manager (involved in Self-Service Password Reset, and received Henry's mailbox)
- **Henry Nzekwu:** General User (involved in application access verification, email sending, and mailbox handover)

1. User Provisioning



The screenshot shows the Microsoft Entra admin center interface. A red box highlights the title 'Bulk user create: UserCreateTemplate.csv'. Below it, a table lists the results of the bulk user creation. The table has columns for Status, accountEnabled, Object ID, Display name, and User name. All users listed are successful and have their accounts enabled.

Status	accountEnabled	Object ID	Display name	User name
Success	True	89271be6-b142-4ad0-8715-56a...	Chika Nwobi	chikanwobi@taiwohassan.onmic...
Success	True	08933d8a-b593-4682-841a-53ff...	Rita Akpan	ritaakpan@taiwohassan.onmicr...
Success	True	5a0b8691-d5e1-46e2-94f8-1f5d...	Emem Akpabio	ememakpabio@taiwohassan.on...
Success	True	3cbd46fe-4022-41ea-aeeb-4a60...	Willy Obaro	willyobaro@taiwohassan.onmicr...
Success	True	883fc8c-1751-431b-af4e-7dc3f...	Sean Davies	seandavies@taiwohassan.onmicr...
Success	True	70491c71-d9ea-4da5-89b2-169...	Dereemi Atanda	deremiatanda@taiwohassan.on...
Success	True	c12e1e9e-445b-4116-9bb5-c0a9...	Ayo Popoola	ayopopoola@taiwohassan.onmi...
Success	True	085177d0-0468-4b1d-a789-b53...	Henry Nzekwu	henrynzekwu@taiwohassan.onm...
Success	True	d27a9387-3c56-425e-b07d-7f19...	Ademola Lookman	ademolalookman@taiwohassan...
Success	True	8176b91b-97b5-4e37-8ec7-c551...	Jack Dorsey	jackdorsey@taiwohassan.onmicr...

Screenshot of **all created users** in Entra ID

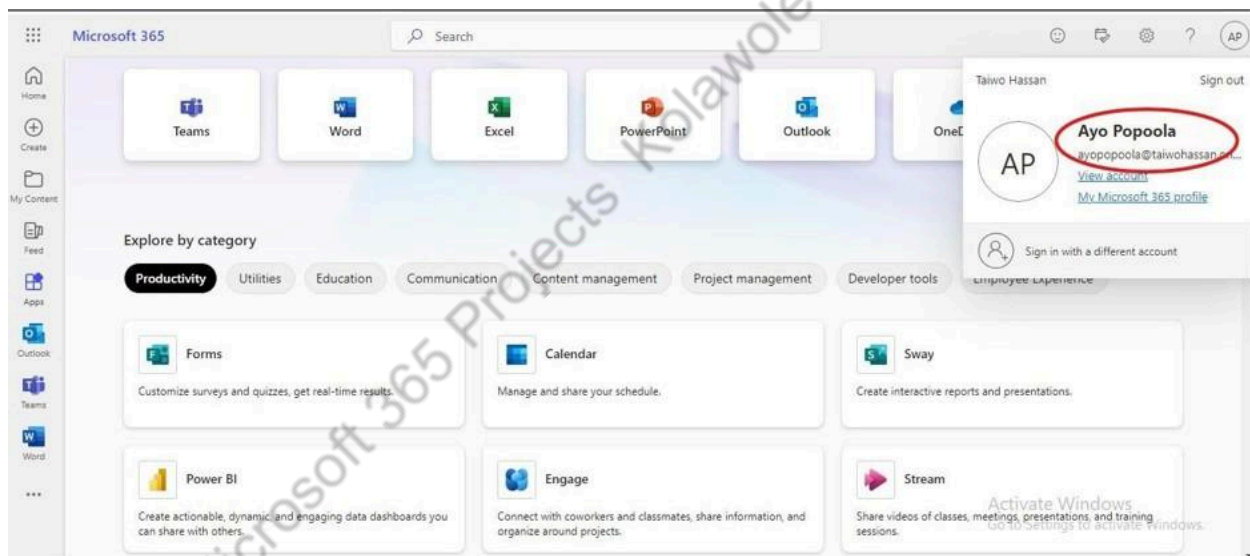
Deliverable: Screenshot showing the "Bulk user create: UserCreateTemplate.csv" results with all new users successfully provisioned.

Process Undertaken:

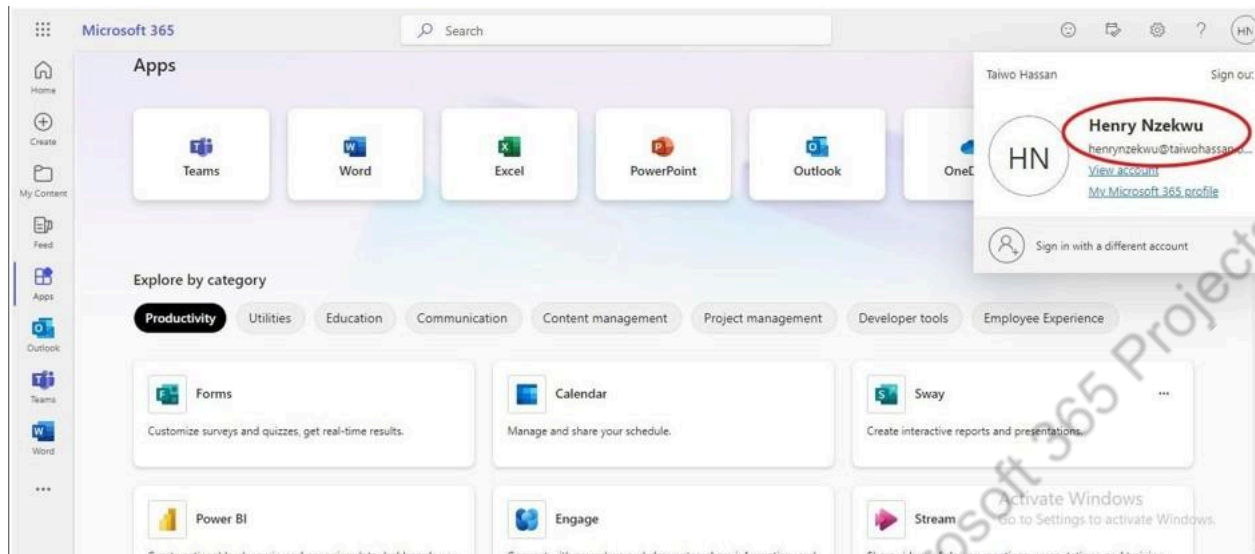
1. **Navigation:** Logged into the Microsoft Entra admin centre (formerly Azure Active Directory).

2. **User Access:** Navigated to "Identity" > "Users".
3. **Bulk Creation:** Utilized the "Bulk user create" feature. This involved:
 - Downloading the provided CSV template.
 - Populating the template with the details of all new employees (Display Name, User Principal Name, etc.).
 - Uploading the completed CSV file through the portal.
4. **Verification:** The system displayed the "Bulk operation results" page, confirming the "Status" as "Success" for each new user, along with their "Display name" and "User name".

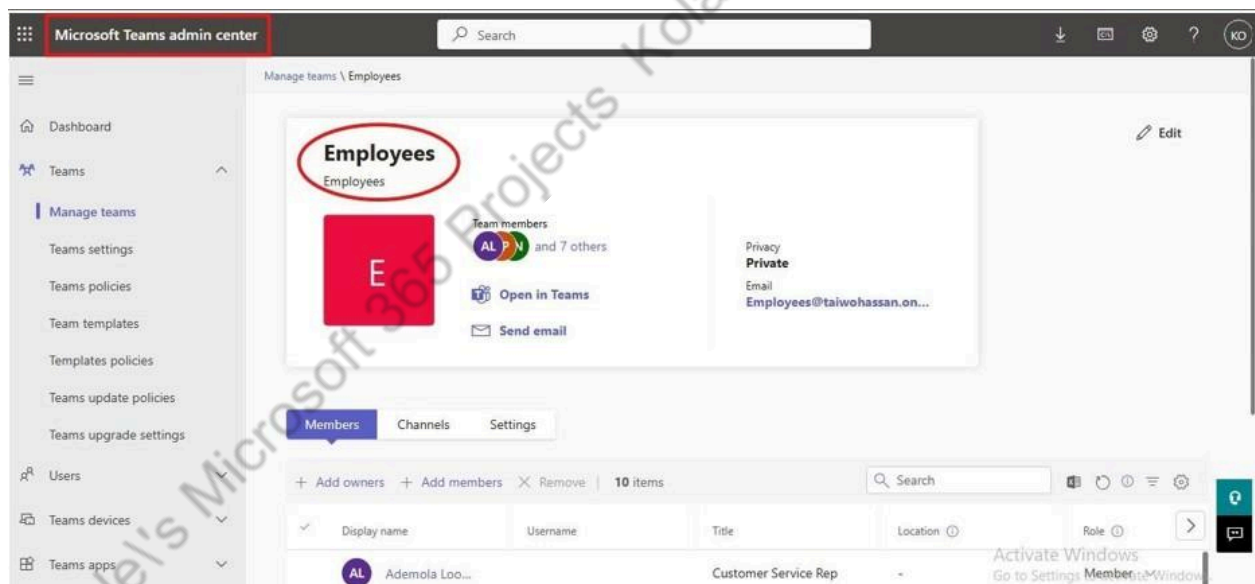
2. Application Access & Teams Group Verification



A random user, "Ayo Popoola", can access Organization applications



A random user, "Henry Nzekwu", can access Organization applications



Employees Group enabled in Microsoft Teams for Users

Deliverable:

- Screenshots verifying that "Ayo Popoola" and "Henry Nzekwu" can access organization applications from the Microsoft 365 portal.
- Screenshot confirming the "Employees" group is enabled and accessible within Microsoft Teams.

Process Undertaken:

For App Access (Ayo Popoola & Henry Nzekwu):

1. **User Login:** Logged into the Microsoft 365 portal separately as "Ayo Popoola" and "Henry Nzekwu".
2. **App Verification:** Confirmed visibility and potential access to various core organization applications (e.g., Teams, Word, Excel, PowerPoint, Outlook) directly from the Microsoft 365 portal home page under the "Apps" section.

For Teams Group Verification:

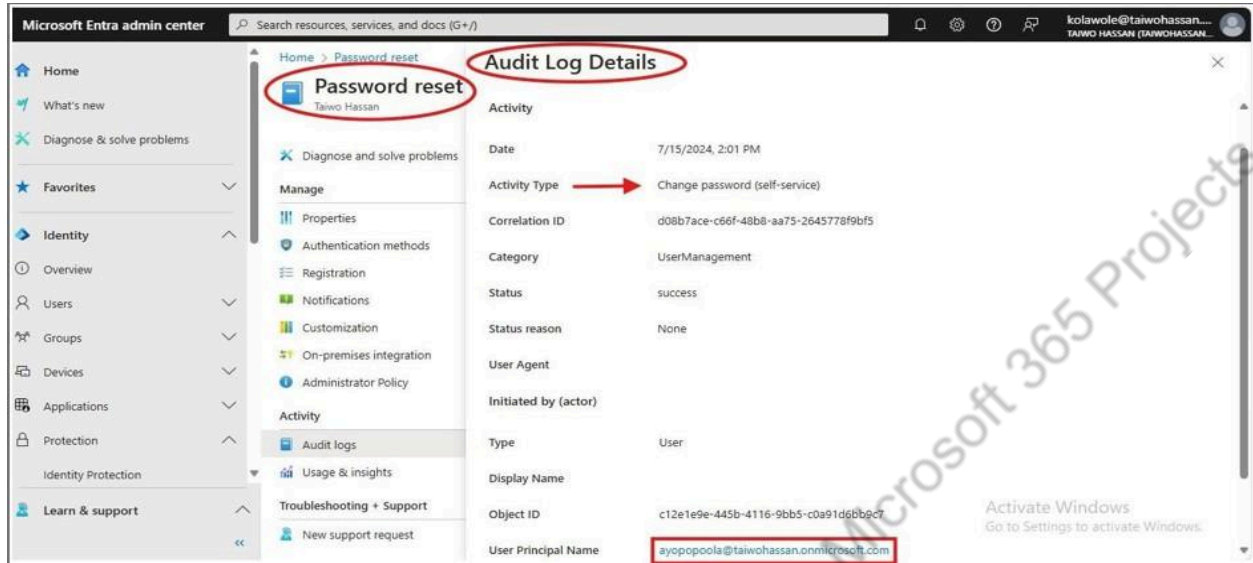
1. **Teams Admin Centre Access:** Logged into the Microsoft Teams admin centre.
2. **Manage Teams:** Navigated to "Teams" > "Manage teams".
3. **Group Location:** Located and selected the "Employees" team within the list of managed teams.
4. **Membership and Status Check:** Verified the team's active status and confirmed that users were correctly listed as members under the "Members" tab.
5. **Client-Side Verification:** From a user's Microsoft Teams client, navigated to the "Teams" section, confirmed the presence of the "Employees" group (e.g., within "M365 GROUP 1"), and verified access to its "General" channel and content, including the welcome message.

3. SSPR Reset from Audit Log (Chika Nwobi and Ayo Popoola)

The screenshot displays the Microsoft Entra admin center interface. On the left, the 'Password reset' link is highlighted in the 'Activity' section. The main pane shows 'Audit Log Details' for a specific activity. The activity is a 'Change password (self-service)' performed on 7/15/2024 at 1:43 PM. The user agent is 'User' and the user principal name is 'chikanwobi@taiwohassan.onmicrosoft.com'. The status is 'success'.

Field	Value
Date	7/15/2024, 1:43 PM
Activity Type	Change password (self-service)
Correlation ID	27486810-1caa-4c16-a92e-18a7b2e2cbb8
Category	UserManagement
Status	success
Status reason	None
User Agent	User
Initiated by (actor)	
Type	User
Display Name	
Object ID	89271be6-b142-4ad0-8715-56a2d85b1b61
User Principal Name	chikanwobi@taiwohassan.onmicrosoft.com

SSPR Reset For Chika Nwobi From Audit Log



SSPR Reset For Ayo Popoola From Audit Log

Deliverable: Screenshots of the Entra ID audit logs displaying successful Self-Service Password Resets for "Chika Nwobi" and "Ayo Popoola".

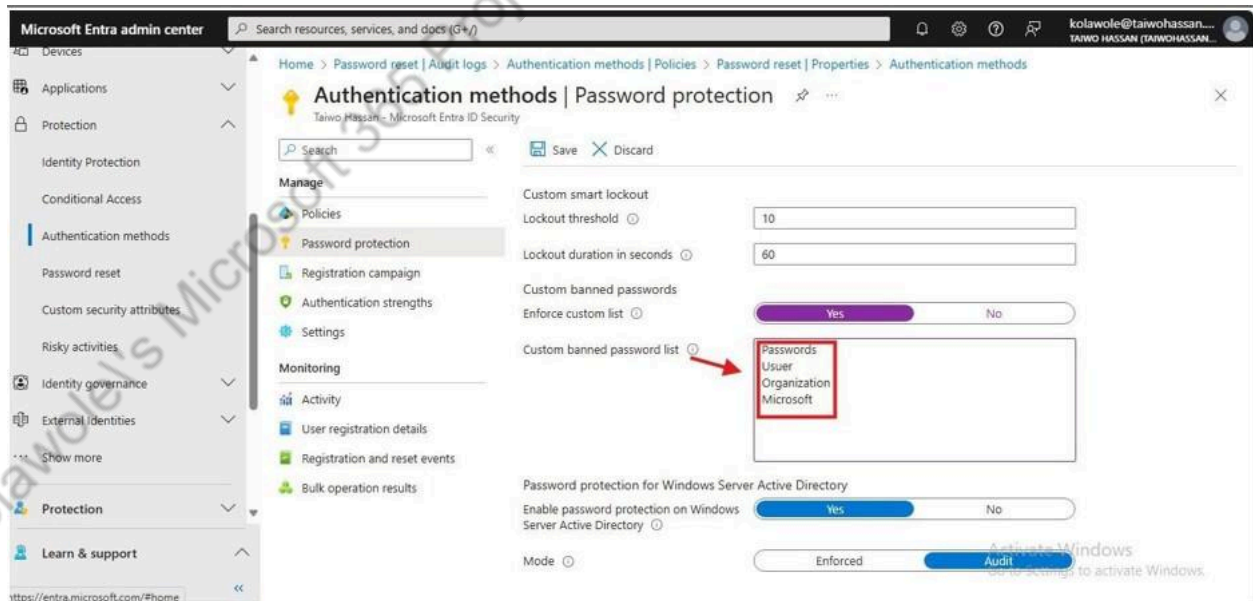
Process Undertaken:

1. **Navigation:** Logged into the Microsoft Entra admin centre.
2. **Audit Logs Access:** Navigated to "Identity" > "Audit logs".
3. **Filtering:** Applied the following filters to isolate the relevant events:
 - o **Activity Type:** Selected "Change password (self-service)".
 - o **User Principal Name:** Filtered for `chikanwobi@taiwohassan.onmicrosoft.com` for Chika's entry and `ayopopoola@taiwohassan.onmicrosoft.com` for Ayo's entry.
4. **Event Review:** Examined the detailed entries for each user, confirming the "Status" of the operation as "SUCCESS" and identifying the "Activity" as a "Password reset" initiated by the "User".

4. MFA and Password Policy Configuration



MFA service settings showing the configured device trust duration.



Entra ID Password Protection settings with the custom banned password list

Deliverable:

- Screenshot of MFA service settings showing the configured device trust duration.
- Screenshot of Entra ID Password Protection settings with the custom banned password list.

Process Undertaken:

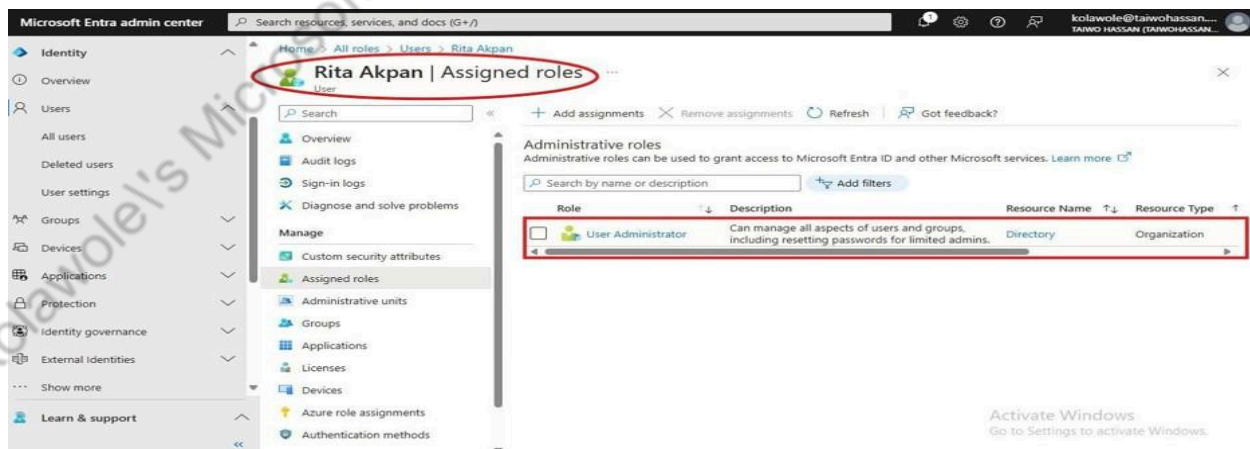
For MFA Configuration:

1. **Navigation:** Logged into the Microsoft Entra admin centre.
2. **Authentication Methods:** Navigated to "Protection" > "Authentication methods".
3. **MFA Settings:** Accessed "Multi-factor authentication" settings (or relevant Conditional Access policy).
4. **Trust Device Duration:** Configured the "Number of days users can trust devices" to 90 days. Enabled verification options such as "Text message to phone" and "Notification through mobile app".

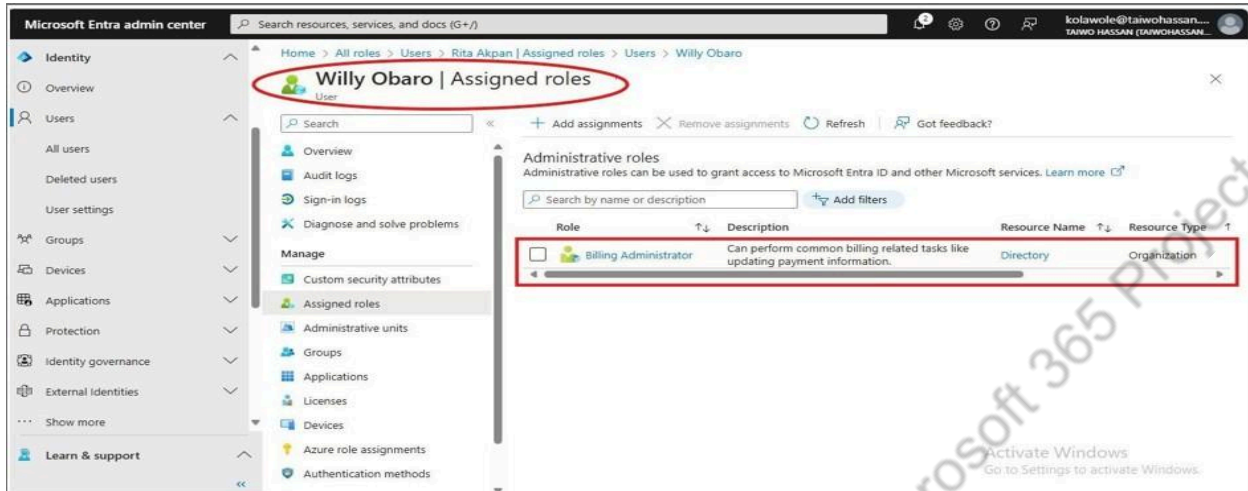
For Password Policy Configuration:

1. **Navigation:** Logged into the Microsoft Entra admin centre.
2. **Password Protection:** Navigated to "Protection" > "Authentication methods" > "Password protection".
3. **Custom Banned Passwords:** Enabled the "Enforce custom list" option.
4. **Word List Addition:** Added the required words to the "Custom banned password list": "Passwords", "User", "Organization", "Microsoft".
5. **Policy Verification (Implicit):** The presence of these words in the configured list demonstrates the policy's enforcement capabilities.

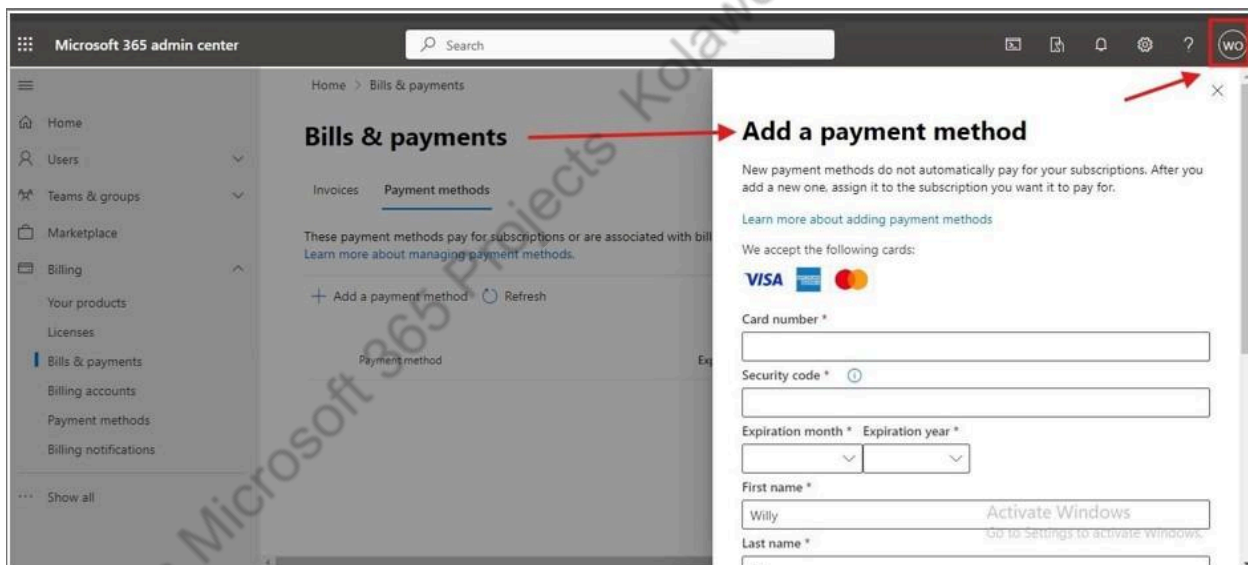
5. Role-Based Access Control (RBAC) Implementation



"Rita Akpan" is assigned the "User Administrator" role



"Willy Obaro" is assigned the "Billing Administrator" role



Test to prove "Willy Obaro" as a Financial Analyst can perform the Billing Administrator role

Deliverable:

- Screenshot confirming "Rita Akpan" is assigned the "User Administrator" role.
- Screenshot confirming "Willy Obaro" is assigned the "Billing Administrator" role, including a demonstration of role functionality.

Process Undertaken:

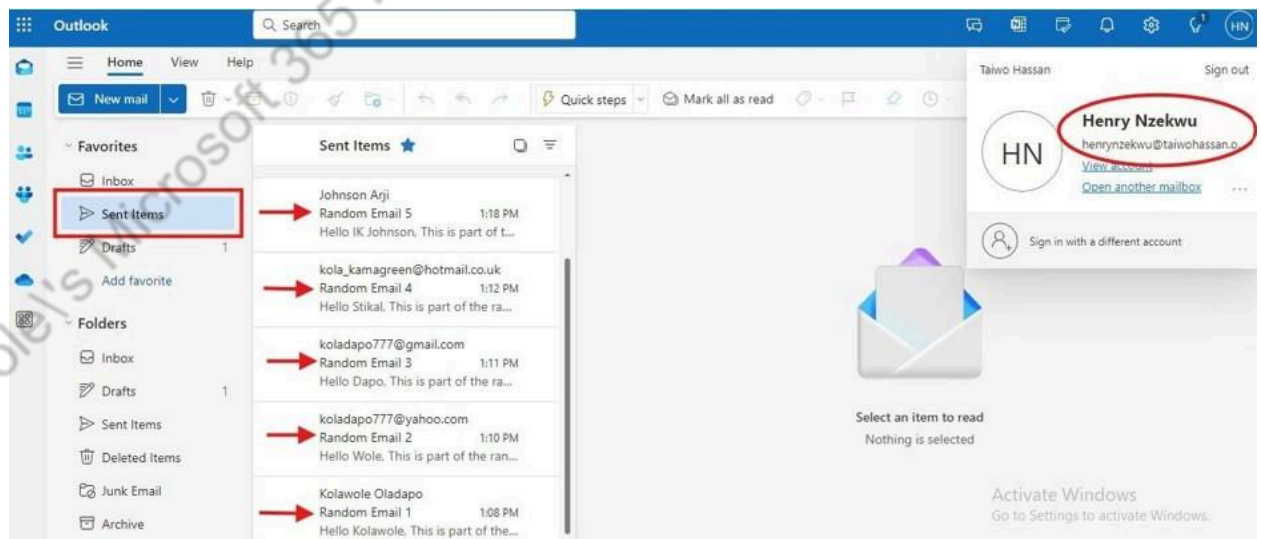
For Assigning User Administrator (Rita Akpan):

1. **Navigation:** Logged into the Microsoft Entra admin centre.
2. **User Access:** Navigated to "Identity" > "Users", then searched for and selected "Rita Akpan".
3. **Role Assignment:** Accessed "Assigned roles" from Rita Akpan's user profile menu.
4. **Role Selection:** Clicked "+ Add assignments" and selected "User Administrator", confirming its assignment to the "Directory" resource.

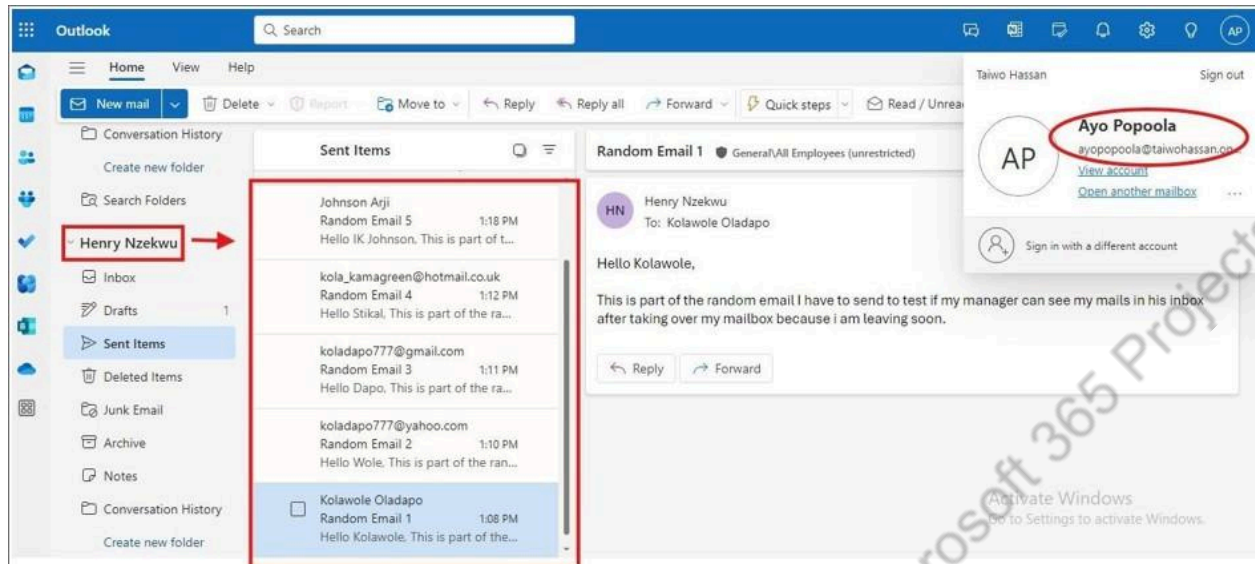
For Assigning Billing Administrator (Willy Obaro):

1. **Navigation:** Logged into the Microsoft Entra admin centre.
2. **User Access:** Navigated to "Identity" > "Users", then searched for and selected "Willy Obaro".
3. **Role Assignment:** Accessed "Assigned roles" from Willy Obaro's user profile menu.
4. **Role Selection:** Clicked "+ Add assignments" and selected "Billing Administrator", confirming its assignment to the "Directory" resource.
5. **Role Functionality Test:** Logged into the Microsoft 365 admin centre as "Willy Obaro". Navigated to "Billing" > "Bills & payments" > "Payment methods" and successfully accessed the "Add a payment method" page, demonstrating the permissions granted by the "Billing Administrator" role.

6. Email Management (Offboarding)



"Henry Nzekwu's" mailbox (specifically "Sent Items")



Henry's Email is visible and accessible in "Ayo Popoola", Henry's Manager, after offboarding

Deliverable: Screenshot showing Henry Nzekwu's mailbox (specifically "Sent Items") visible and accessible within Ayo Popoola's (the manager's) Outlook inbox.

Process Undertaken:

1. **Email Sending (Henry):** Logged in as "Henry Nzekwu" and sent 5 random emails to various recipients, populating his "Sent Items" folder.
2. **Mailbox Delegation (Administrator Action):** As an administrator, accessed the Exchange Admin Centre (EAC) or utilized PowerShell to:
 - Grant "Ayo Popoola" (Henry's manager) "Full Access" or "Read and Manage" permissions to Henry Nzekwu's mailbox.
3. **Delegated Mailbox Access (Manager's Action):** Logged into Outlook as "Ayo Popoola".
4. **Open Shared Mailbox:** Added Henry Nzekwu's mailbox as a shared mailbox or opened it directly via Outlook's "Open & Export" feature.
5. **Email Verification:** Navigated to Henry Nzekwu's "Sent Items" folder within Ayo Popoola's Outlook view, confirming the presence and content of the previously sent emails.

END OF TASK

Kolawole's Microsoft 365 Projects Kolawole's Microsoft 365 Projects