

Microsoft 365 Identity and Services – Enterprise Administration

Case Project:

Task 1: Exchange Administration

- 1.1 Create two user mailboxes named “yourname-User1” and yourname-User2”
- 1.2 Create a distribution list named: Yourname-DistList”
 - Distribution list should receive emails from outside company
 - Distribution list should be controlled with Owner and only the owner can add/remove members
- 1.3 Add users created in step one to the distribution list created in step 2
- 1.4 From you GBC email, send an email to the distribution list and show both users received it.
- 1.5 Select 5 Users to receive updates before they’re released to everyone else.
- 1.6 Add this disclaimer to your emails
 - “This disclaimer is added by yourname for case project”
- 1.7 Configure DLP so no health information can be shared using email or sharepoint
- 1.8 Block emails with .html attachments

Task 2: Power Platform Administration

- 2.1 Enable tenant level analytics
- 2.2 Identify the list of existing connections in Power Apps (may be empty)
- 2.3 Identify of the name of the AI Builder used to “Extract information from receipts”

Task 3: MFA

- 3.1 Enable Multi Factor Authentication
- 3.2 Enforce MFA
- 3.3 Setup MFA

Task 4: Customer lockbox

- 4.1 Enable customer lockbox

Task 5: Security

- 5.1 Block .html extension for emails
- 5.2 Create anti Phishing policy and apply your desired settings and make sure the spam messages are moved to quarantine
- 5.3 Create a Safe link policy

~~~~~

Paste your screenshots here

## Microsoft 365 Identity and Services – Enterprise Administration

---

### Task 1: Exchange Administration

1.1 Create two user mailboxes named “yourname-User1” and yourname-User2”

To create and manage a **user mailbox**, we can add or delete a user mail box on Microsoft 365 admin center (active users page). We can create a **shared mailbox** on Exchange admin center.

The screenshot shows the Microsoft 365 Admin Center interface. The left sidebar has sections like Home, Recipients, Mailboxes, Mail flow, Roles, Migration, Mobile, Reports, Insights, Public folders, Organization, Settings, and Other features. The main area is titled "Manage mailboxes" with a sub-instruction: "Create and manage settings for shared mailboxes. You can also manage settings for user mailboxes, but to add or delete them you must go to the Microsoft 365 admin center and do this on the active users page. Learn more about mailboxes". Below this is a table listing 8 items:

| Display name ↑   | Email address                             | Recipient type | Archive status | Last modified time  |
|------------------|-------------------------------------------|----------------|----------------|---------------------|
| 101511792        | jennifermbaegbu.onmicrosoft.com           | UserMailbox    | None           | 4/7/2024, 9:50 PM   |
| Chinedu          | Chi@jennifermbaegbu.onmicrosoft.com       | UserMailbox    | None           | 4/7/2024, 12:15 ... |
| Enya Irish       | enya@jennifermbaegbu.onmicrosoft.com      | UserMailbox    | None           | 4/6/2024, 9:39 PM   |
| George Frank     | gfrank020@jennifermbaegbu.onmicrosoft.com | UserMailbox    | None           | 4/7/2024, 12:16 ... |
| Grace Kelly      | gkelly010@jennifermbaegbu.onmicrosoft.com | UserMailbox    | None           | 4/6/2024, 11:34 ... |
| Jennifer Mbaegbu | iam@jennifermbaegbu.onmicrosoft.com       | UserMailbox    | None           | 4/5/2024, 11:37 ... |

Figure 1: Add or Delete User Mailbox via Microsoft 365 Admin Center

The screenshot shows the Microsoft 365 Admin Center interface. The left sidebar has sections like Home, Users (Active users, Contacts, Guest users, Deleted users), Devices, Teams & groups, Billing, Setup, Health, and Show all. The main area is titled "Add a user" under "Active users". The "Basics" tab is selected. The form fields include:

- First name: Jennifer
- Last name: Mbaegbu
- Display name: Jennifer Mbaegbu
- Username: jennifer-User1
- Domains: jennifermbaegbu.onmicrosoft.com
- Automatically create a password (checkbox checked)
- Password (input field)
- Require this user to change their password when they first sign in (checkbox)
- Send password in email upon completion (checkbox)

Figure 2: Create User mailbox on Microsoft 365 Admin Center

## Microsoft 365 Identity and Services – Enterprise Administration

The image displays two screenshots of Microsoft 365 administration interfaces.

**Microsoft 365 Admin Center (Top Screenshot):**

- Left Sidebar:** Home, Users (Active users selected), Contacts, Guest users, Deleted users, Devices, Teams & groups, Billing, Setup, Health, Show all.
- Header:** Active users - Microsoft 365 admin center, https://portal.office.com/AdminPortal/Home/#/users, Search bar.
- Content:** Active users table with columns: Display name ↑, Username, Licenses. Data includes:
  - [REDACTED] jennifermbaegbu.onmicrosoft.com Microsoft 365 Business Premium
  - Chinedu Chi@jennifermbaegbu.onmicrosoft.com Microsoft 365 Business Premium
  - Enya Irish eirish@jennifermbaegbu.onmicrosoft.com Microsoft 365 Business Premium
  - George Frank gfrank020@jennifermbaegbu.onmicrosoft.com Microsoft 365 Business Premium
  - Grace Kelly gkelly010@jennifermbaegbu.onmicrosoft.com Microsoft 365 Business Premium
  - Jennifer-Shared jen-shared@jennifermbaegbu.onmicrosoft.com Microsoft 365 Business Premium
  - Jennifer Mba jennifer-User2@jennifermbaegbu.onmicrosoft.com Microsoft 365 Business Premium
  - Jennifer Mbaegbu jennifer-User1@jennifermbaegbu.onmicrosoft.com Microsoft 365 Business Premium
  - Jennifer Mbaegbu iam@jennifermbaegbu.onmicrosoft.com Power Pages vTrial for Makers , Microsoft Copilot Studio Vi
  - Lorenzo Falcon lfalcon@jennifermbaegbu.onmicrosoft.com Microsoft 365 Business Premium
- Bottom Right:** Help & support, Give Feedback buttons.

**Exchange Admin Center (Bottom Screenshot):**

- Left Sidebar:** Home, Recipients, Mailboxes (selected), Groups, Resources, Contacts, Mail flow, Roles, Migration, Mobile, Reports, Insights, Public folders, Organization, Settings.
- Header:** Exchange admin center, https://admin.exchange.microsoft.com/#/mailboxes, Search (Preview) bar.
- Content:** Manage mailboxes table with columns: Display name ↑, Email address, Recipient type, Archive status, Last modified time. Data includes:
  - [REDACTED] jennifermbaegbu.onmicrosoft.com UserMailbox None 4/7/2024, 9:50 PM
  - Chinedu Chi@jennifermbaegbu.onmicrosoft.com UserMailbox None 4/7/2024, 12:15 ...
  - Enya Irish eirish@jennifermbaegbu.onmicrosoft.com UserMailbox None 4/6/2024, 9:39 PM
  - Jennifer Mba** jennifer-User2@jennifermbaegbu.onmicrosoft.com UserMailbox None 4/20/2024, 1:49 ...
  - Jennifer Mbaegbu** jennifer-User1@jennifermbaegbu.onmicrosoft.com UserMailbox None 4/20/2024, 1:43 ...
  - Jennifer Mbaegbu iam@jennifermbaegbu.onmicrosoft.com UserMailbox None 4/5/2024, 11:37 ...
  - Jennifer-Shared Jennifer-Shared@jennifermbaegbu.onmicrosoft.com SharedMailbox None 4/6/2024, 11:40 ...
  - Lorenzo Falcon lfalcon@jennifermbaegbu.onmicrosoft.com UserMailbox None 4/6/2024, 9:59 PM

Figure 3: New User Mailbox active on Exchange Admin Center

## Microsoft 365 Identity and Services – Enterprise Administration

### 1.2 Create a distribution list named: Yourname-DistList"

- Distribution list should receive emails from outside company
- Distribution list should be controlled with Owner and only the owner can add/remove members

The screenshot shows the Microsoft Exchange Admin Center interface. The left sidebar has a 'Groups' section selected. The main area is titled 'Groups' and shows a table of existing groups. A new group, 'Jennifer-Dist', has been added and is listed with the email address 'jennifer-dist@jenifermbaegbu.onmicrosoft.com'. The 'Distribution list' tab is highlighted in the top navigation bar.

Figure 4: Create Distribution List

The screenshot shows the 'Add a group' wizard step 'Group type'. It lists several options: Basics (selected), Owners, Members, Settings (highlighted with a blue circle), and Finish. To the right, there are fields for 'Group email address' (set to 'jennifer-distlist') and 'Domains' (set to 'jenifermbaegbu.onmicrosoft.com'). Under 'Communication', there is a checked checkbox for 'Allow people outside of my organization to send email to this Distribution group'. Under 'Joining the group', the 'Closed' option is selected. Under 'Leaving the group', the 'Closed' option is also selected. A note at the bottom states: 'After the group is created, you'll be able to edit settings to specify if external senders can email the group and whether or not to send copies of group conversations to members.' At the bottom of the screen are 'Back', 'Next', and 'Cancel' buttons.

Figure 5: Distribution List can receive emails from external contacts and closed settings -[only owner can add or remove members]

### 1.3 Add users created in step one to the distribution list created in step 2

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot displays two identical views of a Microsoft 365 distribution list named "Jennifer-DistList". The interface includes a header bar with icons for refresh, close, and user information (Jennifer Mbaegbu, JM). Below the header are two tabs: "General" and "Members", with "General" being the active tab.

**General Tab Content:**

- Name:** Jennifer-DistList
- Description:** Distribution list group • 1 owner • 2 members
- Basic information:**
  - Name:** Jennifer-DistList
  - Description:** Distribution list that can receive emails from outside company and controlled by an owner.
- Email addresses:**
  - Primary:** jennifer-distlist@jennifermbaegbu.onmicrosoft.com
- Aliases:**
  - Edit**
- Role assignments:** Not allowed
- Created on:** 4/20/2024, 2:12 PM

**Members Tab Content:**

- Owners (1):** Jennifer Mbaegbu (iam@jennifermbaegbu.onmicrosoft.com)
- View all and manage owners**
- Members (2):**

| Jennifer Mbaegbu                    | Jennifer Mba                        |
|-------------------------------------|-------------------------------------|
| jennifer-                           | jennifer-                           |
| User1@jennifermbaegbu.onmicrosoft.c | User2@jennifermbaegbu.onmicrosoft.c |
| om                                  | om                                  |
- View all and manage members**

## Microsoft 365 Identity and Services – Enterprise Administration

---

The screenshot shows the Microsoft 365 Identity and Services - Enterprise Administration interface. At the top, there is a dark header bar with icons for file, notifications, settings, and help, followed by the user name "Jennifer Mbaegbu" and a profile icon. Below the header, the main content area has a title "Jennifer-DistList" with a large blue circular icon containing a white letter "J". Below the title, it says "Distribution list group • 1 owner • 2 members". There are three tabs: "General", "Members" (which is underlined in blue), and "Settings".  
  
The "Members" tab displays two sections: "Owners (1)" and "Members (2)".  
  
Under "Owners (1)", there is one entry:  

Jennifer Mbaegbu  
iam@jennifermbaegbu.onmicrosoft.com

[View all and manage owners](#)

  
  
Under "Members (2)", there are two entries:  

|                                       |                                       |
|---------------------------------------|---------------------------------------|
| Jennifer Mbaegbu<br>jennifer-         | Jennifer Mbaegbu<br>jennifer-         |
| User1@jennifermbaegbu.onmicrosoft.com | User2@jennifermbaegbu.onmicrosoft.com |

[View all and manage members](#)

## Microsoft 365 Identity and Services – Enterprise Administration

1.4 From you GBC email, send an email to the distribution list and show both users received it.

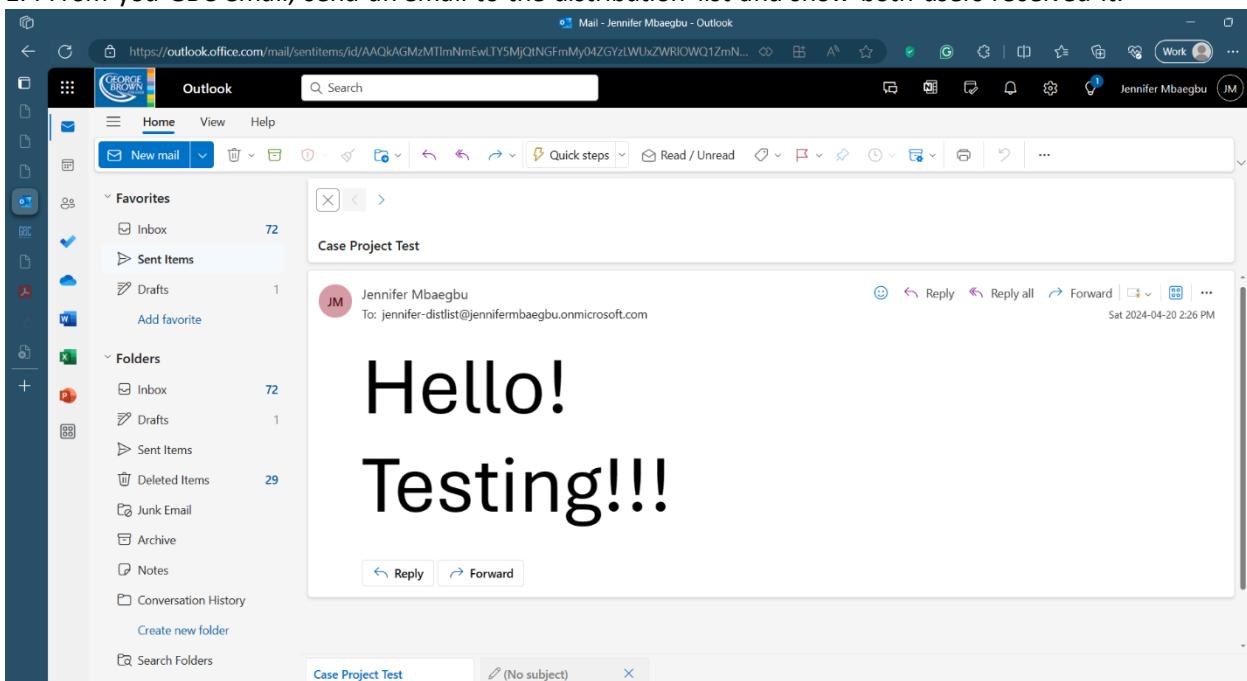


Figure 6: Test Email sent via GBC email

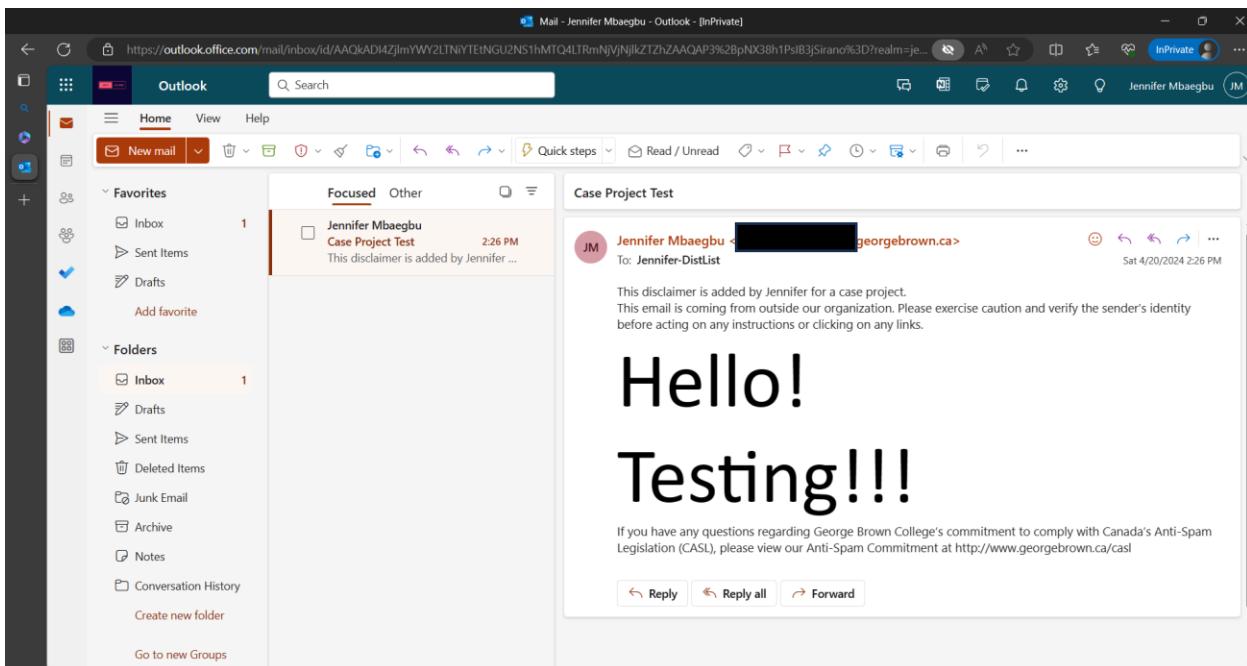


Figure 7: Email received via jennifer-User1@domain.com

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot displays two Microsoft Outlook windows side-by-side.

**Top Window (Distribution List):** The title bar reads "Mail - Jennifer Mbaegbu - Outlook - [InPrivate]". The main content shows a distribution list named "Jennifer-DistList" with 2 members: Jennifer Mbaegbu and Jennifer Mba. The "About" section states it's a distribution list that can receive emails from outside the company and is controlled by an owner. The "Members" section lists the two members with their respective icons and names.

**Bottom Window (Incoming Email):** The title bar reads "Mail - Jennifer Mba - Outlook - [InPrivate]". The inbox shows an incoming email from "Case Project Test" with the subject "Case Project Test". The email body contains a disclaimer: "This disclaimer is added by Jennifer Mbaegbu for a case project. This email is coming from outside our organization. Please exercise caution and verify the sender's identity before acting on any instructions or clicking on any links." Below the disclaimer, the message body says "Hello! Testing!!!". At the bottom of the email view, there are buttons for "Reply", "Reply all", and "Forward".

Figure 8: Email received via second User's email

## Microsoft 365 Identity and Services – Enterprise Administration

### 1.5 Select 5 Users to receive updates before they're released to everyone else.

The screenshot shows the Microsoft 365 admin center interface. On the left, there's a navigation sidebar with various categories like Resources, Billing, Support, Settings, Admin centers, and Reports. The main area is titled "Organization profile" and contains a table of settings. One row, "Release preferences", is expanded, showing options for releasing features: "Standard release for everyone", "Targeted release for everyone", and "Targeted release for select users". The third option is selected. Below this, there are two buttons: "Select users" and "Upload users". A list of users currently targeted for release is shown, including Chinedu, Enya Irish, Jennifer Mbægbu, and Lorenzo Falcon, each with a "Remove" button. A "Save" button is at the bottom right.

Figure 9: Target Release Preference

### 1.6 Add this disclaimer to your emails “This disclaimer is added by yourname for case project”

The screenshot shows the Exchange admin center interface. The left sidebar includes Home, Recipients, Mail flow, Rules, Remote domains, Accepted domains, Connectors, Alerts, Alert policies, Roles, Migration, Mobile, Reports, Insights, Public folders, Organization, and Settings. The main area is titled "Rules" and shows a table of existing rules: "External Disclaimer", "Monitor Email Links2", "Block HTML Attachm...", and "Case Project". The "Case Project" rule is selected. A modal window titled "Case Project" is open, showing the "Conditions" tab. It has a "Name" field set to "Case Project" and a "Apply this rule if" section where "The sender" is set to "is external/internal". Below that is a "Do the following" section with "Apply a disclaimer to the ..." and "prepend a disclaimer" options, along with a note about prepending a specific message and falling back to "Wrap". At the bottom of the modal are "Save" and "Cancel" buttons.

Figure 10: Case-Project-Disclaimer created

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the Exchange admin center interface. On the left, there's a navigation pane with various options like Home, Recipients, Mail flow, and Rules. The 'Rules' section is currently selected. In the main content area, there's a 'Rules' heading and a table listing four rules. One rule, 'Case Project', is highlighted and has its details expanded on the right. The 'Mode' for this rule is set to 'Enforce'. Other settings shown include Severity (High), Senders address (Matching HeaderOrEnvelope), Priority (3), and a description ('Is received from 'Outside the organization''. There are also sections for 'Rule settings' and 'For rule processing errors'.

Figure 11 Case-Project-Disclaimer Enabled

### 1.7 Configure DLP so no health information can be shared using email or sharepoint

The screenshot shows the Microsoft Compliance portal's 'Create policy' wizard. The first step is 'Start with a template or create a custom policy'. It includes a sidebar with steps: 'Template or custom policy', 'Name', 'Admin units', 'Locations', 'Policy settings', 'Policy mode', and 'Finish'. Below this, there's a search bar and a dropdown for 'All countries or regions'. The main area shows 'Categories' (Financial, Medical and health, Privacy, Custom) and 'Regulations' (Australia Health Records Act (HRIP Act), Canada Health Information Act (HIA), Canada Personal Health Information Act (PHIA) - Manitoba, Canada Personal Health Act (PHIPA) - Ontario, U.K. Access to Medical Reports Act, U.S. Health Insurance Act (HIPAA)). The 'Medical and health' category is selected, and 'Canada Personal Health Act (PHIPA) - Ontario' is detailed as helping detect the presence of information subject to Canada Personal Health Information Protection Act (PHIPA) for Ontario, including data like passport numbers and health information. A list of protected information is also provided.

Figure 12: Create DLP to stop users from sharing health information

## Microsoft 365 Identity and Services – Enterprise Administration

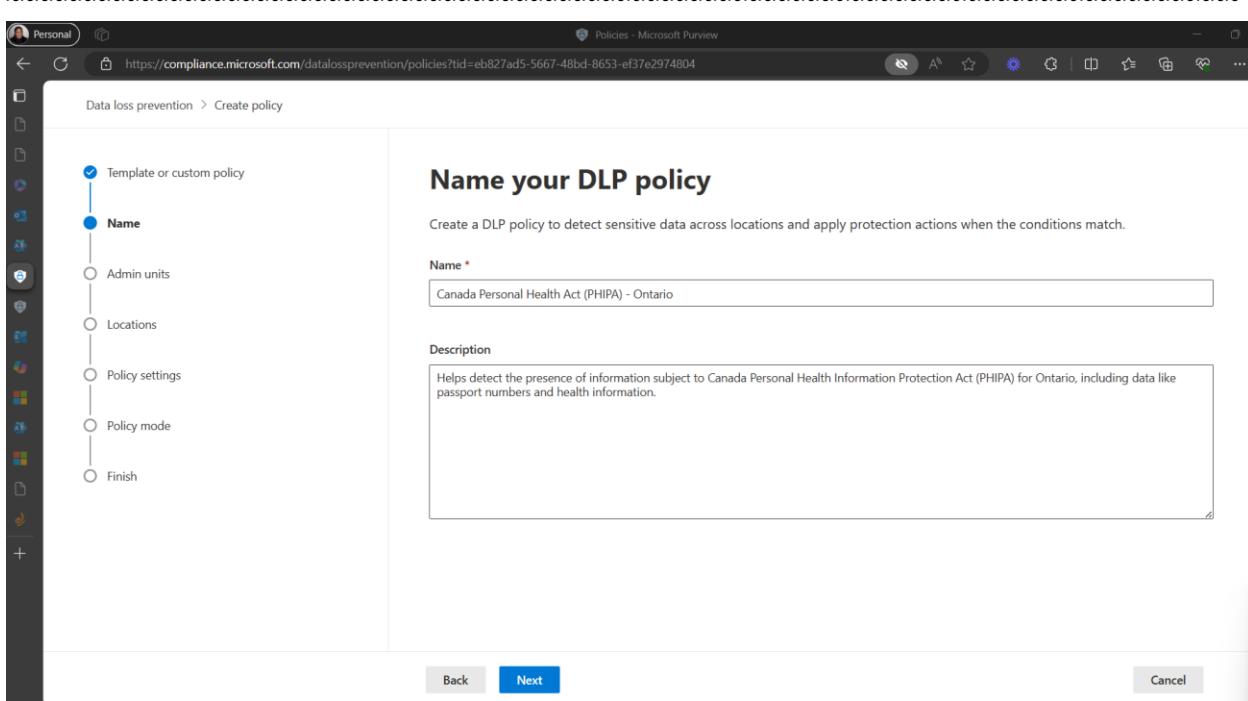


Figure 13: Name Data Loss Prevention Policy

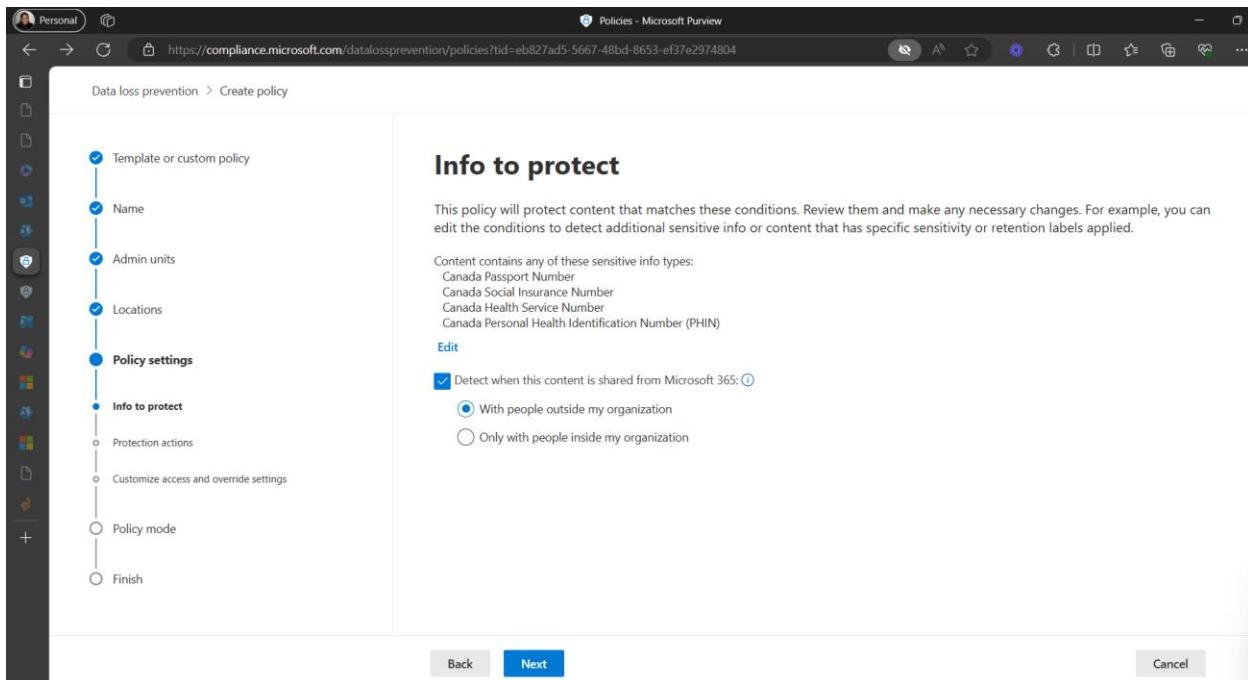


Figure 14: Information to protect

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows a browser window titled "Policies - Microsoft Purview" with the URL <https://compliance.microsoft.com/datalossprevention/policies?tid=eb827ad5-5667-48bd-8653-ef37e2974804>. The page is titled "Data loss prevention > Create policy". On the left, a vertical navigation pane lists steps: "Template or custom policy" (checked), "Name" (checked), "Admin units" (checked), "Locations" (checked), "Policy settings" (checked), "Info to protect" (unchecked), "Protection actions" (checked), "Customize access and override settings" (unchecked), "Policy mode" (unchecked), and "Finish" (unchecked). The main content area is titled "Protection actions" and contains the following text: "We'll automatically create detailed activity reports so you can review the content that matches this policy. What else do you want to do?". It includes several checkboxes for optional actions:

- When content matches the policy conditions, show policy tips to users and send them an email notification  
Tips appear to users in their apps (like Outlook, OneDrive, and SharePoint) and help them learn how to use sensitive info responsibly. You can use the default tip or customize it to your liking. [Learn more about notifications and tips](#)
- Detect when a specific amount of sensitive info is being shared at one time  
At least  or more instances of the same sensitive info type
- Send incident reports in email  
By default, you and your global admin will automatically receive the email. Incident reports are supported only for activity in Exchange, SharePoint, OneDrive, and Teams.  
[Choose what to include in the report and who receives it](#)
- Send alerts if any of the DLP rules match  
By default, you and any global admins will automatically be alerted if a DLP rule is matched.  
[Customize alert configuration](#)
- Restrict access or encrypt the content in Microsoft 365 locations

At the bottom are "Back", "Next", and "Cancel" buttons.

Figure 15: Actions to take

The screenshot shows a browser window titled "Policies - Microsoft Purview" with the URL <https://compliance.microsoft.com/datalossprevention/policies?tid=eb827ad5-5667-48bd-8653-ef37e2974804>. The page is titled "Data loss prevention > Create policy". On the left, a vertical navigation pane lists steps: "Template or custom policy" (checked), "Name" (checked), "Admin units" (checked), "Locations" (checked), "Policy settings" (checked), "Policy mode" (checked), and "Finish" (unchecked). The main content area is titled "Policy mode" and contains the following text: "You can test this policy before turning it on to verify if it needs improvement or if it meets all your objectives. If you turn the policy on right away, you can edit it later and safely test those changes in simulation mode." It includes a yellow callout box with the text: "At this time, simulation mode isn't supported for these locations you selected: On-premises file repositories." Below this, there are three radio button options:

- Run the policy in simulation mode  
We'll show you items that match the policy's conditions to help you evaluate its impact. Your data won't be affected; the policy stays off while in simulation mode. [Learn more about simulation mode](#)
  - Show policy tips while in simulation mode.
  - Turn the policy on if it's not edited within fifteen days of simulation
- Turn the policy on immediately  
After the policy is created, it'll take up to an hour before any changes are enforced.
- Leave the policy turned off  
Decide to test or activate the policy later.

At the bottom are "Back", "Next", and "Cancel" buttons.

Figure 16: Simulation mode

## Microsoft 365 Identity and Services – Enterprise Administration

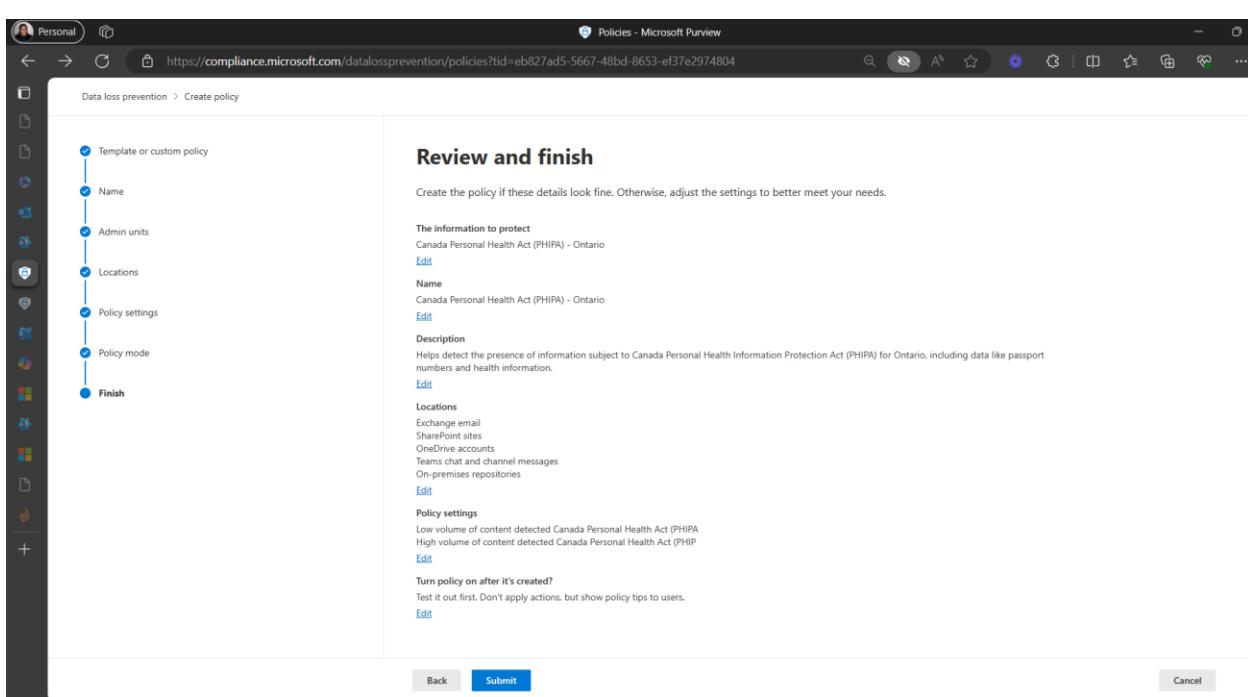


Figure 17: Review

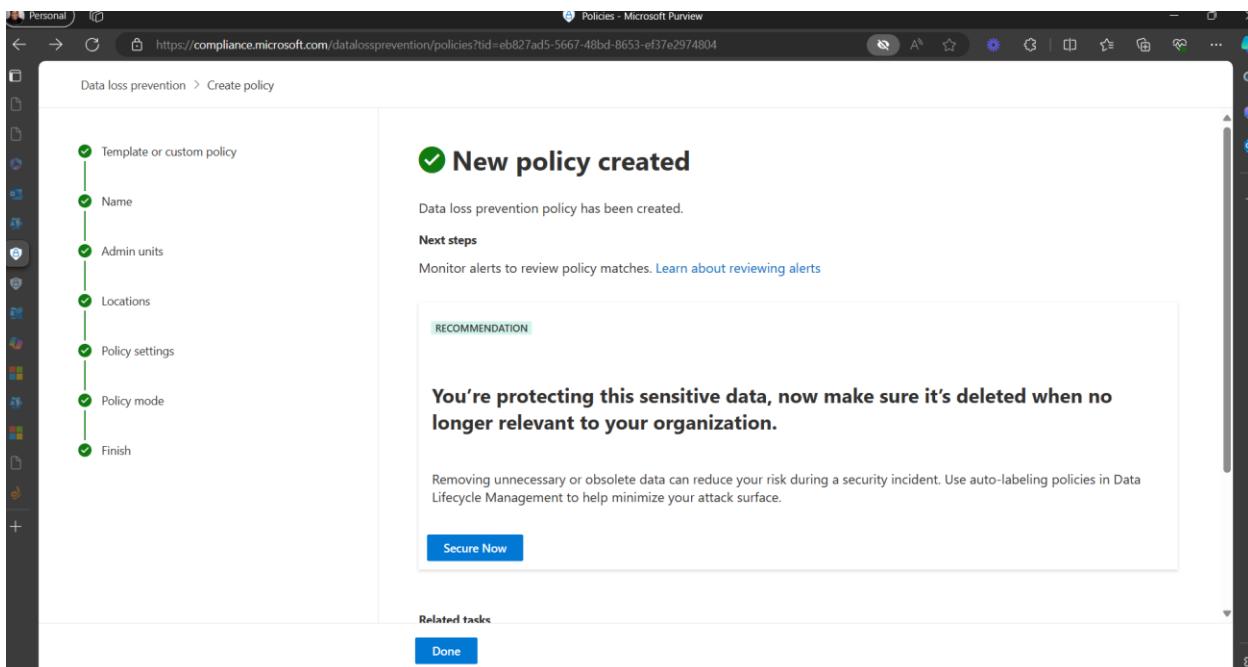


Figure 18: New policy left in simulation mode

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the Microsoft Purview Compliance interface. On the left, a sidebar lists various compliance categories like Data classification, Policies, and Solutions. The main area displays a simulation for the 'Canada Personal Health Act (PHIPA) - Ontario'. It shows a progress bar indicating 'In progress' and several action buttons: Turn the policy on, Download report, Edit the policy, Delete the policy, and Restart the simulation. Below these are tabs for Simulation overview, Items for review, and Alerts. Under Simulation progress, it says '0 Total items scanned'. To the right, under 'Total matches', it displays '0 matches found'. A note states: 'We're scanning specific locations for items that match the policy's conditions. Predicted matches will appear on the Items for review page when ready.' There is also a link to 'Learn more about simulation mode'.

### 1.8 Block emails with .html attachments

The screenshot shows the Exchange admin center interface. The left sidebar includes sections for Home, Recipients, Mail flow, Rules, and many others. The main area is titled 'Rules' and shows a list of transport rules. One rule is highlighted: 'Block html Attachments'. The rule details show it is 'Enabled' with 'Mode' set to 'Enforce'. It has 'Severity' set to 'High' and 'Senders address' set to 'Matching Header'. The 'Priority' is listed as '3'. A note indicates 'Rule status updated successfully'. The rule description is: 'Apply this rule if has an attachment with a file extension that matches one of these values: 'html''.

## Microsoft 365 Identity and Services – Enterprise Administration

### Task 2: Power Platform Administration

#### 2.1 Enable tenant level analytics

Navigate to <https://admin.powerplatform.microsoft.com/home>, go to settings and select Analytics

The screenshot shows the Microsoft Power Platform admin center interface. On the left, there's a navigation sidebar with various options like Home, Environments, Advisor, Analytics, Billing, Settings, Resources, Help + support, Data integration, Data (preview), Policies, and Admin centers. The 'Analytics' section is currently selected. On the right, there's a list of tenant-level analytics settings, each with a brief description. A modal window titled 'Analytics' is overlaid on the main page, focusing on the 'Terms of Service' section. It contains text about aggregating data from environments across all regions in the tenant and copying it into the default environment for reporting. Below this is a toggle switch labeled 'Tenant-level analytics' which is turned on ('Enable'). At the bottom of the modal are 'Save' and 'Cancel' buttons.

Figure 19: Enable Tenant Analytics Level

#### 2.2 Identify the list of existing connections in Power Apps (may be empty)

The screenshot shows the Microsoft Power Apps Discover page. The left sidebar includes options like Home, Create, Learn, Apps, Tables, Flows, Solutions, More, Discover (which is currently selected), and Power Platform. The main area has several cards: 'Solutions' (Author, package, and maintain units of software that extend Microsoft Dataverse), 'Cards' (Author, package, and maintain units of software that extend Microsoft Dataverse), 'Data' (Choices, Connections, Custom connectors, App Management), 'Data Management' (Dataflows, Component libraries, Publishers), and 'App enhancements' (Component libraries, Publishers). The 'Connections' card under the Data category is highlighted with a green rectangular box.

Figure 20: Navigate Data to Connections

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the Microsoft Power Apps Connections page. On the left, there's a navigation sidebar with options like Home, Create, Learn, Apps, Tables, Flows, Solutions, Connections (which is selected and highlighted in pink), and More. The main area has a search bar at the top right. Below it, a section titled "Connections in Jen MBA (default)" lists several connections, each with a small icon, name, modified date, and status. A green box highlights this list.

| Name                                                      | Modified | Status    |
|-----------------------------------------------------------|----------|-----------|
| iam@jennifermbaegbu.onmicrosoft.com SharePoint            | 3 d ago  | Connected |
| iam@jennifermbaegbu.onmicrosoft.com OneDrive for Business | 3 d ago  | Connected |
| Approvals Approvals                                       | 3 d ago  | Connected |
| iam@jennifermbaegbu.onmicrosoft.com Office 365 Users      | 3 d ago  | Connected |
| iam@jennifermbaegbu.onmicrosoft.com Microsoft Teams       | 3 d ago  | Connected |
| iam@jennifermbaegbu.onmicrosoft.com Office 365 Outlook    | 3 d ago  | Connected |

Figure 21: Connections

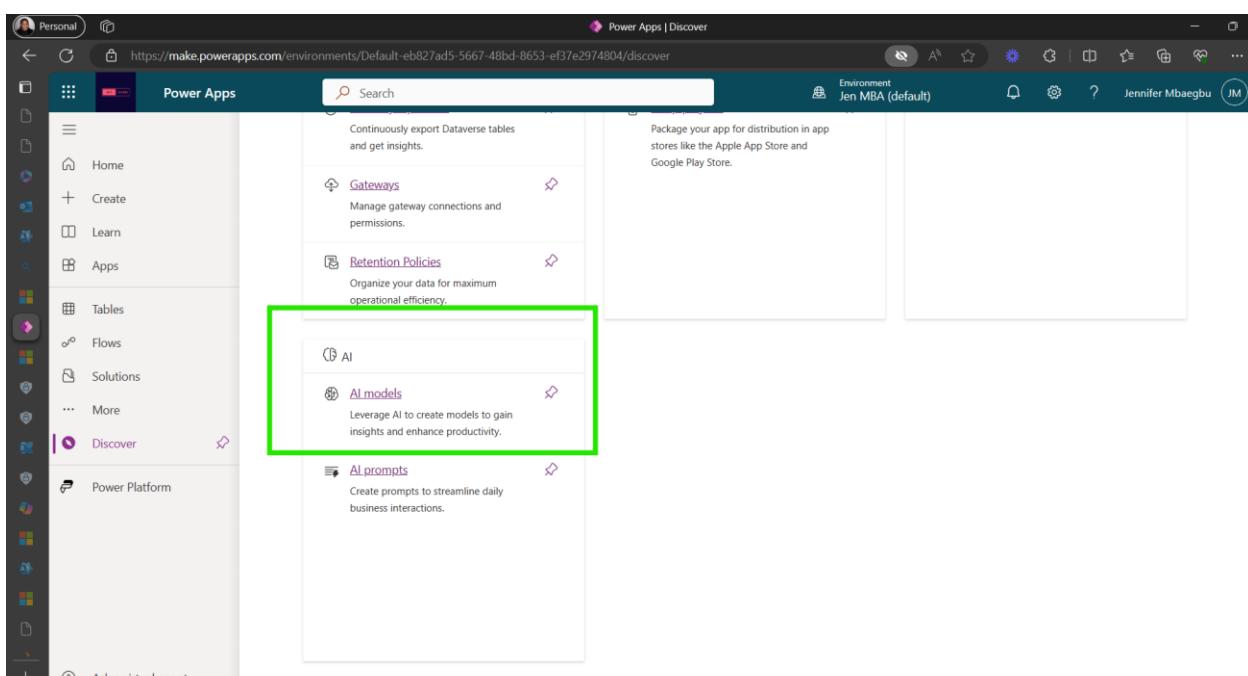
2.3 Identify of the name of the AI Builder used to “Extract information from receipts” **Navigate to Discover tab > AI tab > AI models > Extract Information from receipts.**

The screenshot shows the Microsoft Power Apps Home page. The left sidebar includes Home, Create, Learn, Apps, Tables, Flows, Solutions, More, and Power Platform. A modal window titled "More" is open, allowing users to customize their left navigation items. The main area features a "Welcome, Jennifer!" message and two large buttons: "Start with a page design" and "Start with an app template". Below these are sections for "Discover all" and a table of recent apps. The table has columns for Modified, Owner, and Type.

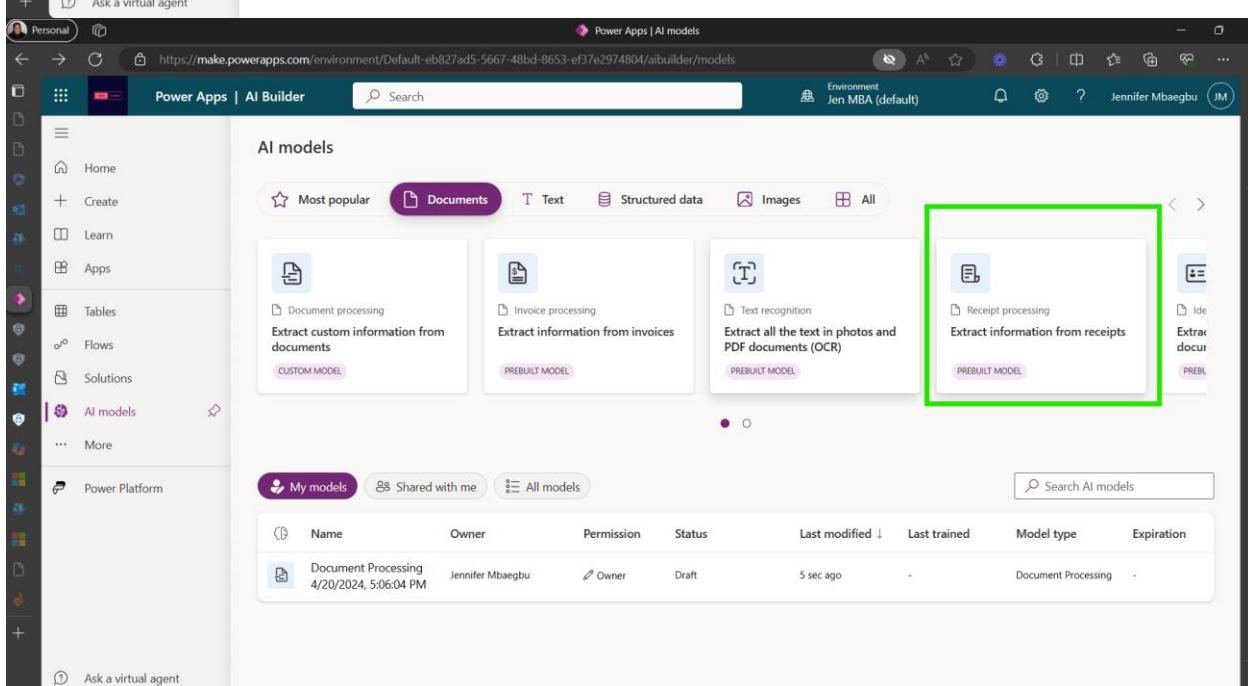
| Modified    | Owner            | Type         |
|-------------|------------------|--------------|
| 3 days ago  | Jennifer Mbaegbu | Canvas       |
| 2 weeks ago | Jennifer Mbaegbu | Model-driven |
| 2 weeks ago | Jennifer Mbaegbu | Model-driven |
| 2 weeks ago | Jennifer Mbaegbu | Model-driven |

## Microsoft 365 Identity and Services – Enterprise Administration

---



The screenshot shows the Microsoft Power Apps Discover page. On the left, there's a navigation sidebar with options like Home, Create, Learn, Apps, Tables, Flows, Solutions, More, Discover, and Power Platform. The main area has a search bar and sections for Dataflows, Gateways, Retention Policies, and AI. A green box highlights the AI section, which contains sub-sections for AI models and AI prompts.

The screenshot shows the Microsoft Power Apps AI Builder page. The left sidebar includes Home, Create, Learn, Apps, Tables, Flows, Solutions, AI models, and Power Platform. The main content area is titled "AI models" and features tabs for Most popular, Documents, Text, Structured data, Images, and All. Under the "Documents" tab, there are four cards: Document processing (Custom Model), Invoice processing (Prebuilt Model), Text recognition (Prebuilt Model), and Receipt processing (Prebuilt Model). The Receipt processing card is highlighted with a green box. Below this, there are tabs for My models, Shared with me, and All models, followed by a table of AI models.

| Name                                         | Owner            | Permission | Status | Last modified | Last trained | Model type          | Expiration |
|----------------------------------------------|------------------|------------|--------|---------------|--------------|---------------------|------------|
| Document Processing<br>4/20/2024, 5:06:04 PM | Jennifer Mbaegbu | Owner      | Draft  | 5 sec ago     | -            | Document Processing | -          |

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the Microsoft Power Apps AI builder interface. On the left, the navigation bar includes 'Personal', 'Home', 'Create', 'Learn', 'Apps', 'Tables', 'Flows', 'Solutions', 'AI models' (which is selected), and 'More'. Below these are 'Power Platform' and 'Upload new'. A central panel titled 'Extract information from receipts' displays a receipt image from Contoso. The receipt details include:  
Merchant name: Contoso  
Merchant address: 123 Main Street Redmond, WA 98052  
Merchant phone number: 987-654-3210  
Transaction date: 6/10/2019  
Transaction time: 13:59  
Purchased items:

|               |          |
|---------------|----------|
| Surface Pro 6 | \$599.00 |
| Surface Pen   | \$99.95  |
| Sub-Total     | \$604.95 |
| Tax           | \$10.45  |
| Total         | \$615.40 |

## Microsoft 365 Identity and Services – Enterprise Administration

---

### Task 3: MFA

#### 3.1 Enable Multi Factor Authentication

The screenshot shows the Microsoft 365 Admin Center interface. The left sidebar is open, showing various administrative categories like Home, Users, Contacts, Guest users, Deleted users, Devices, Teams & groups, Roles, Resources, Billing, Support, Settings, Setup, Reports, and Health. Under the 'Users' category, 'Active users' is selected and highlighted with a yellow box. In the main content area, the title 'Active users' is displayed above a table. The table has columns for 'Display name ↑', 'Username', and 'Licenses'. There are eight rows of user data. At the top of the table, there are several buttons: 'Add a user', 'User templates', 'Add multiple users', 'Multi-factor authentication' (which is highlighted with a green box), 'Delete a user', and a search bar. Below the table, there is a 'Choose col' button.

Figure 22: Launch MFA from Microsoft 365 Admin Center - Users - Active Users

The screenshot shows the 'Multi-factor authentication' page within the Microsoft 365 Admin Center. At the top, there is a note: 'Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. Learn more about how to license other users. Before you begin, take a look at the multi-factor auth deployment guide.' Below this, there is a 'bulk update' button. The main area contains a table with columns: 'DISPLAY NAME', 'USER NAME', and 'MULTI-FACTOR AUTH STATUS'. The table lists eight users. To the right of the table, a modal window titled 'Select a user' is open, showing the same list of users. The user 'Jennifer Mbaegbu' is highlighted with a blue box in the table.

## Microsoft 365 Identity and Services – Enterprise Administration

This screenshot shows the Microsoft 365 Identity and Services - Enterprise Administration interface. The user is navigating to the Multi-factor authentication settings for users. The page displays a list of users with their display names, user names, and current multi-factor auth status (Disabled, Enforced, or Enabled). A specific user, Lorenzo Falcon, is highlighted. On the right side, there is a sidebar with a profile picture and name, followed by a 'quick steps' section with 'Enable' and 'Manage user settings' options.

| DISPLAY NAME     | USER NAME                                      | MULTI-FACTOR AUTH STATUS |
|------------------|------------------------------------------------|--------------------------|
| 101511792        | 101511792@jennifermbaegbu.onmicrosoft.com      | Disabled                 |
| Chinedu          | Chi@jennifermbaegbu.onmicrosoft.com            | Enforced                 |
| Enya Irish       | eirish@jennifermbaegbu.onmicrosoft.com         | Disabled                 |
| Jennifer Mba     | jennifer-User2@jennifermbaegbu.onmicrosoft.com | Disabled                 |
| Jennifer Mbaegbu | jennifer-User1@jennifermbaegbu.onmicrosoft.com | Disabled                 |
| Jennifer Mbaegbu | iam@jennifermbaegbu.onmicrosoft.com            | Enabled                  |
| Jennifer-Shared  | jen-shared@jennifermbaegbu.onmicrosoft.com     | Disabled                 |
| Lorenzo Falcon   | lfalcon@jennifermbaegbu.onmicrosoft.com        | Disabled                 |

This screenshot shows the same Microsoft 365 Identity and Services - Enterprise Administration interface, but with a modal dialog box overlaid. The dialog is titled 'About enabling multi-factor auth' and contains text explaining the deployment guide and a link to register for multi-factor auth. It includes two buttons: 'enable multi-factor auth' and 'cancel'.

## Microsoft 365 Identity and Services – Enterprise Administration

Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. Learn more about how to license other users. Before you begin, take a look at the multi-factor auth deployment guide.

bulk update

| DISPLAY NAME     | USER NAME                                      | MULTI-FACTOR AUTH STATUS |
|------------------|------------------------------------------------|--------------------------|
| 101511792        | 101511792@jennifermbaegbu.onmicrosoft.com      | Disabled                 |
| Chinedu          | Chi@jennifermbaegbu.onmicrosoft.com            | Enabled                  |
| Enya Irish       | eirish@jennifermbaegbu.onmicrosoft.com         | Disabled                 |
| Jennifer Mba     | jennifer-User2@jennifermbaegbu.onmicrosoft.com | Enabled                  |
| Jennifer Mbuegbu | jennifer-User1@jennifermbaegbu.onmicrosoft.com | Disabled                 |
| Jennifer Mbuegbu | iam@jennifermbaegbu.onmicrosoft.com            | Enabled                  |
| Jennifer-Shared  | jen-shared@jennifermbaegbu.onmicrosoft.com     | Disabled                 |
| Lorenzo Falcon   | lfalcon@jennifermbaegbu.onmicrosoft.com        | Enabled                  |

### 3.2 Enforce MFA

Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. Learn more about how to license other users. Before you begin, take a look at the multi-factor auth deployment guide.

bulk update

| DISPLAY NAME                                         | USER NAME                                      | MULTI-FACTOR AUTH STATUS |
|------------------------------------------------------|------------------------------------------------|--------------------------|
| <input checked="" type="checkbox"/> 101511792        | 101511792@jennifermbaegbu.onmicrosoft.com      | Enabled                  |
| <input type="checkbox"/> Chinedu                     | Chi@jennifermbaegbu.onmicrosoft.com            | Enforced                 |
| <input checked="" type="checkbox"/> Enya Irish       | eirish@jennifermbaegbu.onmicrosoft.com         | Enabled                  |
| <input checked="" type="checkbox"/> Jennifer Mba     | jennifer-User2@jennifermbaegbu.onmicrosoft.com | Enabled                  |
| <input checked="" type="checkbox"/> Jennifer Mbuegbu | jennifer-User1@jennifermbaegbu.onmicrosoft.com | Enabled                  |
| <input checked="" type="checkbox"/> Jennifer Mbuegbu | iam@jennifermbaegbu.onmicrosoft.com            | Enabled                  |
| <input checked="" type="checkbox"/> Jennifer-Shared  | jen-shared@jennifermbaegbu.onmicrosoft.com     | Enabled                  |
| <input checked="" type="checkbox"/> Lorenzo Falcon   | lfalcon@jennifermbaegbu.onmicrosoft.com        | Enabled                  |

7 selected

quick steps

Disable  
Enforce  
Manage user settings

## Microsoft 365 Identity and Services – Enterprise Administration

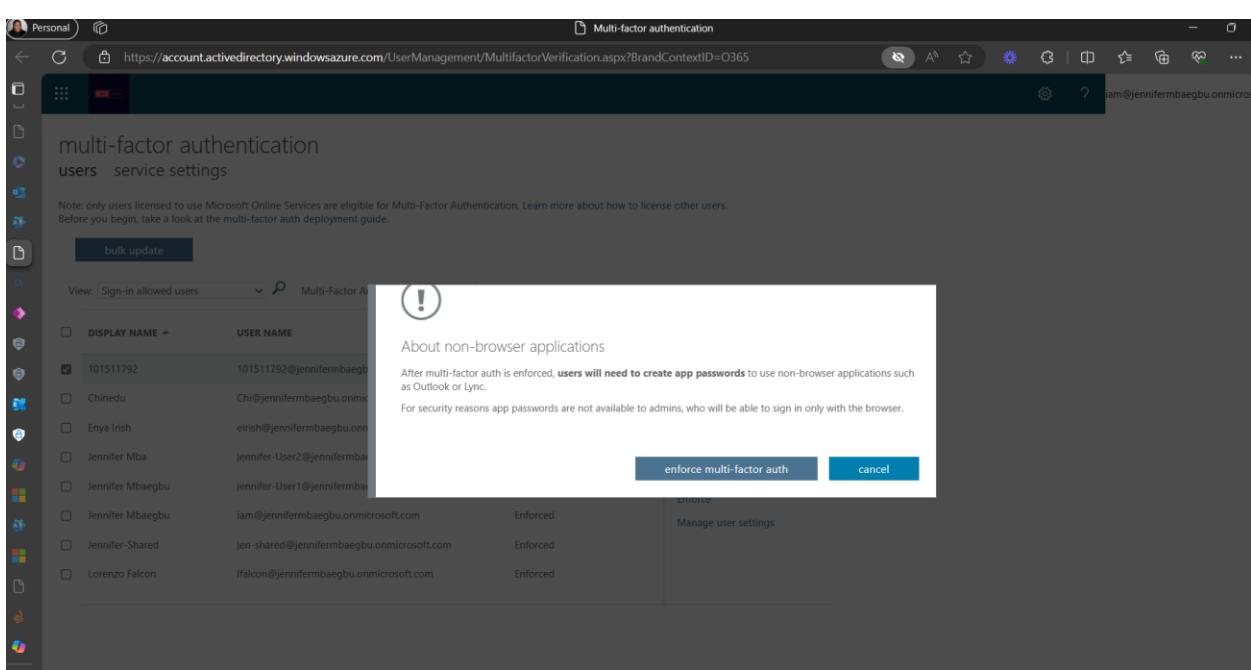


Figure 23: Enforce Multi-factor Authentication

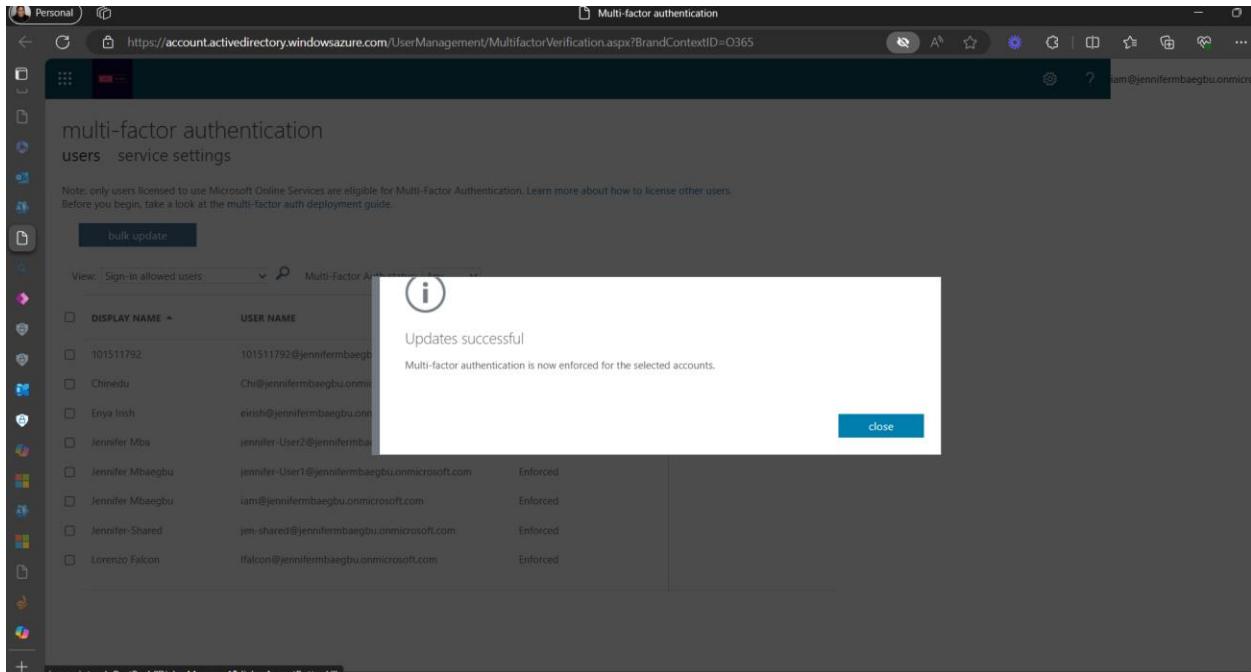


Figure 24: Multi-factor authentication enforced

## Microsoft 365 Identity and Services – Enterprise Administration

---

### 3.3 Setup MFA

The image contains two screenshots of a web browser window. The top screenshot shows the Microsoft login page with a message about Action Required for MFA setup. The bottom screenshot shows a step-by-step guide for setting up the Microsoft Authenticator app.

**Screenshot 1: Microsoft 365 Identity and Services – Enterprise Administration**

Sign in to your account - [InPrivate]  
https://login.microsoftonline.com/common/login

**Microsoft**  
nedu@jennifermbaegbu.onmicrosoft.com

**Action Required**

Your organization requires additional security information. Follow the prompts to download and set up the Microsoft Authenticator app.

[Use a different account](#)  
[Learn more about the Microsoft Authenticator app](#)

**Next**

**Screenshot 2: My Sign-Ins | Register | Microsoft.com - [InPrivate]**

Jen Cloud

Keep your account secure

**Microsoft Authenticator**

**Start by getting the app**

On your phone, install the Microsoft Authenticator app. [Download now](#)

After you install the Microsoft Authenticator app on your device, choose "Next".

[I want to use a different authenticator app](#)

**Next**

## Microsoft 365 Identity and Services – Enterprise Administration

~~~~~

My Sign-Ins | Register | Microsoft.com - [InPrivate]

Jen Cloud

Keep your account secure

Microsoft Authenticator

Set up your account

If prompted, allow notifications. Then add an account, and select "Work or school".

Back Next

My Sign-Ins | Register | Microsoft.com - [InPrivate]

Jen Cloud

Keep your account secure

Microsoft Authenticator

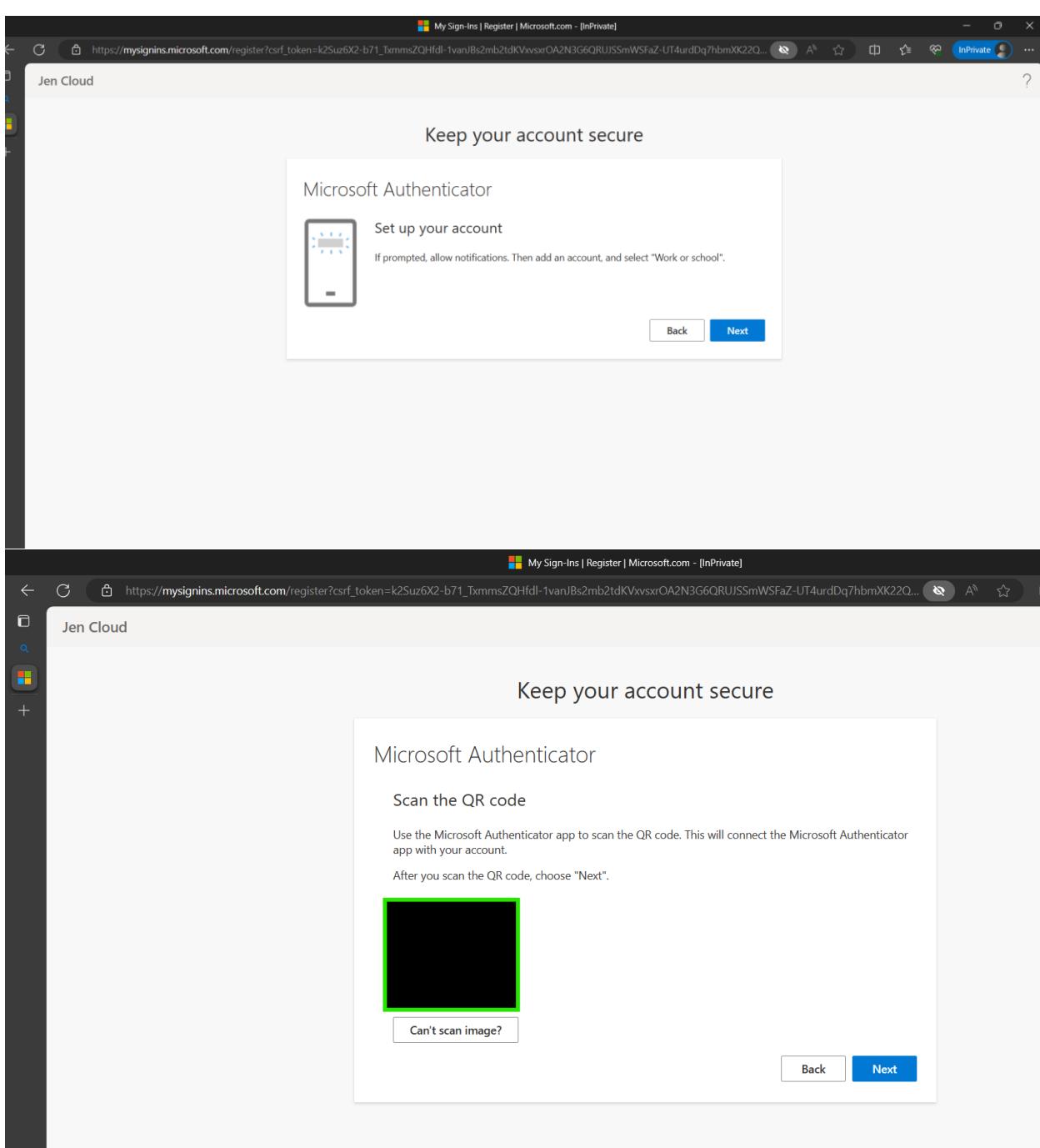
Scan the QR code

Use the Microsoft Authenticator app to scan the QR code. This will connect the Microsoft Authenticator app with your account.

After you scan the QR code, choose "Next".

Can't scan image?

Back Next



Microsoft 365 Identity and Services – Enterprise Administration

The image consists of two vertically stacked screenshots from a Microsoft Edge browser window. Both screenshots show the URL https://mysignins.microsoft.com/register?csrf_token=k2Suz6X2-b71_TxmmsZQHfdl-1vanJBs2mb2tdKVvxsxOA2N3G6QRUJSSmWSFaZ-UT4urdDq7hbmXK22Q... in the address bar, with the 'InPrivate' tab selected.

Screenshot 1: Keep your account secure

This screenshot shows the 'Microsoft Authenticator' setup step. It features a smartphone icon with a checkmark and the text 'Let's try it out'. Below it, a green square placeholder is shown where a QR code would normally appear. The text 'Approve the notification we're sending to your app by entering the number shown below.' is displayed. At the bottom are 'Back' and 'Next' buttons.

Screenshot 2: Success!

This screenshot shows the successful registration of the Microsoft Authenticator app. A green toast notification on the right side of the screen reads 'Microsoft Authenticator app was successfully registered' with a timestamp of 'Sat, 20 Apr 2024 21:37:42 GMT'. The main message area says 'Success!' and provides instructions: 'Great job! You have successfully set up your security info. Choose "Done" to continue signing in.' It lists the 'Default sign-in method:' as 'Microsoft Authenticator' and includes a 'Done' button at the bottom.

Microsoft 365 Identity and Services – Enterprise Administration

Task 4: Customer lockbox

4.1 Enable customer lockbox:

The screenshot shows the Microsoft 365 Subscriptions interface. On the left, there's a navigation menu with options like Home, Users, Devices, Teams & groups, Roles, Resources, Billing, Purchase services, Your products, Licenses, Bills & payments, Billing accounts, Payment methods, Billing notifications, Cost Management, Support, Settings, and Domains. The main area is titled 'Your products' and displays a table of products. A green box highlights the 'Products from Microsoft and others (5)' section, which includes Microsoft 365 Business Premium, Microsoft Copilot Studio Viral Trial, Microsoft Fabric (Free), Microsoft Power Automate Free, and Power Pages vTrial for Makers. The table columns include Product name, Assigned licenses, Purchased quantity, and Subscription status.

Figure 25: Microsoft 365 subscription verified not to have the customer lockbox feature

Microsoft 365 Premium do not have the customer lockbox feature, however below is the navigation to locating it on either Microsoft 365 E5 or Microsoft 365 E3 with advanced compliance add-on

The screenshot shows the Microsoft 365 Admin center. The left navigation menu is identical to Figure 25. The main area is titled 'Org settings' and has tabs for Services, Security & privacy (which is highlighted with a green box), and Organization profile. Below the tabs is a table of settings with columns for Name and Description. The settings listed are Account Linking, Adoption Score, Azure Speech Services, Bookings, Calendar, Copilot for Sales, and Cortana.

Figure 26: On Microsoft 365 Admin center, navigate to Settings - Org Settings - Security and Privacy

Microsoft 365 Identity and Services – Enterprise Administration

Task 5: Security

5.1 Block .html extension for emails

The screenshot shows the Microsoft Exchange Admin Center interface. On the left, there's a navigation menu with various options like Home, Recipients, Mail flow, Rules, Roles, Migration, Mobile, Reports, Insights, Public folders, Organization, and Settings. The 'Rules' section is currently selected. In the center, a 'New transport rule' wizard is open. The first step, 'Set rule conditions', is selected. Below it, there are three other options: 'Set rule settings' (radio button), 'Review and finish' (radio button), and 'Next' (button). The main pane displays the configuration for the rule. It has sections for 'Name' (set to 'Block .html Extension for emails'), 'Apply this rule if' (set to 'Any attachment file extension includes these words: .html'), 'Do the following' (set to 'Block the message delete the message without notifying anyone'), and 'Except if' (empty). A modal window titled 'specify words or phrases' is also visible, showing a single item: '.html'. At the bottom right of the main pane, there are 'Save' and 'Cancel' buttons.

Figure 27: .html is specified

Microsoft 365 Identity and Services – Enterprise Administration

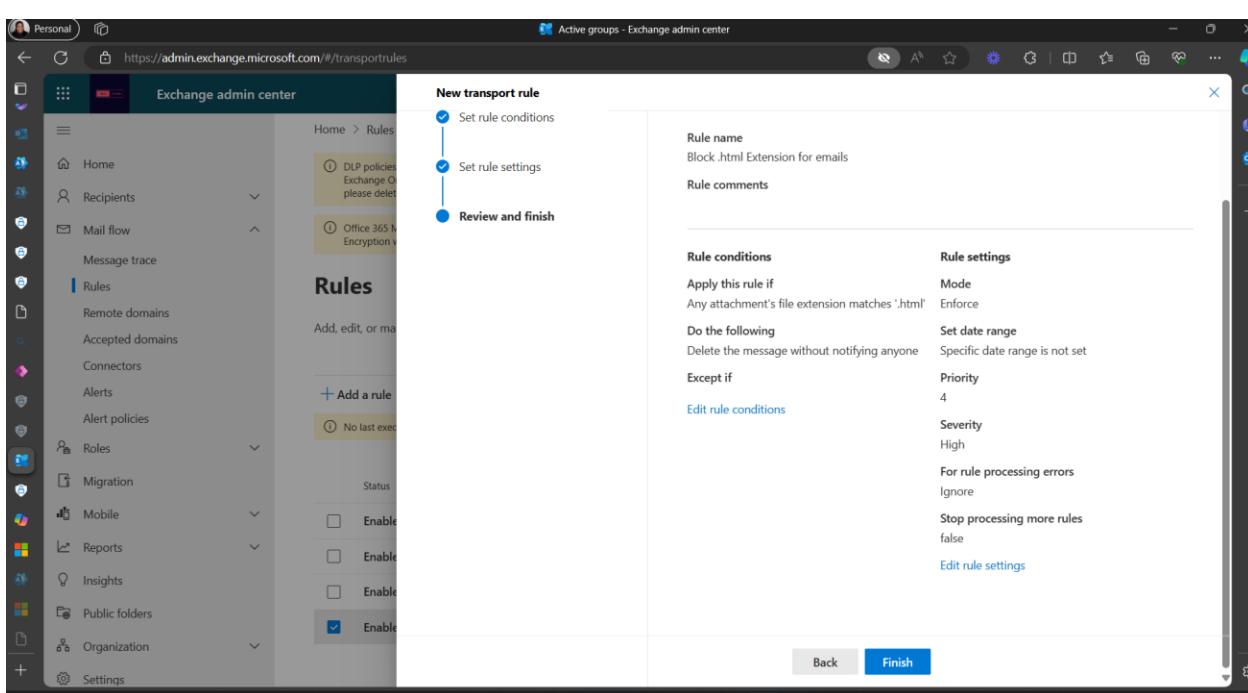
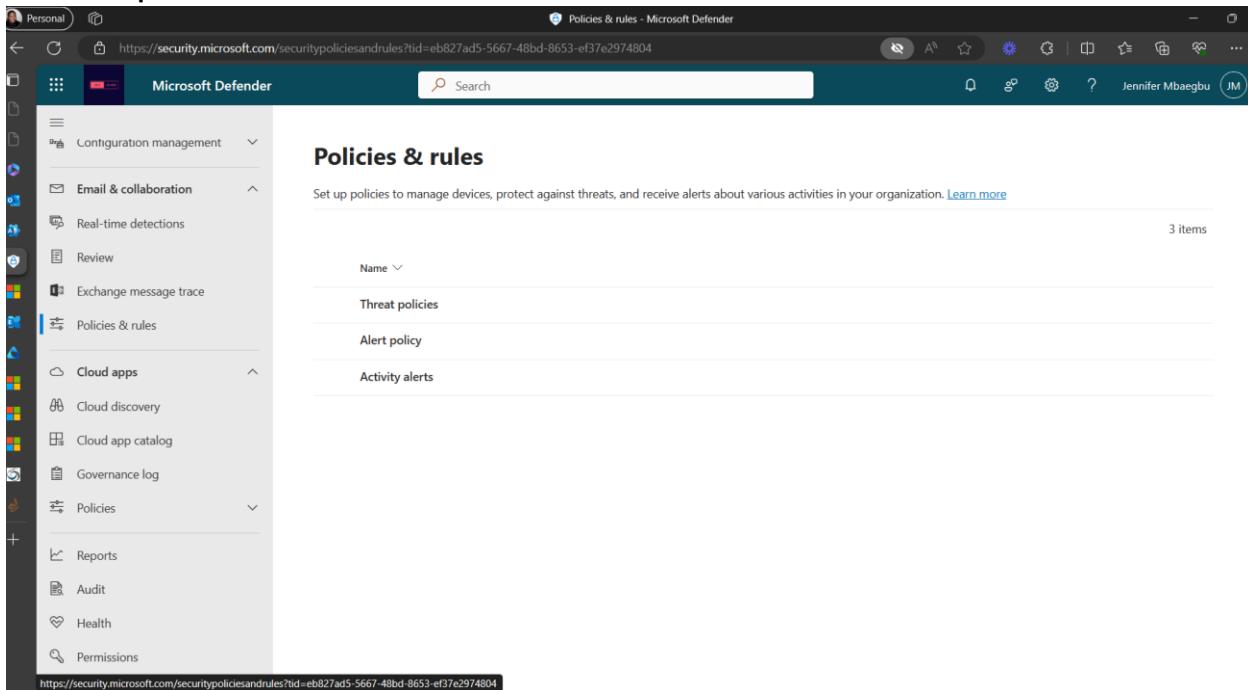


Figure 28: Review New Transport Rule on Exchange Center to Block .html

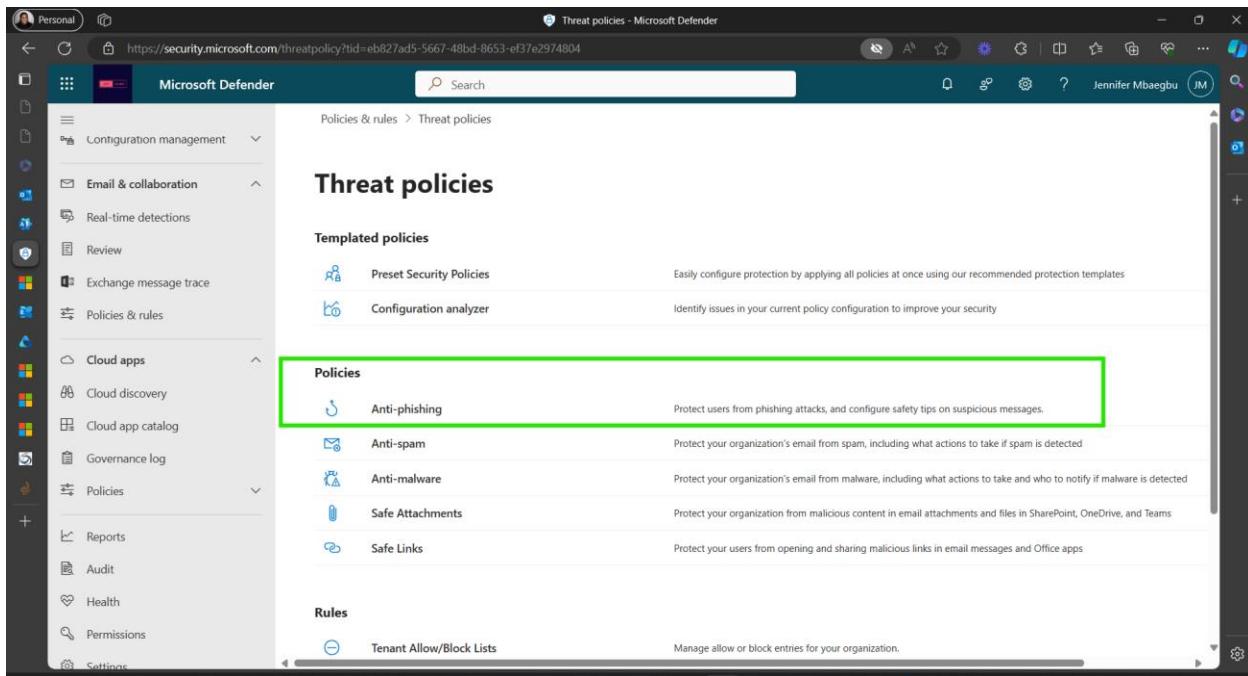
Status	Rule	Priority	Action
<input type="checkbox"/> Enabled	External Disclaimer	0	X
<input type="checkbox"/> Enabled	Monitor Email Links2	1	X
<input type="checkbox"/> Enabled	Case Project	2	X
<input checked="" type="checkbox"/> Enabled	Block html Attachme...	3	X

Microsoft 365 Identity and Services – Enterprise Administration

5.2 Create anti Phishing policy and apply your desired settings and make sure the spam messages are moved to quarantine

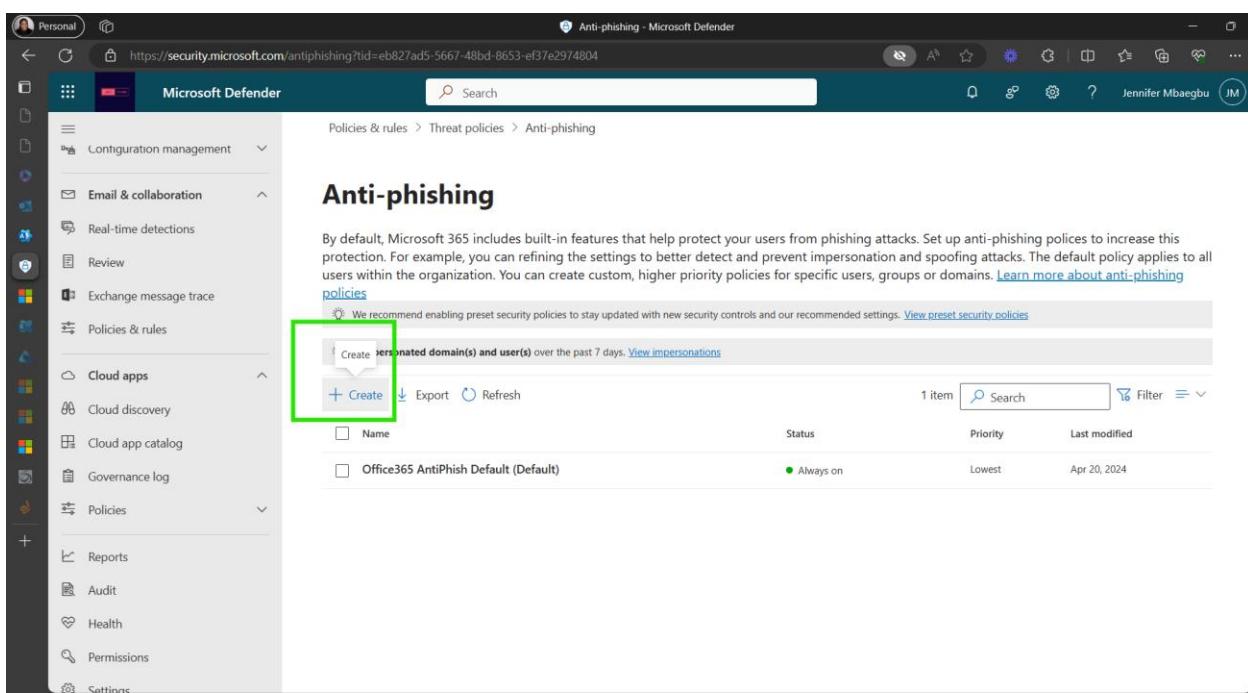


The screenshot shows the Microsoft Defender interface for 'Policies & rules'. The left sidebar includes sections like Configuration management, Email & collaboration, Real-time detections, Review, Exchange message trace, Policies & rules (which is expanded), Cloud apps, Cloud discovery, Cloud app catalog, Governance log, Policies, Reports, Audit, Health, and Permissions. The main content area is titled 'Policies & rules' and contains a sub-section 'Threat policies'. It displays three items: Threat policies, Alert policy, and Activity alerts. A note at the top says 'Set up policies to manage devices, protect against threats, and receive alerts about various activities in your organization.' with a 'Learn more' link.



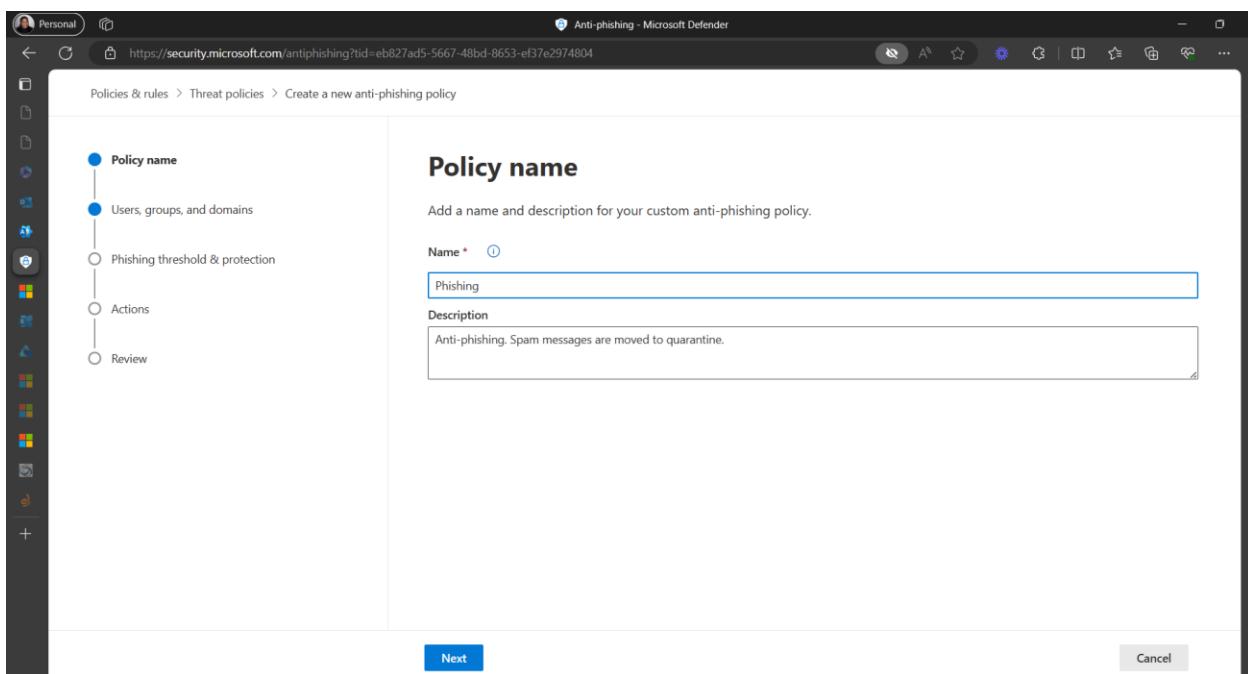
The screenshot shows the Microsoft Defender interface for 'Threat policies'. The left sidebar is identical to the previous screenshot. The main content area is titled 'Threat policies' and shows two sections: 'Templated policies' (with Preset Security Policies and Configuration analyzer) and 'Policies'. The 'Policies' section is highlighted with a green box and lists five items: Anti-phishing, Anti-spam, Anti-malware, Safe Attachments, and Safe Links. The 'Anti-phishing' item is also highlighted with a green box. Below this is a 'Rules' section with 'Tenant Allow/Block Lists'. A note at the bottom right says 'Manage allow or block entries for your organization.'

Microsoft 365 Identity and Services – Enterprise Administration



The screenshot shows the Microsoft Defender interface for managing threat policies. The left sidebar includes sections for Configuration management, Email & collaboration, Real-time detections, Review, Exchange message trace, Policies & rules, Cloud apps, Cloud discovery, Cloud app catalog, Governance log, Policies, Reports, Audit, Health, Permissions, and Settings. The main content area is titled "Anti-phishing" and displays a list of policies. A green box highlights the "+ Create" button. The table shows one item:

Name	Status	Priority	Last modified
Office365 AntiPhish Default (Default)	Always on	Lowest	Apr 20, 2024



The screenshot shows the "Create a new anti-phishing policy" wizard. On the left, a navigation tree shows "Policy name" selected, followed by "Users, groups, and domains", "Phishing threshold & protection", "Actions", and "Review". The main area is titled "Policy name" and contains fields for "Name" (set to "Phishing") and "Description" (set to "Anti-phishing. Spam messages are moved to quarantine."). At the bottom are "Next" and "Cancel" buttons.

Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows two steps of a wizard for creating a new anti-phishing policy:

Step 1: Users, groups, and domains

This step allows you to define which users, groups, and domains should be included or excluded from the policy.

Step 2: Phishing threshold & protection

This step allows you to set thresholds and protections for phishing emails, including impersonation and spoof protection.

Left sidebar (common to both steps):

- Policy name (checked)
- Users, groups, and domains** (checked)
- Phishing threshold & protection (checked)
- Actions
- Review

Step 1: Users, groups, and domains

Users: Chinedu, Enya Irish, Lorenzo Falcon, Jennifer Mba, Jennifer Mbaegbu, 101511792, Nedu Mbaegbu, Jennifer Mbaegbu.

Groups: Jennifer-Dist, Jennifer-G2, Jennifer-DistList, Jennifer-Shared, Jennifer-Team.

Domains: jennifermbaegbu.onmicrosoft.com.

Exclude these users, groups and domains

Step 2: Phishing threshold & protection

Phishing email threshold: Set to 4 - Most Aggressive.

Impersonation:

- Enable users to protect (0/350) (Learn more about adding users to impersonation protection)
- Manage 0 sender(s)
- Enable domains to protect (1) (Enable impersonation protection for these internal and external sender domains.)
- Include domains I own (View my domains)
- Include custom domains

Figure 29: Setting up threshold and protection

Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows a browser window titled "Anti-phishing - Microsoft Defender" at the URL <https://security.microsoft.com/antiphishing?tid=eb827ad5-5667-48bd-8653-ef37e2974804>. The page is part of a "Policies & rules" section under "Threat policies". A vertical navigation pane on the left lists steps: "Policy name" (checkmark), "Users, groups, and domains" (checkmark), "Phishing threshold & protection" (checkmark), "Actions" (selected, highlighted in blue), and "Review" (radio button). The main content area is titled "Actions" and describes setting actions for messages. It includes sections for "Message actions" (dropdown set to "Quarantine the message") and "Apply quarantine policy" (dropdown set to "AdminOnlyAccessPolicy"). There are also sections for "If a message is detected as user impersonation" and "If Mailbox Intelligence detects an impersonated user", both with dropdowns set to "Quarantine the message". At the bottom are "Back", "Next", and "Cancel" buttons.

The screenshot shows the same browser window after the policy has been created. The title bar remains "Anti-phishing - Microsoft Defender" at the URL <https://security.microsoft.com/antiphishing?tid=eb827ad5-5667-48bd-8653-ef37e2974804>. The navigation pane shows the completed steps: "Policy name" (checkmark), "Users, groups, and domains" (checkmark), "Phishing threshold & protection" (checkmark), "Actions" (checkmark), and "Review" (checkmark). The main content area displays a green checkmark icon and the text "New anti-phishing policy created". It also states "Your anti-phishing policy Phishinh has been created. It will go into effect immediately". Below this are "Related features" links: "View this policy", "View anti-phishing policies", and "Learn more about anti-phishing policies". At the bottom is a "Done" button.

Figure 30 Anti-Phishing Policy Created

Microsoft 365 Identity and Services – Enterprise Administration

5.3 Create a Safe link policy

The screenshot shows the Microsoft Defender Threat policies page. On the left, there's a navigation sidebar with various categories like Configuration management, Email & collaboration, Policies & rules, Cloud apps, and Reports. Under Policies & rules, 'Safe Links' is highlighted with a green box. The main content area is titled 'Threat policies' and contains sections for 'Templated policies' (Preset Security Policies, Configuration analyzer) and 'Policies'. The 'Safe Links' policy is listed under Policies, with a brief description: 'Protect your users from opening and sharing malicious links in email messages and Office apps'. Below this is a 'Rules' section for Tenant Allow/Block Lists.

The screenshot shows the Microsoft Defender Safe links page. The navigation sidebar is identical to the previous screen. The main content area is titled 'Safe links' and includes a note about preset security policies. A 'Create' button is highlighted with a green box. Below it is a table listing two items: 'Safe Links' (Status: On, Priority: 0) and 'Built-in protection (Microsoft)' (Status: On, Priority: Lowest). There are also 'Export', 'Refresh', and 'Reports' buttons at the top of the table.

Figure 31: Create Safe Links Policy

Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the 'Create safe links policy' wizard. On the left, a sidebar lists steps: 'Name your policy' (selected), 'Users and domains', 'URL & click protection settings', 'Notification', and 'Review'. The main area is titled 'Name your policy' with the sub-instruction 'Add a name and description for your safe links policy.' It contains fields for 'Name' (set to 'Safe Links') and 'Description' (set to 'Protect users from malicious URLs'). At the bottom are 'Next' and 'Cancel' buttons.

The screenshot shows the 'URL & click protection settings' step of the wizard. The sidebar now includes 'Users and domains' (selected) and 'URL & click protection settings' (selected). The main area is titled 'URL & click protection settings' with the sub-instruction 'Set your Safe Links URL and click protection settings for this policy. [Learn more](#)'. It contains sections for 'Email' (with checkboxes for 'On' and several sub-options like 'Apply Safe Links to email messages sent within the organization'), 'Teams' (with a single checked option), and 'Office 365 Apps' (with a note about URLs not being rewritten). At the bottom are 'Back' and 'Next' buttons.

Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows a Microsoft Edge browser window with the URL <https://security.microsoft.com/safelinksy2?tid=eb827ad5-5667-48bd-8653-ef37e2974804>. The title bar says "Safe links - Microsoft Defender". The main content area displays a success message: "New Safe Links policy created" with a checkmark icon. Below it, a note states: "Your Safe Links policy **Safe Links** has been created. It will go into effect immediately". A sidebar on the left lists steps: "Name your policy", "Users and domains", "URL & click protection settings", "Notification", and "Review", all marked with green checkmarks. At the bottom right is a blue "Done" button.