

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       | enirish@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
- Toolbar:** Add a user, User templates, Add multiple users, Multi-factor authentication, Delete a user, Refresh, Search active users list.
- Table:**| Display name ↑ | Username | Licenses |
| --- | --- | --- |
| [Redacted] | [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 |

**Buttons:** Help & support, Give Feedback.

**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
  - Toolbar:** Add a shared mailbox, Mailflow setting, Refresh, Export mailboxes, 8 items, Filter, Search.
  - Table:**| Display name ↑ | Email address | Recipient type | Archive status | Last modified time | Choose columns |
| --- | --- | --- | --- | --- | --- |
| [Redacted] | [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 with one item. The item is 'Jennifer-Dist' with the email address 'jennifer-dist@jenifermbaegbu.onmicrosoft.com'. The table includes columns for Group name, Group email, Sync status, and Created on.

Figure 4: Create Distribution List

The screenshot shows the 'Add a group' wizard, step 2: 'Group type'. On the left, there's a navigation pane with 'Groups' selected. The main area shows a flowchart with 'Group type' at the top, followed by 'Basics', 'Owners', 'Members', and 'Settings' at the bottom. 'Settings' is highlighted with a blue circle. To the right, there are fields for 'Group email address' (set to 'jeniffer-distlist') and 'Domains' (set to 'jenifermbaegbu.onmicrosoft.com'). Under 'Communication', there's a checked checkbox for 'Allow people outside of my organization to send email to this Distribution group'. Under 'Joining the group', 'Closed' is selected. Under 'Leaving the group', 'Closed' 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.'

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 side-by-side windows from the Microsoft 365 Identity and Services interface, specifically for managing a distribution list group.

**Left Window (General View):**

- Name:** Jennifer-DistList
- Type:** Distribution list group
- Owner:** 1 owner
- Members:** 2 members
- General Tab:** Selected. Other tabs include Members and Settings.
- Message Bar:** Microsoft 365 Groups offer more collaboration tools. [Learn more](#)
- 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

**Right Window (Members View):**

- Name:** Jennifer-DistList
- Type:** Distribution list group
- Owner:** 1 owner
- Members:** 2 members
- Members Tab:** Selected. Other tabs include General and Settings.
- Owners (1):**
  - Jennifer Mbaegbu  
iam@jennifermbaegbu.onmicrosoft.com
- Members (2):**
  - Jennifer Mbaegbu:** jennifer-User1@jennifermbaegbu.onmicrosoft.com
  - Jennifer Mbaegbu:** jennifer-User2@jennifermbaegbu.onmicrosoft.com
- View all and manage owners**
- View all and manage members**

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the Microsoft 365 Identity and Services - Enterprise Administration interface. The title bar reads "Microsoft 365 Identity and Services – Enterprise Administration". The main content area displays a distribution list group named "Jennifer-DistList". The "Members" tab is selected. The list shows one owner and two members. The owner is "Jennifer Mbaegbu" (iam@jennifermbaegbu.onmicrosoft.com). There are two additional users listed under "Members": "Jennifer Mbaegbu" (User1@jennifermbaegbu.onmicrosoft.com) and "Jennifer Mbaegbu" (User2@jennifermbaegbu.onmicrosoft.com). Links to "View all and manage owners" and "View all and manage members" are present.

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

## Microsoft 365 Identity and Services – Enterprise Administration

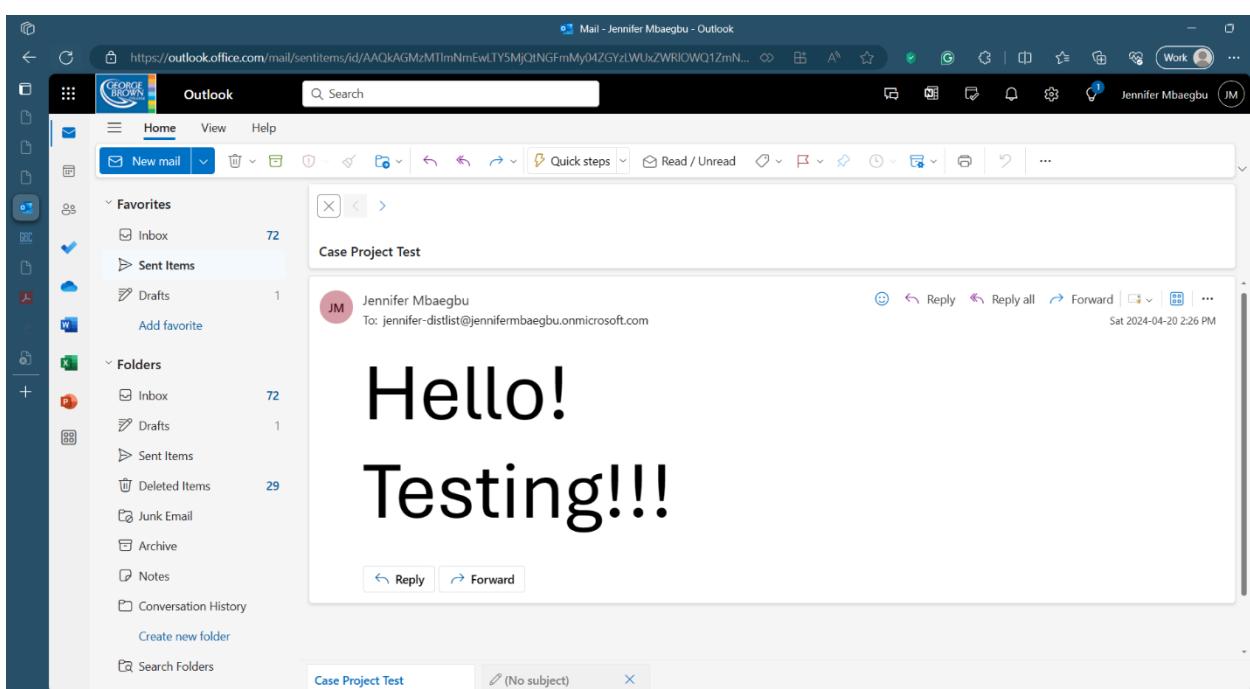


Figure 6: Test Email sent via GBC email

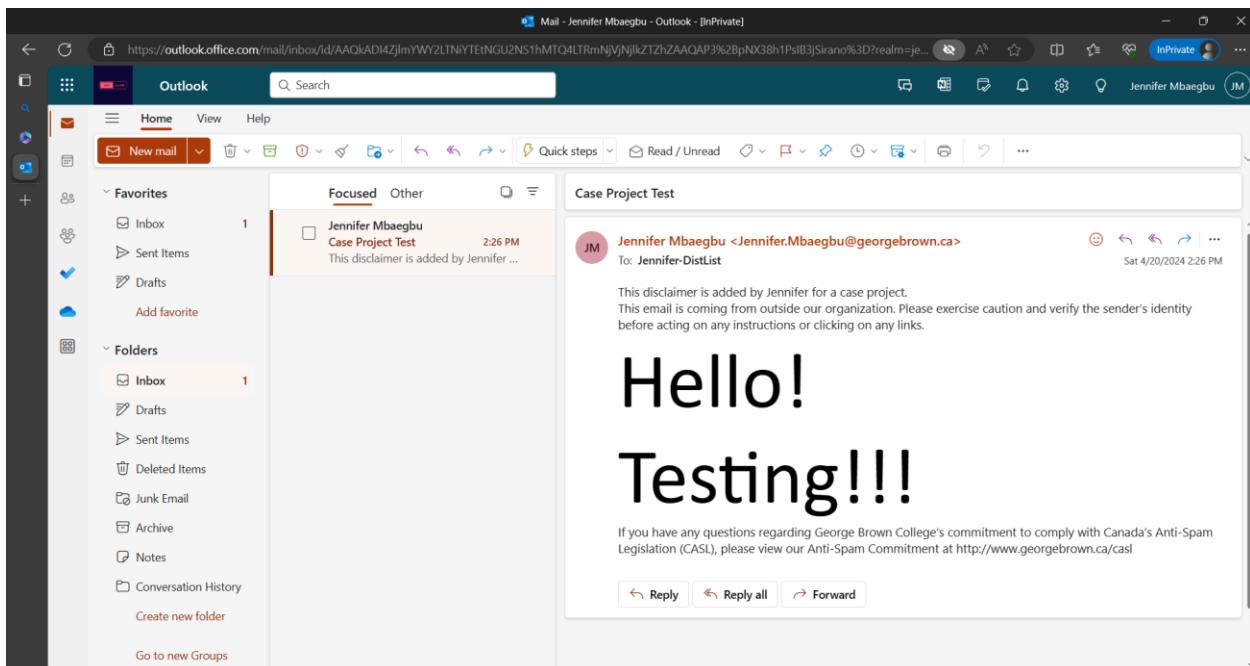


Figure 7: Email received via jennifer-User1@domain.com

## Microsoft 365 Identity and Services – Enterprise Administration

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

**Top Window (Jennifer Mbaegbu's Outlook):**

- The title bar shows "Mail - Jennifer Mbaegbu - Outlook - [InPrivate]".
- The left sidebar shows "Favorites" (Inbox, Sent Items, Drafts) and "Folders" (Inbox, Drafts, Sent Items, Deleted Items, Junk Email, Archive, Notes, Conversation History).
- The main pane shows a distribution list named "Jennifer-DistList" with 2 members: Jennifer Mbaegbu and Jennifer Mba.
- A message from "jennifer-distlist@jennifermbaegbu.onmicrosoft.com" is visible in the inbox.

**Bottom Window (Jennifer Mbaegbu's Outlook):**

- The title bar shows "Mail - Jennifer Mba - Outlook - [InPrivate]".
- The left sidebar shows "Favorites" (Inbox, Sent Items, Drafts) and "Folders" (Inbox, Drafts, Sent Items, Deleted Items, Junk Email, Archive, Notes, Conversation History).
- The main pane 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."
- The message footer includes "Hello! Testing!!!", "If you have any questions regarding George Brown College's commitment to comply with Canada's Anti-Spam Legislation (CASL), please view our Anti-Spam Commitment at <http://www.georgebrown.ca/casl>", and 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 settings like Resources, Billing, Support, and Admin centers. The main area is titled 'Organization profile' and contains a table of organization settings. A modal window titled 'Release preferences' is open on the right. It explains that this setting doesn't affect Microsoft 365 apps. It offers three options: 'Standard release for everyone' (radio button), 'Targeted release for everyone' (radio button), and 'Targeted release for select users' (radio button, which is selected). Below this are 'Select users' and 'Upload users' buttons. A list of users currently on the targeted release is shown, including Chinedu, Enya Irish, Jennifer Mbaegbu, and Lorenzo Falcon, each with a 'Remove' button. A 'Save' button is at the bottom right of the modal.

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' (Enabled, Priority 0), 'Monitor Email Links2' (Enabled, Priority 1), 'Block HTML Attachm...' (Enabled, Priority 2), and 'Case Project' (Disabled, Priority 3). A modal window titled 'Case Project' is open on the right. It has tabs for 'Conditions' and 'Settings'. Under 'Conditions', it says 'Name \* Case Project' and 'Apply this rule if \* The sender is external/internal'. Under 'Do the following \*', it says 'Apply a disclaimer to the ... prepend a disclaimer'. A note says 'Prepend "This disclaimer is added by Jennifer for a case project." and fall back to action "Wrap" if the disclaimer can't be inserted'. Under 'Except if', it says 'Select one'. At the bottom 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 menu with options like Home, Recipients, Mail flow, Message trace, Rules, Remote domains, Accepted domains, Connectors, Alerts, Alert policies, Roles, Migration, Mobile, Reports, Insights, Public folders, Organization, and Settings. The main content area is titled 'Rules' and contains a table of rules. One rule, 'Case Project', is highlighted and has its details expanded. The rule settings include:

- Rule name:** Case Project
- Mode:** Enforce
- Severity:** High
- Set date range:** Specific date range is not set
- Senders address:** Matching HeaderOrEnvelope
- Priority:** 3
- For rule processing errors:** Ignore
- Rule description:** Apply this rule if *Is received from 'Outside the organization'*

A green notification bar at the top right says 'Rule status updated successfully'.

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 interface for creating a new DLP policy. On the left, there's a navigation tree with 'Data loss prevention > Create policy' and options for 'Template or custom policy', 'Name', 'Admin units', 'Locations', 'Policy settings', 'Policy mode', and 'Finish'. The main content area is titled 'Start with a template or create a custom policy' and includes a search bar and a dropdown for 'All countries or regions'. It lists categories and regulations:

| Categories                | Regulations                                              |
|---------------------------|----------------------------------------------------------|
| Financial                 | Australia Health Records Act (HRIP Act)                  |
| <b>Medical and health</b> | <b>Canada Personal Health Act (PHIPA) - Ontario</b>      |
| Privacy                   | Canada Health Information Act (HIA)                      |
| Custom                    | Canada Personal Health Information Act (PHIA) - Manitoba |
|                           | <b>Canada Personal Health Act (PHIPA) - Ontario</b>      |
|                           | U.K. Access to Medical Reports Act                       |
|                           | U.S. Health Insurance Act (HIPAA)                        |

To the right, under 'Protect this information:', there's a list of items:

- Canada Passport Number
- Canada Social Insurance Number
- Canada Health Service Number
- Canada Personal Health Identification Number (PHIN)

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

## Microsoft 365 Identity and Services – Enterprise Administration

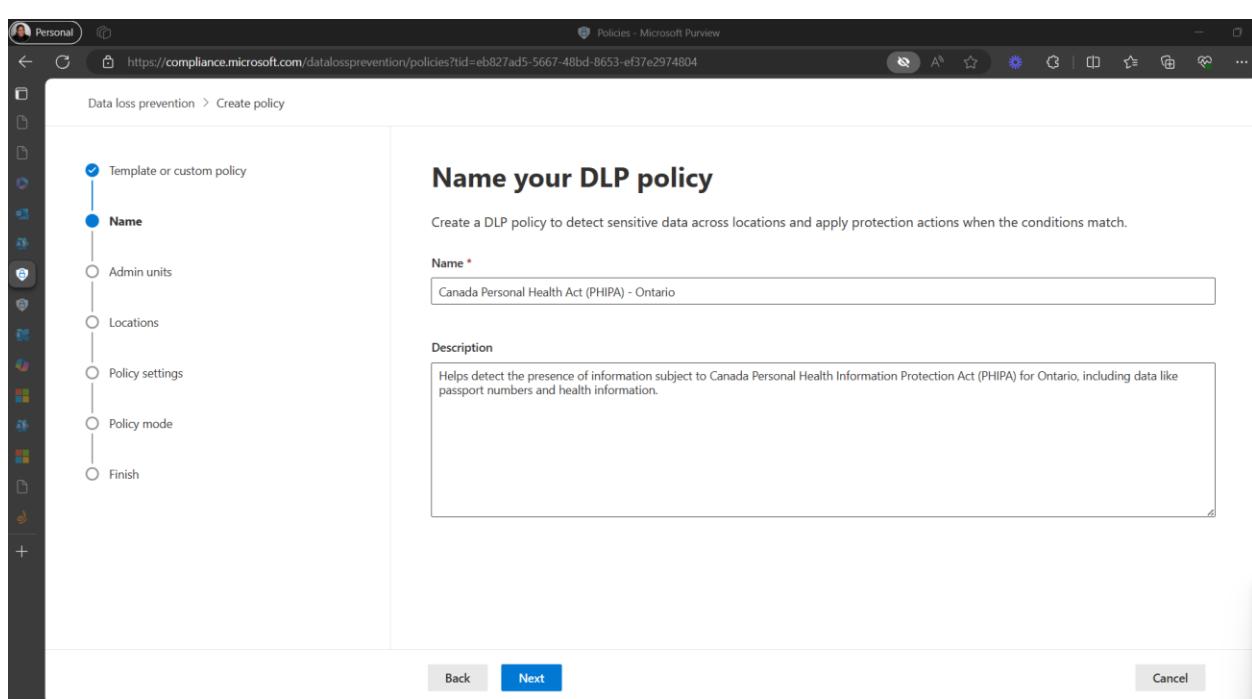


Figure 13: Name Data Loss Prevention Policy

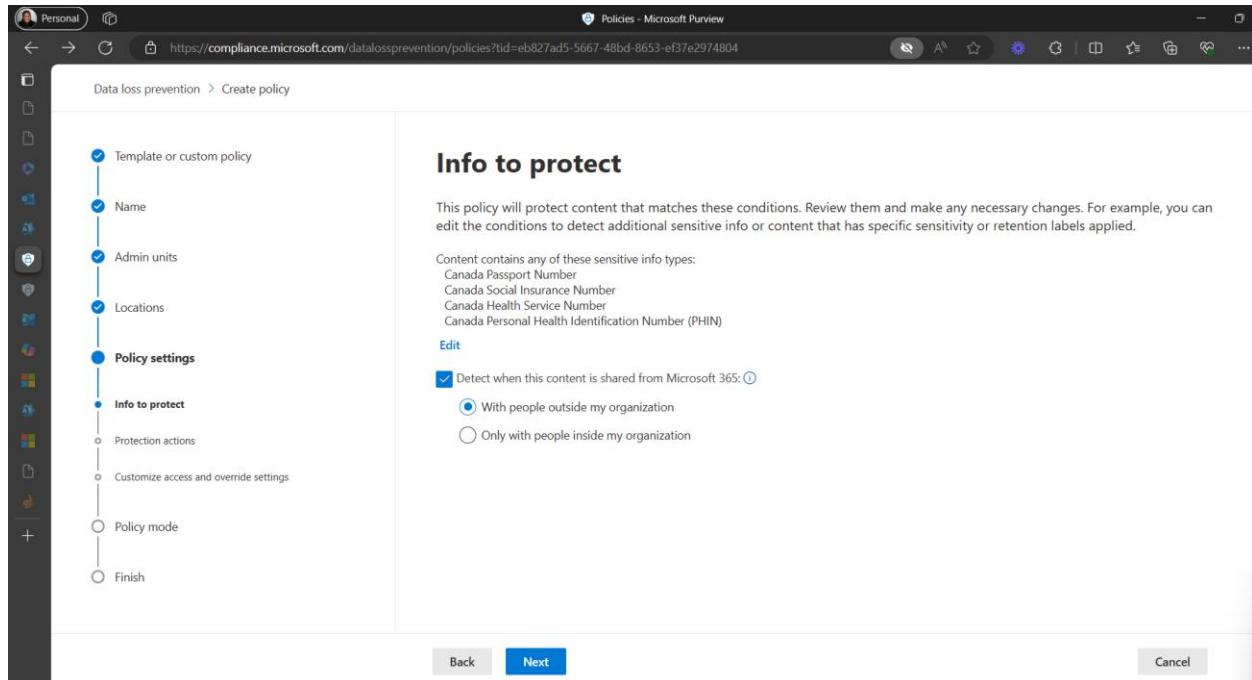


Figure 14: Information to protect

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the 'Create policy' wizard in the Microsoft 365 Identity and Services - Enterprise Administration interface. The current step is 'Protection actions'. On the left, a vertical navigation pane lists steps: 'Template or custom policy', 'Name', 'Admin units', 'Locations', 'Policy settings' (selected), 'Info to protect', 'Protection actions' (under Policy settings), 'Customize access and override settings', 'Policy mode' (under Protection actions), and 'Finish'. The main panel title is 'Protection actions'. It contains a note: 'We'll automatically create detailed activity reports so you can review the content that matches this policy. What else do you want to do?'. Below this are several configuration options with checkboxes:

- 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

Figure 15: Actions to take

The screenshot shows the 'Create policy' wizard in the Microsoft 365 Identity and Services - Enterprise Administration interface. The current step is 'Policy mode'. On the left, the navigation pane shows the same steps as Figure 15, with 'Policy mode' selected. The main panel title is 'Policy mode'. It contains a note: '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.' Below this 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.

Figure 16: Simulation mode

## Microsoft 365 Identity and Services – Enterprise Administration

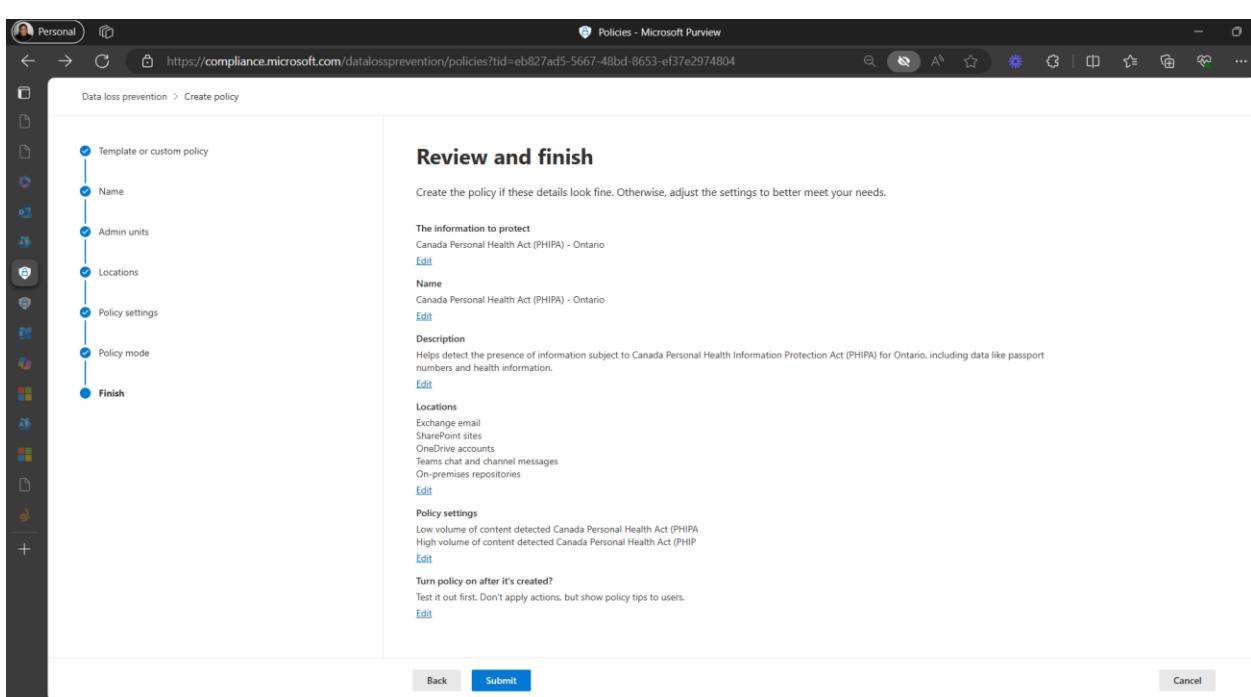


Figure 17: Review

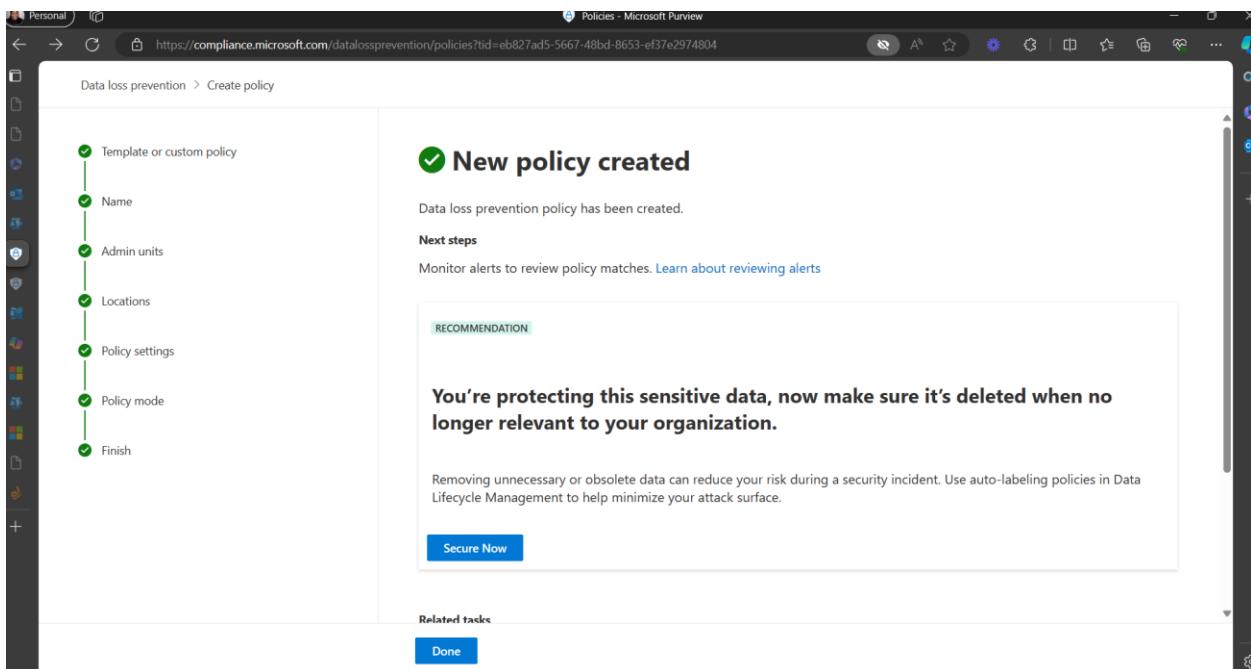


Figure 18: New policy left in simulation mode

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the Microsoft Purview Compliance interface. The left sidebar has sections for Data classification, Data connectors, Alerts, Policies, Roles & scopes, Trials, Solutions (Catalog, Audit, Content search, Communication compliance, Data loss prevention), and eDiscovery. The main area shows a simulation for the Canada Personal Health Act (PHIPA) - Ontario. It indicates "In progress". There are tabs for Simulation overview, Items for review, and Alerts. Under Simulation progress, it says "0 Total items scanned". Under Total matches, it says "0 matches found". A note says "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." A link "Learn more about simulation mode" is provided.

### 1.8 Block emails with .html attachments

The screenshot shows the Exchange admin center Rules page. The left sidebar includes Home, Recipients, Mail flow (Message trace, Rules, Remote domains, Accepted domains, Connectors, Alerts, Alert policies, Roles), Migration, Mobile, Reports, Insights, Public folders, Organization, and Settings. The main area shows a message about DLP policies being deprecated and a note about Office 365 Message Encryption. Below is a "Rules" section with a table of existing rules:

| Status                              | Rule    | Priority               | Stop proc |   |
|-------------------------------------|---------|------------------------|-----------|---|
| <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 |

To the right, there is a "Block html Attachments" configuration panel with sections for Rule settings (Rule name: Block html Attachments, Mode: Enforce, Severity: High, Set date range: Specific date range is not set, Senders address: Matching Header, Priority: 3), For rule processing errors (Ignore), and Rule description (Apply this rule if: has an attachment with a file extension that matches one of these values: 'html'). A success message "Rule status updated successfully" is shown.

## 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

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the Microsoft Power Platform admin center interface. On the left, there is 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. The main content area displays a list of tenant settings under the 'Analytics' category. One setting, 'Enable tenant level analytics', is highlighted with a purple background. To the right of this list is a panel titled 'Analytics' which contains sections for 'Terms of Service' and 'Tenant-level analytics'. A toggle switch labeled 'Enable' is shown in the 'Tenant-level analytics' section. At the bottom right of the main content area 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 for Home, Create, Learn, Apps, Tables, Flows, Solutions, More, Discover, and Power Platform. The main content area features several cards: 'websites and connect it to your app', 'and employees—no coding required', 'gain insights', 'Data', 'Choices', 'Connections' (which is highlighted with a green border), 'Custom connectors', 'Cards', 'Power Apps', 'Solutions', 'Data Management', 'Dataflows', 'App enhancements', 'Component libraries', and 'App Management'. The 'Connections' card provides a link to see all data connections in the environment.

Figure 20: Navigate Data to Connections

## Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows the Microsoft Power Apps interface. On the left, there's a navigation bar with options like Home, Create, Learn, Apps, Tables, Flows, Solutions, Connections (which is selected and highlighted in pink), and More. Below these are sections for Power Platform and Ask a virtual agent. The main content area is titled "Power Apps" and has a search bar. A "New connection" button is visible. The "Connections in Jen MBA (default)" section is highlighted with a green box. It contains a table with columns: Name, Modified, and Status. The data in the table is as follows:

| 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

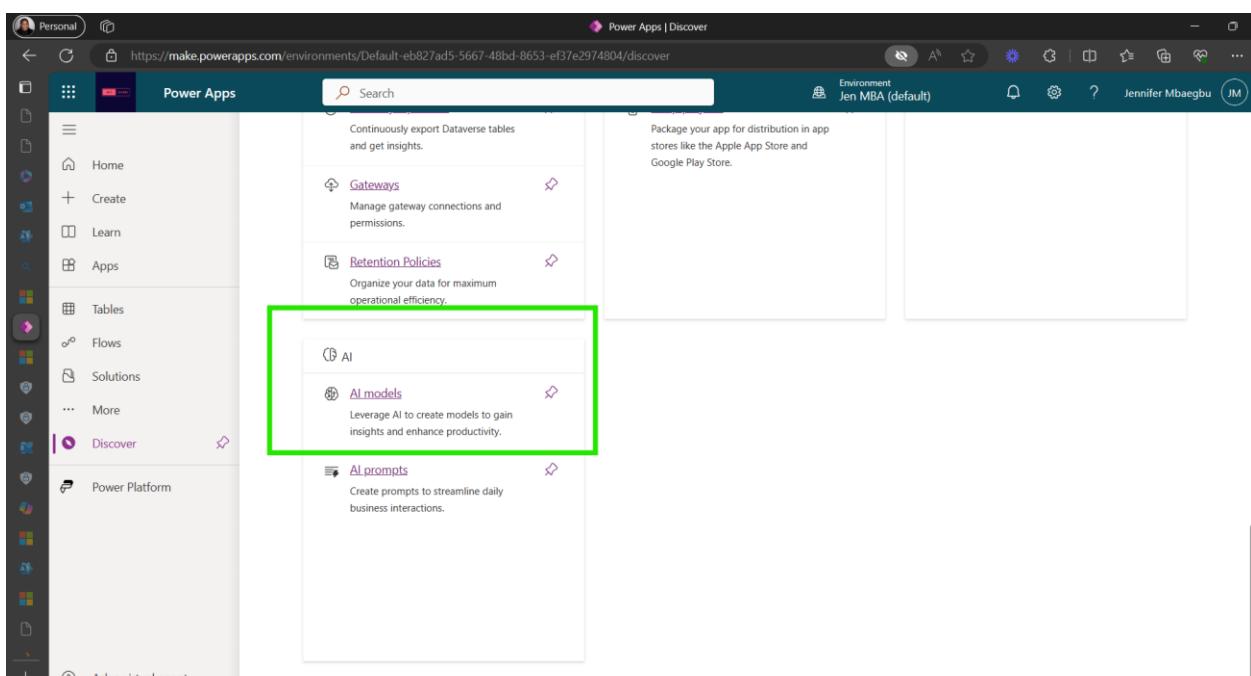
2.3 Identify of the name of the AI Builder used to “Extract information from receipts” **Navigate to Discover tab > AI tab > AI models > Extract Information from receipts.**

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 "More" dropdown is open, showing options like Tables, Flows, Websites, Chatbots, AI hub, Solutions, Cards, Choices, Connections, and Dataflows. 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 items. The table has columns: Modified, Owner, and Type. The data is as follows:

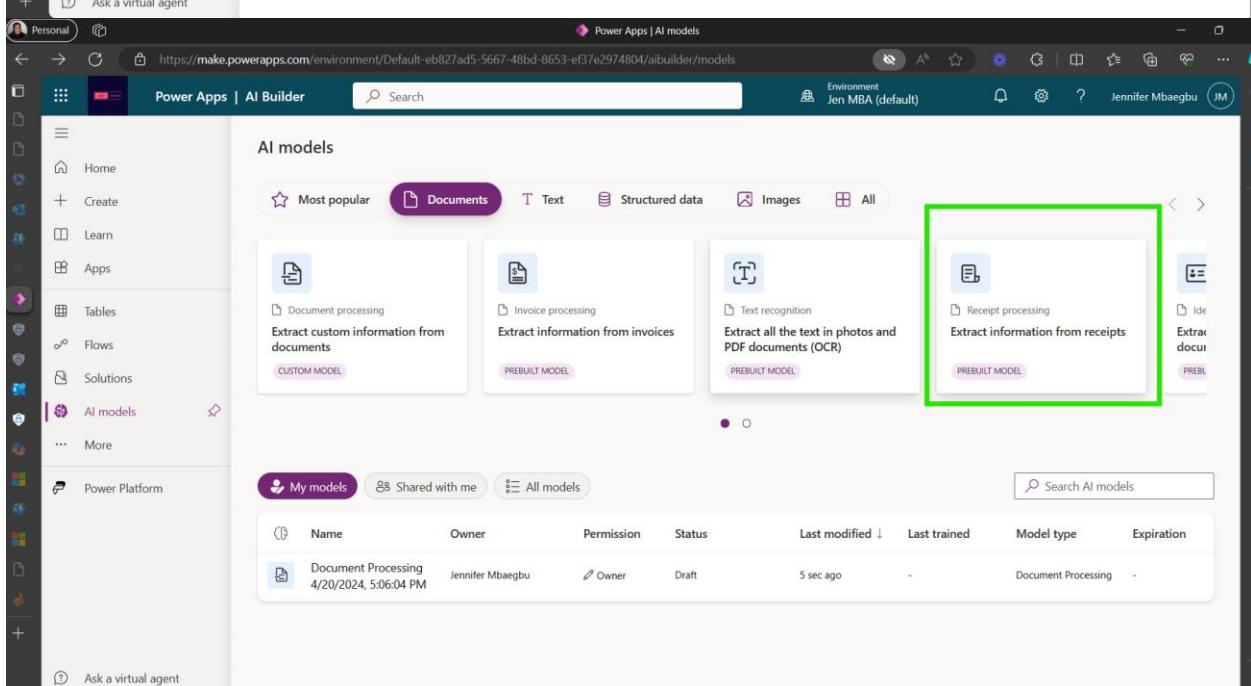
| Modified    | Owner            | Type         |
|-------------|------------------|--------------|
| 3 days ago  | Jennifer Mbaegbu | Canvas       |
| 2 weeks ago | Jennifer Mbaegbu | Model-driven |
| 2 weeks ago | Jennifer Mbaegbu | Model-driven |
| 2 weeks ago | Jennifer Mbaegbu | Model-driven |

## 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 displays several cards. One card for 'AI' is highlighted with a green box. It contains sections for 'AI models' and 'AI prompts'. The 'AI models' section is described as 'Leverage AI to create models to gain insights and enhance productivity.' Another card for 'Retention Policies' is also visible.

The screenshot shows the Microsoft Power Apps AI Builder page. The left sidebar includes Home, Create, Learn, Apps, Tables, Flows, Solutions, AI models (which is selected and highlighted with a green box), and Power Platform. The main content area is titled 'AI models' and features a 'Documents' tab selected. It lists four pre-built AI models: 'Document processing', 'Invoice processing', 'Text recognition', and 'Receipt processing'. The 'Receipt processing' model is highlighted with a green box. Below the models, there's a table for 'My models' showing one entry: 'Document Processing' created on 4/20/2024 at 5:06:04 PM by Jennifer Mbaegbu, with a status of 'Draft'.

## 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:

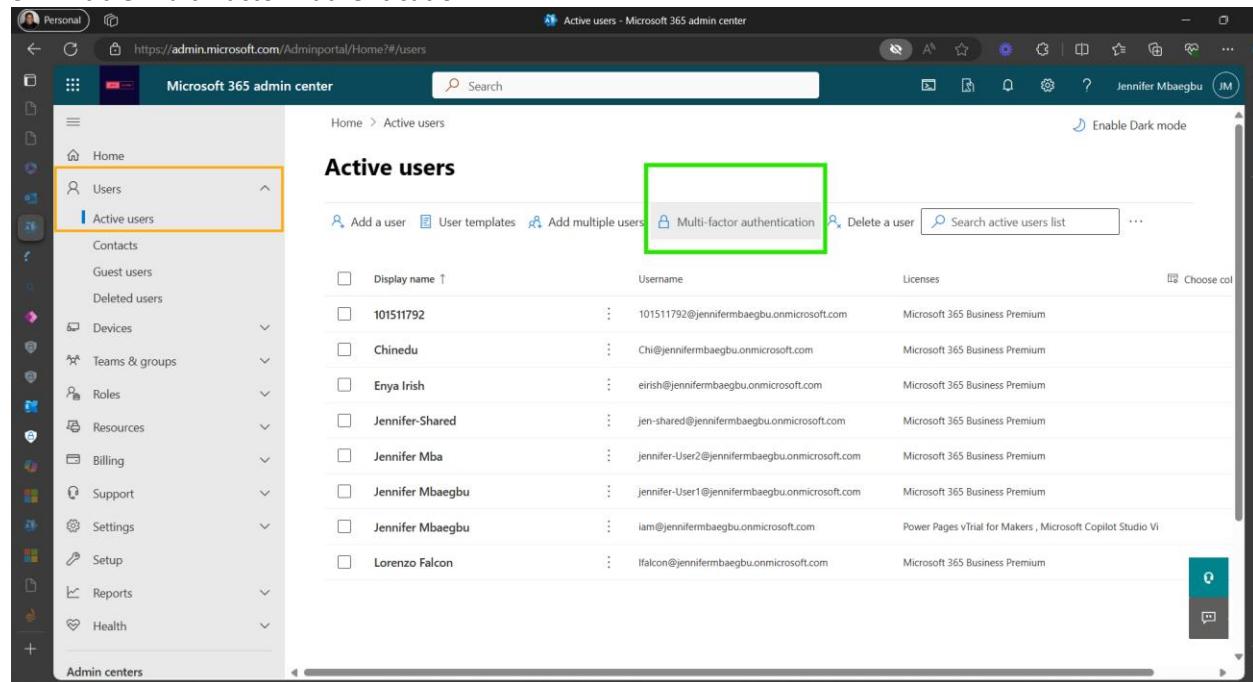
|               |          |
|---------------|----------|
| Surface Pro 6 | \$599.00 |
| Surface Pen   | \$99.95  |
| Sub-Total     | \$604.95 |
| Tax           | \$10.45  |
| Total         | \$615.40 |

## Microsoft 365 Identity and Services – Enterprise Administration

---

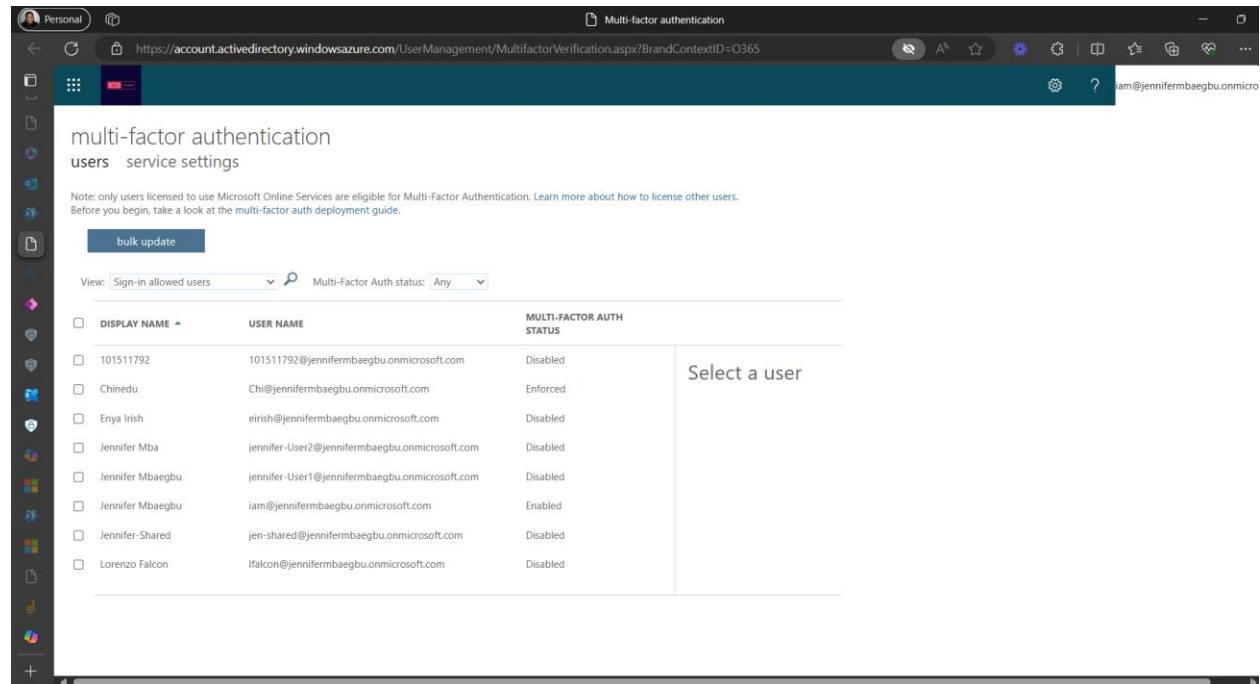
### Task 3: MFA

#### 3.1 Enable Multi Factor Authentication



The screenshot shows the Microsoft 365 Admin Center interface. The left sidebar has a 'Users' section with 'Active users' selected, highlighted by a yellow box. The main content area is titled 'Active users' and contains a table of user information. At the top of this table, there is a button labeled 'Multi-factor authentication' which is highlighted with a green box. Other buttons visible include 'Add a user', 'User templates', 'Add multiple users', 'Delete a user', and a search bar.

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 'bulk update' button highlighted with a blue box. Below it is a search bar with filters for 'View: Sign-in allowed users' and 'Multi-Factor Auth status: Any'. The main table lists users with columns for 'DISPLAY NAME', 'USER NAME', and 'MULTI-FACTOR AUTH STATUS'. One user, 'Jennifer Mbaegbu', has 'Enabled' status. A modal window titled 'Select a user' is overlaid on the table, covering the last two columns of the first few rows.

| 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                 |

## 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 section. 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 'quick steps' section containing 'Enable' and 'Manage user settings' buttons.

| 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 instructions: 'Please read the deployment guide if you haven't already.' and 'If your users do not regularly sign in through the browser, you can send them to this link to register for multi-factor auth: <https://aka.ms/MFASetup>'. There are two buttons at the bottom: 'enable multi-factor auth' and 'cancel'.

## Microsoft 365 Identity and Services – Enterprise Administration

multi-factor authentication

users service settings

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                  |

Updates successful  
Multi-factor auth is now enabled for the selected accounts.

close

### 3.2 Enforce MFA

multi-factor authentication

users service settings

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      | Enabled                  |
| Chinedu          | Chi@jennifermbaegbu.onmicrosoft.com            | Enforced                 |
| Enya Irish       | eirish@jennifermbaegbu.onmicrosoft.com         | Enabled                  |
| Jennifer Mba     | jennifer-User2@jennifermbaegbu.onmicrosoft.com | Enabled                  |
| Jennifer Mbuegbu | jennifer-User1@jennifermbaegbu.onmicrosoft.com | Enabled                  |
| Jennifer Mbuegbu | iam@jennifermbaegbu.onmicrosoft.com            | Enabled                  |
| Jennifer-Shared  | jen-shared@jennifermbaegbu.onmicrosoft.com     | Enabled                  |
| Lorenzo Falcon   | lfalcon@jennifermbaegbu.onmicrosoft.com        | Enabled                  |

7 selected

quick steps

Disable

Enforce

Manage user settings

## Microsoft 365 Identity and Services – Enterprise Administration

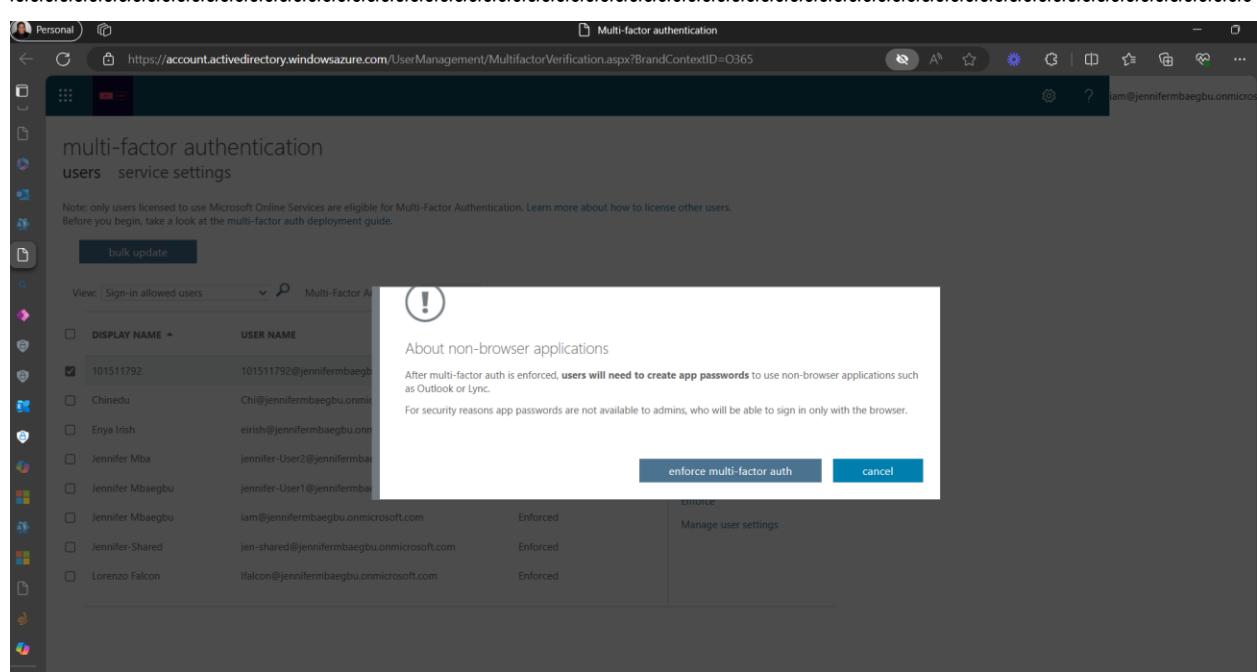


Figure 23: Enforce Multi-factor Authentication

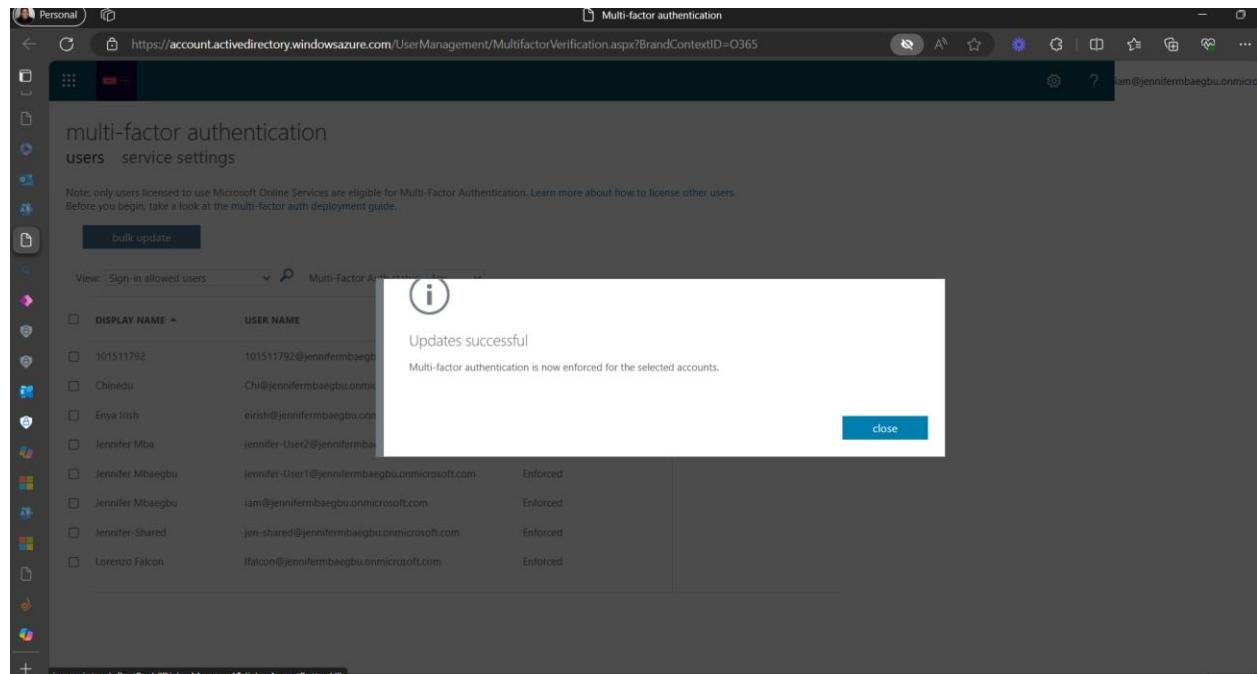


Figure 24: Multi-factor authentication enforced

## Microsoft 365 Identity and Services – Enterprise Administration

---

### 3.3 Setup MFA

The image contains two screenshots from a Microsoft Edge browser window. Both screenshots show a Microsoft sign-in page with an 'InPrivate' tab selected.

**Screenshot 1:** The top screenshot shows a 'Sign in to your account - [InPrivate]' page. It displays the Microsoft logo and the email address 'nedu@jennifermbaegbu.onmicrosoft.com'. A large central box titled 'Action Required' states: 'Your organization requires additional security information. Follow the prompts to download and set up the Microsoft Authenticator app.' Below this are links to 'Use a different account' and 'Learn more about the Microsoft Authenticator app', followed by a blue 'Next' button.

**Screenshot 2:** The bottom screenshot shows a 'My Sign-Ins | Register | Microsoft.com - [InPrivate]' page. It has a header 'Jen Cloud'. A central box titled 'Keep your account secure' contains the text 'Microsoft Authenticator' and 'Start by getting the app'. It includes a blue circular icon with a person and a lock, and the text: 'On your phone, install the Microsoft Authenticator app. Download now'. Below this, it says 'After you install the Microsoft Authenticator app on your device, choose "Next".' There is also a link 'I want to use a different authenticator app'. At the bottom of this box is a blue 'Next' button.

## 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

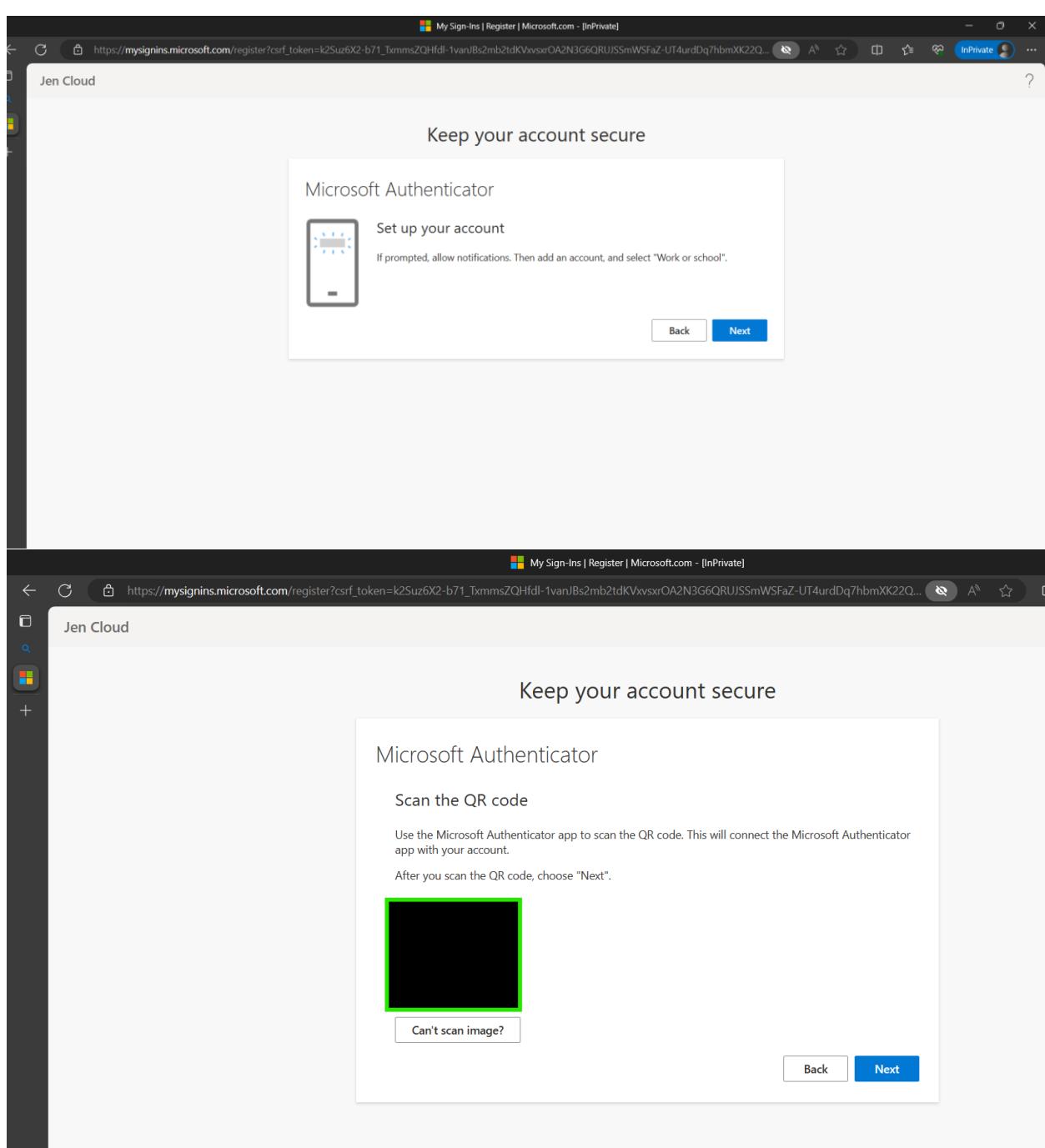
Scan the QR code

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 web browser window. Both screenshots have a dark grey header bar with the Microsoft logo, 'My Sign-Ins | Register | Microsoft.com - [InPrivate]' and a URL 'https://mysignins.microsoft.com/register?csrf_token=k2Suz6X2-b71_TxmmsZQHfdl-1vanJBs2mb2tdKVvxsxOA2N3G6QRUJSSmWSFaZ-UT4urdDq7hbmXK22Q...'. The browser's address bar shows 'Jen Cloud'.

Screenshot 1: Step 1 - Let's try it out

This screenshot shows the 'Keep your account secure' page. A central box is titled 'Microsoft Authenticator' and contains a smartphone icon with a checkmark. Below it is the text 'Let's try it out'. A horizontal line separates this from the instruction 'Approve the notification we're sending to your app by entering the number shown below.' To the right of this line is a small green square containing a black rectangle. At the bottom are 'Back' and 'Next' buttons.

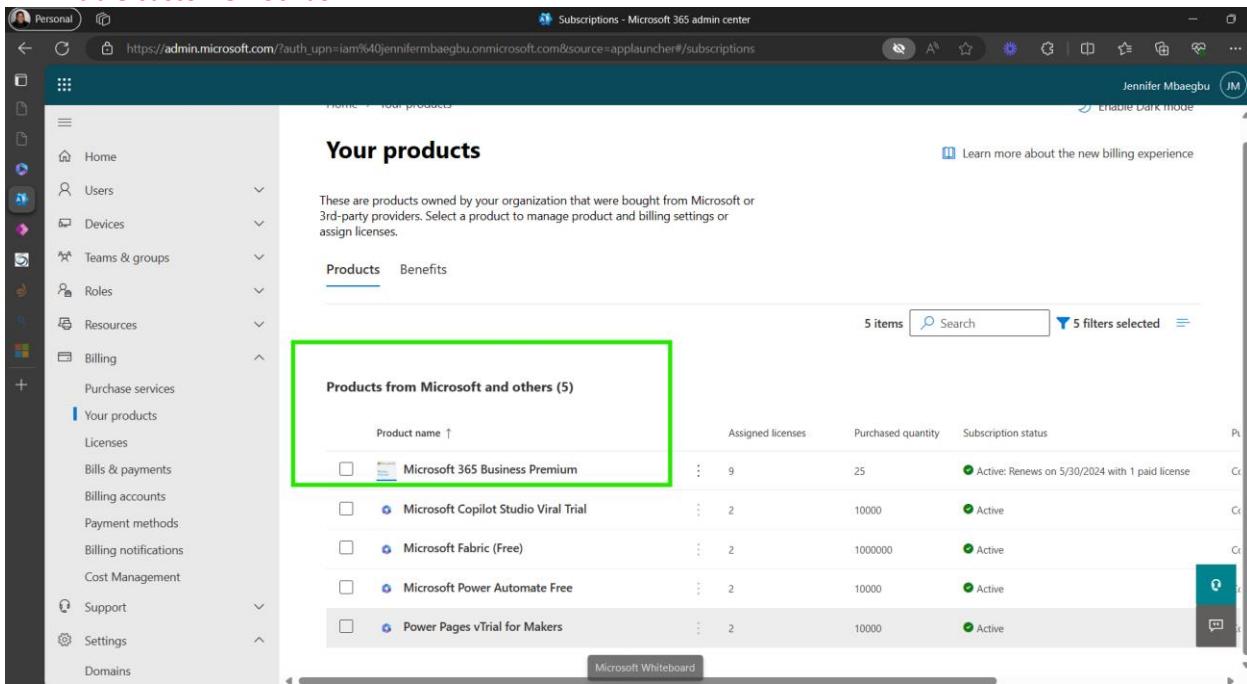
Screenshot 2: Step 2 - Success!

This screenshot shows the same 'Keep your account secure' page after the process is completed. The central box now displays 'Success!' and the message 'Great job! You have successfully set up your security info. Choose "Done" to continue signing in.' Below this, under 'Default sign-in method:', there is a list item with a Microsoft Authenticator icon and the text 'Microsoft Authenticator'. At the bottom right is a large blue 'Done' button. In the top right corner of the main window, there is a green status bar with the text 'Microsoft Authenticator app was successfully registered' and the date 'Sat, 20 Apr 2024 21:37:42 GMT'.

Microsoft 365 Identity and Services – Enterprise Administration

Task 4: Customer lockbox

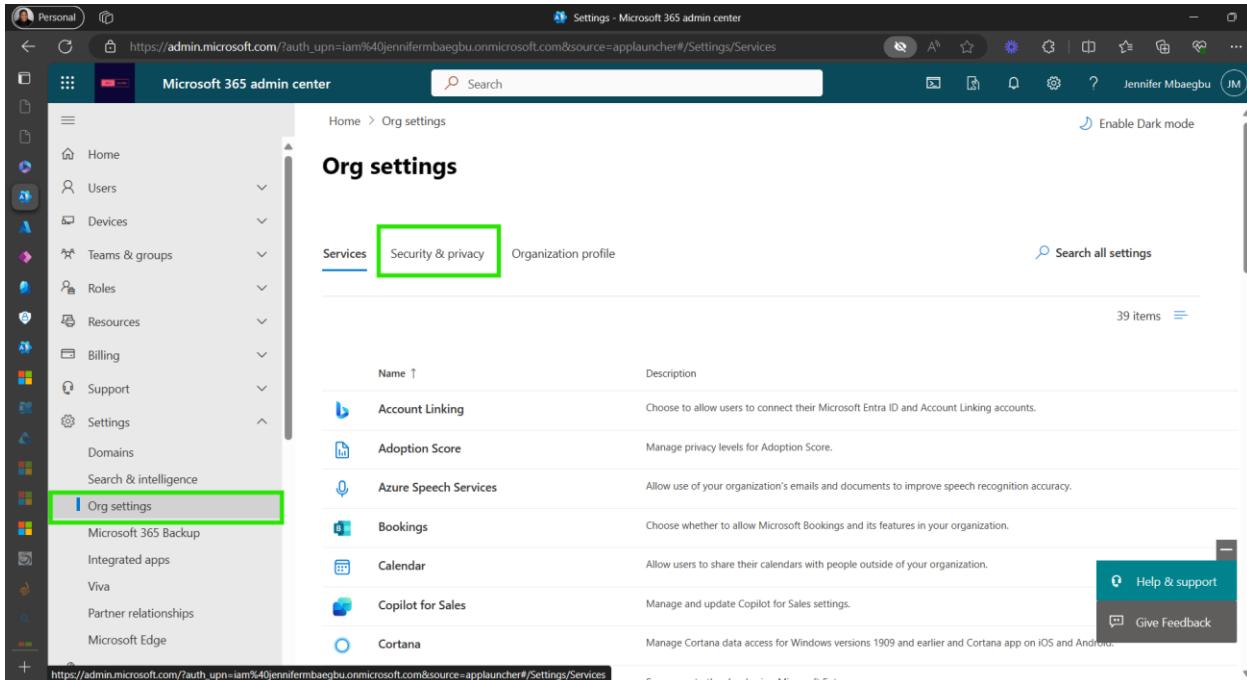
4.1 Enable customer lockbox:



The screenshot shows the Microsoft 365 Subscriptions page. 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 contains a sub-section 'Products from Microsoft and others (5)'. This section lists five products with columns for Product name, Assigned licenses, Purchased quantity, and Subscription status. The products listed are Microsoft 365 Business Premium, Microsoft Copilot Studio Viral Trial, Microsoft Fabric (Free), Microsoft Power Automate Free, and Power Pages vTrial for Makers.

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 with the 'Org settings' page selected. The navigation menu on the left includes Home, Users, Devices, Teams & groups, Roles, Resources, Billing, Support, Settings, Domains, Search & intelligence, and Org settings. The 'Org settings' option is highlighted with a green box. In the main content area, there are three tabs: Services (selected), Security & privacy (highlighted with a green box), and Organization profile. Below these tabs is a table listing various services with their names and descriptions. The services listed are Account Linking, Adoption Score, Azure Speech Services, Bookings, Calendar, Copilot for Sales, and Cortana.

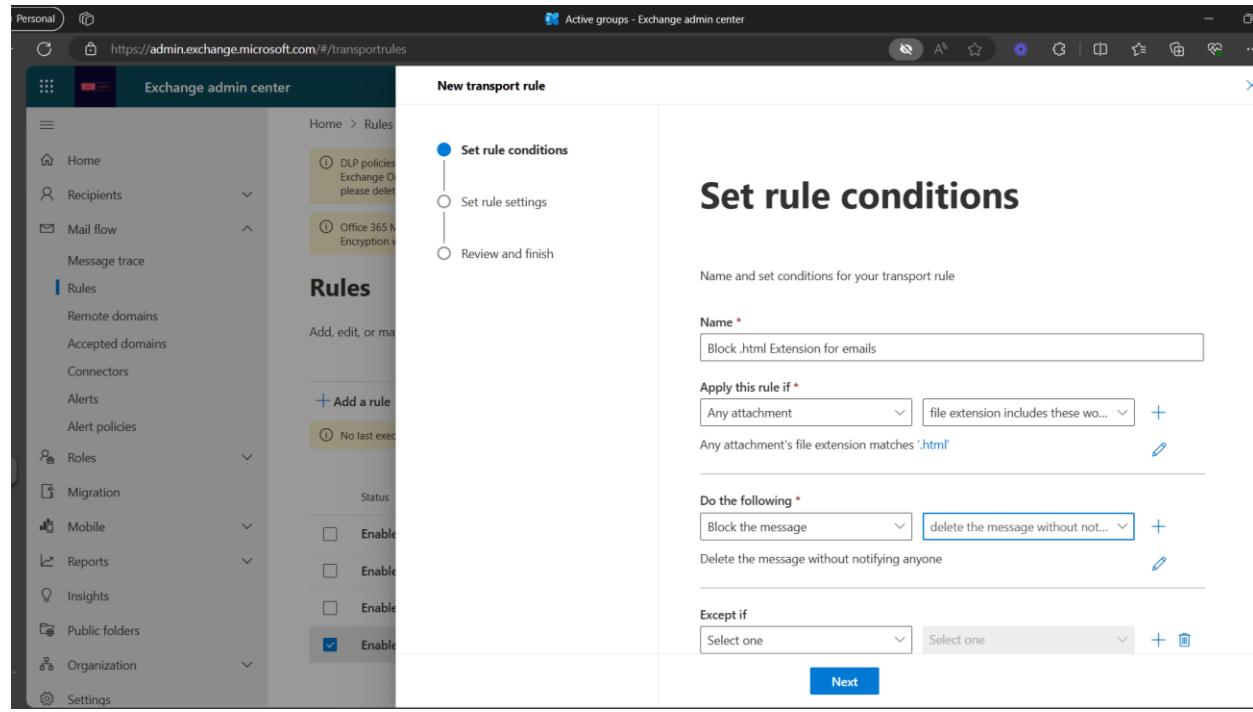
Figure 26: On Microsoft 365 Admin center, navigate to Settings - Org Settings - Security and Privacy

Microsoft 365 Identity and Services – Enterprise Administration

Microsoft 365 Identity and Services – Enterprise Administration

Task 5: Security

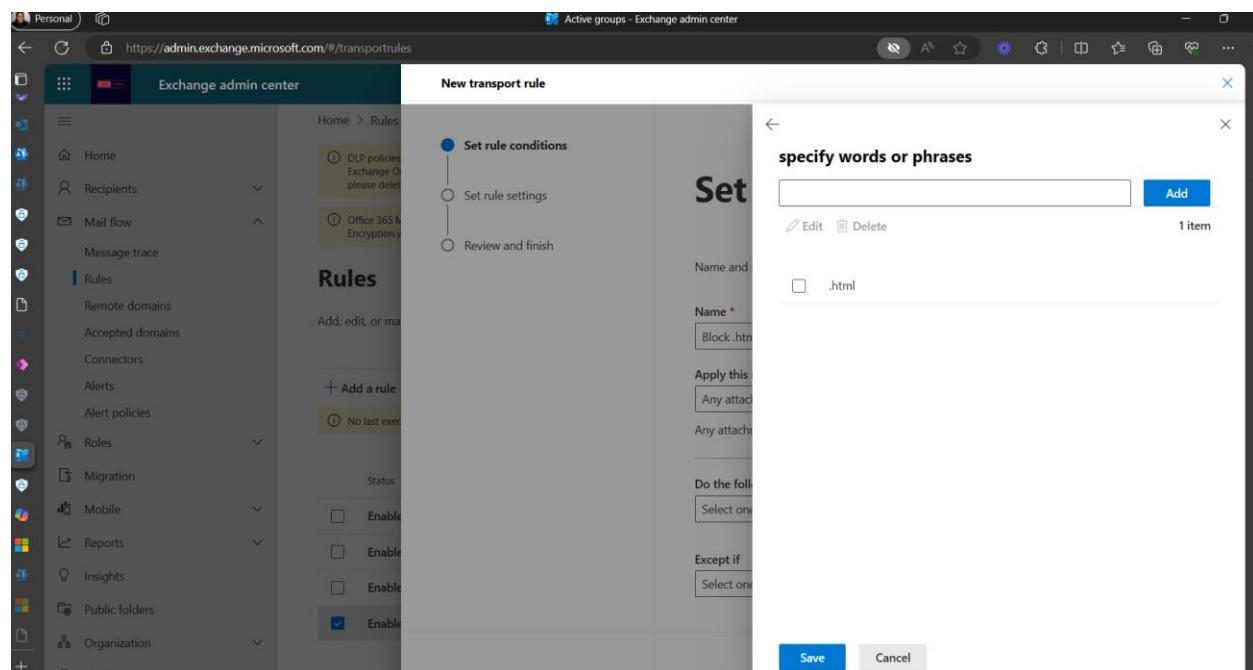
5.1 Block .html extension for emails



The screenshot shows the Exchange admin center interface. On the left, the navigation menu is visible 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 main content area, a 'New transport rule' wizard is open. The first step, 'Set rule conditions', is selected. The configuration pane shows:

- Name:** Block .html Extension for emails
- Apply this rule if:** Any attachment file extension includes these words...
Any attachment's file extension matches '.html'
- Do the following:** Block the message, delete the message without notifying anyone
- Except if:** Select one

A 'Next' button is at the bottom right of the configuration pane.



This screenshot shows the continuation of the transport rule creation process. The 'Set rule conditions' step is still active. A modal dialog titled 'specify words or phrases' is open, prompting the user to enter words or phrases to exclude. The input field contains '.html'. The configuration pane below the modal is identical to the previous screenshot, showing the rule name and its conditions and actions.

Figure 27: .html is specified

Microsoft 365 Identity and Services – Enterprise Administration

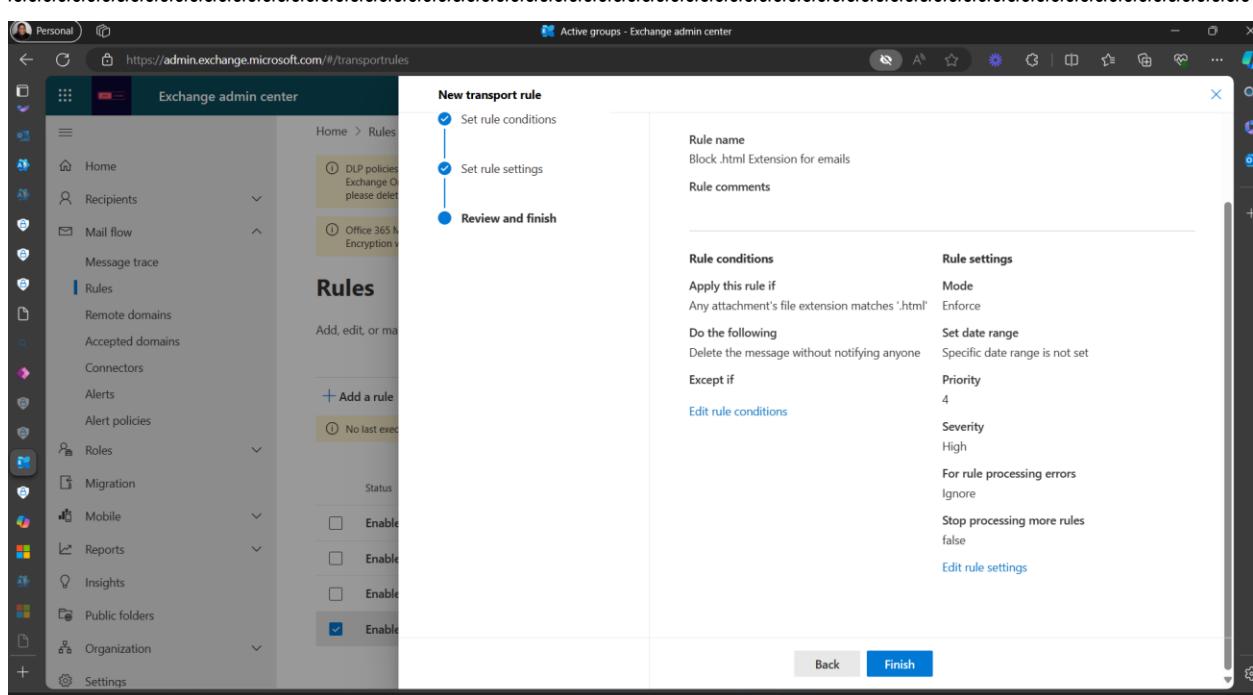


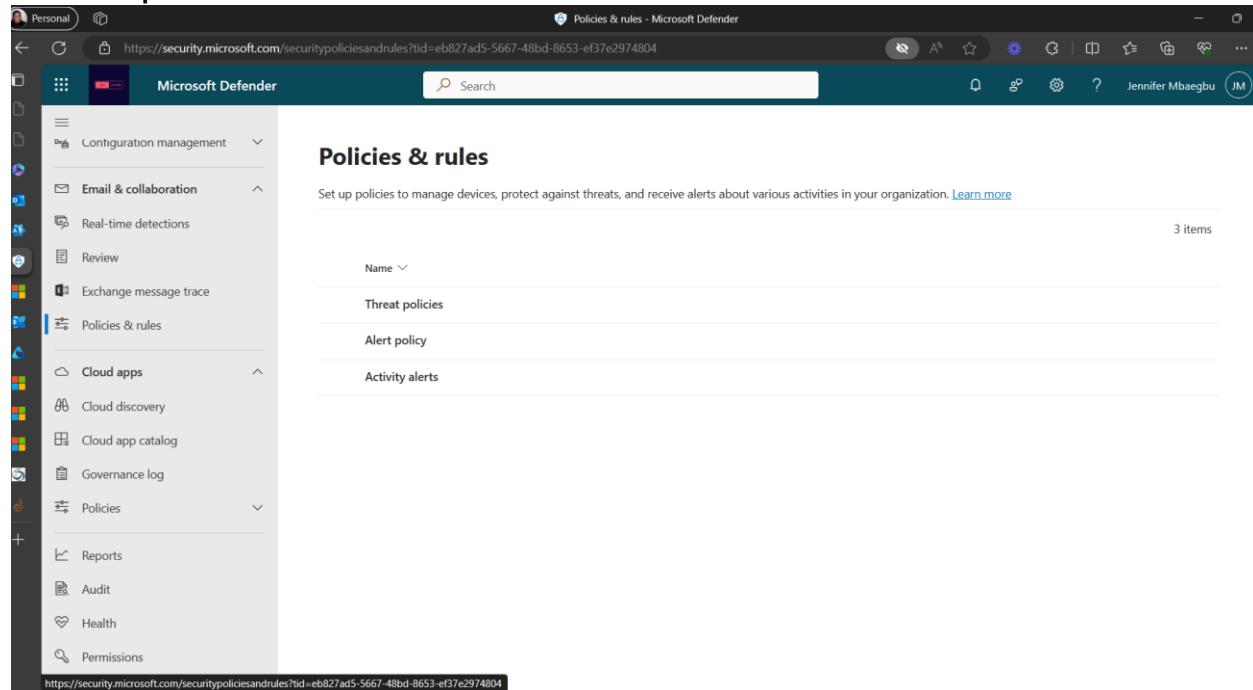
Figure 28: Review New Transport Rule on Exchange Center to Block .html

The screenshot shows the Exchange Admin Center interface. The 'Rules' section is selected in the navigation menu. A specific rule, 'Block html Attachments', is highlighted. The rule details are as follows:

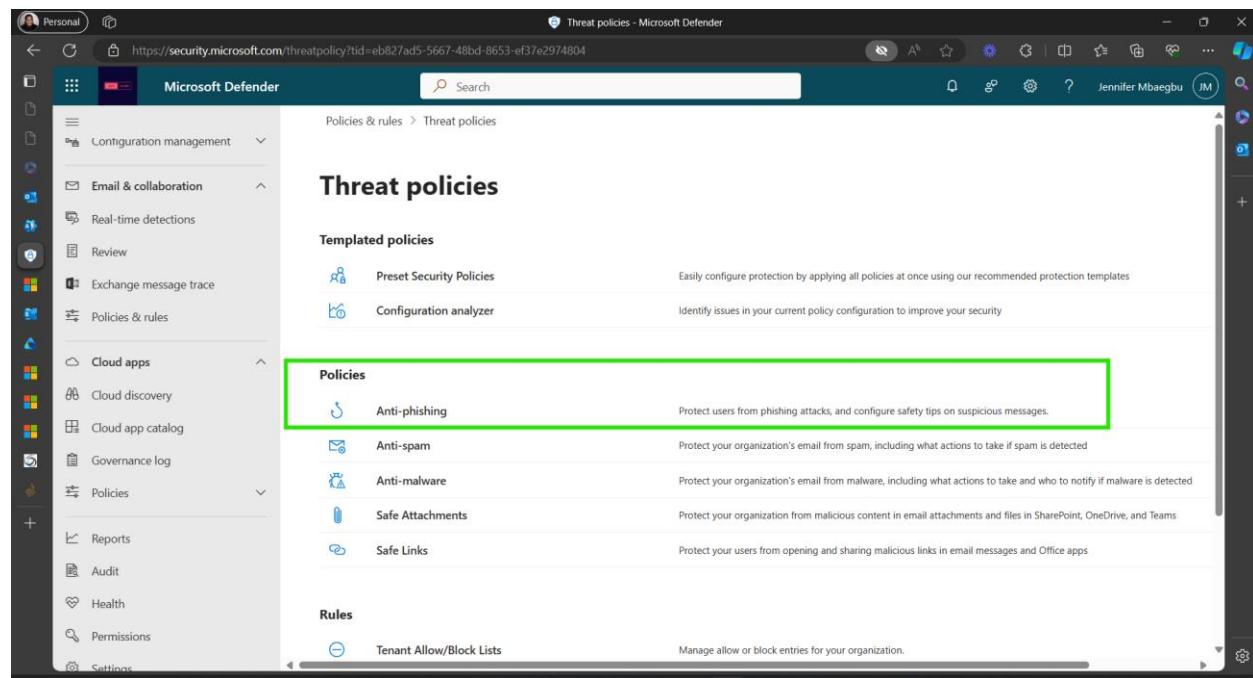
- Status:** Enabled
- Enable or disable rule:** Enabled
- Rule settings:**
 - Rule name:** Block html Attachments
 - Mode:** Enforce
 - Set date range:** Specific date range is not set
 - Senders address:** Matching Header
 - Priority:** 3
 - For rule processing errors:** Ignore
- Rule description:** 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

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

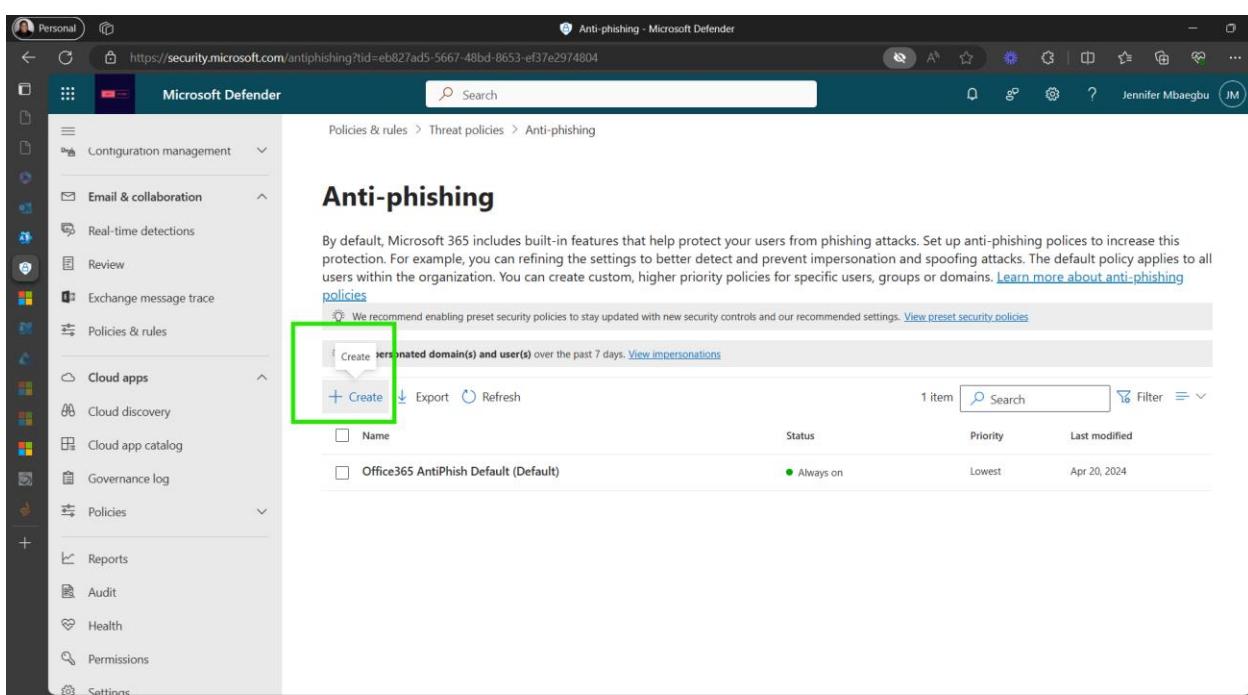


The screenshot shows the Microsoft Defender interface for 'Policies & rules'. The left sidebar includes sections like Configuration management, Email & collaboration, Real-time detections, Review, Exchange message trace, Policies & rules (which is expanded), Cloud apps, Cloud discovery, Cloud app catalog, Governance log, Policies, Reports, Audit, Health, and Permissions. The main content area is titled 'Policies & rules' and contains a sub-section 'Threat policies'. It lists 'Name' (dropdown), 'Threat policies', 'Alert policy', and 'Activity alerts'. A note says 'Set up policies to manage devices, protect against threats, and receive alerts about various activities in your organization.' with a 'Learn more' link. At the bottom, there are three items listed: 'Name' (dropdown), 'Threat policies', and 'Alert policy'. The URL in the address bar is <https://security.microsoft.com/securitypoliciesandrules?tid=eb827ad5-5667-48bd-8653-ef37e2974804>.



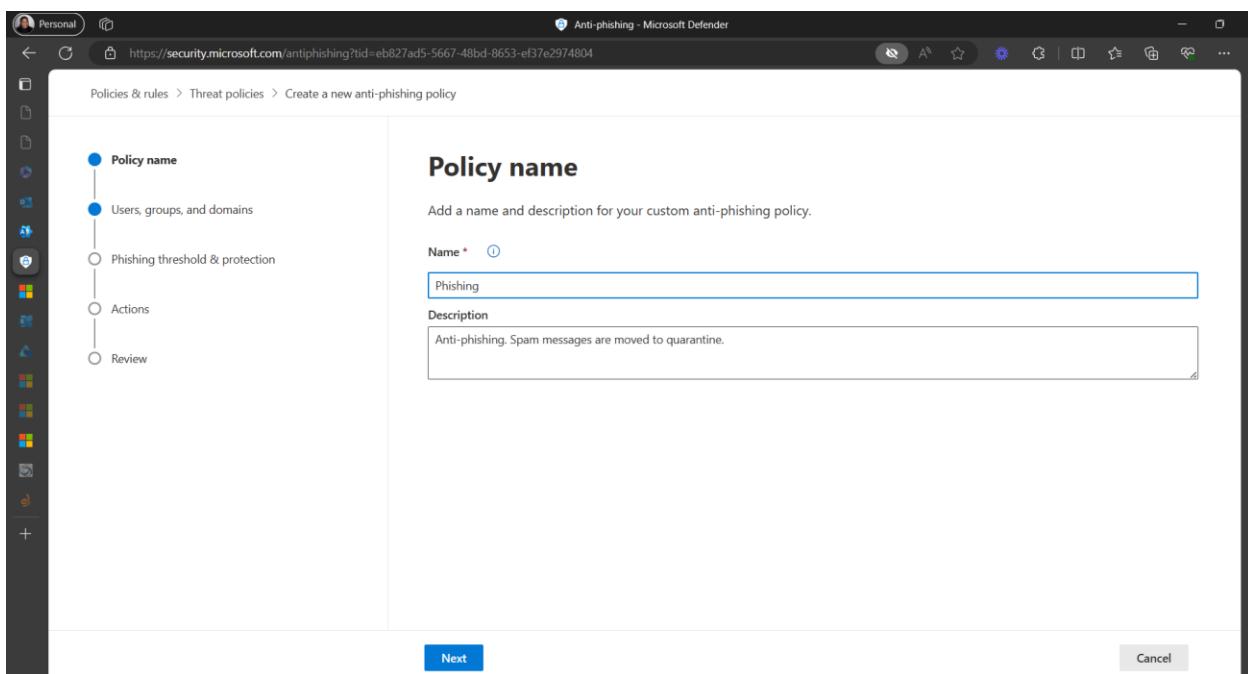
The screenshot shows the Microsoft Defender interface for 'Threat policies'. The left sidebar is identical to the previous screenshot. The main content area is titled 'Threat policies' and shows 'Policies & rules > Threat policies'. It has two sections: 'Templated policies' (Preset Security Policies, Configuration analyzer) and 'Policies'. The 'Policies' section is highlighted with a green box and lists five items: 'Anti-phishing' (selected), 'Anti-spam', 'Anti-malware', 'Safe Attachments', and 'Safe Links'. Each item has a description. Below this is a 'Rules' section with 'Tenant Allow/Block Lists'. The URL in the address bar is <https://security.microsoft.com/threatpolicy?tid=eb827ad5-5667-48bd-8653-ef37e2974804>.

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" dialog. On the left, a navigation pane lists steps: Policy name (selected), Users, groups, and domains, Phishing threshold & protection, Actions, and Review. The main area is titled "Policy name" and contains fields for "Name" (Phishing) and "Description" (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 consecutive steps in the 'Create a new anti-phishing policy' wizard.

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. The 'Include these users, groups and domains *' section lists several users and groups:

- 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.

Step 2: Phishing threshold & protection

This step lets you set phishing thresholds and impersonation protection. The 'Phishing email threshold' slider is set to '4 - Most Aggressive'. Under 'Impersonation', the 'Enable users to protect (0/350)' checkbox is checked, and 'Enable domains to protect (1)' is also checked. Under 'Enable domains to protect (1)', 'Include domains I own' and 'Include custom domains' are selected.

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 titled "Policies & rules > Threat policies > Create a new anti-phishing policy". On the left, a vertical navigation pane 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 contains instructions: "Set what actions you'd like this policy to take on messages. You may need to turn on certain protections to access all available policy actions." It includes sections for "Message actions" (dropdown set to "Quarantine the message") and "Apply quarantine policy" (dropdown set to "AdminOnlyAccessPolicy"). Below these are sections for "If a message is detected as user impersonation" and "If a message is detected as domain impersonation", both with dropdowns set to "Quarantine the message". A note states: "We'll quarantine the message for you to review and decide whether it should be released. [Learn how to manage quarantined messages](#)". There is also a section for "If Mailbox Intelligence detects an impersonated user" with a dropdown set to "AdminOnlyAccessPolicy". At the bottom are "Back", "Next", and "Cancel" buttons.

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 titled "Policies & rules > Threat policies > Create a new anti-phishing policy". The left navigation pane shows all steps completed with checkmarks: Policy name, Users, groups, and domains, Phishing threshold & protection, Actions, and Review. The main content area displays a success message: "New anti-phishing policy created" with a green checkmark icon. It 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, 'Threat policies' is selected. 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 highlighted with a green box. Below it, there's a section for 'Rules' (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 enabling preset security policies. It features a 'Create' button highlighted with a green box, along with other buttons for Export, Refresh, and Reports. A table lists two items: 'Safe Links' (Status: On, Priority: 0) and 'Built-in protection (Microsoft)' (Status: On, Priority: Lowest).

Figure 31: Create Safe Links Policy

Microsoft 365 Identity and Services – Enterprise Administration

The screenshot shows a Microsoft Edge browser window with the URL <https://security.microsoft.com/safelinksv2?tid=eb827ad5-5667-48bd-8653-ef37e2974804>. The page title is "Safe links - Microsoft Defender". The left sidebar has a "Personal" profile icon and a list of icons for various Microsoft services. The main content area shows a navigation path: "Policies & rules > Threat policies > Create safe links policy". On the left, a vertical list of steps is shown: "Name your policy" (selected), "Users and domains", "URL & click protection settings", "Notification", and "Review". The right panel is titled "Name your policy" and 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 same Microsoft Edge browser window continuing through the "Create safe links policy" wizard. The left sidebar and navigation path remain the same. The vertical step list now includes "Name your policy", "Users and domains", "URL & click protection settings" (selected), "Notification", and "Review". The right panel is titled "URL & click protection settings" and contains sections for "Email", "Teams", and "Office 365 Apps". Under "Email", there are several checkboxes: "On: Safe Links checks a list of known, malicious links when users click links in email. URLs are rewritten by default." (checked), "Apply Safe Links to email messages sent within the organization" (checked), "Apply real-time URL scanning for suspicious links and links that point to files" (checked), "Wait for URL scanning to complete before delivering the message" (checked), and "Do not rewrite URLs; do checks via Safe Links API only." (checked). Below these are buttons for "Do not rewrite the following URLs in email (0)" and "Manage 0 URLs". Under "Teams", there is one checked checkbox: "On: Safe Links checks a list of known, malicious links when users click links in Microsoft Teams. URLs are not rewritten." Under "Office 365 Apps", there is a note: "Once Click Link checker is set up, malicious links within certain areas like links in Microsoft Office apps, LinkedIn, and more will be removed." 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.