~~~~~~

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

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.

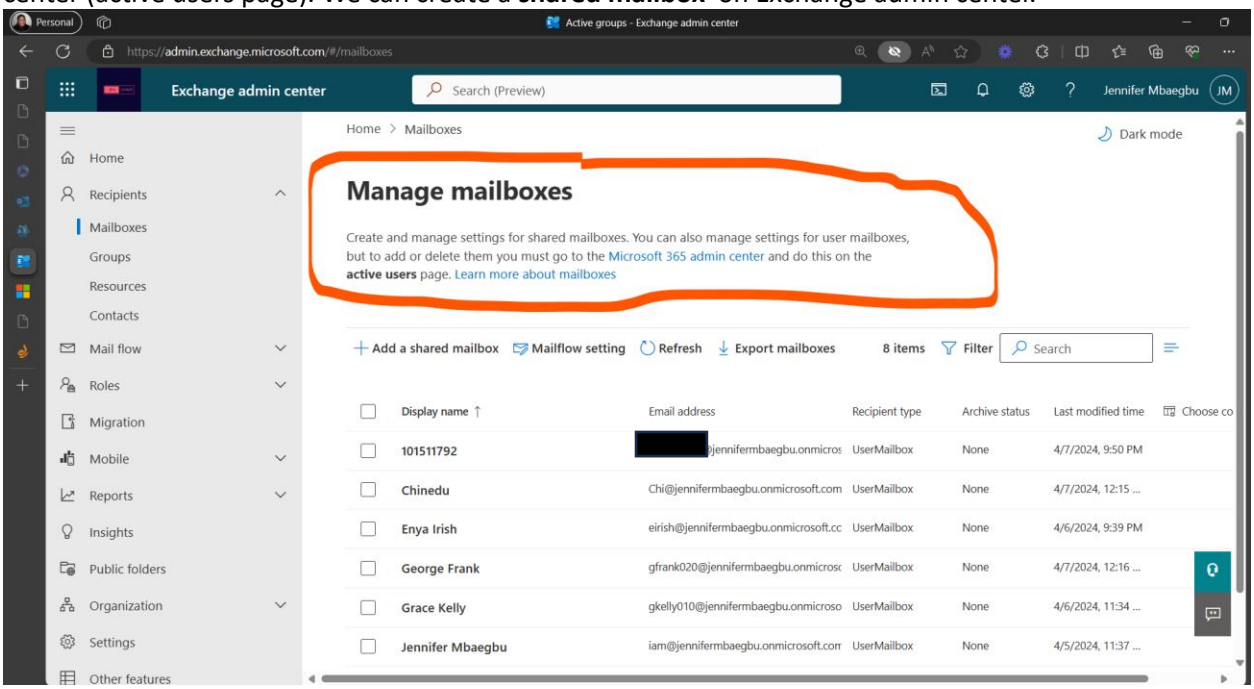


Figure 1: Add or Delete User Mailbox via Microsoft 365 Admin Center

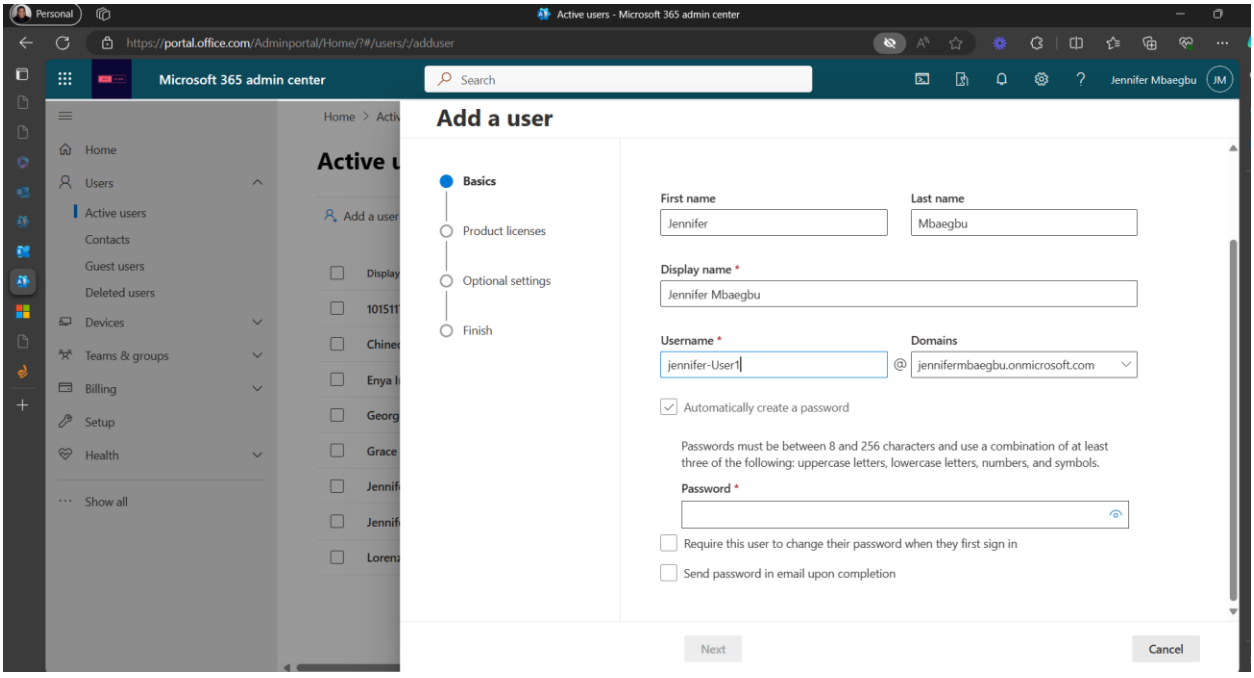


Figure 2: Create User mailbox on Microsoft 365 Admin Center

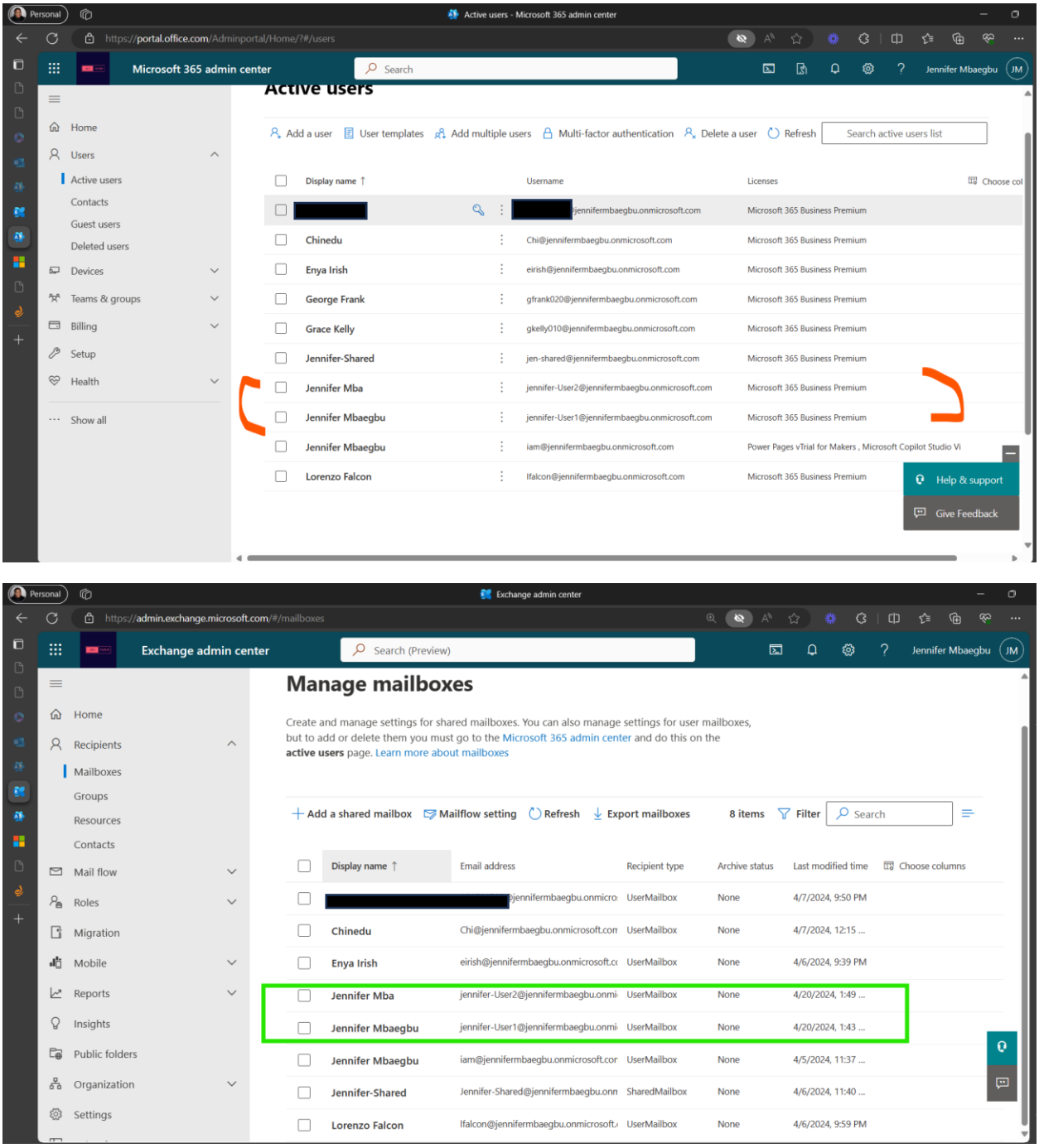


Figure 3: New User Mailbox active on Exchange Admin Center

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

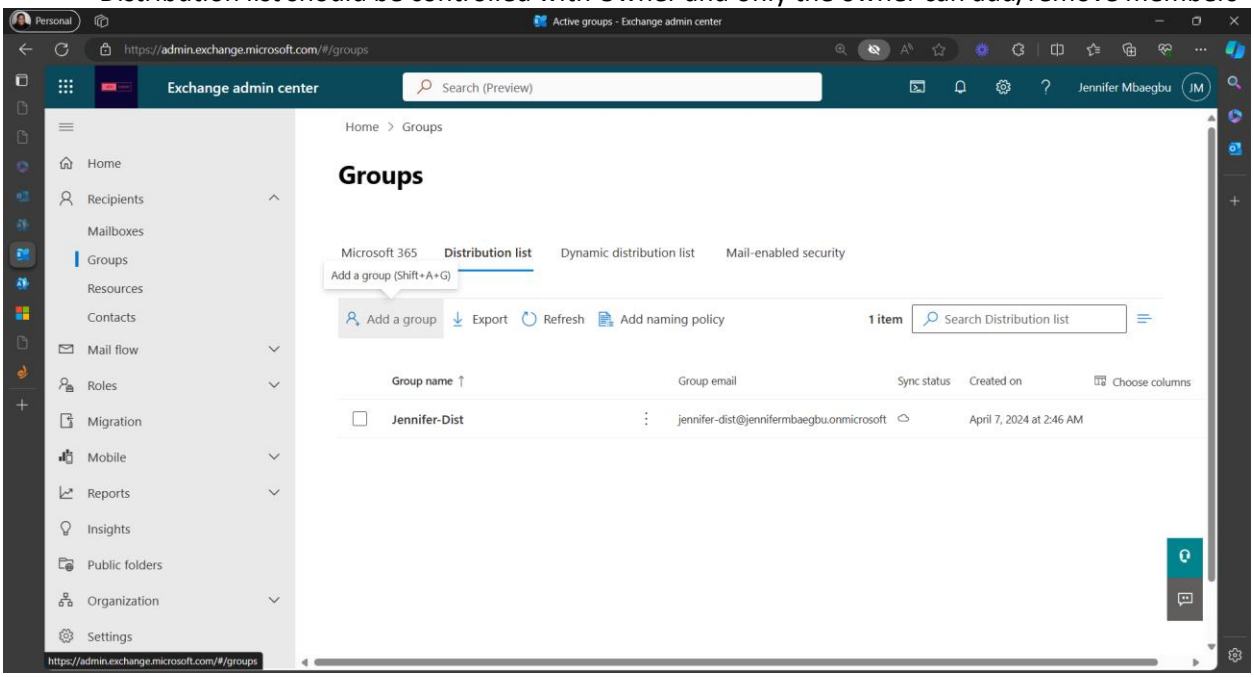


Figure 4: Create Distribution List

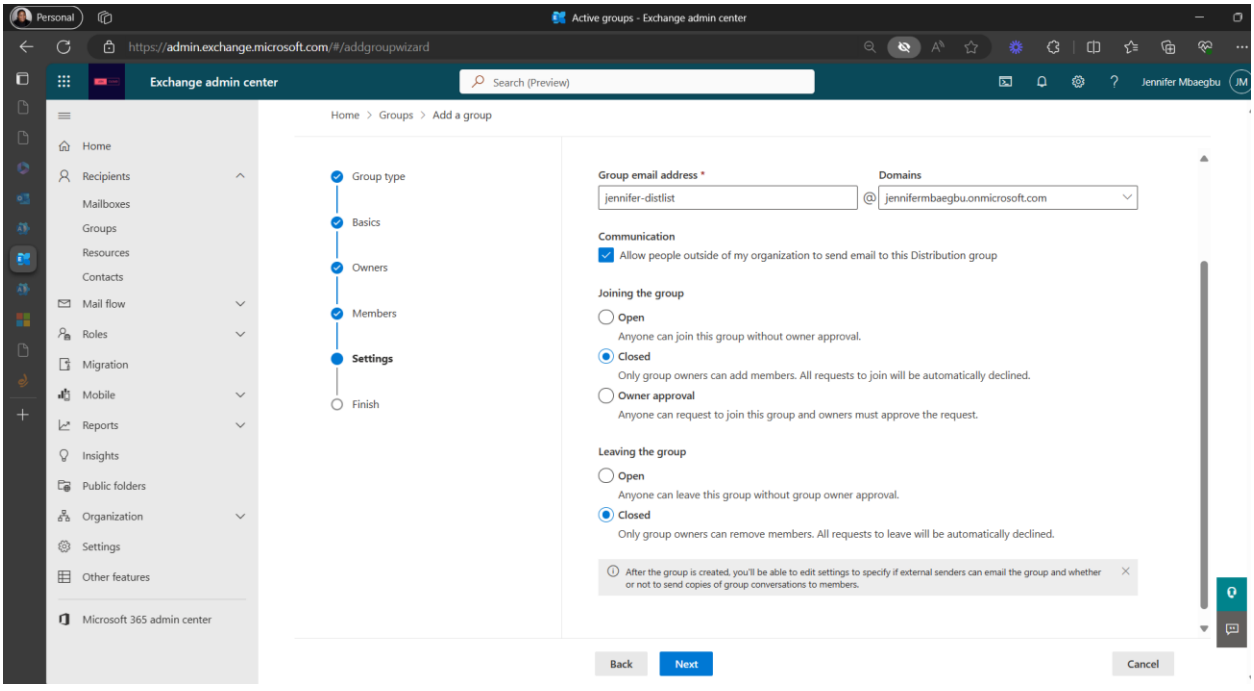
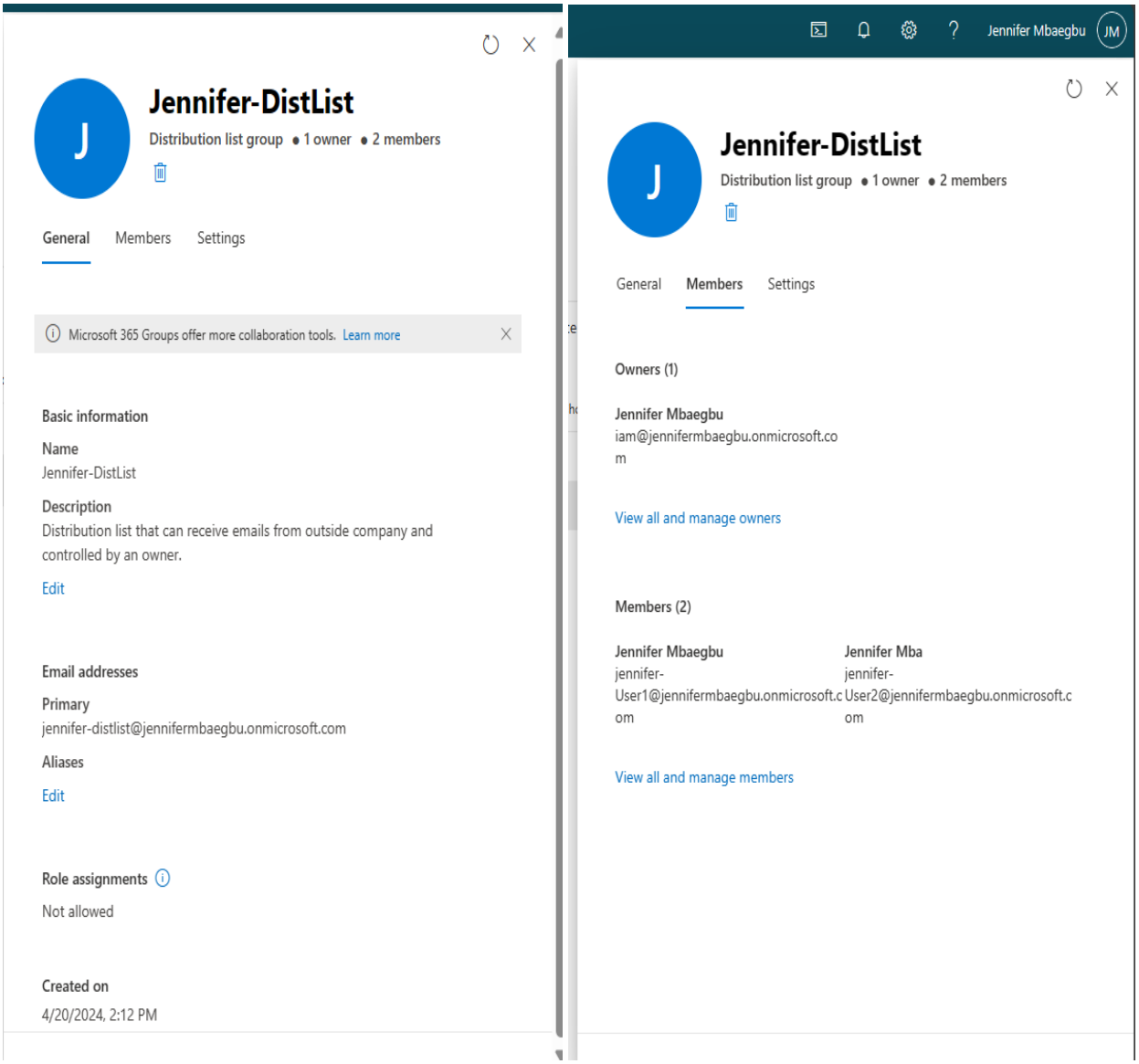
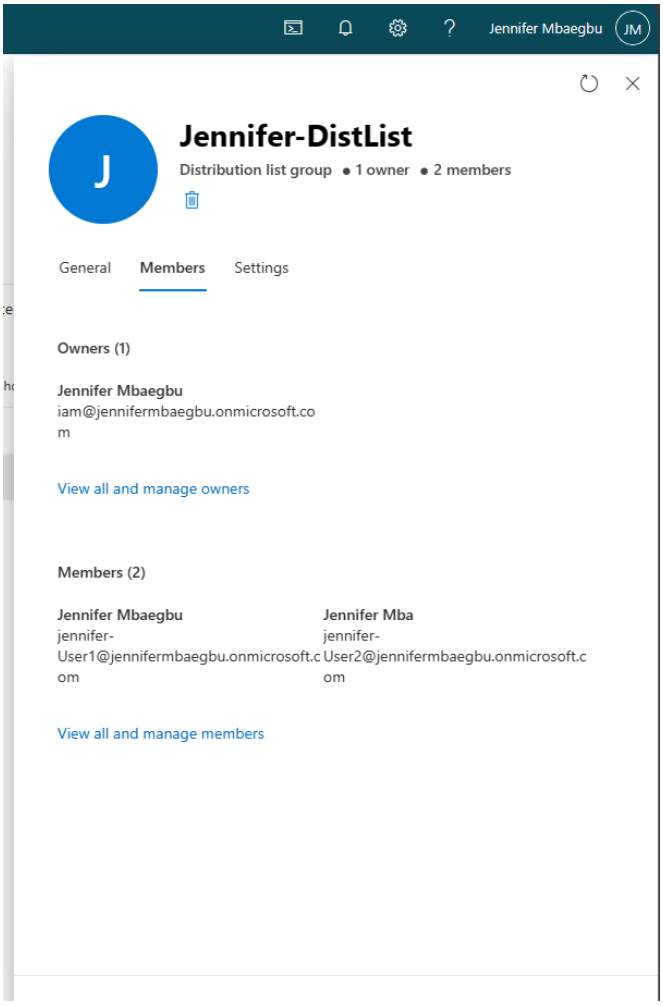


Figure 5: Distribution List can receive emails from external contacts and closed settings -[only owner can add or remove members]

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


Jennifer-DistList
Distribution list group • 1 owner • 2 members
General
Members
Settings
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.
Edit
Email addresses
Primary
jennifer-distlist@jennifermbaegbu.onmicrosoft.com
Aliases
Edit
Role assignments
Not allowed
Created on
4/20/2024, 2:12 PM
Jennifer Mbaegbu
JM
Jennifer-DistList
Distribution list group • 1 owner • 2 members
General
Members
Settings
Owners (1)
Jennifer Mbaegbu
iam@jennifermbaegbu.onmicrosoft.com
View all and manage owners
Members (2)
Jennifer Mbaegbu
jennifer-User1@jennifermbaegbu.onmicrosoft.com
Jennifer Mba
jennifer-User2@jennifermbaegbu.onmicrosoft.com
View all and manage members



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

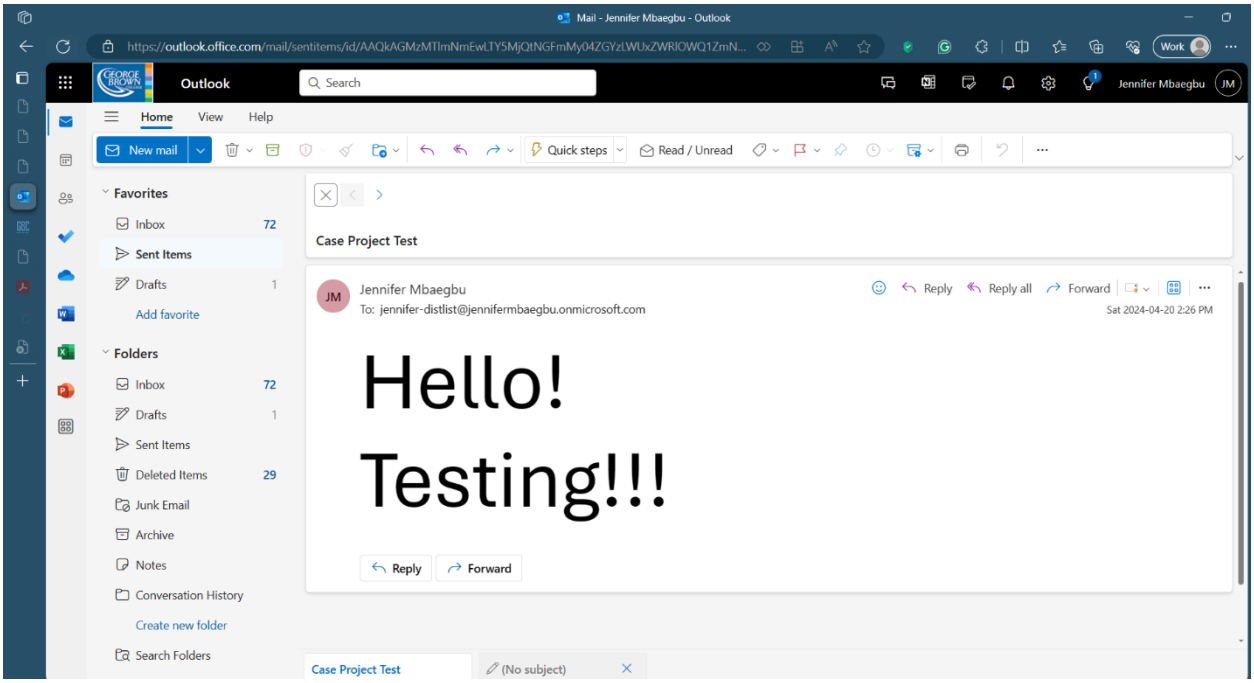


Figure 6: Test Email sent via GBC email

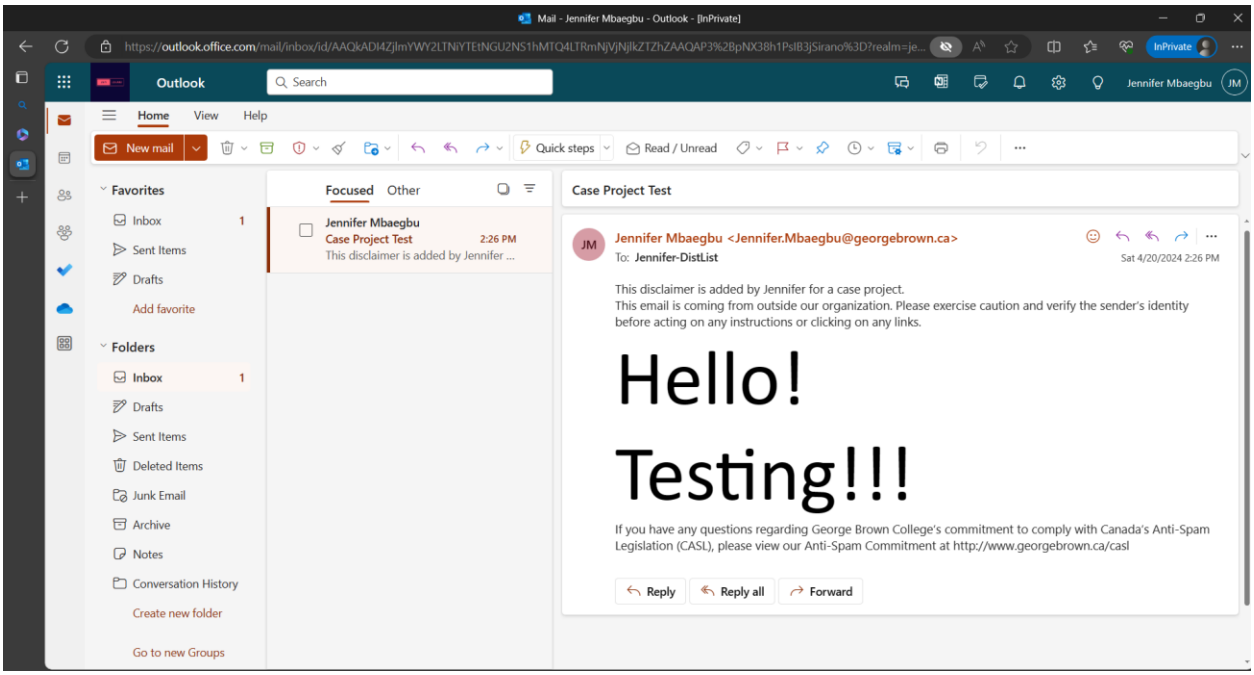


Figure 7: Email received via jennifer-User1@domain.com

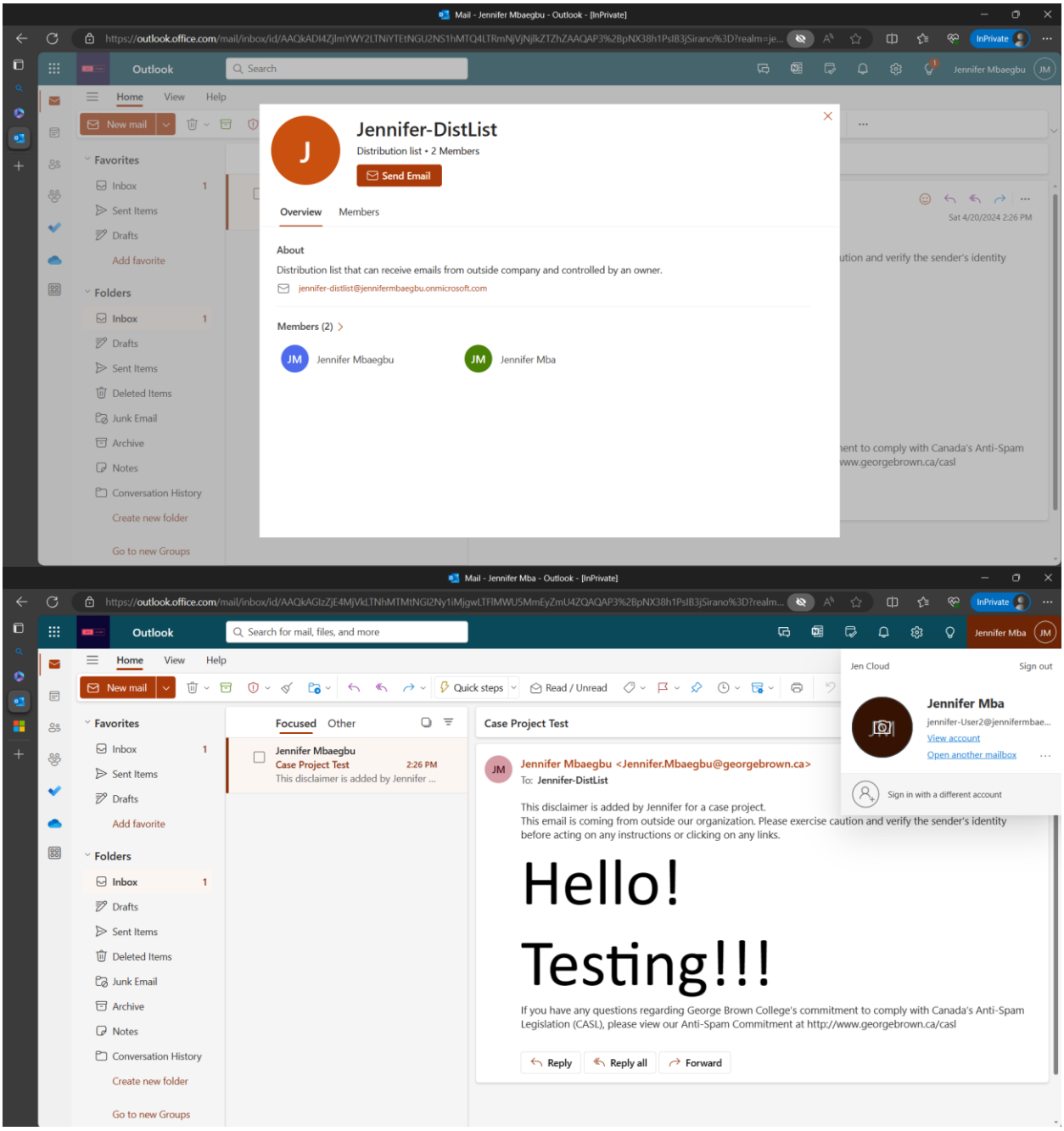


Figure 8: Email received via second User's email

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

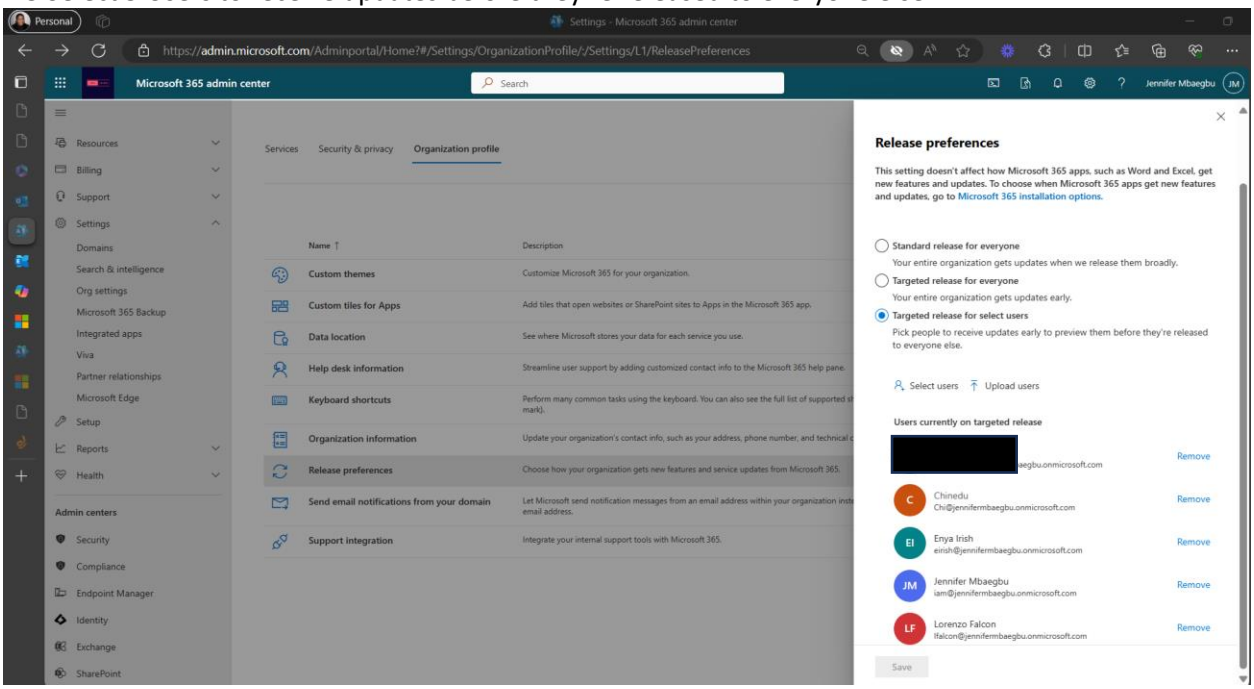


Figure 9: Target Release Prefrence

1.6 Add this disclaimer to your emails "This disclaimer is added by yourname for case project"

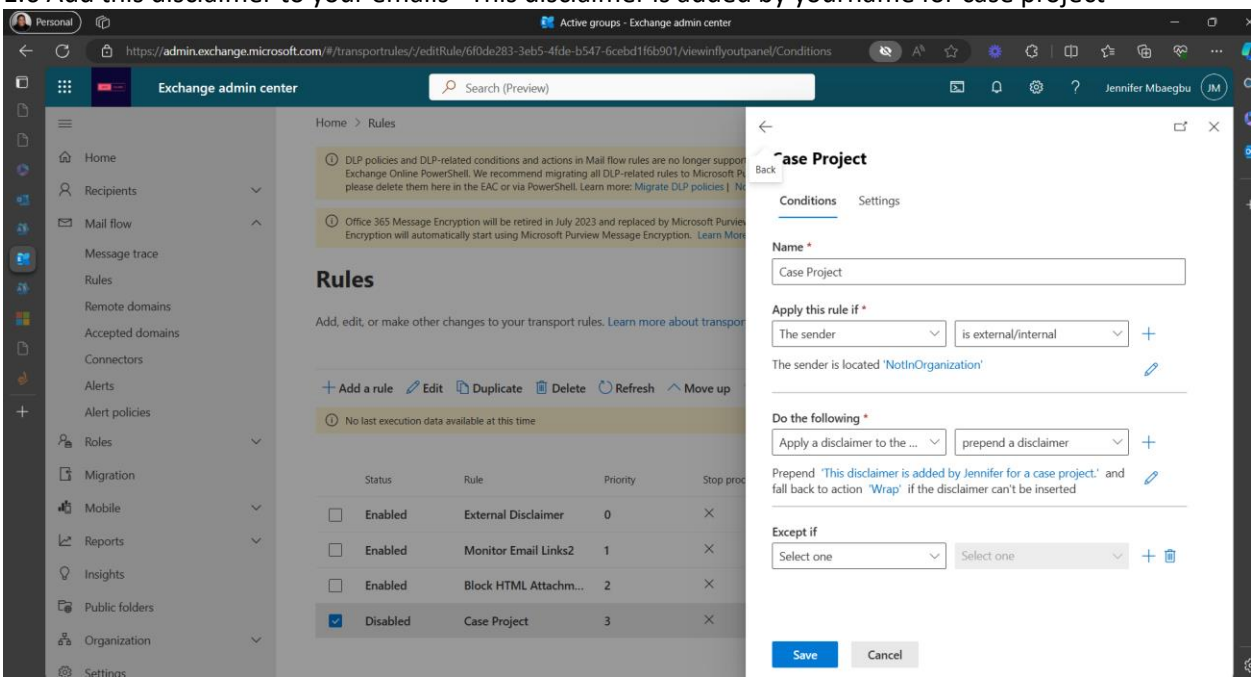


Figure 10: Case-Project-Disclaimer created

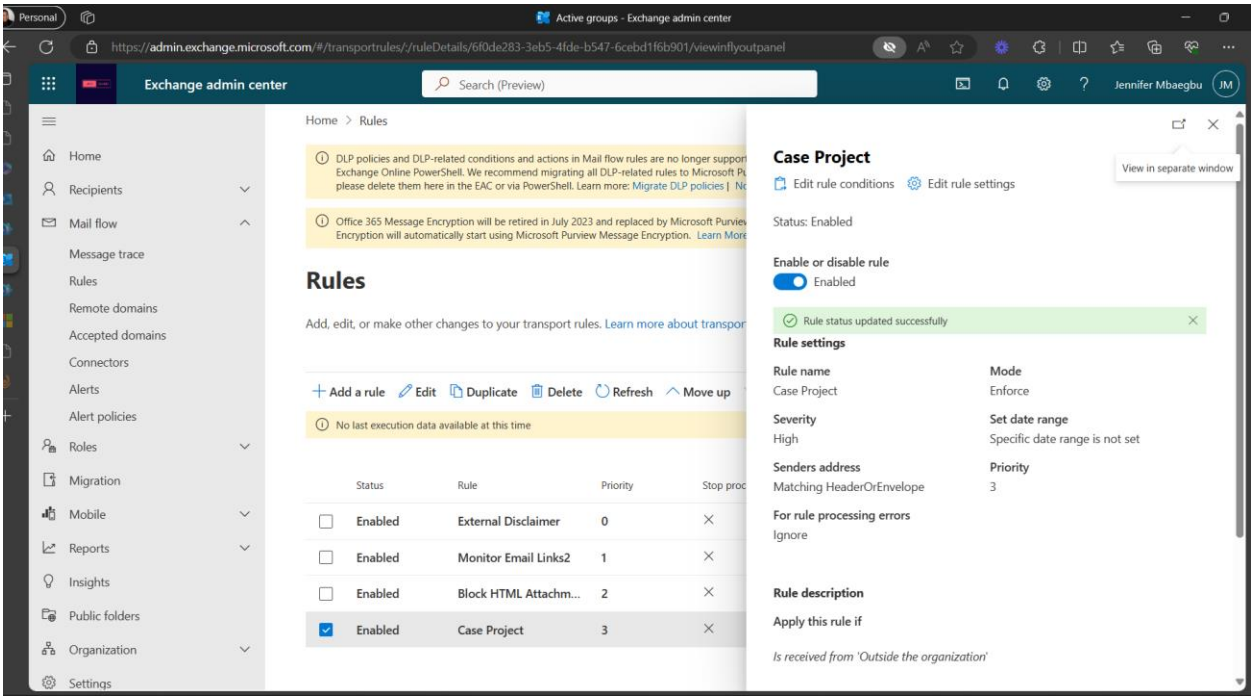


Figure 11Case-Project-Disclaimer Enabled

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

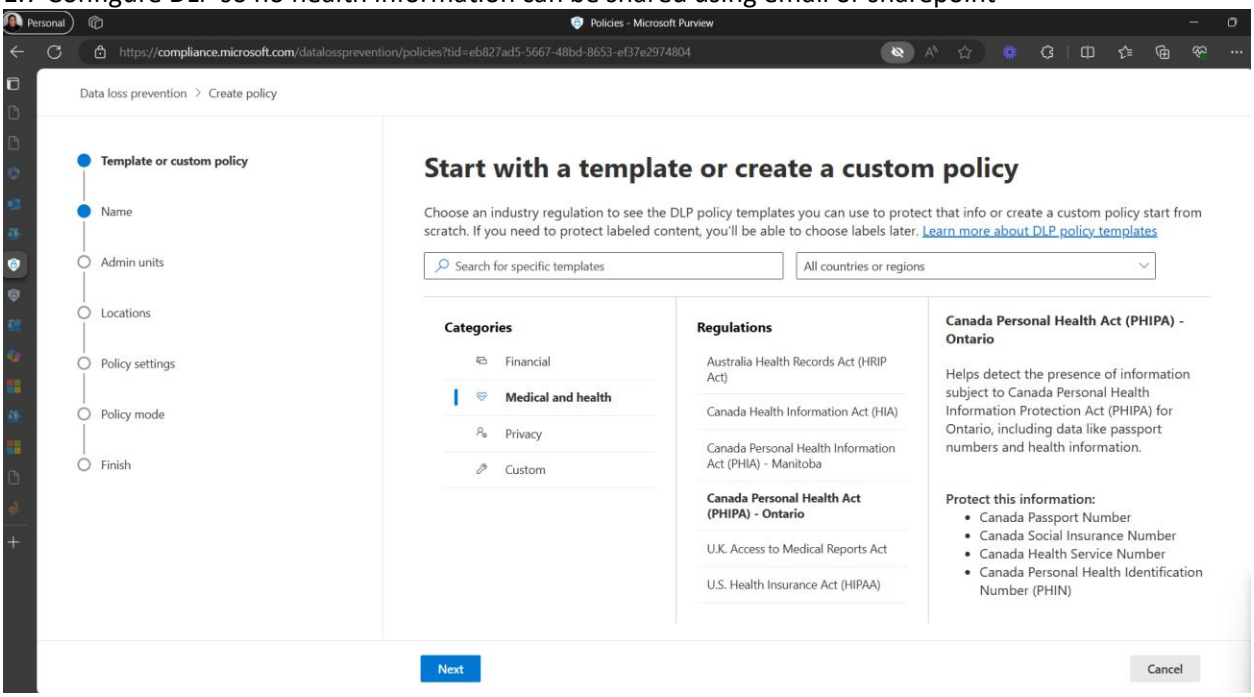


Figure 12: Create DLP to stop users from sharing health information

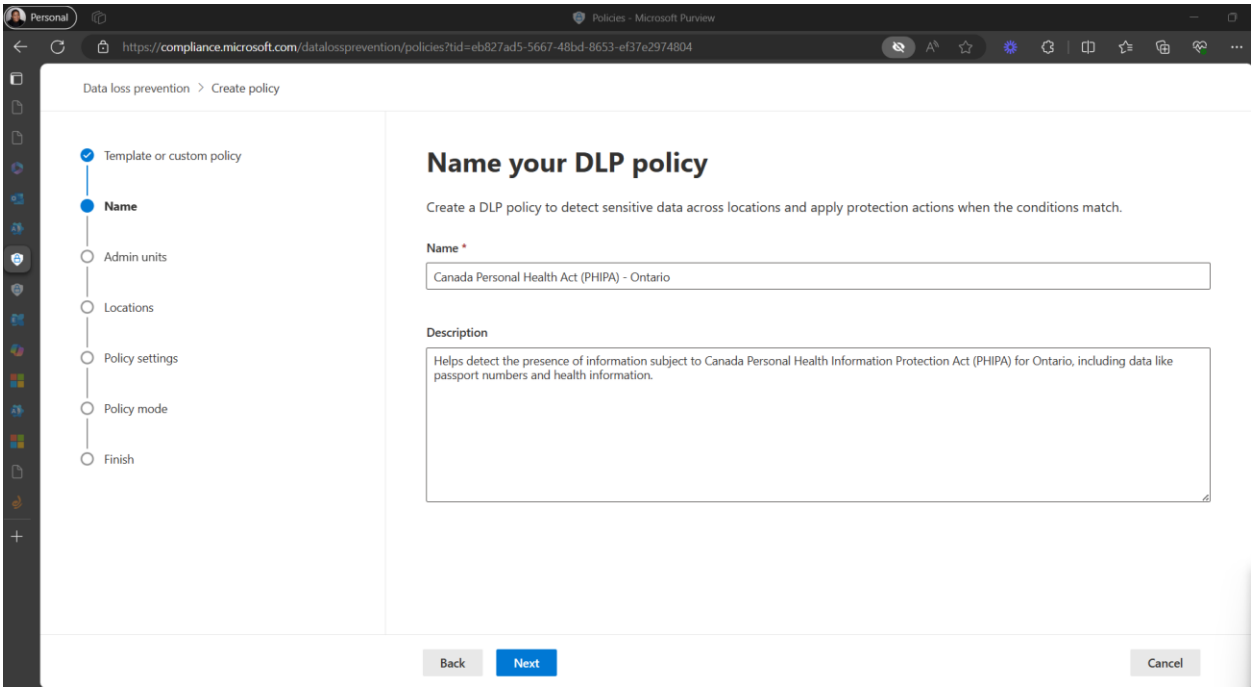


Figure 13: Name Data Loss Prevention Policy

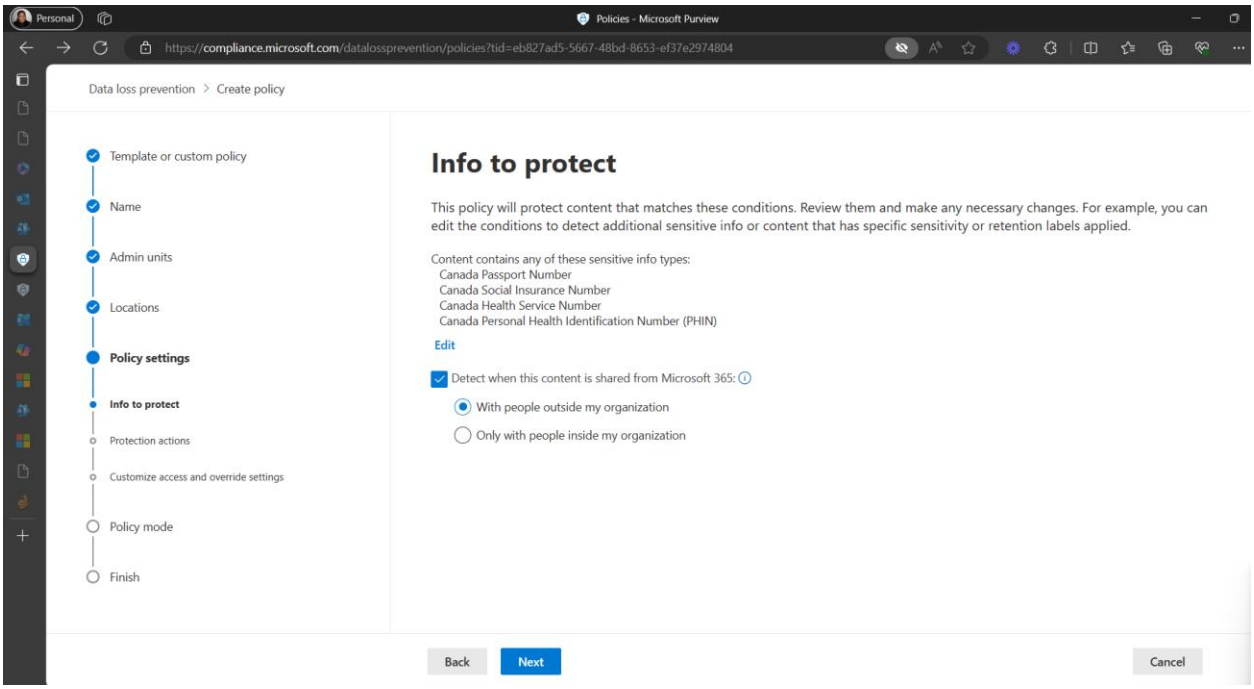


Figure 14: Information to protect

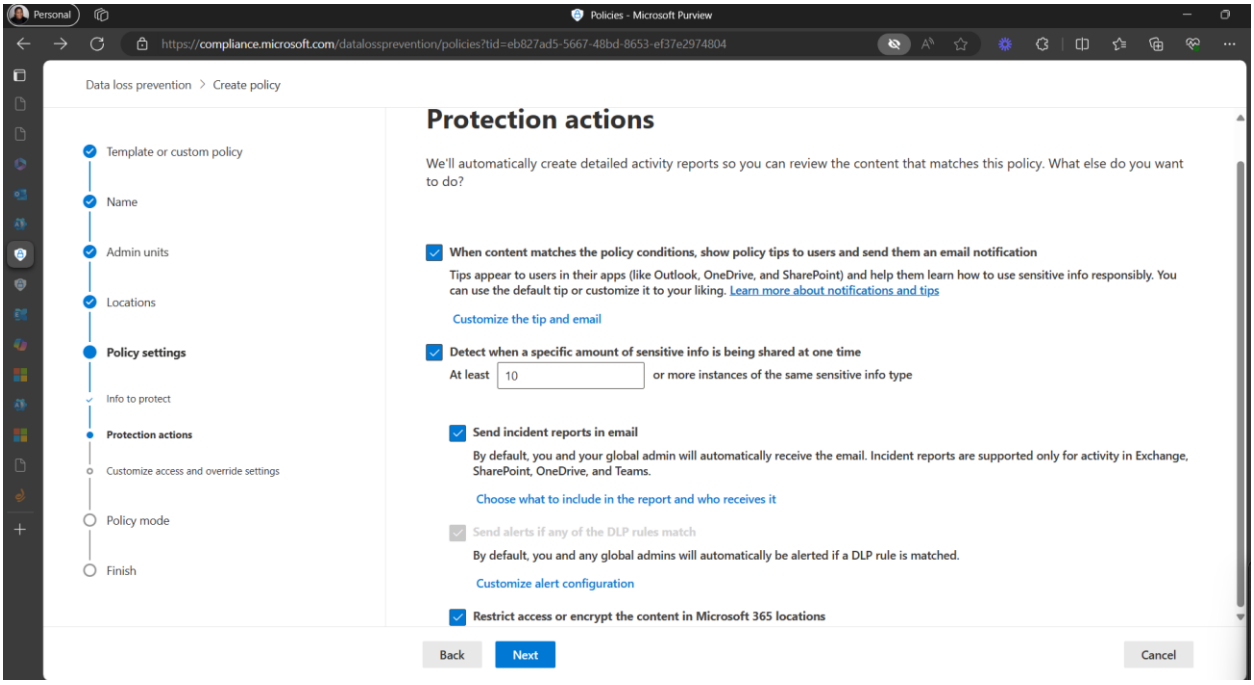


Figure 15: Actions to take

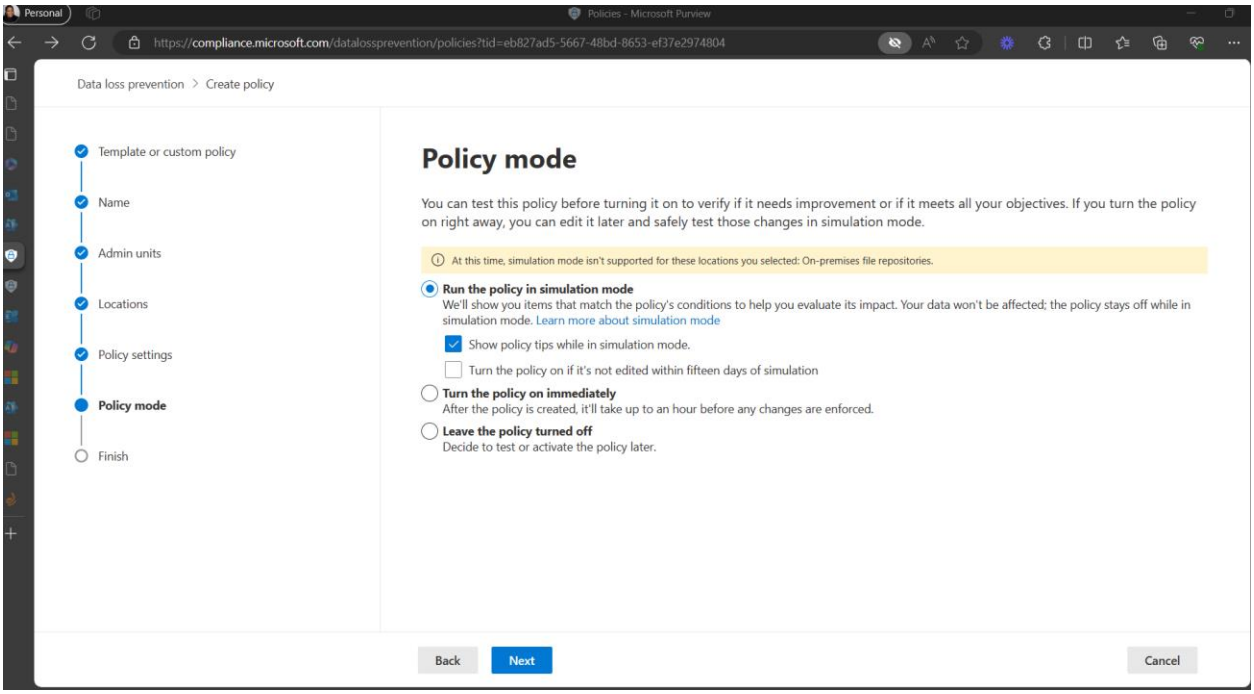


Figure 16: Simulation mode

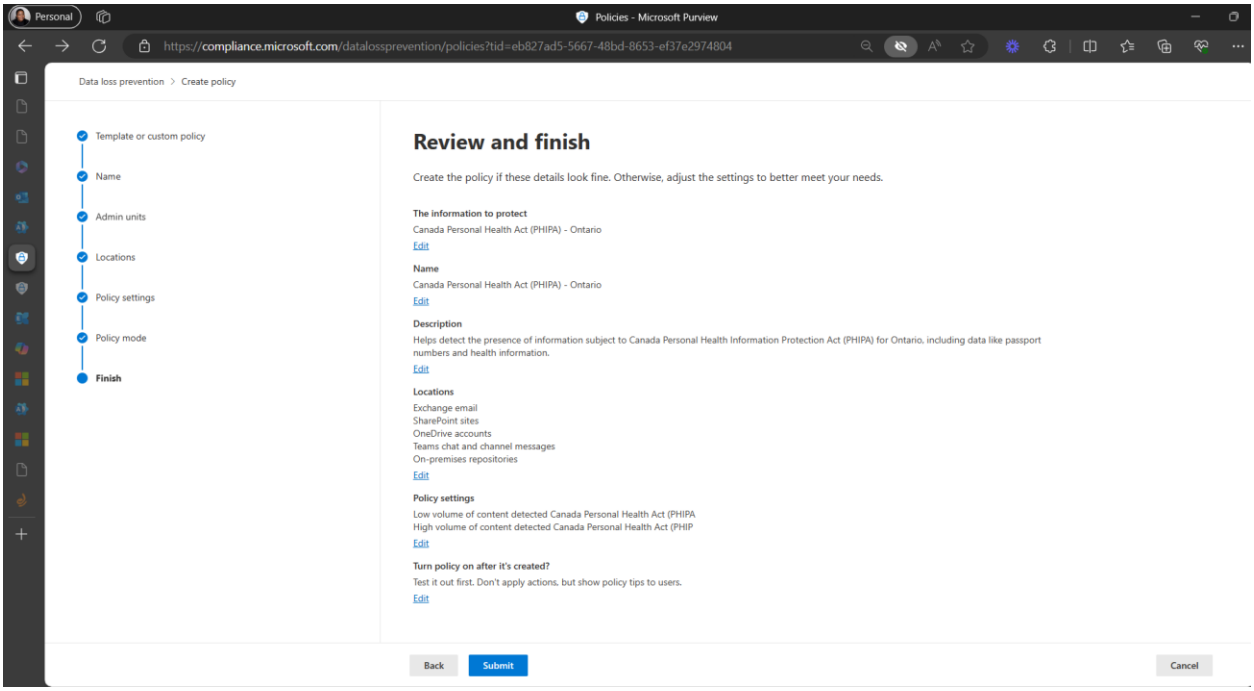


Figure 17: Review

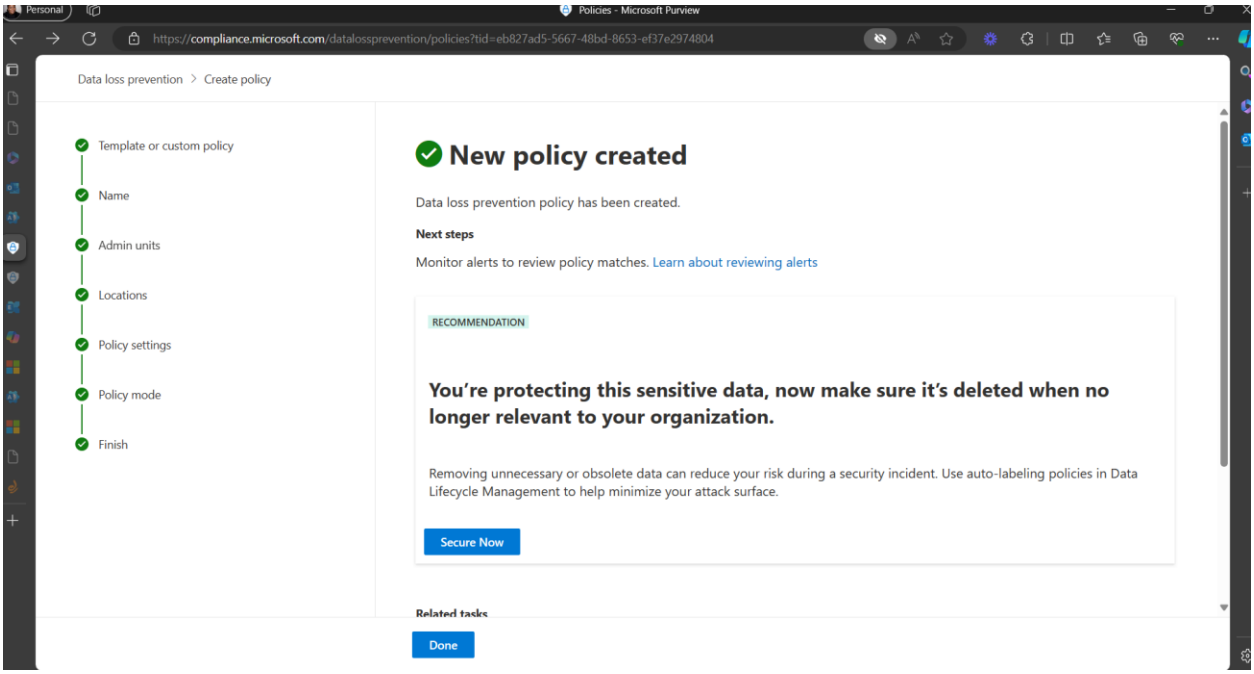
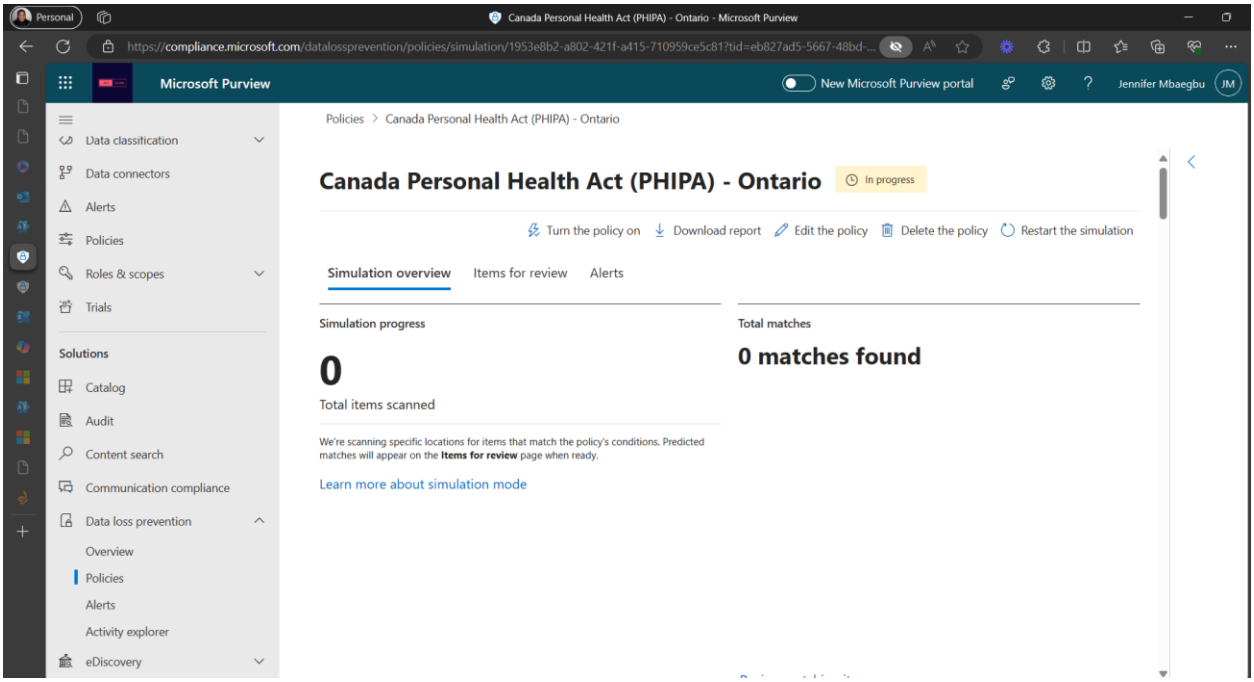
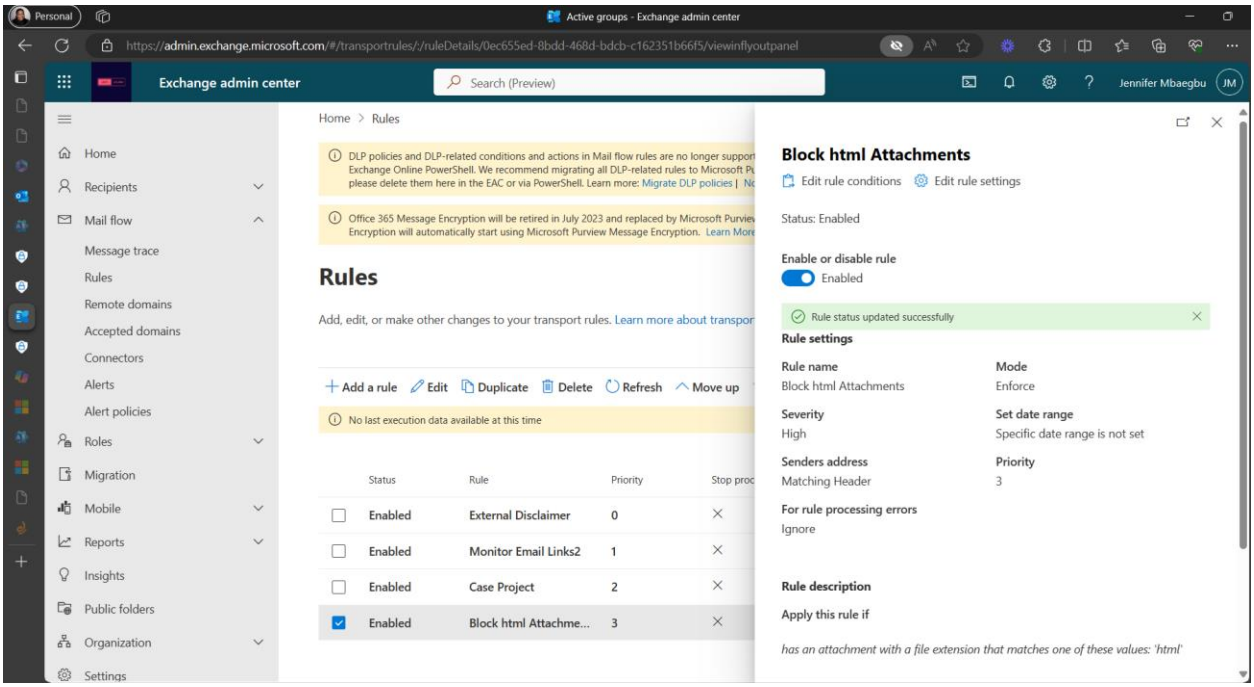


Figure 18: New policy left in simulation mode



1.8 Block emails with .html attachments



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

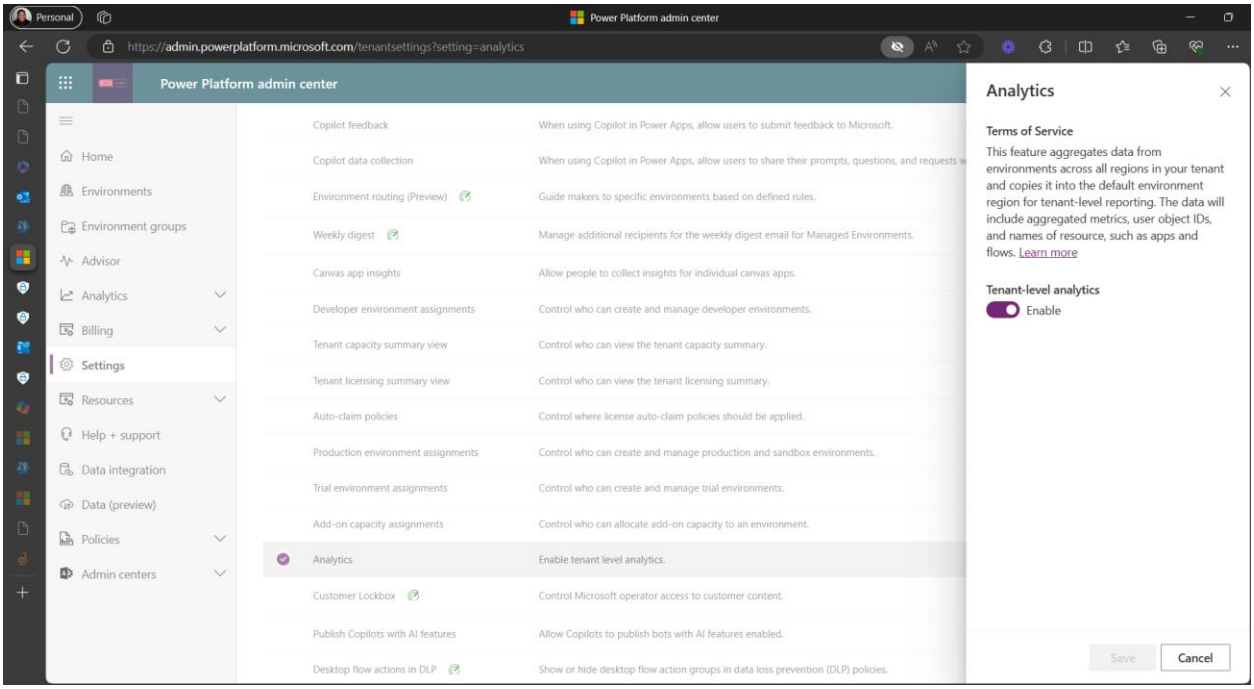


Figure 19: Enable Tenant Analytics Level

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

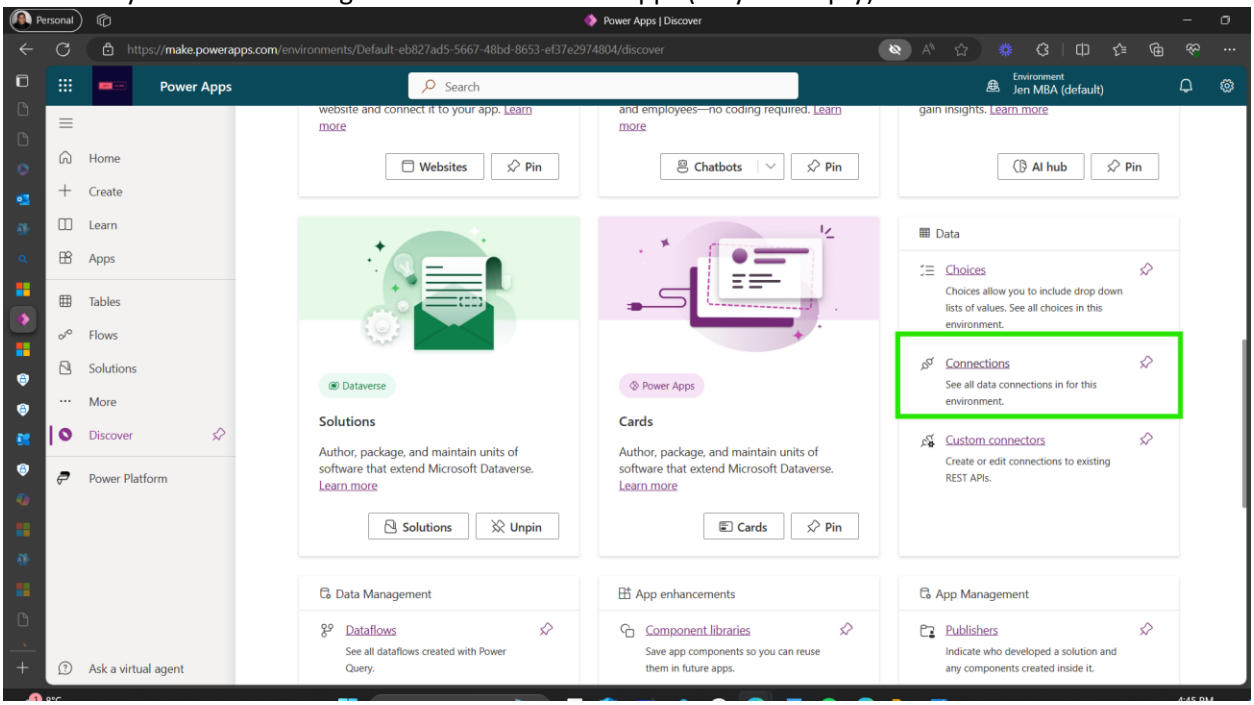


Figure 20: Navigate Data to Connections

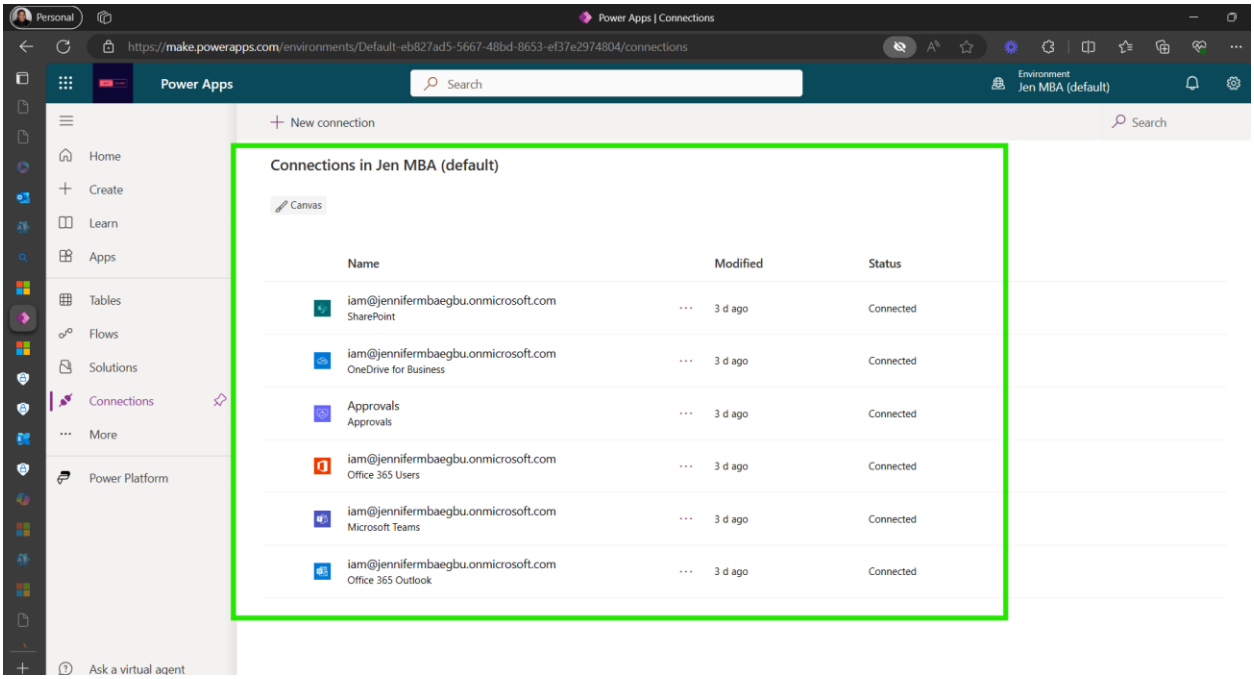
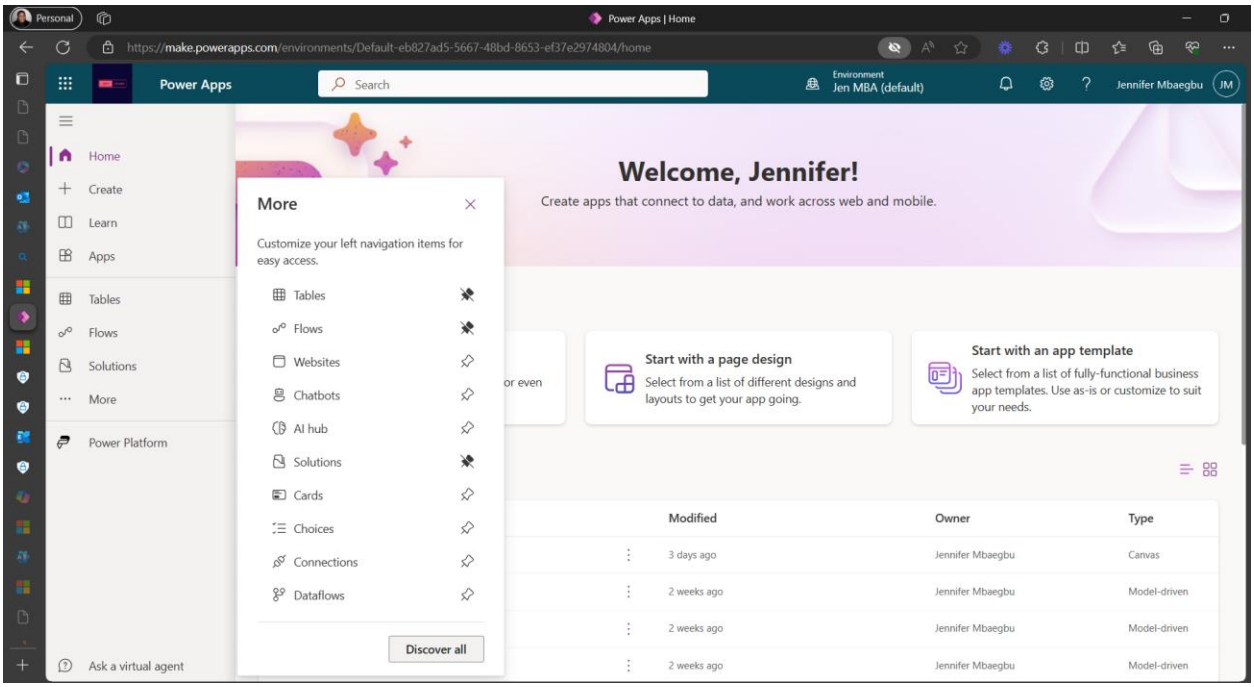
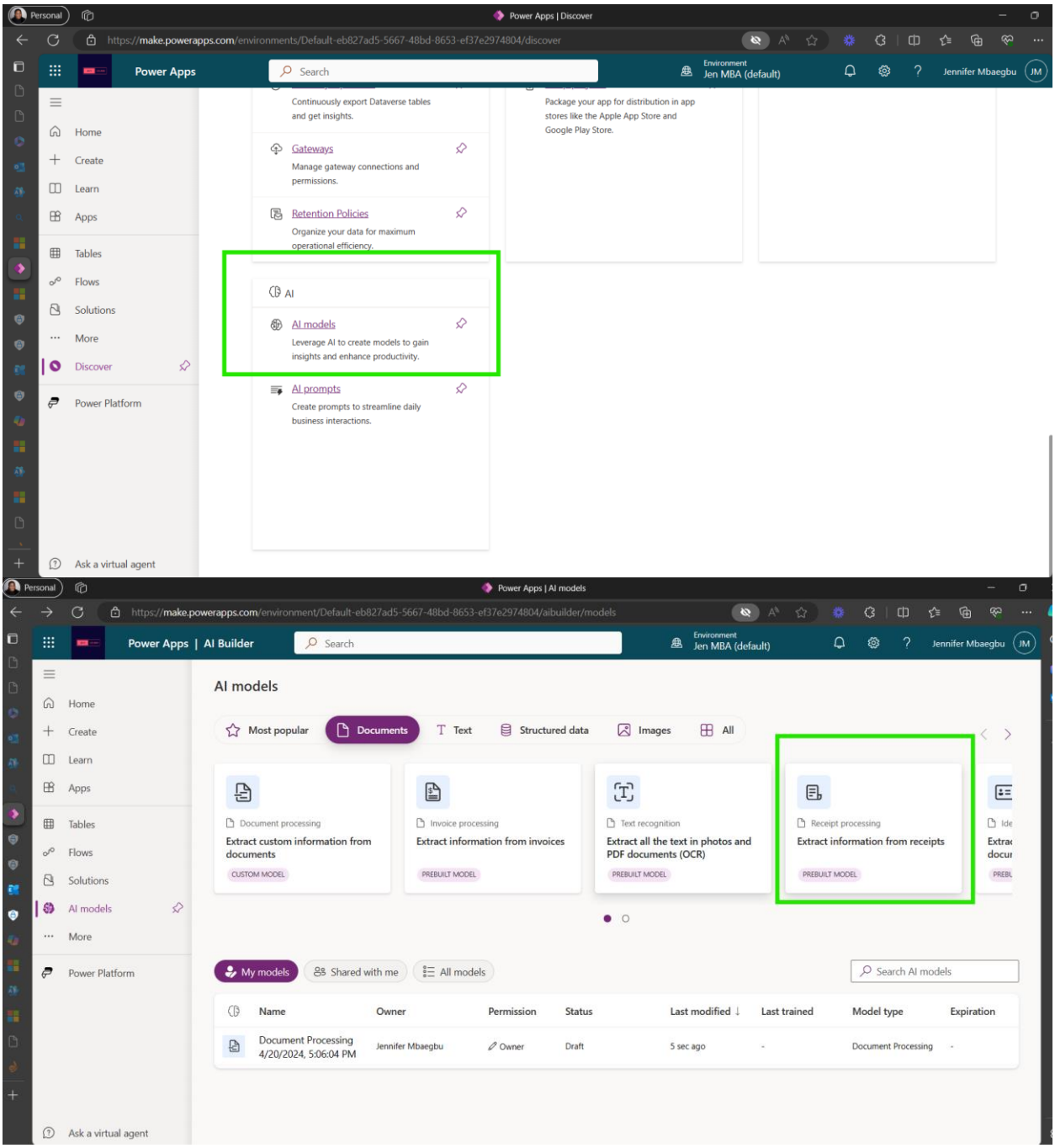
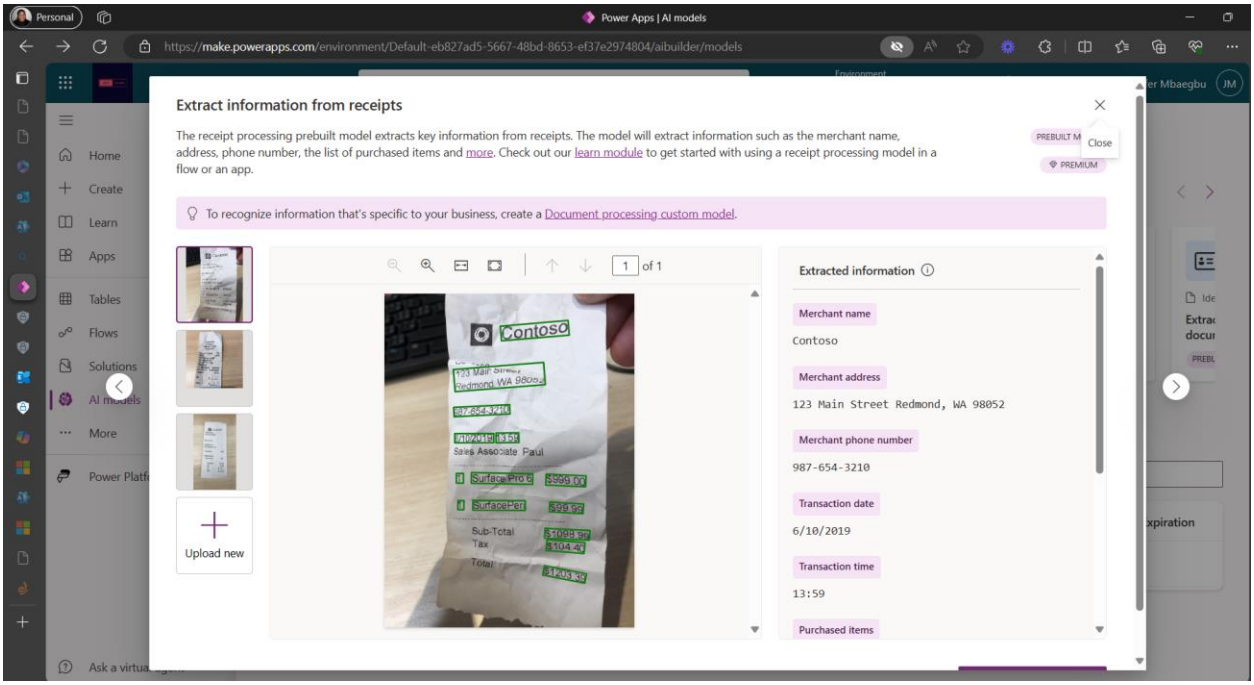


Figure 21: Connections

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.**




Power Apps | Discover
https://make.powerapps.com/environments/Default-eb827ad5-5667-48bd-8653-ef37e2974804/discover
Power Apps
Search
Environment
Jen MBA (default)
Jennifer Mbaegbu
Home
Create
Learn
Apps
Tables
Flows
Solutions
More
Discover
Power Platform
Ask a virtual agent
Continuously export Dataverse tables and get insights.
Package your app for distribution in app stores like the Apple App Store and Google Play Store.
Gateways
Manage gateway connections and permissions.
Retention Policies
Organize your data for maximum operational efficiency.
AI
AI models
Leverage AI to create models to gain insights and enhance productivity.
AI prompts
Create prompts to streamline daily business interactions.
Power Apps | AI models
https://make.powerapps.com/environment/Default-eb827ad5-5667-48bd-8653-ef37e2974804/aibuilder/models
Power Apps | AI Builder
AI models
Most popular
Documents
Text
Structured data
Images
All
Document processing
Extract custom information from documents
CUSTOM MODEL
Invoice processing
Extract information from invoices
PREBUILT MODEL
Text recognition
Extract all the text in photos and PDF documents (OCR)
PREBUILT MODEL
Receipt processing
Extract information from receipts
PREBUILT MODEL
My models
Shared with me
All models
Search AI models
Name
Owner
Permission
Status
Last modified
Last trained
Model type
Expiration
Document Processing 4/20/2024, 5:06:04 PM
Jennifer Mbaegbu
Owner
Draft
5 sec ago
Document Processing


Power Apps | AI models
https://make.powerapps.com/environment/Default-eb827ad5-5667-48bd-8653-ef37e2974804/aibuilder/models
Extract information from receipts
The receipt processing prebuilt model extracts key information from receipts. The model will extract information such as the merchant name, address, phone number, the list of purchased items and more. Check out our learn module to get started with using a receipt processing model in a flow or an app.
Close
PREMIUM
To recognize information that's specific to your business, create a Document processing custom model.
Upload new
1 of 1
Contoso
Extracted information
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
Home
Create
Learn
Apps
Tables
Flows
Solutions
AI models
More

Task 3: MFA

3.1 Enable Multi Factor Authentication

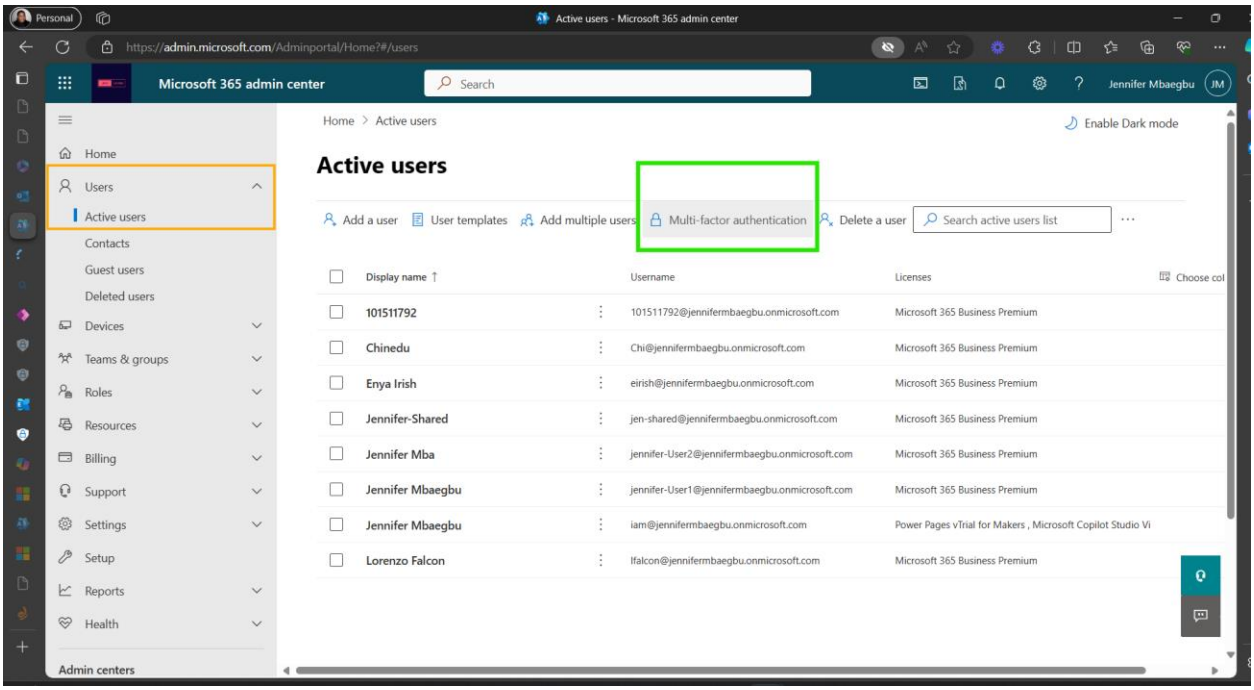
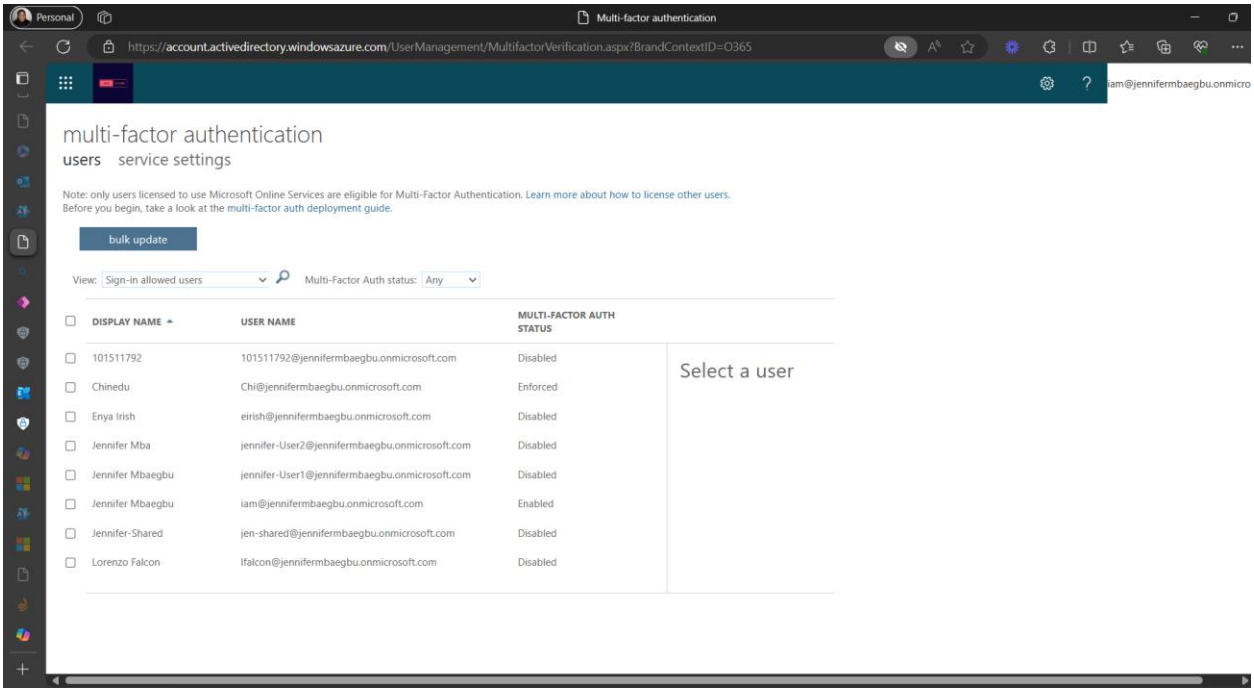
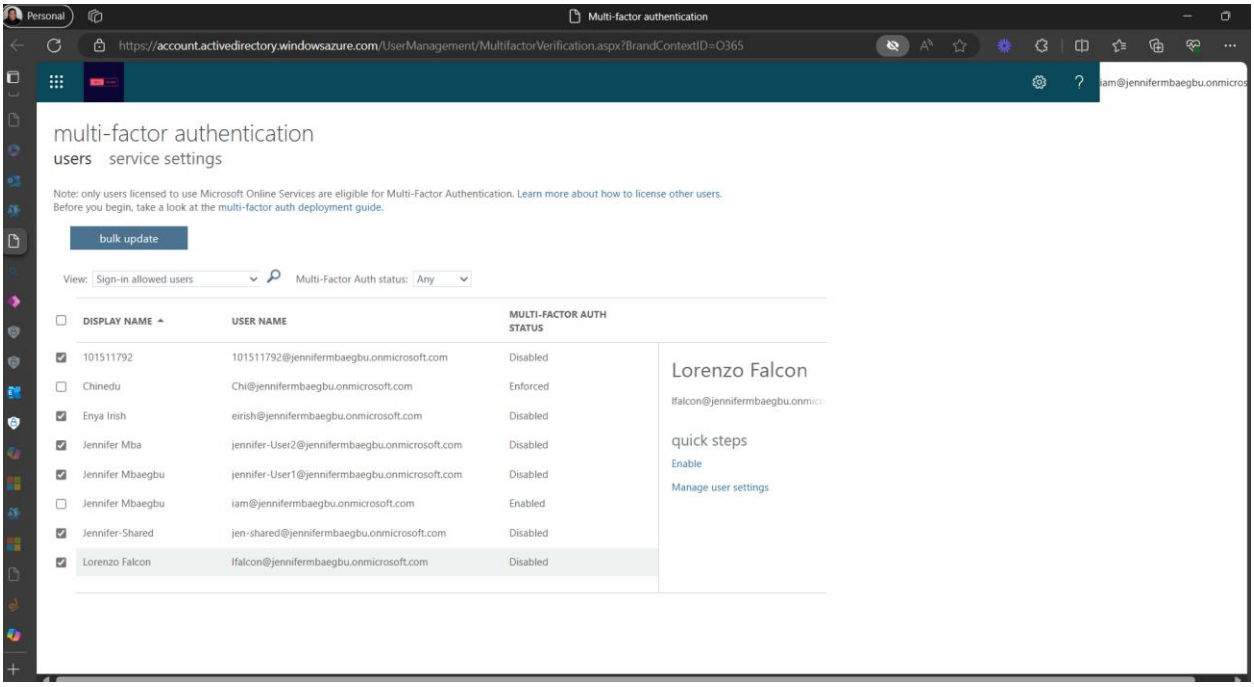
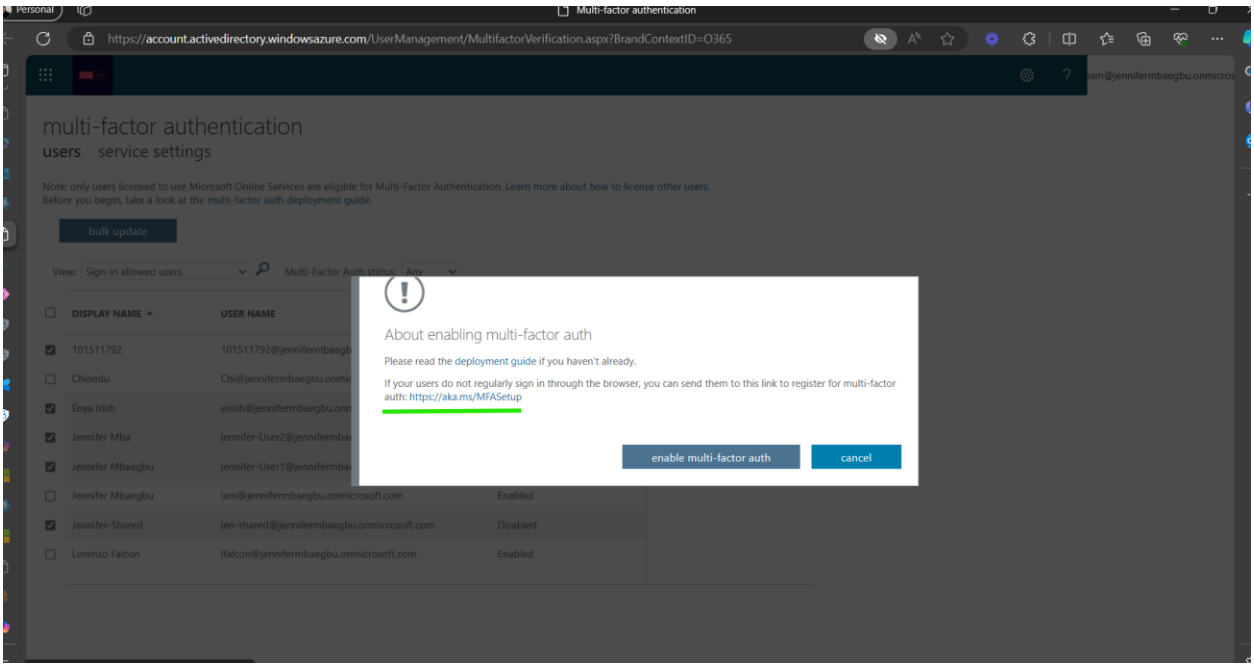
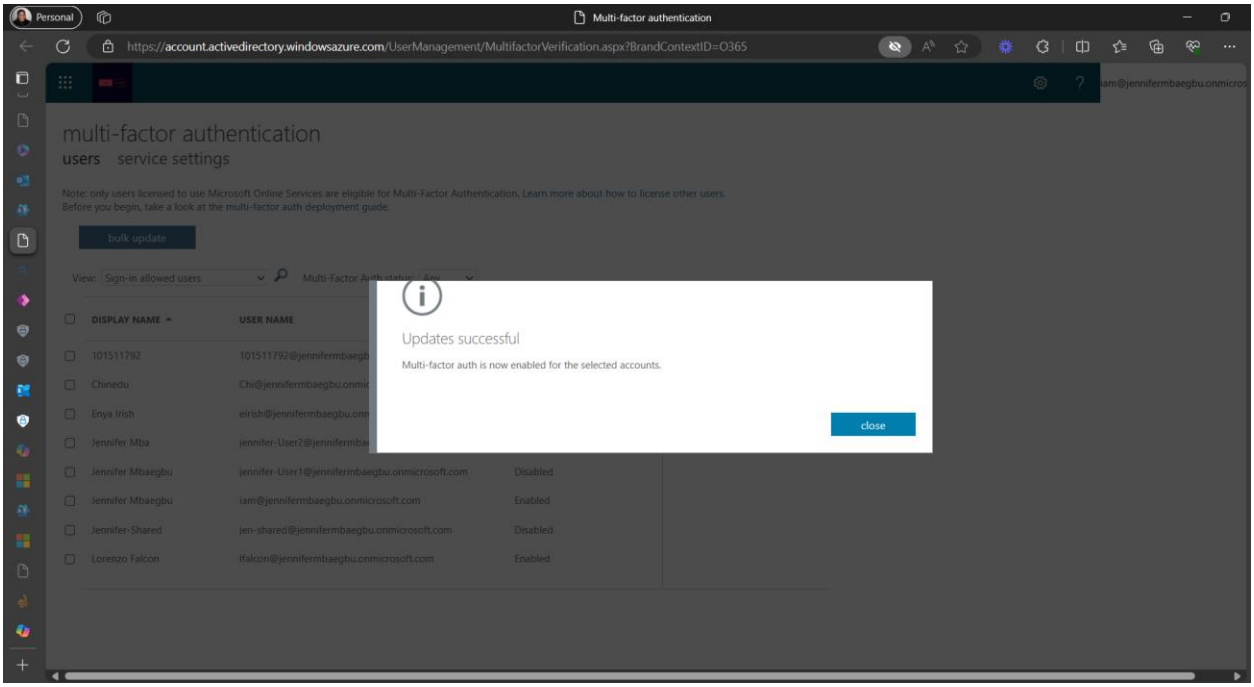


Figure 22: Launch MFA from Microsoft 365 Admin Center - Users - Active Users

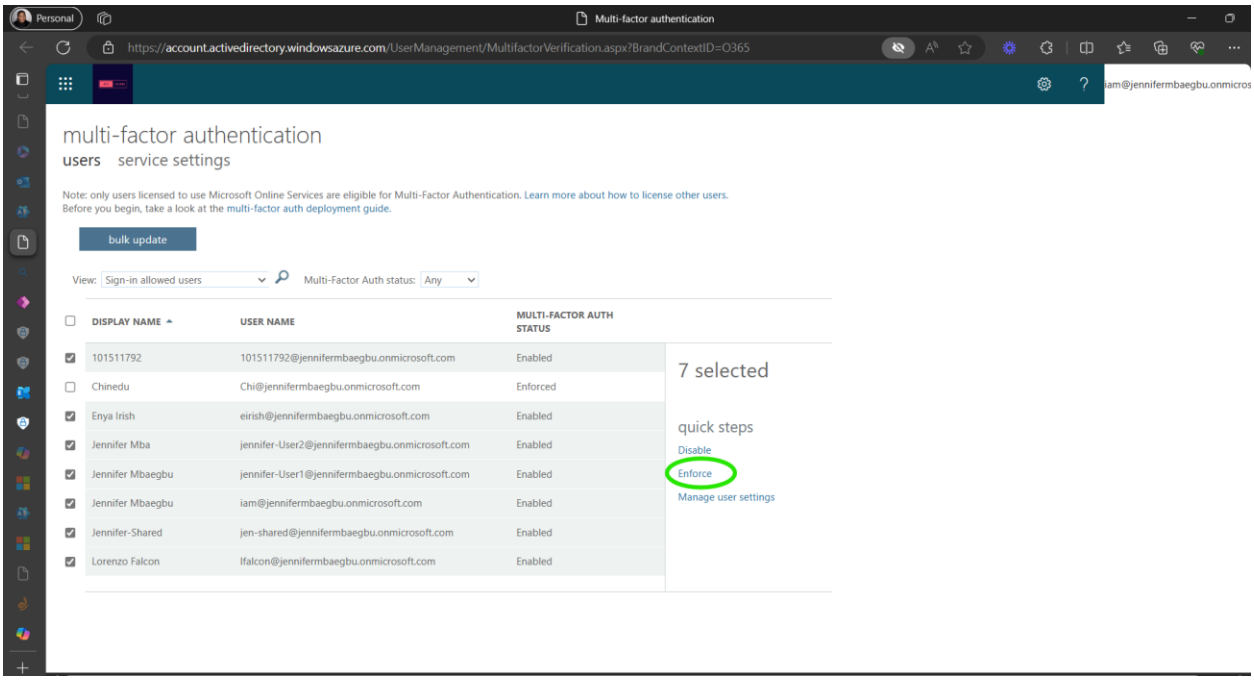



Personal
Multi-factor authentication
https://account.activedirectory.windowsazure.com/UserManagement/MultifactorVerification.aspx?BrandContextID=O365
multi-factor authentication
users service settings
Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. Learn more about how to license other users.
Before you begin, take a look at the multi-factor auth deployment guide.
bulk update
View: Sign-in allowed users
Multi-Factor Auth status: Any
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
Lorenzo Falcon
quick steps
Enable
Manage user settings


Multi-factor authentication
https://account.activedirectory.windowsazure.com/UserManagement/MultifactorVerification.aspx?BrandContextID=O365
multi-factor authentication
users service settings
bulk update
About enabling multi-factor auth
Please read the deployment guide if you haven't already.
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
enable multi-factor auth
cancel



3.2 Enforce MFA



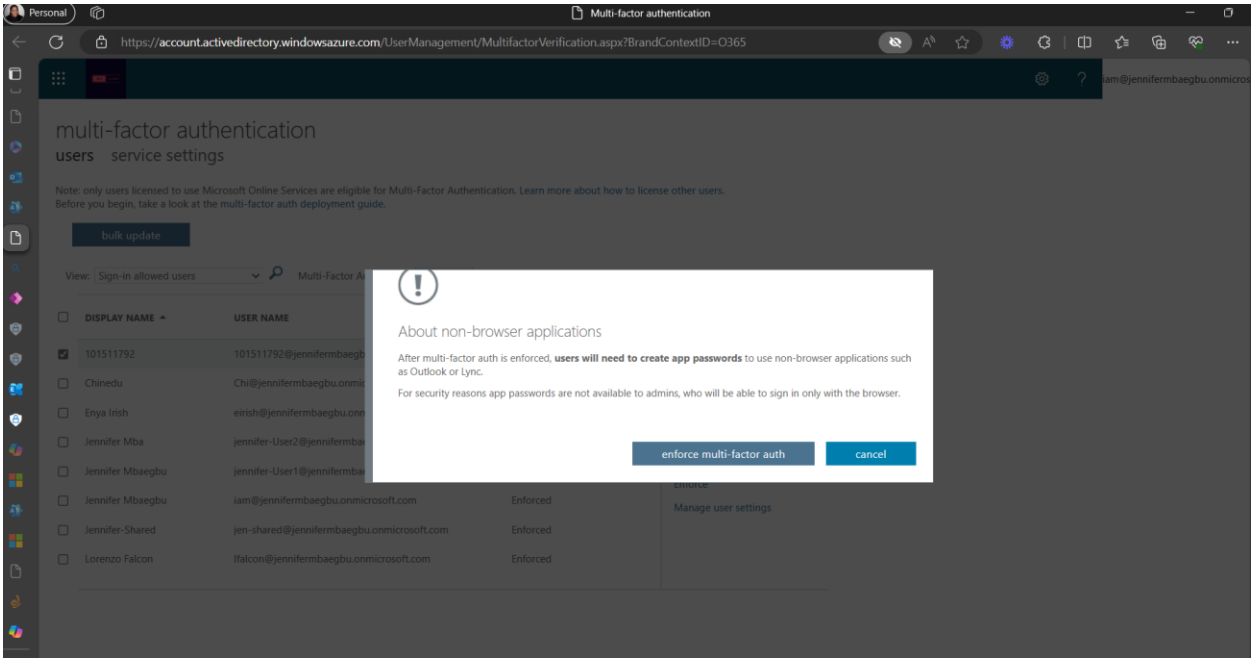


Figure 23: Enforce Multi-factor Authentication

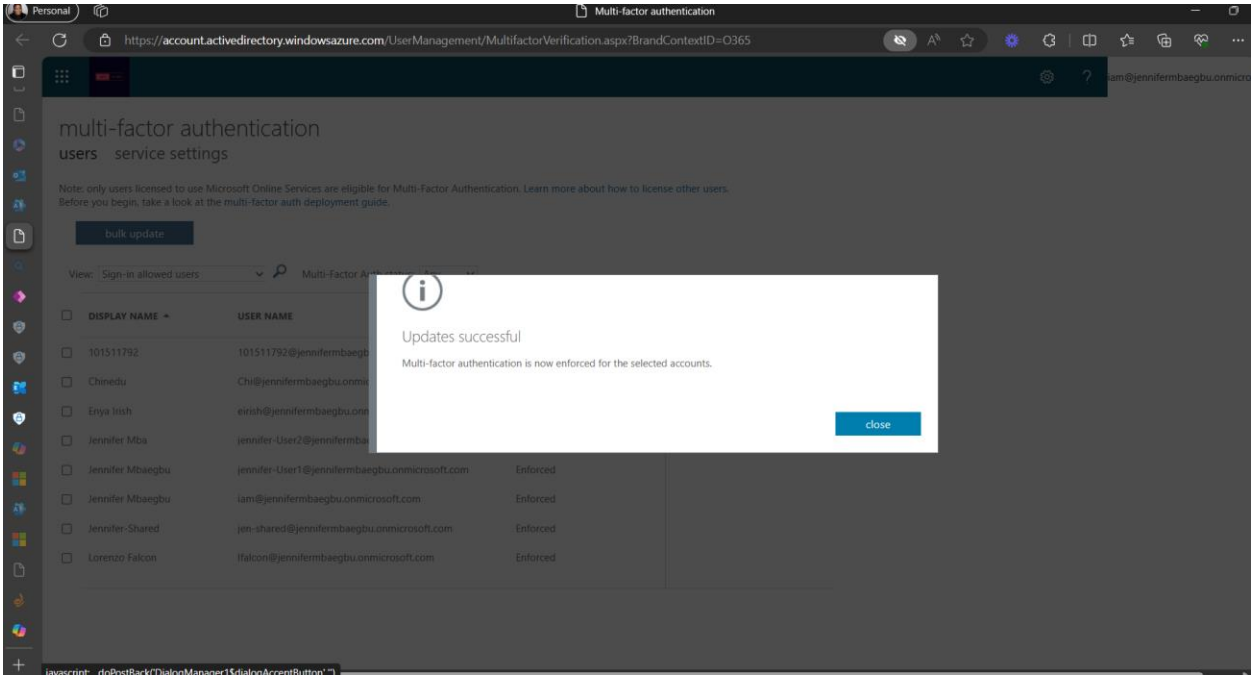
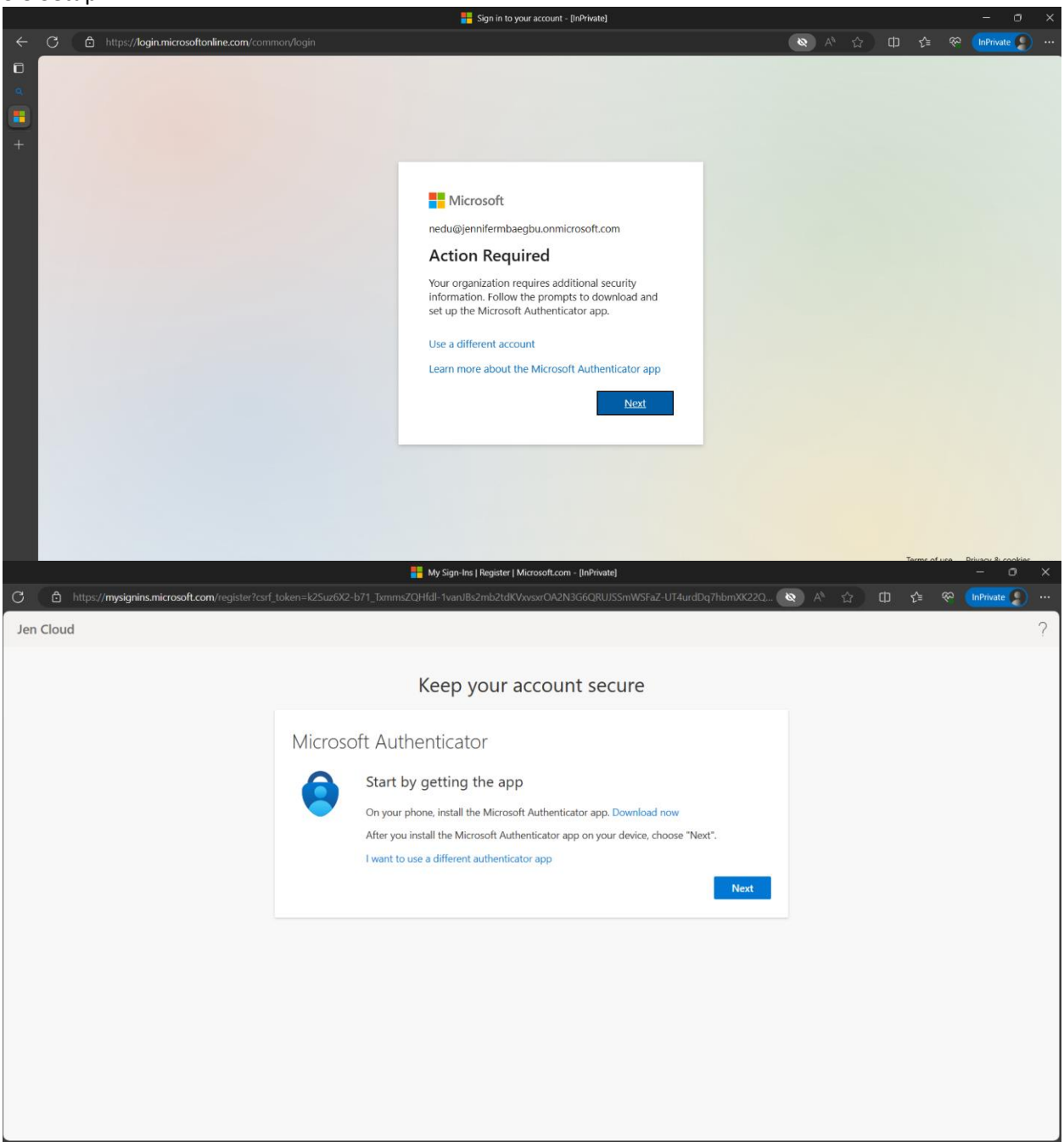
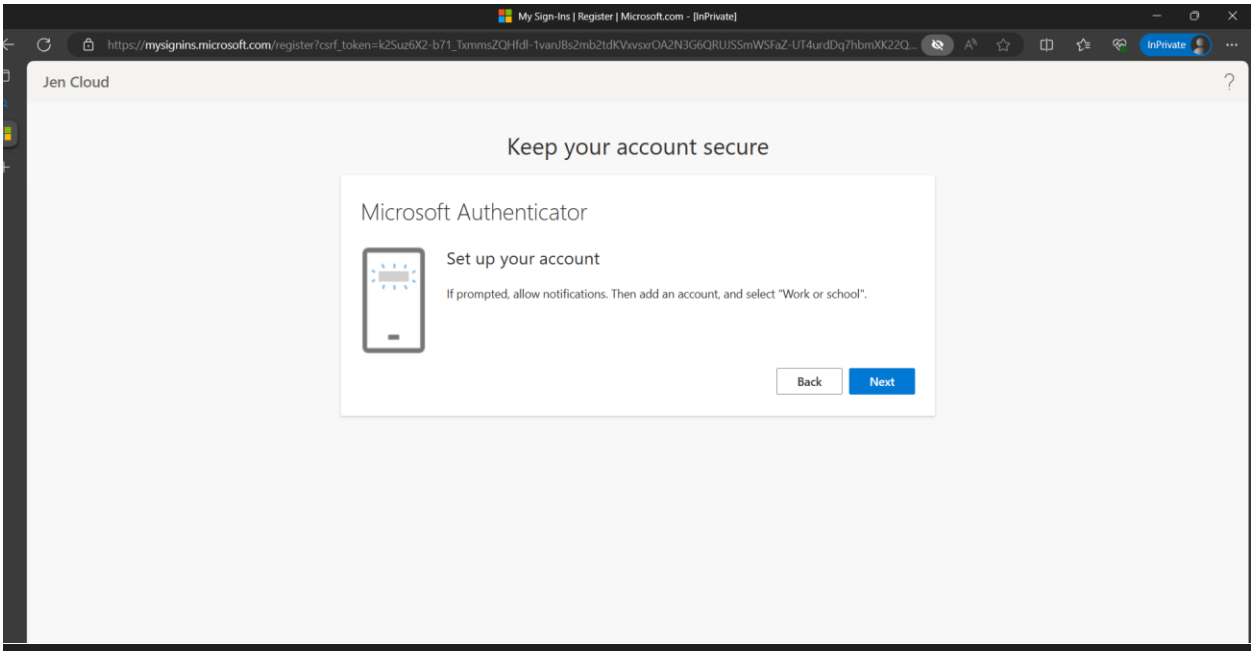
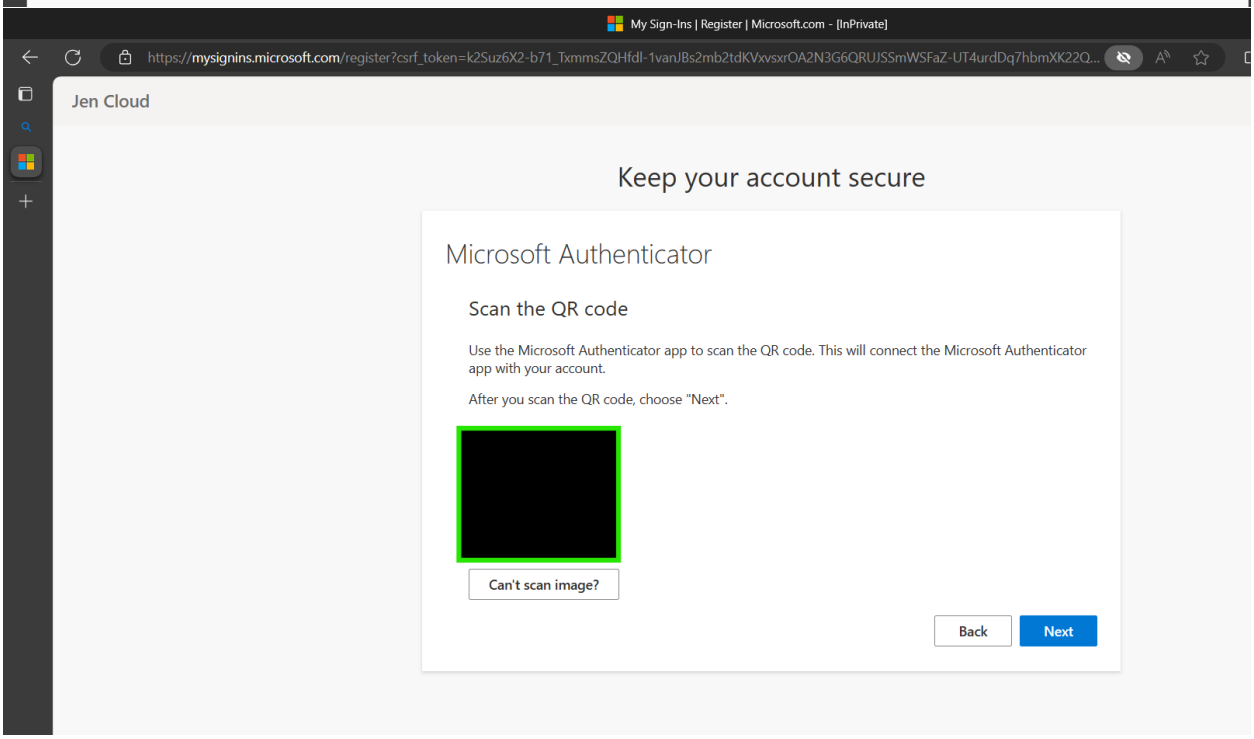


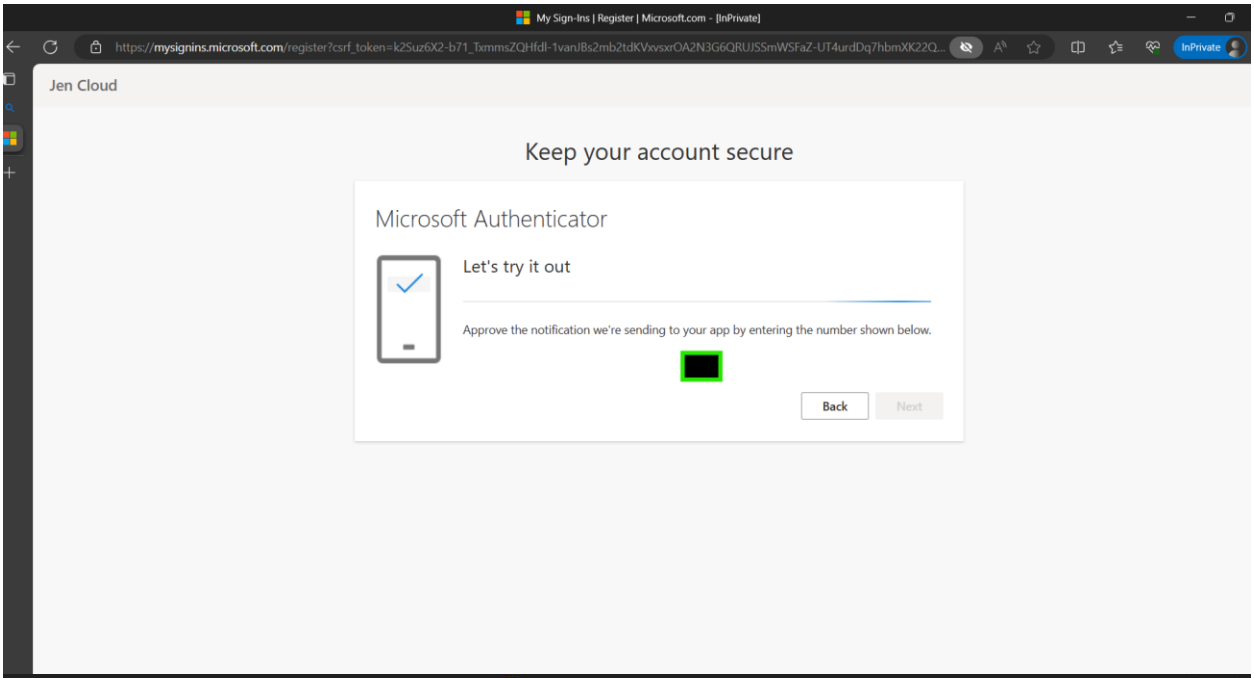
Figure 24: Multi-factor authentication enforced

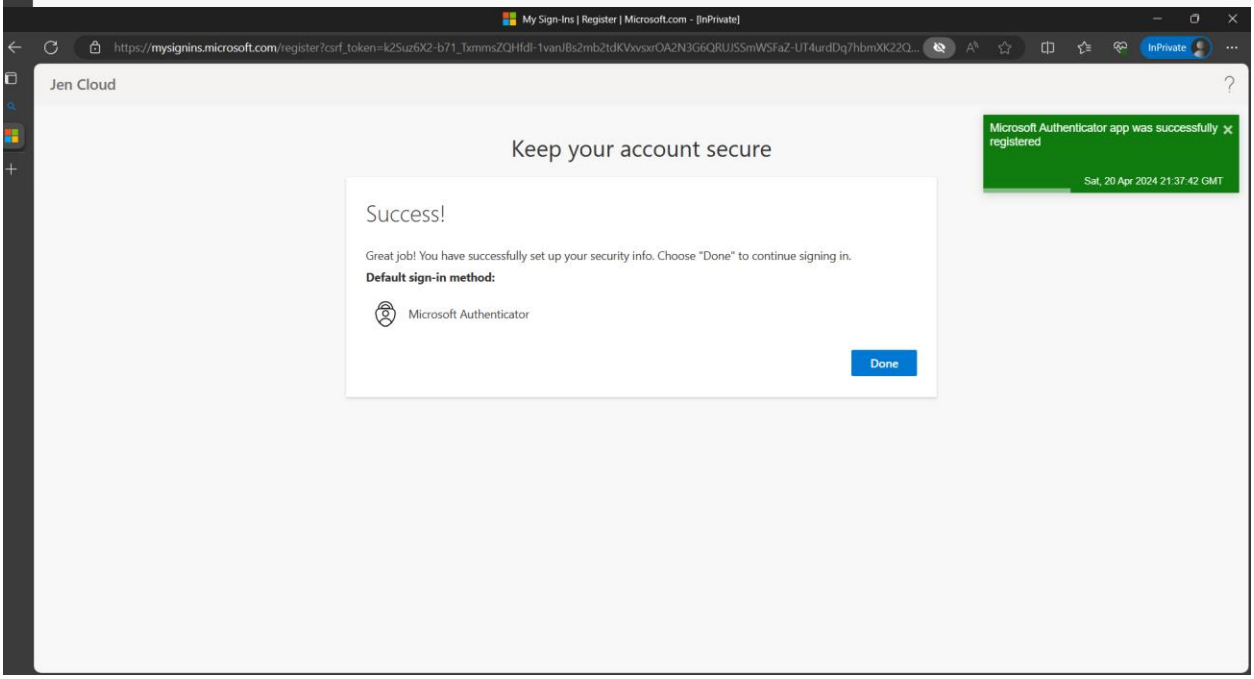
3.3 Setup MFA


Sign in to your account - [InPrivate]
https://login.microsoftonline.com/common/login
InPrivate
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
My Sign-Ins | Register | Microsoft.com - [InPrivate]
https://mysignins.microsoft.com/register?csrf_token=k2Suz6X2-b71_TxmmsZQHfdl-1vanJBs2mb2tdKVxvsxrOA2N3G6QRUJSSmWSFaZ-UT4urdDq7hbmXK22Q...
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


My Sign-Ins | Register | Microsoft.com - [InPrivate]
https://mysignins.microsoft.com/register?csrf_token=k2Suz6X2-b71_TxmmsZQHfdl-1vanJBs2mb2tdKVxvsxrOA2N3G6QRUJSSmWSFaZ-UT4urdDq7hbmXK22Q...
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]
https://mysignins.microsoft.com/register?csrf_token=k2Suz6X2-b71_TxmmsZQHfdl-1vanJBs2mb2tdKVxvsxrOA2N3G6QRUJSSmWSFaZ-UT4urdDq7hbmXK22Q...
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


My Sign-Ins | Register | Microsoft.com - [InPrivate]
https://mysignins.microsoft.com/register?csrf_token=k2Suz6X2-b71_TxmmsZQHfdI-1vanJBs2mb2tdKVxvsxrOA2N3G6QRUJSSmWSFaZ-UT4urdDq7hbmXK22Q...
InPrivate
Jen Cloud
Keep your account secure
Microsoft Authenticator
Let's try it out
Approve the notification we're sending to your app by entering the number shown below.
Back
Next


My Sign-Ins | Register | Microsoft.com - [InPrivate]
https://mysignins.microsoft.com/register?csrf_token=k2Suz6X2-b71_TxmmsZQHfdI-1vanJBs2mb2tdKVxvsxrOA2N3G6QRUJSSmWSFaZ-UT4urdDq7hbmXK22Q...
InPrivate
Jen Cloud
Microsoft Authenticator app was successfully registered
Sat, 20 Apr 2024 21:37:42 GMT
Keep your account secure
Success!
Great job! You have successfully set up your security info. Choose "Done" to continue signing in.
Default sign-in method:
Microsoft Authenticator
Done

Task 4: Customer lockbox

4.1 Enable customer lockbox:

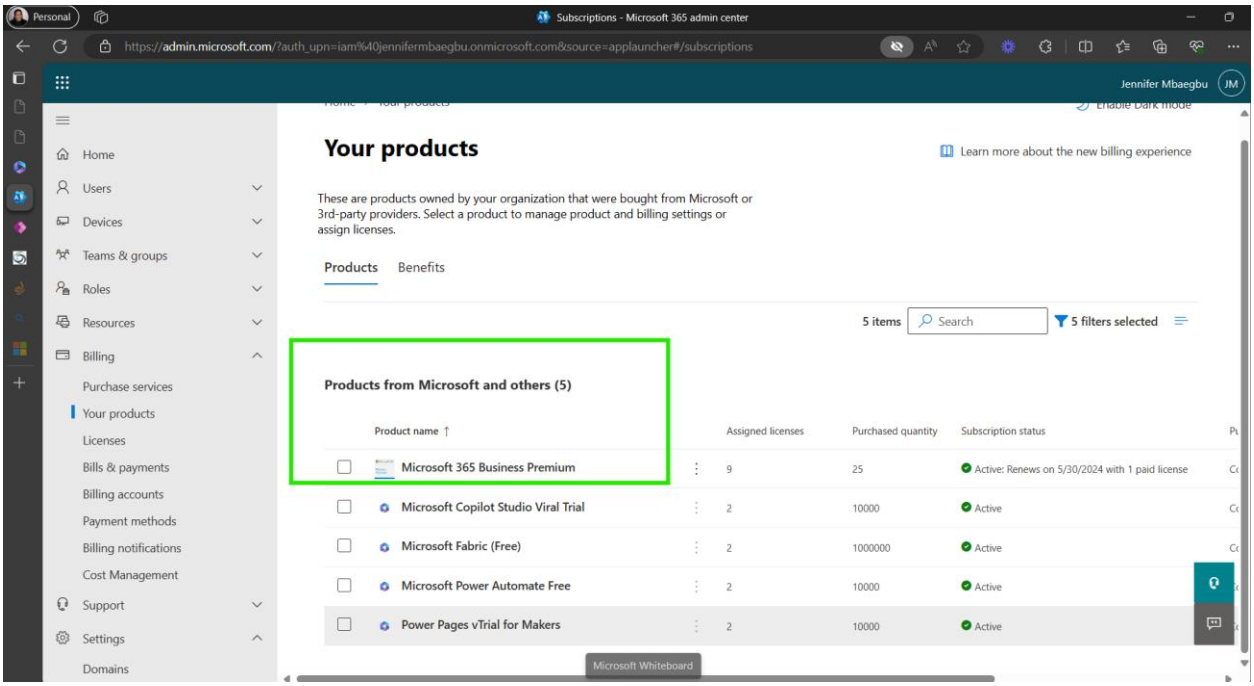


Figure 25: Microsoft 365 subscription verifed not to have the customer lockbox feature

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

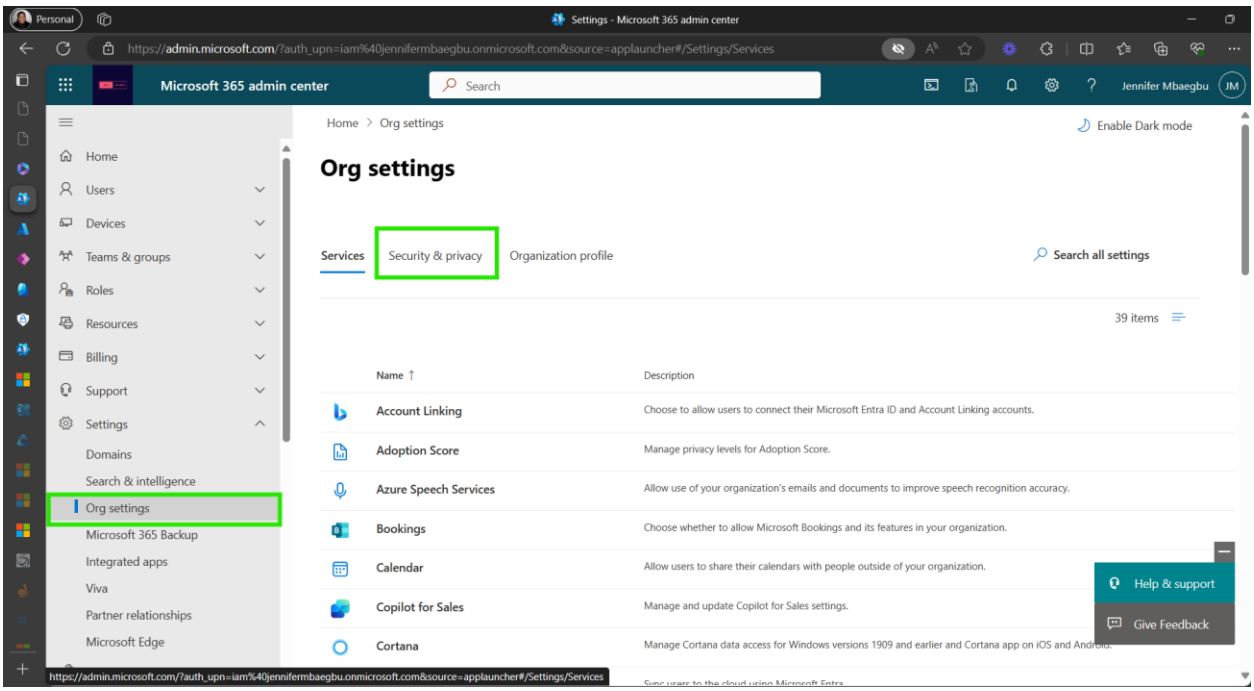
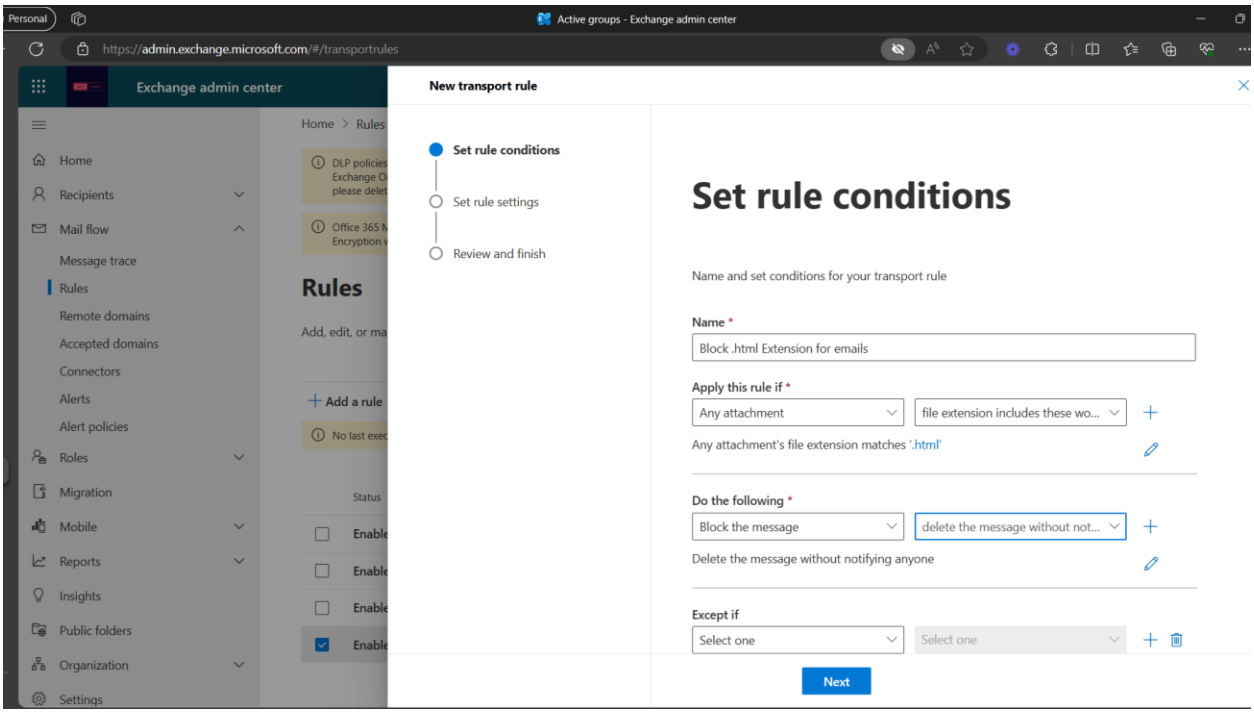


Figure 26: On Microsoft 365 Admin center, navigate to Settings - Org Settings - Security and Privacy

Task 5: Security

5.1 Block .html extension for emails



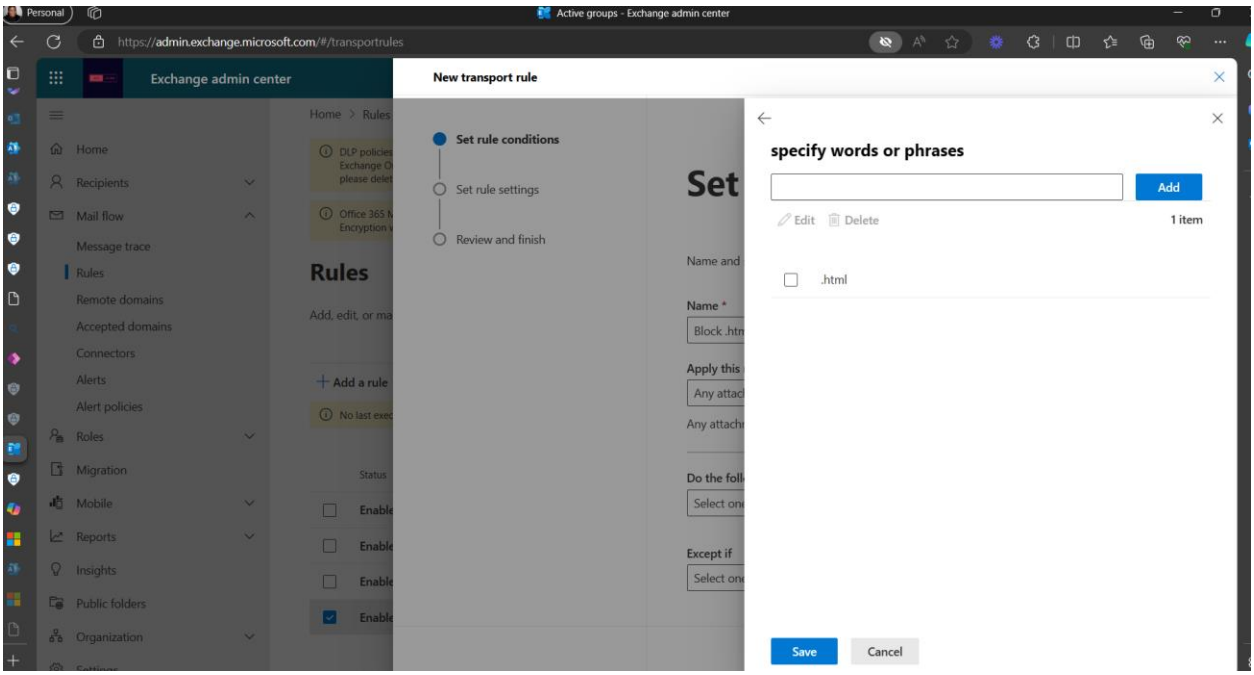


Figure 27: .html is specified

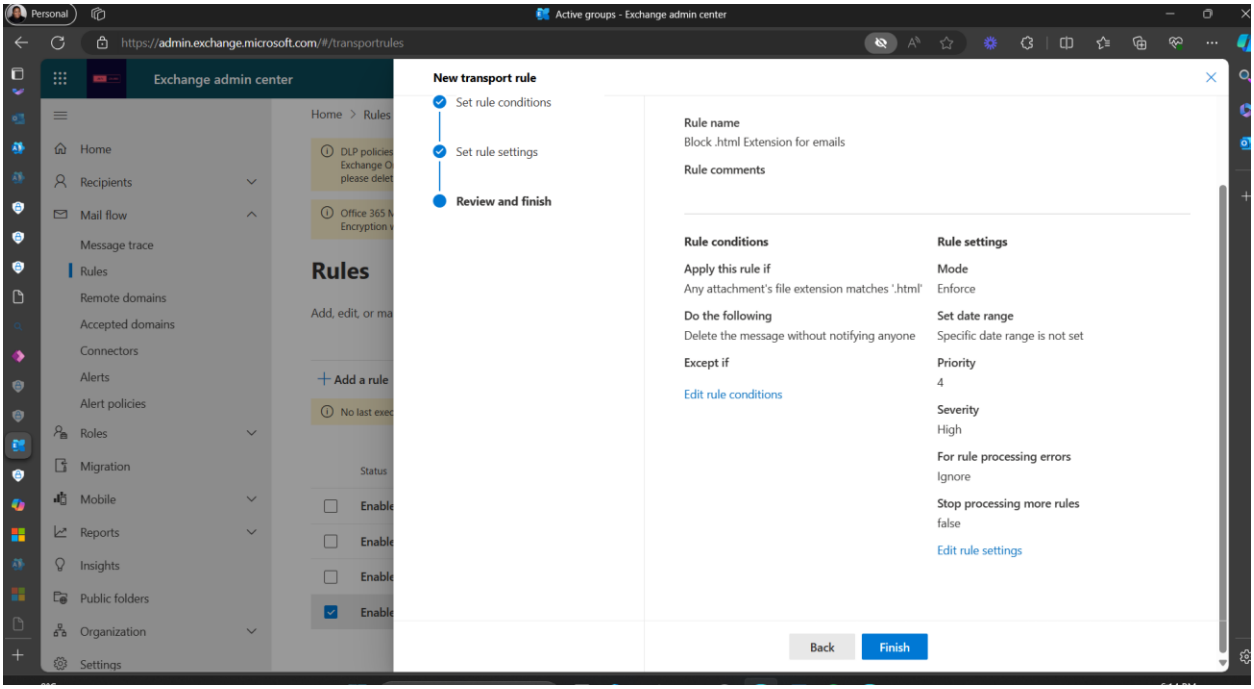
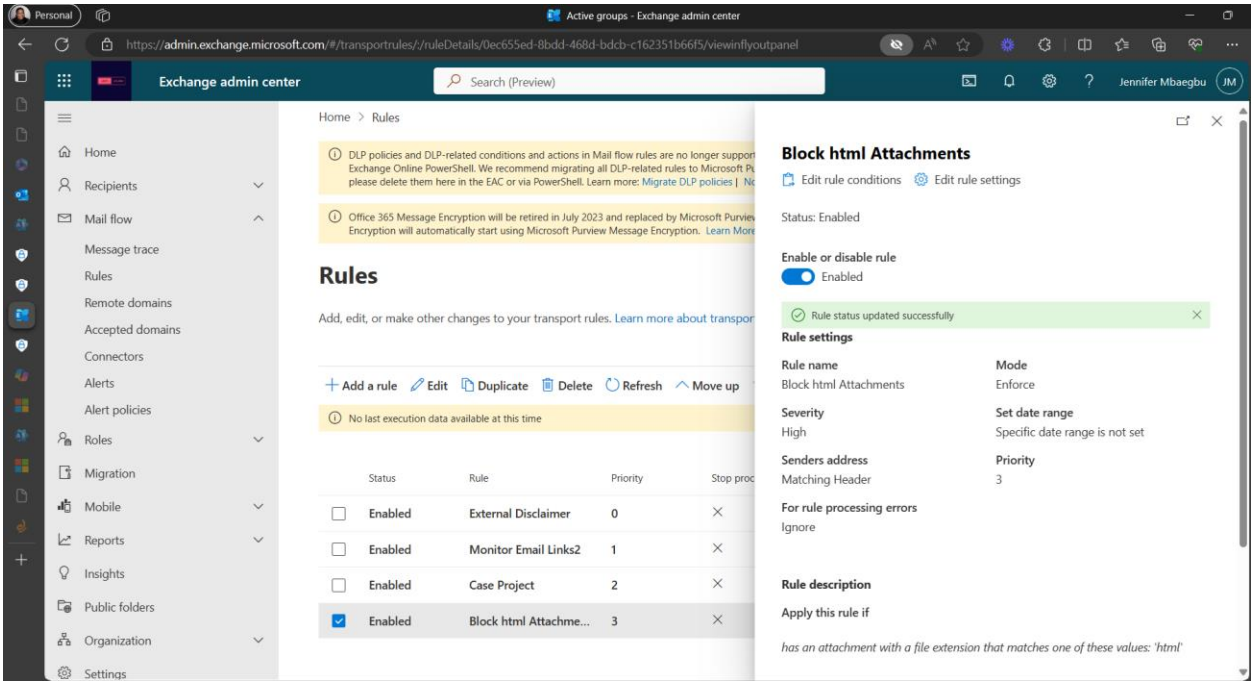
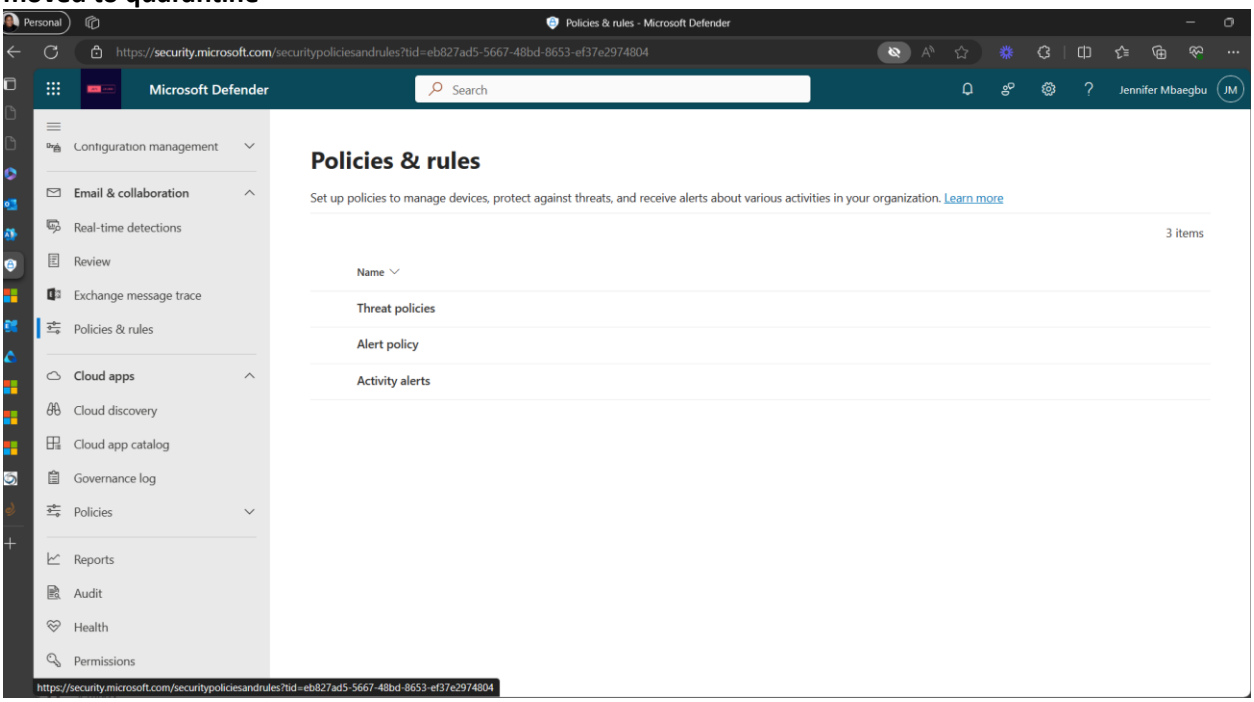
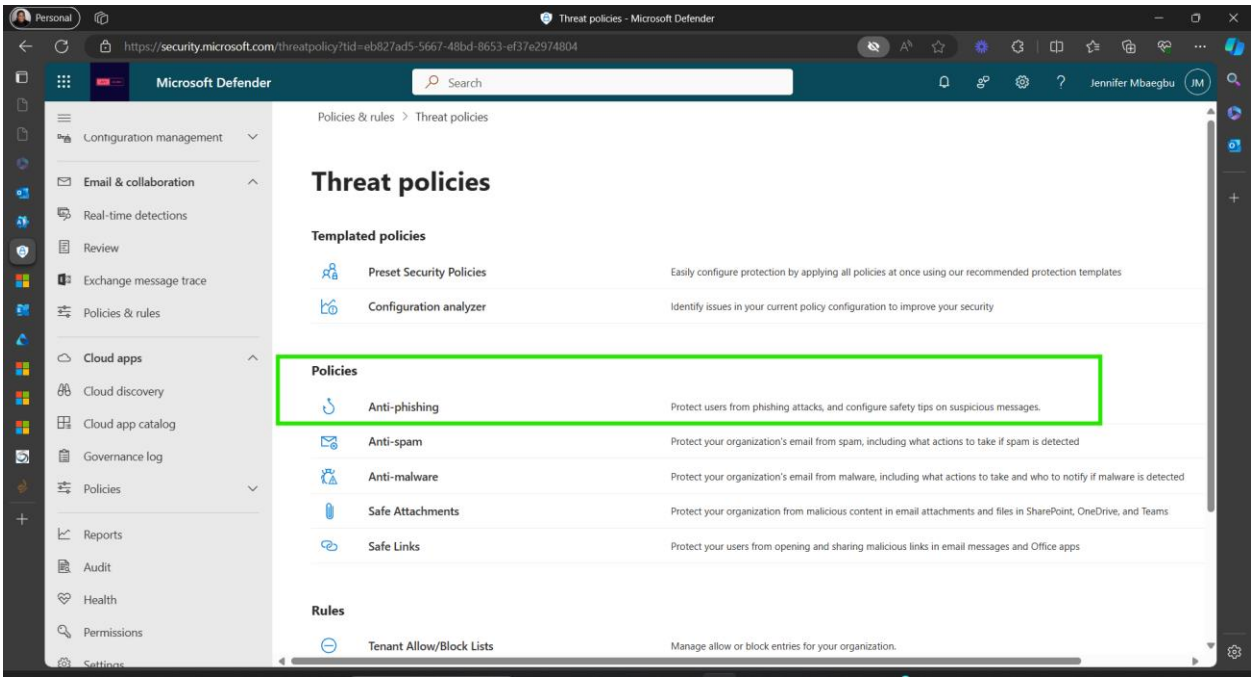


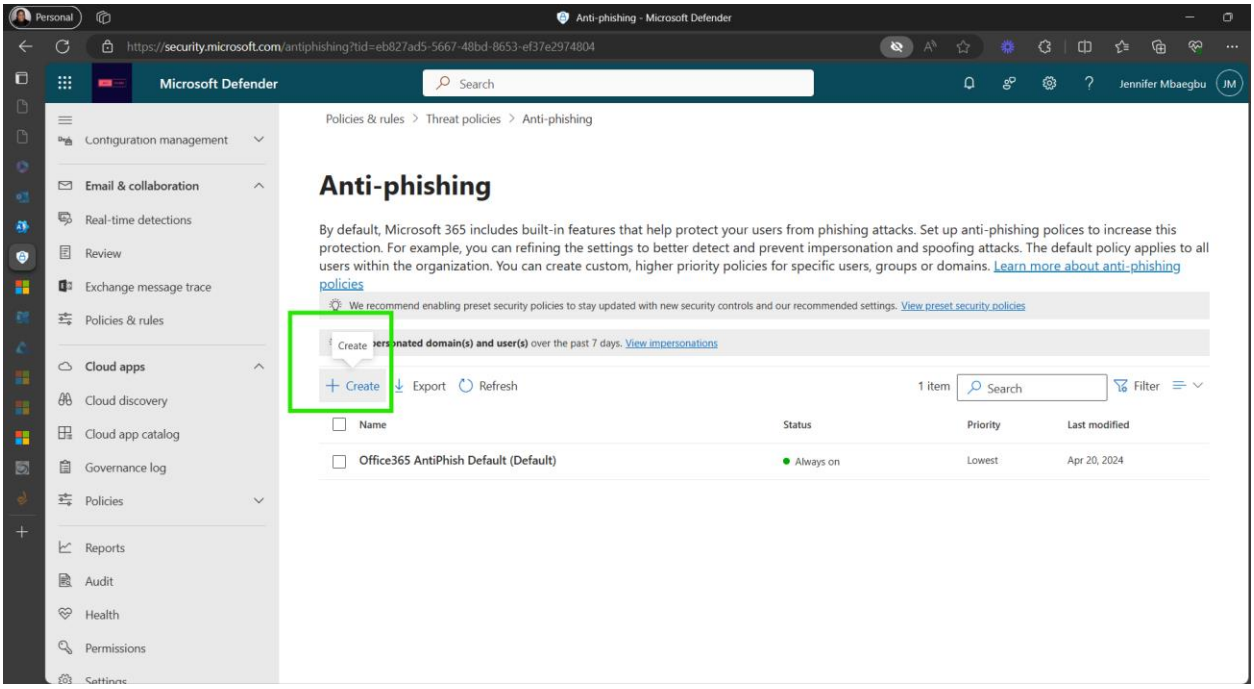
Figure 28: Review New Transport Rule on Exchange Center to Block .html

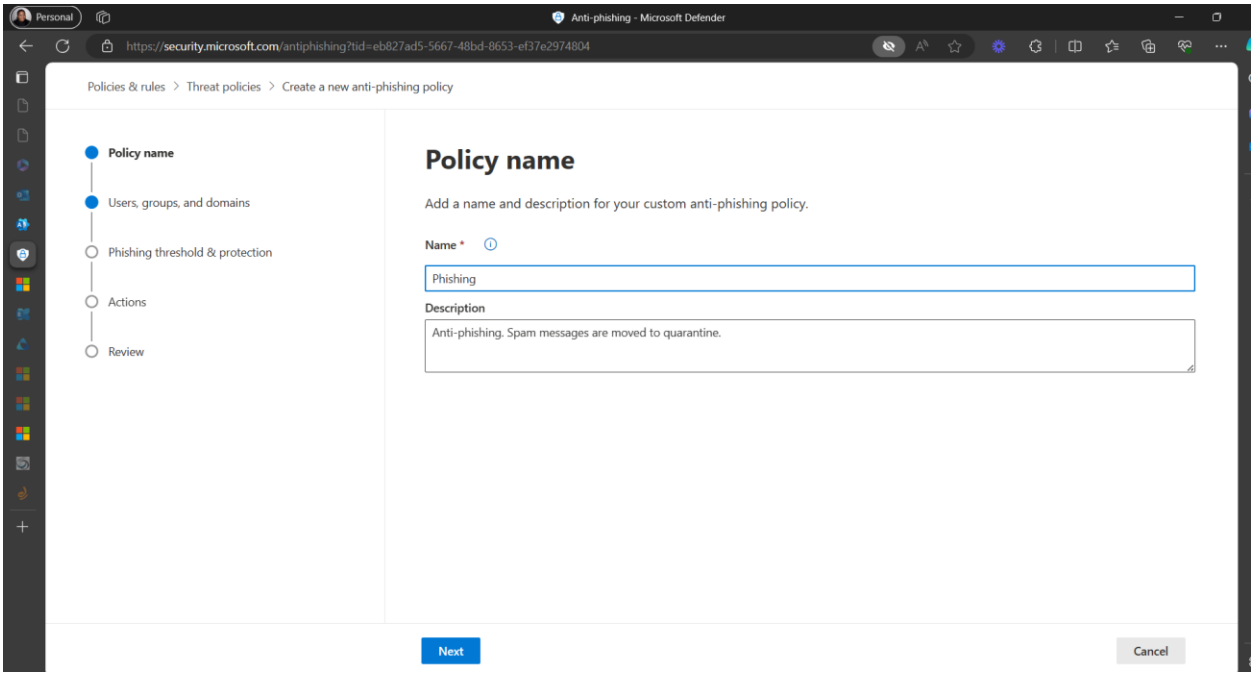


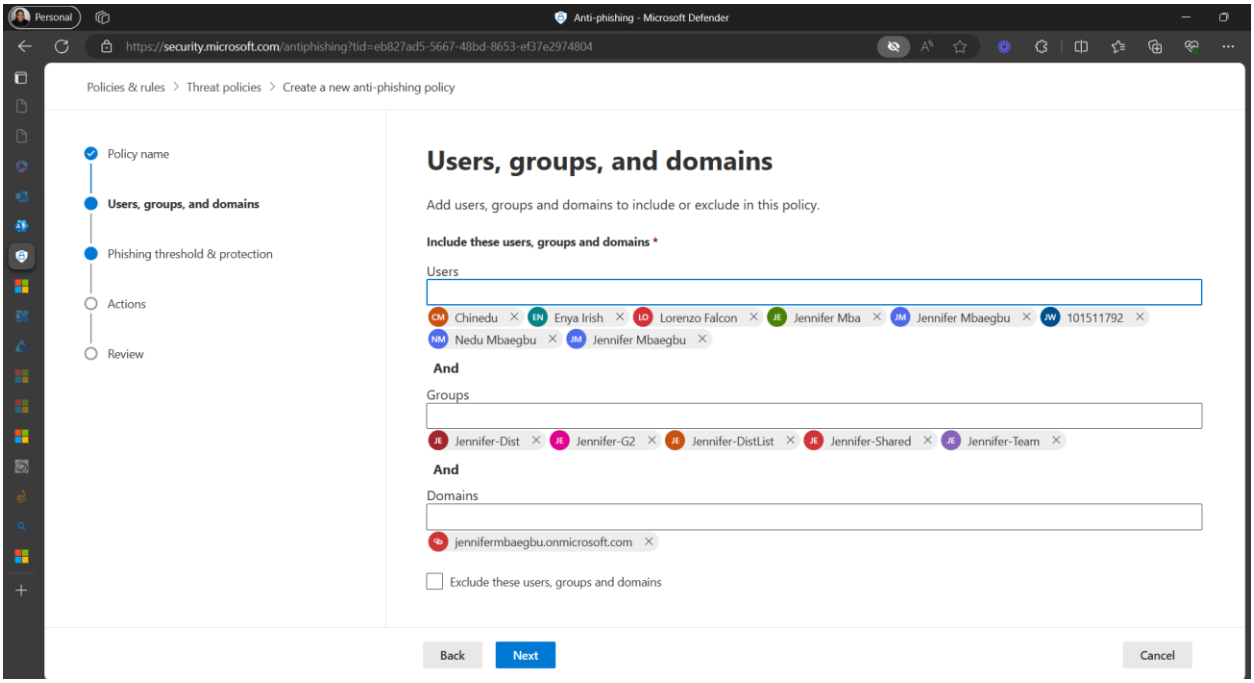
5.2 Create anti Phishing policy and apply your desired settings and make sure the spam messages are moved to quarantine






Anti-phishing - Microsoft Defender
https://security.microsoft.com/antiphishing?tid=eb827ad5-5667-48bd-8653-ef37e2974804
Microsoft Defender
Search
Jennifer Mbaegbu
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
Policies & rules > Threat policies > Anti-phishing
Anti-phishing
By default, Microsoft 365 includes built-in features that help protect your users from phishing attacks. Set up anti-phishing polices to increase this protection. For example, you can refining the settings to better detect and prevent impersonation and spoofing attacks. The default policy applies to all users within the organization. You can create custom, higher priority policies for specific users, groups or domains. Learn more about anti-phishing policies
We recommend enabling preset security policies to stay updated with new security controls and our recommended settings. View preset security policies
Create
+ Create
Export
Refresh
1 item
Search
Filter
Name
Status
Priority
Last modified
Office365 AntiPhish Default (Default)
Always on
Lowest
Apr 20, 2024


Anti-phishing - Microsoft Defender
https://security.microsoft.com/antiphishing?tid=eb827ad5-5667-48bd-8653-ef37e2974804
Policies & rules > Threat policies > Create a new anti-phishing policy
Policy name
Users, groups, and domains
Phishing threshold & protection
Actions
Review
Policy name
Add a name and description for your custom anti-phishing policy.
Name *
Phishing
Description
Anti-phishing. Spam messages are moved to quarantine.
Next
Cancel



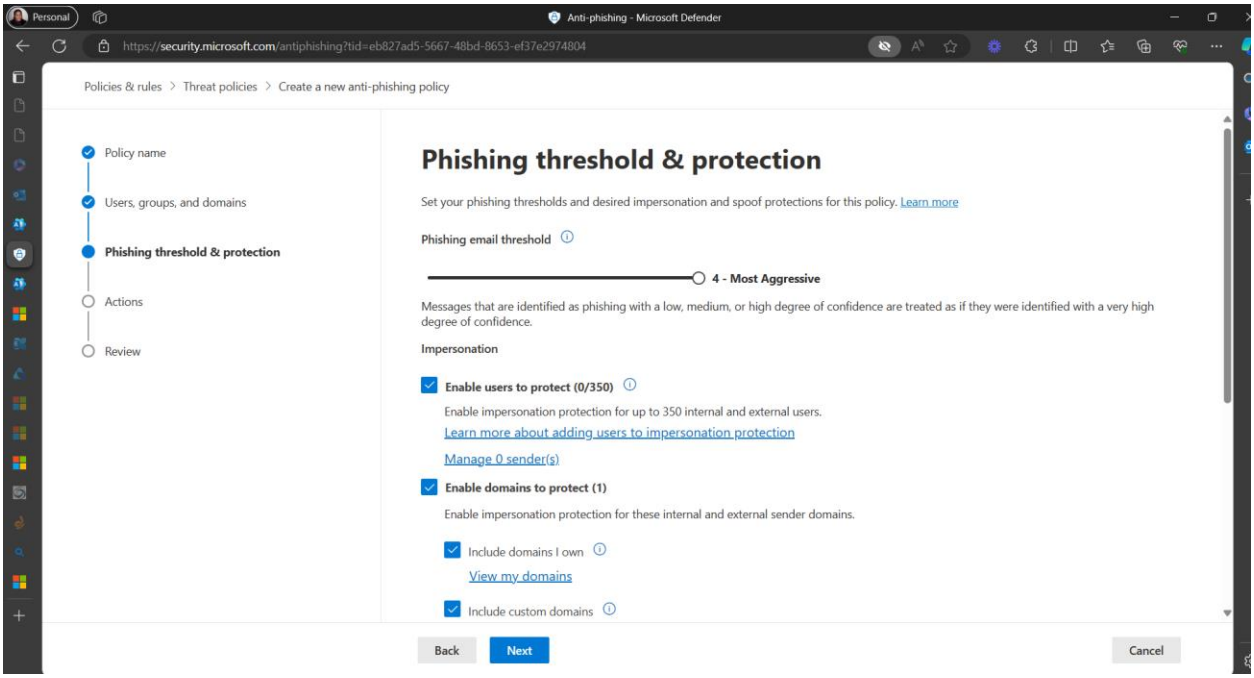
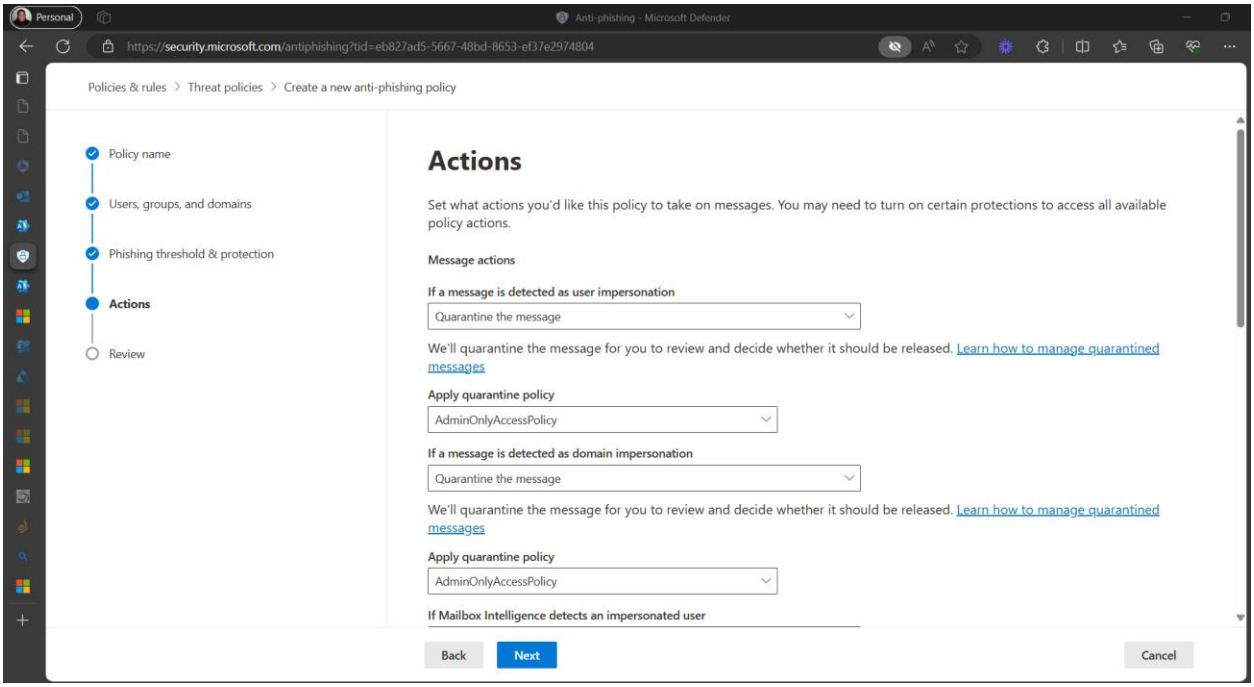


Figure 29: Setting up threshold and protection



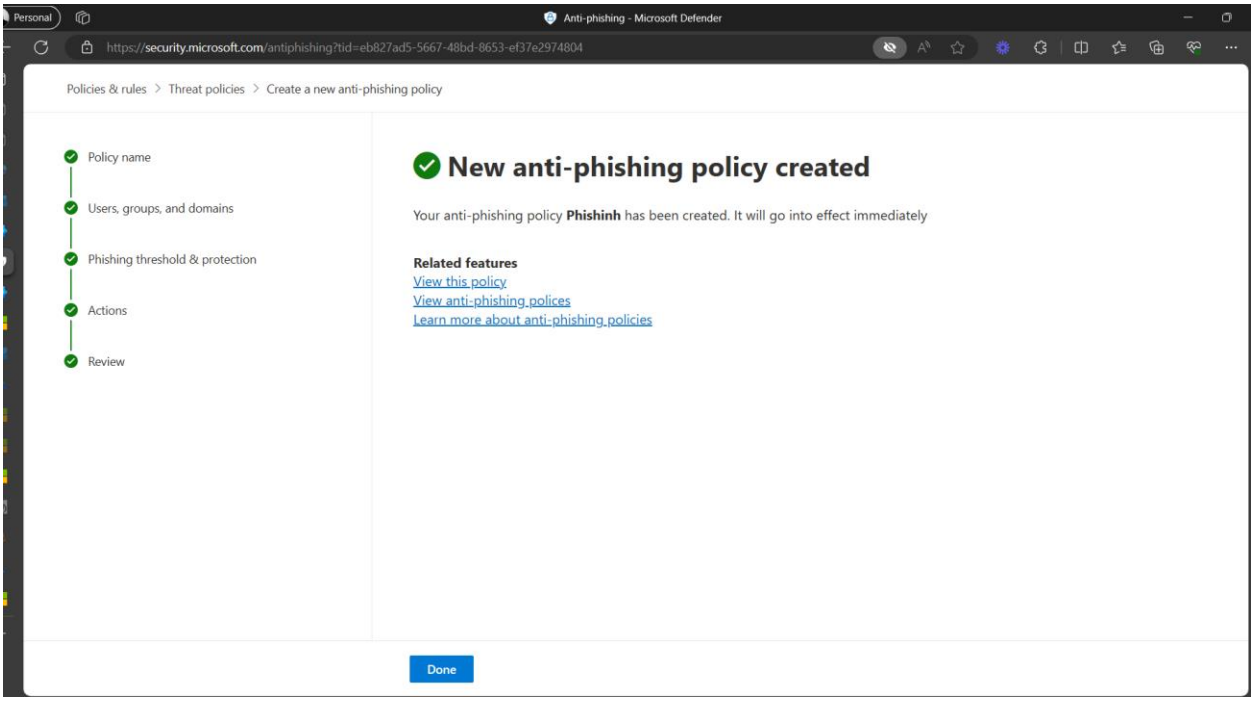
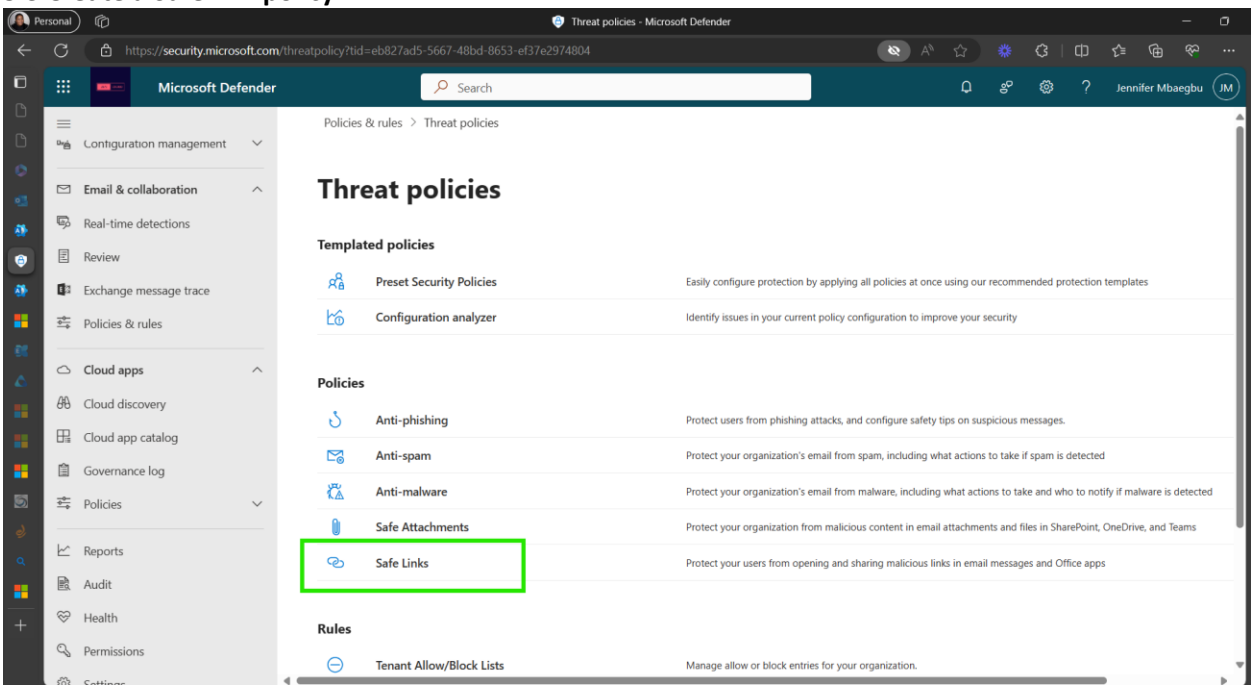


Figure 30Anti-Phishing Policy Created

5.3 Create a Safe link policy



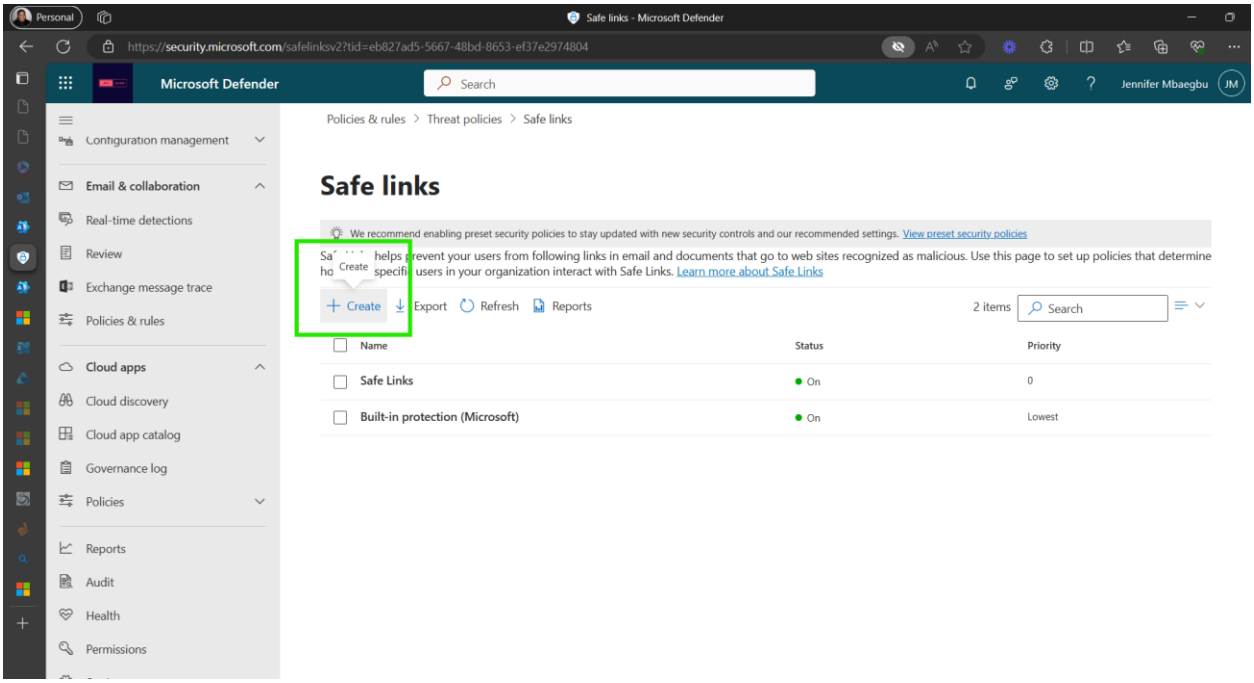
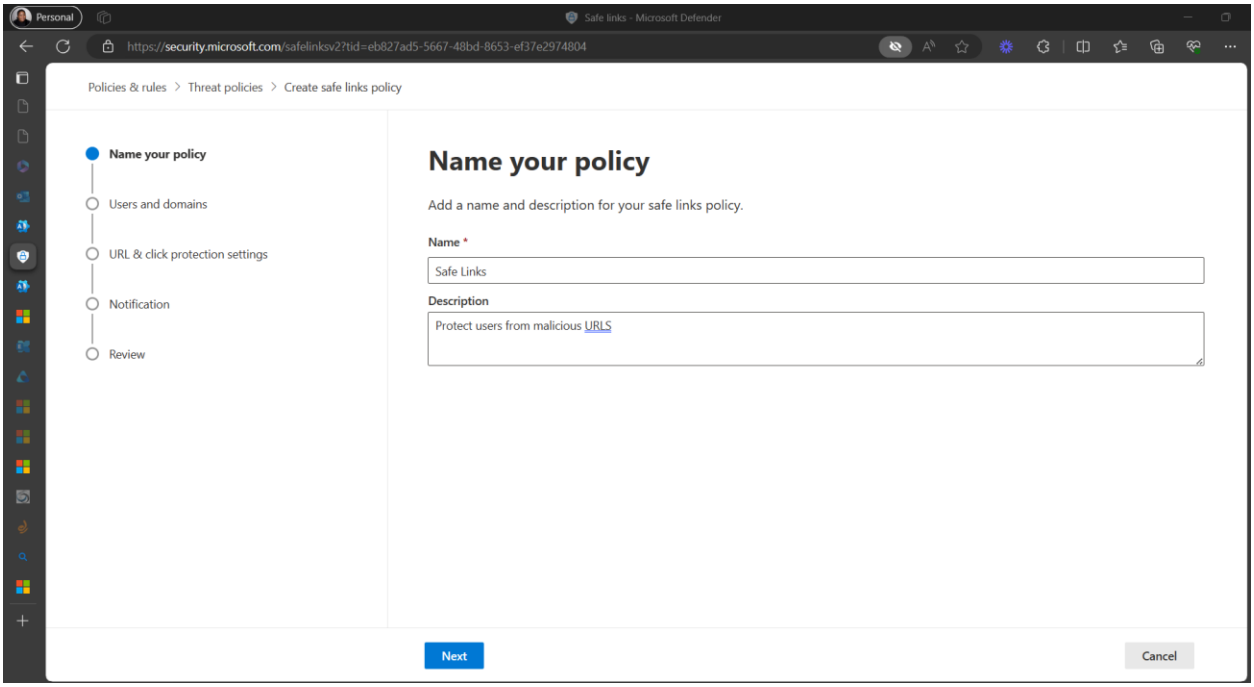
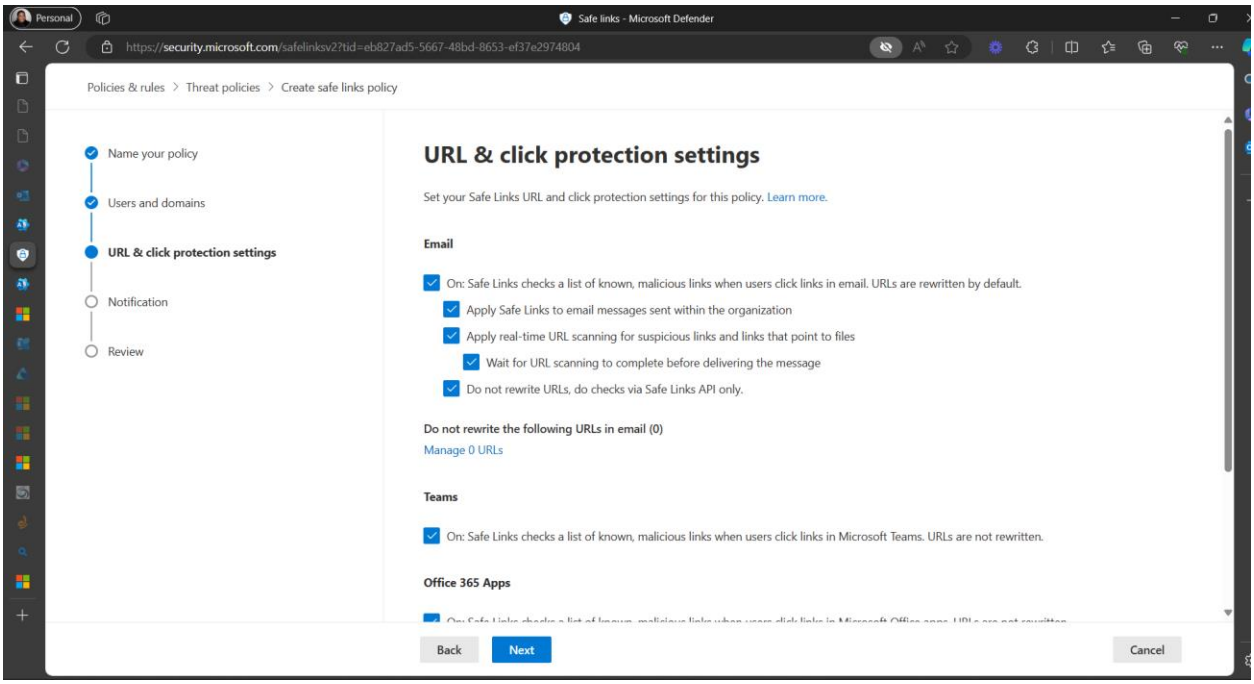
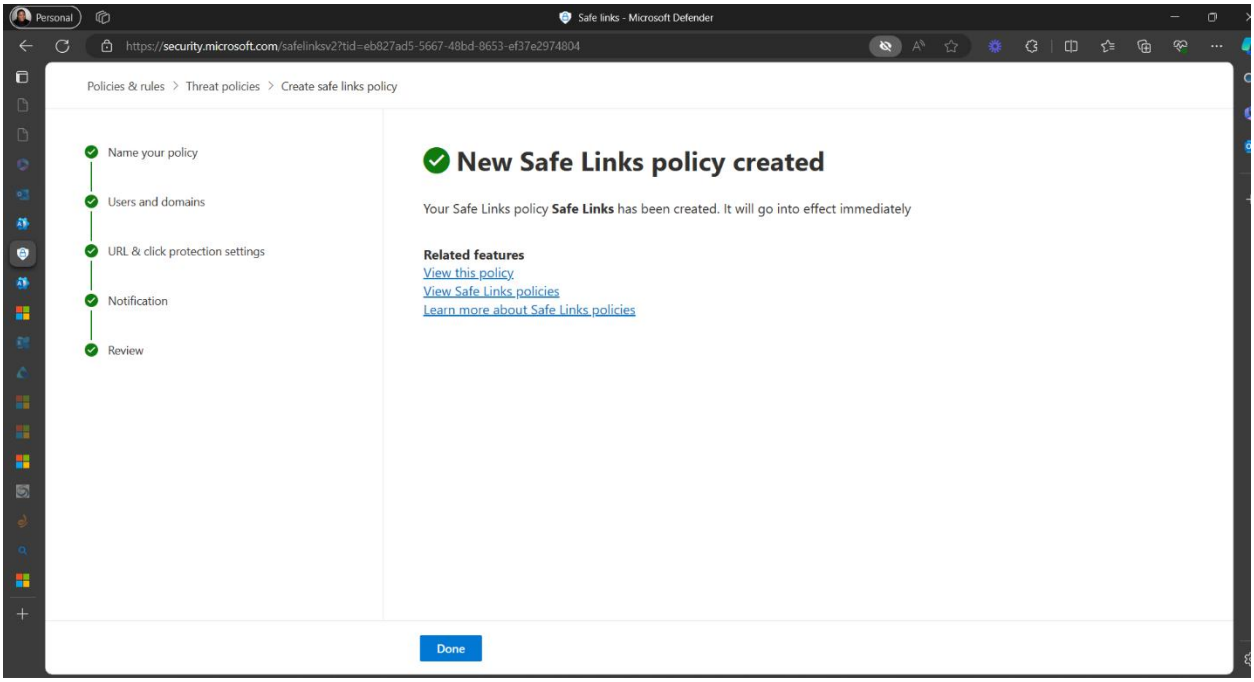


Figure 31: Create Safe Links Policy


Personal
Safe links - Microsoft Defender
https://security.microsoft.com/safelinksv2?tid=eb827ad5-5667-48bd-8653-ef37e2974804
Policies & rules > Threat policies > Create safe links policy
Name your policy
Users and domains
URL & click protection settings
Notification
Review
Name your policy
Add a name and description for your safe links policy.
Name *
Safe Links
Description
Protect users from malicious URLS
Next
Cancel


Personal
Safe links - Microsoft Defender
https://security.microsoft.com/safelinksv2?tid=eb827ad5-5667-48bd-8653-ef37e2974804
Policies & rules > Threat policies > Create safe links policy
Name your policy
Users and domains
URL & click protection settings
Notification
Review
URL & click protection settings
Set your Safe Links URL and click protection settings for this policy. Learn more.
Email
On: Safe Links checks a list of known, malicious links when users click links in email. URLs are rewritten by default.
Apply Safe Links to email messages sent within the organization
Apply real-time URL scanning for suspicious links and links that point to files
Wait for URL scanning to complete before delivering the message
Do not rewrite URLs, do checks via Safe Links API only.
Do not rewrite the following URLs in email (0)
Manage 0 URLs
Teams
On: Safe Links checks a list of known, malicious links when users click links in Microsoft Teams. URLs are not rewritten.
Office 365 Apps
Back
Next
Cancel


Personal
Safe links - Microsoft Defender
https://security.microsoft.com/safelinksv2?tid=eb827ad5-5667-48bd-8653-ef37e2974804
Policies & rules > Threat policies > Create safe links policy
Name your policy
Users and domains
URL & click protection settings
Notification
Review
New Safe Links policy created
Your Safe Links policy Safe Links has been created. It will go into effect immediately
Related features
View this policy
View Safe Links policies
Learn more about Safe Links policies
Done