

Project: Implementing and Managing Microsoft 365 Environment for a Mid-Sized Organization

Objective: To provide hands-on experience in implementing, configuring, and managing a Microsoft 365 environment for a fictional mid-sized organization named "TechSolutions Inc."

Scenario: TechSolutions Inc. is a mid-sized IT services company with 300 employees. The company is transitioning to Microsoft 365 to improve collaboration, security, and productivity. As part of the IT team, you are responsible for setting up and managing the Microsoft 365 environment. This case project will cover various aspects of Microsoft 365, including user and group management, security and compliance, and service configuration.

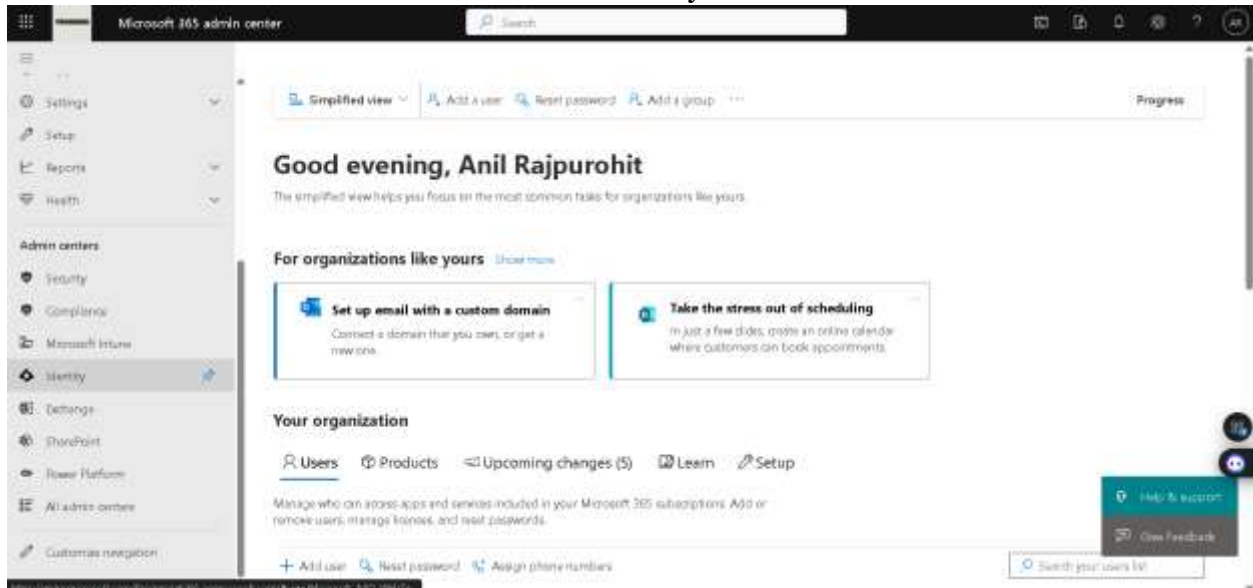
Tasks:

Task 1: Setting Up and Configuring User Accounts

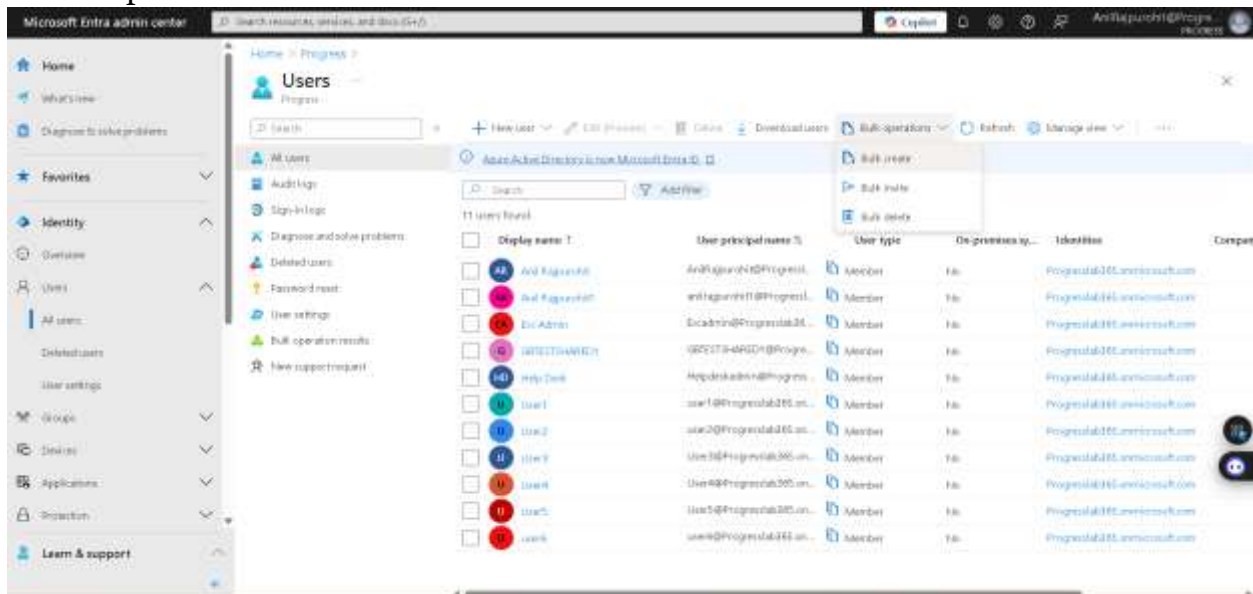
1. Bulk Import Users:

- Use the Microsoft 365 admin center to bulk import 10 users from a CSV file.

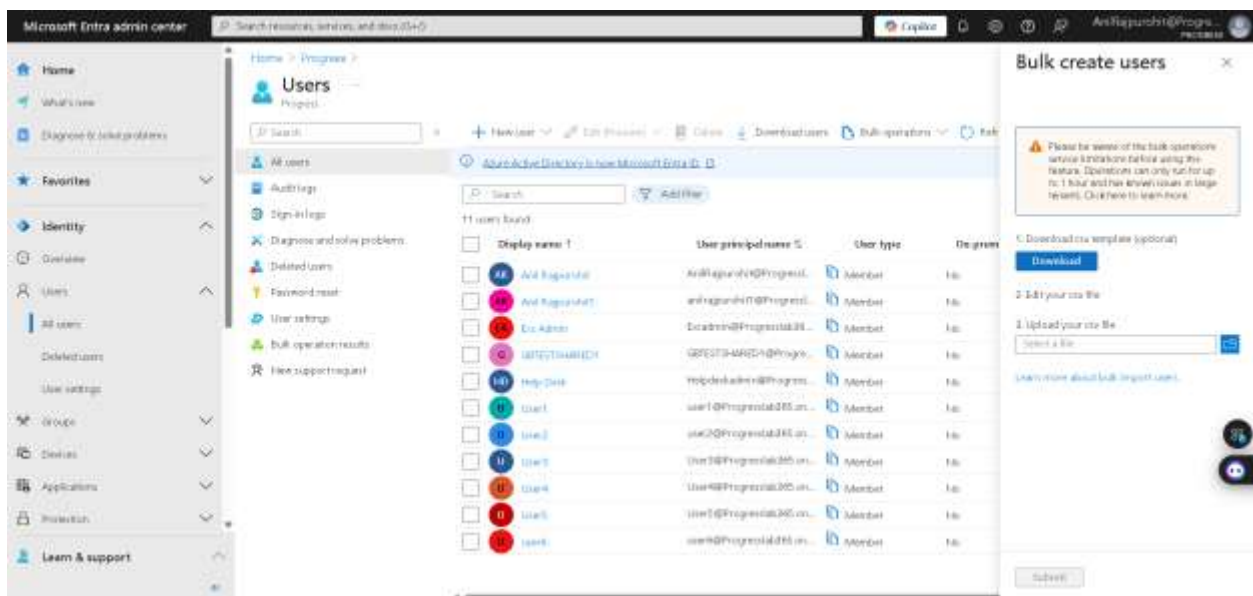
Step 1: In order to bulk import 10 users from a CSV file. First, goto Microsoft 365 admin center then under admin centers click on Identity to access Entra Admin Center.



Step 2: Now from microsoft Entra Admin Center, under Identity -> Users -> All Users -> Bulk operation -> Bulk create.



Step 3: Download .csv template.



Step 4: Received the template, changed it according to our needs like added 10 new users and their passwords.

Name (display name) Required	User name (user principal name) Required	Initial password (password profile) Required	Block sign-in (password) Required	First name Last name Job title Department Usage location Street address
Sophia Martinez	sophia.martinez@progreslab365.onmicrosoft.com	initialpassword11.23	No	
Ethan Johnson	EthanJohnson@progreslab365.onmicrosoft.com	initialpassword11.24	No	
Clara Williams	ClaraWilliams@progreslab365.onmicrosoft.com	initialpassword11.25	No	
Liam Brown	LiamBrown@progreslab365.onmicrosoft.com	initialpassword11.26	No	
Ava Miller	AvaMiller@progreslab365.onmicrosoft.com	initialpassword11.27	No	
Noah Anderson	NoahAnderson@progreslab365.onmicrosoft.com	initialpassword11.28	No	
Isabella Taylor	isabella.taylor@progreslab365.onmicrosoft.com	initialpassword11.29	No	
Mason Thomas	MasonThomas@progreslab365.onmicrosoft.com	initialpassword11.30	No	
Emma White	EmmaWhite@progreslab365.onmicrosoft.com	initialpassword11.31	No	
Lucas Harris	LucasHarris@progreslab365.onmicrosoft.com	initialpassword11.32	No	

Step 5: Now in Bulk create users, upload our new users .csv file then click on Next.

Bulk create users

Please be aware of the bulk operations service limitations before using this feature. Operations can only run for up to 1 hour and has known issues in large tenants. Click here to learn more.

- Download our template (optional)
- Get your file
- Upload your file

File uploaded successfully

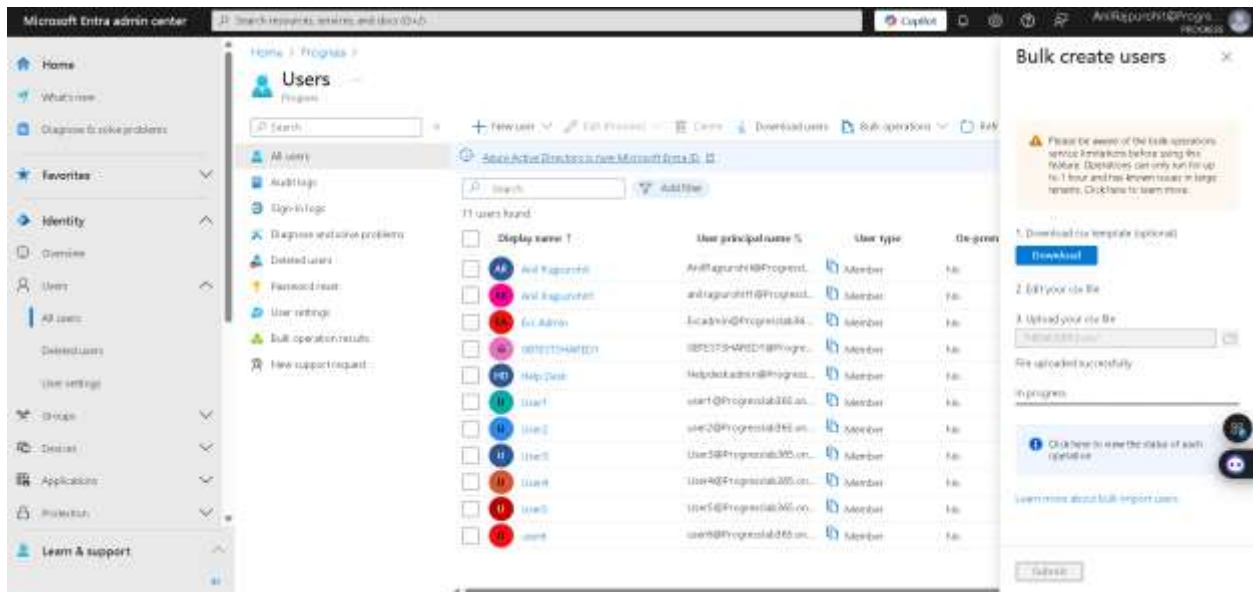
[Learn more about bulk import users](#)

Users

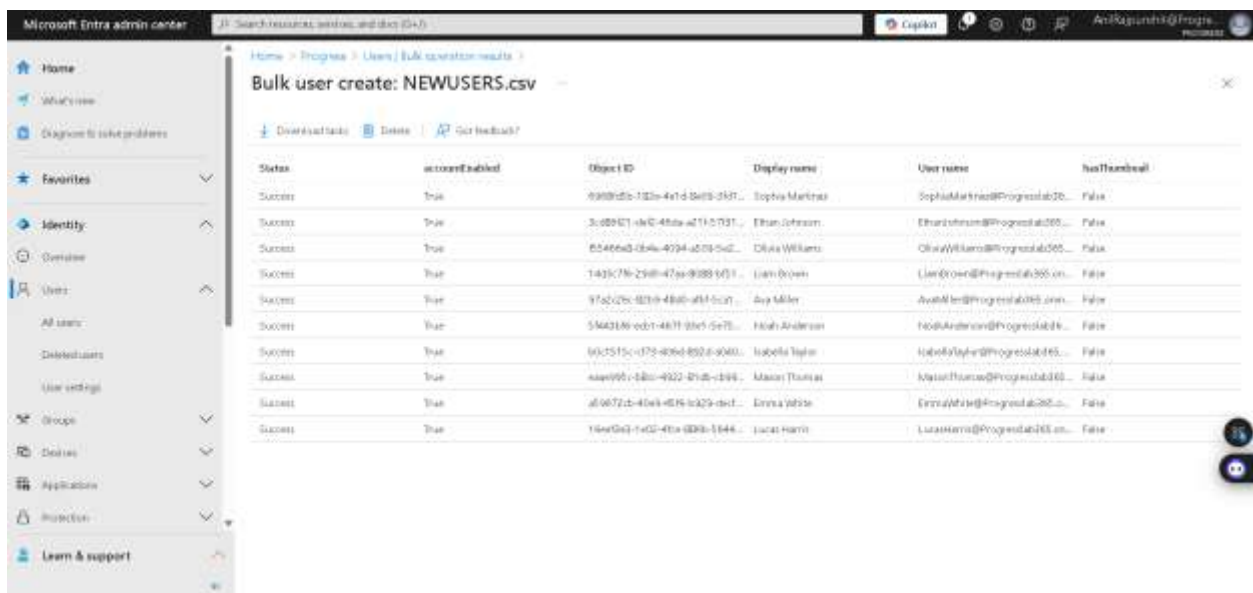
11 users found

Display name	User principal name	User type	Is group
Add Request	anilgundeti@progreslab365.onmicrosoft.com	Member	No
Add Request	anilgundeti@progreslab365.onmicrosoft.com	Member	No
Ethan Johnson	EthanJohnson@progreslab365.onmicrosoft.com	Member	No
Help Desk	helpdesk@progreslab365.onmicrosoft.com	Member	No
User1	user1@progreslab365.onmicrosoft.com	Member	No
User2	user2@progreslab365.onmicrosoft.com	Member	No
User3	user3@progreslab365.onmicrosoft.com	Member	No
User4	user4@progreslab365.onmicrosoft.com	Member	No
User5	user5@progreslab365.onmicrosoft.com	Member	No
User6	user6@progreslab365.onmicrosoft.com	Member	No
User7	user7@progreslab365.onmicrosoft.com	Member	No
User8	user8@progreslab365.onmicrosoft.com	Member	No
User9	user9@progreslab365.onmicrosoft.com	Member	No
User10	user10@progreslab365.onmicrosoft.com	Member	No
User11	user11@progreslab365.onmicrosoft.com	Member	No

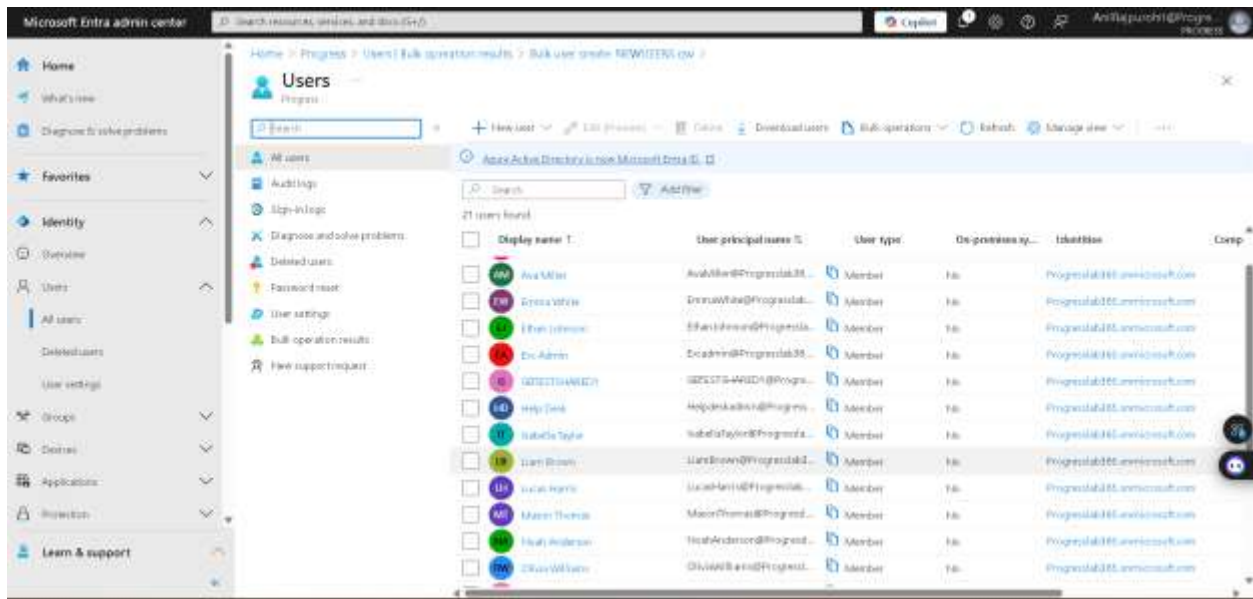
Step 6: File uploaded successfully, and to check the status of each user click on below link. (learn more about bulk import users)



Step 7: We can see that all our users account is successfully enabled.

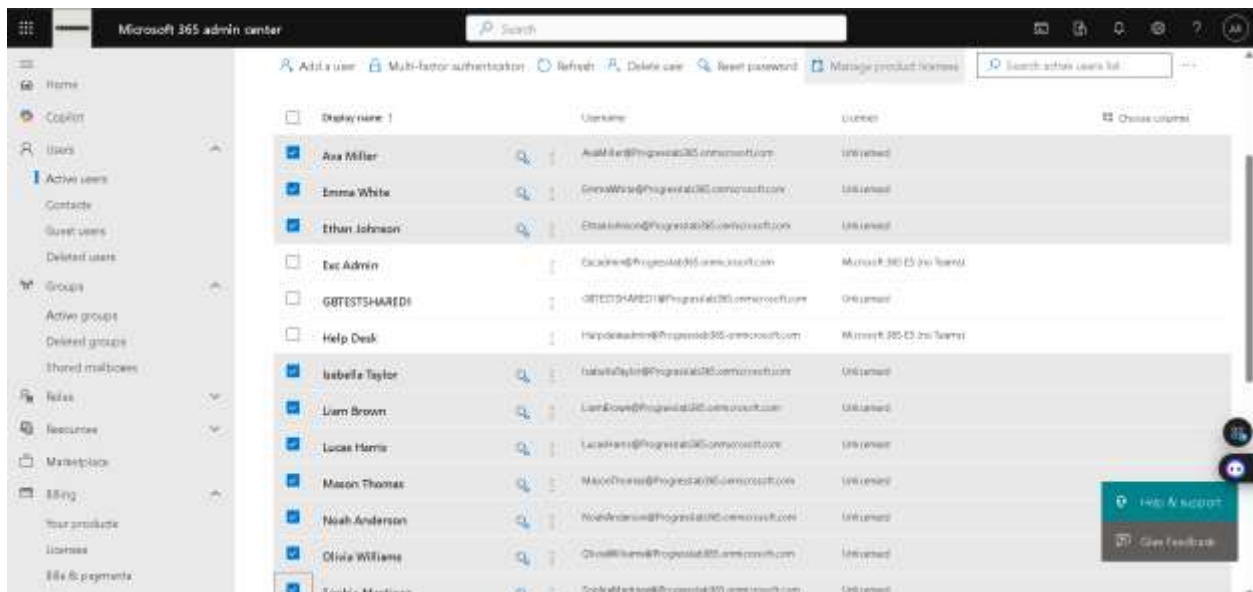


Step 8: Verifying from Entra admin center -> Identity -> Users -> All users. All our new members are successfully added to the list.

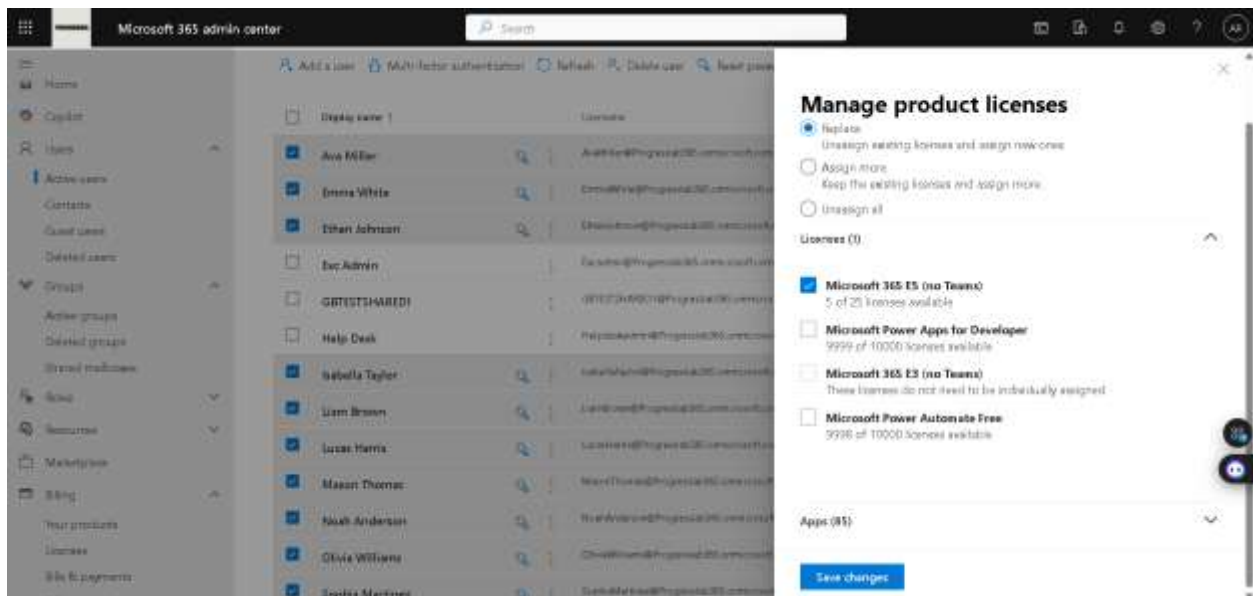


- Assign appropriate licenses (Microsoft 365 E3 or E5) to the imported users.

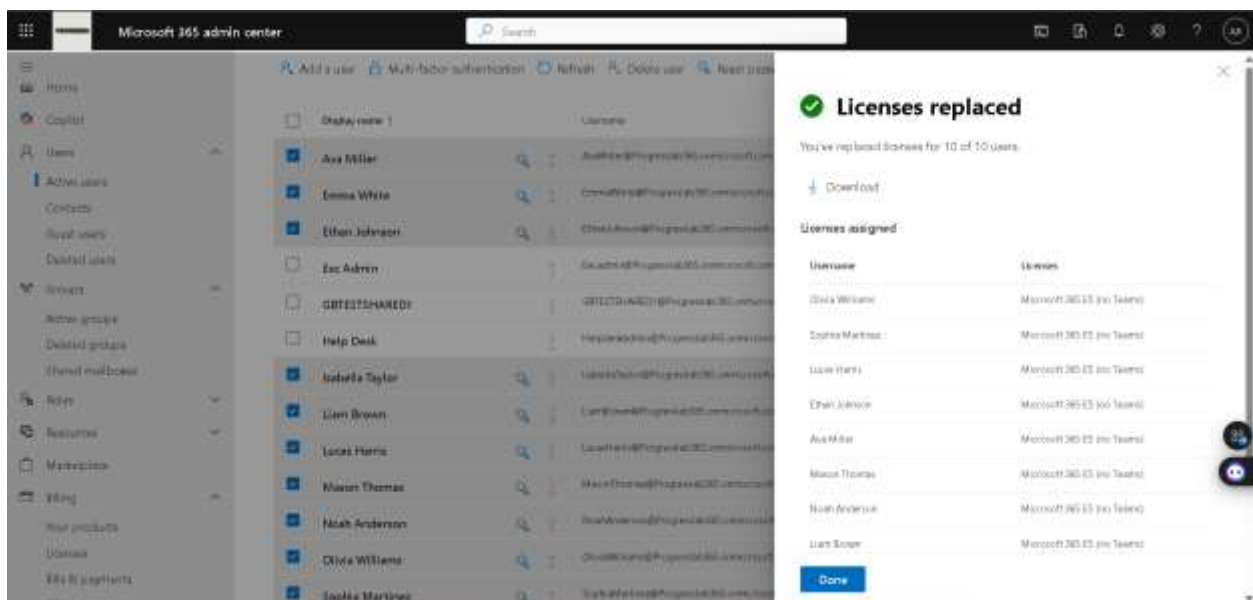
Step 1: First, go to Microsoft 365 admin center, then Users -> Active users. Select all the new users with no licenses then click on manage product licenses.



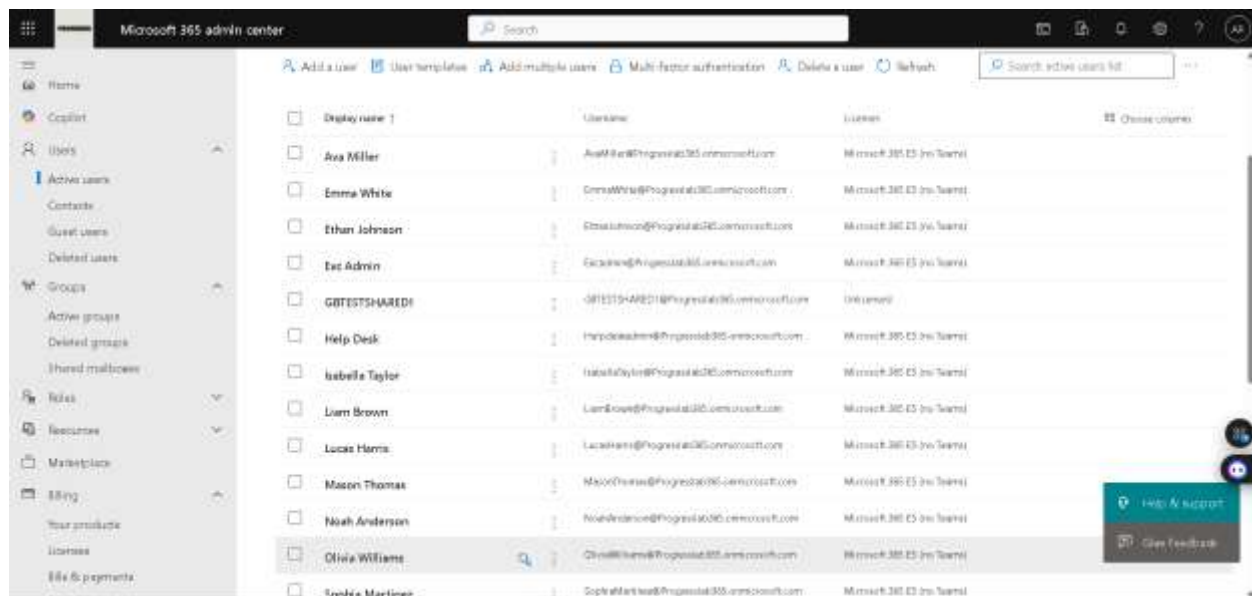
Step 2: Select replace and E5 licenses then click on save changes. This way we can assign licenses in one go.



Step 3: Our licenses has been successfully assigned to new users.



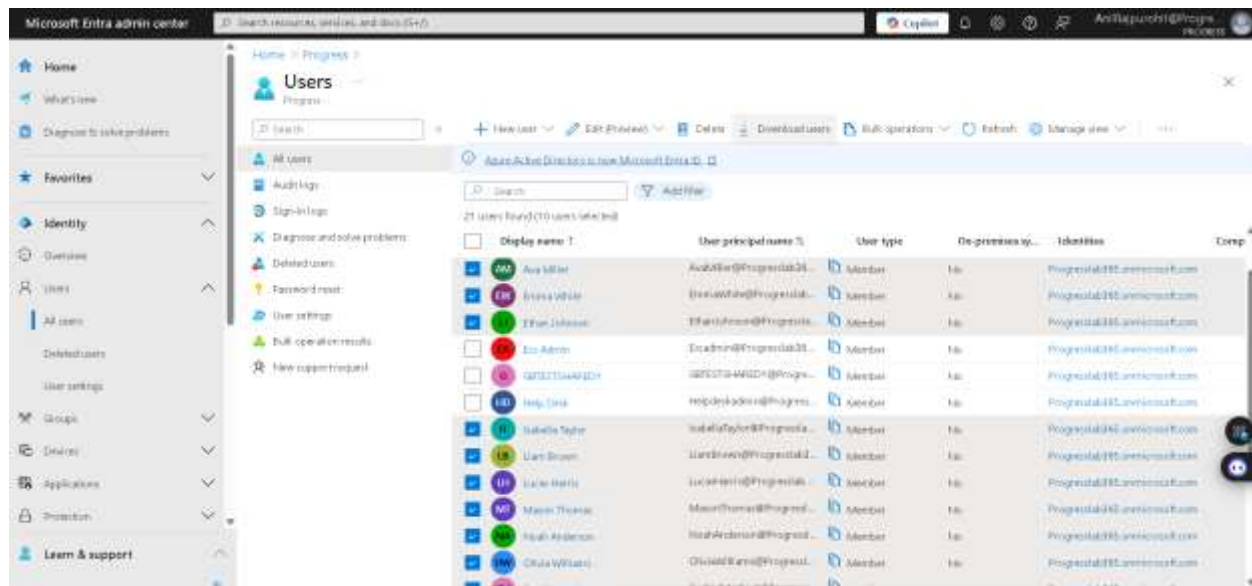
Step 4: Let's re-verify from Admin center -> users -> active users. All our members have an E5 license assigned to them.



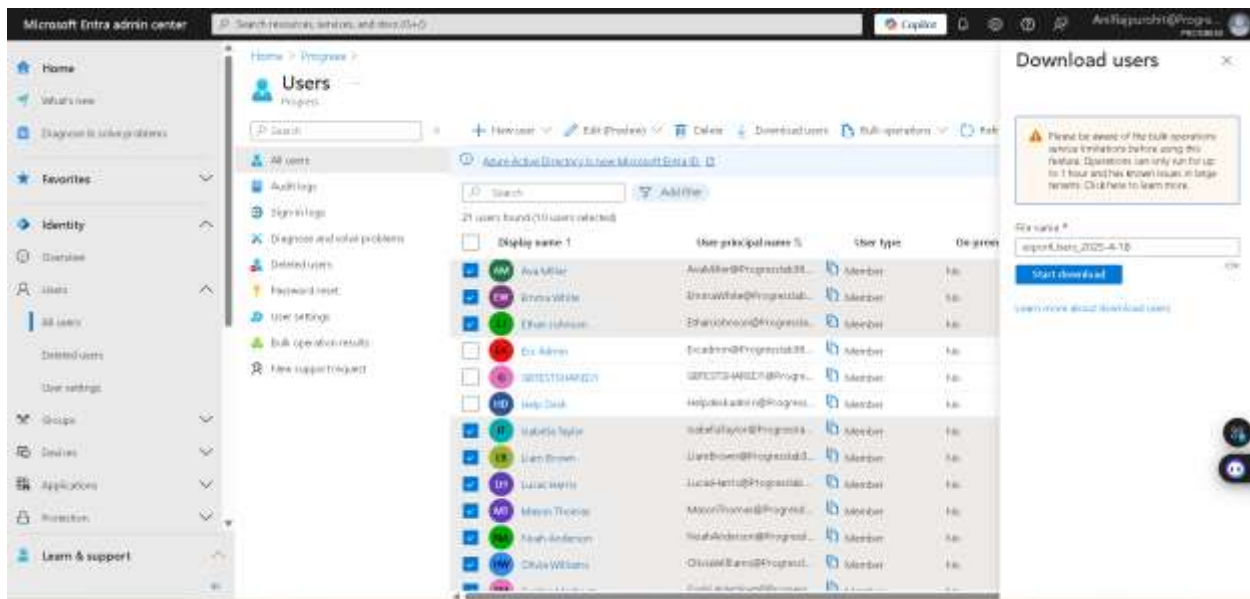
2. Configure User Profiles:

- Ensure each user has a profile picture, contact information, and job title set.
- Configure user settings to include organization-specific information.

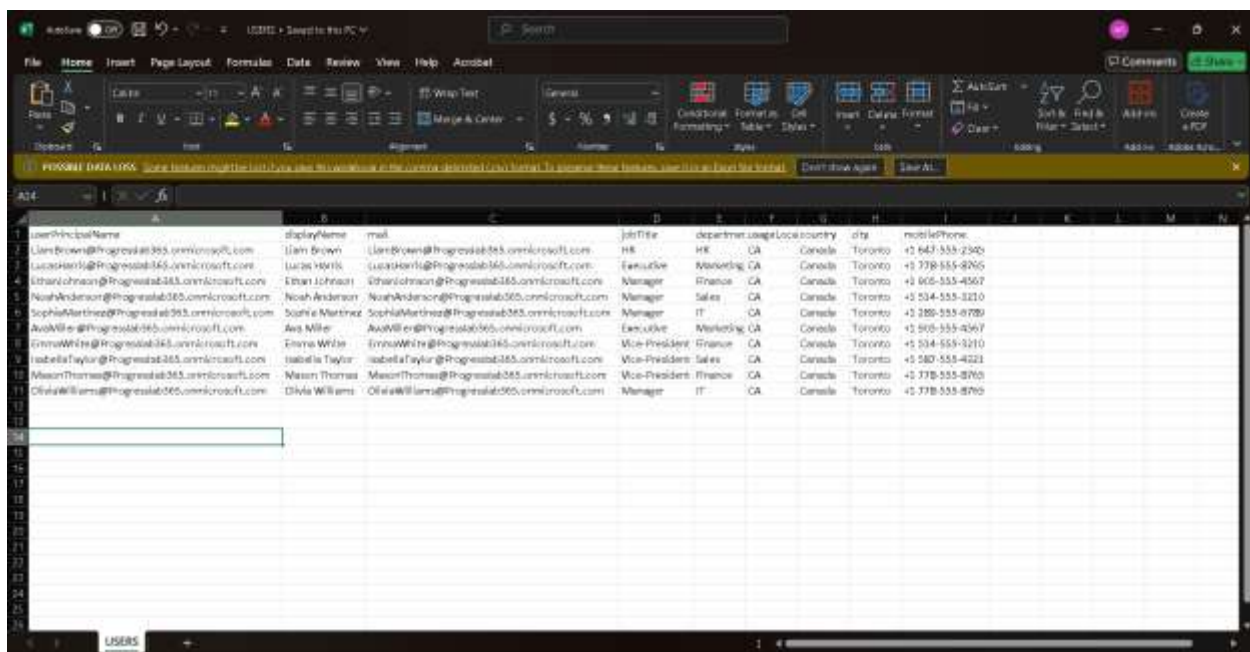
Step 1: To update user's profile, from Entra Admin Center -> Identity -> Users -> All users. Now select all the users to update their profile then click on Download users.



Step 2: Start download the user's file.



Step 3: After downloading the users file, updated all the section we need like job title, department (organization specific), usage location, country, city, and mobile number then saved the file in .csv format.



Step 4: As we want to update all the user's profile in one go, we will be using PowerShell. First, connect to Microsoft graph then imported our updated .csv file and update all new user's profile.


```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (c) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PowerShell

Connect-MyGraph -Domain "Your-Exchange-Alt"

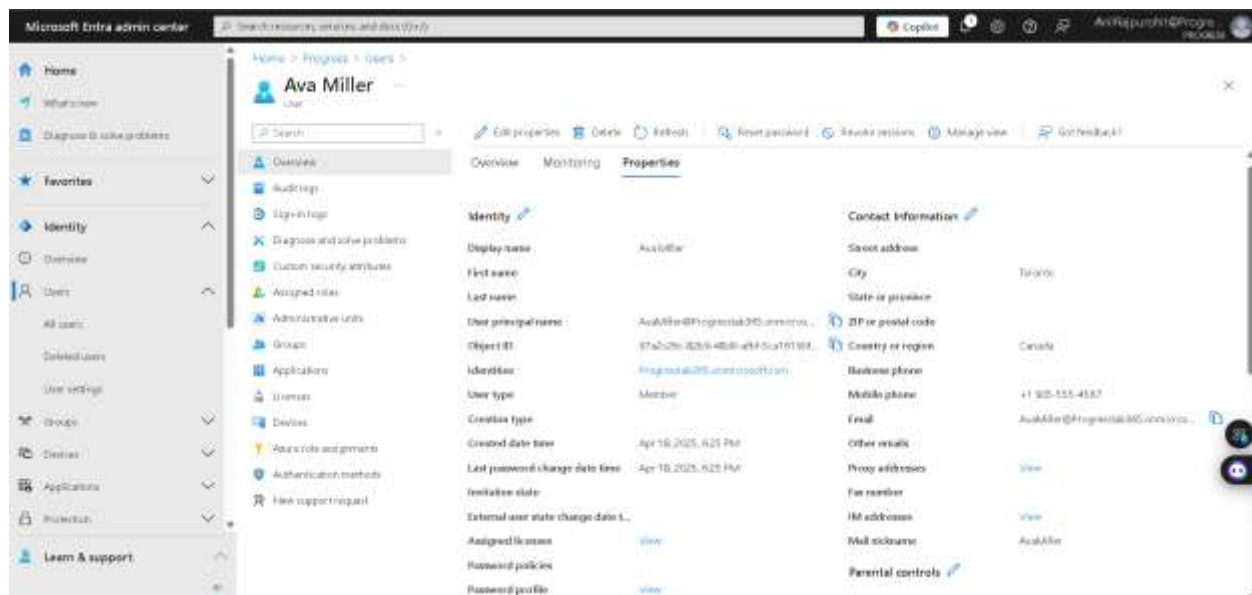
Welcome to Microsoft Graph!

Connected via delegated access using 168ddec-26d6-e3f1-b3d8-29e6b0d4624e
Resource: https://aka.ms/graph/sdk/powershell
MSI Docs: https://aka.ms/graph/sdk/powershell/docs
API Docs: https://aka.ms/graph/docs

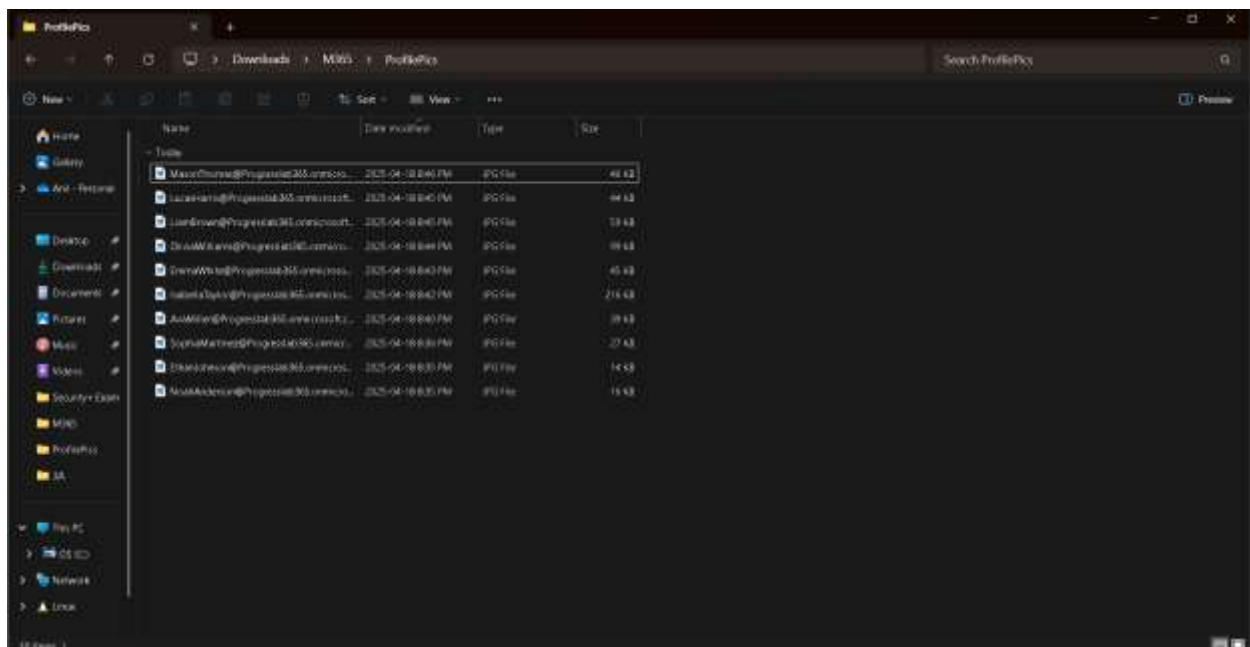
NOTE: You can use the -NoWelcome parameter to suppress this message.

PS C:\Users\user> Get-MyGraph -Domain "Your-Exchange-Alt" | ForEach-Object { Update-MyUser -User $_.Name -Displayname $_.displayname -Mail $_.mail -JobTitle $_.jobtitle -Department $_.department -UsageLocation $_.usageLocation -Country $_.country -City $_.city -HomePhone $_.homePhone }
PS C:\Users\user>
```

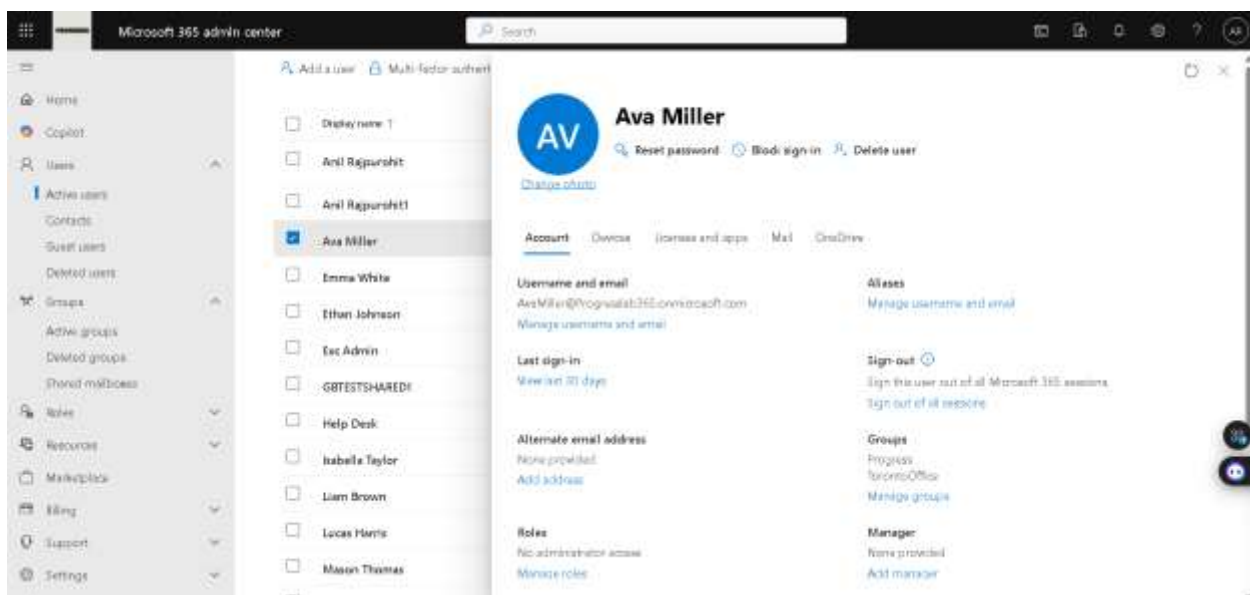
Step 5: Let's verify profile of our new user's, go to Entra admin center -> Identity -> users -> active users. Then select one new user. e.g. Ava miller and go to properties and we can view that users profile has been updated successfully.



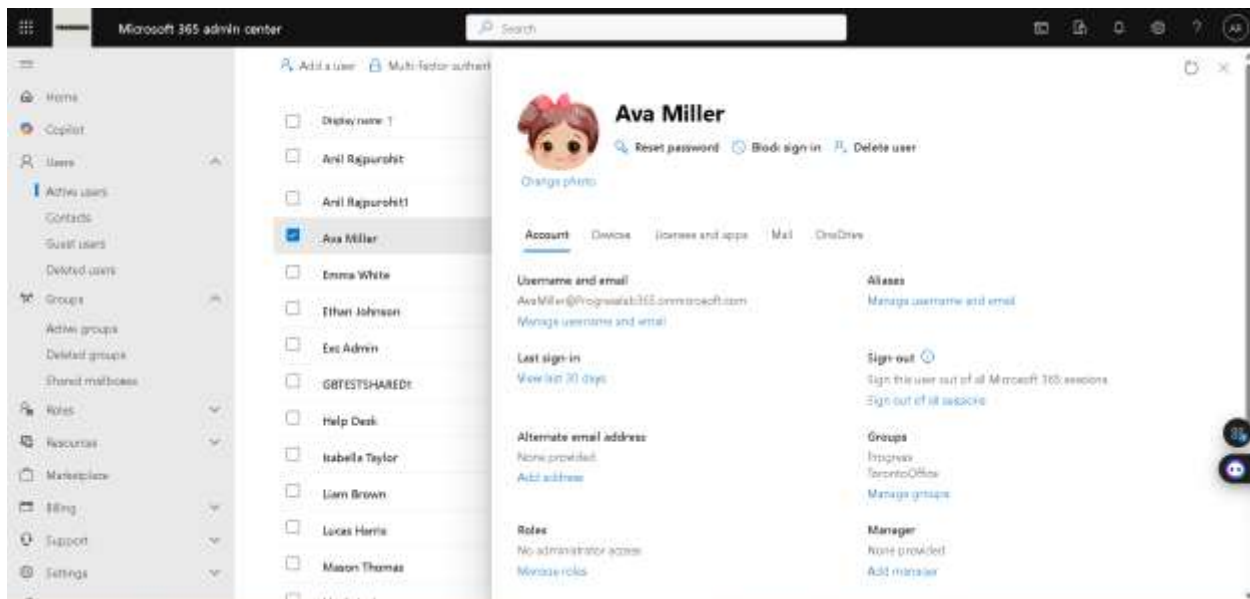
Step 6: Lets upload profile pictures for new user's, make a folder that contains all the pictures in .jpg format.



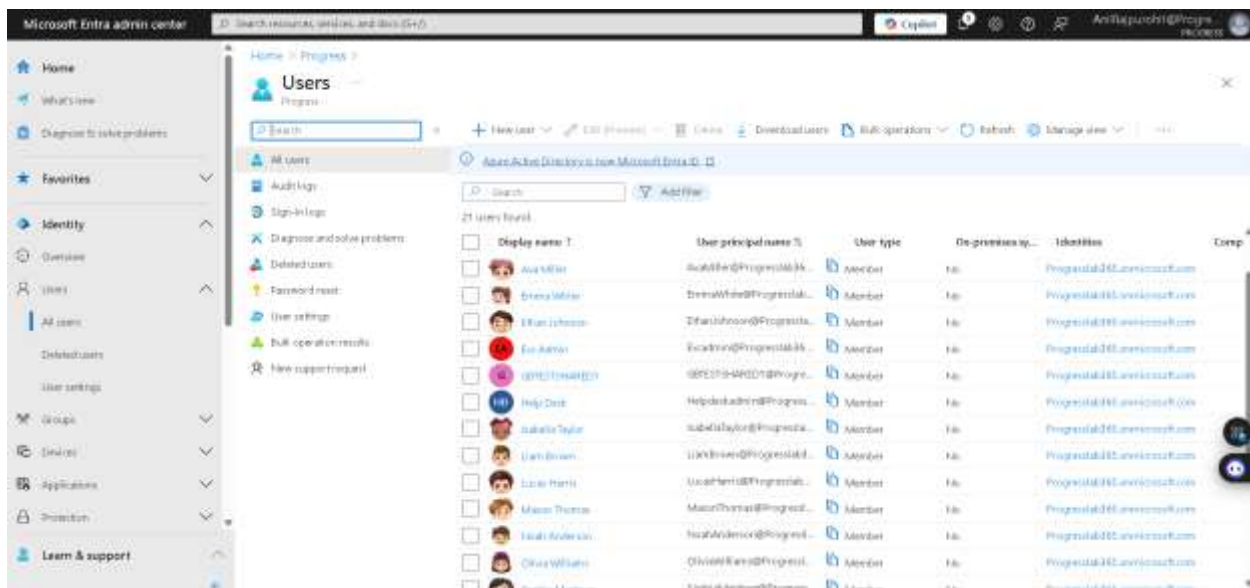
Step 7: Wanted to complete this task via PowerShell, but due to several errors as PowerShell was not accepting Set-UserPhoto. So, uploaded all new user's profile pictures manually from Microsoft 365 Admin center. First go to Users -> active users -> select the user then click in change photo.



Step 8: Successfully uploaded Ava Miller profile picture.



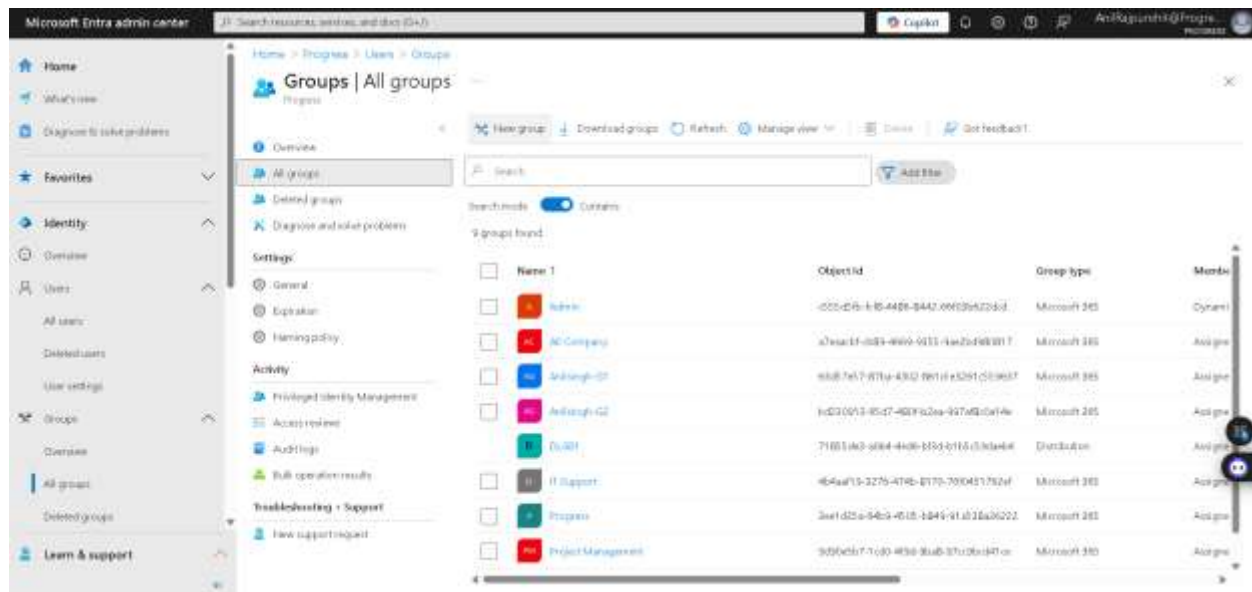
Step 9: To verify for all user's, go to Entra admin center -> Identity -> users -> all users. Profile picture for all new user's has been successfully added.



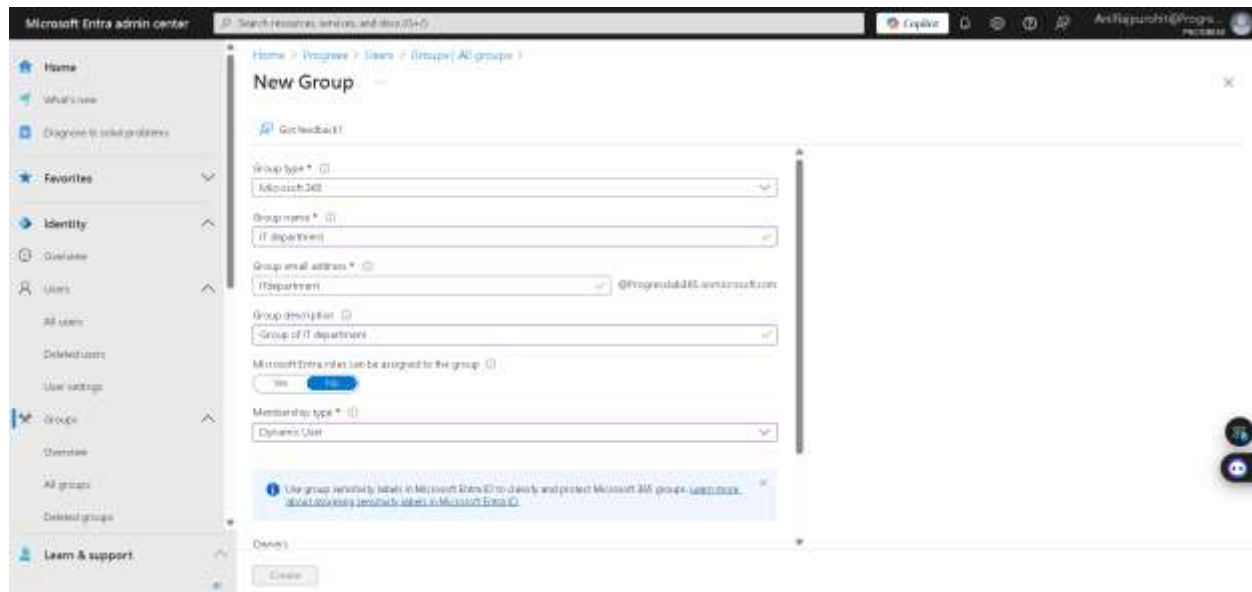
3. Create Office 365 Groups:

- Create three Office 365 groups for different departments: IT, HR, and Marketing.
- IT department group creation

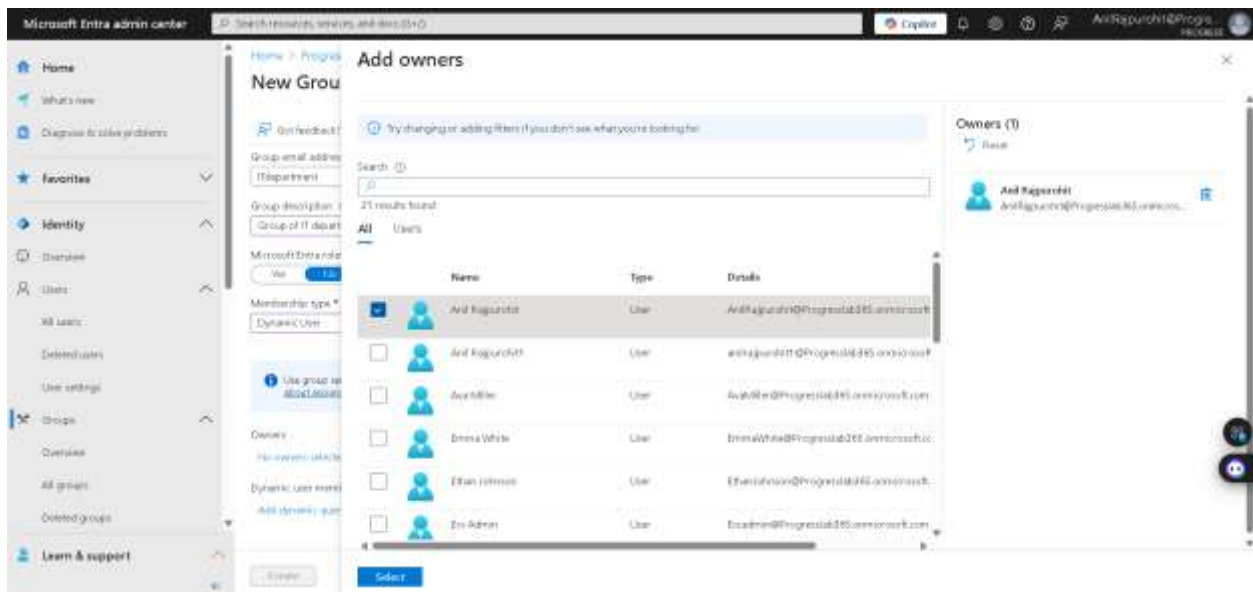
Step 1: From Entra admin center, go to identity -> Groups -> all groups -> new group.



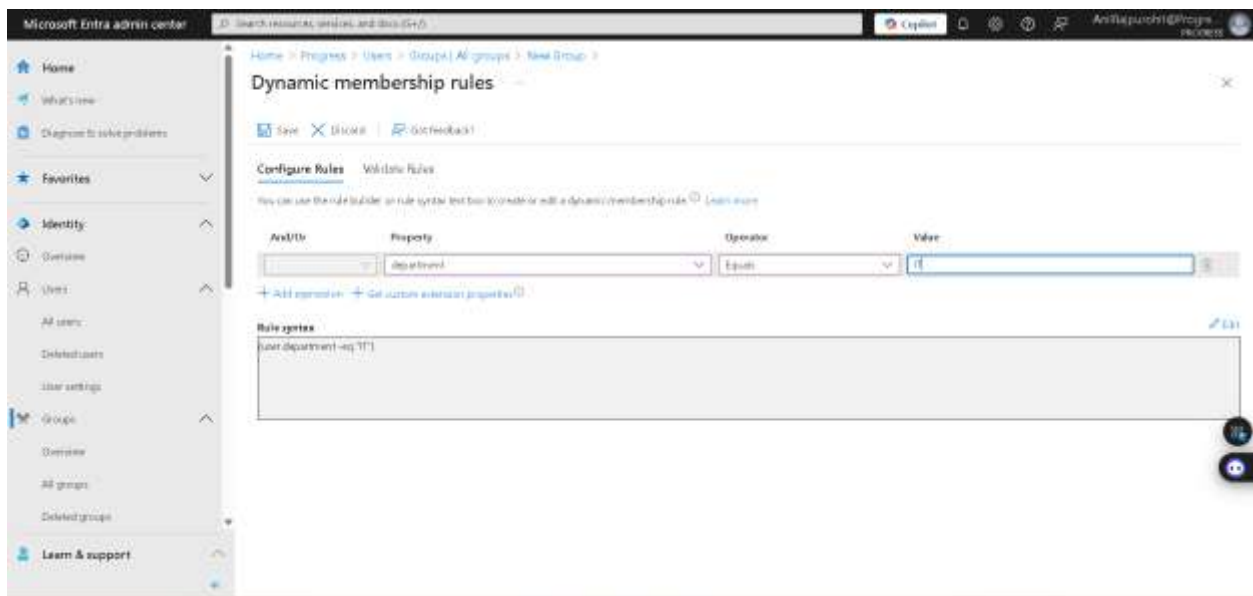
Step 2: Now fill all the details like Group type, name, email address, description, membership type. We selected membership types as dynamic as we want to add our users to their respected department group and we can do that by creating a dynamic group.



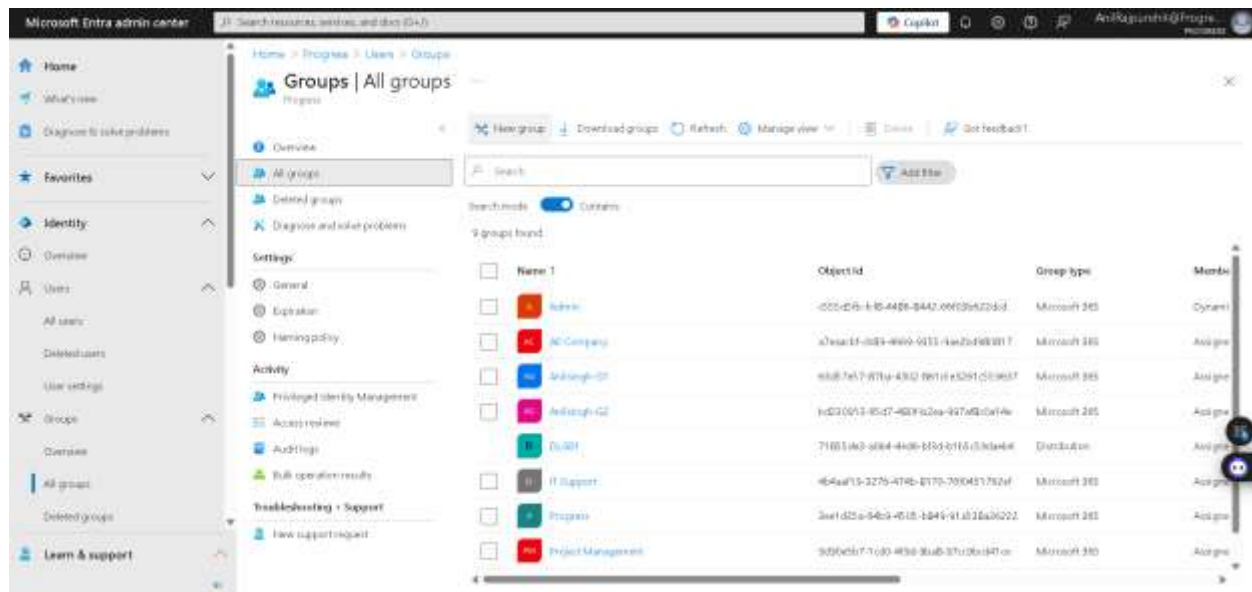
Step 3: Add global admin as group owners then click on select.



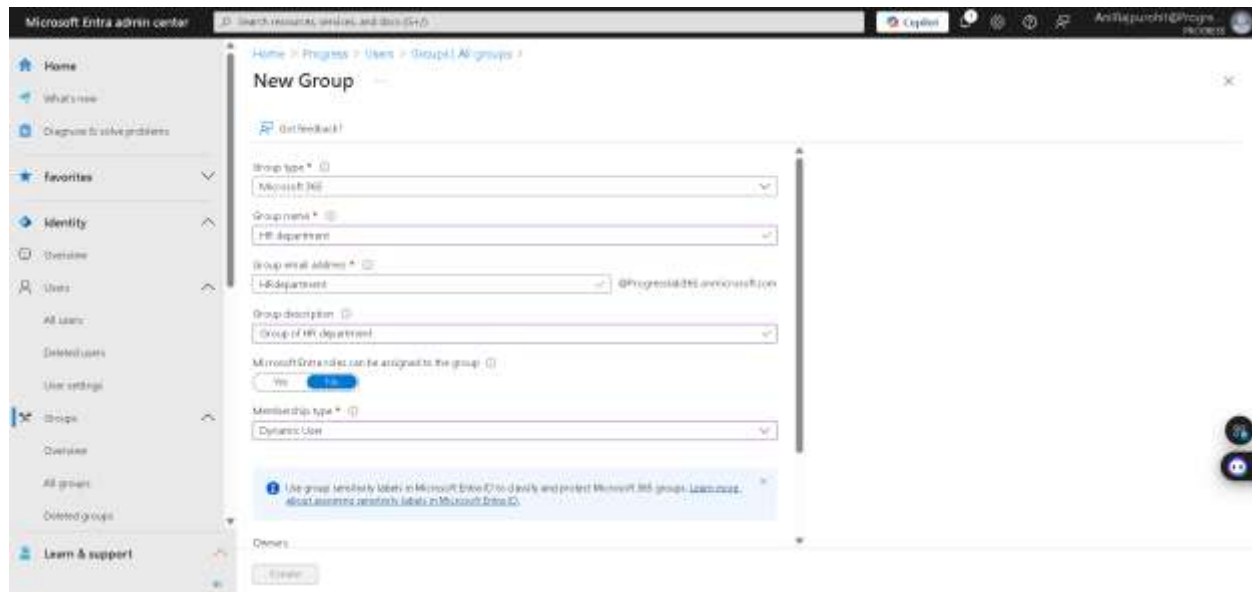
Step 4: Create a dynamic membership rule for automatically adding member by looking at their department value. Then click on Save.



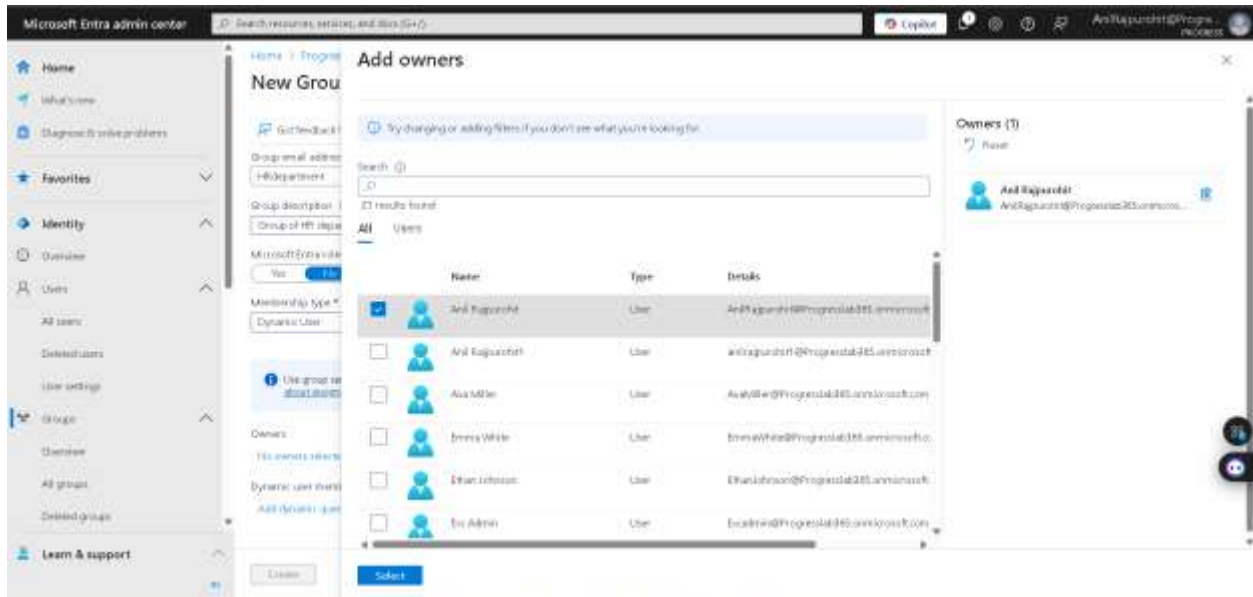
Step 5: Now, click on create to create our new Microsoft 365 group.



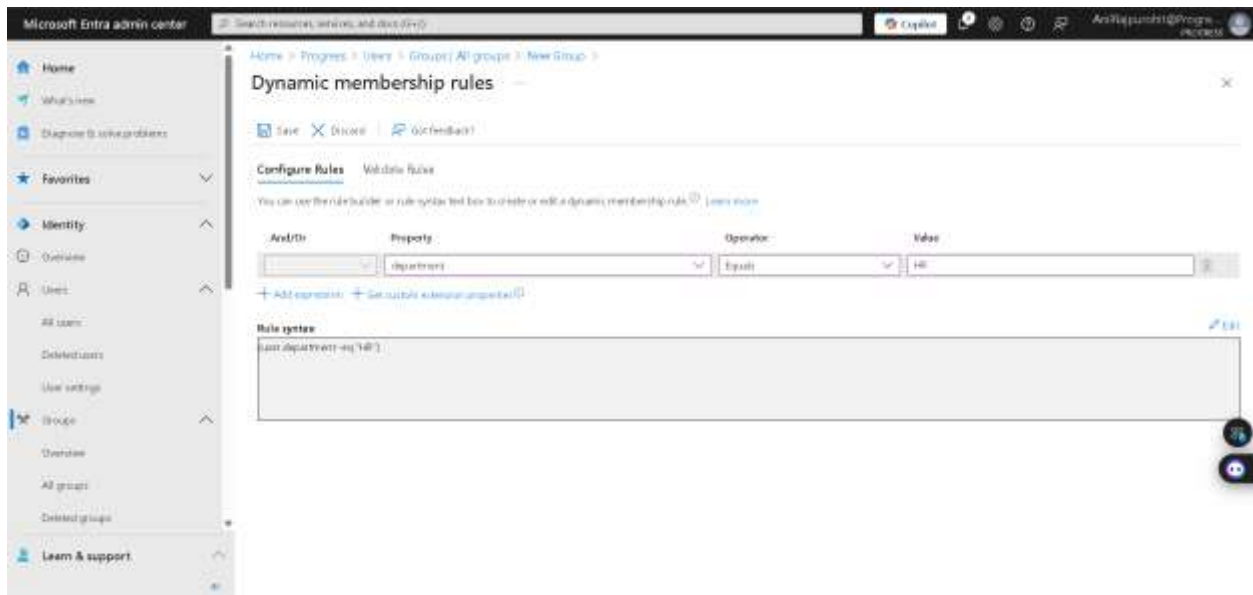
Step 2: Now fill all the details like Group type, name, email address, description, membership type. We selected membership types as dynamic as we want to add our users to their respected department group and we can do that by creating a dynamic group.



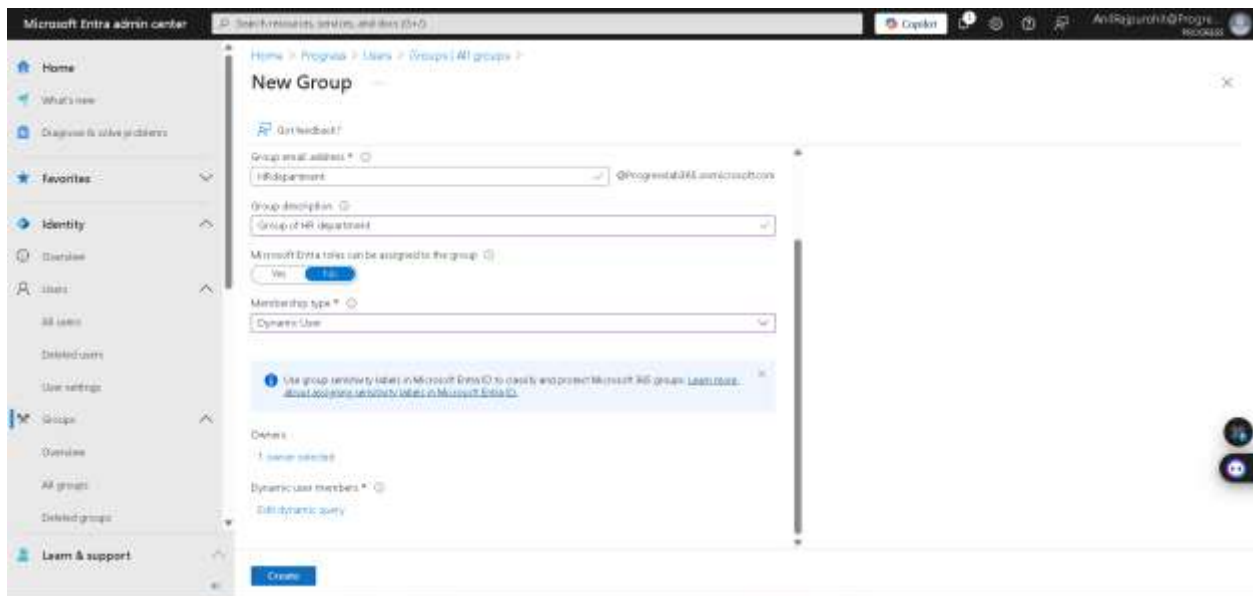
Step 3: Add global admin as group owners then click on select.



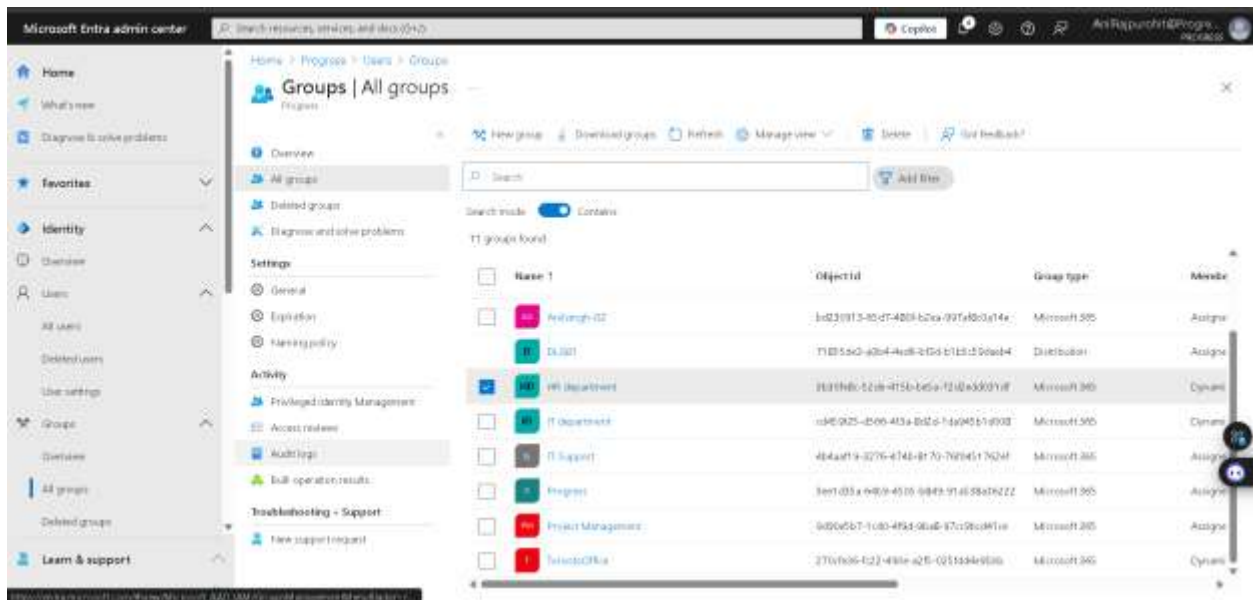
Step 4: Create a dynamic membership rule for automatically adding member by looking at their department value. Then click on Save.



Step 5: Now, click on create to create our new Microsoft 365 group.

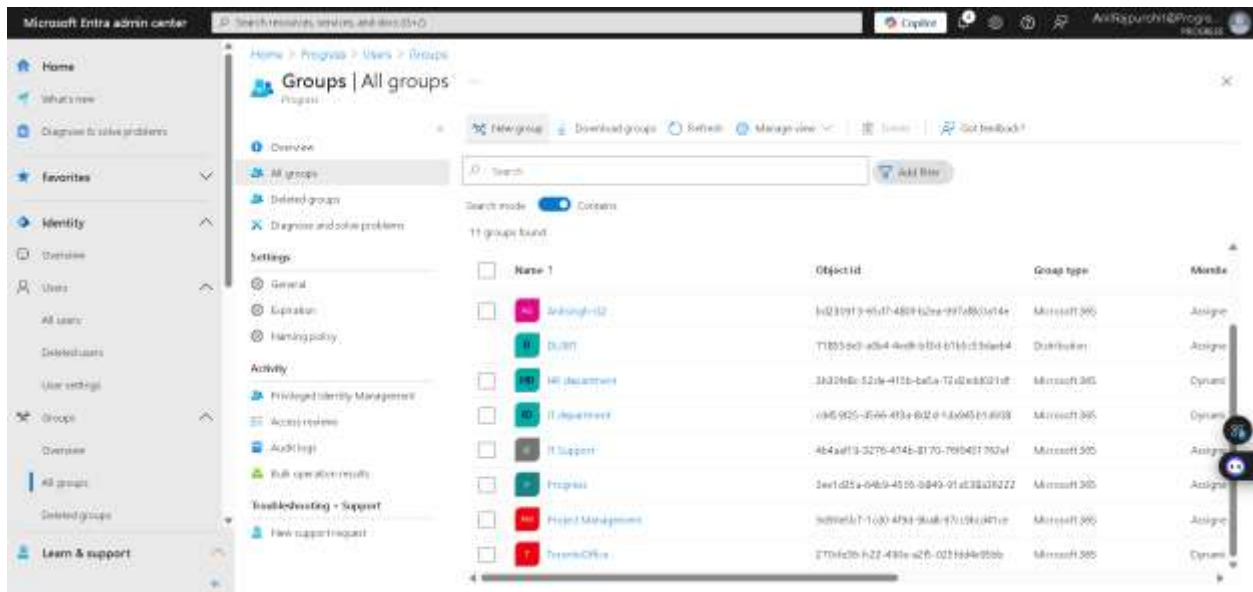


Step 6: Our group has been successfully created.

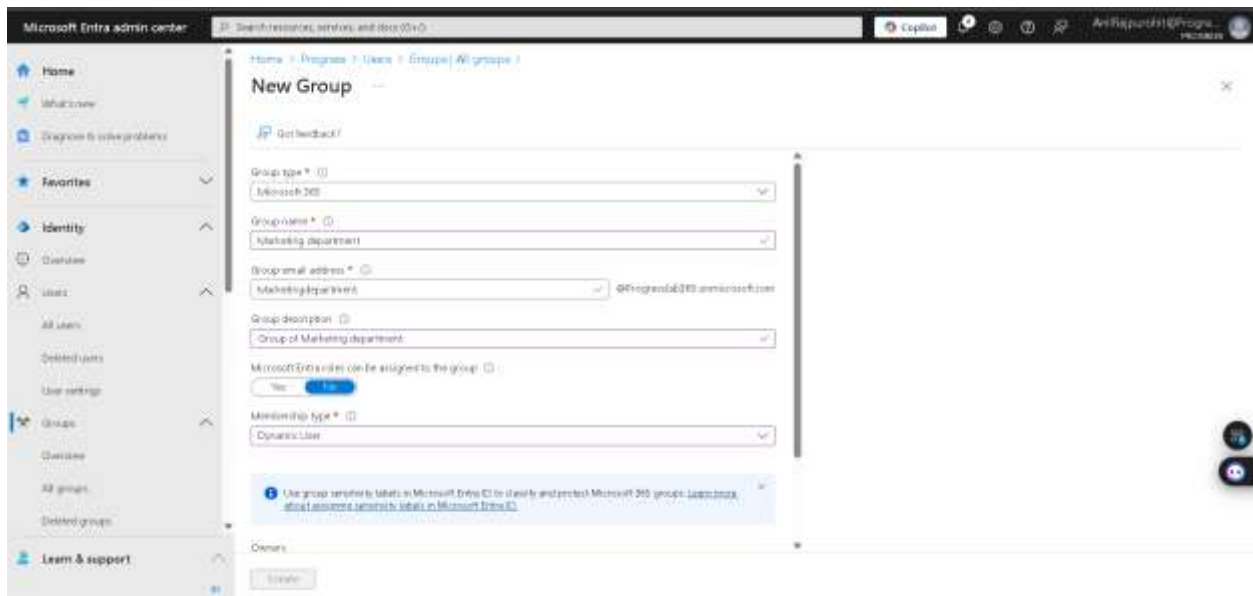


Marketing department group creation

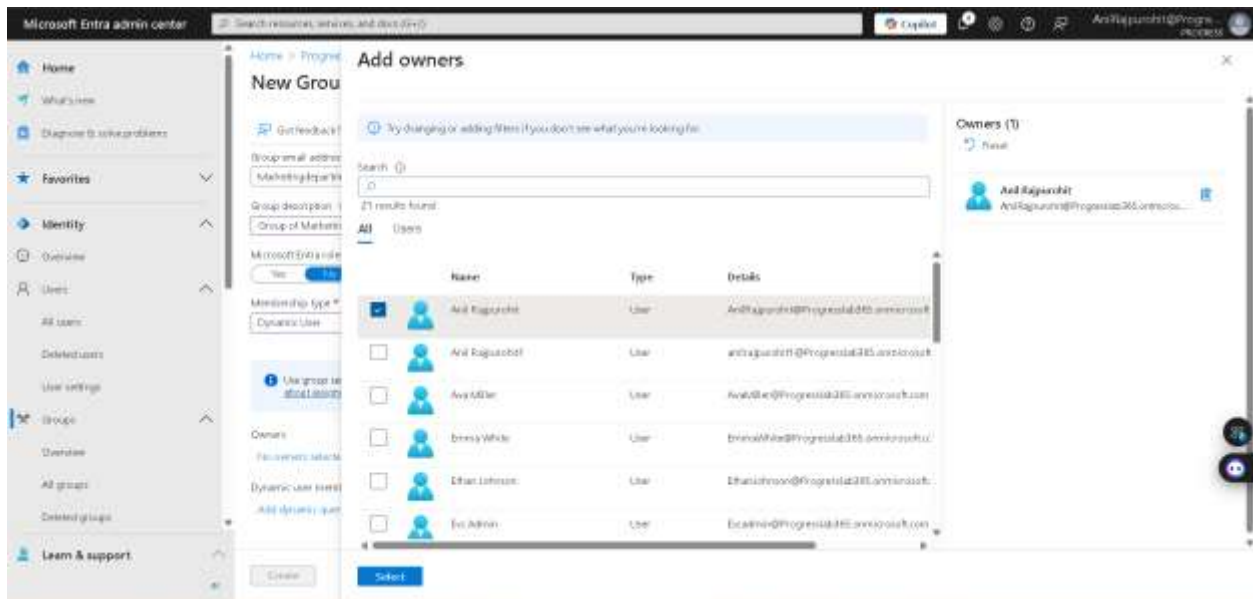
Step 1: From Entra admin center, go to identity -> Groups -> all groups -> new group.



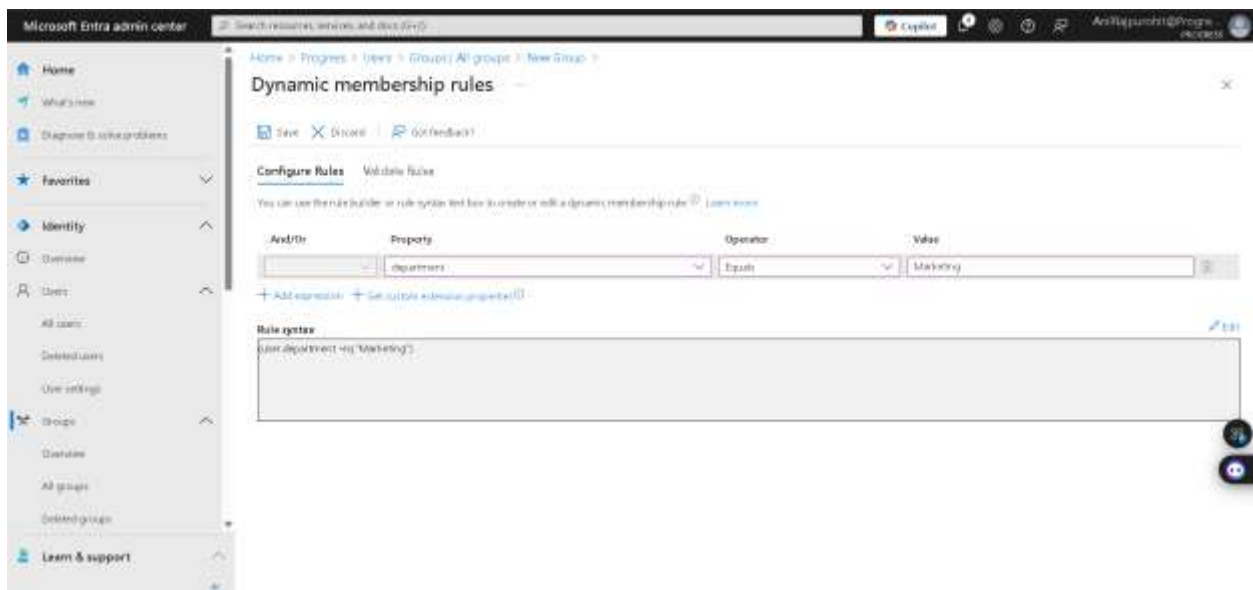
Step 2: Now fill all the details like Group type, name, email address, description, membership type. We selected membership types as dynamic as we want to add our users to their respected department group and we can do that by creating a dynamic group.



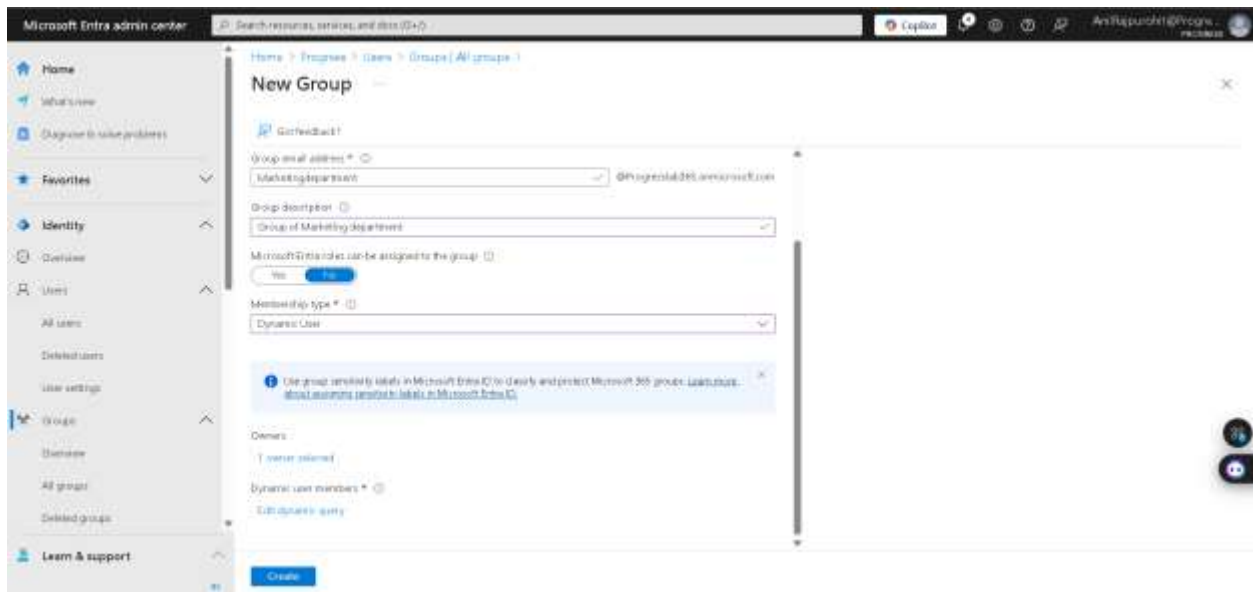
Step 3: Add global admin as group owners then click on select.



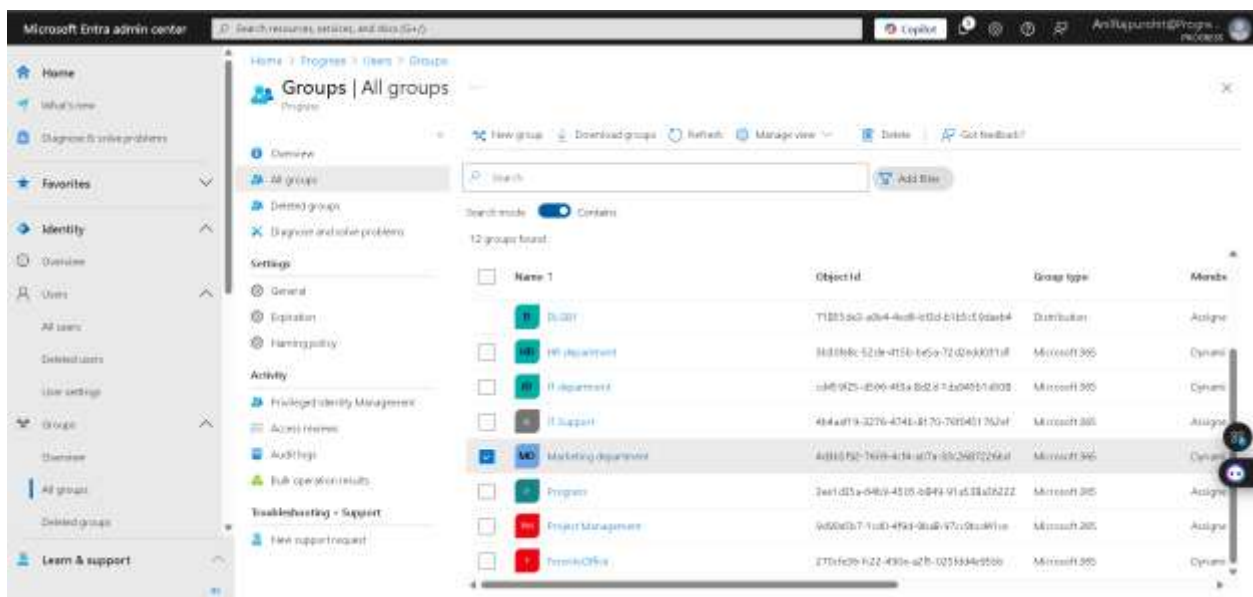
Step 4: Create a dynamic membership rule for automatically adding member by looking at their department value. Then click on Save.



Step 5: Now, click on create to create our new Microsoft 365 group.



Step 6: Our group has been successfully created.

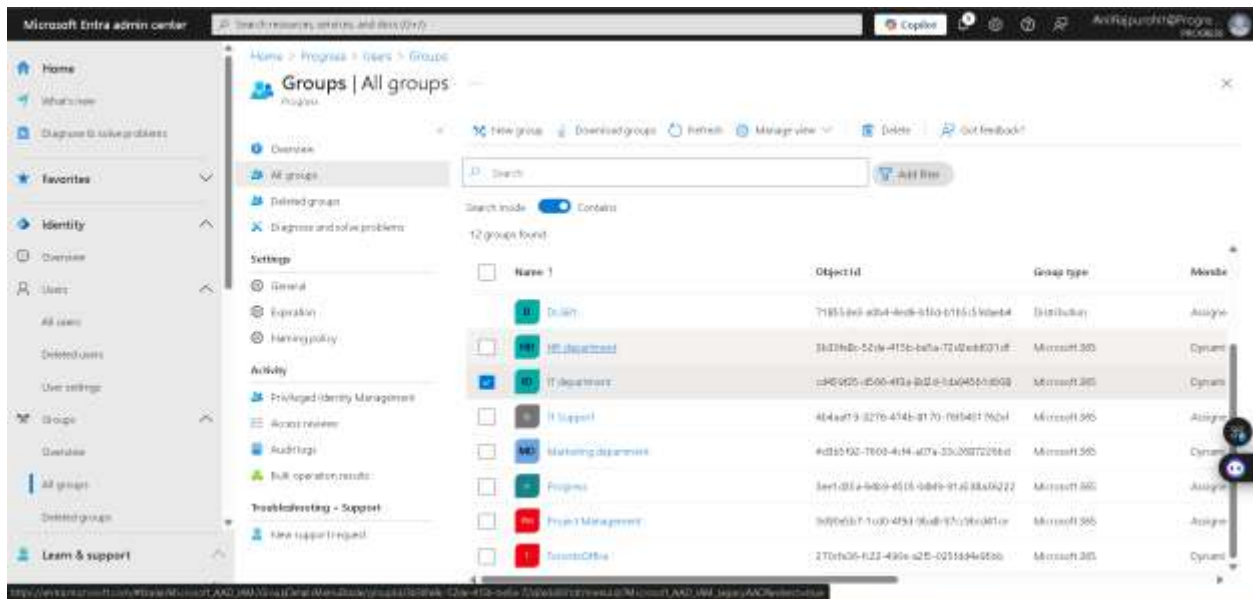


- Add users to their respective groups.

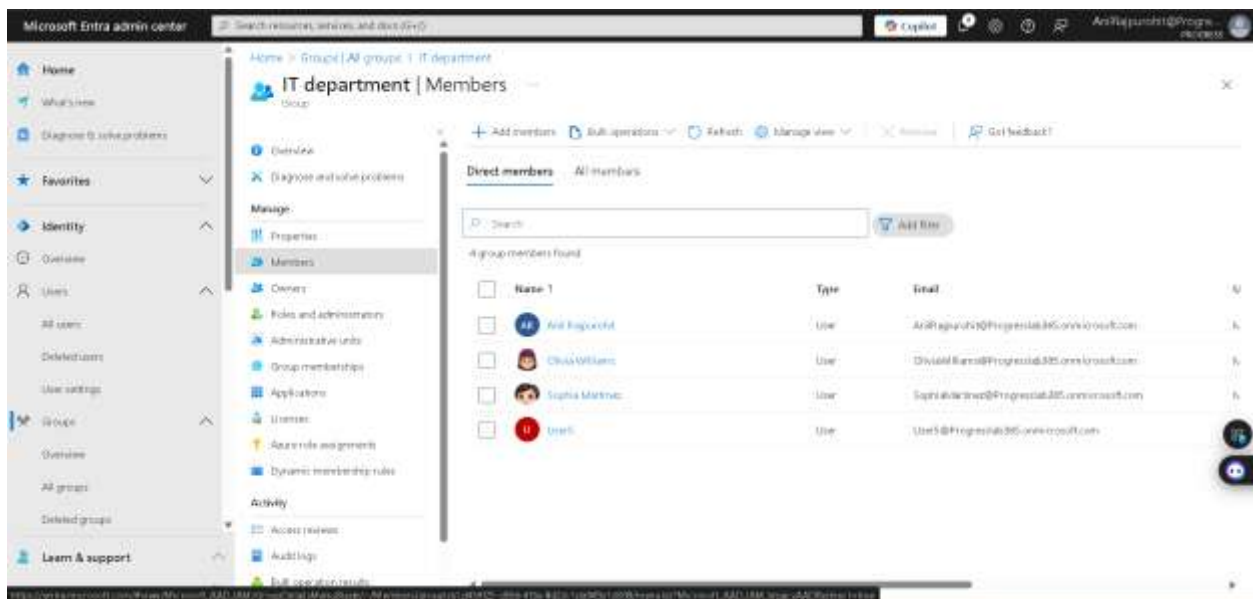
For IT department group

Step 1: As we created all the groups as dynamic group and used query for adding them to respected groups by looking at their departments.

To check first go to Entra admin center -> Identity -> groups -> all groups. Select the target group e.g. IT department.



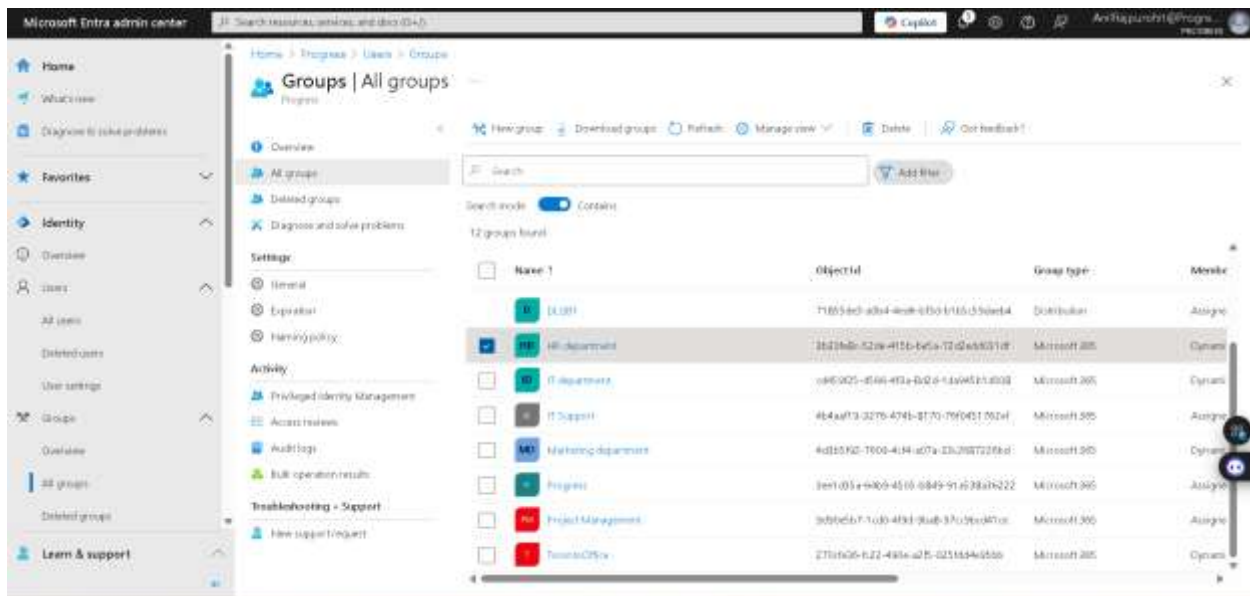
Step 2: In IT department group, under members we can see all the users got updated automatically based on their department.



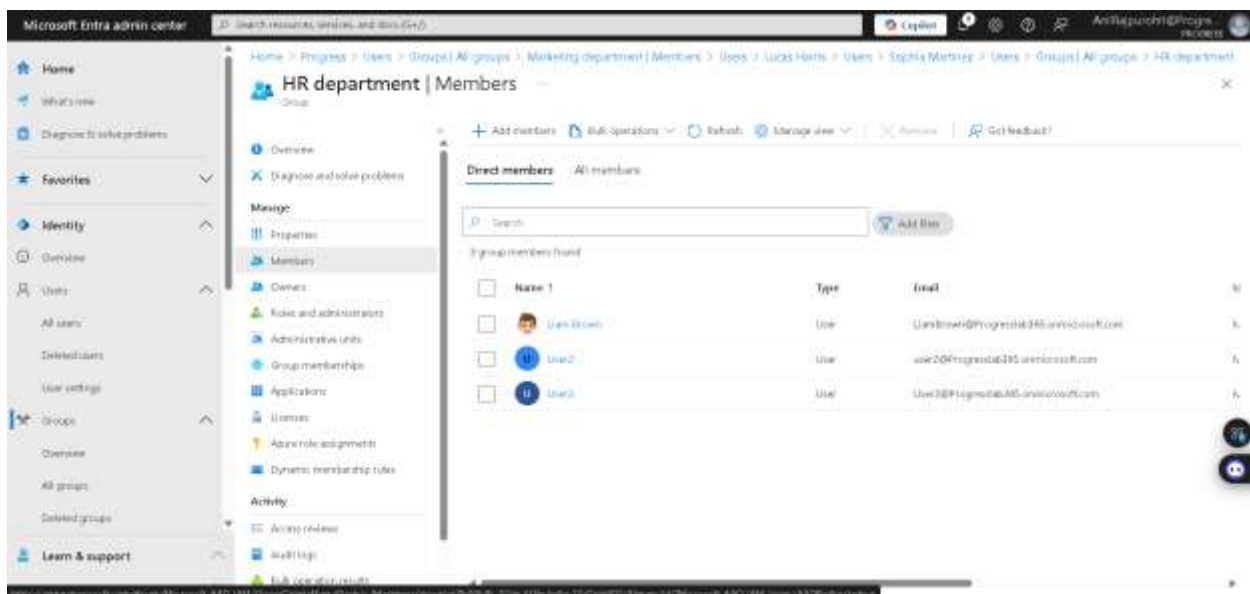
For HR department group

Step 1: As we created all the groups as dynamic group and used query for adding them to respected groups by looking at their departments.

To check first go to Entra admin center -> Identity -> groups -> all groups. Select the target group e.g. HR department.



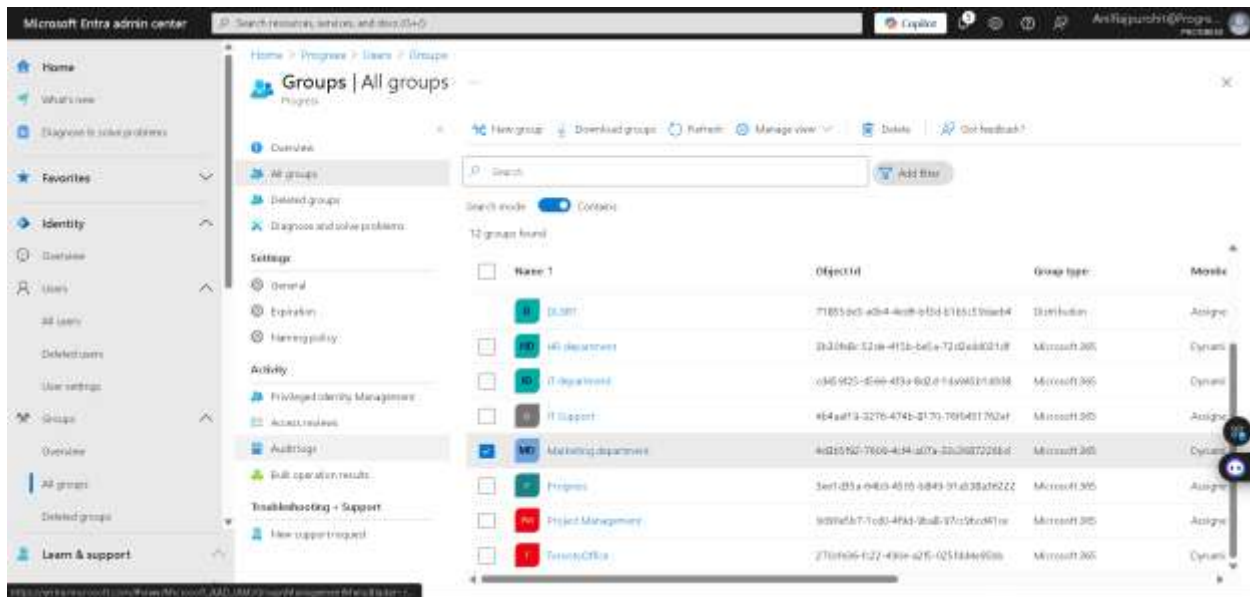
Step 2: In HR department group, under members we can see all the users got updated automatically based on their department.



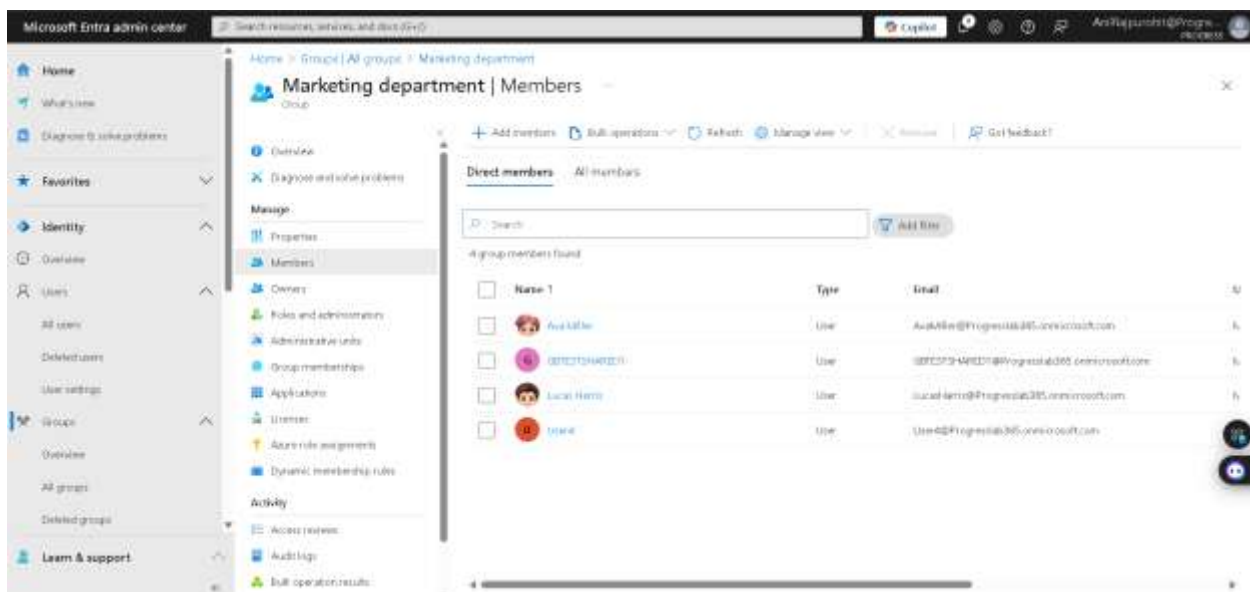
For Marketing department group

Step 1: As we created all the groups as dynamic group and used query for adding them to respected groups by looking at their departments.

To check first go to Entra admin center -> Identity -> groups -> all groups. Select the target group e.g. Marketing department.



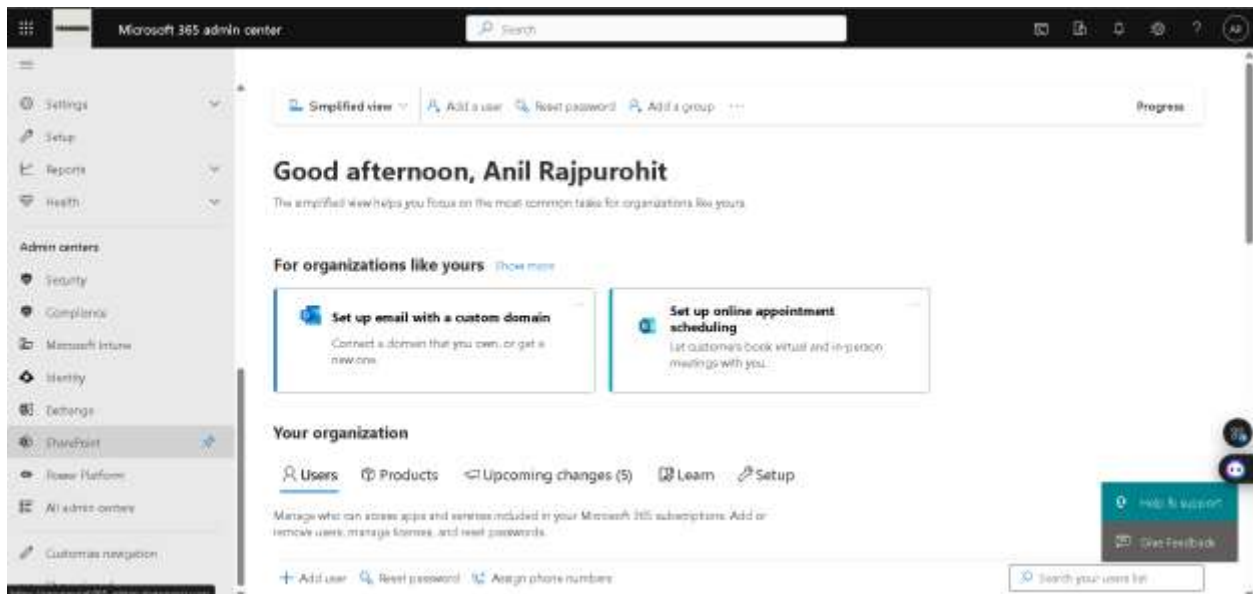
Step 2: In Marketing department group, under members we can see all the users got updated automatically based on their department.



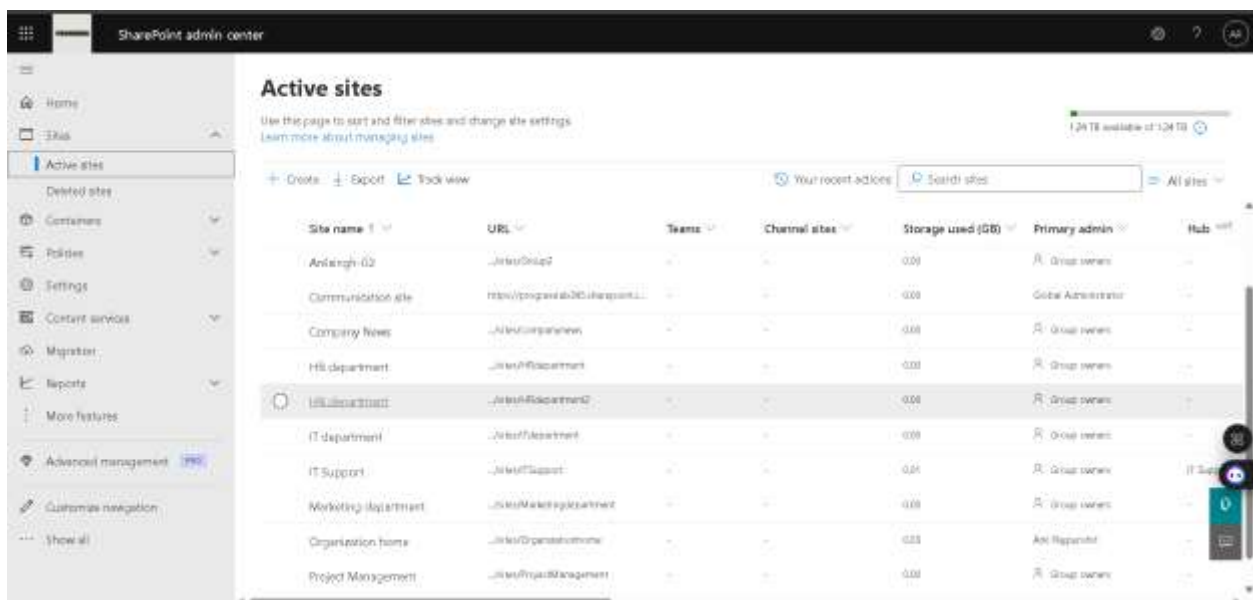
4. Configure User Permissions:

- Assign specific permissions to the HR group to access sensitive HR documents in SharePoint.

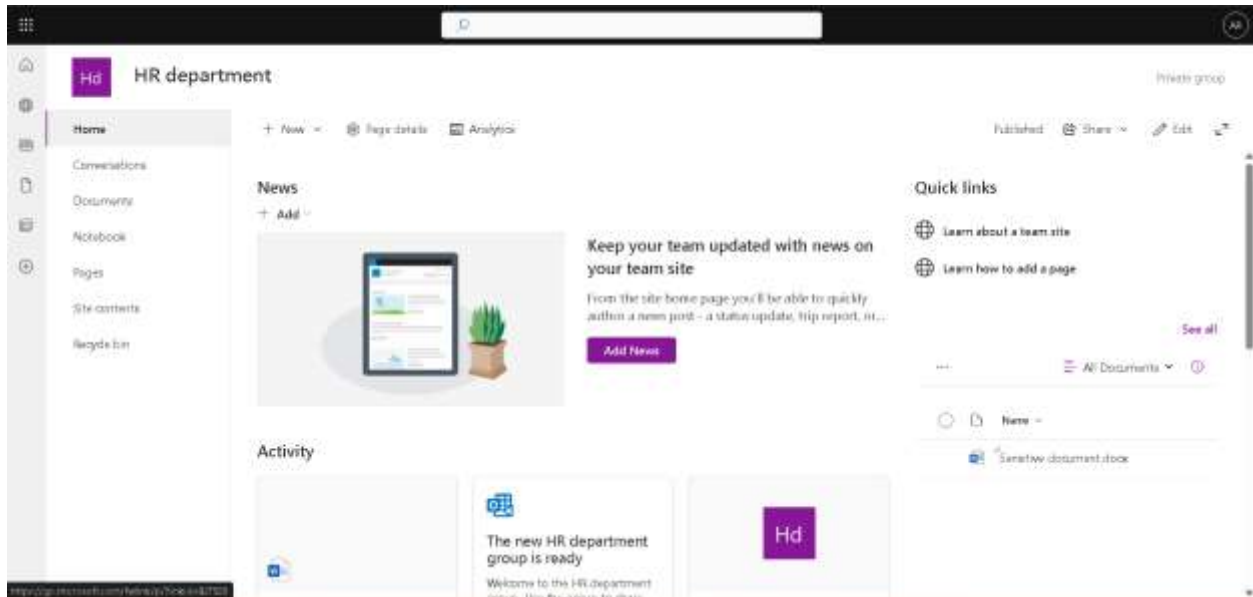
Step 1: To assign HR group access to sensitive HR document in SharePoint, from Microsoft 365 admin center under admin centers -> SharePoint.



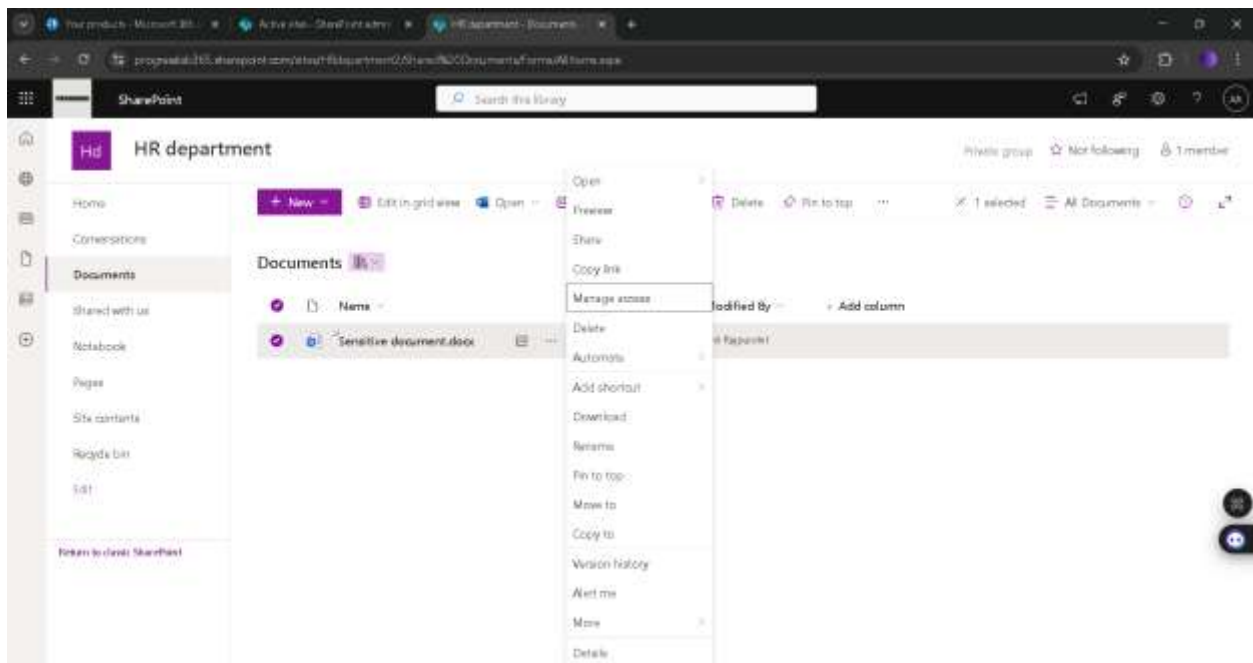
Step 2: From SharePoint admin center, sites -> active sites -> HR department.



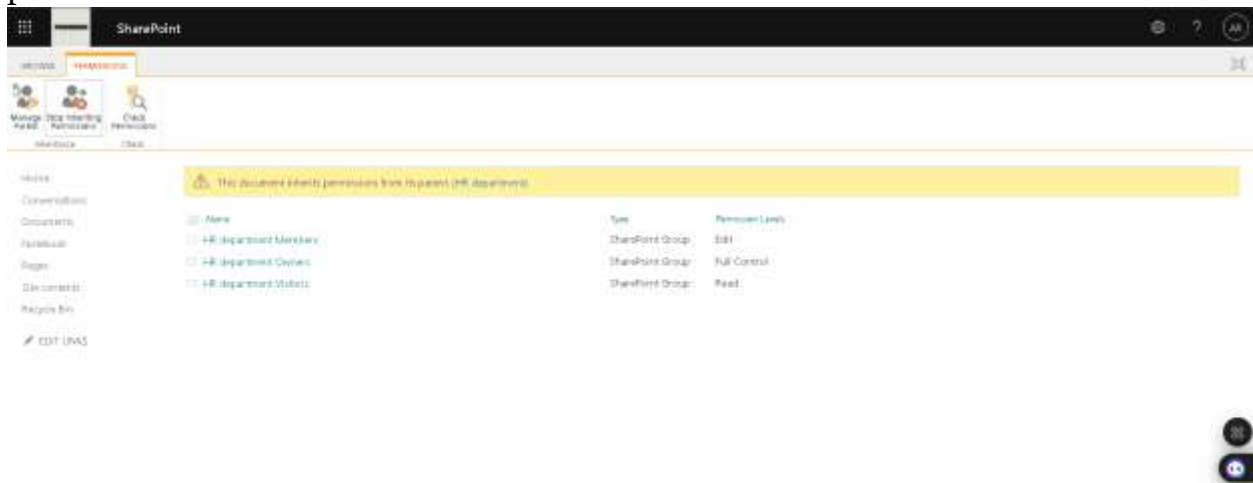
Step 3: To manage the sensitive document, click on Documents.



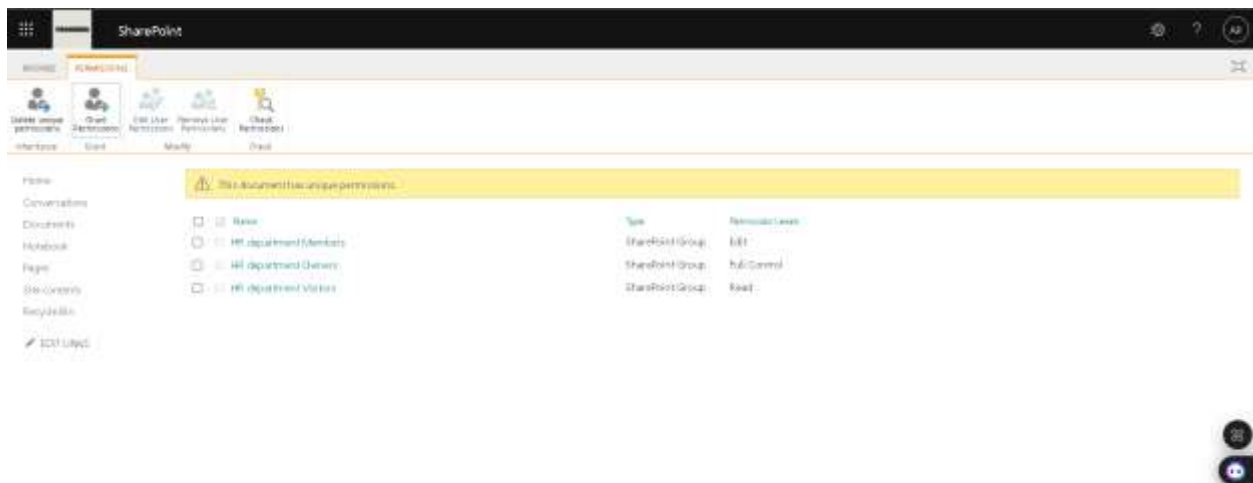
Step 4: In documents, select the respective sensitive HR file then click on three dots besides it. Then select manage access.



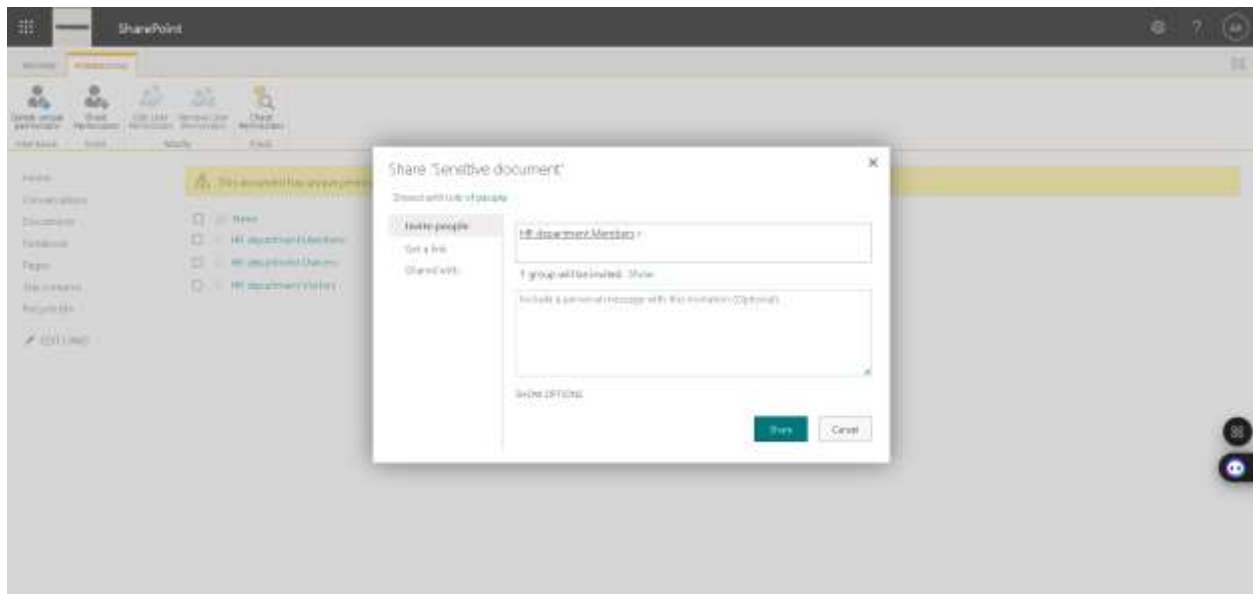
Step 5: First, click on stop inheriting permissions, so that we can add custom permissions to this file.



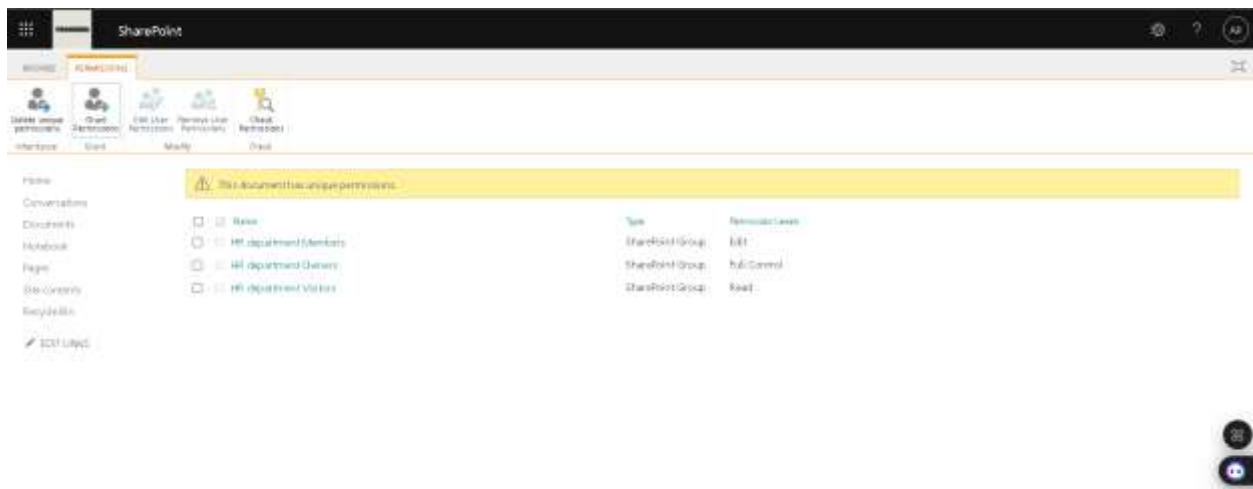
Step 6: Click on grant access to edit the permission of the file.



Step 7: Select HR department members, as we want to provide HR team access to sensitive HR documents then click on share.



Step 8: Now, we can see HR team have edit access to this sensitive HR file.



- Ensure the Marketing group has permission to create and manage Microsoft Teams.

Skipping this task, as we are using free trial version and it doesn't contain teams platform.

LEARNING & OPINION

We can now only assign licenses from admin center and not from Entra admin center now. We can assign licenses in one go to many users at a time. Also, from Entra admin center we can add users in bulk.

From PowerShell, we can do repetitive work in one go, e.g. updating user's details and uploading their profile pictures.

We can create groups with membership types as dynamic, so our users will be added automatically to their respected department group.

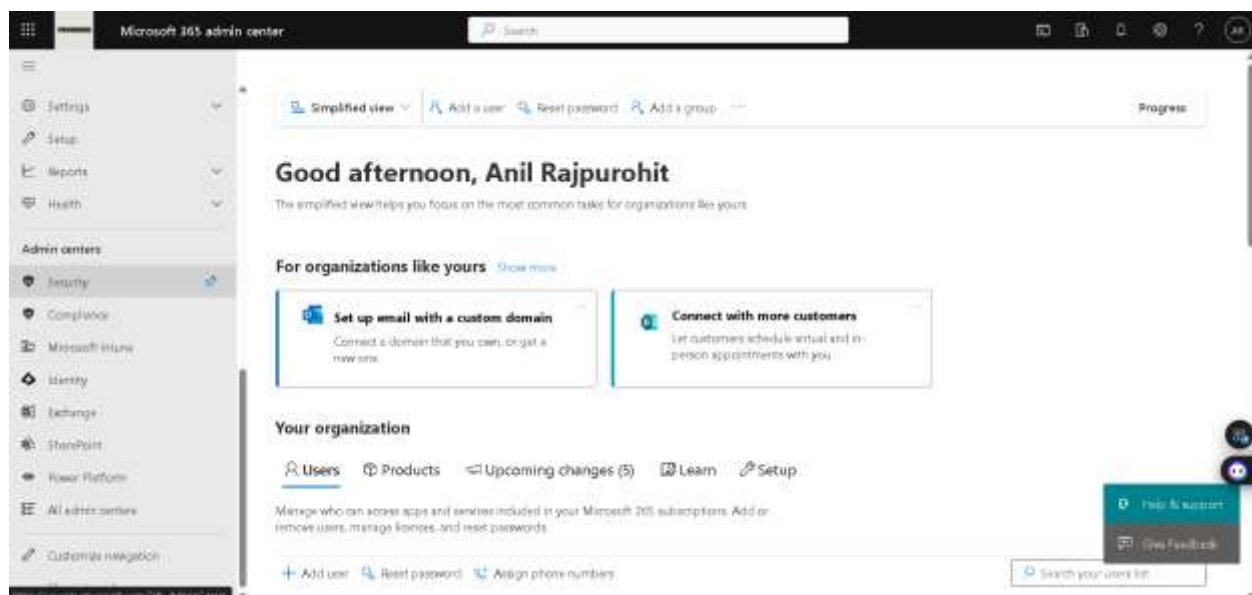
In SharePoint, for files and documents we can stop inheriting permissions, so that we can add custom permissions to that file.(If that file or directory is sensitive)

Task 2: Implementing Security Measures

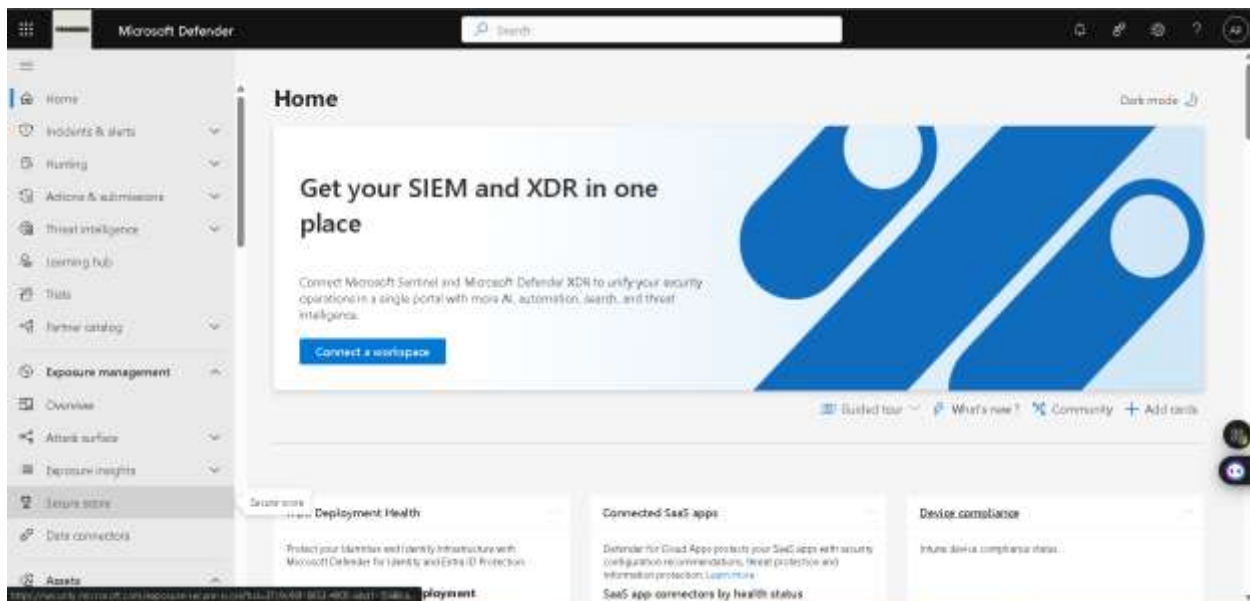
1. Set Up and Configure Microsoft Defender for Office 365:

- Access the MS Defender and navigate to Secure Score.

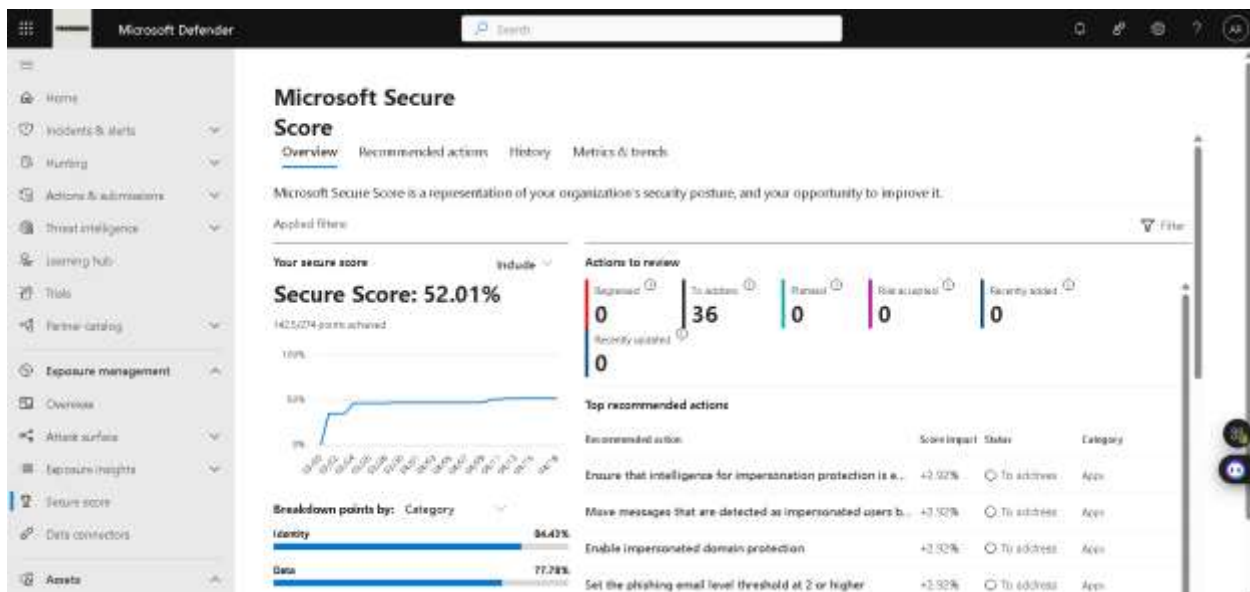
Step 1: First, from Microsoft 365 admin center under admin centers -> Security to access Microsoft defender.



Step 2: From Microsoft Defender, under Exposure management -> Secure score.

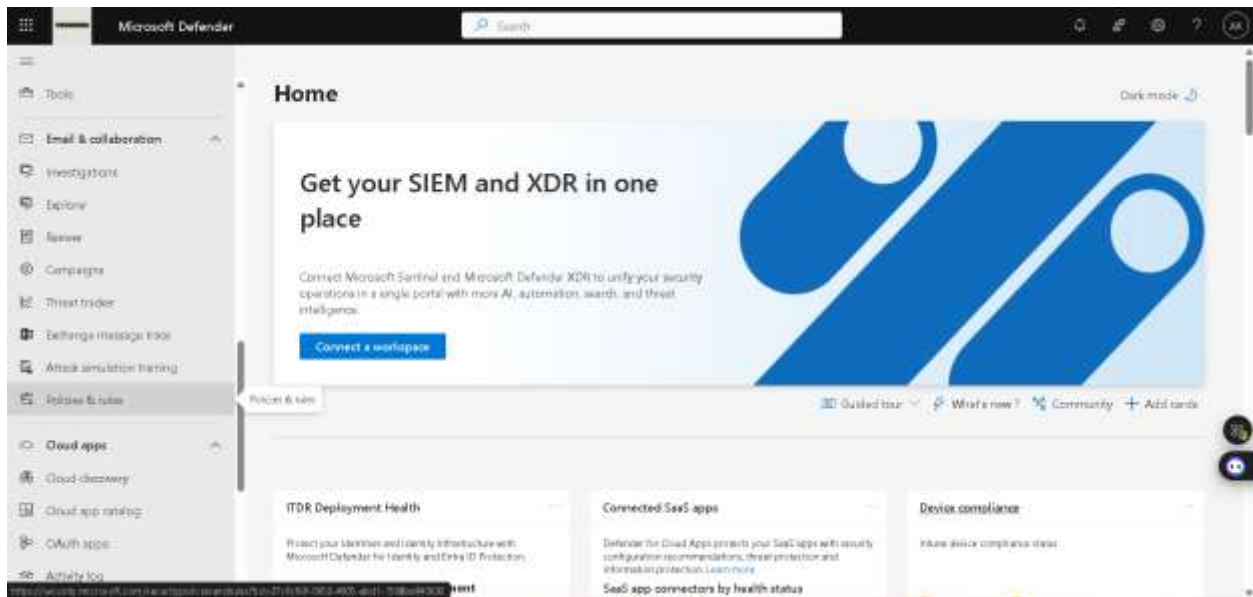


Step 3: We can view secure score for our organization here, our organization secure score currently only at 52.01% and healthy secure score is generally above 80%. We can complete recommended actions to increase our score.

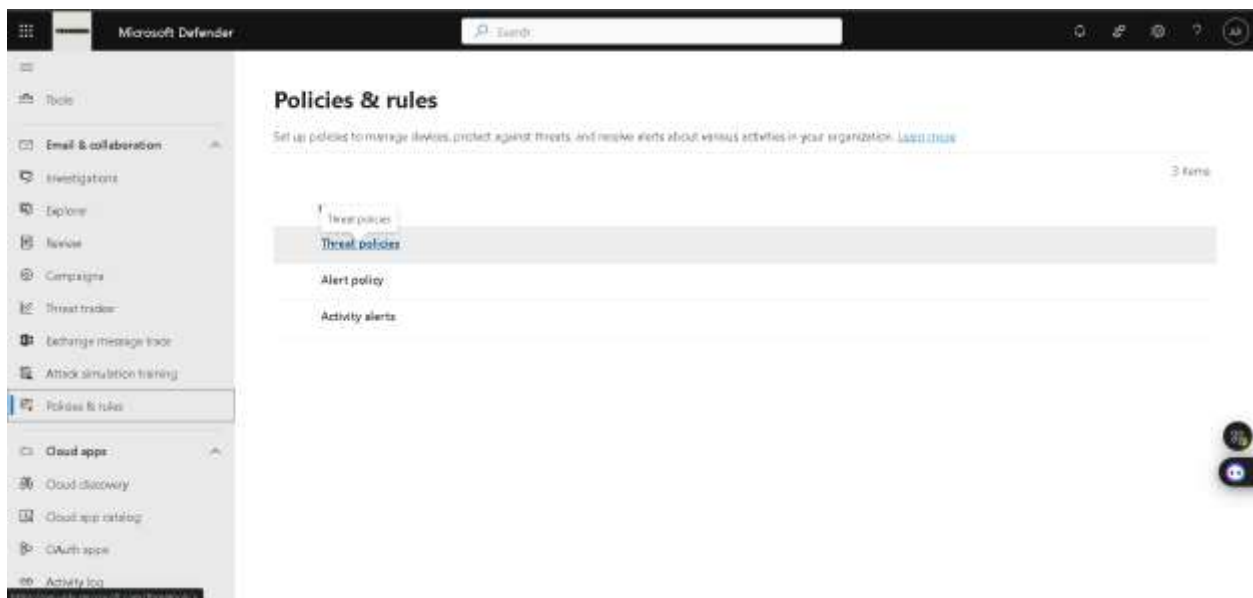


- Ensure that Safe Links and Safe Attachments have been enabled for all users.

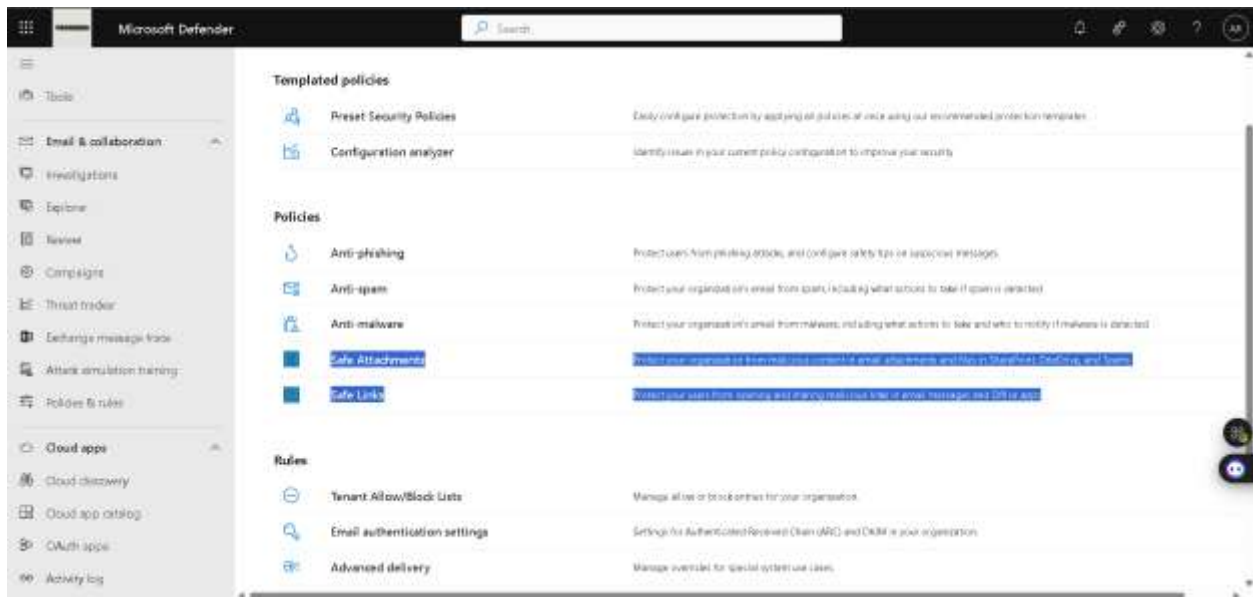
Step 1: From Microsoft Defender, under email & collaboration click on Policies & rules.



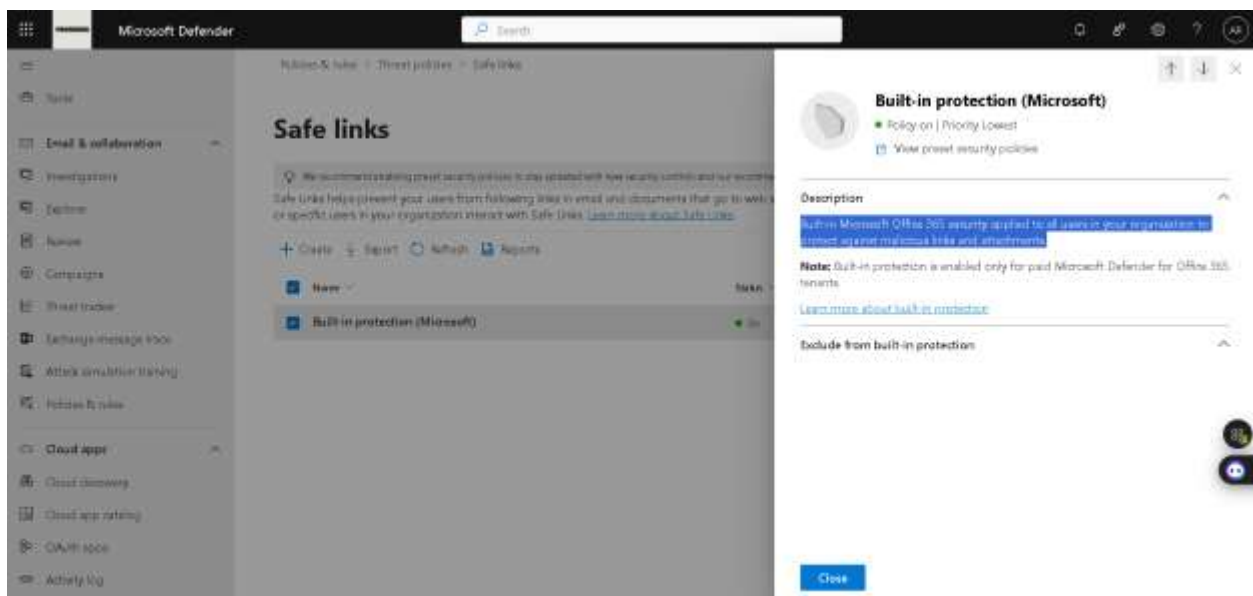
Step 2: Now, select Threat Policies.



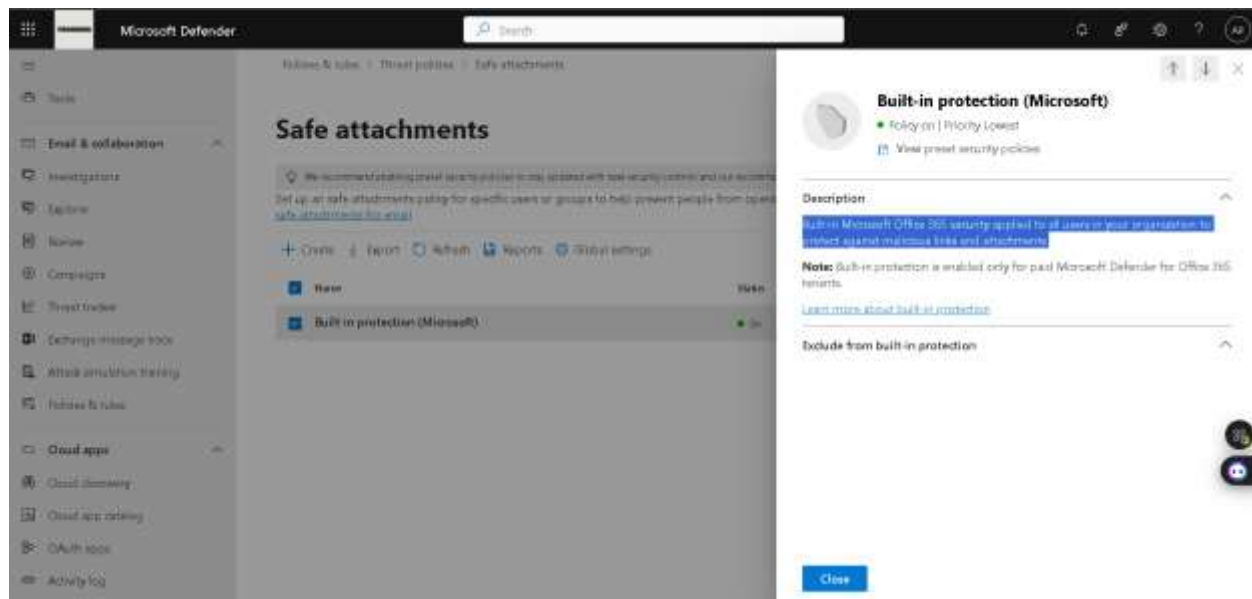
Step 3: We can see that for our organization both Safe attachments and safe links policies are active.



Step 4: To check detailed info of Safe links policy, click in safe links then built-in protection to view detailed info.

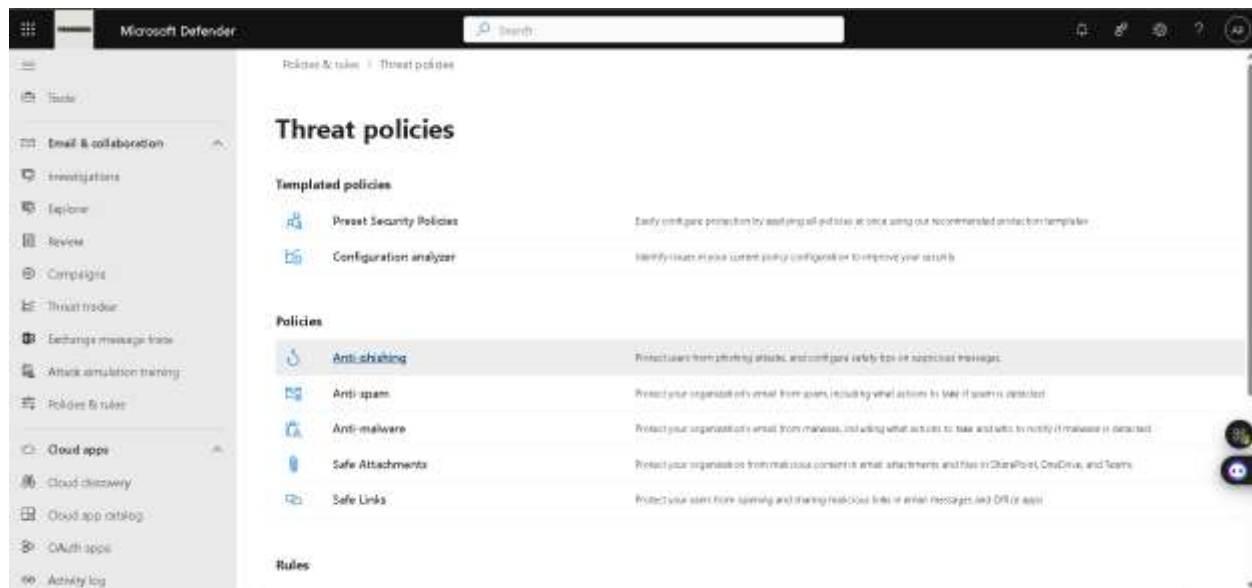


Step 5: To check detailed info of safe attachments policy, click in attachments then built-in protection to view detailed info.

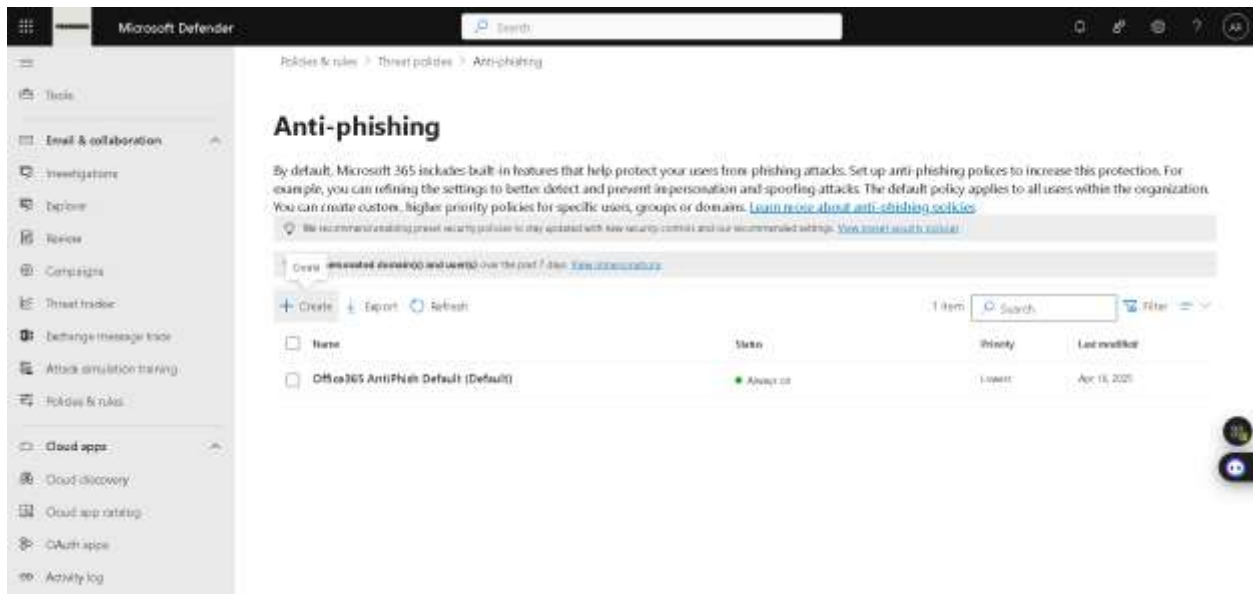


- Navigate to Policies and rules, then configure at least one policy to protect against phishing, malware, or spam.

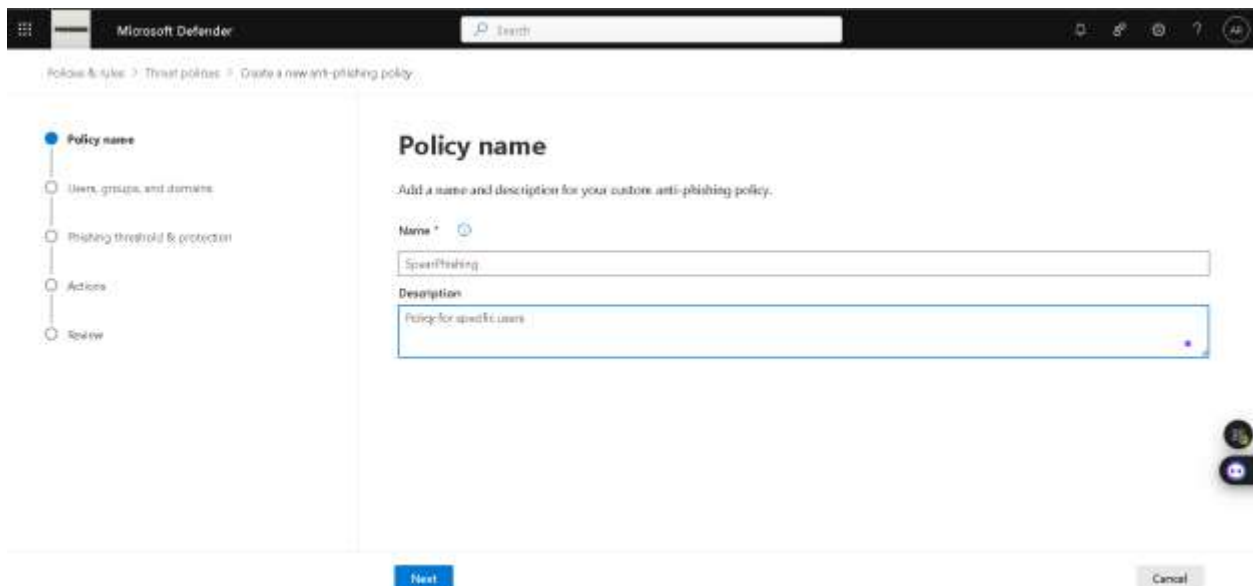
Step 1: To configure a policy, from Defender -> email & collaboration -> policies & rules -> threat policies -> Anti phishing. (As we are configuring this policy)



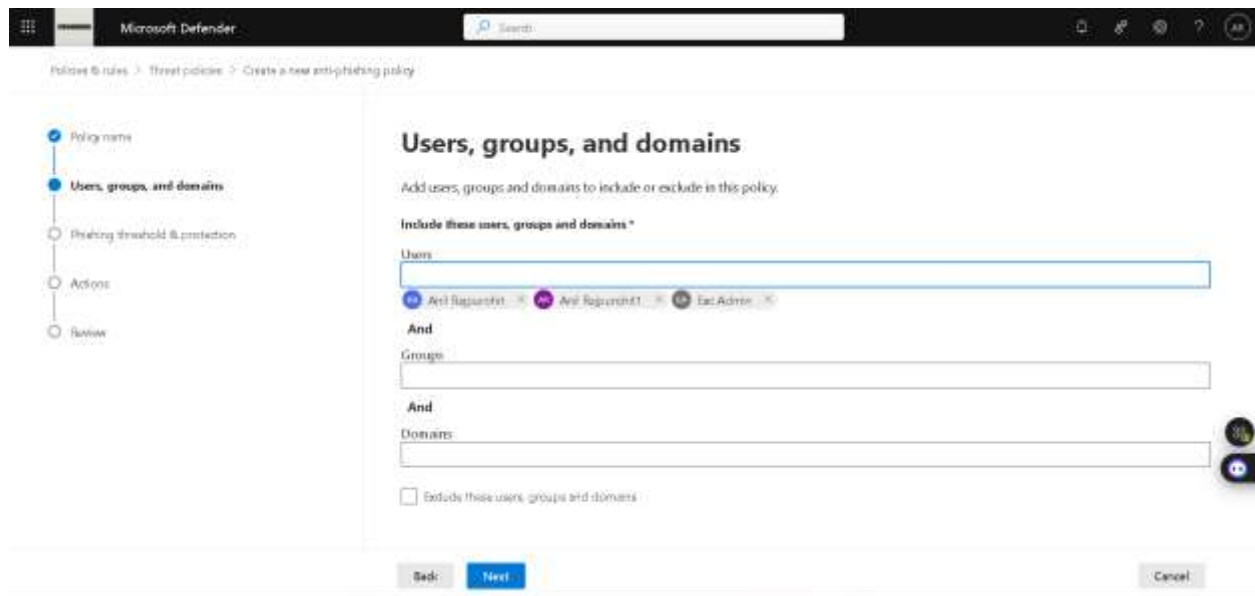
Step 2: In anti-phishing, click on create.



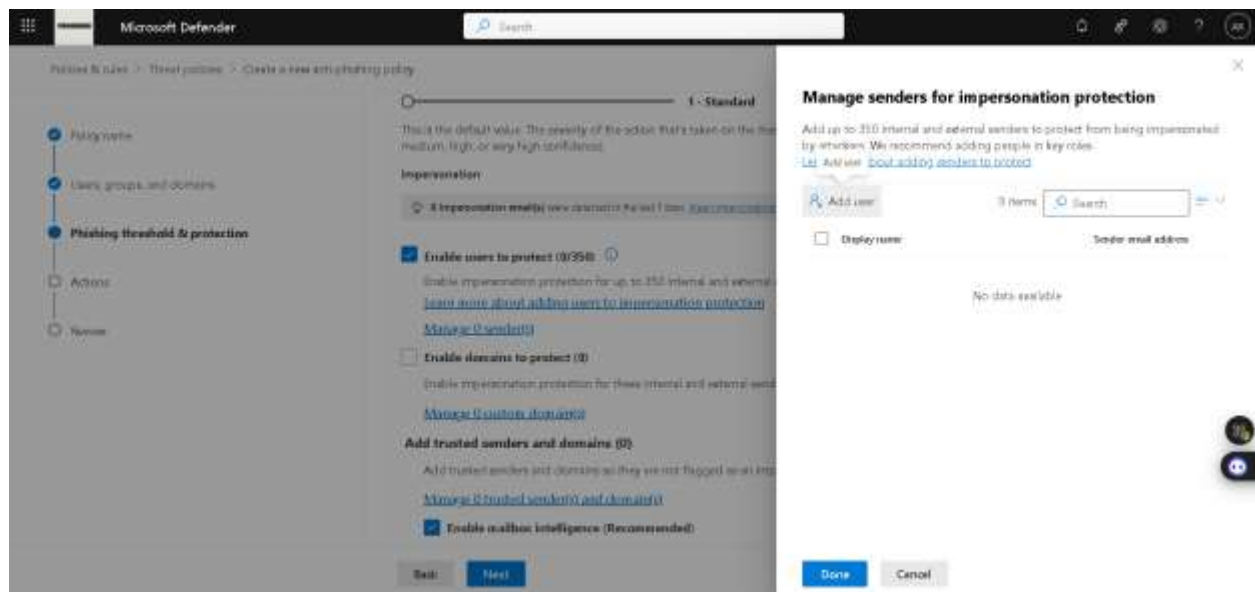
Step 3: As we already have Microsoft default anti-phishing policy, let's create more granular policy to protect specific sensitive users from phishing. Fill name and description of policy then Next.



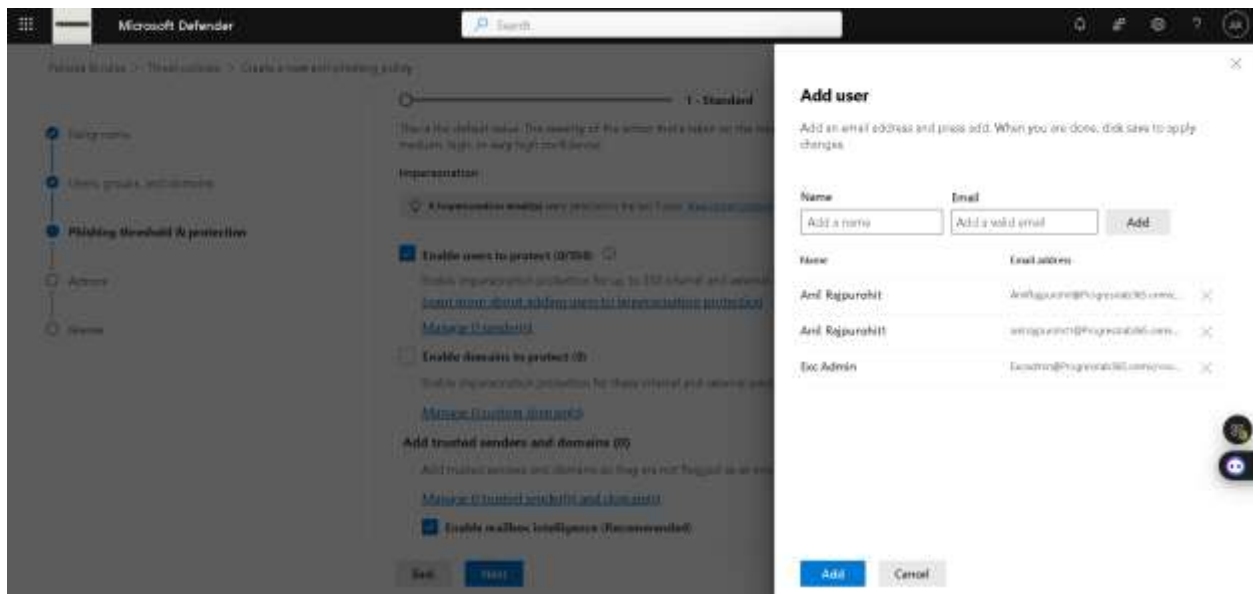
Step 3: Selected admins to include in this policy, as these are sensitive accounts. Then next.



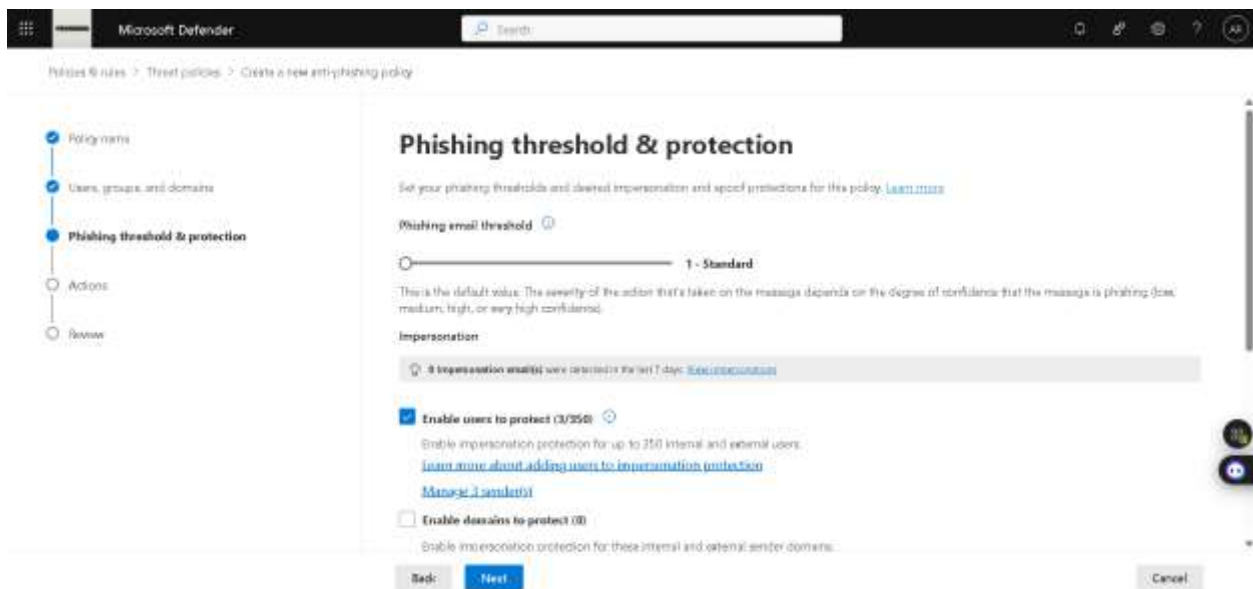
Step 4: Again select the users we want to protect from phishing attacks. Under Enable users to protect -> Manage 0 users -> then Add user.



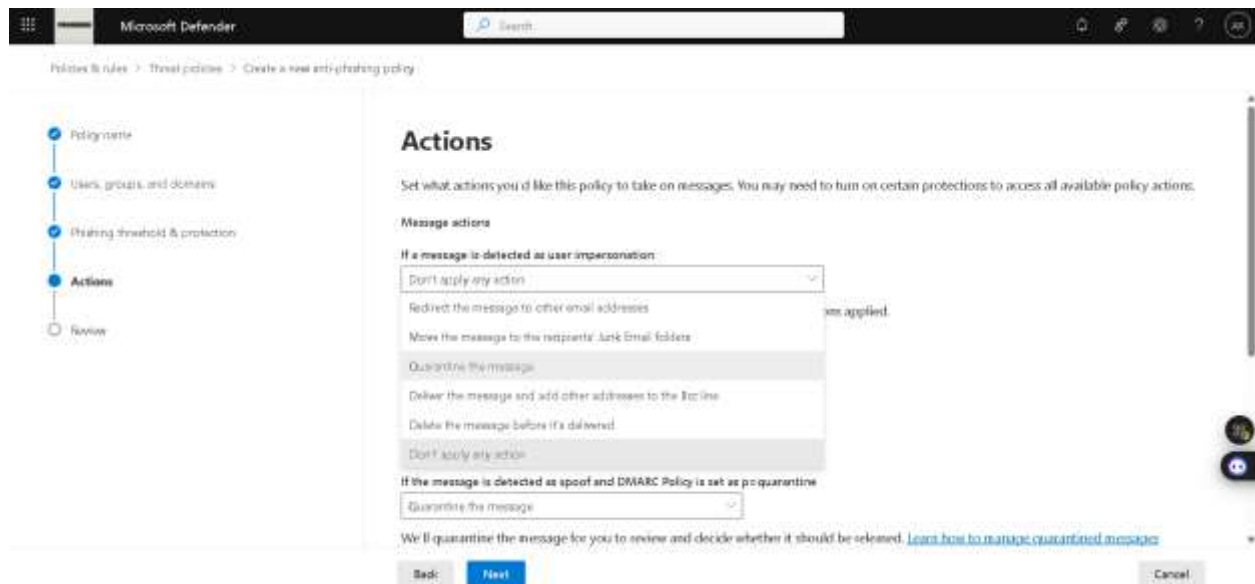
Step 5: Added all the admin accounts here. Then click on add.



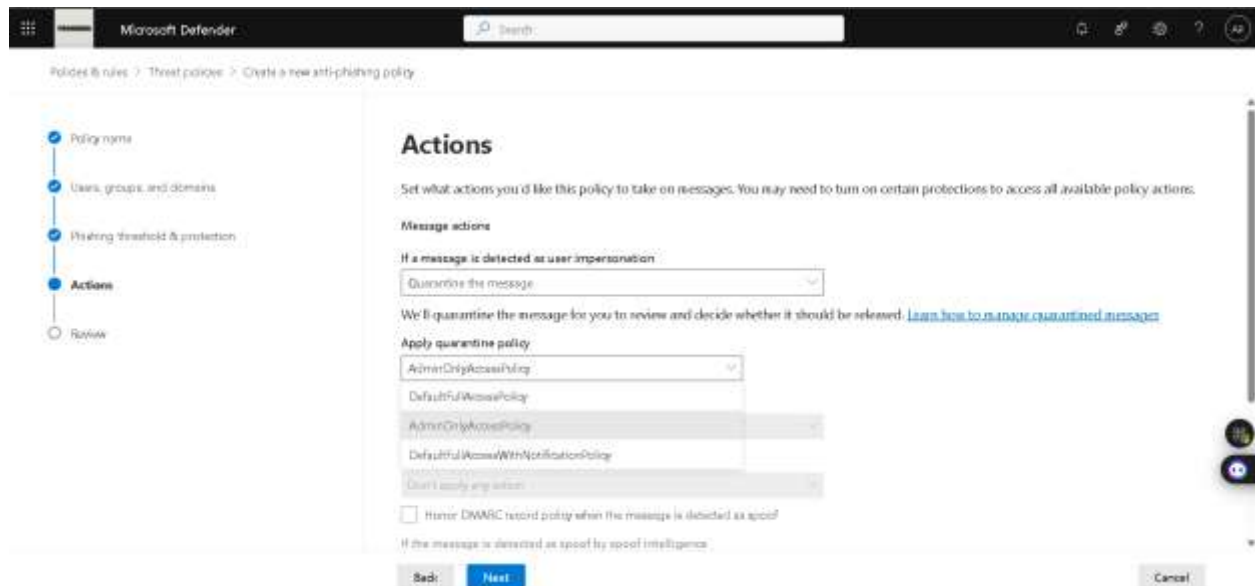
Step 6: We can see that our users has been selected, now click on next.



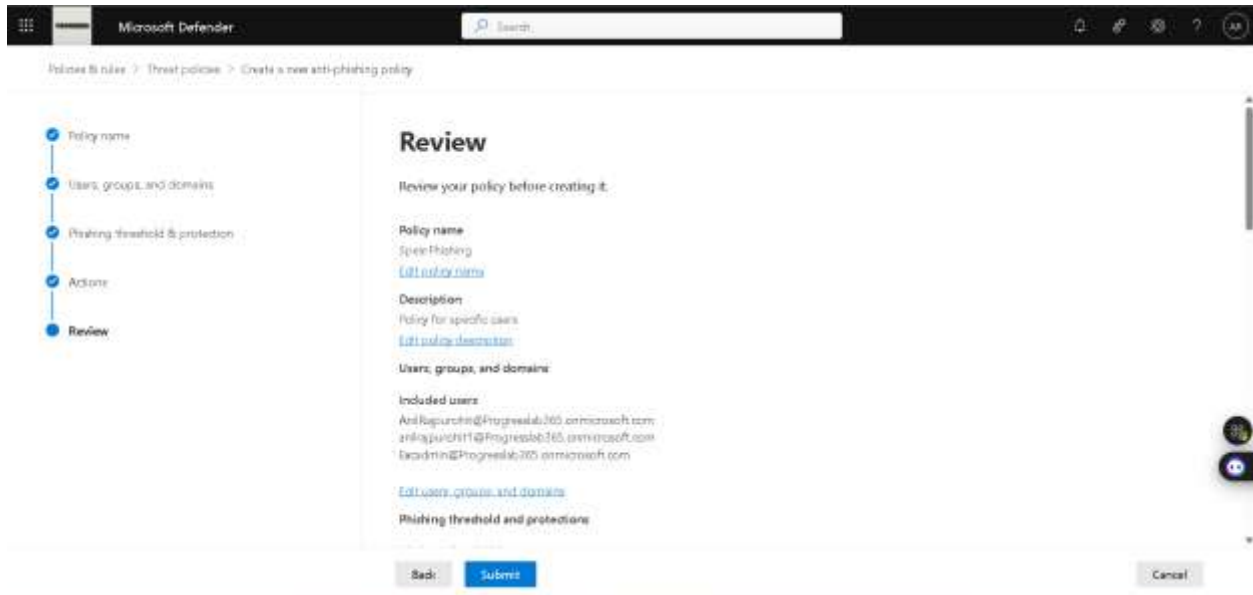
Step 7: Now select Quarantine the message, if a message is detected as user impersonation. Because we want to verify the message first then we can decide next actions.



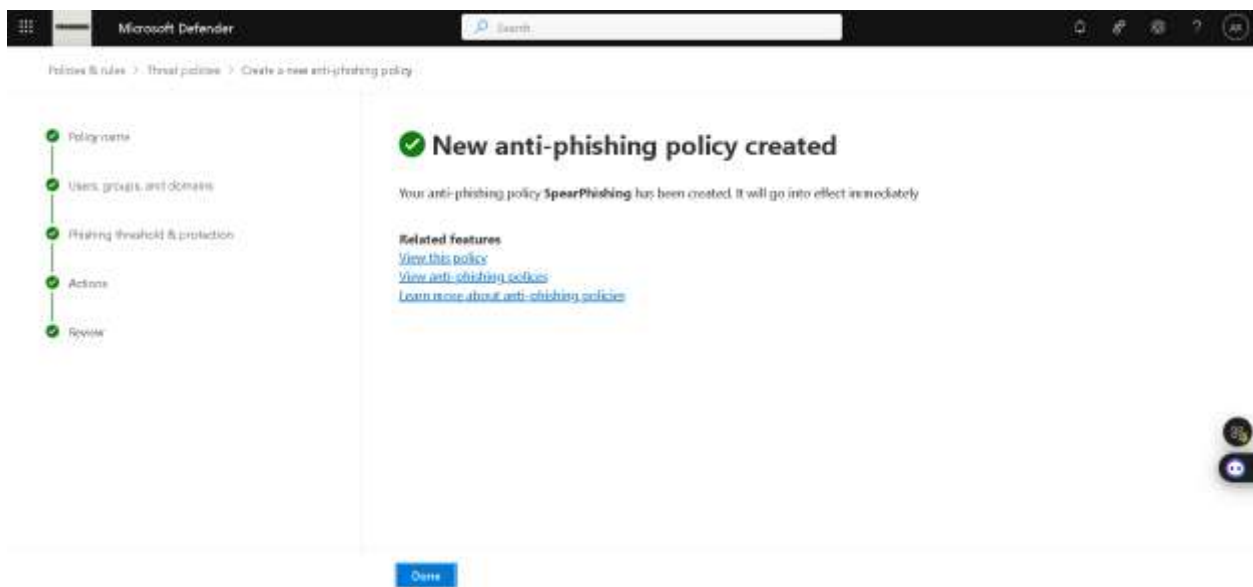
Step 8: Now, as we want to provide access to only admins for our quarantine policy select AdminOnlyAccessPolicy. Then Next.



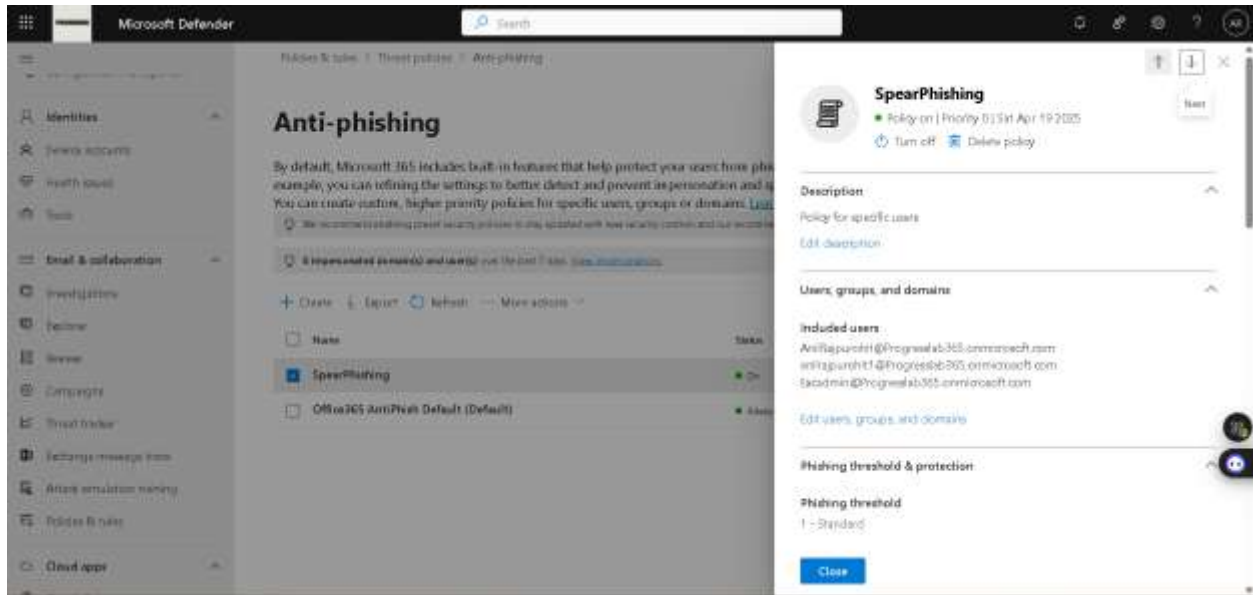
Step 9: Review our new policy details and click on submit.



Step 10: Our policy has been successfully created.



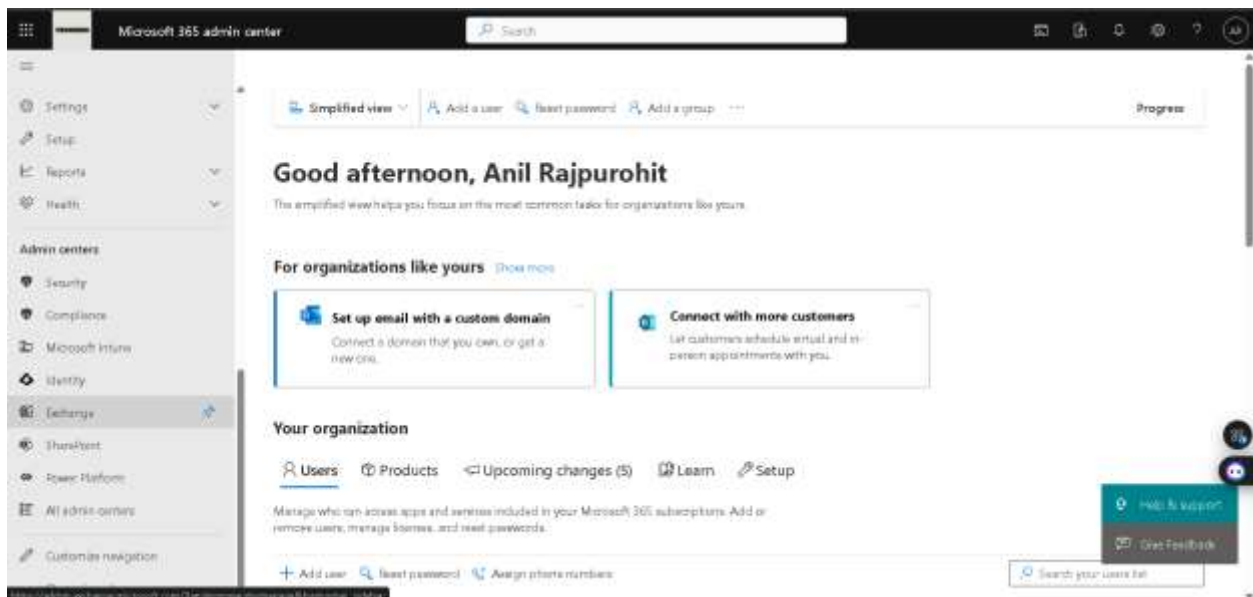
Step 11: We can view our new active policy under Defender -> email & collaboration -> policies & rules -> threat policies -> Anti phishing.



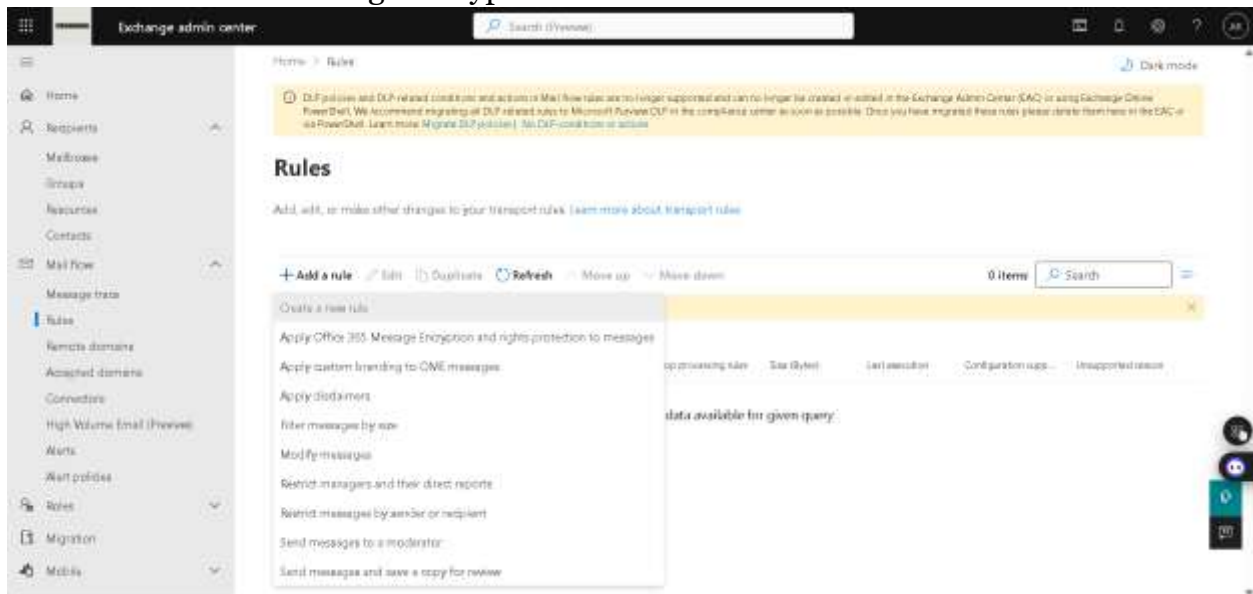
2. Set Up Data Encryption:

- Configure Microsoft 365 Message Encryption.
- Ensure that emails from inside the organization are automatically encrypted.

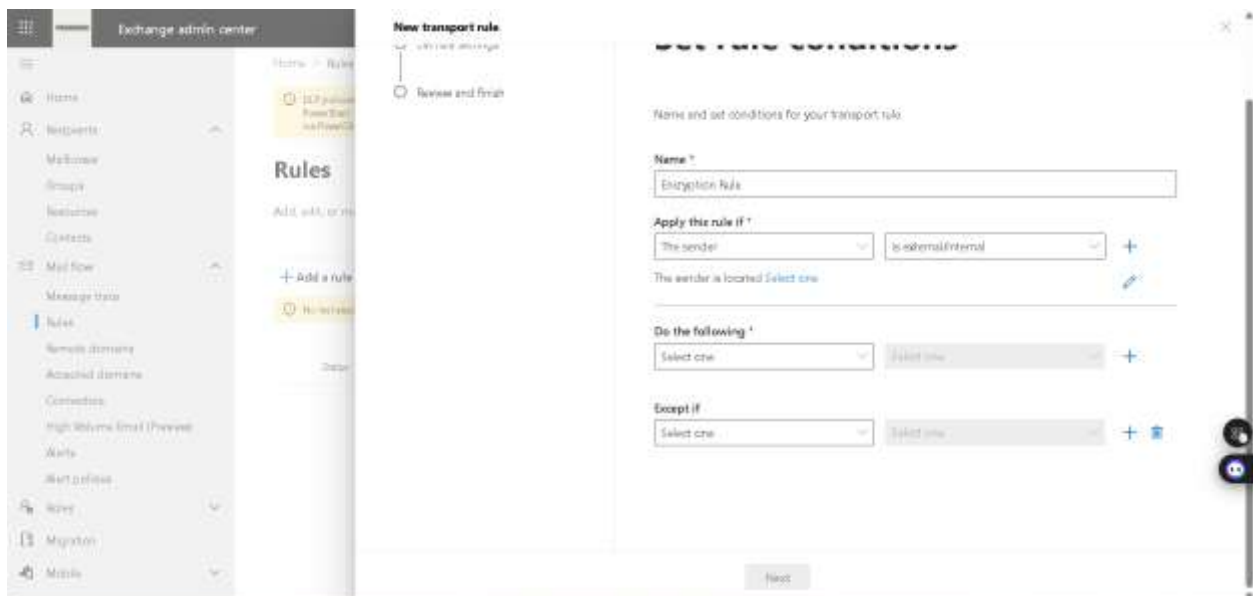
Step 1: From Microsoft 365 admin center, under admin centers select Exchange.



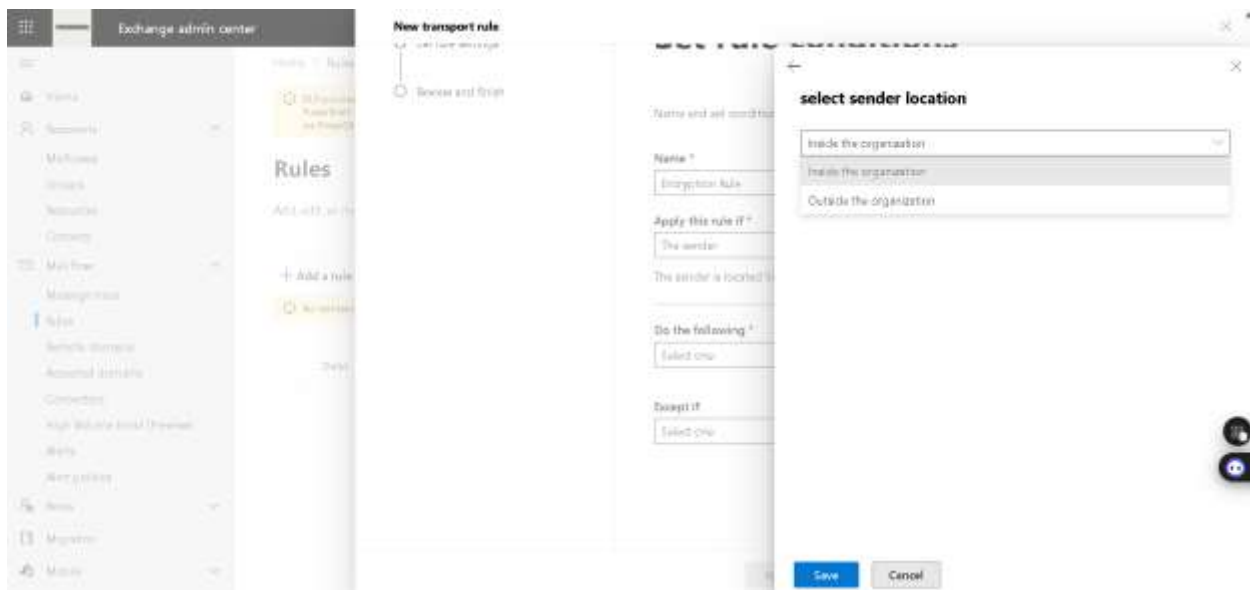
Step 2: In exchange admin center, mail flow -> rules -> Add a rule -> create a new rule. To create a rule for message encryption.



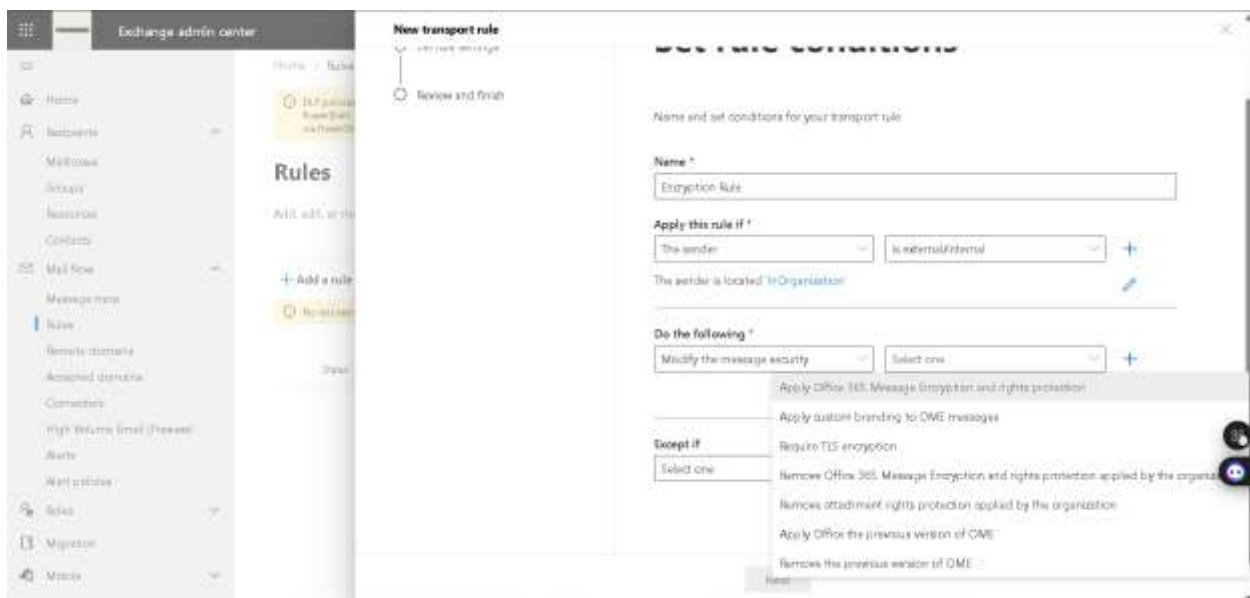
Step 3: Provide details like name, then select the condition. E.g. This policy will apply to the sender which is external/internal.



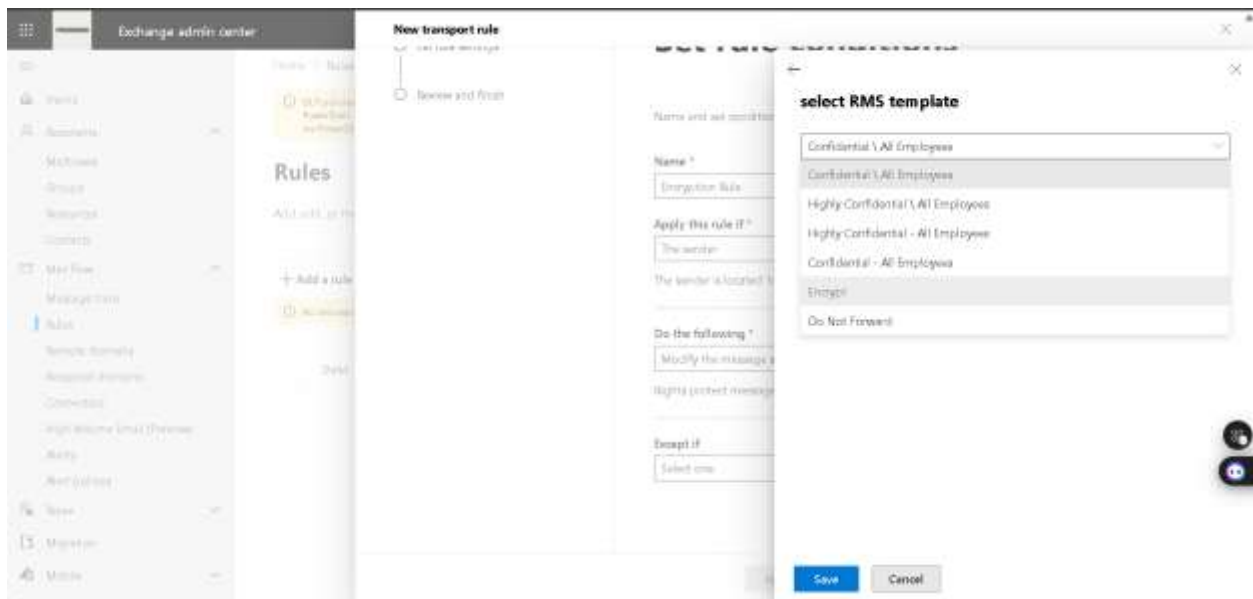
Step 4: Now, more specific we want only from inside the organization then save.



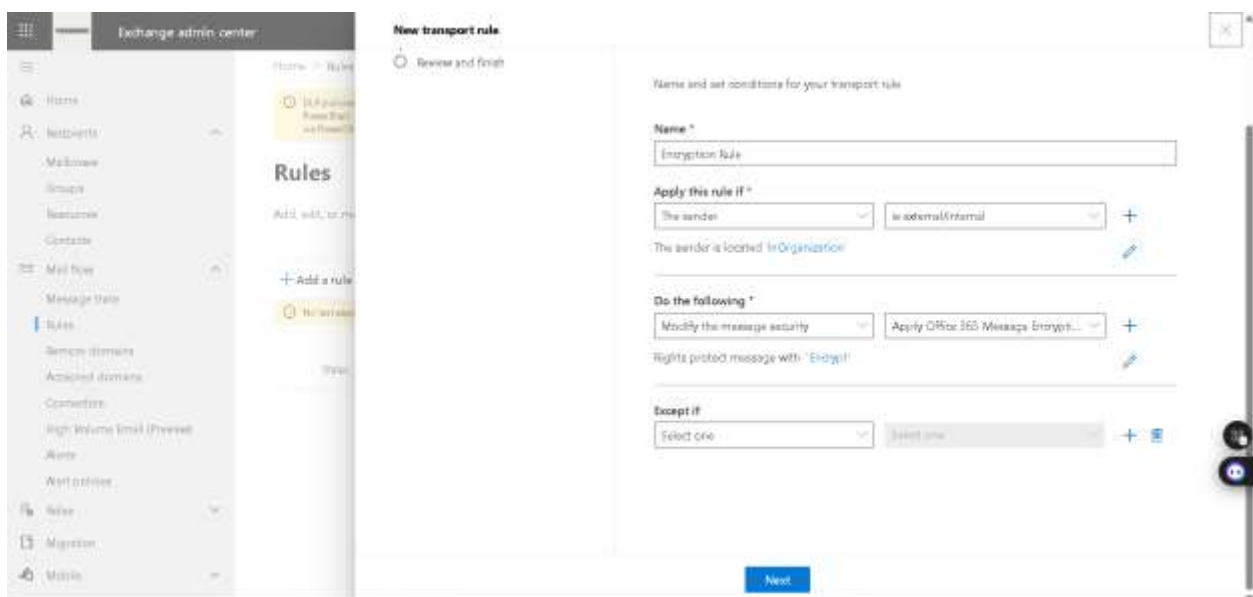
Step 5: Next condition, Modify the message security for Office 365 message encryption and right protection.



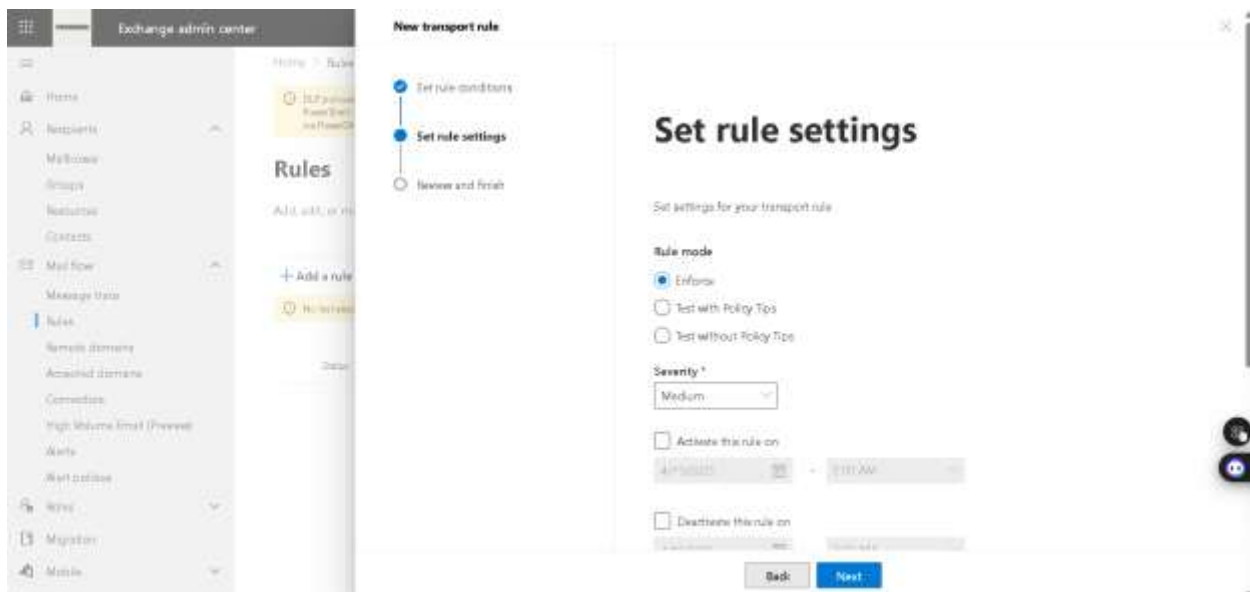
Step 6: RMS template as encrypt then save the condition.



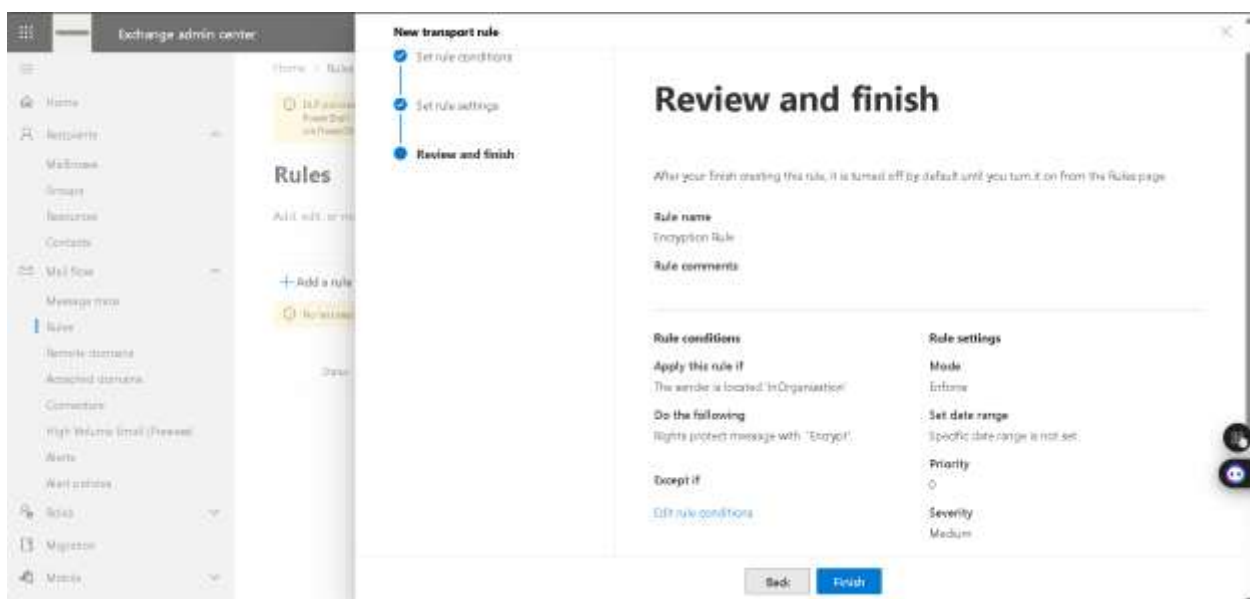
Step 7: Verify the rule and we don't want to exclude anyone. Then click on next.



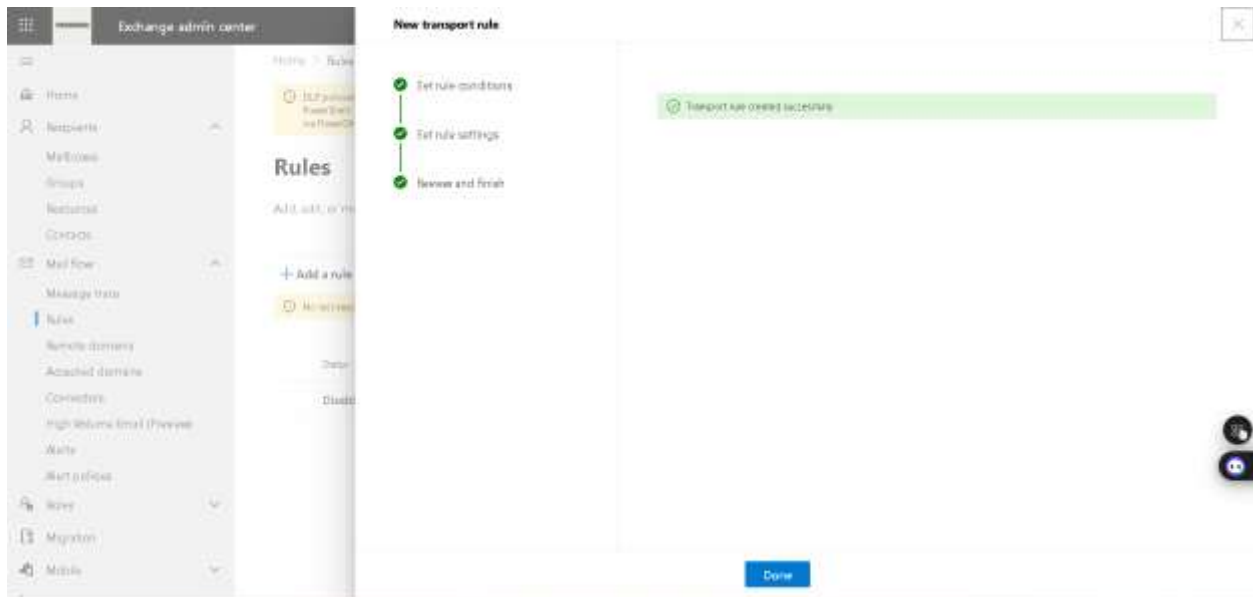
Step 8: Enforce the rule, choose the severity then Next.



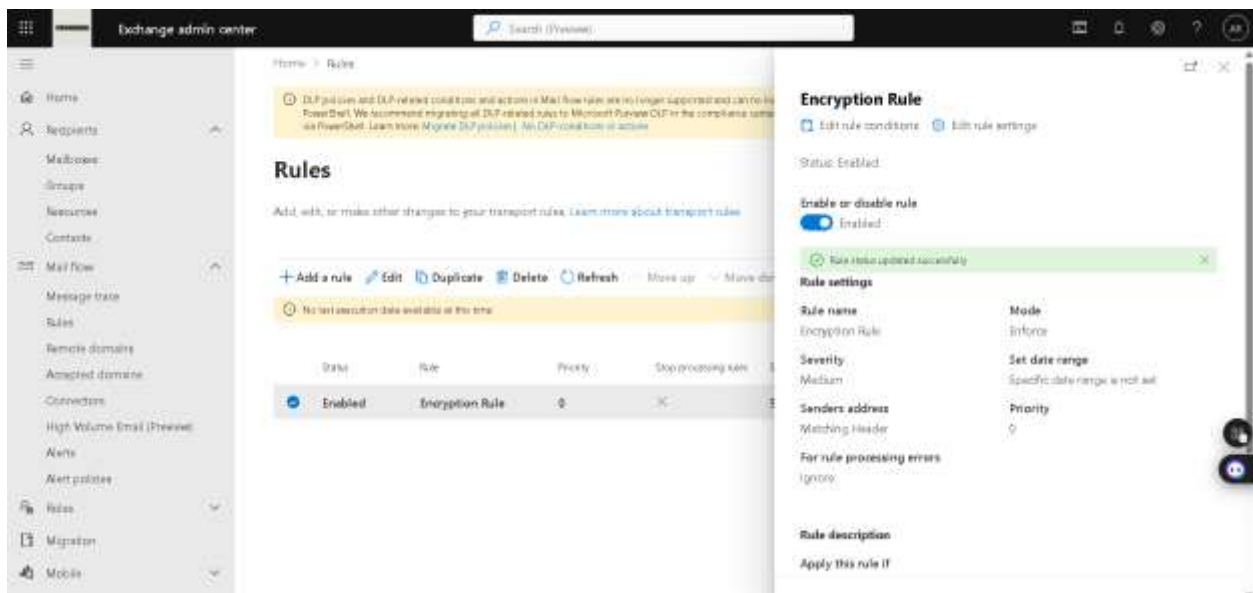
Step 9: Review the whole rule and click on finish.



Step 10: Our new rule has been successfully created.



Step 11: Verify rule status from exchange admin center -> mail flow -> rules.



LEARNING & OPINION

Healthy secure score is generally above 80%. We can complete recommended actions to increase our score.

Microsoft provide many built-in policies to secure the environment from cyber-attacks like safe link, safe attachment, Anti-spam, anti-phishing, and anti-malware policies.

In policies, we have option to Quarantine the message, if a message is detected as user impersonation. Because we want to verify the message first then we can decide next actions.

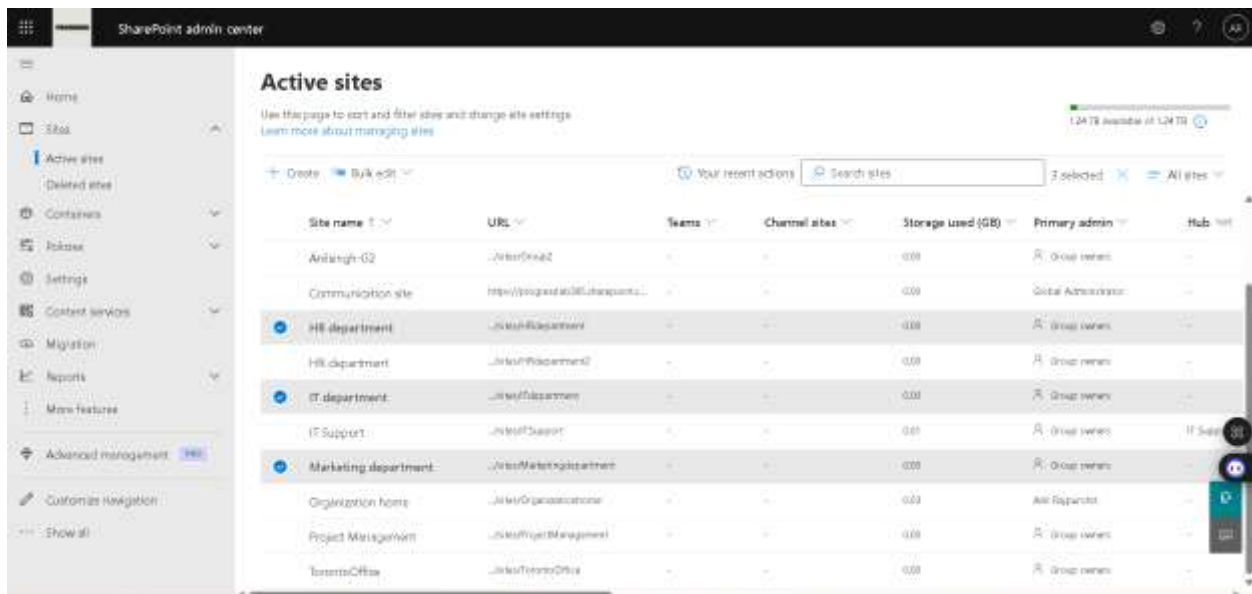
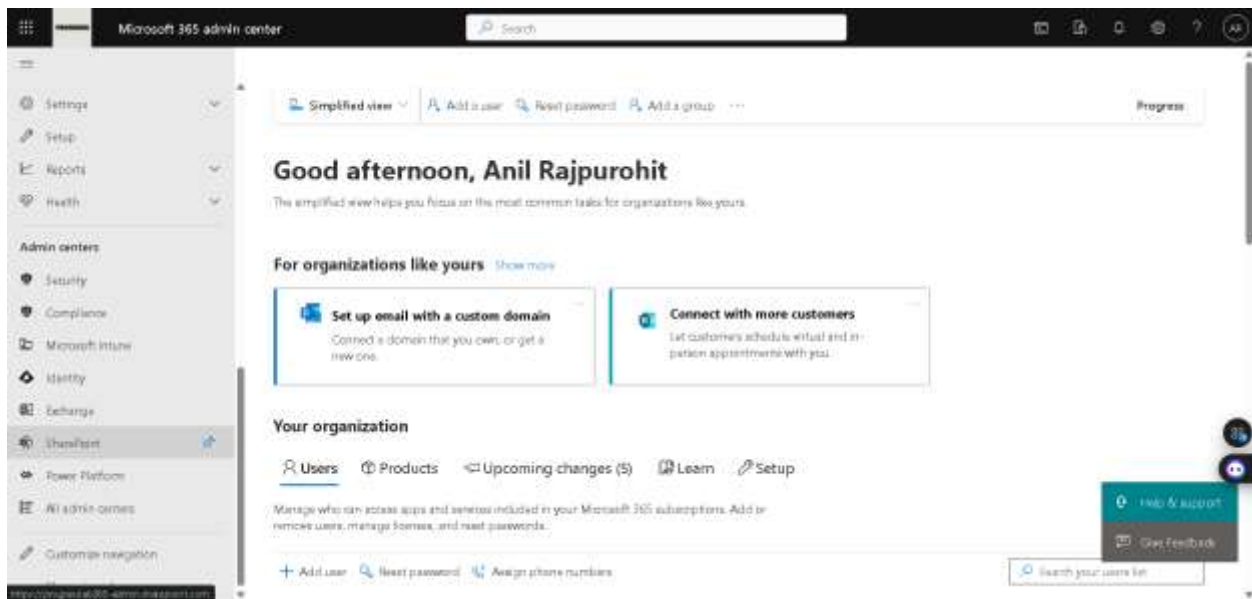
We can also create rules for encrypting messages inside the organization, so that even if anyone get access to the data. They won't be able to get anything from that.

Task 3: Configuring and Managing Collaboration Tools

1. Set Up SharePoint Online:

- Create an online SharePoint site for each department (IT, HR, Marketing).

Step 1: From Microsoft 365 admin center, under admin centers select SharePoint.



SharePoint admin center

Active sites

Use this page to sort and filter sites and then learn more about managing sites.

[+ Create](#)
[Edit](#)
[Membership](#)

Site name

- Antikah-G2
- Communication site
- HR department
- IT department
- IT Support
- Marketing department
- Organization home
- Project Management
- TorontoOffice

HR department

Private group

[Email](#)
[View site](#)

Group of HR department

This site has a compliance policy set to block deletion.

General Activity Membership Settings

Basic info	Email address	Other info
Name HR department Description Group of HR department Edit	Primary HRdepartment@Progreslab265.onmicrosoft.com Aliases Edit	Created 4/18/25 at 9:23 PM by HR department Owners from My AAD Portal

Site info

SharePoint admin center

Active sites

Use this page to sort and filter sites and then learn more about managing sites.

[+ Create](#)
[Edit](#)
[Membership](#)

Site name

- Antikah-G2
- Communication site
- HR department
- IT department
- IT Support
- Marketing department
- Organization home
- Project Management
- TorontoOffice

IT department

Private group

[Email](#)
[View site](#)

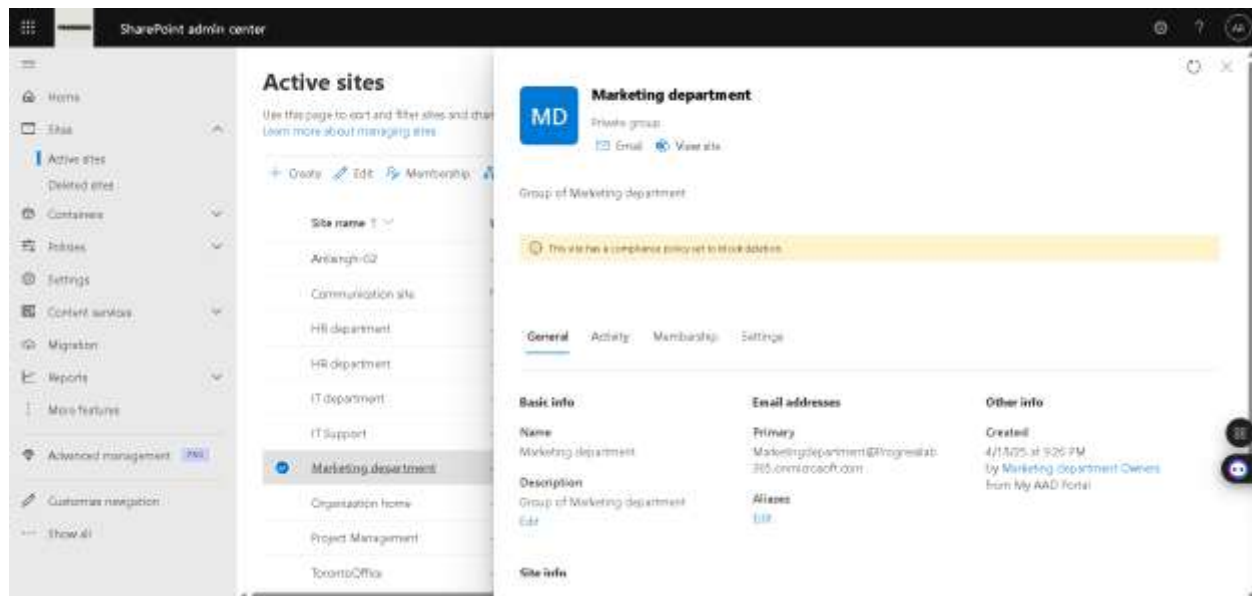
Group of IT department

This site has a compliance policy set to block deletion.

General Activity Membership Settings

Basic info	Email address	Other info
Name IT department Description Group of IT department Edit	Primary ITdepartment@Progreslab265.onmicrosoft.com Aliases Edit	Created 4/18/25 at 9:17 PM by IT department Owners from My AAD Portal

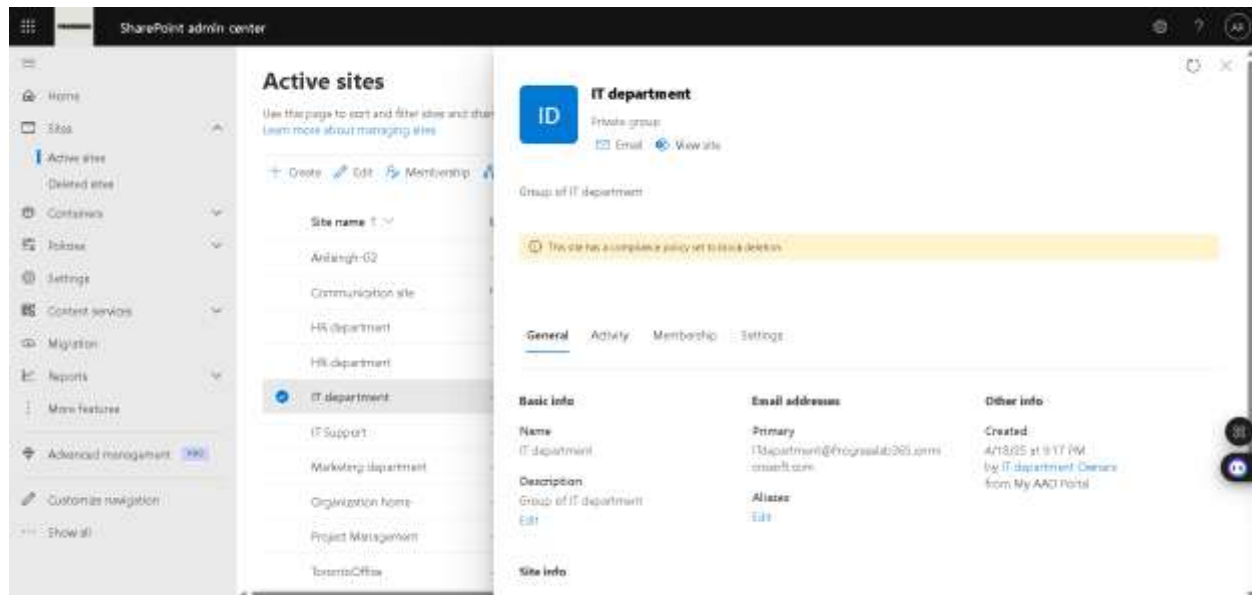
Site info



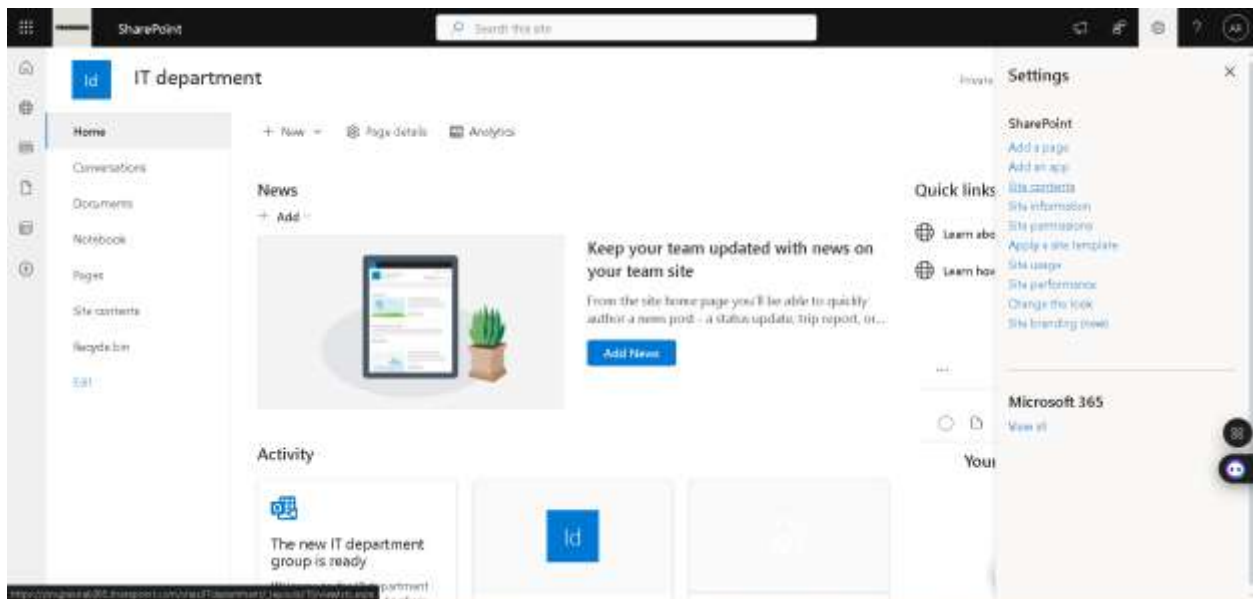
- Configure document libraries and permissions for each site.

For IT department SharePoint

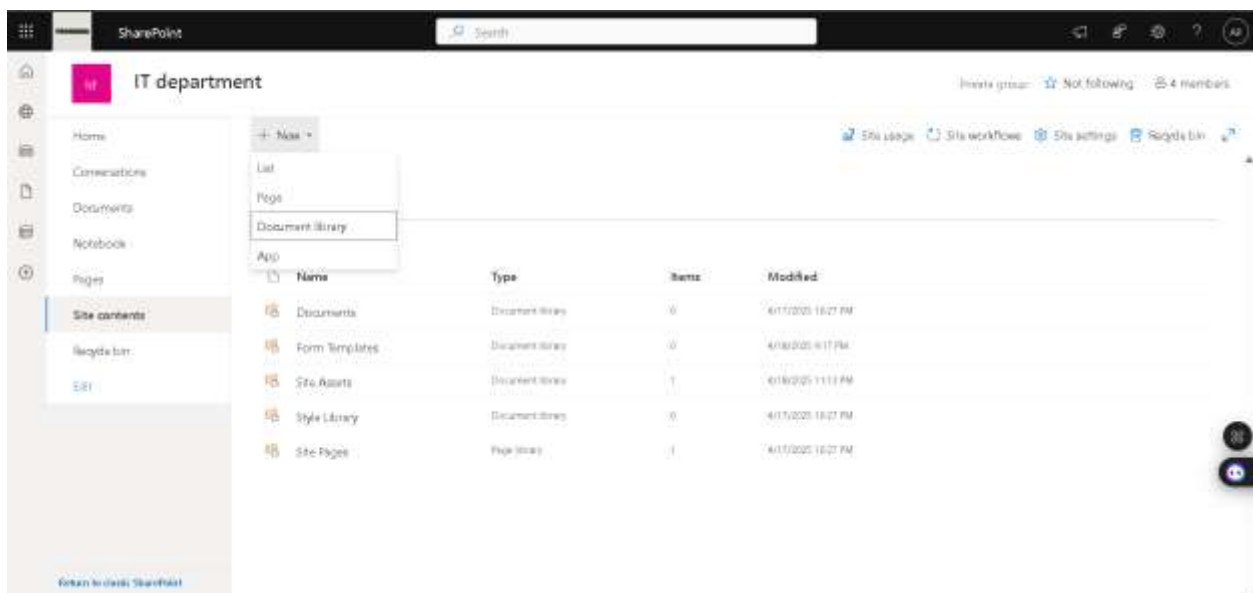
Step 1: From SharePoint admin center, go to sites -> active sites -> It department -> View site.



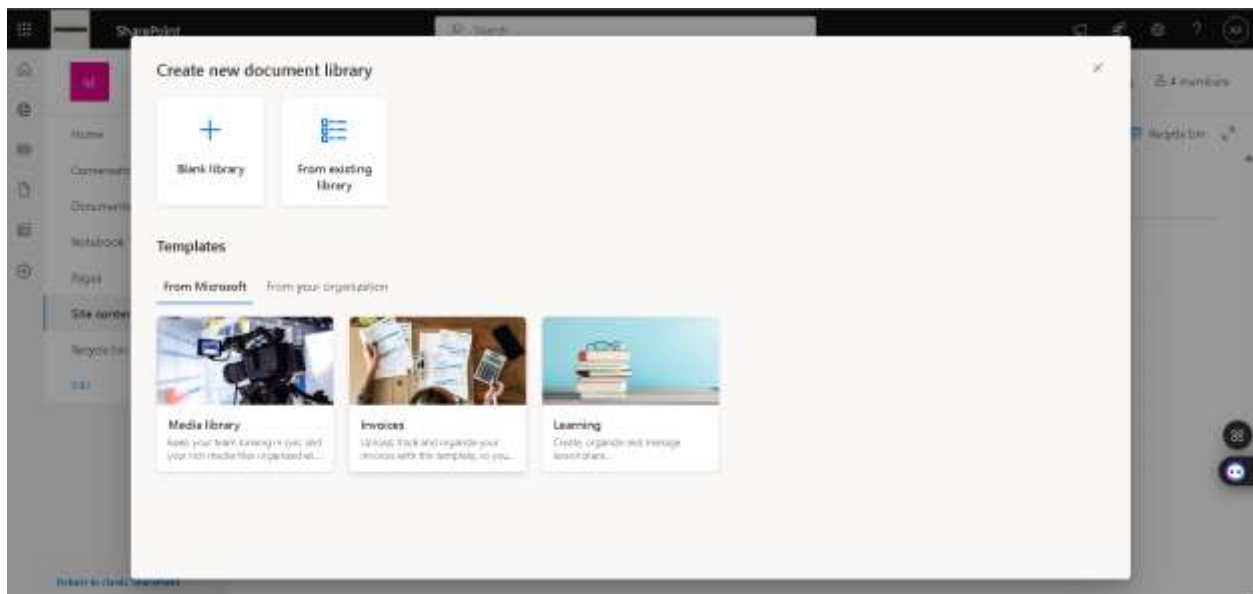
Step 2: Now from IT department SharePoint site, click on settings sign -> site contents.



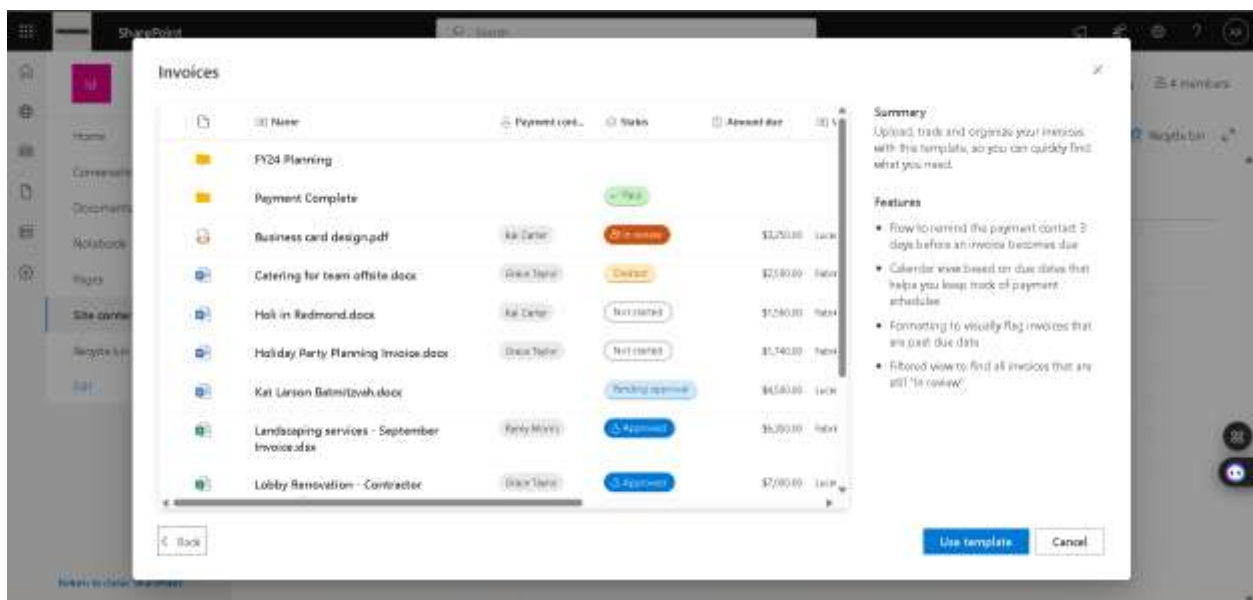
Step 3: Under site contents, new -> document library.



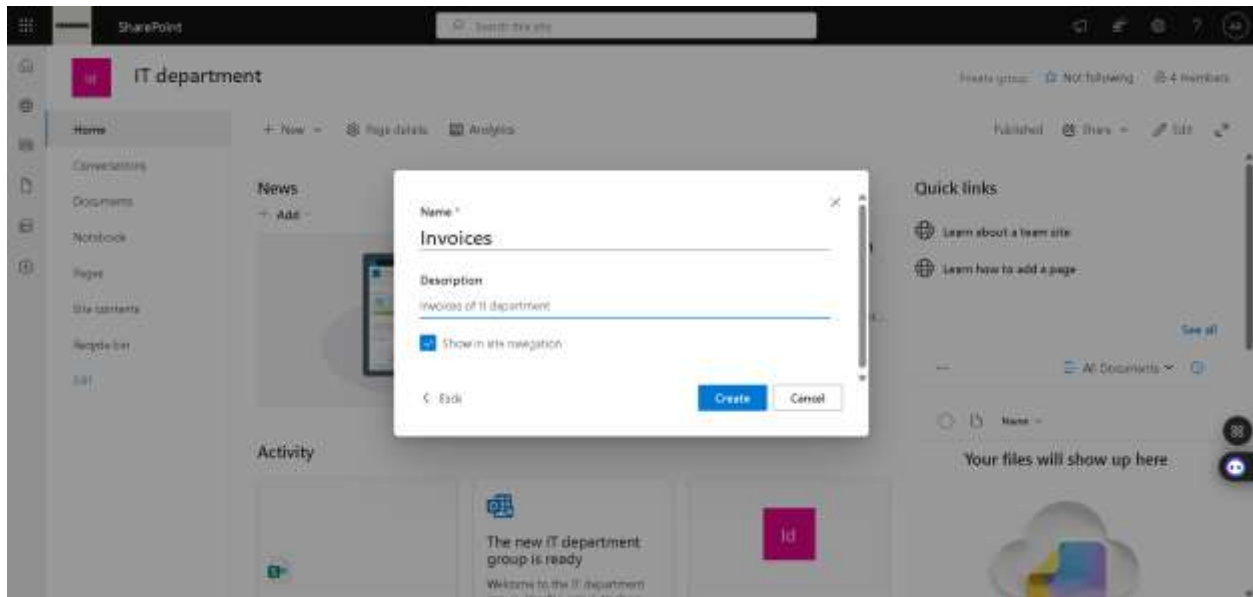
Step 4: We can select from template or create a blank library. We will select Invoices template.



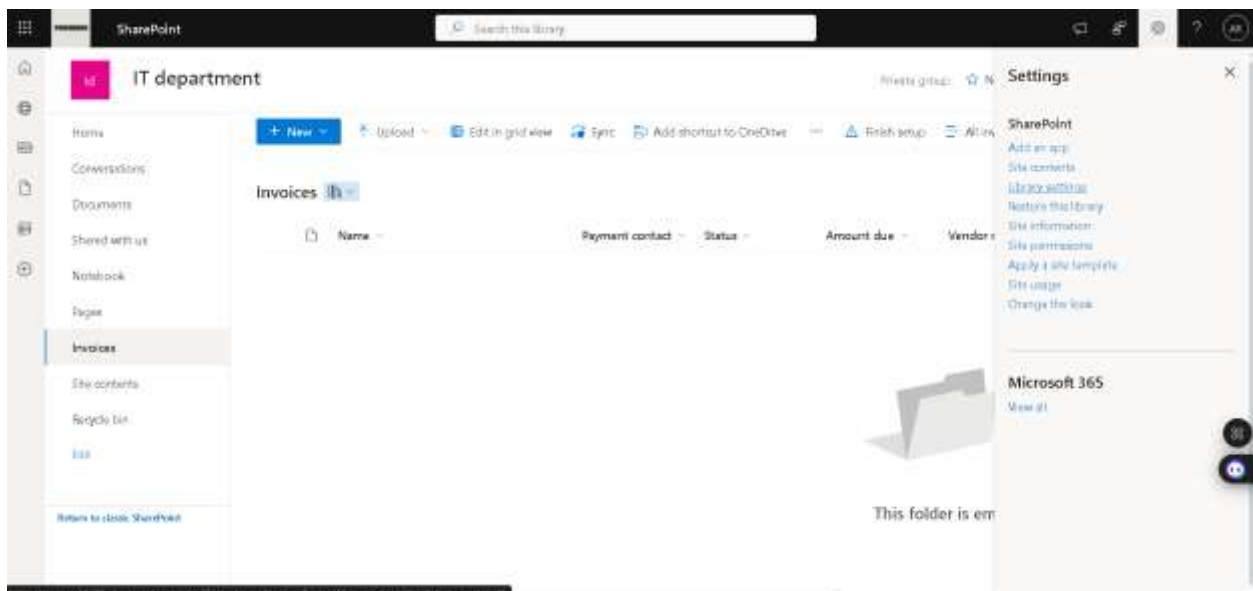
Step 5: We can see features of the template then click on use template.



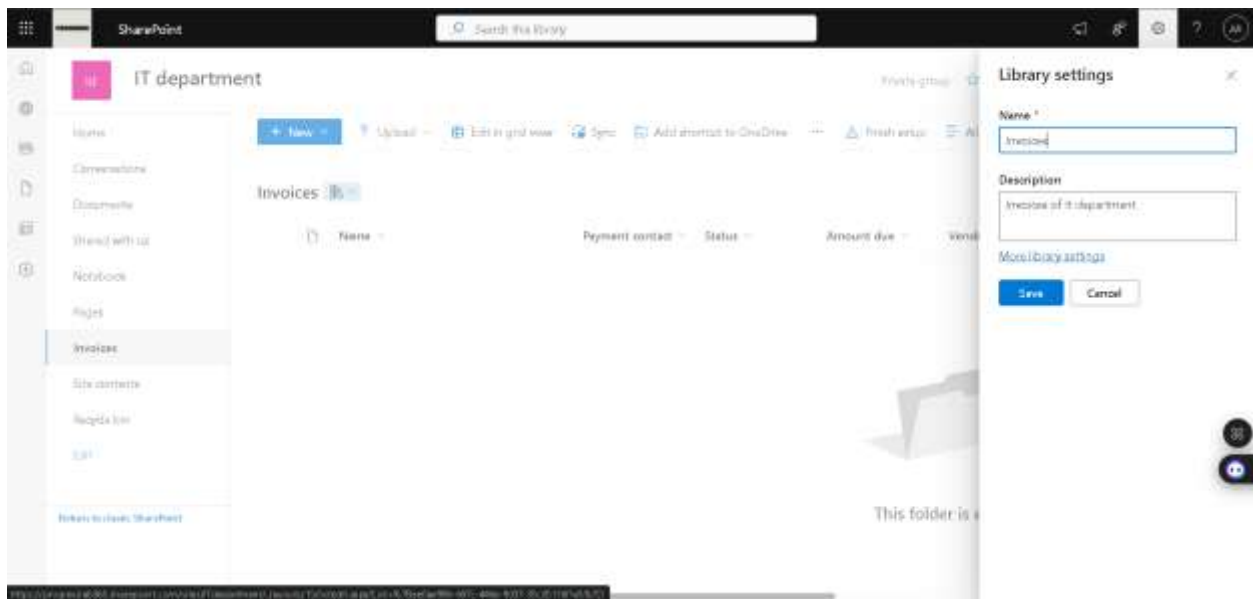
Step 6: We want to create a Invoices library, so fill name and description then create.



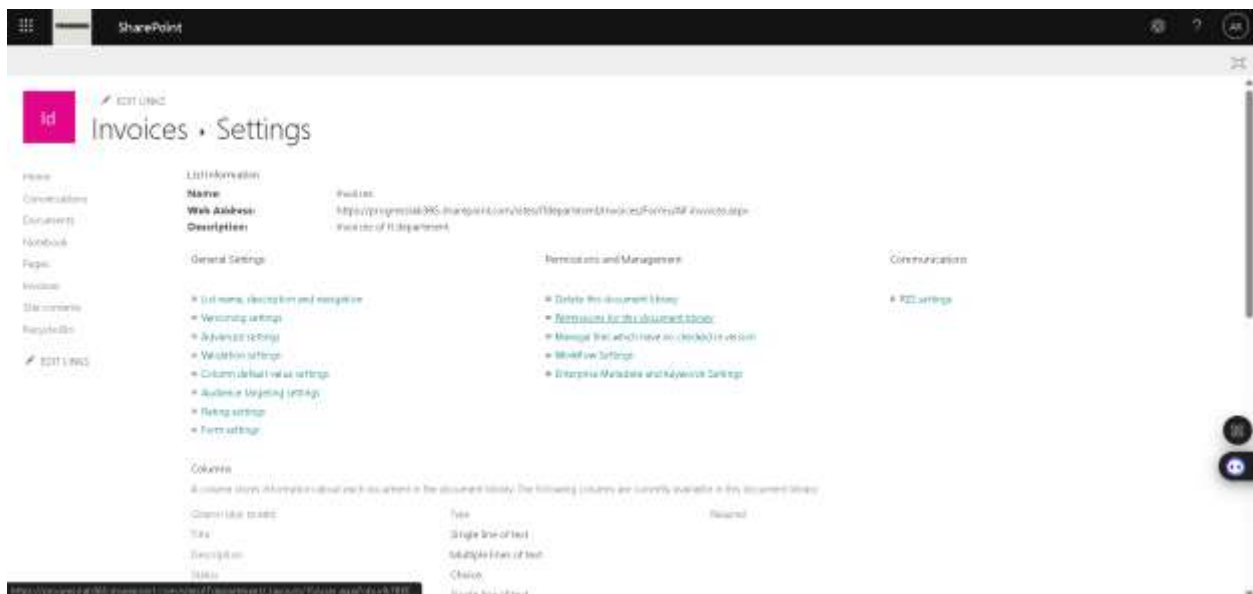
Step 7: Invoices library has been created, now select settings sign -> library settings.



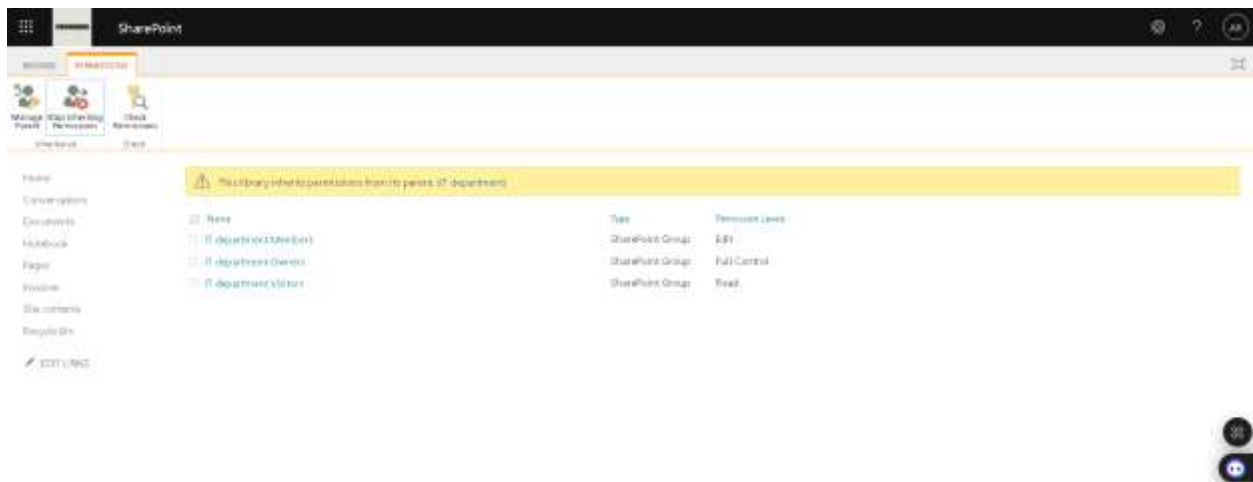
Step 8: Click on more library settings now.



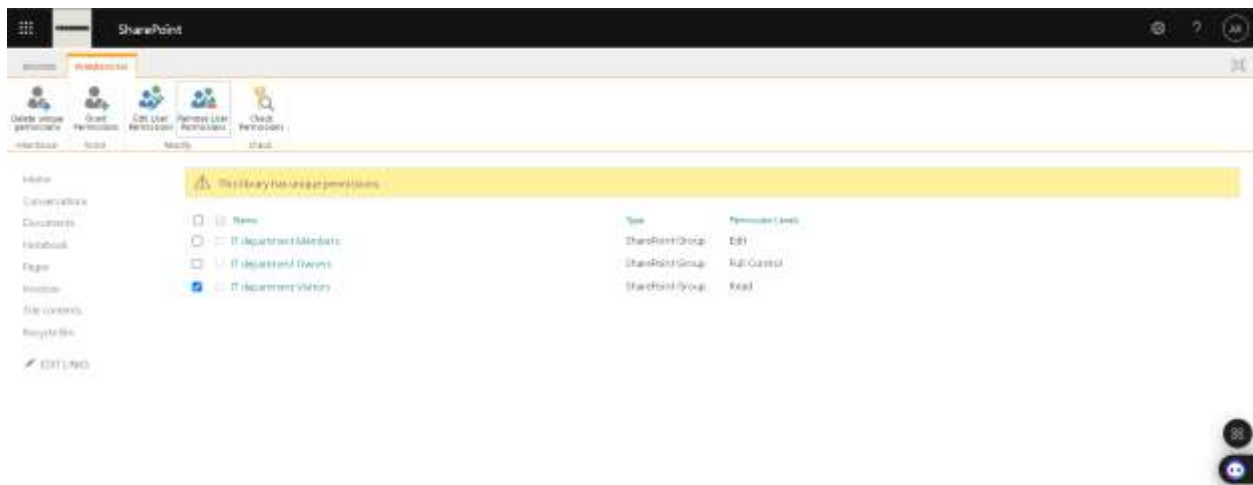
Step 9: Now, select under Permissions & Management ->permissions for this document library.



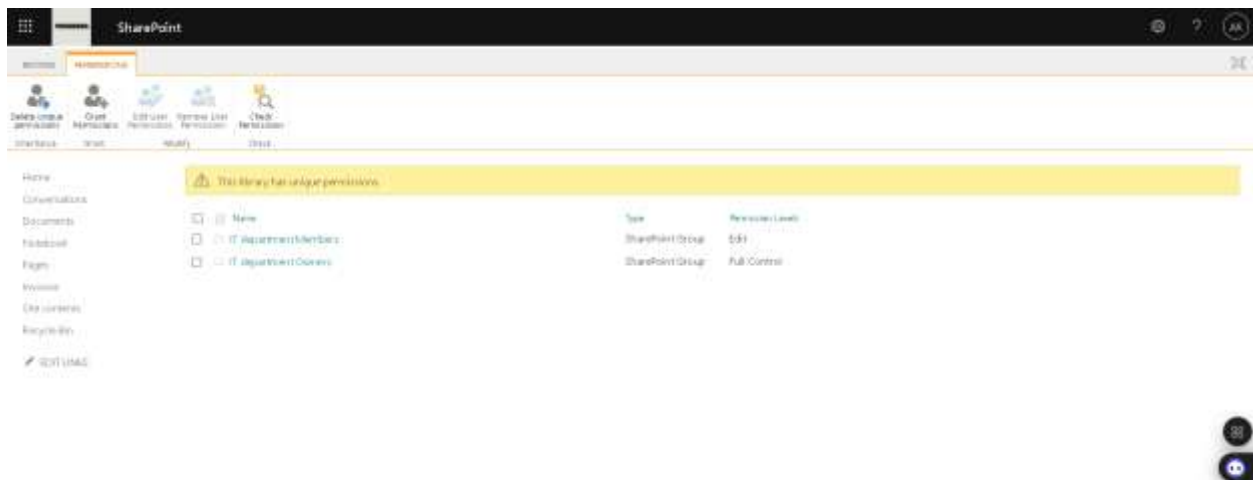
Step 10: First, click on stop inheriting permissions, so that we can add custom permissions to this library.



Step 11: As this is invoices of IT department, we don't want visitors to even read this library. So, we will select IT department visitors then remove user permissions.

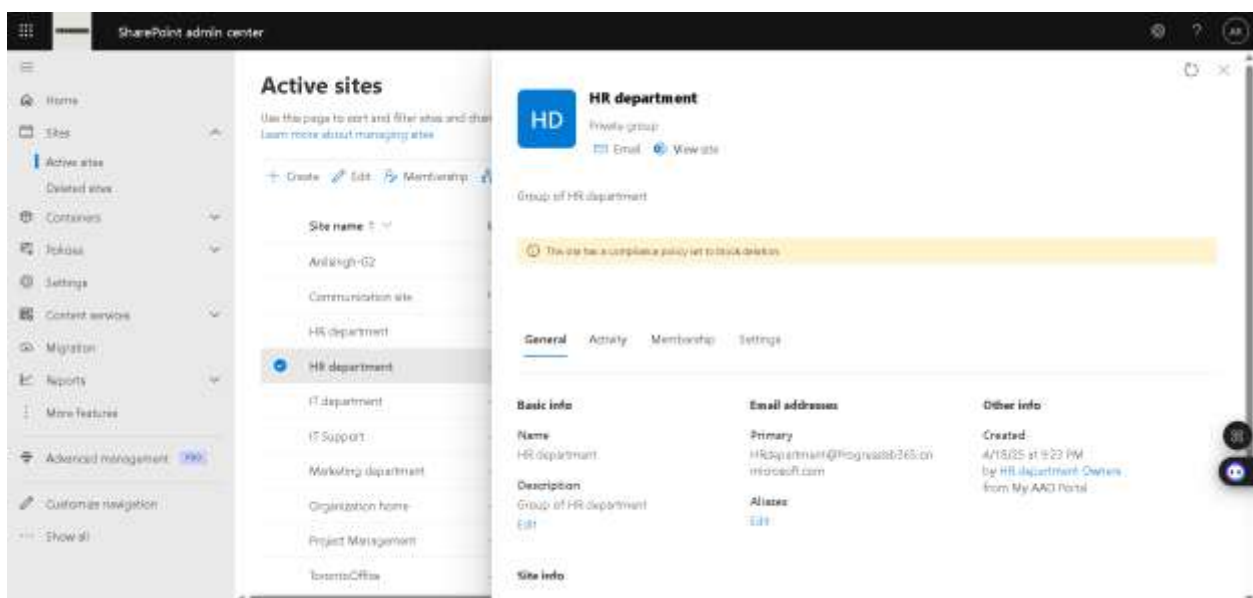


Step 12: Now for this library, we have only members which we need.

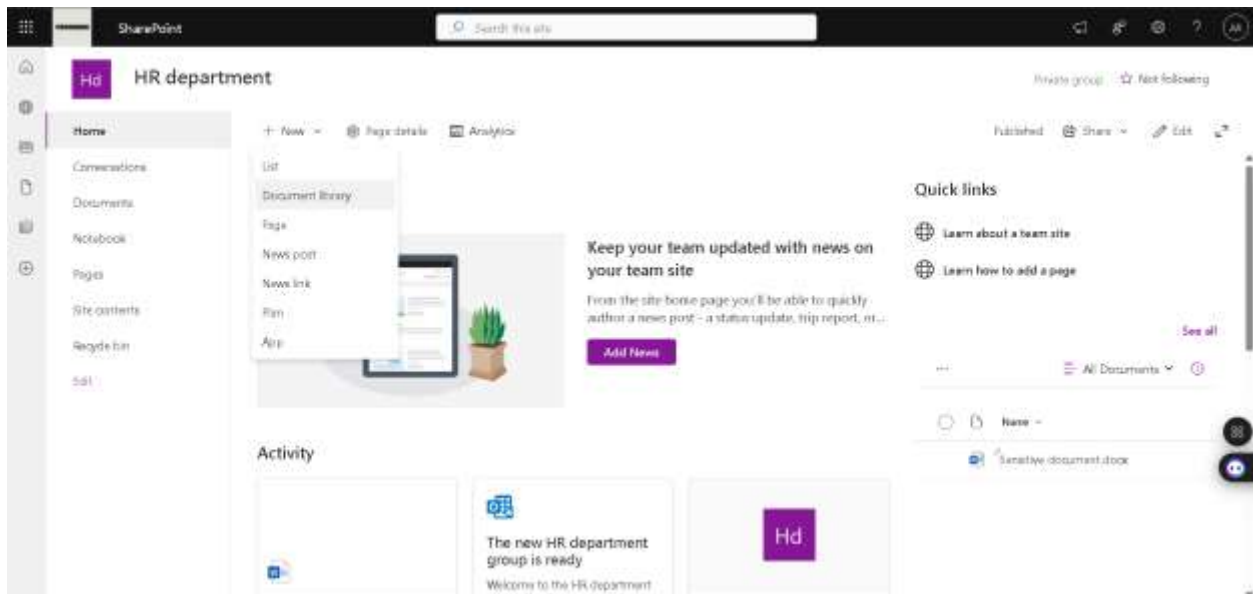


For HR department SharePoint

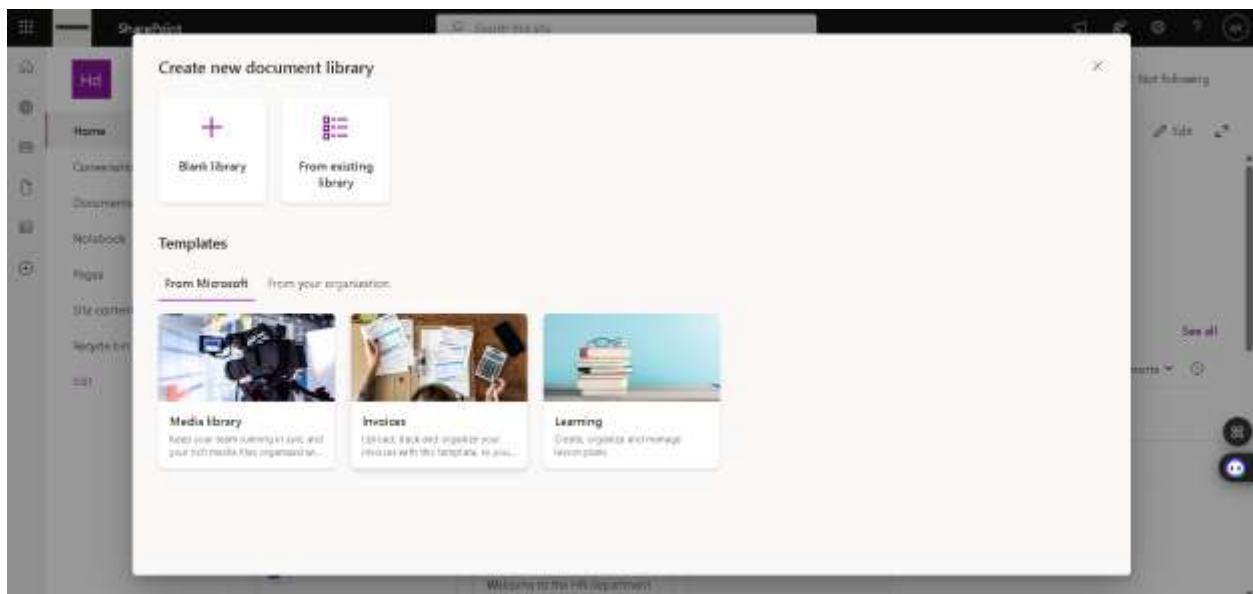
Step 1: From SharePoint admin center, go to sites -> active sites -> HR department -> View site.



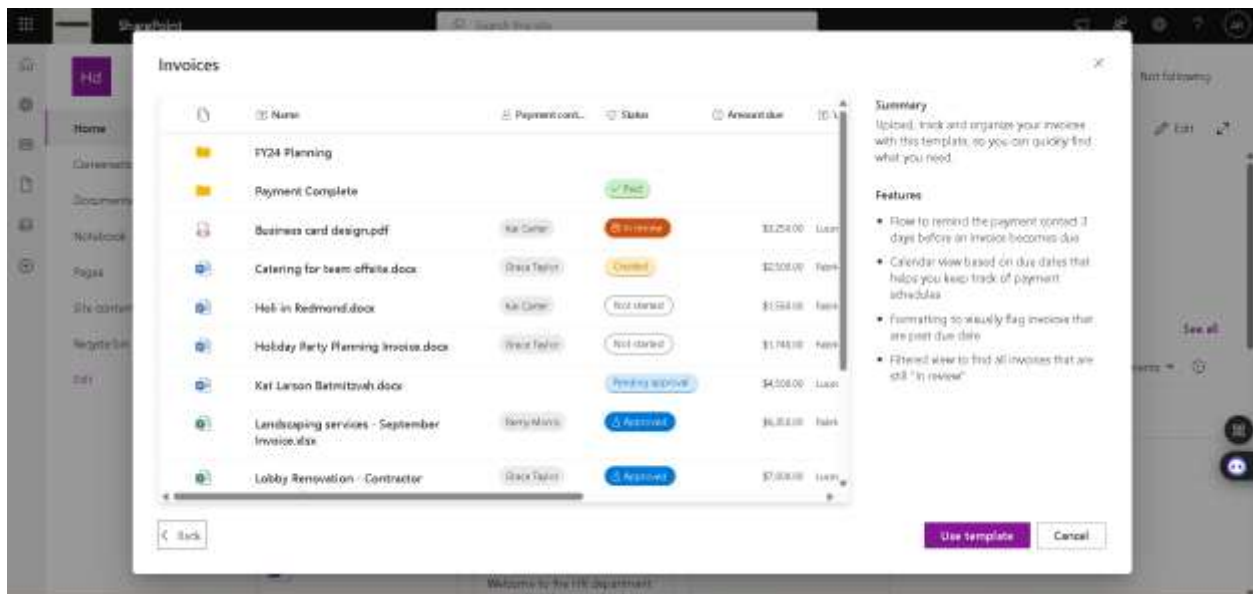
Step 2: Now from HR department SharePoint site, click on New -> Document library.



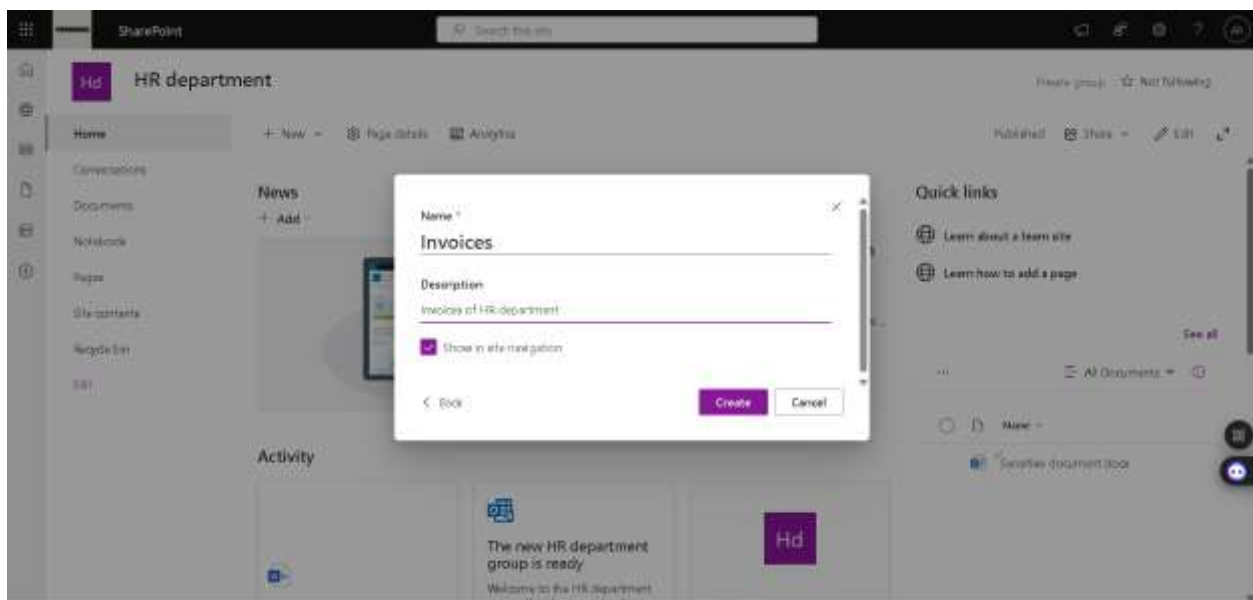
Step 3: We can select from template or create a blank library. We will select Invoices template.



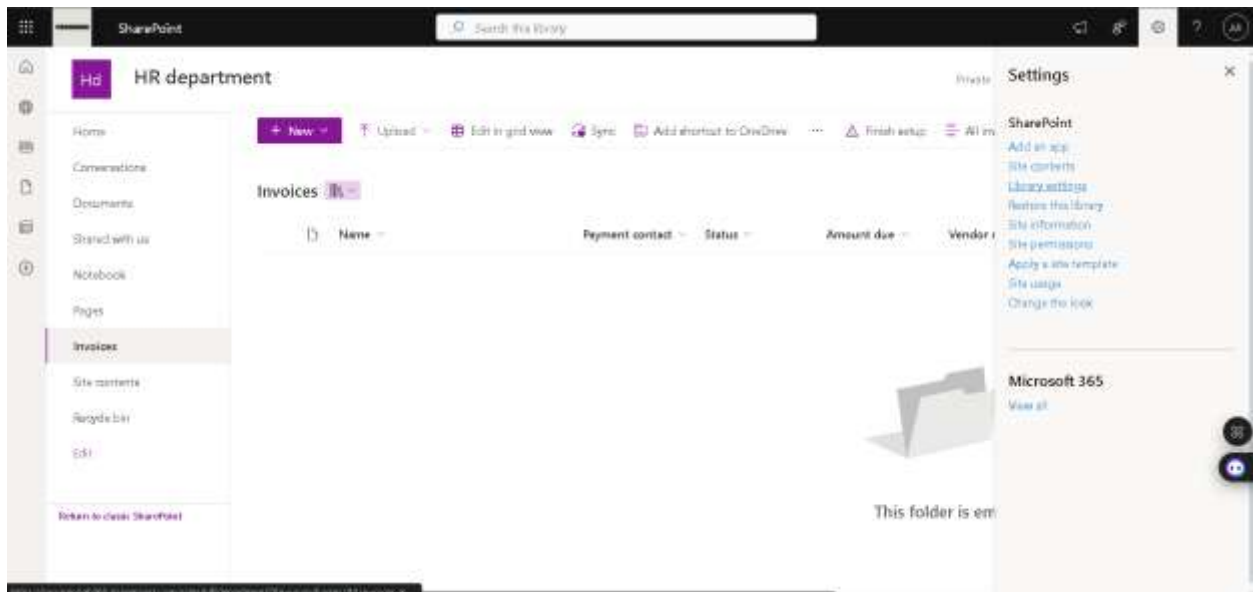
Step 4: We can see features of the template then click on use template.



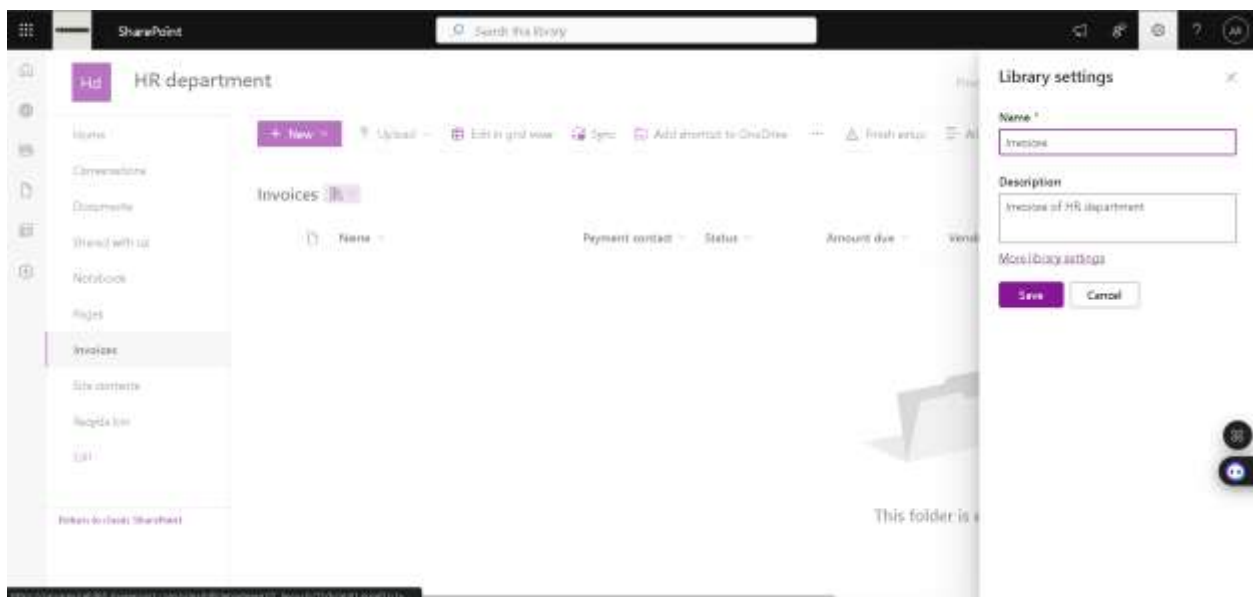
Step 5: We want to create a Invoices library, so fill name and description then create.



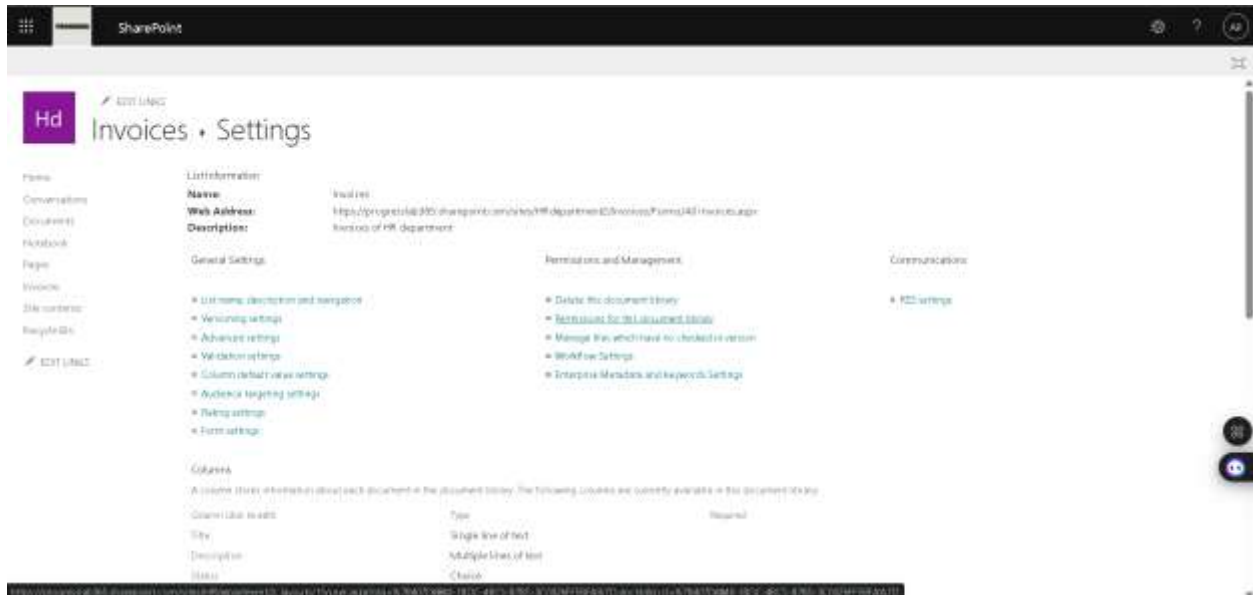
Step 6: Invoices library has been created, now select settings sign -> library settings.



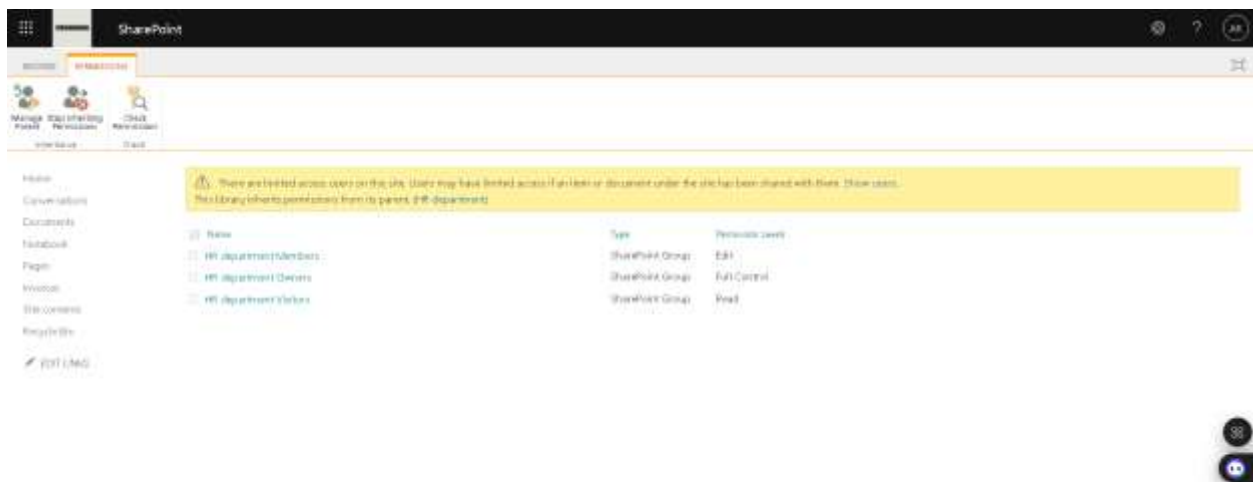
Step 7: Click on more library settings now.



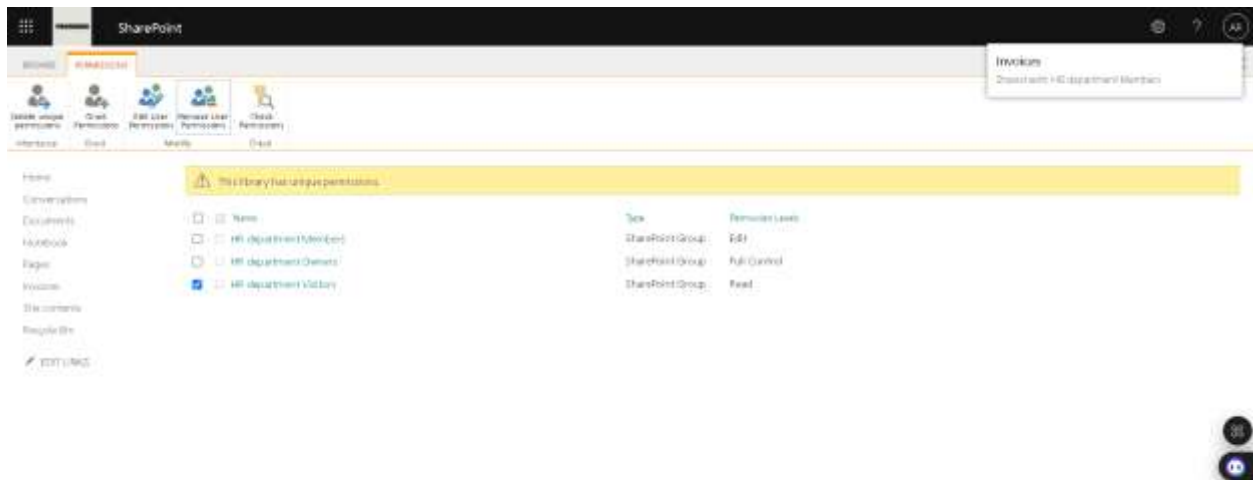
Step 8: Now, select under Permissions & Management ->permissions for this document library.



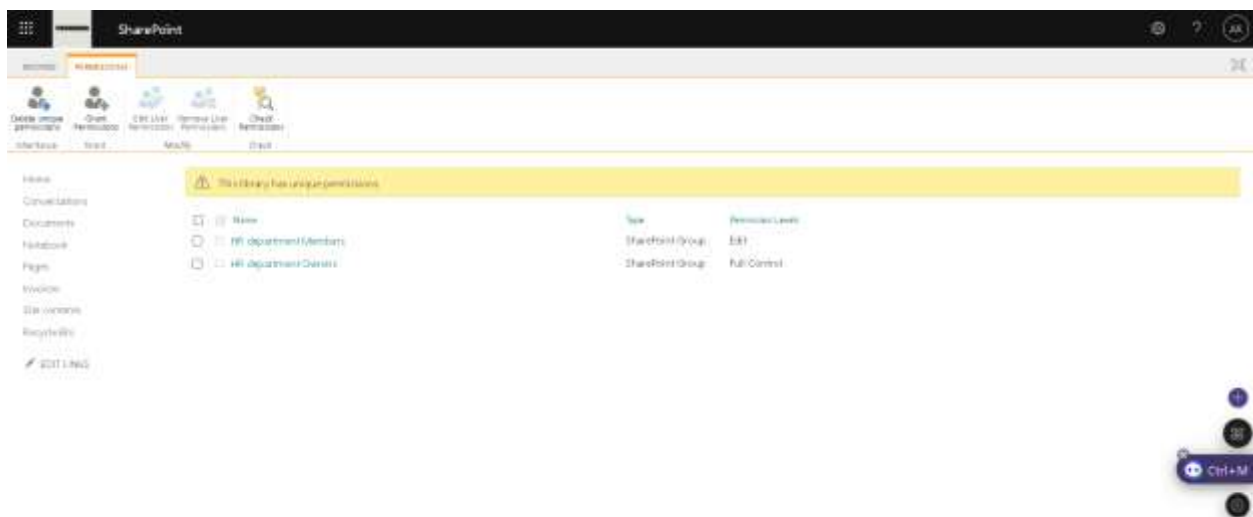
Step 9: First, click on stop inheriting permissions, so that we can add custom permissions to this library.



Step 10: As this is invoices of HR department, we don't want visitors to even read this library. So, we will select HR department visitors then remove user permissions.

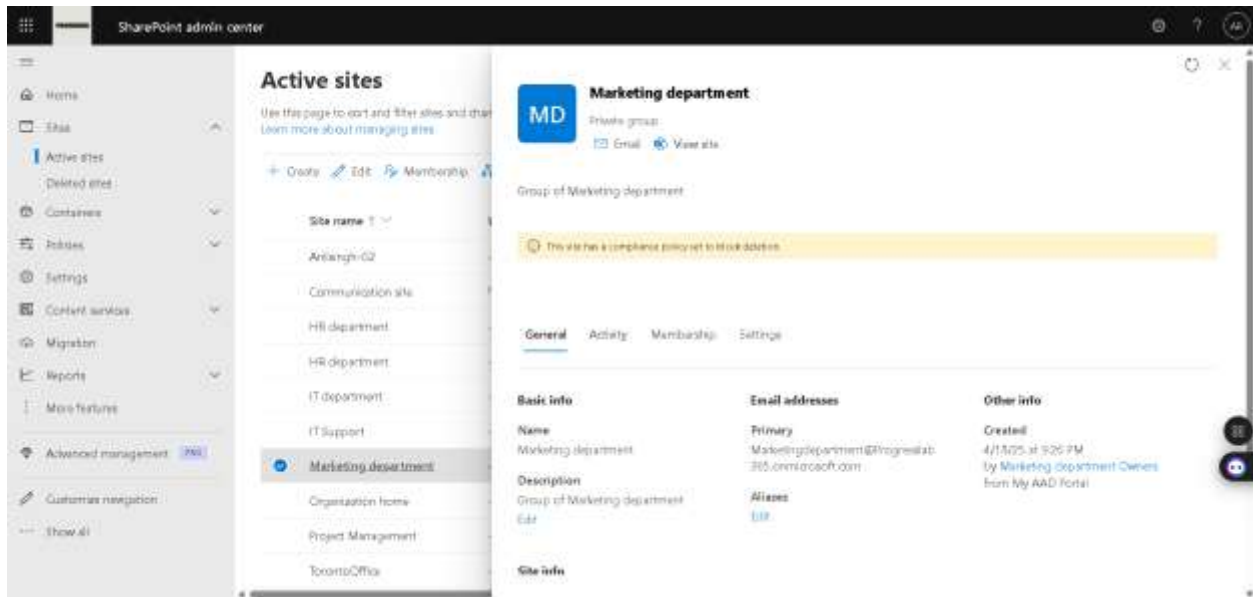


Step 11: Now for this library, we have only members which we need.

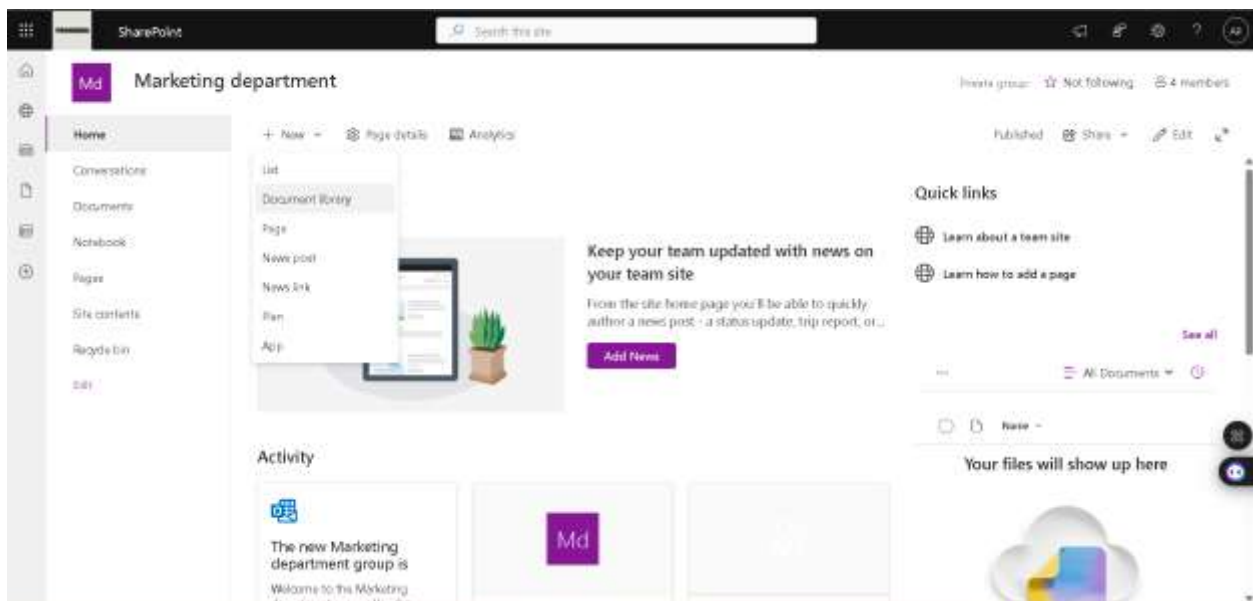


For Marketing department SharePoint

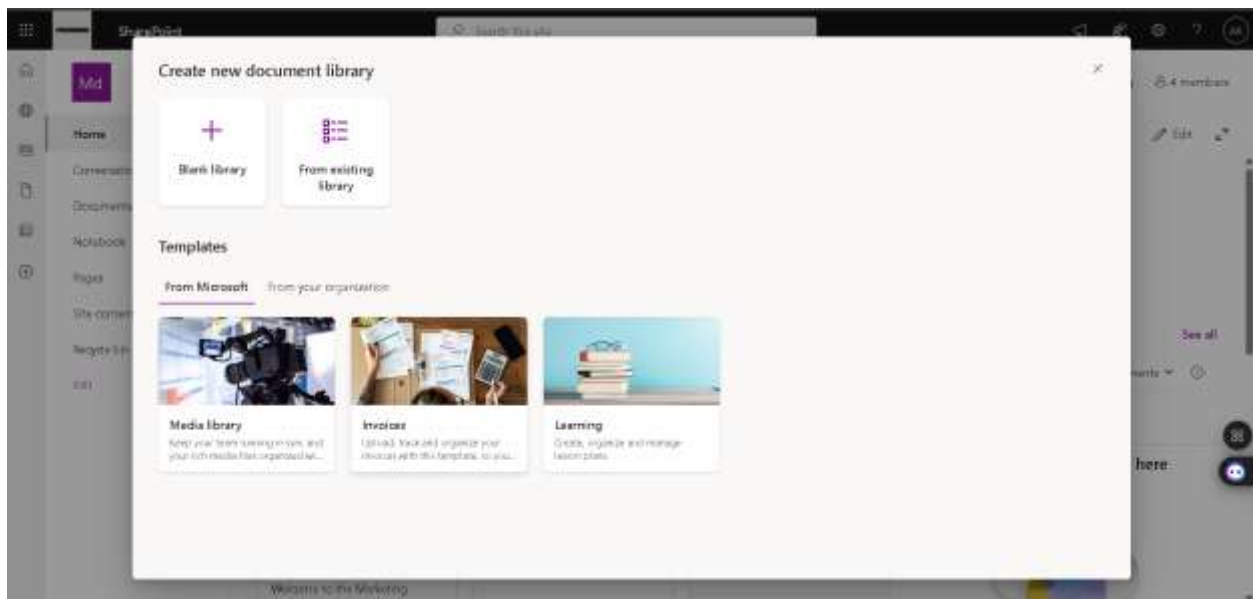
Step 1: From SharePoint admin center, go to sites -> active sites -> Marketing department -> View site.



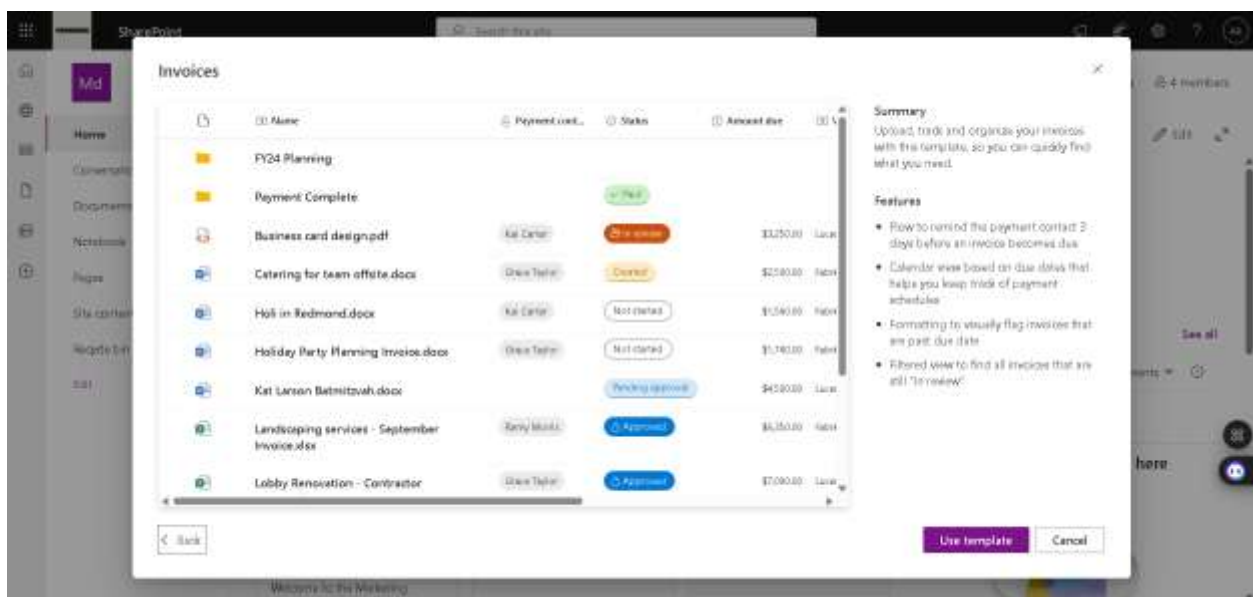
Step 2: Now from Marketing department SharePoint site, click on New -> Document library.



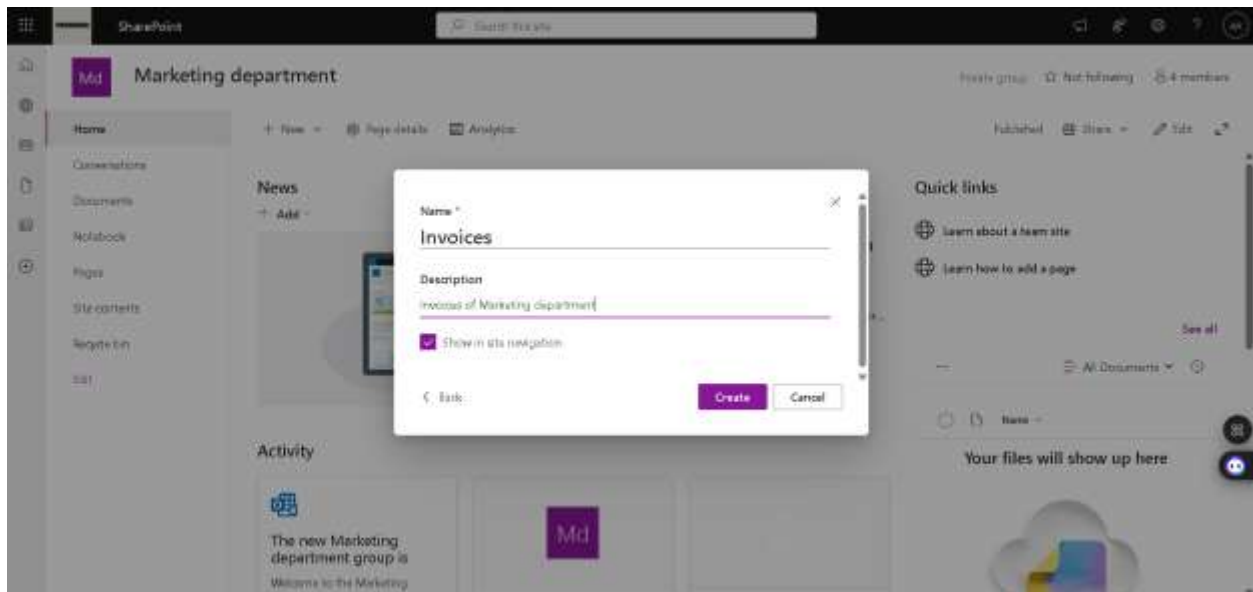
Step 3: We can select from template or create a blank library. We will select Invoices template.



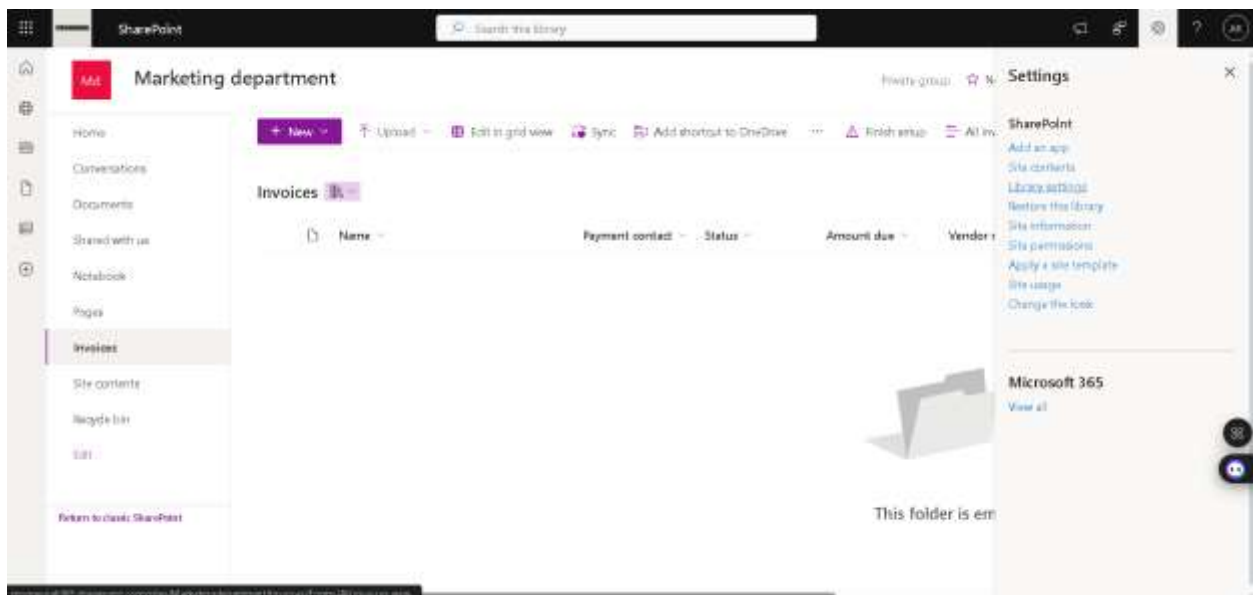
Step 4: We can see features of the template then click on use template.



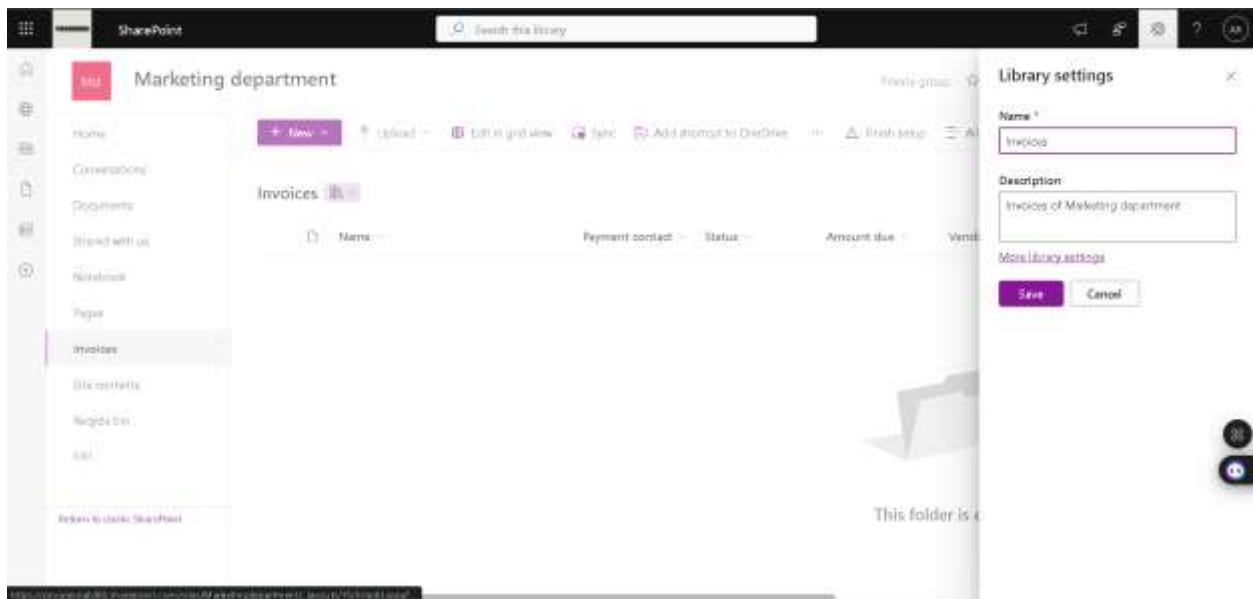
Step 5: We want to create a Invoices library, so fill name and description then create.



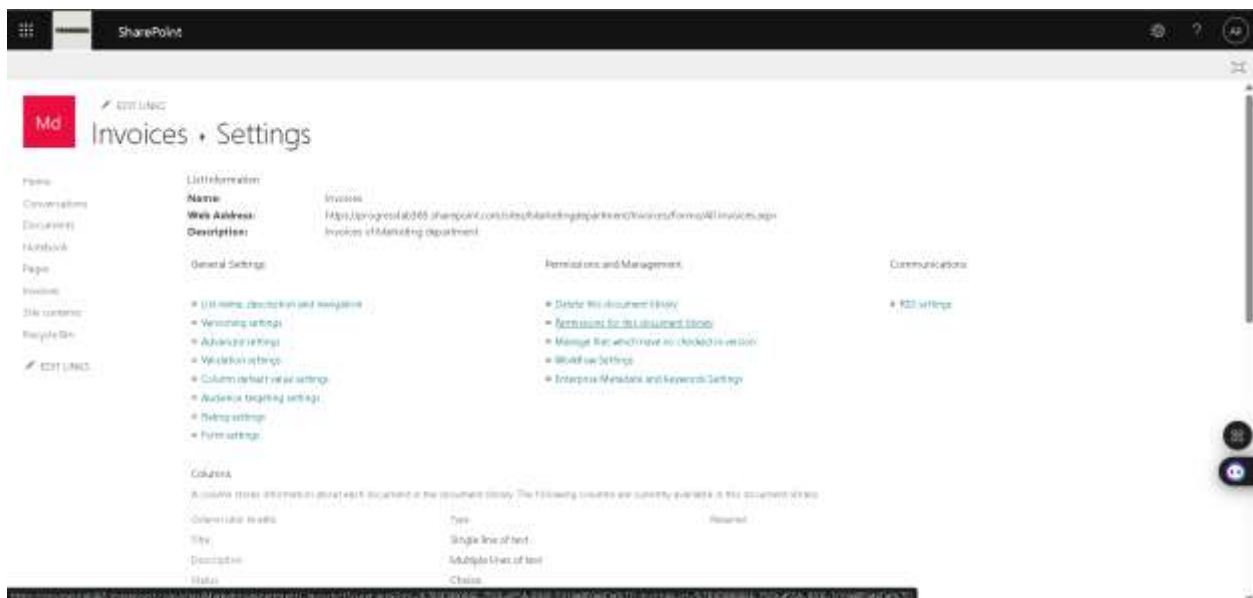
Step 6: Invoices library has been created, now select settings sign -> library settings.



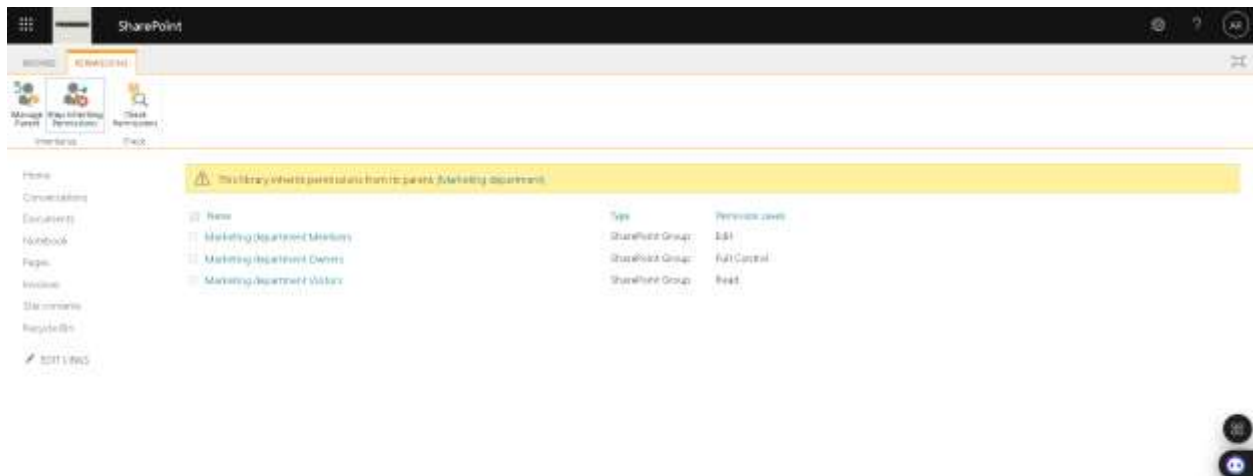
Step 7: Click on more library settings now.



Step 8: Now, select under Permissions & Management ->permissions for this document library.

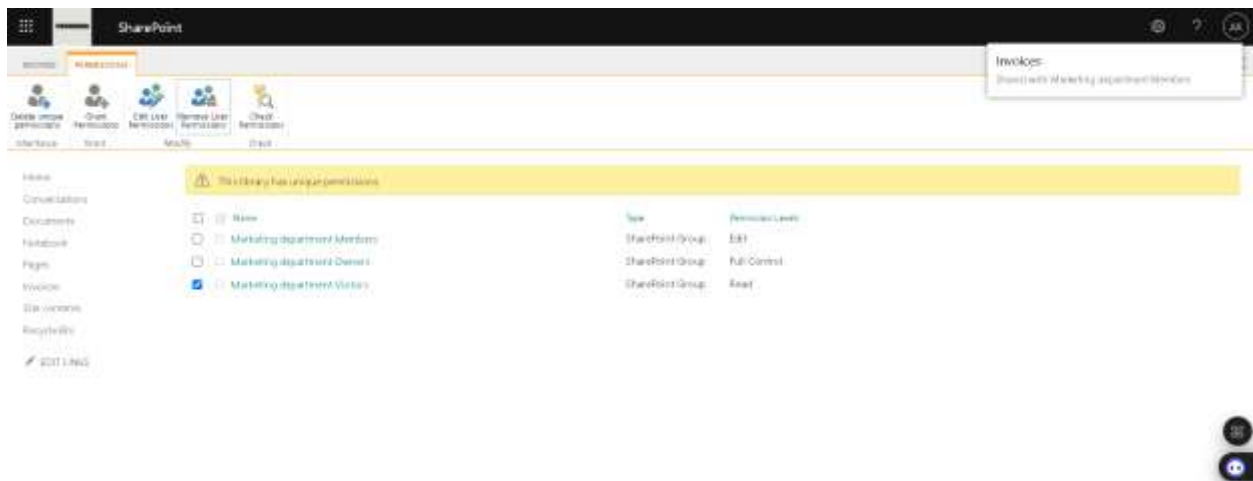


Step 9: First, click on stop inheriting permissions, so that we can add custom permissions to this library.



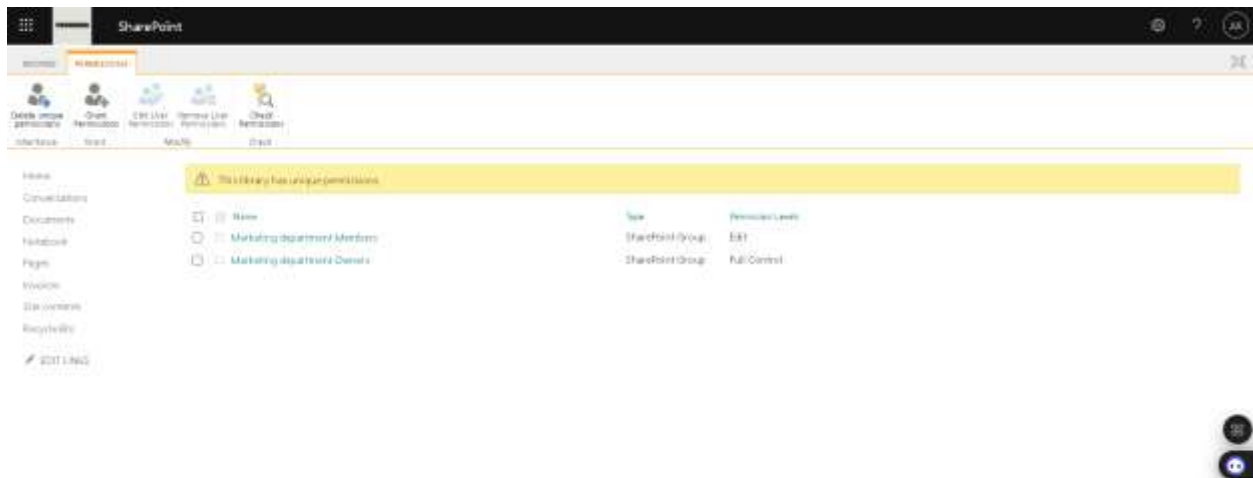
Screenshot

Step 10: As this is invoices of Marketing department, we don't want visitors to even read this library. So, we will select It department visitors then remove user permissions.



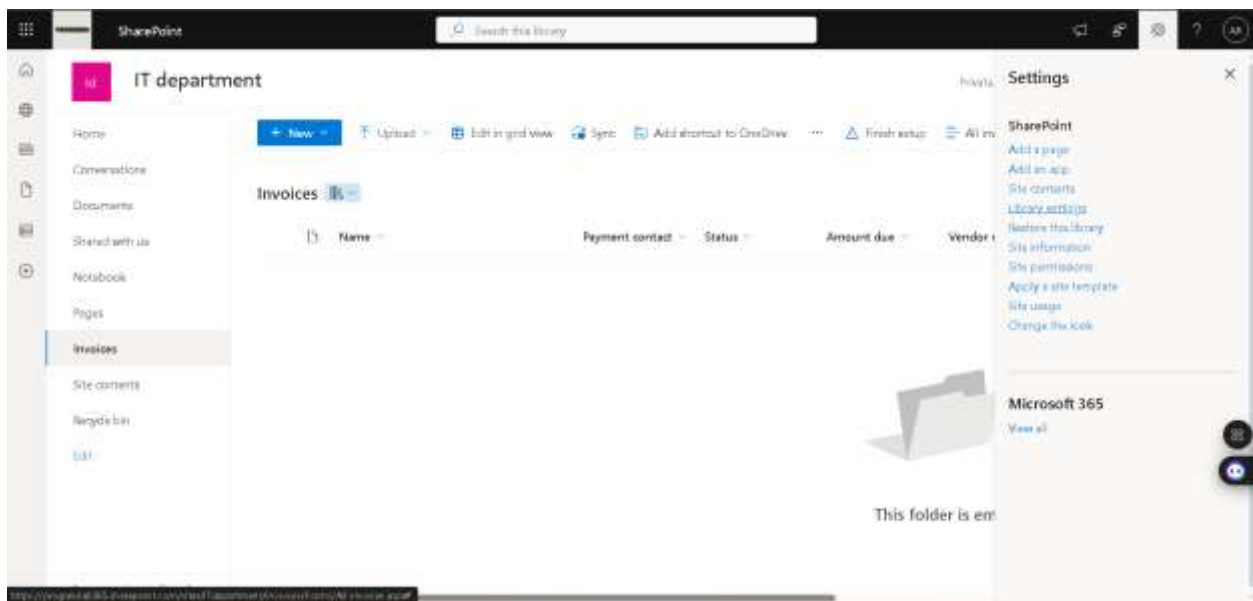
Screenshot

Step 11: Now for this library, we have only members which we need.

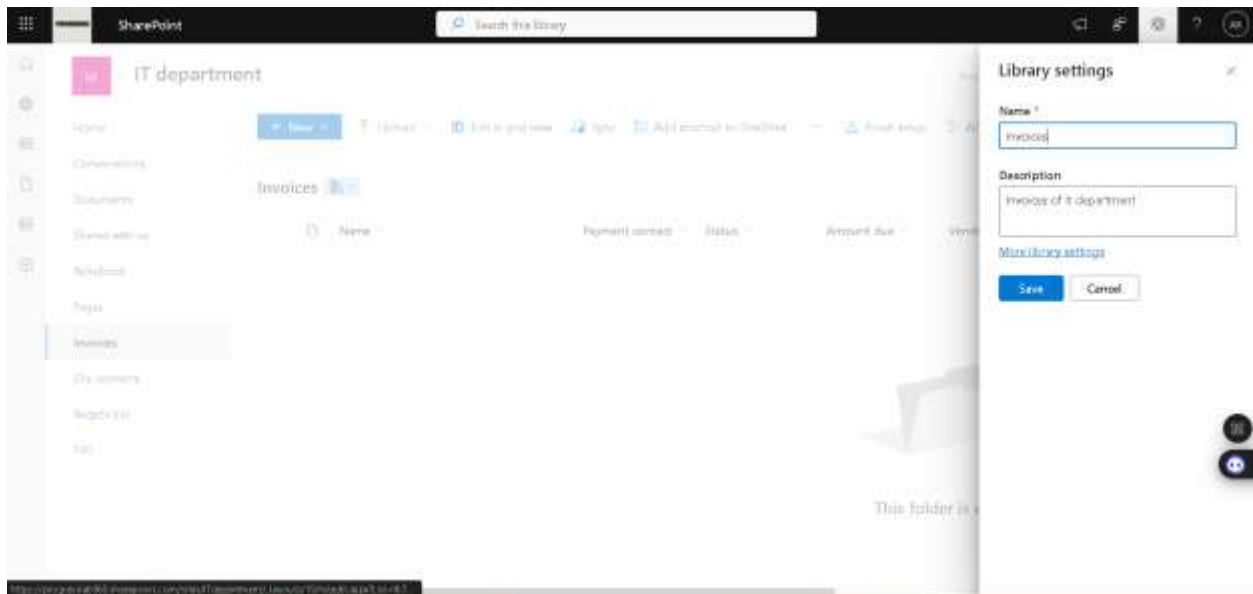


- Enable versioning and content approval for the HR document library.

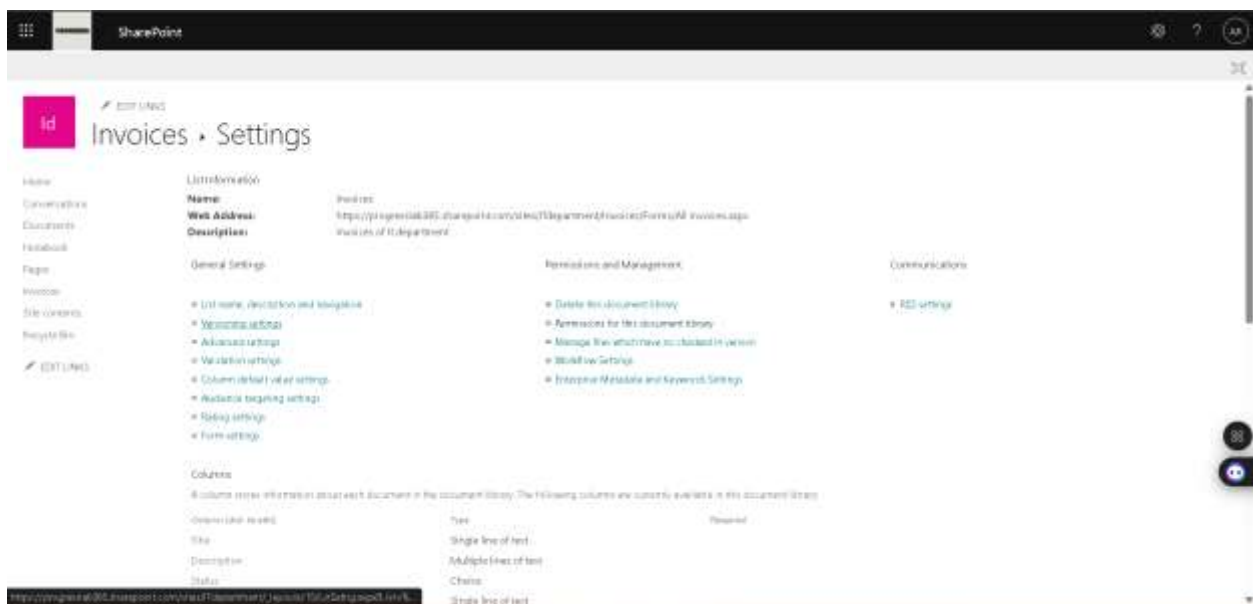
Step 1: We selected IT department SharePoint Site, under invoices (as we want to enable versioning and content approval) click on settings sign -> library settings.



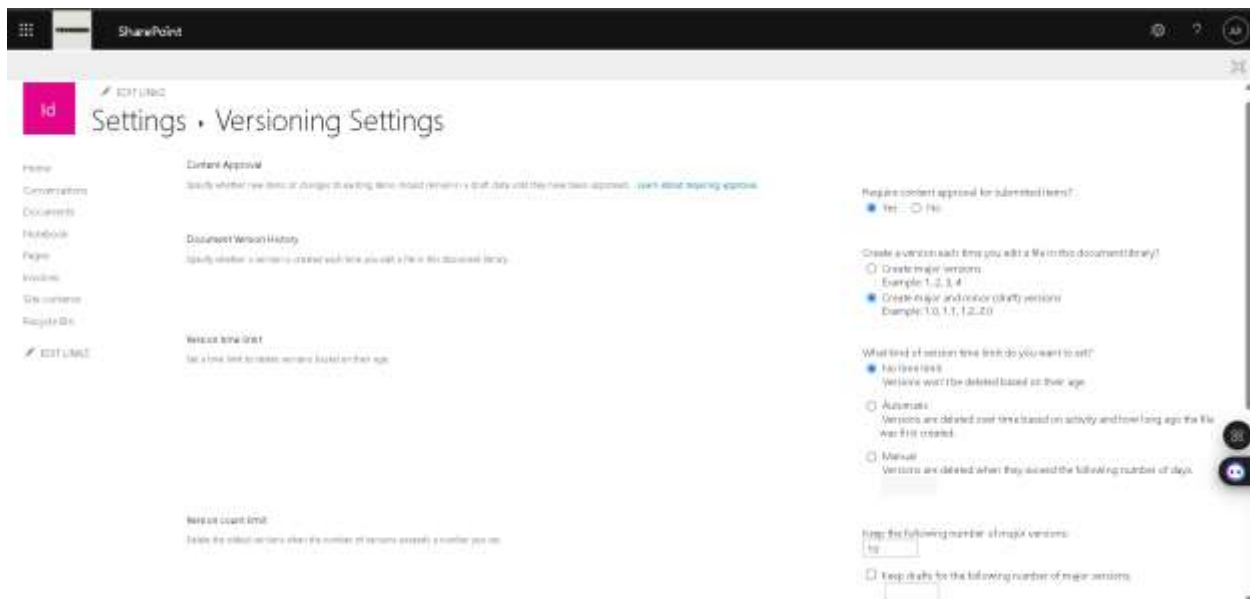
Step 2: Click on more library settings.



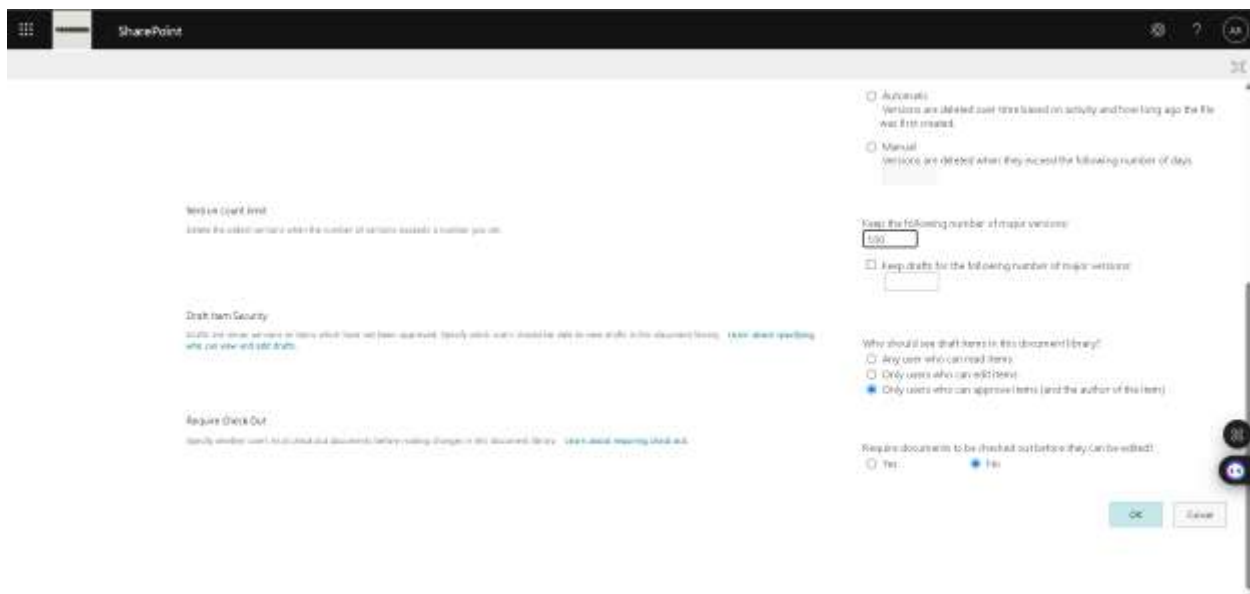
Step 3: Now under global settings, click on versioning settings.



Step 4: Choose all the versioning settings we need like create major and minor versions.



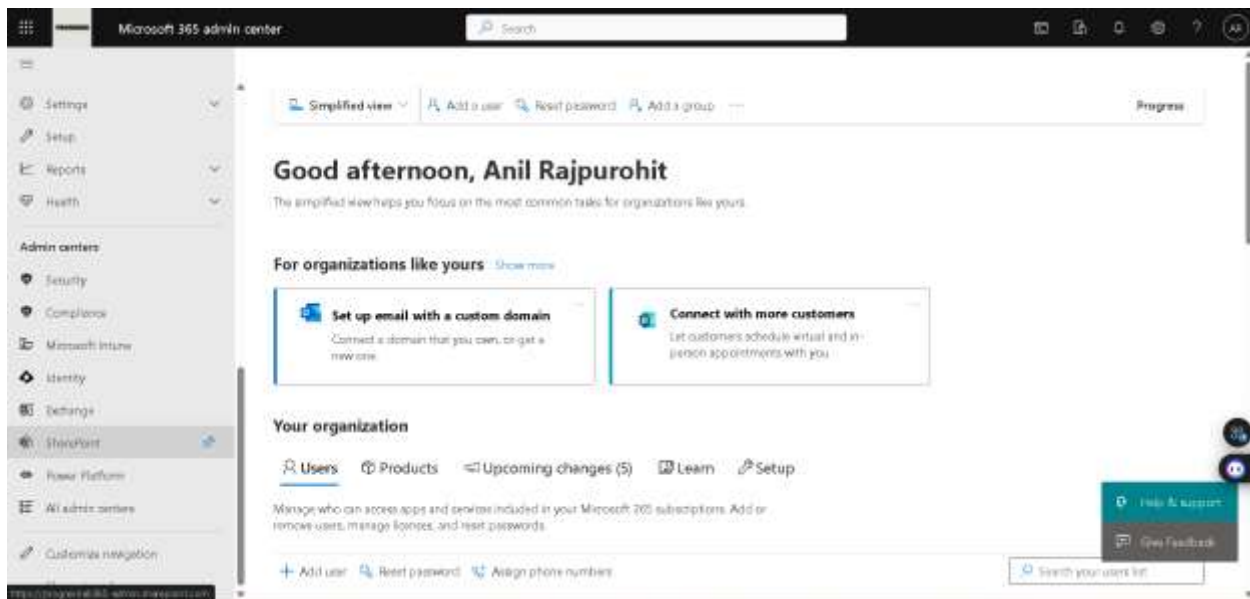
Step 5: We choose 100 as major version, as this is minimum limit and 500 is maximum. Select other settings then OK.



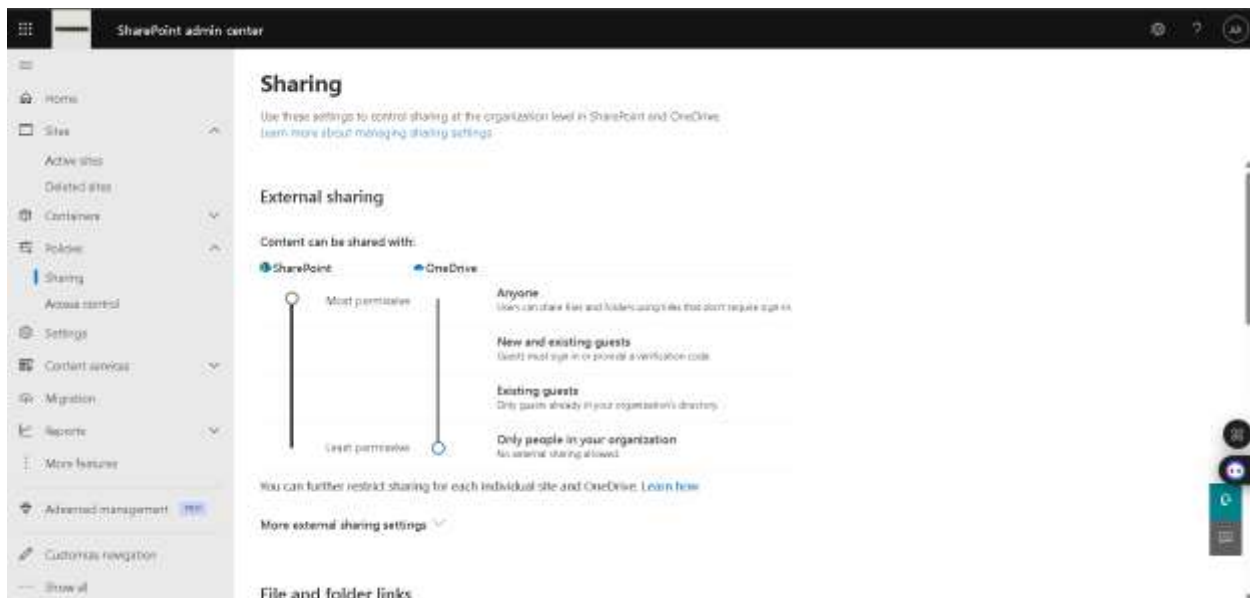
2. Implement OneDrive for Business:

- Configure OneDrive settings to restrict external sharing.

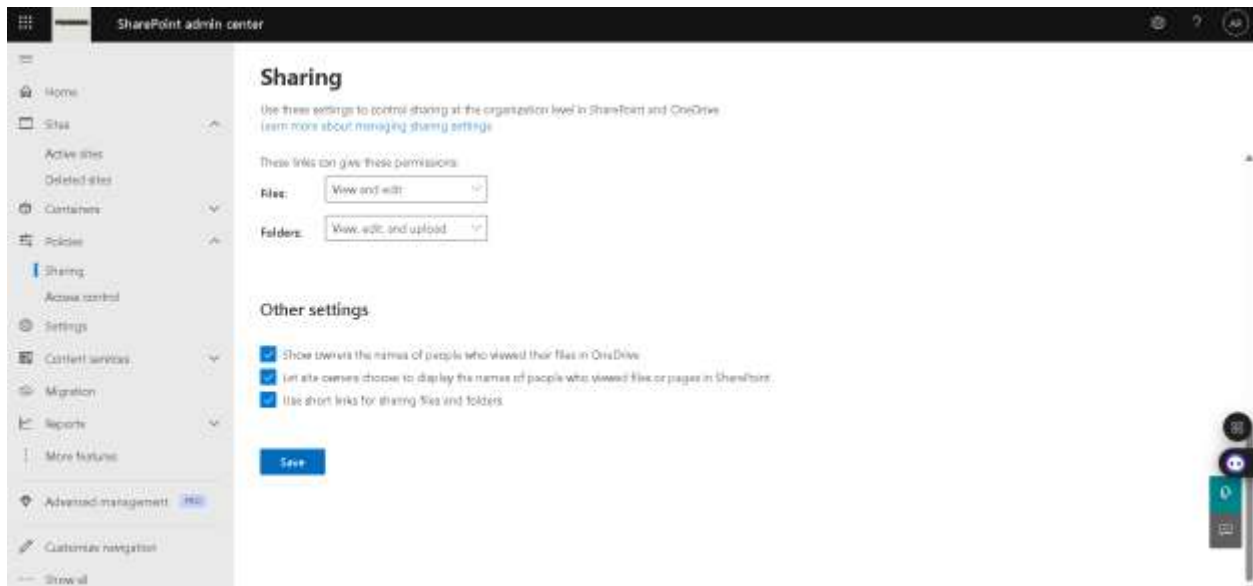
Step 1: From Microsoft 365 admin center, under admin centers -> SharePoint.



Step 2: For managing global settings, from SharePoint admin center -> policies -> sharing. As we want our OneDrive to restrict external settings. So, we move our bar to Only people in your organization option.

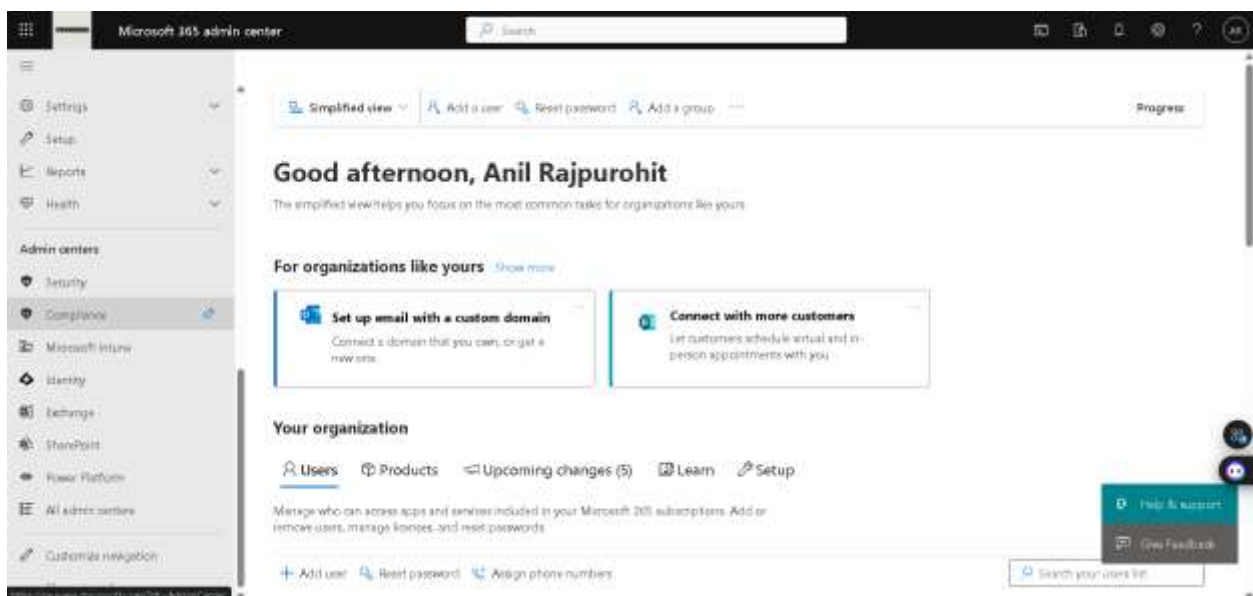


Step 3: Click on save to Save our OneDrive settings globally.

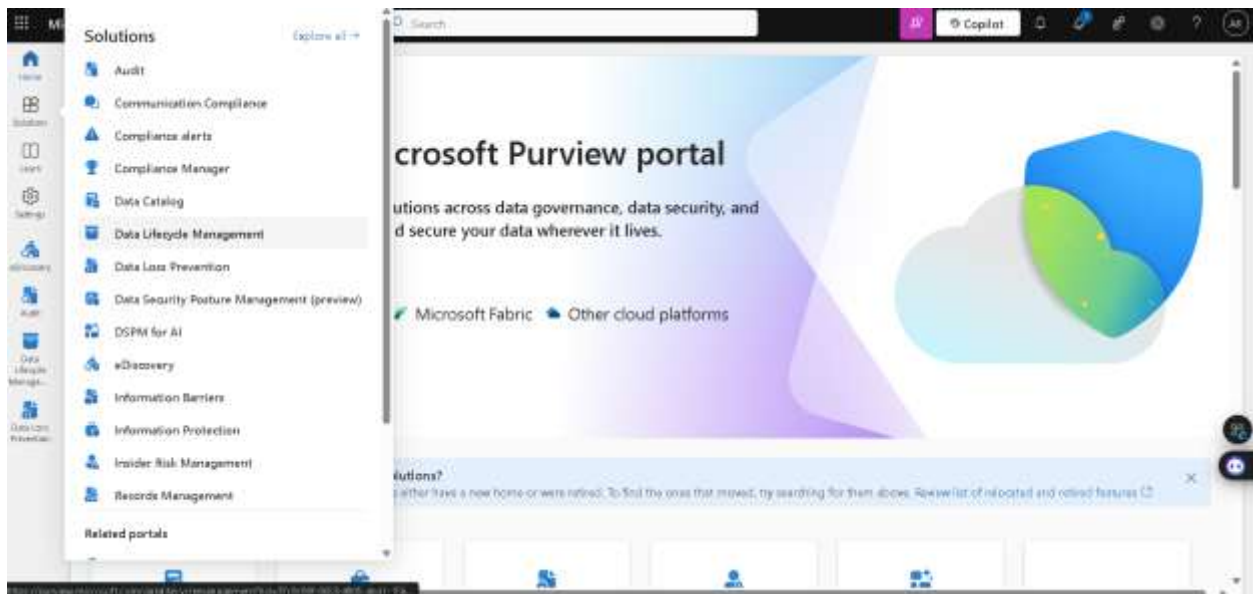


- Enable file retention policies to ensure data is retained for at least five years.

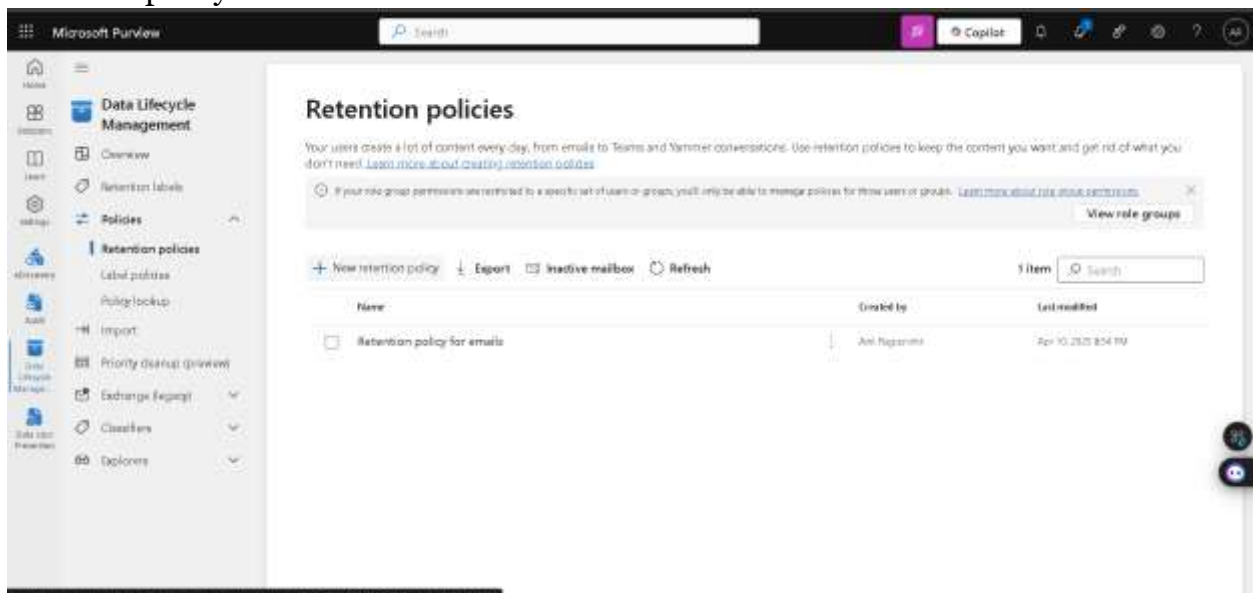
Step 1: From Microsoft 365 admin center, under admin centers select compliance to access Purview portal.



Step 2: To create retention policy for data. In Microsoft Purview, go to Solutions ->Data Lifecycle Management.



Step 3: In Data Lifecycle Management, under policies -> retention policies -> New retention policy.



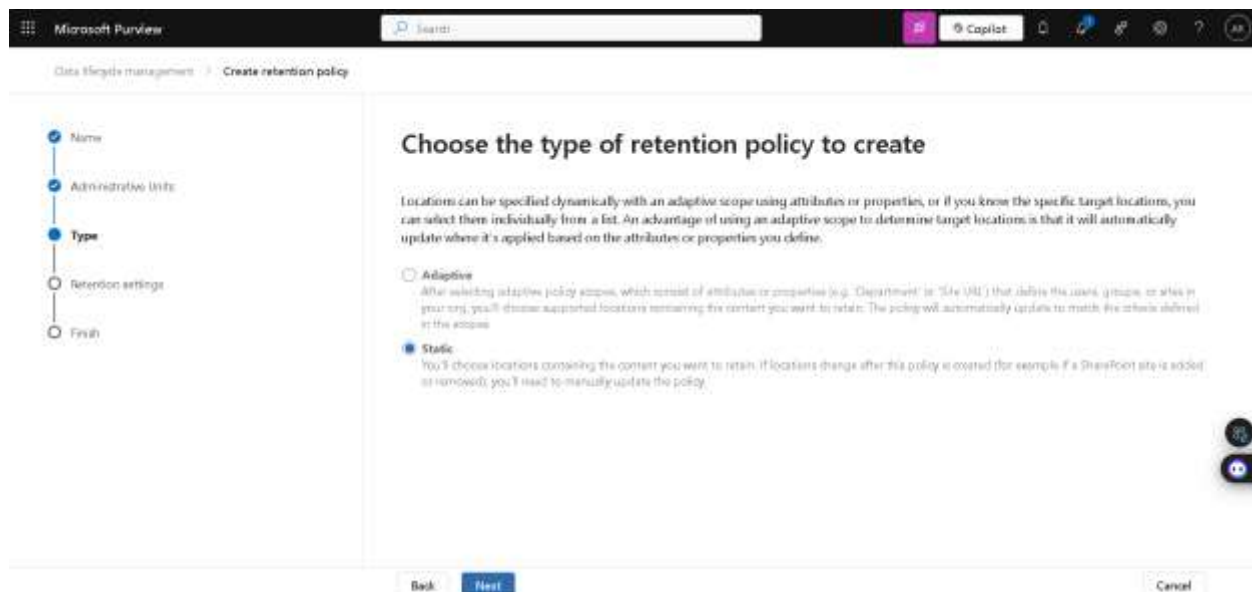
Step 4: Provide name and description for your retention policy.

The screenshot shows the 'Name your retention policy' step in the Microsoft Purview interface. On the left, a vertical navigation pane lists the steps: Name (selected), Administrative units, Type, Retention settings, and Finish. The main area has a title 'Name your retention policy'. Below the title, there is a 'Name *' field with the text 'Retention policy for data'. Below that is a 'Description' field with the text 'To keep data retained for at least five years:'. At the bottom of the main area, there are 'Next' and 'Cancel' buttons.

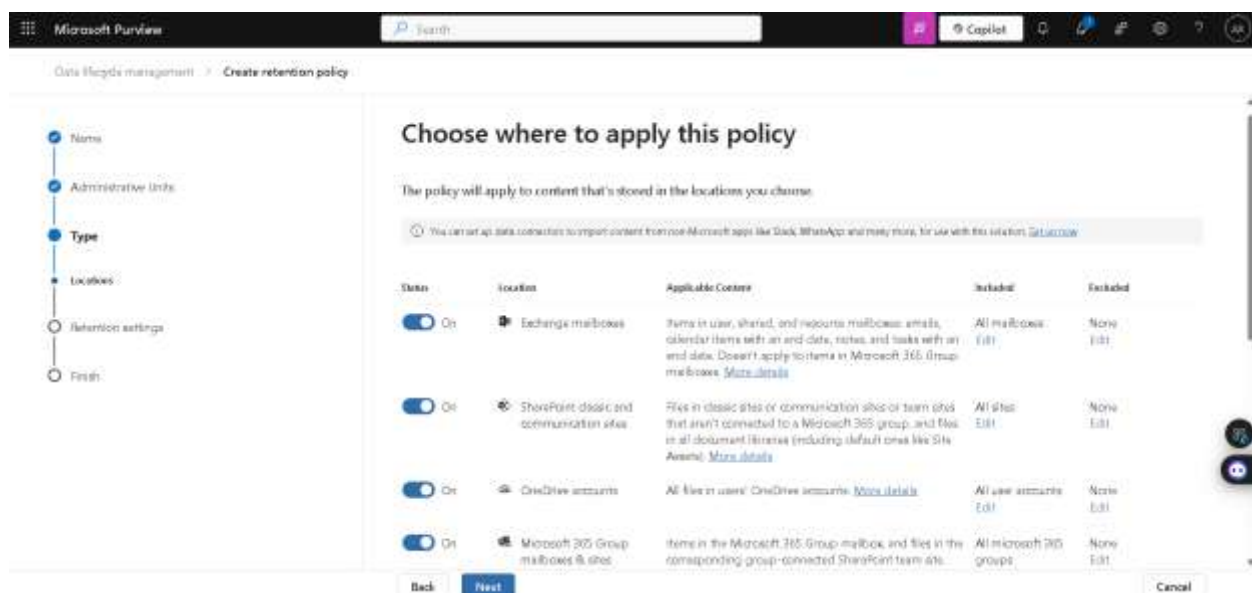
Step 5: As we haven't created any admin units, we won't be able to assign any admin units here. So, we keep it as full directory and click on next.

The screenshot shows the 'Policy Scope' step in the Microsoft Purview interface. On the left, the vertical navigation pane lists the steps: Name, Administrative Units (selected), Type, Retention settings, and Finish. The main area has a title 'Policy Scope'. Below the title, there is a text block: 'Choose the admin units you'd like to apply this policy to. Your selections will effect the options you have at the locations selection step.' Below this is a '+ Add or remove admin units' button. Underneath is a section titled 'Admin Units' with a single option 'Full directory'. At the bottom of the main area, there are 'Back', 'Next', and 'Cancel' buttons.

Step 6: Now we have two options adaptive and static, adaptive is better overall as it will update with our attributes and properties. But we are going with static and click on next.



Step 7: Choose all locations where we want to apply this policy, then click in next.



Step 8: Now, we can set the retention period here, So we go to retain items for a specific period ->5 years.

Microsoft Purview | Search | Copilot

Data lifecycle management > Create retention policy

Decide if you want to retain content, delete it, or both

- ☒ **Retain items for a specific period**
Items will be retained for the period you choose.
 - Retain items for a specific period: 5 years
 - Start the retention period based on: When items were created
 - At the end of the retention period:
 - ☒ Delete items automatically
 - ☐ Do nothing
- ☐ **Retain items forever**
Items will be retained forever, even if users delete them.
- ☐ **Only delete items when they reach a certain age**
Items won't be retained, but when they reach the age you choose, we'll delete them from where they're placed.

Back Next Cancel

Step 9: Here we will review the policy details and click on Submit.

Microsoft Purview | Search | Copilot

Data lifecycle management > Create retention policy

Review and finish

It will take up to a week to apply this policy to the locations you selected.

Policy name
Retention policy for data
[Edit](#)

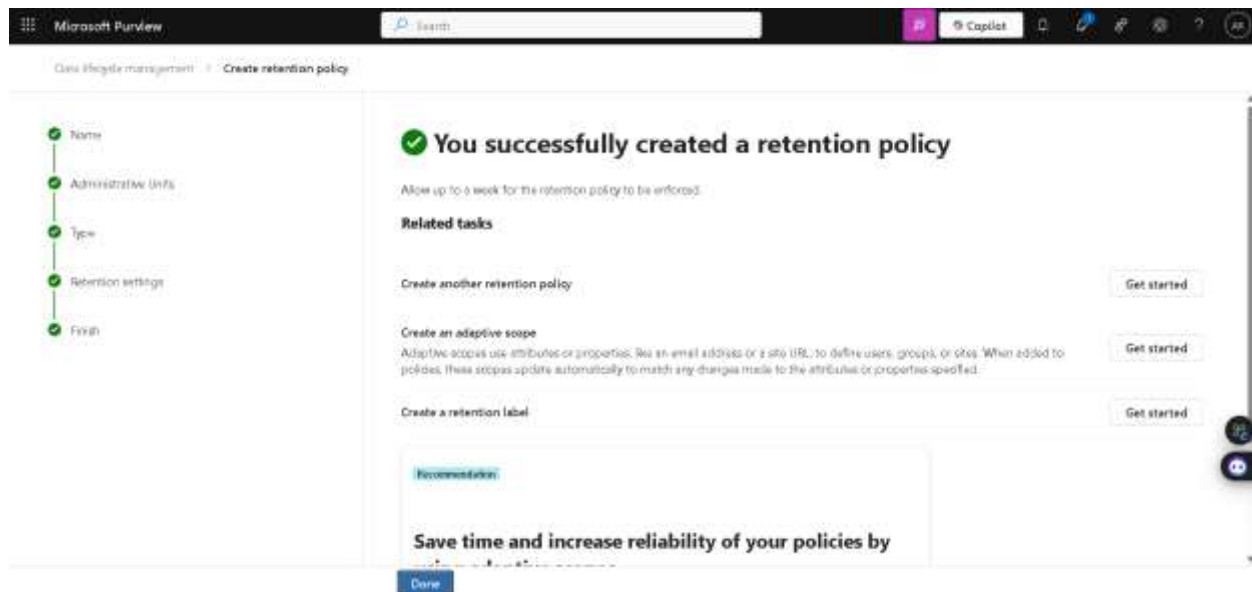
Description
To keep data retained for at least five years
[Edit](#)

Locations to apply the policy
Exchange mailboxes (All Recipients)
SharePoint classic and communication sites (All Sites)
OneDrive accounts (All Sites)
Microsoft 365 Group mailboxes & sites (All Groups)
[Edit](#)

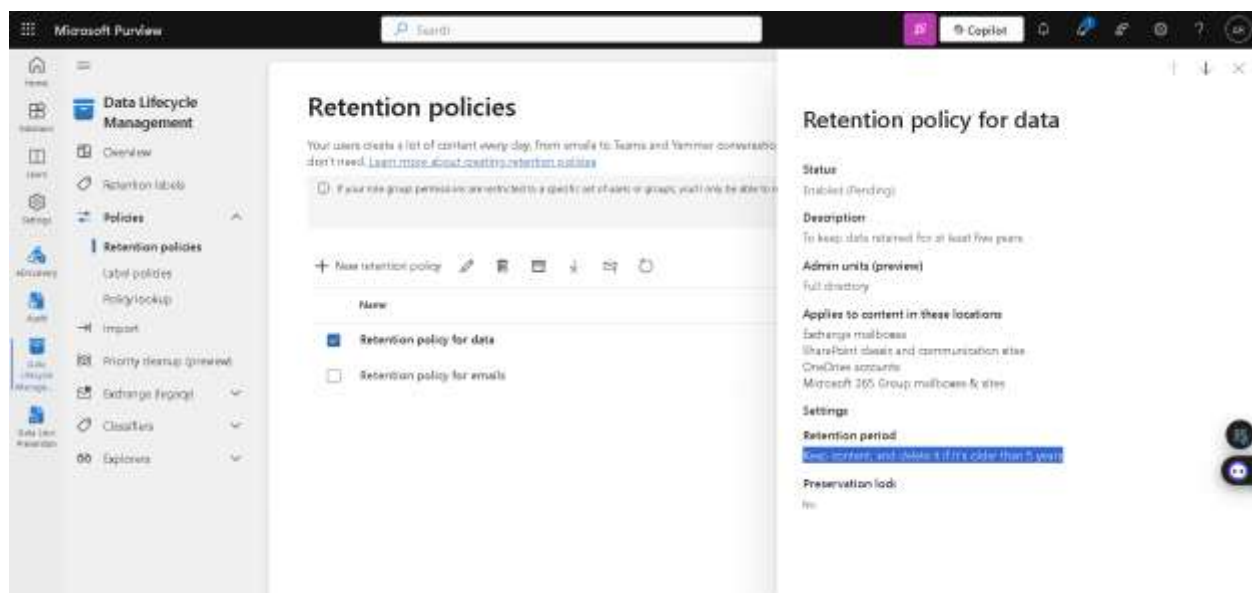
Retention settings
Retain items for 5 years based on when they were created
Delete items at end of retention period
[Edit](#)

Back Submit Cancel

Step 10: Our retention has been successfully created.



Step 11: We can view our policy now under Retention policies.



- Set up a policy to automatically move old files to the Recycle Bin after a year.

Step 1: In Microsoft Purview -> solutions -> Data lifecycle management -> retention labels -> create a label.



Step 2: Fill all the details here like name, description, and description for admins then Next.

Step 3: Select, retain items forever or a specific period then click on Next.

Microsoft Purview Search Copilot

Create retention label

Home Label Settings **Period** Finish

Define label settings

We'll apply the settings you choose to labeled items.

- ☒ **Retain items forever or for a specific period**
Labeled items can't be permanently deleted during this period. You'll define how long the retention period is and what happens to items during and after the retention period in the next steps.
- ☐ **Enforce actions after a specific period**
Labeled items won't be retained. You can decide whether they should be deleted, or relabeled when the period you specify in the next step ends.
- ☐ **Just label items**
Choose this setting if you only want to classify labeled items. The items won't be retained and your users won't be restricted from editing, moving, or deleting them.

Back Next Cancel

Step 4: Now, as we only want to retain old files for one year then move to recycle bin. Select, retain items as 1 year then next.

Microsoft Purview Search Copilot

Create retention label

Home Label Settings **Period** Finish

Define the retention period

Specify how long the retention period should be.

Retain items for
Custom

of 1 years 0 months 0 days

Start the retention period based on
When items were created

+ Create new event type

Back Next Cancel

Step 5: This label won't send files to the Recycle Bin literally, but it **deletes** them after a year — files then go to the **Recycle Bin**, where they remain for 93 days by default. Now select delete items automatically then next.

Create retention label

Step 6: Choose what happens after the retention period

These settings determine what happens to items when the retention period ends.

- ☒ **Delete items automatically**
We'll permanently remove labeled items from wherever they're stored.
- ☐ **Start a disposition review**
Let the disposition reviewers you assign in the next step decide if items can be safely deleted or whether other actions (such as changing the retention period) should be taken. [Learn more](#)
- ☐ **Change the label**
You can extend the period by choosing an existing label to replace this one with. [Learn more about relabeling items](#)
- ☐ **Run a Power Automate flow**
Customize what happens to labeled items with a Power Automate flow. You can run a flow to meet a specific business need, such as moving labeled items to a custom location or sending email notifications. [Learn more about running a Power Automate flow](#)
- ☐ **Deactivate retention settings**
Labeled items won't be retained or deleted when their retention settings are deactivated. You'll have to manually remove any items that you want deleted.

Buttons: Back, Next, Cancel

Step 6: Review retention label details then click on create label.

Create retention label

Step 7: Review and finish

Name

Name: Delete Files After 1 Year
[Edit](#)

Description for users

Auto-Delete Files After 1 Year
[Edit](#)

Description for admins

Label to delete files after 1 year from organization
[Edit](#)

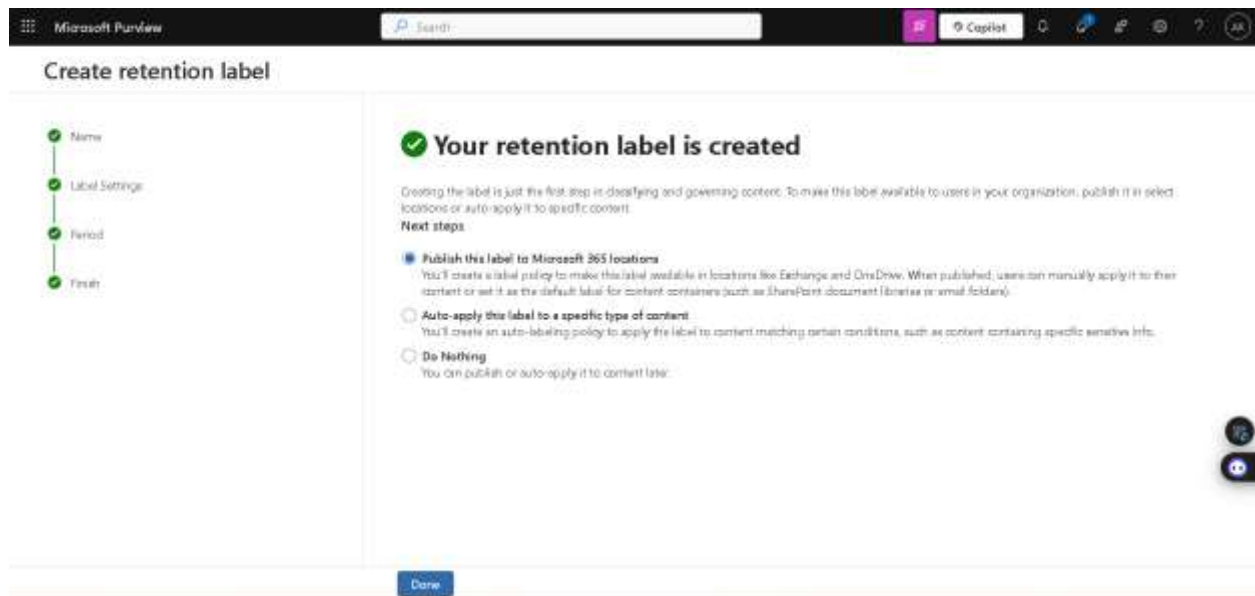
Retention settings

Retention period: 1 year
[Edit](#)

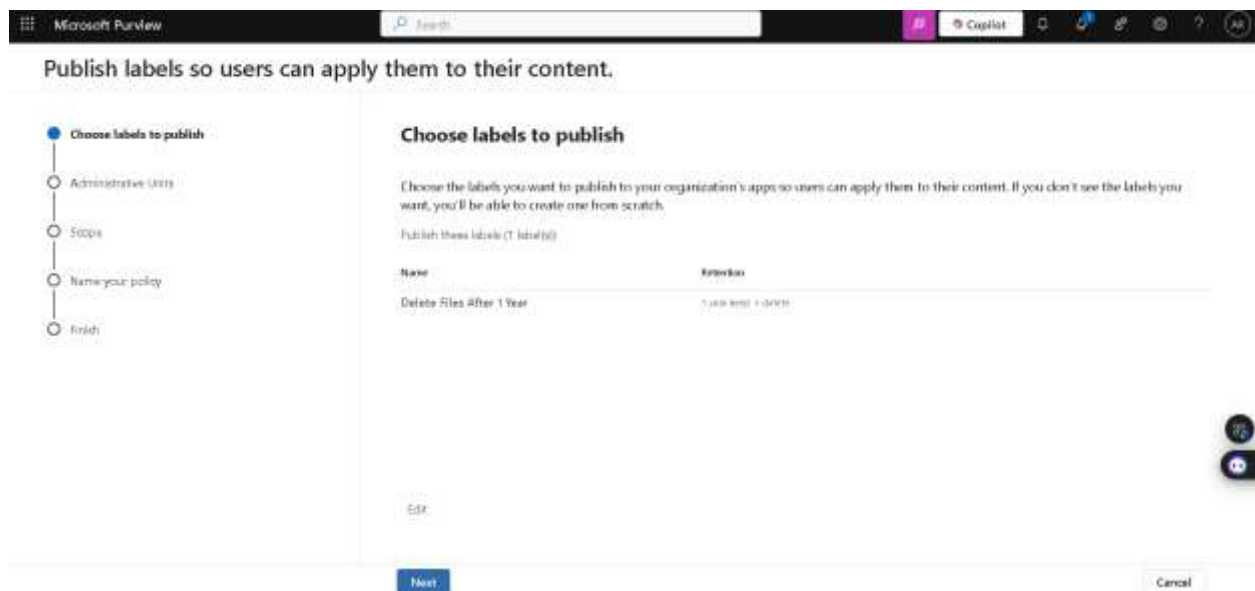
Retention action: Delete and Delete
[Edit](#)

Buttons: Back, Create label, Cancel

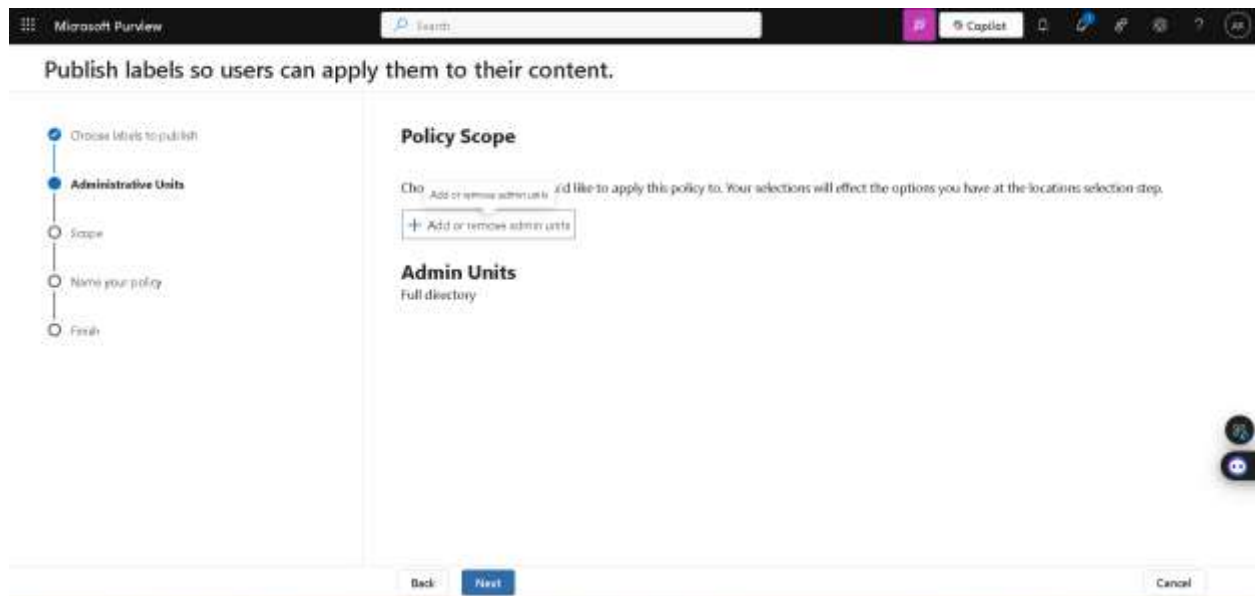
Step 7: Our retention label has been successfully created, now select publish this label to Microsoft 365 locations then done.



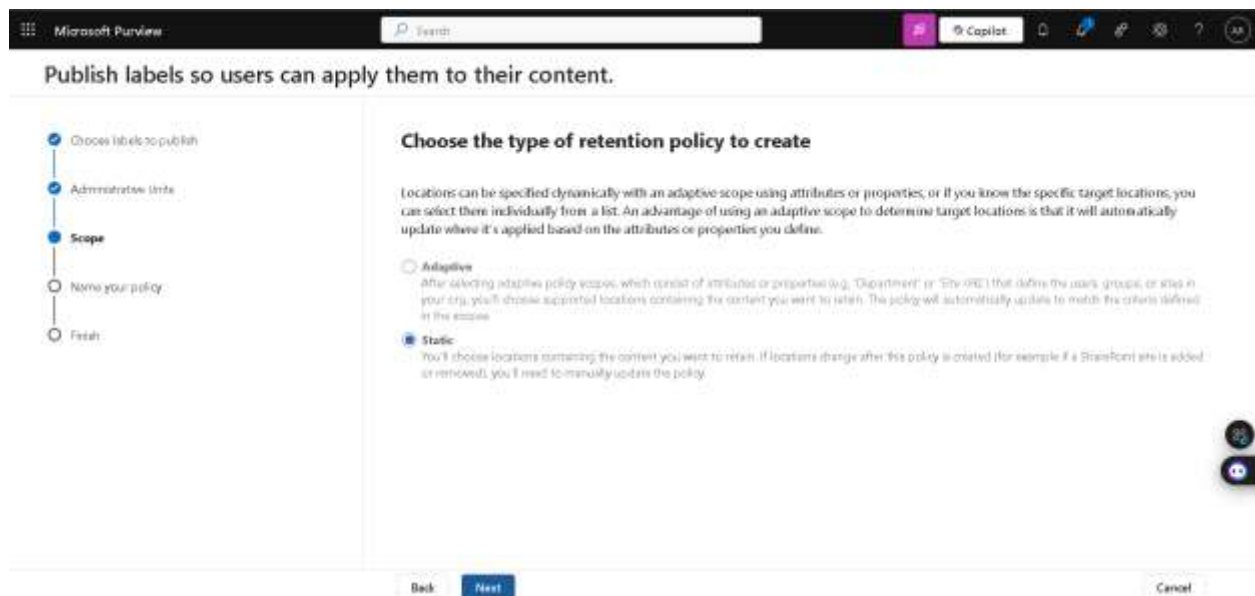
Step 8: Now we are using this label to create the policy, click on next.



Step 9: As we want to apply this policy to whole organization, we keep it as full directory then next.



Step 10: Now we have two options adaptive and static, adaptive is better overall as it will update with our attributes and properties. But we are going with static and click on next.



Step 11: We will publish this policy to all locations, then click on next.

Microsoft Purview Search Copilot

Publish labels so users can apply them to their content.

Choose labels to publish Administrative Units Scope **Publish to users and groups** Name your policy Finish

Choose where to publish labels

When published, users in your organization will be able to apply this label to items in the locations you choose.

☐ You can set up data connectors to import content from non-Microsoft apps like Slack, WhatsApp and many more, for use with this solution. [Get started](#)

☒ All locations: Include content in Exchange email, Office 365 groups, OneDrive and SharePoint documents

☐ Let me choose specific locations

Back Next Cancel

Step 12: Provide name and description for the new policy then next.

Microsoft Purview Search Copilot

Publish labels so users can apply them to their content.

Choose labels to publish Administrative Units Scope **Name your policy** Finish

Name your policy

Name *

Delete After 1 Year

Description

Delete After 1 Year

Back Next Cancel

Step 13: Review policy details and click on submit.

Microsoft Purview

Search

Copilot

Publish labels so users can apply them to their content.

Choose labels to publish

Administrative limits

Scope

Name your policy

Finish

Finish

Most labels will become available to your users within a week. Labels will appear in Outlook and Outlook on the web only for mailboxes that have at least 10 MB of data.

Choose labels to publish

1 label(s) will be published (made available) so your users can classify their content

Delete Files After 1 Year 1 year keep -> delete

Edit

Applies to content in these locations

Exchange mailboxes (All Recipients)

SharePoint sites and communication sites (All Sites)

OneDrive accounts (All Sites)

Microsoft 365 Group mailboxes & sites (All Groups)

Edit

Name

Delete Files After 1 Year

Edit

Description

Delete Files After 1 Year

Edit

Back Submit Cancel

Step 14: We can see our new label under Purview -> solutions -> data lifecycle management -> retention labels.

Microsoft Purview

Search

Copilot

Labels

Make labels with Records Management to access your more label settings. Create a label with Records

Create labels for items that need exceptions to your retention policies. Exceptions include items from being permanently deleted. For example, if you need even more label options, use the [label for exceptions](#)

+ -

Name

Delete Files After 1 Year

Delete Files After 1 Year

Description for admins

Label to delete files after 1 year from organization

Description for users

Auto-Delete Files After 1 Year

Retention

Retention duration	Action
1 year	Auto-delete

Type

Based on when items are created

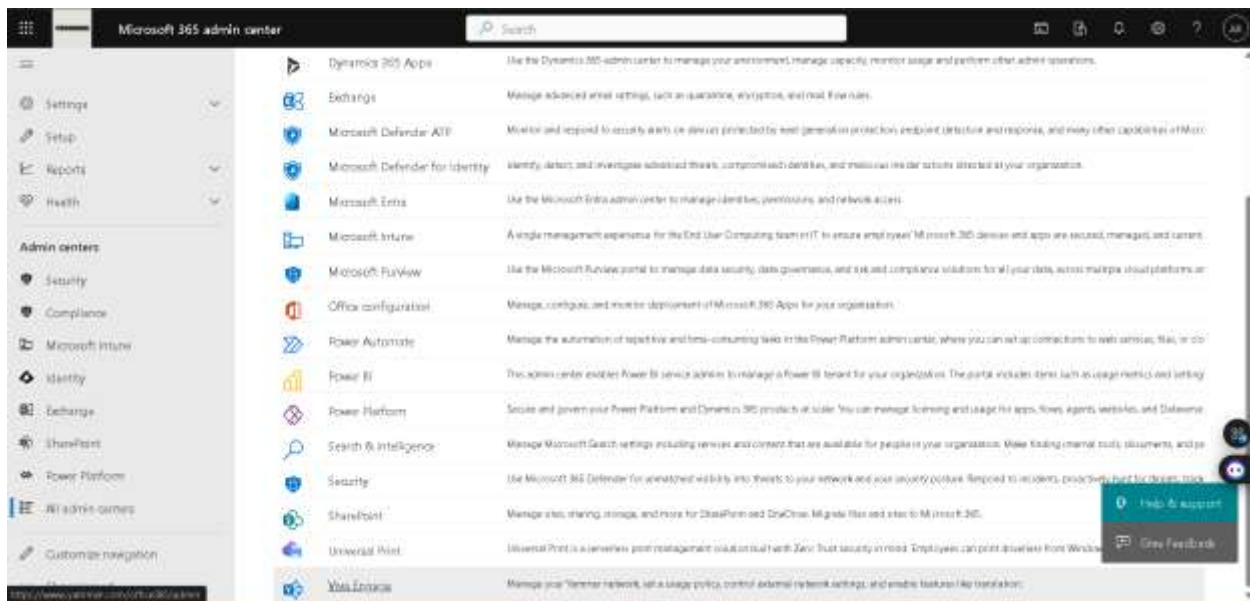
Created by	Created date
Anil Rajapathi	Apr 16, 2023, 3:05 AM

Last modified by	Last modified
Anil Rajapathi	Apr 16, 2023, 3:05 AM

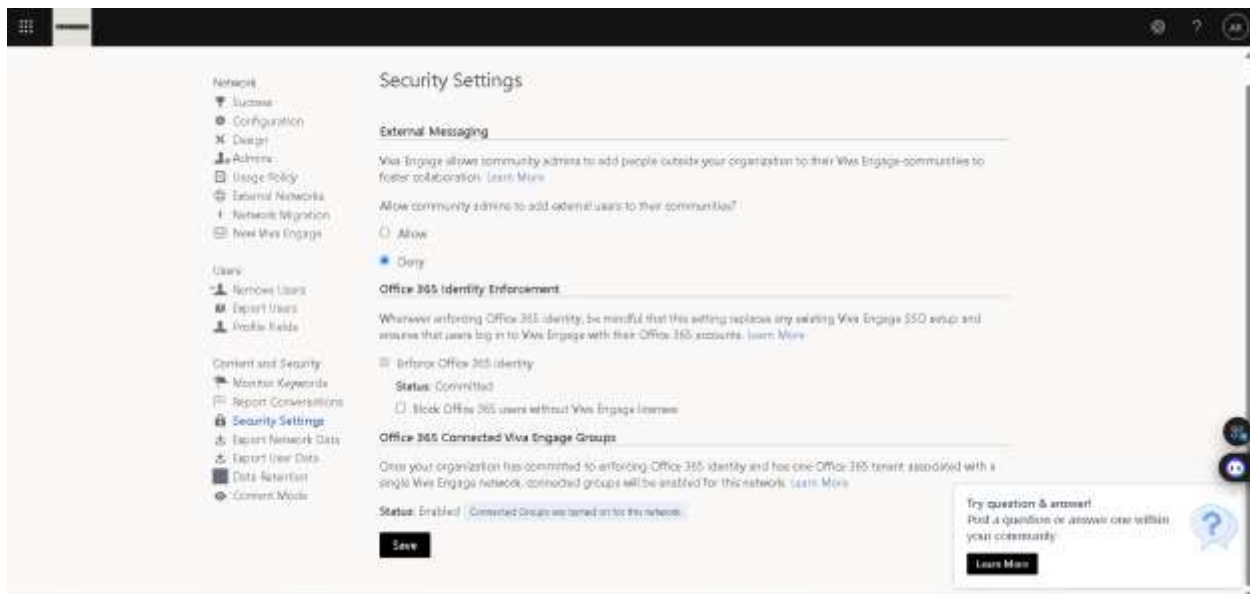
3. Set Up Viva Engage for Enterprise Social Networking:

- Configure Viva to allow only internal communications.

Step 1: From Microsoft 365 admin center, under admin centers select Viva engage.

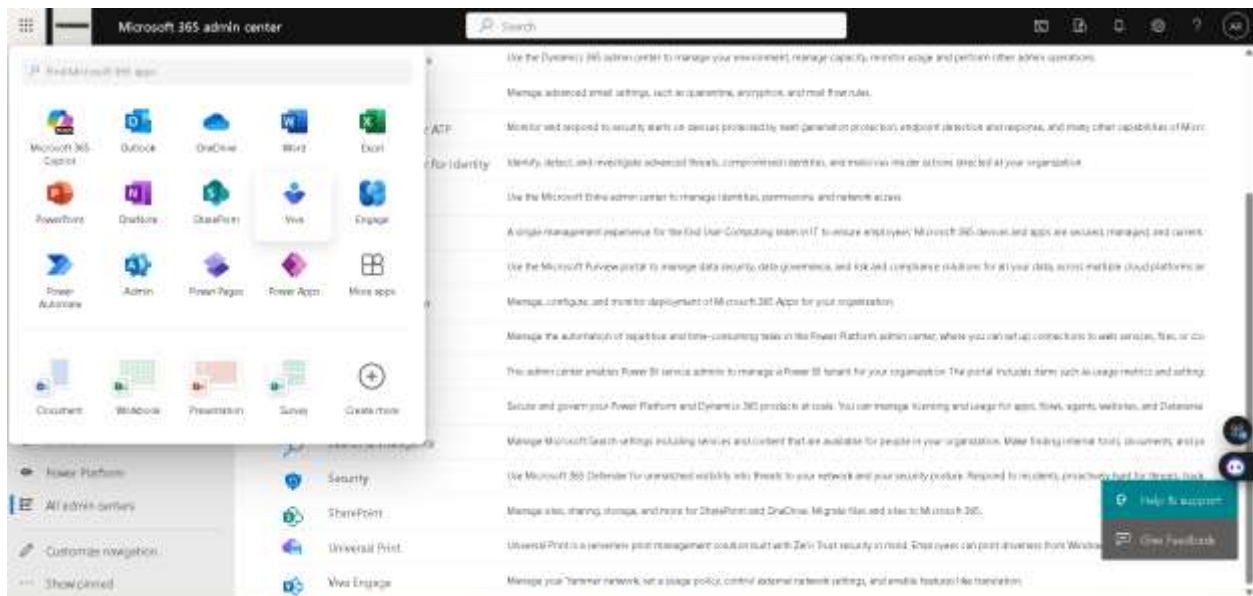


Step 2: In Viva engage admin, under security settings deny community to add users to their community then click on save.

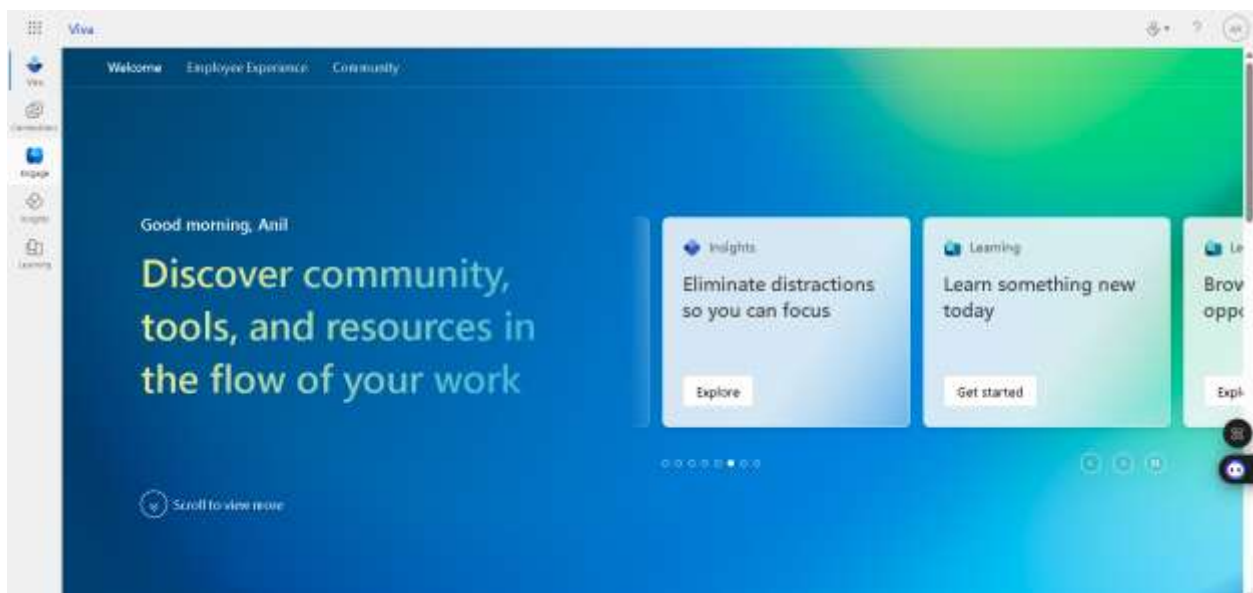


- Set up groups for company-wide announcements and department-specific discussions.

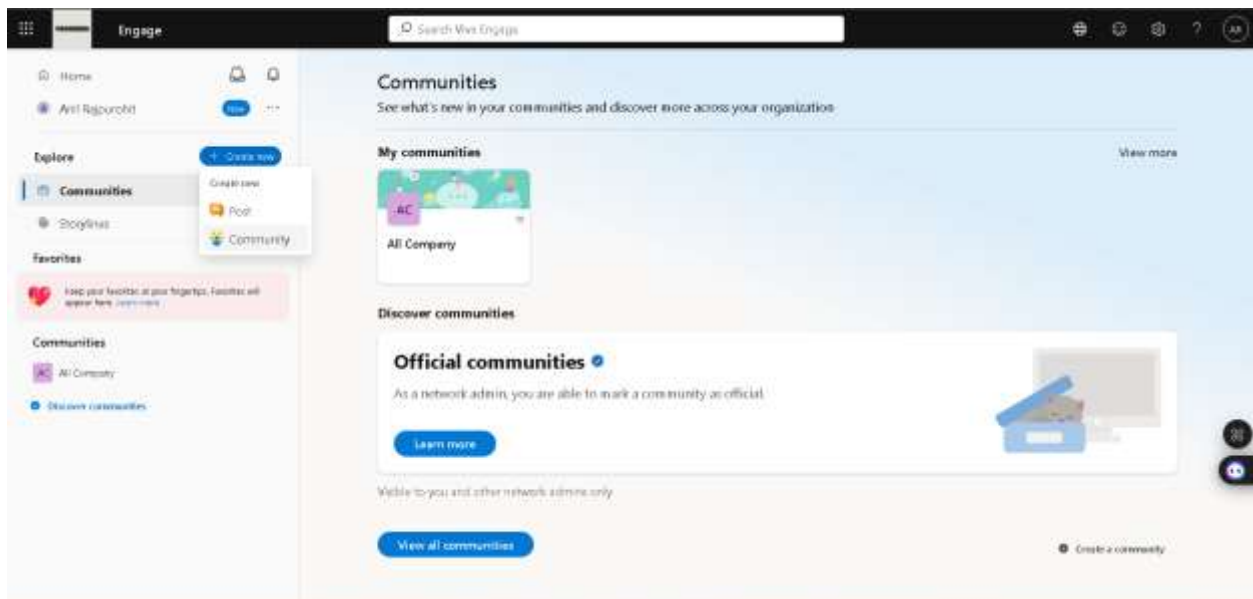
Step 1: Go to Viva portal.



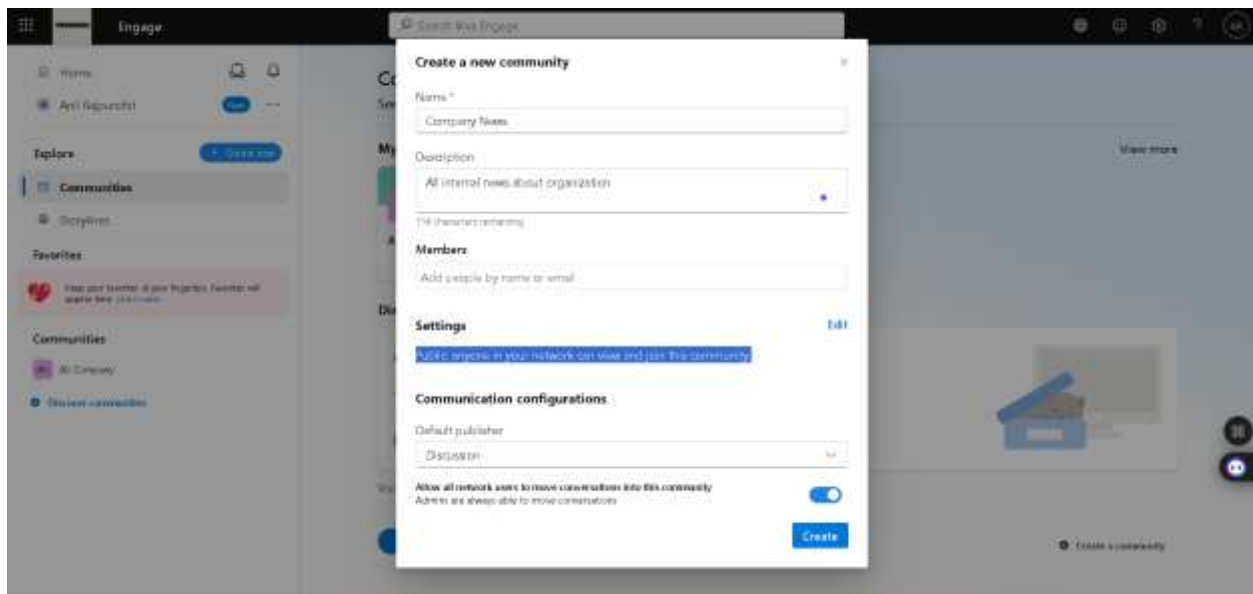
Step 2: In viva portal, go to engage.



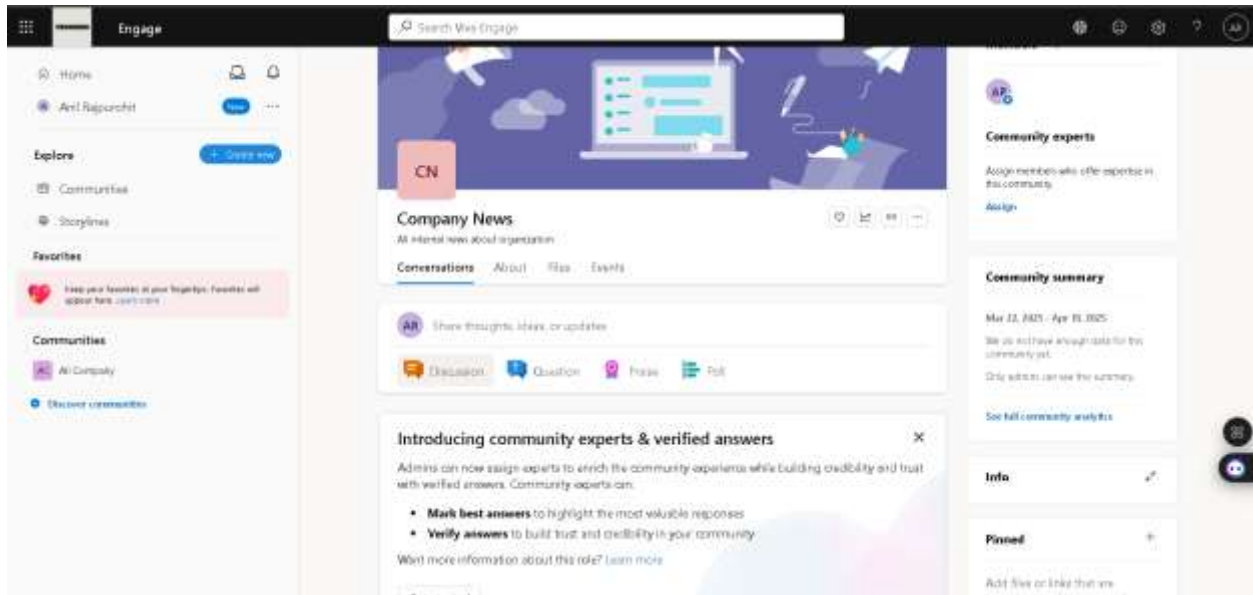
Step 3: In viva engage, under communities -> create new -> community.



Step 4: Provide community details, settings to allow anyone in our network to view and join this community then click on save.

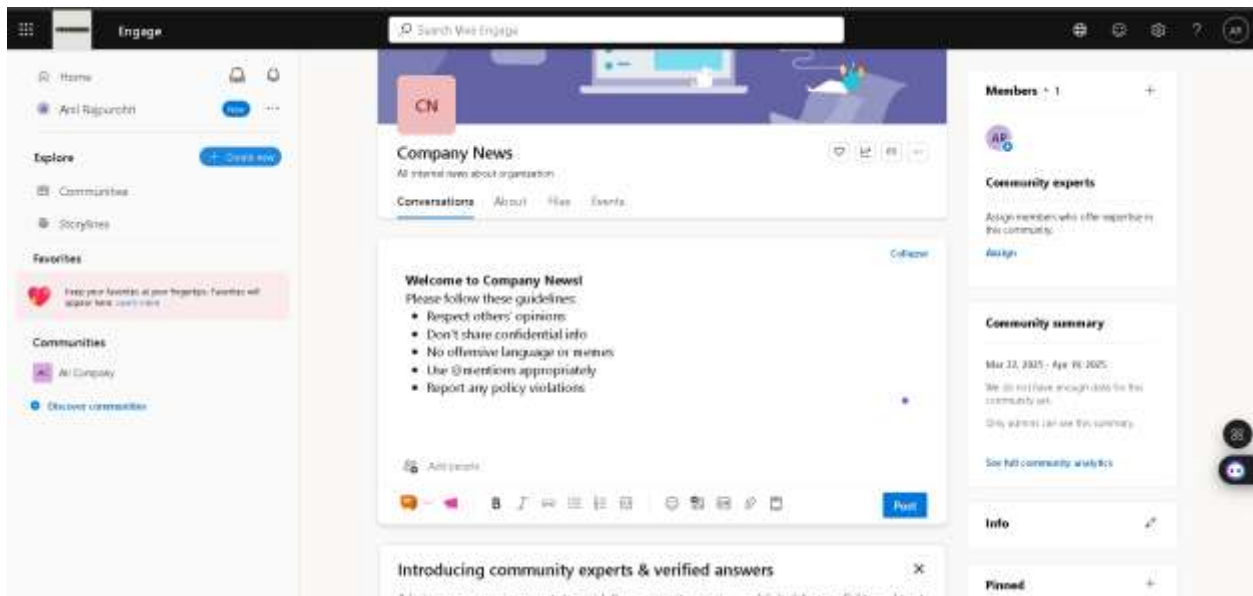


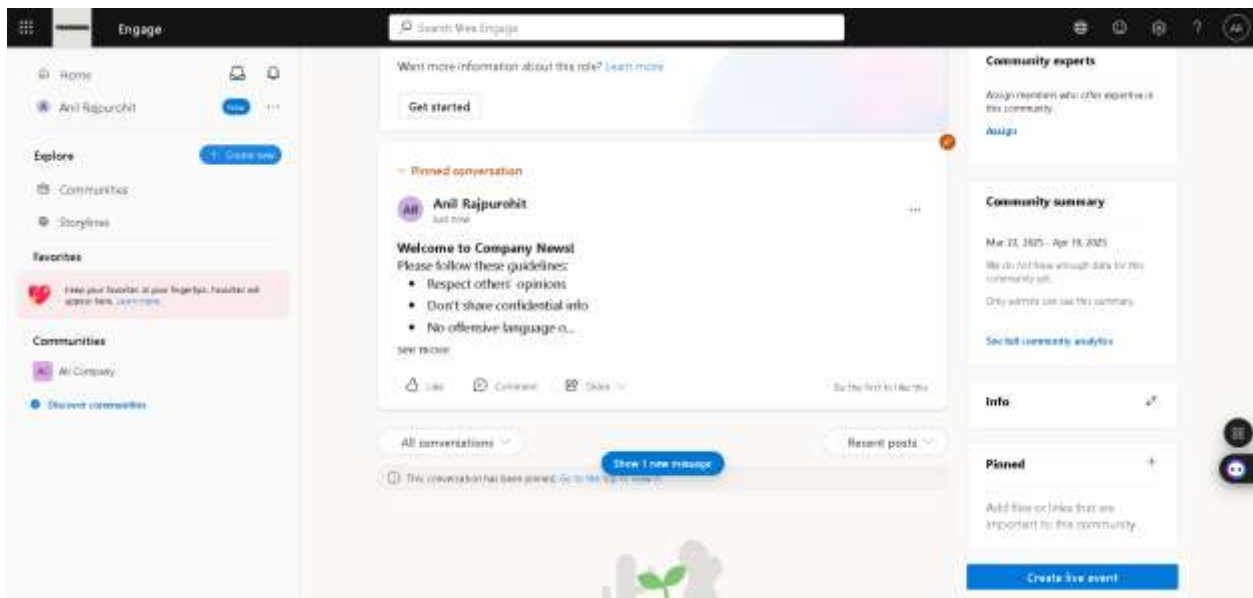
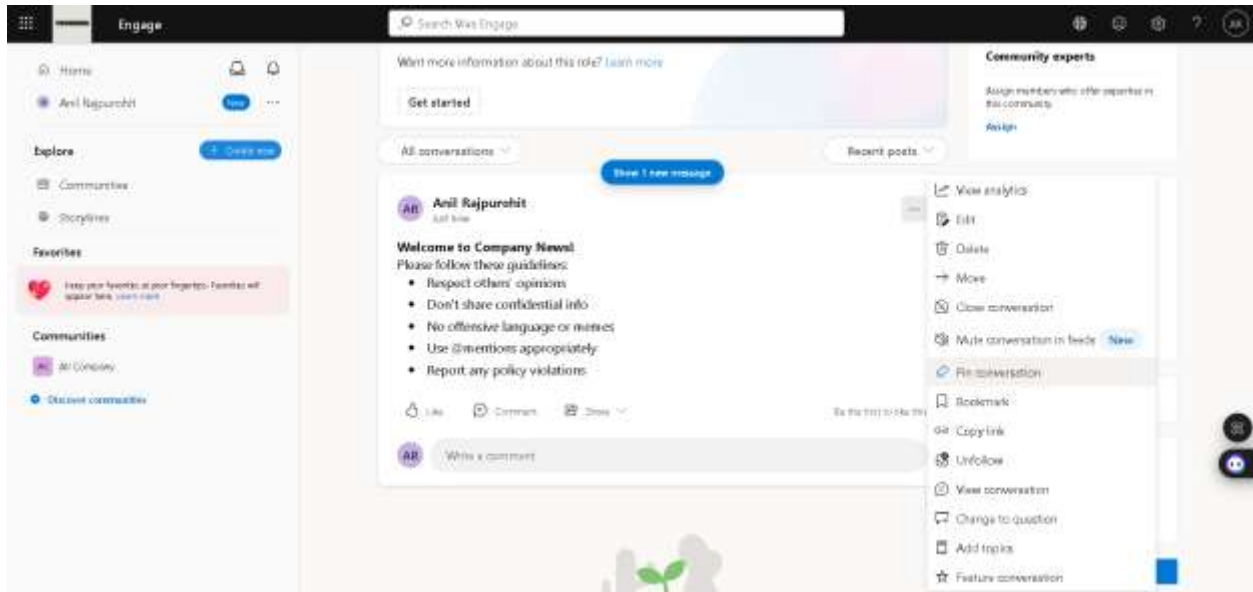
Step 5: Our new community has been successfully created.



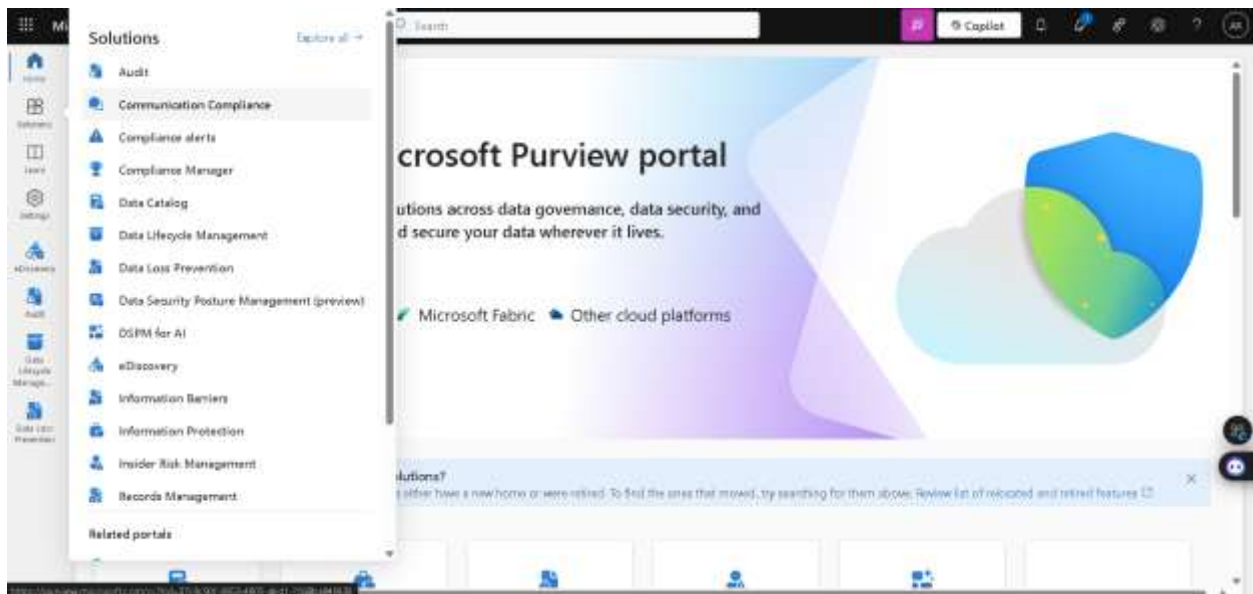
- Ensure compliance with the company's social media policy.

Step 1: First, we will post some guidelines for this community and pin it, so that everyone knows about it. E.g. No offensive language or memes.

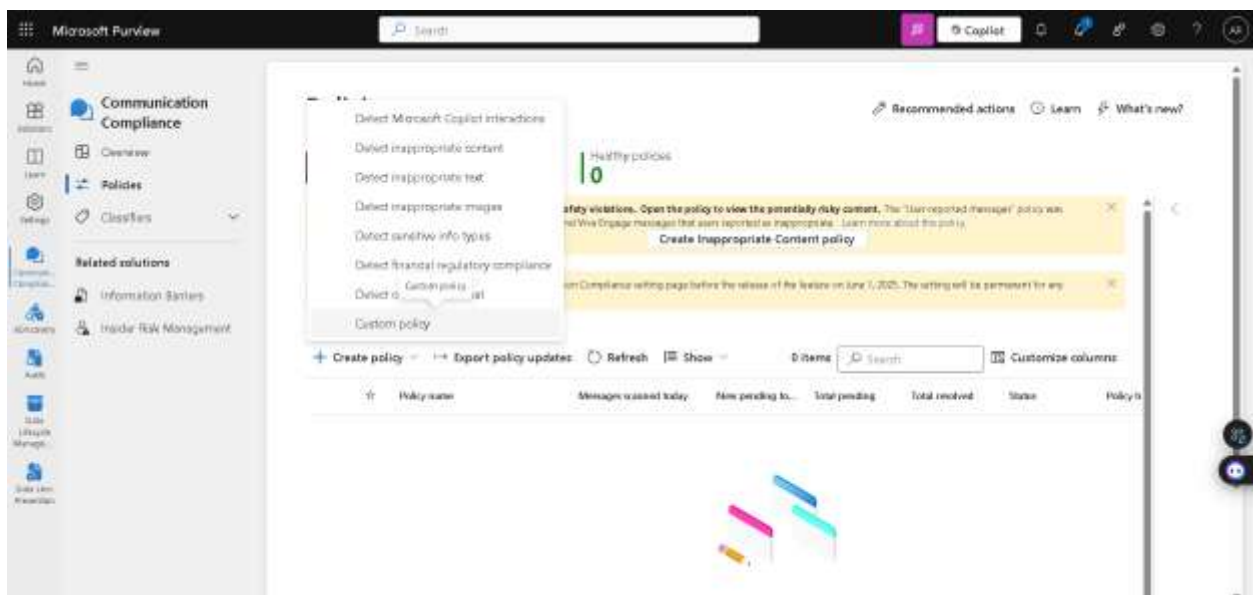




Step 2: Now from Purview portal, solutions -> communication compliance.



Step 3: In communication compliance -> policies -> custom policy.



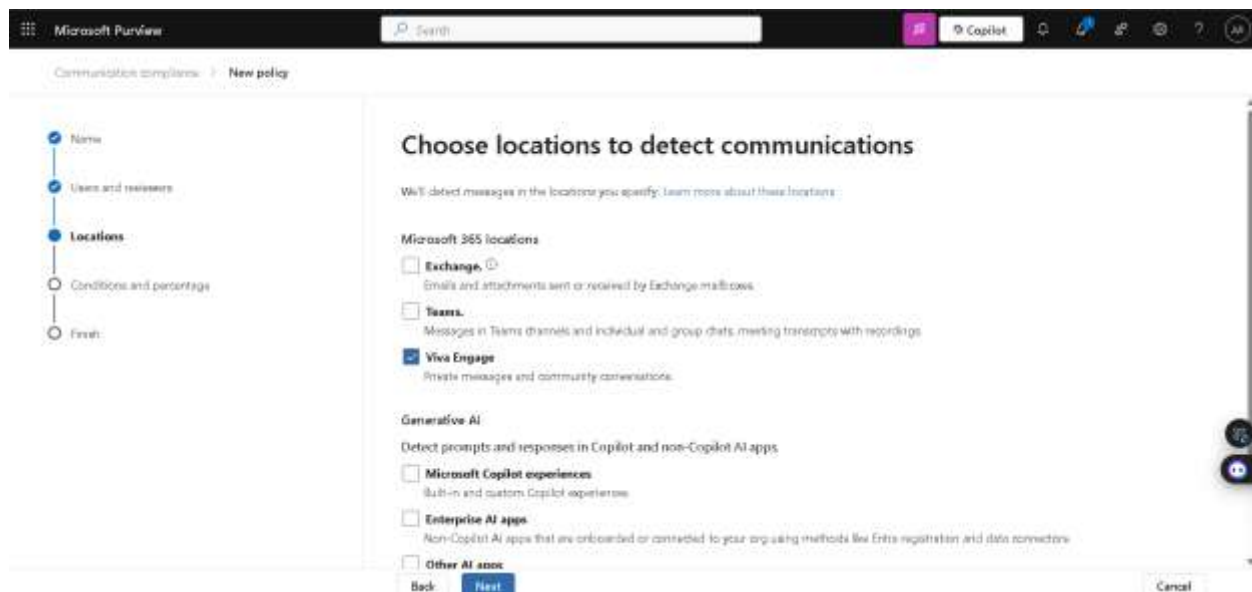
Step 4: Fill all the details about policy like name, description then next.

The screenshot shows the 'Name and describe your policy' step in the Microsoft Purview 'New policy' wizard. On the left, a progress bar indicates the current step is 'Name'. The main area contains three input fields: 'Name' with the value 'Social media policy', 'Description' with the value 'compliance with the company's social media policy', and 'Preserve policy matches' with the value 'Global Setting'. At the bottom, there are 'Next' and 'Cancel' buttons.

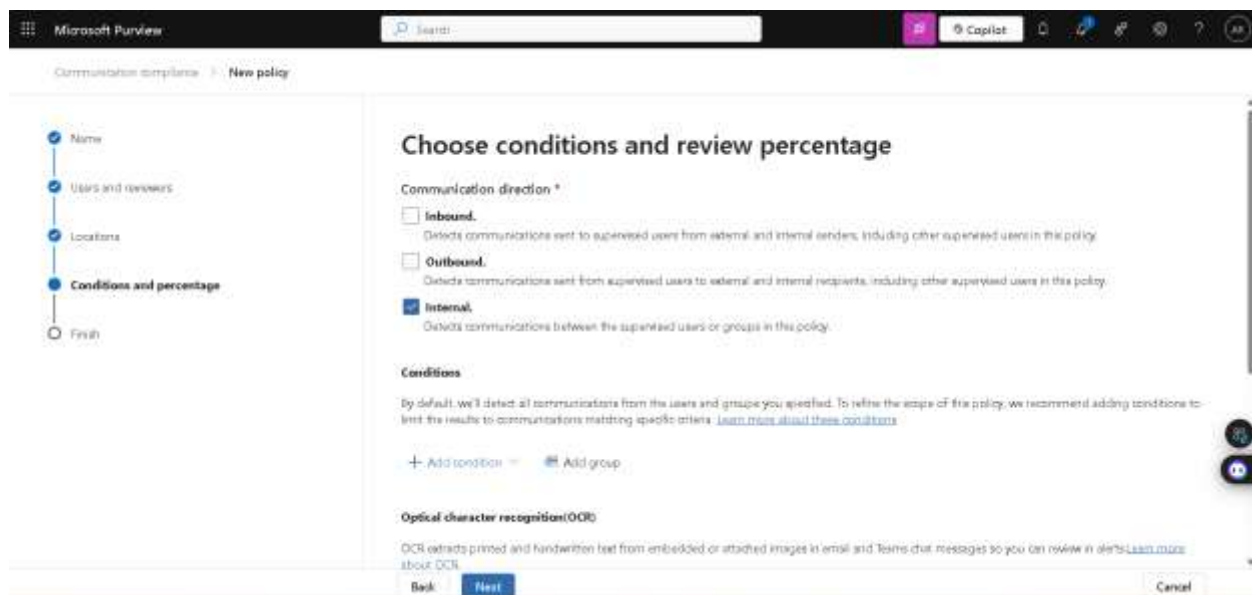
Step 5: As we want to apply this policy to all users in organization. So, select all users and add reviewers then next.

The screenshot shows the 'Choose users and groups' step in the Microsoft Purview 'New policy' wizard. On the left, the progress bar shows 'Users and reviewers' as the current step. The main area has three sections: 'Choose users and groups' with 'All users' selected, 'Excluded users and groups' with an empty search box, and 'Reviewers' with 'All RightsAdmins' selected. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.

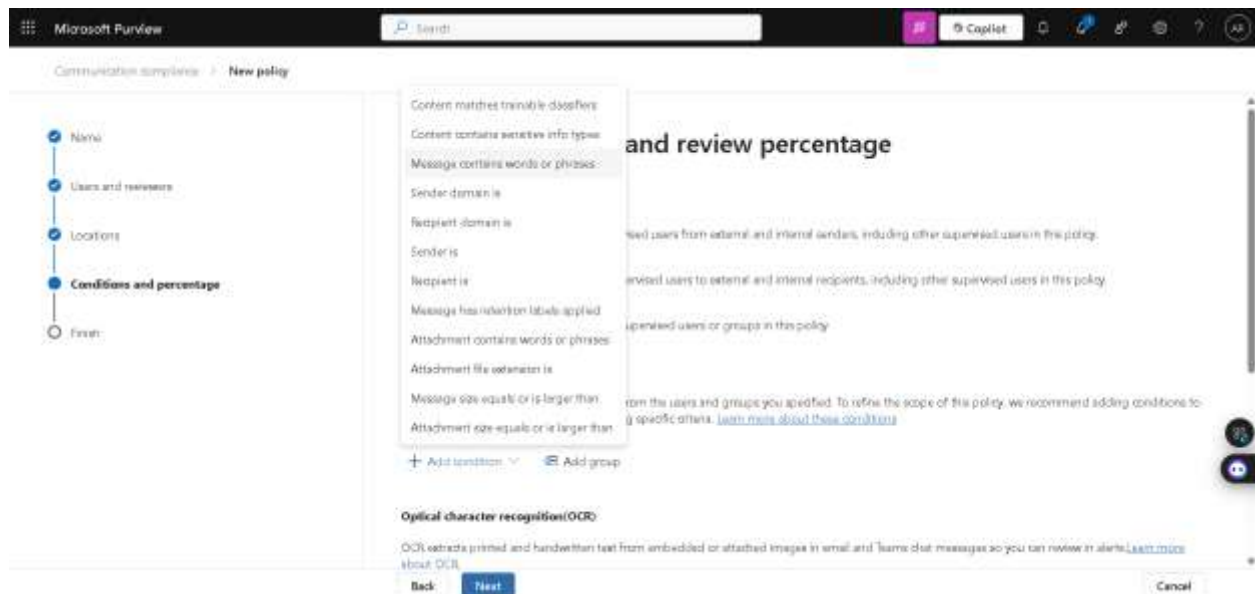
Step 6: As we are creating this policy for viva engage, selected viva engage then next.



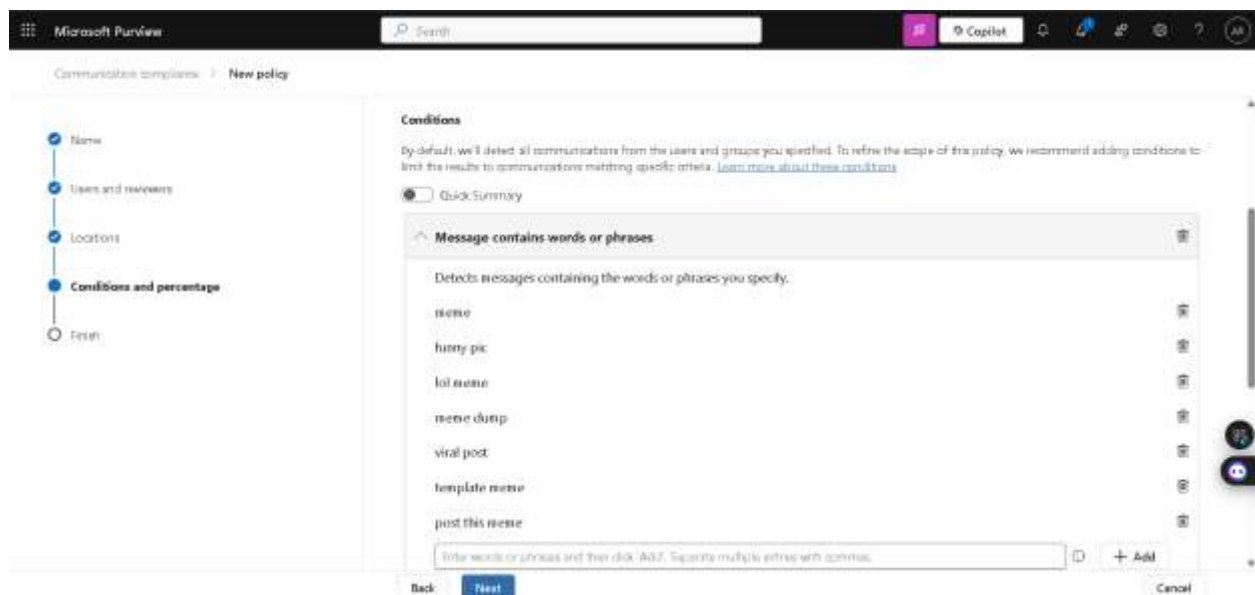
Step 7: Selected Communication direction as internal, as communication is internal.



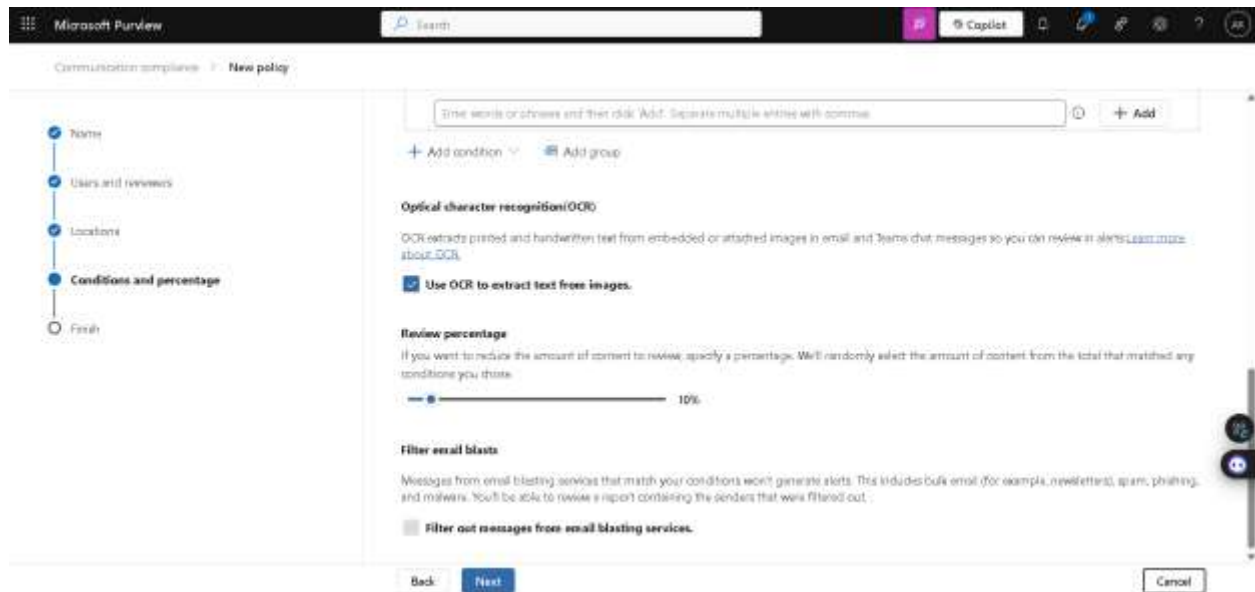
Step 8: Add condition for message contains words or phrases.



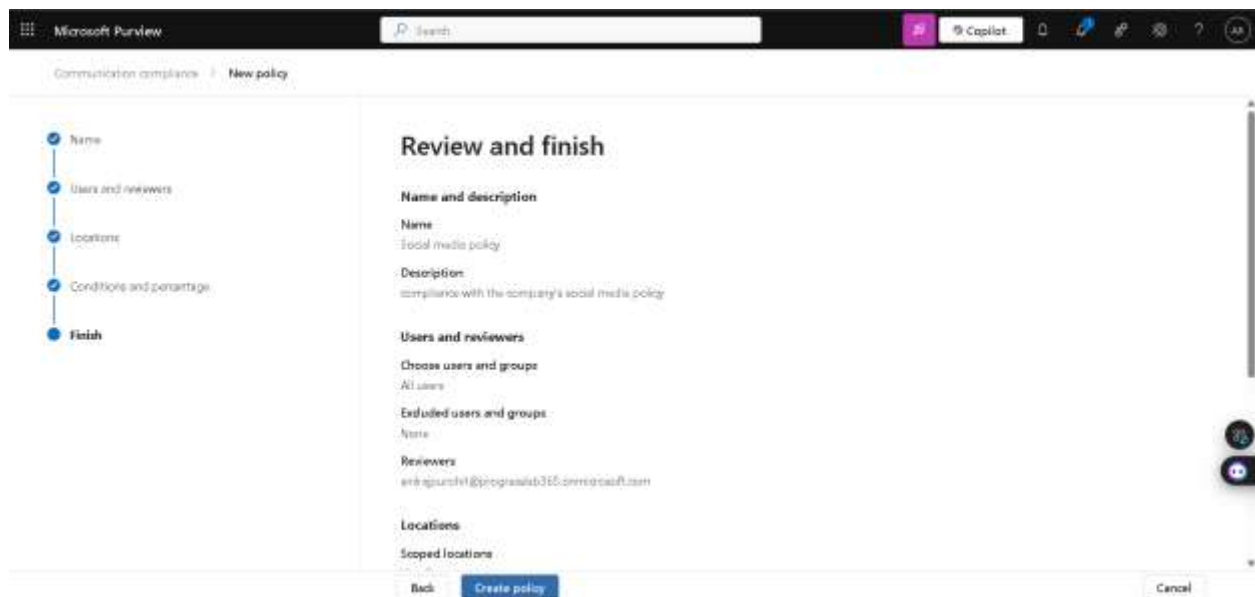
Step 9: As we created this policy to block users from sharing memes content in engage communication. So, provided some words and phrases to restrict them.



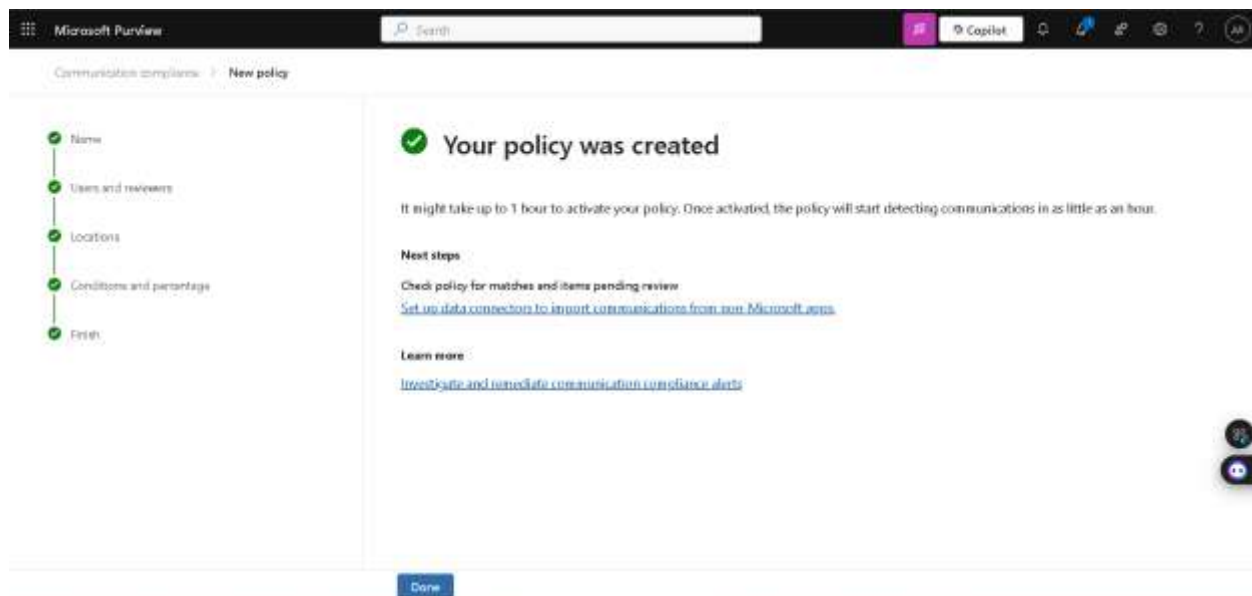
Step 10: Select use OCR to extract text from images then next.



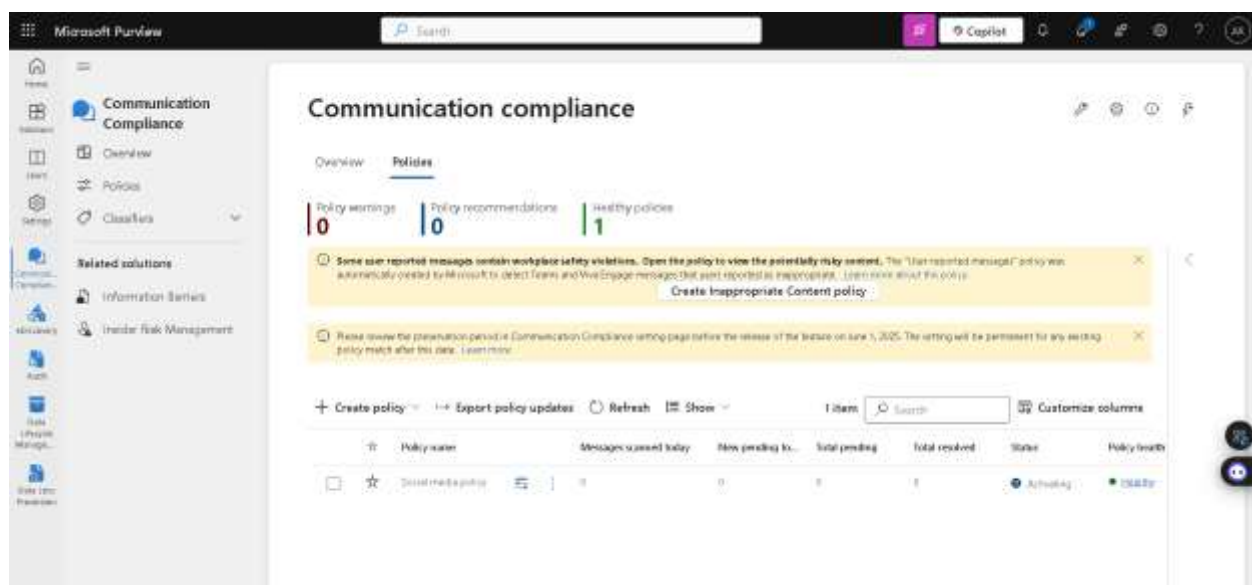
Step 11: Review policy details then click on create policy.



Step 12: Our new policy for social media has been successfully created then done.



Step 13: We can view our policy in communication compliance -> policies.



LEARNING & OPINION

If we create Microsoft 365 groups for each department (IT, HR, Marketing). That will already create a SharePoint team site too for those particular groups. So, we don't need to create them again.

If we have any sensitive documents in our SharePoint and we don't want visitors to even read this library. So, we can select that SharePoint site visitors then remove user permissions to read.

For documents versions, we choose minimum 100 or maximum 500 as major versions allowed.

For managing global settings, we can set OneDrive to restrict external settings. So, we move our bar to Only people in your organization option.

If a retention policy is for 1 year, then that file will be deleted and go to the Recycle Bin, where they remain for 93 days by default.

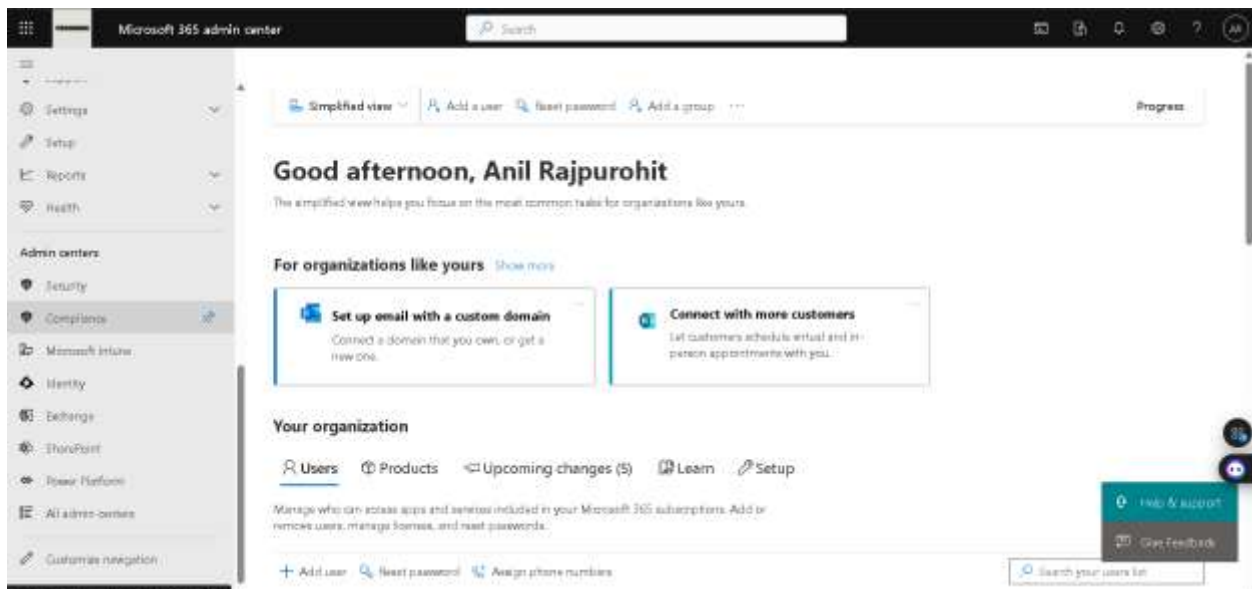
We can create policy for Communication too, so that users will adhere organizations guidelines.

Task 4: Monitoring and Reporting

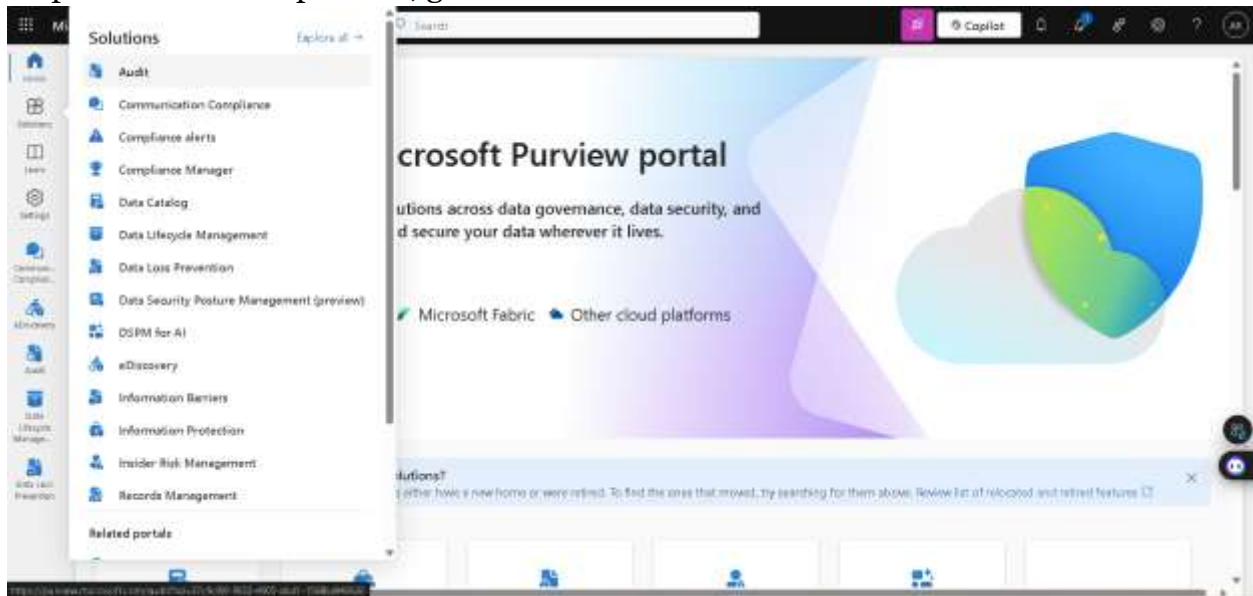
1. Configure Audit Logs:

- Enable and configure audit logging in the Microsoft 365 compliance center.

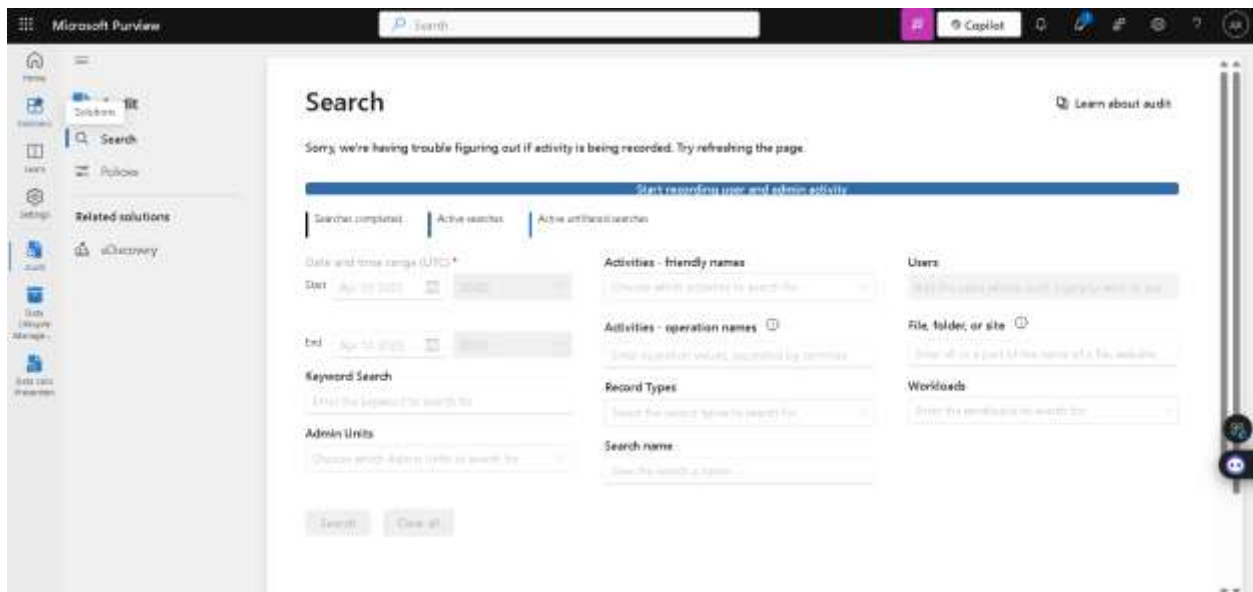
Step 1: From Microsoft 365 admin center, under admin centers select compliance.



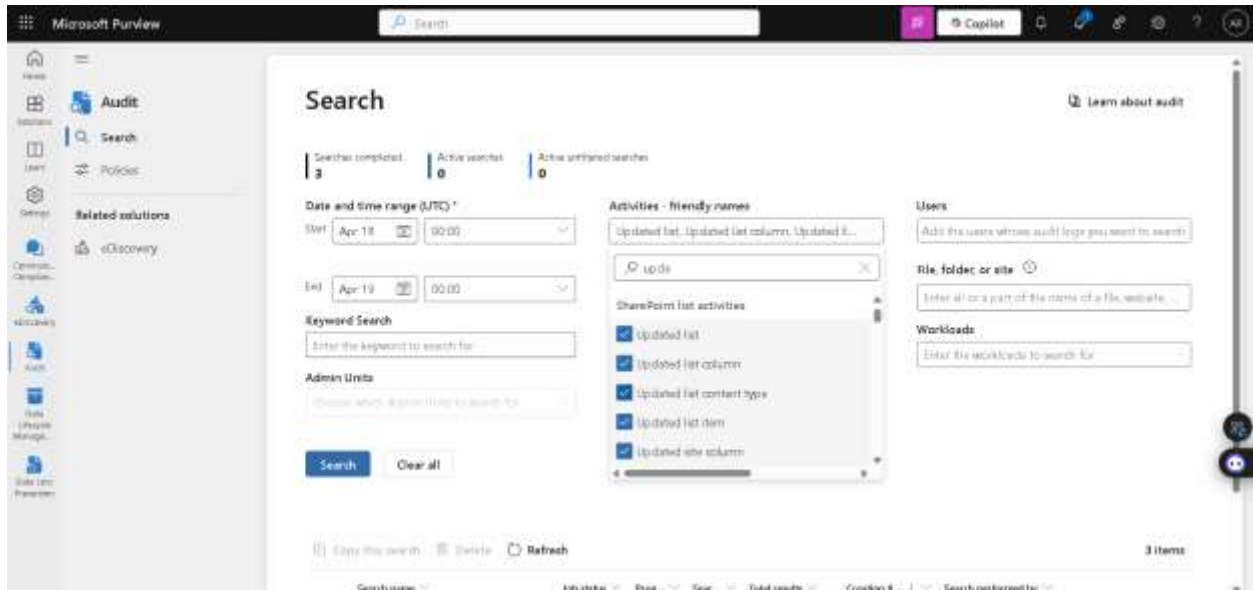
Step 2: In Microsoft Purview, go to solutions -> Audit.



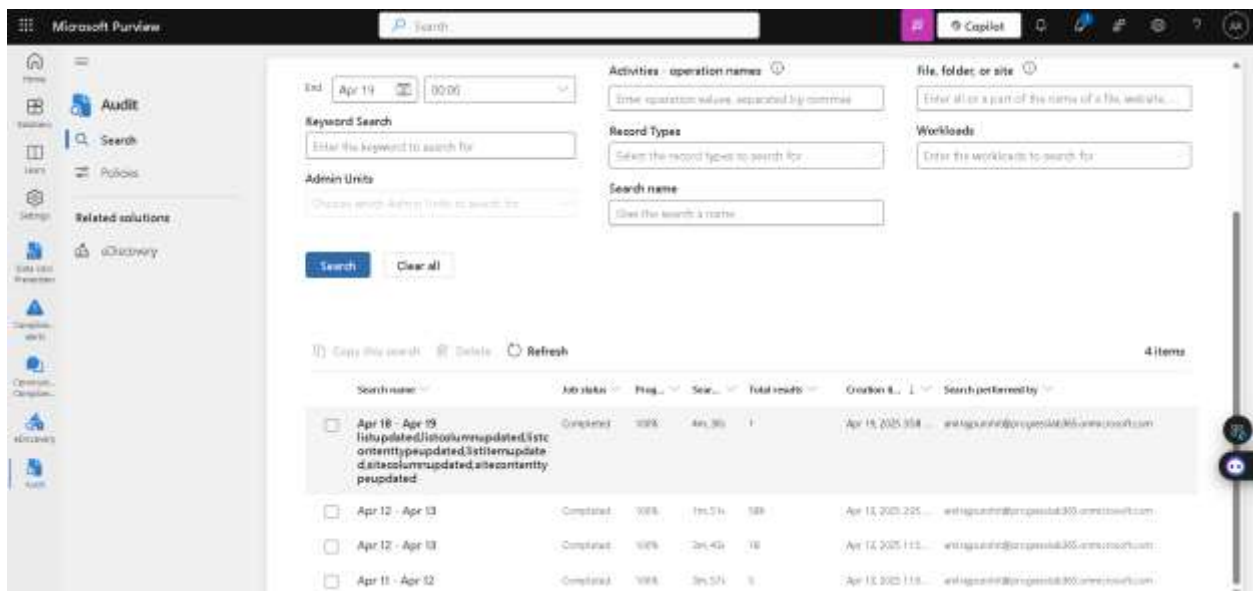
Step 3: Then click on start recording user and admin activity.



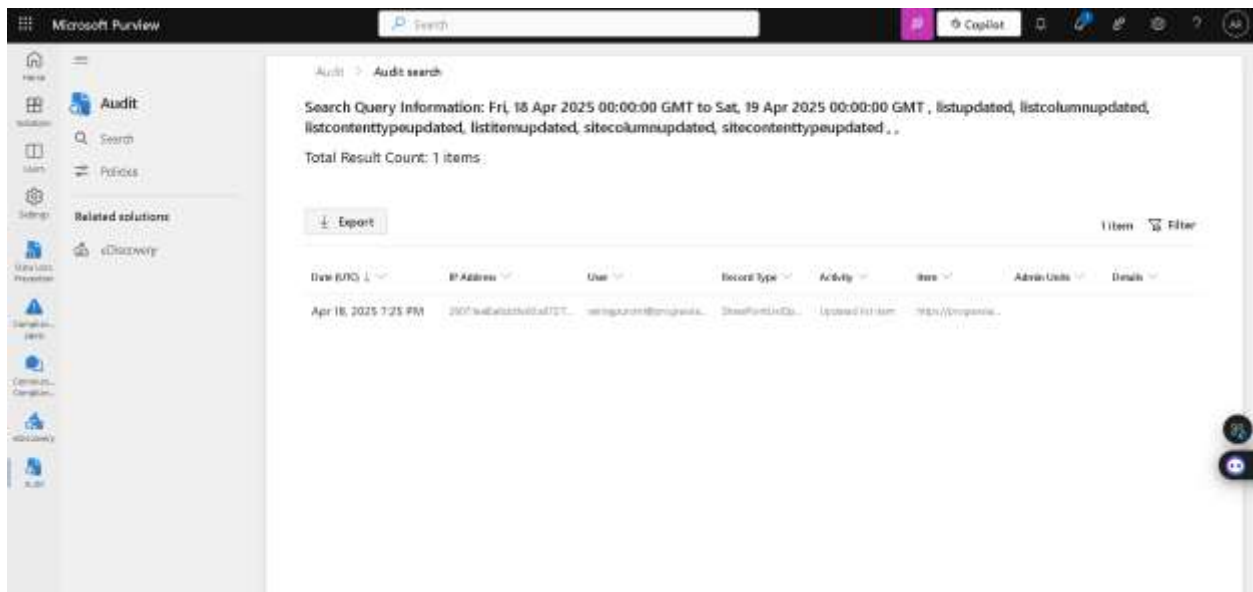
Step 4: We got a client error, so we will try from Windows PowerShell.



Step 2: Now click on our latest audit report.



Step 3: We can view logs here from 18 Apr 2025 to 19 Apr 2025. Also, their record type, activity, user, date etc. Now, to export the log click on Export.



Step 4: Audit log file is ready to download now, click on Download file.



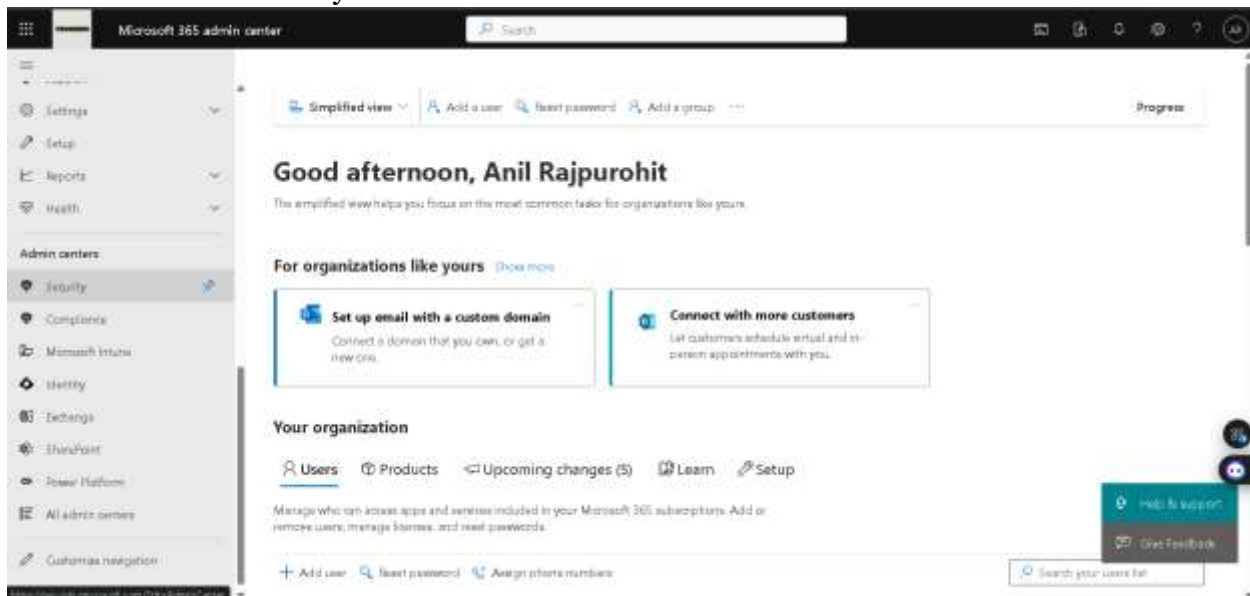
Step 5: We can view our audit log in excel file now. For instance, we can view that global admin updated items in SharePoint site on 2025-04-18 at 19.25.12.

RecordID	CreationDate	RecordType	Operation	User	AuditData
2015647	2025-04-18T19:25:22.0000000Z	36	ListItemUpdated	anilrajpur	...@progresslab365.com
...
...

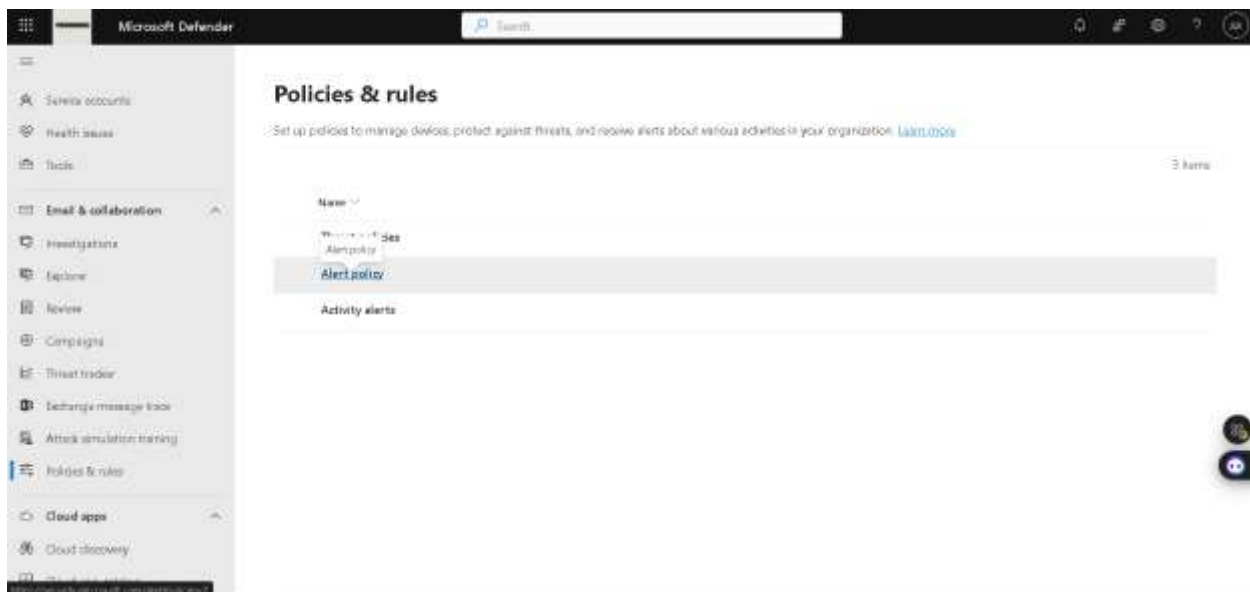
2. Set Up Alerts:

- Configure alert policies to notify administrators of suspicious activities, such as multiple failed logins attempts or mass deletion of files.

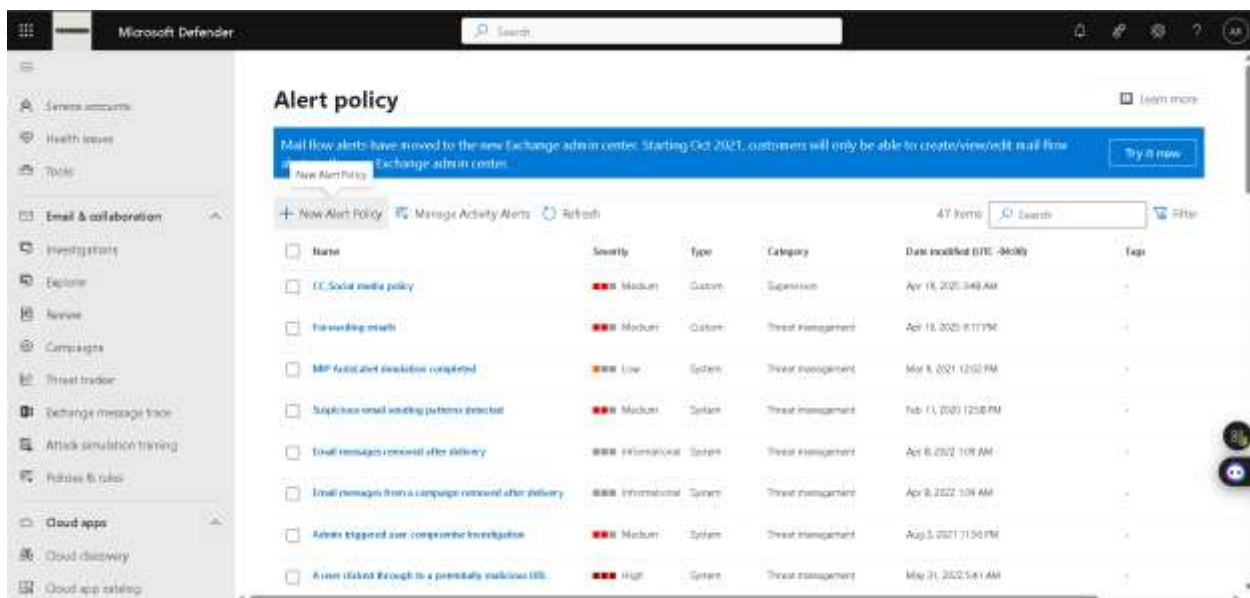
Step 1: To configure security alerts, go to Microsoft 365 Admin Center and under admin centers click on Security.



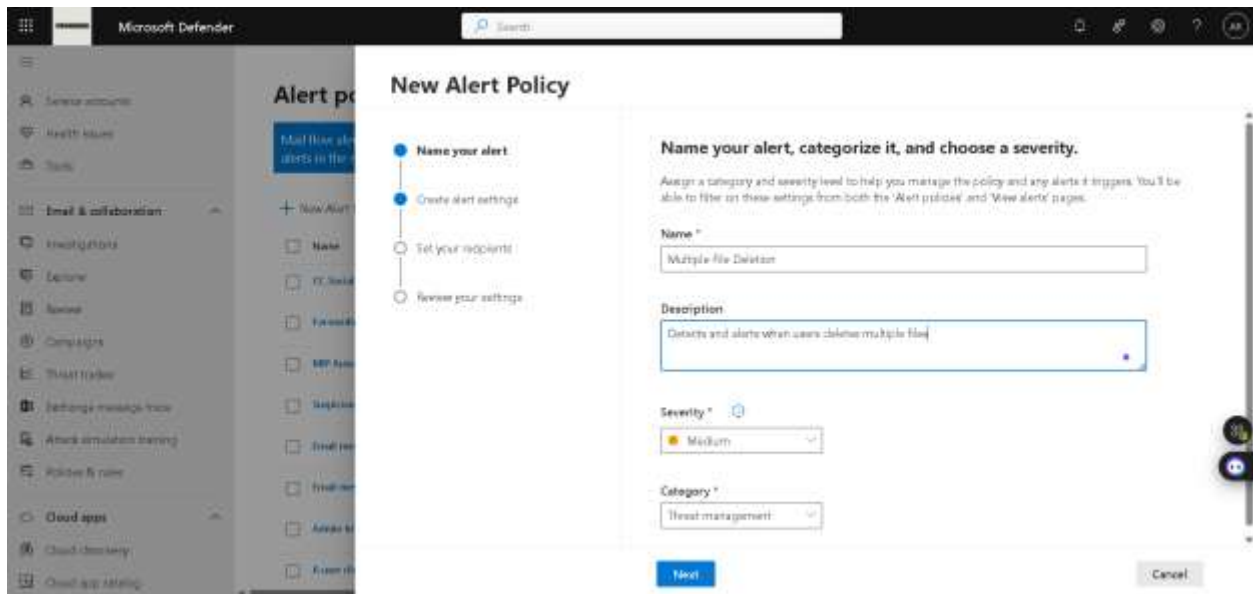
Step 2: We are in Microsoft Defender now and from here we can manage and configure security alerts. From Microsoft defender, under email & collaboration go to Policies & rules -> alert policy.



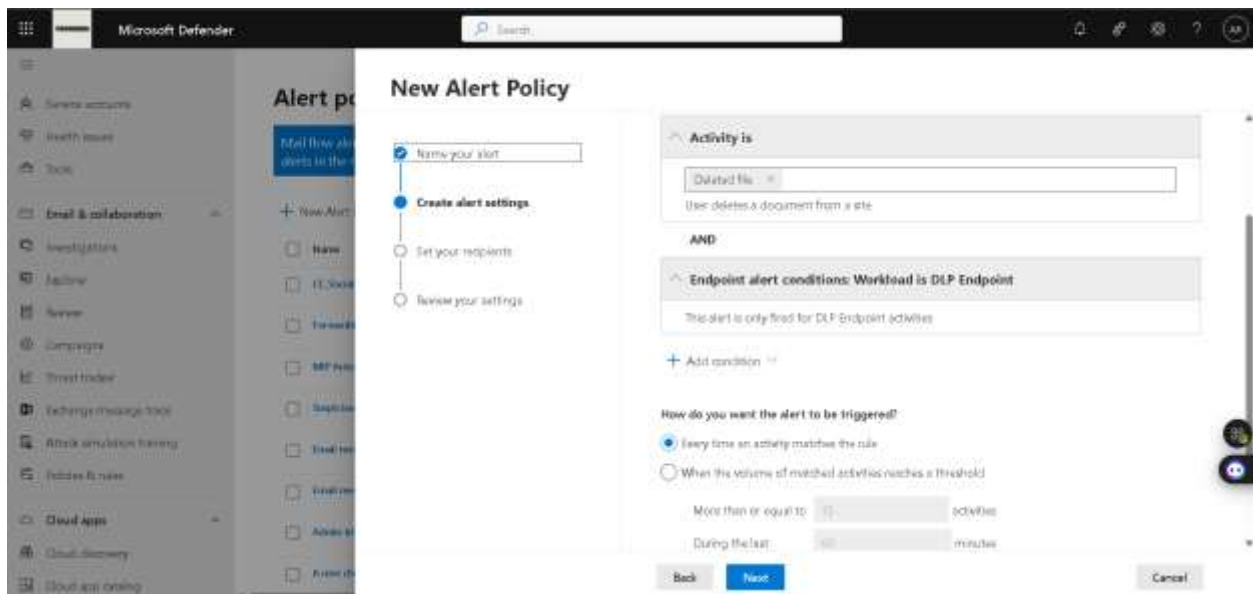
Step 3: We can view all the default policies here, now to create a new policy click on New alert policy.



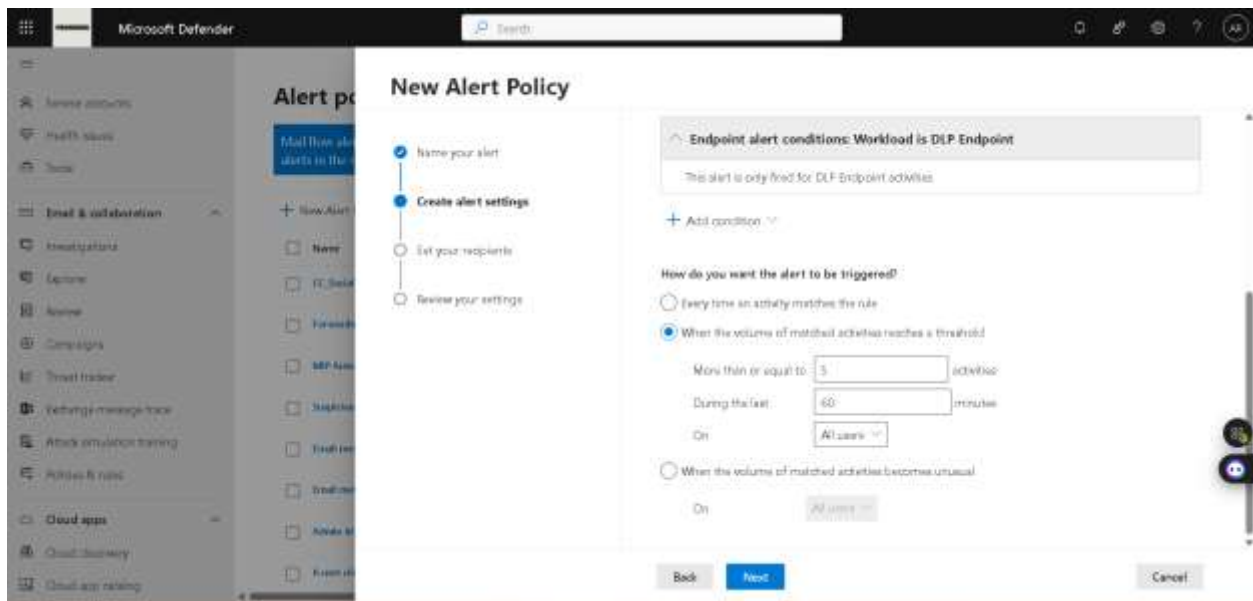
Step 4: Provide name, description, severity level, and category to the policy then click on next.



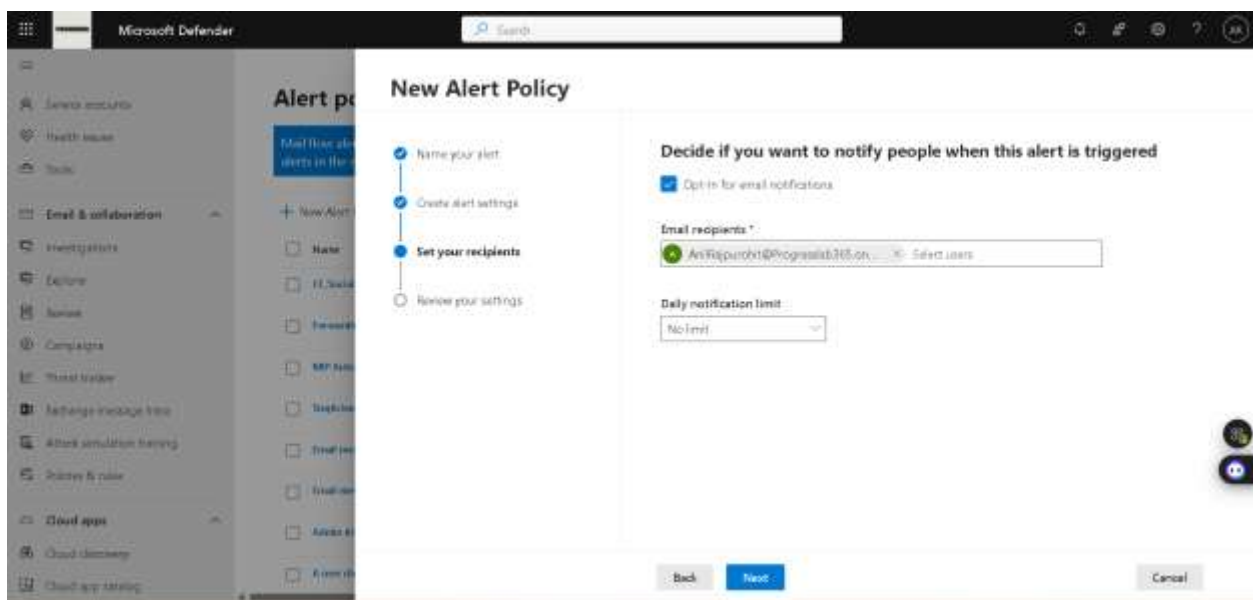
Step 5: We choose the activity here, which is deleted file (as we are creating policy for mass deletion). Then choose every time an activity matches the rule for our alert to be triggered and click on Next.



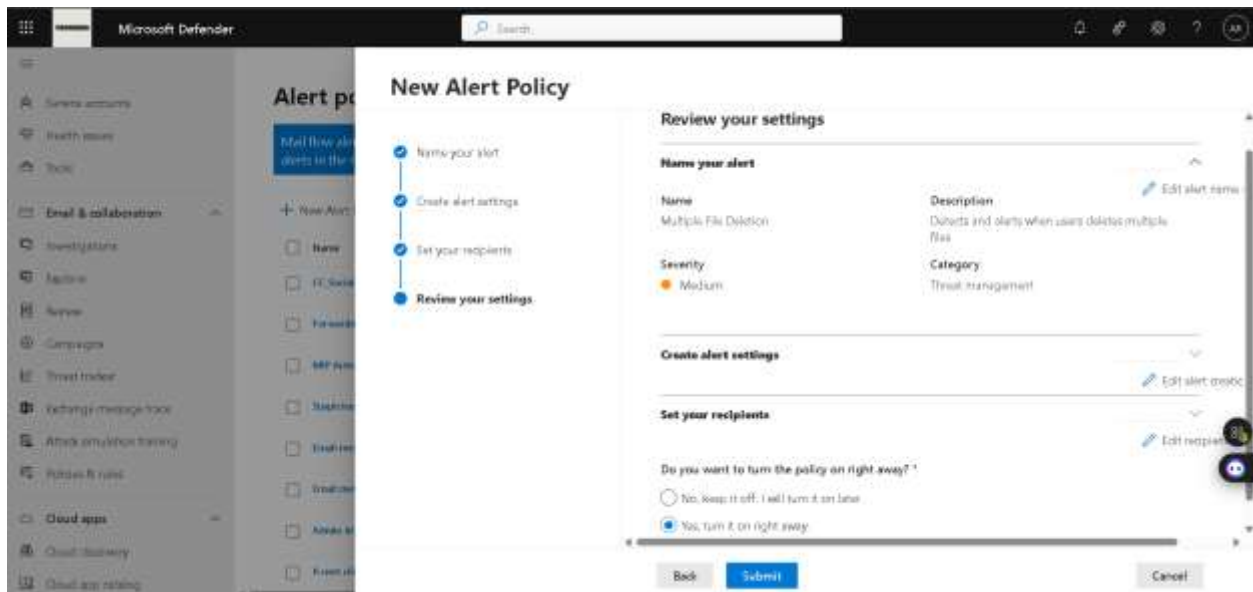
Step 6: We choose volume as more than 5, if a user deletes more than 5 files in 60 minutes this policy will be activated.



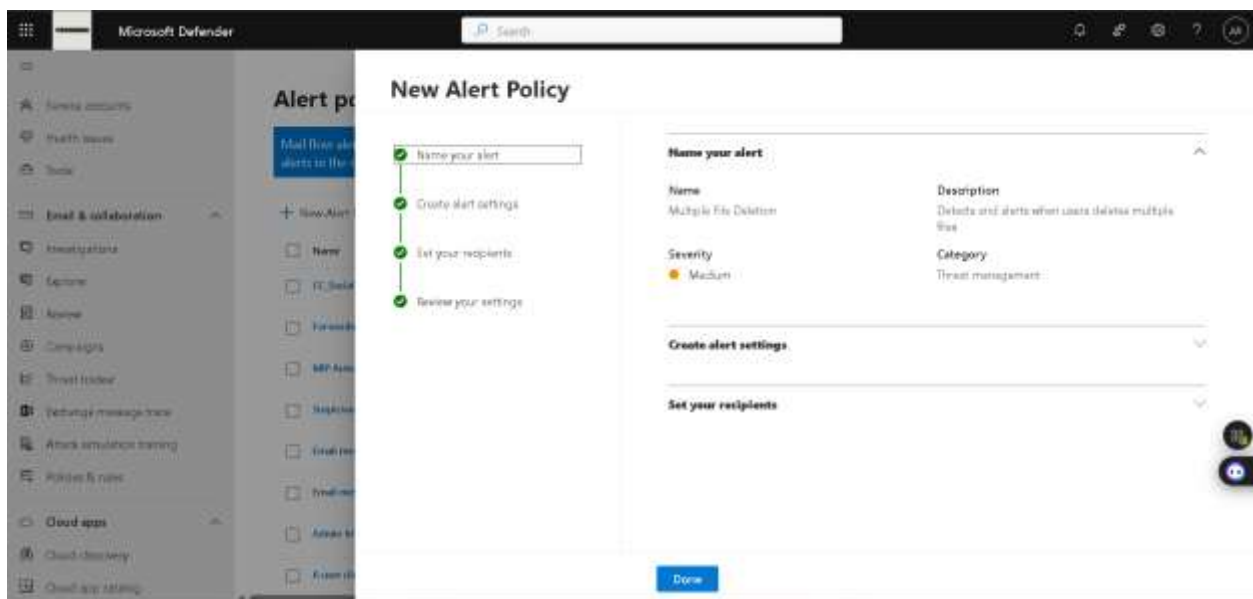
Step 7: Choose email recipients to get email notifications, then click on next.



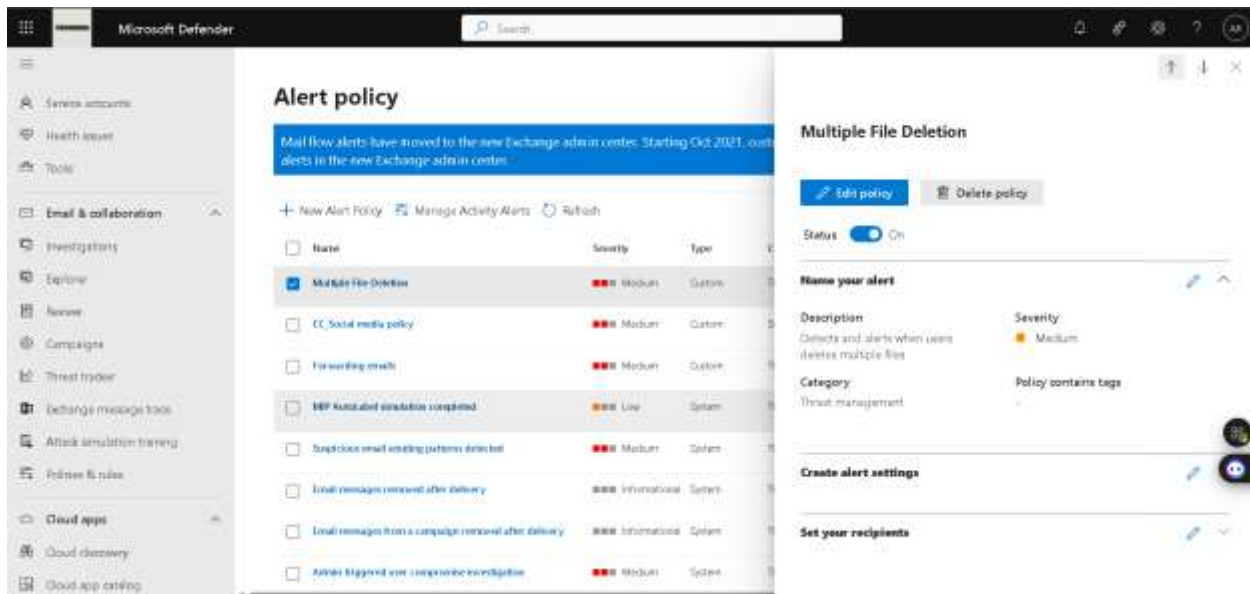
Step 8: Review policy details and turn on policy right away, then click on Submit.



Step 9: Policy has been created successfully.

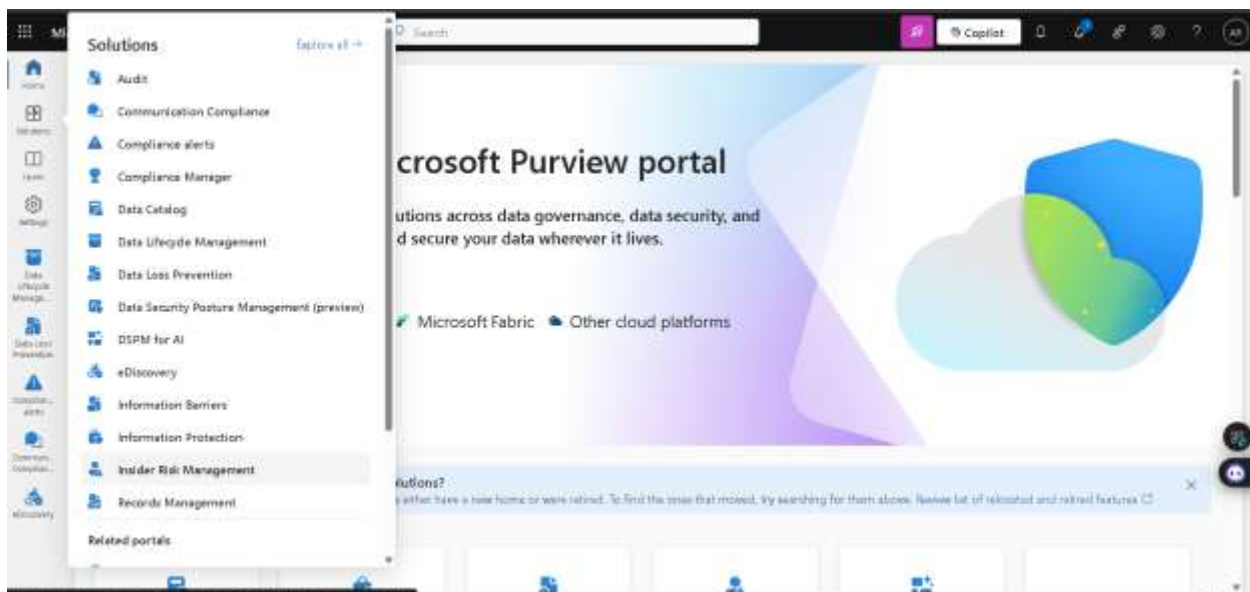


Step 10: We can see our new policy under Alert policy now.

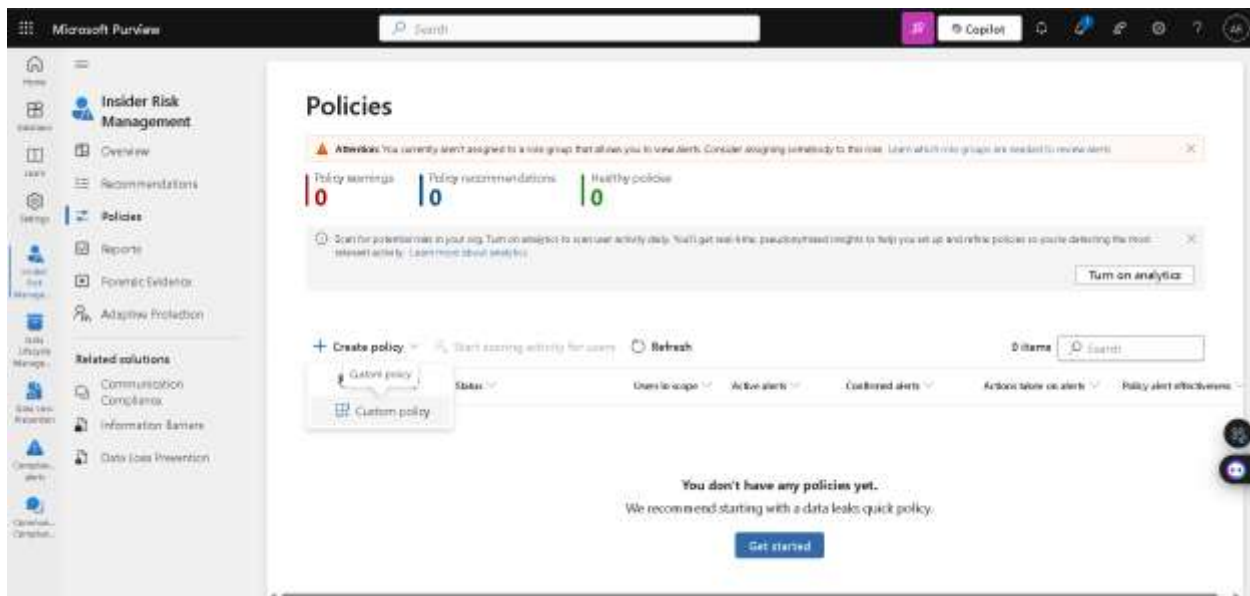


- Set up notifications for data loss prevention (DLP) policy breaches. (You can navigate to Insider risk management)

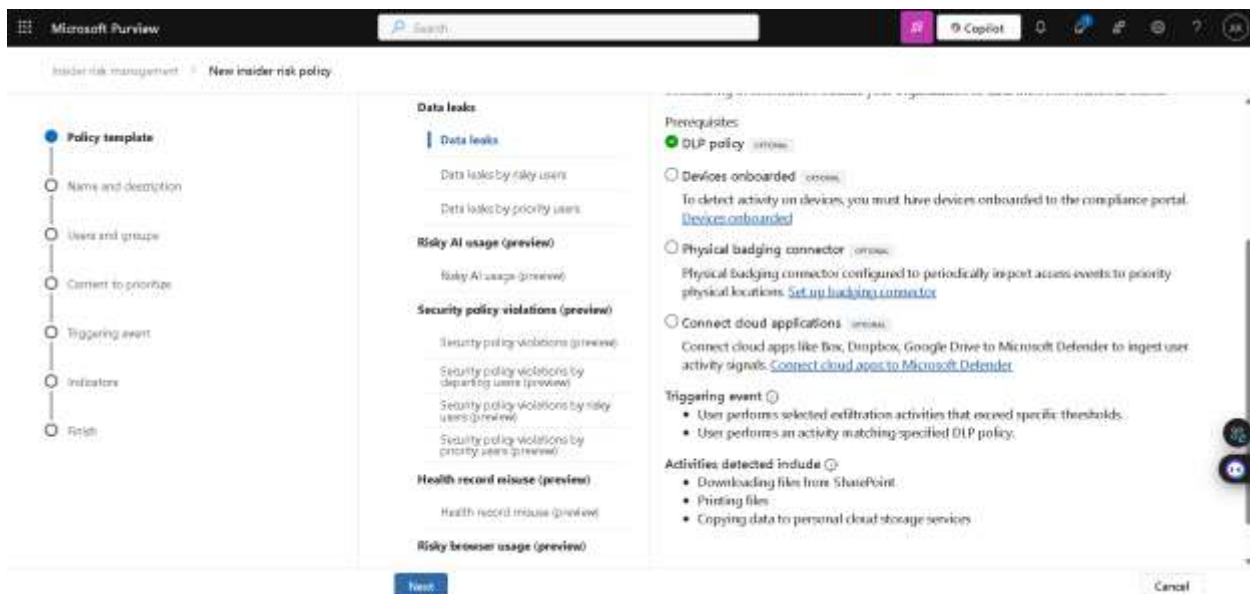
Step 1: In purview portal, solutions -> Insider risk management.



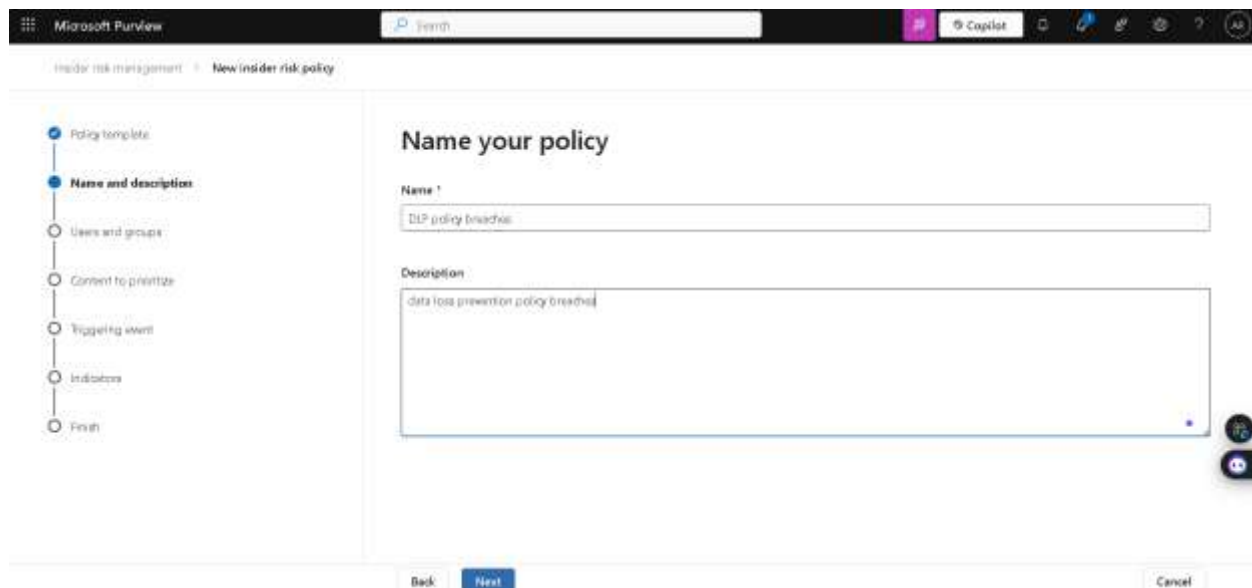
Step 2: In insider risk management, policies -> custom policy.



Step 3: We need a DLP policy to create this policy, and we already have a DLP policy created for protecting credit card details. We are going to use that here.

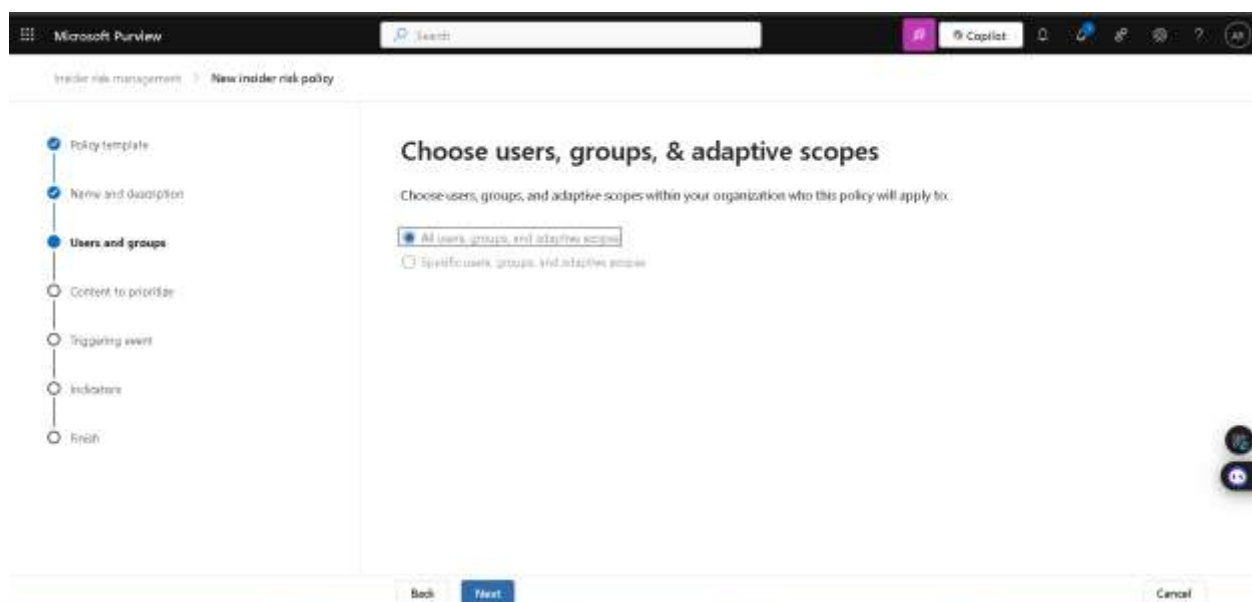


Step 4: Fill policy name and description, then click on next.



This screenshot shows the 'Name your policy' step in the Microsoft Purview 'New insider risk policy' wizard. The left sidebar contains a progress indicator with steps: Policy template, Name and descriptions (current), Users and groups, Content to prioritize, Triggering event, Indicators, and Finish. The main area has a 'Name' field containing 'DLP policy breaches' and a 'Description' field containing 'data loss prevention policy breaches'. At the bottom are 'Back', 'Next', and 'Cancel' buttons.

Step 5: Now, choose all user then next.



This screenshot shows the 'Choose users, groups, & adaptive scopes' step in the Microsoft Purview 'New insider risk policy' wizard. The left sidebar shows the progress indicator with 'Users and groups' as the current step. The main area has the instruction 'Choose users, groups, and adaptive scopes within your organization who this policy will apply to.' Below this are two radio button options: 'All users, groups, and adaptive scopes' (which is selected) and 'Specific users, groups, and adaptive scopes'. At the bottom are 'Back', 'Next', and 'Cancel' buttons.

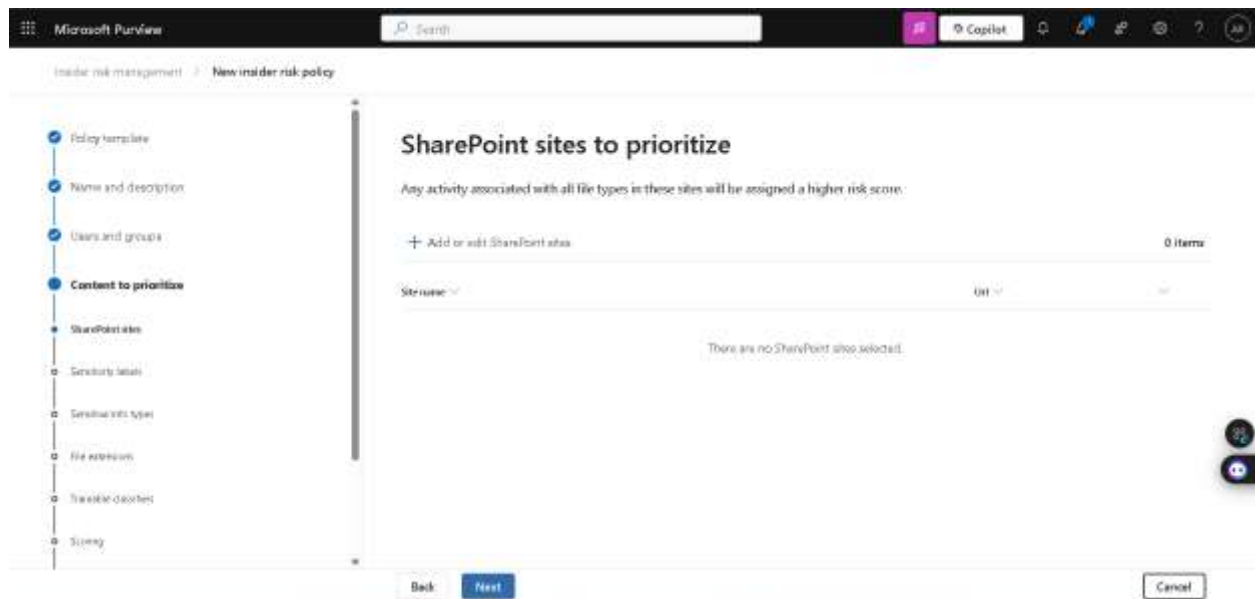
Step 6: We don't want to exclude any users or groups.

This screenshot shows the 'Exclude users and groups (optional) (preview)' step in the Microsoft Purview 'New insider risk policy' wizard. The left sidebar indicates the current step is 'Exclude users and groups', with previous steps like 'Policy template' and 'Name and description' completed. The main area is divided into two sections: 'Users' and 'Groups'. Each section has a '+ Add users/groups to exclude' button and a '0 items' count. Below these are input fields for 'Name' and 'Email', and a 'Remove' button. A message 'No users excluded yet' is displayed in the Users section, and 'No groups excluded yet' is displayed in the Groups section. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.

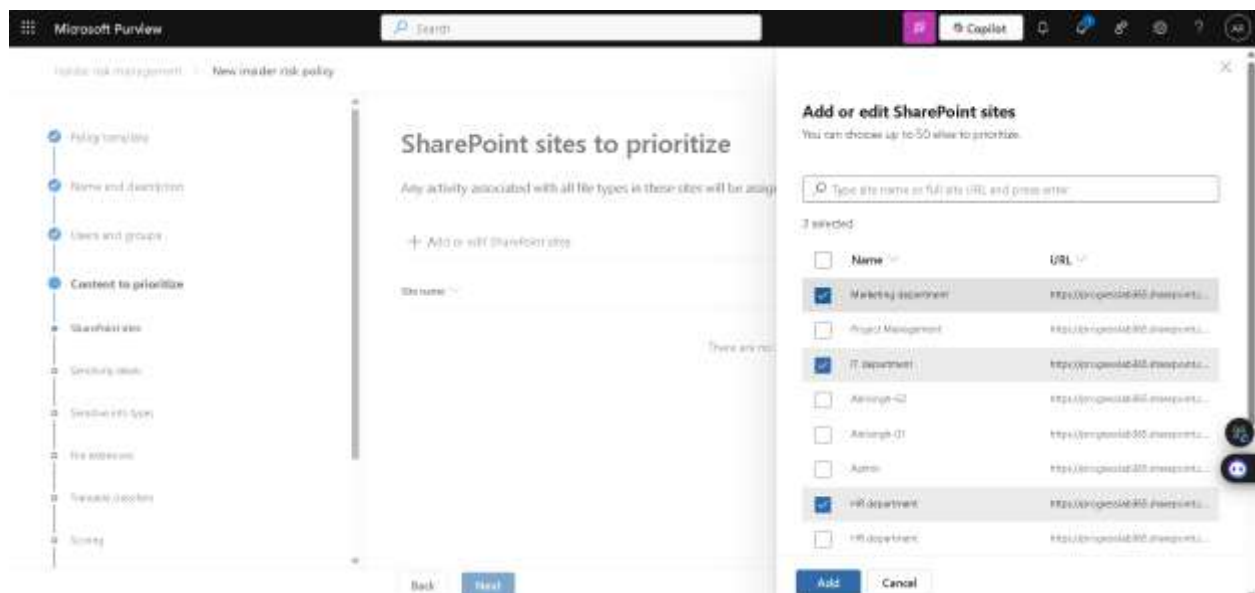
Step 7: Choose the content, we want to prioritize.

This screenshot shows the 'Decide whether to prioritize content' step in the Microsoft Purview 'New insider risk policy' wizard. The left sidebar shows the current step is 'Content to prioritize', with previous steps like 'Policy template' and 'Name and description' completed. The main area has a heading 'Decide whether to prioritize content' and a paragraph explaining that content can be prioritized based on factors like where it's stored and how it's classified. There are two radio button options: 'I want to prioritize content' (selected) and 'I don't want to prioritize content right now'. Under the selected option, there are five checkboxes: 'SharePoint sites', 'Sensitivity labels', 'Sensitive info types', 'File extensions', and 'Trimmable classifiers', all of which are checked. A link 'Learn about the benefits of prioritizing content' is provided. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.

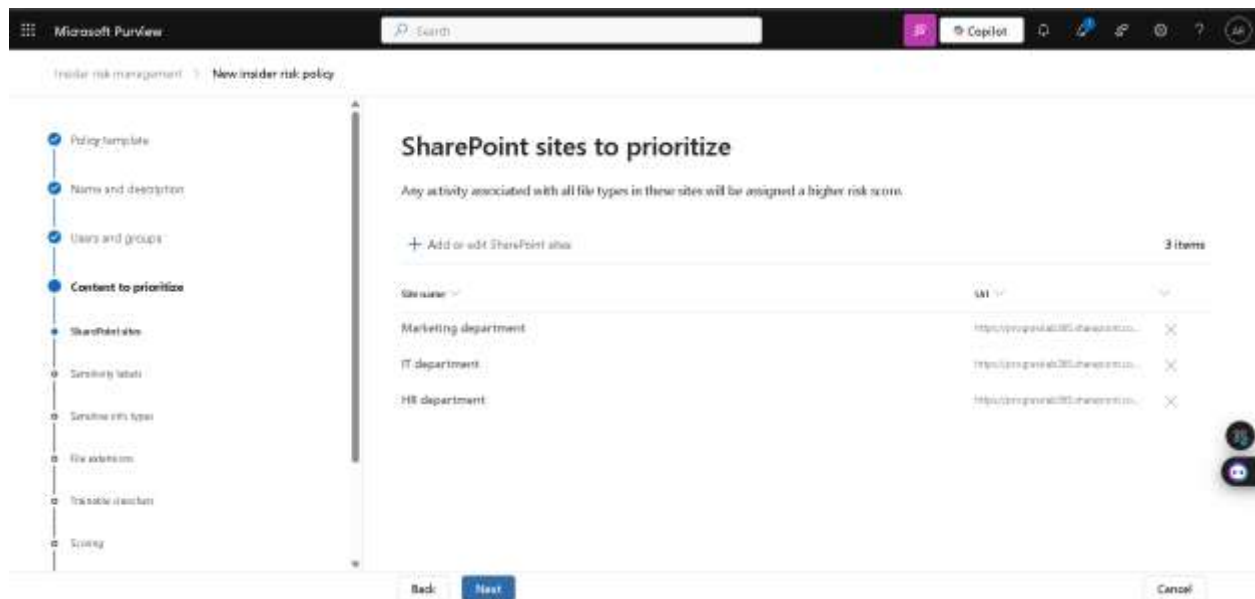
Step 8: To select SharePoint sites, click on add or edit SharePoint sites.



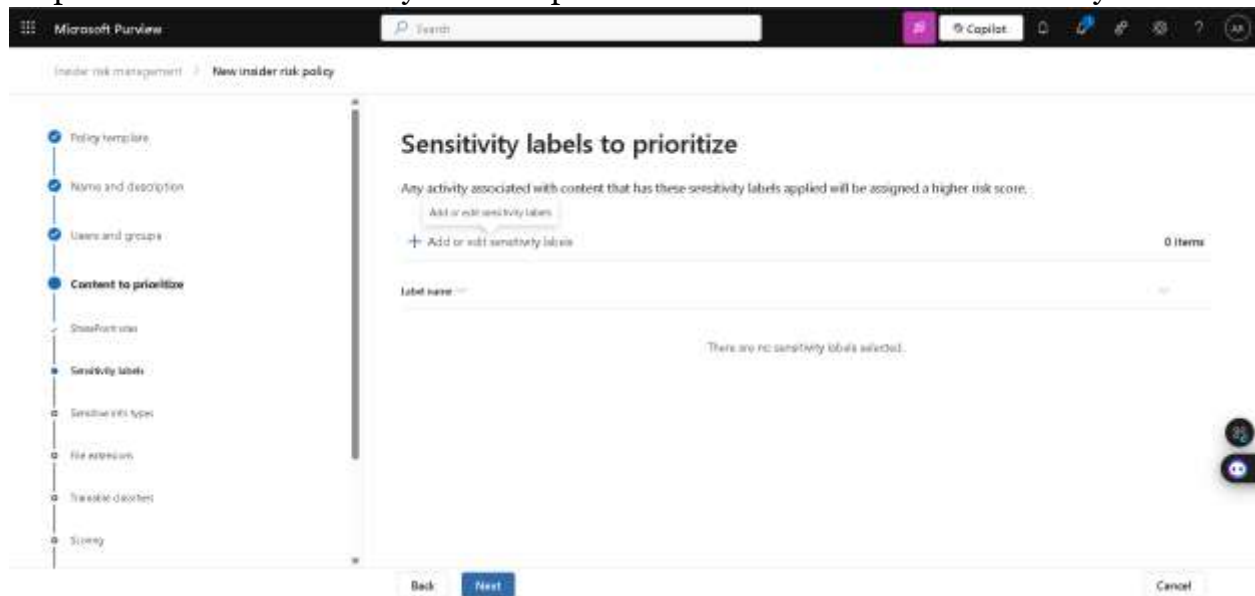
Step 9: Selected our target SharePoint sites then add.



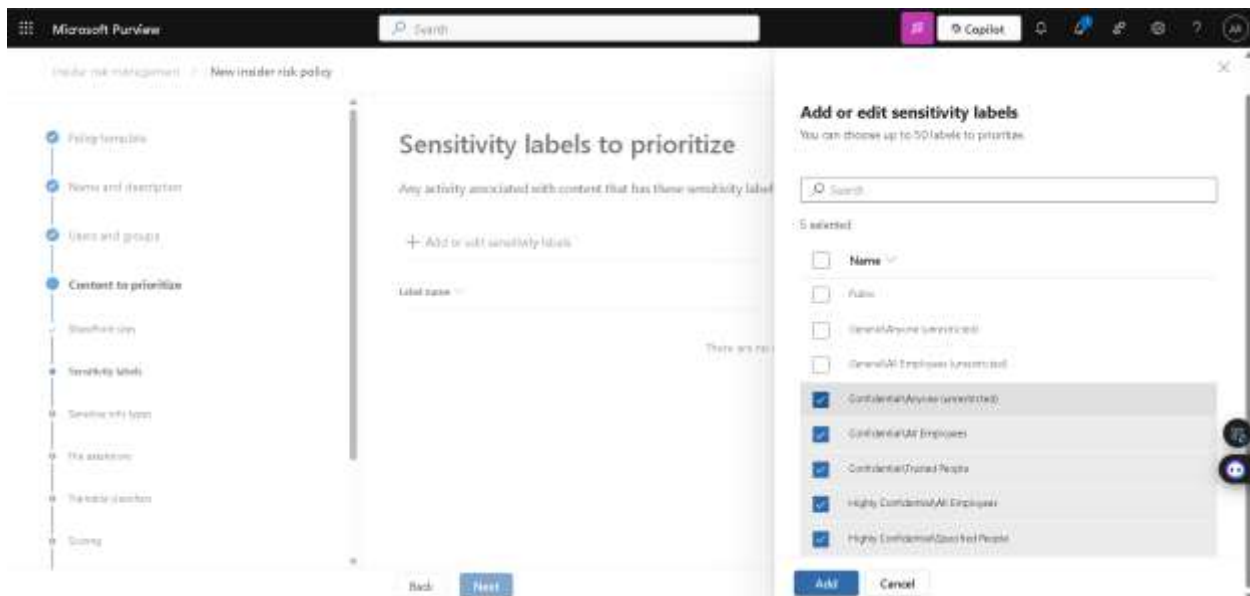
Step 10: Check SharePoint sites then next.



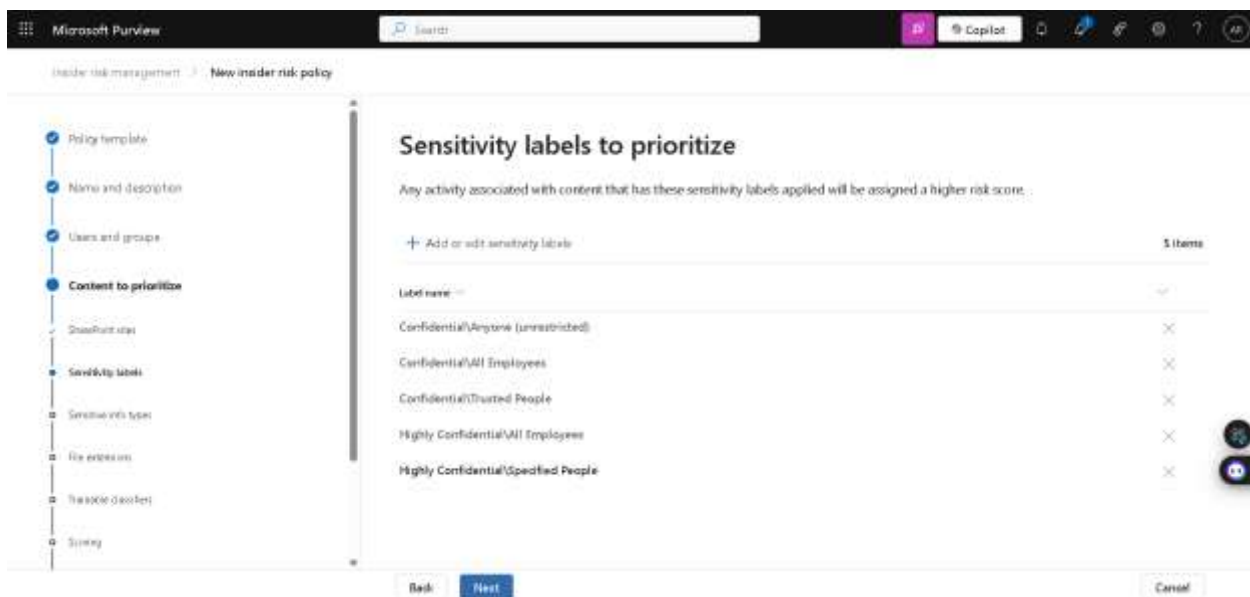
Step 11: To choose sensitivity labels to prioritize click on add or edit sensitivity labels.



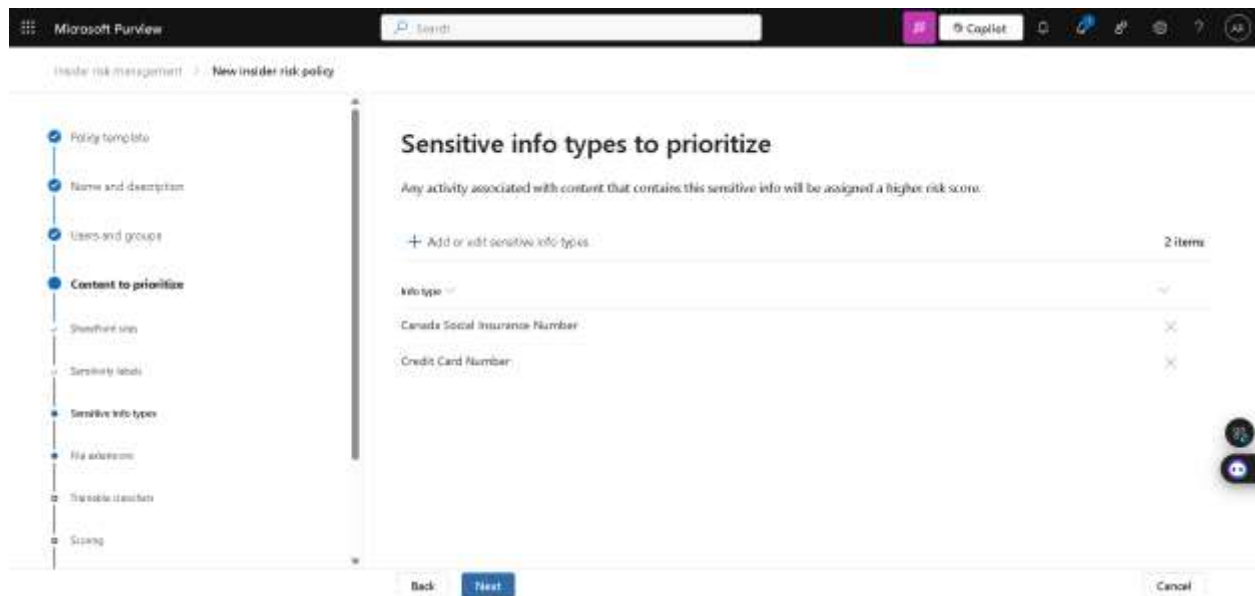
Step 12: Select all the sensitivity labels we need then add.



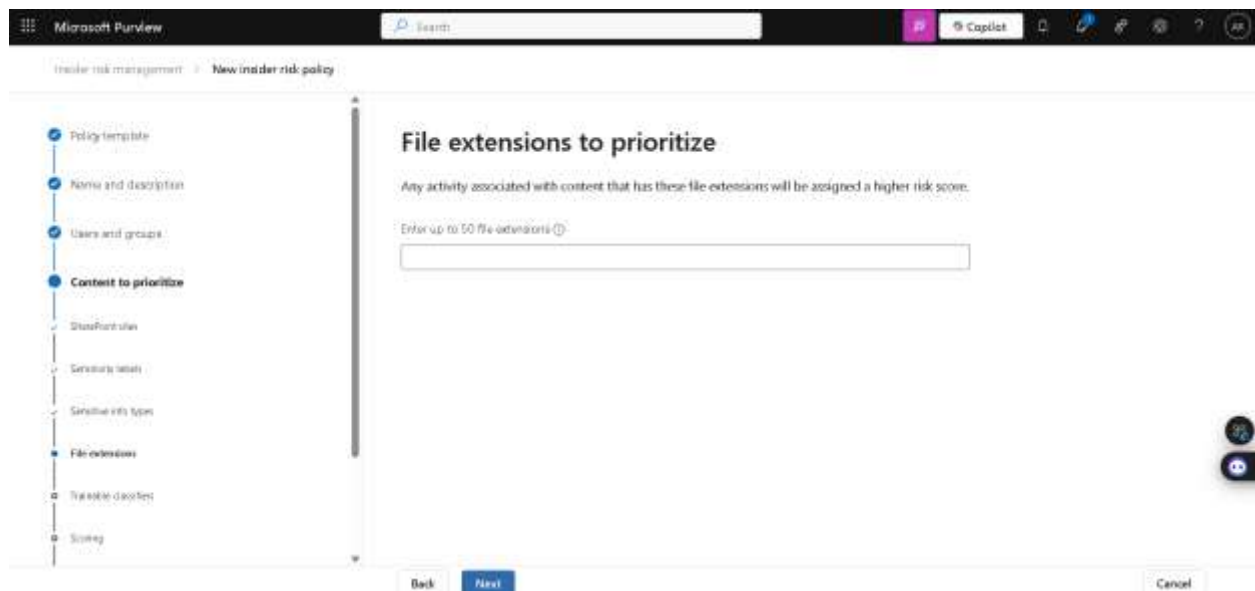
Step 13: Review our sensitivity labels details.



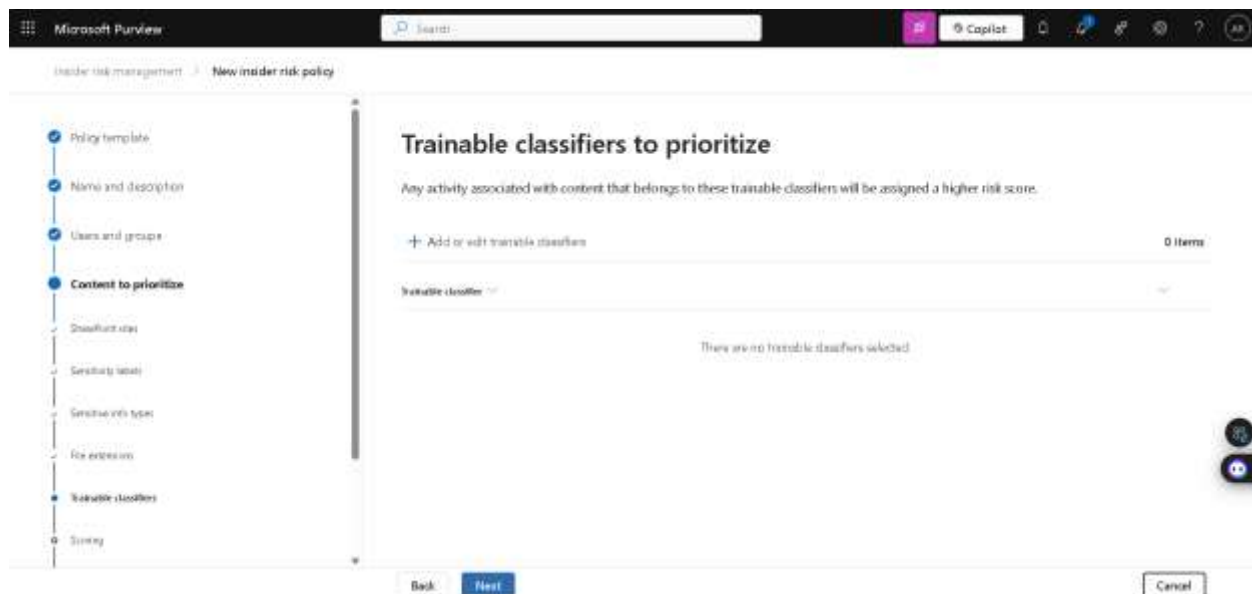
Step 14: Sensitivity info types, like in this policy we need credit cards. So, we selected credit cards here.



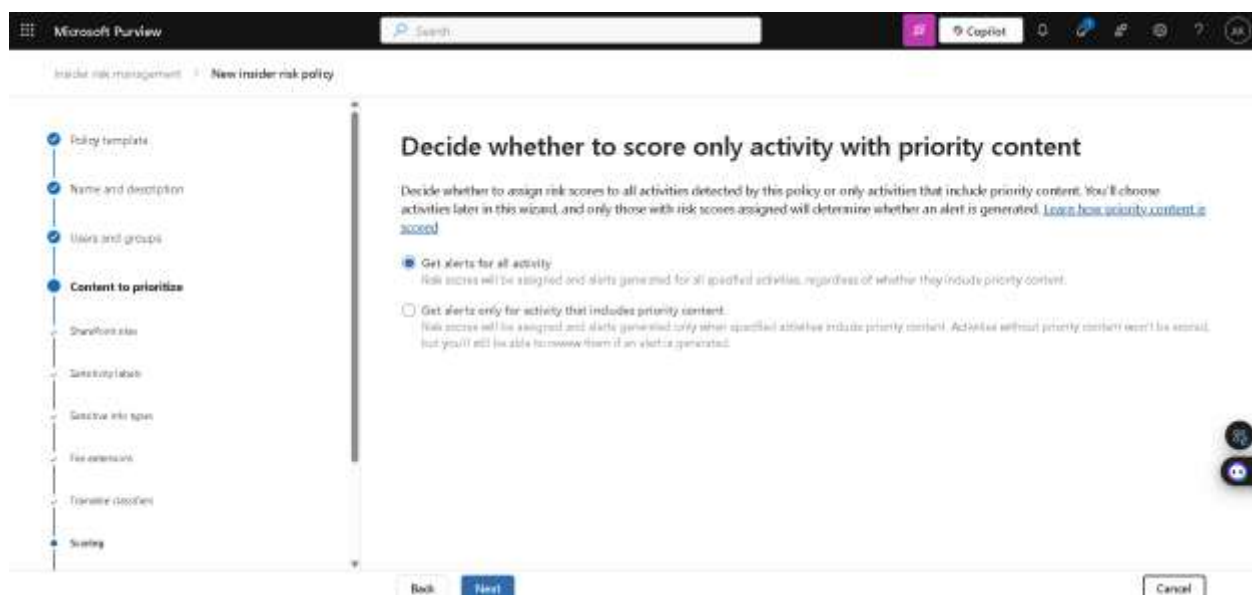
Step 15: We don't want to prioritize any file extensions.



Step 16: We don't want to prioritize any trainable classifiers.



Step 17: we choose to get alerts for all activity.



Step 18: Here we selected our DLP policy then next.

Microsoft Purview Search Copilot

Insider risk management > New insider risk policy

Policy template
Name and description
Users and groups
Content to prioritize
Triggering event
Indicators
Finish

Choose triggering event for this policy

Choose one or more triggering events to determine when a policy will begin assigning risk scores to a user's activity. [Learn more](#)

☒ **User matches a data loss prevention (DLP) policy**
Policy will start assigning risk scores when a user performs an activity matching the DLP policy you select. The DLP policy must be configured to generate High severity incident reports. [Learn more about DLP policy requirements](#).

Select a DLP policy

Canada Financial Data

☐ Canada Financial Data
☐ Default Office 365 DLP policy
☐ Default policy for Teams
☐ Default policy for devices

☐ Downloading content from OneDrive
☐ Sending email with attachments to security outside the organization

Back Next Cancel

Step 19: Choose indicators from here.

Microsoft Purview Search Copilot


Insider risk management > New insider risk policy

Policy template
Name and description
Users and groups
Content to prioritize
Triggering event
Indicators
Finish









Indicators

The following indicators are used to generate alerts for the activity detected by the policy template you selected. [Learn more](#)

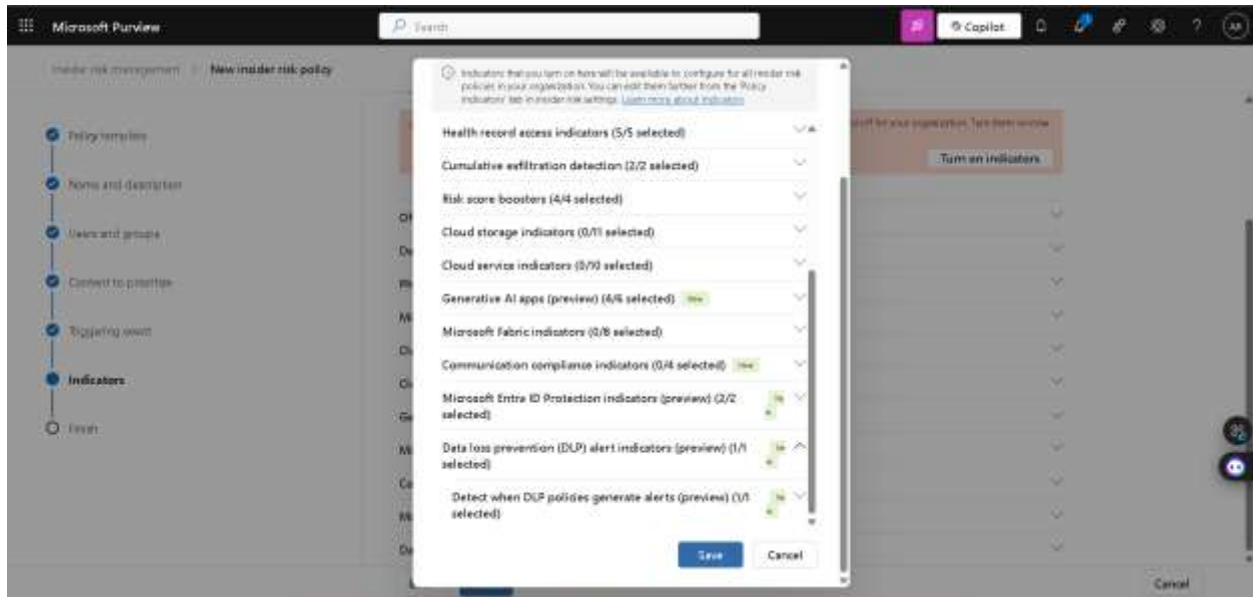
Total indicators selected: 0/91

 The indicators needed to create this policy aren't available to select because they're currently turned off for your organization. Turn them on now to continue.

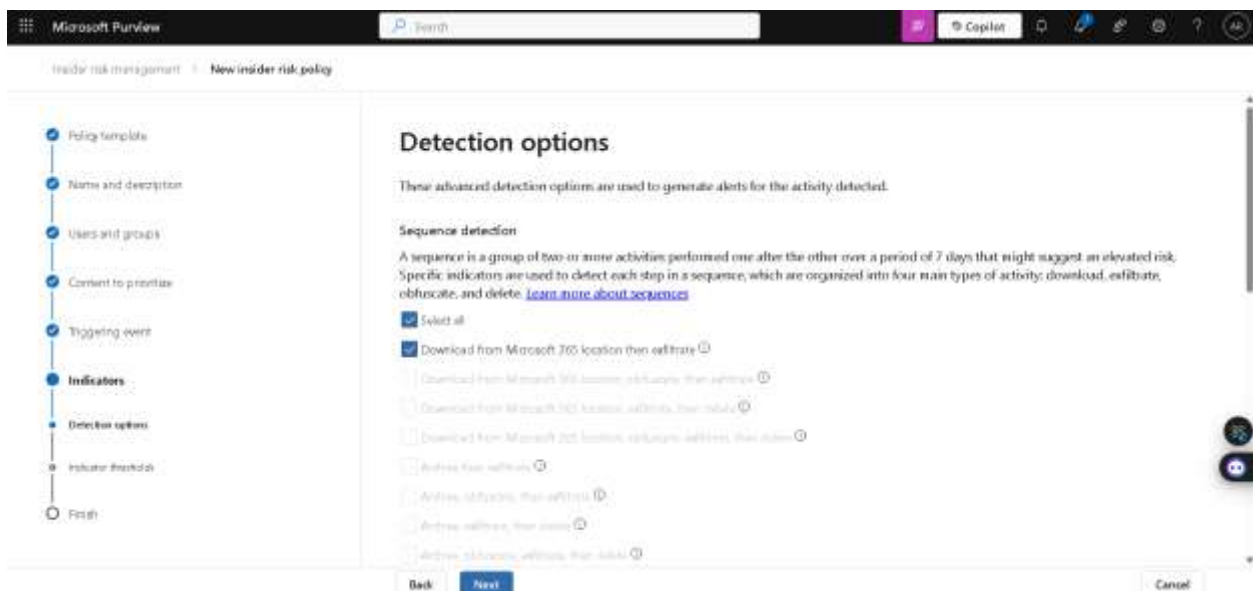
[Turn on indicators](#)

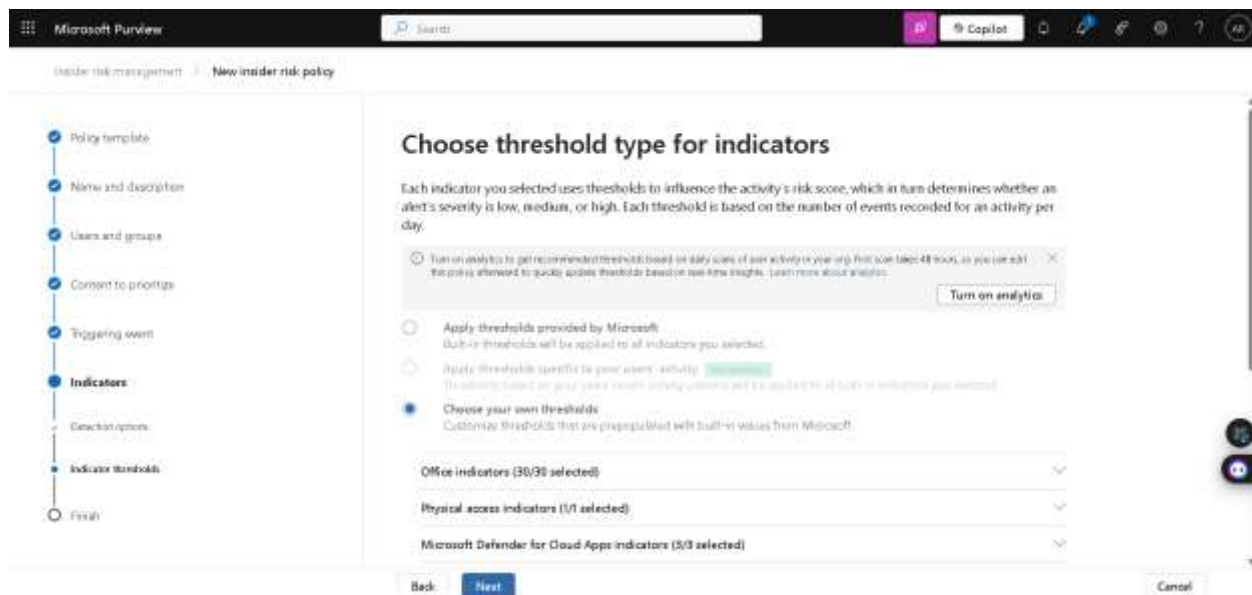
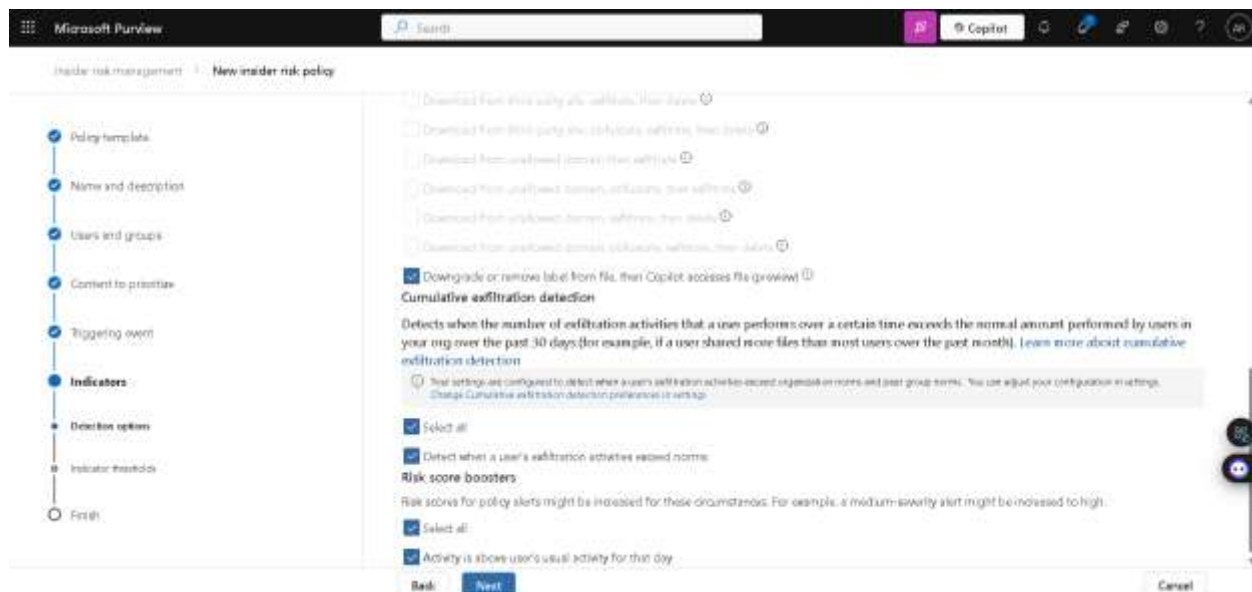
Office indicators (0/30 selected) 
Device indicators (0/15 selected) 
Physical access indicators (0/1 selected) 
Microsoft Defender for Cloud Apps indicators (0/3 selected) 
Cloud storage indicators (0/11 selected) 
Cloud service indicators (0/10 selected) 
Generative AI apps (preview) (0/6 selected)  

Back Next Cancel



Step 20: Under detection option, we choose all then next.

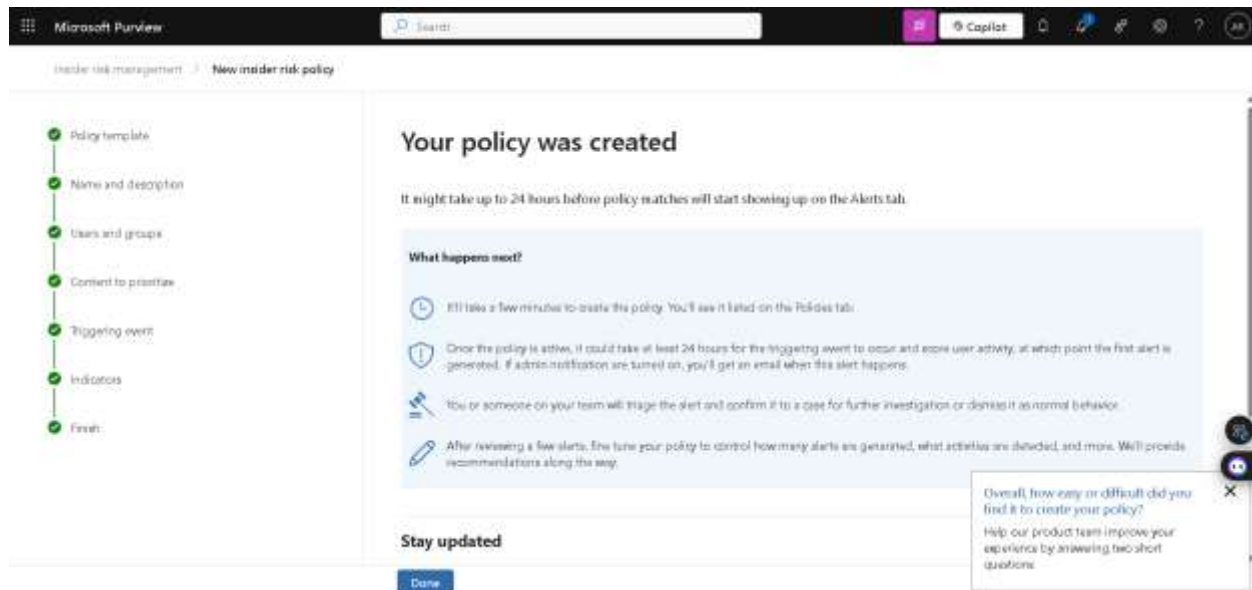




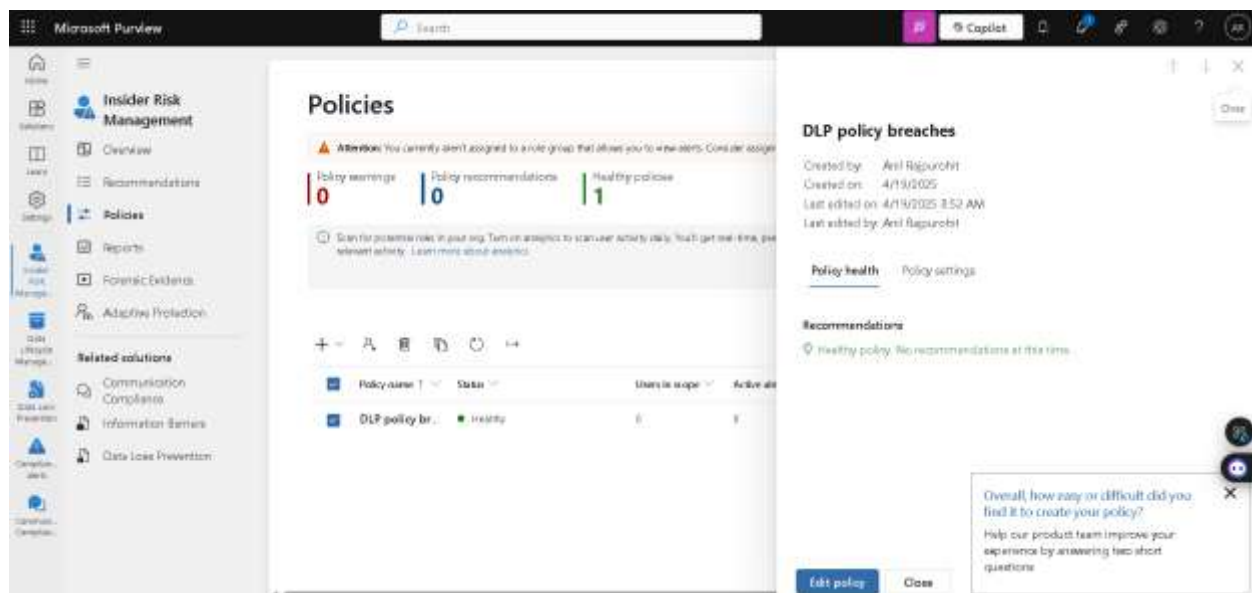
Step 21: Selected our alerts settings.

Step 22: Review settings of our policy then click on Submit.

Step 23: Our policy has been successfully created.



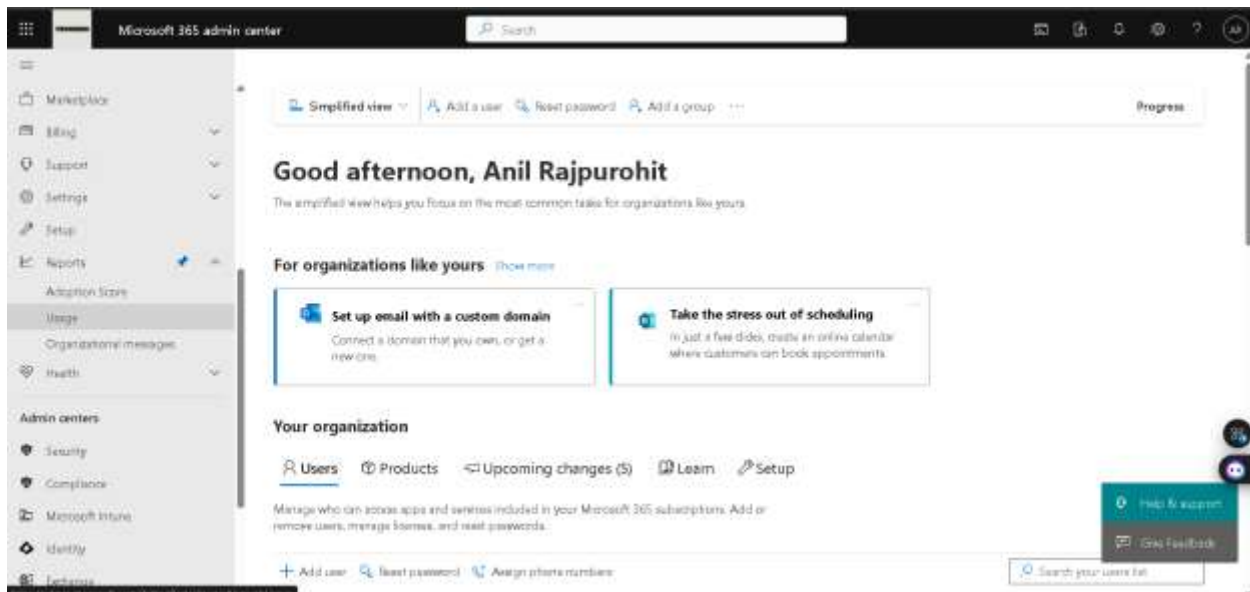
Step 24: We can view our policy under Insider risk management -> policies.



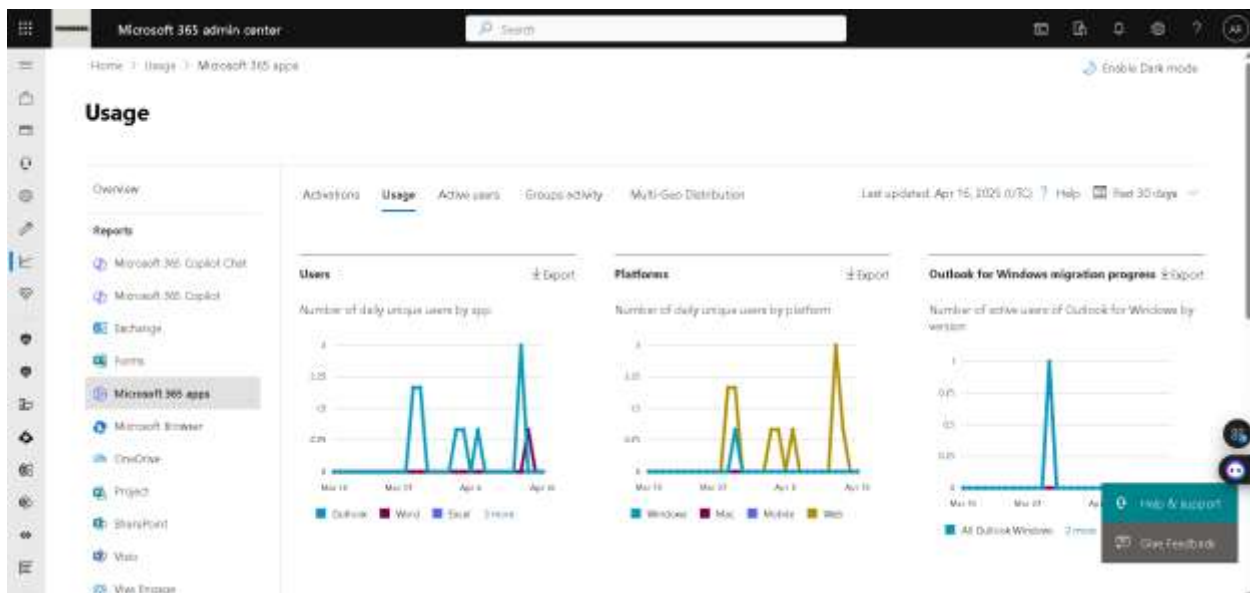
3. Generate Usage Reports:

- Use the Microsoft 365 admin center to generate reports on user activity, email usage, and SharePoint site usage.

Step 1: To generate usage reports, go to Microsoft 365 admin center -> usage.

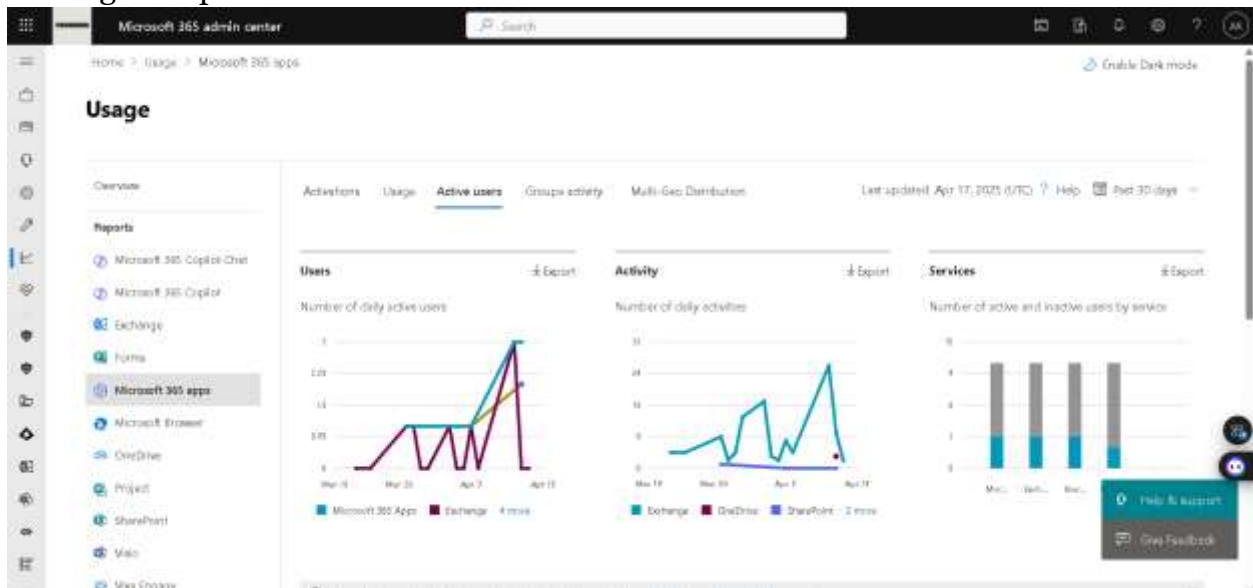


Step 2: Under Usage -> Microsoft 365 Apps -> usage. We can also export usage by clicking on export.

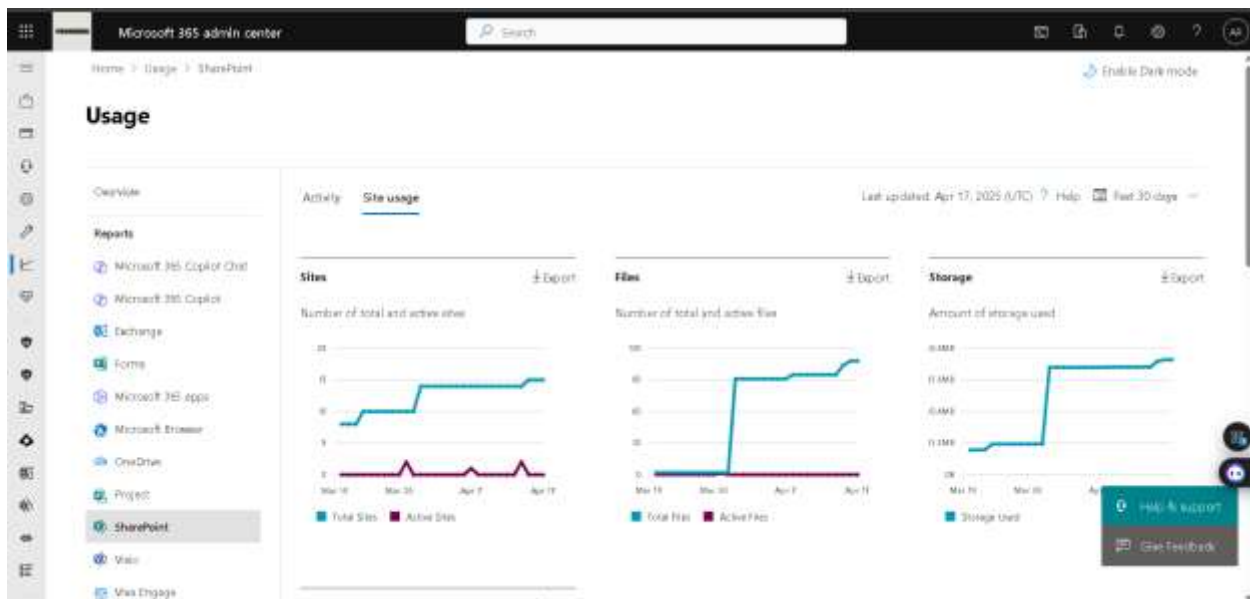


Report Refresh Date	Report Period	Report Date	Outlook	Word	Excel	PowerPoint	OneNote	Teams
2025-04-16	30	2025-04-16	0	0	0	0	0	0
2025-04-16	30	2025-04-15	0	0	0	0	0	0
2025-04-16	30	2025-04-14	0	1	0	0	0	0
2025-04-16	30	2025-04-13	3	0	0	0	0	0
2025-04-16	30	2025-04-12	0	0	0	0	0	0
2025-04-16	30	2025-04-11	0	0	0	0	0	0
2025-04-16	30	2025-04-10	0	0	0	0	0	0
2025-04-16	30	2025-04-09	0	0	0	0	0	0
2025-04-16	30	2025-04-08	0	0	0	0	0	0
2025-04-16	30	2025-04-07	1	0	0	0	0	0
2025-04-16	30	2025-04-06	0	0	0	0	0	0
2025-04-16	30	2025-04-05	1	0	0	0	0	0
2025-04-16	30	2025-04-04	1	0	0	0	0	0
2025-04-16	30	2025-04-03	0	0	0	0	0	0
2025-04-16	30	2025-04-02	0	0	0	0	0	0
2025-04-16	30	2025-04-01	0	0	0	0	0	0
2025-04-16	30	2025-03-31	0	0	0	0	0	0
2025-04-16	30	2025-03-30	1	0	0	0	0	0
2025-04-16	30	2025-03-29	2	0	0	0	0	0
2025-04-16	30	2025-03-28	0	0	0	0	0	0
2025-04-16	30	2025-03-27	0	0	0	0	0	0
2025-04-16	30	2025-03-26	0	0	0	0	0	0
2025-04-16	30	2025-03-25	0	0	0	0	0	0

Step 3: Under Usage -> Microsoft 365 Apps -> active users. We can also export usage by clicking on export.



Step 4: Under Usage -> exchange -> email activity. We can also export usage by clicking on export.



SharePointSiteUsageSiteCount_H_2025-03-01...

File Home Insert Page Layout Formulas Data Review View Help Acrobat

PROTECTED DATA: Some features might be hidden due to your data protection settings. To access these features, you may need to adjust the settings. Don't show this message Show this message

Report Refresh Date

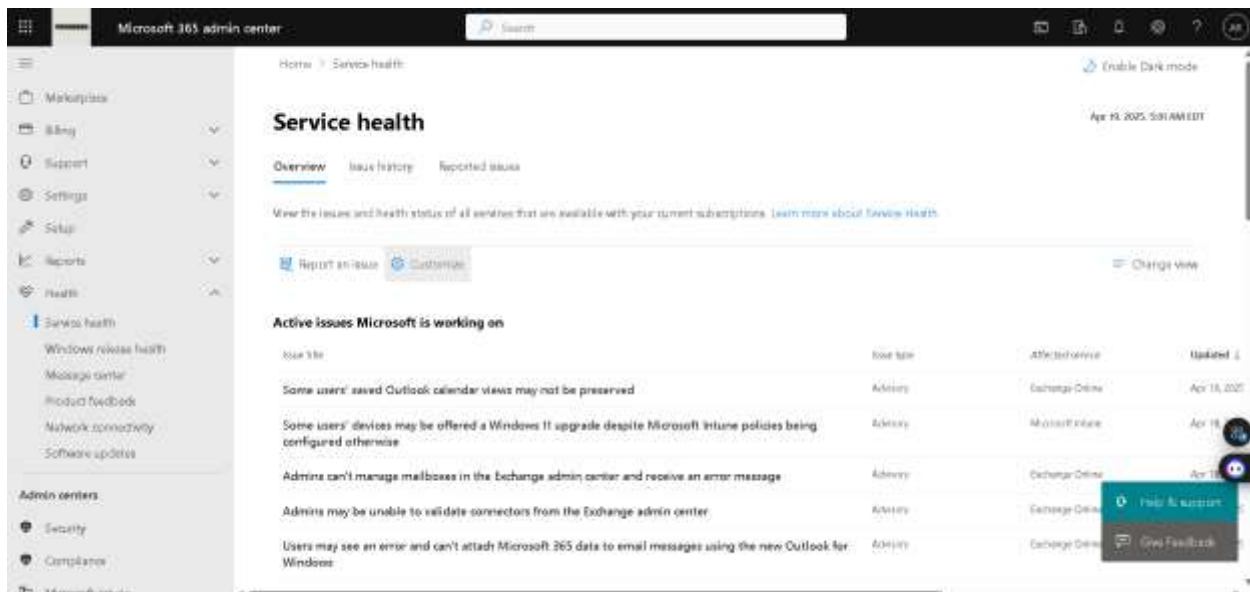
Report Refresh Date	Site Type	Total	Active	Report Date	Report Period
2025-06-17	AI	10	0	2025-06-17	30
2025-06-17	AI	10	0	2025-06-16	30
2025-06-17	AI	10	0	2025-06-15	30
2025-06-17	AI	14	2	2025-06-14	30
2025-06-17	AI	14	0	2025-06-13	30
2025-06-17	AI	14	0	2025-06-12	30
2025-06-17	AI	14	0	2025-06-11	30
2025-06-17	AI	14	0	2025-06-10	30
2025-06-17	AI	14	0	2025-06-09	30
2025-06-17	AI	14	0	2025-06-08	30
2025-06-17	AI	14	1	2025-06-07	30
2025-06-17	AI	14	0	2025-06-06	30
2025-06-17	AI	14	0	2025-06-05	30
2025-06-17	AI	14	0	2025-06-04	30
2025-06-17	AI	14	0	2025-06-03	30
2025-06-17	AI	14	0	2025-06-02	30
2025-06-17	AI	14	0	2025-06-01	30
2025-06-17	AI	10	0	2025-05-31	30
2025-06-17	AI	10	2	2025-05-29	30
2025-06-17	AI	10	0	2025-05-28	30
2025-06-17	AI	10	0	2025-05-27	30
2025-06-17	AI	10	0	2025-05-26	30

SharePointSiteUsageSiteCount_H_2025-03-01...

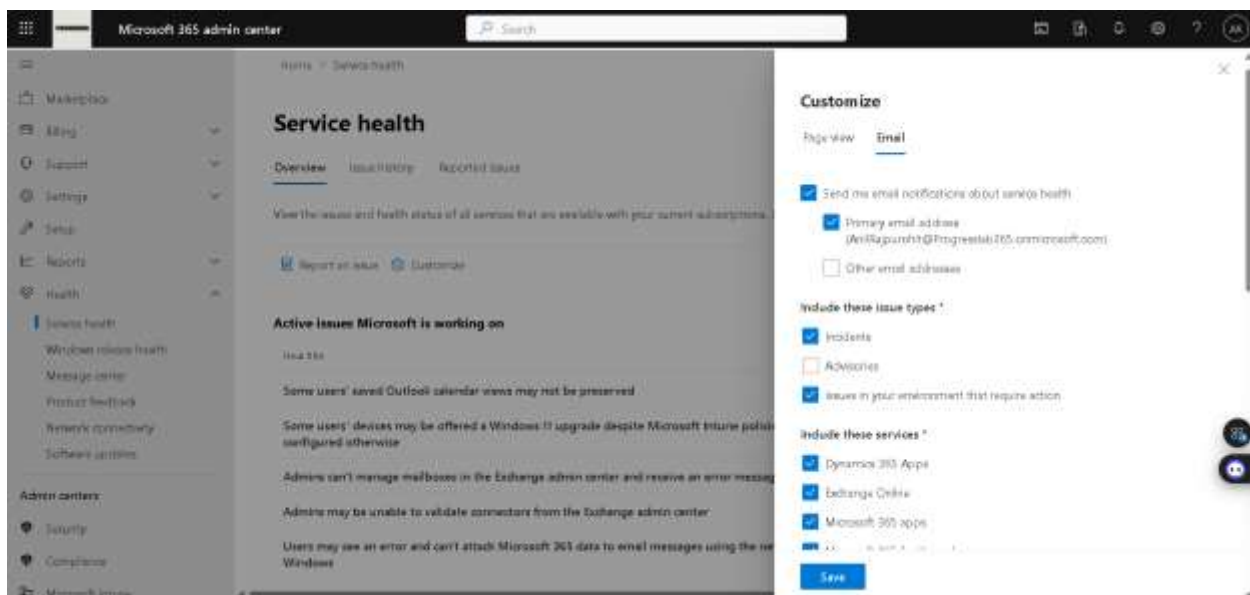
4. Implement and Monitor Service Health:

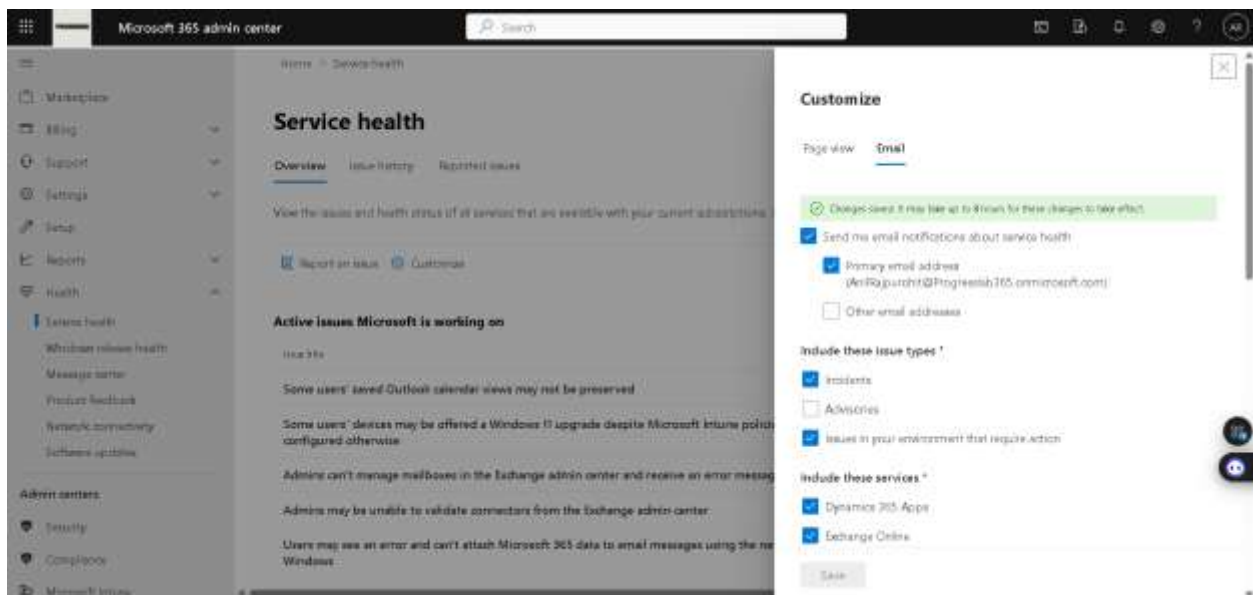
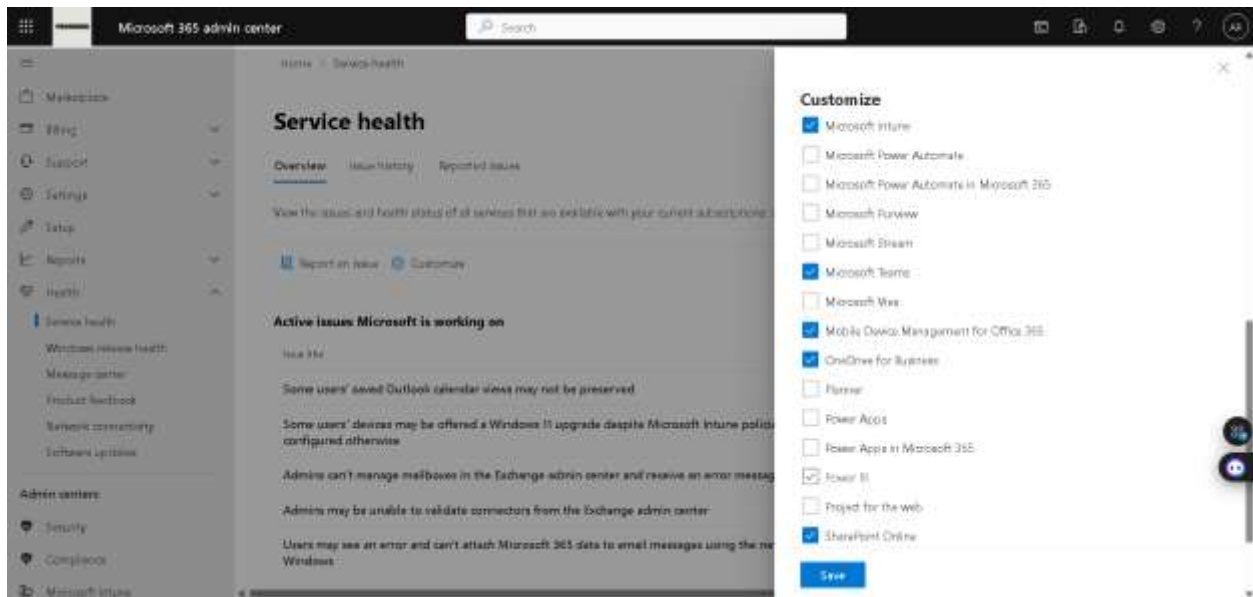
- Set up service health alerts to notify administrators of any issues with Microsoft 365 services.

Step 1: In Microsoft 365 admin center, health -> service health -> customize.



Step 2: Here we can select, which notification to get on our email id. Then click on Save.





- Monitor the Service Health dashboard regularly to ensure all services are running smoothly.

Step 1: To monitor the Service Health dashboard, in Microsoft 365 admin center -> health -> service health.

Microsoft 365 admin center

Service health

Overview | Issue history | Reported issues

View the issues and health status of all services that are available with your current subscriptions. [Learn more about Service Health](#)

[Report an issue](#) [Customize](#) [Change view](#)

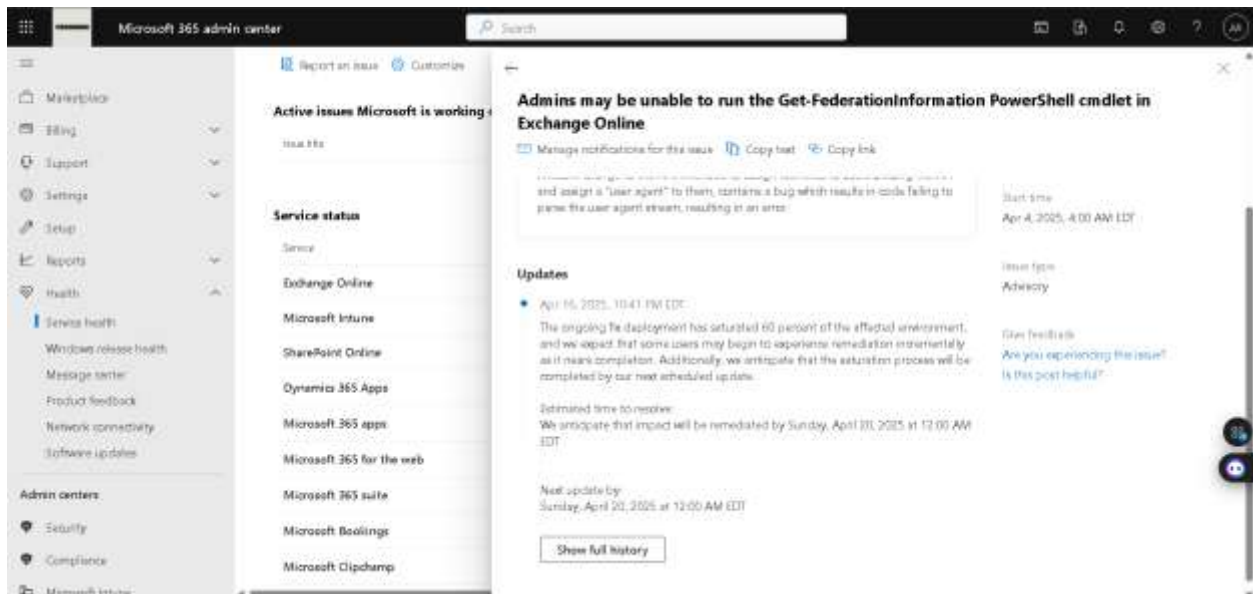
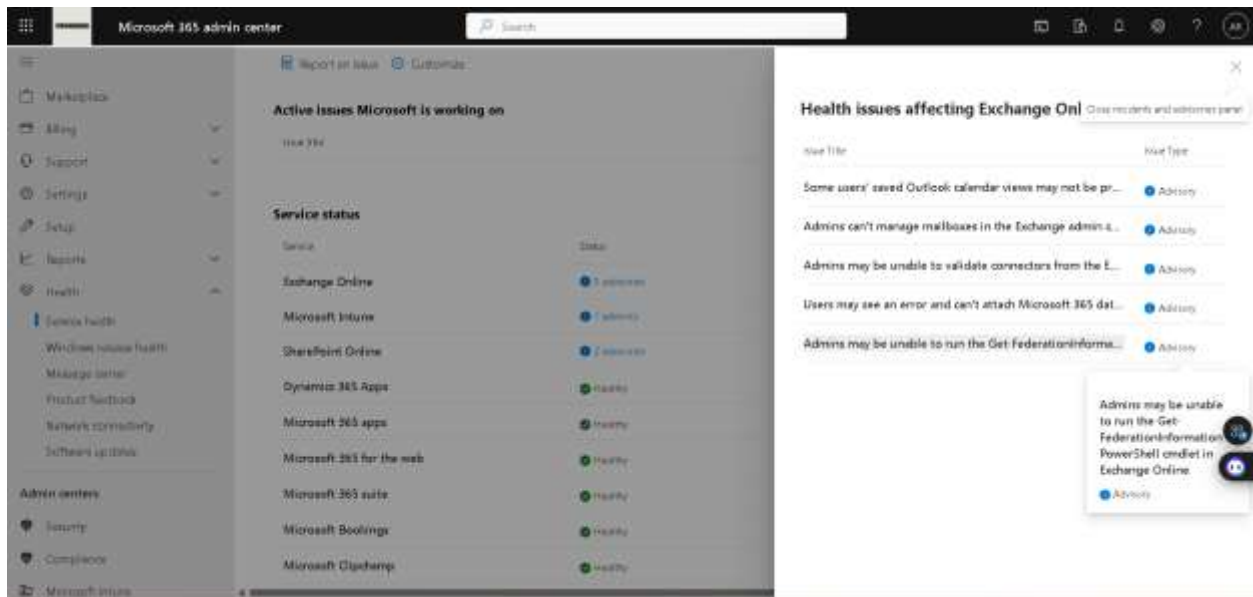
Active issues Microsoft is working on

Issue title	Issue type	Affected service	Updated
Some users' saved Outlook calendar views may not be preserved	Advisory	Exchange Online	Apr 16, 2021
Some users' devices may be offered a Windows 11 upgrade despite Microsoft Intune policies being configured otherwise	Advisory	Microsoft Intune	Apr 16, 2021
Admins can't manage mailboxes in the Exchange admin center and receive an error message	Advisory	Exchange Online	Apr 16, 2021
Admins may be unable to validate connectors from the Exchange admin center	Advisory	Exchange Online	Apr 17, 2021
Users may see an error and can't attach Microsoft 365 data to email messages using the new Outlook for Windows	Advisory	Exchange Online	Apr 17, 2021
Admins may be unable to run the Get-FederationInformation PowerShell cmdlet in Exchange Online	Advisory	Exchange Online	Apr 17, 2021
Users' SharePoint Online pages may be failing to generate thumbnails of webparts	Advisory	SharePoint Online	Apr 16, 2021

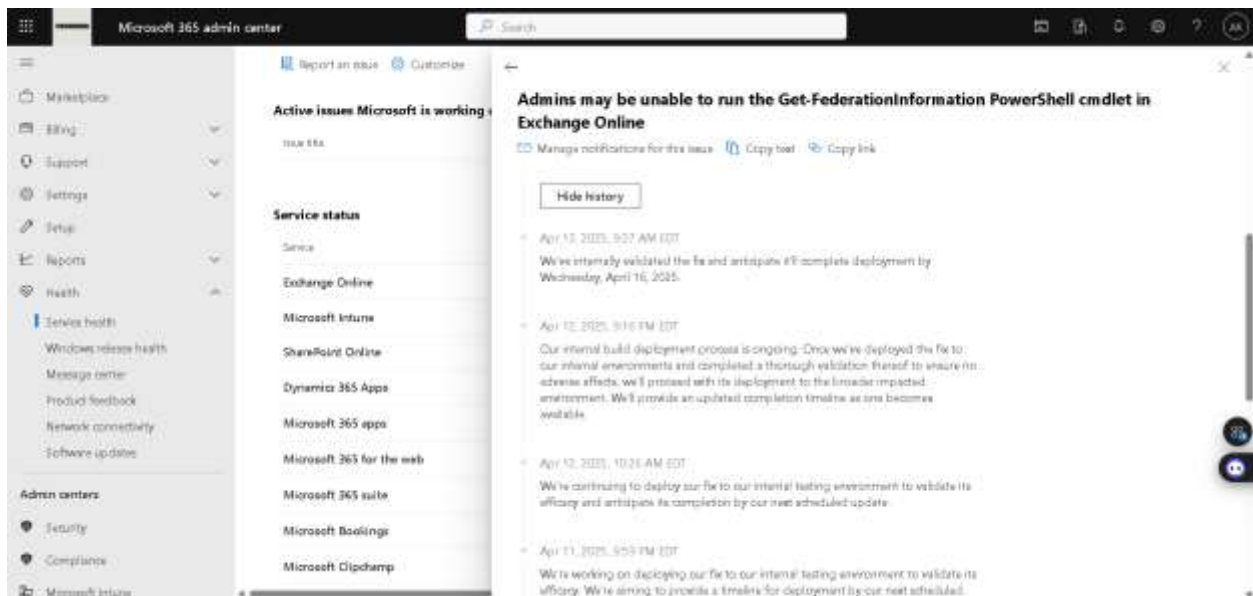
Service status

Service	Status
Exchange Online	3 advisory
Microsoft Intune	1 advisory
SharePoint Online	2 advisory
Dynamics 365 Apps	Healthy
Microsoft 365 apps	Healthy
Microsoft 365 for the web	Healthy
Microsoft 365 suite	Healthy
Microsoft Bookings	Healthy
Microsoft Clipchamp	Healthy
Microsoft Defender XDR	Healthy
Microsoft Entra	Healthy
Microsoft Forms	Healthy

Step 2: We can check info about advisories for many services, and we should stay updated about those services .So, We can help our users accordingly.



Step 3: We can also check history of those advisories, what actions has been taken and all.



LEARNING & OPINION

Creating security alerts is really important in terms of security. As, if some incident is happening and that can be malicious to our organization, then admin should be immediately notified. For that we can create Security alerts, like in above example, we created a policy for mail forwarding. Because if an attacker gain access to an admin account and he change admin mail setting to forward all the mail to his mail id. He can have access to all the sensitive mails which is intended for Admin. We can also block this setting or create an alert if someone use forwarding of mail.