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.

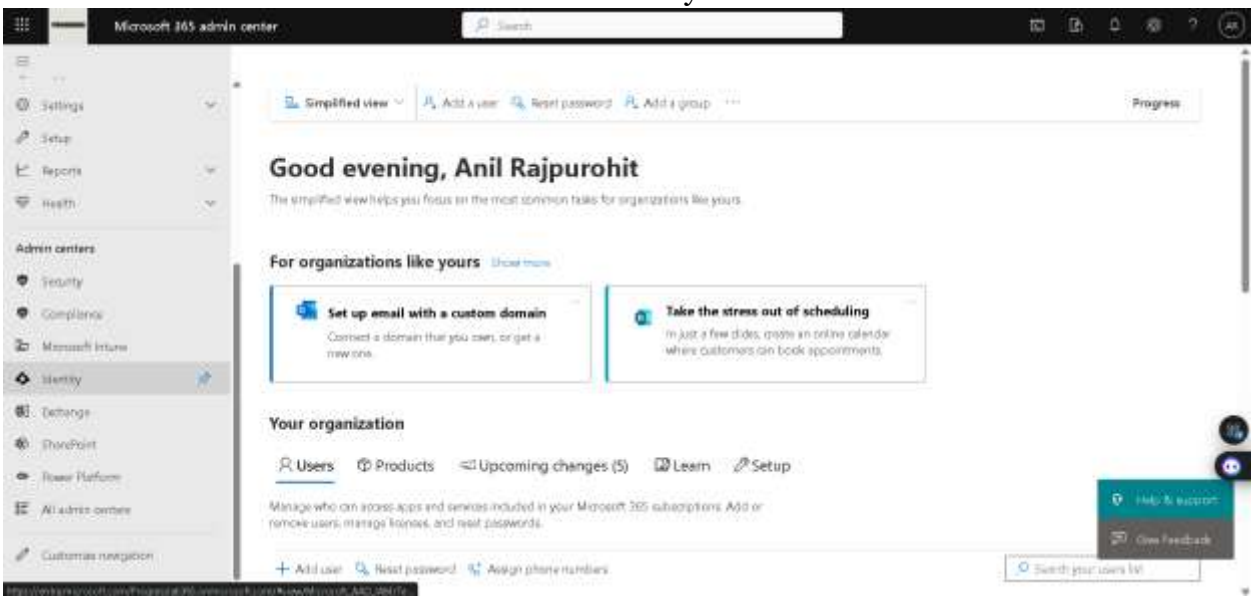
Tasks:

Task 1: Setting Up and Configuring User Accounts

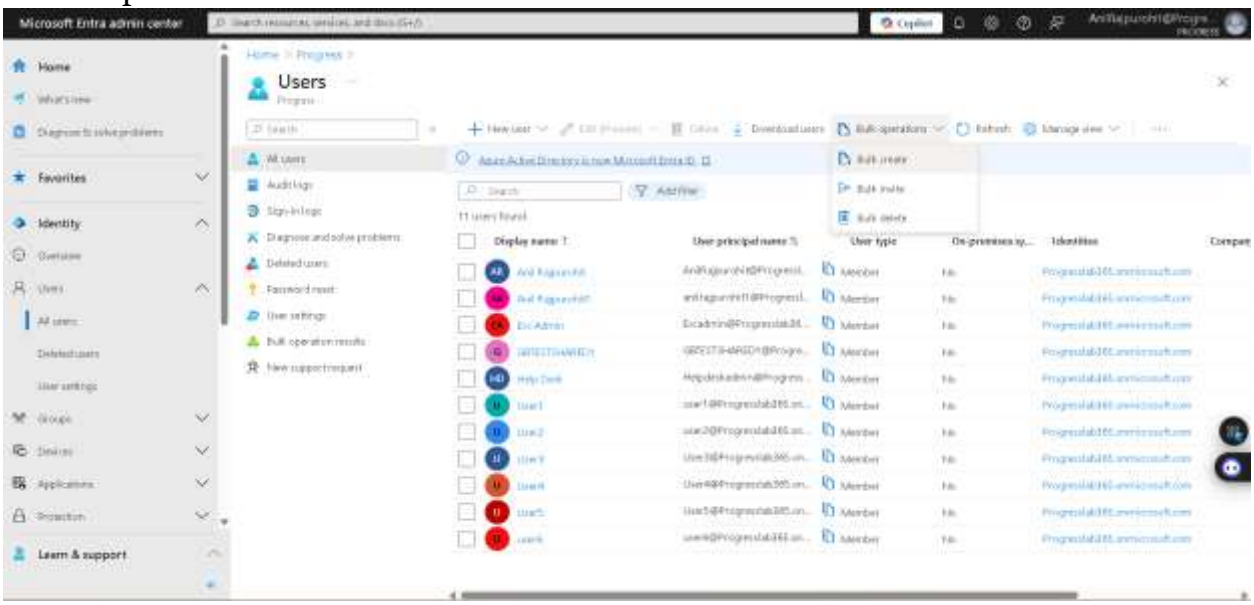
1. Bulk Import Users:

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

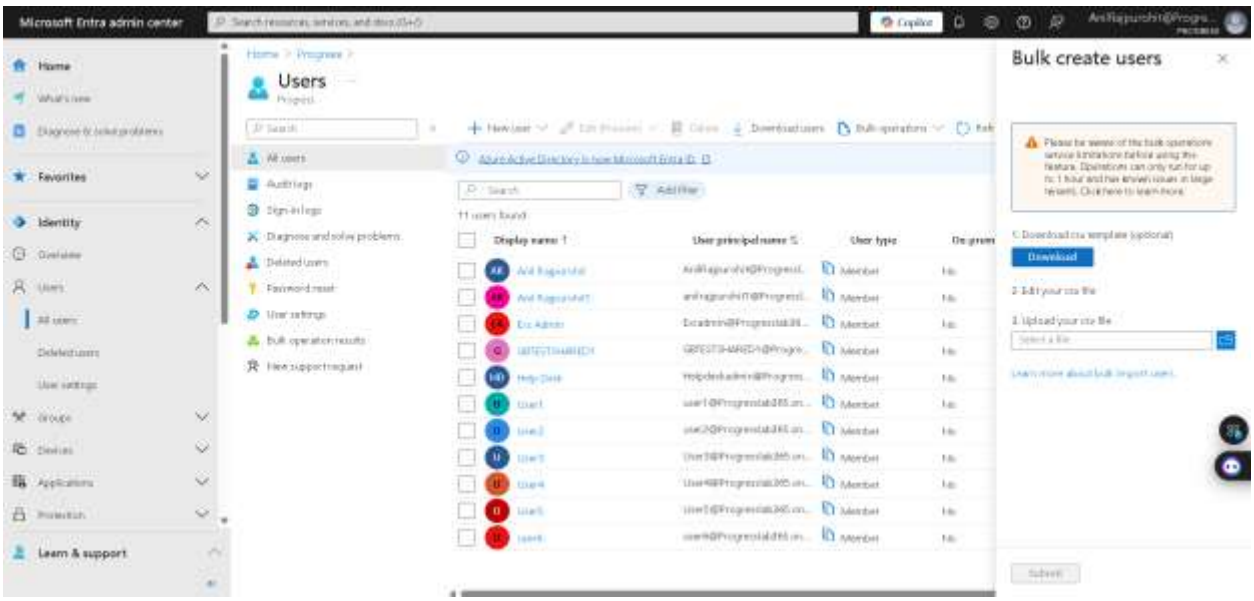
Step 1: In order to bulk import 10 users from a CSV file. First, goto Microsoft 365 admin center then under admin centers click on Identity to access Entra Admin Center.



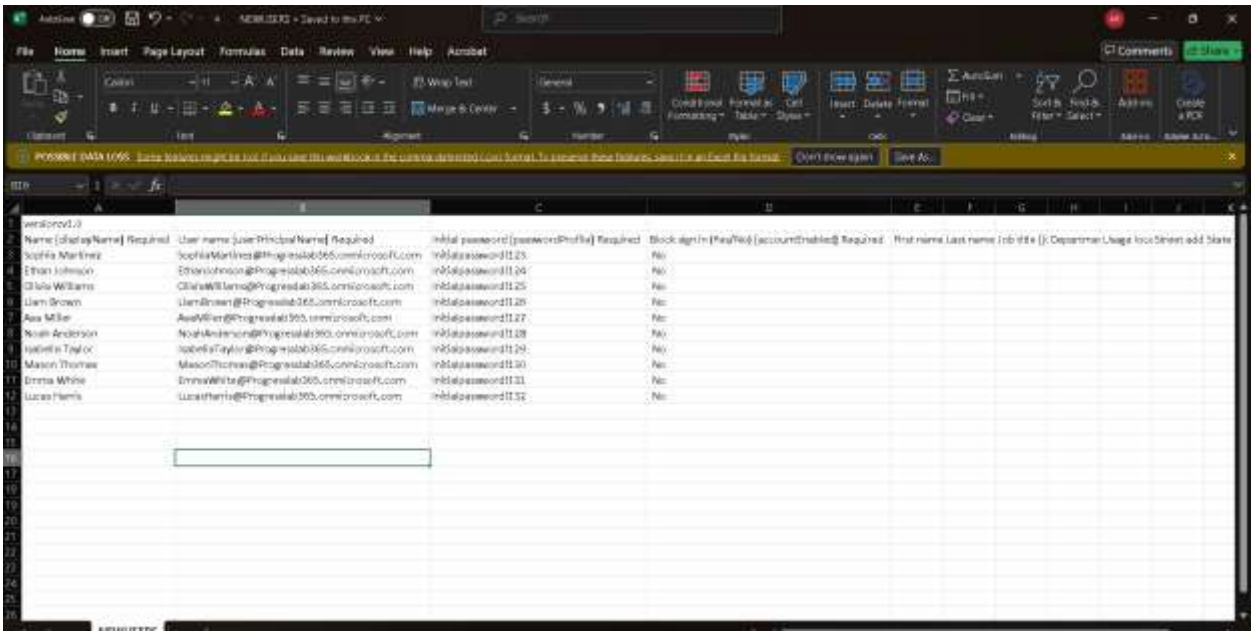
Step 2: Now from microsoft Entra Admin Center, under Identity -> Users -> All Users -> Bulk operation -> Bulk create.



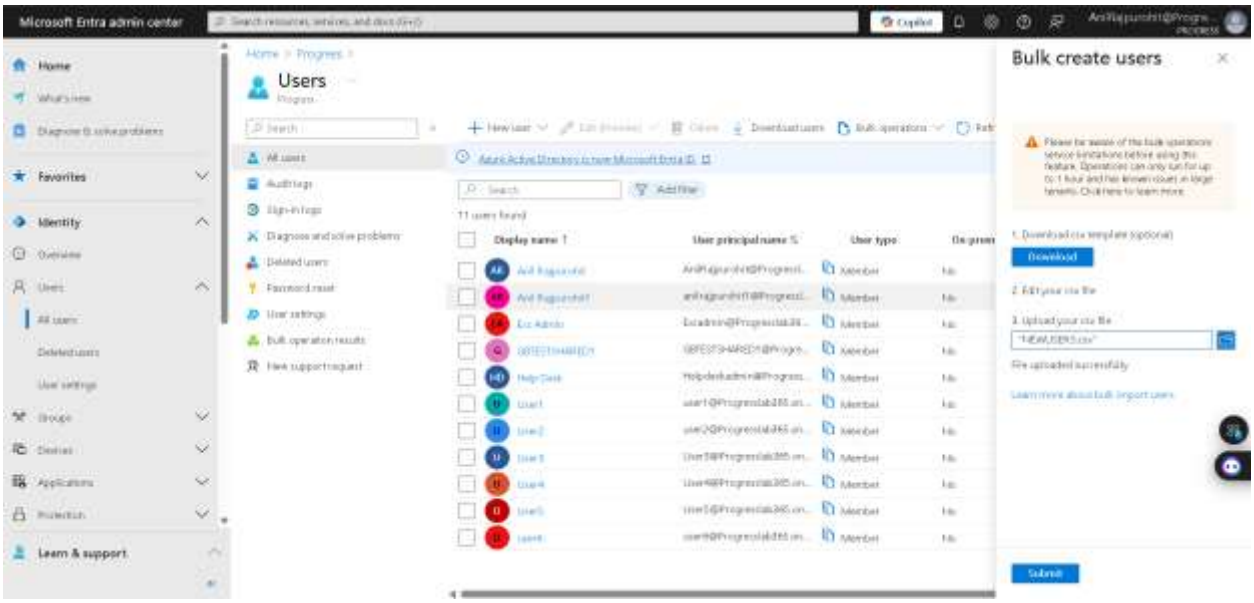
Step 3: Download .csv template.



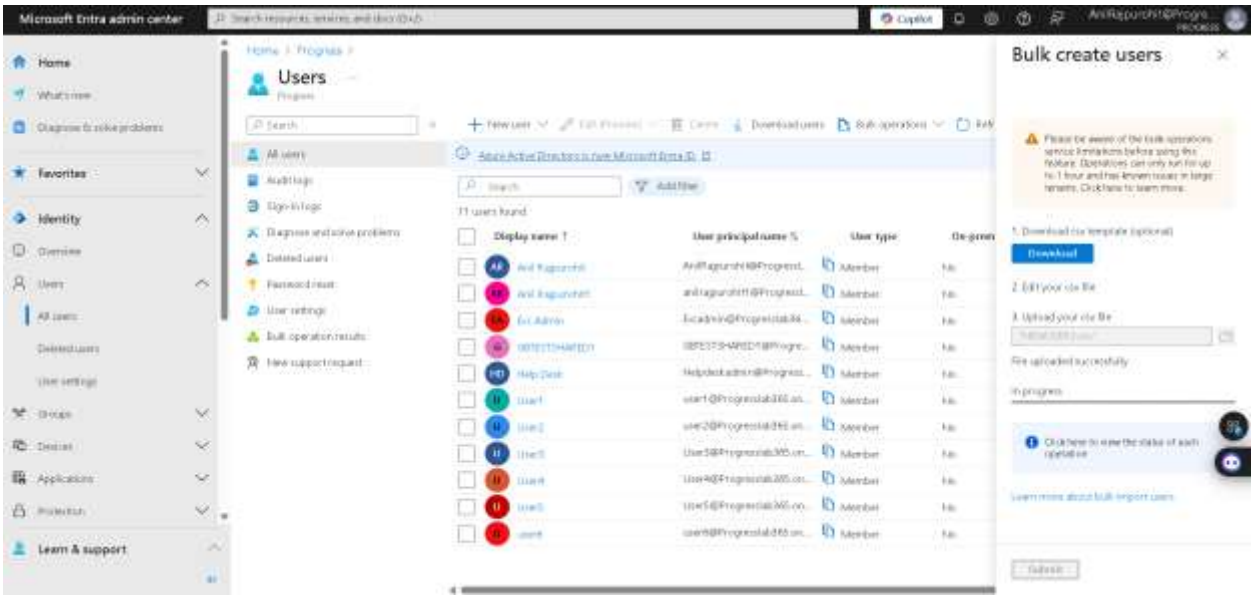
Step 4: Received the template, changed it according to our needs like added 10 new users and their passwords.



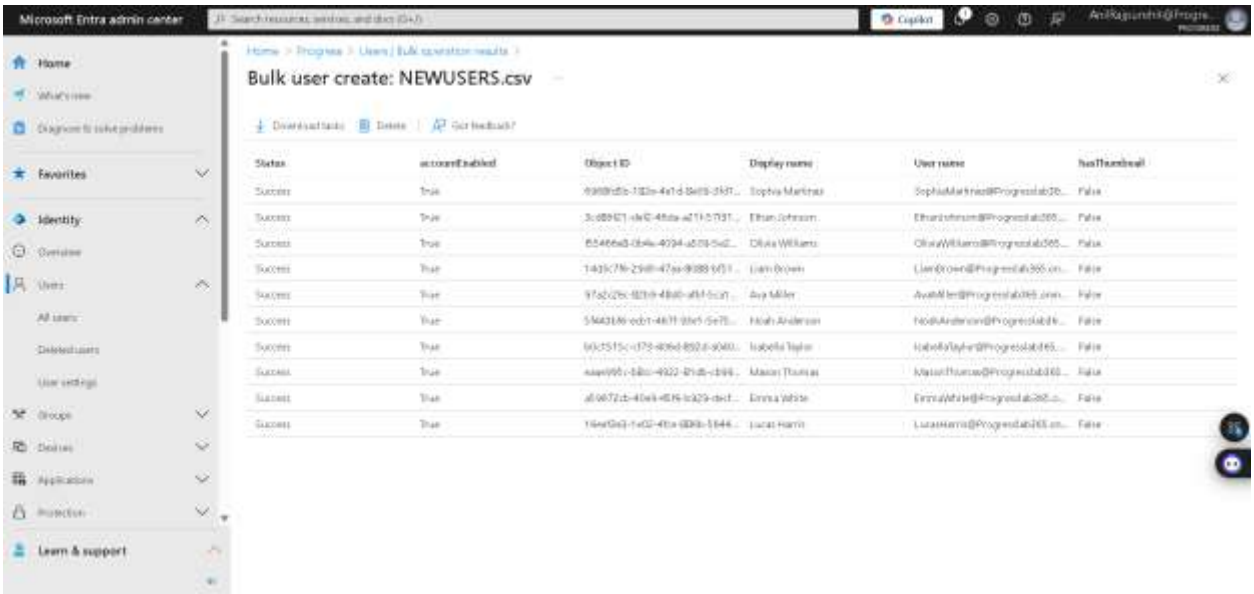
Step 5: Now in Bulk create users, upload our new users .csv file then click on Next.



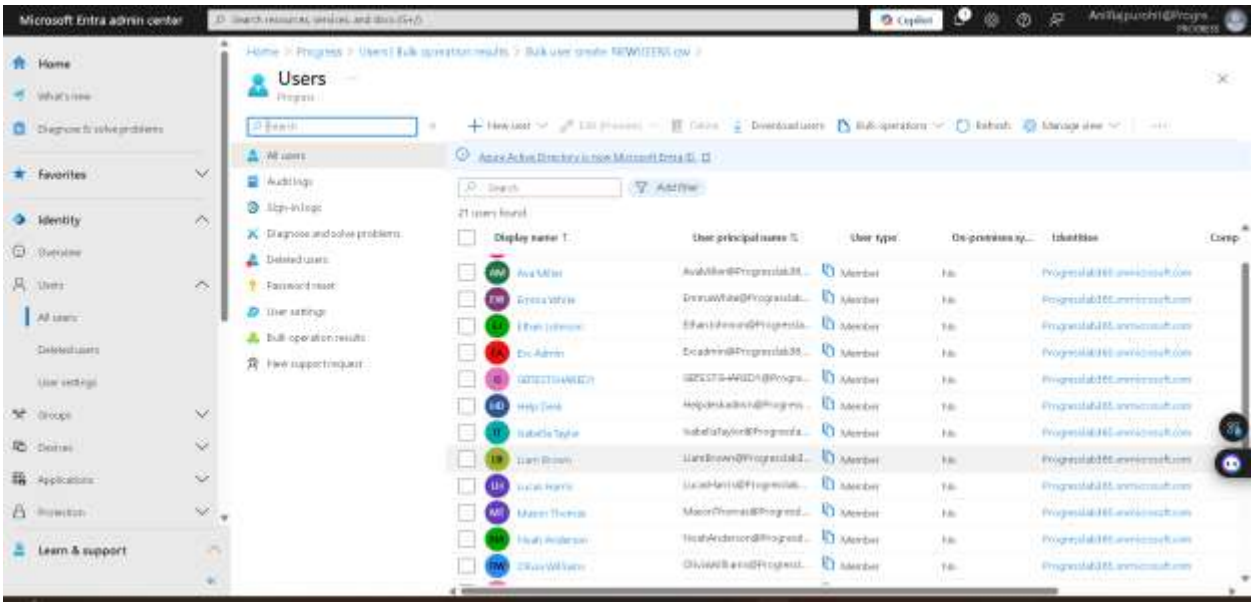
Step 6: File uploaded successfully, and to check the status of each user click on below link. (learn more about bulk import users)



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

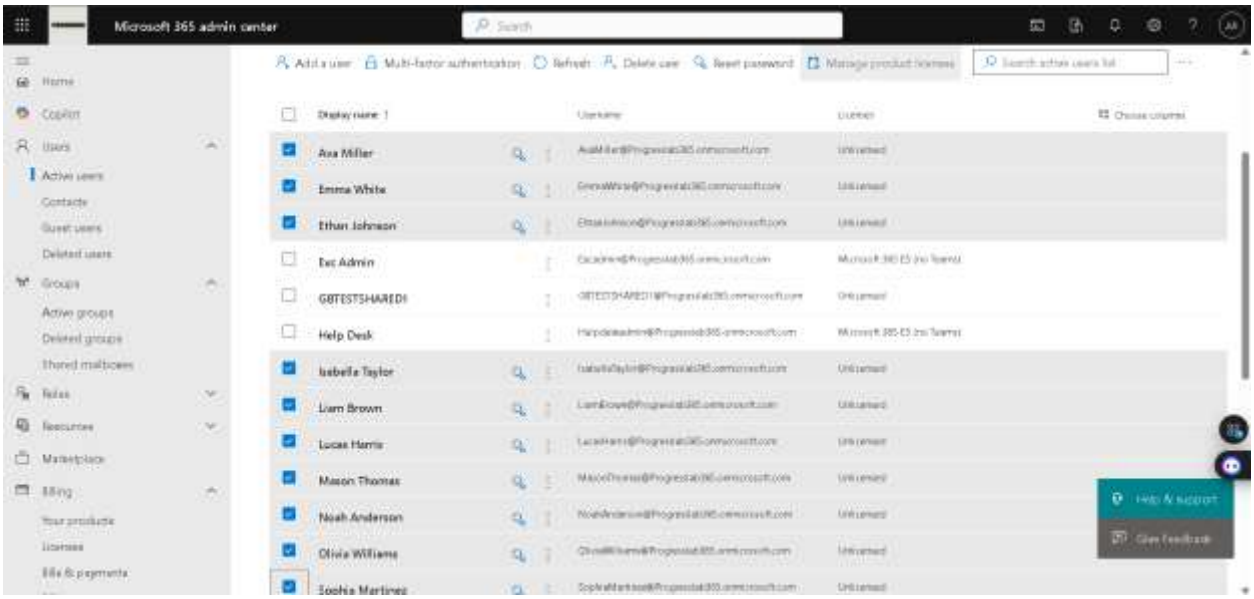


Step 8: Verifying from Entra admin center -> Identity -> Users -> All users. All our new members are successfully added to the list.

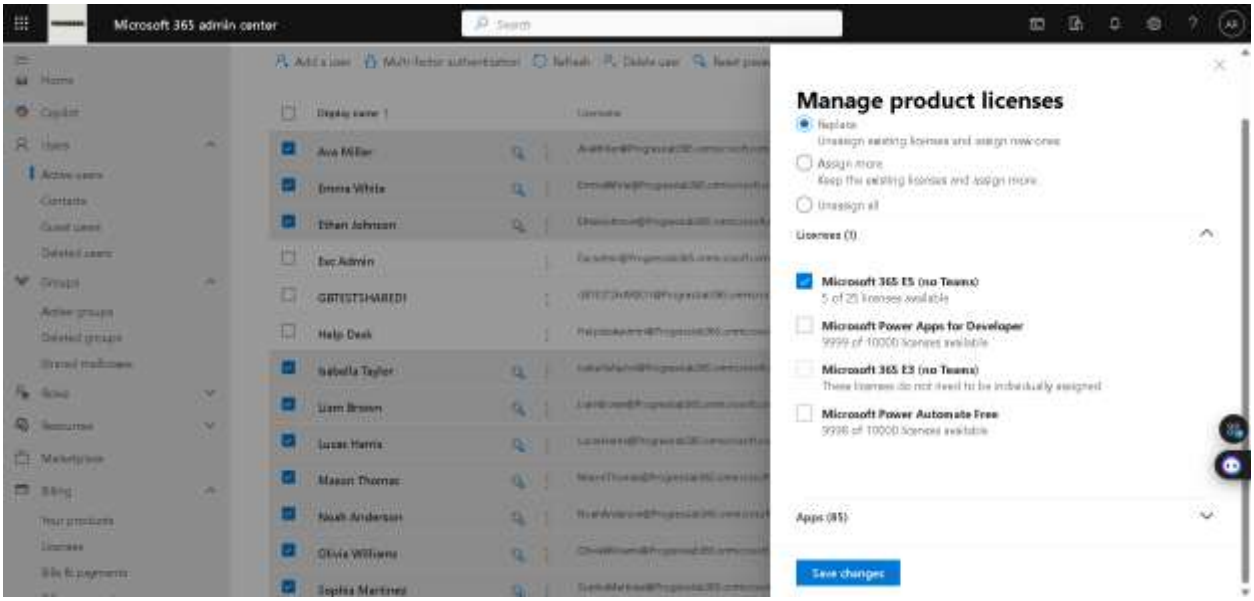


- Assign appropriate licenses (Microsoft 365 E3 or E5) to the imported users.

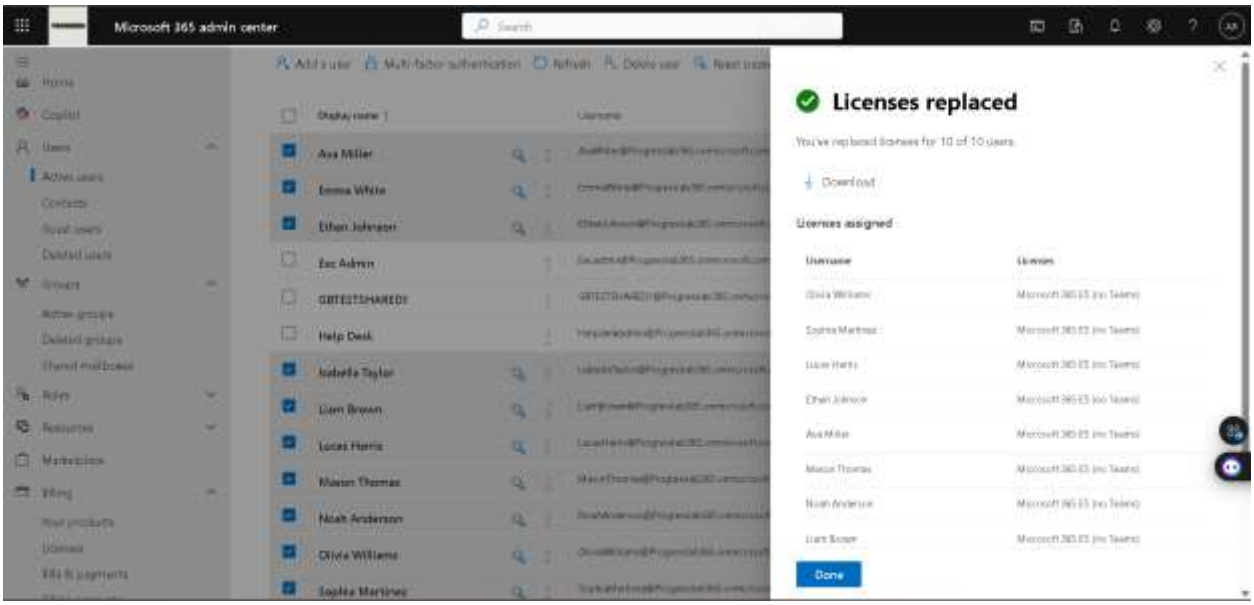
Step 1: First, go to Microsoft 365 admin center, then Users -> Active users. Select all the new users with no licenses then click on manage product licenses.



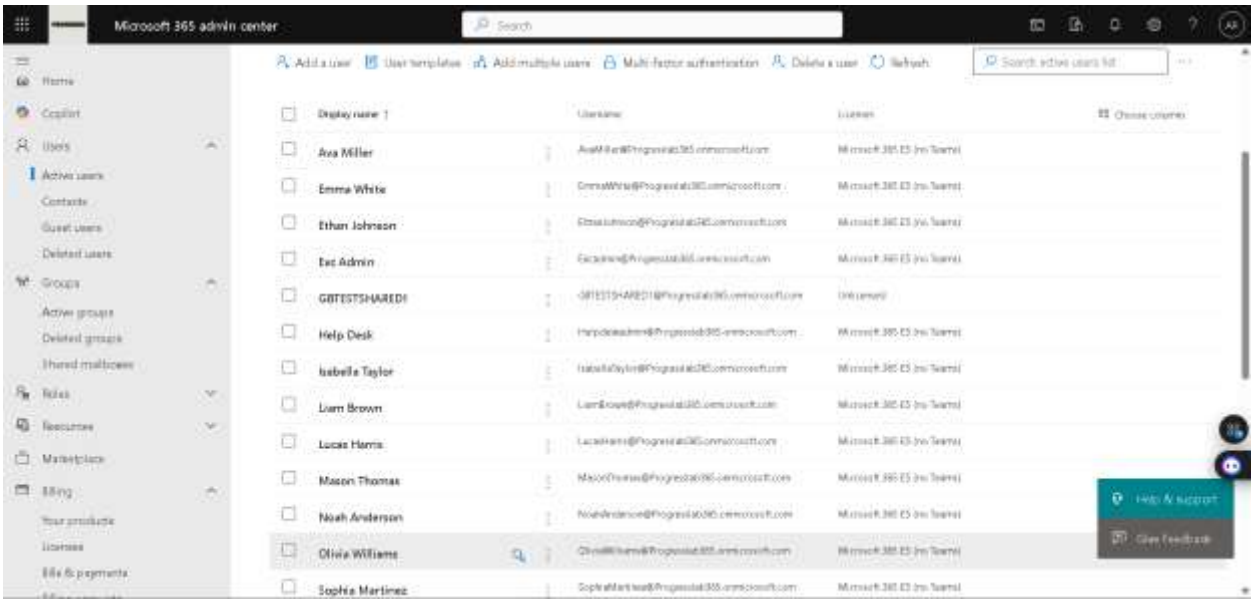
Step 2: Select replace and E5 licenses then click on save changes. This way we can assign licenses in one go.



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



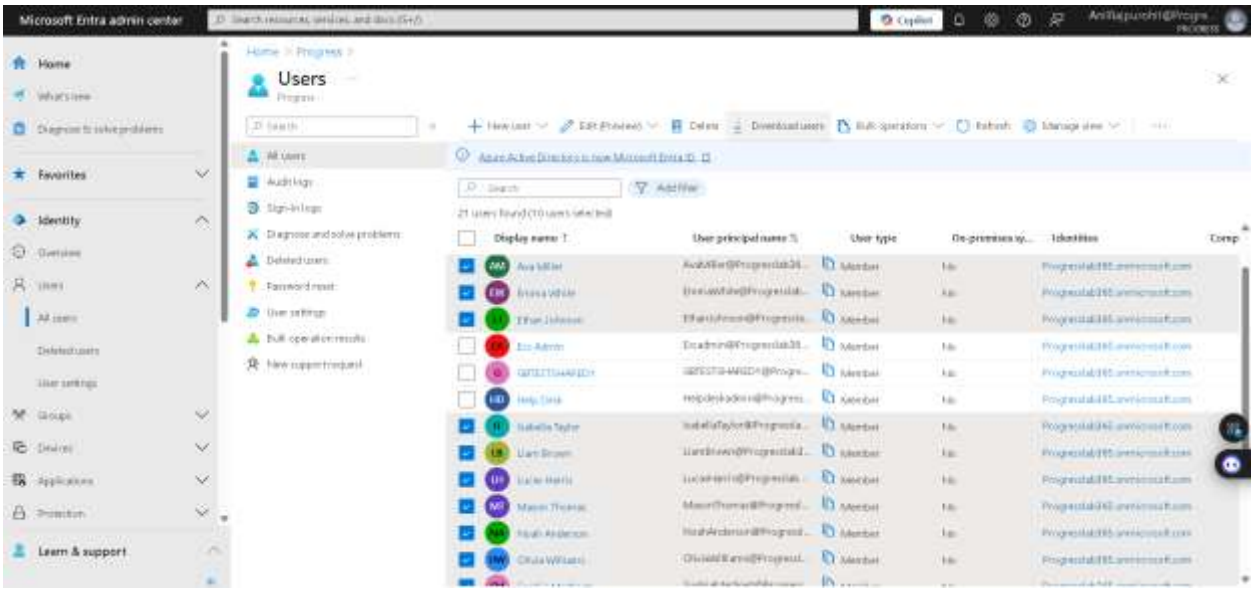
Step 4: Let's re-verify from Admin center -> users -> active users. All our members have an E5 license assigned to them.



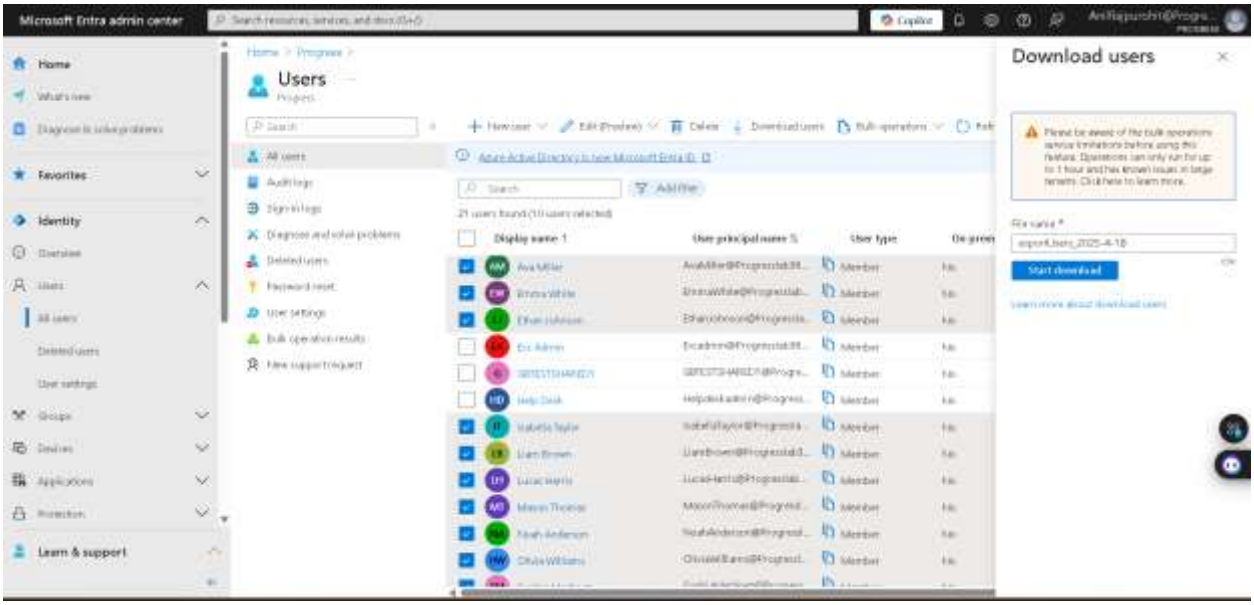
2. Configure User Profiles:

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

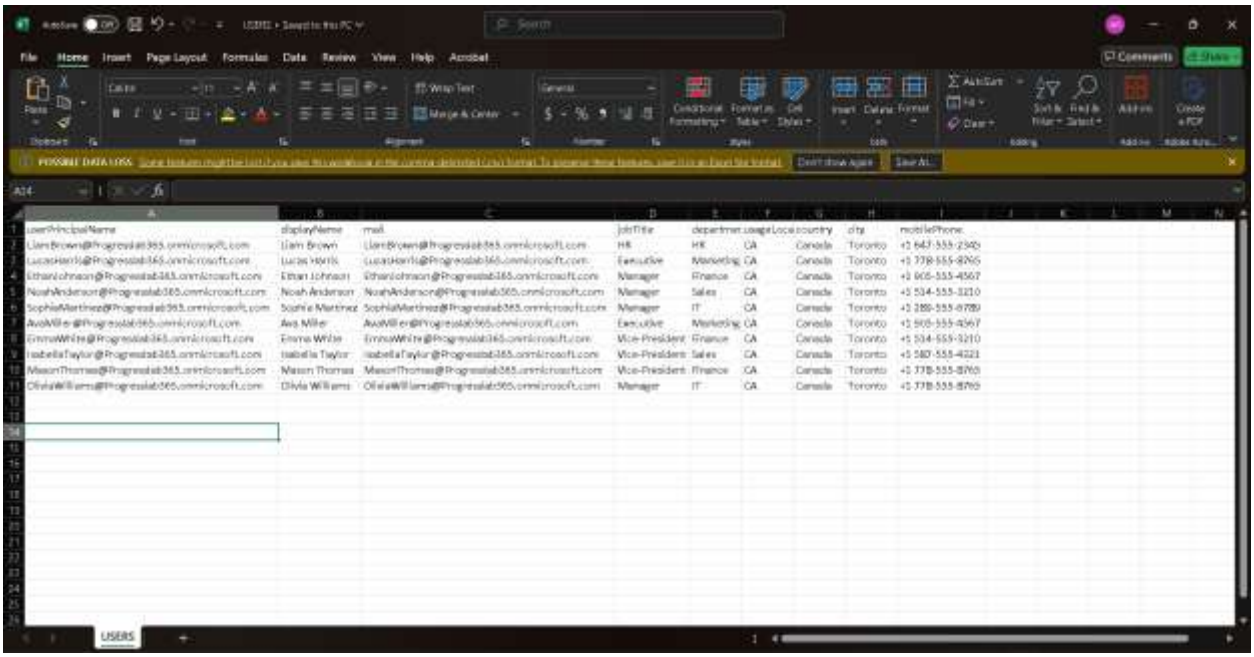
Step 1: To update user's profile, from Entra Admin C enter -> Identity -> Users -> All users. Now select all the users to update their profile then click on Download users.



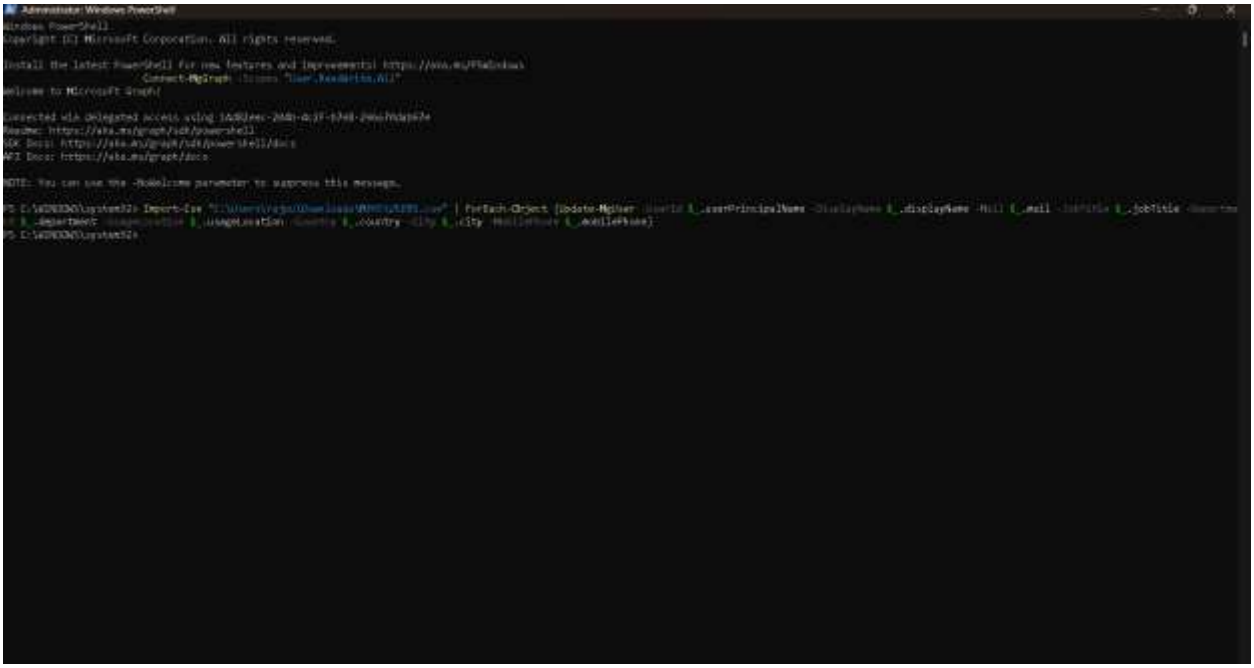
Step 2: Start download the user's file.



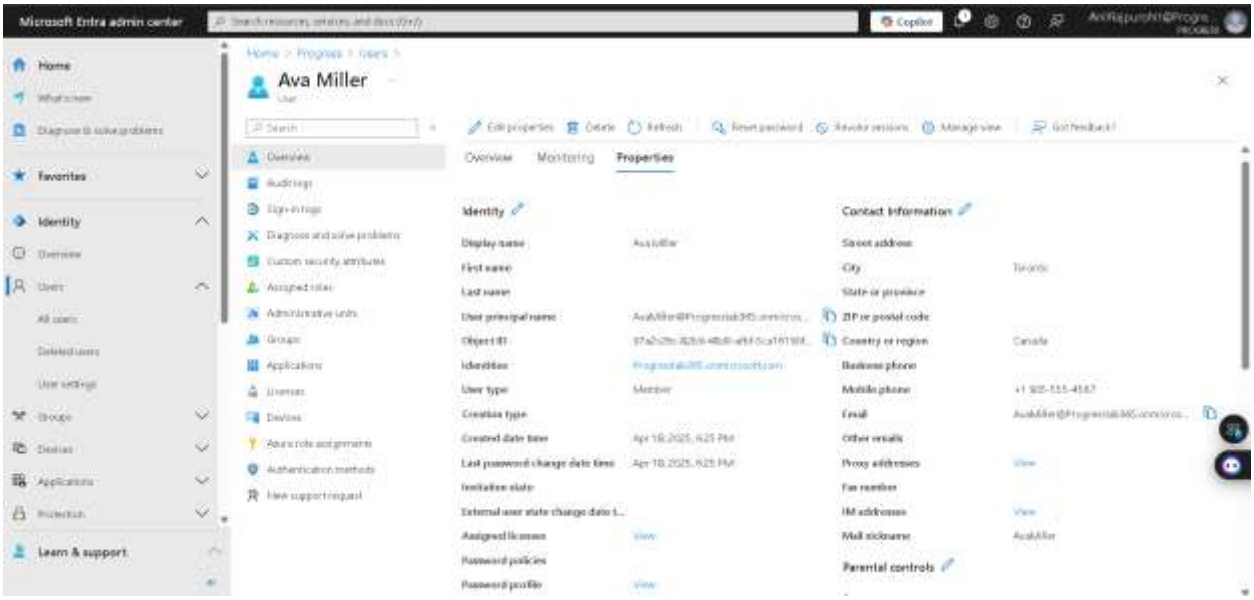
Step 3: After downloading the users file, updated all the section we need like job title, department (organization specific), usage location, country, city, and mobile number then saved the file in .csv format.



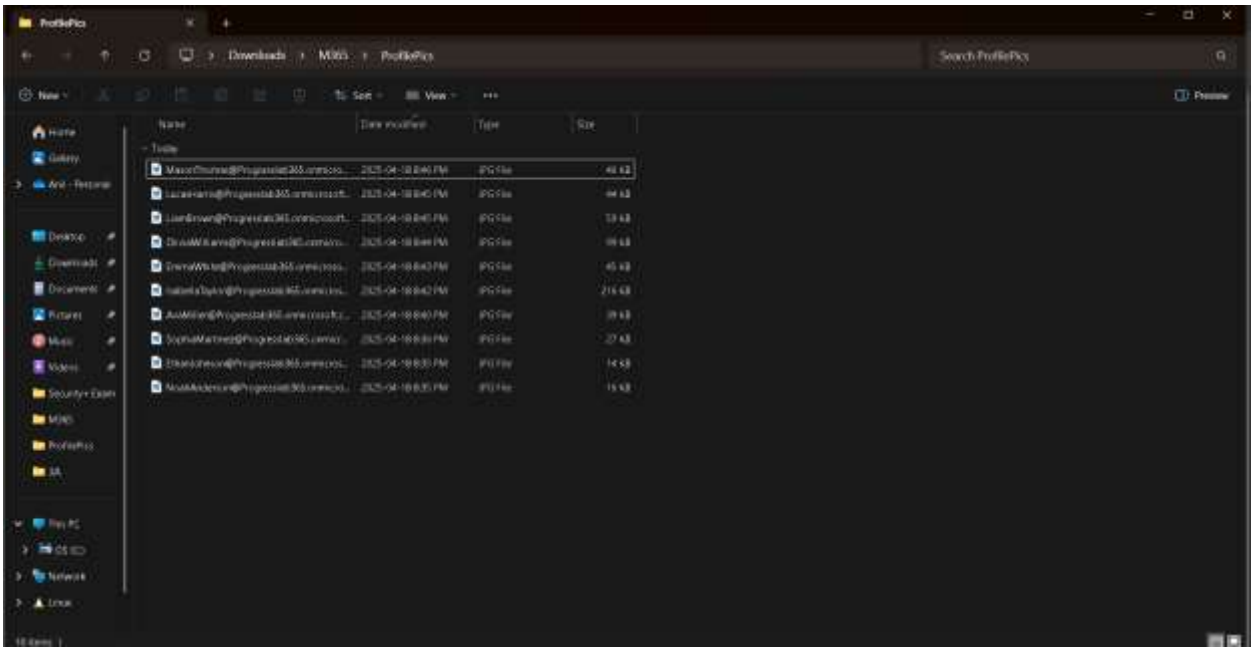
Step 4: As we want to update all the user's profile in one go, we will be using PowerShell. First, connect to Microsoft graph then imported our updated .csv file and update all new user's profile.



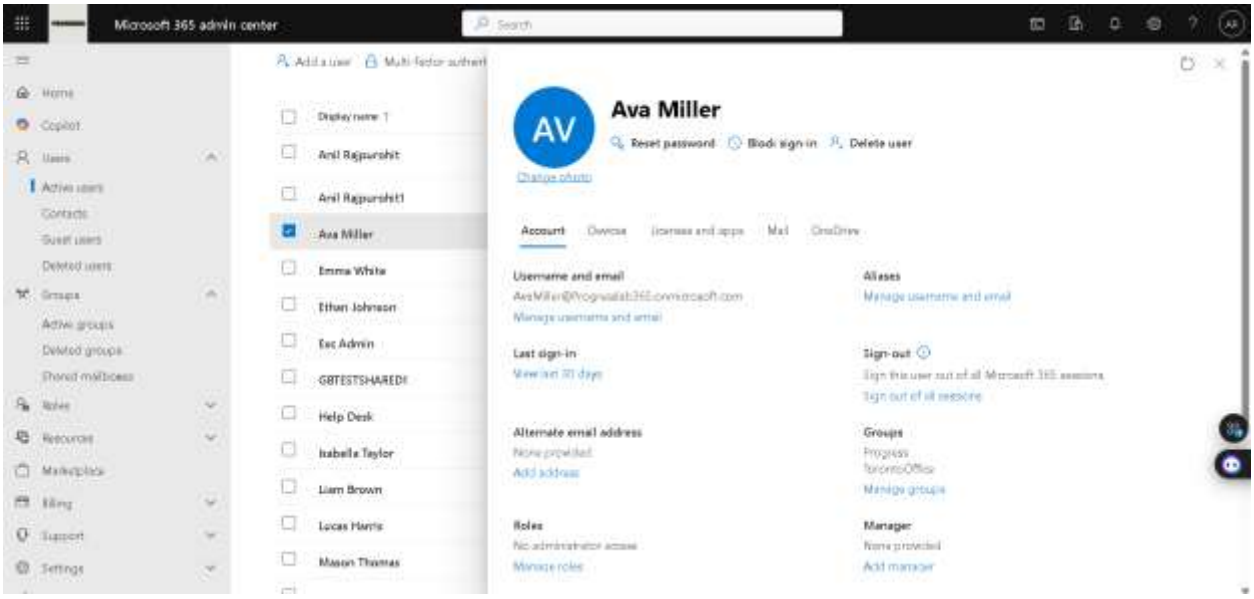
Step 5: Let's verify profile of our new user's, go to Entra admin center -> Identity -> users -> active users. Then select one new user. e.g. Ava miller and go to properties and we can view that users profile has been updated successfully.



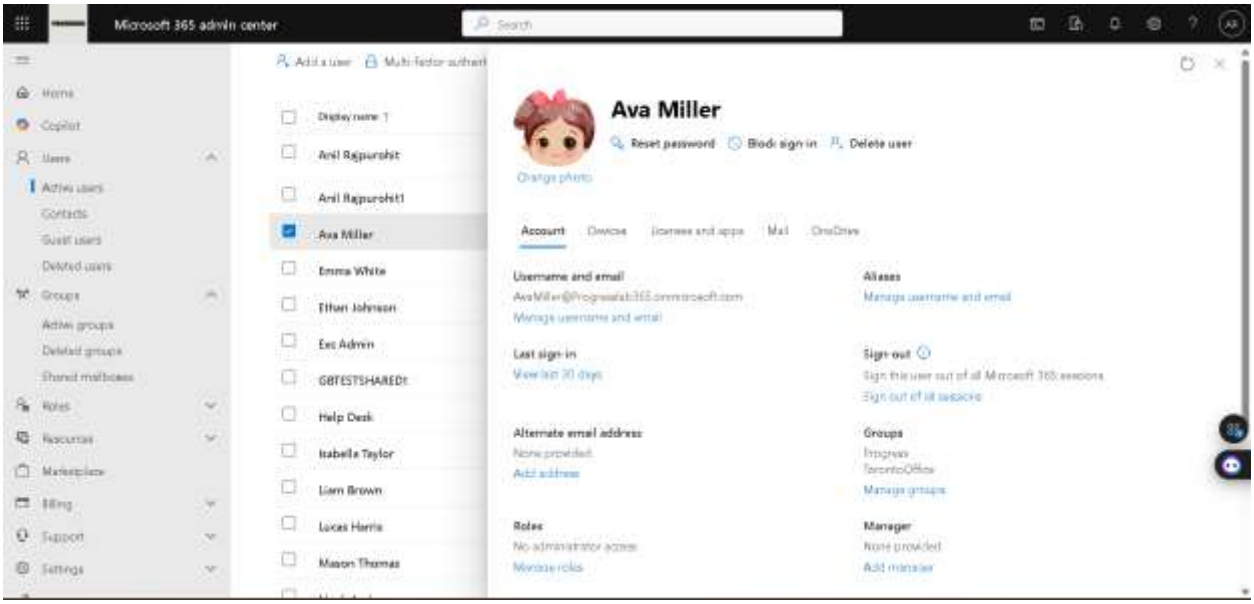
Step 6: Lets upload profile pictures for new user's, make a folder that contains all the pictures in .jpg format.



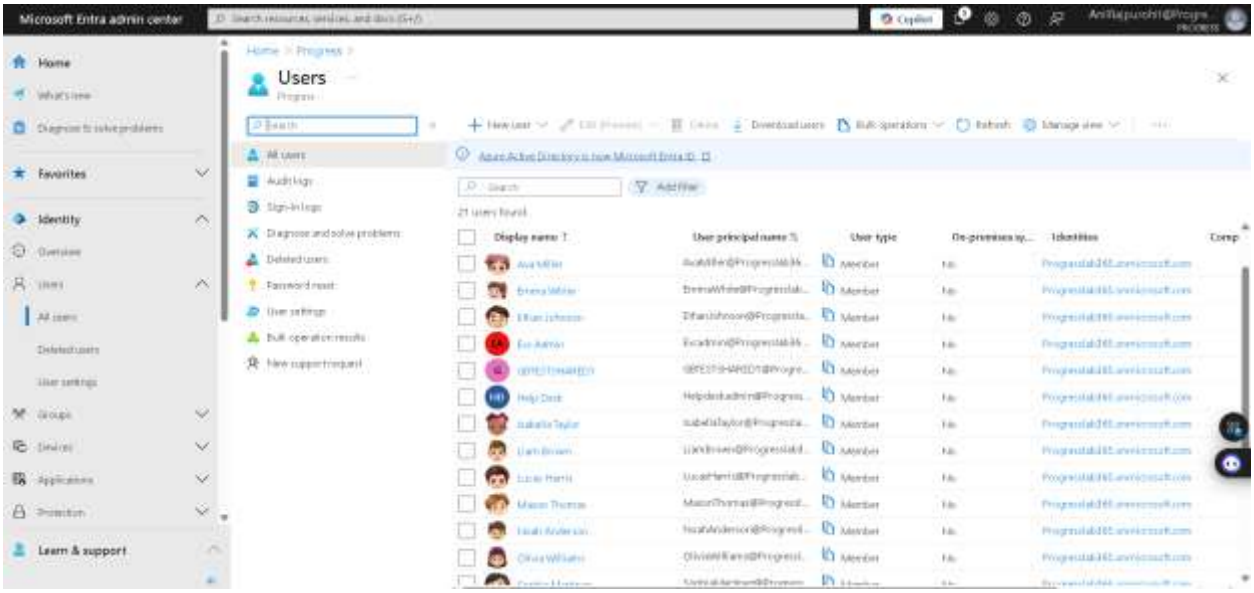
Step 7: Wanted to complete this task via PowerShell, but due to several errors as PowerShell was not accepting Set-UserPhoto. So, uploaded all new user's profile pictures manually from Microsoft 365 Admin center. First go to Users -> active users -> select the user then click in change photo.



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.

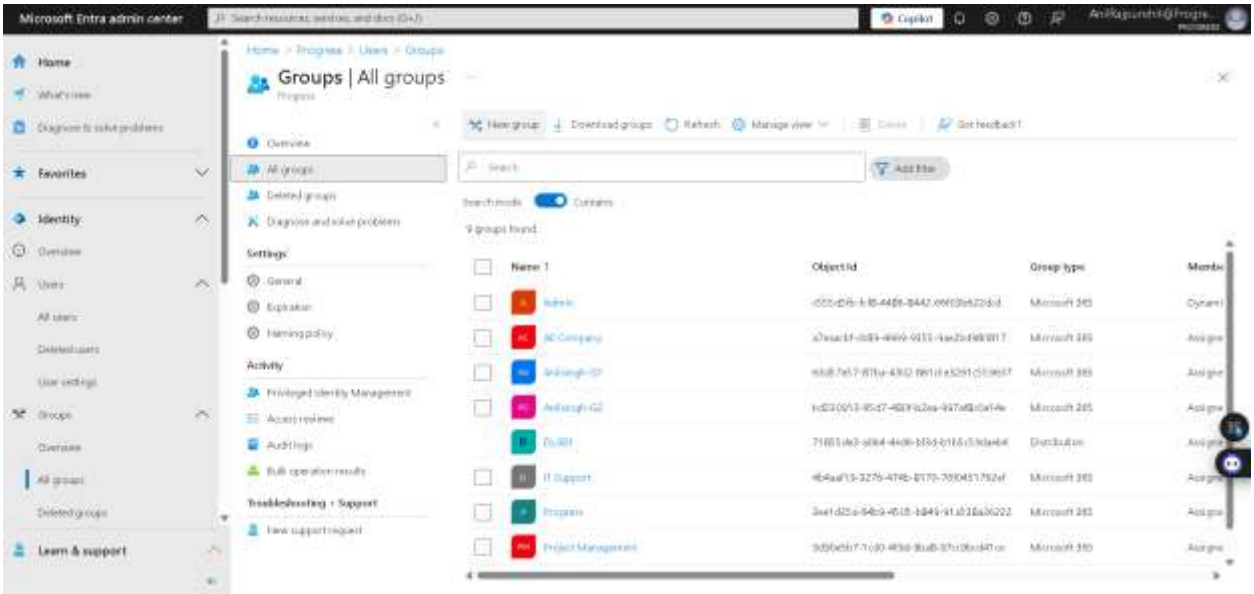


3. Create Office 365 Groups:

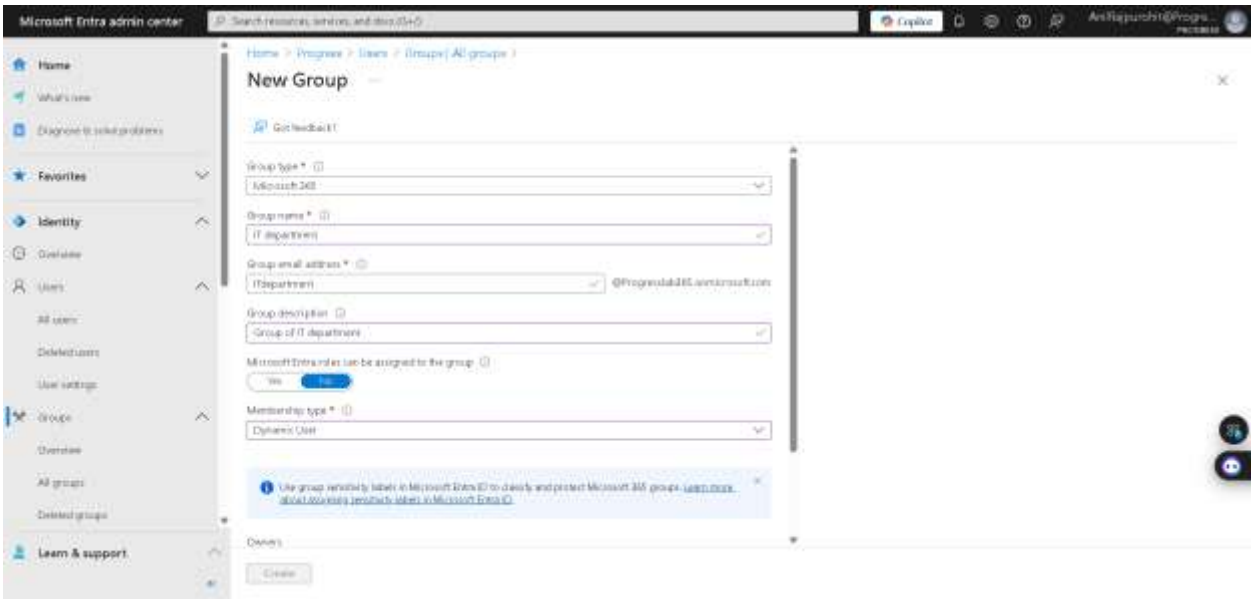
- Create three Office 365 groups for different departments: IT, HR, and Marketing.

IT department group creation

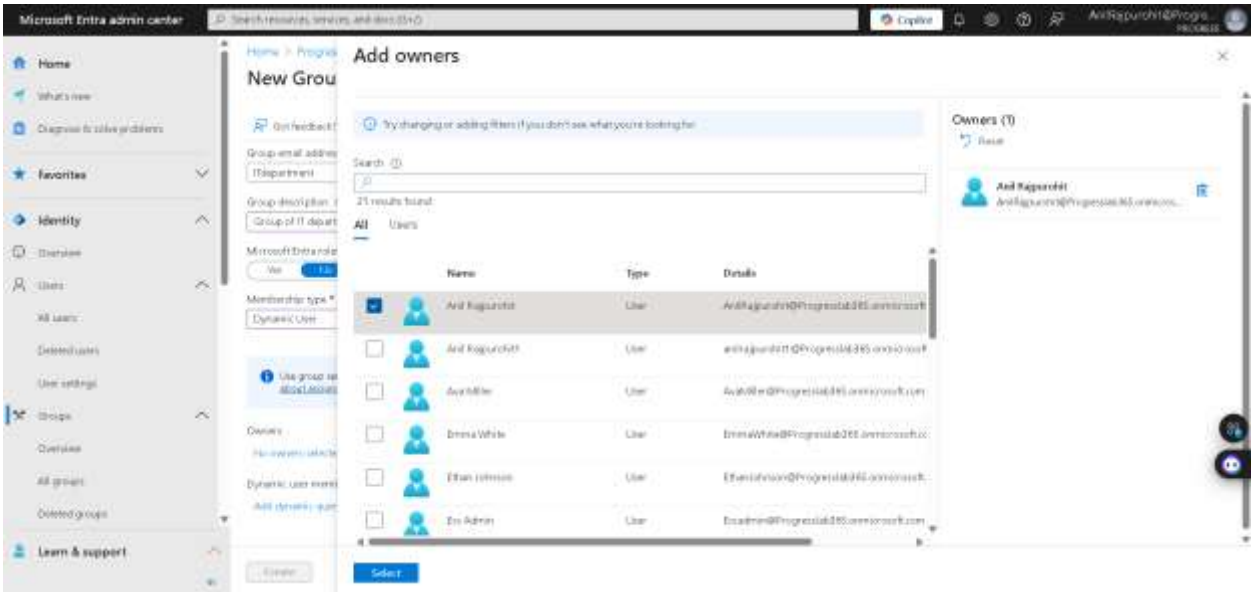
Step 1: From Entra admin center, go to identity -> Groups -> all groups -> new group.



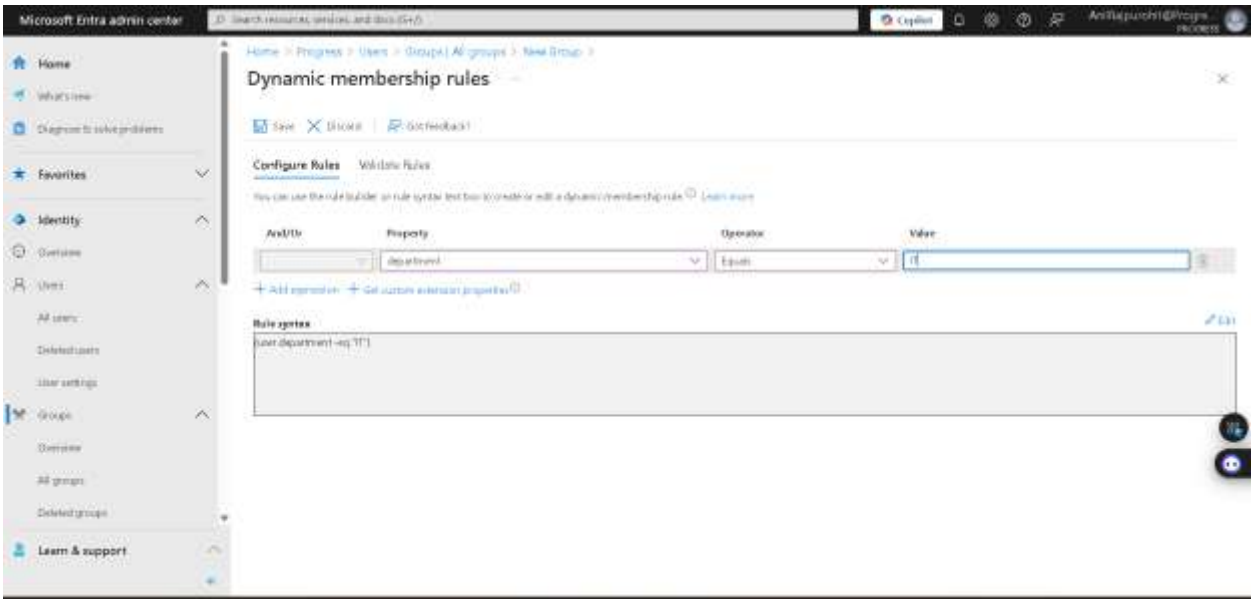
Step 2: Now fill all the details like Group type, name, email address, description, membership type. We selected membership types as dynamic as we want to add our users to their respected department group and we can do that by creating a dynamic group.



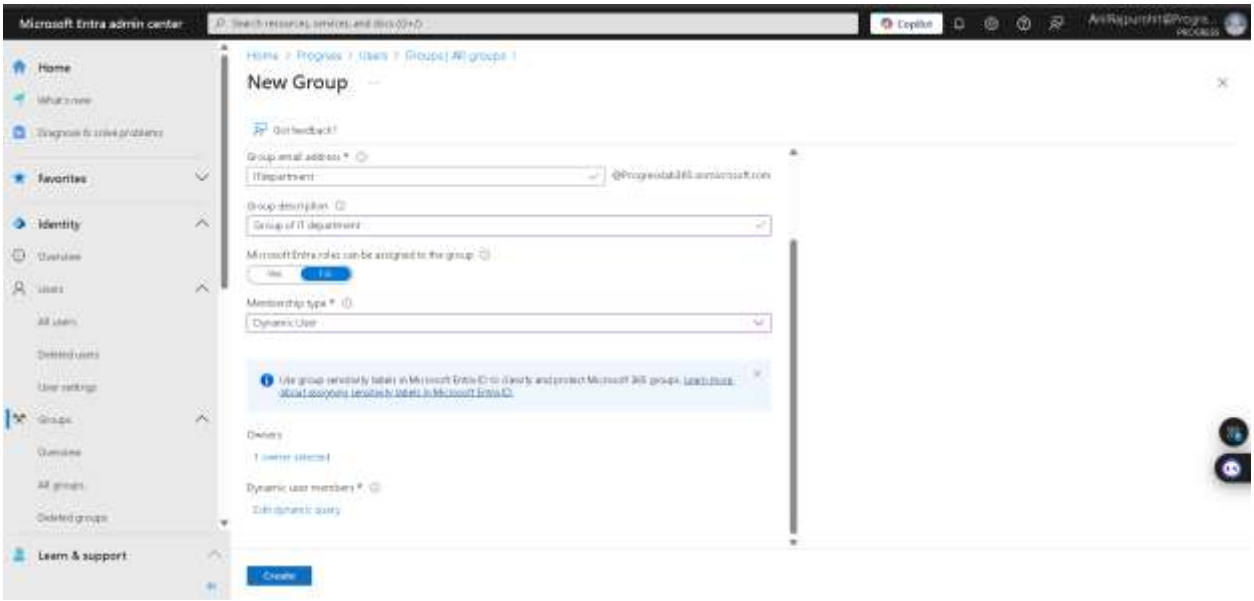
Step 3: Add global admin as group owners then click on select.



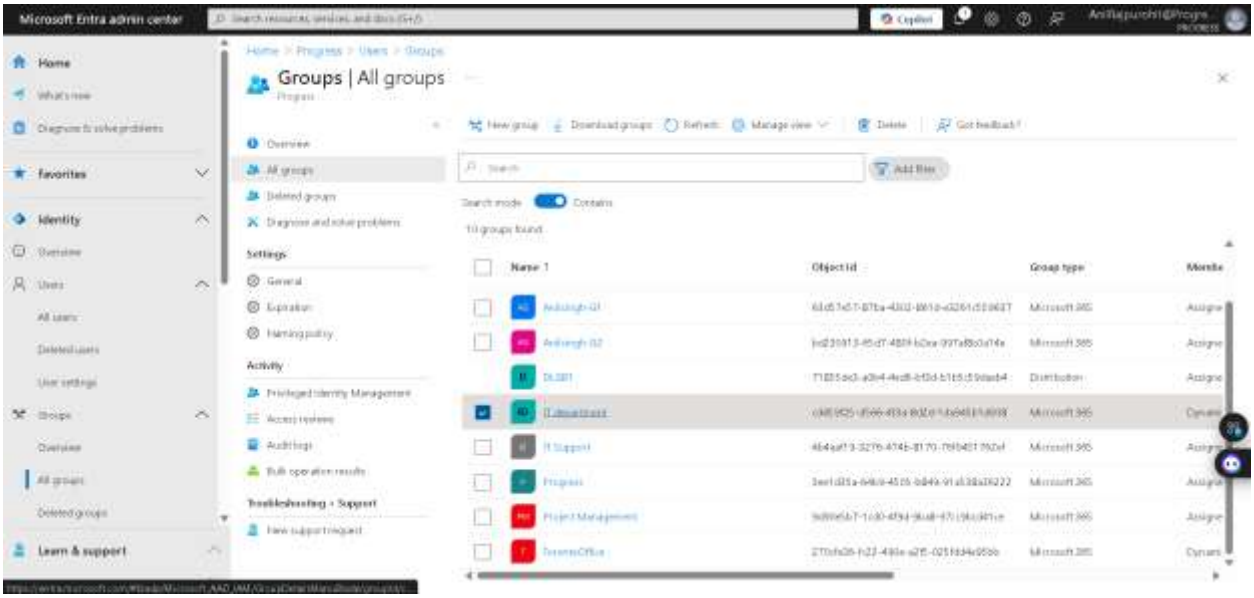
Step 4: Create a dynamic membership rule for automatically adding member by looking at their department value. Then click on Save.



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

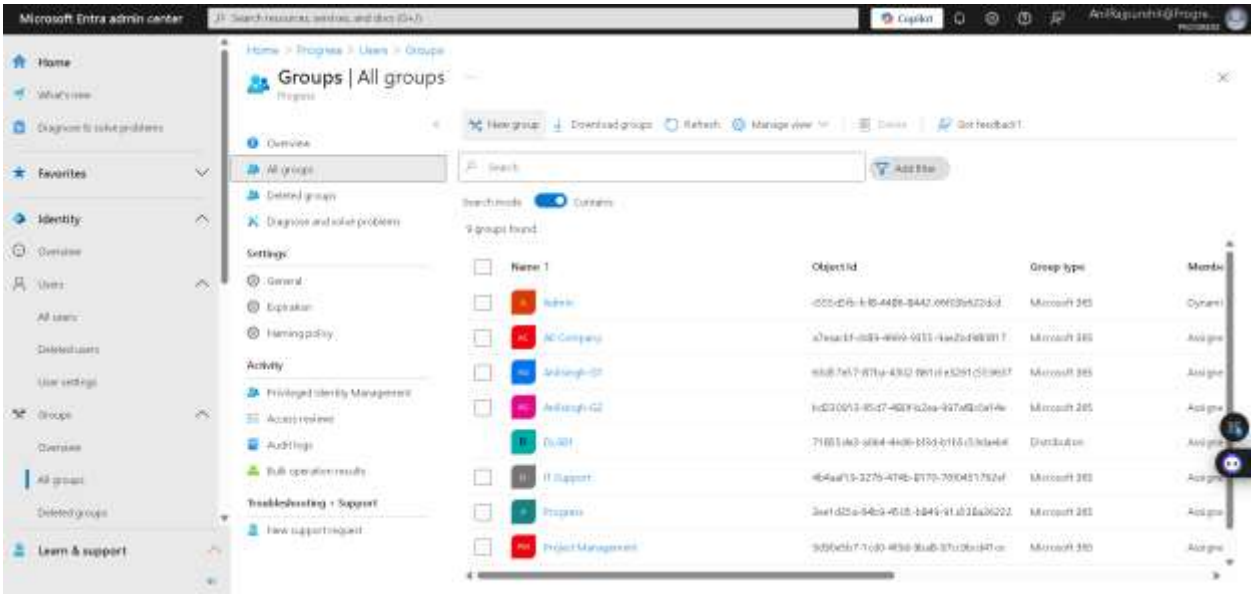


Step 6: Our group has been successfully created.

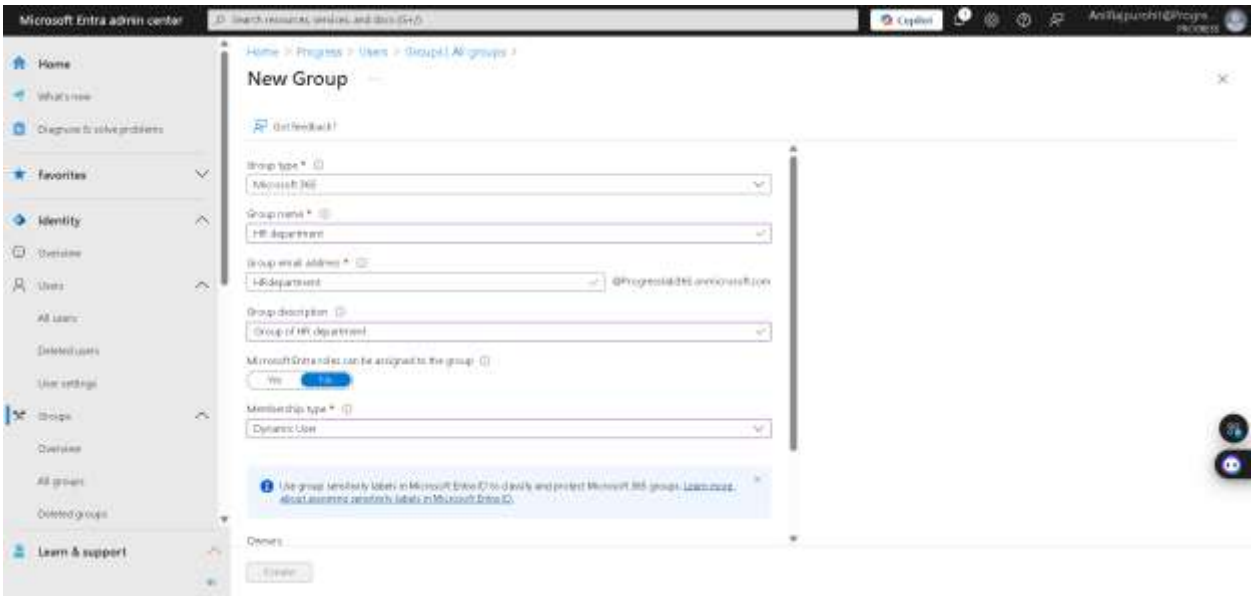


HR department group creation

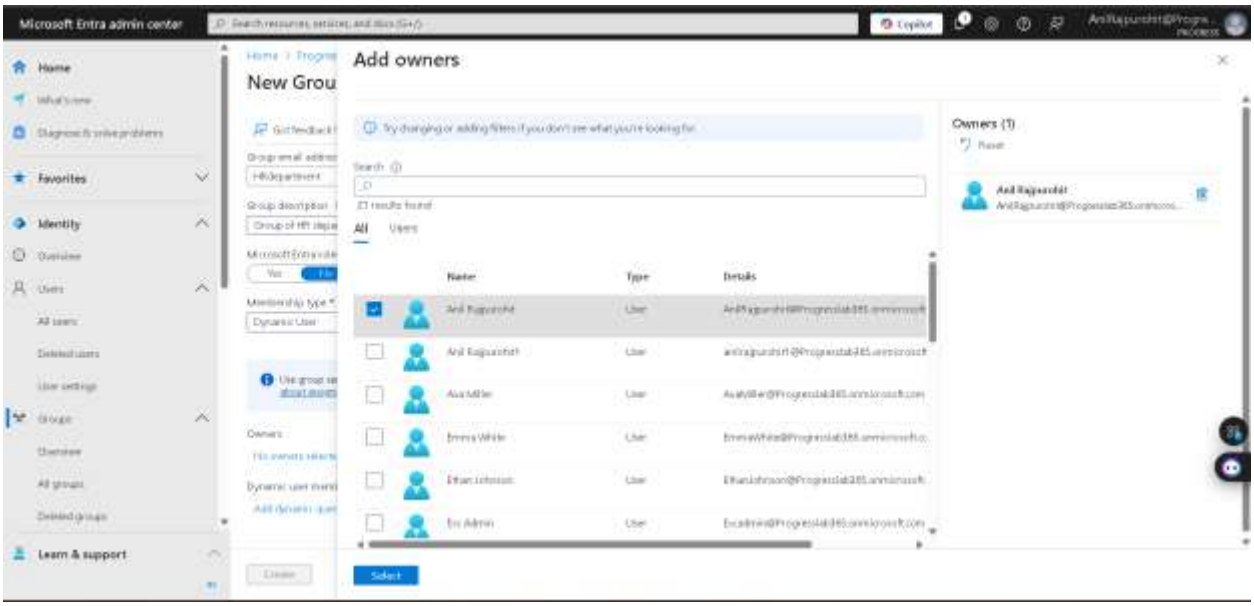
Step 1: From Entra admin center, go to identity -> Groups -> all groups -> new group.



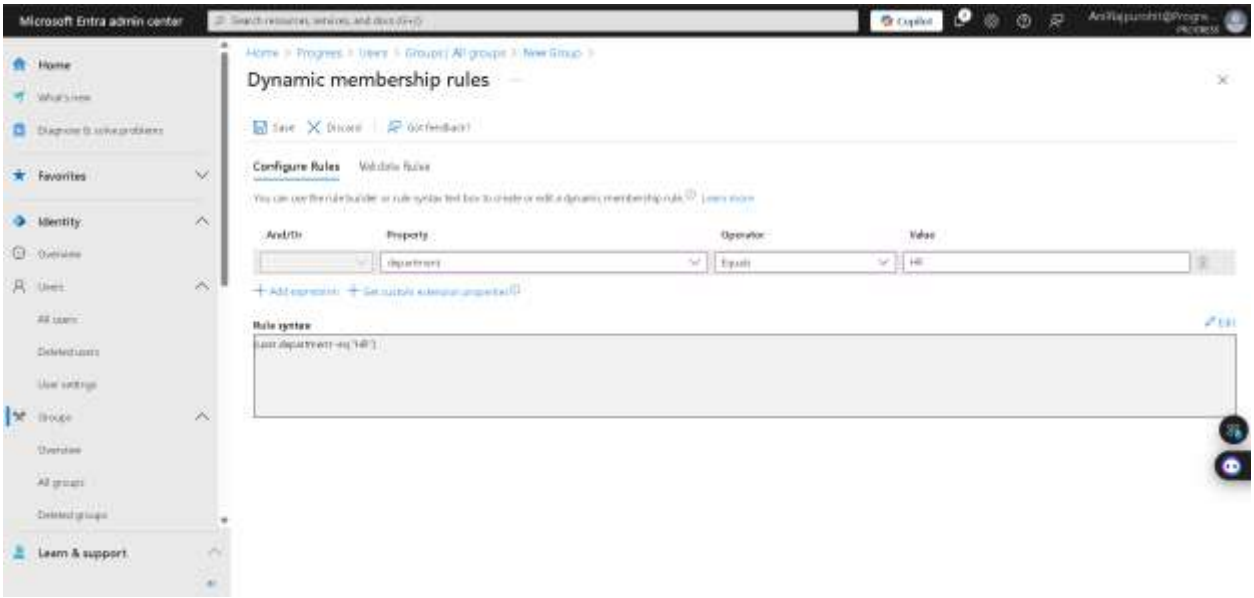
Step 2: Now fill all the details like Group type, name, email address, description, membership type. We selected membership types as dynamic as we want to add our users to their respected department group and we can do that by creating a dynamic group.



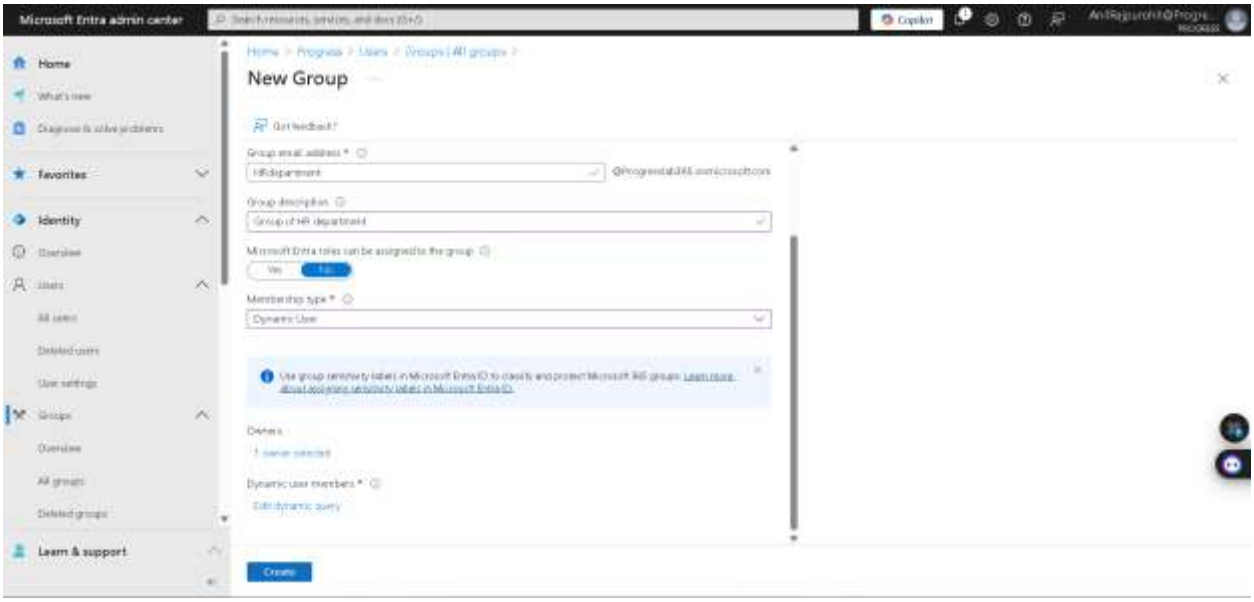
Step 3: Add global admin as group owners then click on select.



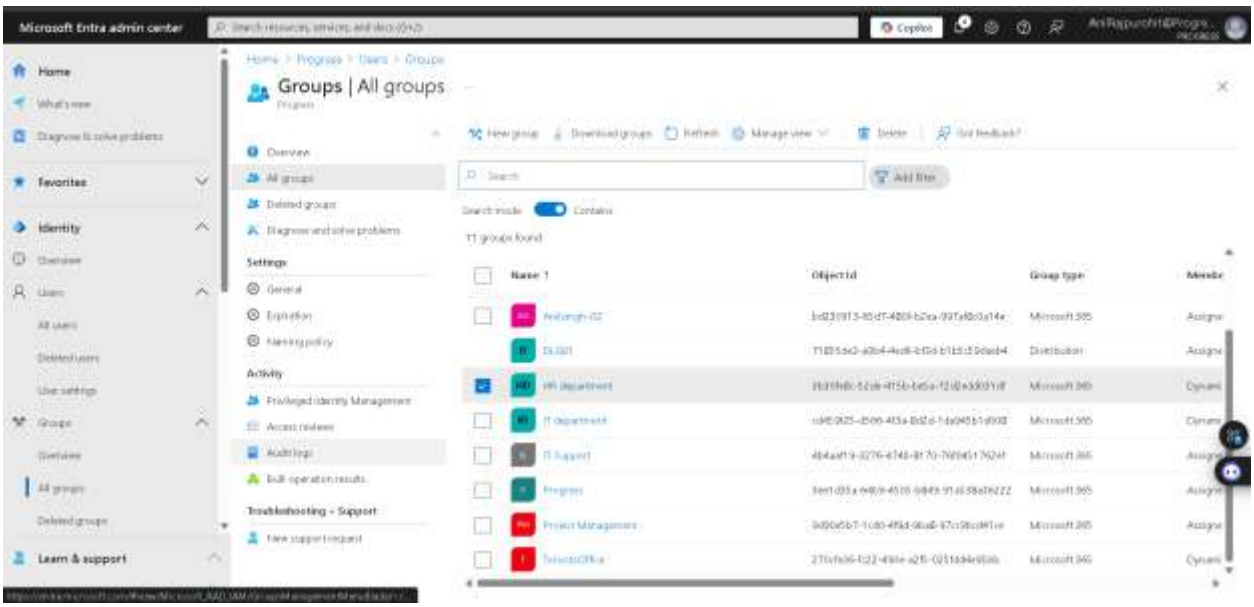
Step 4: Create a dynamic membership rule for automatically adding member by looking at their department value. Then click on Save.



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

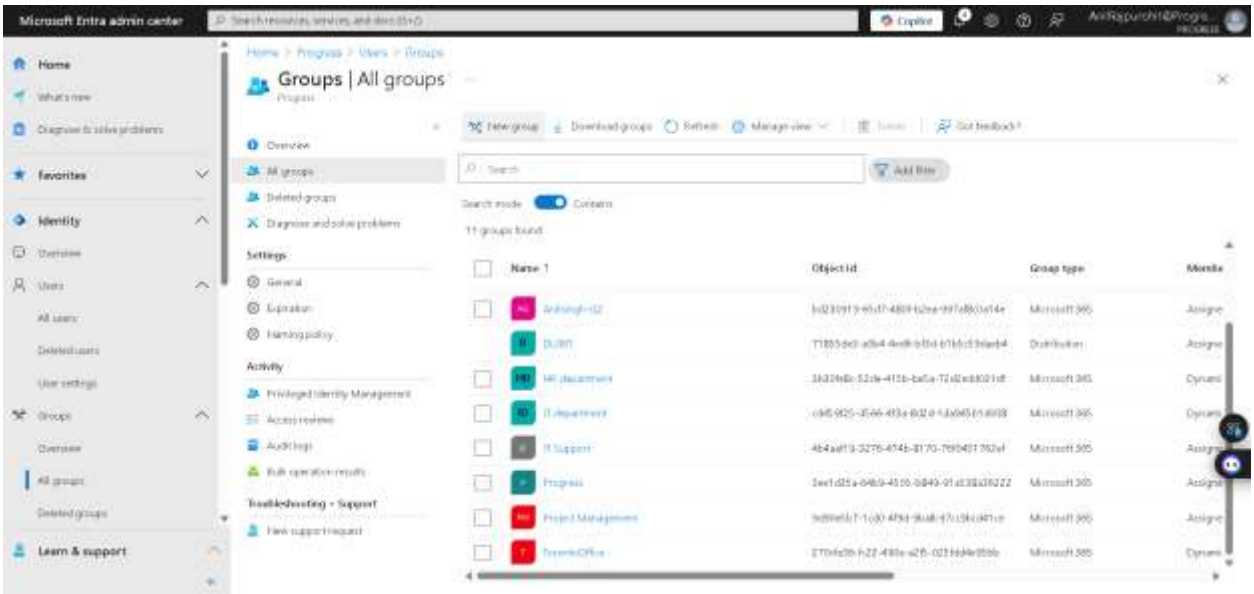


Step 6: Our group has been successfully created.

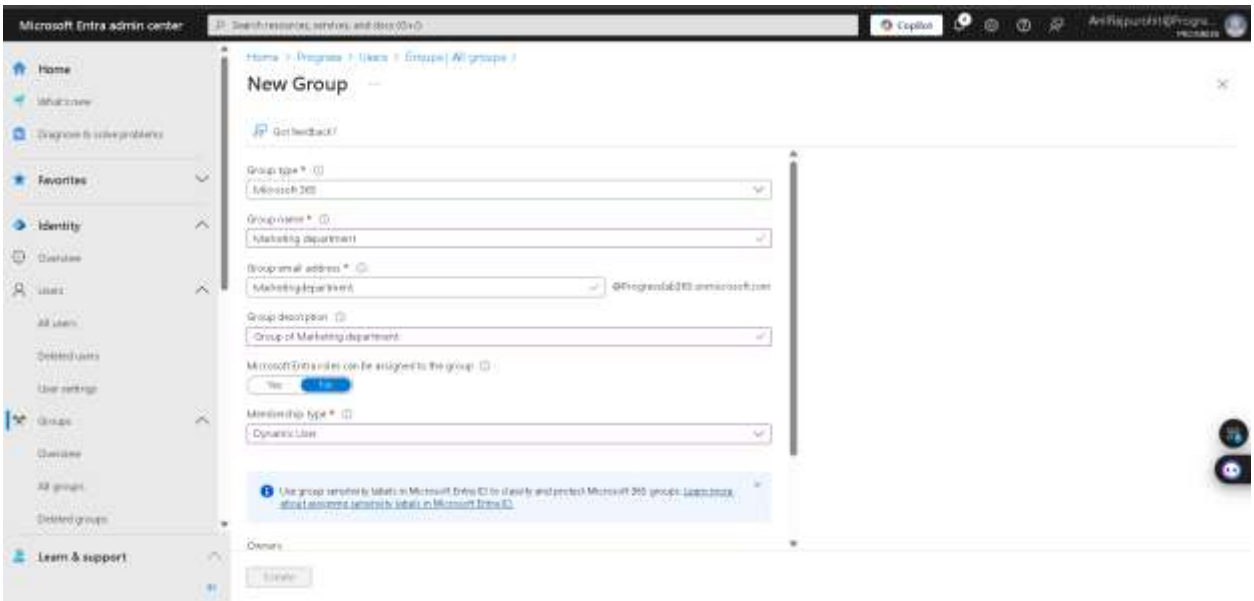


Marketing department group creation

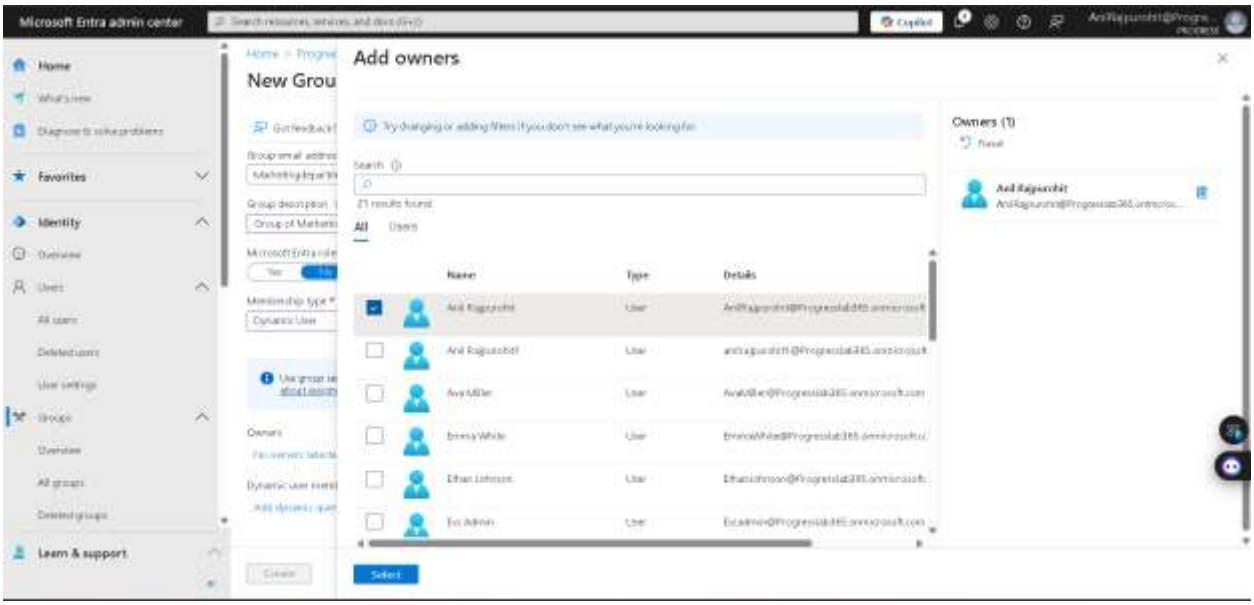
Step 1: From Entra admin center, go to identity -> Groups -> all groups -> new group.



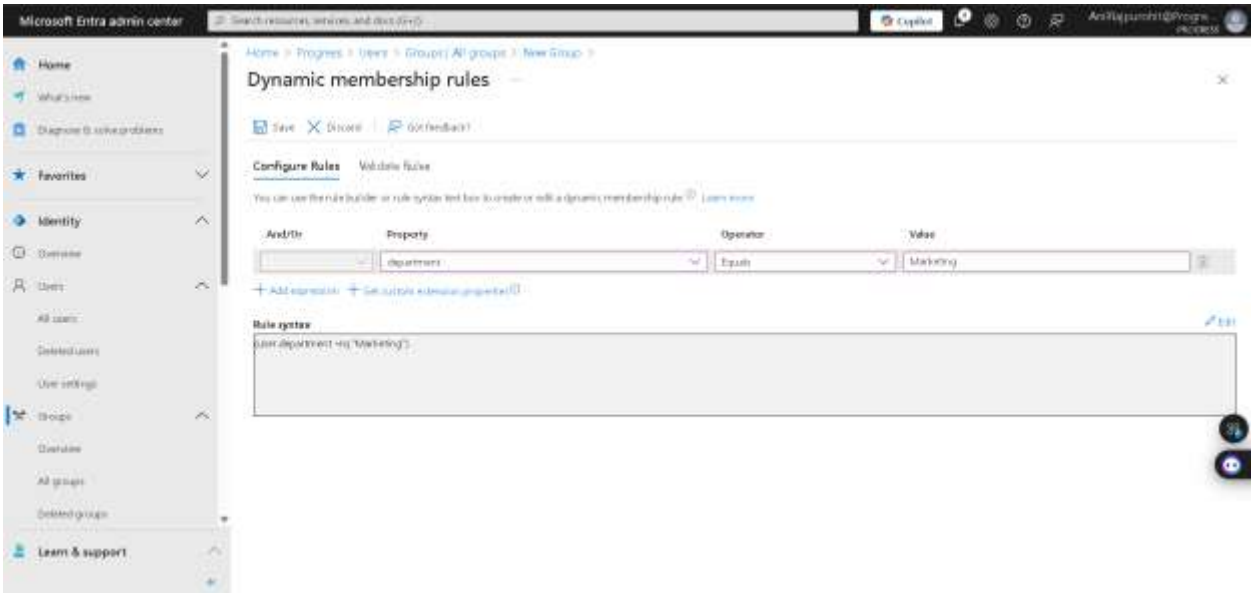
Step 2: Now fill all the details like Group type, name, email address, description, membership type. We selected membership types as dynamic as we want to add our users to their respected department group and we can do that by creating a dynamic group.



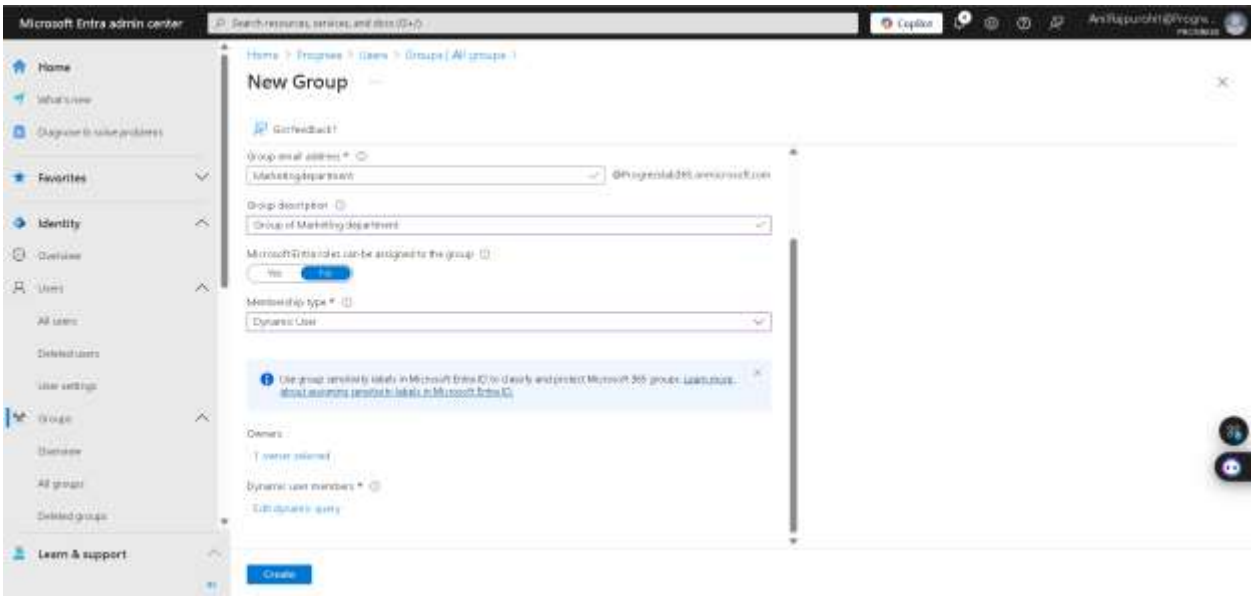
Step 3: Add global admin as group owners then click on select.



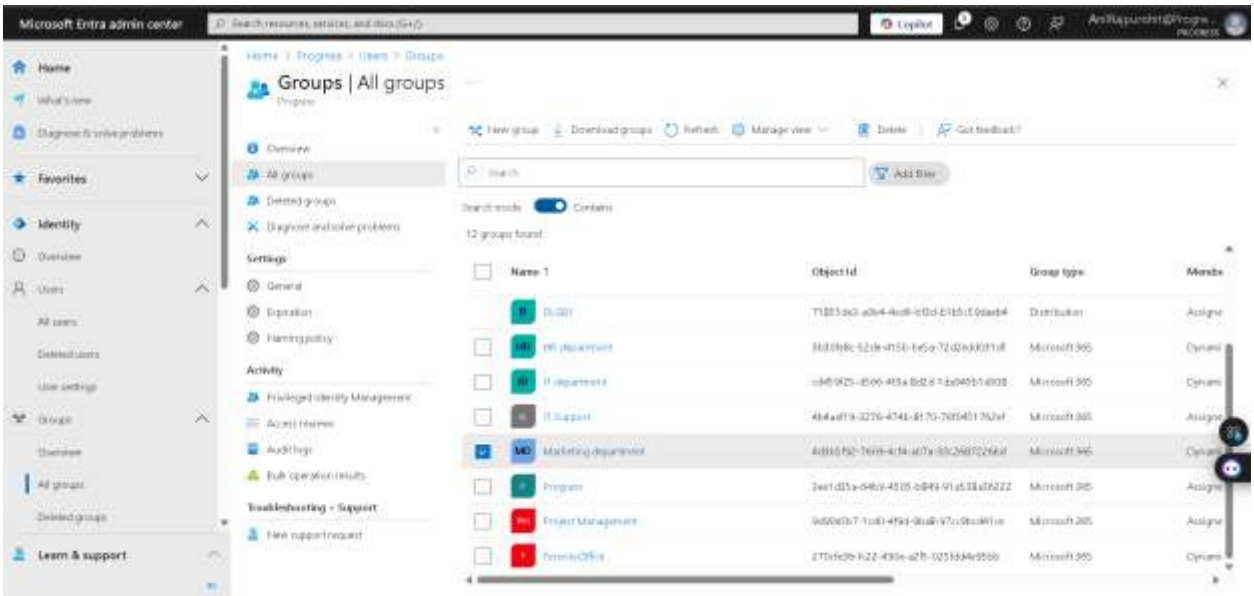
Step 4: Create a dynamic membership rule for automatically adding member by looking at their department value. Then click on Save.



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



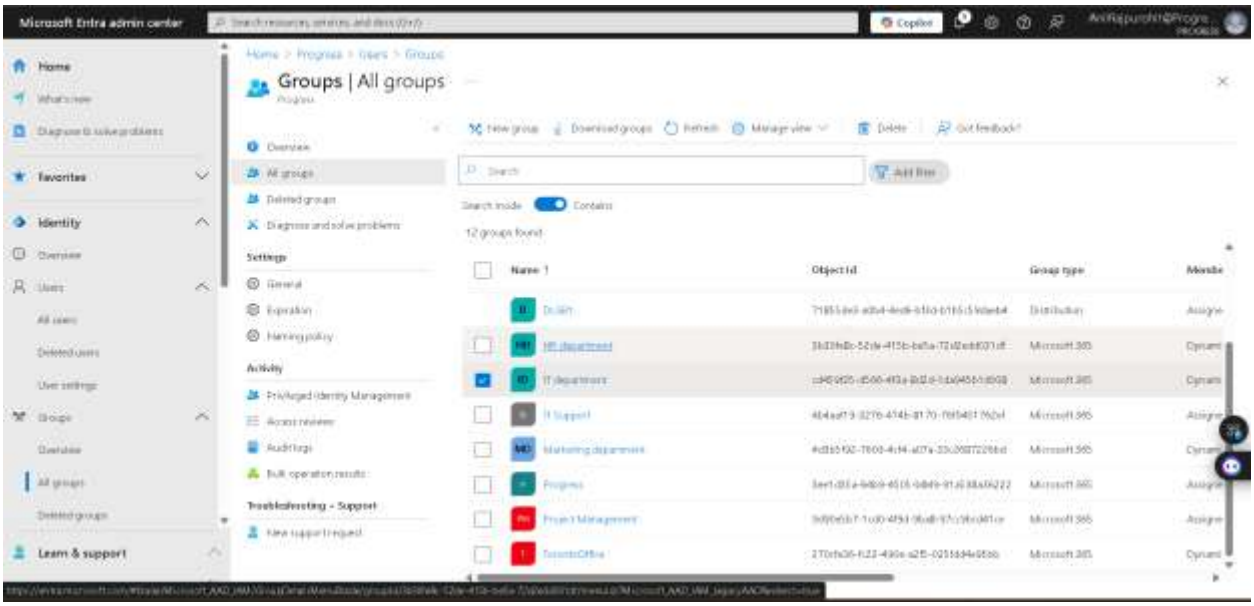
Step 6: Our group has been successfully created.



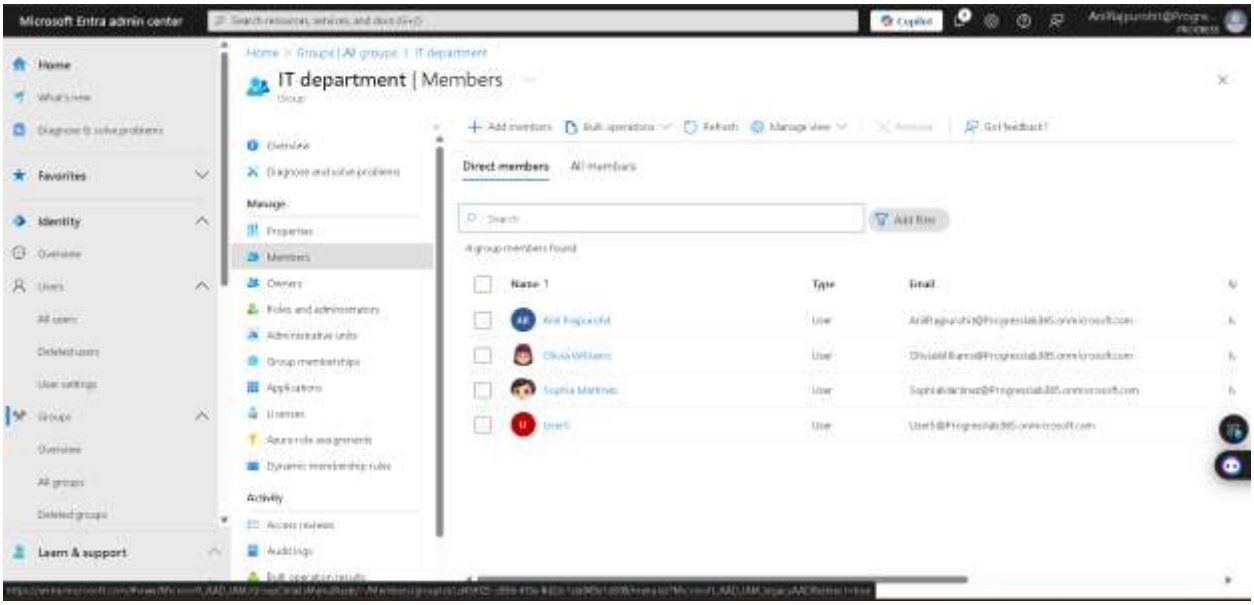
- Add users to their respective groups.

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.

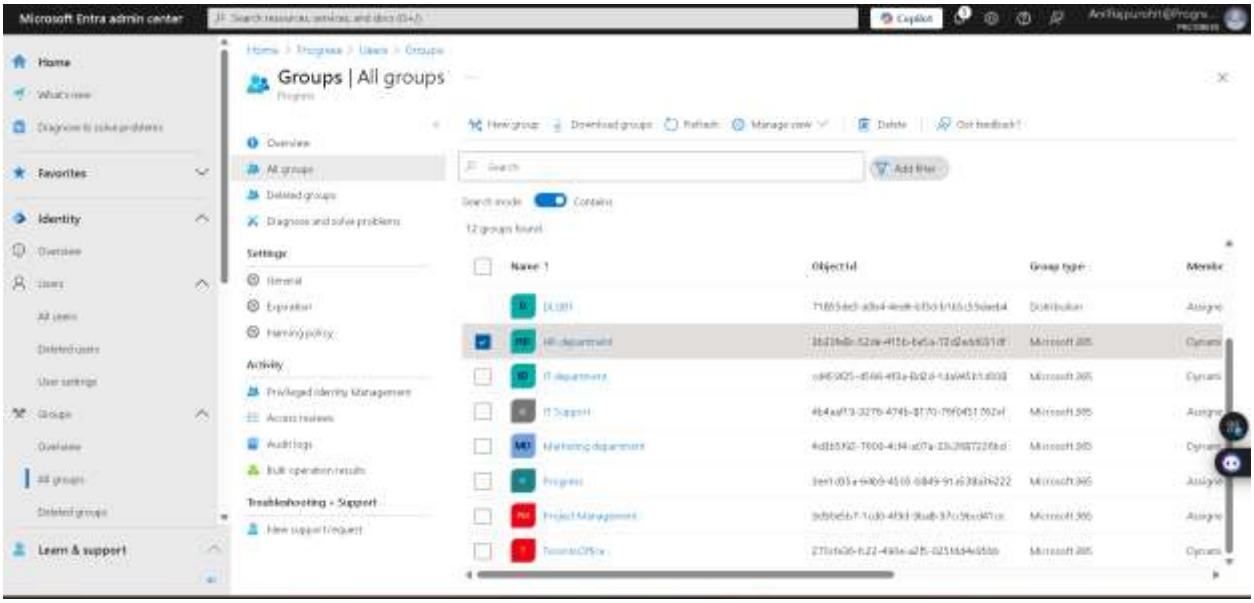


Step 2: In IT department group, under members we can see all the users got updated automatically based on their department.

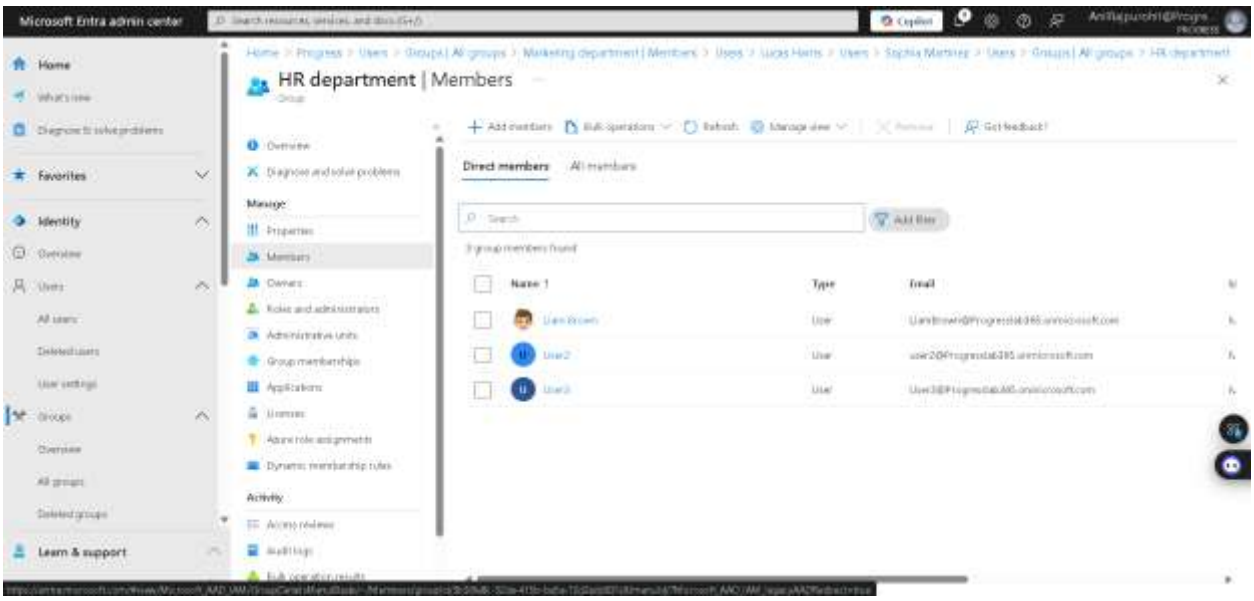


For HR department group

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.

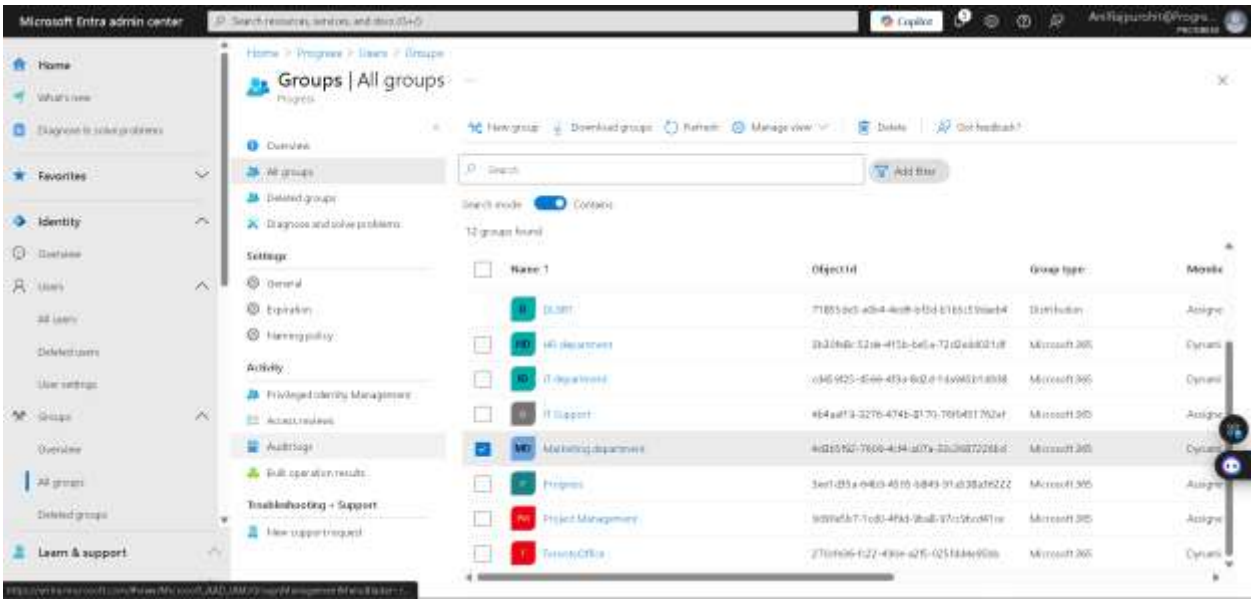


Step 2: In HR department group, under members we can see all the users got updated automatically based on their department.

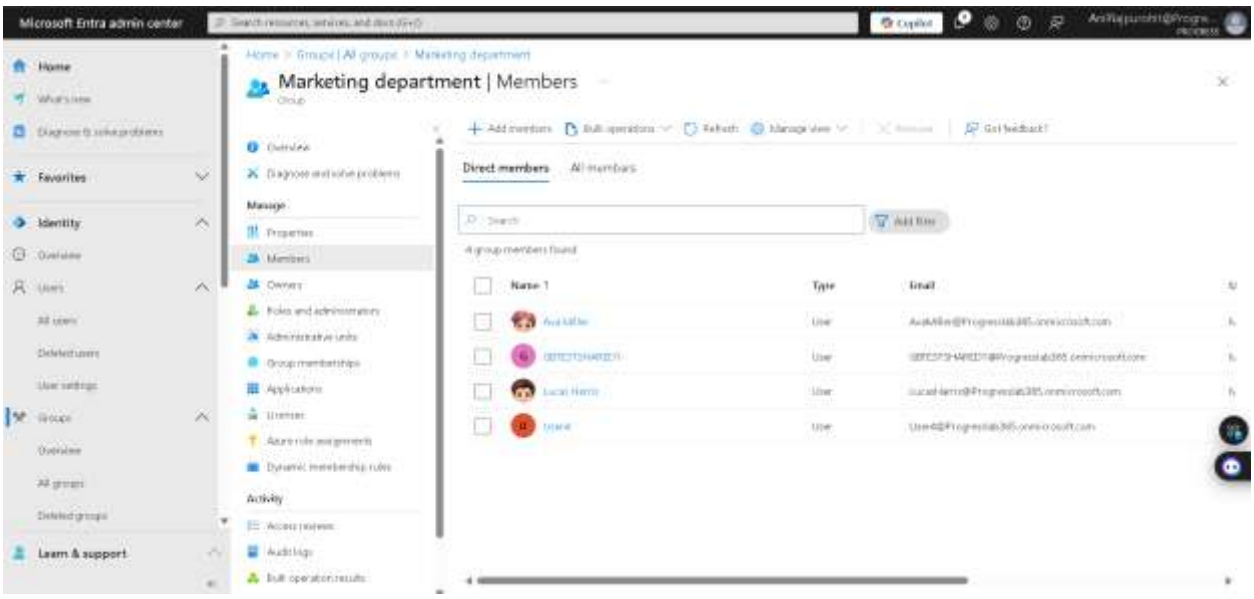


For Marketing department group

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.



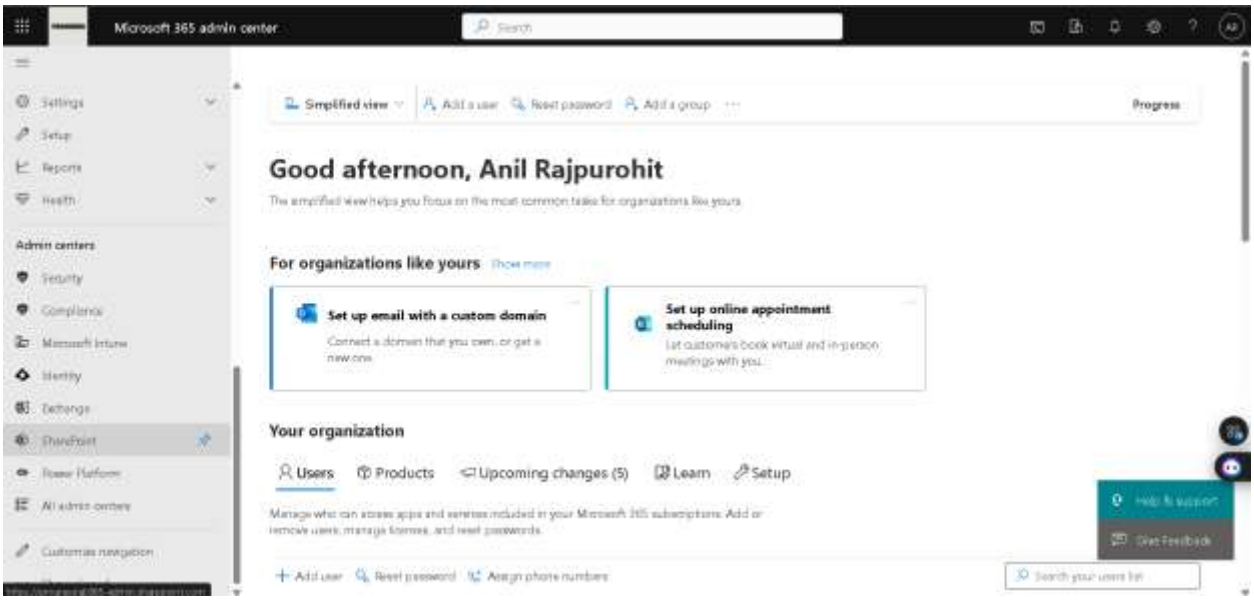
Step 2: In Marketing department group, under members we can see all the users got updated automatically based on their department.



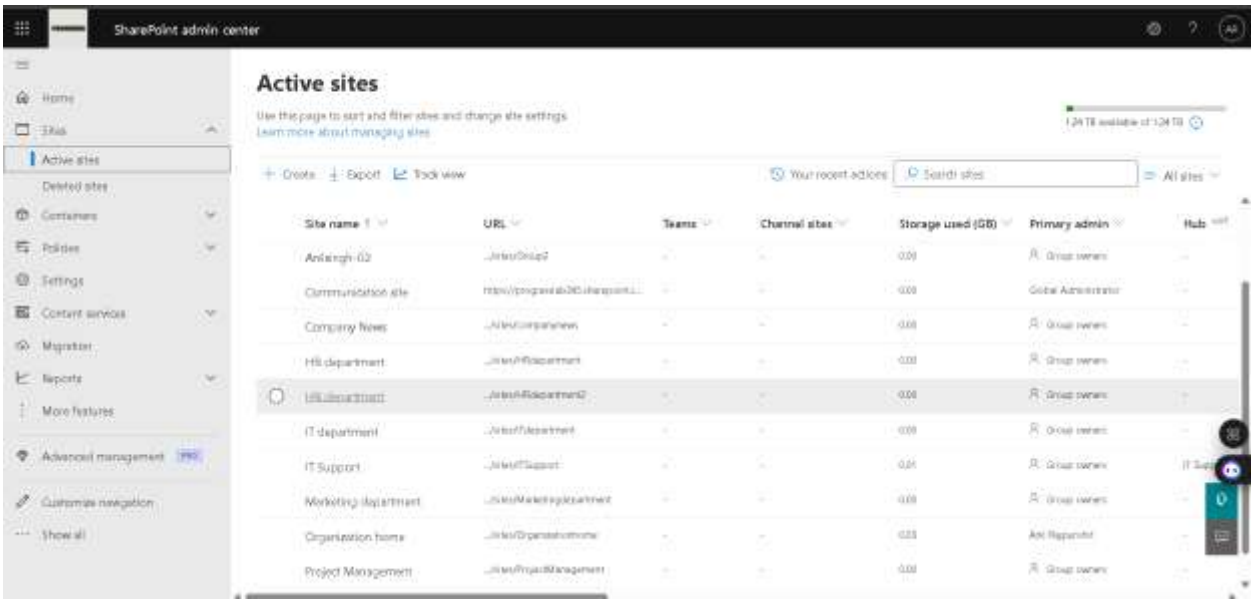
4. Configure User Permissions:

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

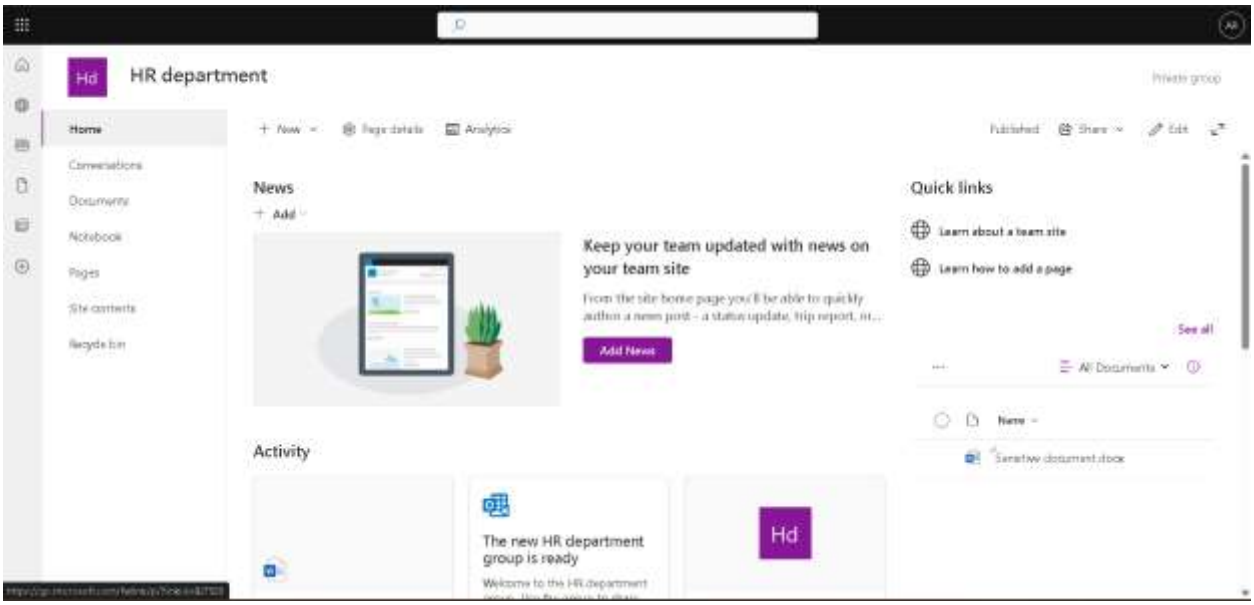
Step 1: To assign HR group access to sensitive HR document in SharePoint, from Microsoft 365 admin center under admin centers -> SharePoint.



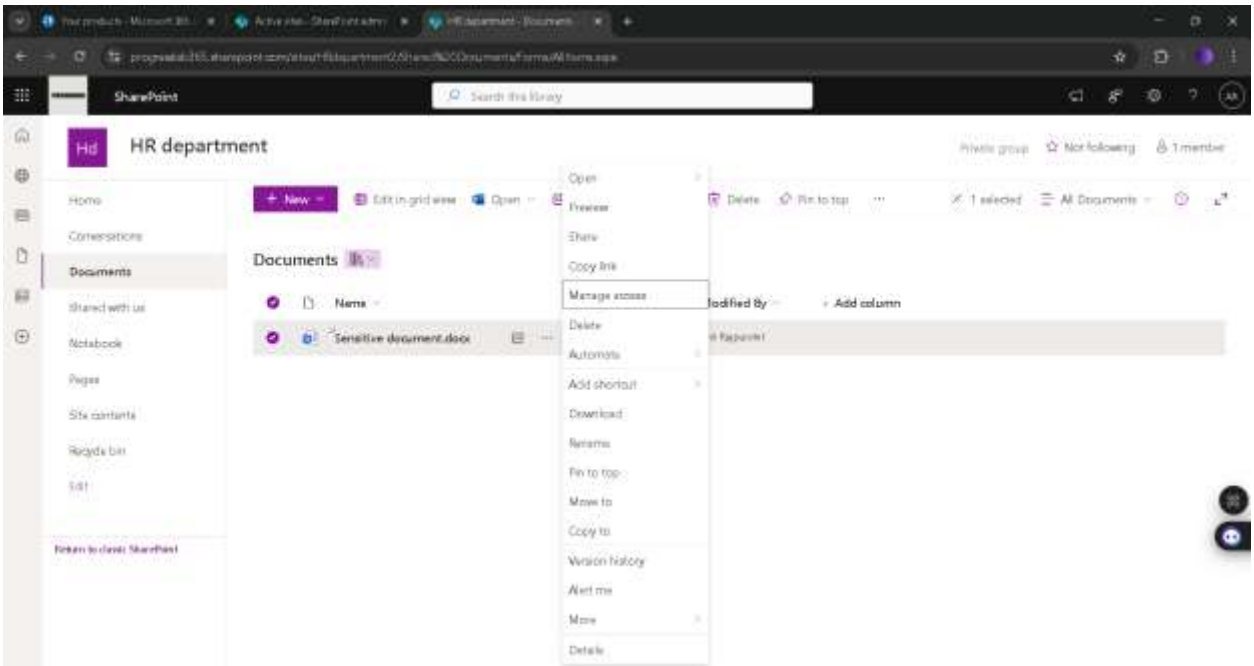
Step 2: From SharePoint admin center, sites -> active sites -> HR department.



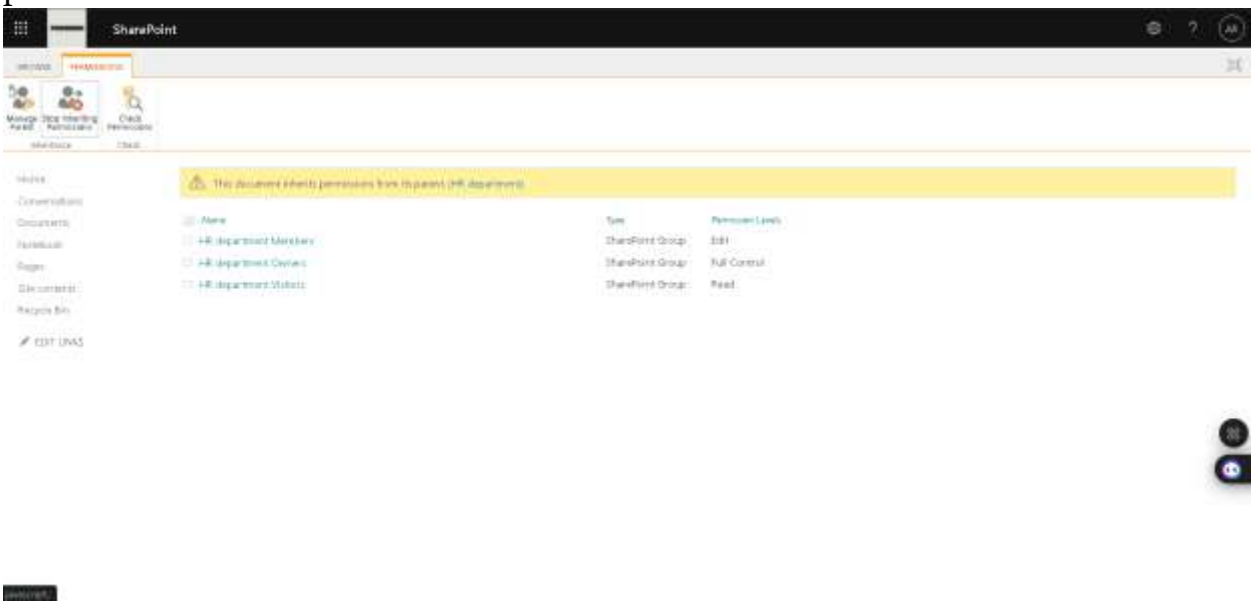
Step 3: To manage the sensitive document, click on Documents.



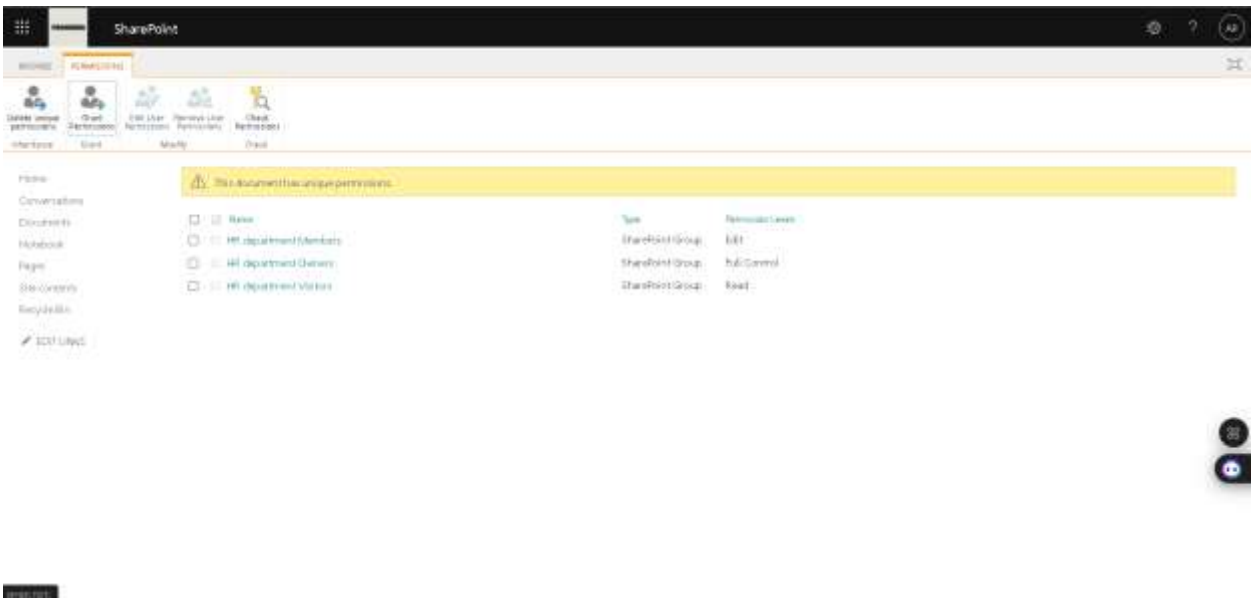
Step 4: In documents, select the respective sensitive HR file then click on three dots besides it. Then select manage access.



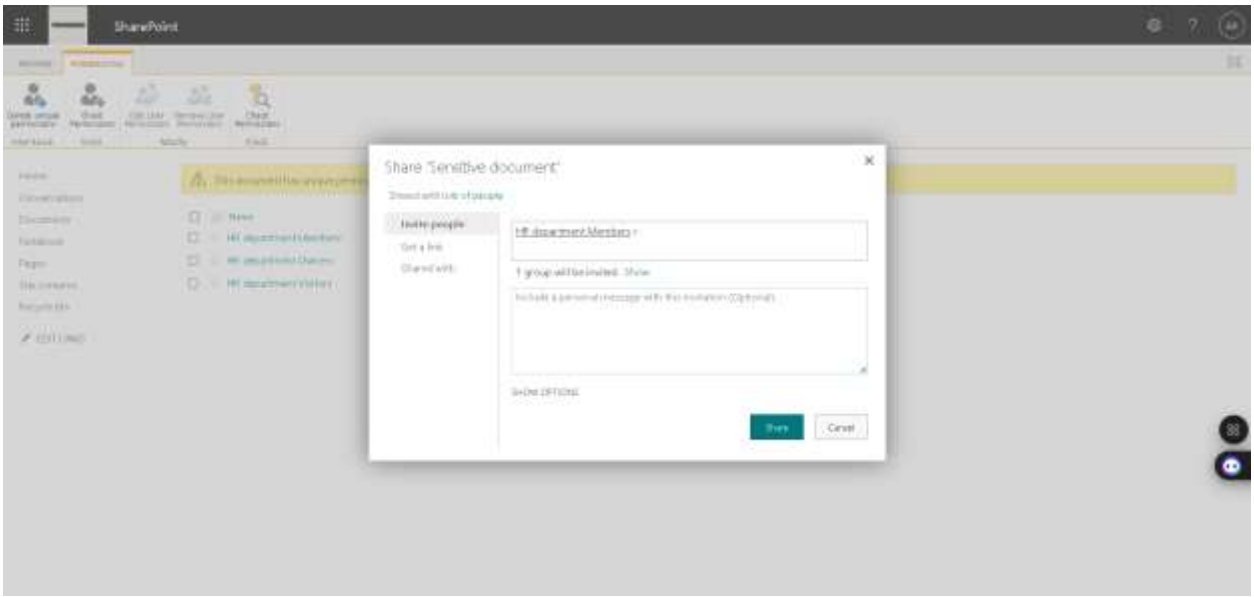
Step 5: First, click on stop inheriting permissions, so that we can add custom permissions to this file.



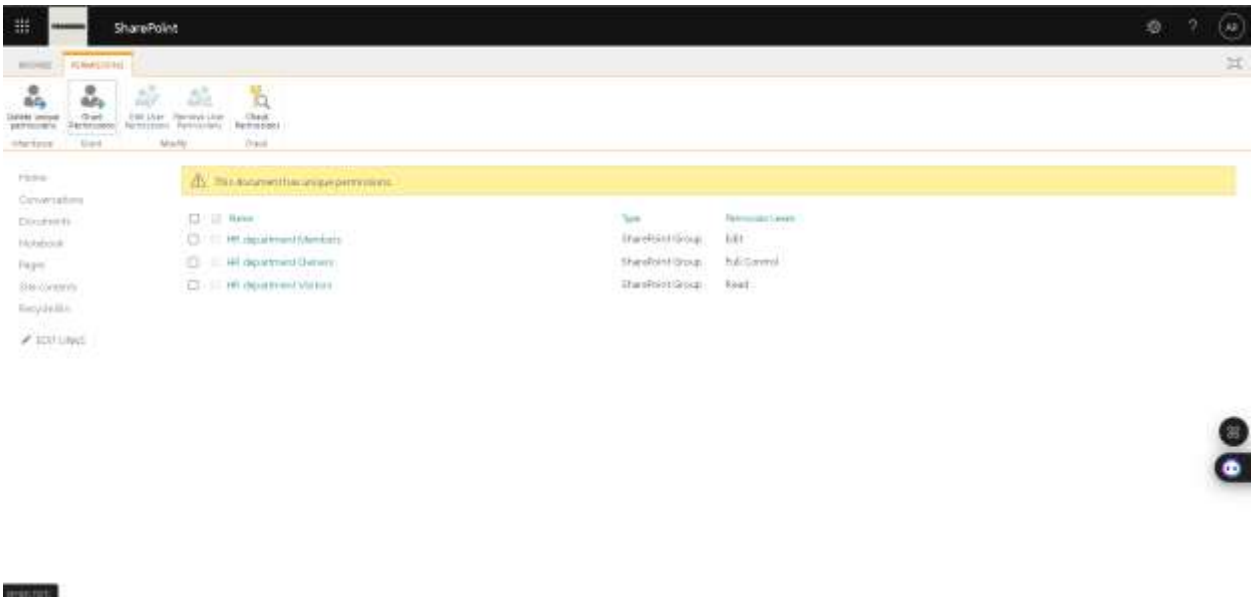
Step 6: Click on grant access to edit the permission of the file.



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.

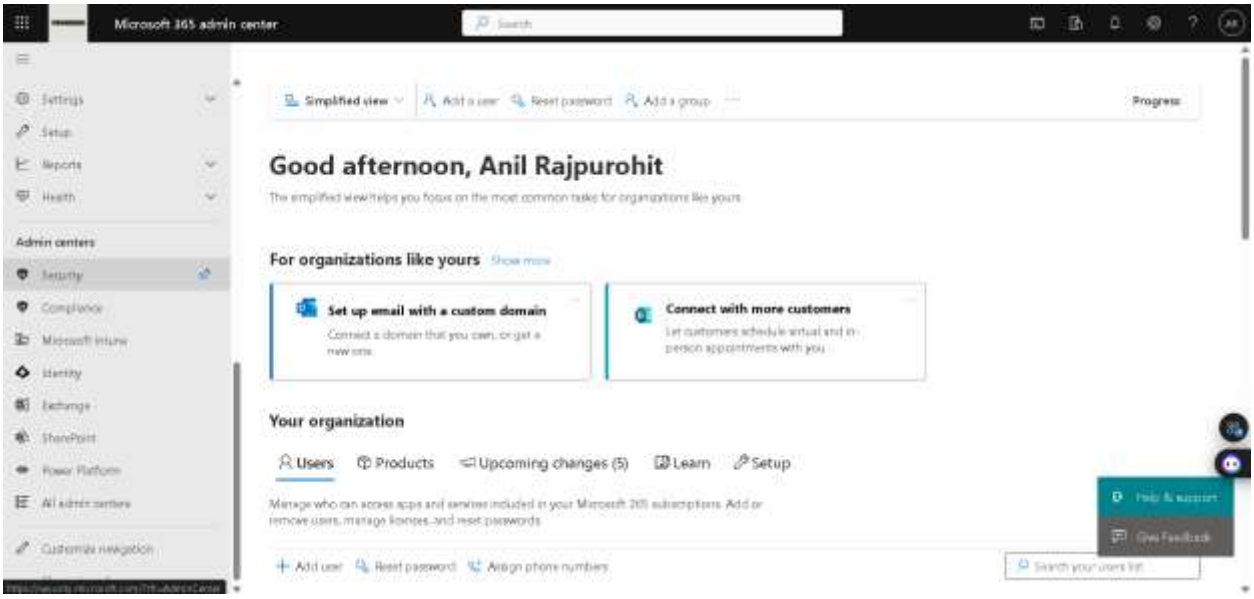
In SharePoint, for files and documents we can stop inheriting permissions, so that we can add custom permissions to that file.(If that file or directory is sensitive)

Task 2: Implementing Security Measures

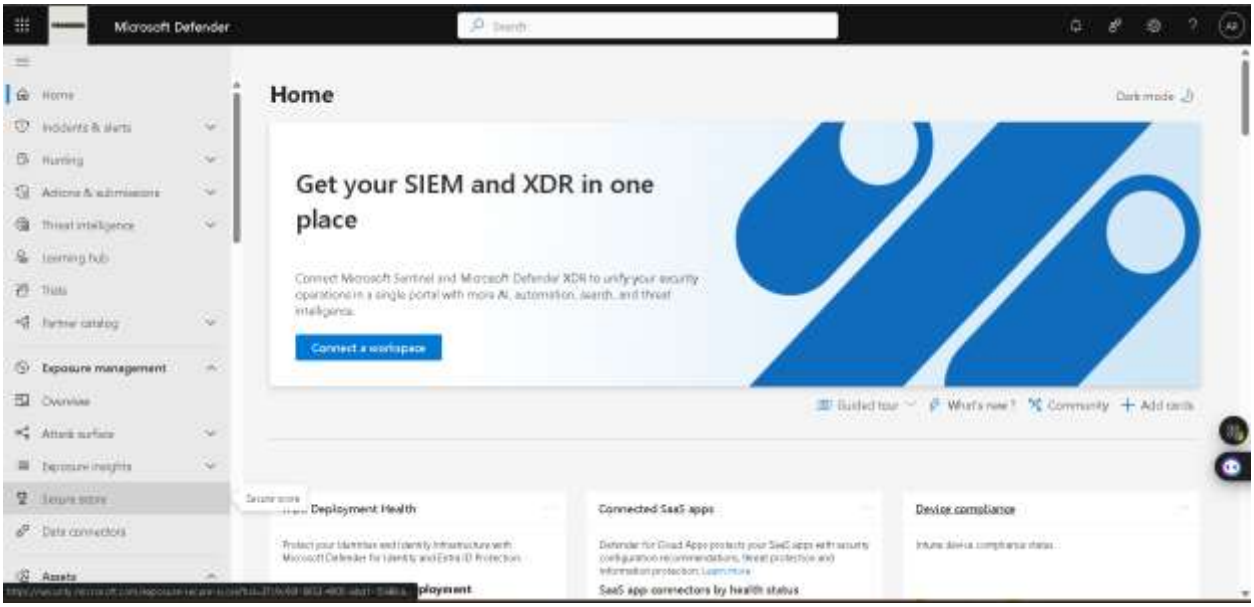
1. Set Up and Configure Microsoft Defender for Office 365:

- Access the MS Defender and navigate to Secure Score.

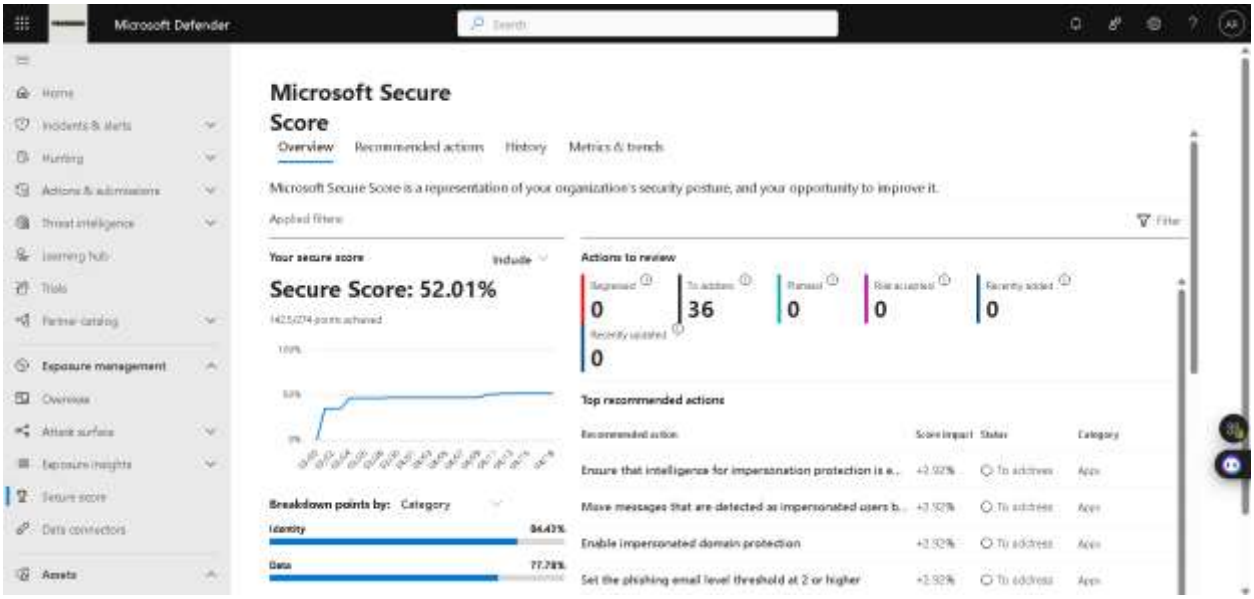
Step 1: First, from Microsoft 365 admin center under admin centers -> Security to access Microsoft defender.



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

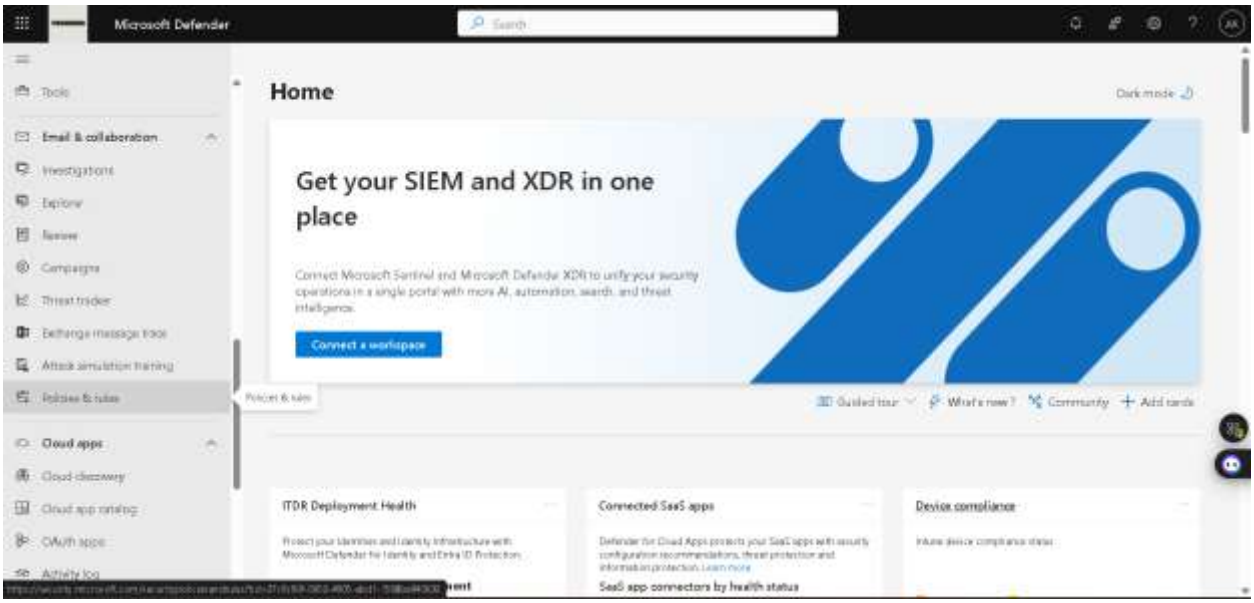


Step 3: We can view secure score for our organization here, our organization secure score currently only at 52.01% and healthy secure score is generally above 80%. We can complete recommended actions to increase our score.

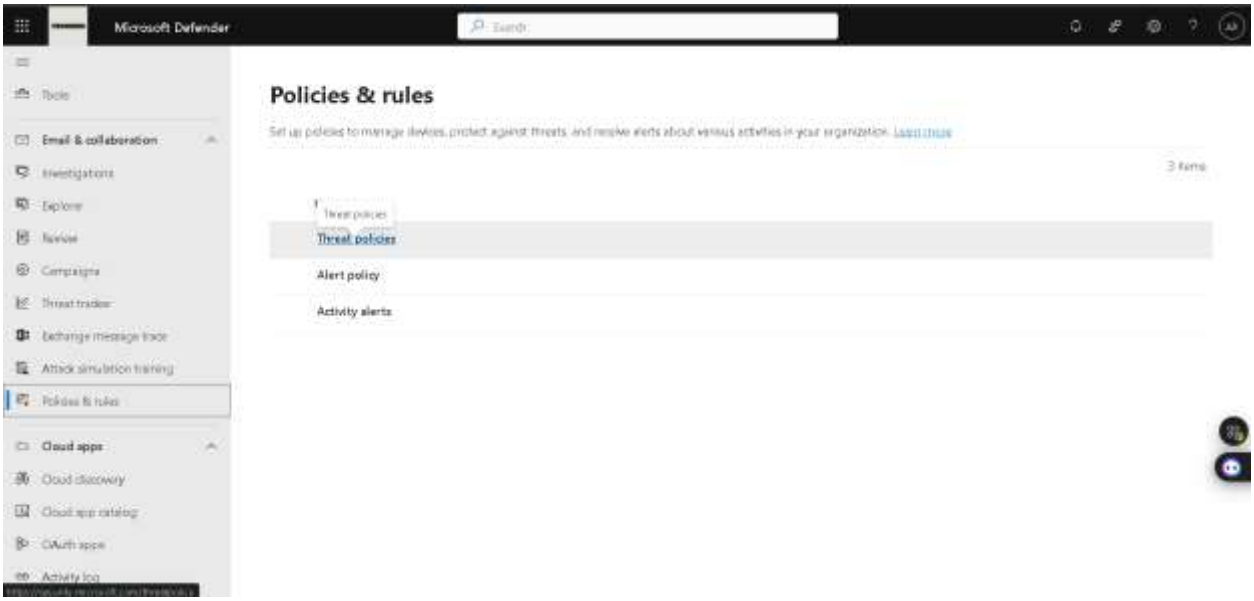


- Ensure that Safe Links and Safe Attachments have been enabled for all users.

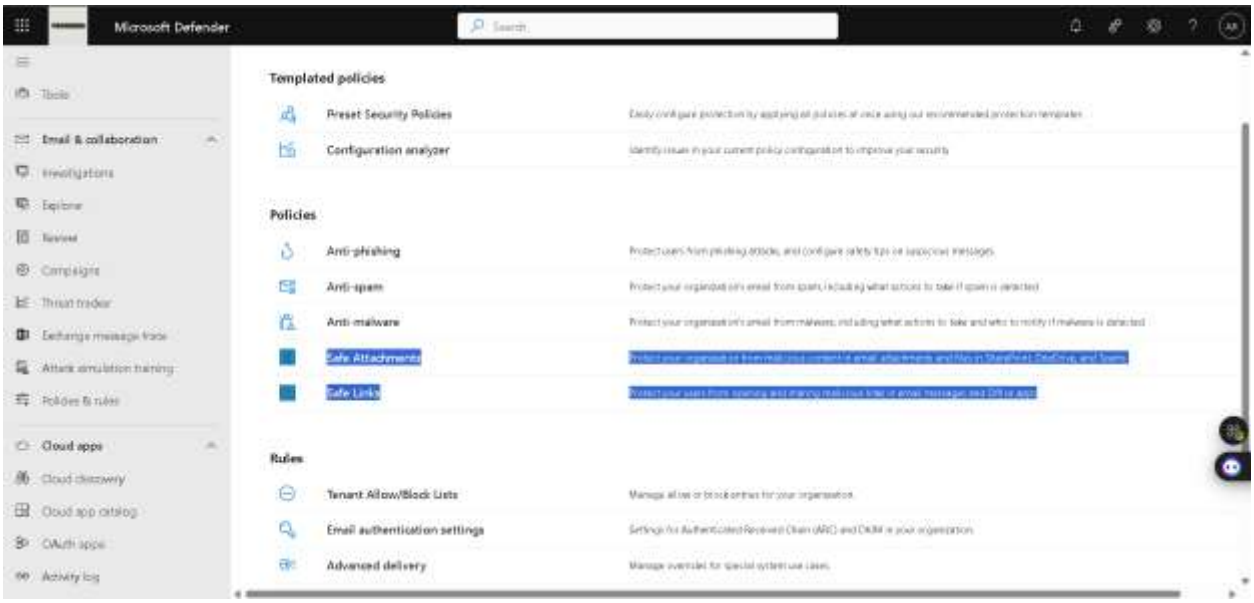
Step 1: From Microsoft Defender, under email & collaboration click on Policies & rules.



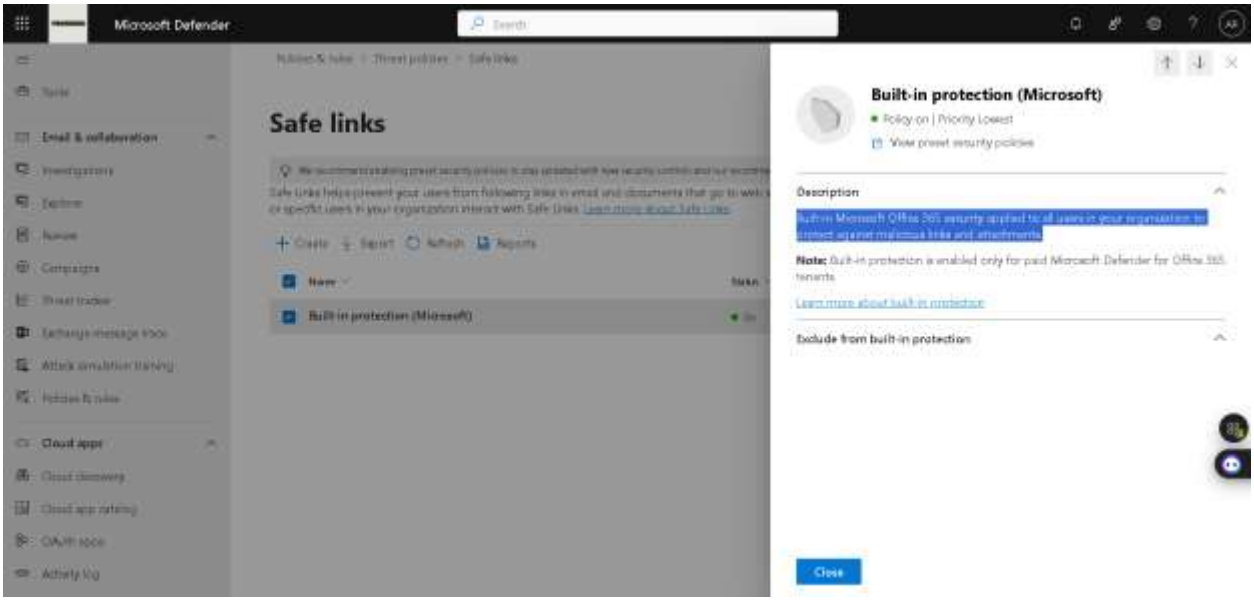
Step 2: Now, select Threat Policies.



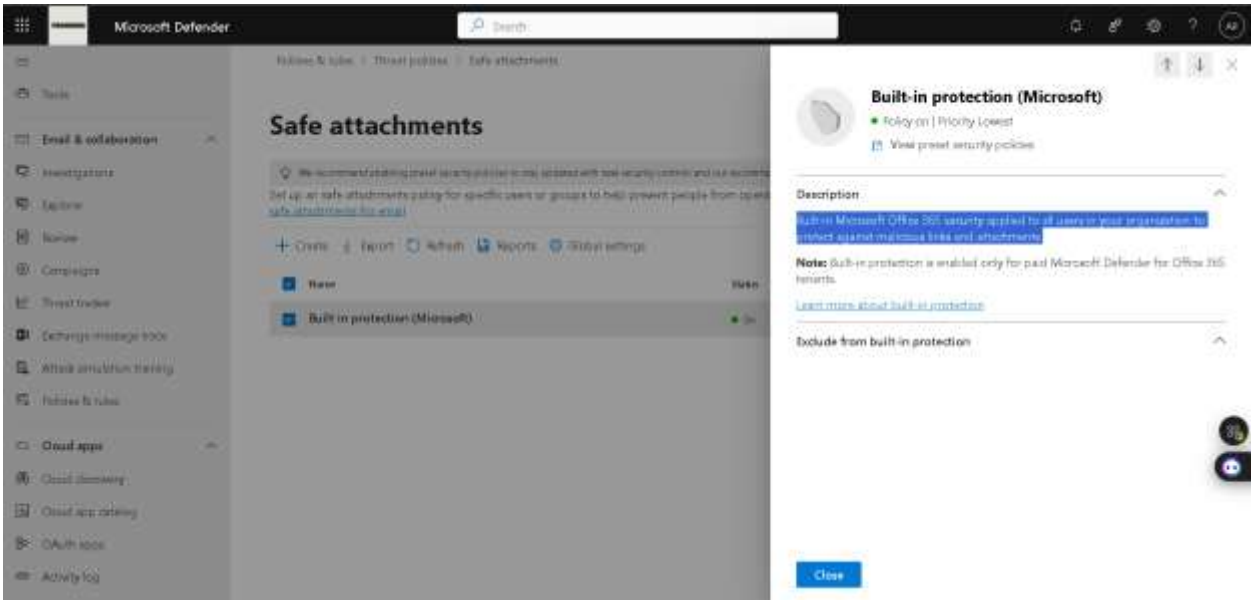
Step 3: We can see that for our organization both Safe attachments and safe links polices are active.



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

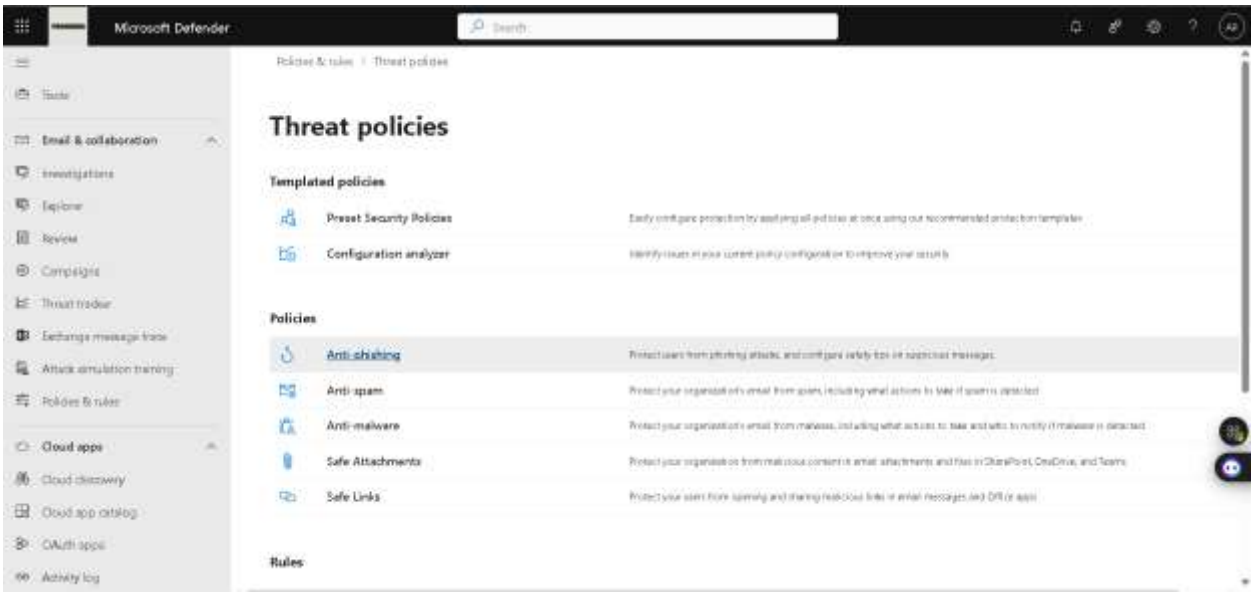


Step 5: To check detailed info of safe attachments policy, click in attachments then built-in protection to view detailed info.

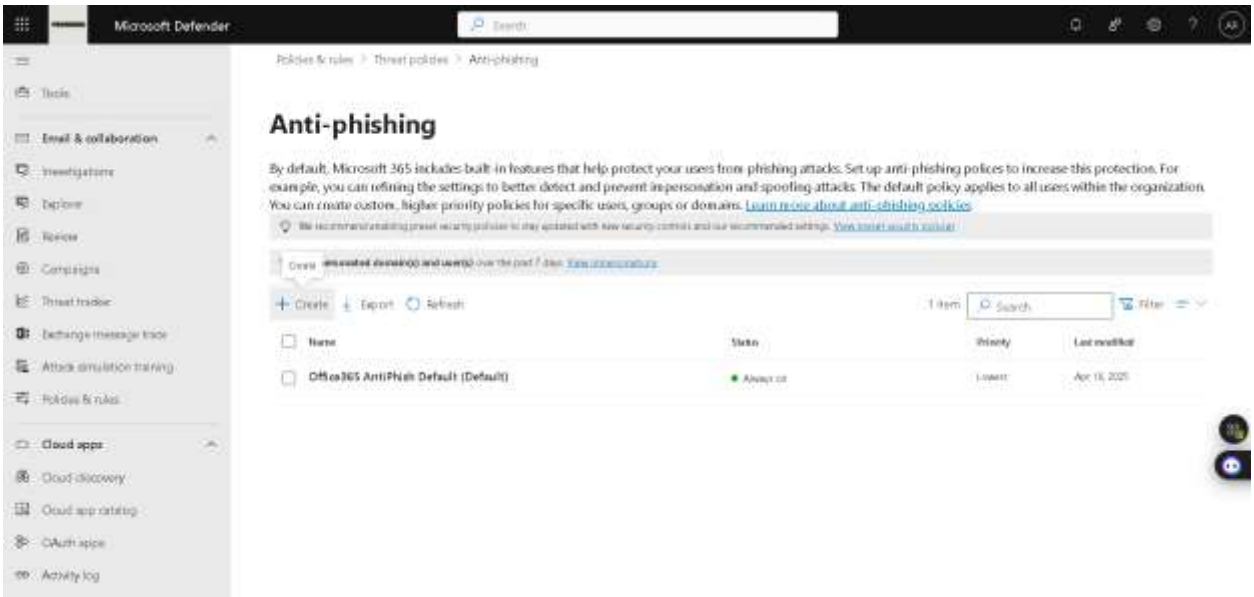


- Navigate to Policies and rules, then configure at least one policy to protect against phishing, malware, or spam.

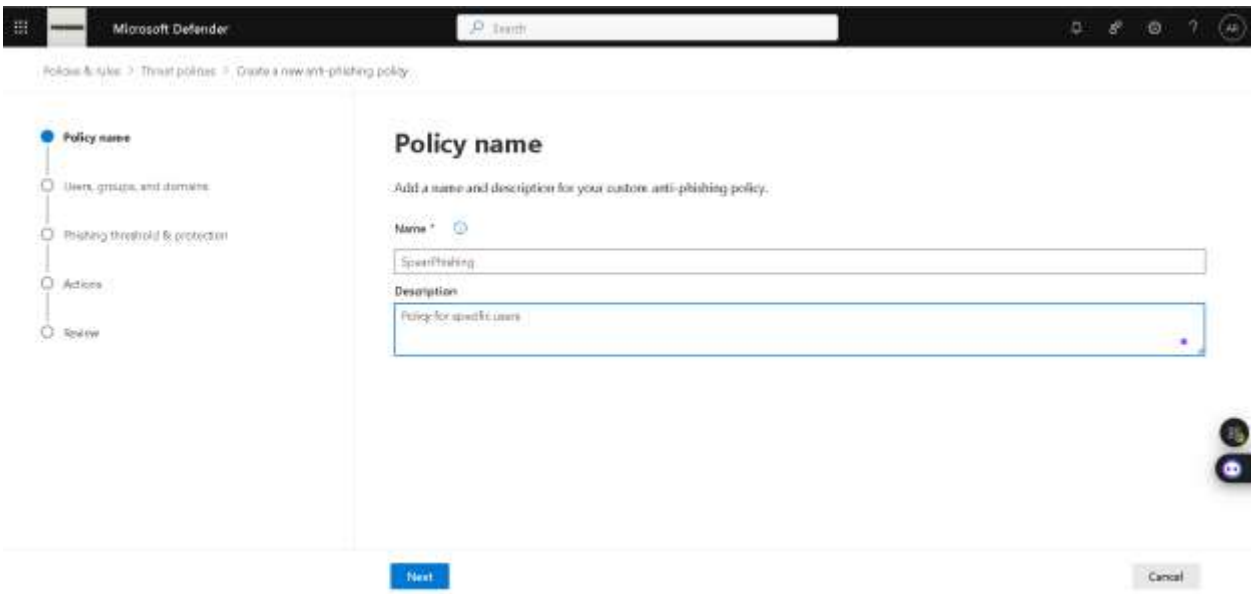
Step 1: To configure a policy, from Defender -> email & collaboration -> policies & rules -> threat policies -> Anti phishing. (As we are configuring this policy)



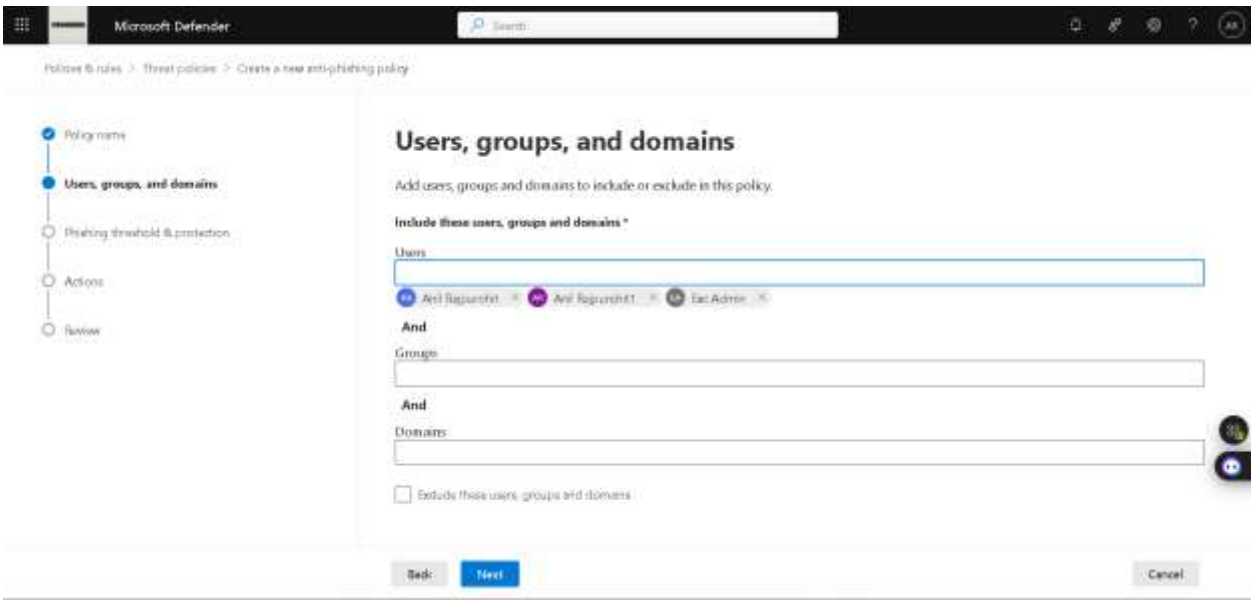
Step 2: In anti-phishing, click on create.



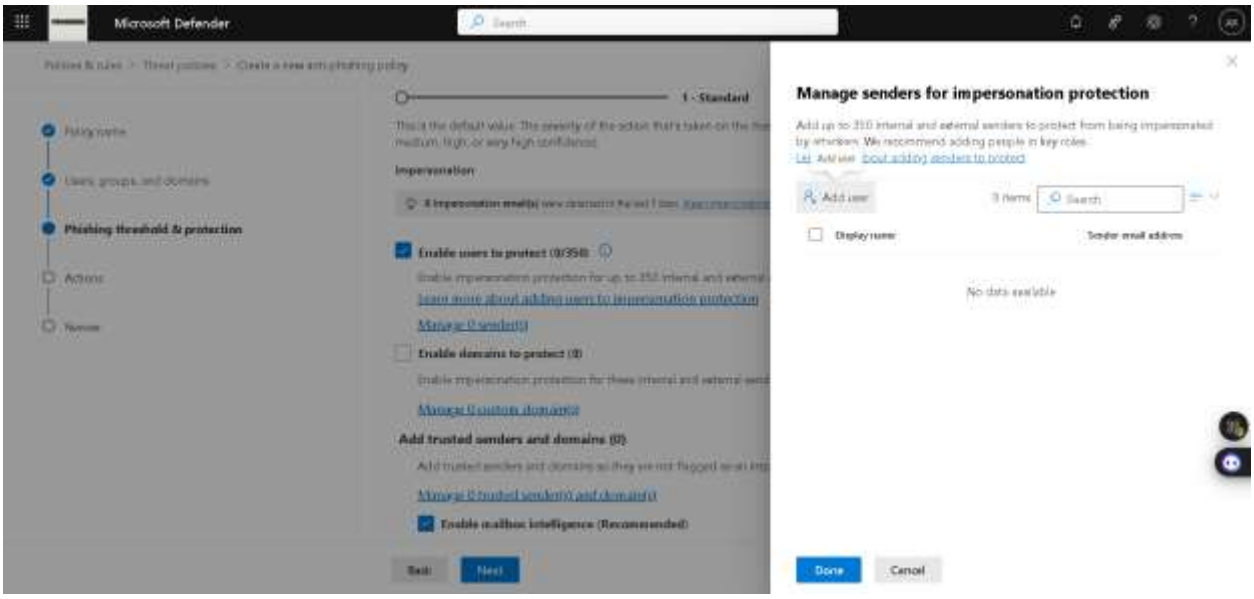
Step 3: As we already have Microsoft default anti-phishing policy, lets create more granular policy to protect specific sensitive users from phishing. Fill name and description of policy then Next.



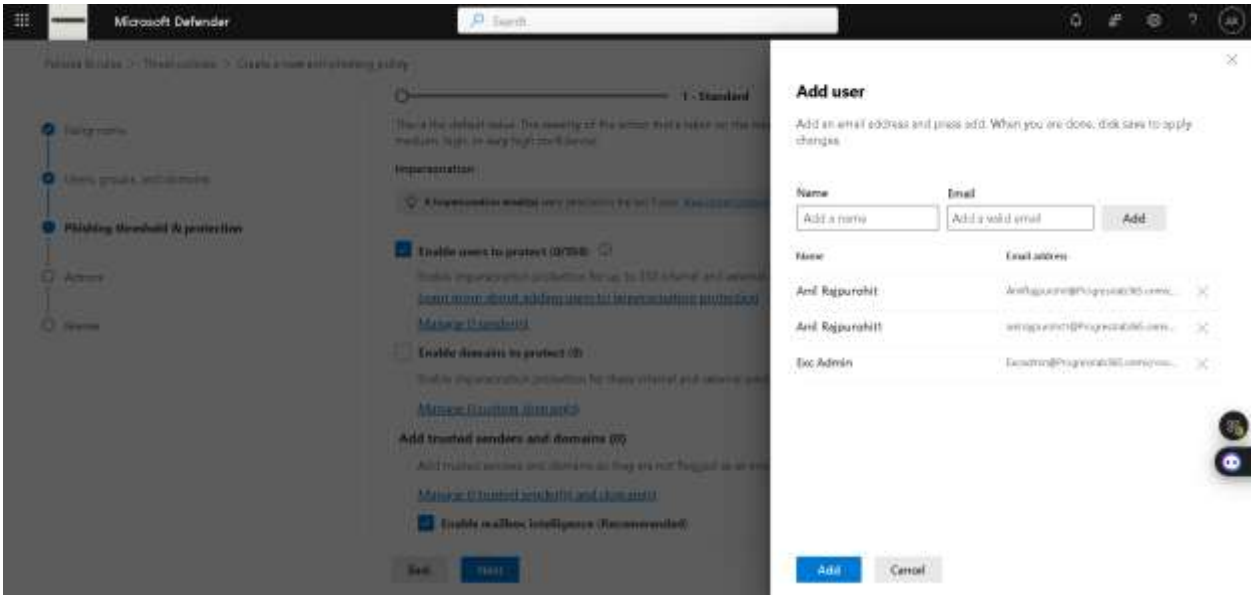
Step 3: Selected admins to include in this policy, as these are sensitive accounts. Then next.



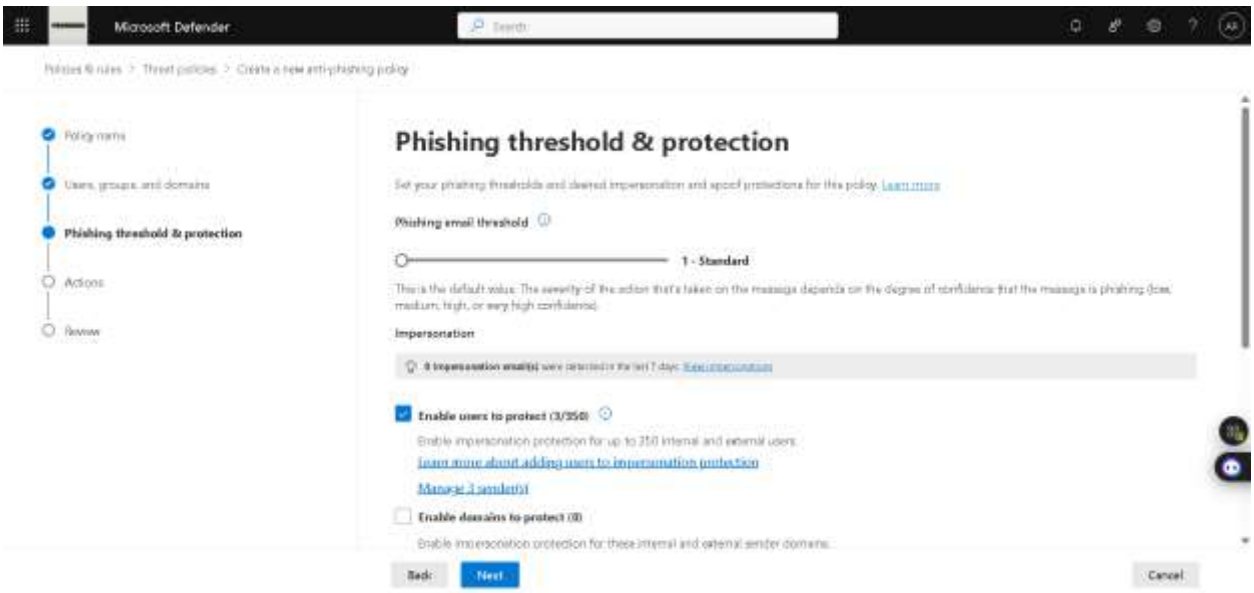
Step 4: Again select the users we want to protect from phishing attacks. Under Enable users to protect -> Manage 0 users -> then Add user.



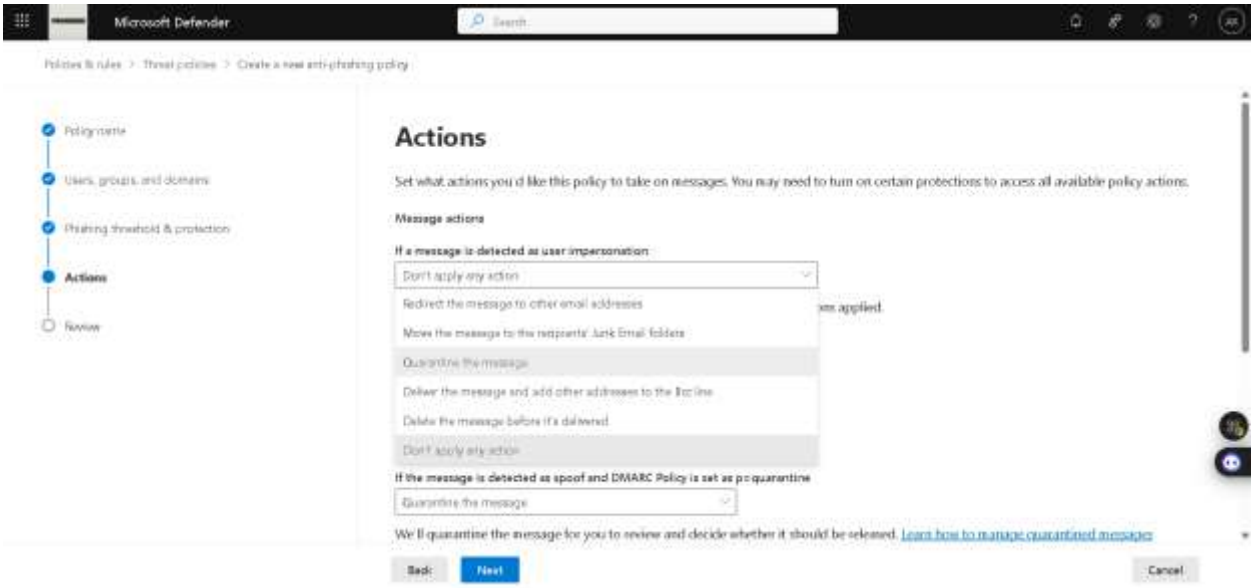
Step 5: Added all the admin accounts here. Then click on add.



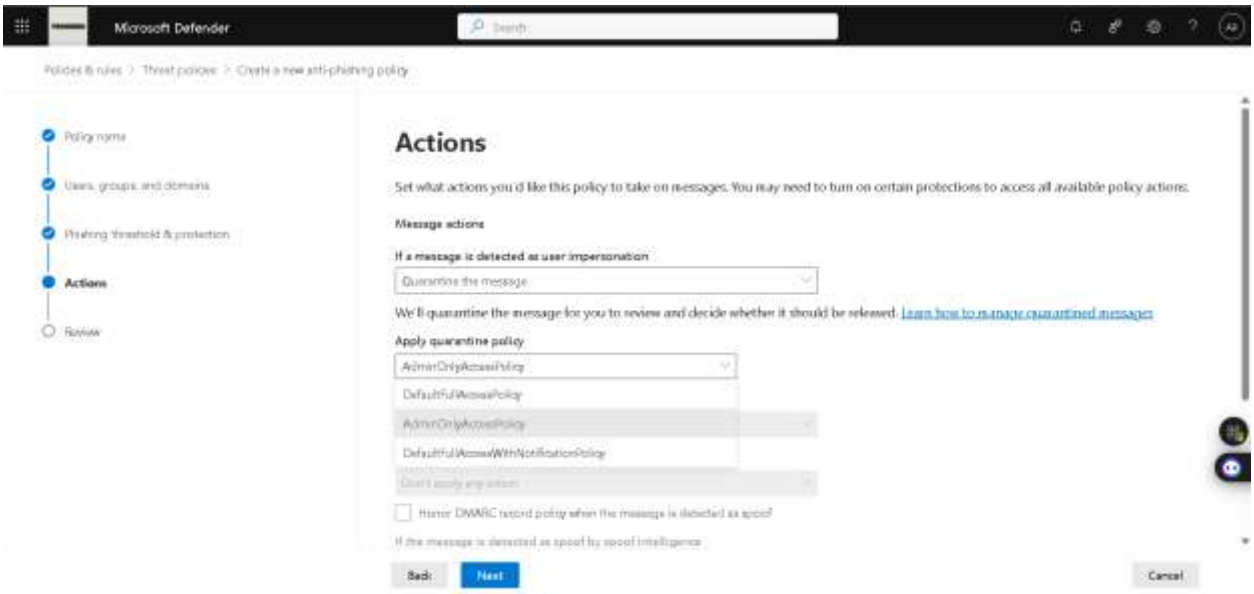
Step 6: We can see that our users has been selected, now click on next.



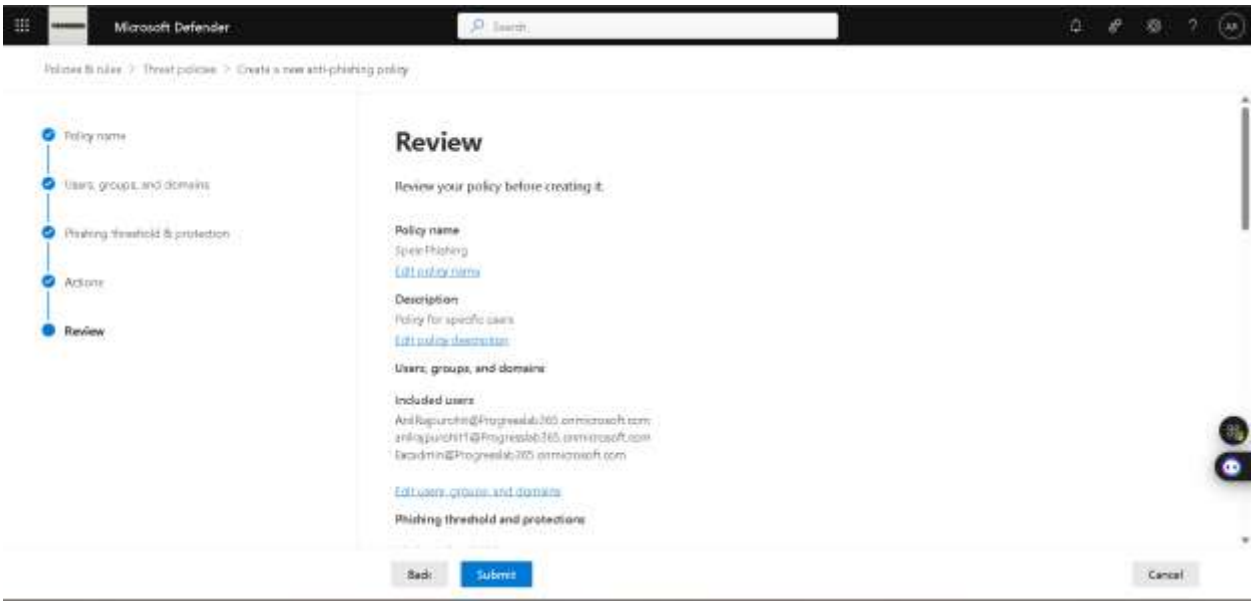
Step 7: Now select Quarantine the message, if a message is detected as user impersonation. Because we want to verify the message first then we can decide next actions.



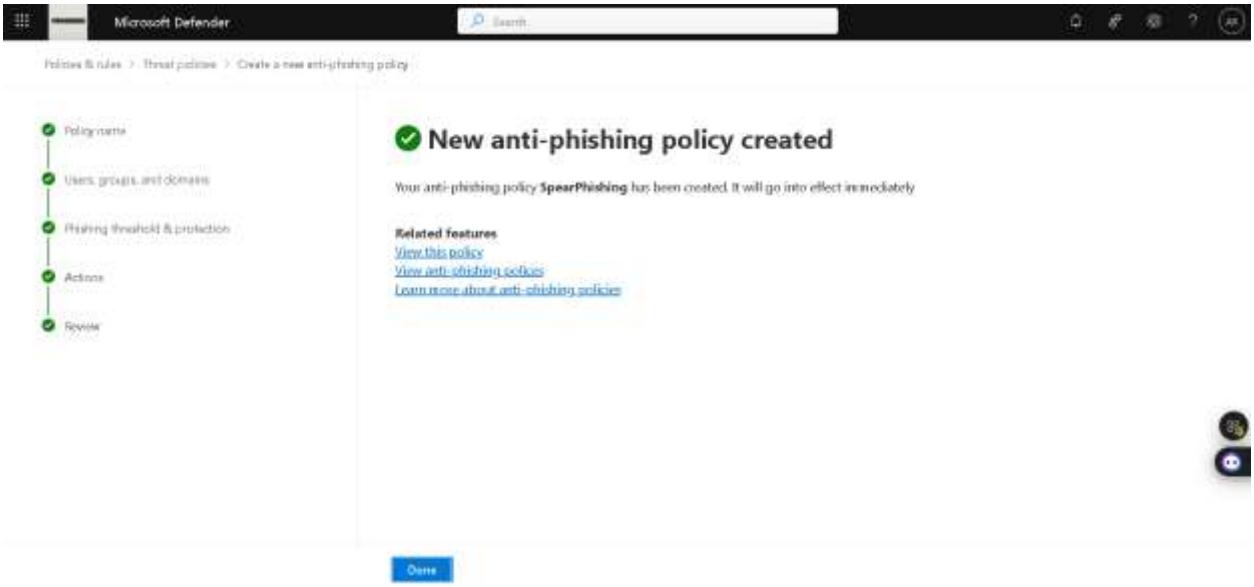
Step 8: Now, as we want to provide access to only admins for our quarentine policy select AdminOnlyAccessPolicy. Then Next.



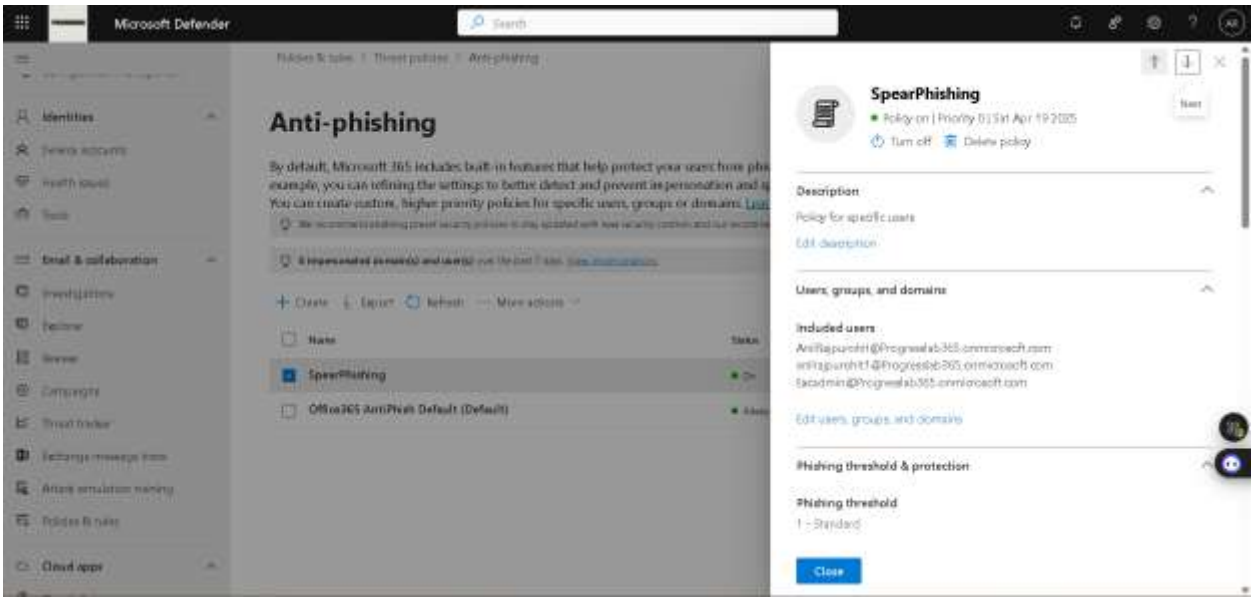
Step 9: Review our new policy details and click on submit.



Step 10: Our policy has been successfully created.



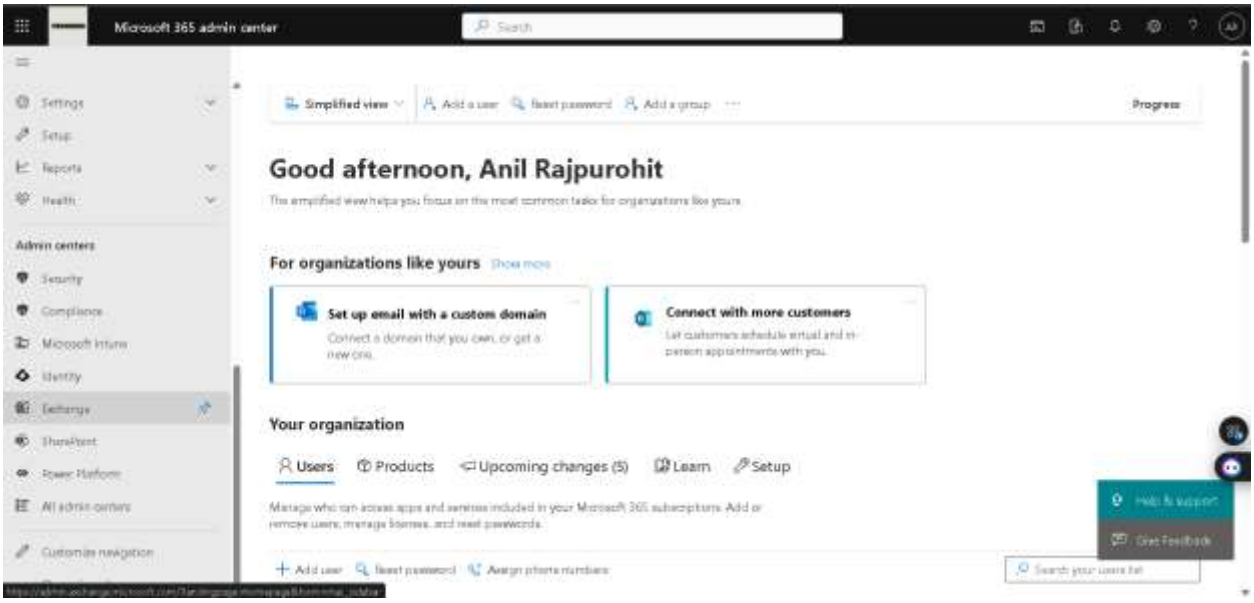
Step 11: We can view our new active policy under Defender -> email & collaboration -> policies & rules -> threat policies -> Anti phishing.



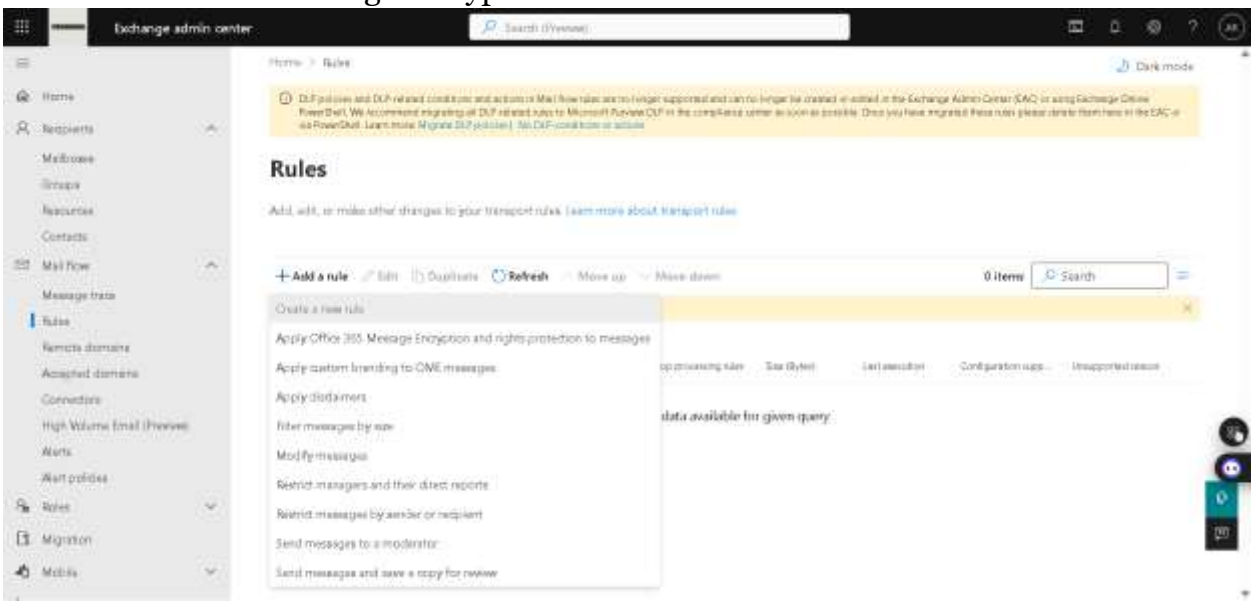
2. Set Up Data Encryption:

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

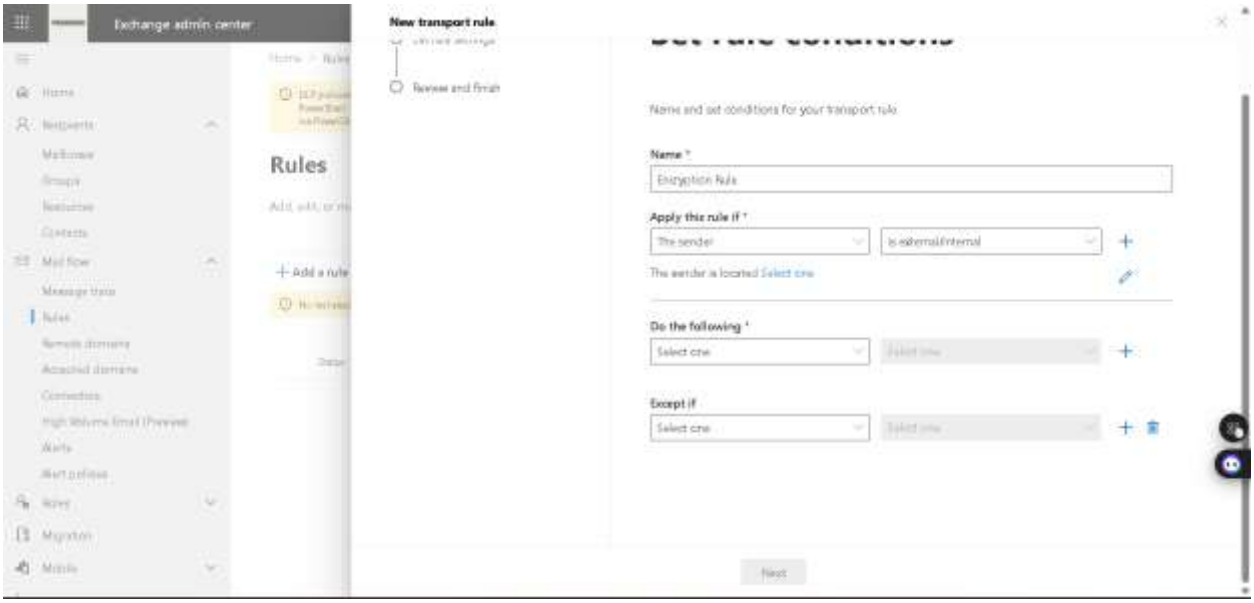
Step 1: Form Microsoft 365 admin center, under admin centers select Exchange.



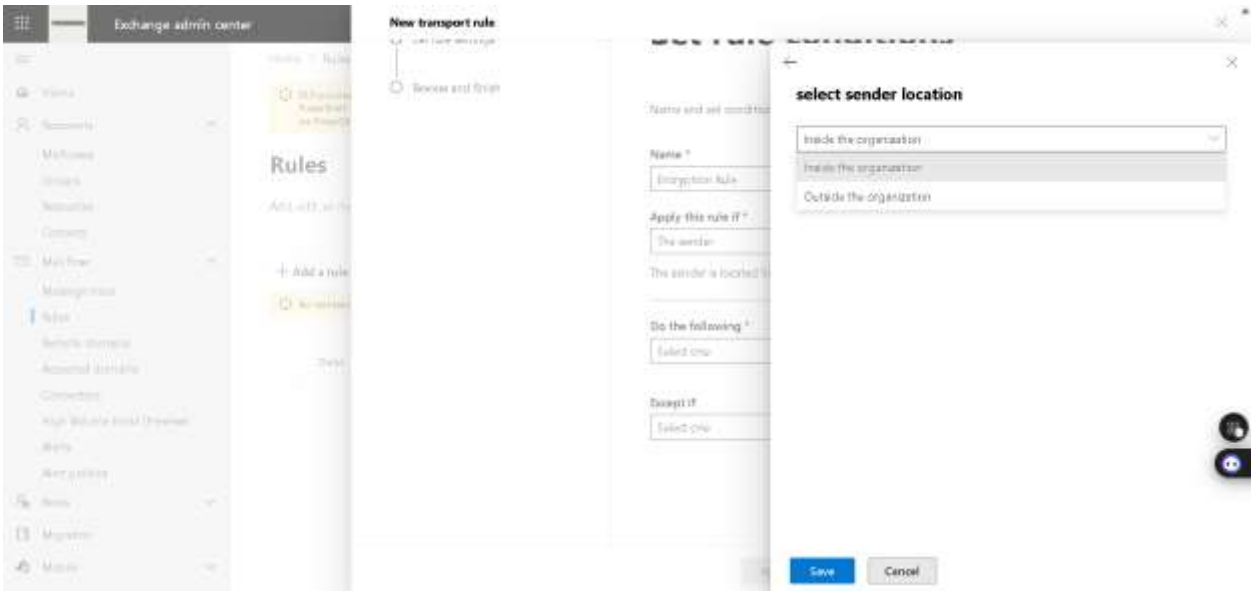
Step 2: In exchange admin center, mail flow -> rules -> Add a rule -> create a new rule. To create a rule for message encryption.



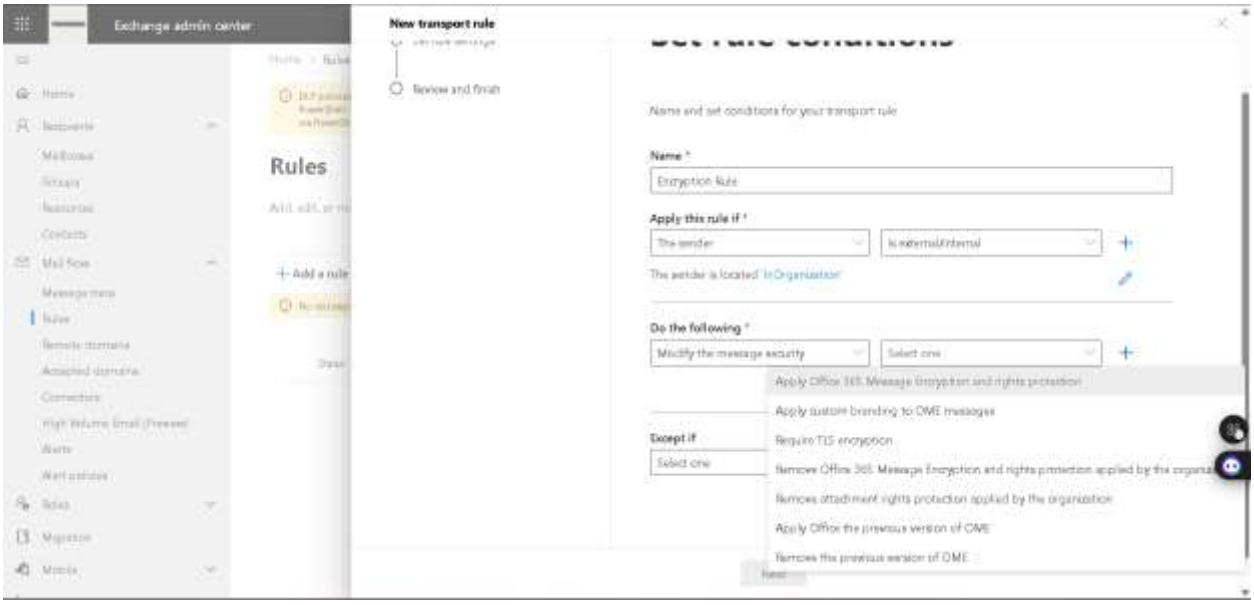
Step 3: Provide details like name, then select the condition. E.g. This policy will apply to the sender which is external/internal.



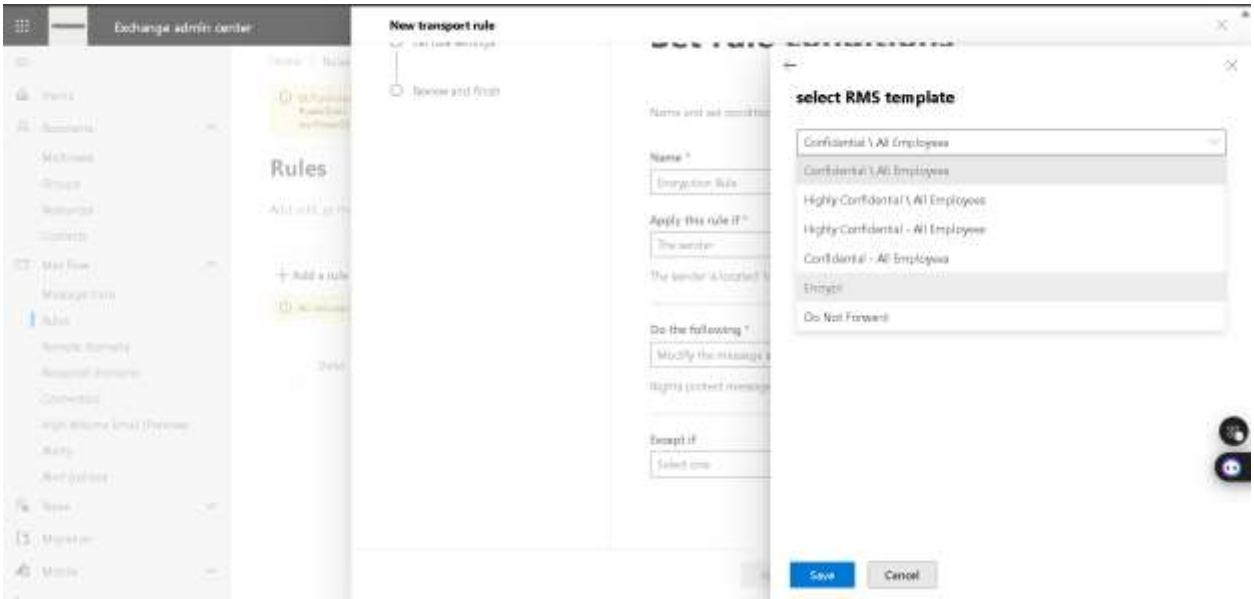
Step 4: Now, more specific we want only from inside the organization then save.



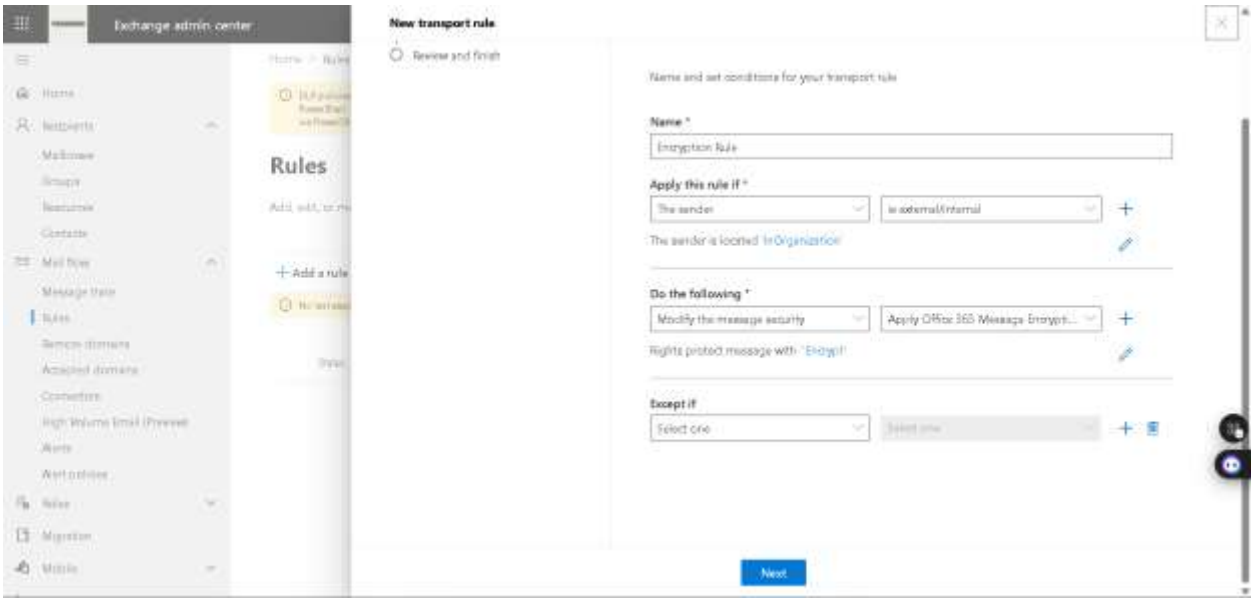
Step 5: Next condition, Modify the message security for Office 365 message encryption and right protection.



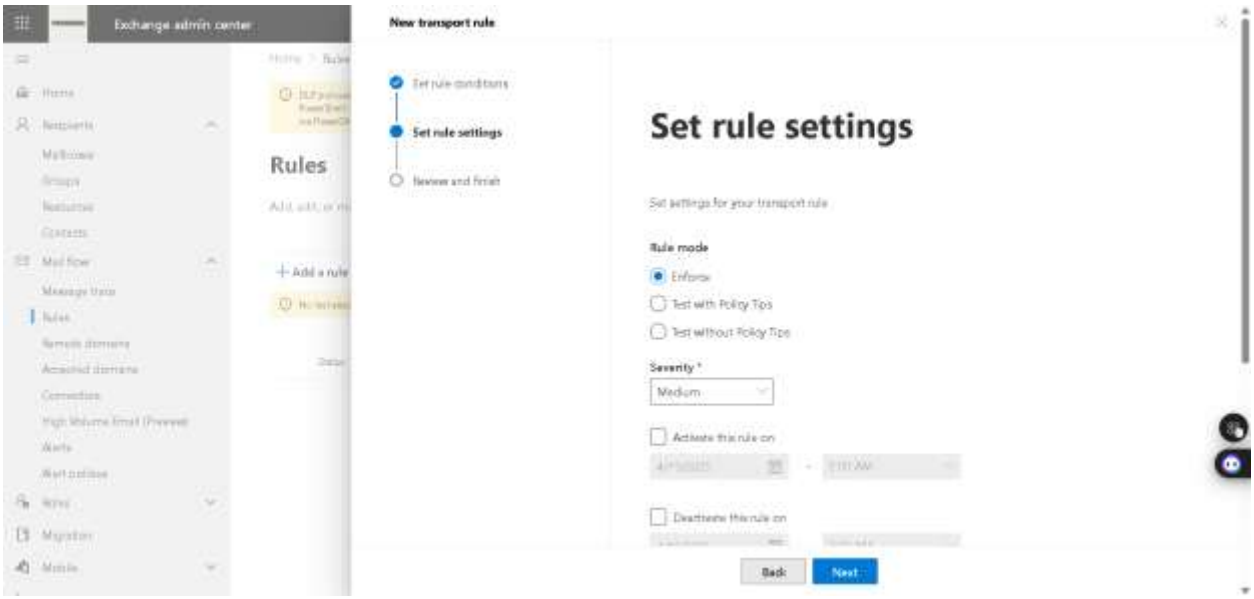
Step 6: RMS template as encrypt then save the condition.



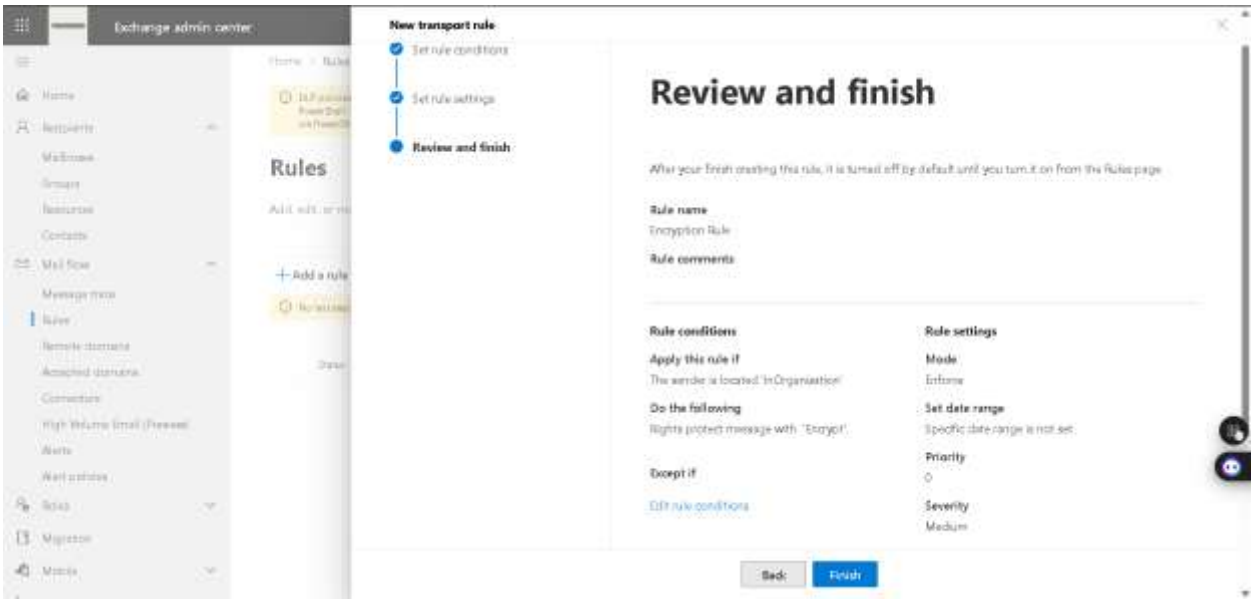
Step 7: Verify the rule and we don't want to exclude anyone. Then click on next.



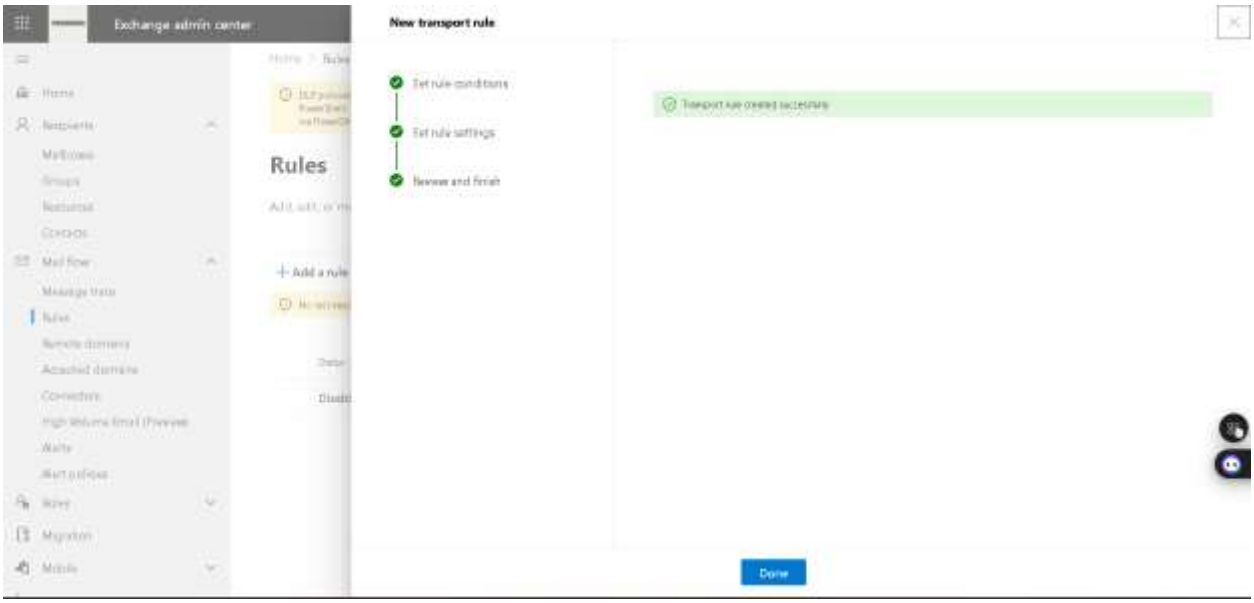
Step 8: Enforce the rule, choose the severity then Next.



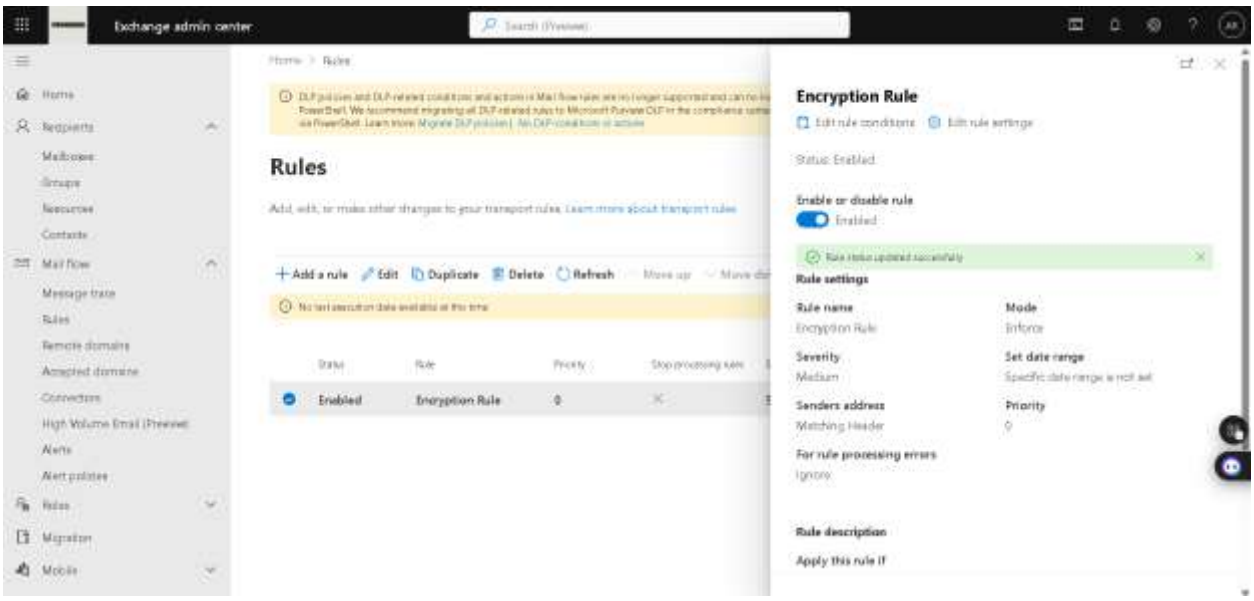
Step 9: Review the whole rule and click on finish.



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.

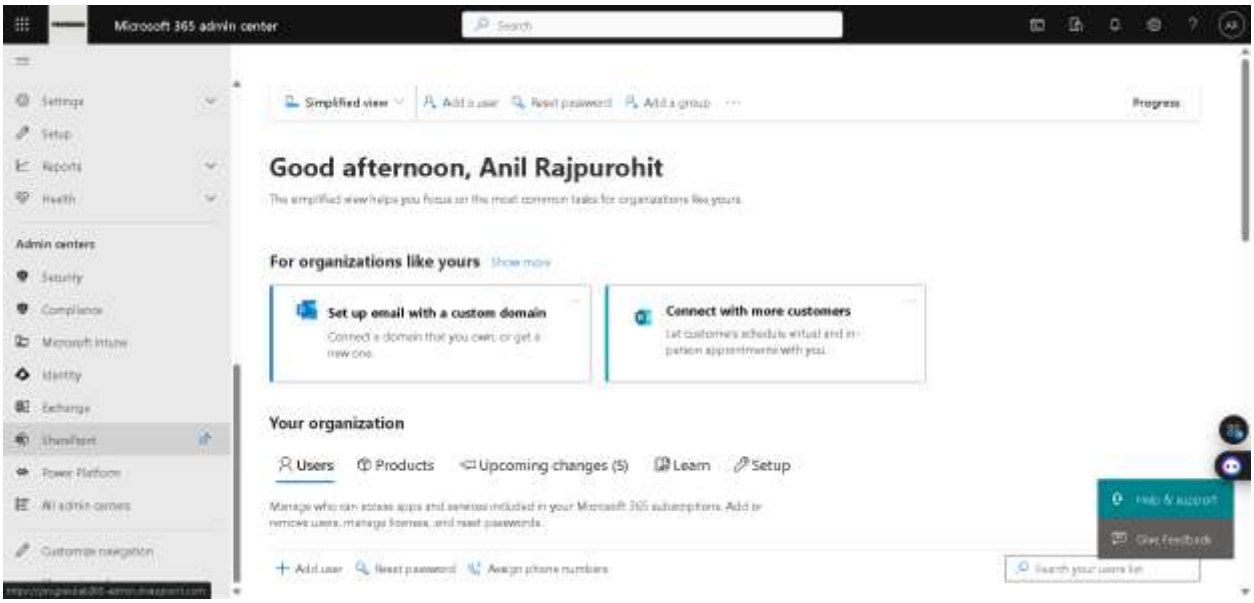
We can also create rules for encrypting messages inside the organization, so that even if anyone get access to the data. They won't be able to get anything from that.

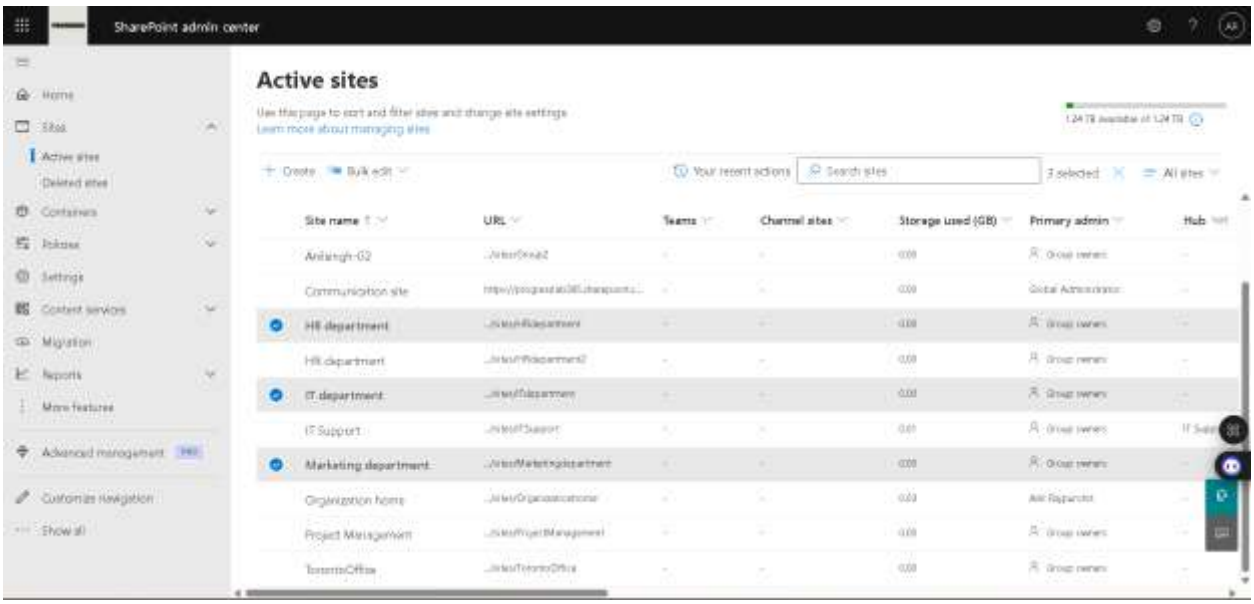
Task 3: Configuring and Managing Collaboration Tools

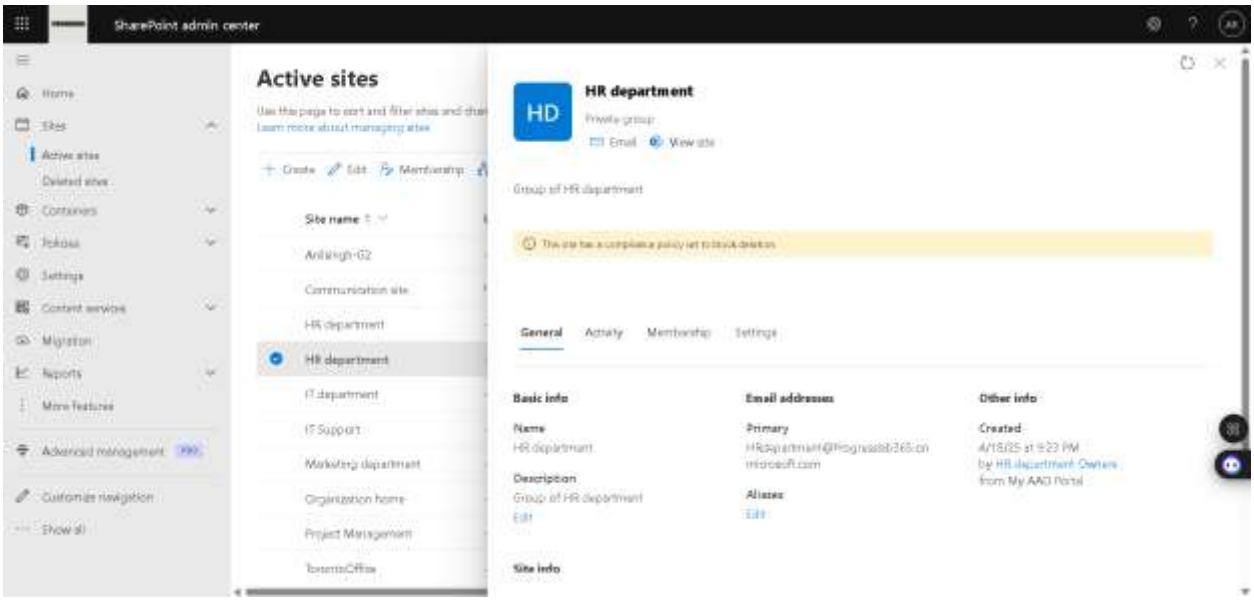
1. Set Up SharePoint Online:

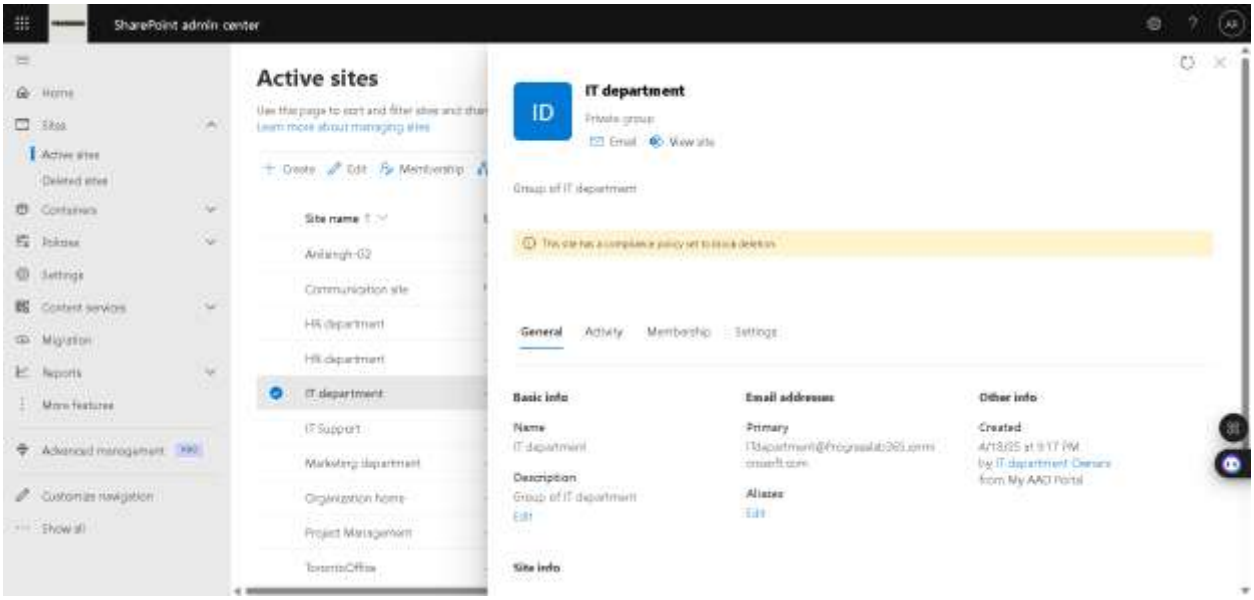
- Create an online SharePoint site for each department (IT, HR, Marketing).

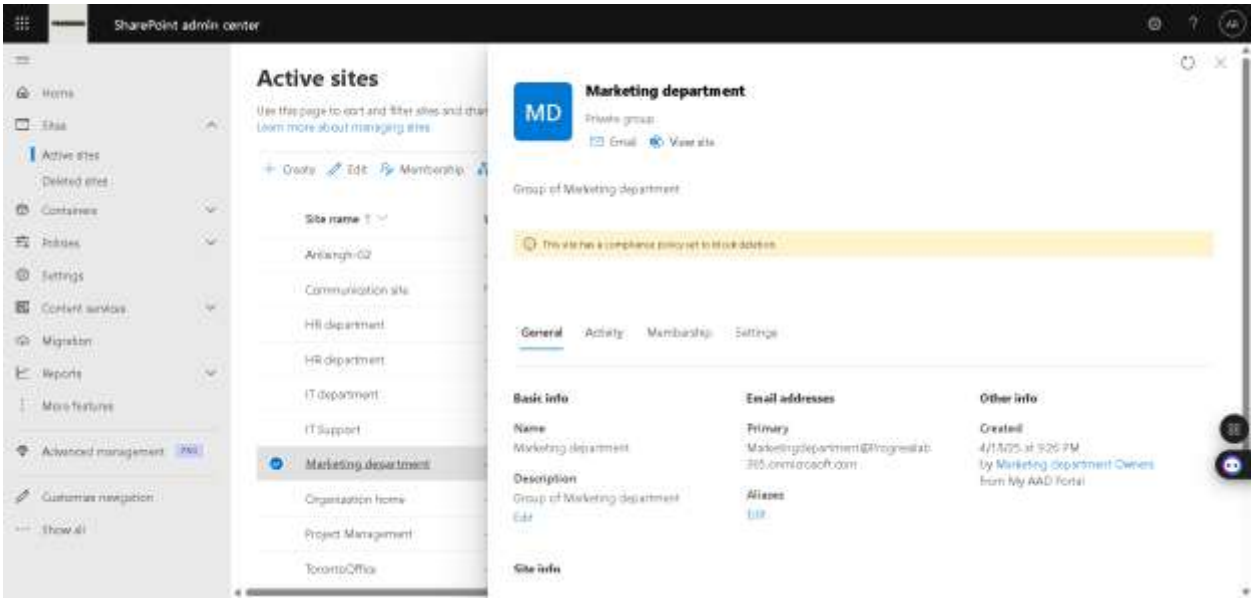
Step 1: From Microsoft 365 admin center, under admin centers select SharePoint.






SharePoint admin center
Active sites
HR department
Group of HR department
General
Activity
Membership
Settings
Basic info
Email addresses
Other info
Name
Description
Primary
Aliases
Created
Site info

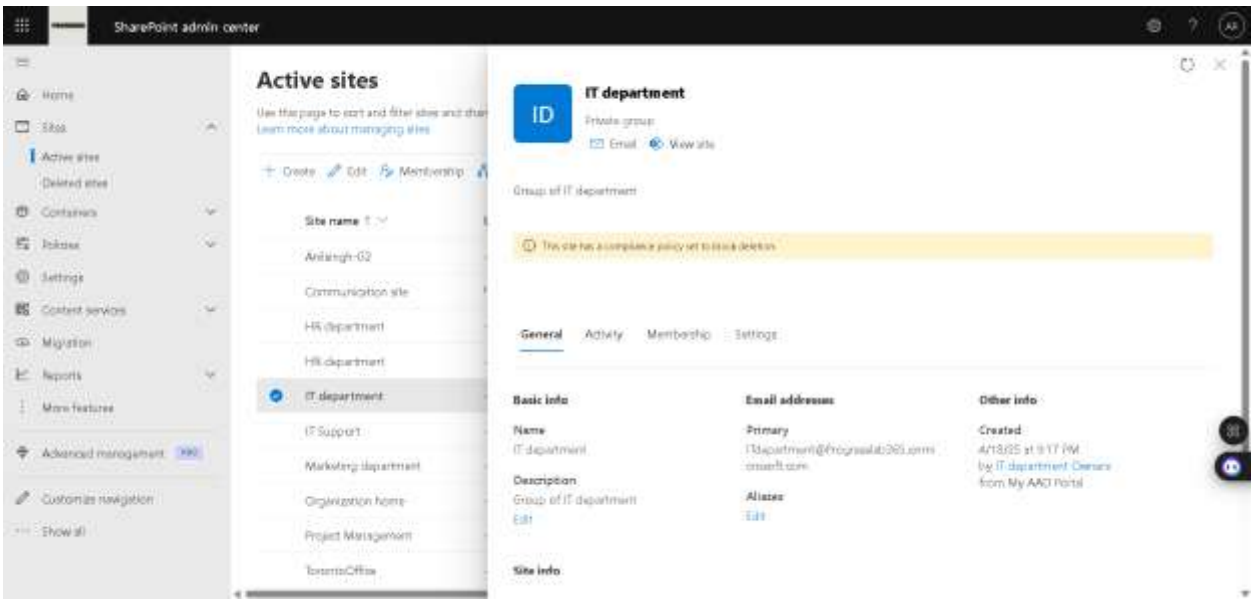

SharePoint admin center
Active sites
IT department
Group of IT department
General
Activity
Membership
Settings
Basic info
Email addresses
Other info
Name
Description
Primary
Aliases
Created
Site info



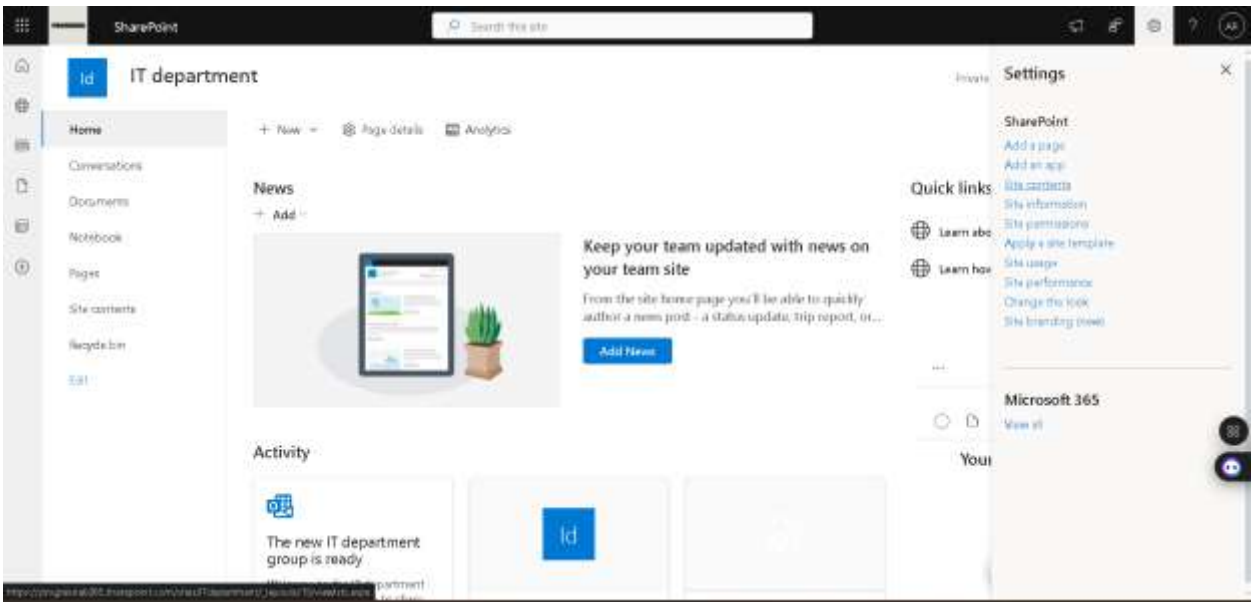
- Configure document libraries and permissions for each site.

For IT department SharePoint

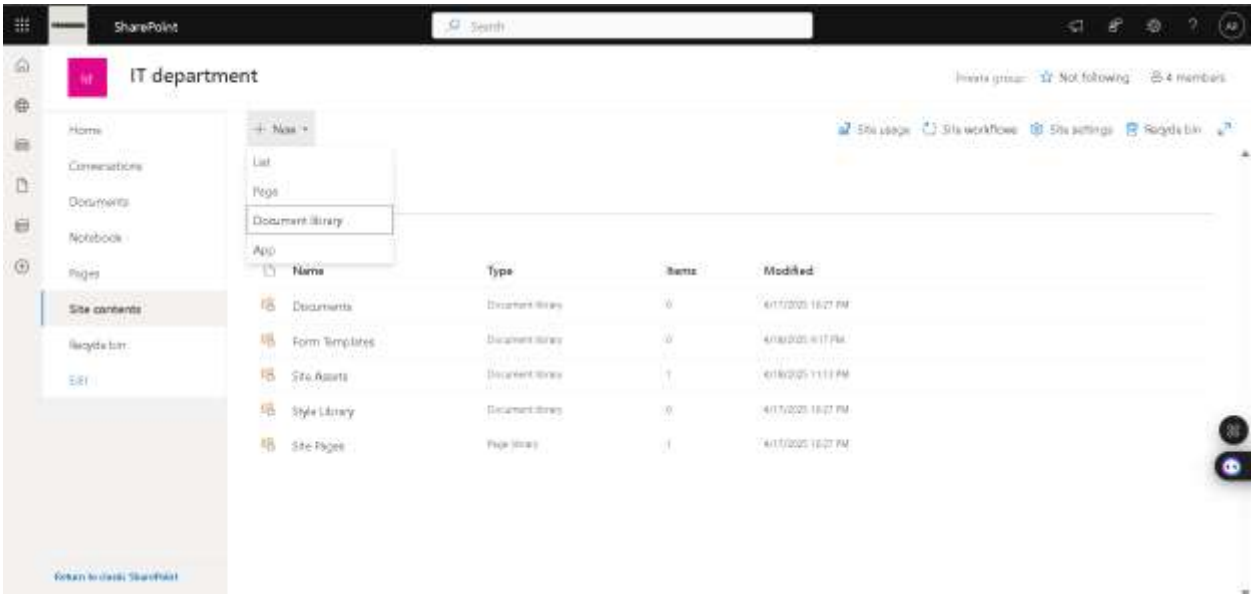
Step 1: From SharePoint admin center, go to sites -> active sites -> It department -> View site.



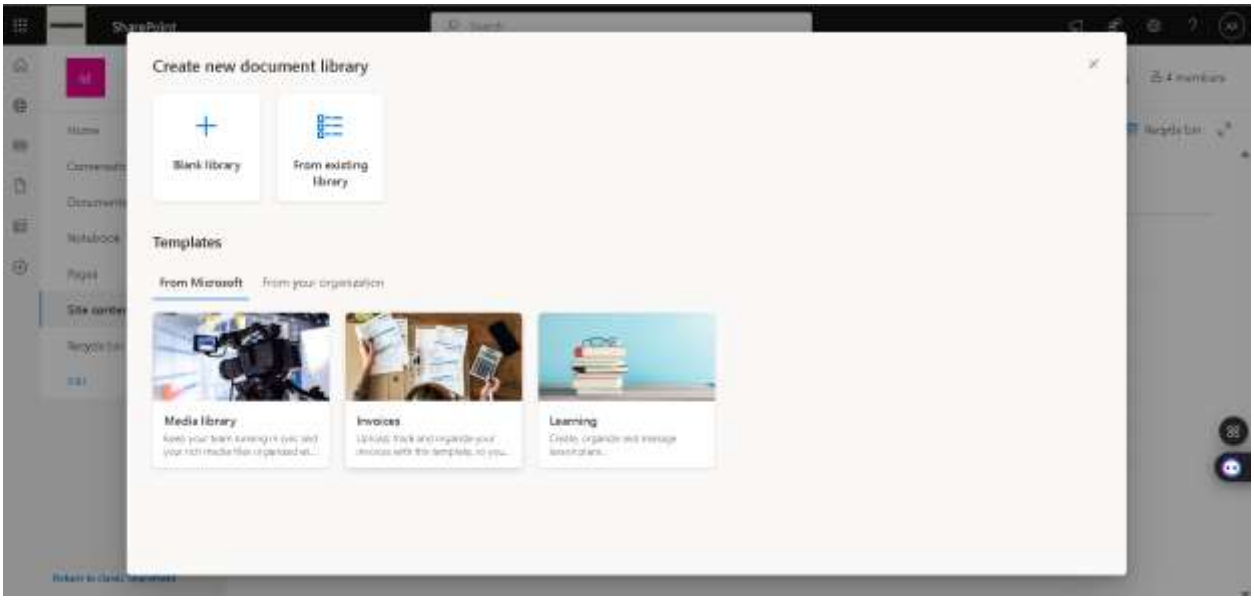
Step 2: Now from IT department SharePoint site, click on settings sign -> site contents.



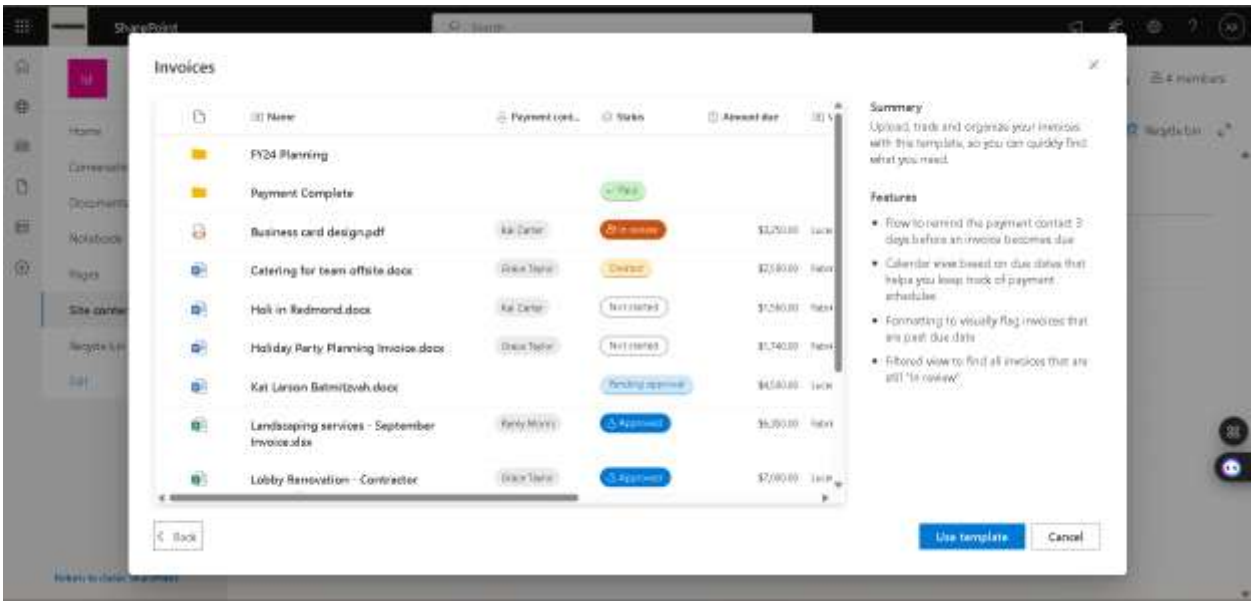
Step 3: Under site contents, new -> document library.



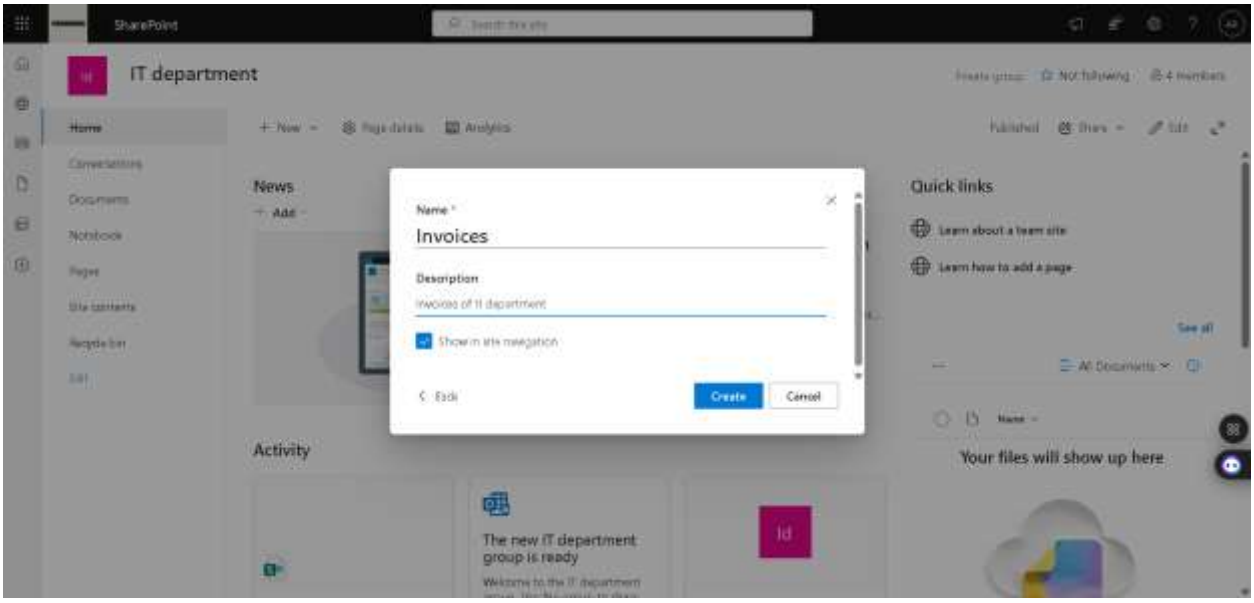
Step 4: We can select from template or create a blank library. We will select Invoices template.



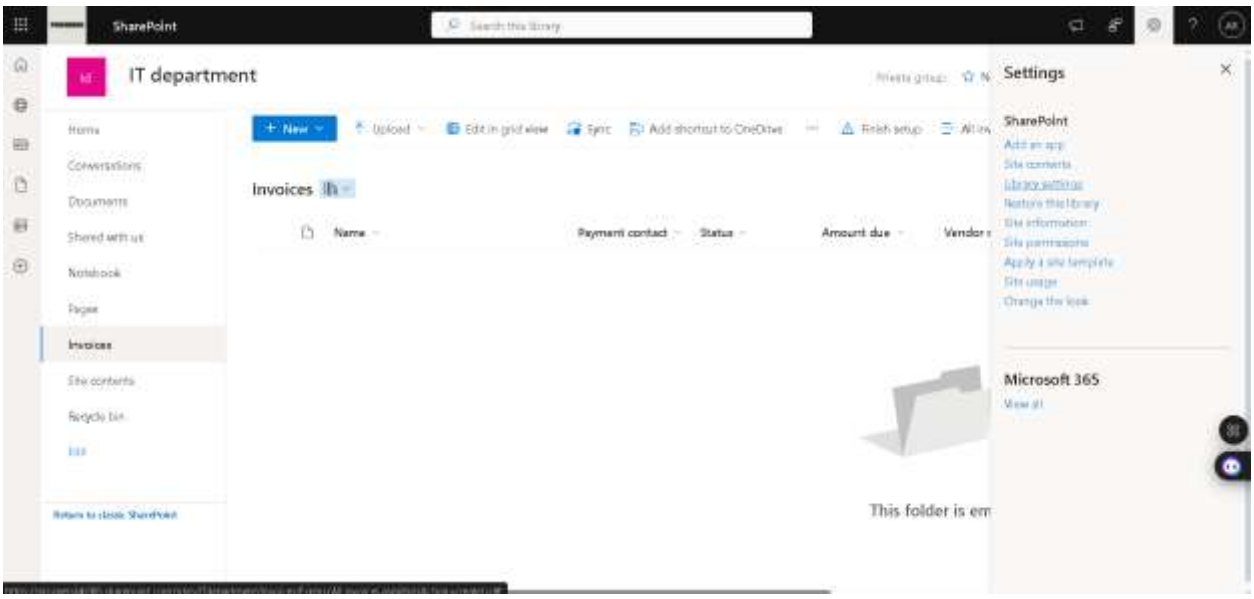
Step 5: We can see features of the template then click on use template.



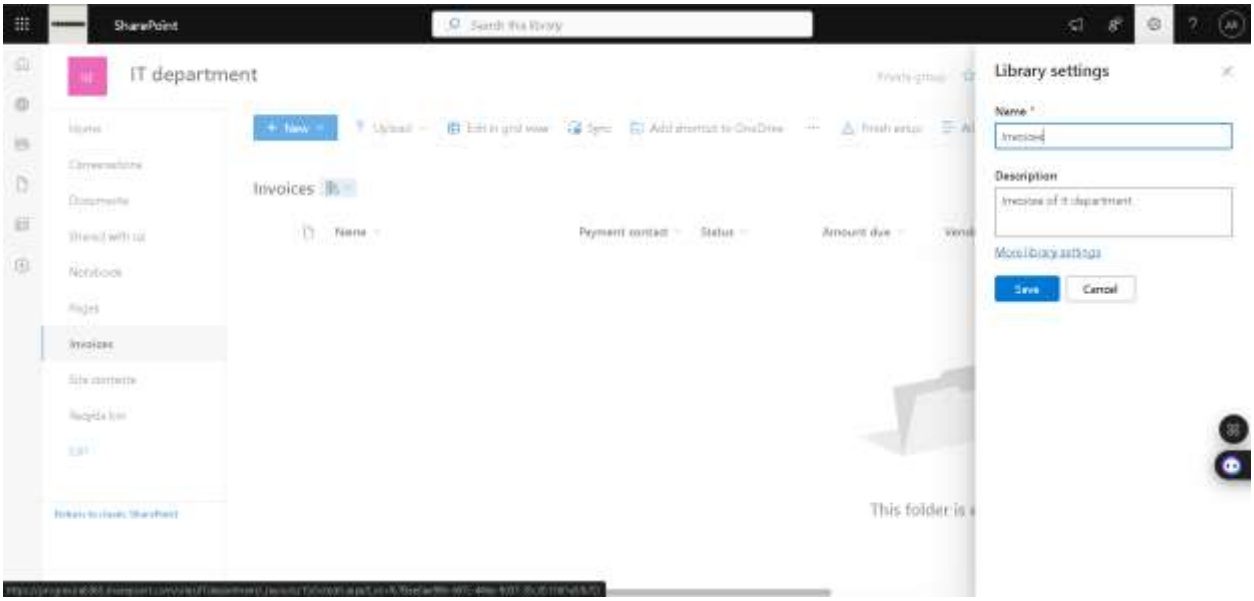
Step 6: We want to create a Invoices library, so fill name and description then create.



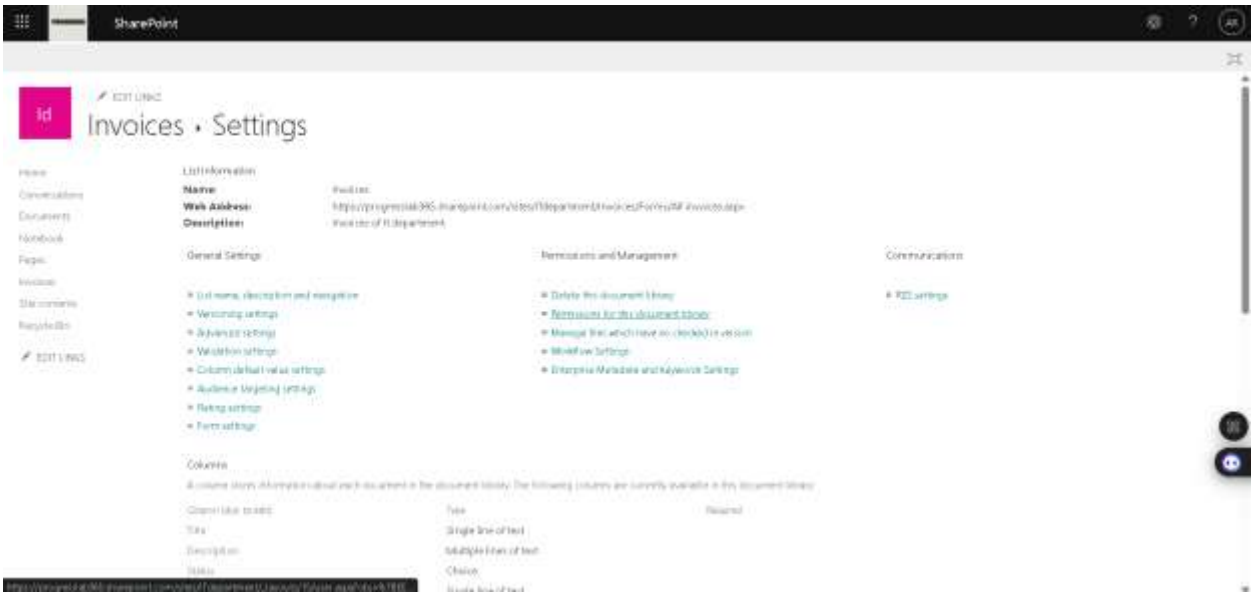
Step 7: Invoices library has been created, now select settings sign -> library settings.



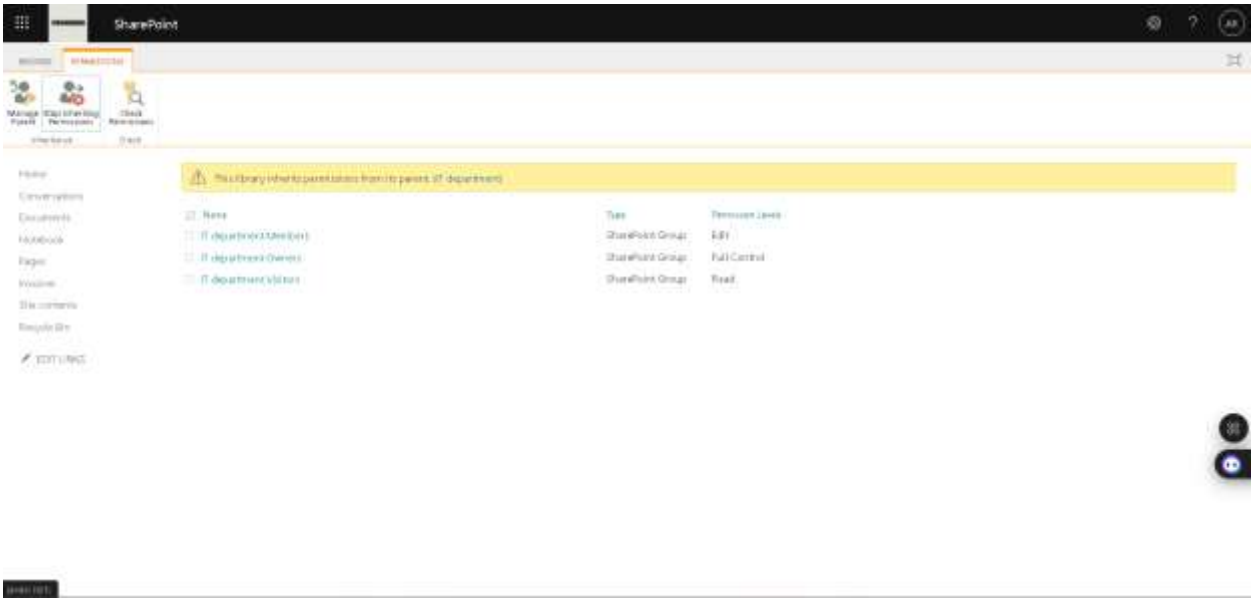
Step 8: Click on more library settings now.



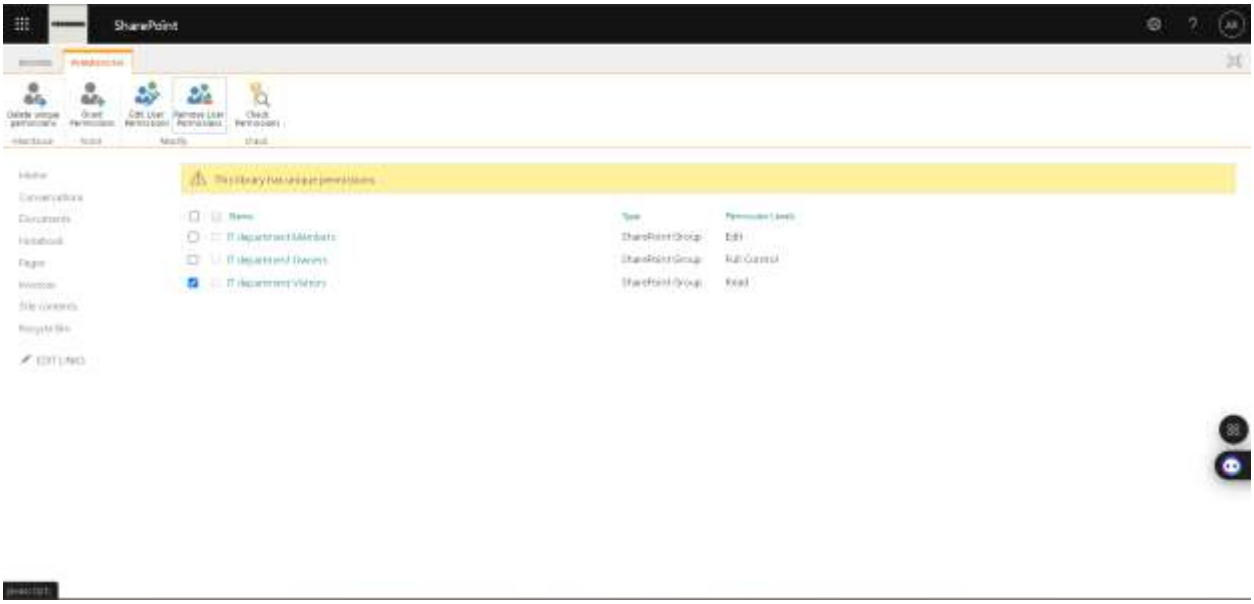
Step 9: Now, select under Permissions & Management ->permissions for this document library.



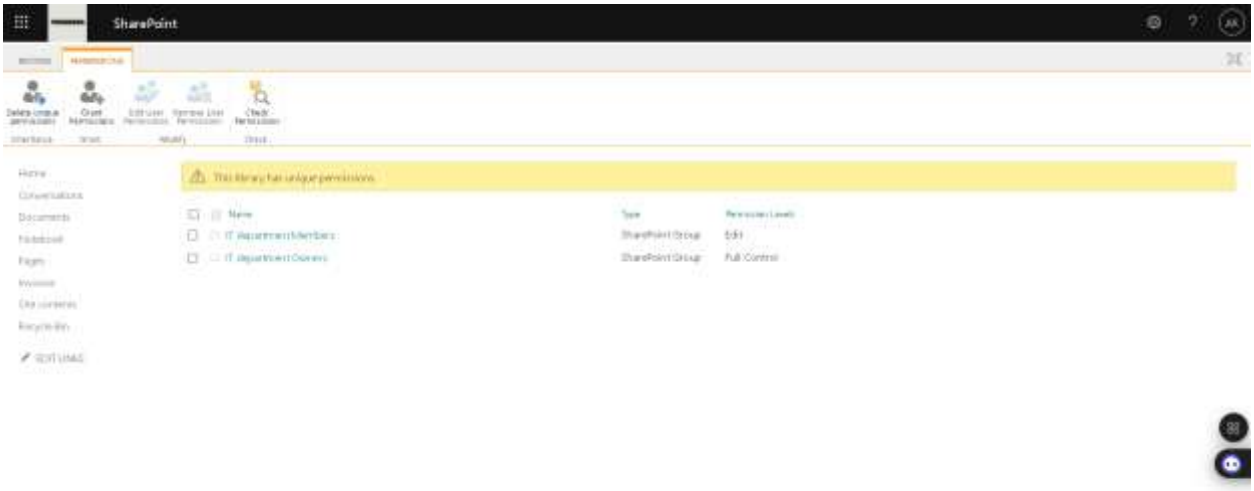
Step 10: First, click on stop inheriting permissions, so that we can add custom permissions to this library.



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.

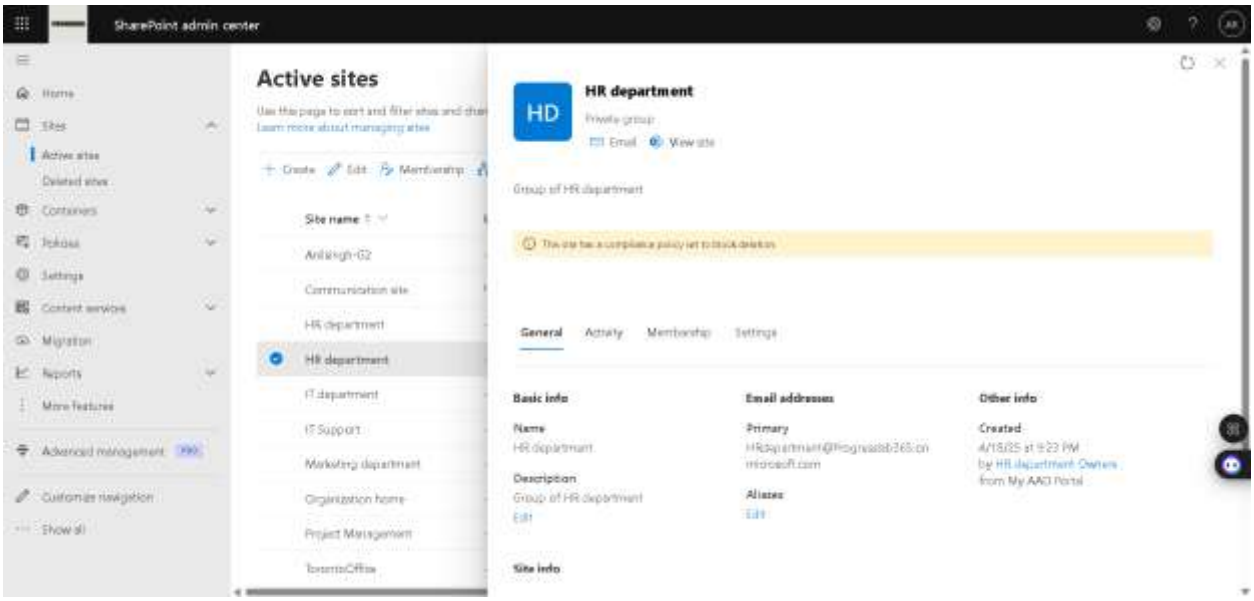


Step 12: Now for this library, we have only members which we need.

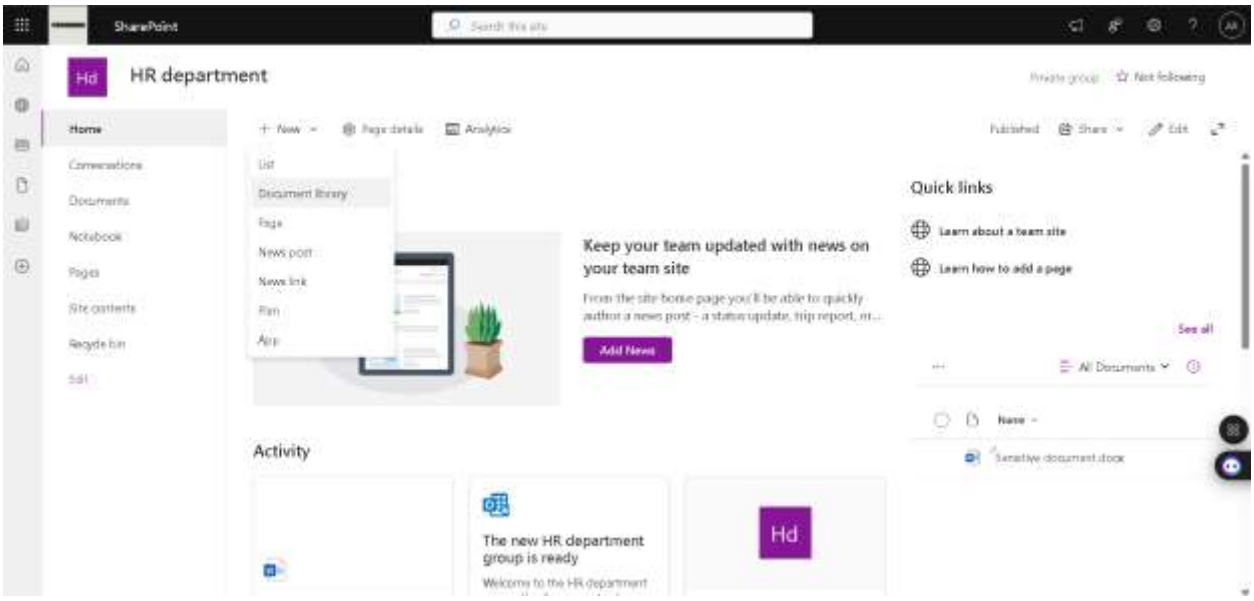


For HR department SharePoint

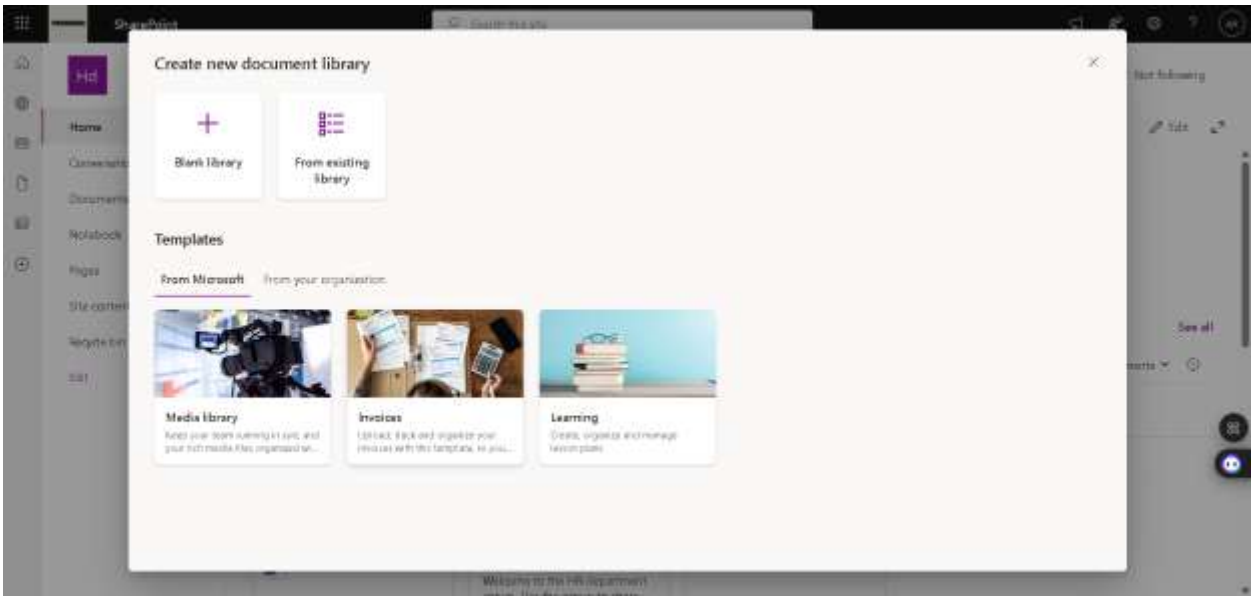
Step 1: From SharePoint admin center, go to sites -> active sites -> HR department -> View site.



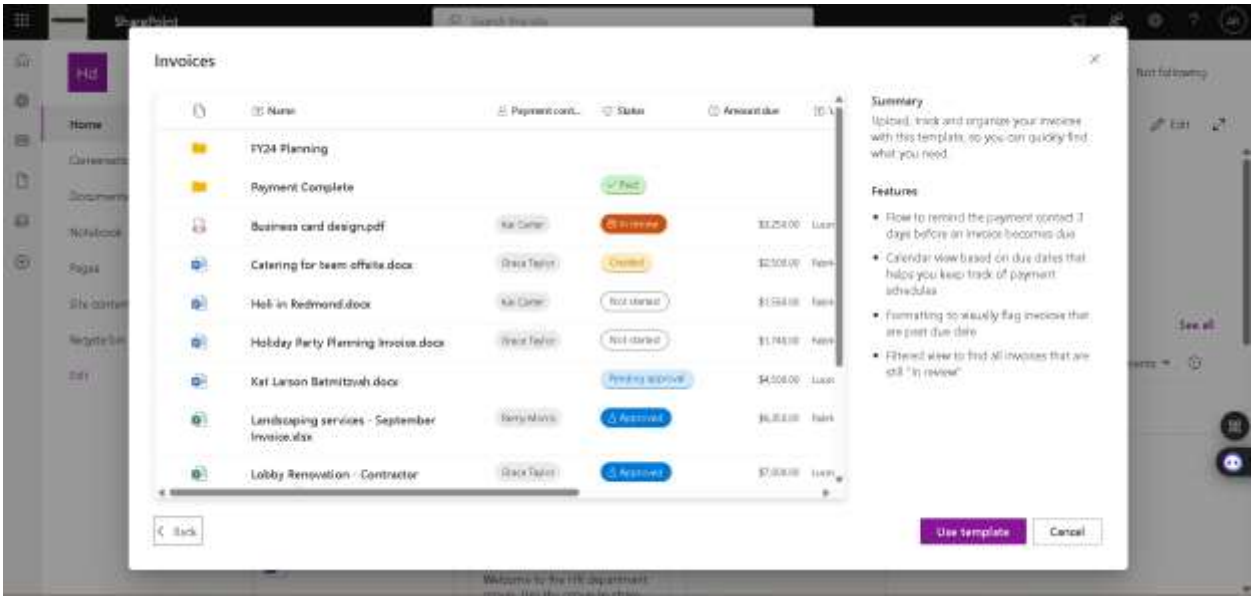
Step 2: Now from HR department SharePoint site, click on New -> Document library.



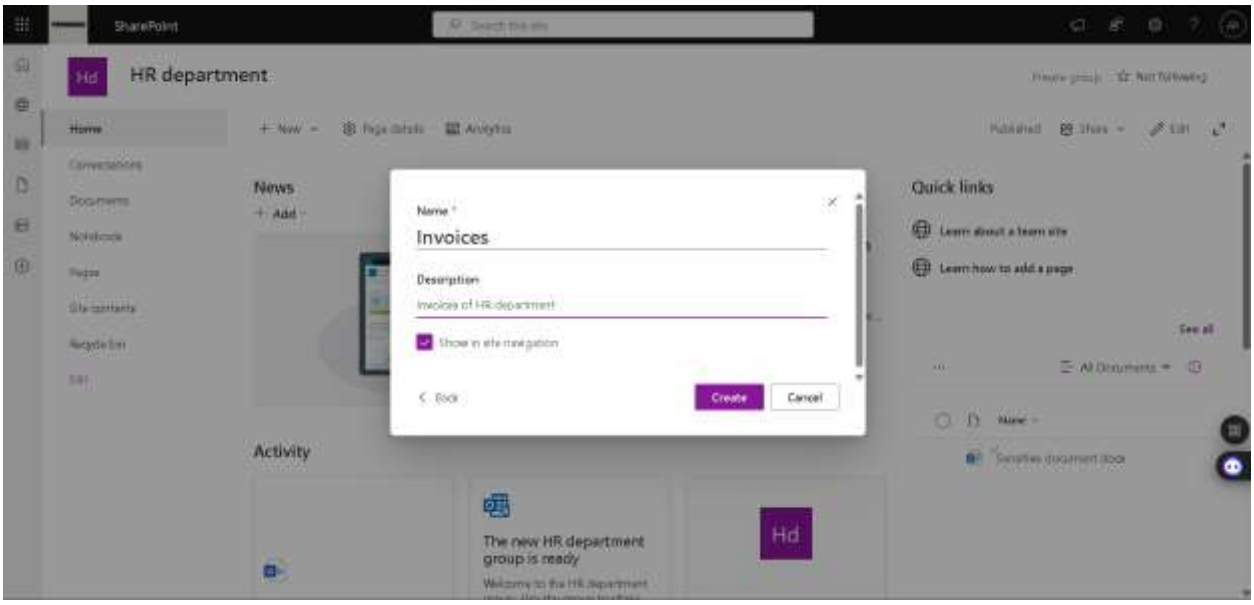
Step 3: We can select from template or create a blank library. We will select Invoices template.



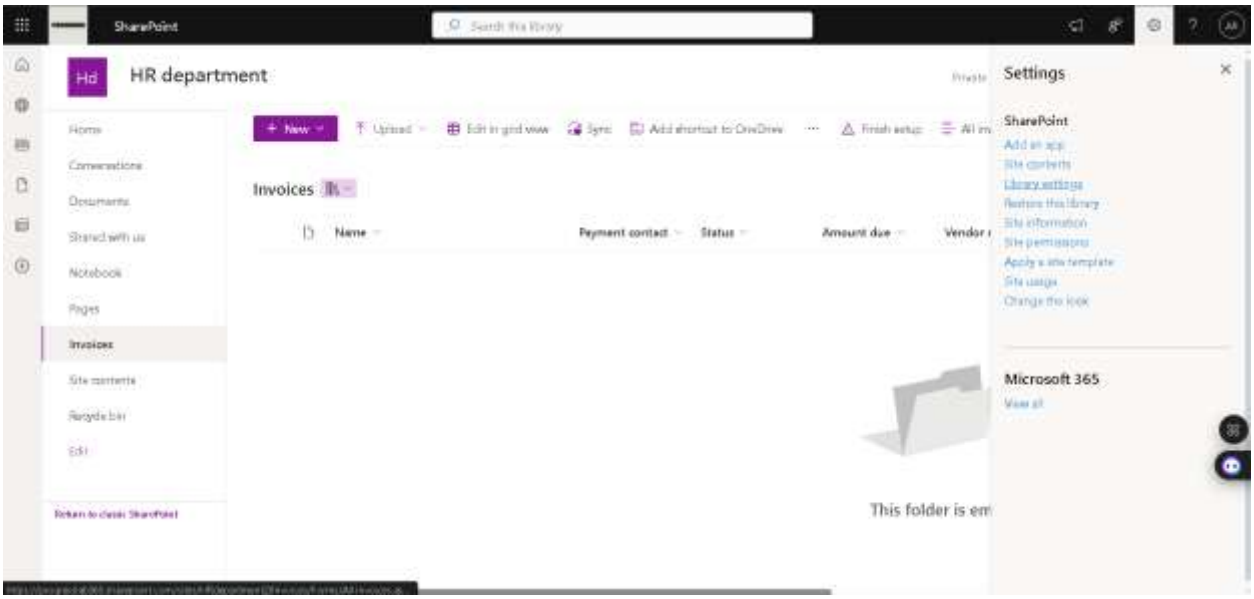
Step 4: We can see features of the template then click on use template.



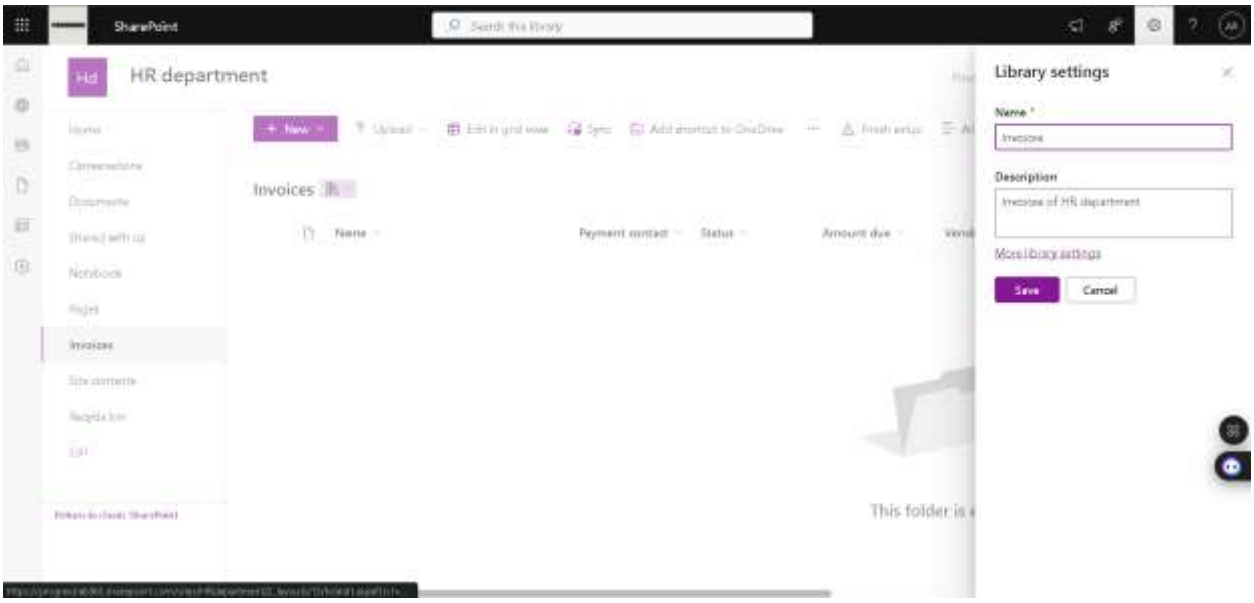
Step 5: We want to create a Invoices library, so fill name and description then create.



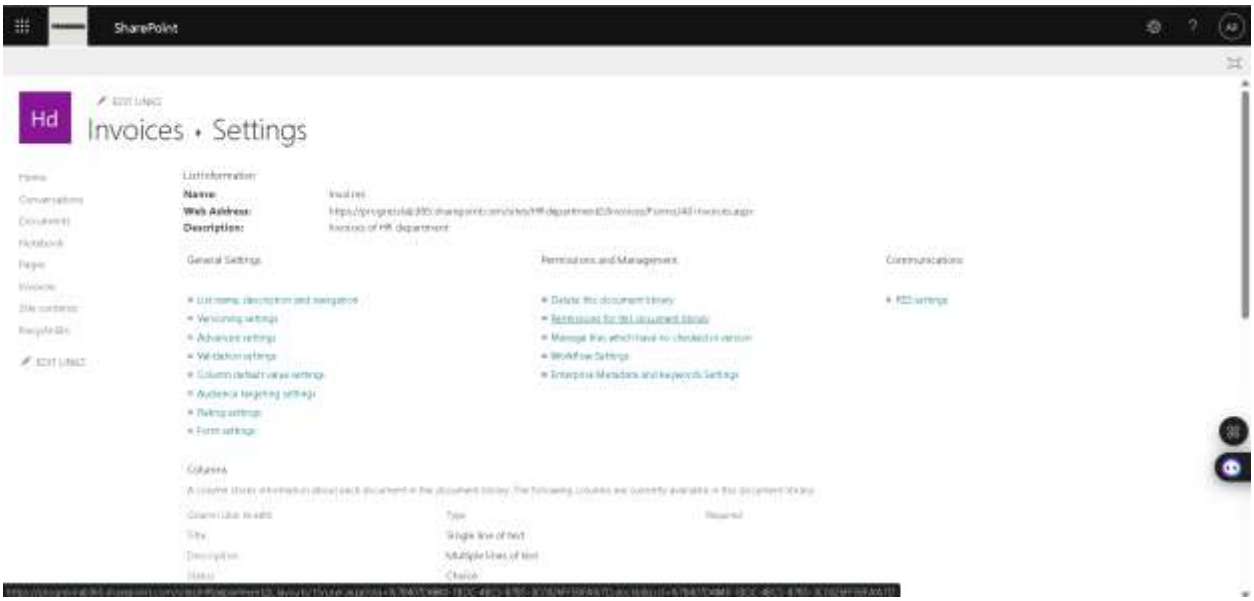
Step 6: Invoices library has been created, now select settings sign -> library settings.



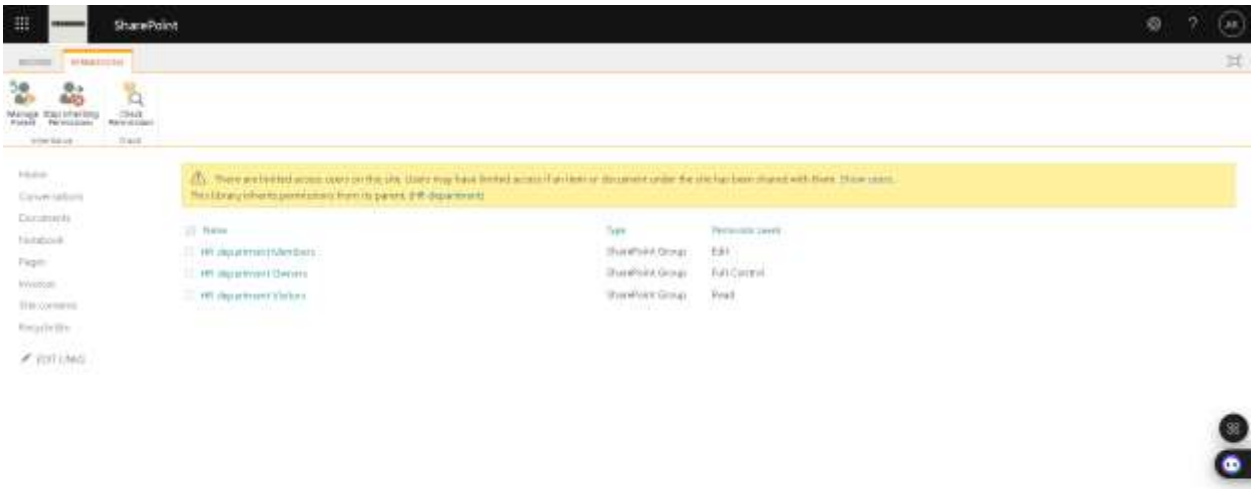
Step 7: Click on more library settings now.



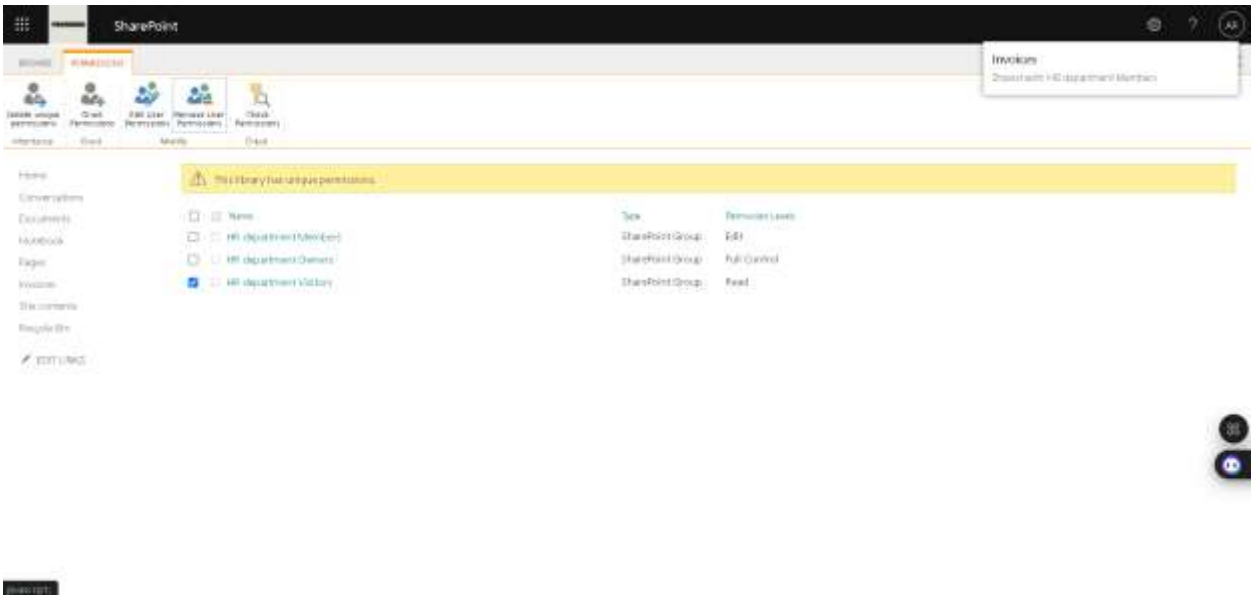
Step 8: Now, select under Permissions & Management ->permissions for this document library.



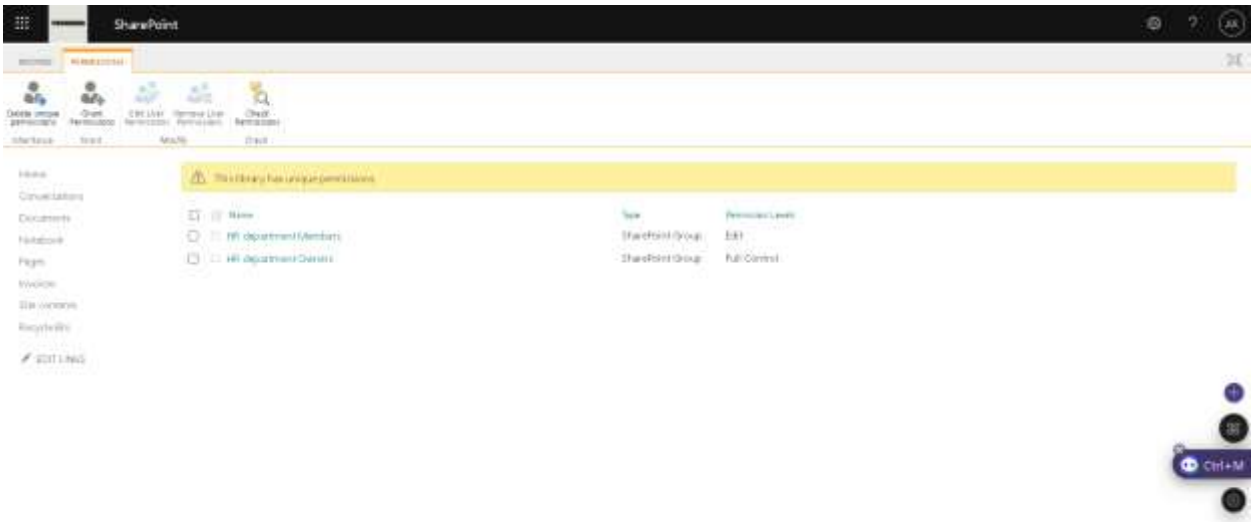
Step 9: First, click on stop inheriting permissions, so that we can add custom permissions to this library.



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

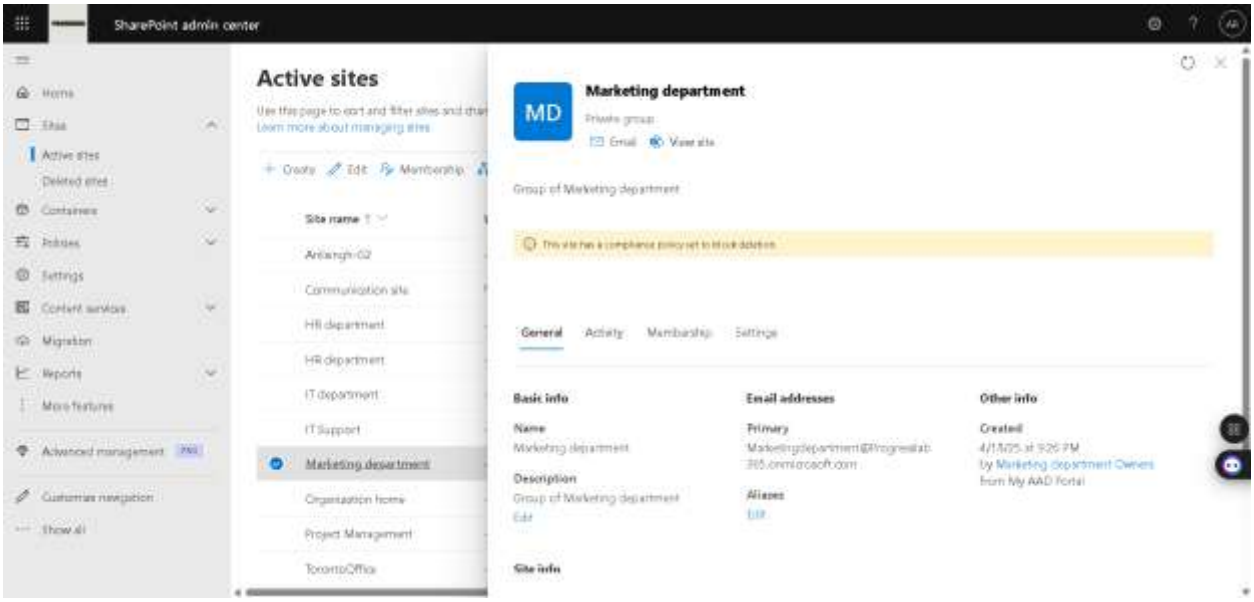


Step 11: Now for this library, we have only members which we need.

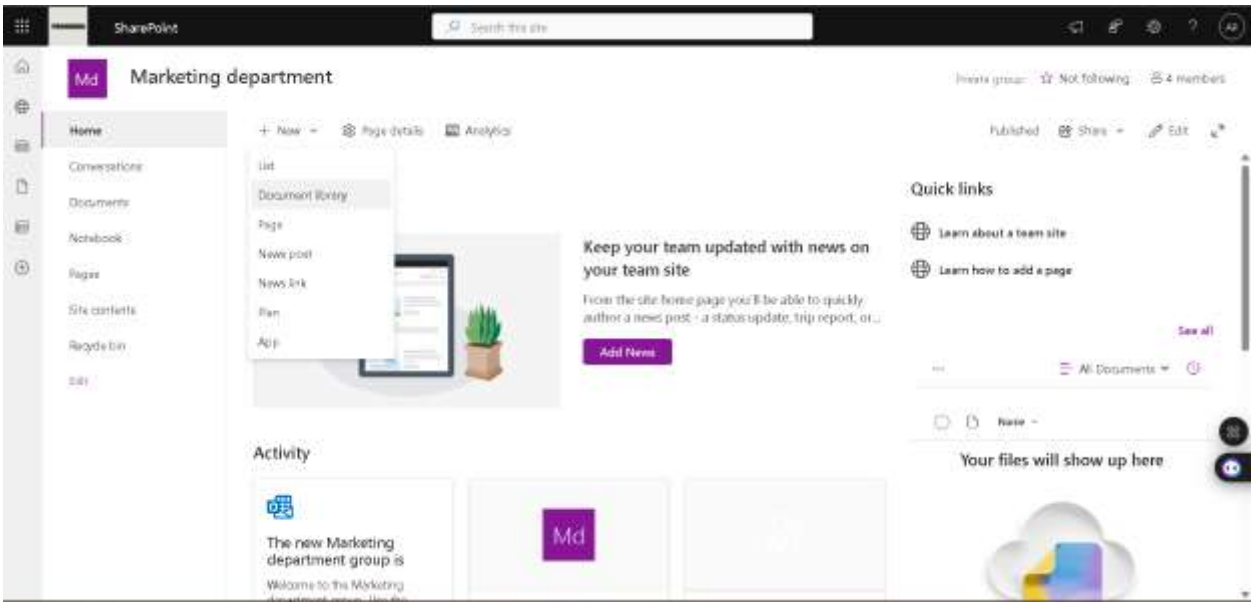


For Marketing department SharePoint

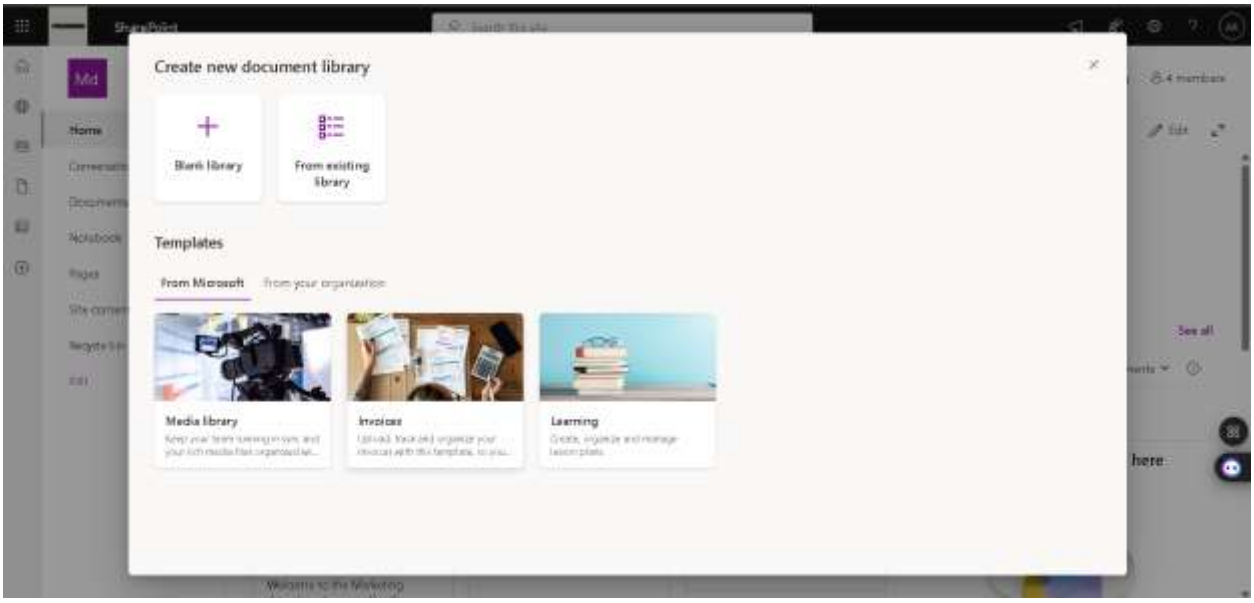
Step 1: From SharePoint admin center, go to sites -> active sites -> Marketing department -> View site.



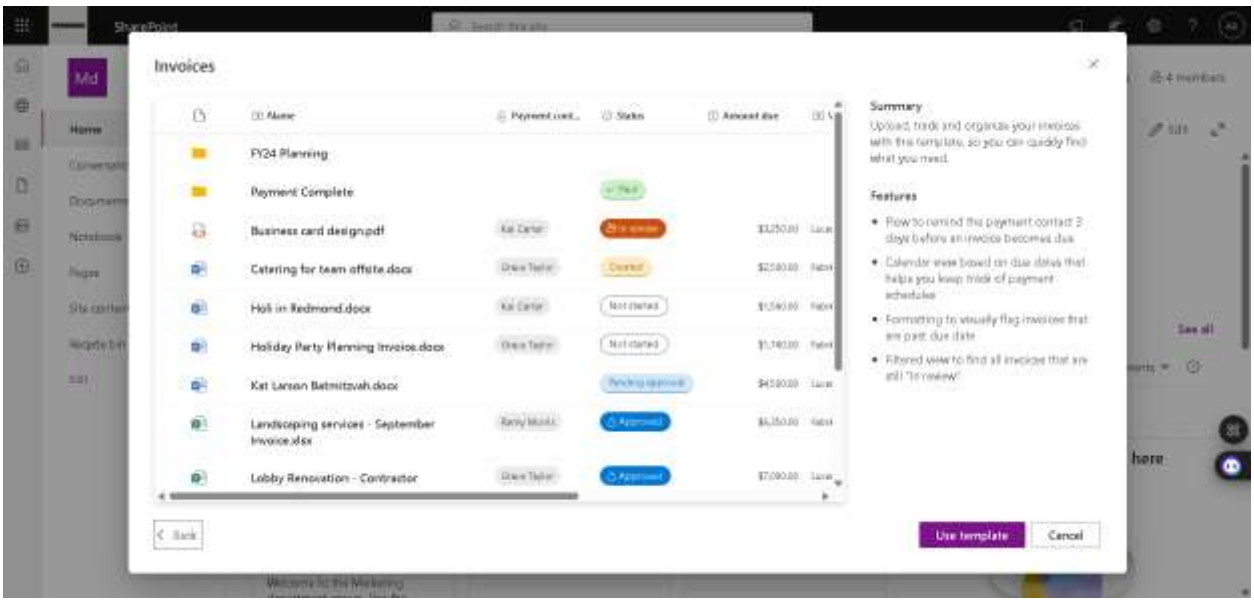
Step 2: Now from Marketing department SharePoint site, click on New -> Document library.



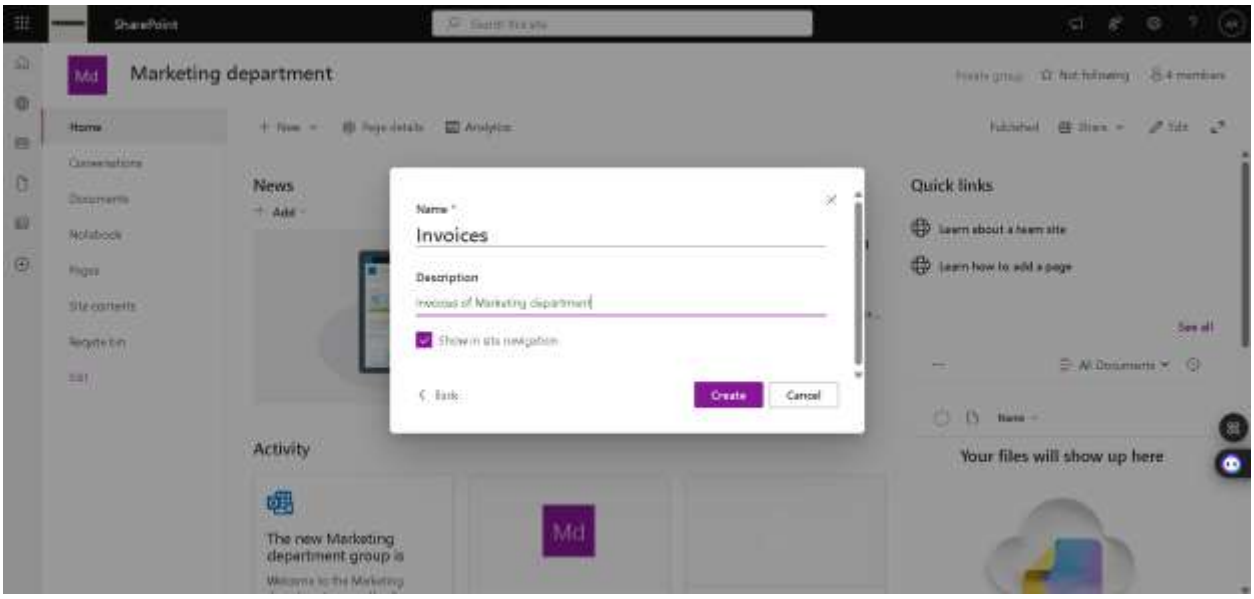
Step 3: We can select from template or create a blank library. We will select Invoices template.



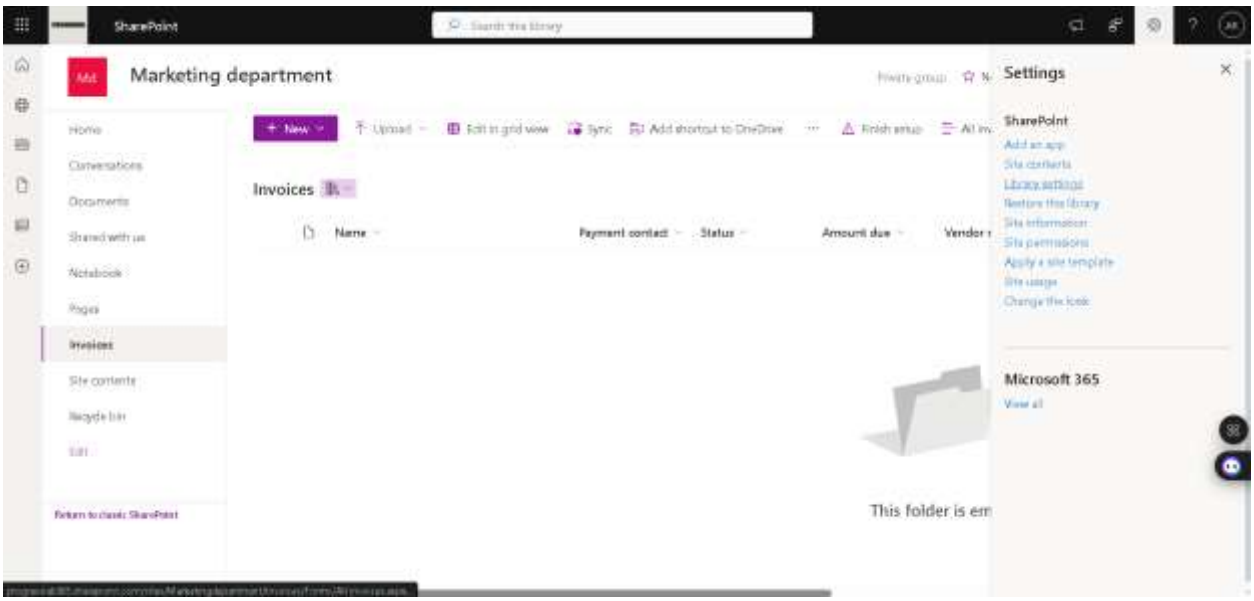
Step 4: We can see features of the template then click on use template.



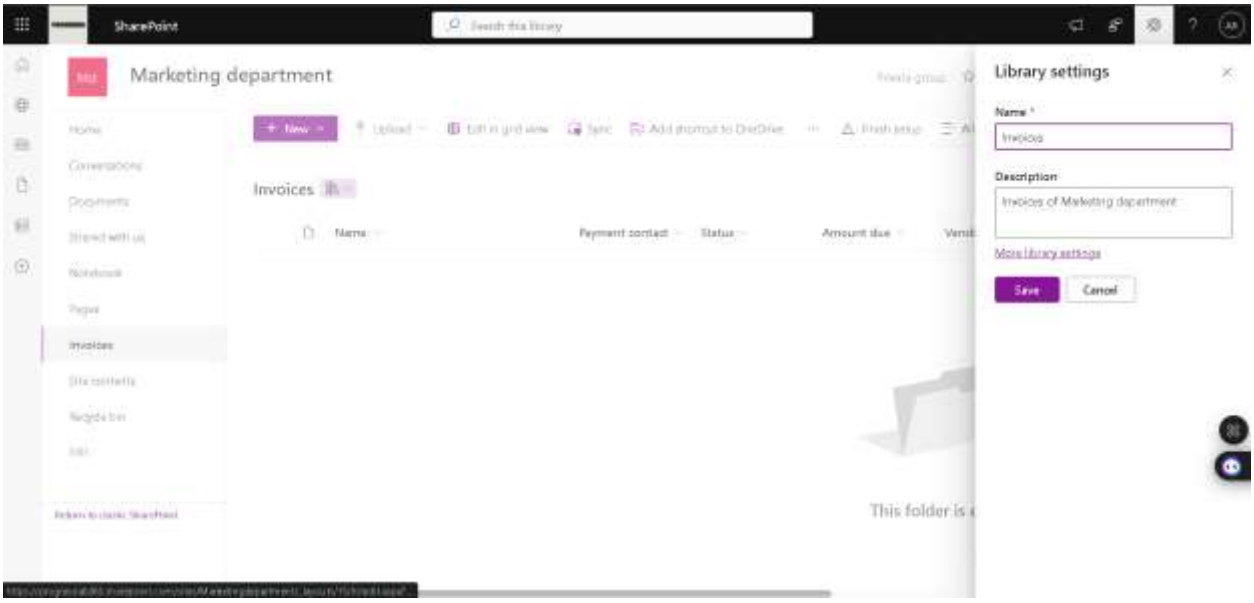
Step 5: We want to create a Invoices library, so fill name and description then create.



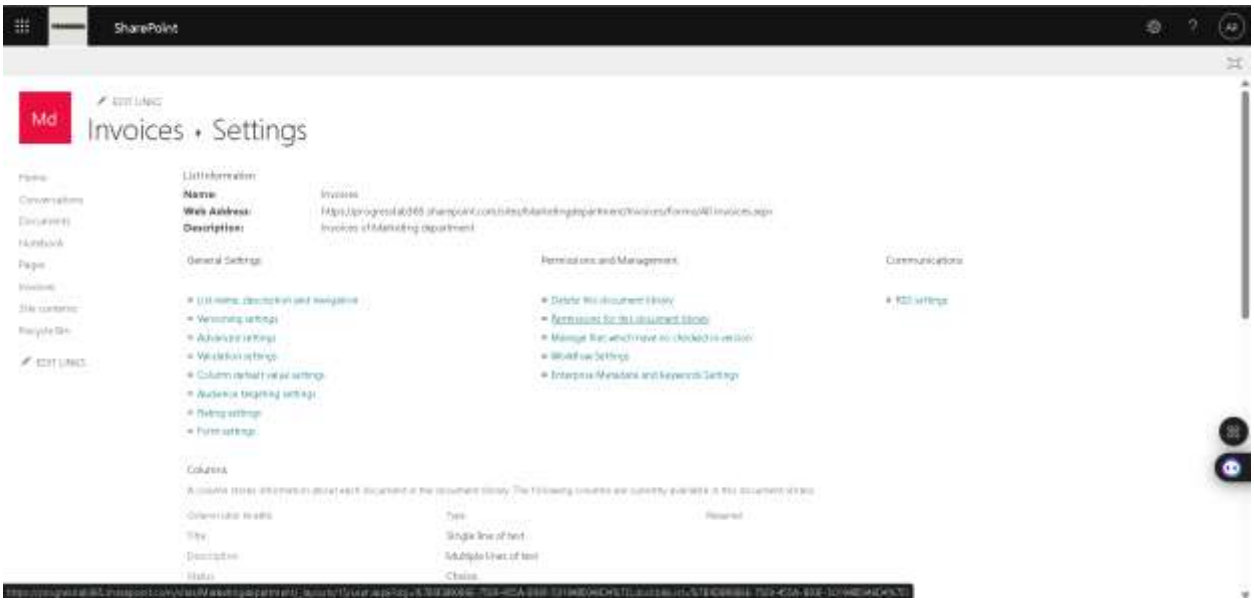
Step 6: Invoices library has been created, now select settings sign -> library settings.



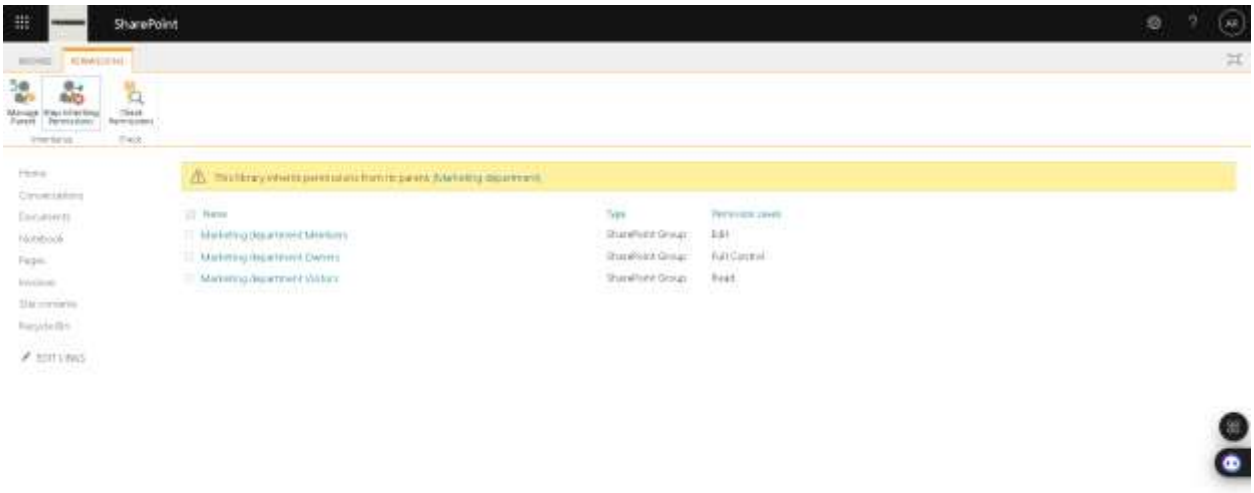
Step 7: Click on more library settings now.



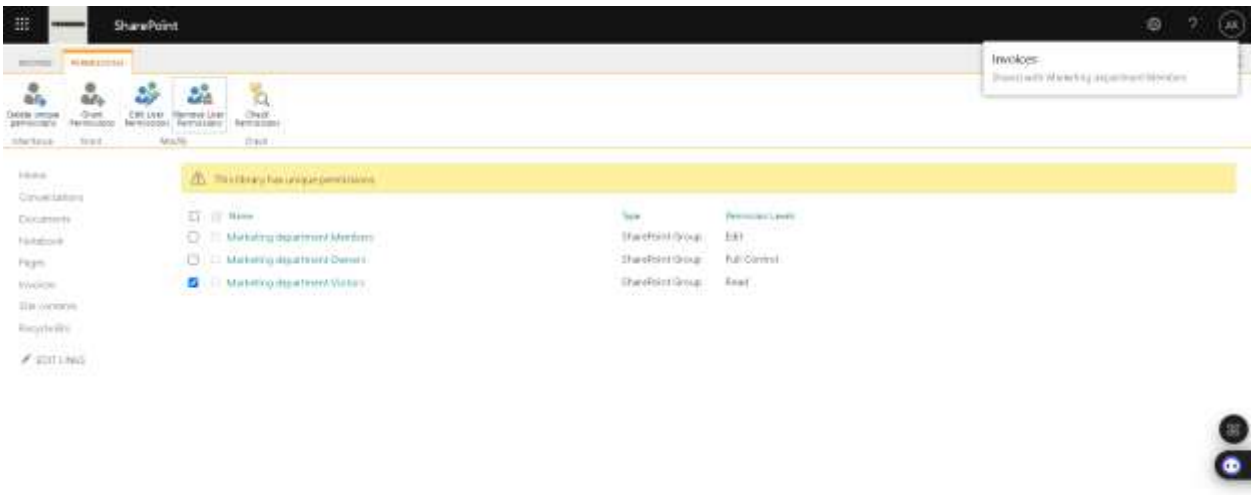
Step 8: Now, select under Permissions & Management ->permissions for this document library.



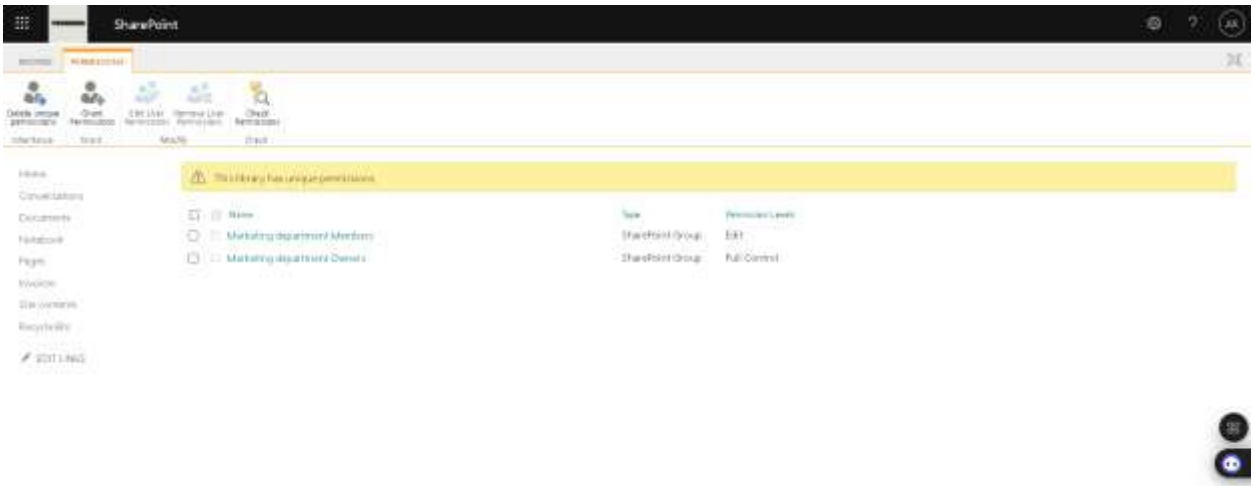
Step 9: First, click on stop inheriting permissions, so that we can add custom permissions to this library.



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.

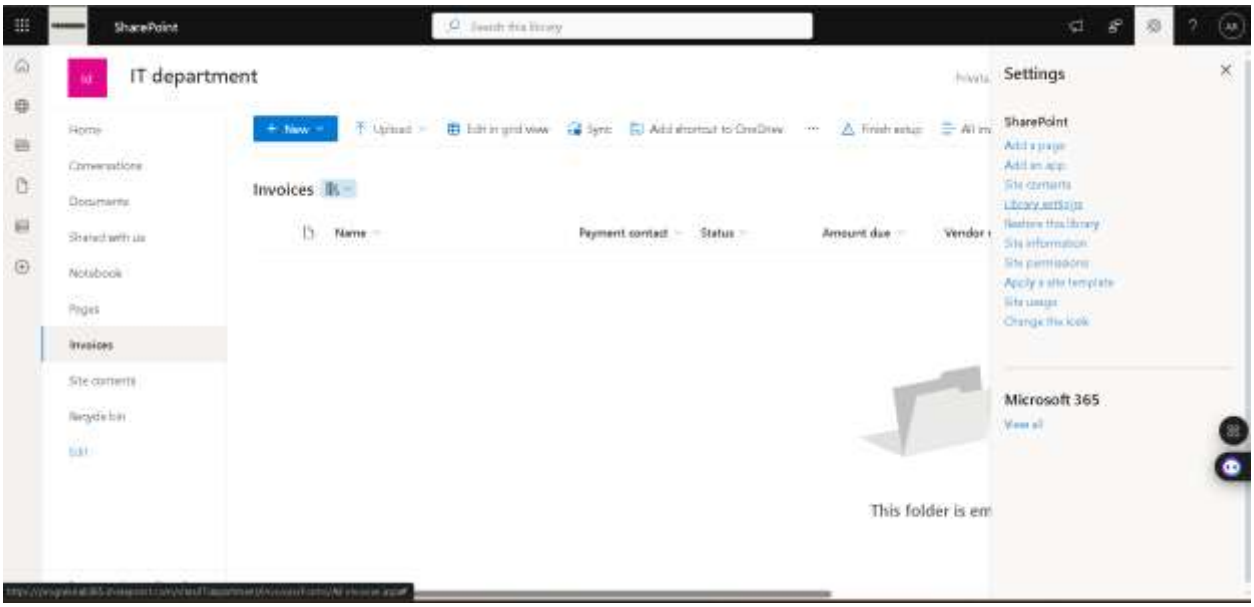


Step 11: Now for this library, we have only members which we need.

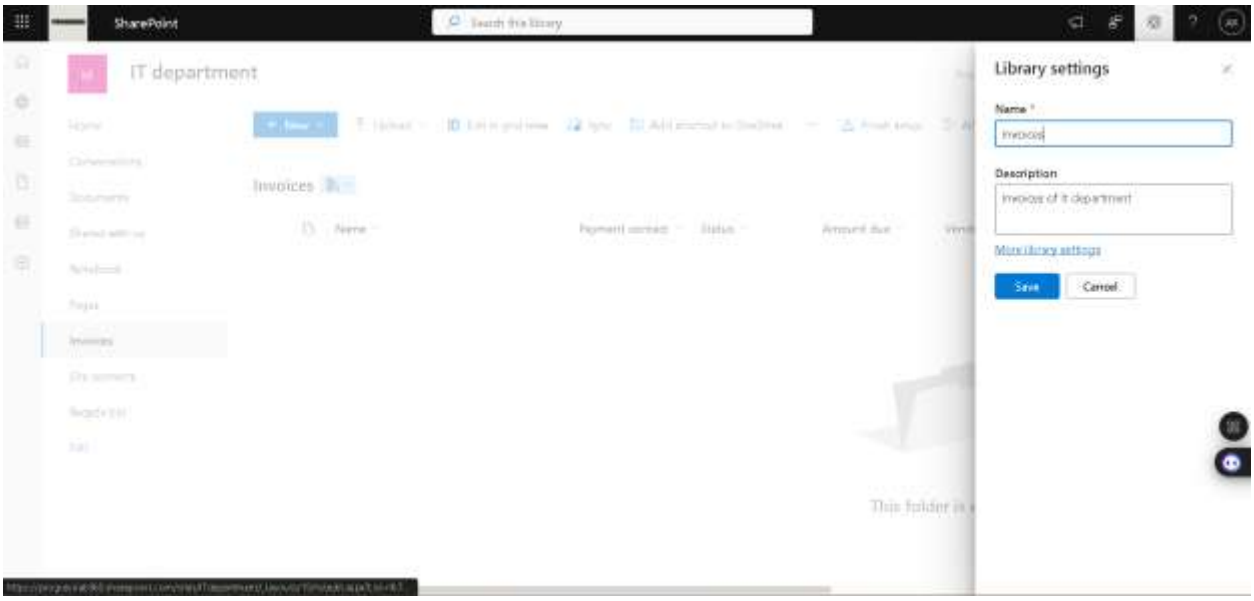


- Enable versioning and content approval for the HR document library.

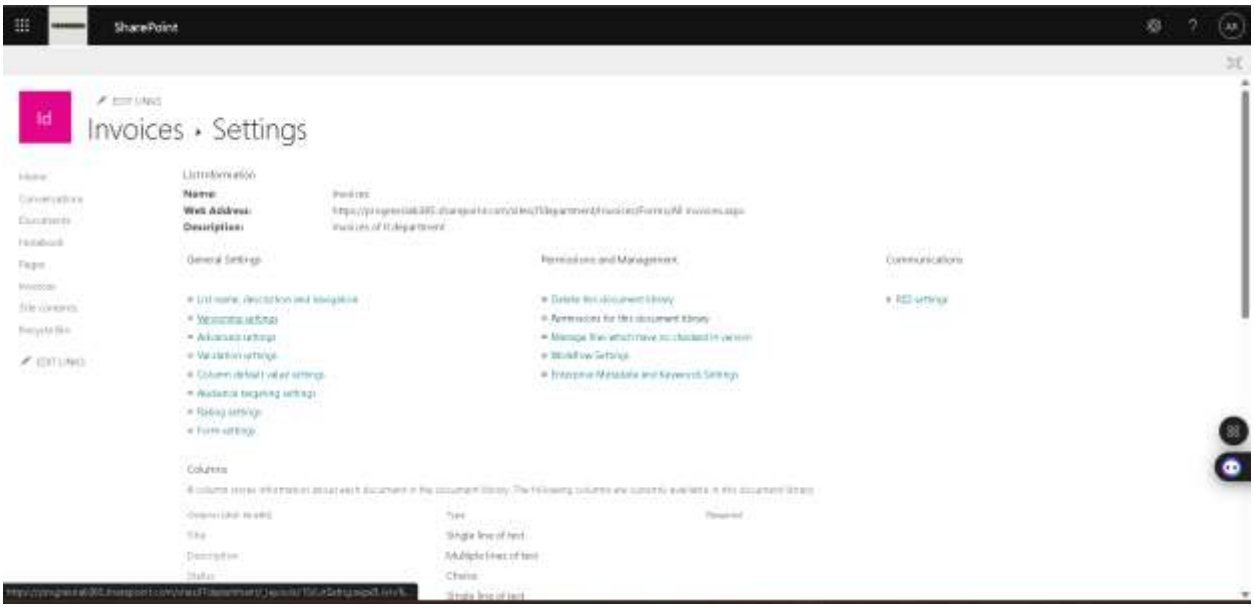
Step 1: We selected IT department SharePoint Site, under invoices (as we want to enable versioning and content approval) click on settings sign -> library settings.



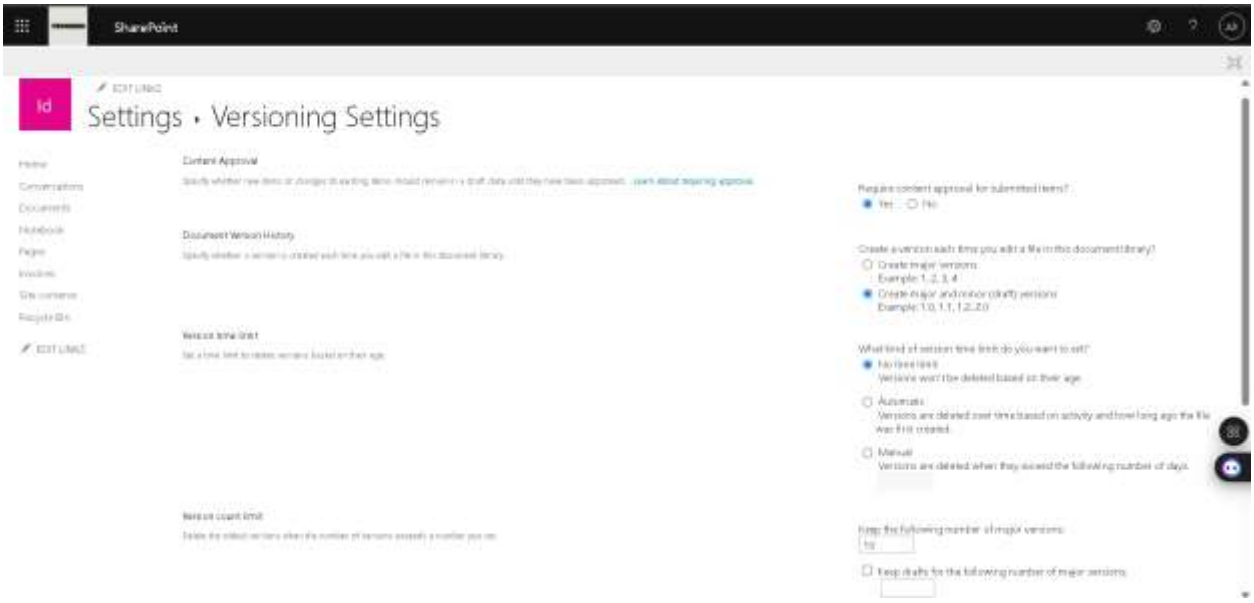
Step 2: Click on more library settings.



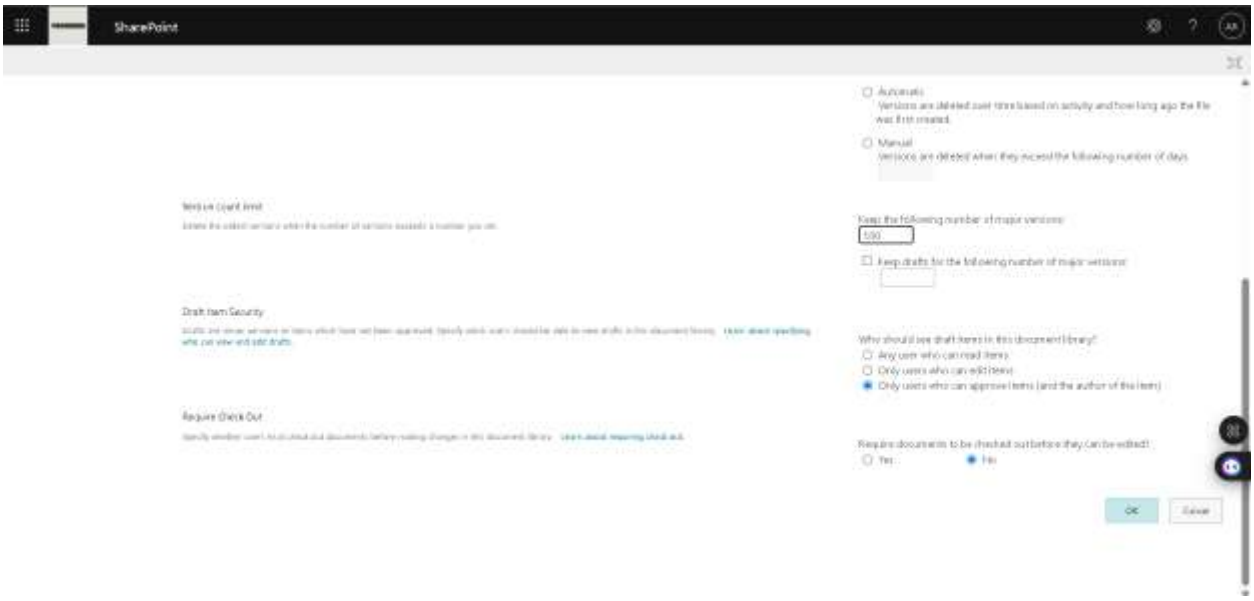
Step 3: Now under global settings, click on versioning settings.



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



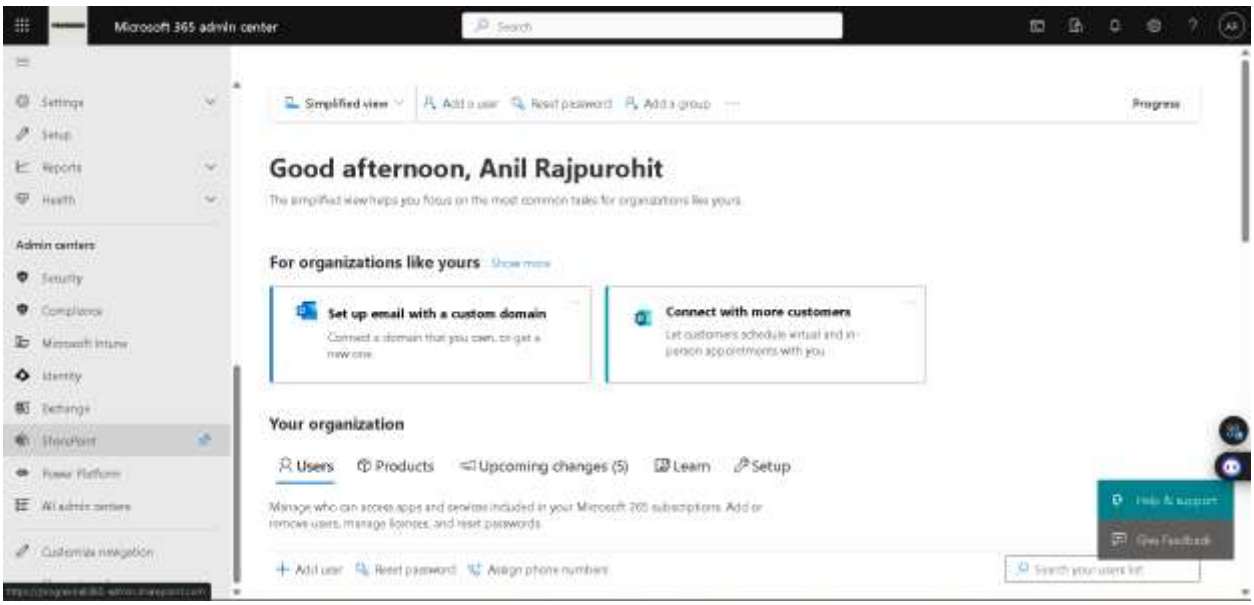
Step 5: We choose 100 as major version, as this is minimum limit and 500 is maximum. Select other settings then OK.



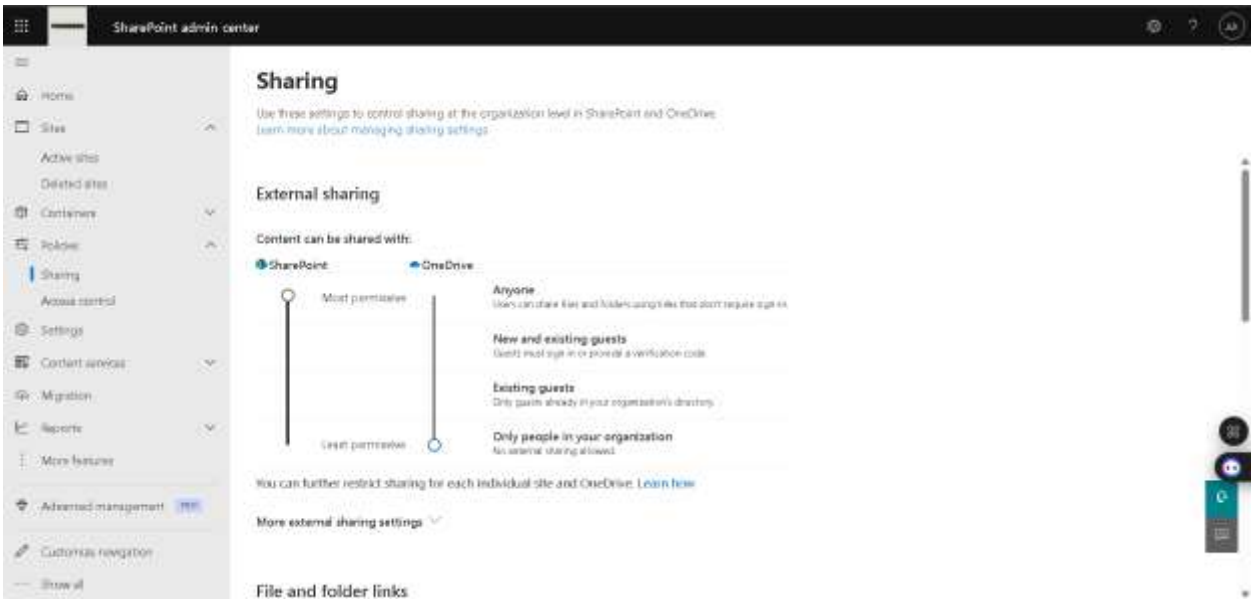
2. Implement OneDrive for Business:

- Configure OneDrive settings to restrict external sharing.

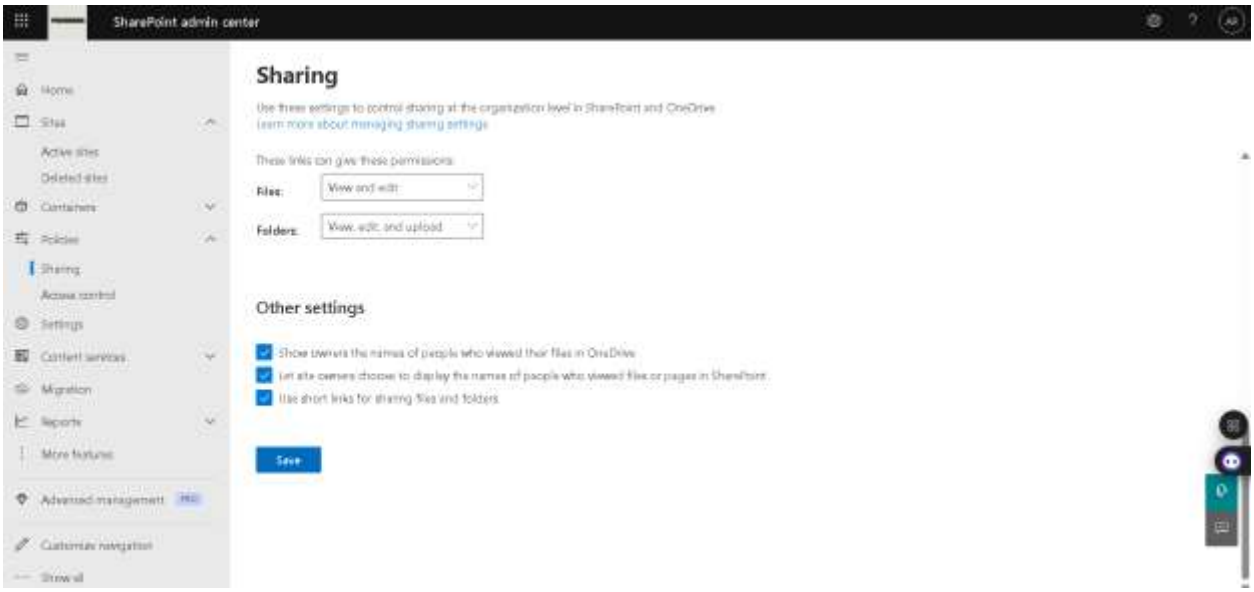
Step 1: From Microsoft 365 admin center, under admin centers -> SharePoint.



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.

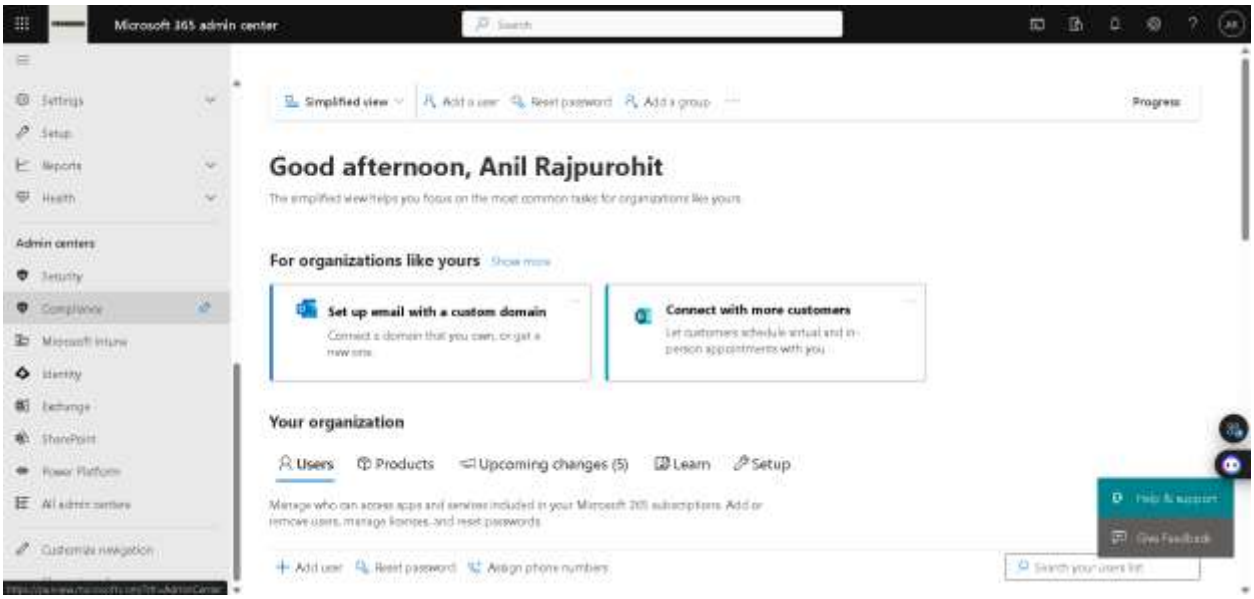


Step 3: Click on save to Save our OneDrive settings globally.

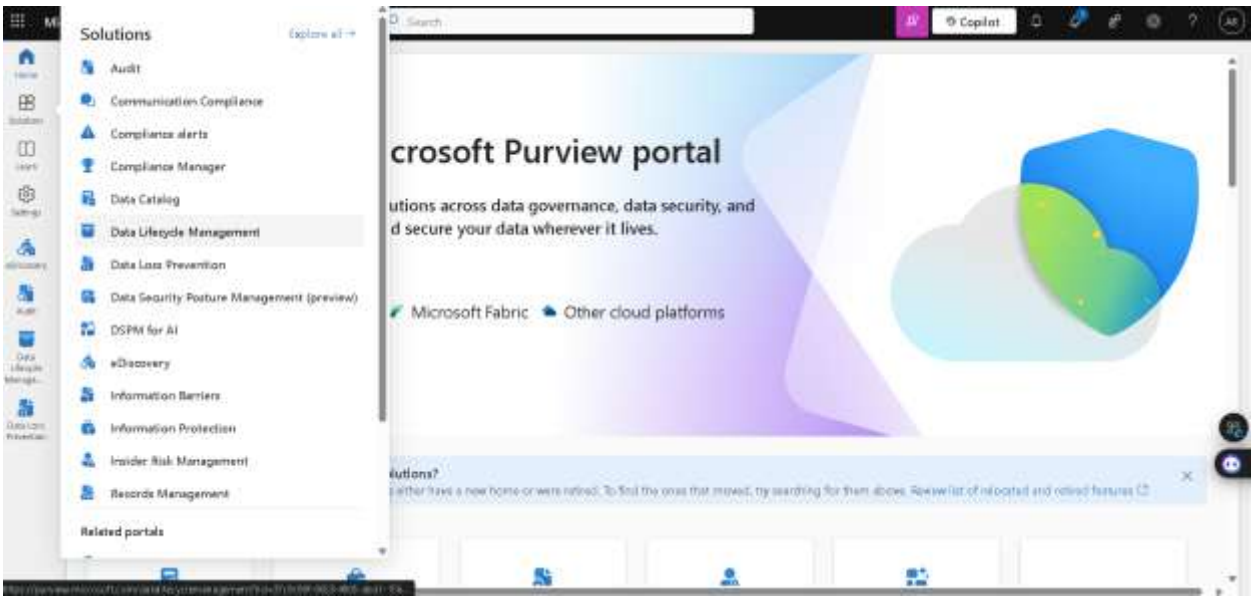


- Enable file retention policies to ensure data is retained for at least five years.

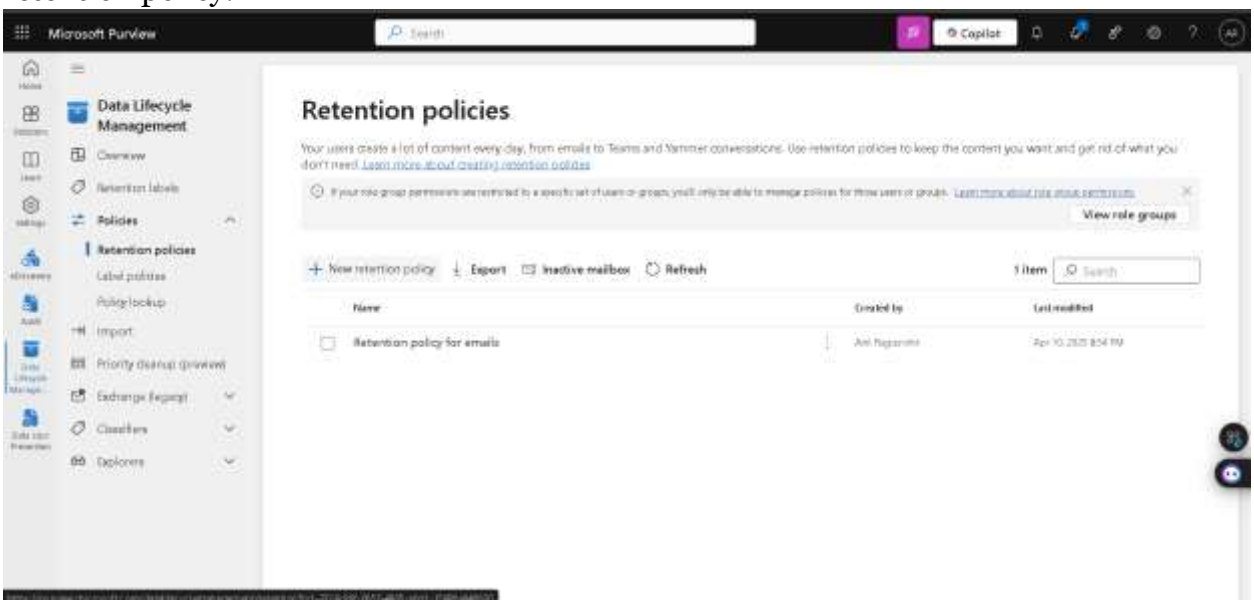
Step 1: From Microsoft 365 admin center, under admin centers select compliance to access Purview portal.



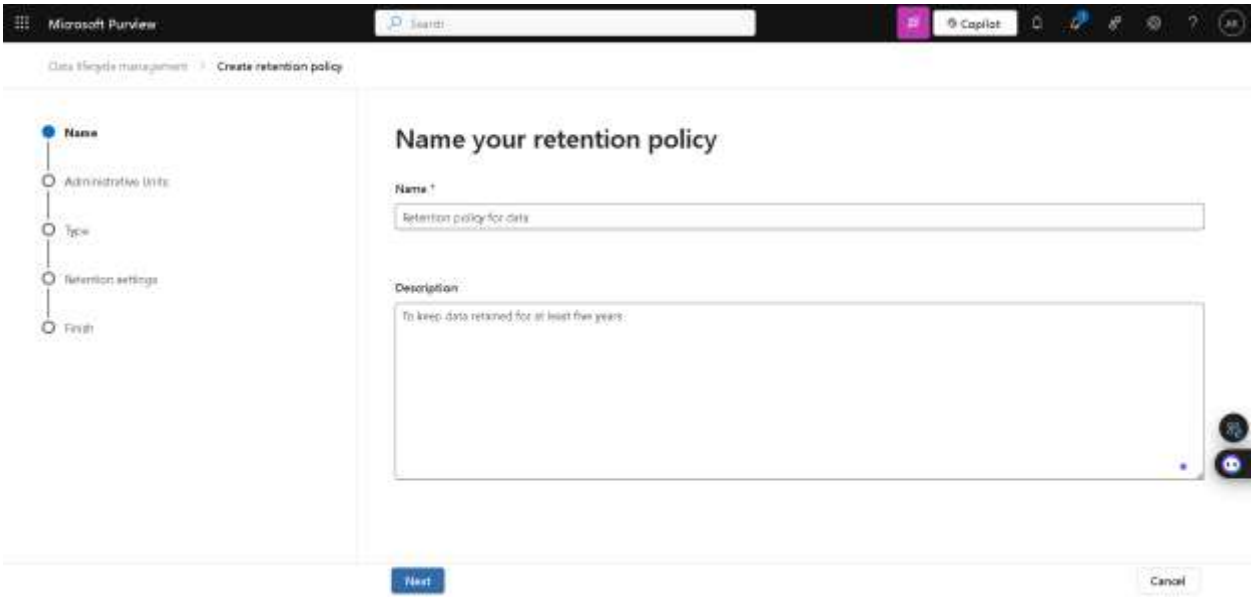
Step 2: To create retention policy for data. In Microsoft Purview, go to Solutions ->Data Lifecycle Management.



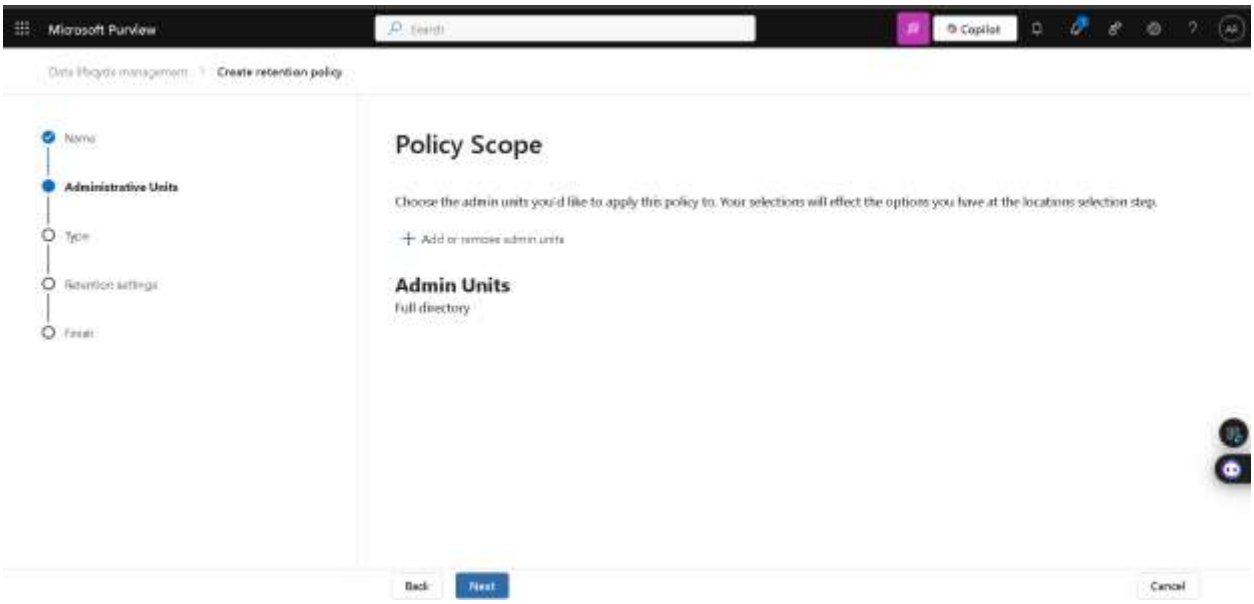
Step 3: In Data Lifecycle Management, under policies -> retention policies -> New retention policy.



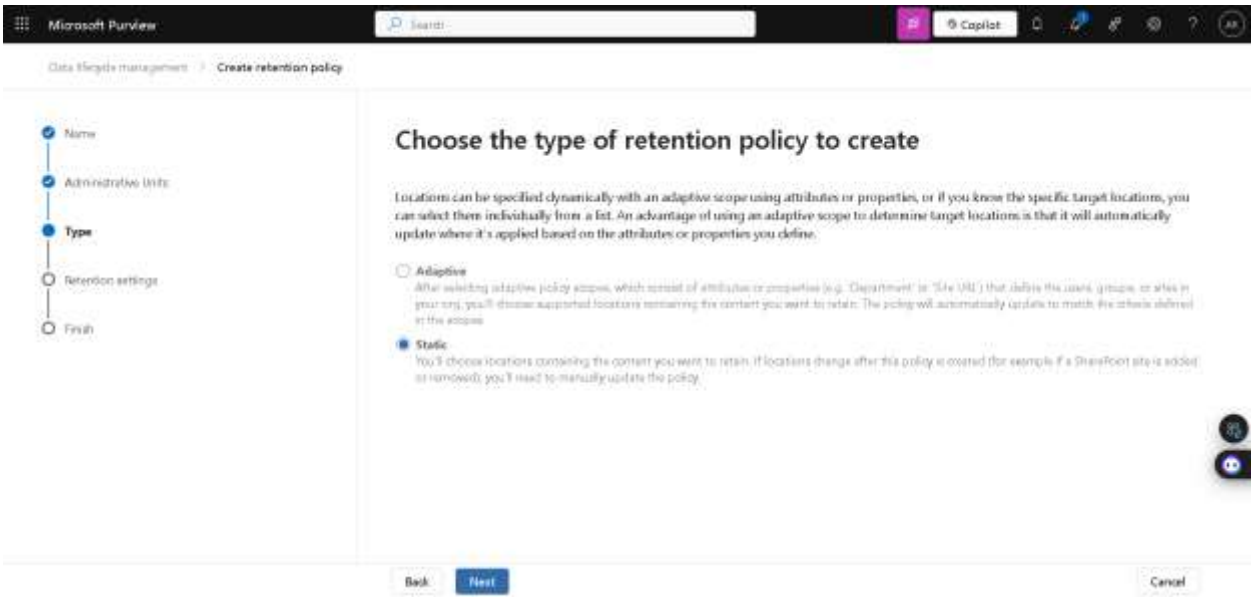
Step 4: Provide name and description for your retention policy.



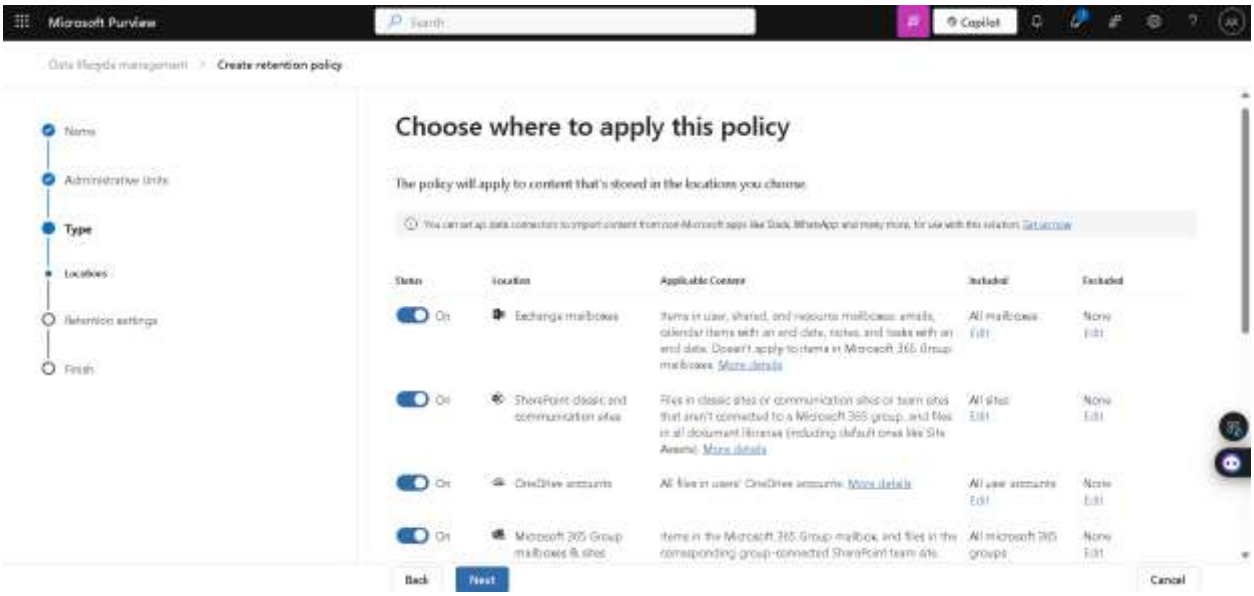
Step 5: As we haven't created anu admin units, we won't be able to assign any admin units here. So, we keep it as full directory and click on next.



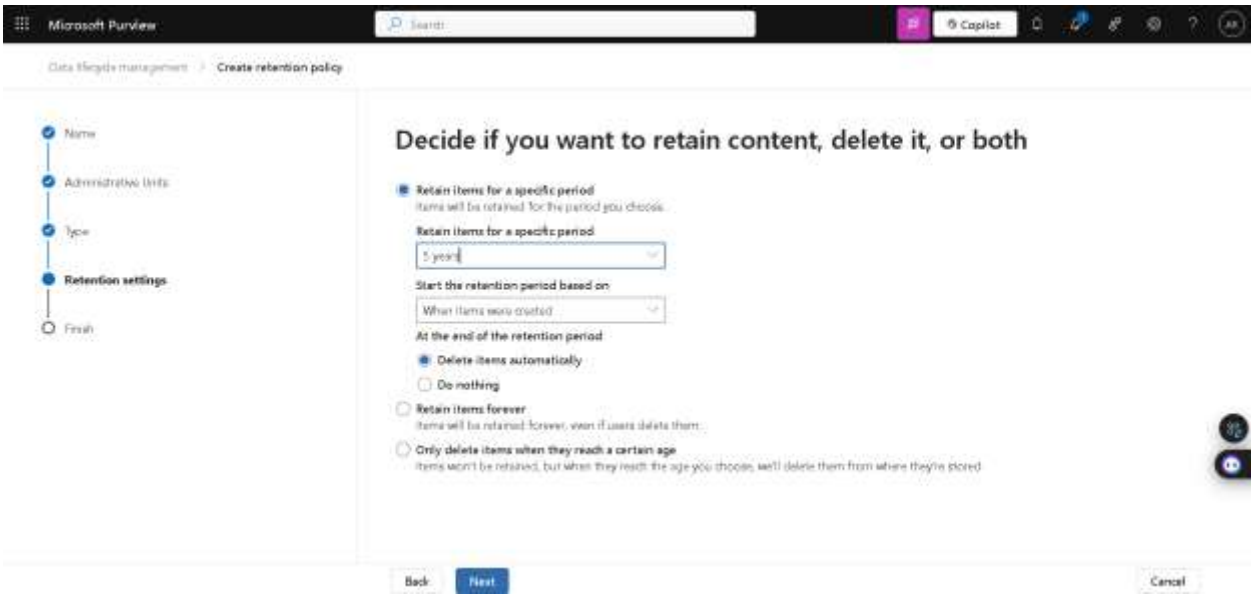
Step 6: Now we have two options adaptive and static, adaptive is better overall as it will update with our attributes and properties. But we are going with static and click on next.



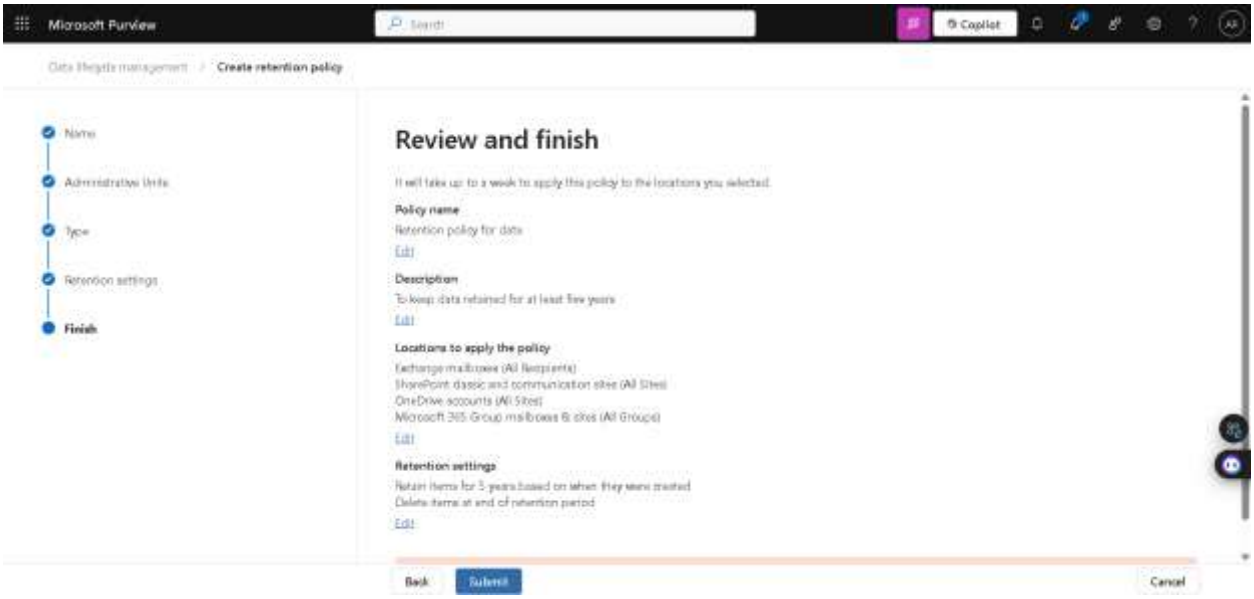
Step 7: Choose all locations where we want to apply this policy, then click in next.



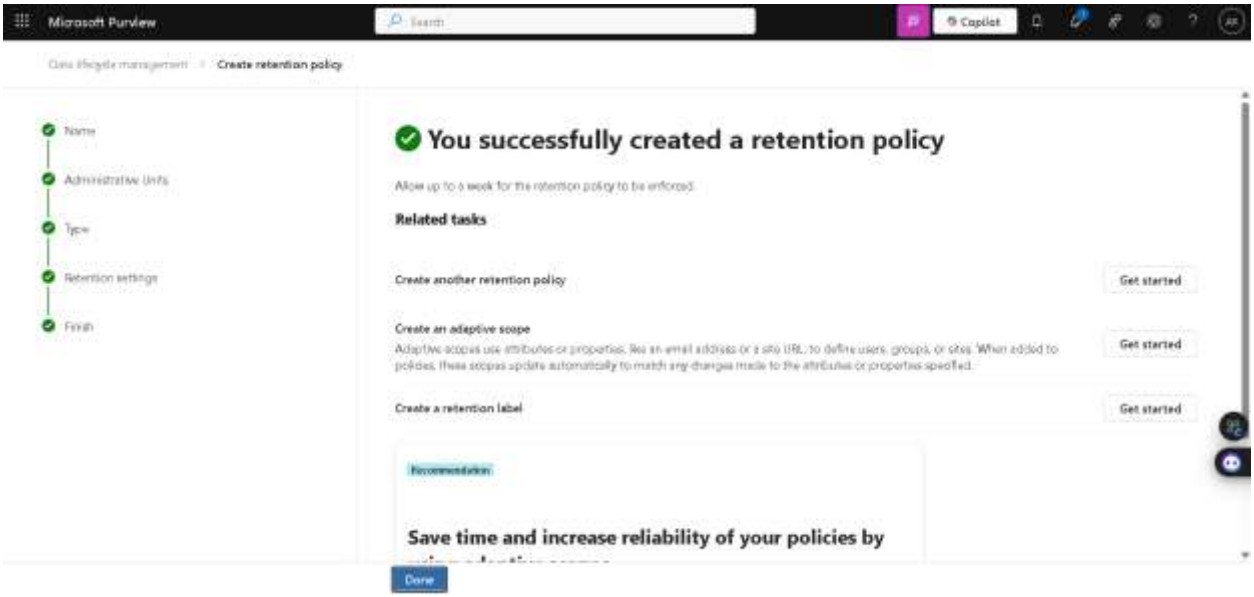
Step 8: Now, we can set the retention period here, So we go to retain items for a specific period ->5 years.



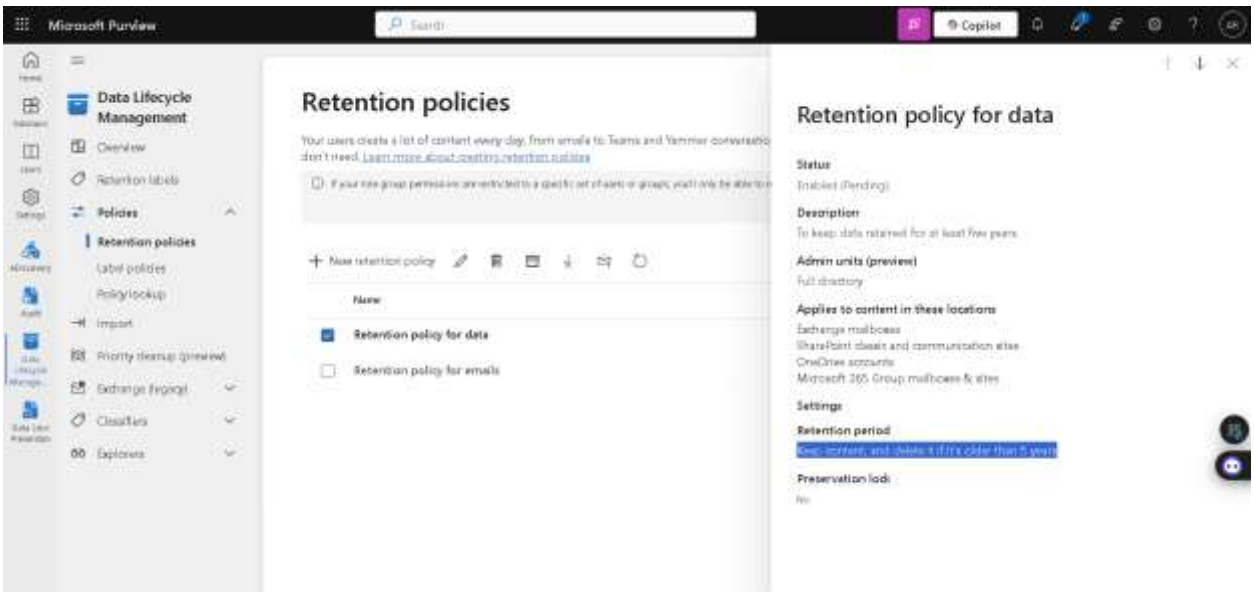
Step 9: Here we will review the policy details and click on Submit.



Step 10: Our retention has been successfully created.



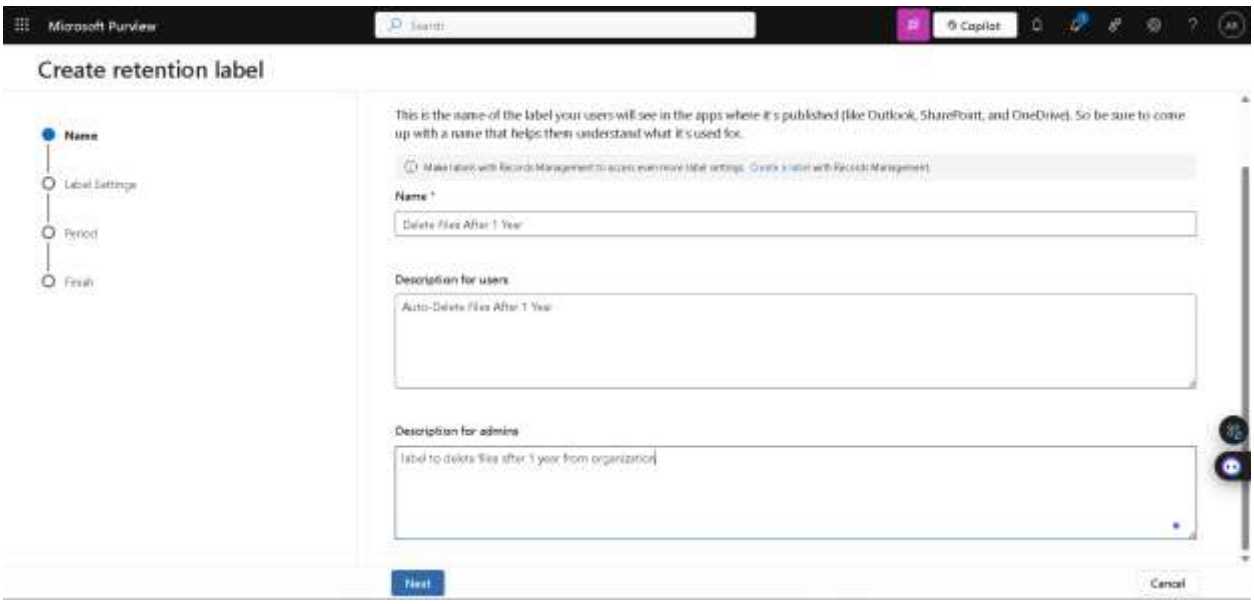
Step 11: We can view our policy now under Retention policies.



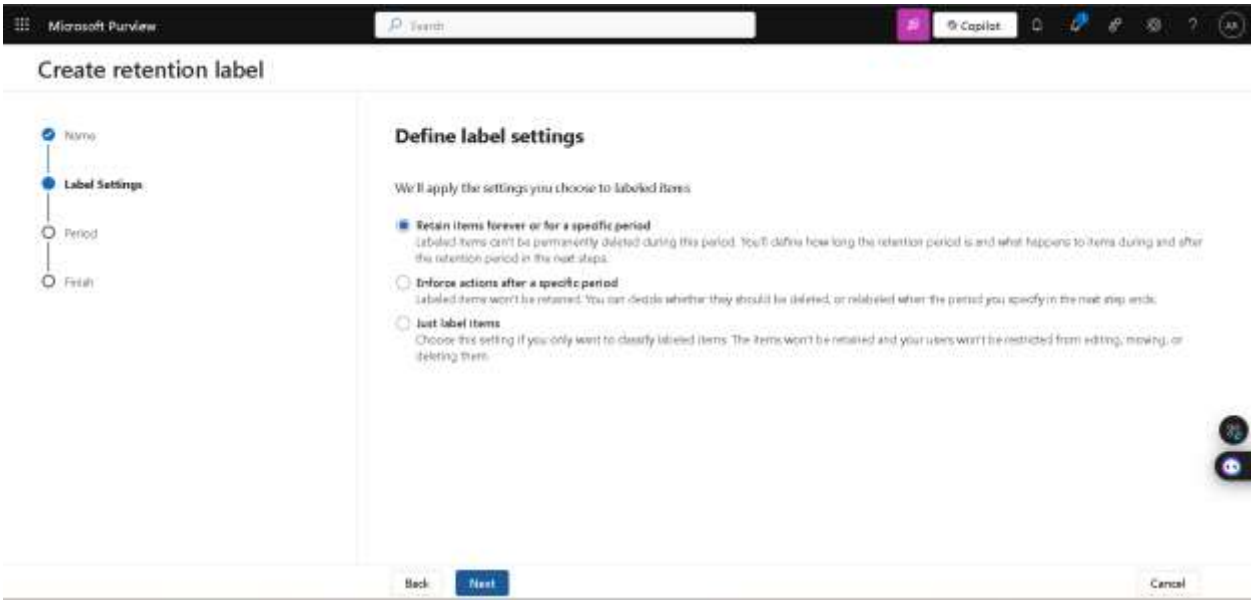
- Set up a policy to automatically move old files to the Recycle Bin after a year.

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

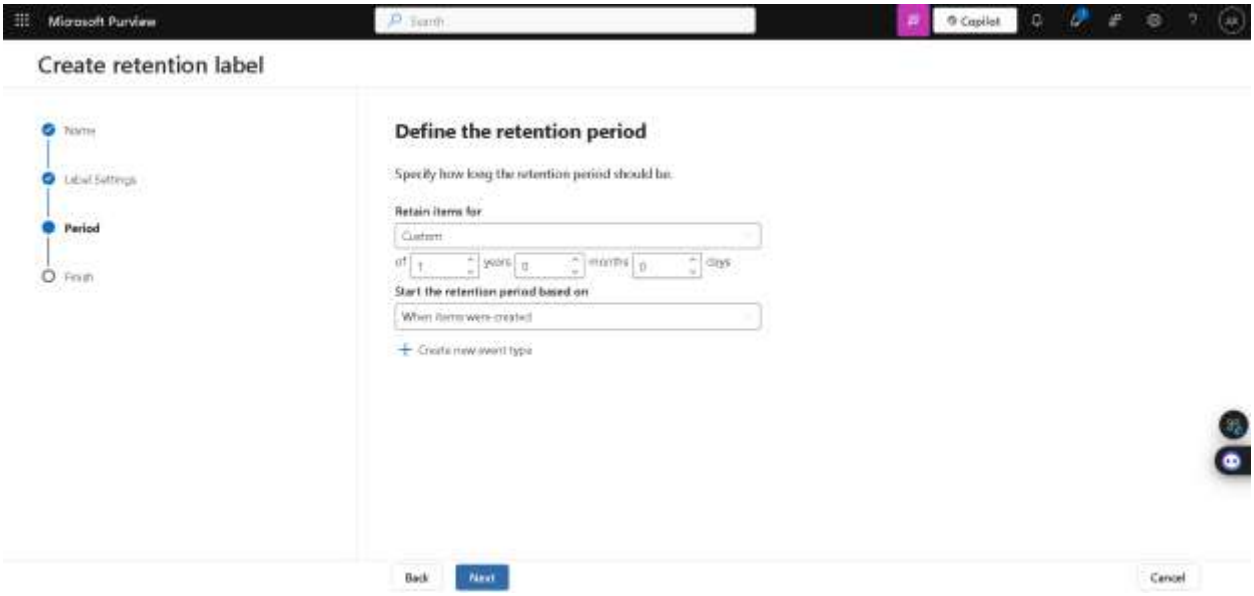
Step 2: Fill all the details here like name, description, and description for admins then Next.



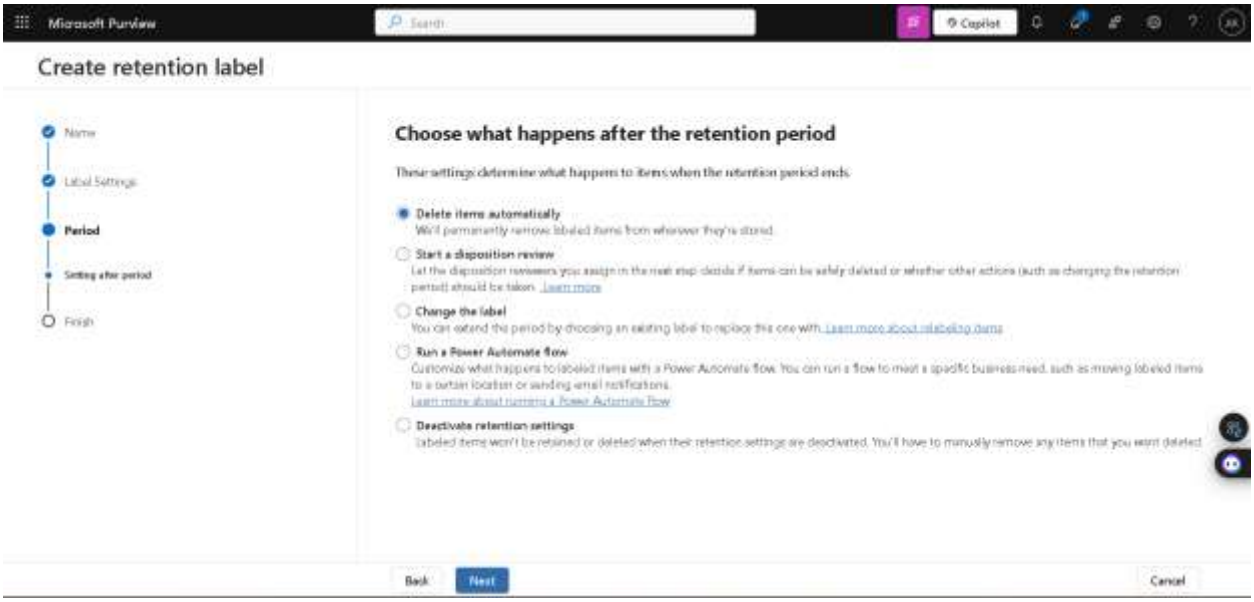
Step 3: Select, retain items forever or a specific period then click on Next.



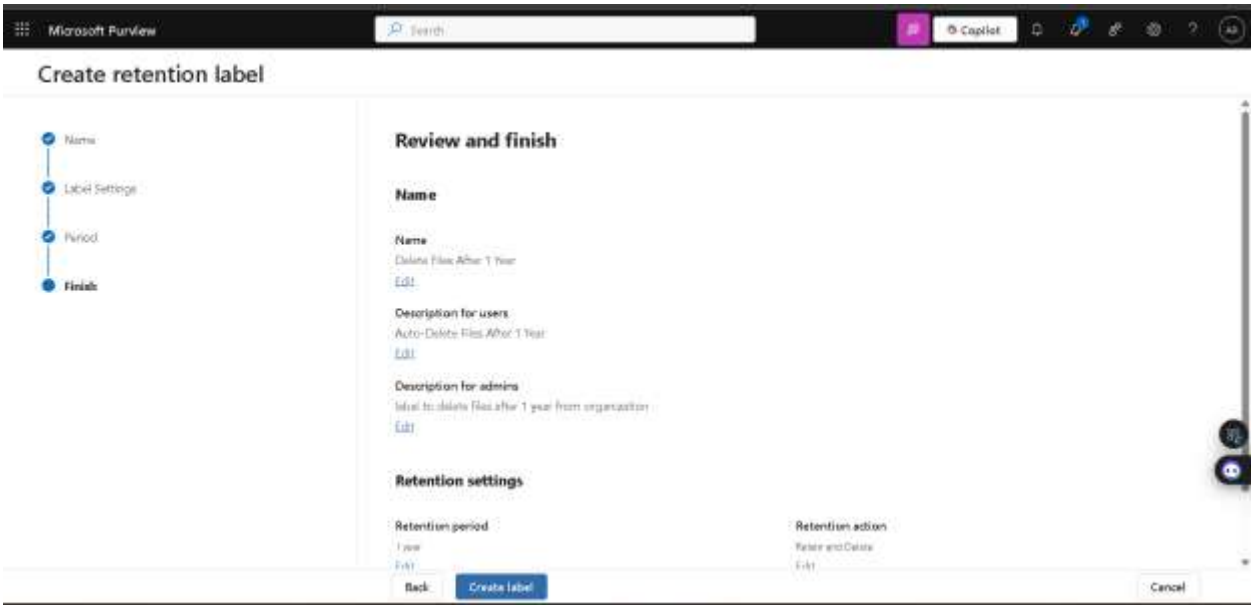
Step 4: Now, as we only want to retain old files for one year then move to recycle bin. Select, retain items as 1 year then next.



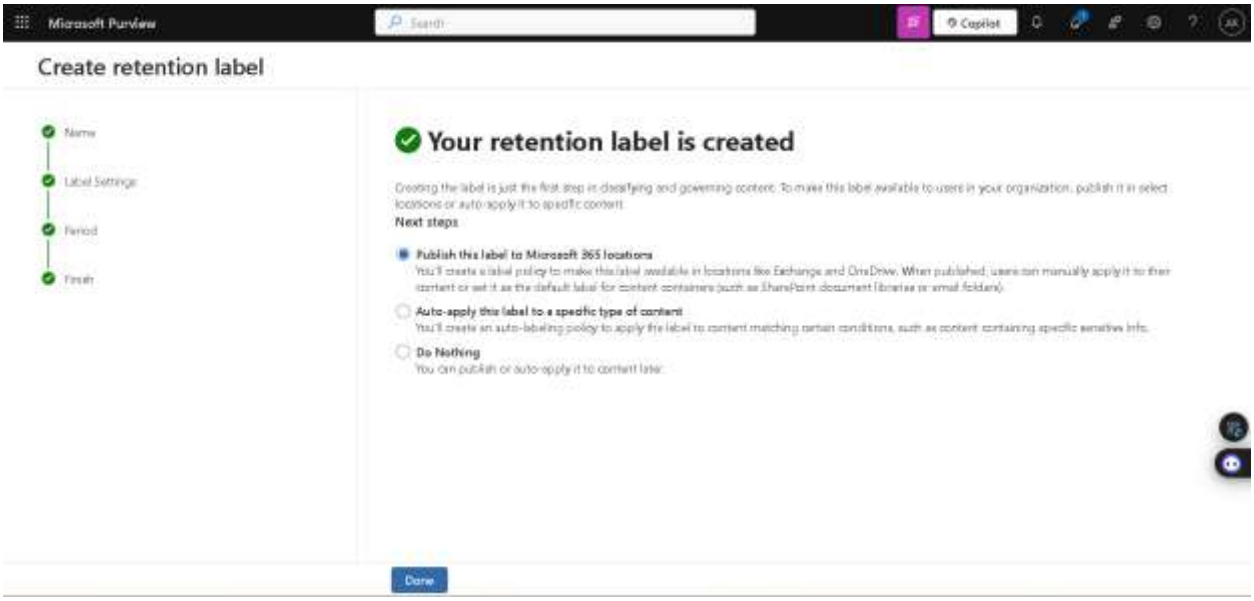
Step 5: This label won't send files to the Recycle Bin literally, but it **deletes** them after a year — files then go to the **Recycle Bin**, where they remain for 93 days by default. Now select delete items automatically then next.



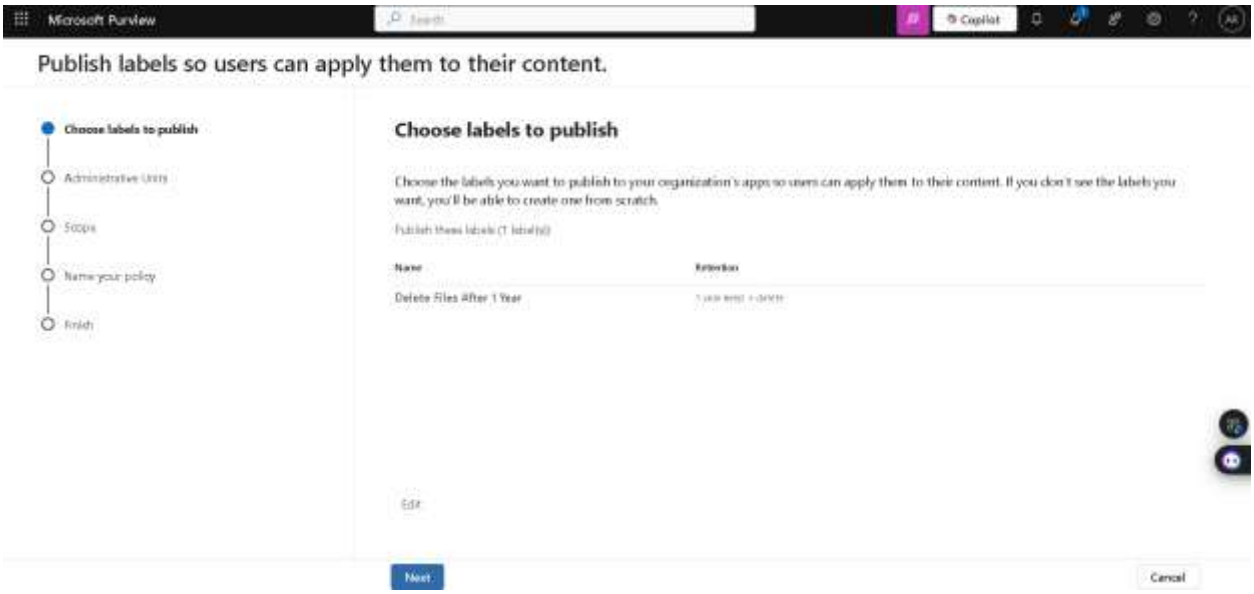
Step 6: Review retention label details then click on create label.



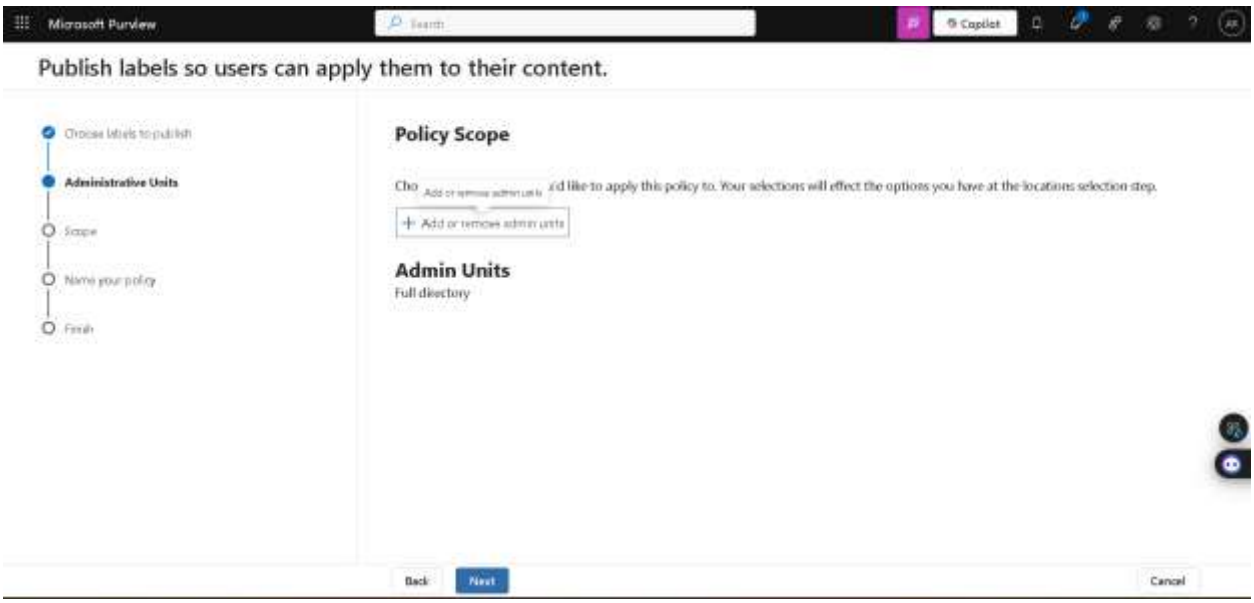
Step 7: Our retention label has been successfully created, now select publish this label to Microsoft 365 locations then done.



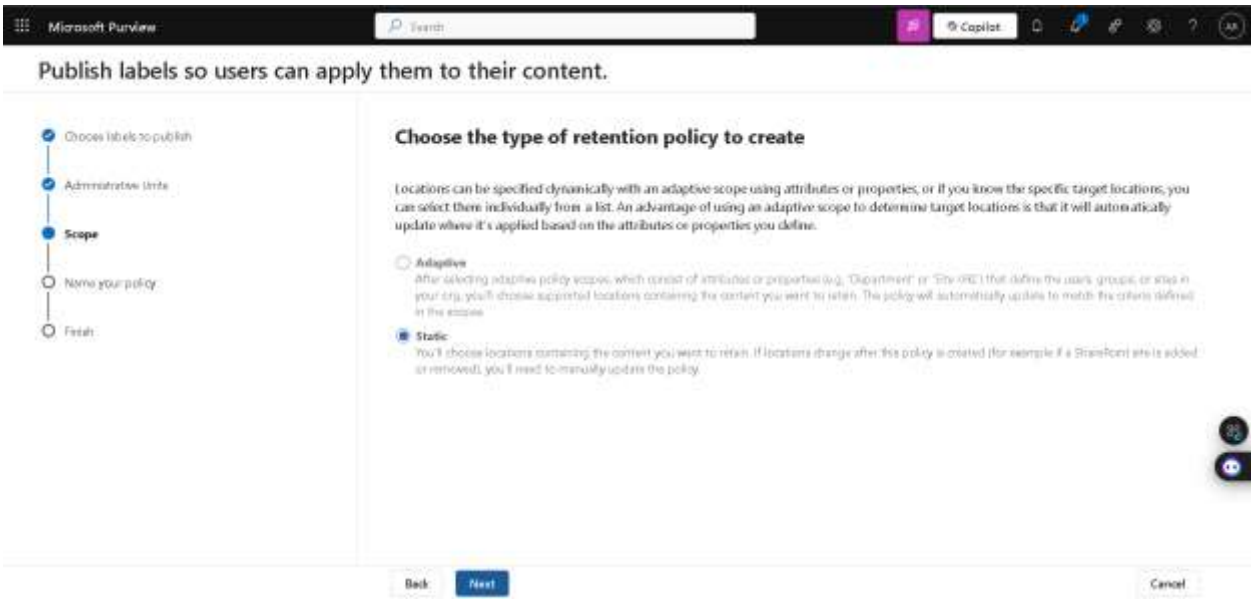
Step 8: Now we are using this label to create the policy, click on next.



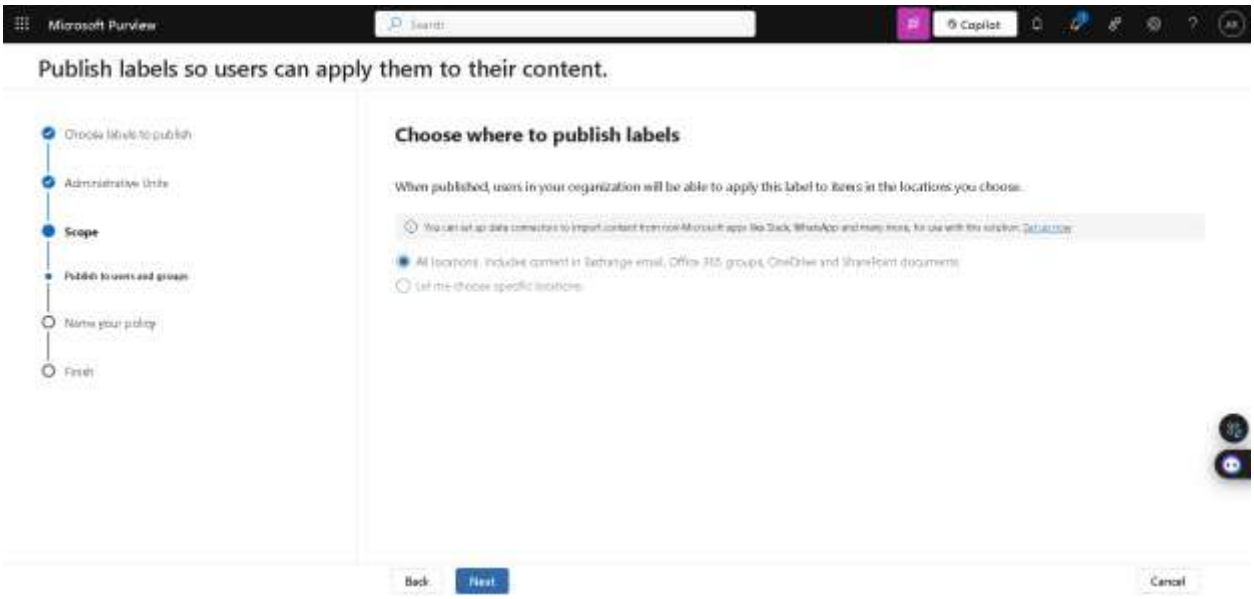
Step 9: As we want to apply this policy to whole organization, we keep it as full directory then next.



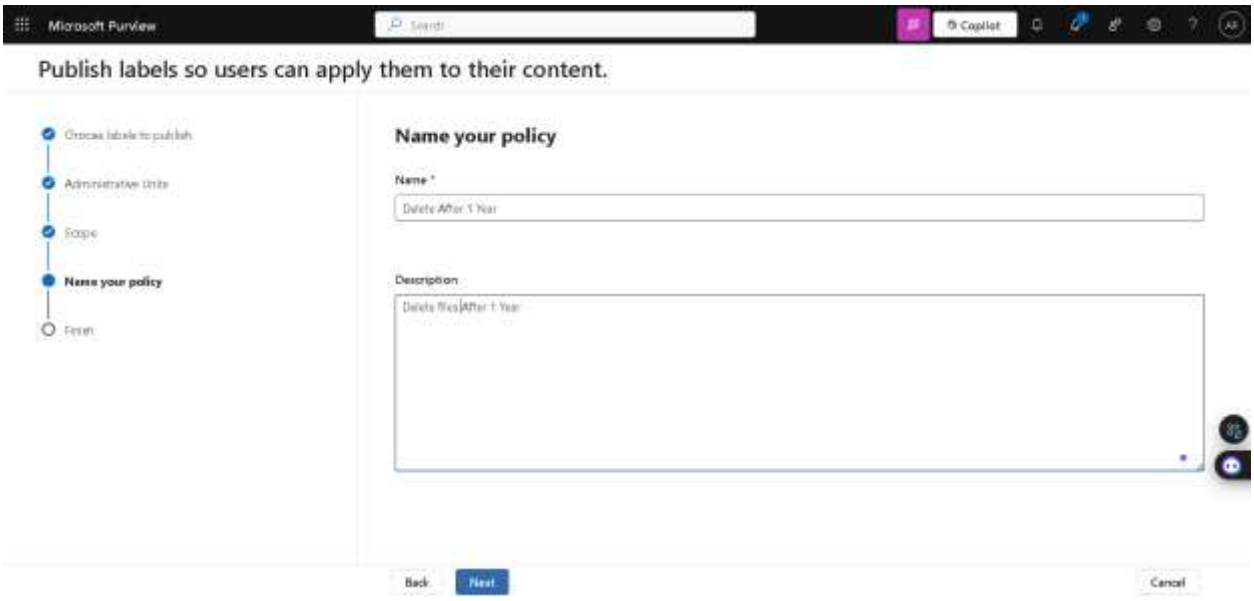
Step 10: Now we have two options adaptive and static, adaptive is better overall as it will update with our attributes and properties. But we are going with static and click on next.



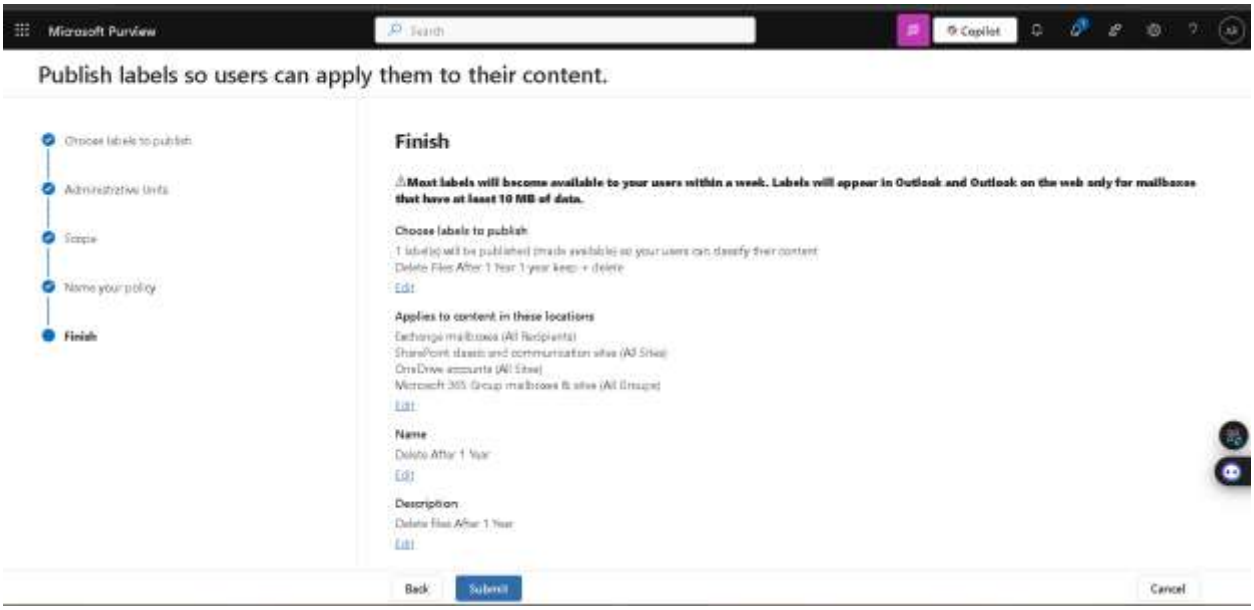
Step 11: We will publish this policy to all locations, then click on next.



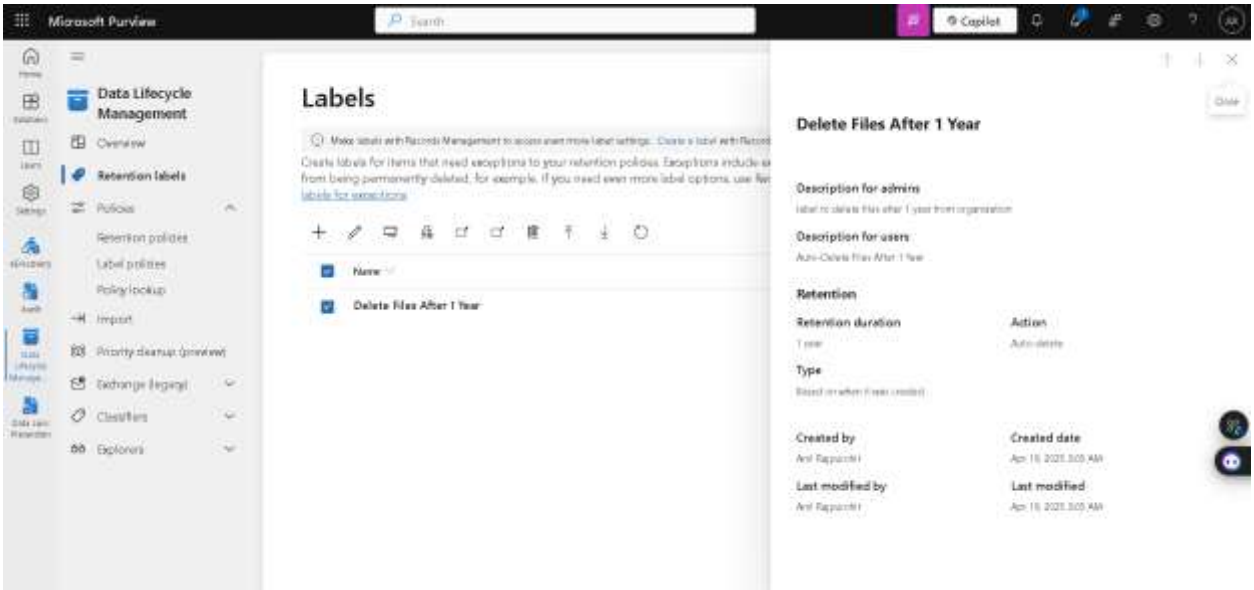
Step 12: Provide name and description for the new policy then next.



Step 13: Review policy details and click on submit.



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

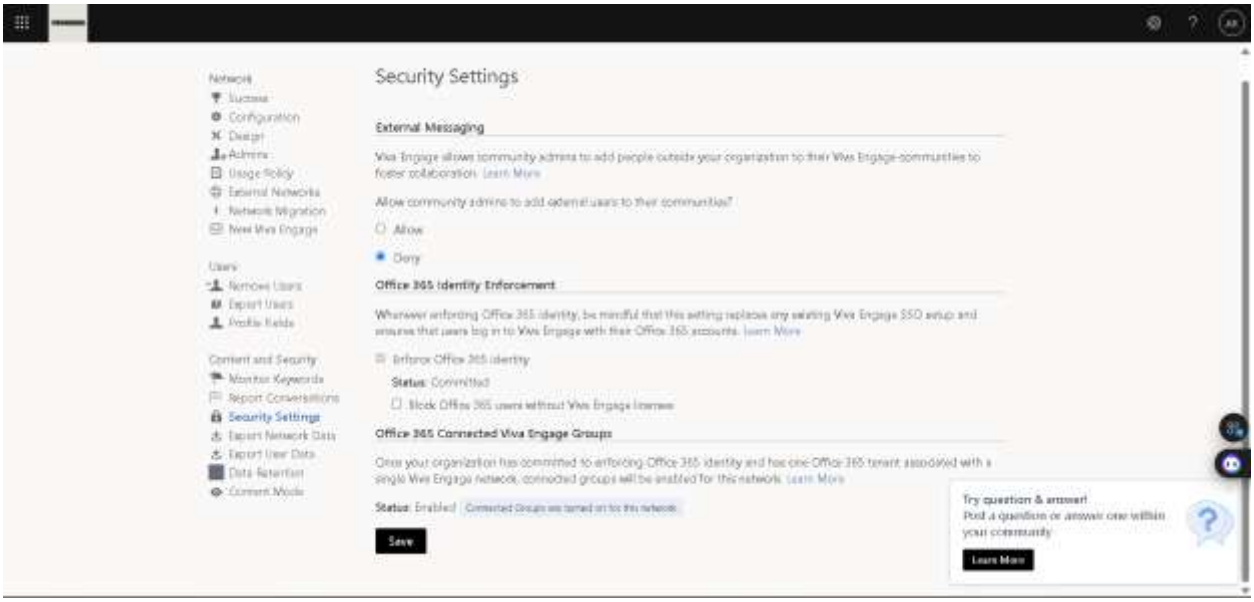


3. Set Up Viva Engage for Enterprise Social Networking:

- Configure Viva to allow only internal communications.

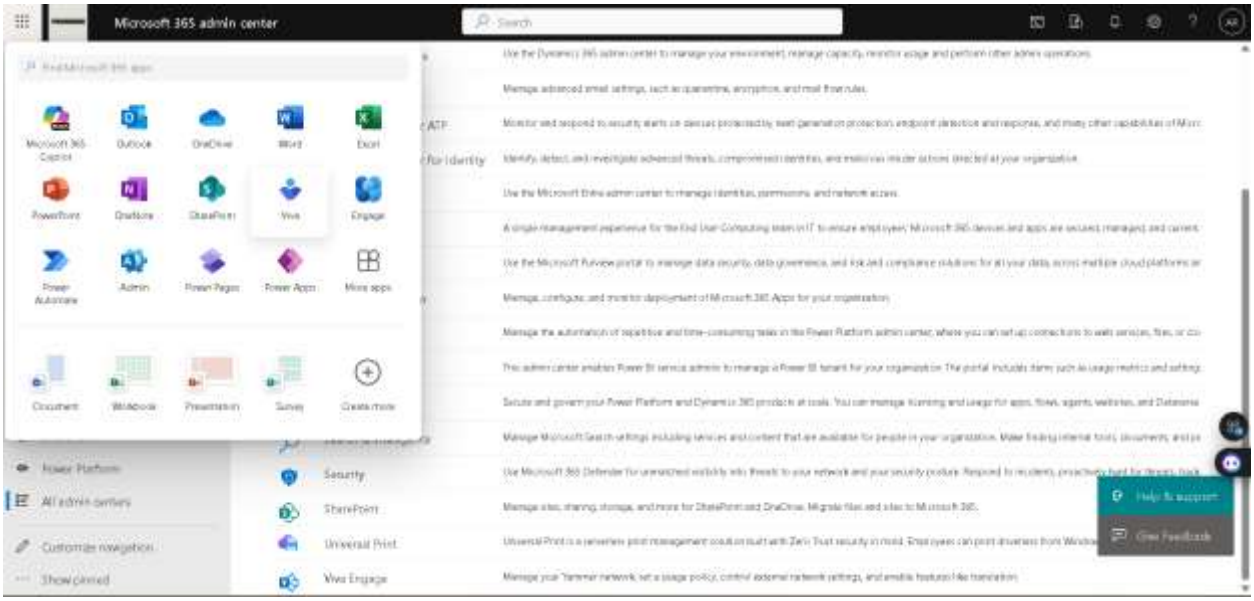
Step 1: From Microsoft 365 admin center, under admin centers select Viva engage.

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

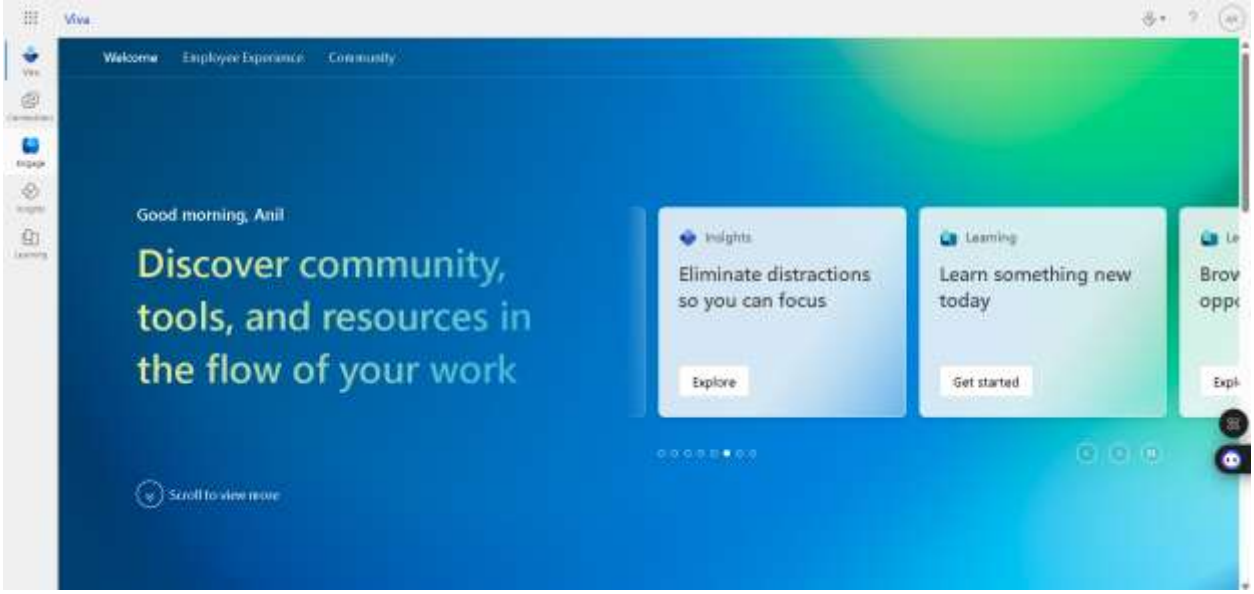


- Set up groups for company-wide announcements and department-specific discussions.

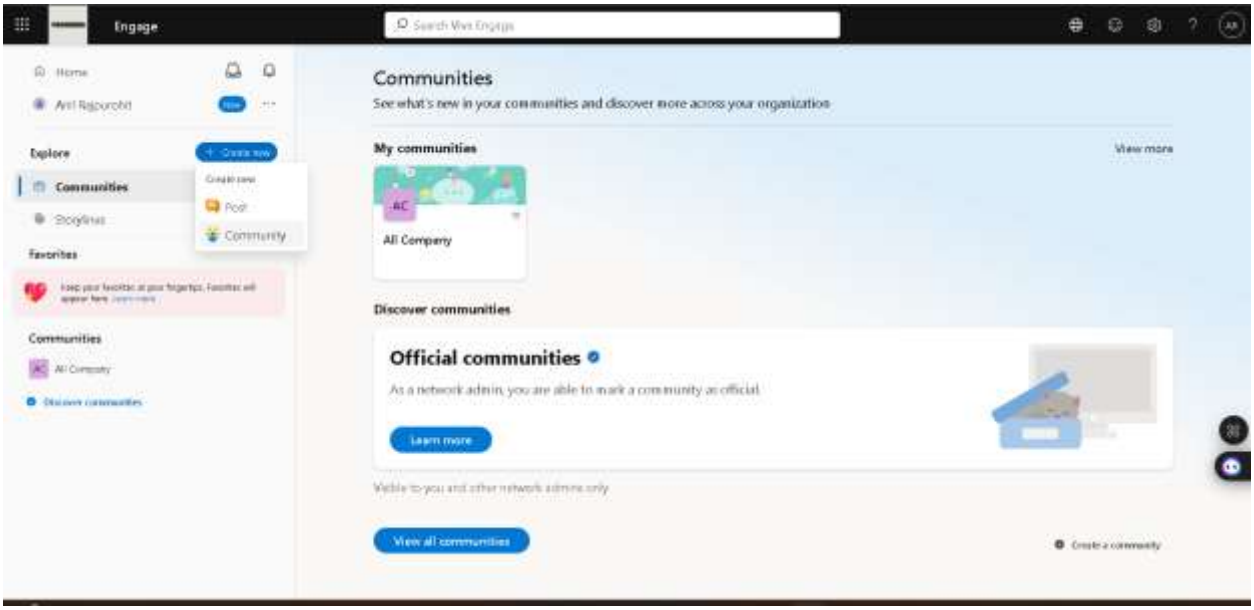
Step 1: Go to Viva portal.



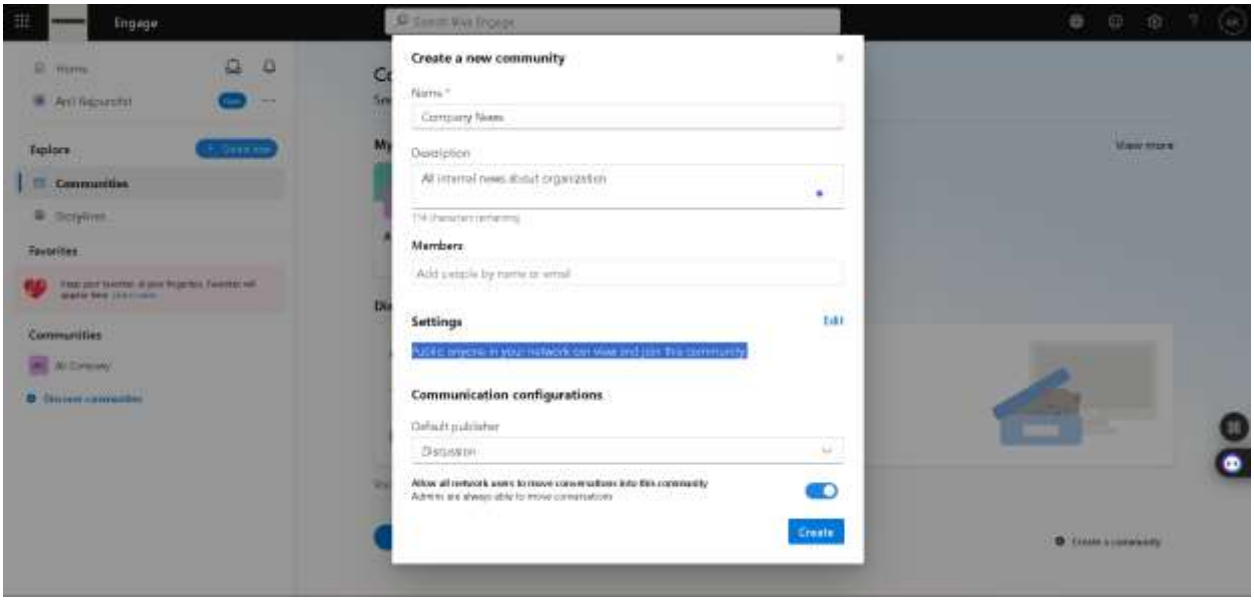
Step 2: In viva portal, go to engage.



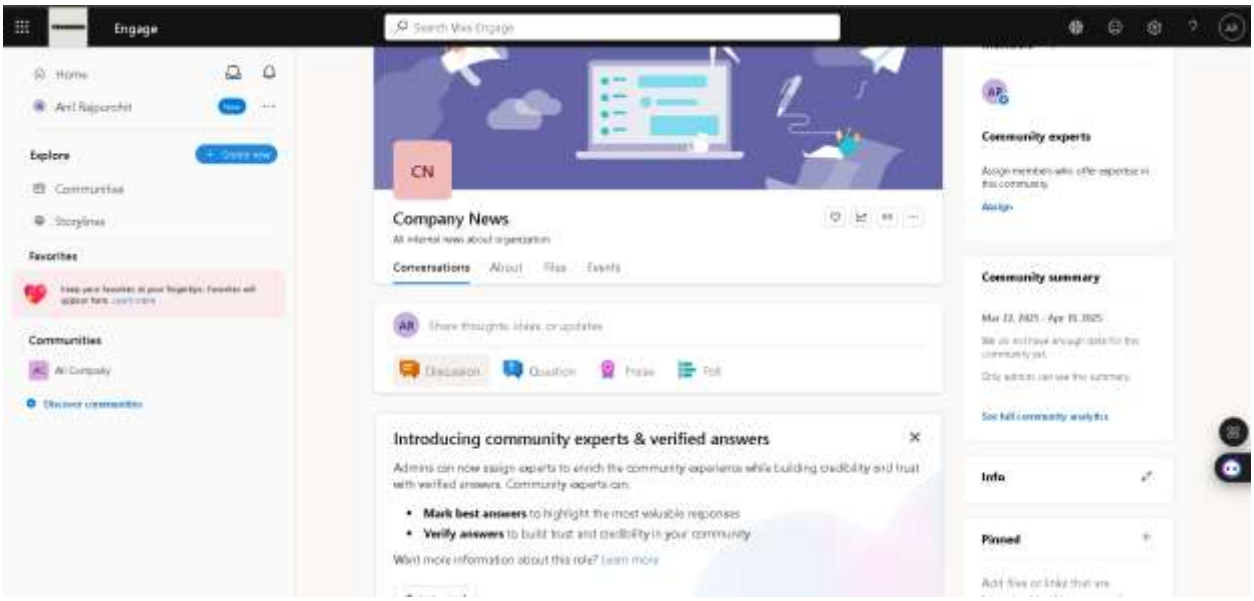
Step 3: In viva engage, under communities -> create new -> community.



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

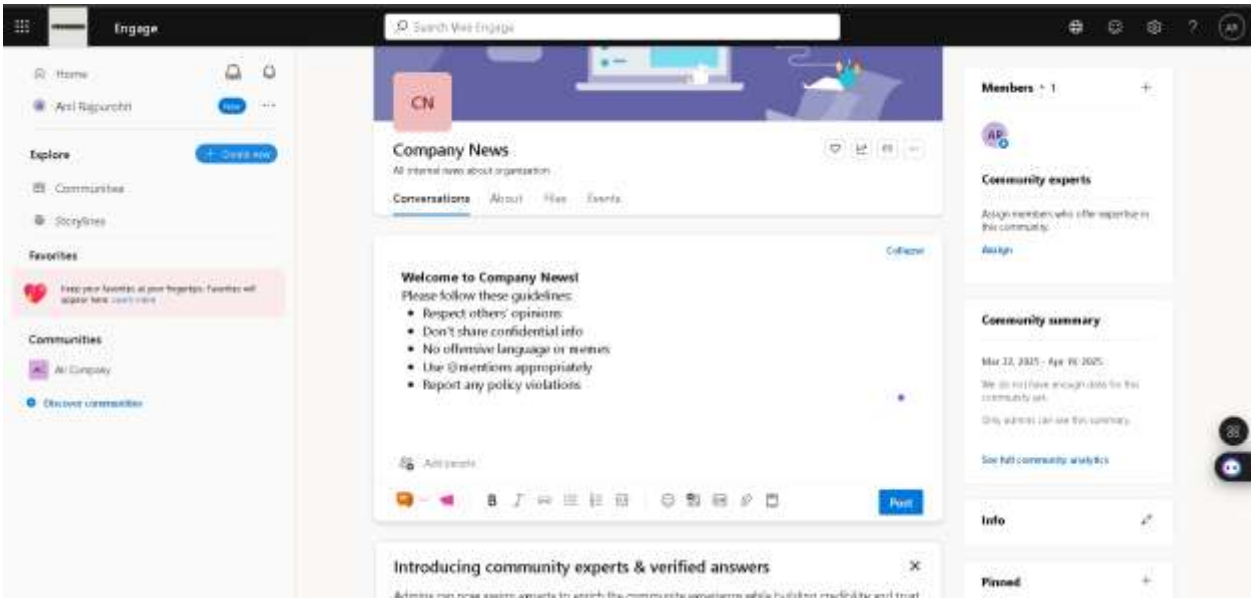


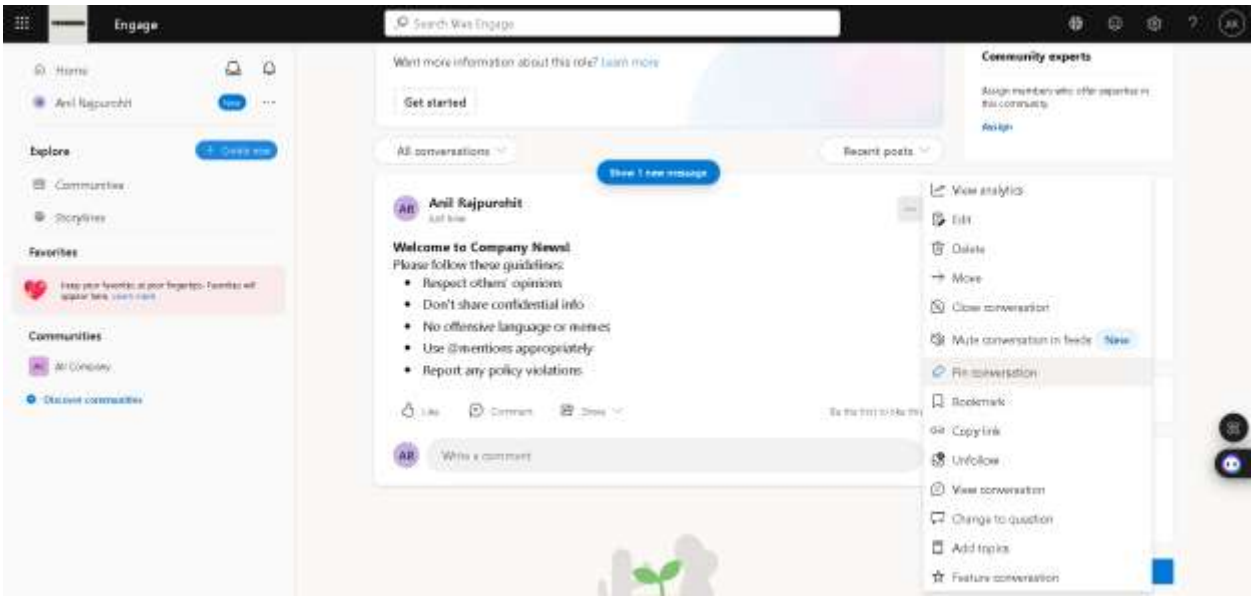
Step 5: Our new community has been successfully created.

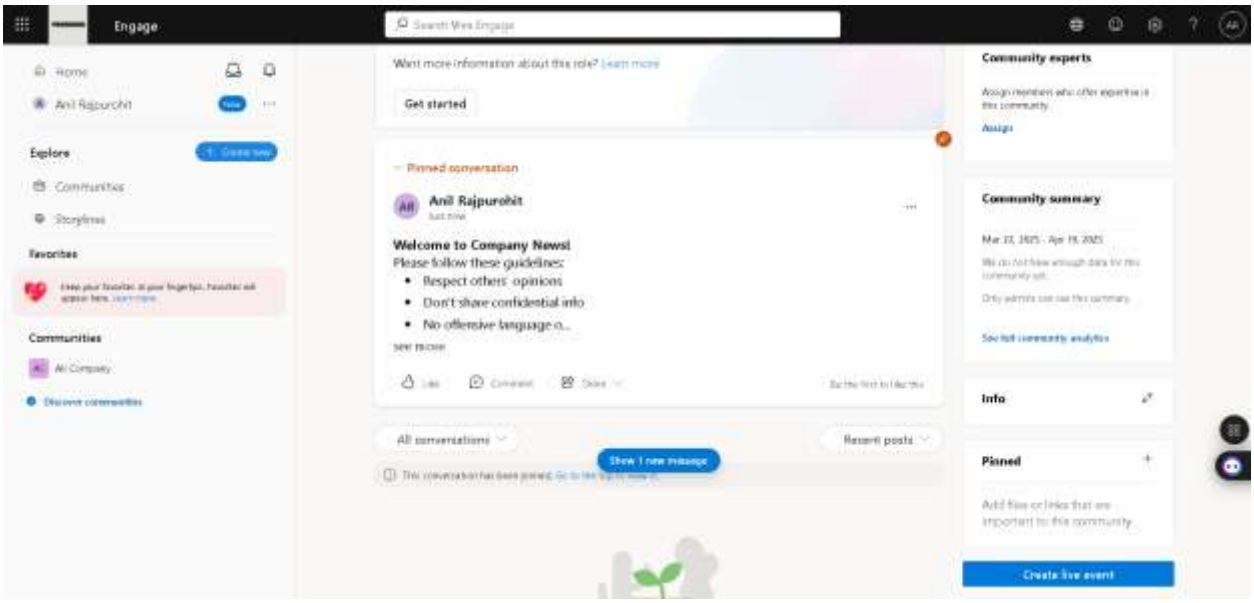


- Ensure compliance with the company's social media policy.

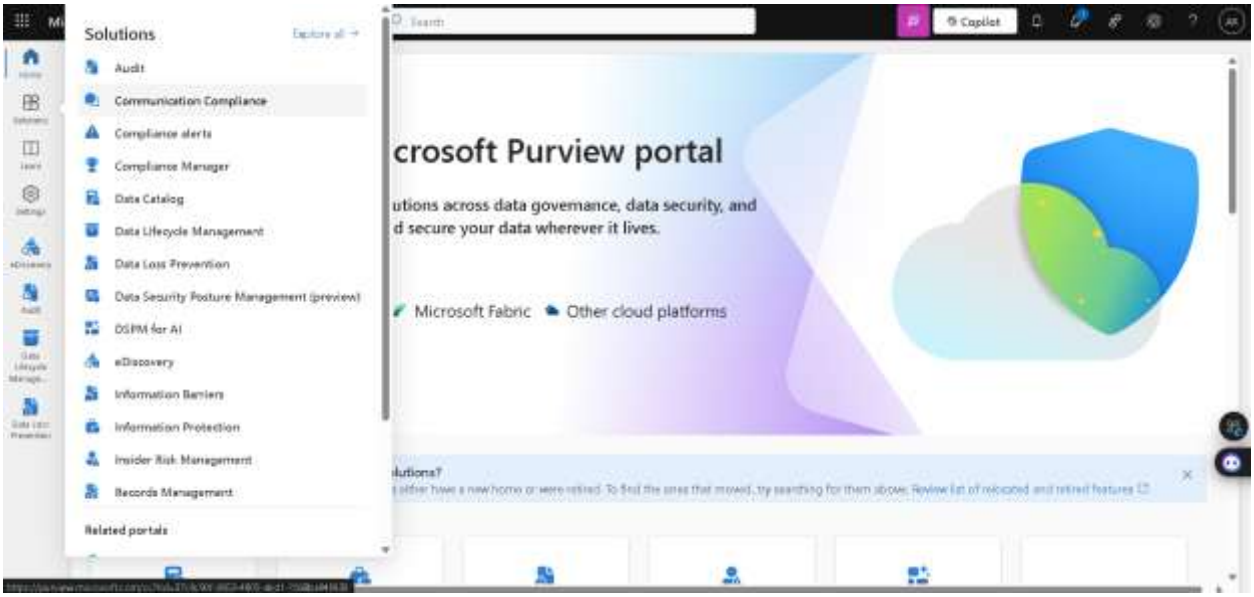
Step 1: First, we will post some guidelines for this community and pin it, so that everyone knows about it. E.g. No offensive language or memes.



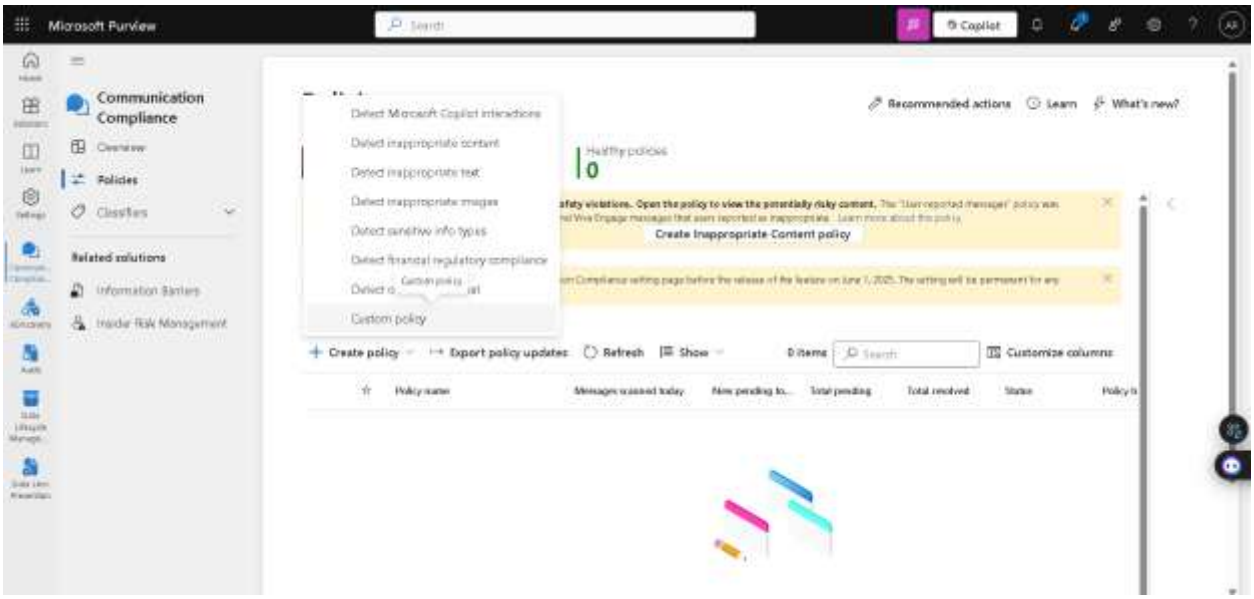




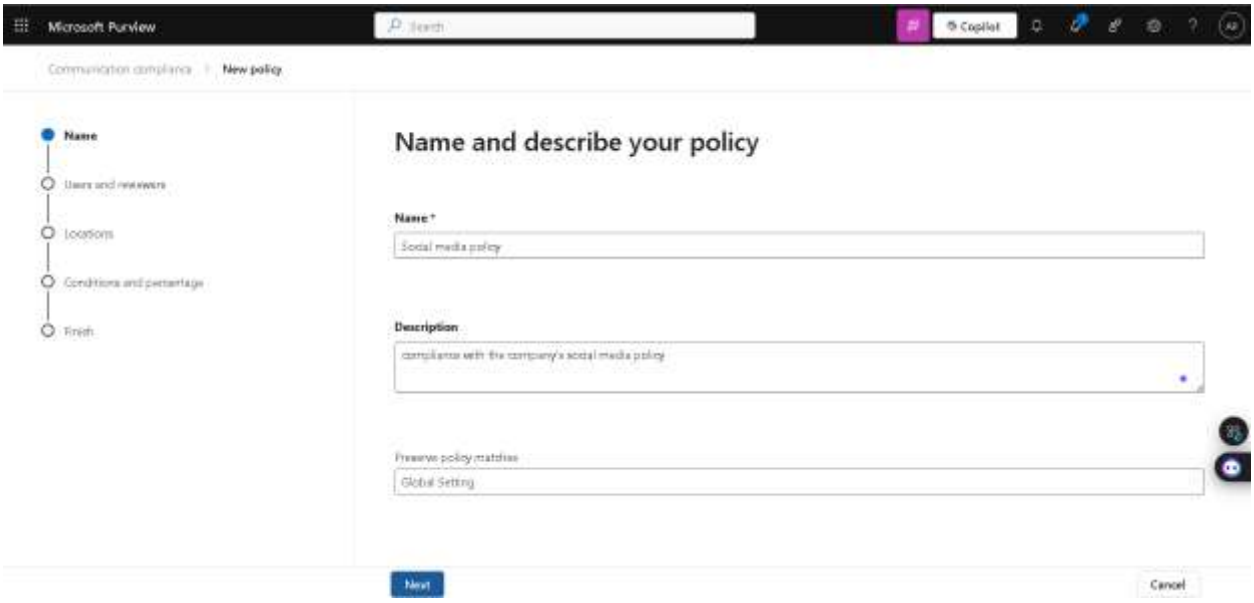
Step 2: Now from Purview portal, solutions -> communication compliance.



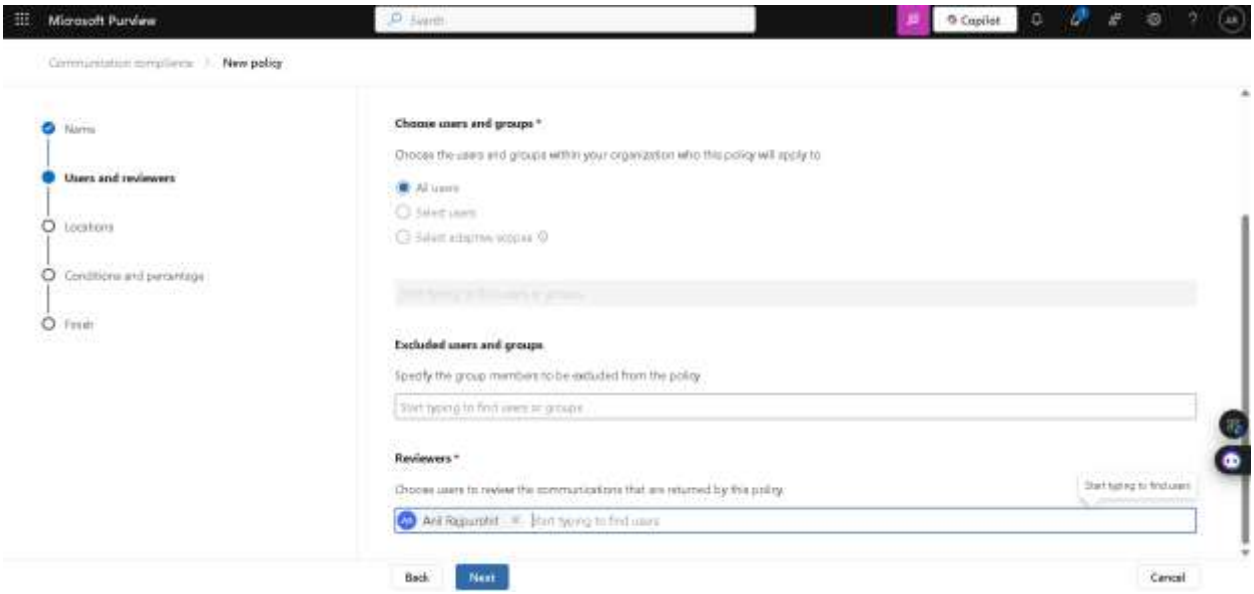
Step 3: In communication compliance -> policies -> custom policy.



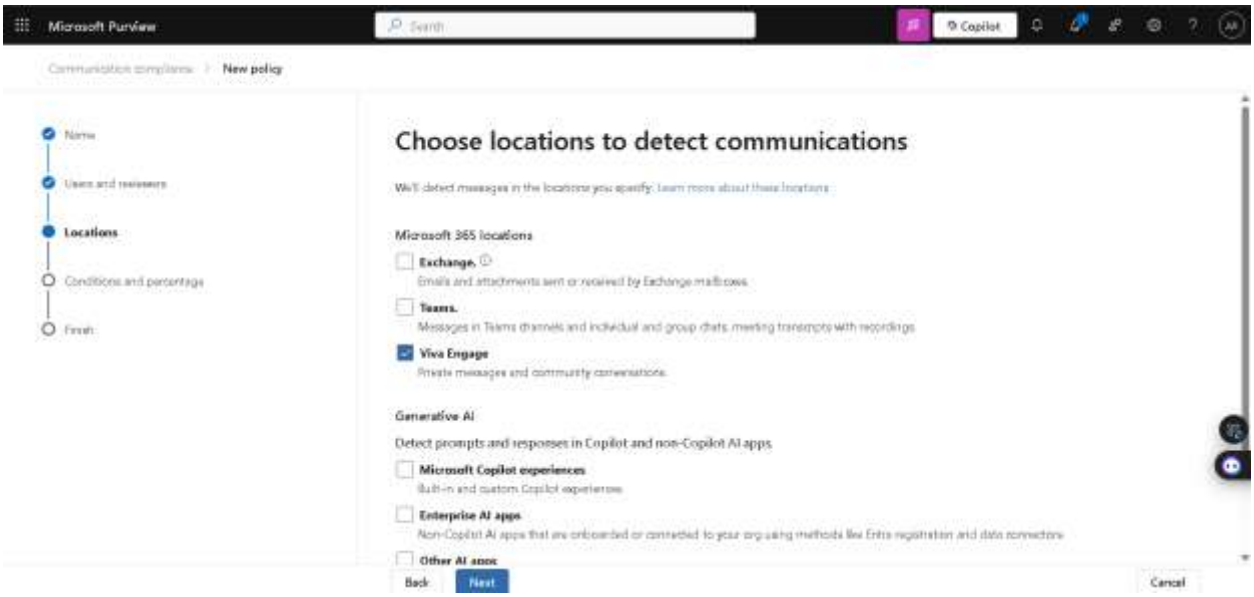
Step 4: Fill all the details about policy like name, description then next.



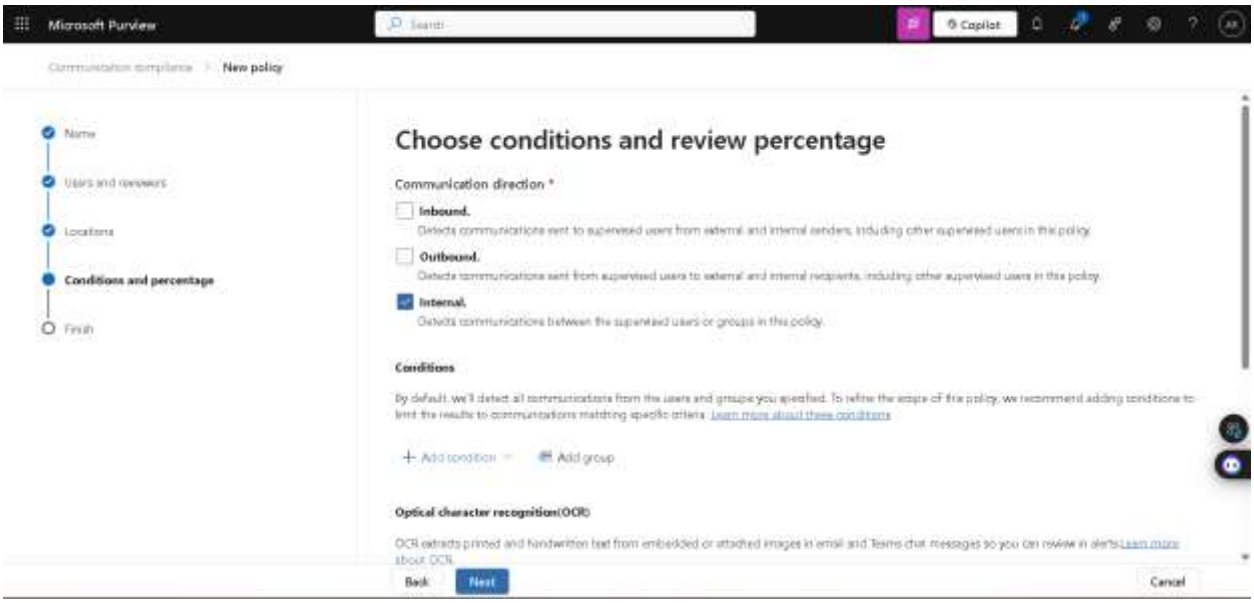
Step 5: As we want to apply this policy to all users in organization. So, select all users and add reviewers then next.



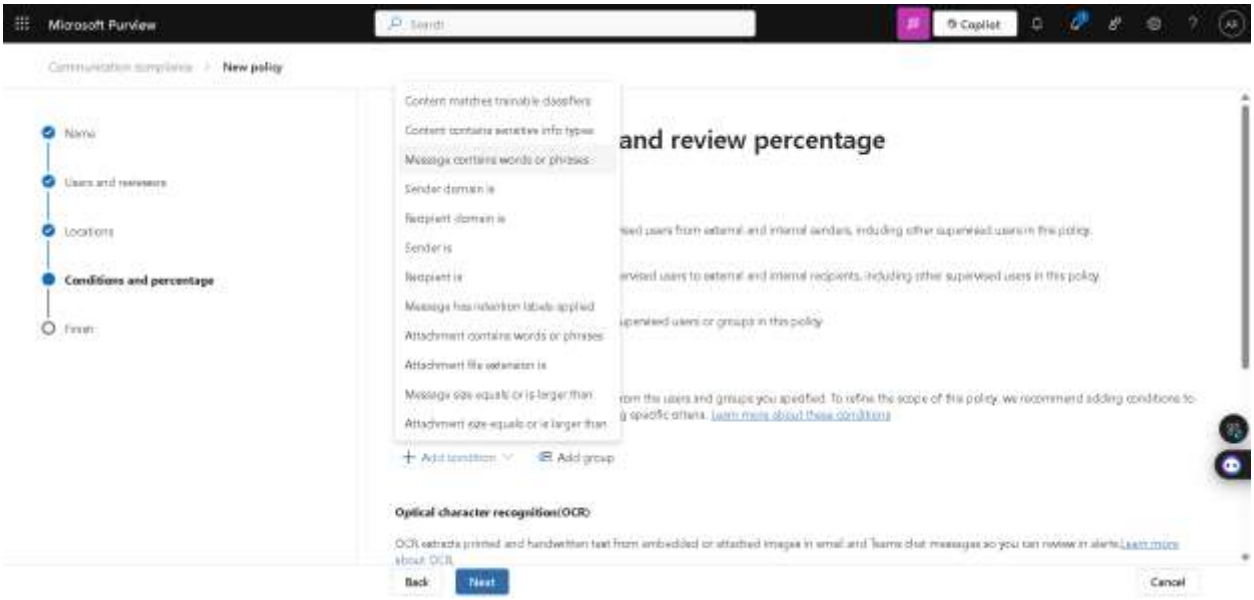
Step 6: As we are creating this policy for viva engage, selected viva engage then next.



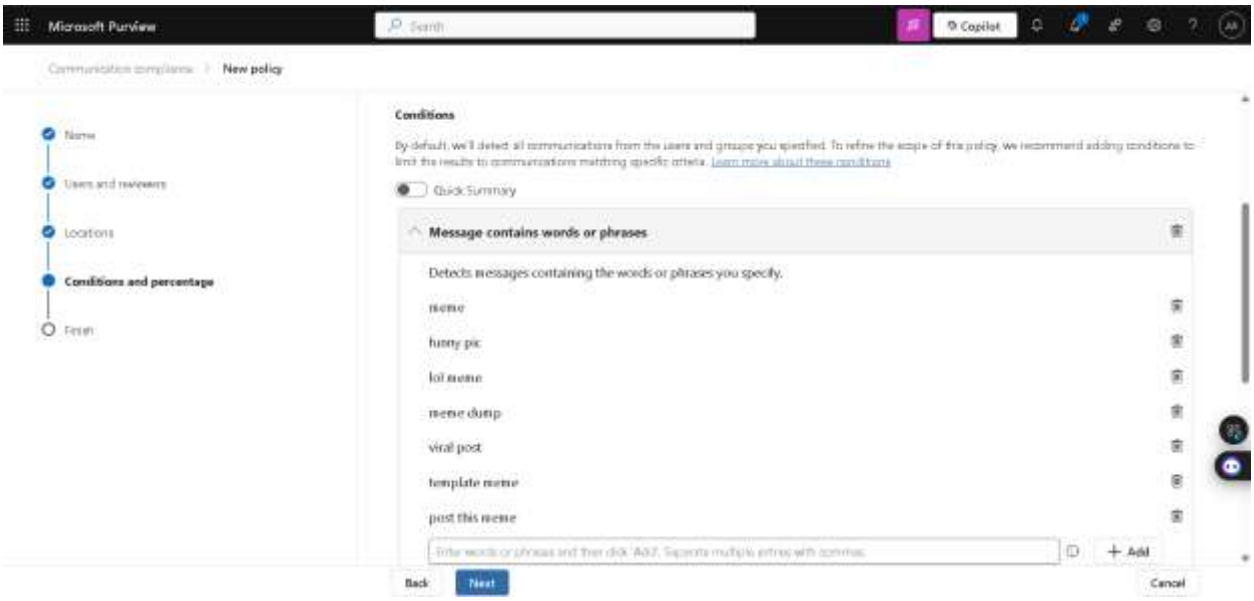
Step 7: Selected Communication direction as internal, as communication is internal.



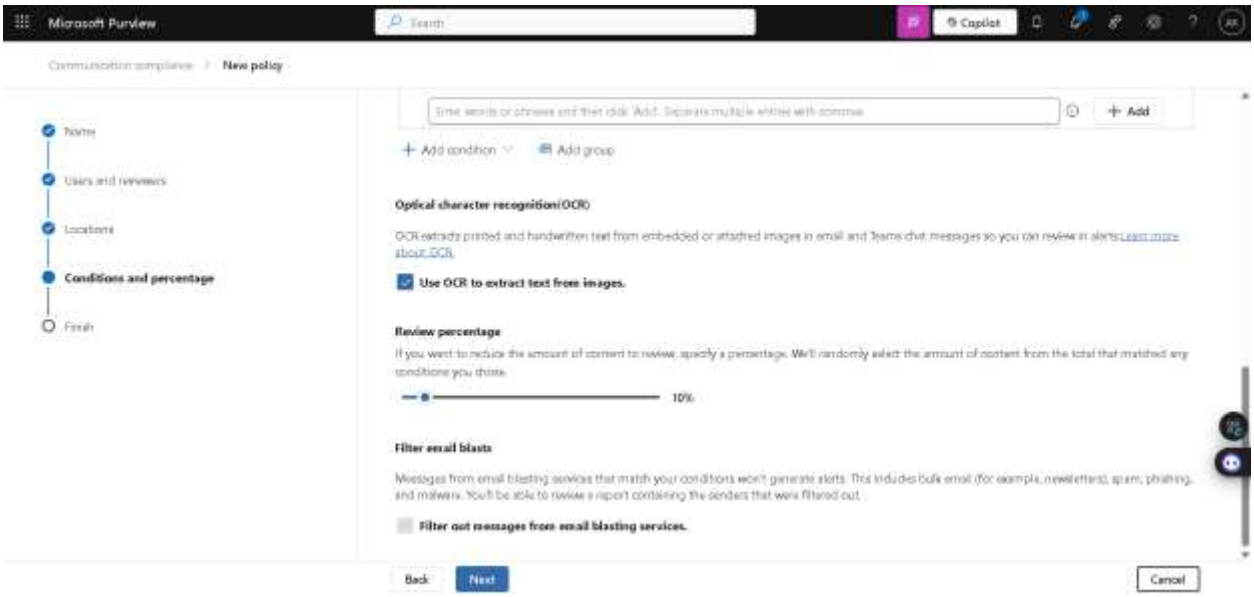
Step 8: Add condition for message contains words or phrases.



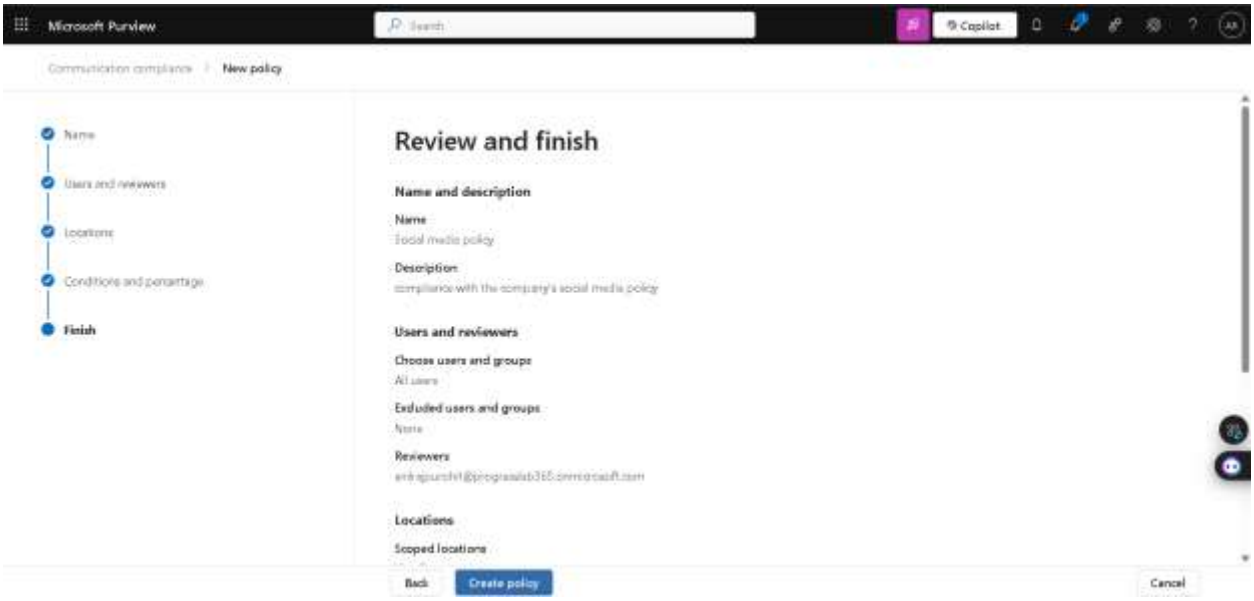
Step 9: As we created this policy to block users from sharing memes content in engage communication. So, provided some words and phrases to restrict them.



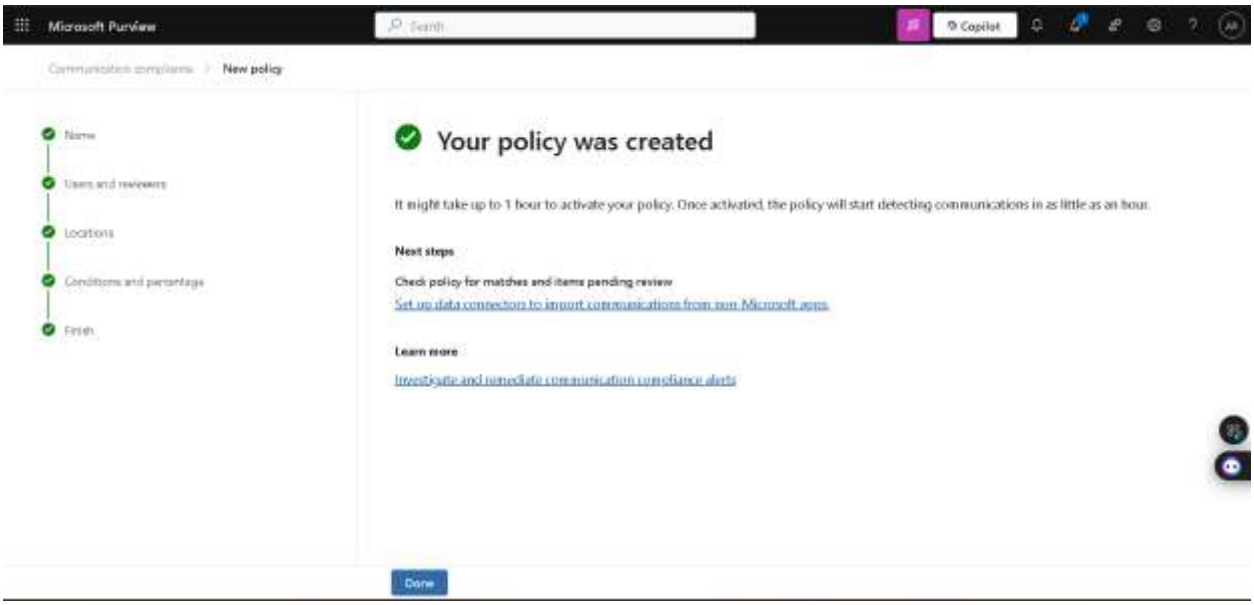
Step 10: Select use OCR to extract text from images then next.



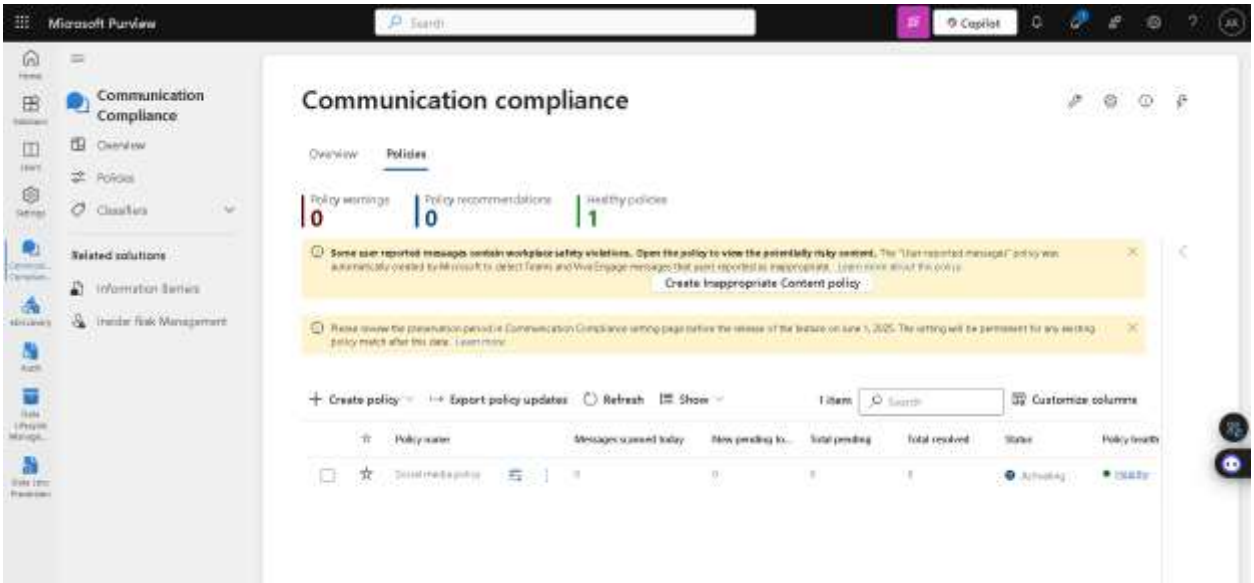
Step 11: Review policy details then click on create policy.



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.

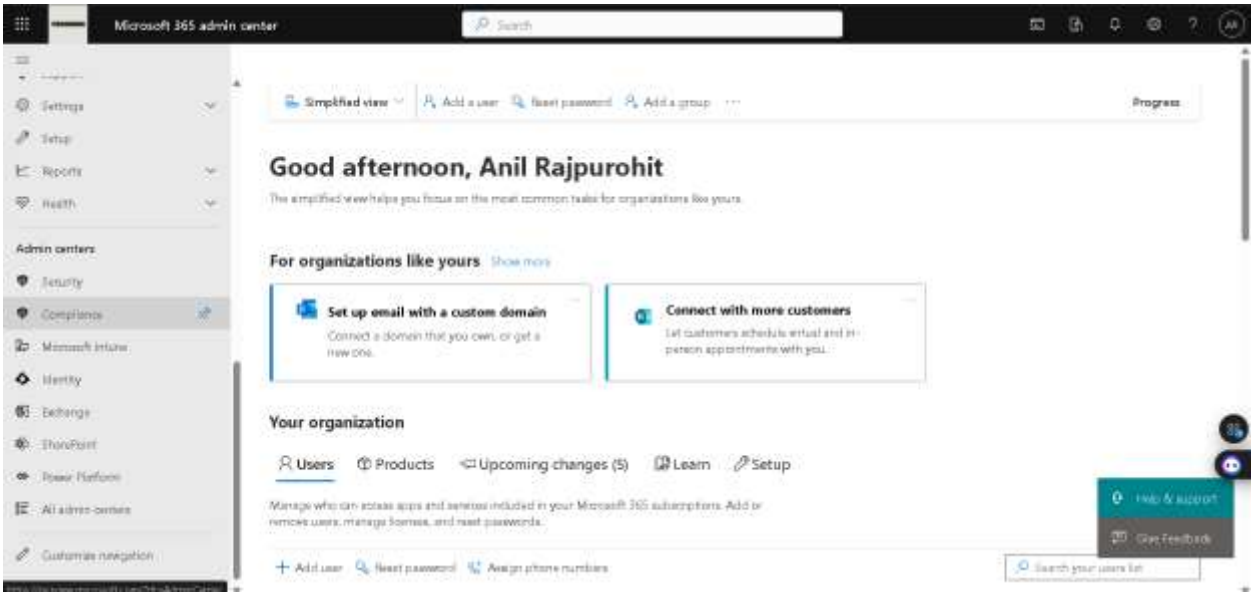
We can create policy for Communication too, so that users will adhere organizations guidelines.

Task 4: Monitoring and Reporting

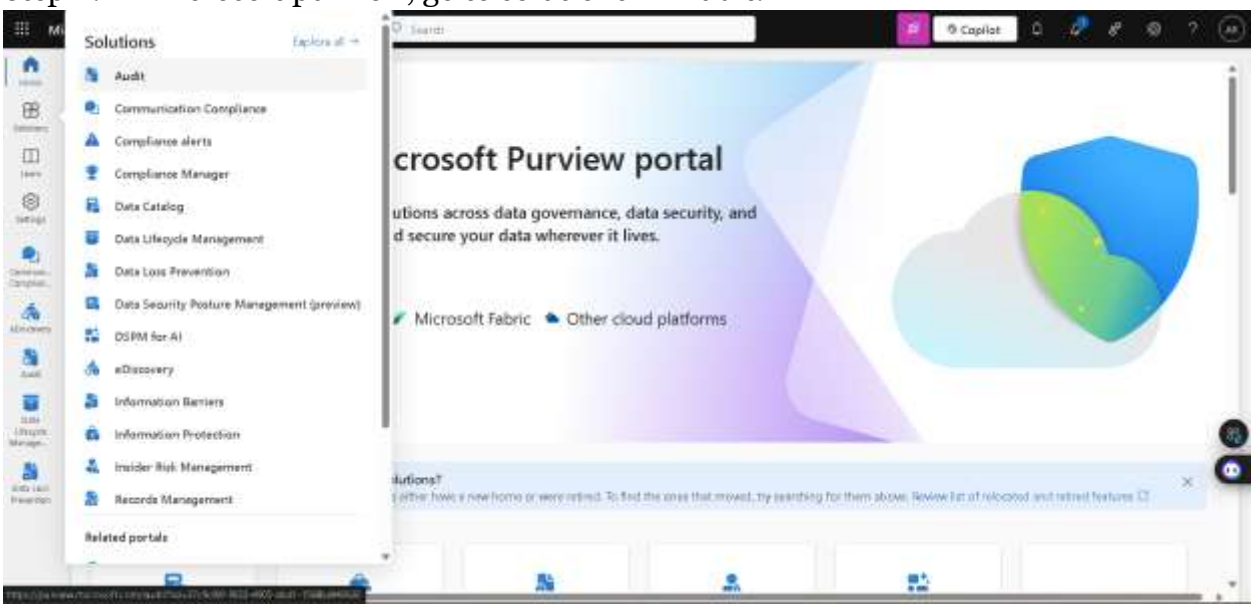
1. Configure Audit Logs:

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

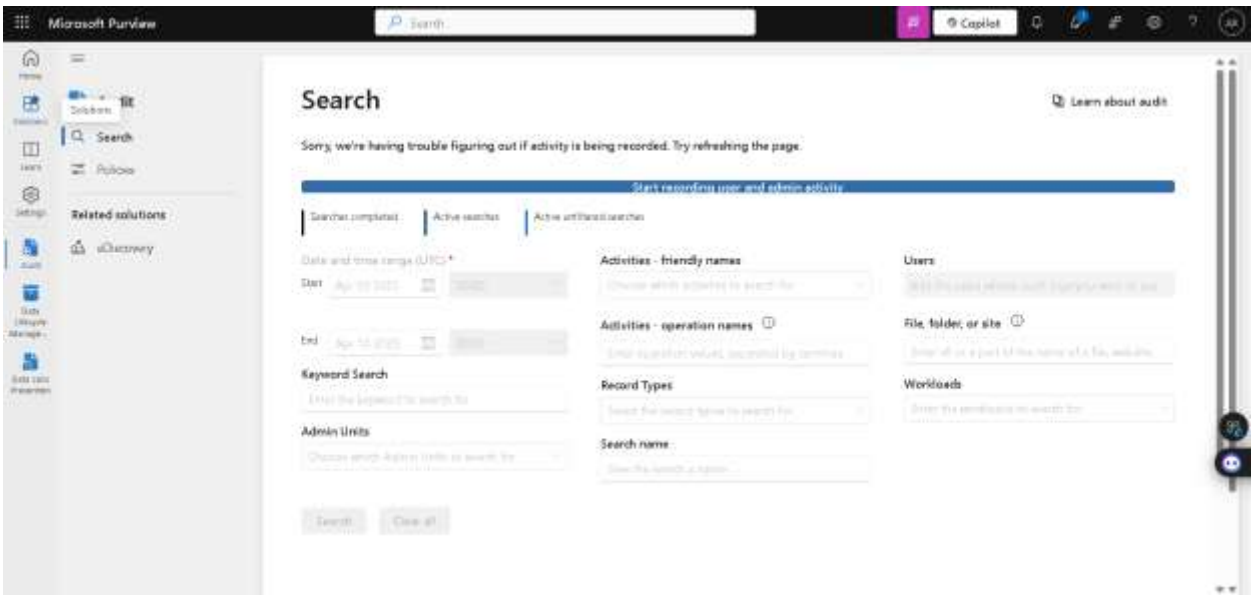
Step 1: From Microsoft 365 admin center, under admin centers select compliance.



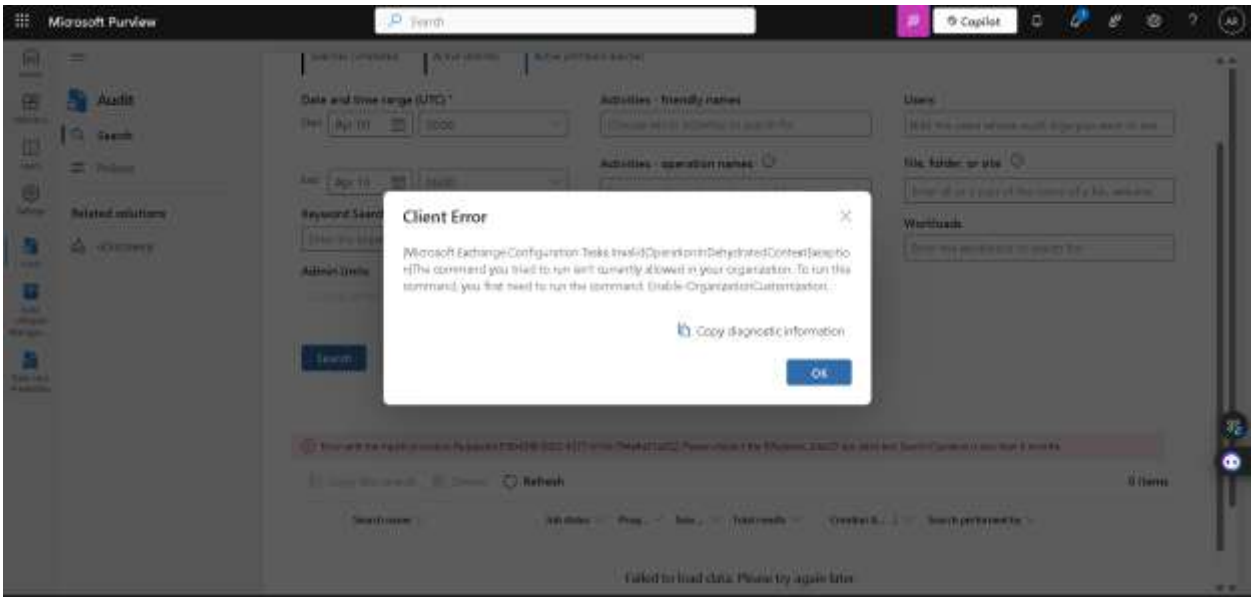
Step 2: In Microsoft purview, go to solutions -> Audit.



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



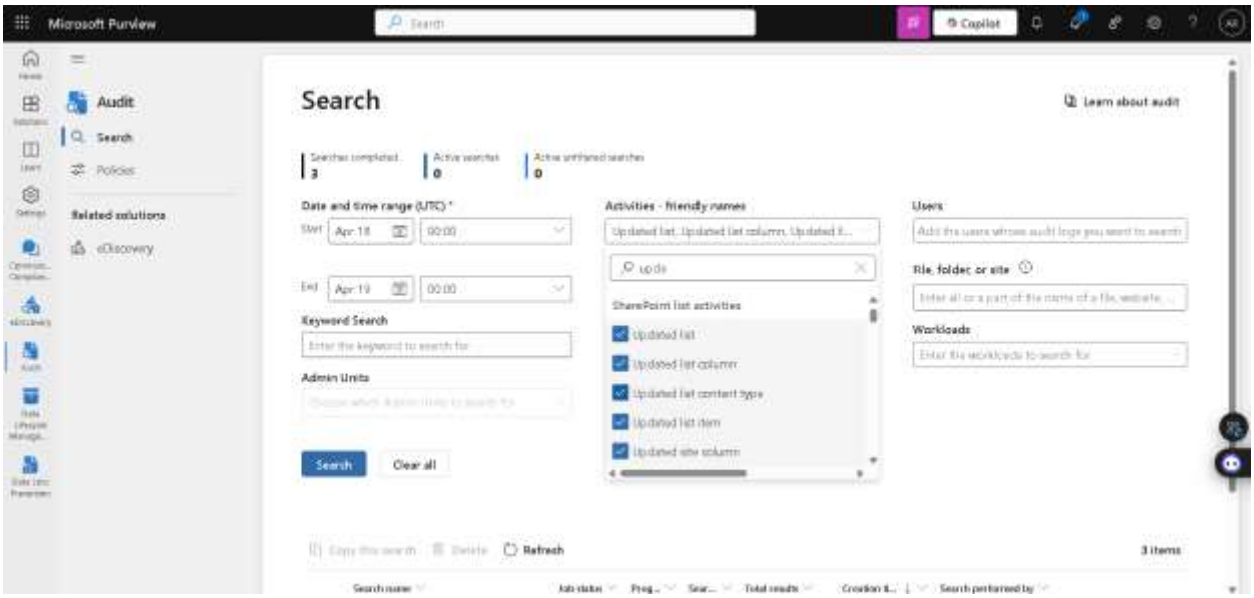
Step 4: We got a client error, so we will try from Windows PowerShell.



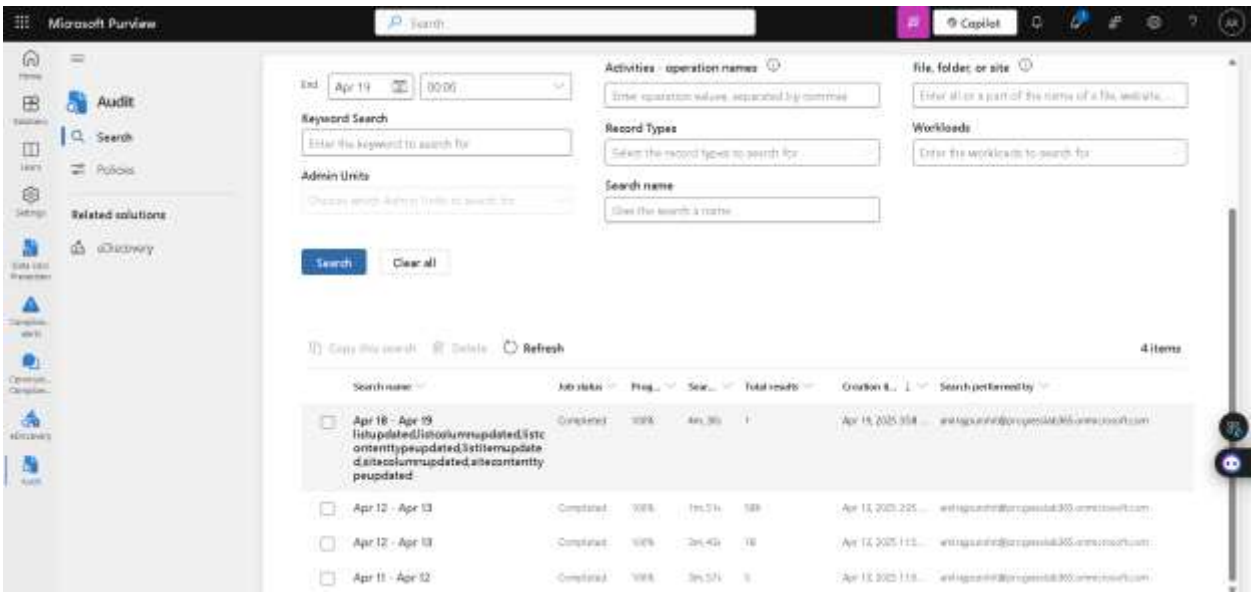
Step 5: First, we will install Microsoft Graph and Exchange online management. Then Connect to exchange online using global admin and set admin audit log config to True.

- Create a custom audit log search to track user activities related to at least one activity in SharePoint such as updating the site content.

Step 1: After waiting for some time for it to be fully functional. We will again to Microsoft purview -> solutions -> Audit. Set the date and time range then search. We selected date from 18 Apr to 19 Apr 2025 and we filtered only SharePoint activities.

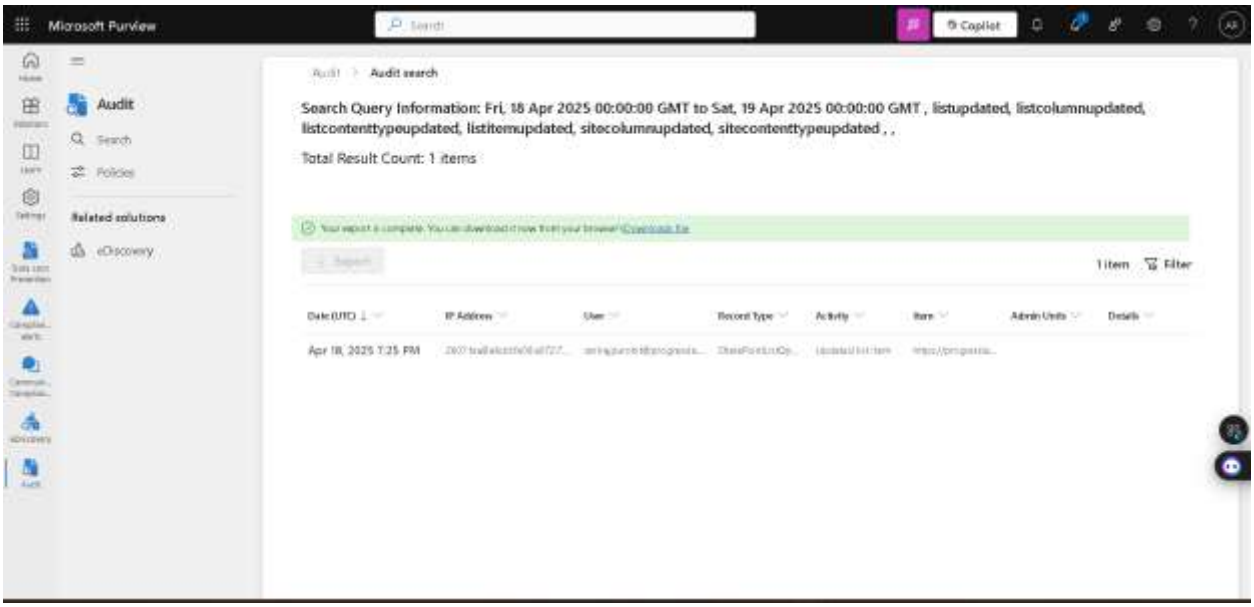


Step 2: Now click on our latest audit report.

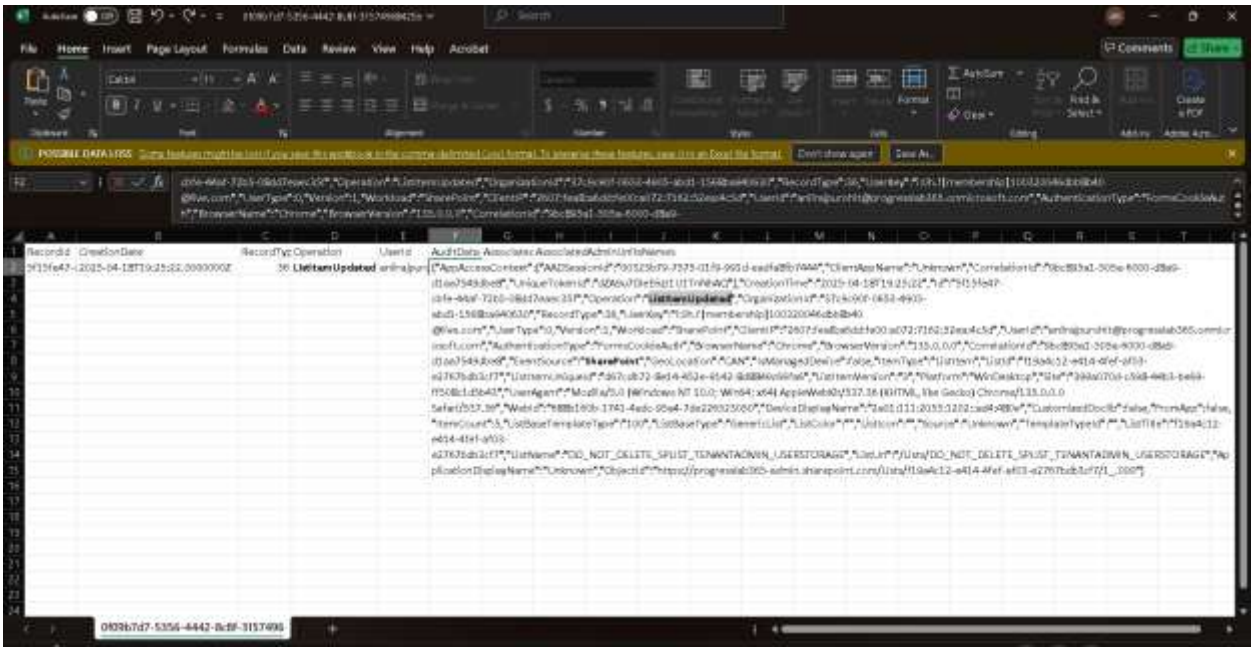


Step 3: We can view logs here from 18 Apr 2025 to 19 Apr 2025. Also, their record type, activity, user, date etc. Now, to export the log click on Export.

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



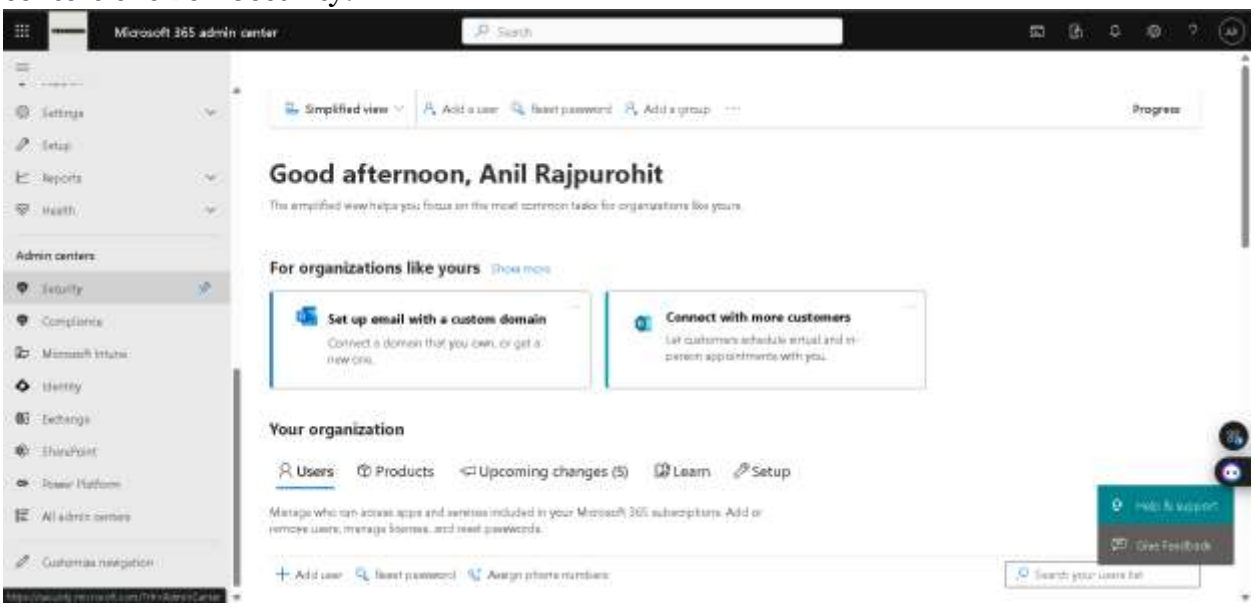
Step 5: We can view our audit log in excel file now. For instance, we can view that global admin updated items in SharePoint site on 2025-04-18 at 19.25.12.



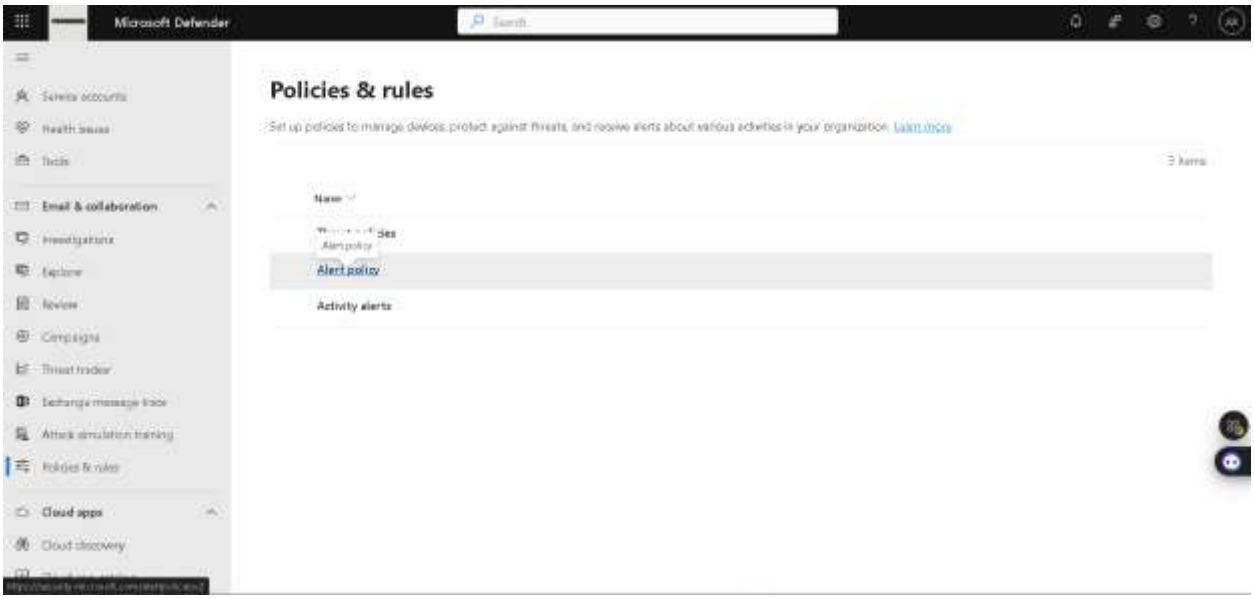
2. Set Up Alerts:

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

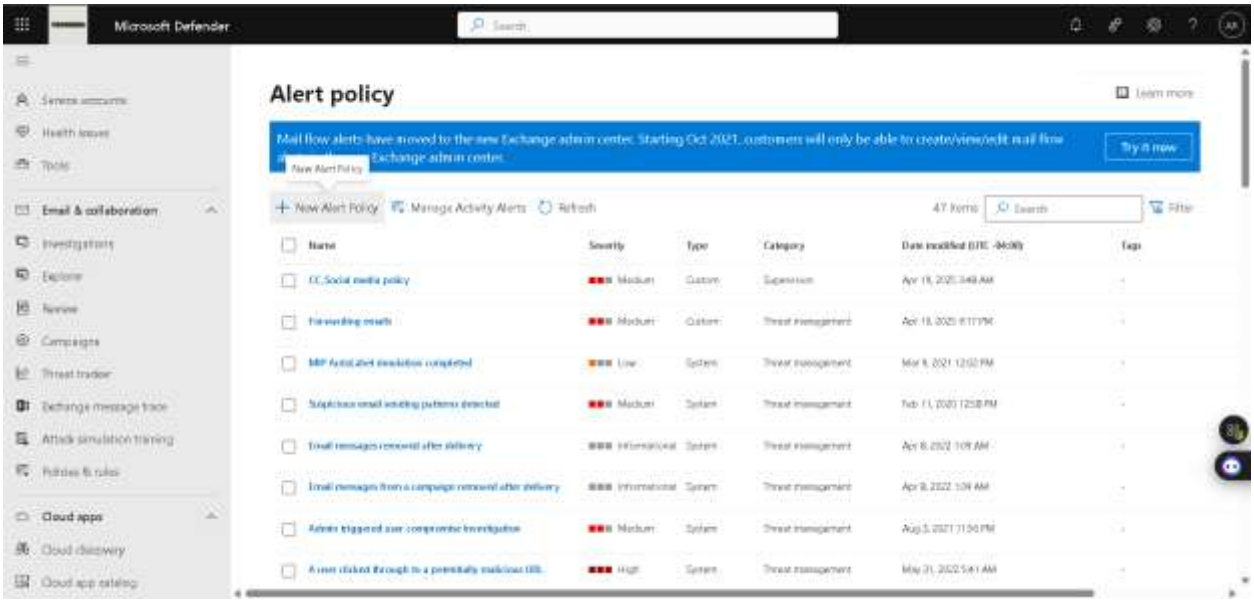
Step 1: To configure security alerts, go to Microsoft 365 Admin Center and under admin centers click on Security.



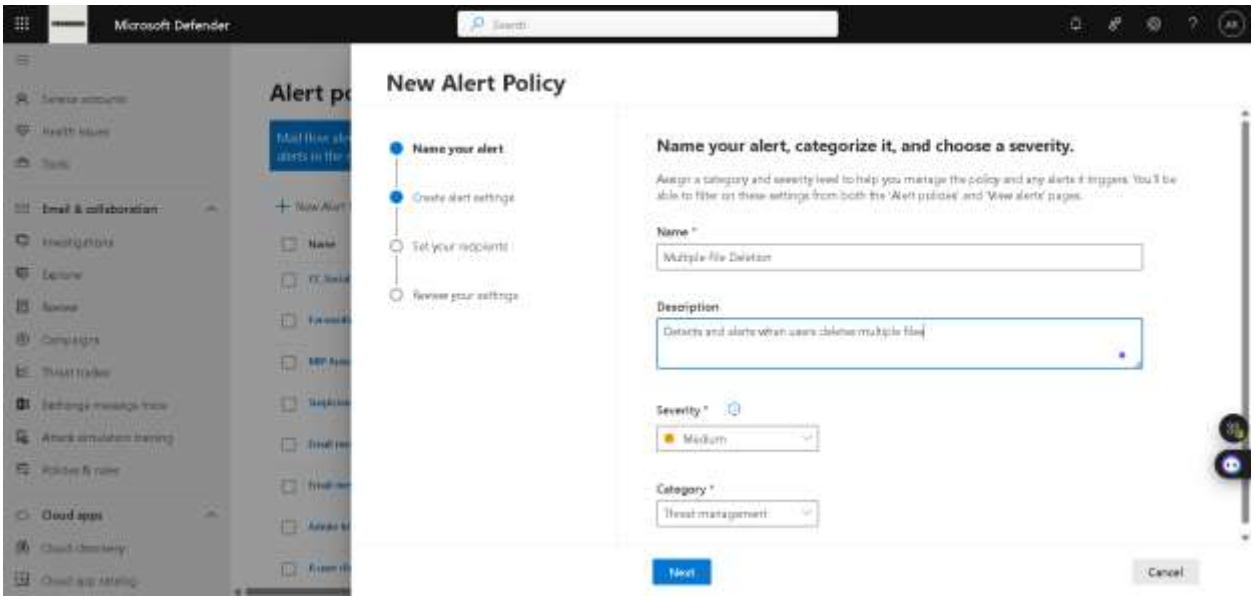
Step 2: We are in Microsoft Defender now and from here we can manage and configure security alerts. From Microsoft defender, under email & collaboration go to Policies & rules -> alert policy.



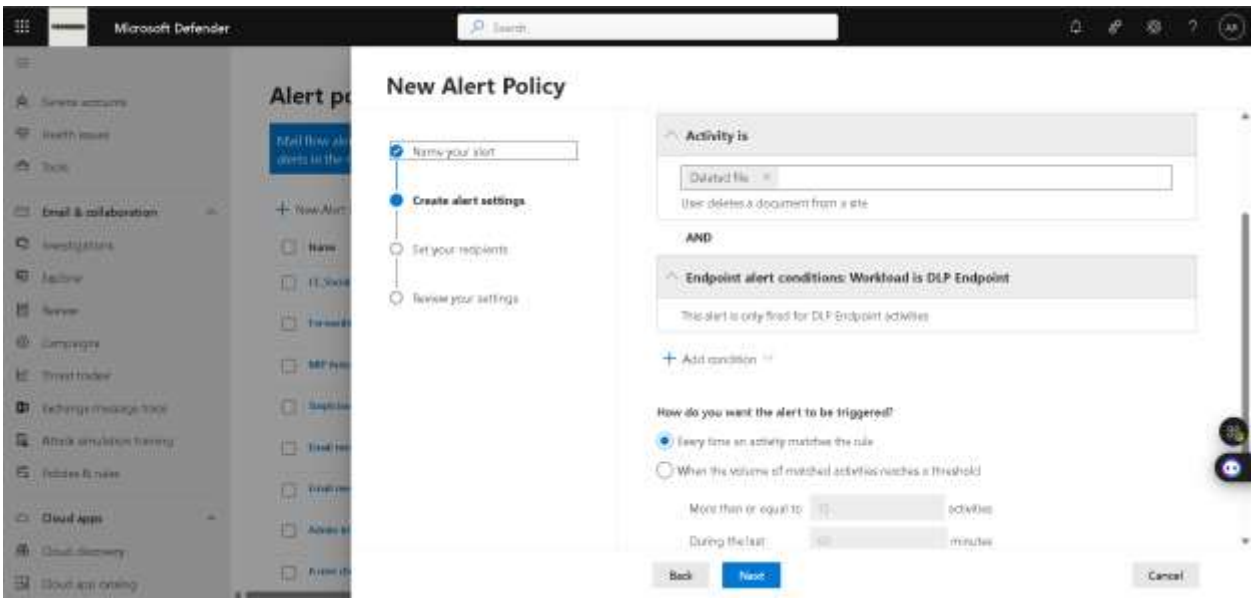
Step 3: We can view all the default policies here, now to create a new policy click on New alert policy.



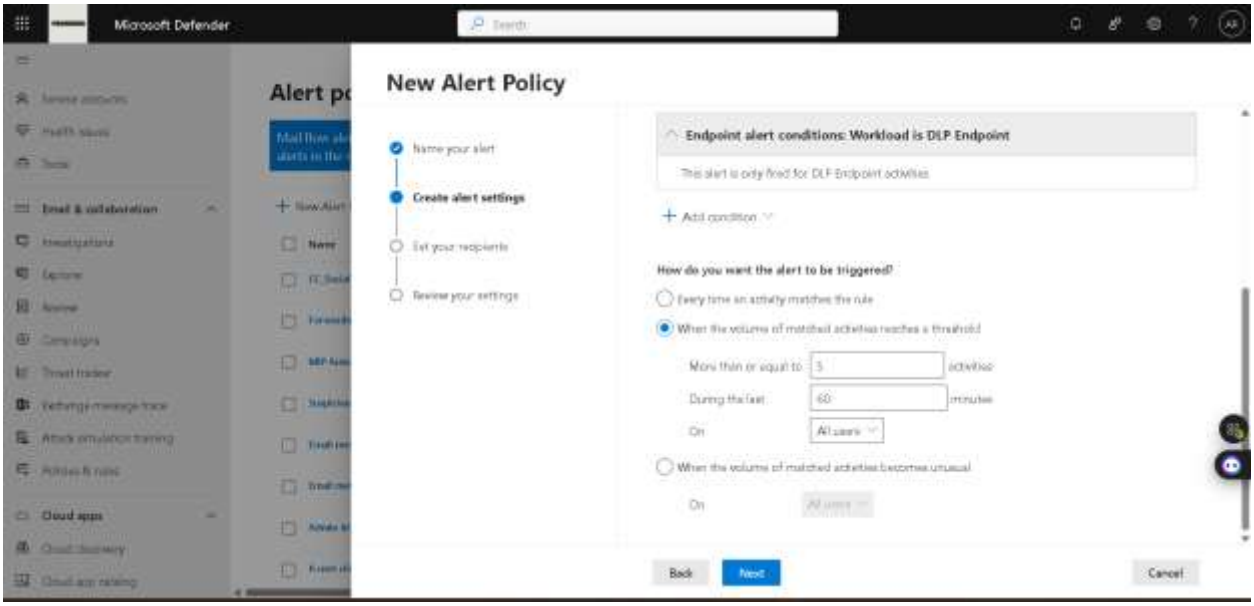
Step 4: Provide name, description, severity level, and category to the policy then click on next.



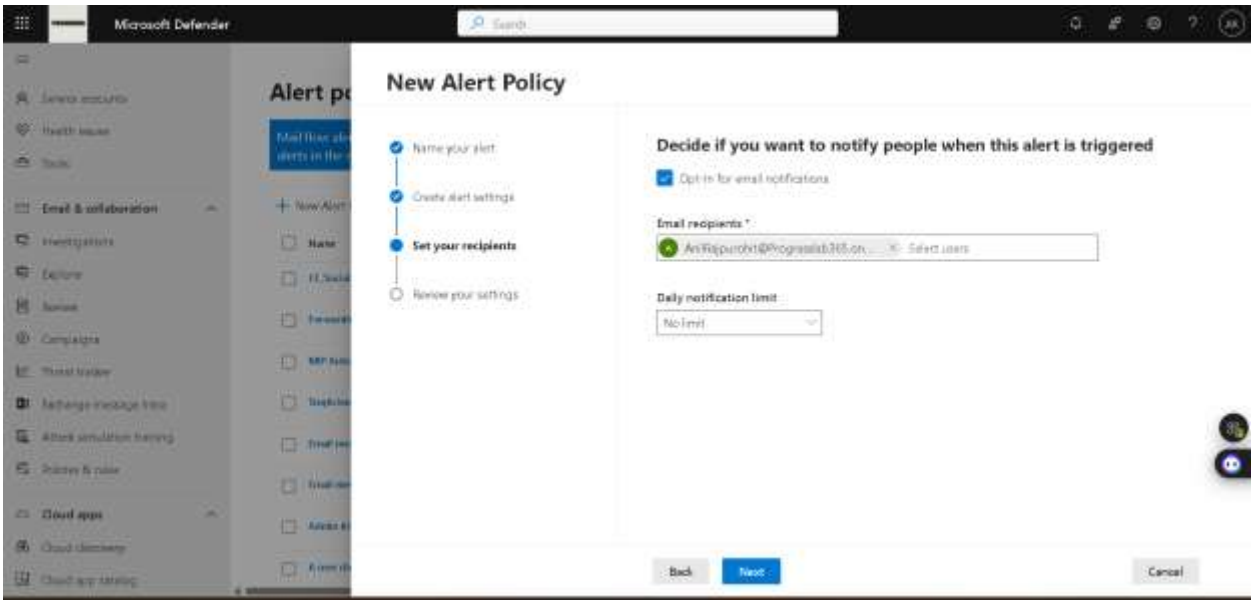
Step 5: We choose the activity here, which is deleted file (as we are creating policy for mass deletion). Then choose every time an activity matches the rule for our alert to be triggered and click on Next.



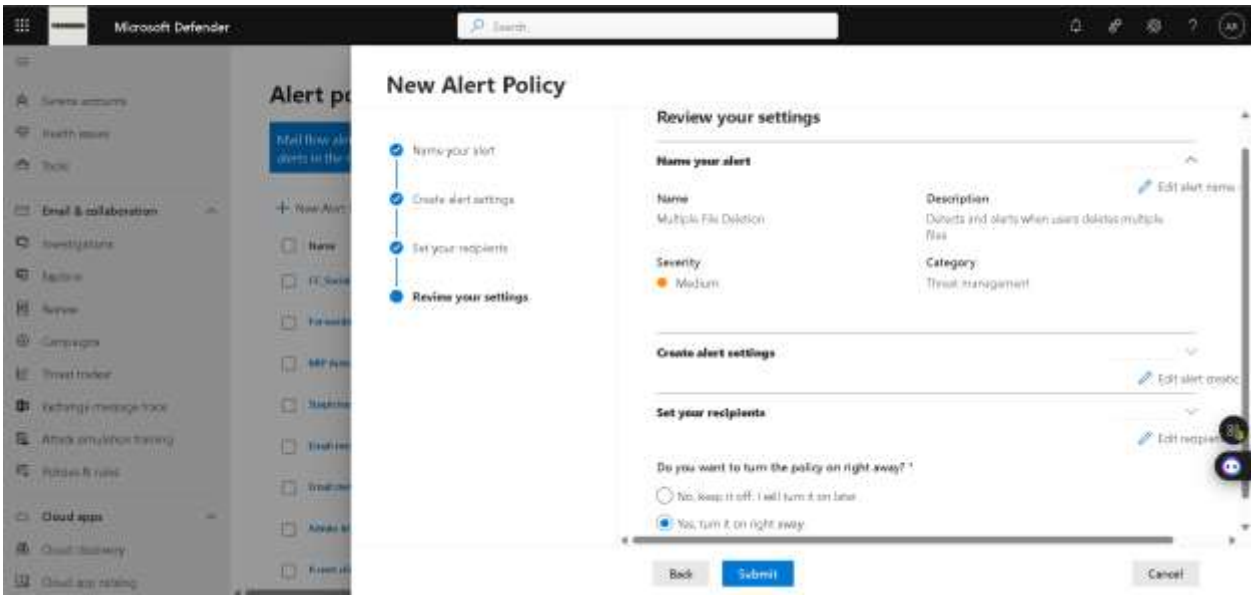
Step 6: We choose volume as more than 5, if a user deletes more than 5 files in 60 minutes this policy will be activated.



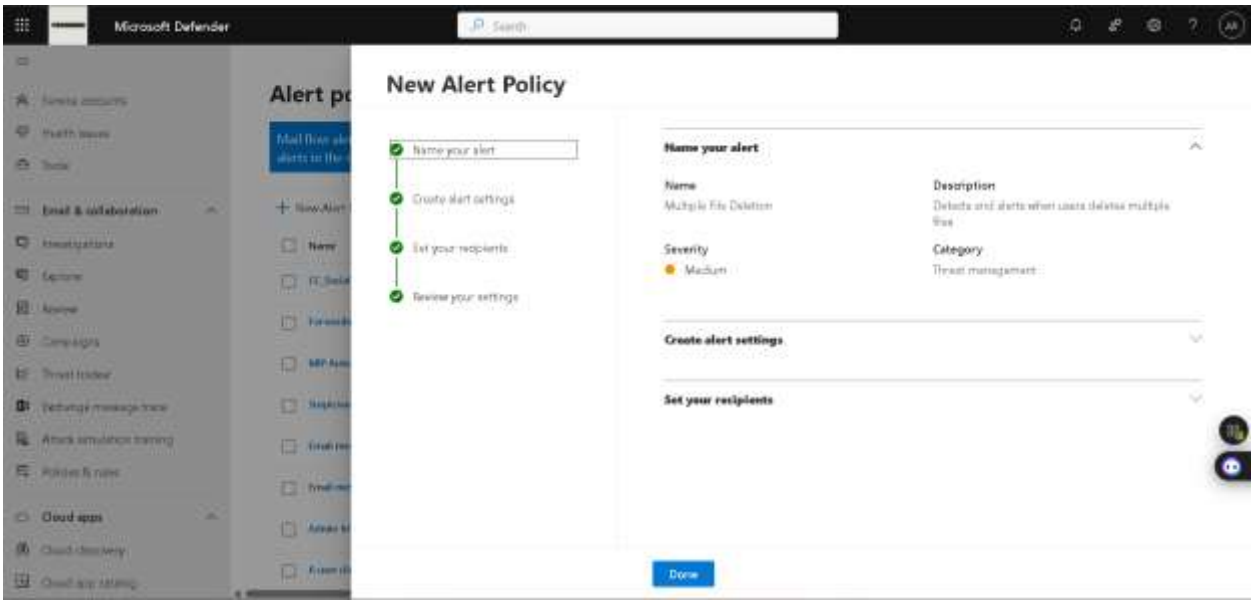
Step 7: Choose email recipients to get email notifications, then click on next.



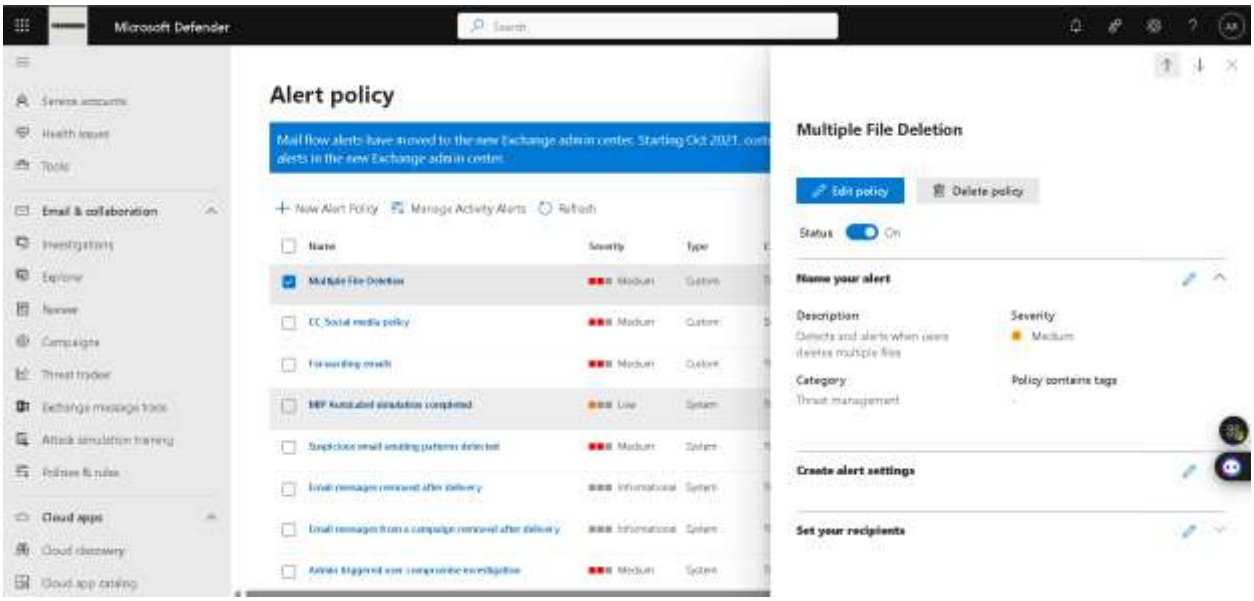
Step 8: Review policy details and turn on policy right away, then click on Submit.



Step 9: Policy has been created successfully.

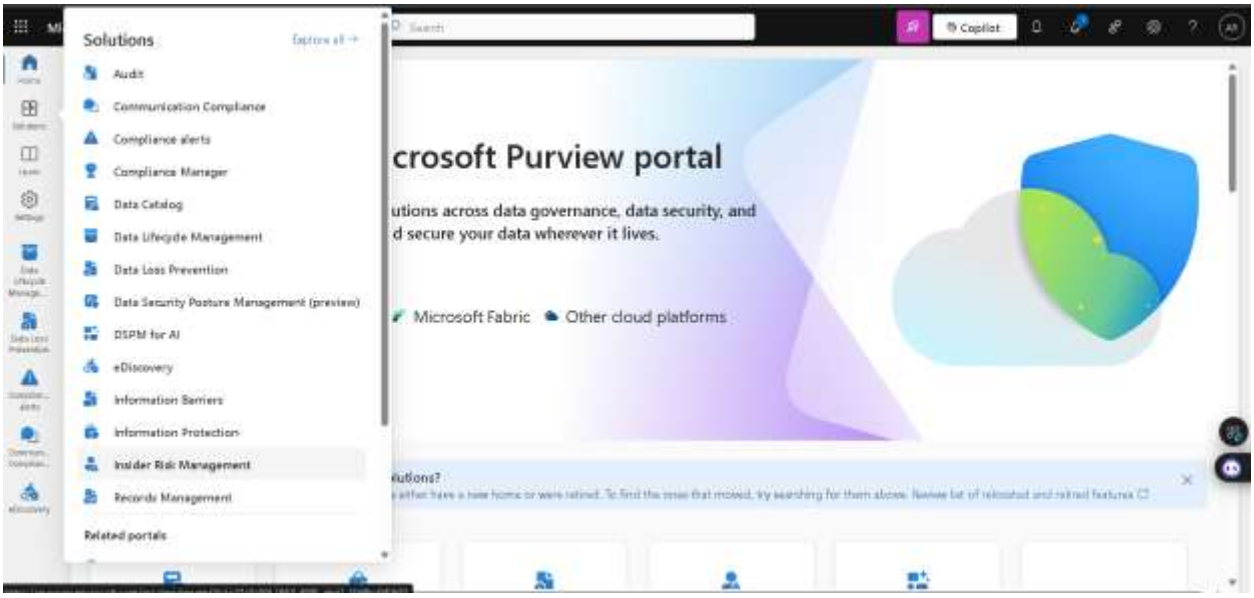


Step 10: We can see our new policy under Alert policy now.

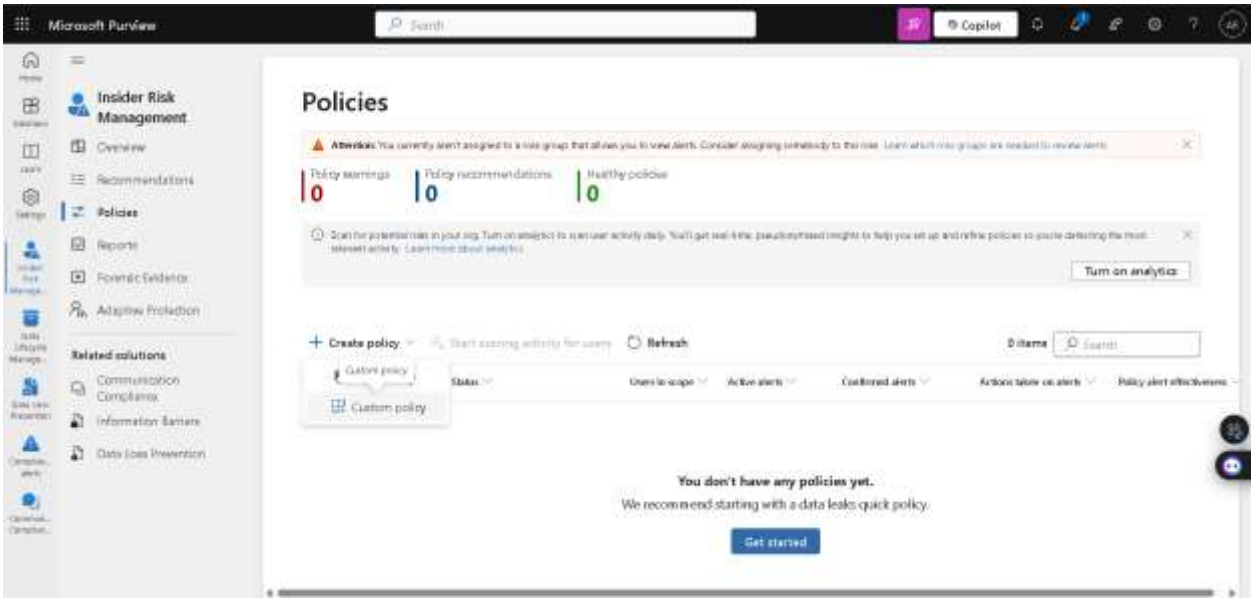


- Set up notifications for data loss prevention (DLP) policy breaches. (You can navigate to Insider risk management)

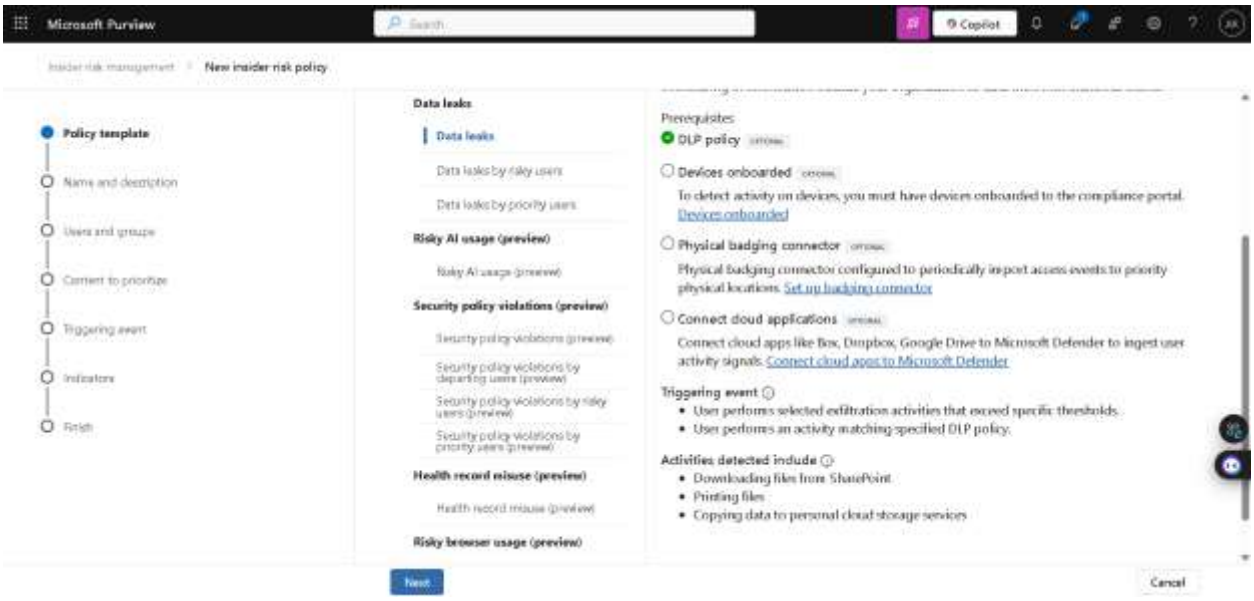
Step 1: In purview portal, solutions -> Insider risk management.



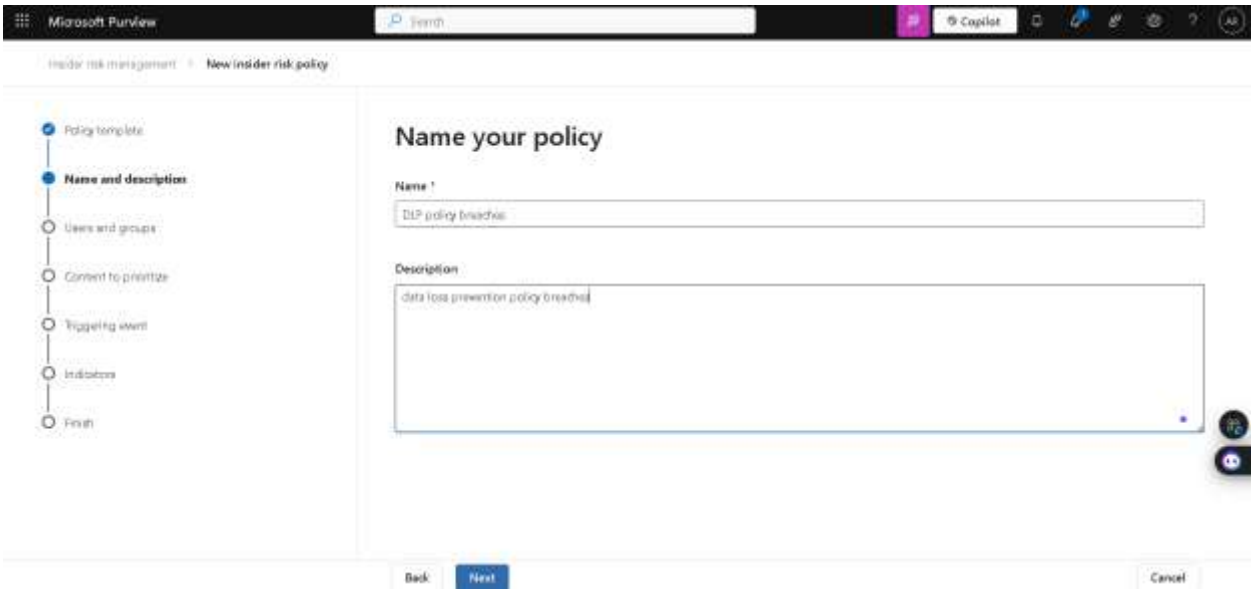
Step 2: In insider risk management, policies -> custom policy.



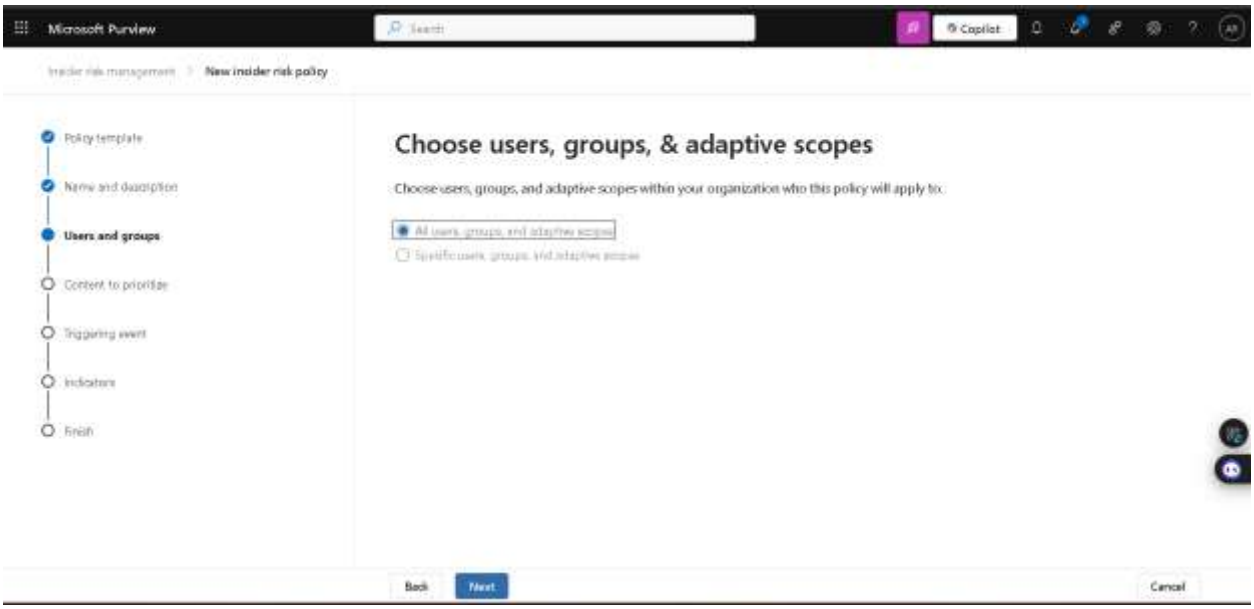
Step 3: We need a DLP policy to create this policy, and we already have a DLP policy created for protecting credit card details. We are going to use that here.



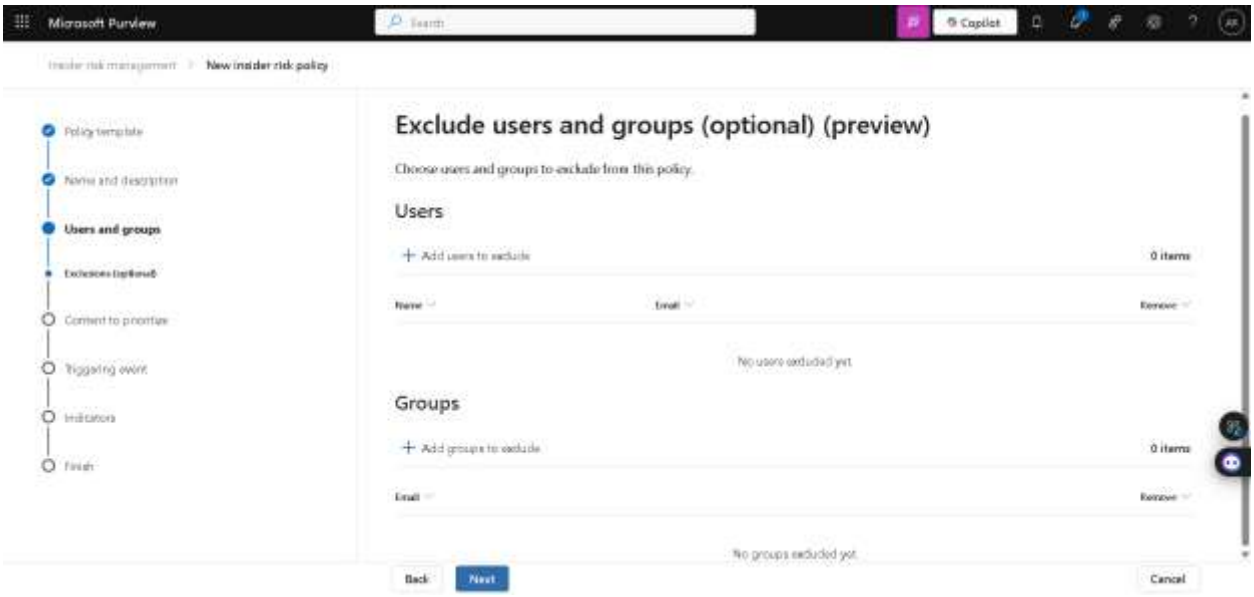
Step 4: Fill policy name and description, then click on next.



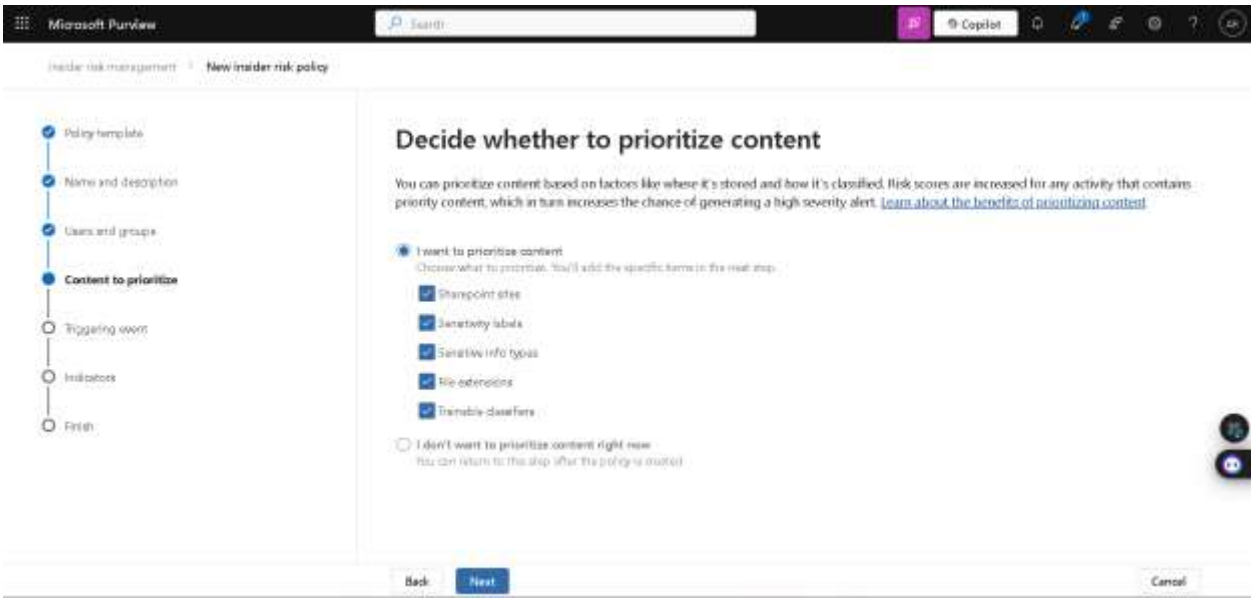
Step 5: Now, choose all user then next.



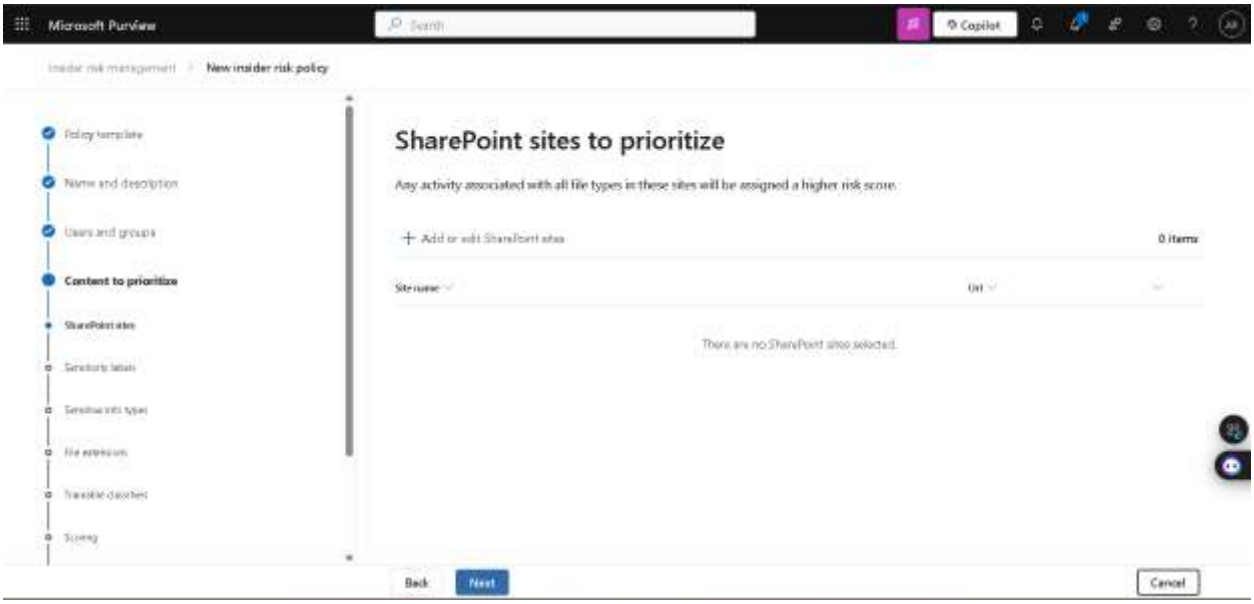
Step 6: We don't want to exclude any users or groups.



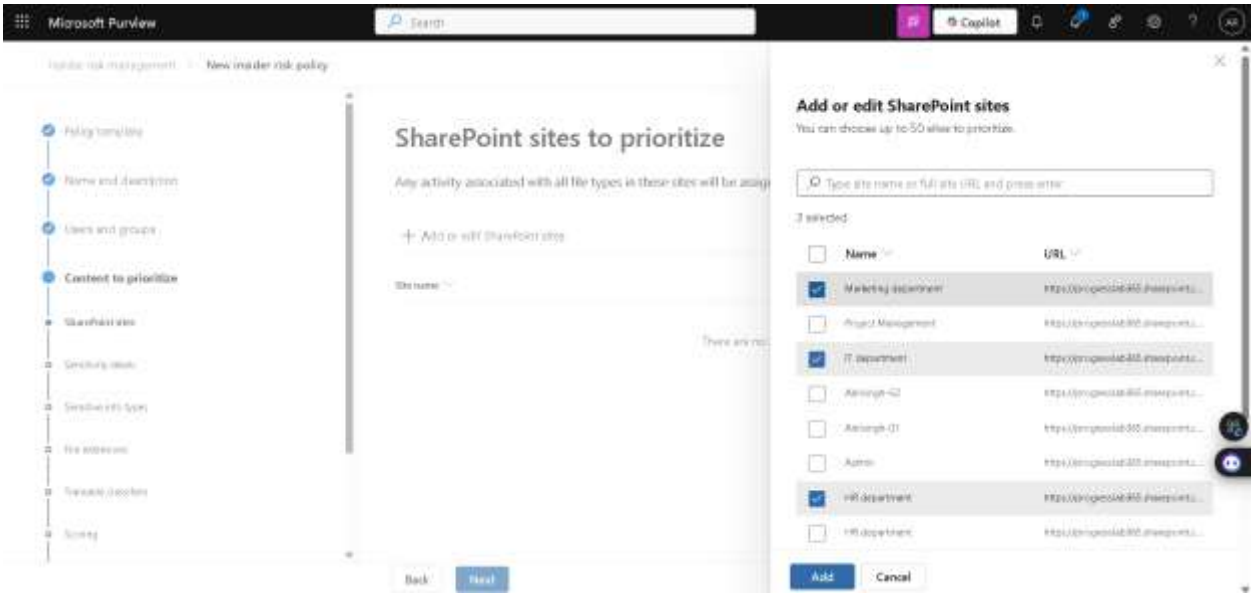
Step 7: Choose the content, we want to prioritize.



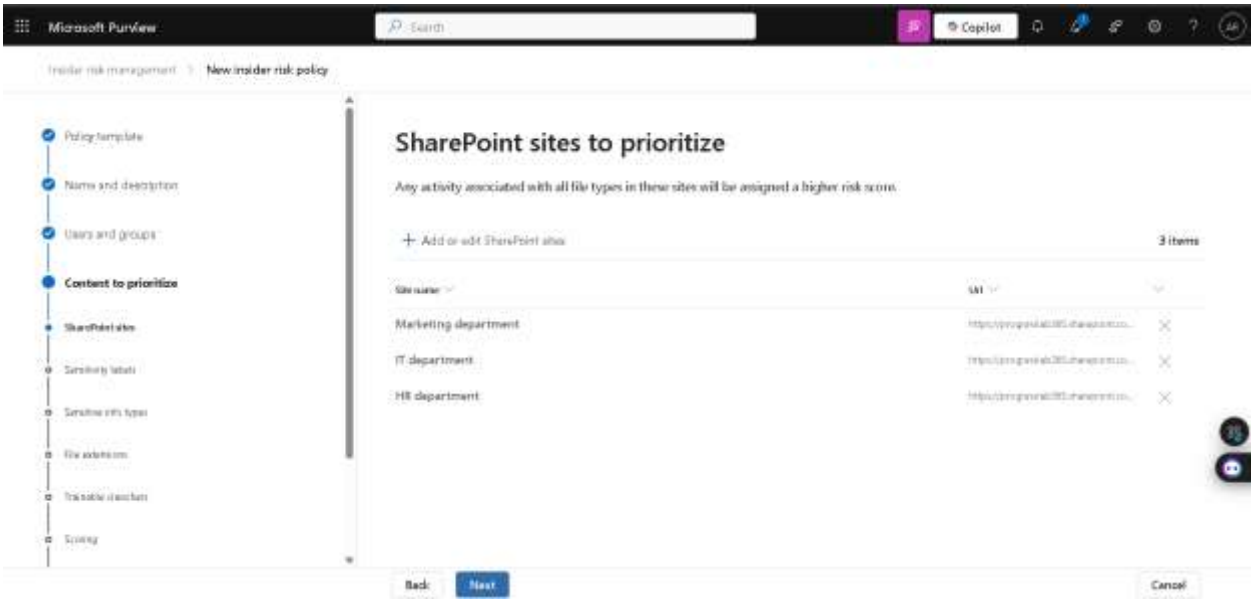
Step 8: To select SharePoint sites, click on add or edit SharePoint sites.



Step 9: Sleeted our target SharePoint sites then add.

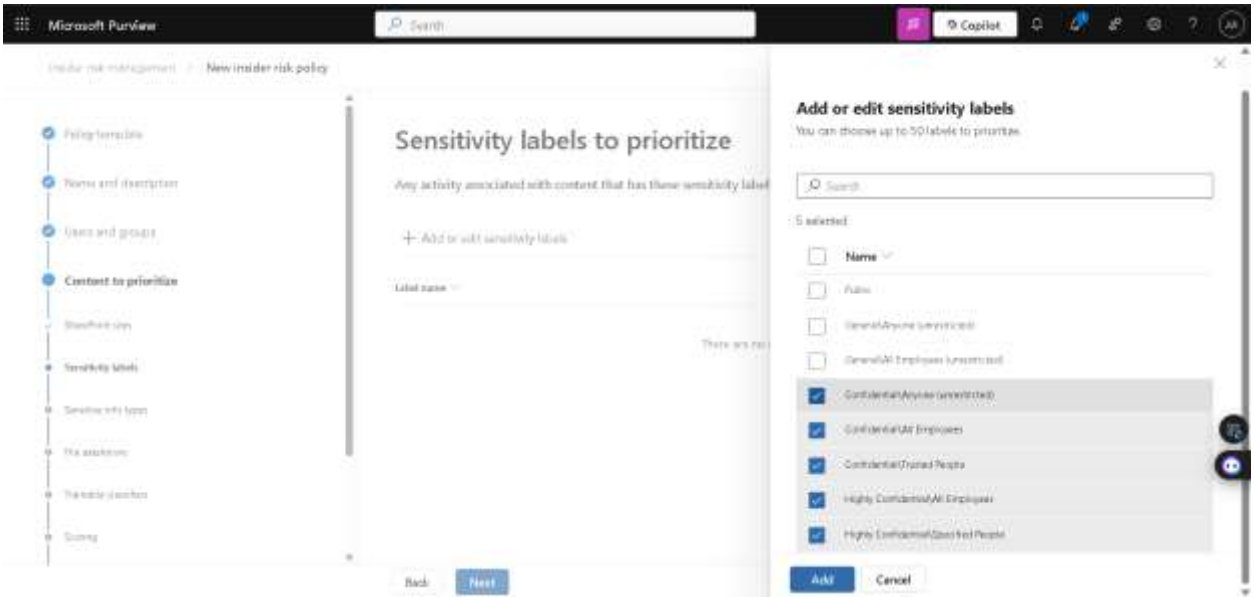


Step 10: Check SharePoint sites then next.

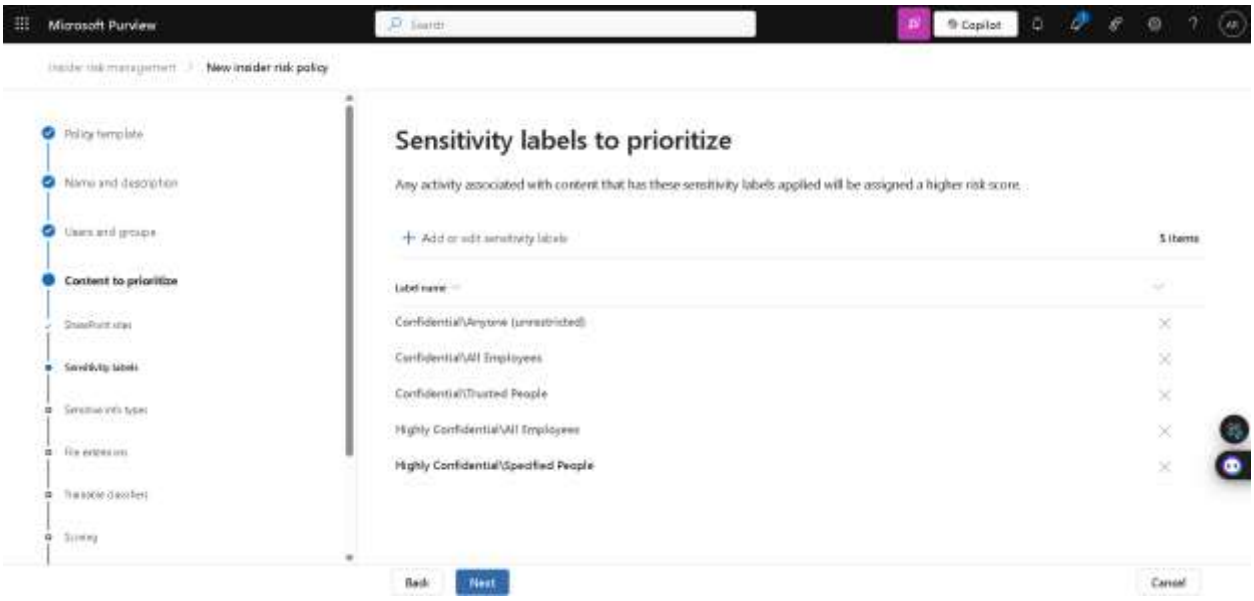


Step 11: To choose sensitivity labels to prioritize click on add or edit sensitivity labels.

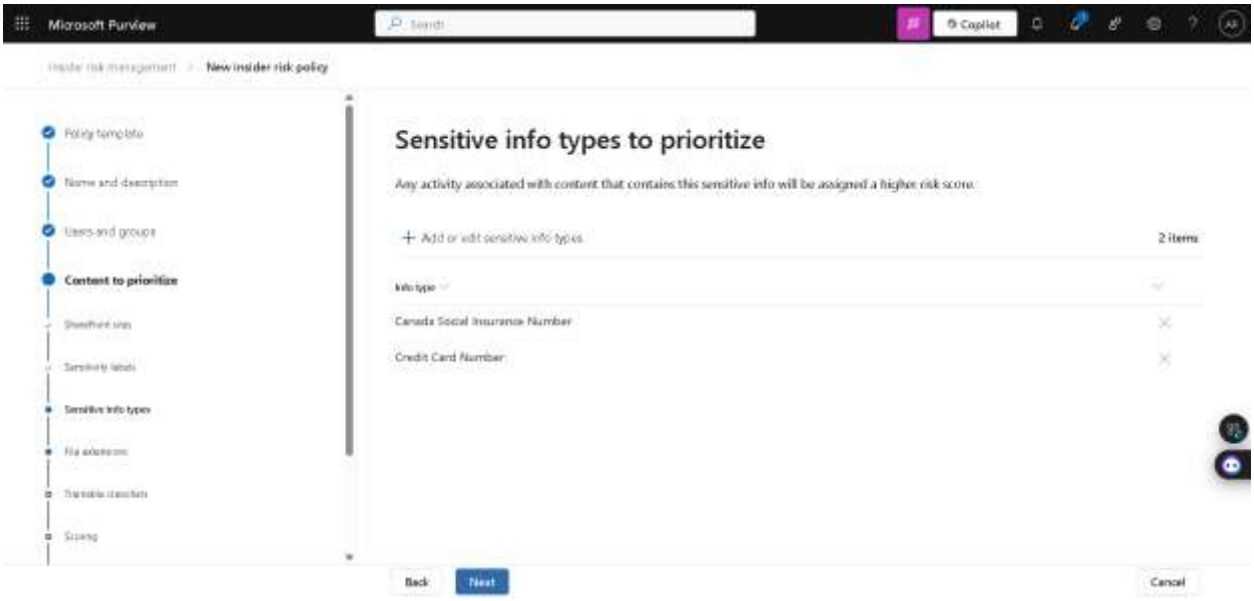
Step 12: Select all the sensitivity labels we need then add.



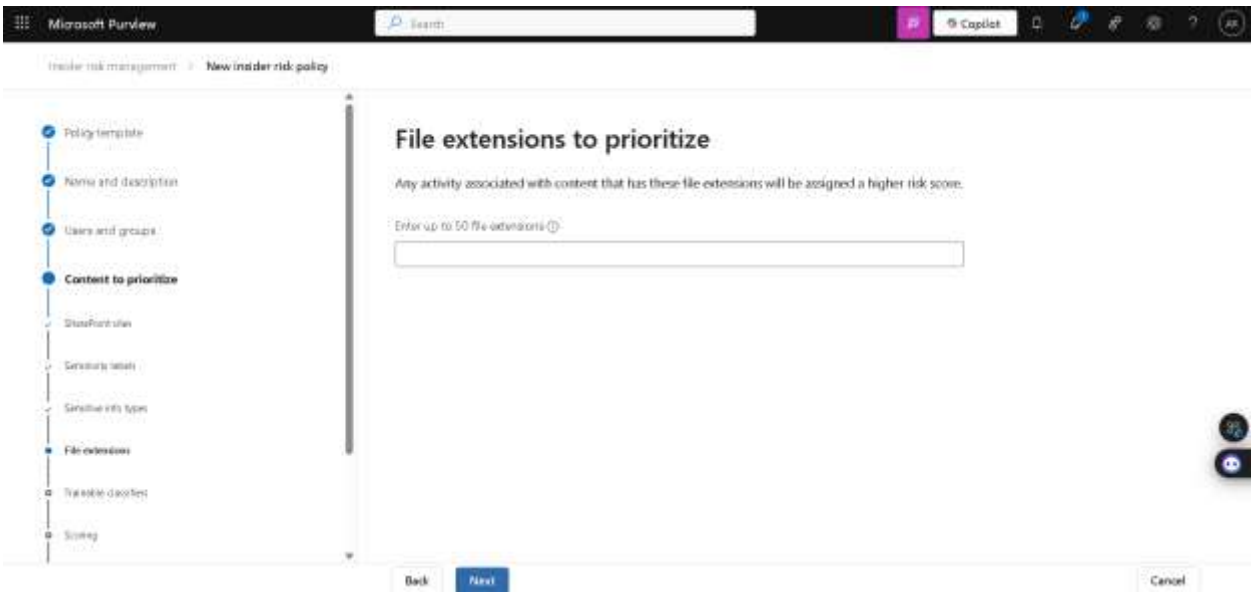
Step 13: Review our sensitivity labels details.



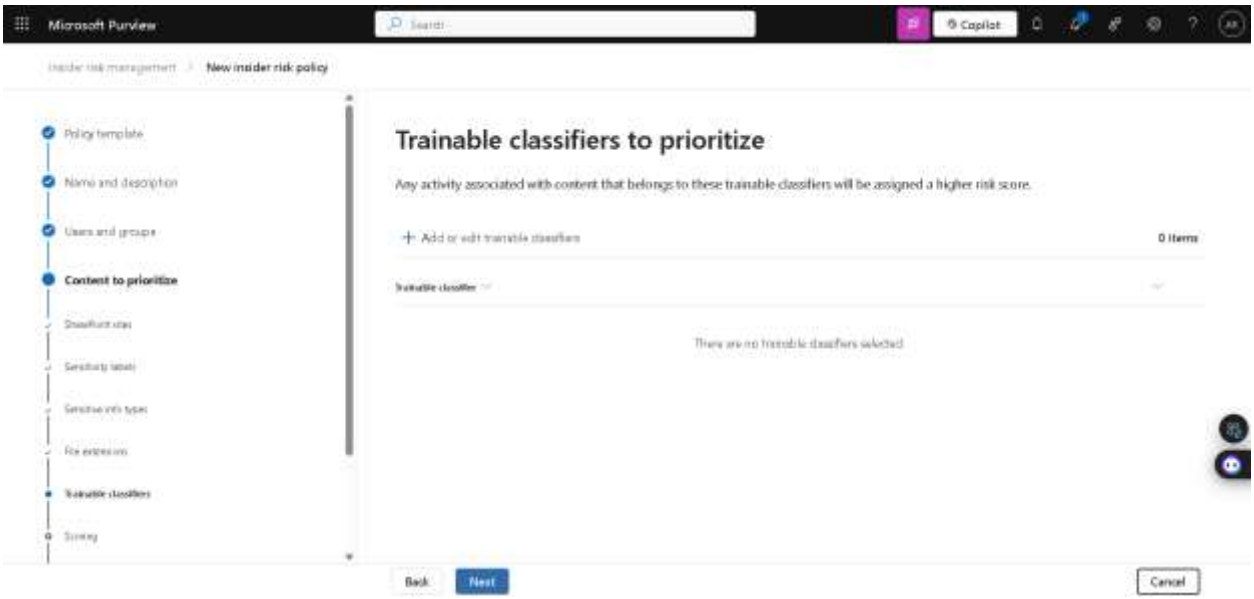
Step 14: Sensitivity info types, like in this policy we need credit cards. So, we selected credit cards here.



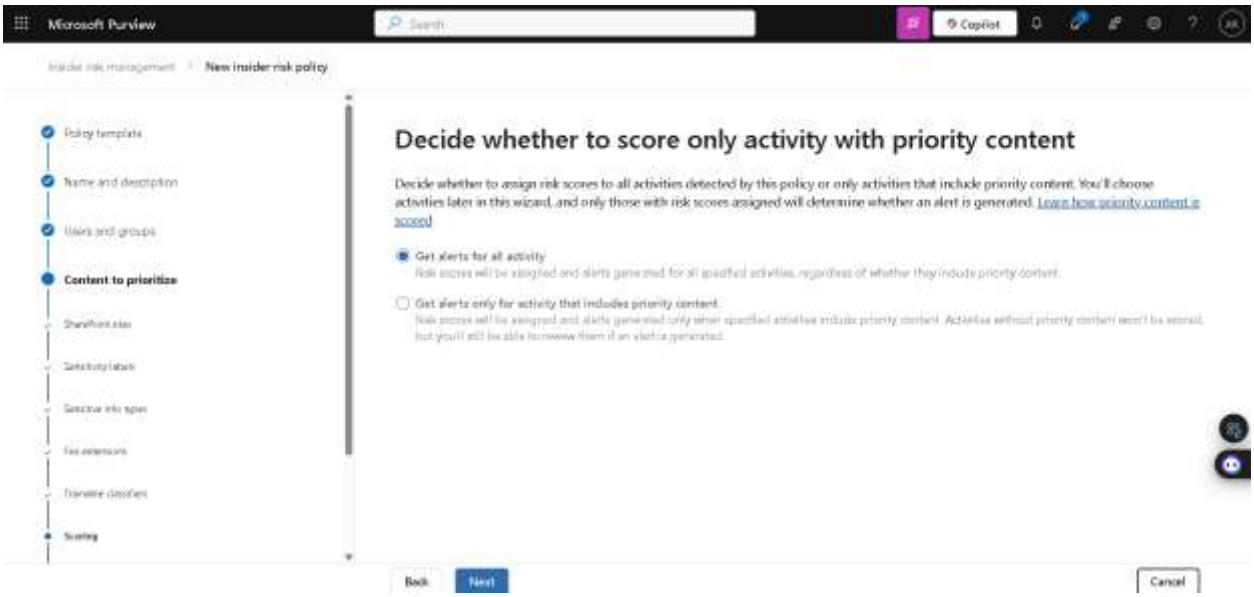
Step 15: We don't want to prioritize any file extensions.



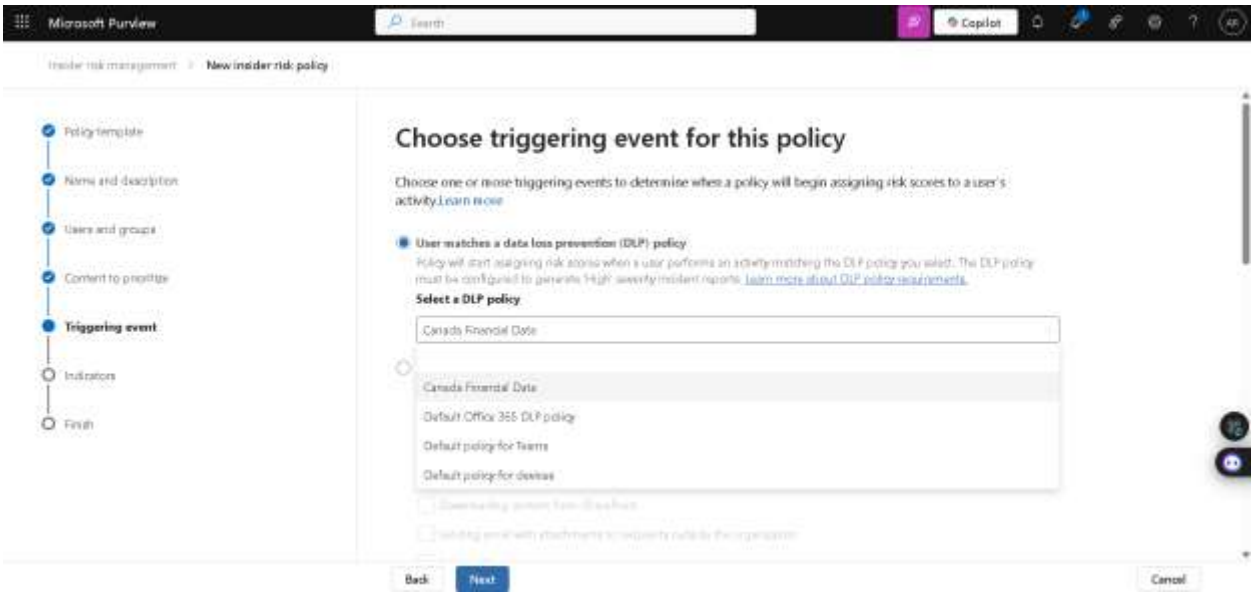
Step 16: We don't want to prioritize any trainable classifiers.



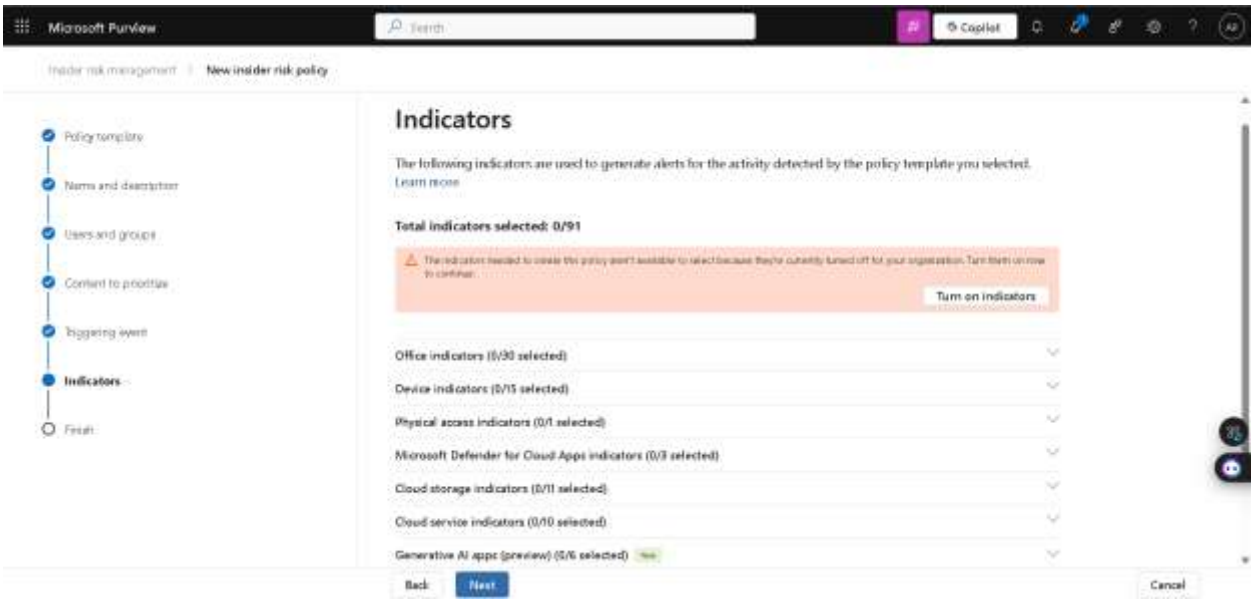
Step 17: we choose to get alerts for all activity.

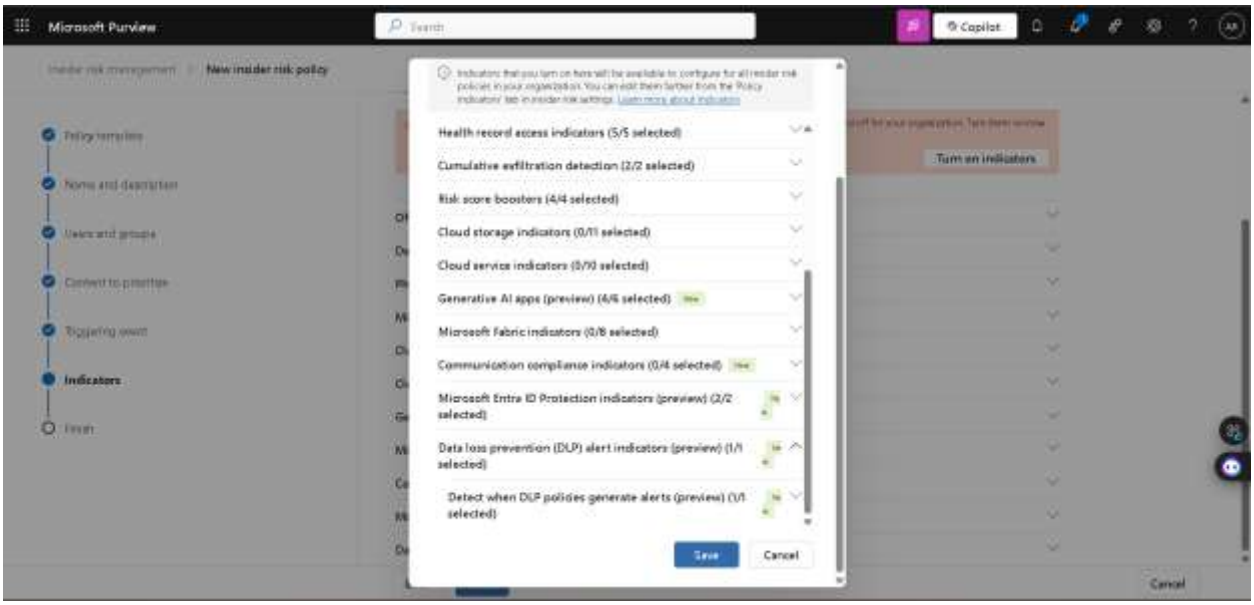


Step 18: Here we selected our DLP policy then next.

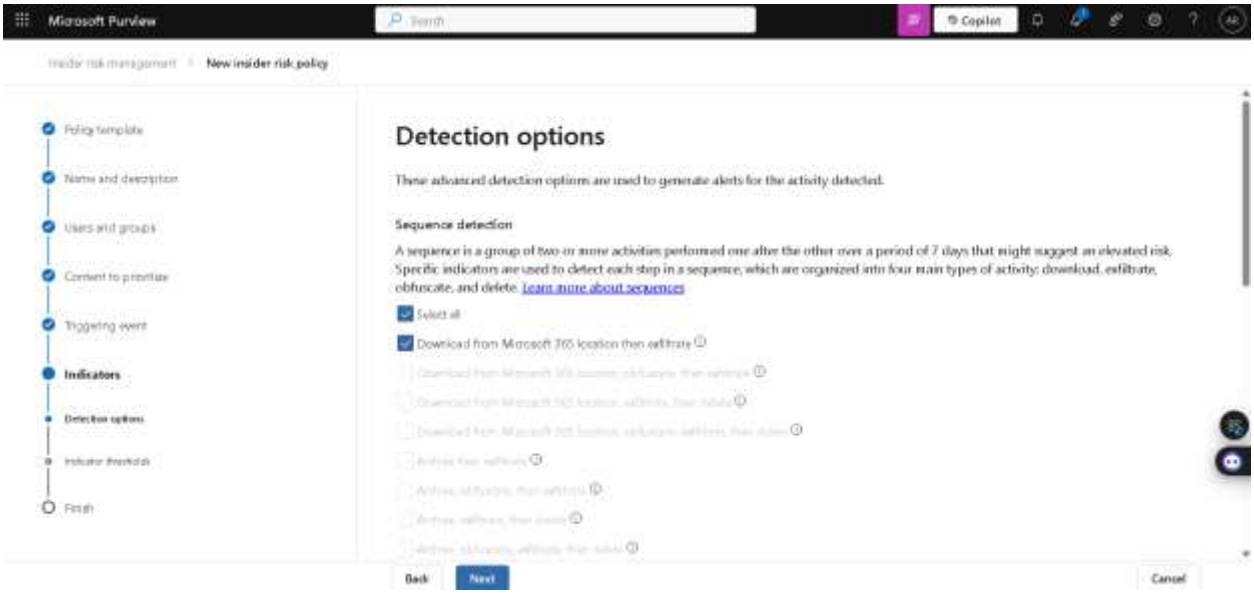


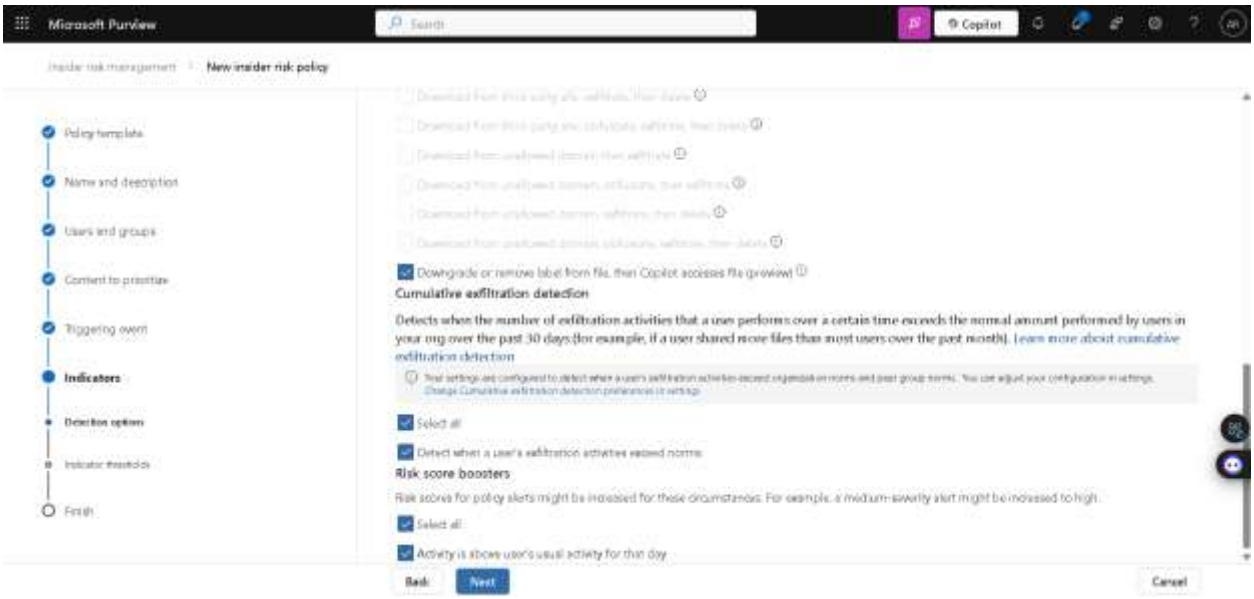
Step 19: Choose indicators from here.

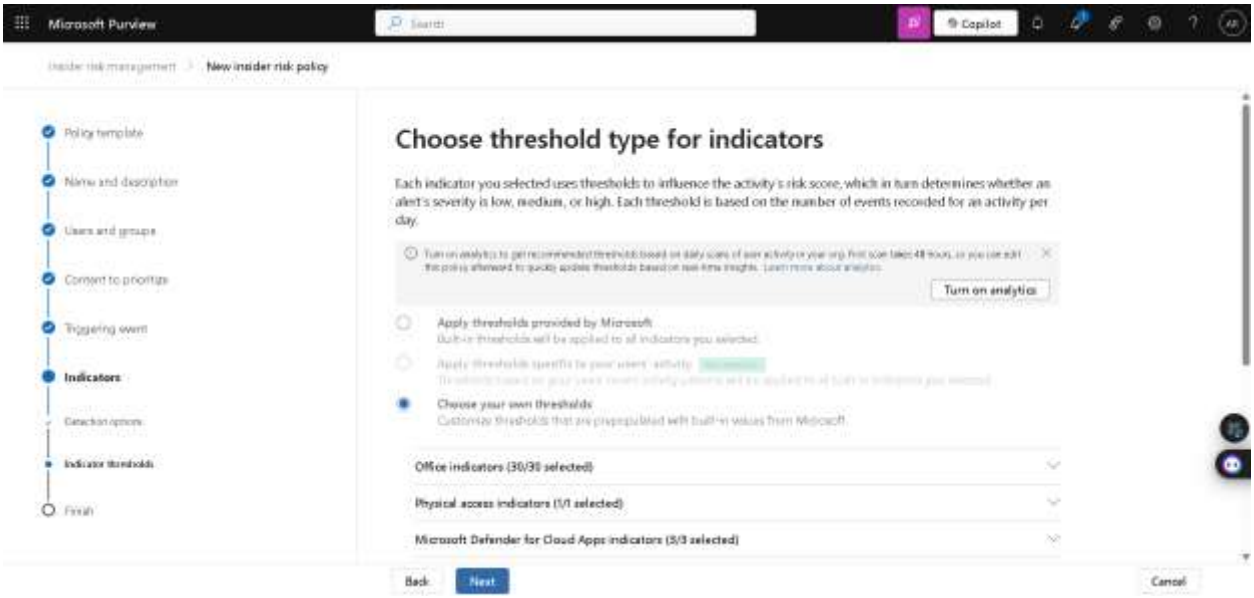




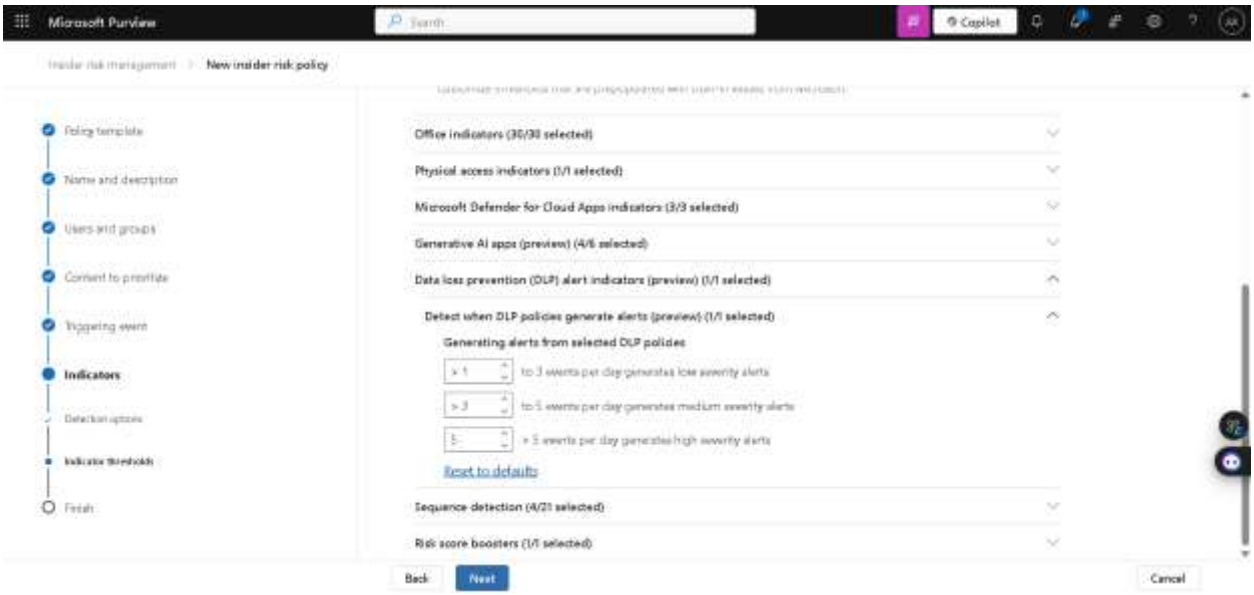
Step 20: Under detection option, we choose all then next.



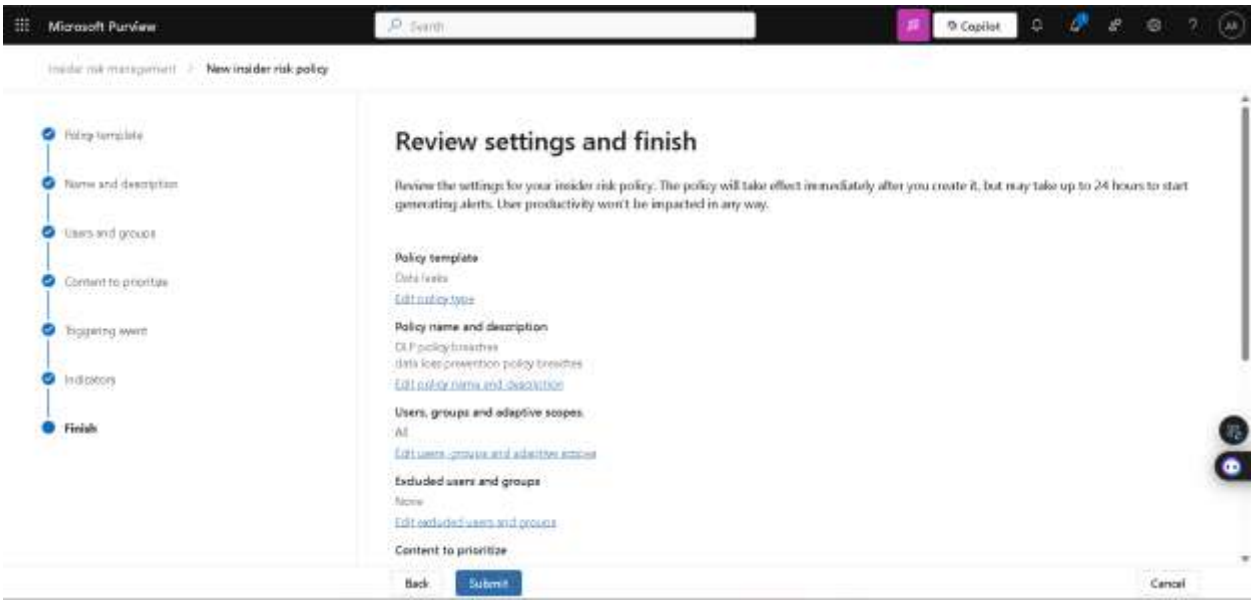




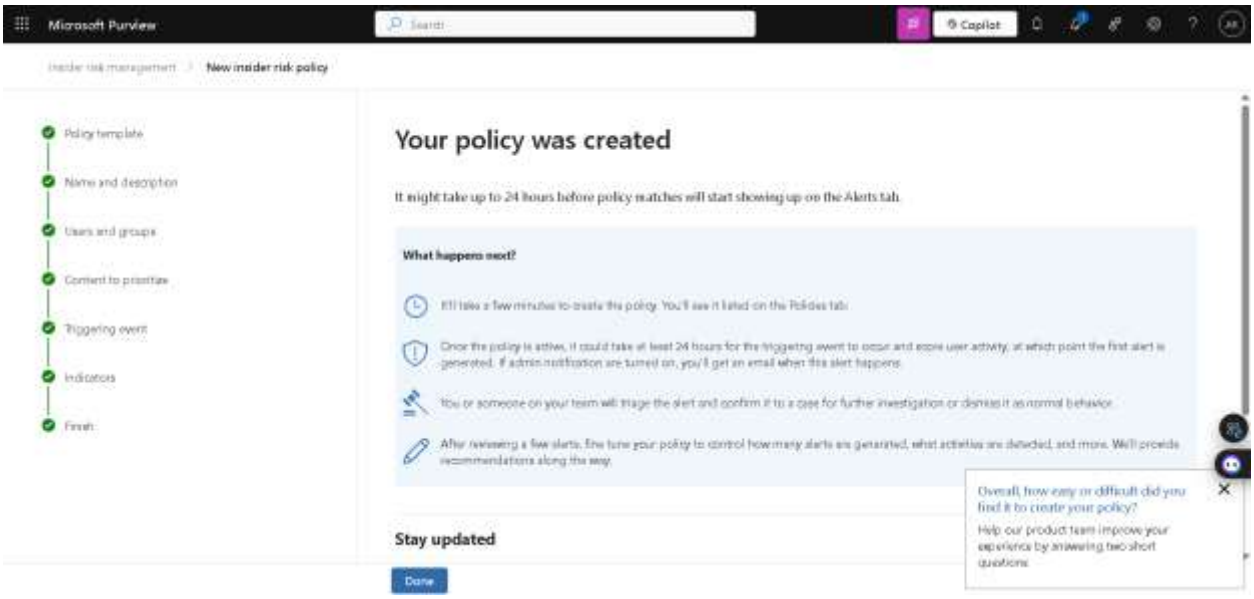
Step 21: Selected our alerts settings.



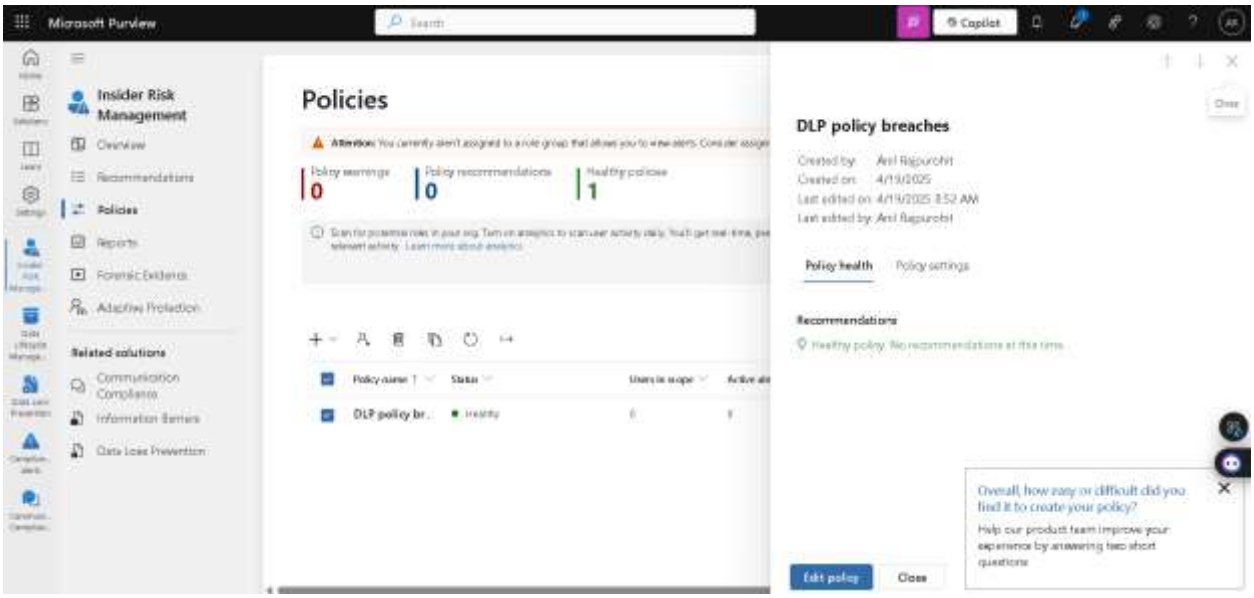
Step 22: Review settings of our policy then click on Submit.



Step 23: Our policy has been successfully created.



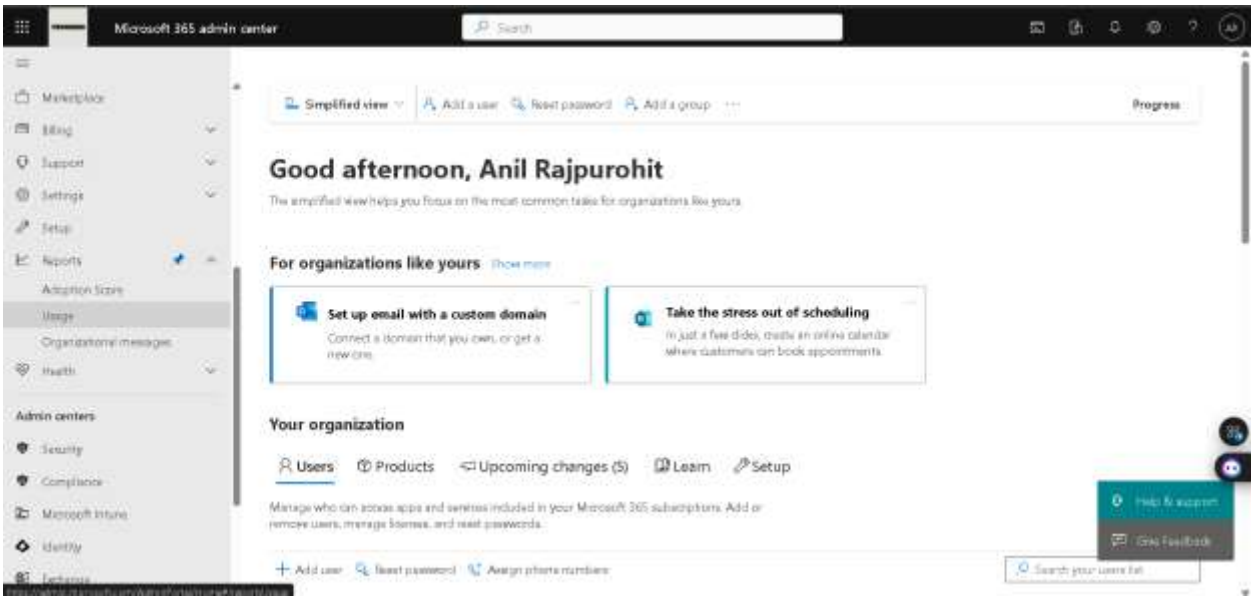
Step 24: We can view our policy under Insider risk management -> policies.



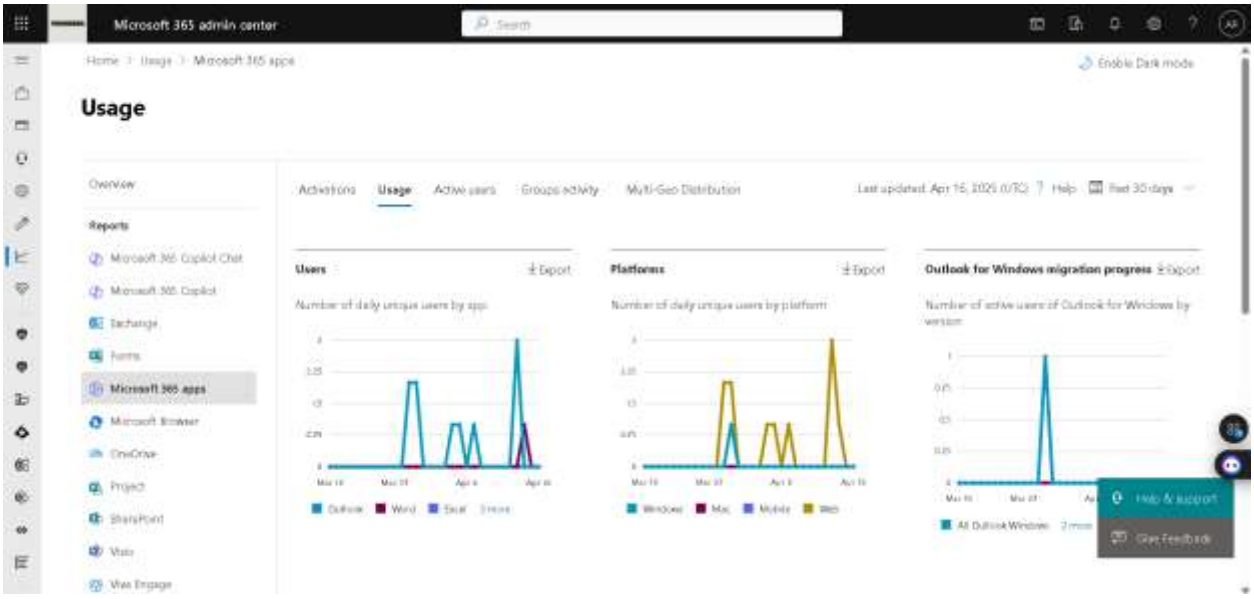
3. Generate Usage Reports:

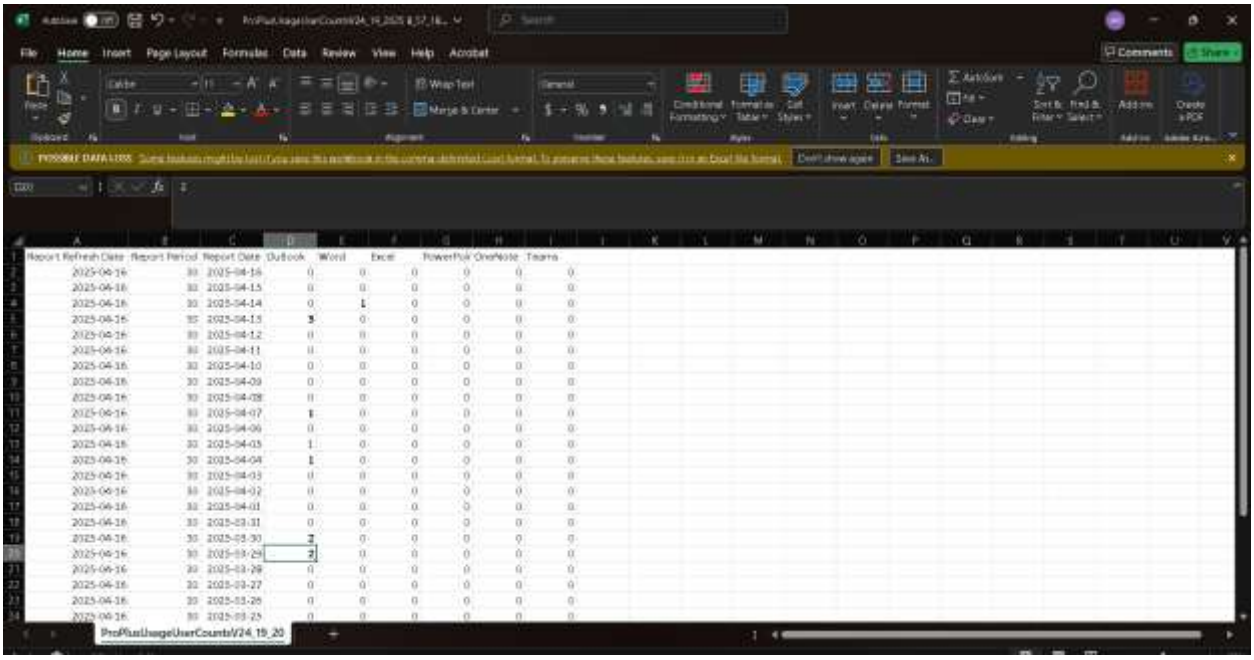
- Use the Microsoft 365 admin center to generate reports on user activity, email usage, and SharePoint site usage.

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

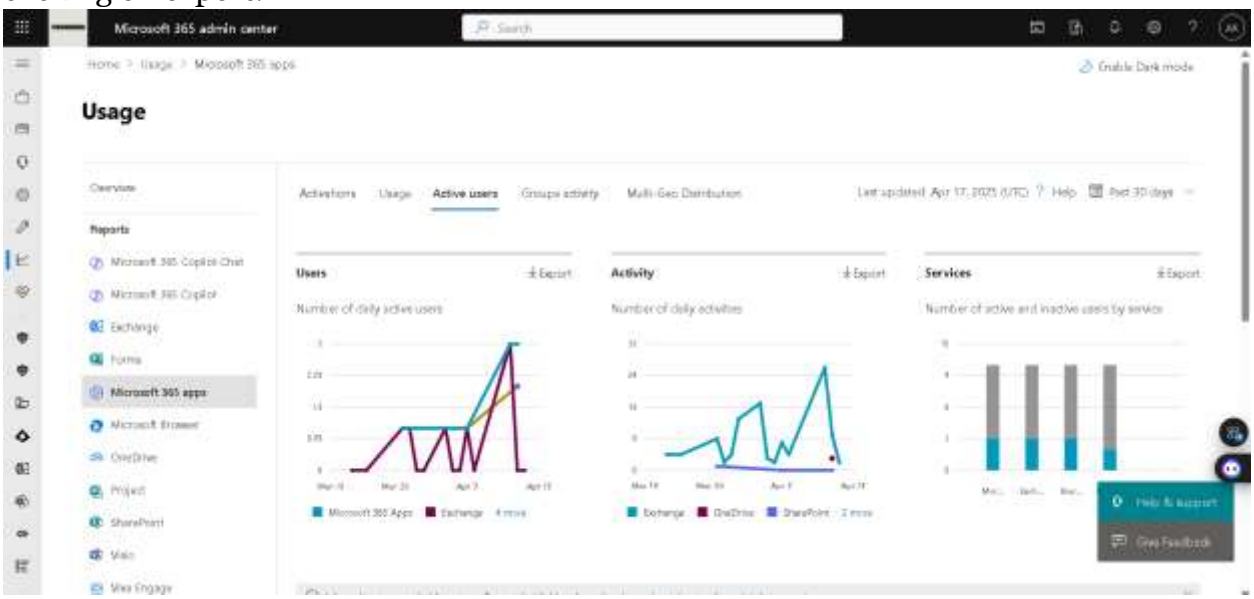


Step 2: Under Usage -> Microsoft 365 Apps -> usage. We can also export usage by clicking on export.

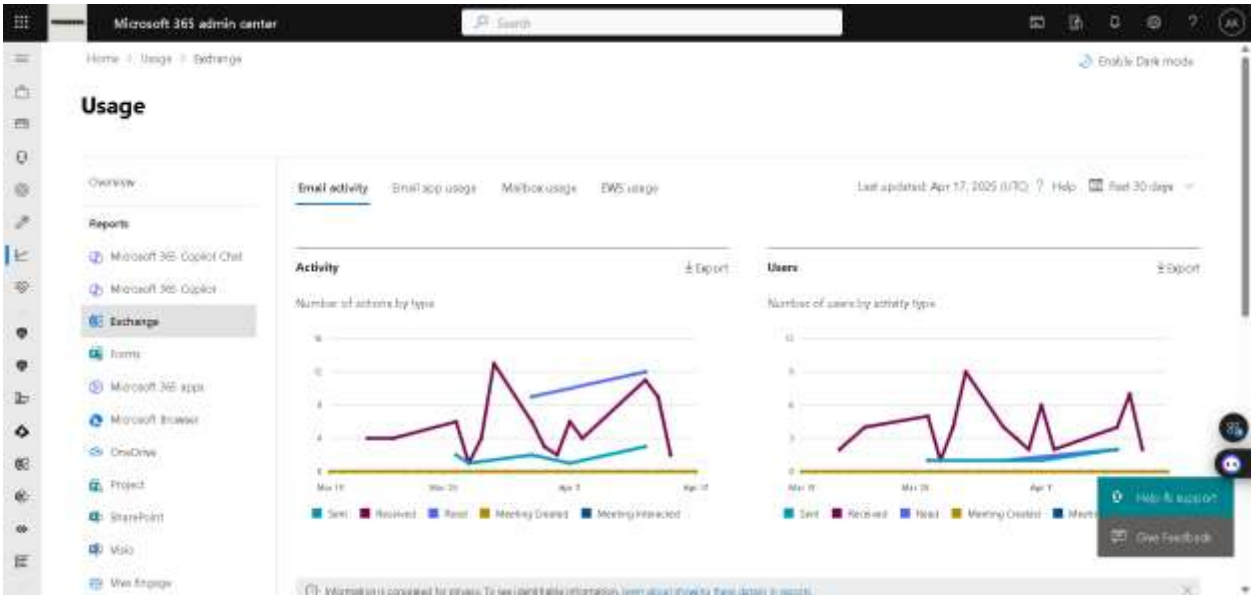


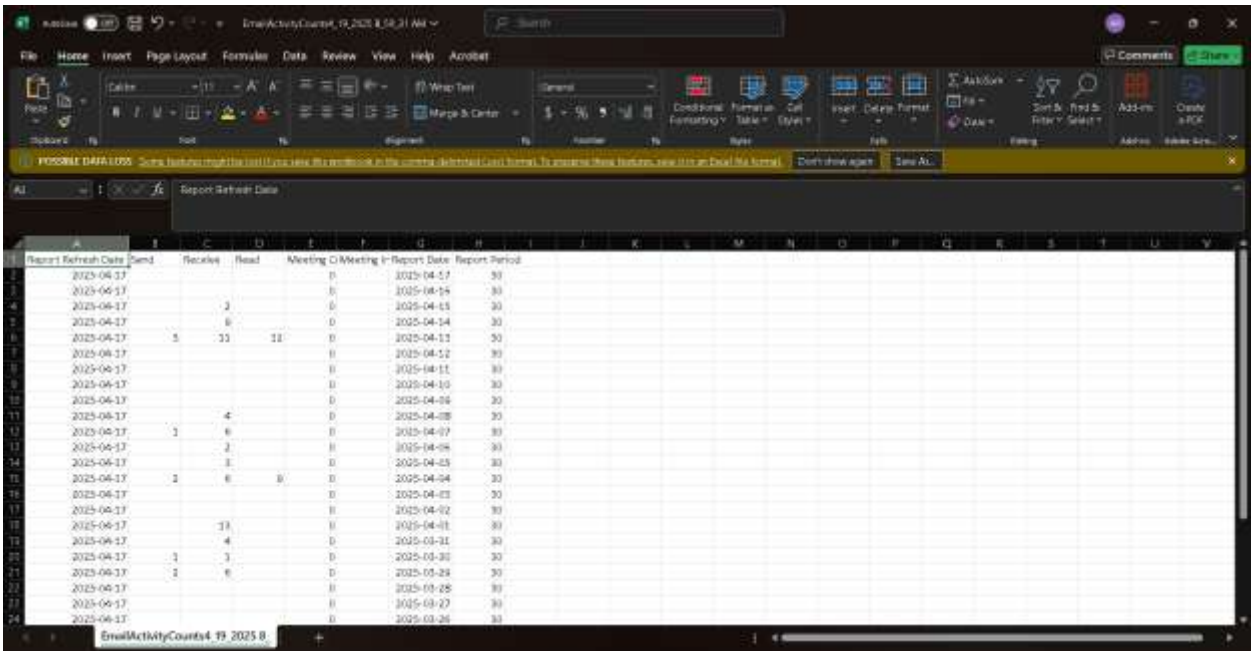


Step 3: Under Usage -> Microsoft 365 Apps -> active users. We can also export usage by clicking on export.

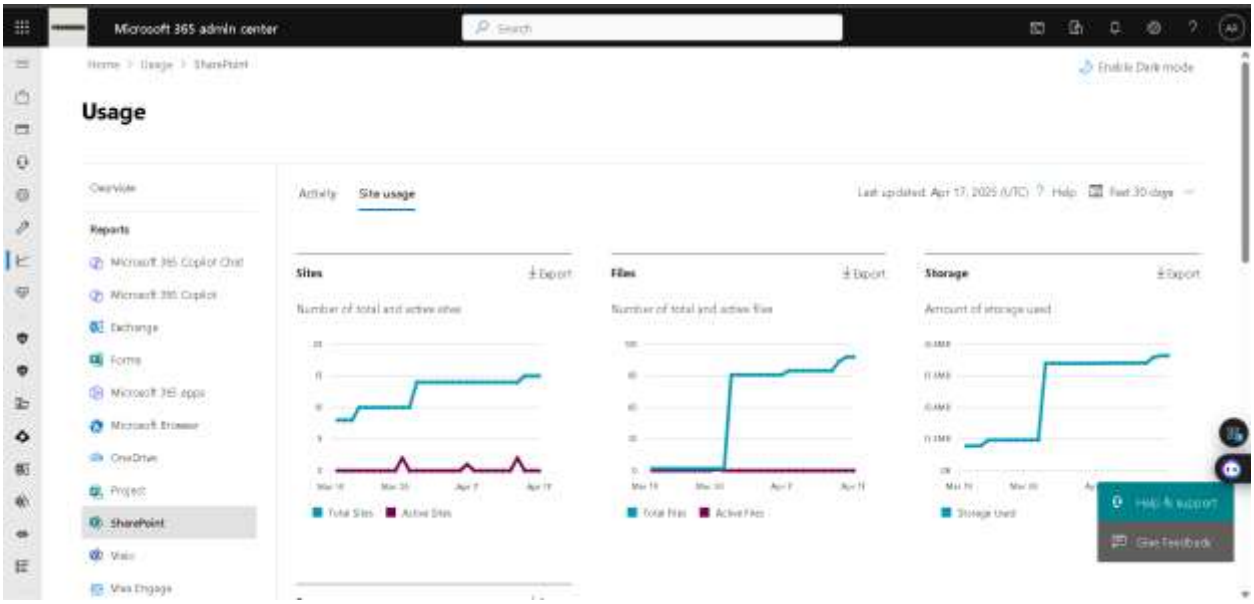


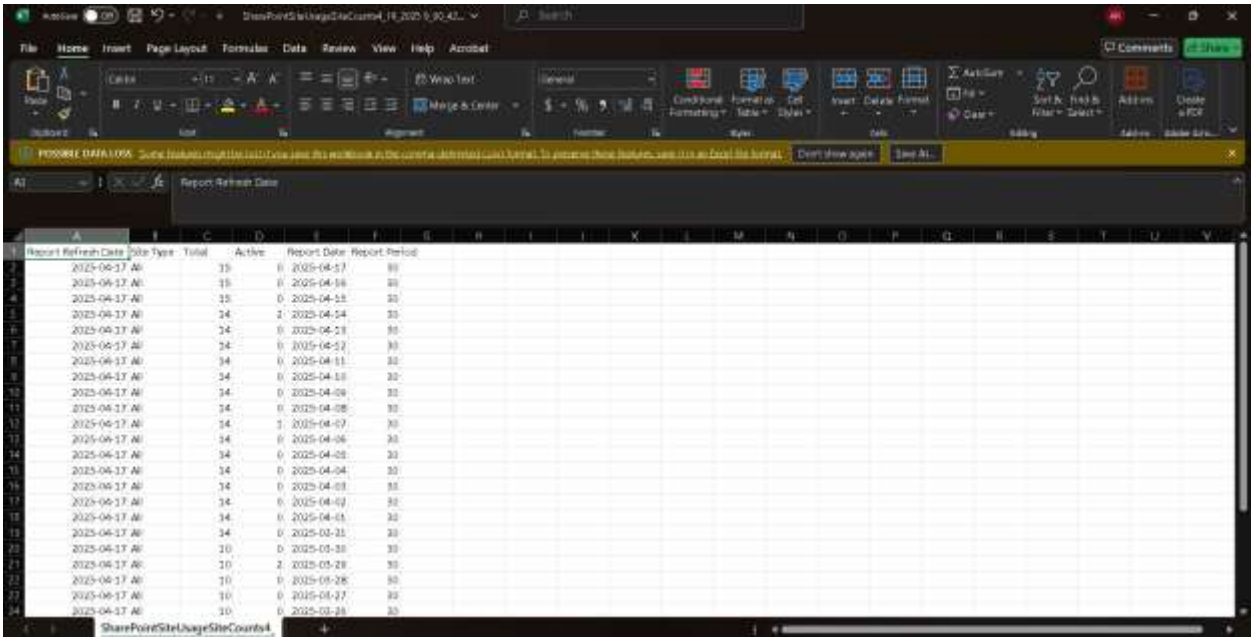
Step 4: Under Usage -> exchange -> email activity. We can also export usage by clicking on export.





Step 5: Under Usage -> SharePoint -> site usage. We can also export usage by clicking on export.

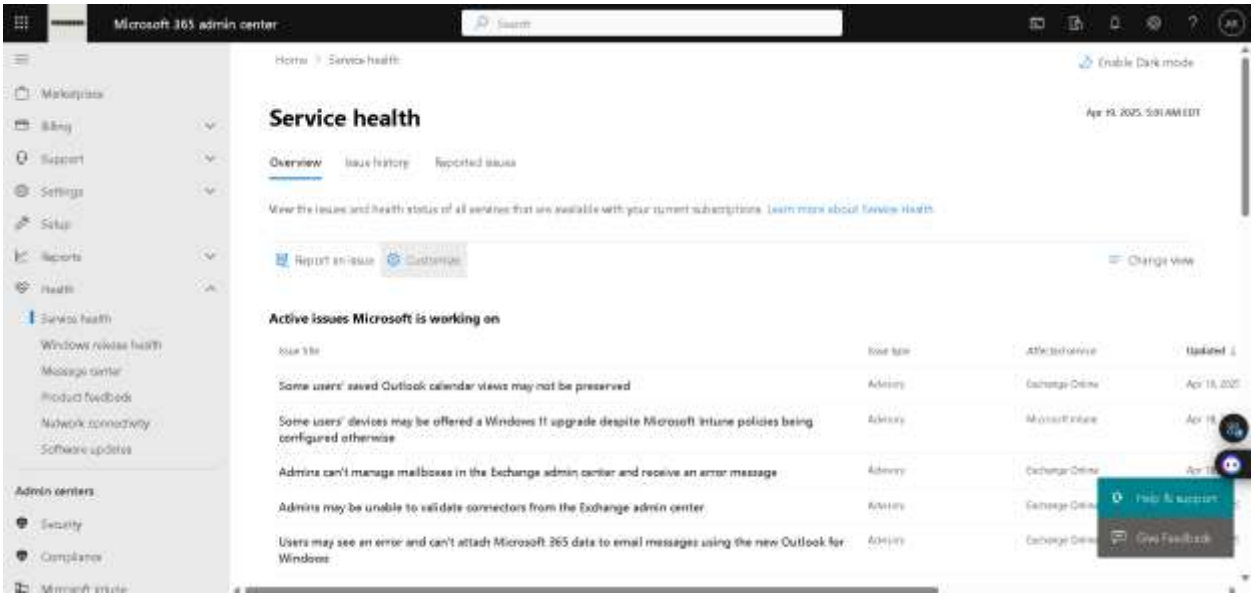




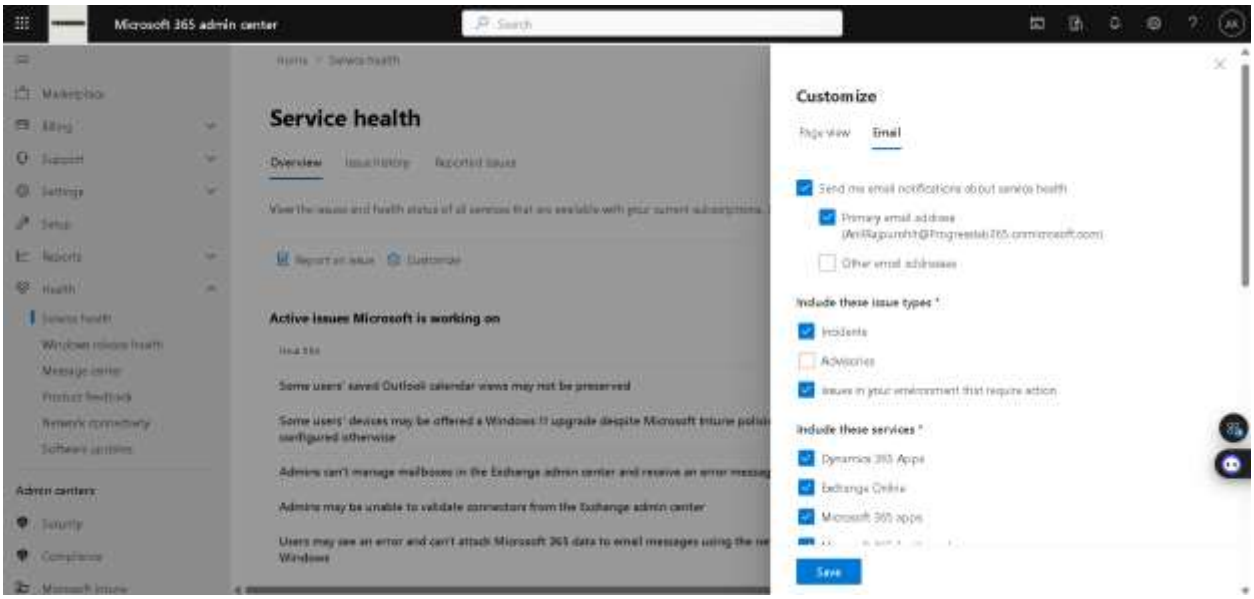
4. Implement and Monitor Service Health:

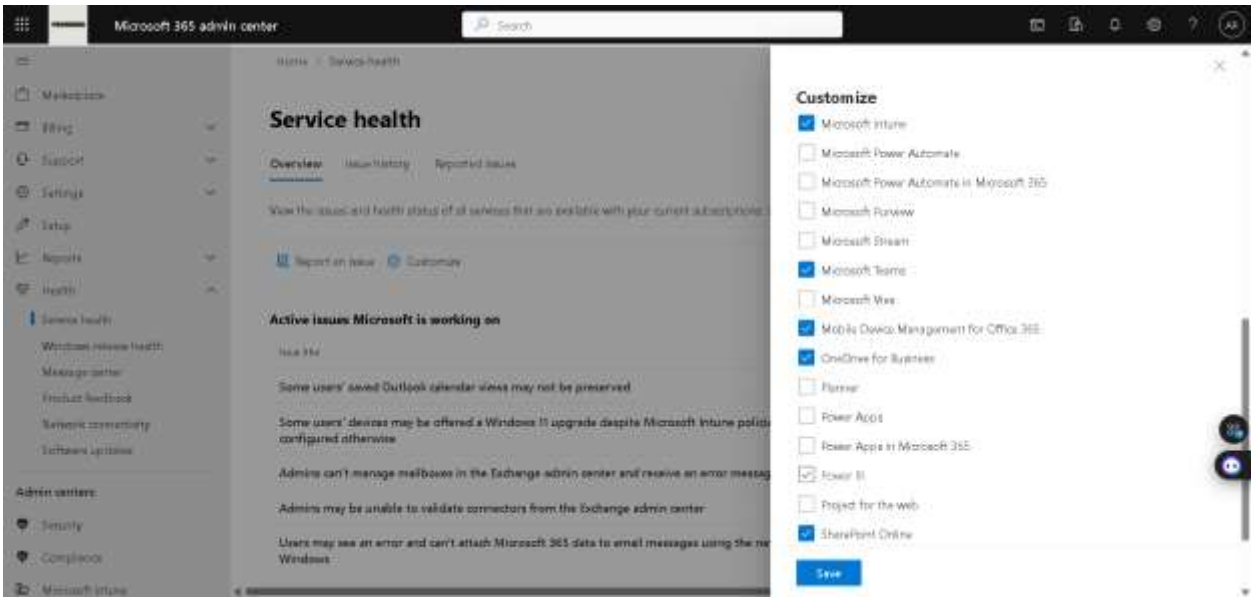
- Set up service health alerts to notify administrators of any issues with Microsoft 365 services.

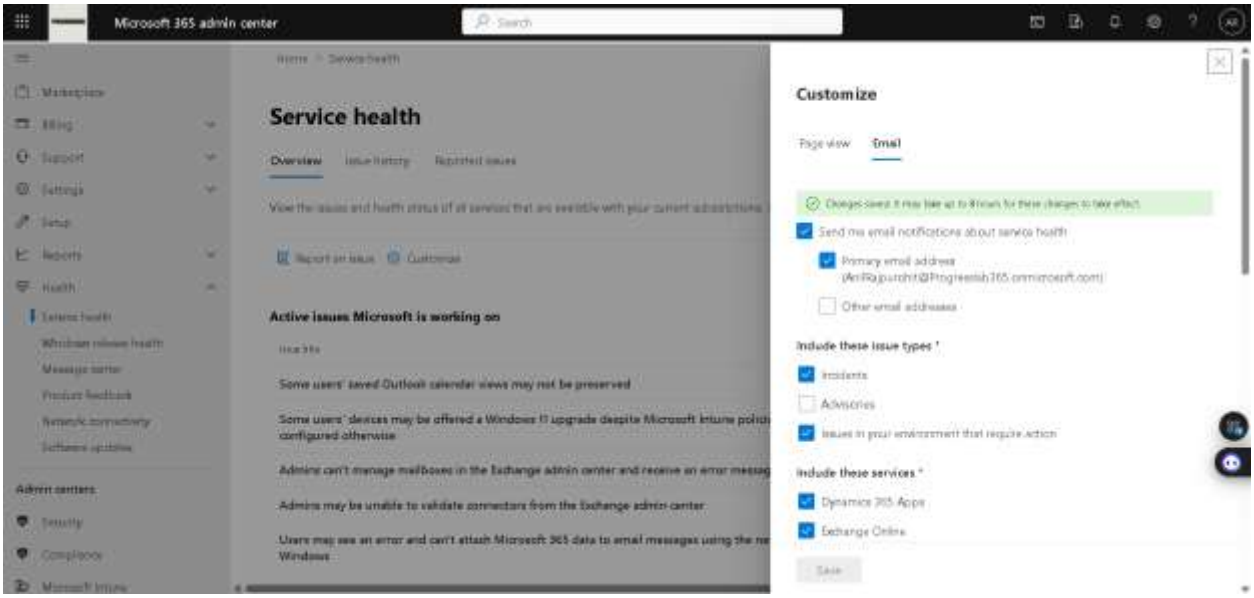
Step 1: In Microsoft 365 admin center, health -> service health -> customize.



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

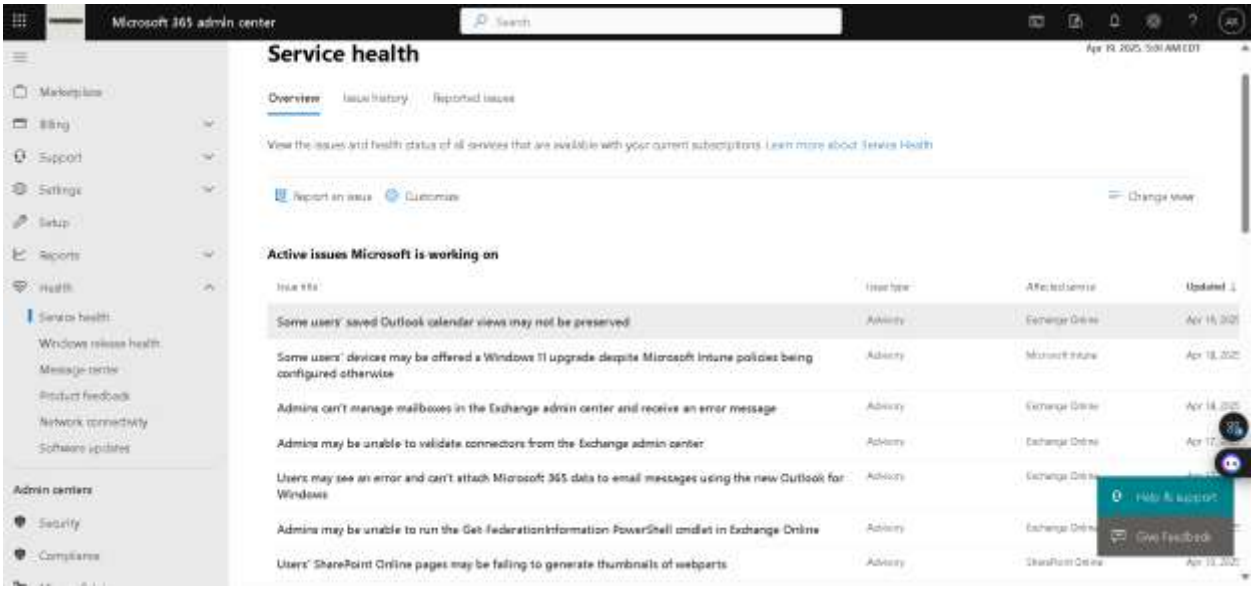


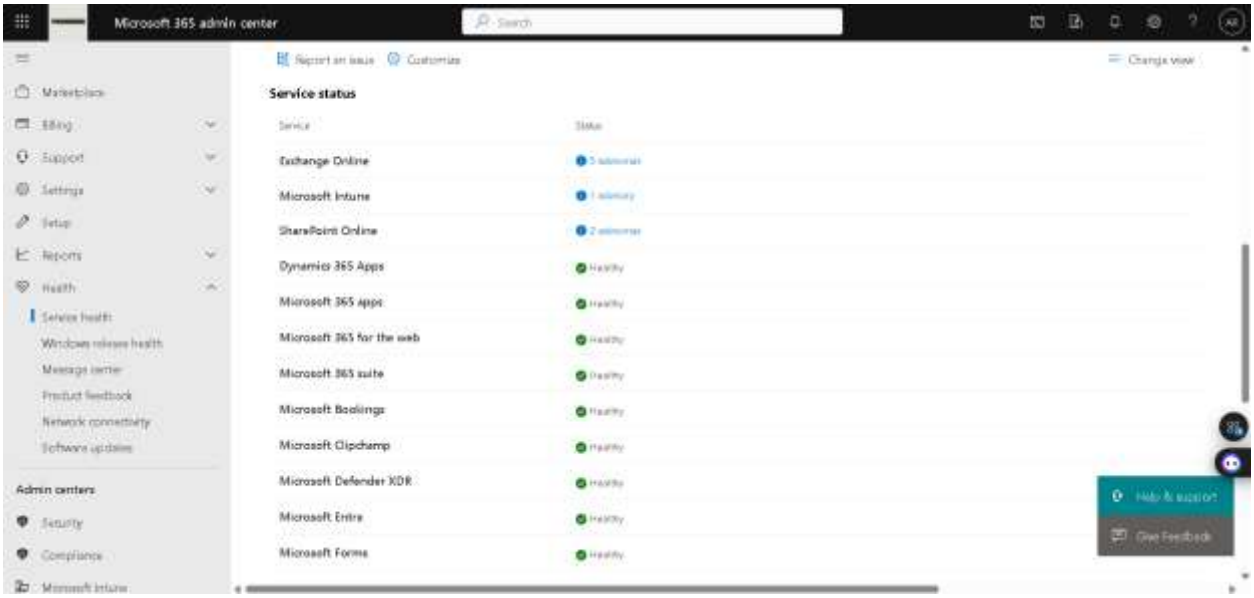




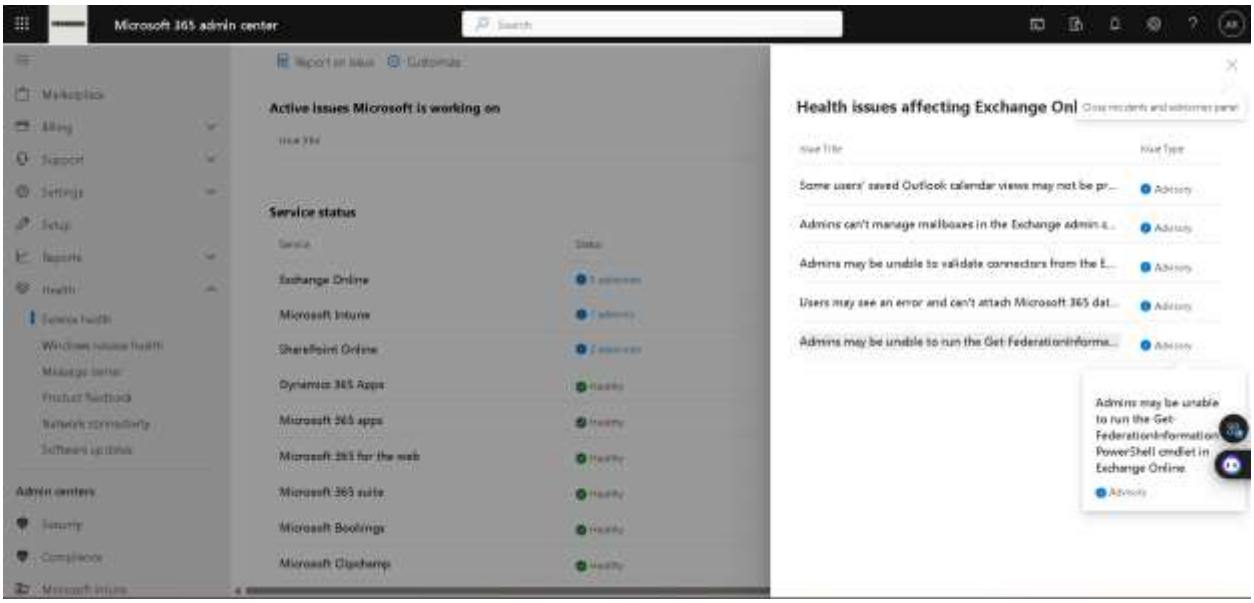
- Monitor the Service Health dashboard regularly to ensure all services are running smoothly.

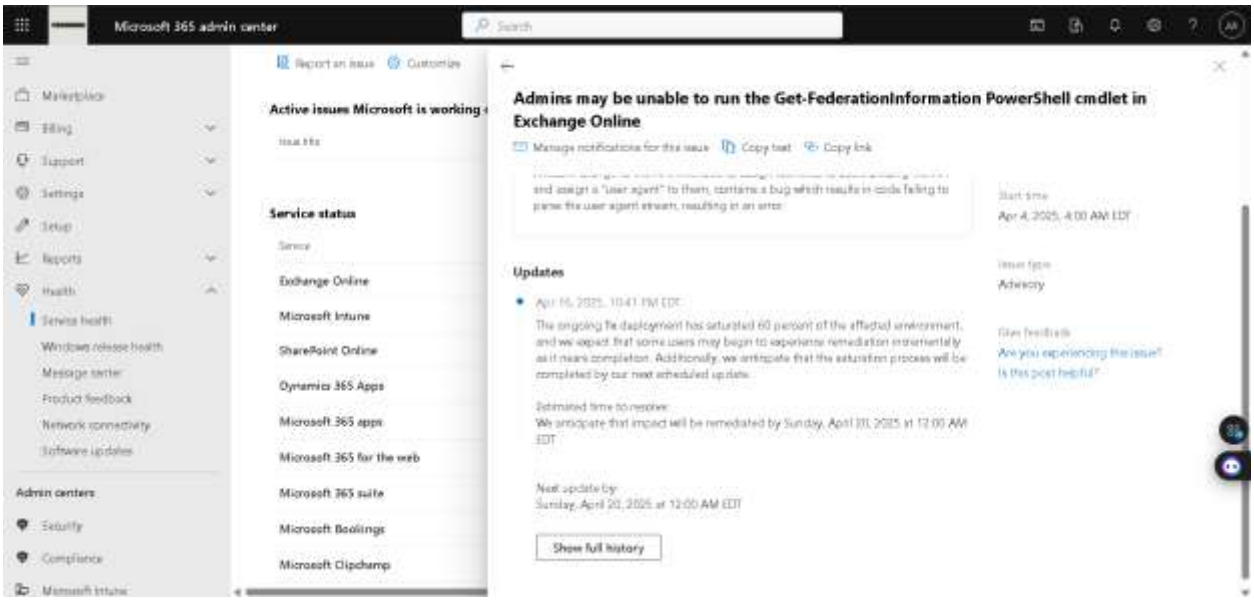
Step 1: To monitor the Service Health dashboard, in Microsoft 365 admin center -> health -> service health.



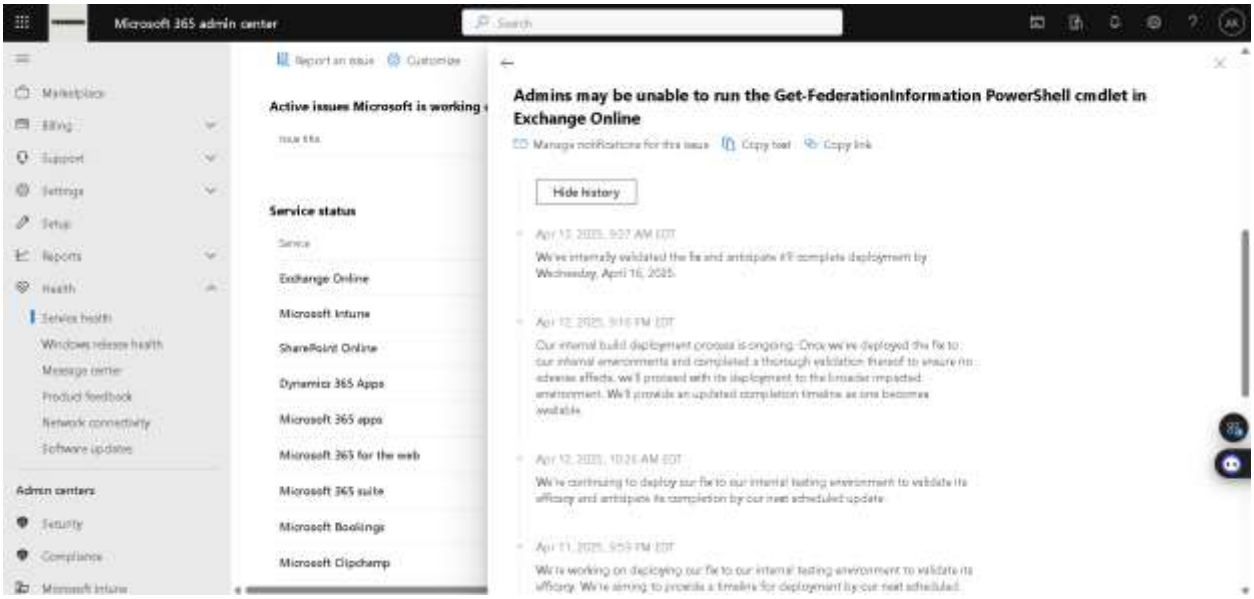


Step 2: We can check info about advisories for many services, and we should stay updated about those services .So, We can help our users accordingly.





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.