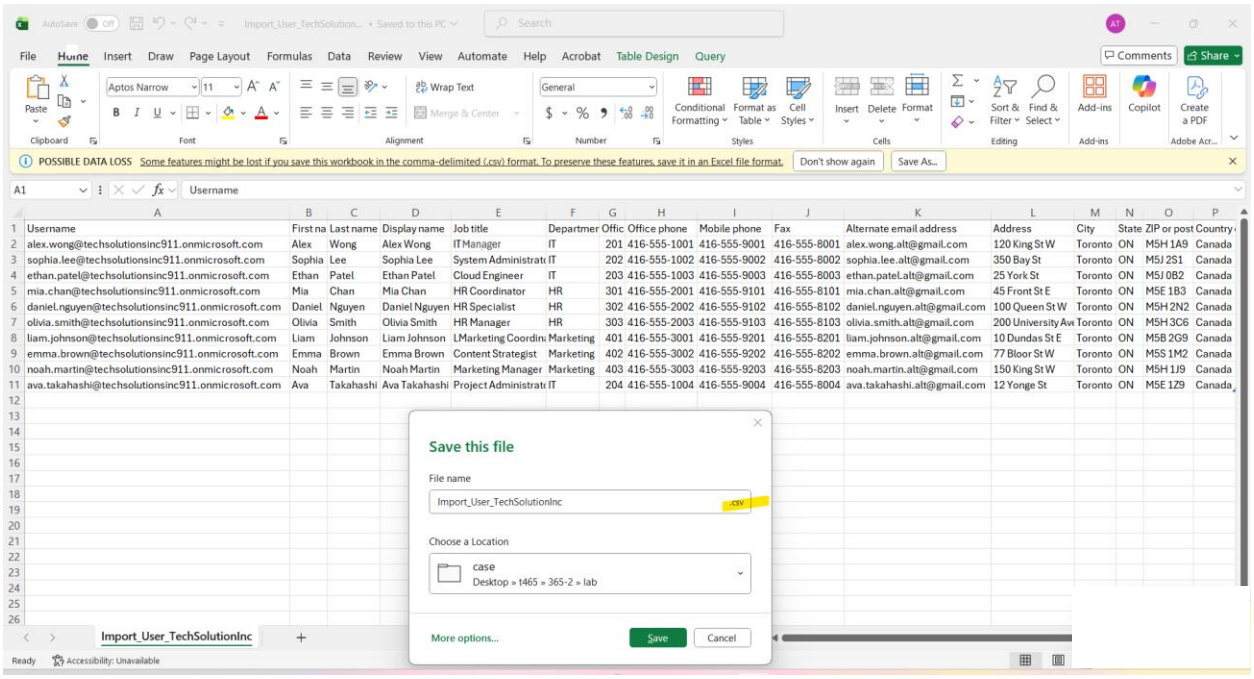
Microsoft 365 Enterprise Security and Operations

Project Overview

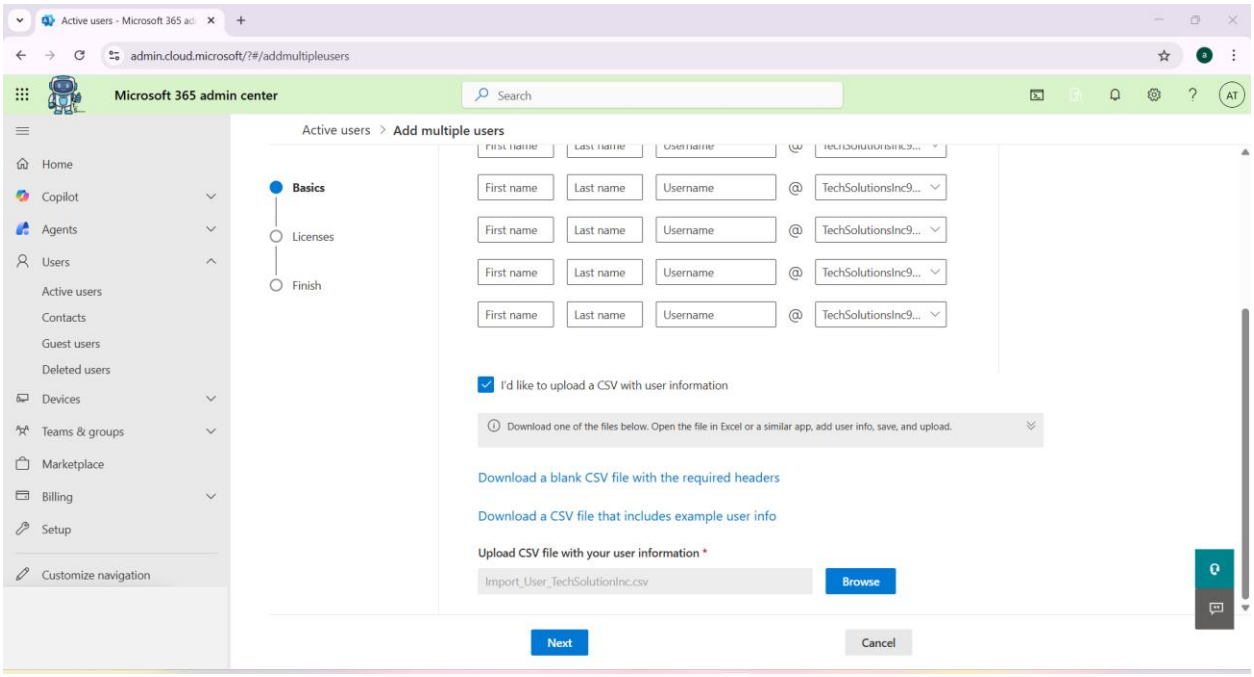
This document presents hands-on experience managing a Microsoft 365 environment in an enterprise context, with a focus on security, compliance, collaboration services, monitoring, and operational governance. The content reflects real-world administrative responsibilities involved in maintaining secure, compliant, and reliable Microsoft 365 services at scale.

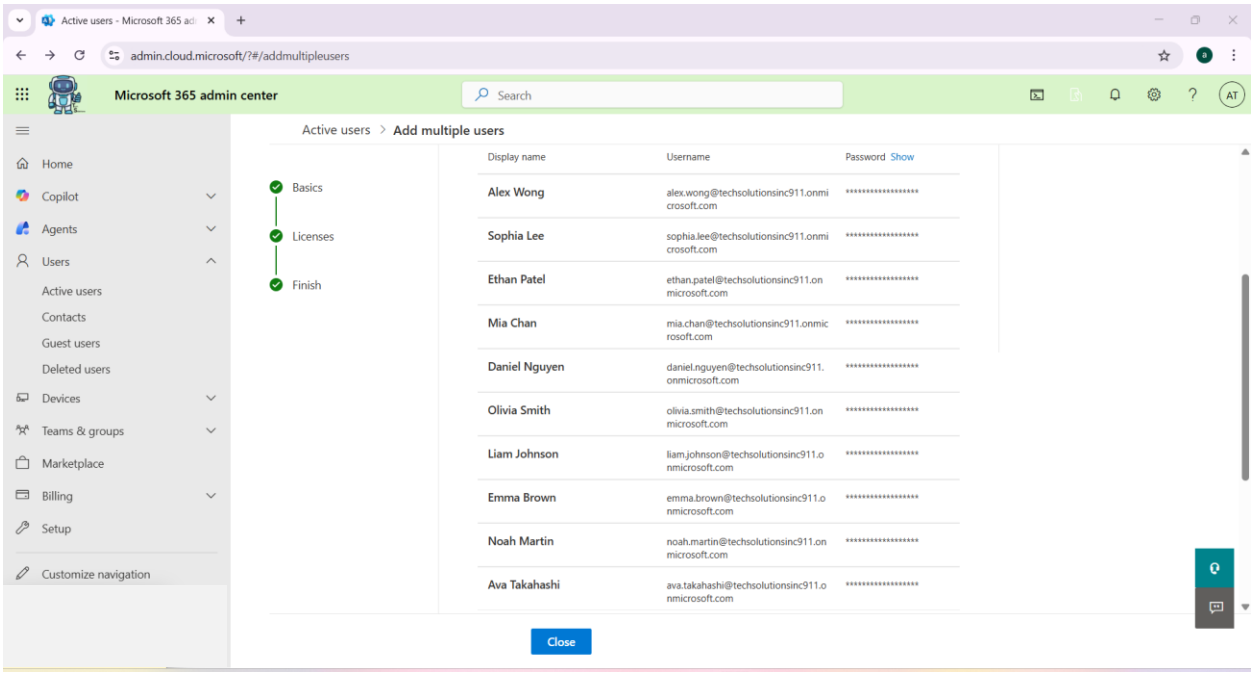
Tenant and User Foundation Management

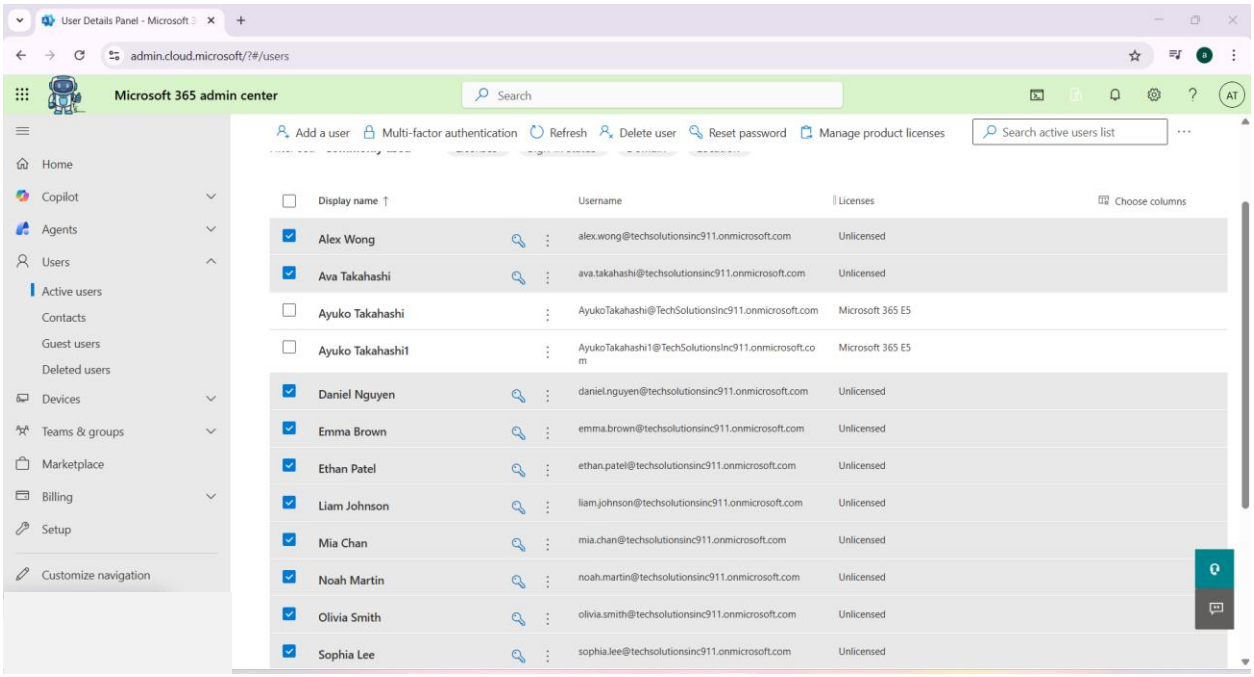
This section documents the foundational configuration of a Microsoft 365 tenant, including bulk user provisioning, license assignment, and user profile standardization to support scalable identity management.



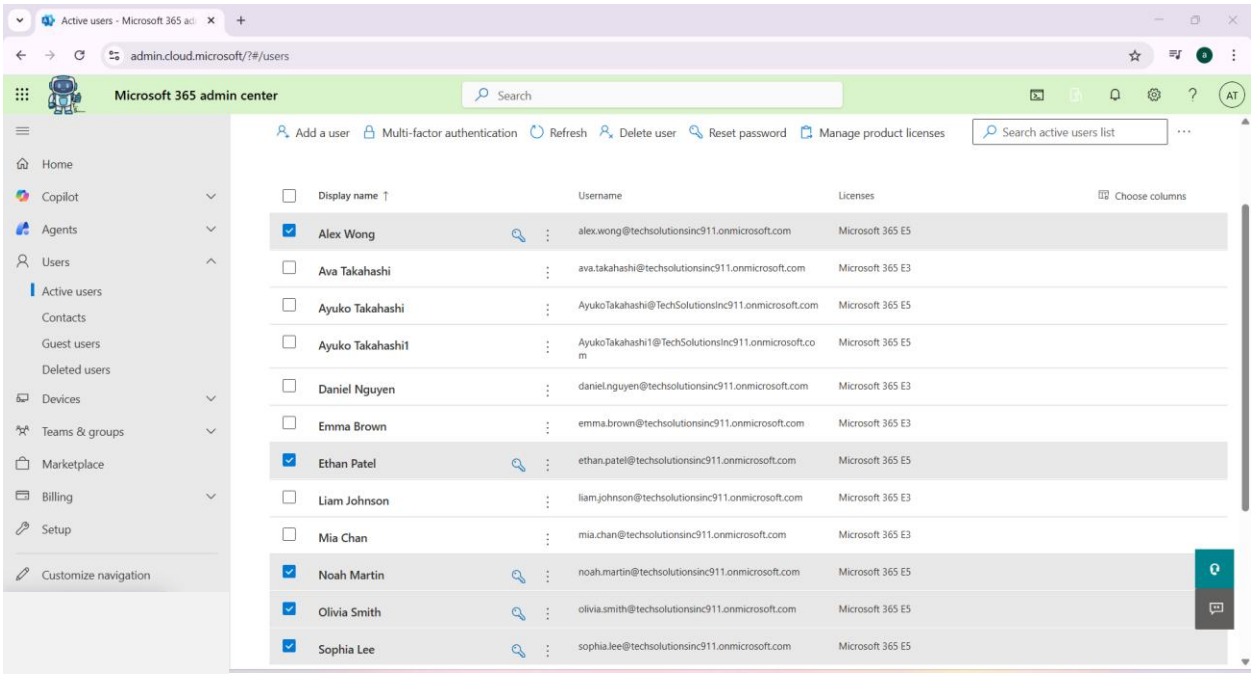
Bulk user provisioning was completed using CSV-based import, successfully onboarding ten users into the Microsoft 365 tenant.


Active users - Microsoft 365 ad
admin.cloud.microsoft/?#/addmultipleusers
Microsoft 365 admin center
Search
Active users > Add multiple users
Home
Copilot
Agents
Users
Active users
Contacts
Guest users
Deleted users
Devices
Teams & groups
Marketplace
Billing
Setup
Customize navigation
Basics
Licenses
Finish
First name
Last name
Username
TechSolutionsInc9...
I'd like to upload a CSV with user information
Download one of the files below. Open the file in Excel or a similar app, add user info, save, and upload.
Download a blank CSV file with the required headers
Download a CSV file that includes example user info
Upload CSV file with your user information *
Import_User_TechSolutionInc.csv
Browse
Next
Cancel


Active users - Microsoft 365 ad
admin.cloud.microsoft/?#/addmultipleusers
Microsoft 365 admin center
Search
Active users > Add multiple users
Home
Copilot
Agents
Users
Active users
Contacts
Guest users
Deleted users
Devices
Teams & groups
Marketplace
Billing
Setup
Customize navigation
Basics
Licenses
Finish
Display name
Username
Password Show
Alex Wong
alex.wong@techsolutionsinc911.onmicrosoft.com
Sophia Lee
sophia.lee@techsolutionsinc911.onmicrosoft.com
Ethan Patel
ethan.patel@techsolutionsinc911.onmicrosoft.com
Mia Chan
mia.chan@techsolutionsinc911.onmicrosoft.com
Daniel Nguyen
daniel.nguyen@techsolutionsinc911.onmicrosoft.com
Olivia Smith
olivia.smith@techsolutionsinc911.onmicrosoft.com
Liam Johnson
liam.johnson@techsolutionsinc911.onmicrosoft.com
Emma Brown
emma.brown@techsolutionsinc911.onmicrosoft.com
Noah Martin
noah.martin@techsolutionsinc911.onmicrosoft.com
Ava Takahashi
ava.takahashi@techsolutionsinc911.onmicrosoft.com
Close



Successful user import was validated through the Active Users view in the Microsoft 365 admin center. *Ayuko Takahashi and Ayuko Takahashi1 are Global admin.

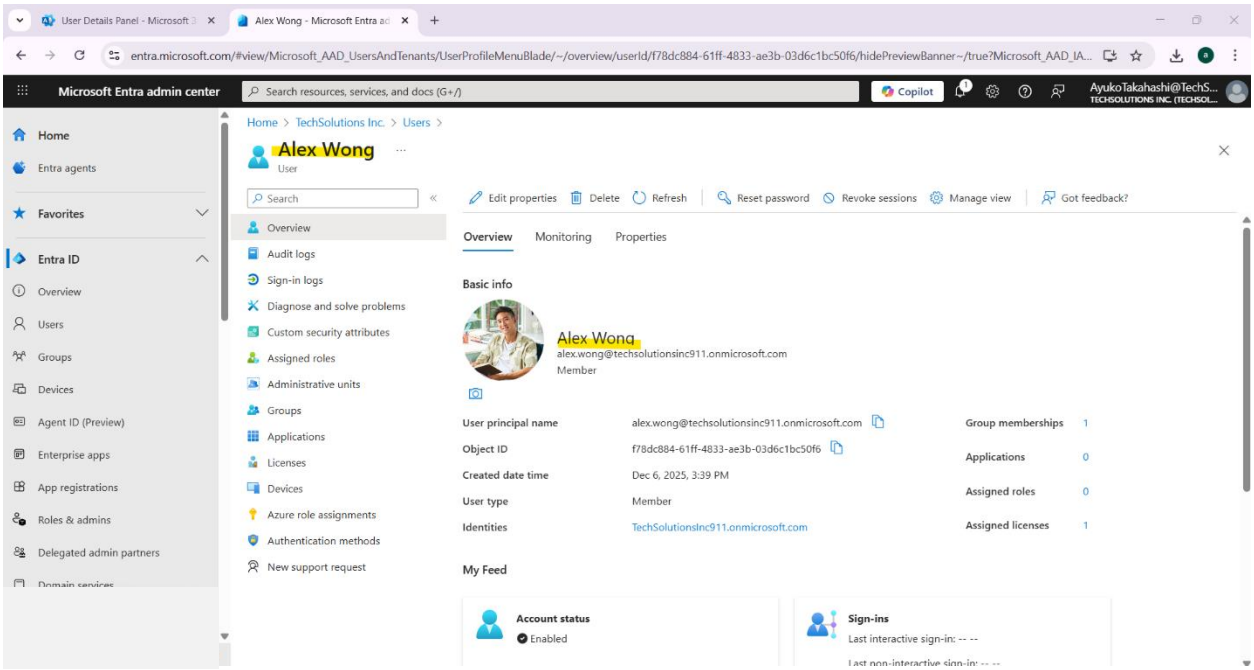


Assigned E5 license to users whose roles need security/compliance features:

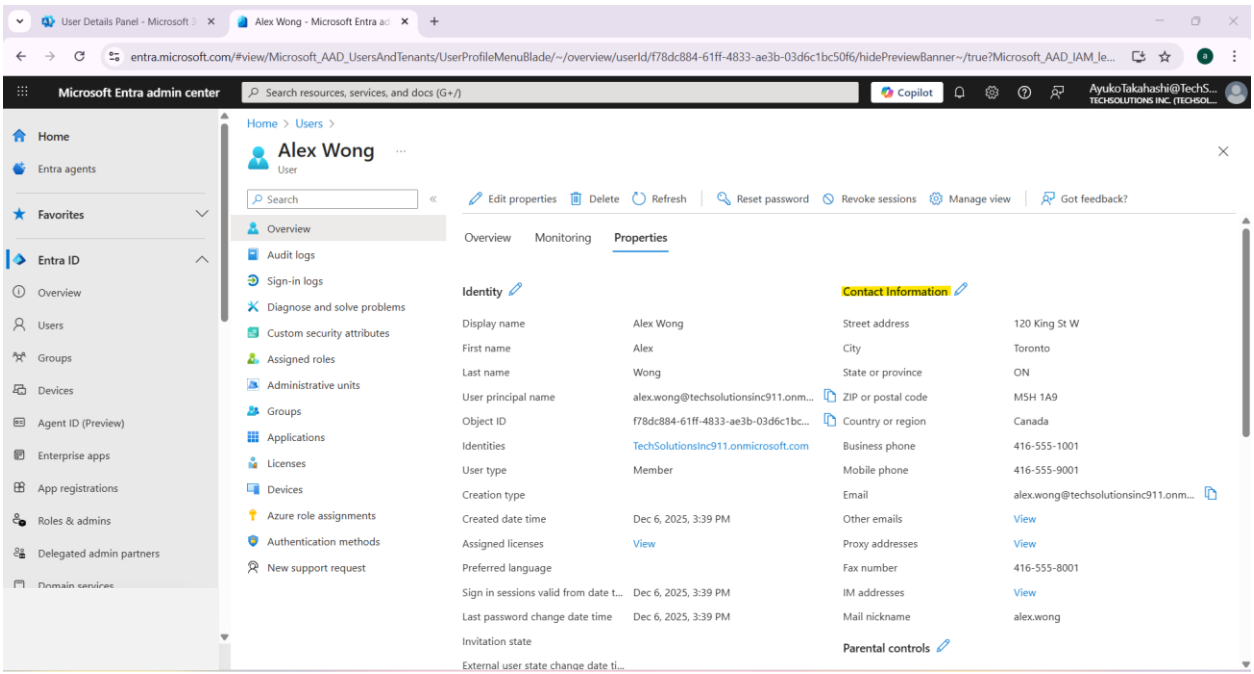
- Alex Wong – IT Manager
- Sophia Lee – System Administrator
- Ethan Patel – Cloud Engineer
- Olivia Smith – HR Manager
- Noah Martin – Marketing Manager

Assigned E3 license to the rest (regular user experience):

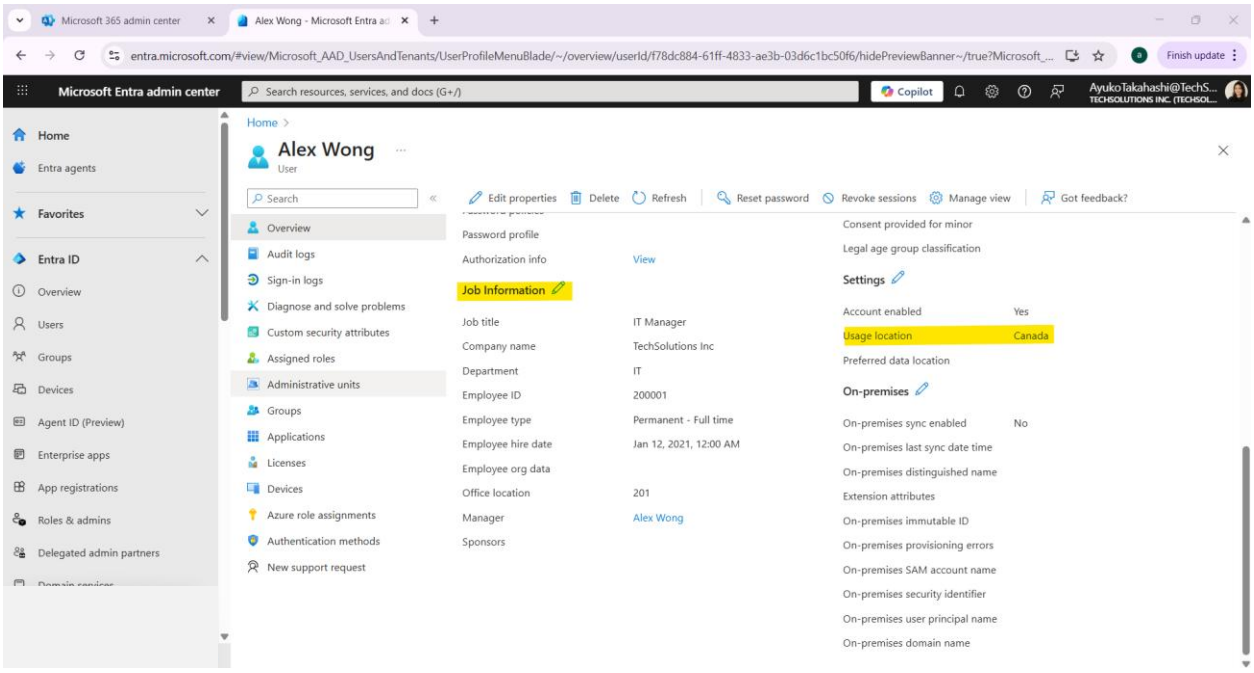
- Mia Chan – HR Coordinator
- Daniel Nguyen – HR Specialist
- Liam Johnson – Marketing Coordinator
- Emma Brown – Content Strategist
- Ava Takahashi – Project Administrator



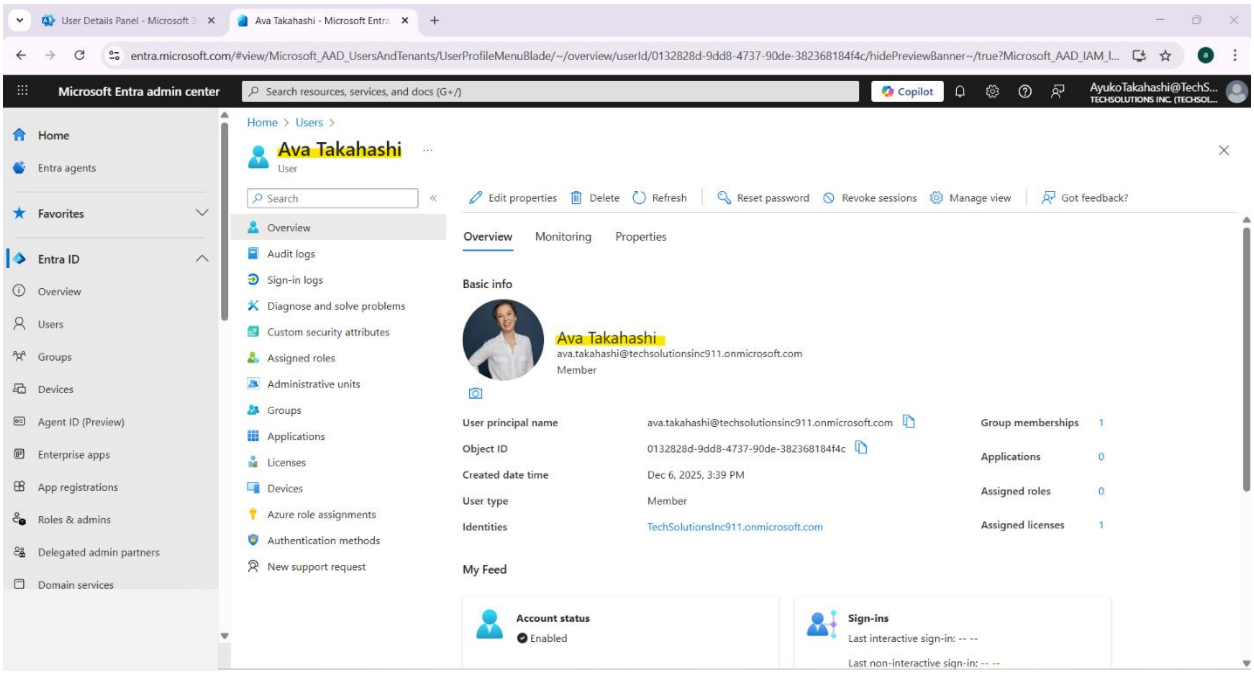
User profile overview for Alex Wong, showing profile photo and identity details.



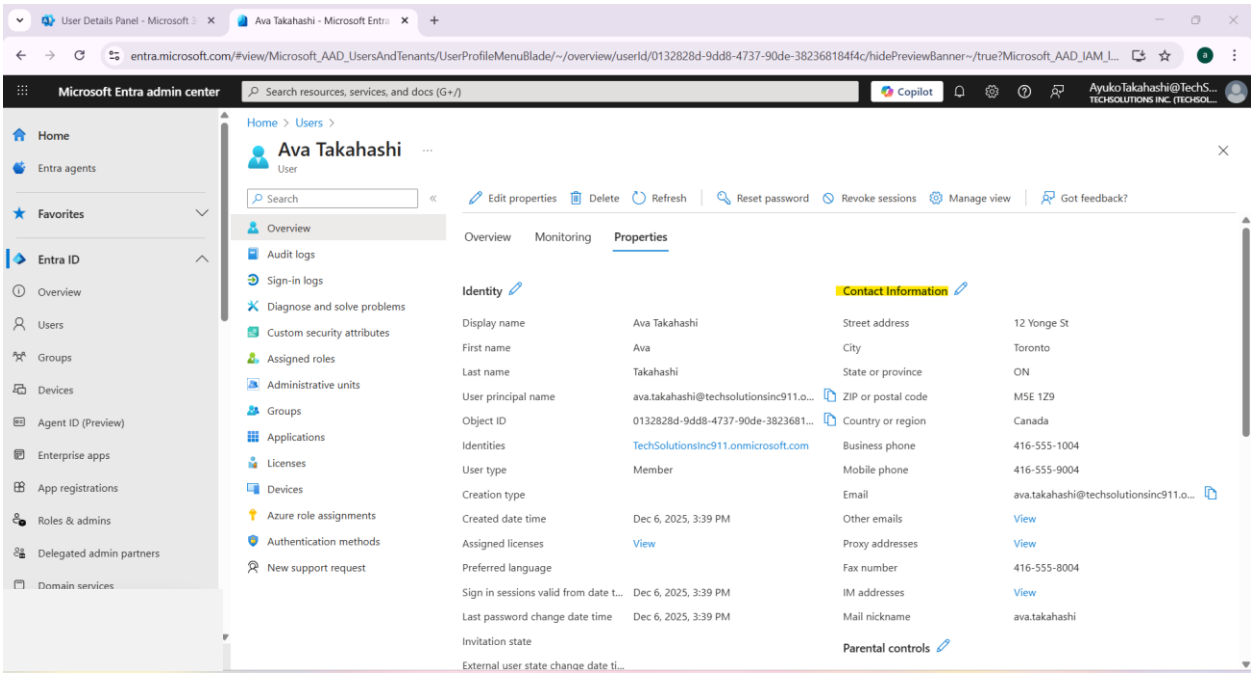
Contact information for Alex Wong, including office phone, mobile phone, and full mailing address.



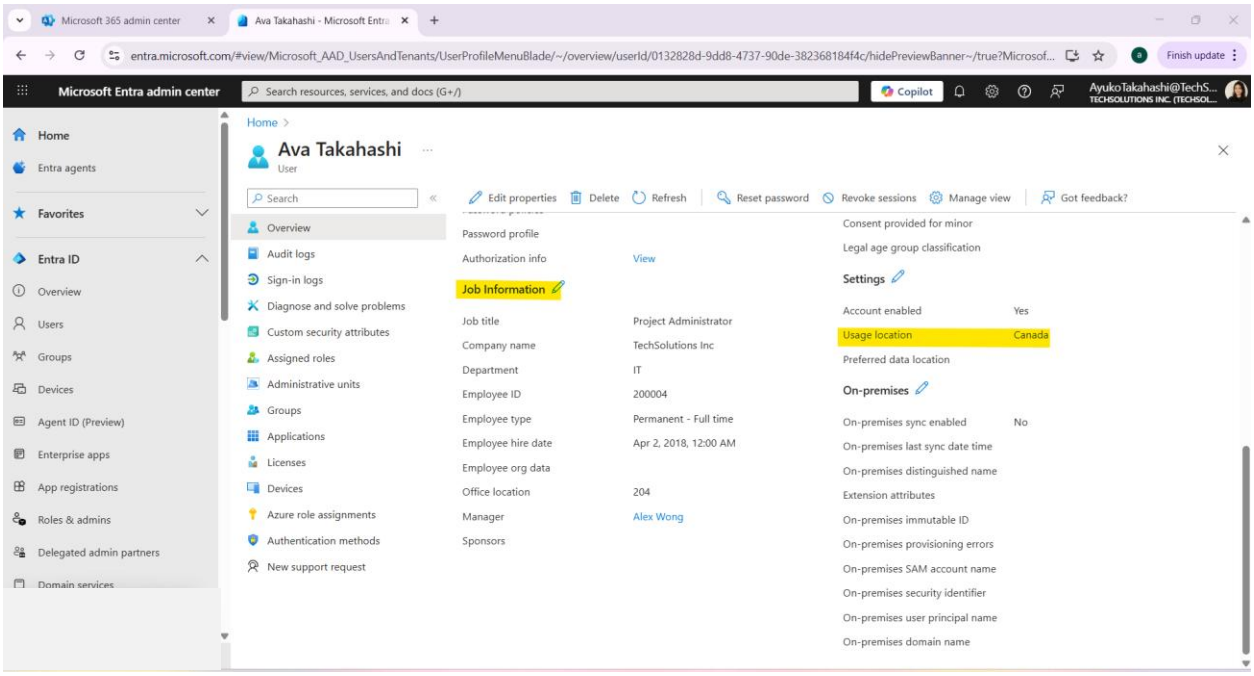
Job and organizational information for Alex Wong, including job title, department, office location, and usage location set to Canada.



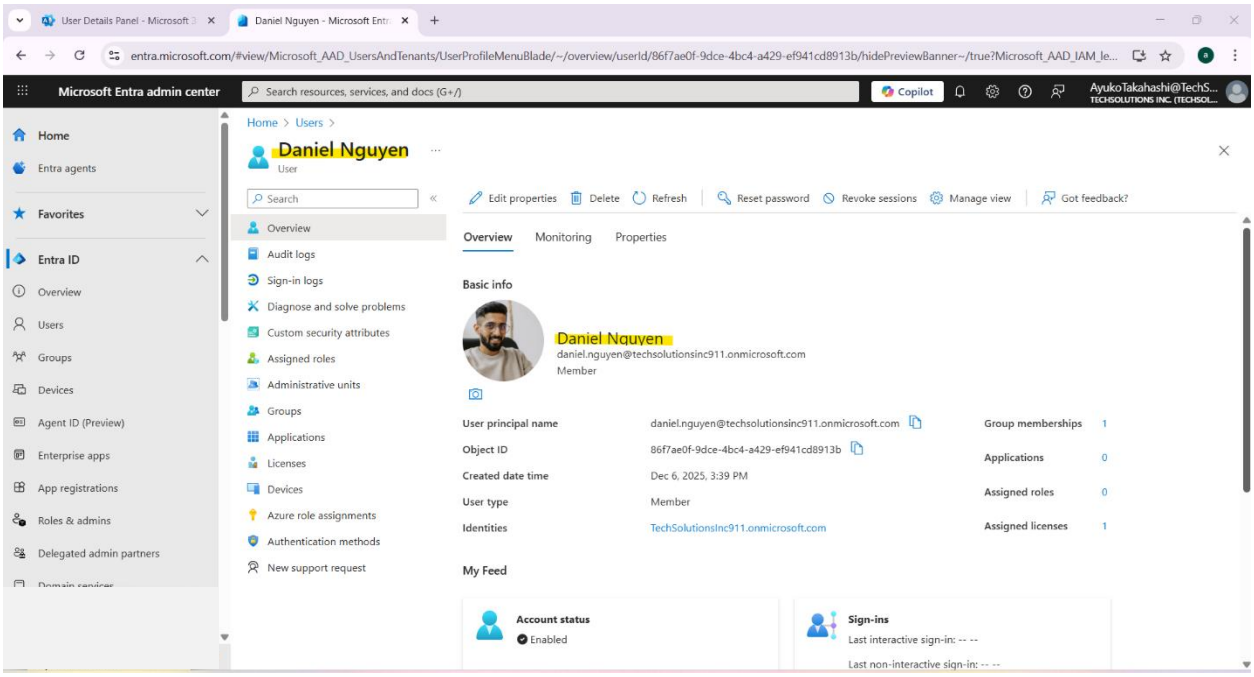
User profile overview for Ava Takahashi, showing profile photo and identity details.



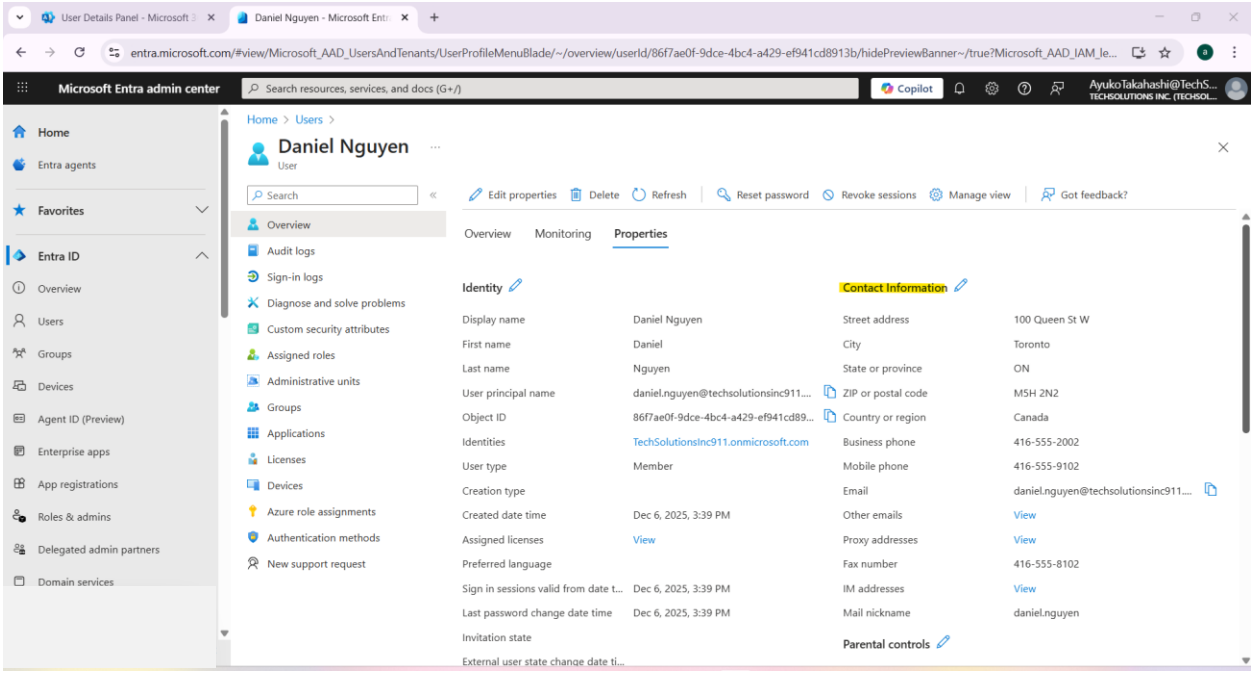
Contact information for Ava Takahashi, including office phone, mobile phone, and full mailing address.



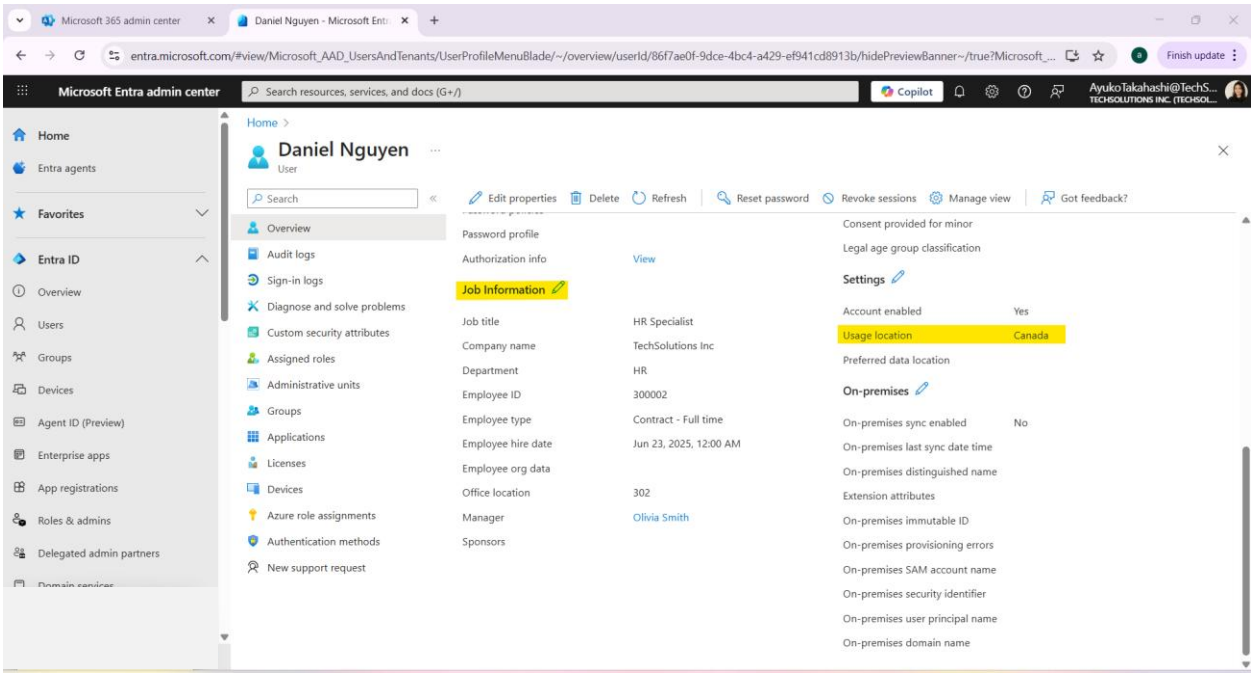
Job and organizational information for Ava Takahashi, including job title, department, office location, and usage location set to Canada.



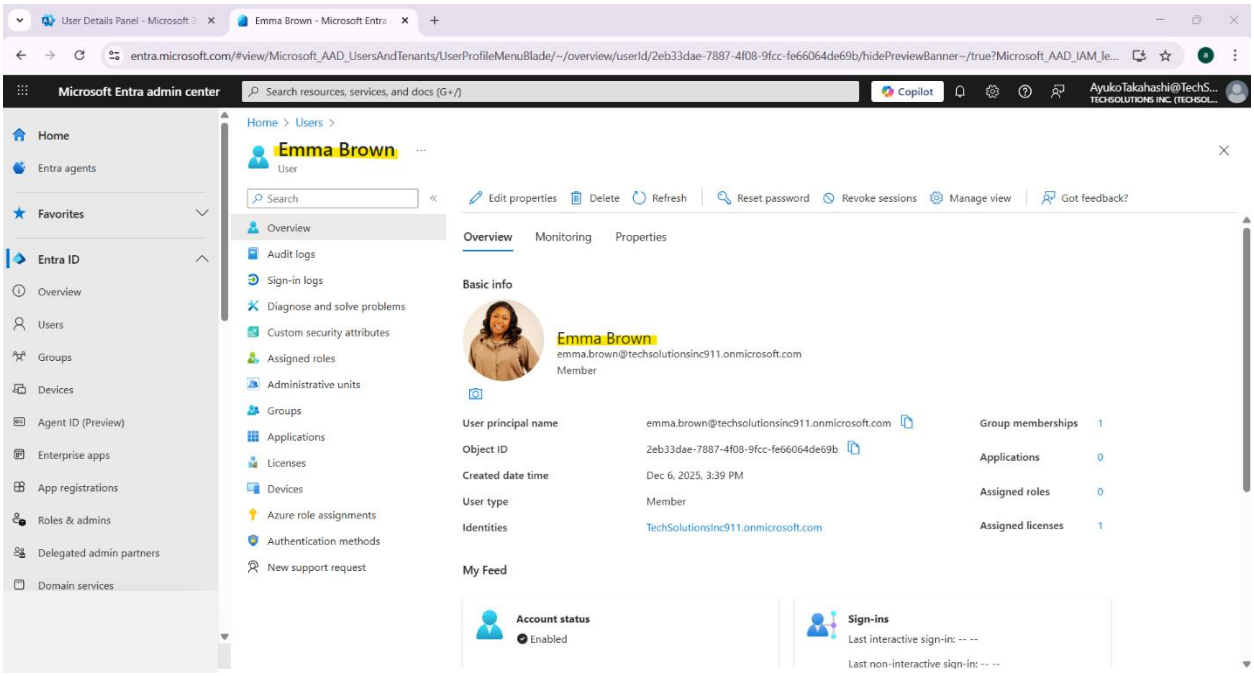
User profile overview for Daniel Nguyen, showing profile photo and identity details.



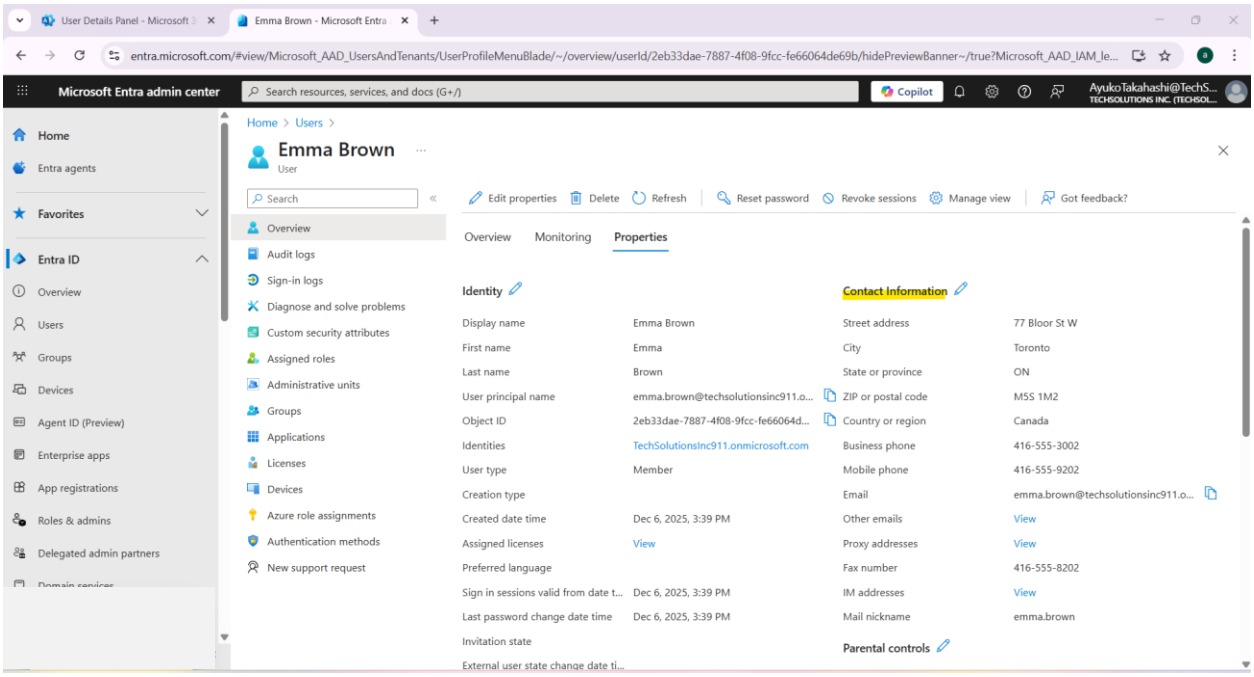
Contact information for Daniel Nguyen, including office phone, mobile phone, and full mailing address.



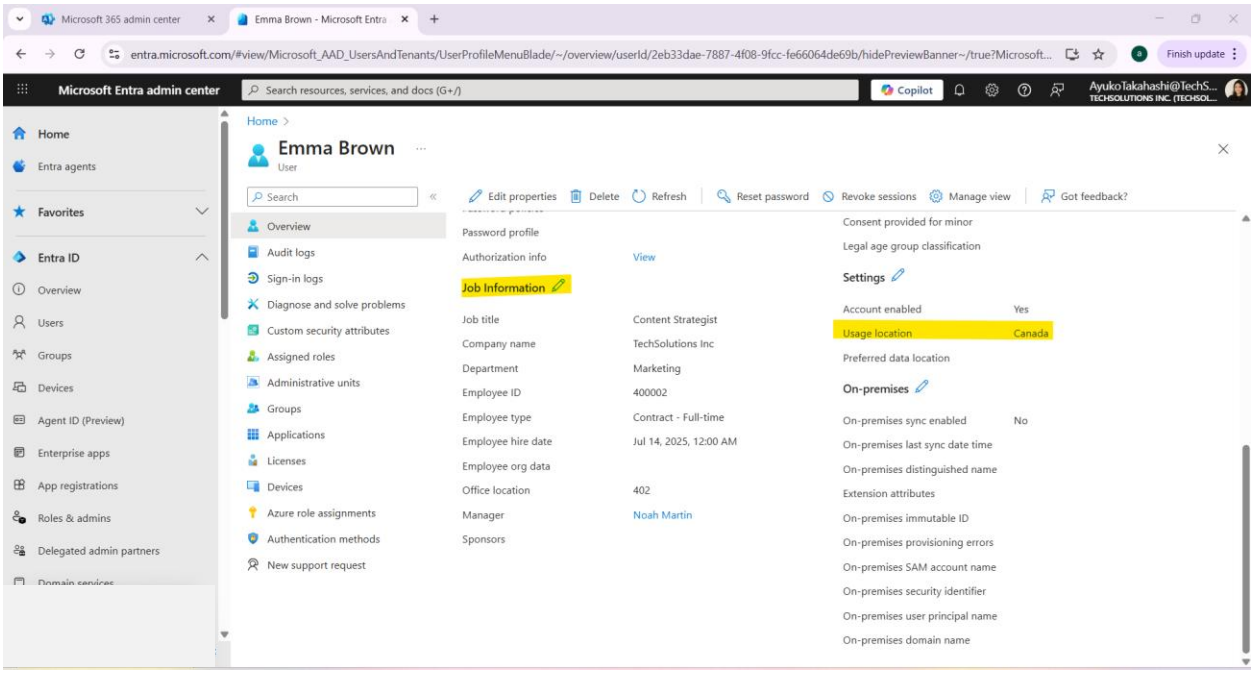
Job and organizational information for Daniel Nguyen, including job title, department, office location, and usage location set to Canada.



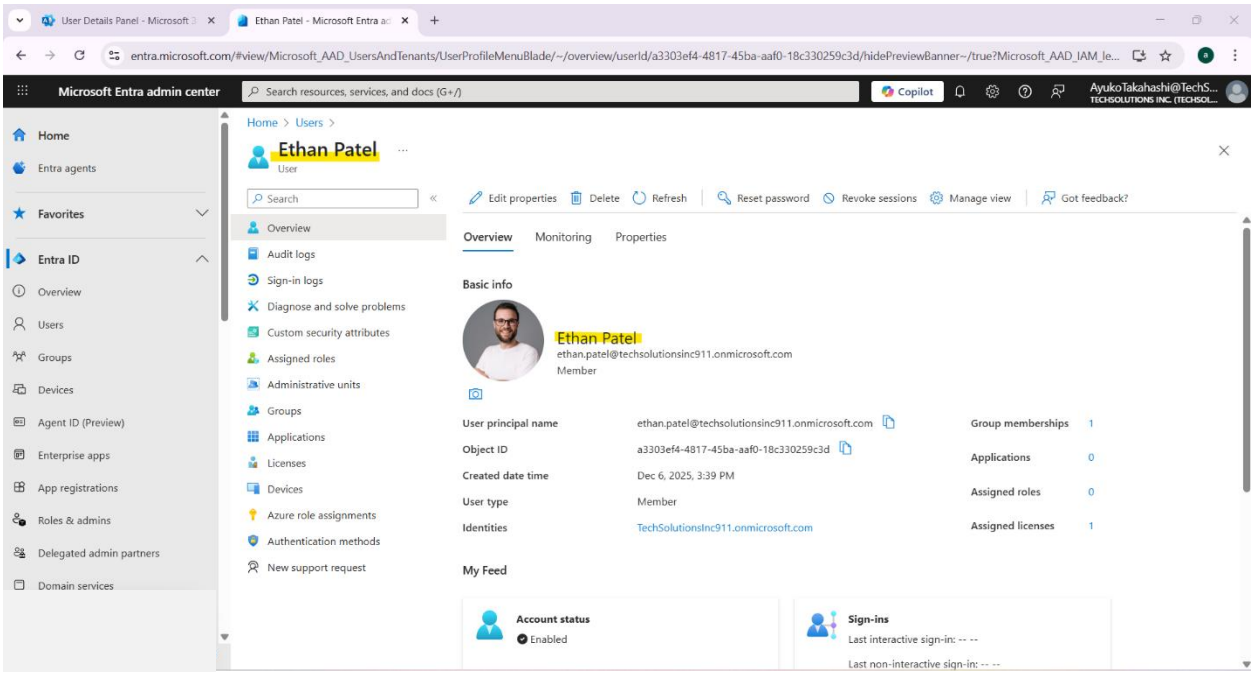
User profile overview for Emma Brown, showing profile photo and identity details.



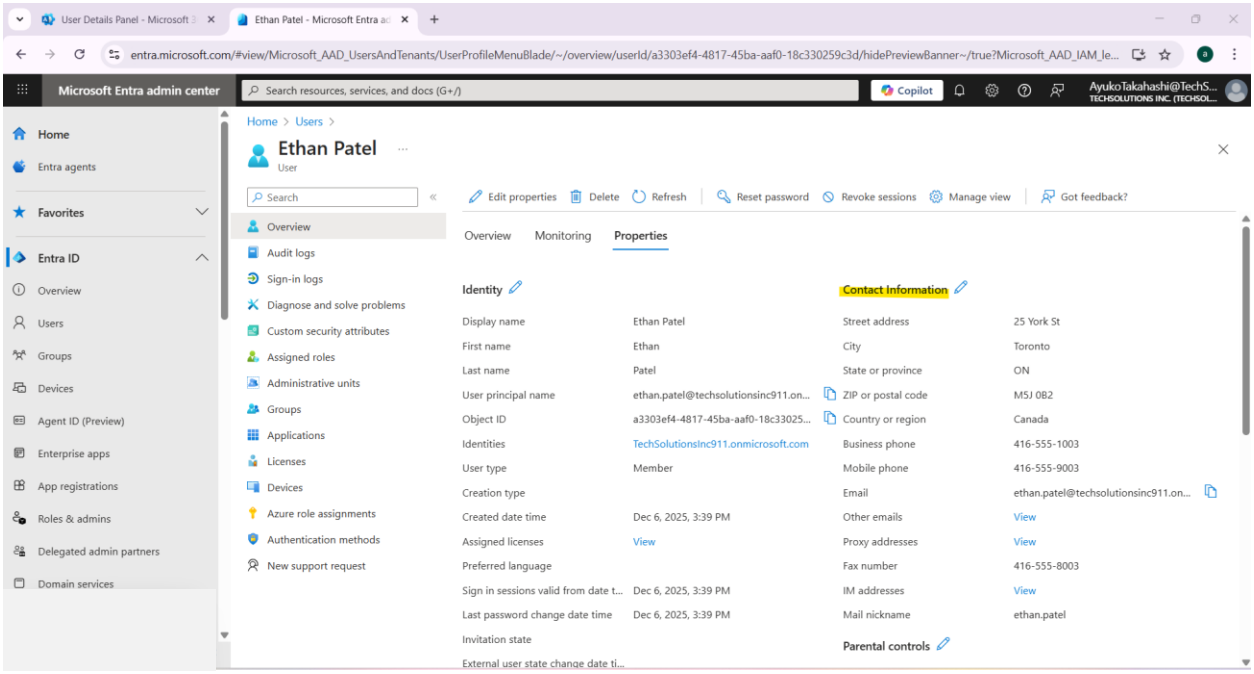
Contact information for Emma Brown, including office phone, mobile phone, and full mailing address.



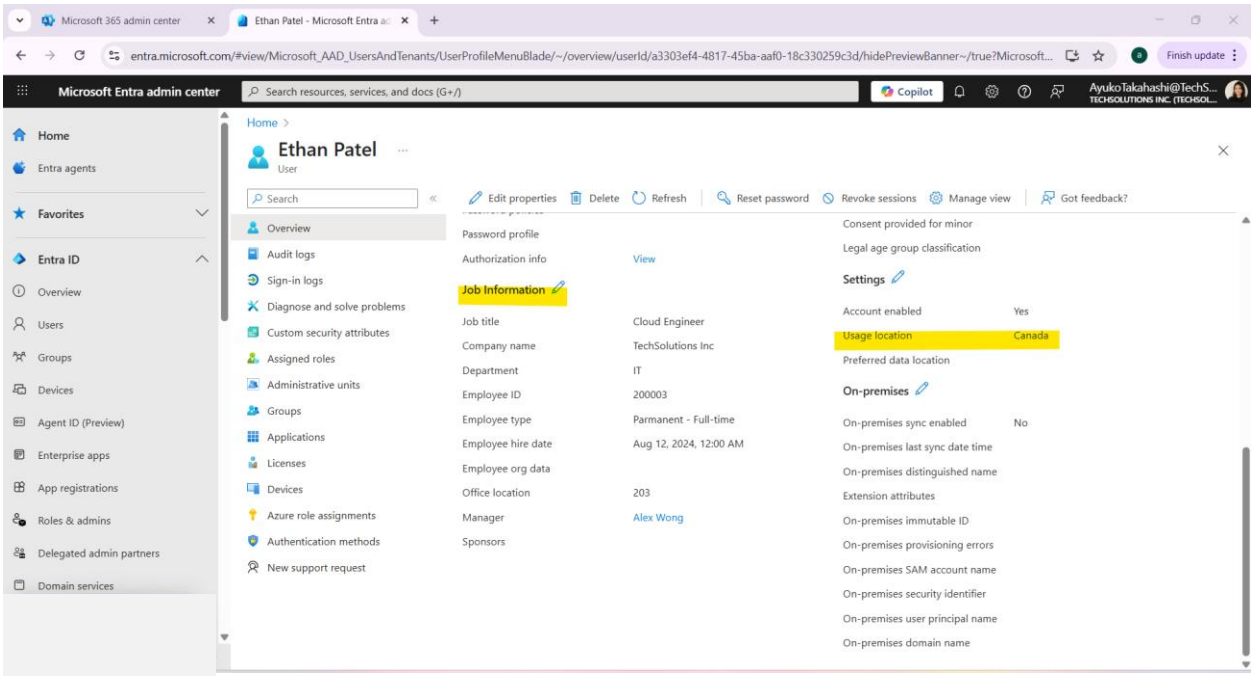
Job and organizational information for Emma Brown, including job title, department, office location, and usage location set to Canada.



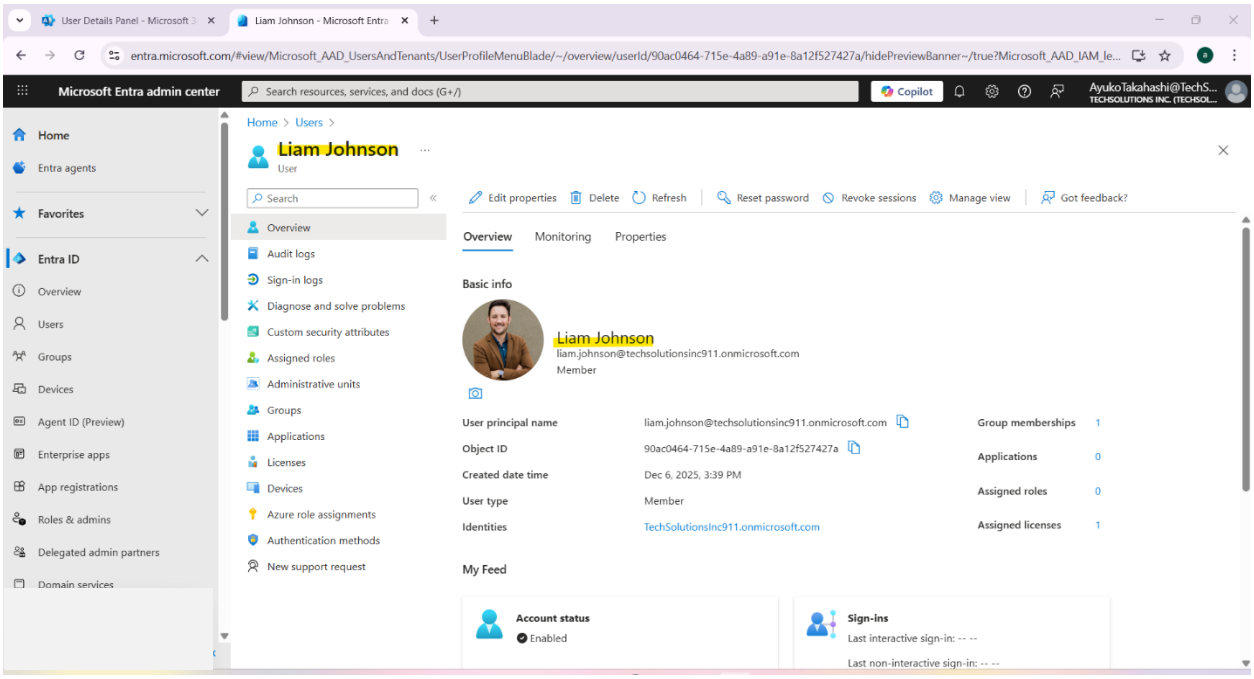
User profile overview for Ethan Patel, showing profile photo and identity details.



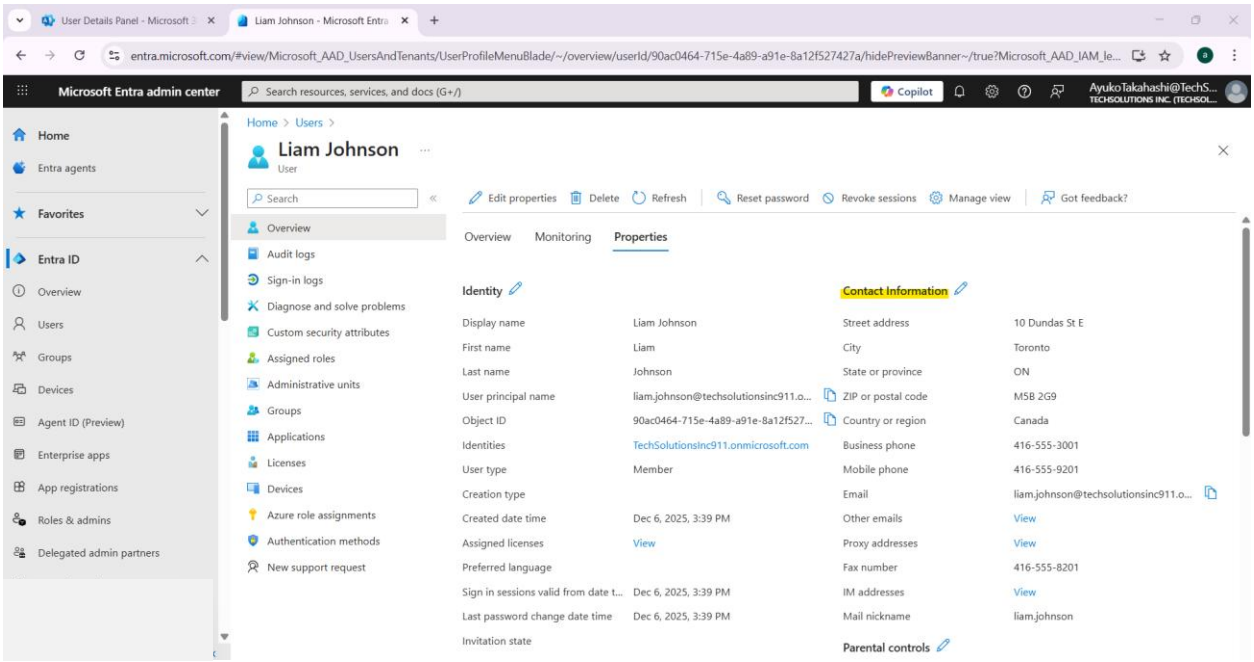
Contact information for Ethan Patel, including office phone, mobile phone, and full mailing address.



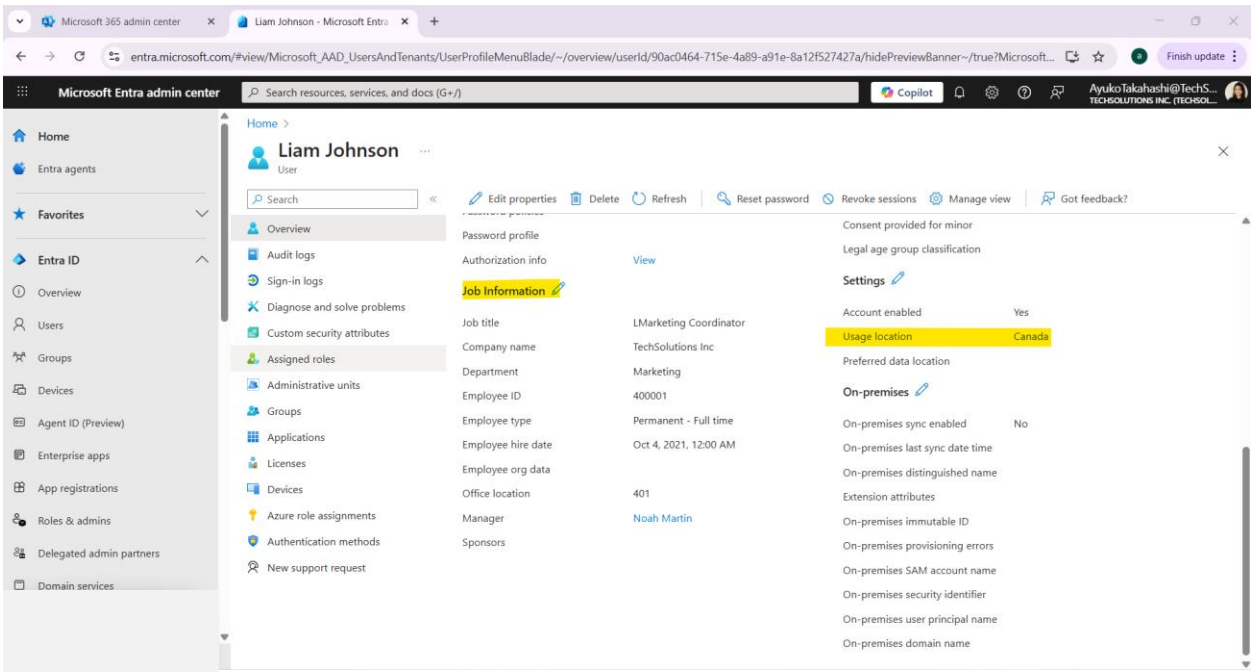
Job and organizational information for Ethan Patel, including job title, department, office location, and usage location set to Canada.



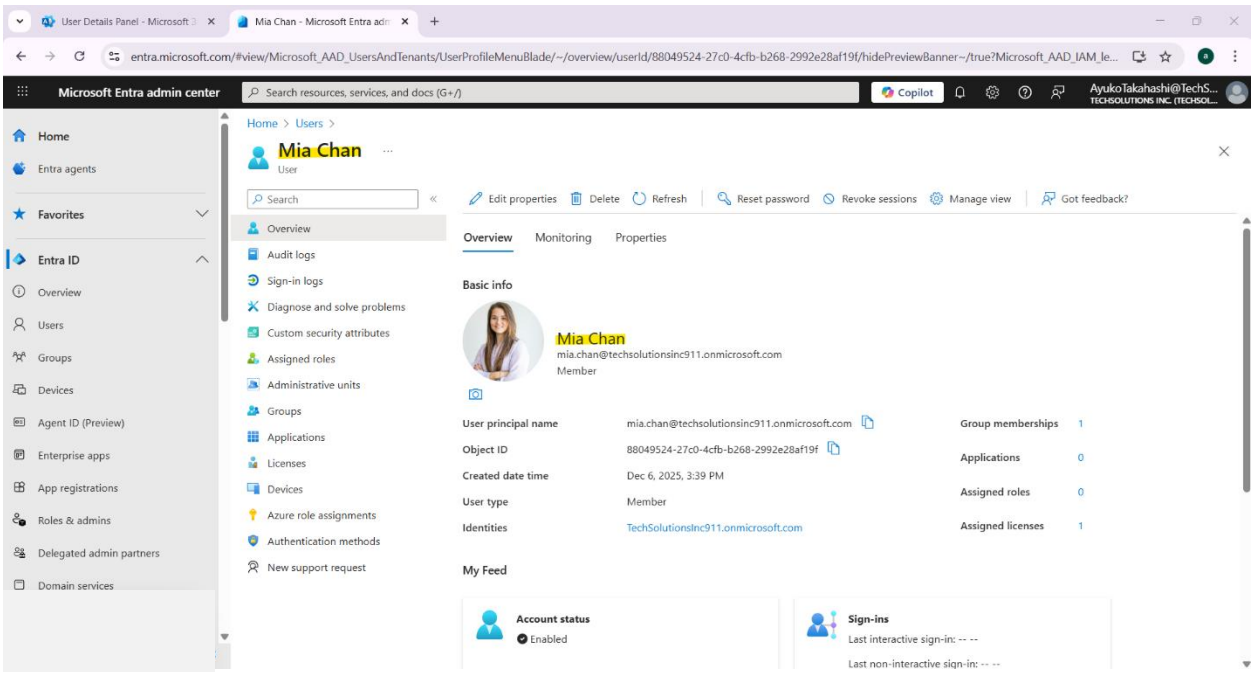
User profile overview for Liam Johnson, showing profile photo and identity details.



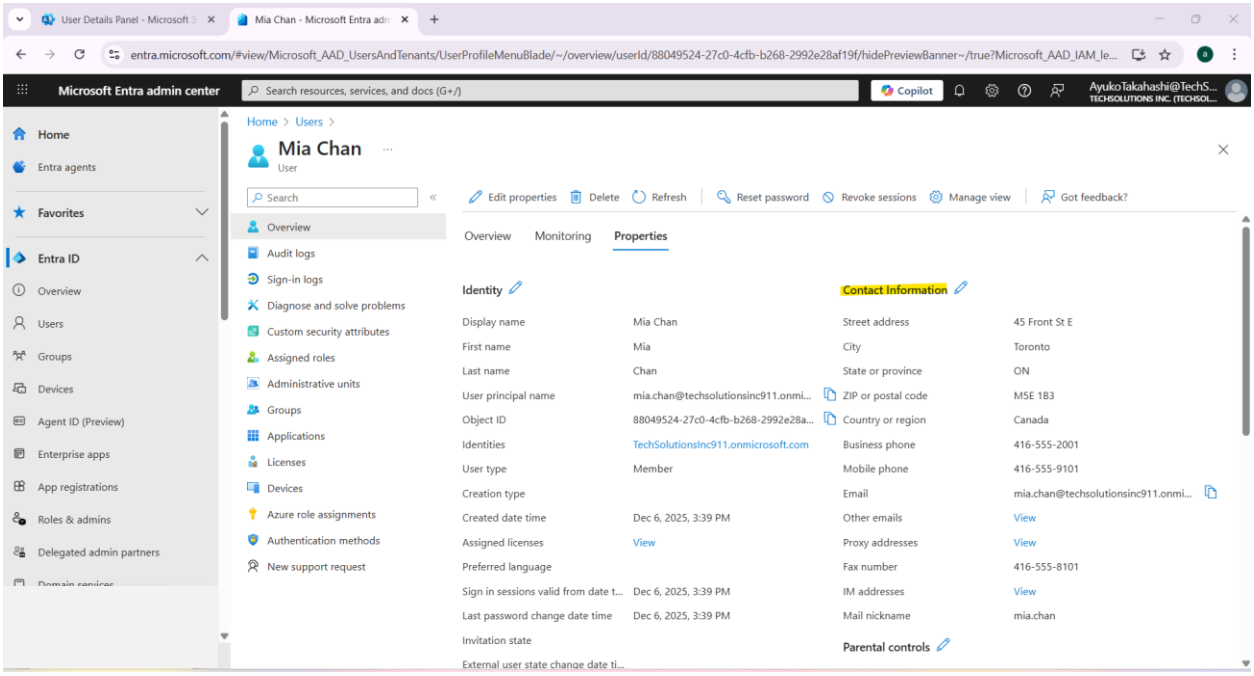
Contact information for Liam Johnson, including office phone, mobile phone, and full mailing address.



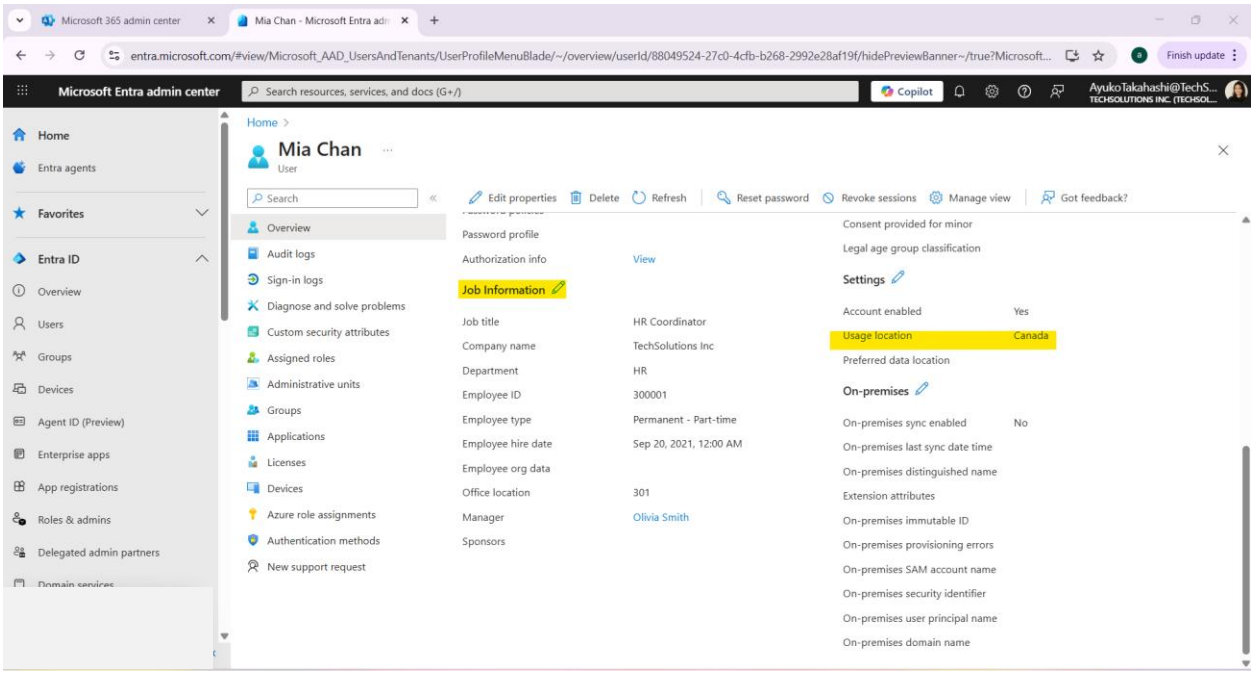
Job and organizational information for Liam Johnson, including job title, department, office location, and usage location set to Canada.



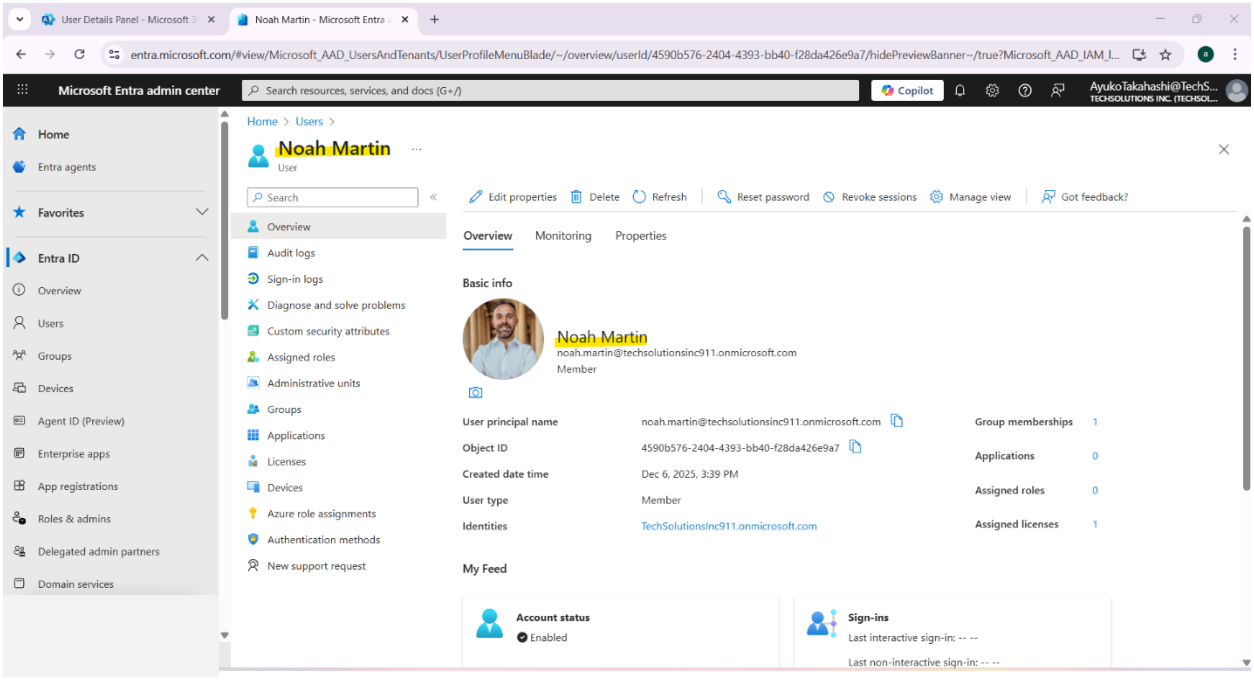
User profile overview for Mia Chan, showing profile photo and identity details.



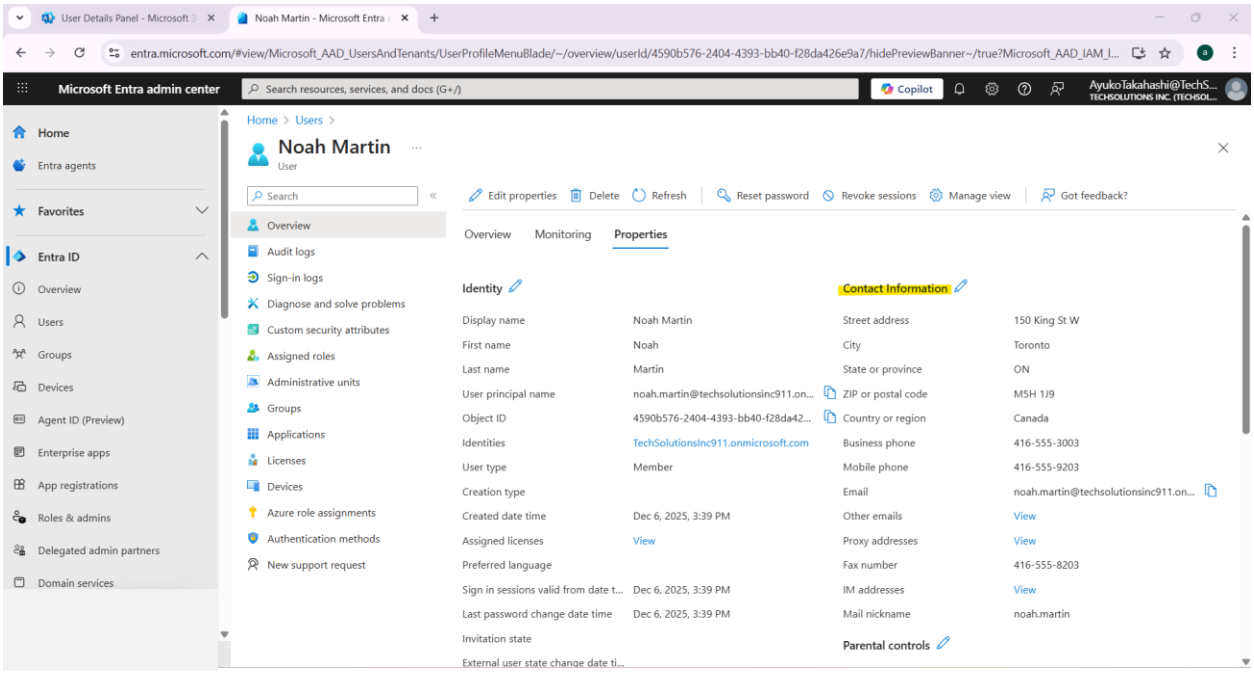
Contact information for Mia Chan, including office phone, mobile phone, and full mailing address.



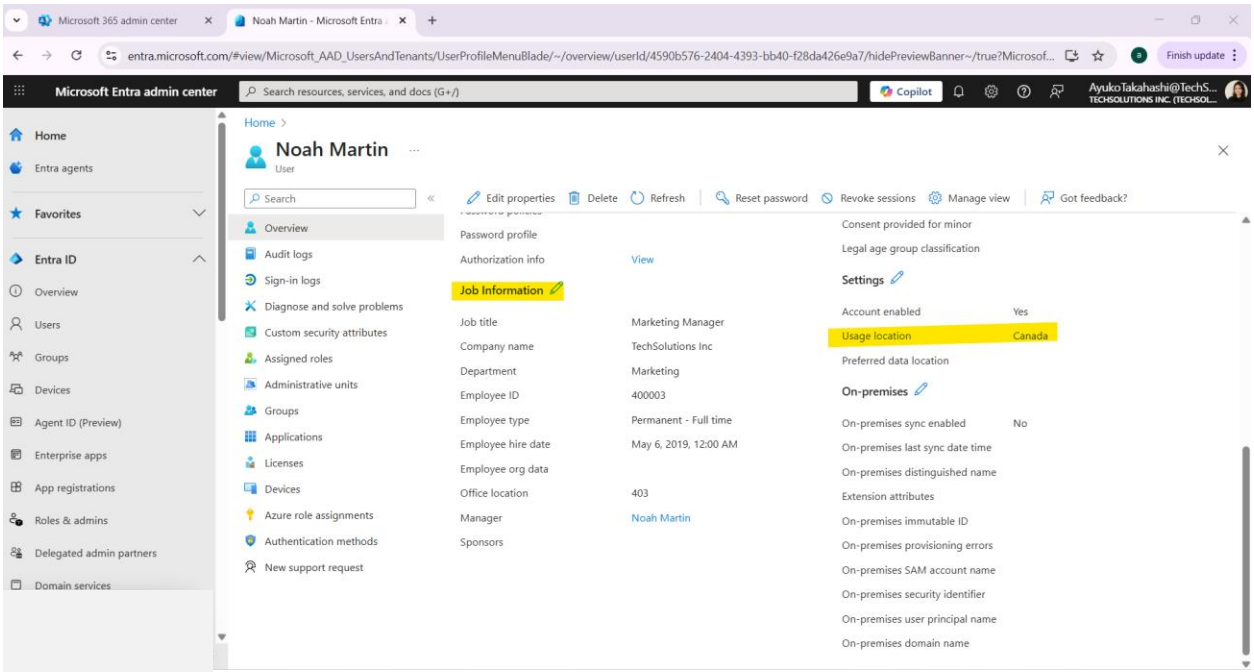
Job and organizational information for Mia Chan, including job title, department, office location, and usage location set to Canada.



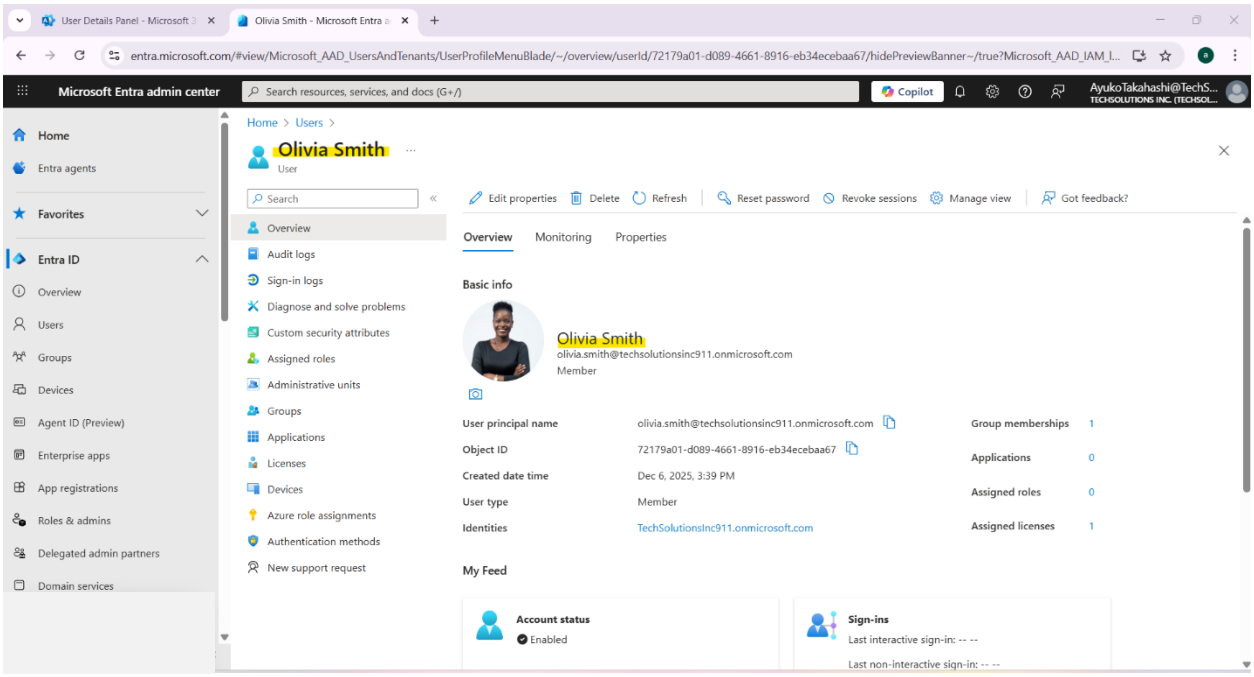
User profile overview for Noah Martin, showing profile photo and identity details.



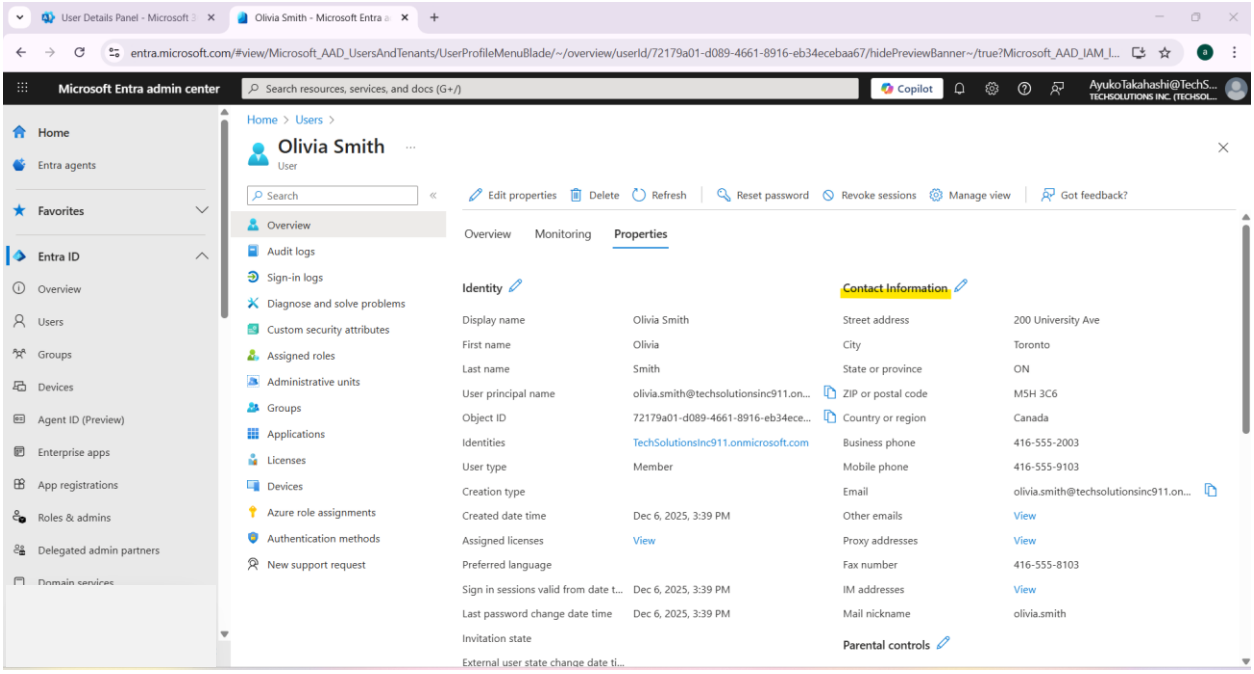
Contact information for Noah Martin, including office phone, mobile phone, and full mailing address.



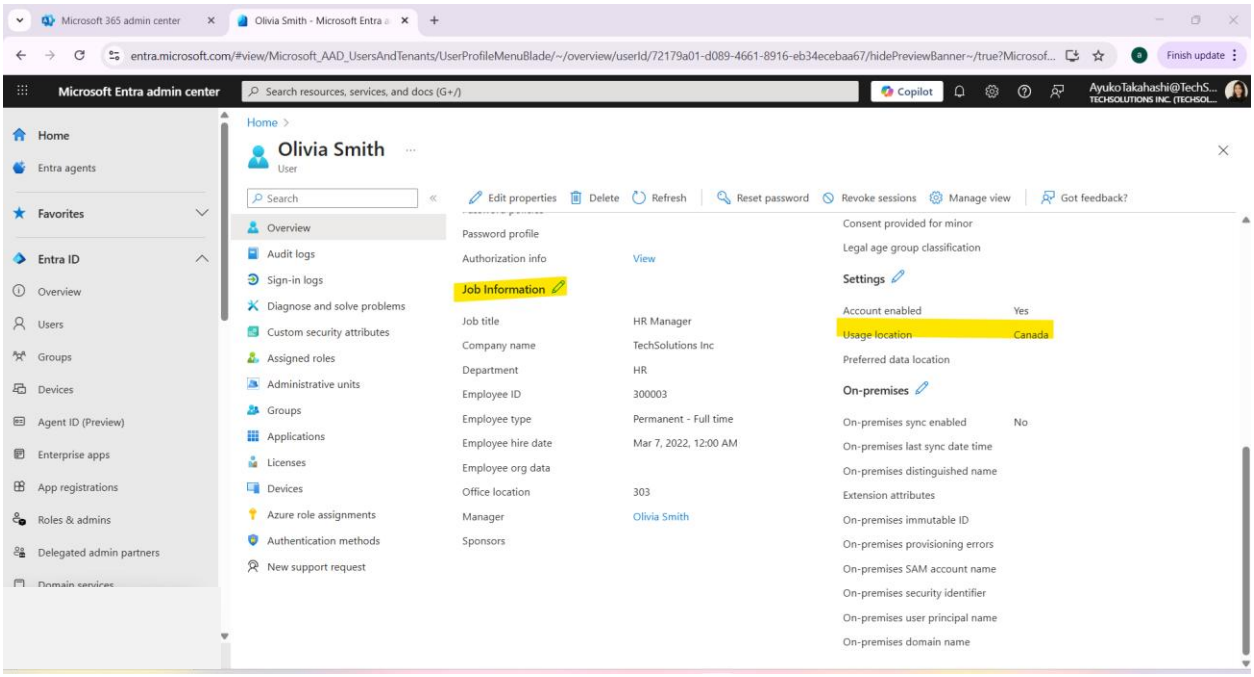
Job and organizational information for Noah Martin, including job title, department, office location, and usage location set to Canada.



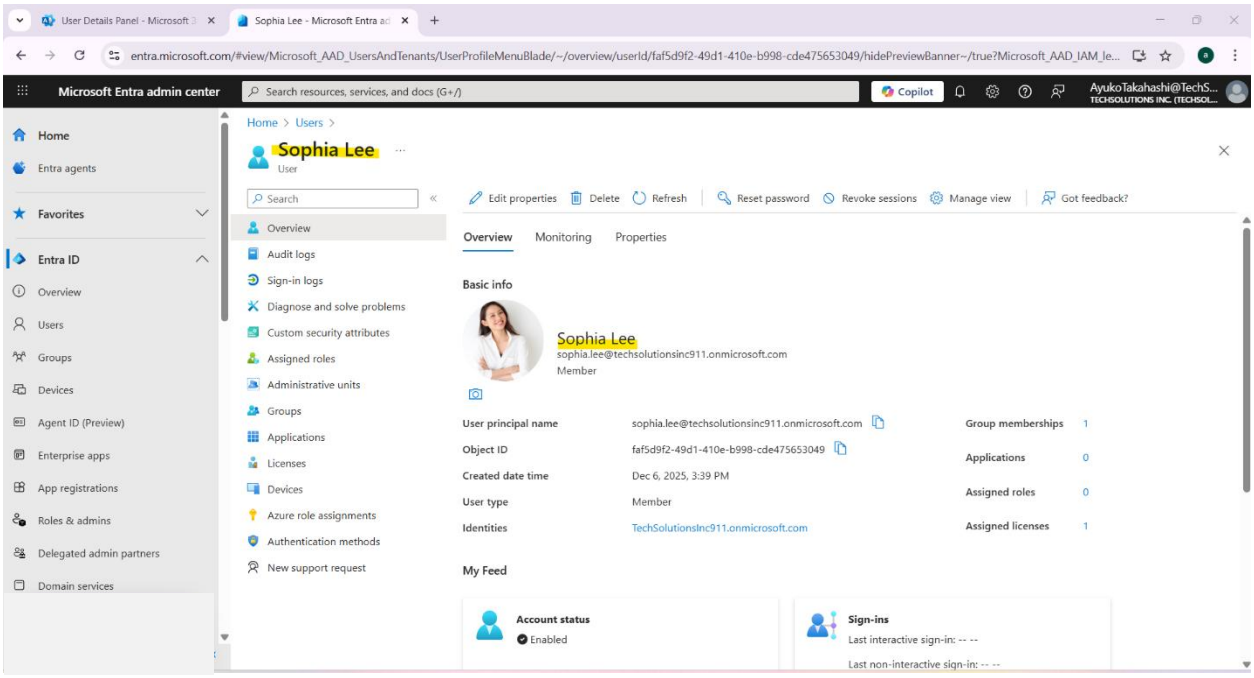
User profile overview for Olivia Smith, showing profile photo and identity details.



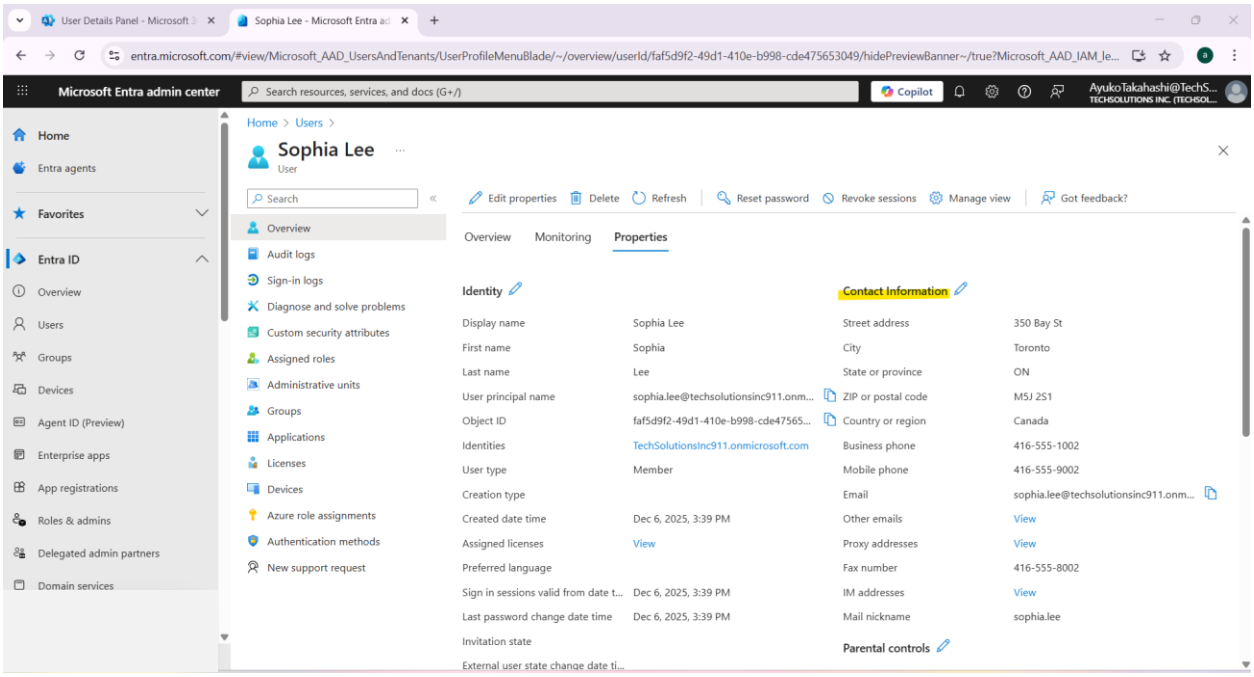
Contact information for Olivia Smith, including office phone, mobile phone, and full mailing address.



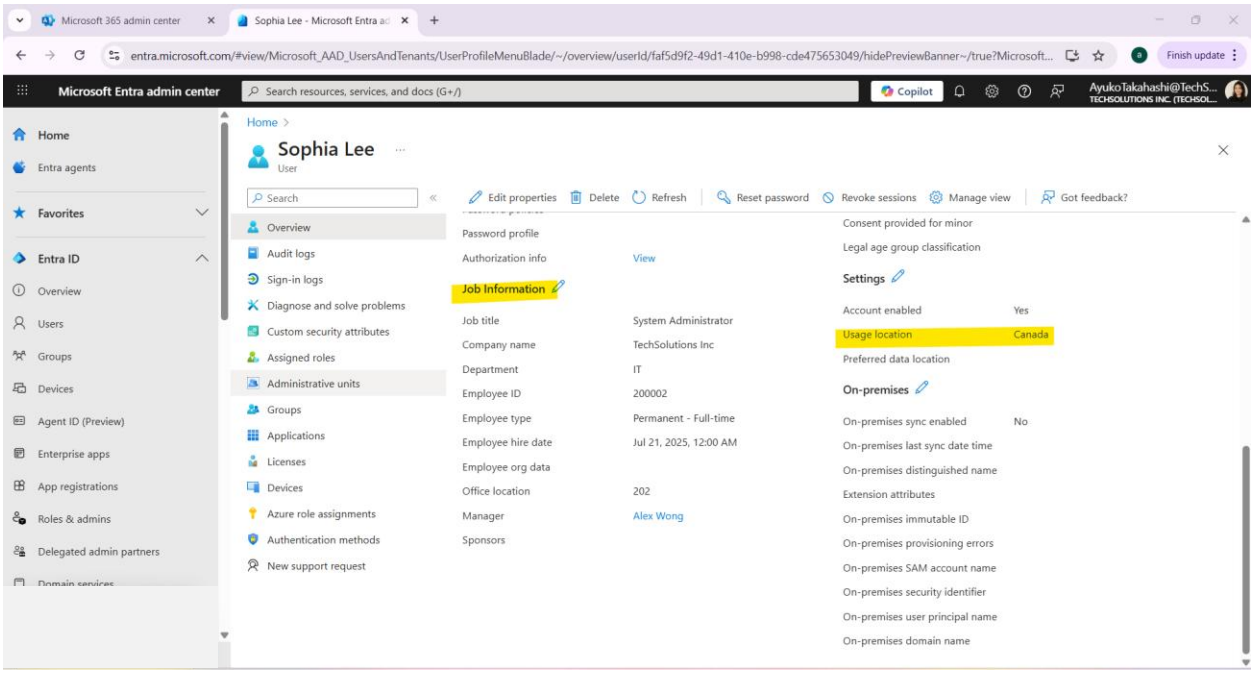
Job and organizational information for Olivia Smith, including job title, department, office location, and usage location set to Canada.



User profile overview for Sophia Lee, showing profile photo and identity details.



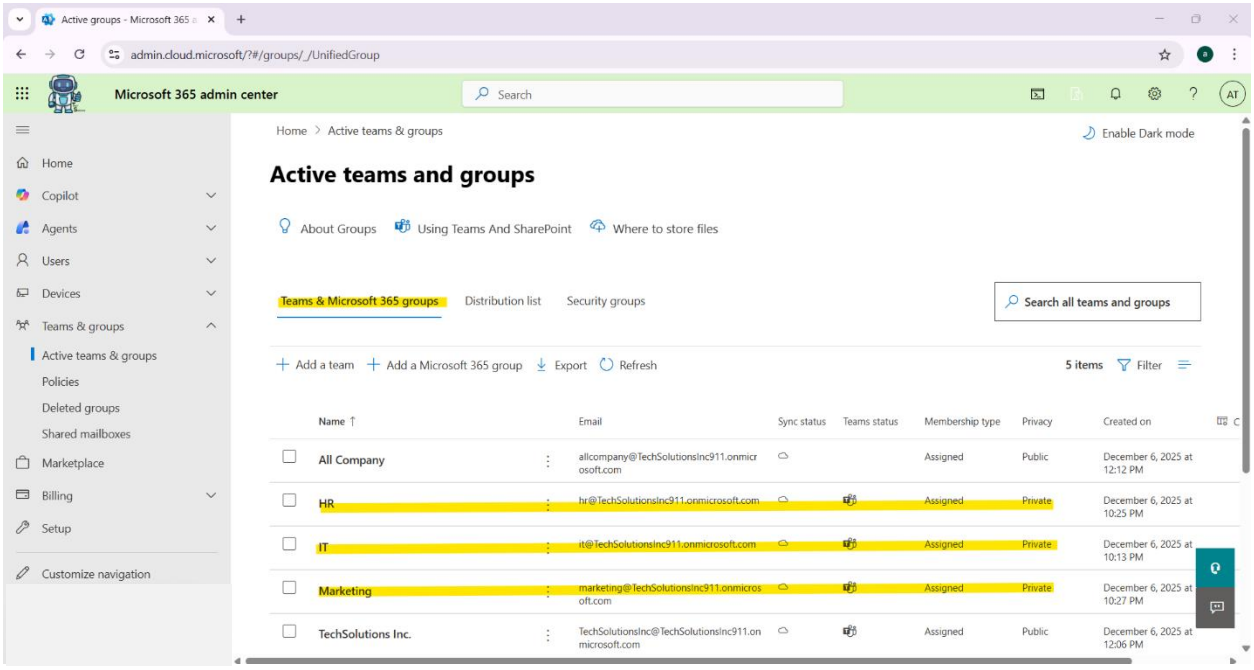
Contact information for Sophia Lee, including office phone, mobile phone, and full mailing address.



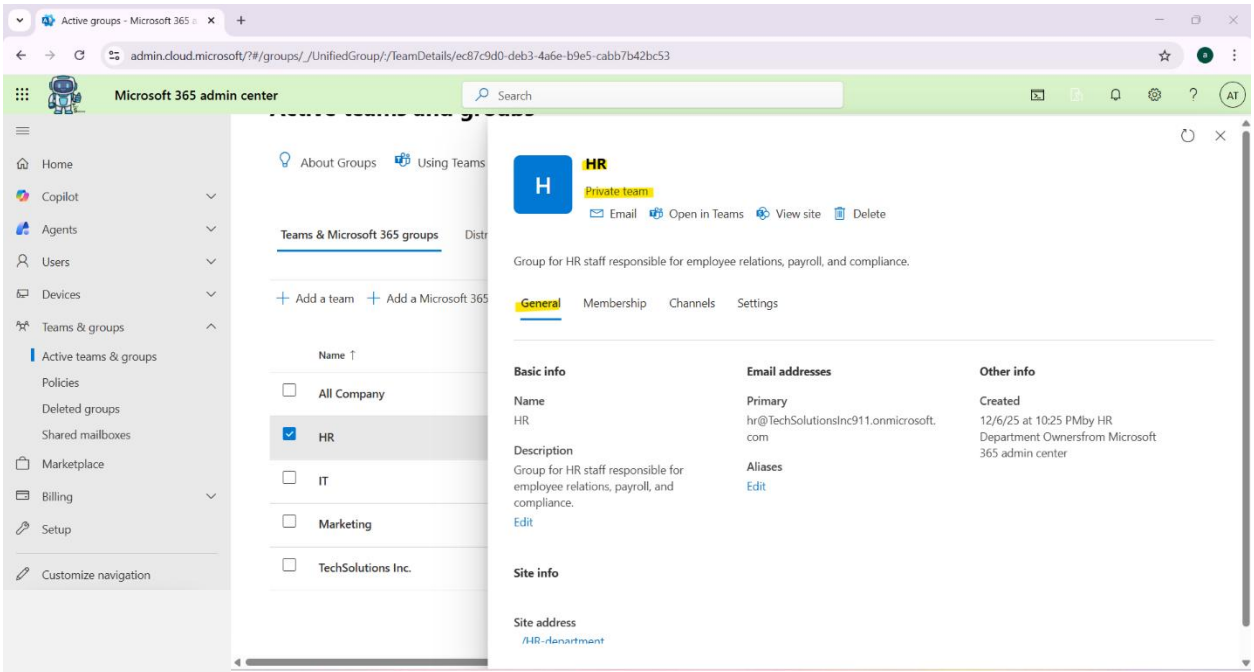
Job and organizational information for Sophia Lee, including job title, department, office location, and usage location set to Canada.

Group, Permission, and Collaboration Governance

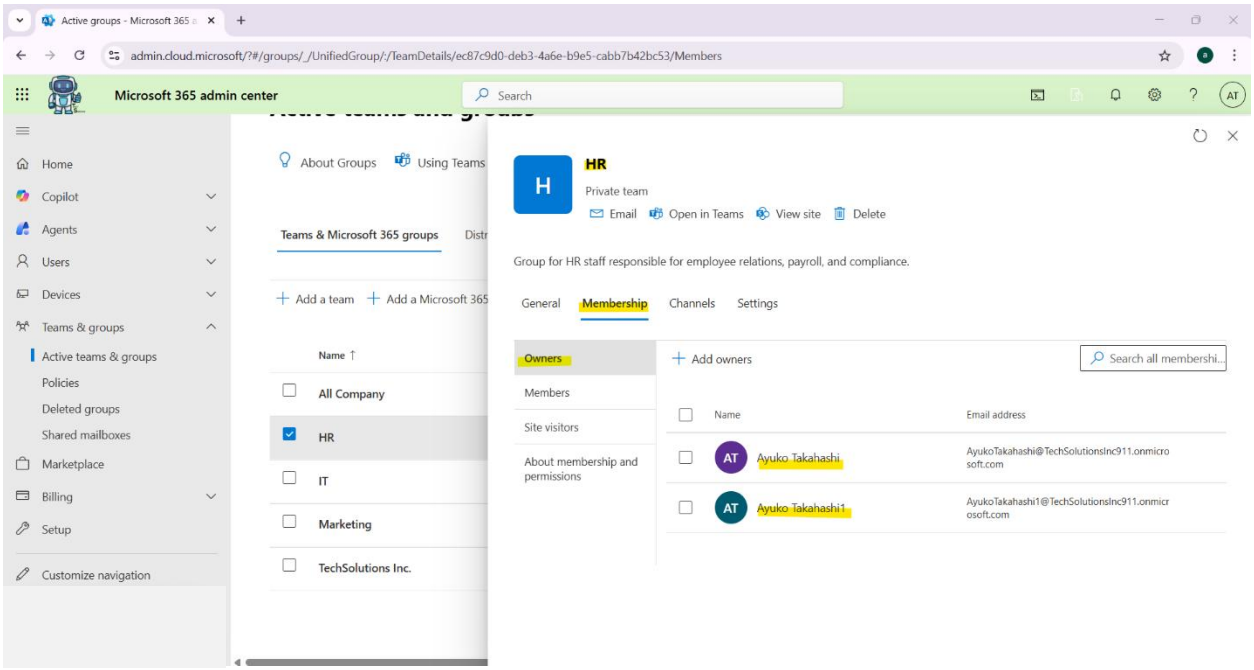
This section demonstrates the creation and governance of Microsoft 365 groups and permissions to support secure departmental collaboration across Teams, SharePoint, and related services.



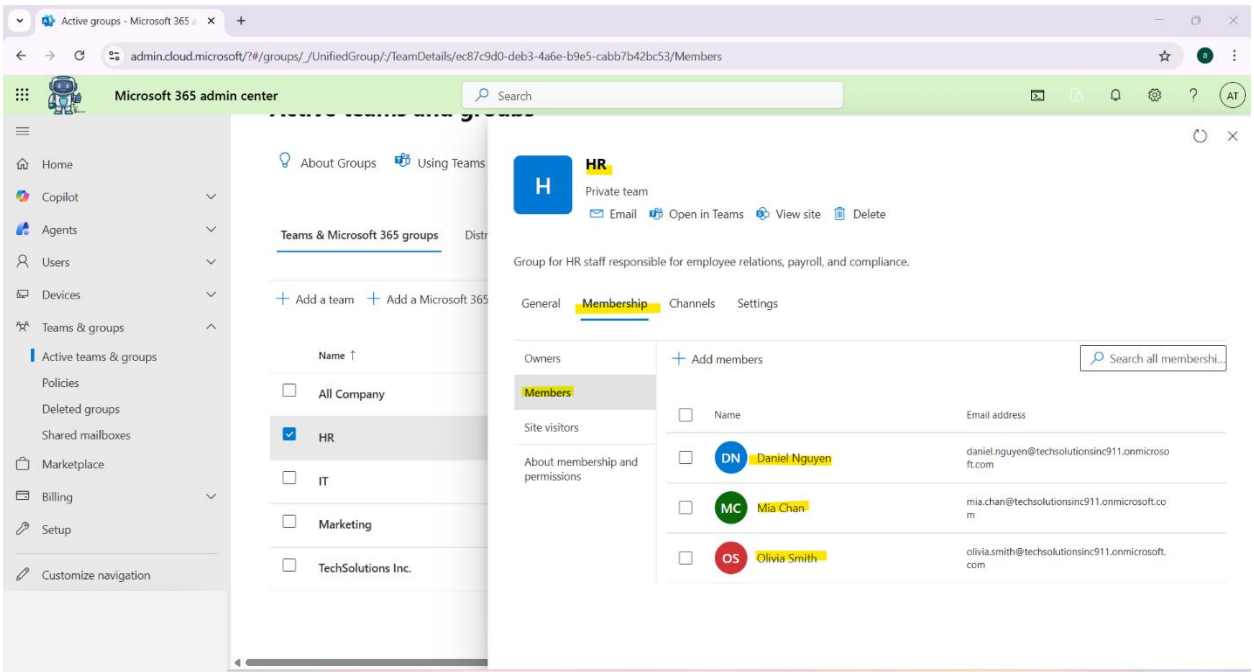
Microsoft 365 groups for HR, IT, and Marketing departments were configured with private visibility to support secure, department-specific collaboration in Teams.



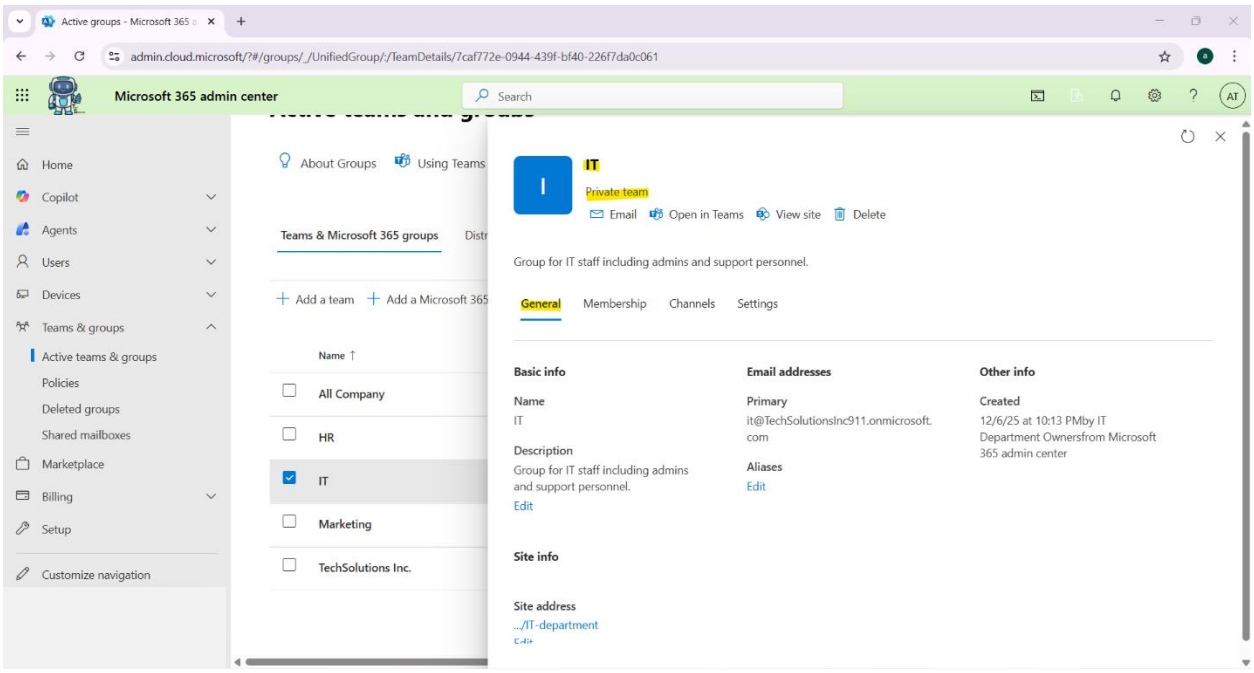
HR department Microsoft 365 group created for departmental collaboration, showing group name, privacy settings and general information.



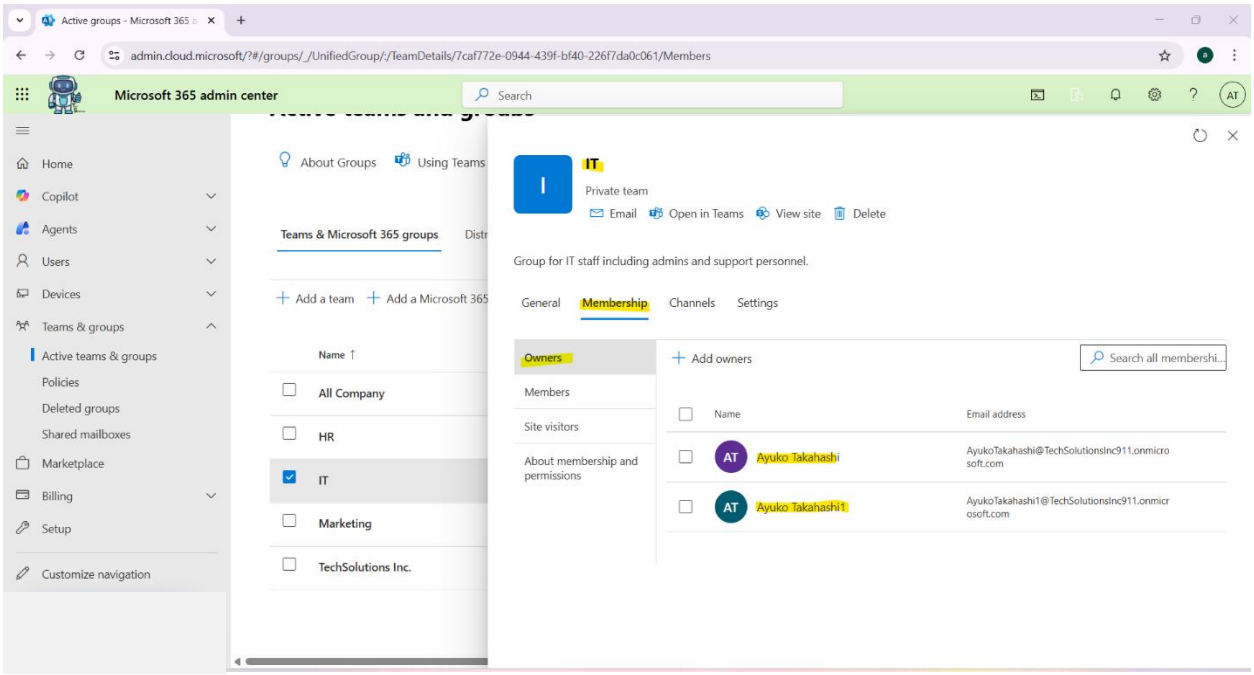
Owners of the HR group, including two Global Admins.



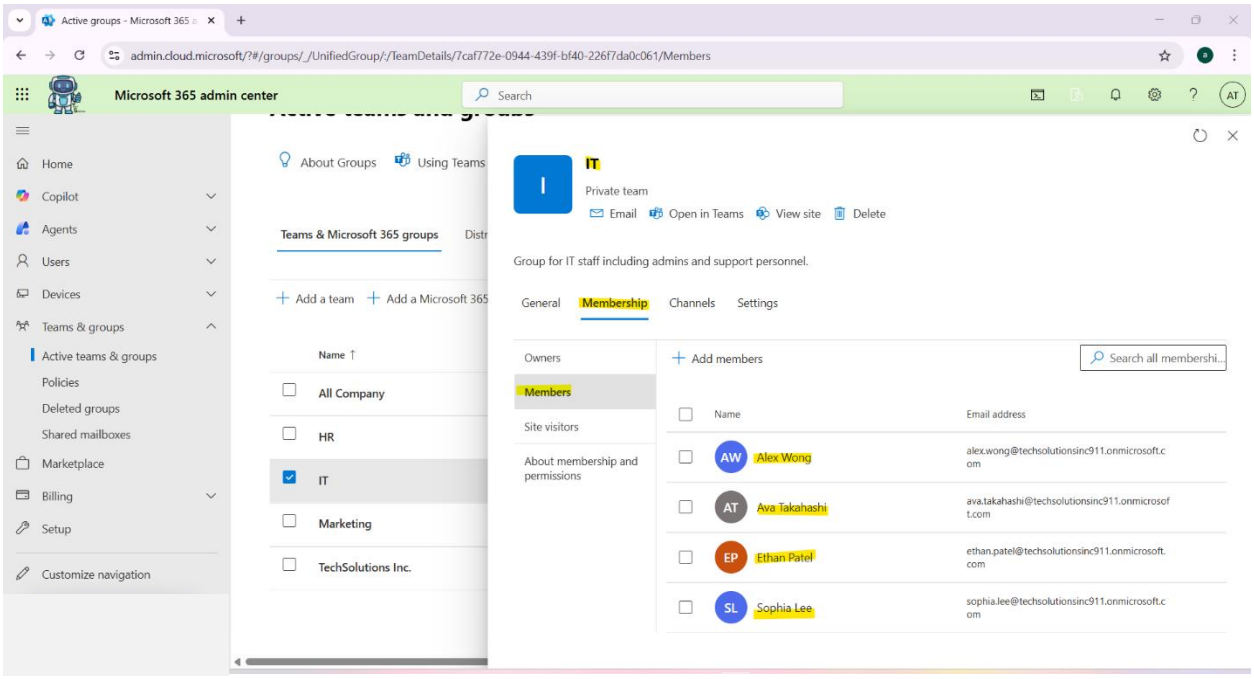
Members of the HR group, including Daniel Nguyen, Mia Chan, and Olivia Smith.



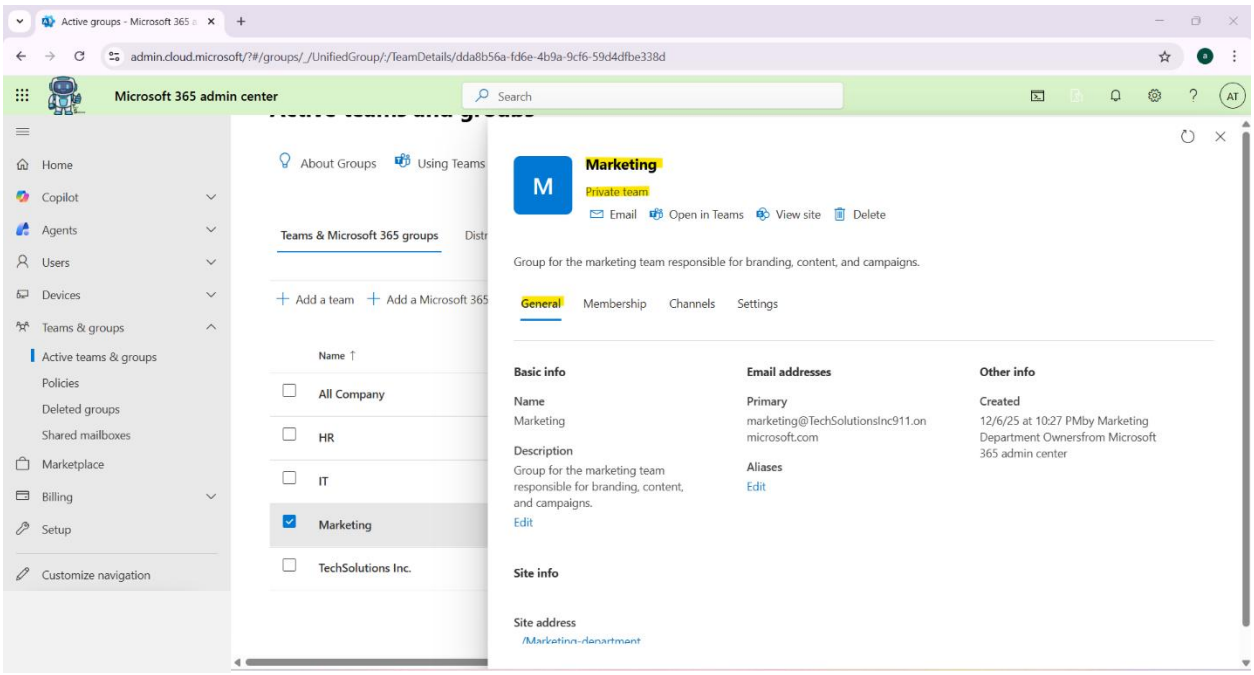
IT department Microsoft 365 group created for departmental collaboration, showing group name, privacy settings and general information.



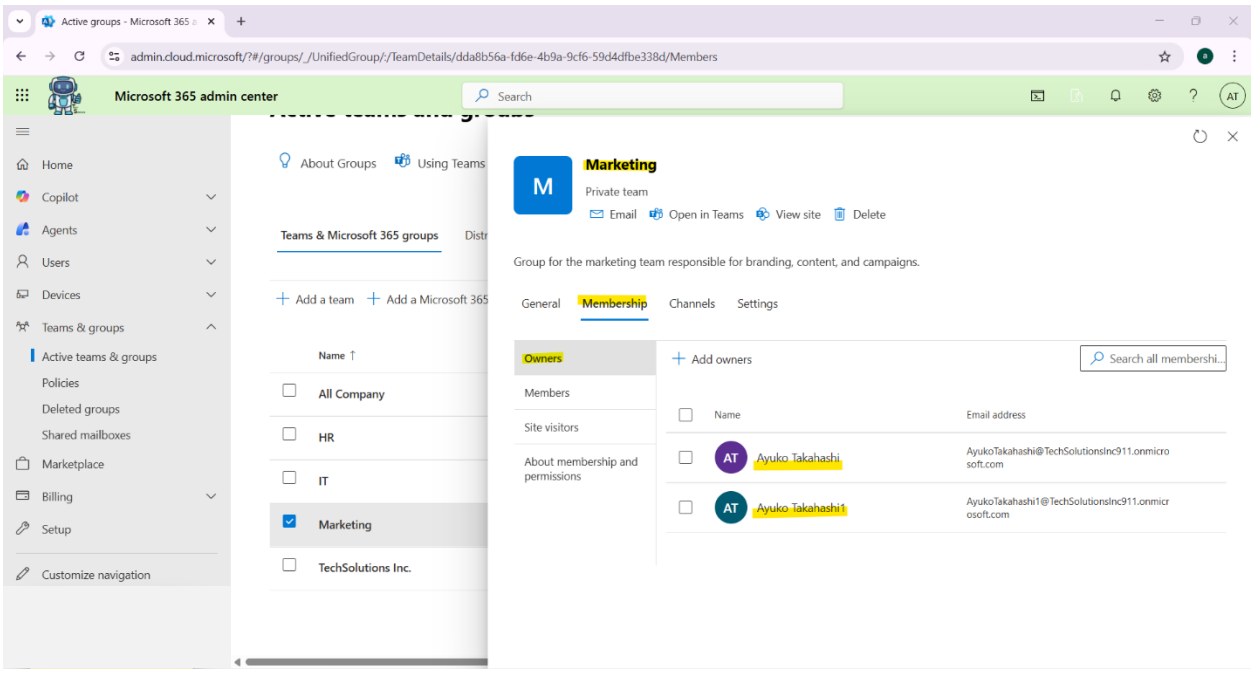
Owners of the IT group, including two Global Admins.



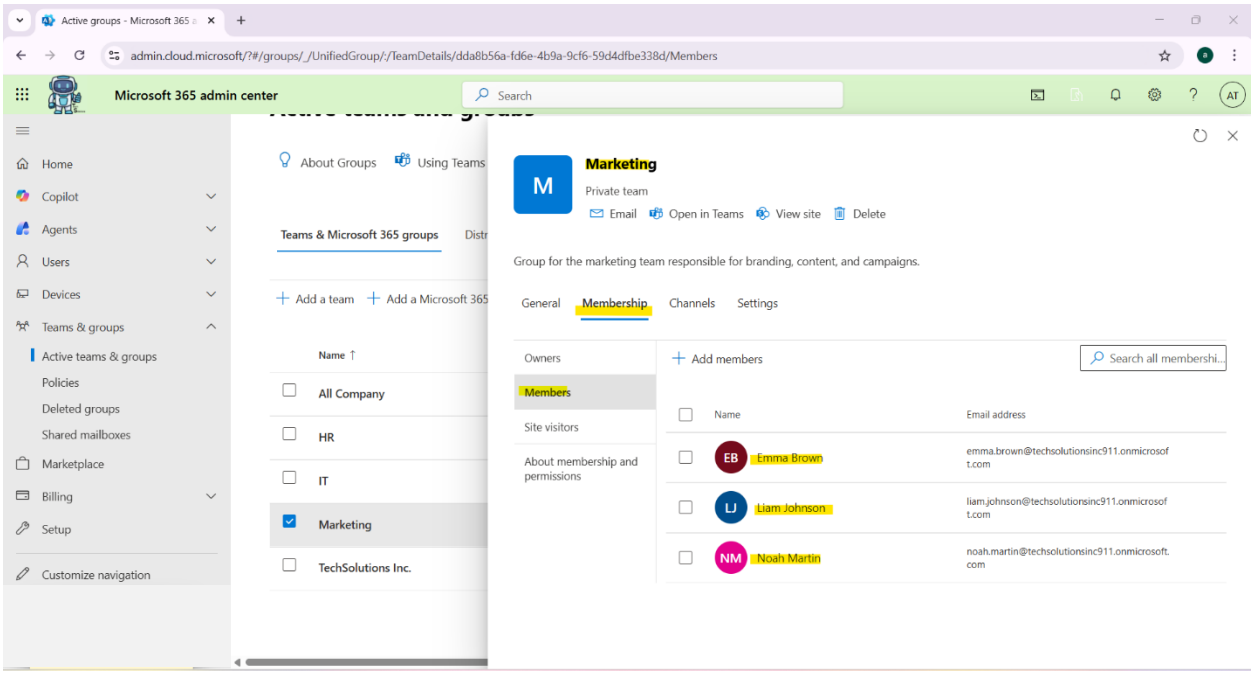
Members of the IT group, including Alex Wong, Ava Takahashi, Ethan Patel, and Sophia Lee.



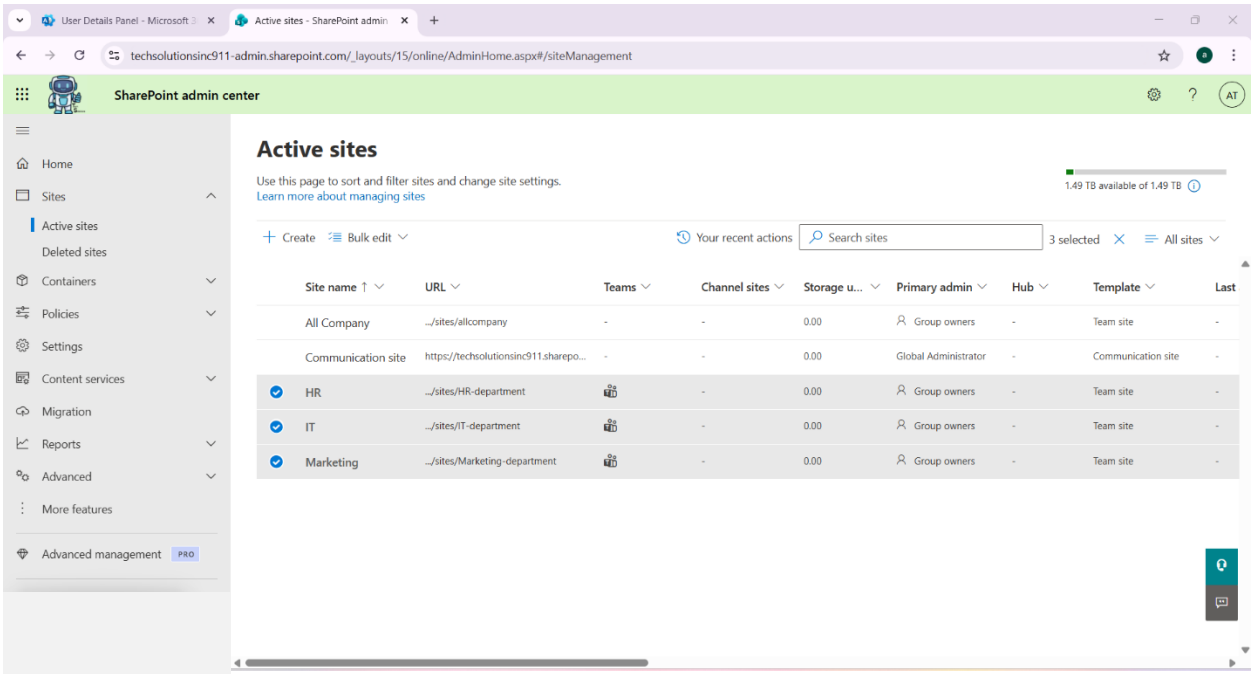
Marketing department Microsoft 365 group created for departmental collaboration, showing group name, privacy settings and general information.



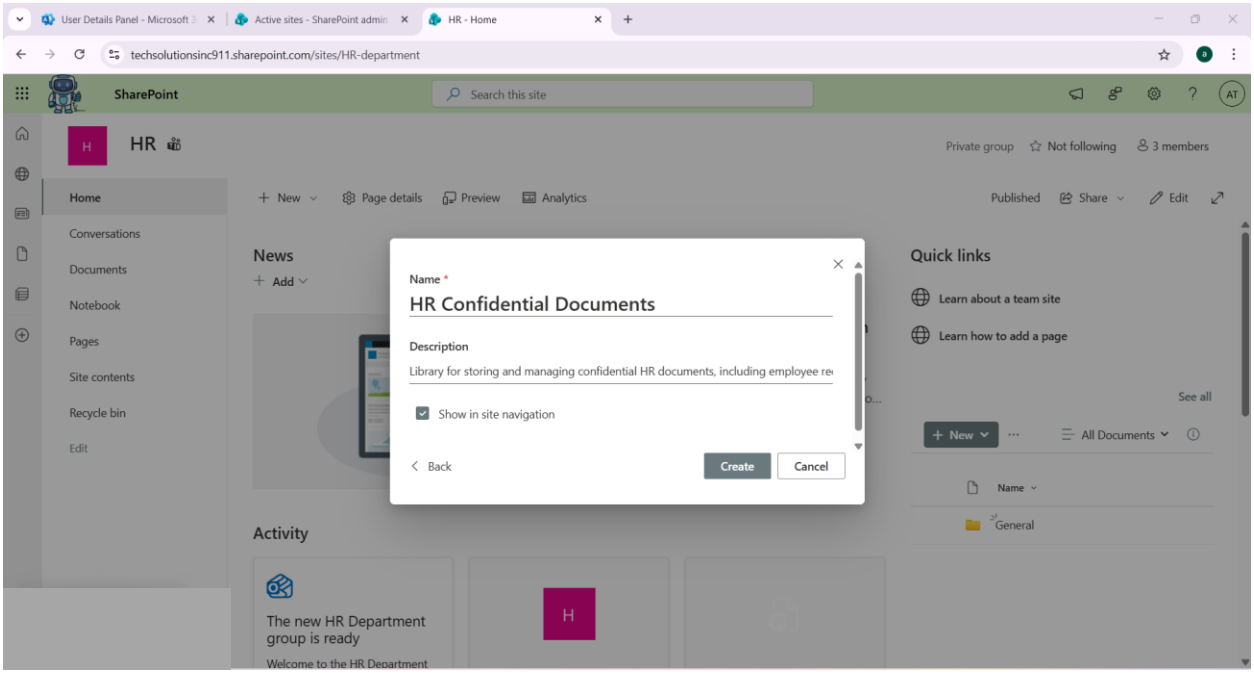
Owners of the Marketing group, including two Global Admins.



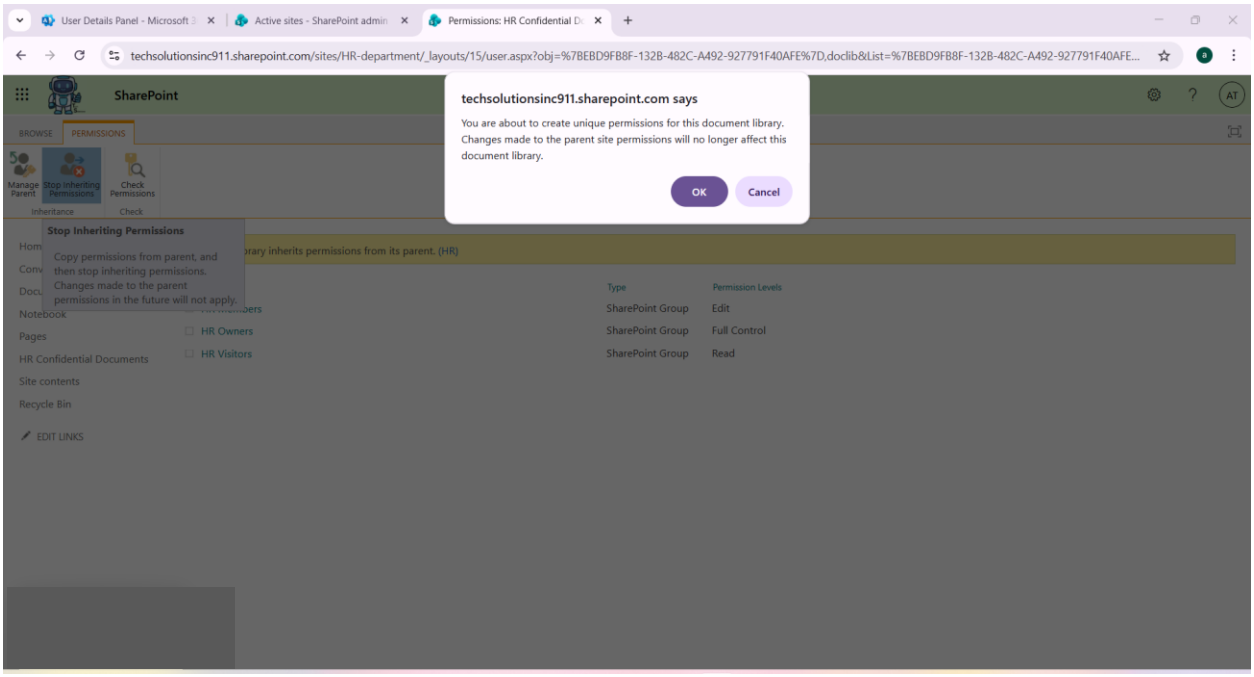
Members of the Marketing group, including Emma Brown, Liam Johnson, and Noah Martin.



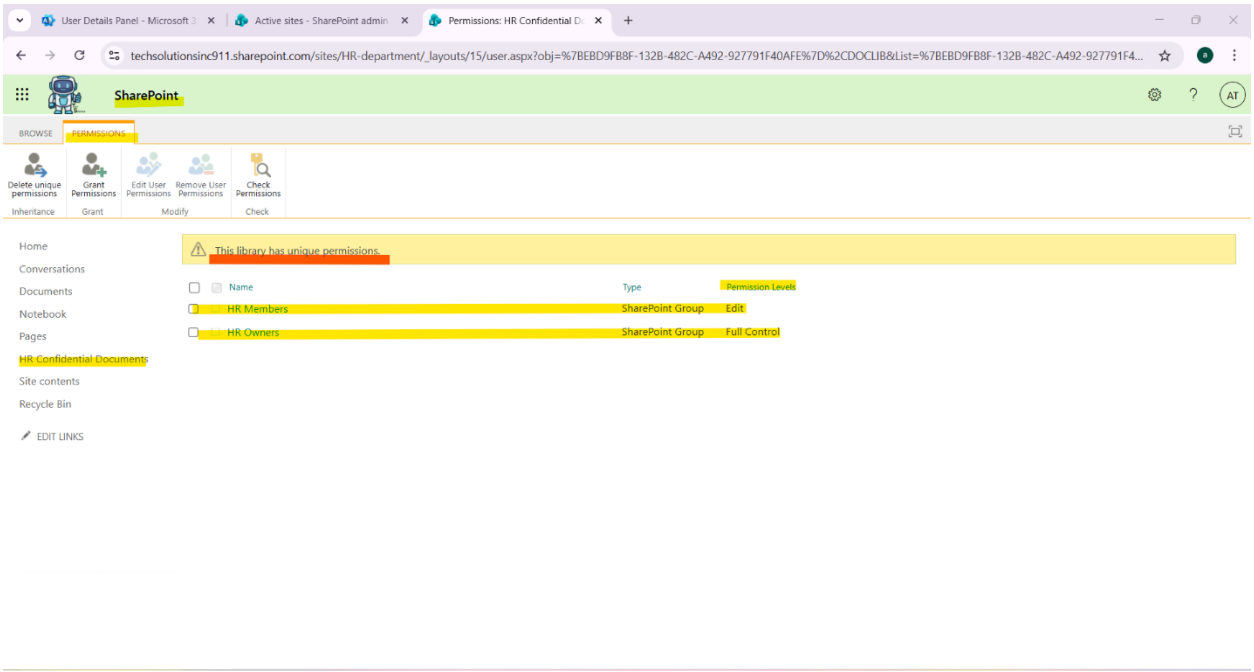
Departmental SharePoint sites were reviewed to confirm successful creation and alignment with corresponding Microsoft 365 groups.

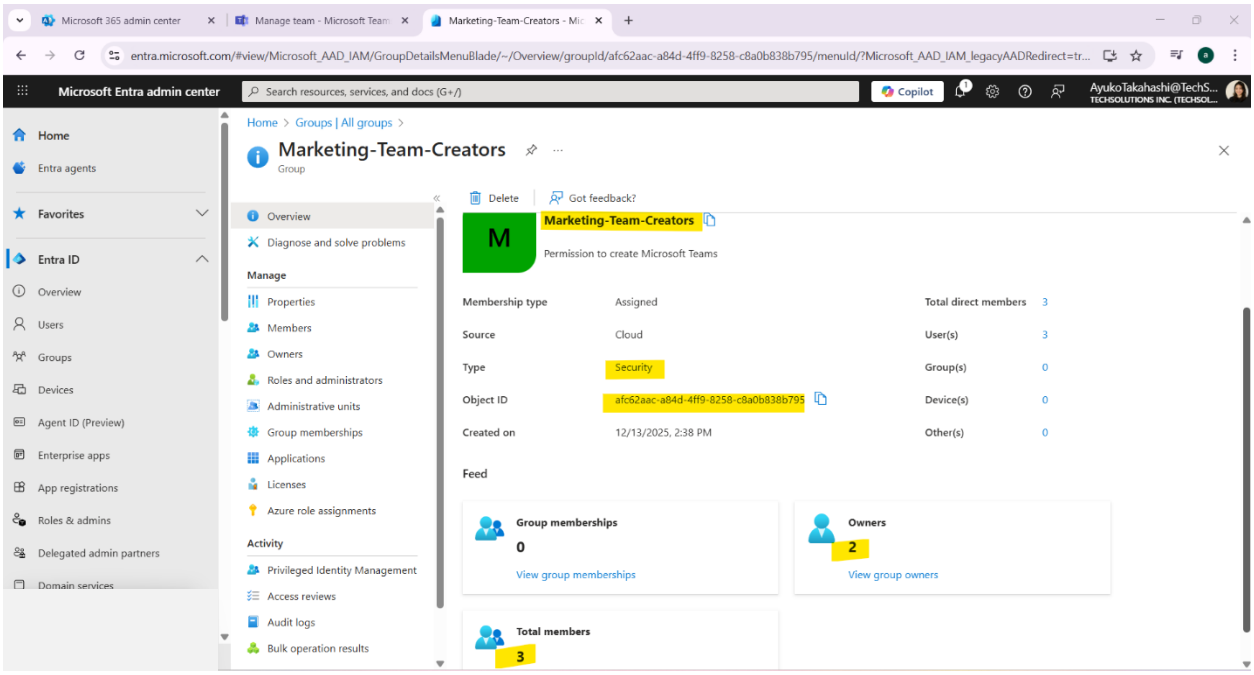


A dedicated HR document library was created to support sensitive content management.

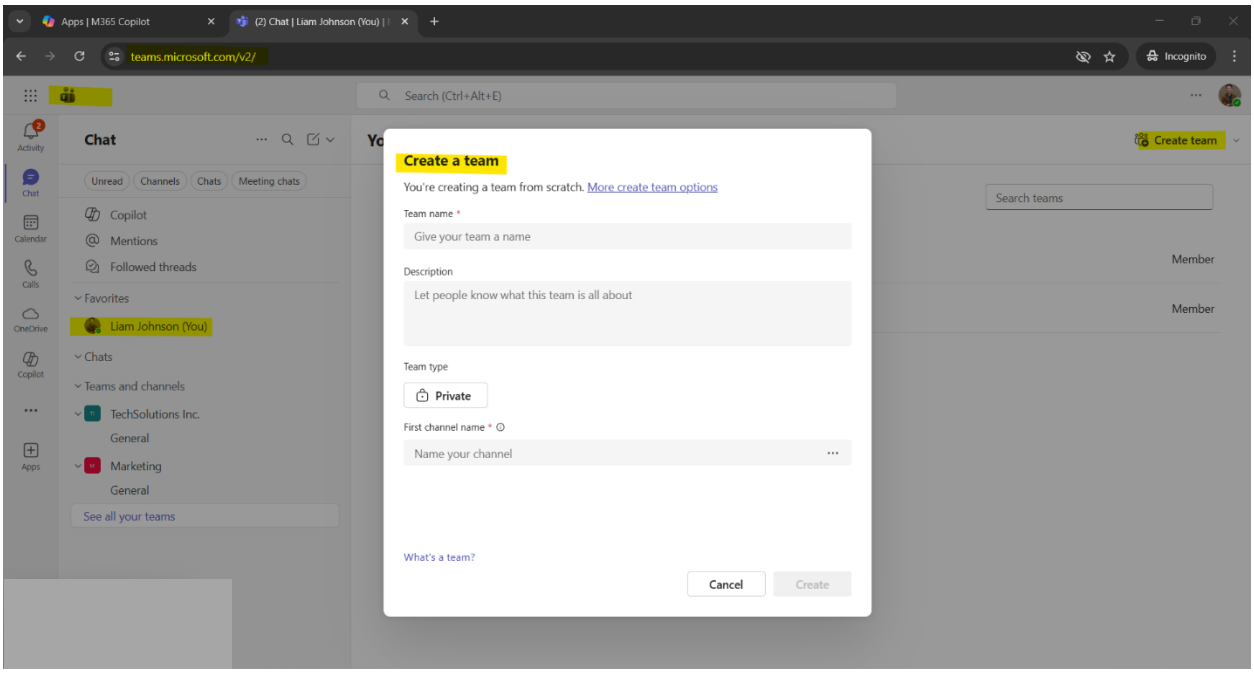


Permission inheritance was disabled for the HR document library, with access refined to remove visitor permissions, assign edit access to HR members, and grant full control to HR owners.





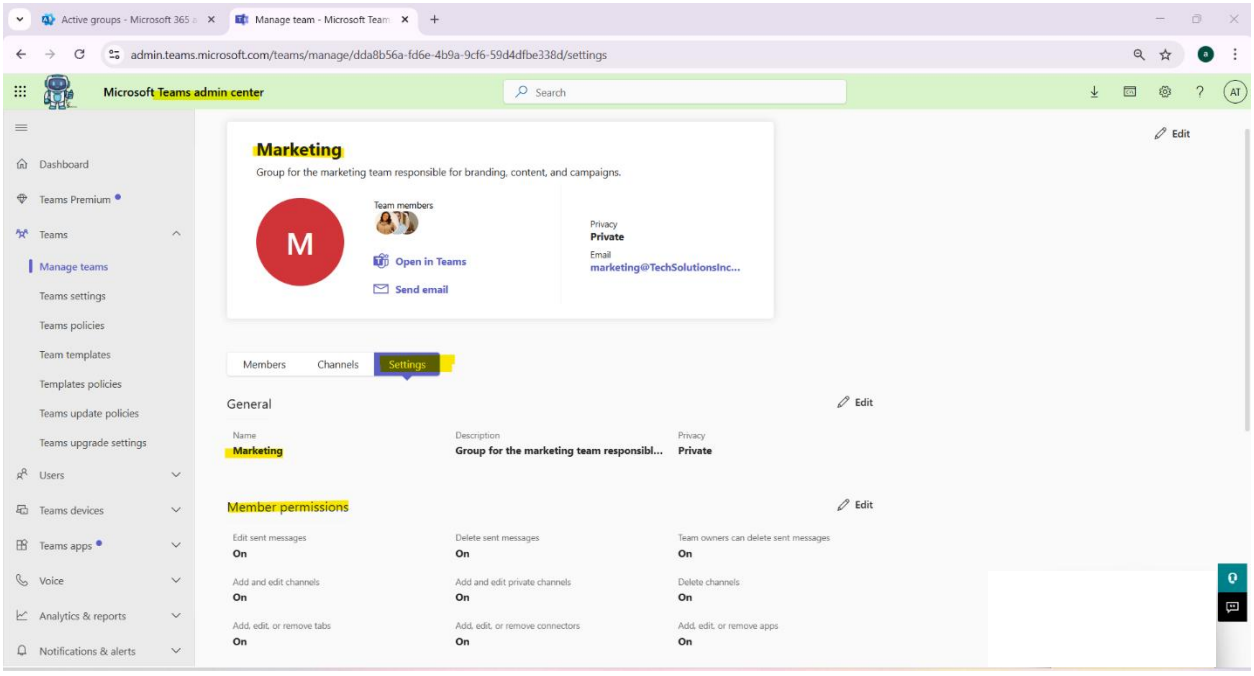
A dedicated Entra ID security group was configured to control Microsoft Teams creation, restricting group and team creation privileges to approved Marketing users.



Team creation permissions were validated by confirming that approved Marketing users retained the ability to create Teams following enforcement of restricted creation policies.

Platform Behavior Note:

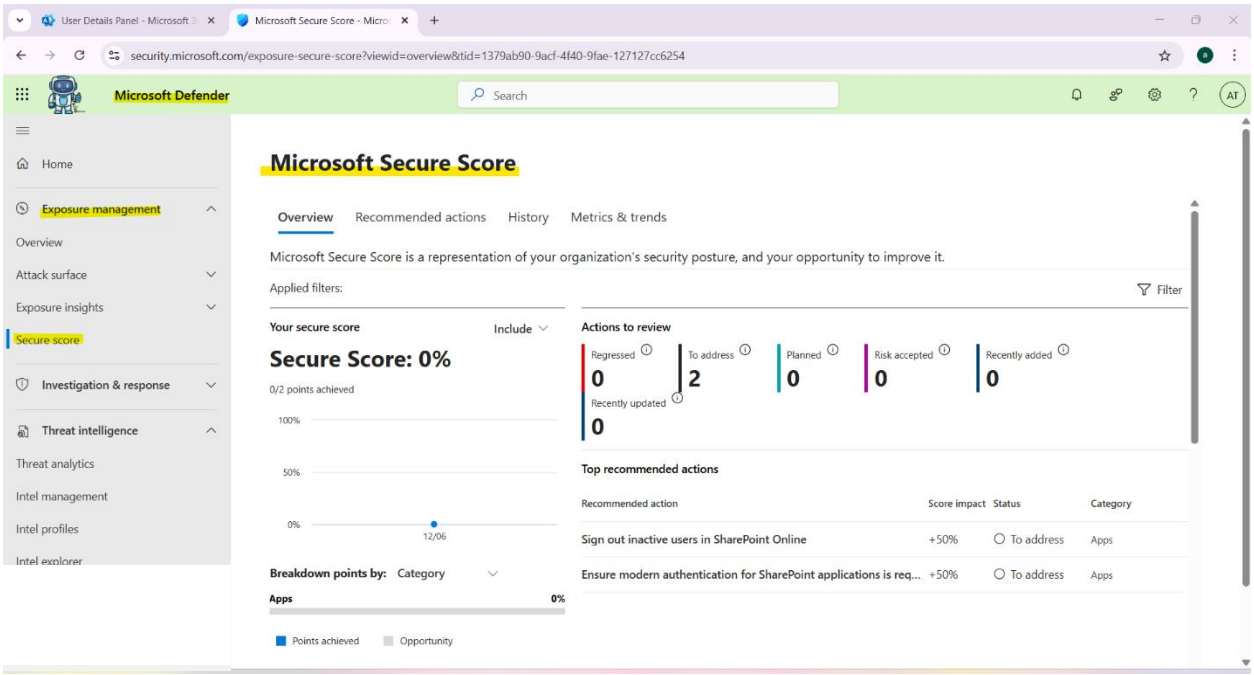
This policy requires a propagation period of up to 48 hours before enforcement is fully reflected in end-user experiences.



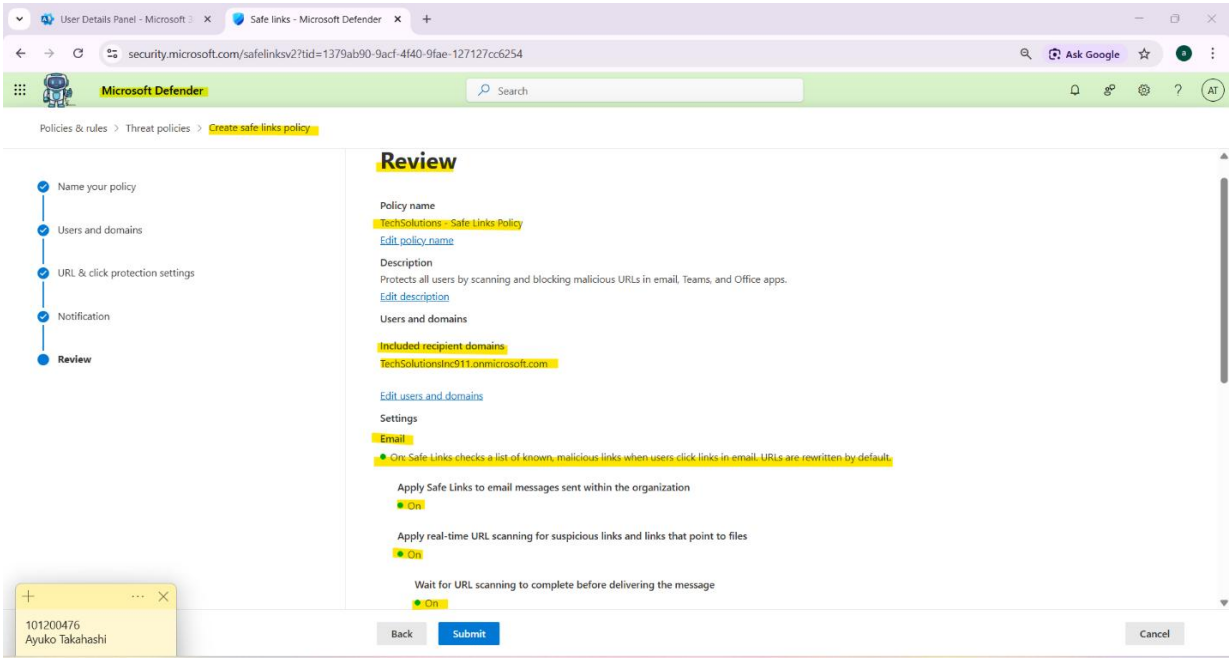
Microsoft Teams Settings page for the Marketing Team, demonstrating that the Marketing Department has full permission to manage channels, conversations, and apps.

Enterprise Security and Threat Protection

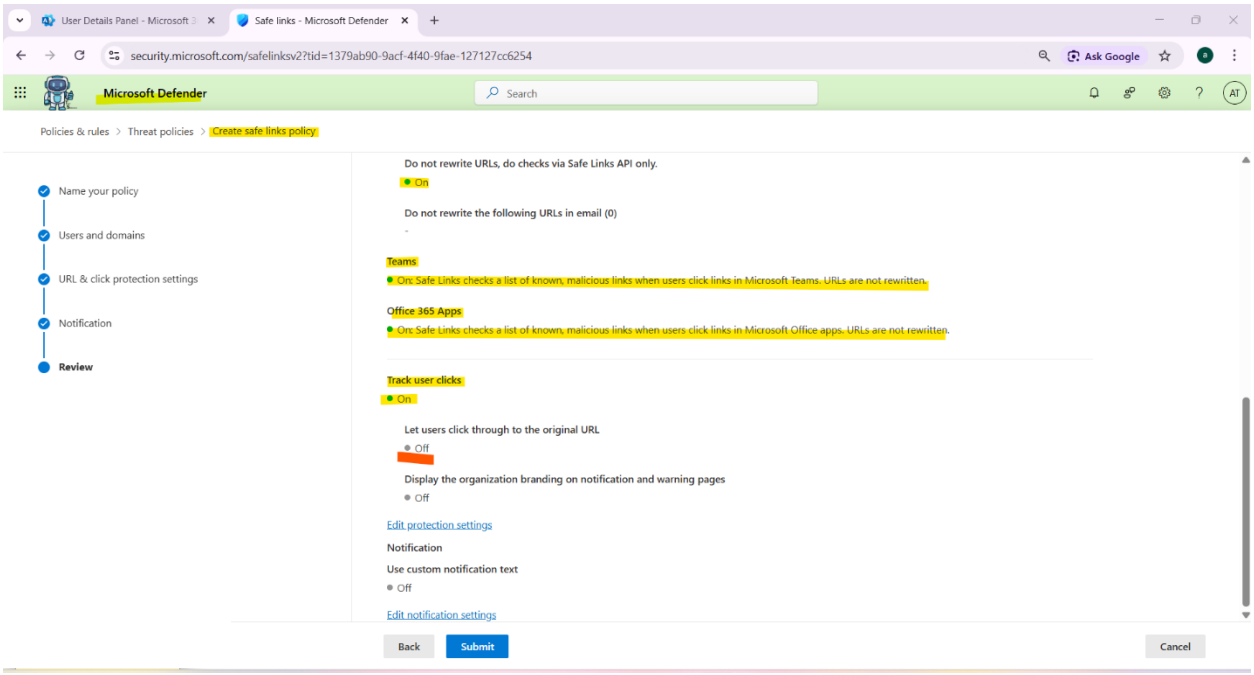
This section documents the configuration of Microsoft 365 security controls, including email threat protection, anti-phishing policies, and impersonation safeguards to reduce organizational risk.



Microsoft Defender Secure Score was reviewed to assess the organization's security posture and baseline protection status.



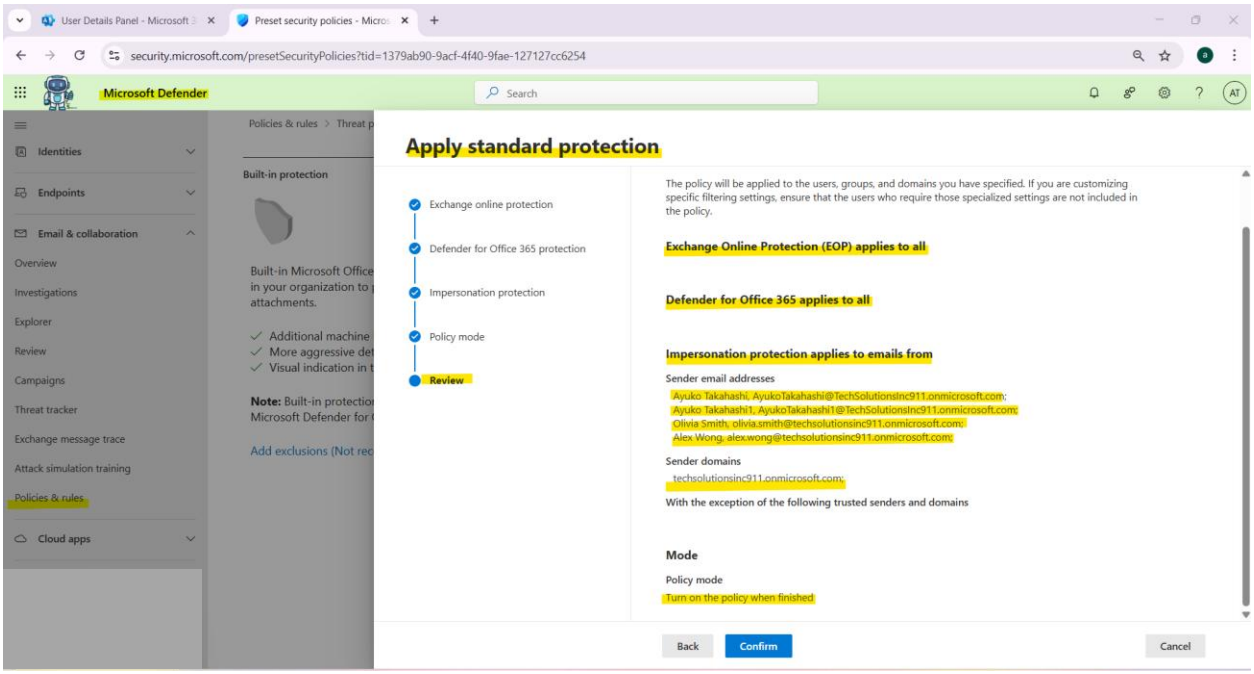
Review of Customized Safe Links Policy, including all users by selecting TechSolutions domain. Safe Links protections enabled for Email and Teams, and Office apps with real-time URL scanning.



Safe Links configured with click protection enforced to block unsafe URLs and track user interactions.

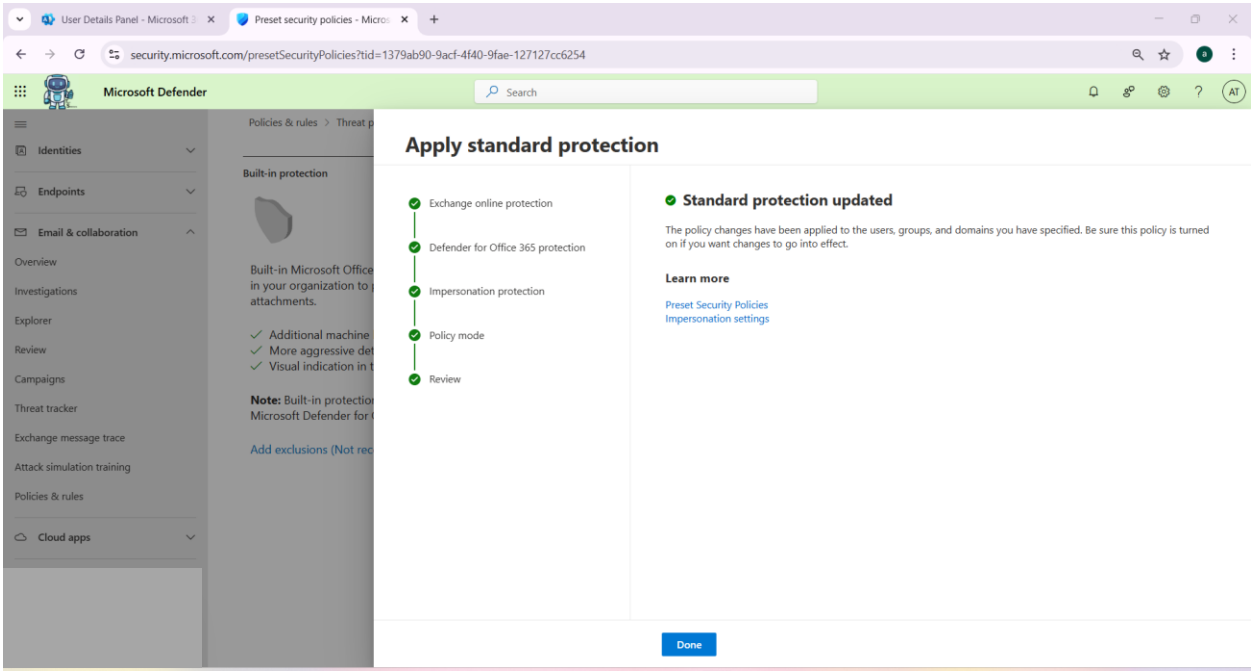
***After submitting the policy, Client error dialog box is presented, saying**
'Microsoft.Exchange.Management.PSDirectInvoke.DirectInvokeCmdletExecutionException' was thrown.

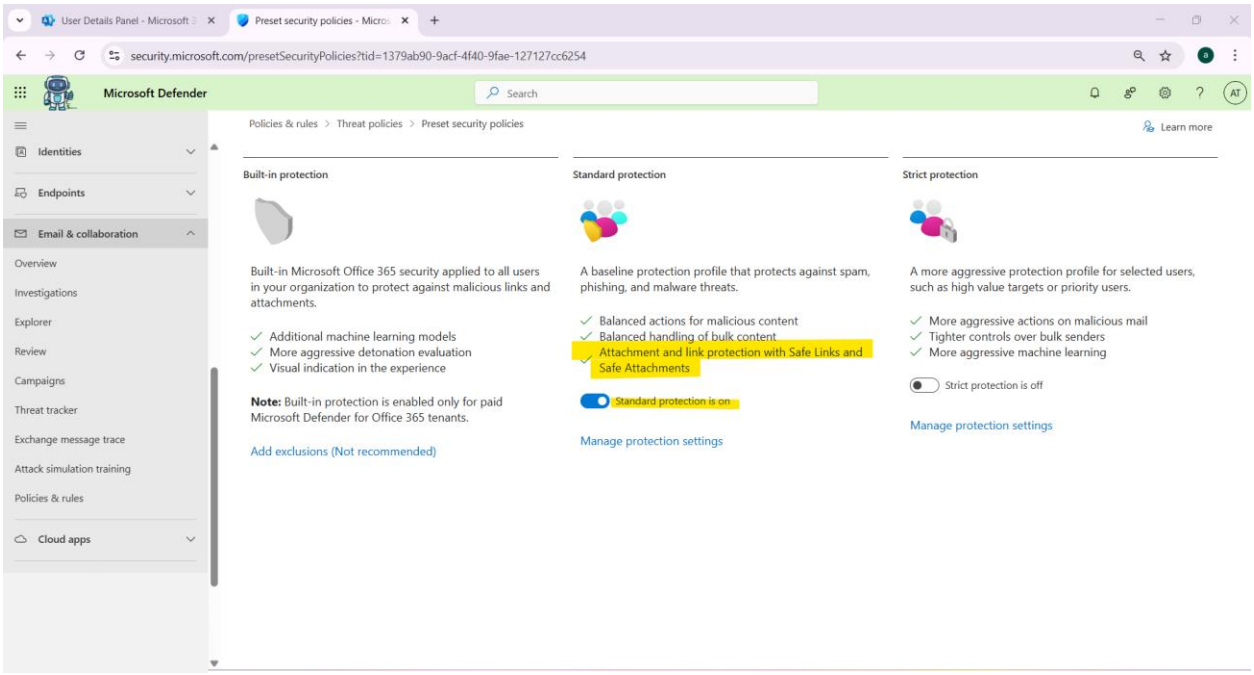
Platform Behavior Note:
This behavior is consistent with initial Exchange Online Defender backend initialization delays, which can occur before preset security policies become fully available. So, navigate to Preset Security Policies to initialize it.



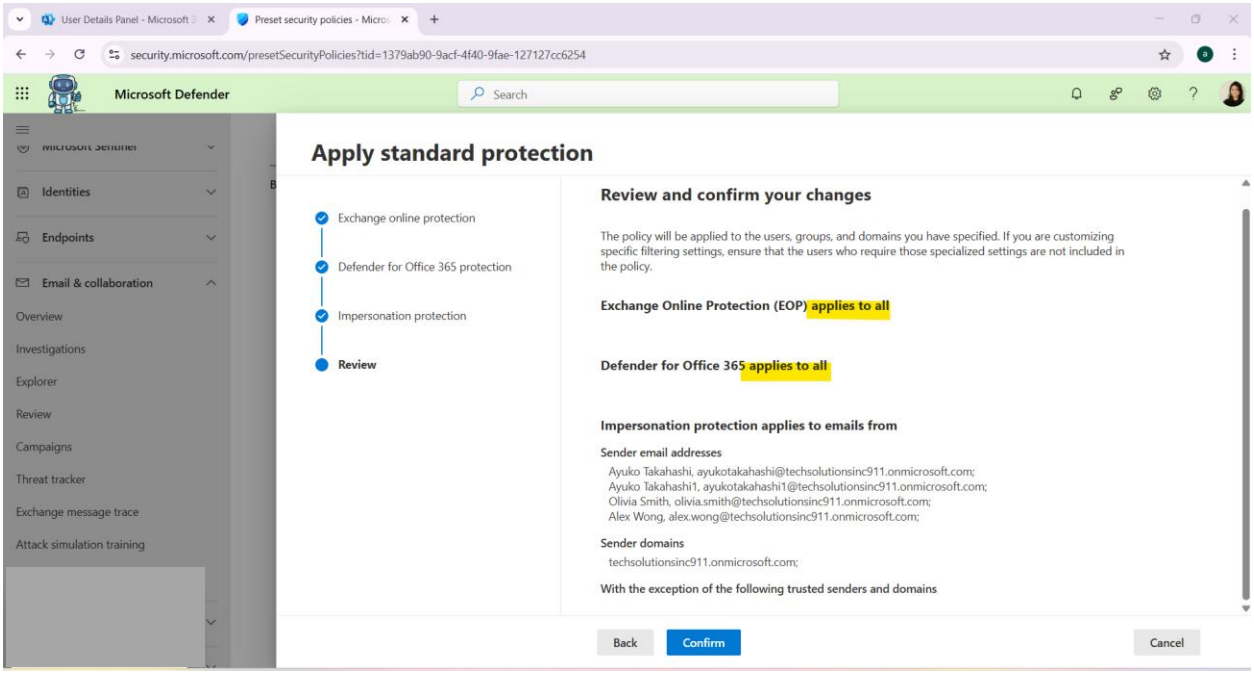
The Standard Preset Security Policy was enabled organization-wide, activating baseline protections including Safe Links, Safe Attachments, and impersonation safeguards.

- Added high-value users (Global Admins, HR Manager, IT Manager) to impersonation protection to reduce spear-phishing and business email compromise (BEC) risks.
- Added organizational domain to Protected Custom Domains to defend against domain spoofing and impersonation attempts.
- Trusted senders and domains left empty to maintain strict impersonation protection.

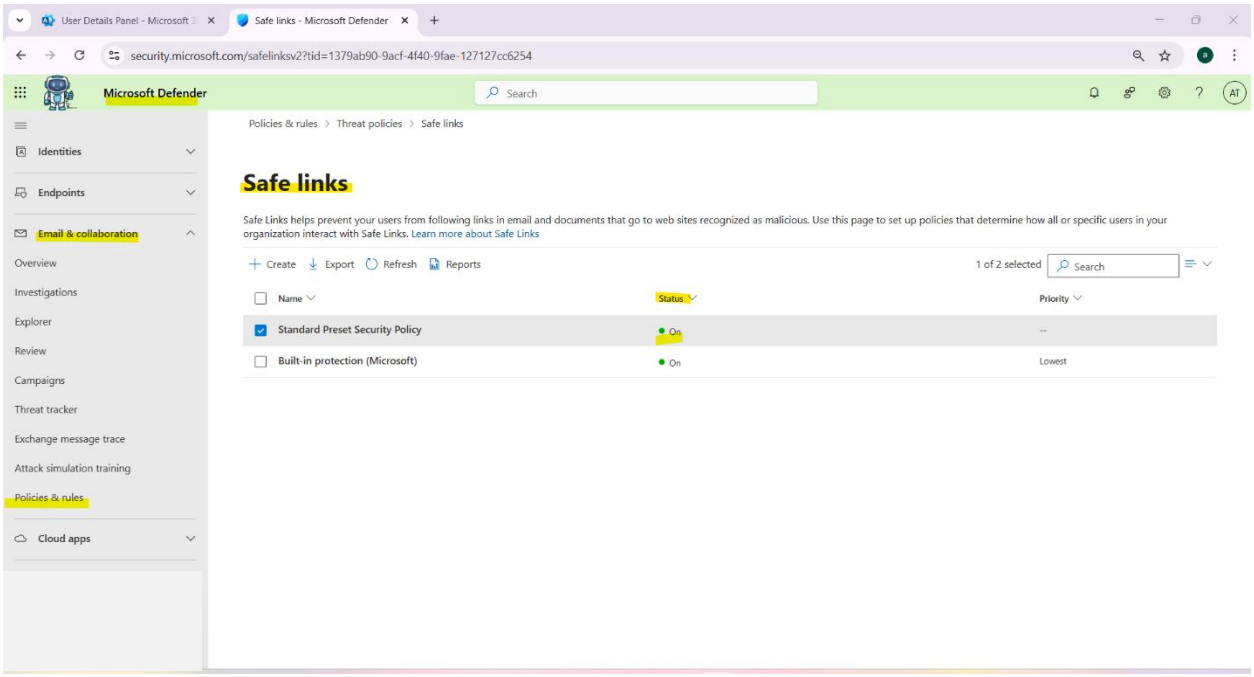




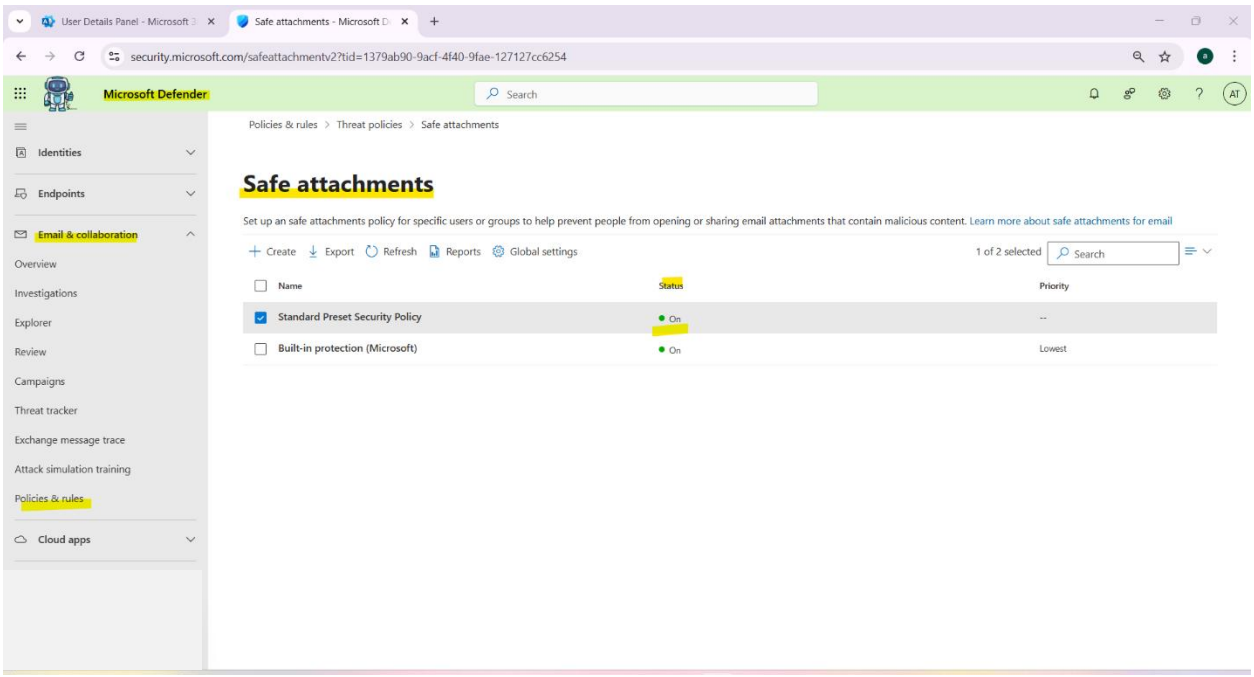
Microsoft Defender for Office 365 Standard protection was applied across the organization, enabling Safe Links and Safe Attachments through centrally managed protection settings.



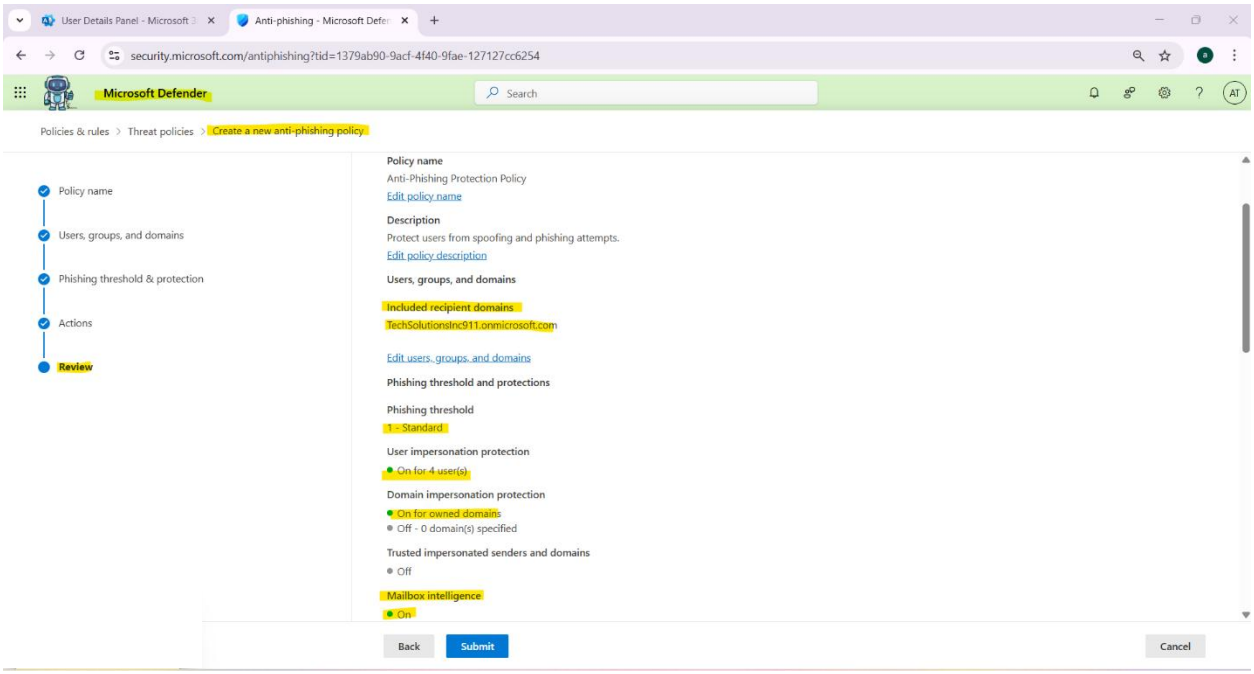
*Impersonation protection was additionally configured for key personnel to mitigate targeted phishing attacks.



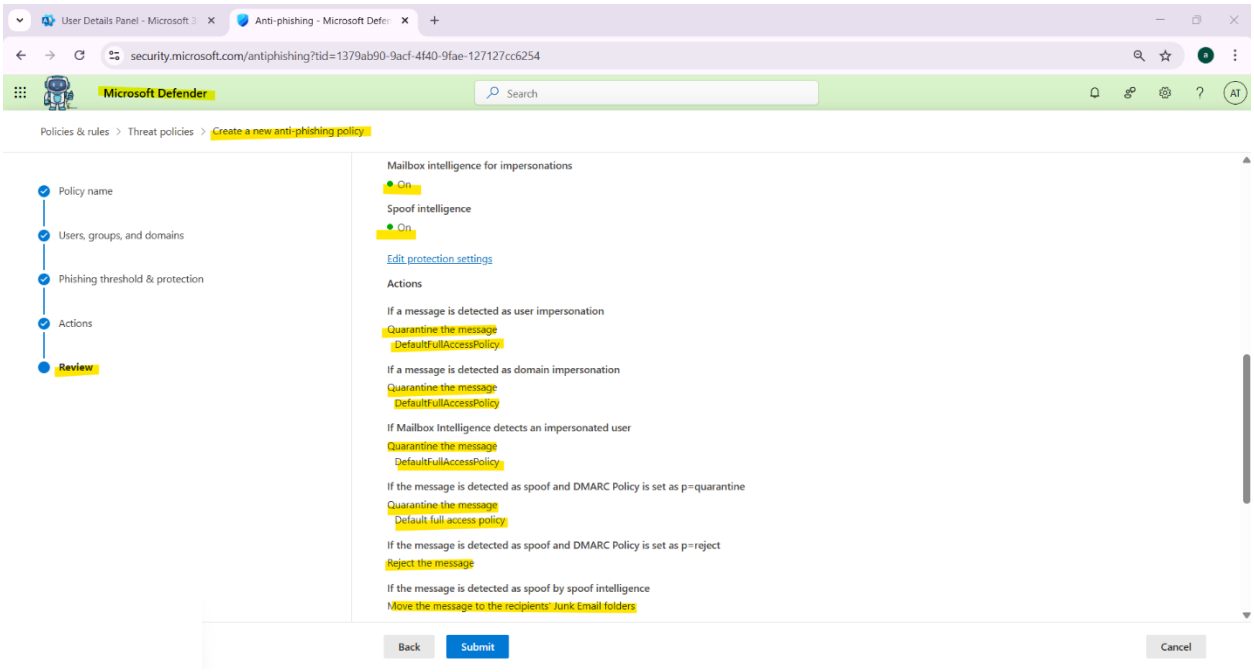
Safe Links protection was validated through the applied Standard Preset Security Policy.

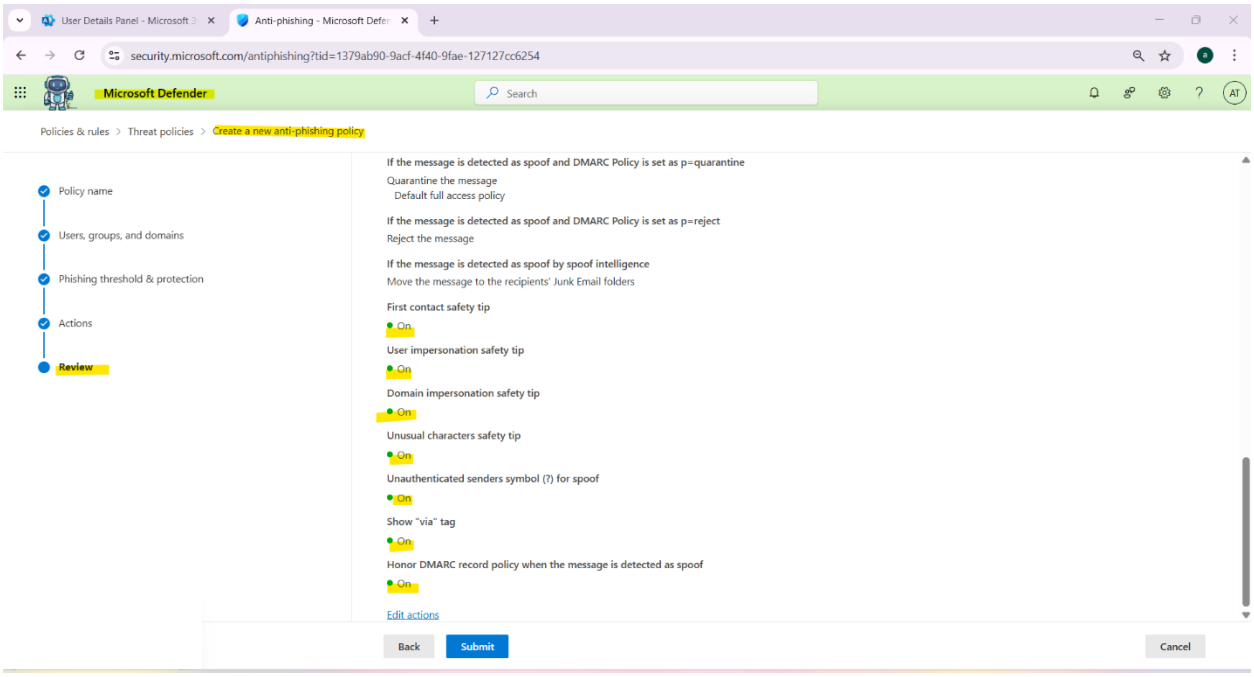


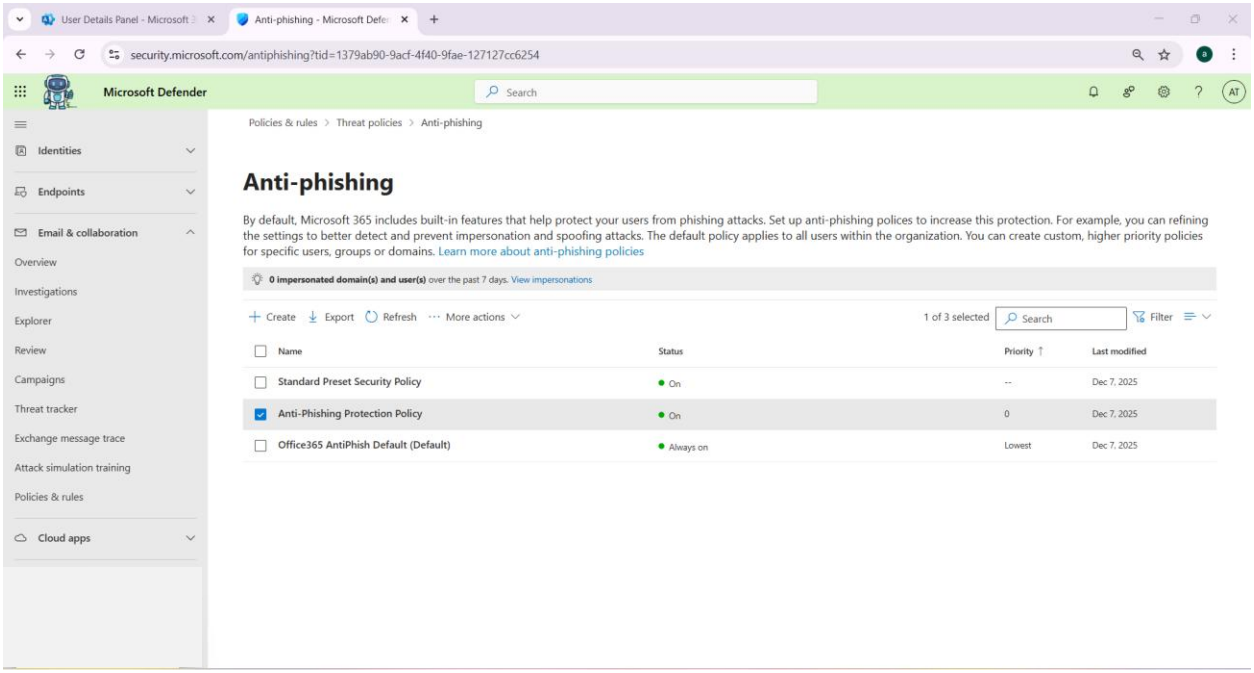
Safe Attachments enforcement was confirmed through the applied Standard Preset Security Policy.



A comprehensive anti-phishing policy was configured, enabling user and domain impersonation protection, mailbox intelligence, spoof detection, DMARC enforcement, and user safety tips. Quarantine actions were applied to high-risk phishing scenarios to prevent malicious email delivery.



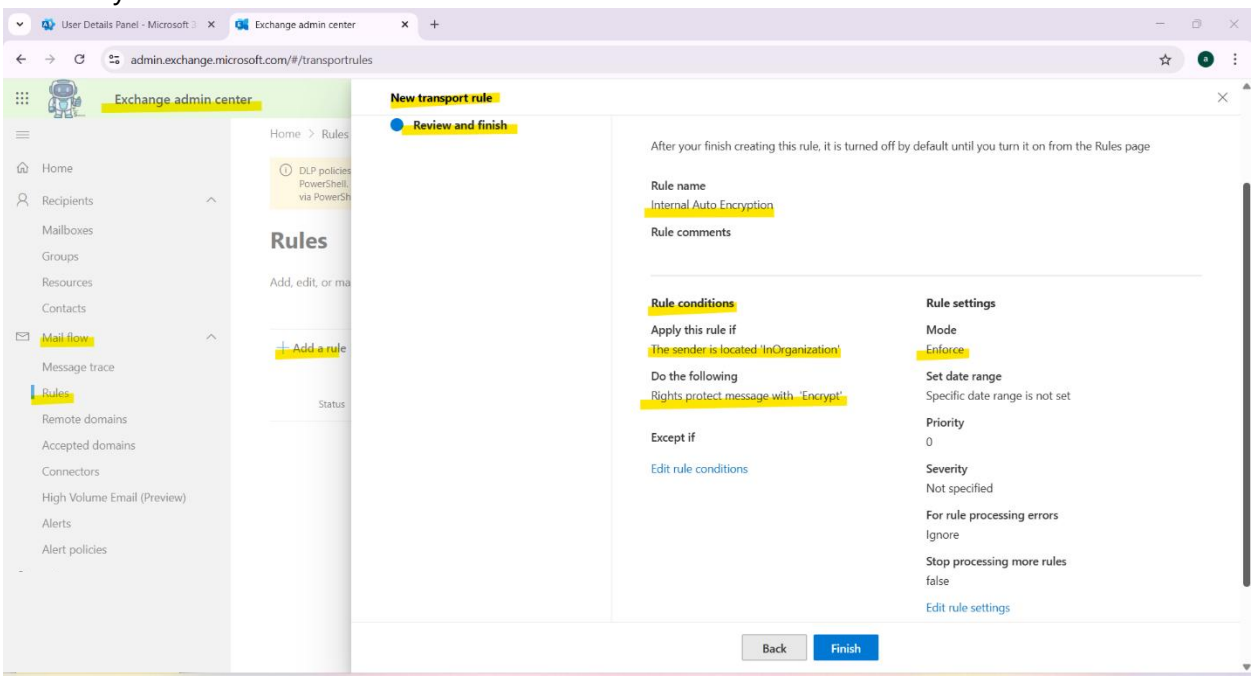




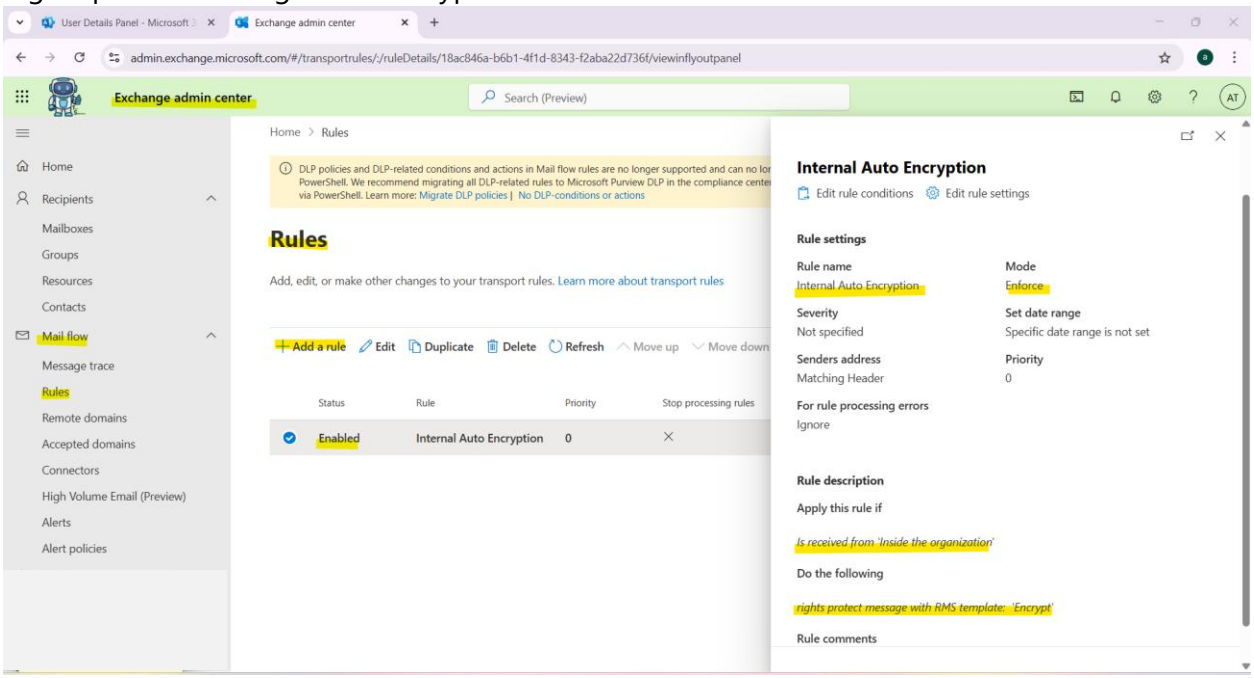
New Anti-Phishing Protection Policy has been created and active.

Data Protection and Message Encryption

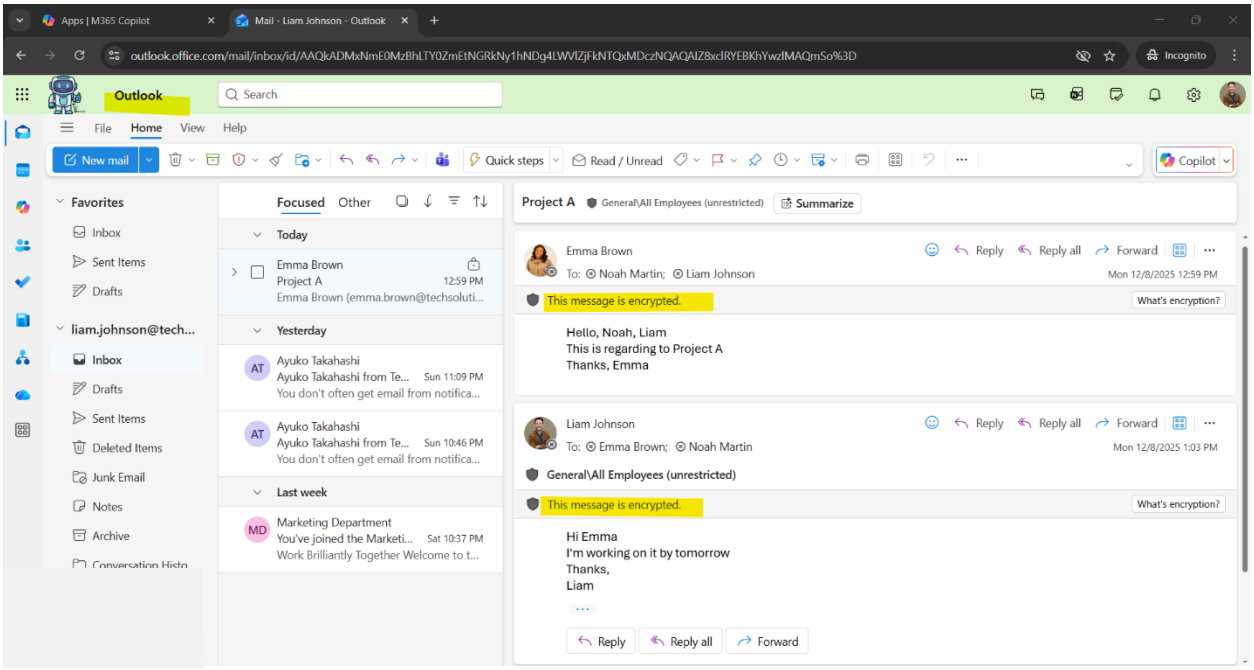
This section demonstrates the implementation of data protection measures, including automatic message encryption, to ensure sensitive communications are protected both internally and externally.



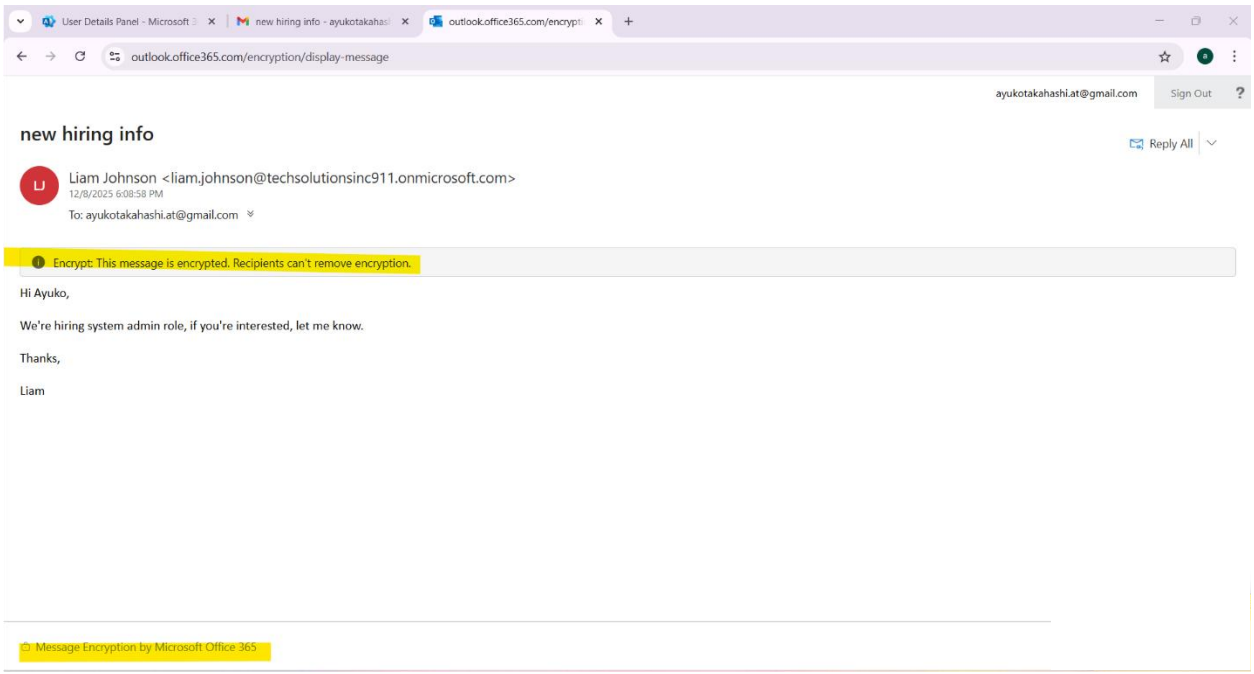
Review the settings: Apply this rule if The sender is located 'In Organization', Do the following: Rights protect message with 'Encrypt'.



An internal auto-encryption rule was configured to automatically protect messages sent from internal users.



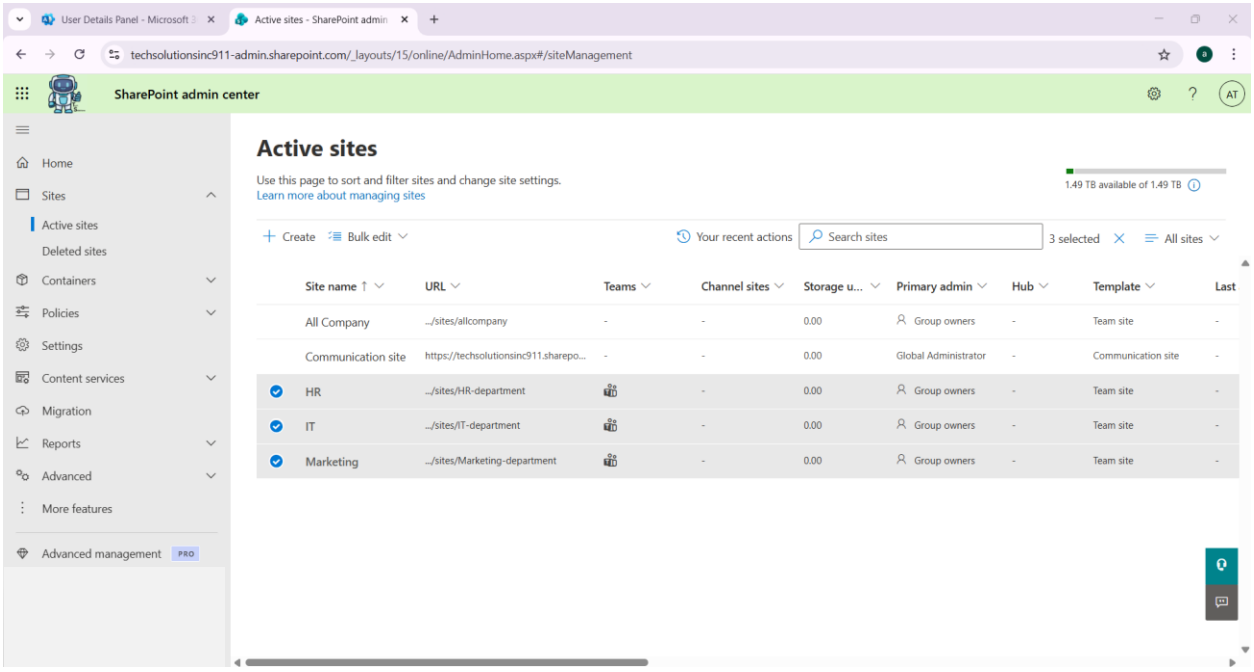
Emails sent from Emma and Liam (Inside organization) are successfully encrypted.



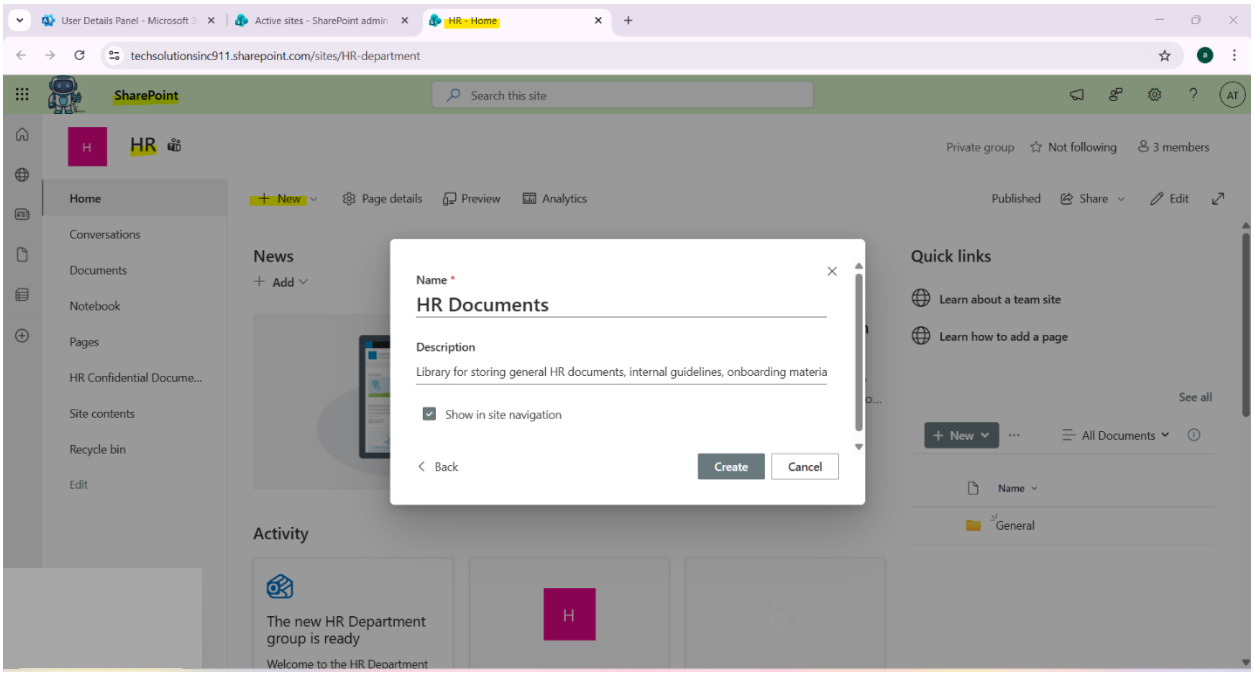
Email sent from Liam to outside organization (my private email address) is also successfully encrypted.

Collaboration Services Configuration and Governance

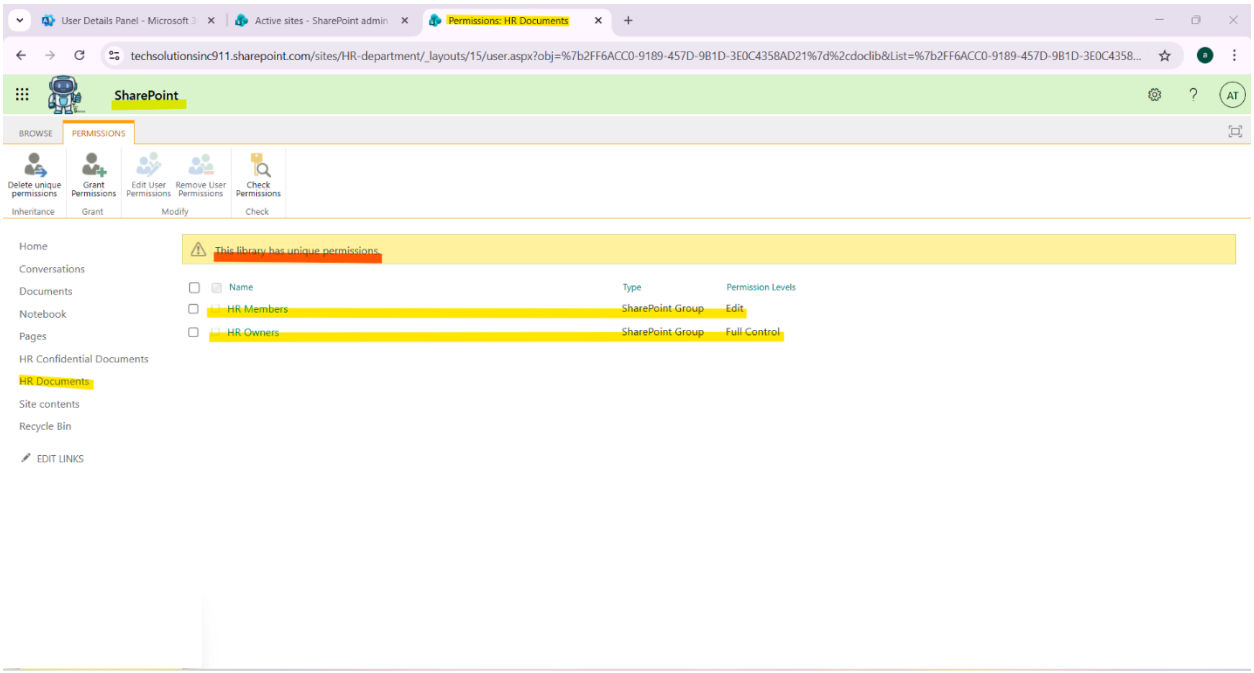
This section outlines the configuration and governance of collaboration platforms such as SharePoint, OneDrive, Teams, and Viva Engage to support secure and policy-compliant collaboration.

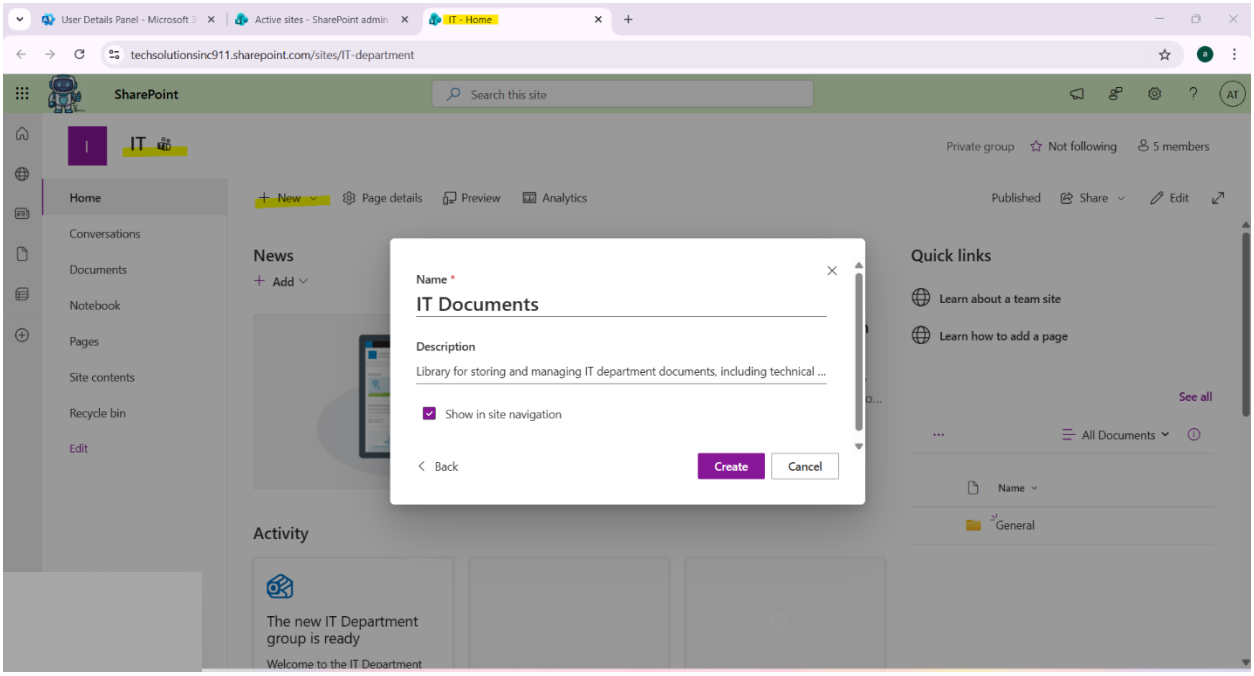


Each department site was created at the same time when each office 365 group was created.

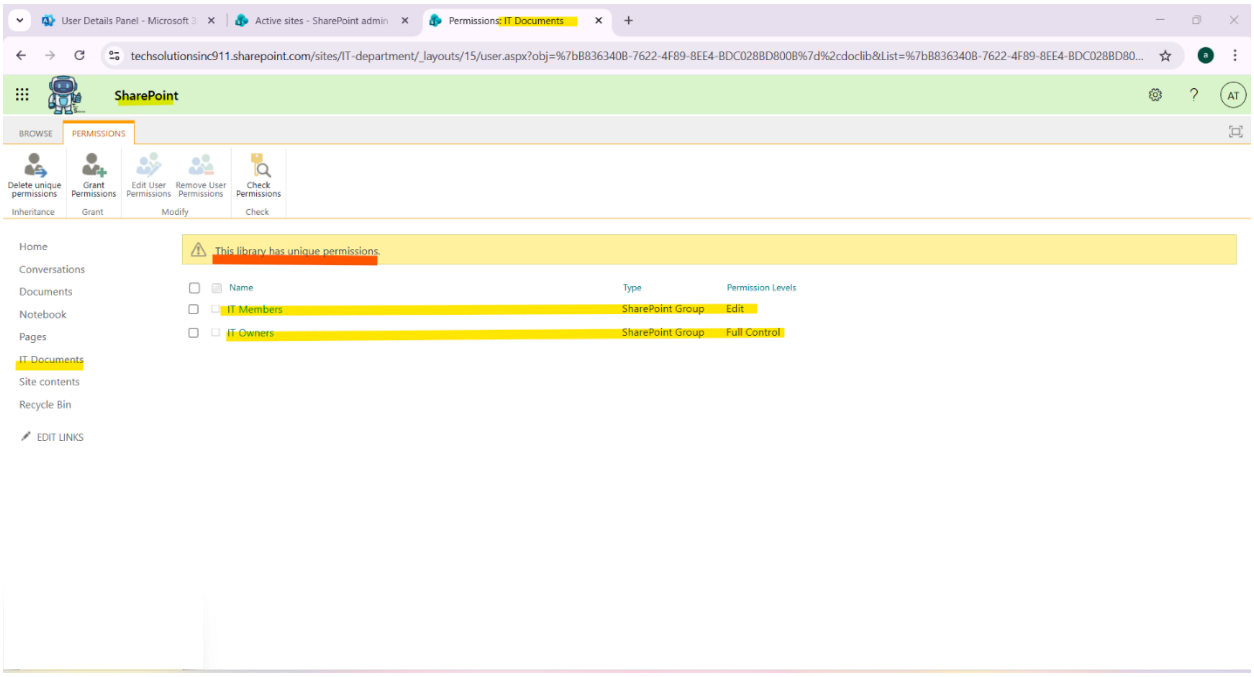


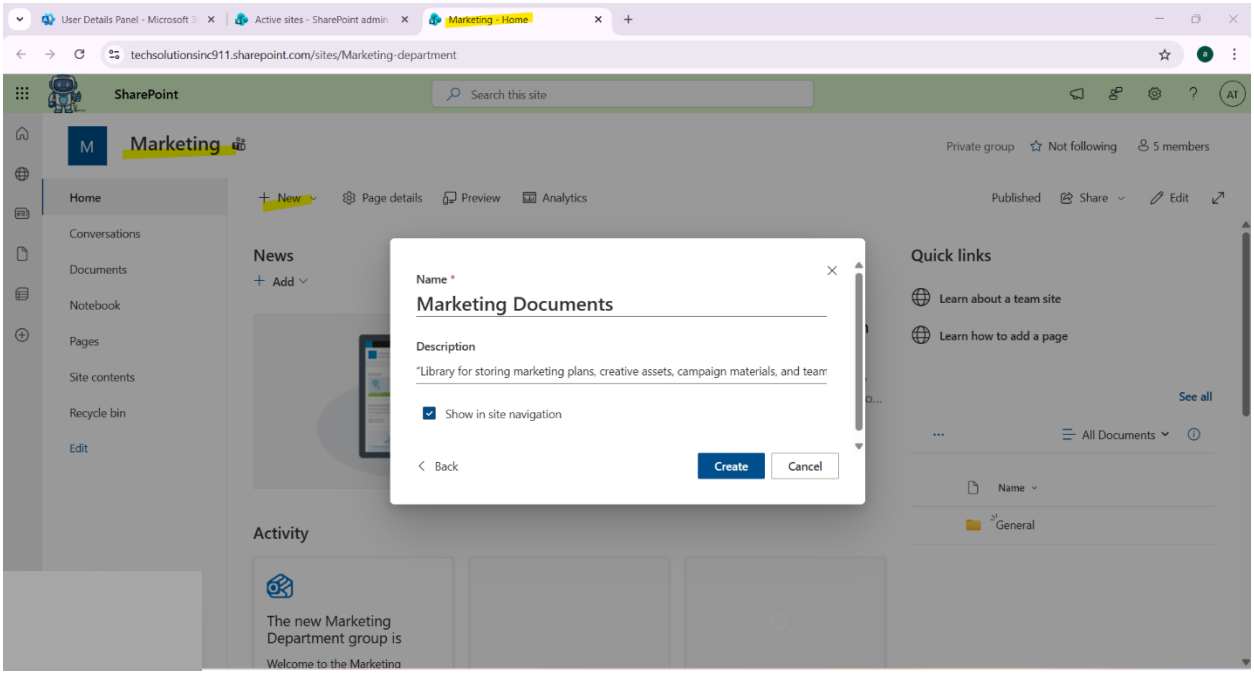
A confidential HR document library was created, with permissions configured to restrict access to authorized HR members and owners.



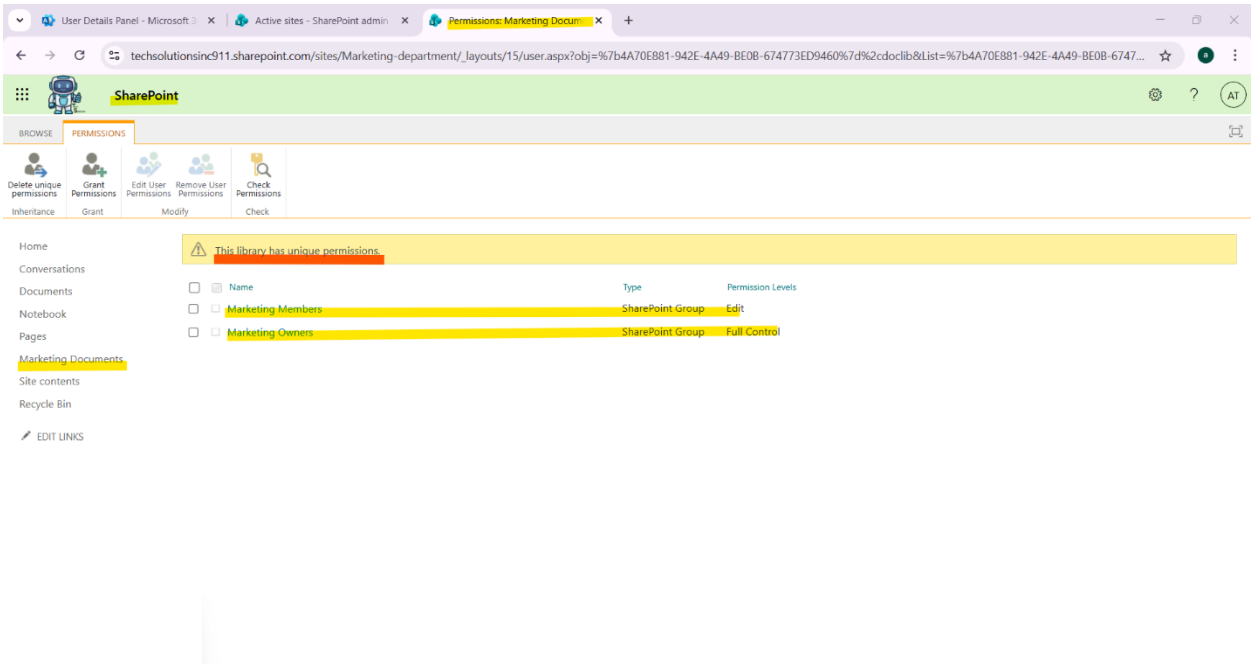


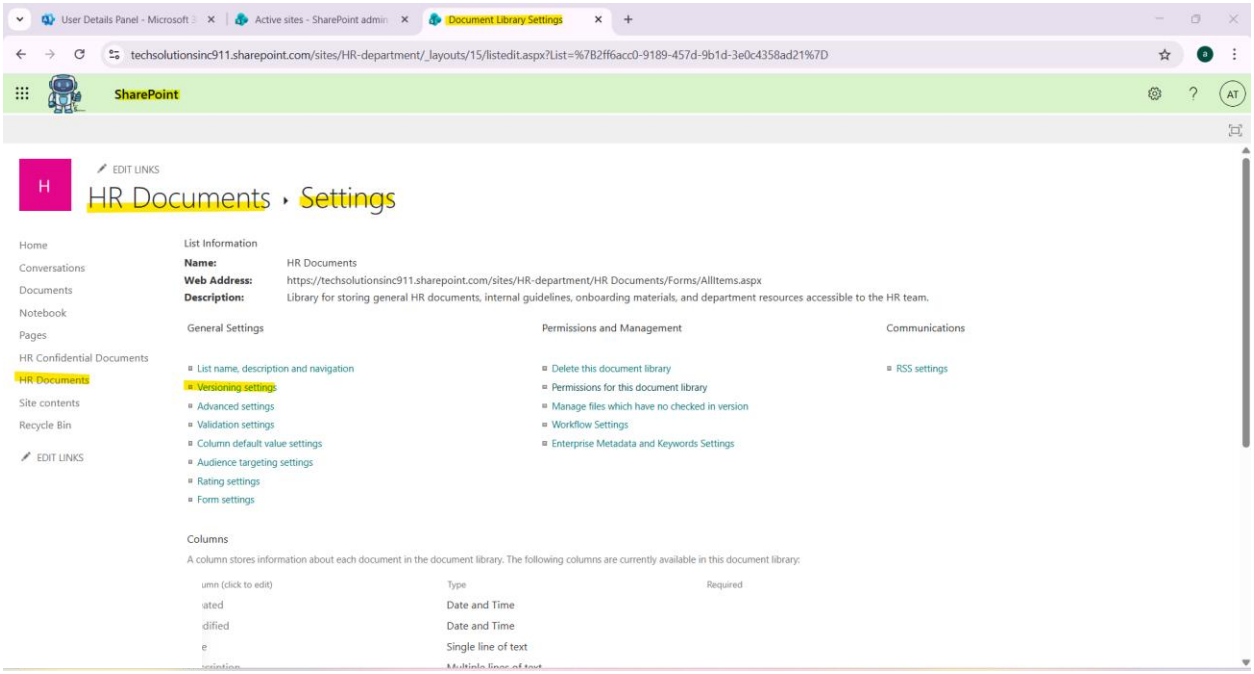
A confidential IT document library was created, with permissions configured to restrict access to authorized IT members and owners.



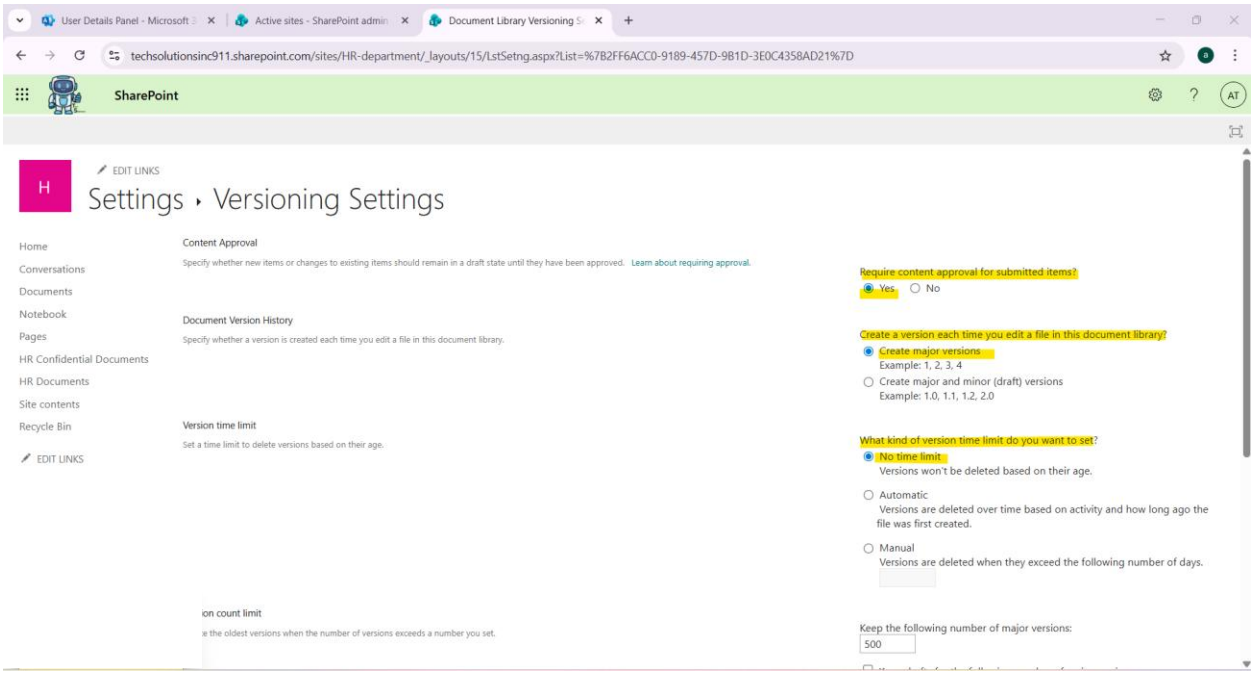


A confidential Marketing document library was created, with permissions configured to restrict access to authorized Marketing members and owners.

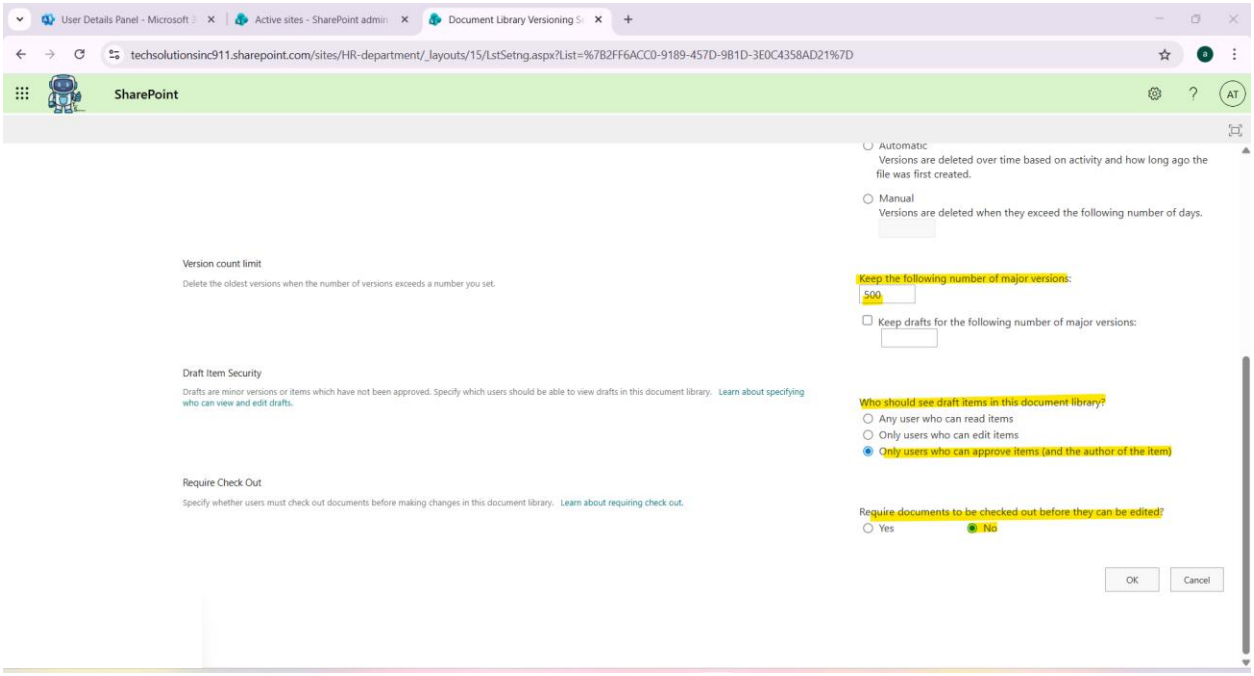




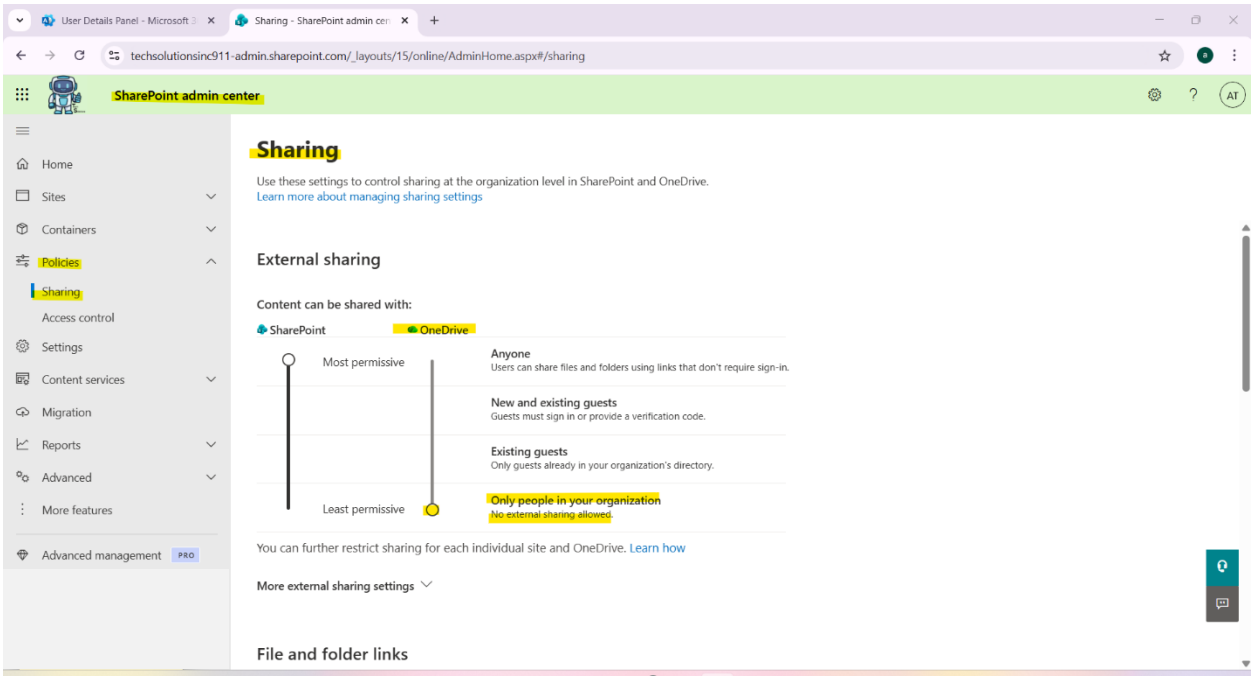
Versioning settings.



Enabled Required content approval and major versioning and set No time limit.



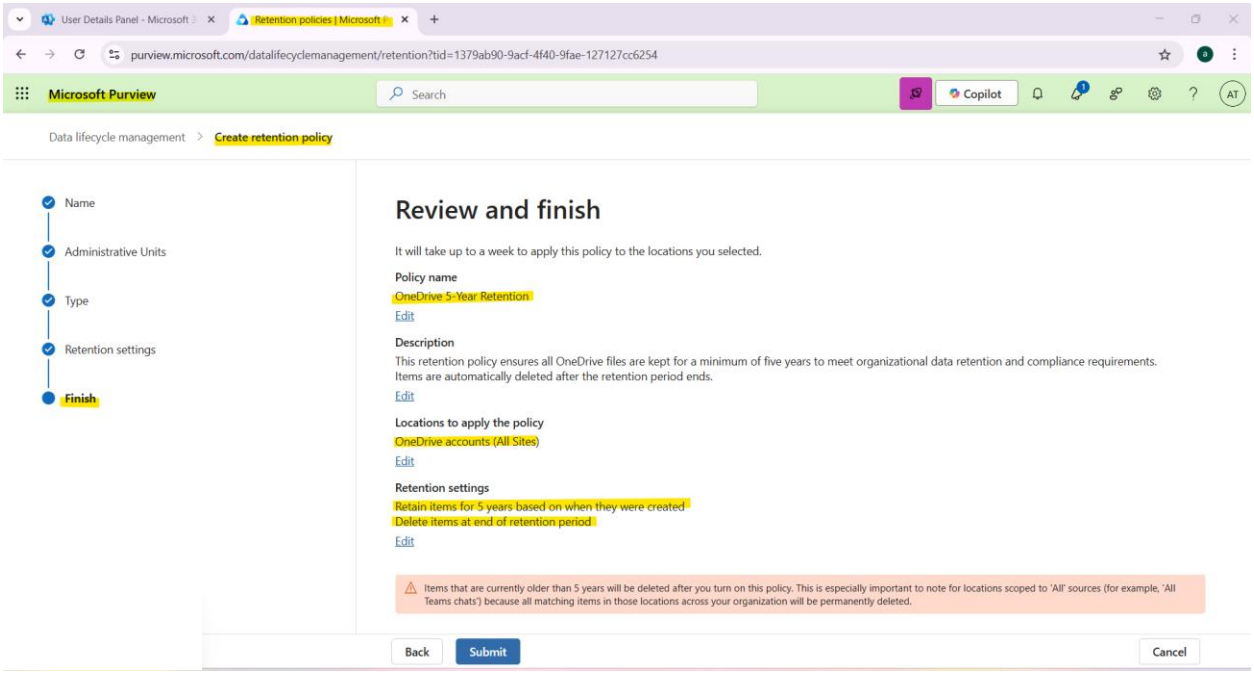
Keep the default number of major version, set who can see draft items as Only users who can approve items, and set No to Require documents to be checked out before they can be edited.



Set Least permissive for No external sharing allowed on OneDrive.

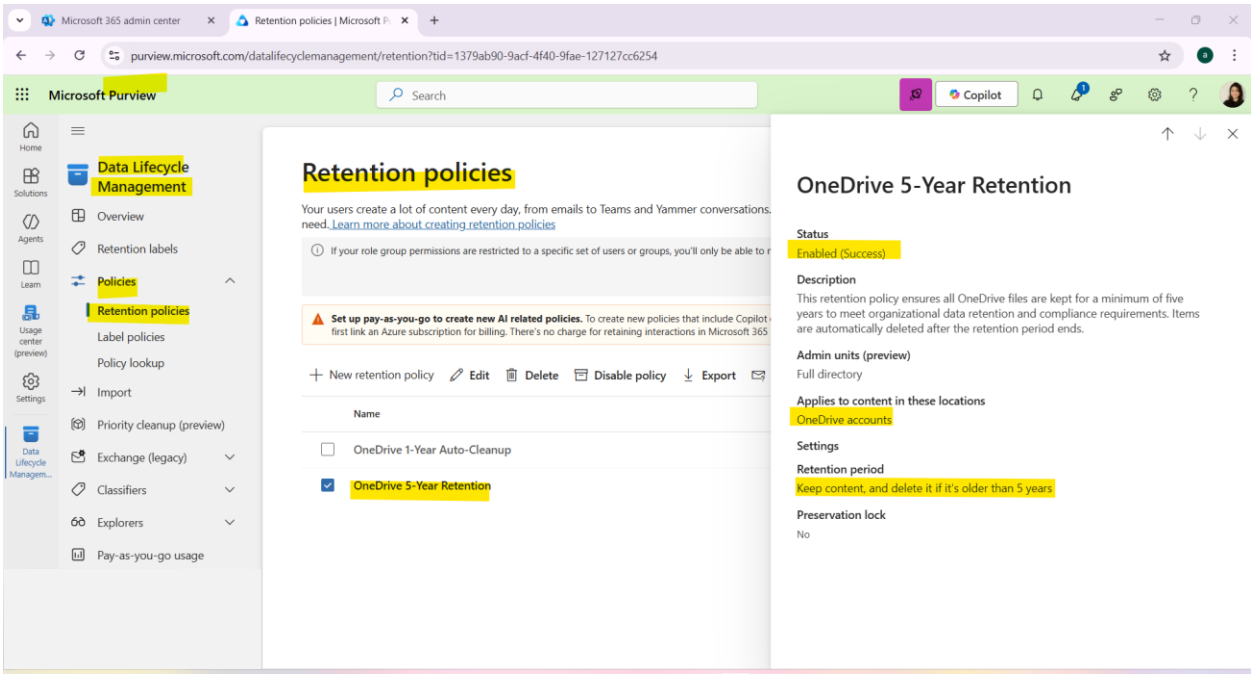
Compliance, Retention, and Information Governance

This section documents compliance and information governance controls, including retention policies and sensitivity labeling, to support regulatory and organizational data management requirements.

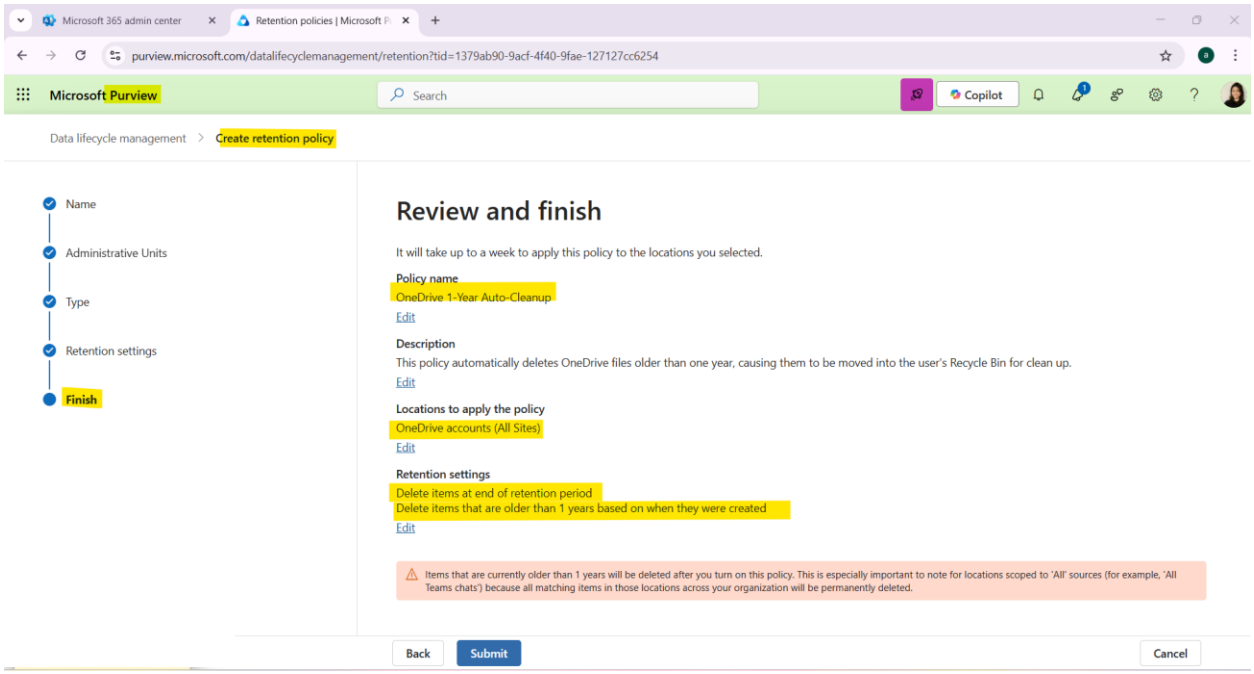


A new retention policy was configured to enforce data lifecycle requirements.

- Locations to apply the policy: OneDrive accounts (All Sites)
- Retention settings: Retain items for 5 years based on when they were created. Delete items at end of retention period.

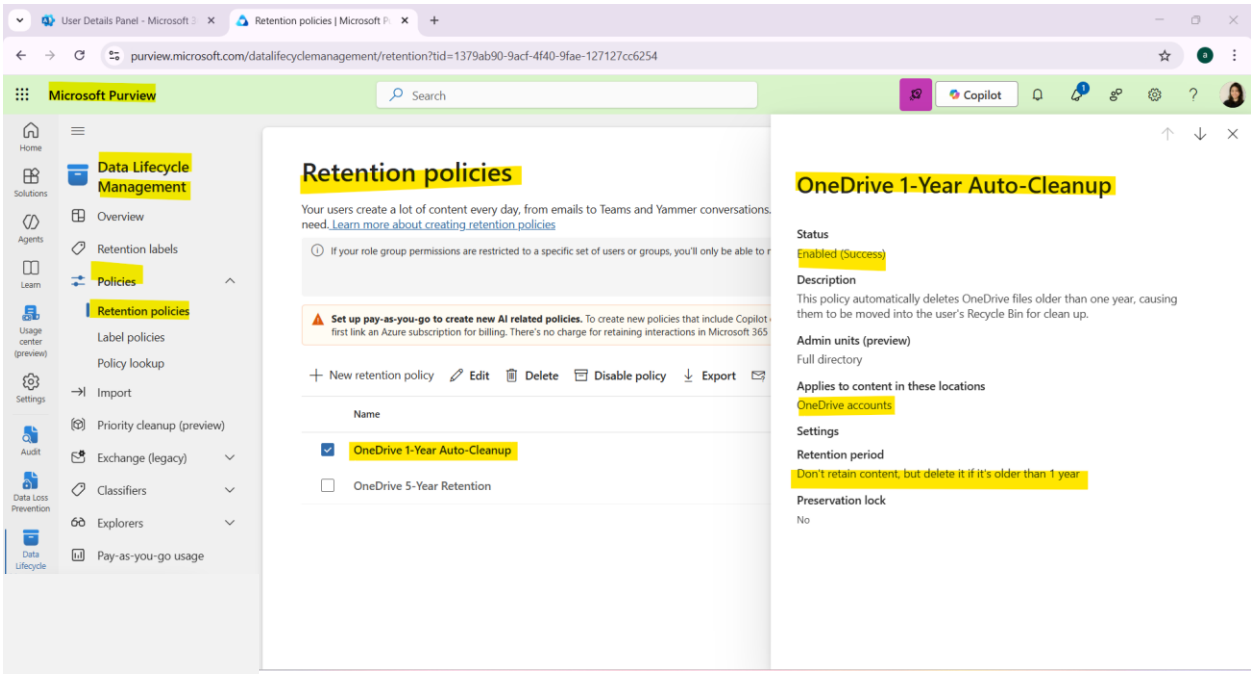


Successful enforcement of the five-year retention policy was confirmed across all OneDrive locations.

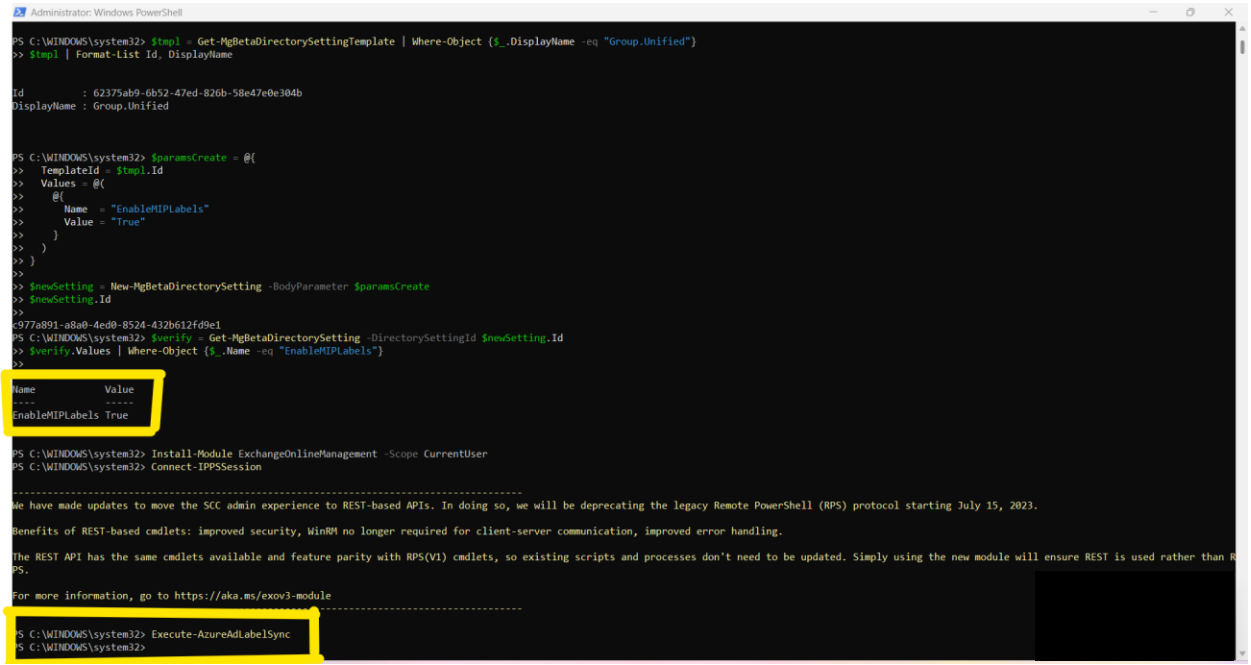


Created New Retention policy.

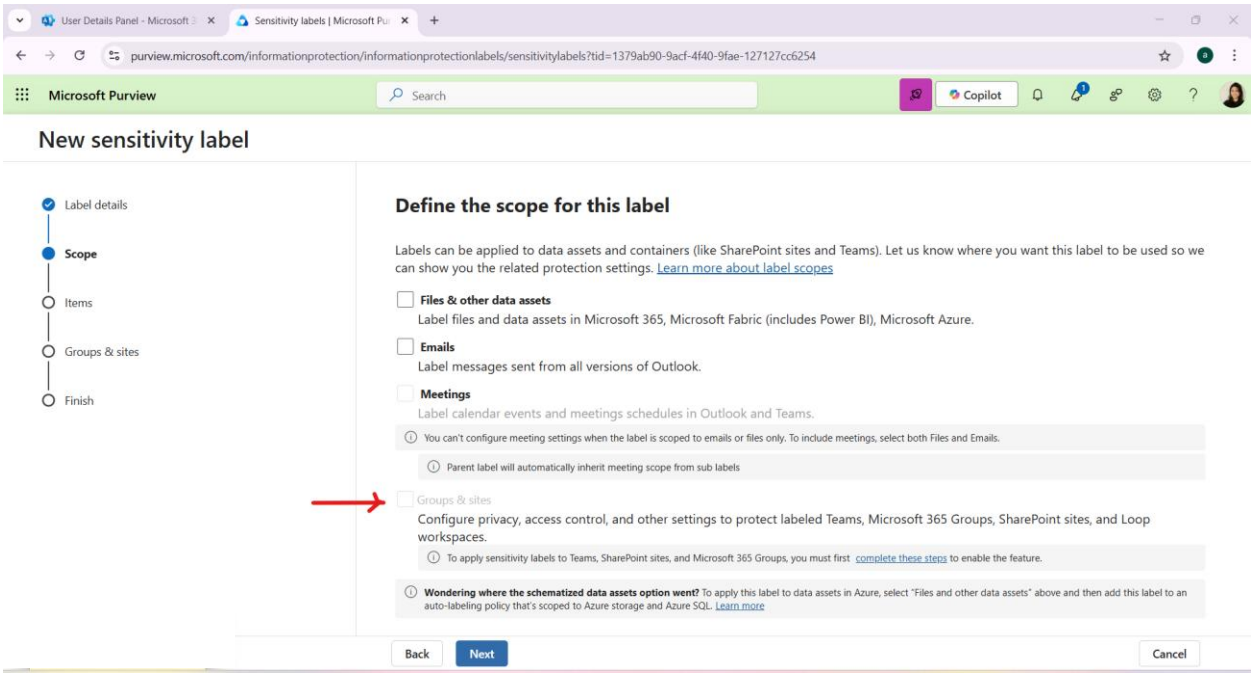
- Locations to apply the policy: OneDrive accounts (All Sites)
- Retention settings: Delete items at end of retention period. Delete items that are older than 1 year based on when they were created.



Successful enforcement of the one-year retention policy was confirmed across all OneDrive locations.



Enable sensitive label option on MS365 groups in Entra ID and sync to Purview by PowerShell.
*Followed the following two links to activate and create sensitive labels on Groups & site level.
Assign sensitivity labels to Microsoft 365 groups in Microsoft Entra ID
Use sensitivity labels to protect content in Microsoft Teams, Microsoft 365 groups, and SharePoint sites



A sensitivity label named “Internal Communications Only” was planned to restrict Viva Engage–related Microsoft 365 Groups to internal users only.

At the time of configuration, the Groups & Sites option in Microsoft Purview was grayed out, even after enabling sensitivity label support for Microsoft 365 Groups via PowerShell and waiting several hours for propagation. This behavior is consistent with known synchronization delays between Microsoft Entra ID and Microsoft Purview.

- 🔹 Planned Configuration (once Groups & Sites becomes available)

If the Groups & Sites option were available, the following settings would be configured:

Group & Site Protection

- Enable: Configure privacy and external access settings for groups and sites
- Privacy: Private – only members can access
- External user access: Not allowed
    - Prevents adding guest users to the Microsoft 365 Group
    - Ensures Viva Engage communities remain internal-only
- External sharing (SharePoint): Only people in the organization
- Default sharing link: People in your organization
- Access from unmanaged devices: Block access
- Authentication context (optional): Require MFA

Label Scope

- Scope: All locations
    - Ensures the label is available for Microsoft 365 Groups, SharePoint sites, Teams, and Viva Engage–connected communities

Auto-labeling

- Skipped

- Label Publishing
  - Label name: Internal Communications Only
  - The label would be published to users and applied to the Microsoft 365 Group associated with the Viva Engage community.

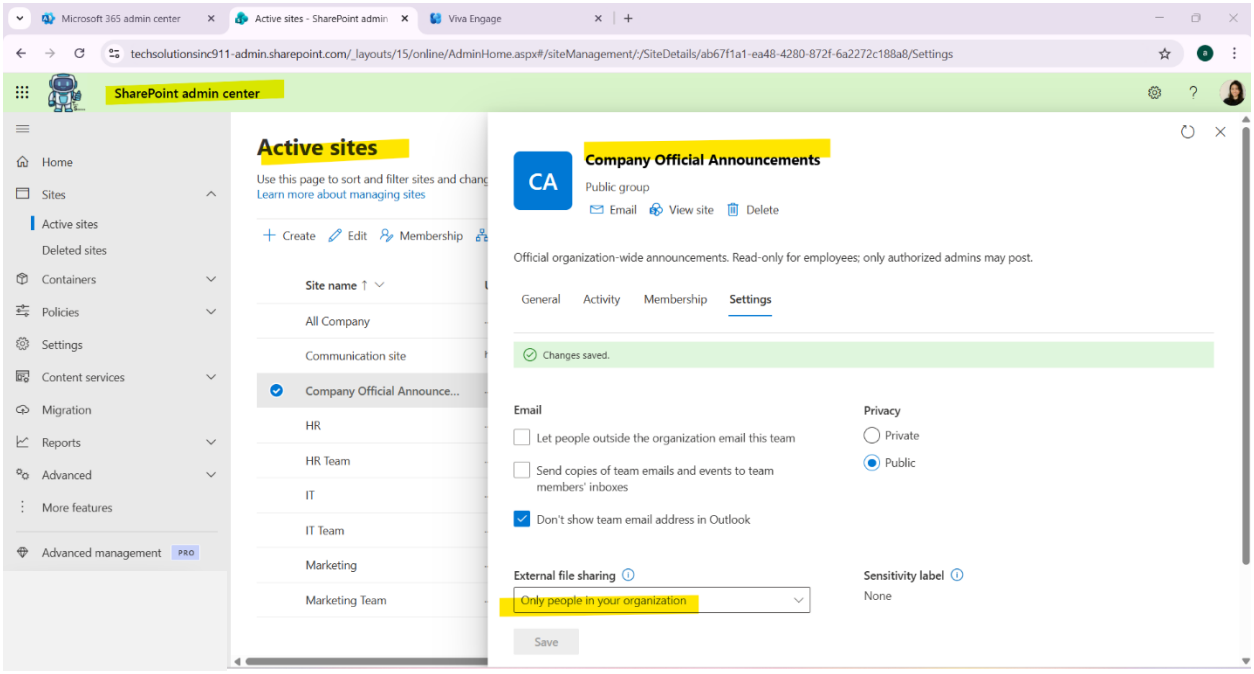
- Outcome (Intended)

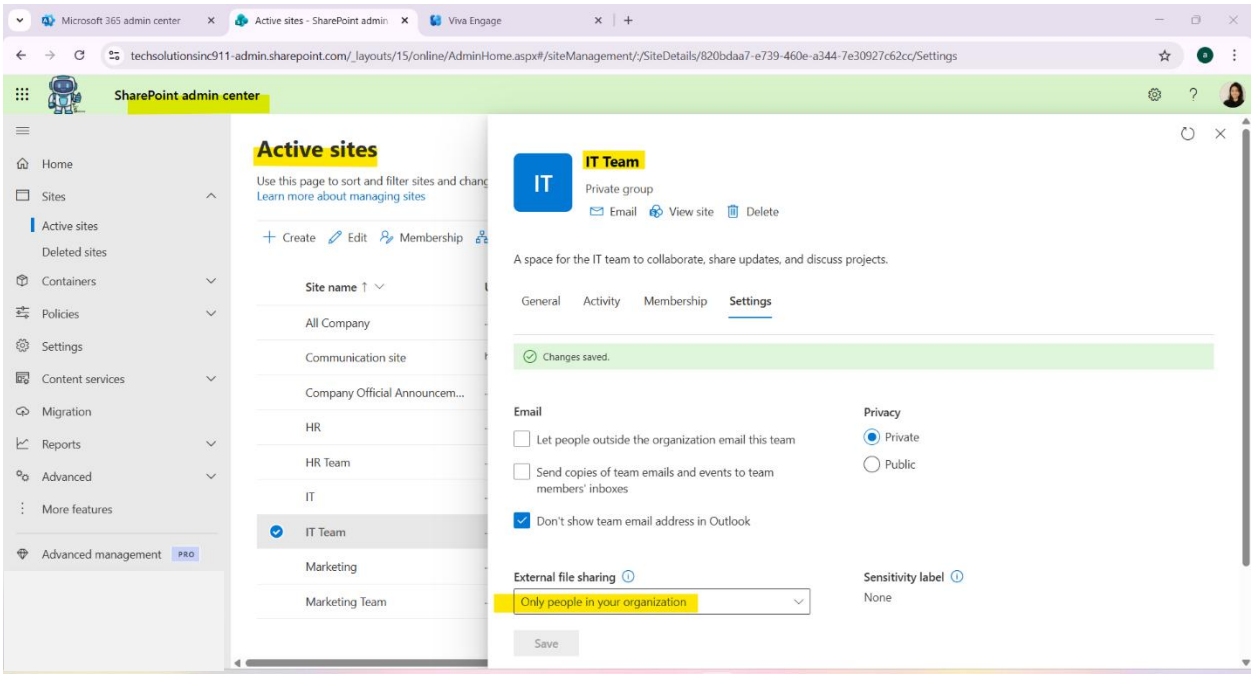
Once applied, the sensitivity label would enforce internal-only communication for Viva Engage by:

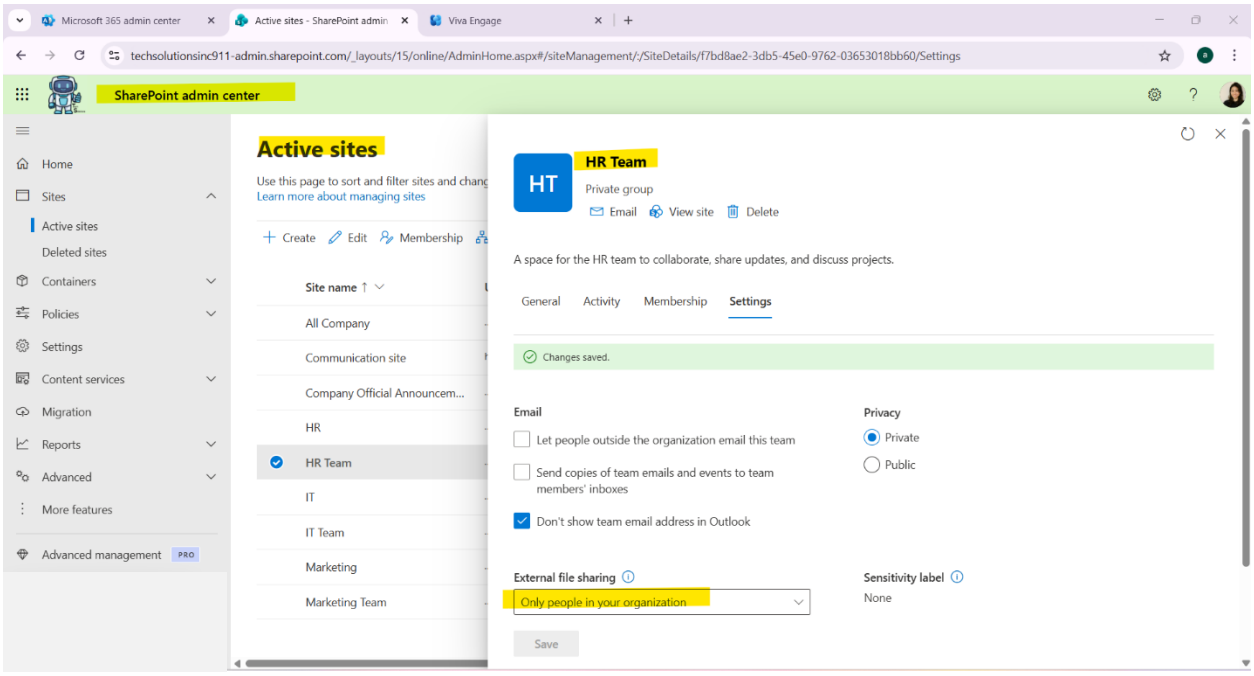
- Blocking external users
- Restricting external sharing
- Ensuring access only from managed and authenticated organizational accounts

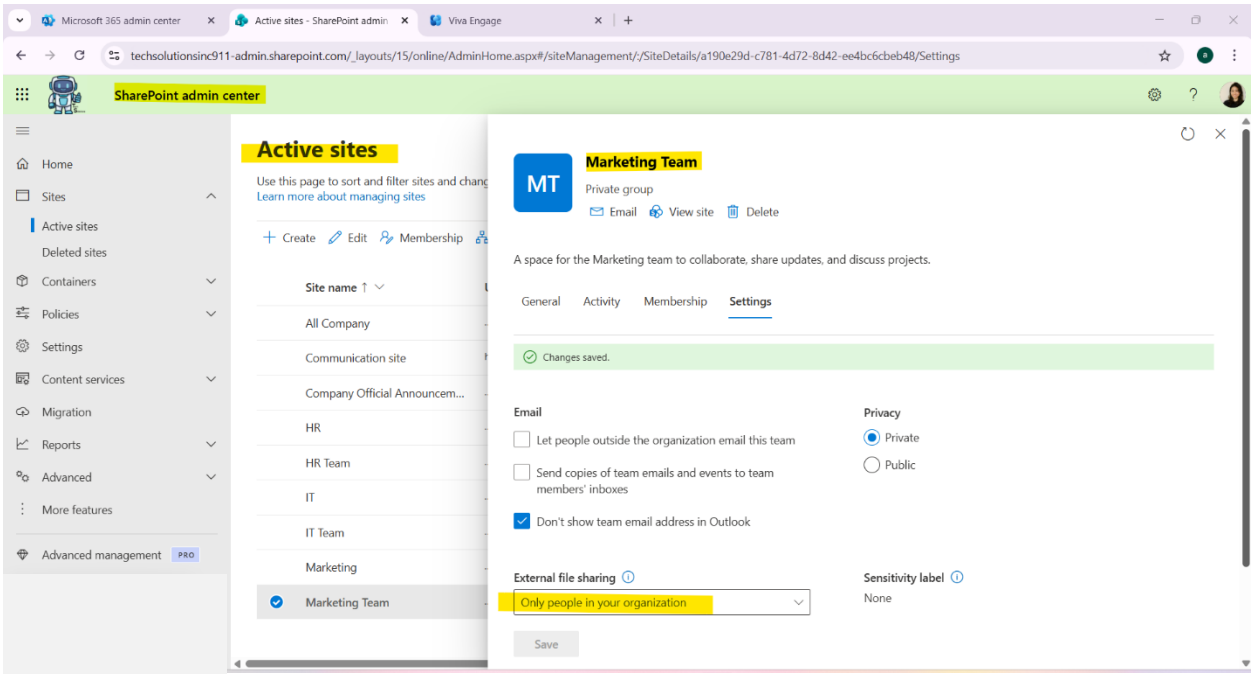
*Also, since there is no more security settings on Viva Engage admin center as well as the sensitive label option hasn't been updated yet, I have configured security setting on Share Point on each MS365 group relating to Viva Engage to allow only the internal file sharing permission.

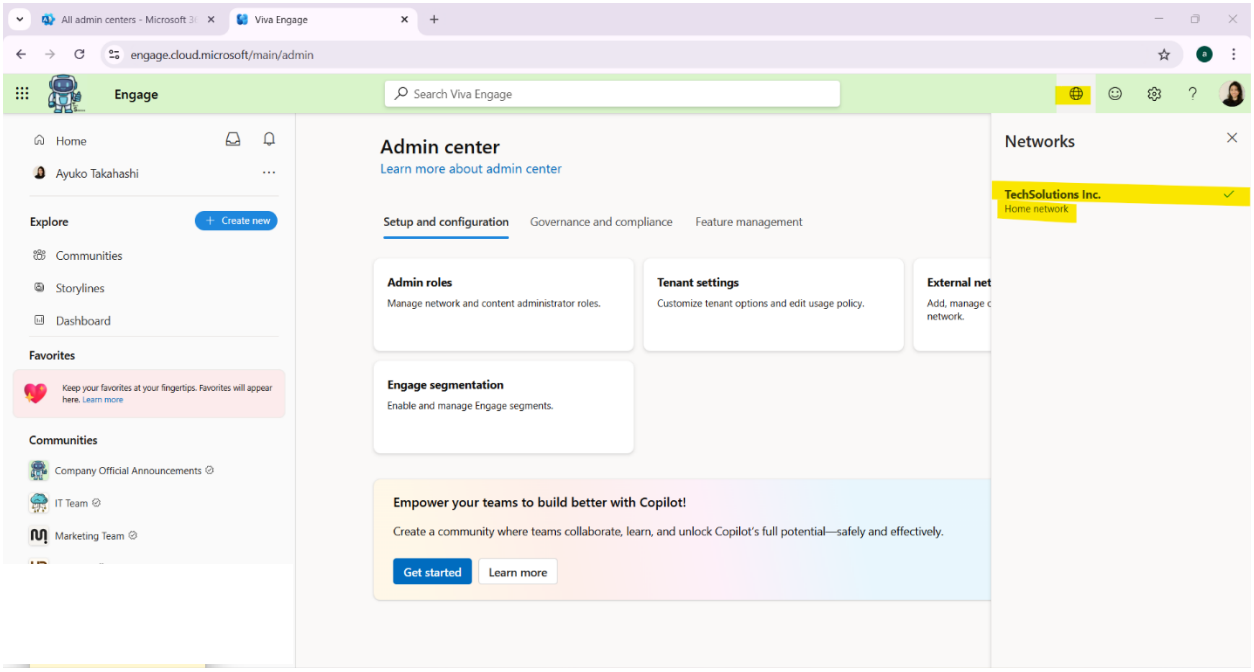
- Company Official Announcements
- IT Team
- HR Team
- Marketing Team



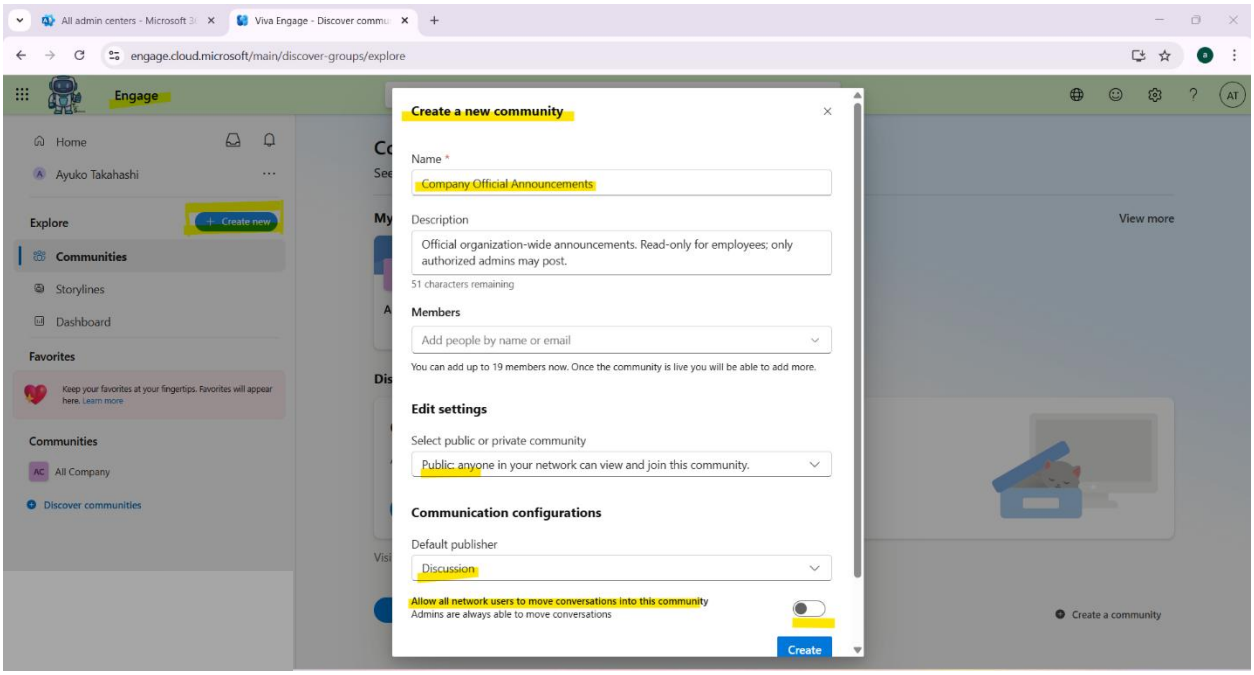

Microsoft 365 admin center
Active sites - SharePoint admin
Viva Engage
techsolutionsinc911-admin.sharepoint.com/_layouts/15/online/AdminHome.aspx#/siteManagement/:/SiteDetails/820bdaa7-e739-460e-a344-7e30927c62cc/Settings
SharePoint admin center
Active sites
Home
Sites
Active sites
Deleted sites
Containers
Policies
Settings
Content services
Migration
Reports
Advanced
More features
Advanced management
PRO
Use this page to sort and filter sites and chang
Learn more about managing sites
Create
Edit
Membership
Site name
All Company
Communication site
Company Official Announcem...
HR
HR Team
IT
IT Team
Marketing
Marketing Team
IT
IT Team
Private group
Email
View site
Delete
A space for the IT team to collaborate, share updates, and discuss projects.
General
Activity
Membership
Settings
Changes saved.
Email
Let people outside the organization email this team
Send copies of team emails and events to team members' inboxes
Don't show team email address in Outlook
Privacy
Private
Public
External file sharing
Only people in your organization
Sensitivity label
None
Save


Microsoft 365 admin center
Active sites - SharePoint admin
Viva Engage
techsolutionsinc911-admin.sharepoint.com/_layouts/15/online/AdminHome.aspx#/siteManagement/:/SiteDetails/f7bd8ae2-3db5-45e0-9762-03653018bb60/Settings
SharePoint admin center
Active sites
Home
Sites
Active sites
Deleted sites
Containers
Policies
Settings
Content services
Migration
Reports
Advanced
More features
Advanced management
PRO
Use this page to sort and filter sites and chang
Learn more about managing sites
Create
Edit
Membership
Site name
All Company
Communication site
Company Official Announcem...
HR
HR Team
IT
IT Team
Marketing
Marketing Team
HT
HR Team
Private group
Email
View site
Delete
A space for the HR team to collaborate, share updates, and discuss projects.
General
Activity
Membership
Settings
Changes saved.
Email
Let people outside the organization email this team
Send copies of team emails and events to team members' inboxes
Don't show team email address in Outlook
Privacy
Private
Public
External file sharing
Only people in your organization
Sensitivity label
None
Save





Just to make sure the Network on Viva Engage is set to only internal.

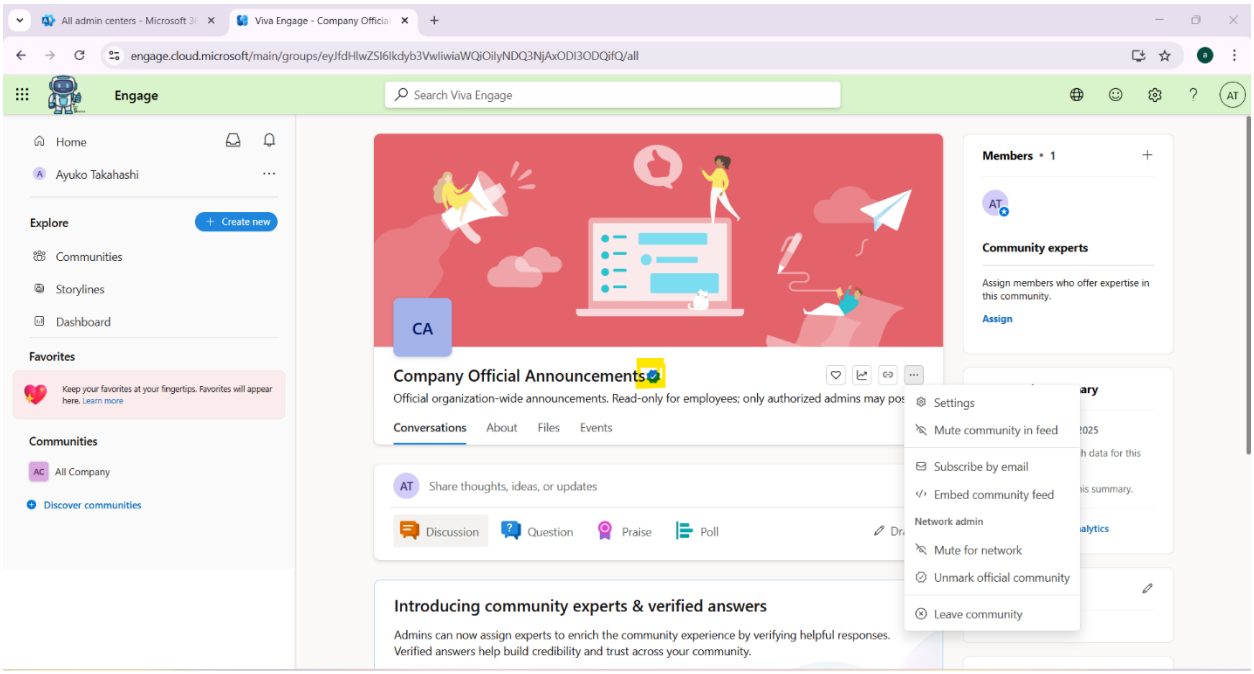


Created Company Announcements community. Set Public and Turn-off for allowing users to move conversations into this community to keep the community clean and announcement-focused.

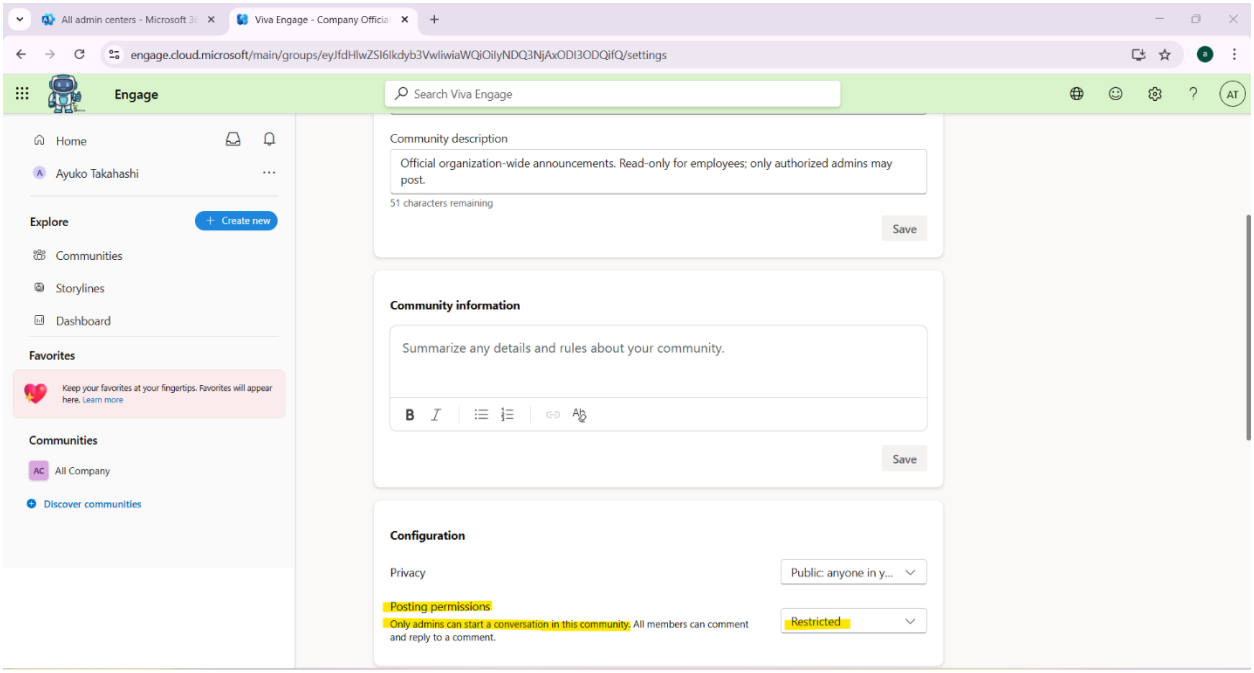
*All Company default community group on the communities pane has been deleted on MS admin center since no option on this default group to modify the following section.

Edit settings: Public: Anyone in your network can view and join this community.

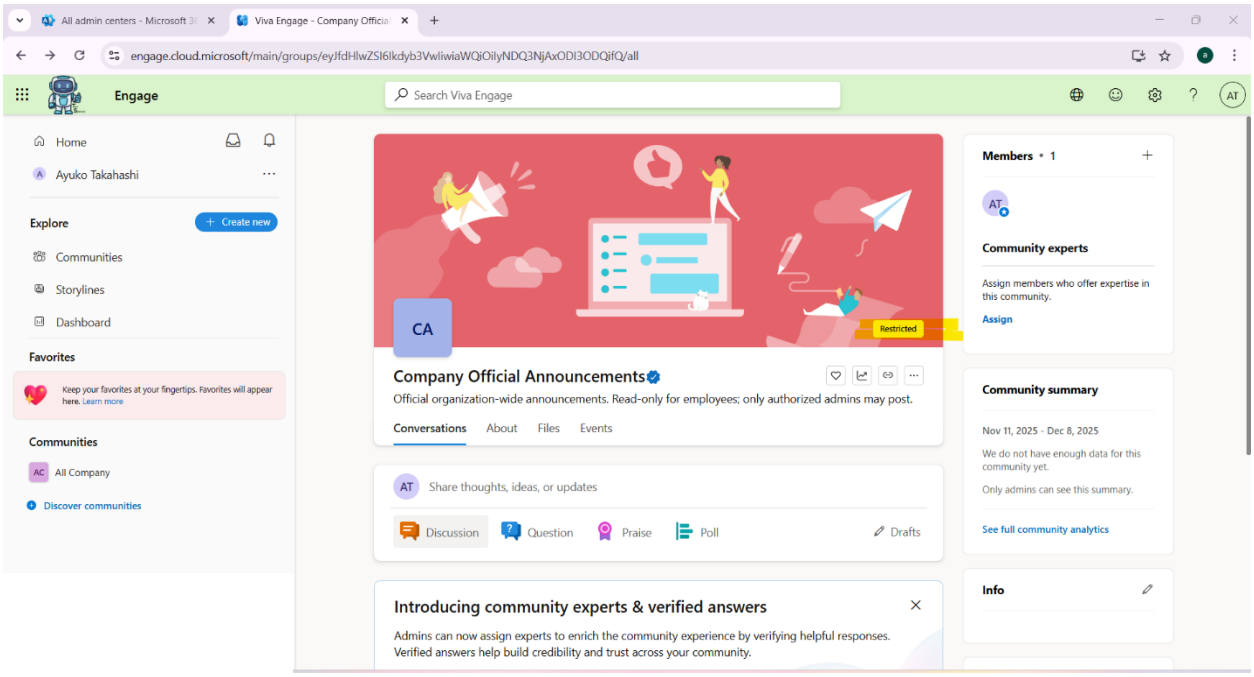
And it will take effect in 24 hours.



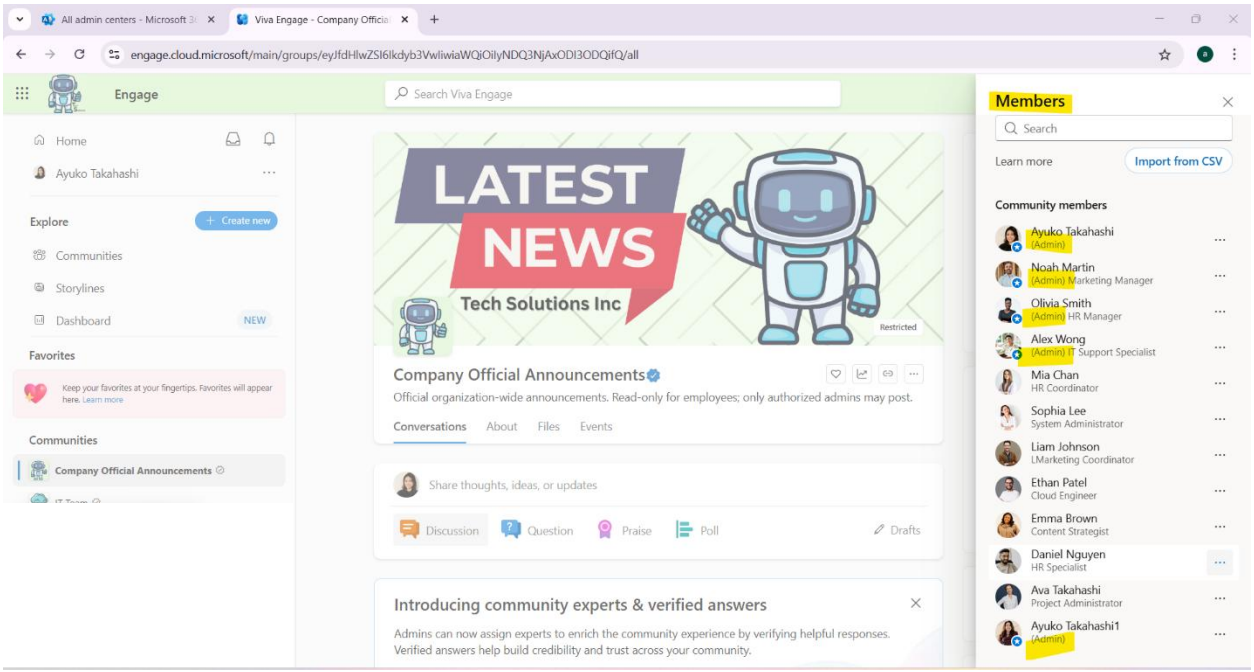
Added official community symbol, and Company Announcements community has been created.



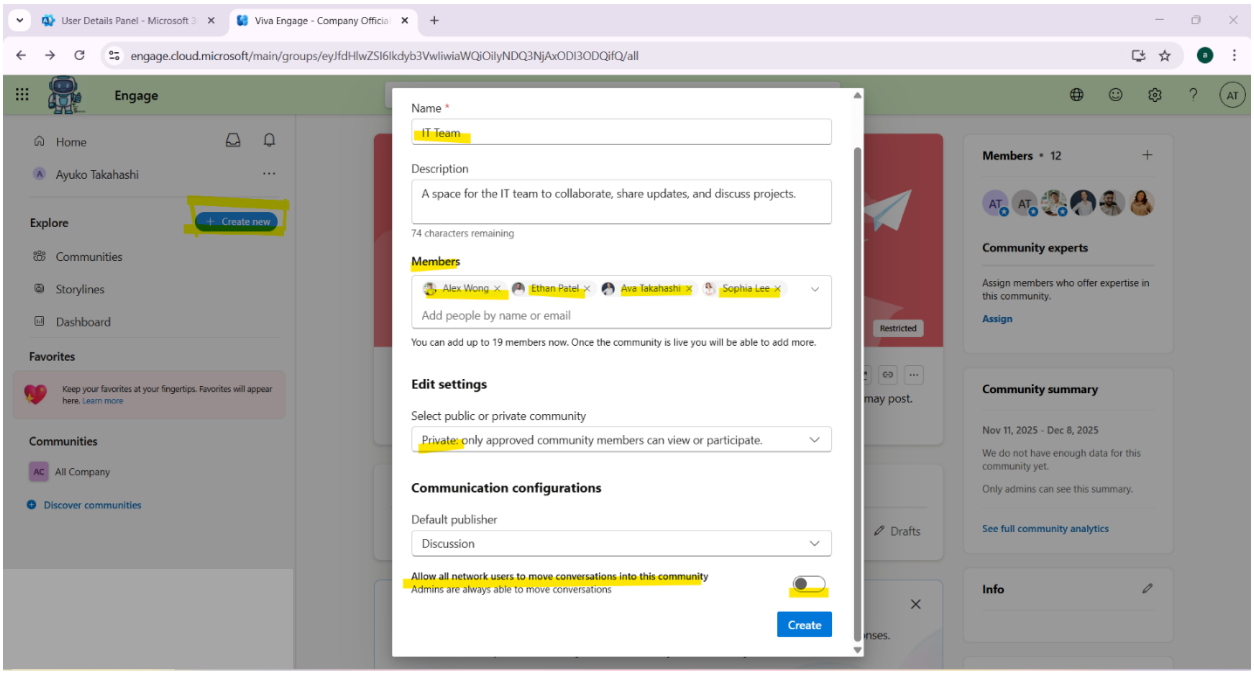
Open community settings and set Restricted on Posting permissions so that only admin can start a conversation in this community.



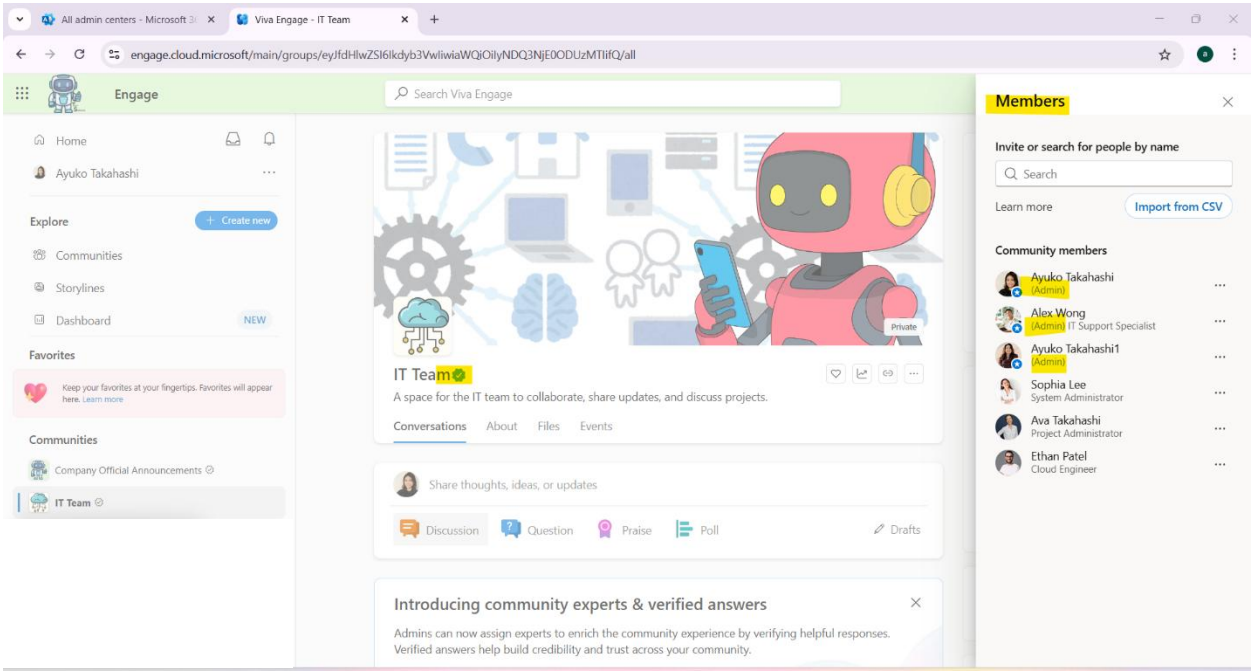
The Restricted icon have appeared on the main display an updated photos.



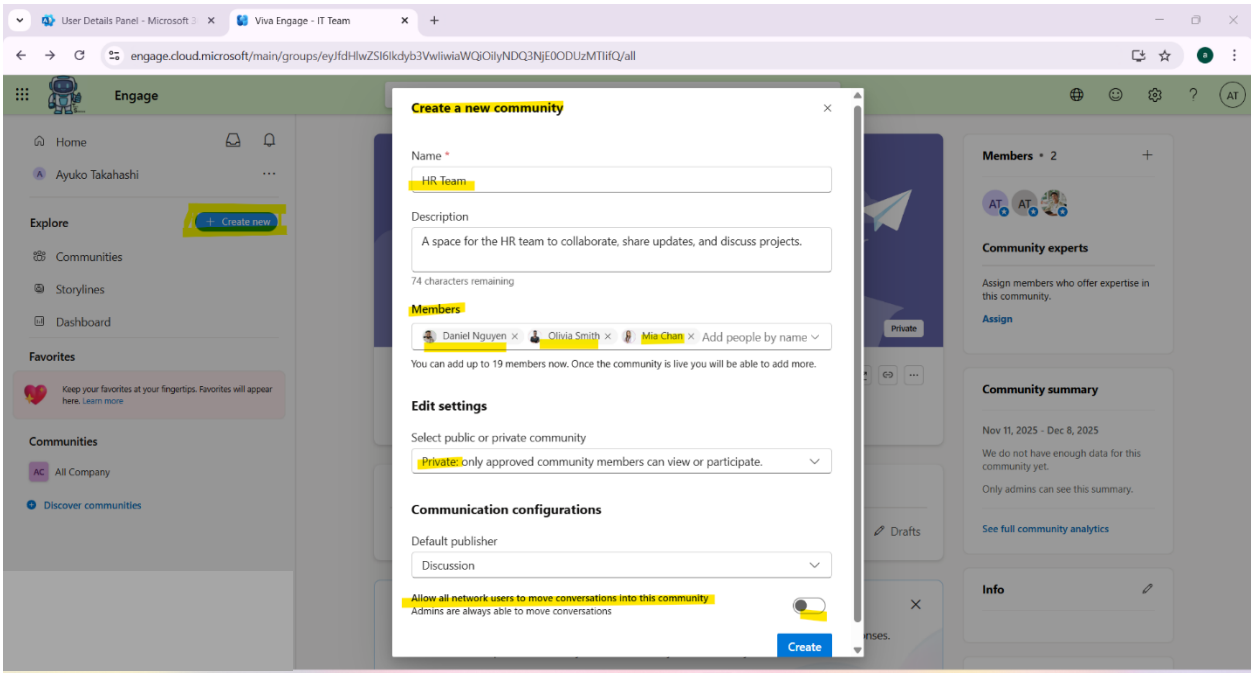
Updated main photos of the site and set global admins and leadership positions (IT Specialist, HR Manager and Marketing Manager) as admins on the company announcement community.



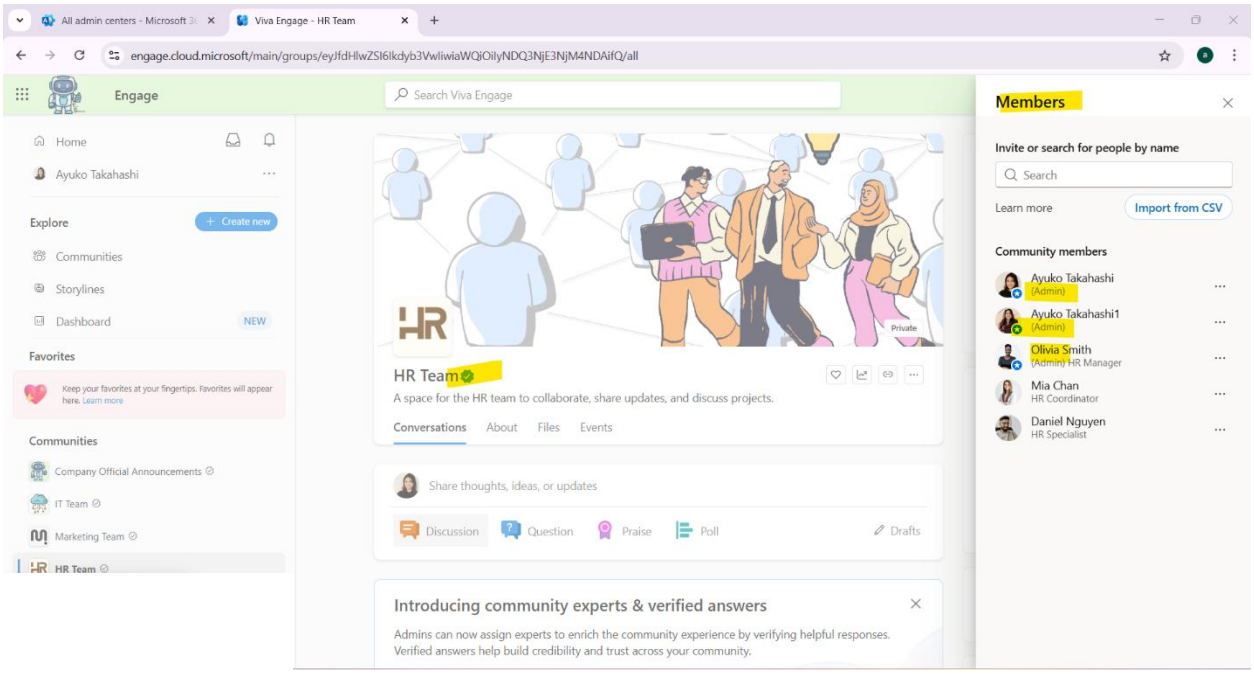
Department-Specific Discussion Groups for IT Team. Add IT members, set as Private and toggled off for not allowing all network users to move conversations into this community.



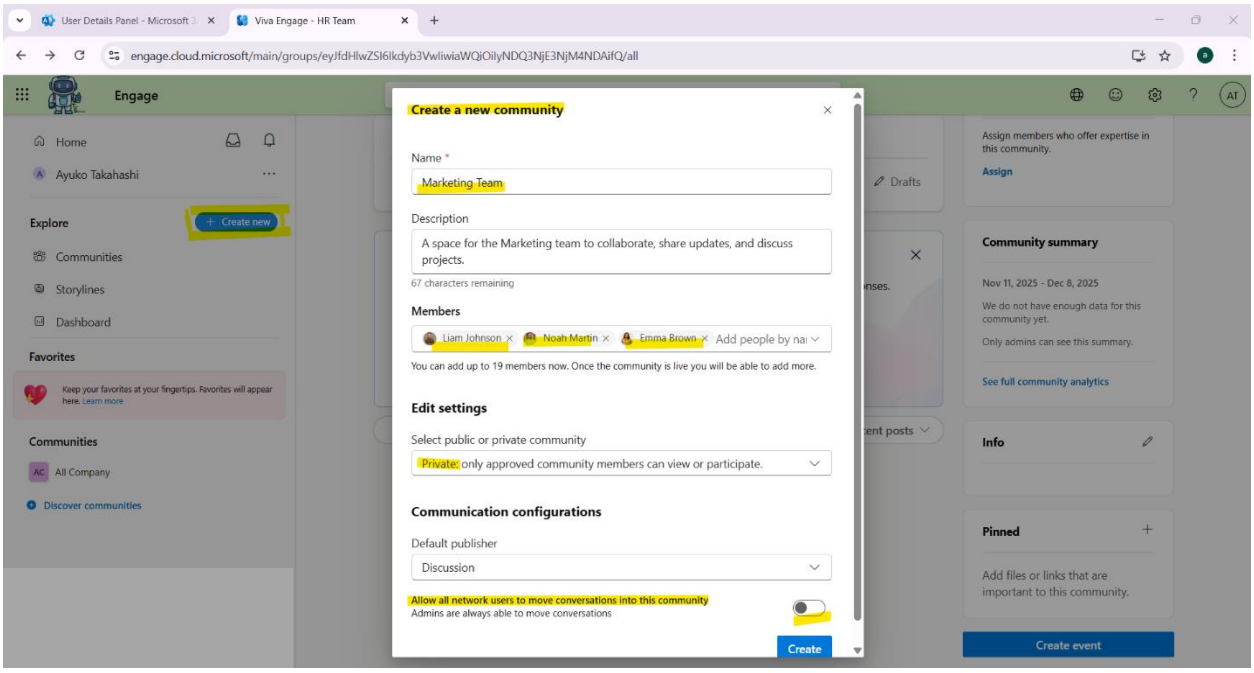
Updated photos, Official badge, and set Global admins and IT specialist as admin on this community.



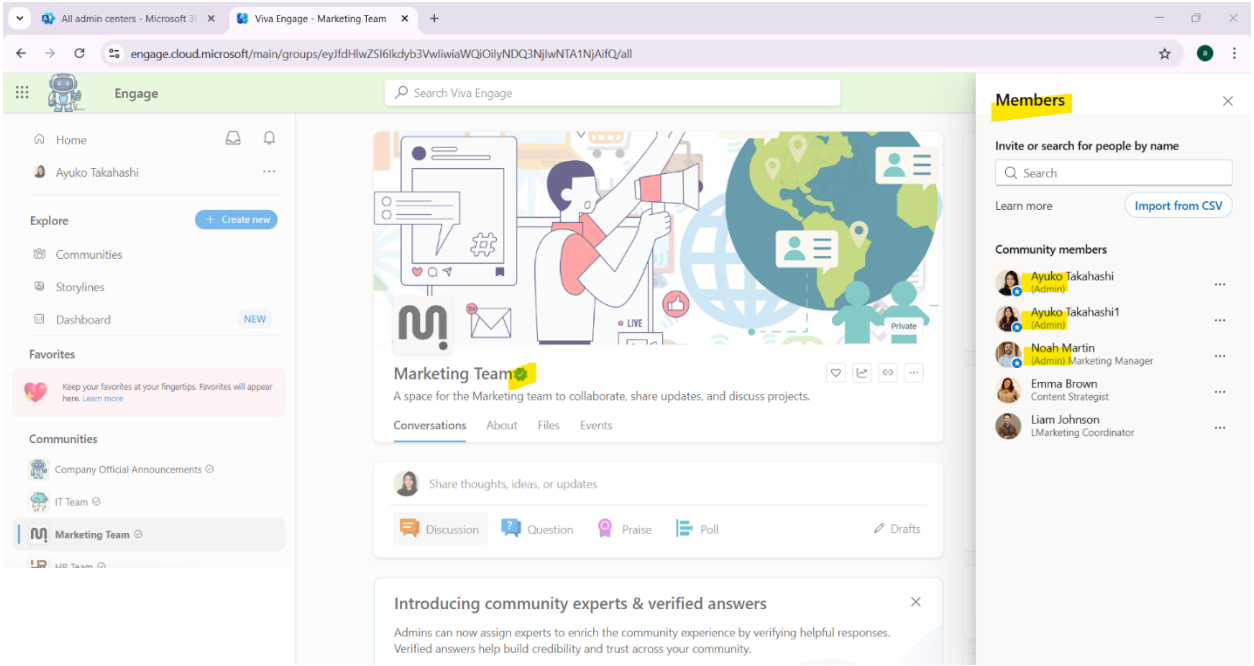
Department-Specific Discussion Groups for HR Team. Add HR members, set as Private and toggled off for not allowing all network users to move conversations into this community.



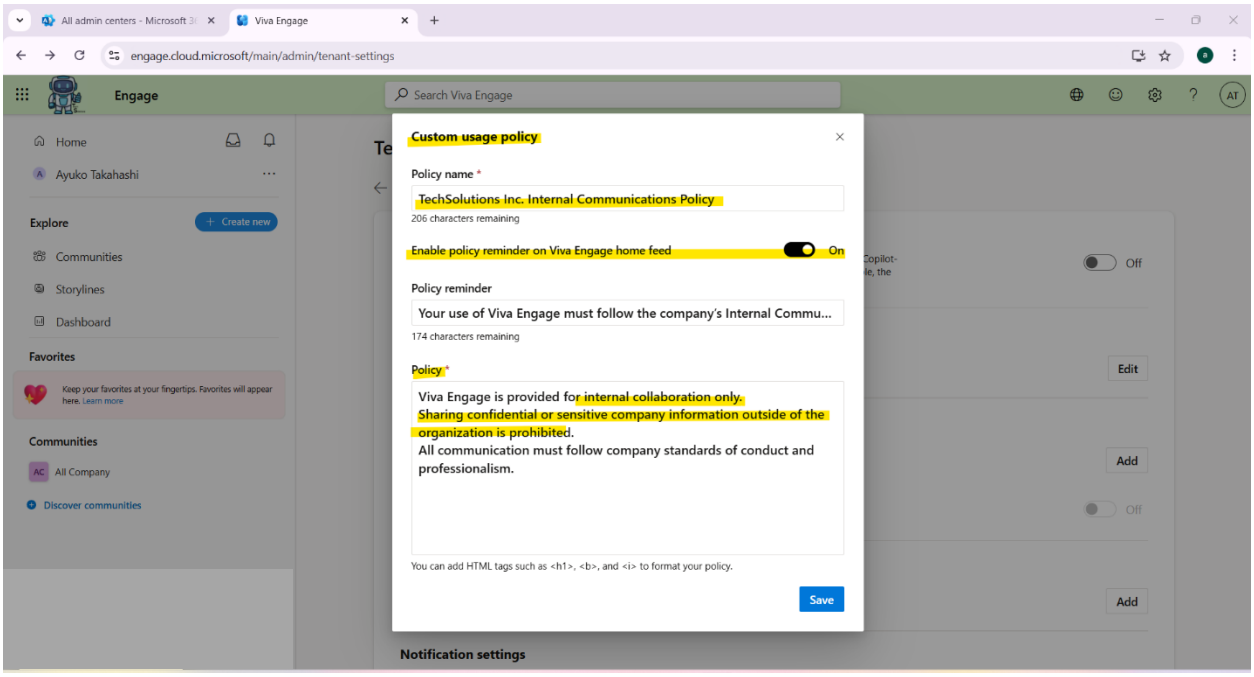
Updated photos, Official badge, and set Global admins and HR manager as admin on this community.



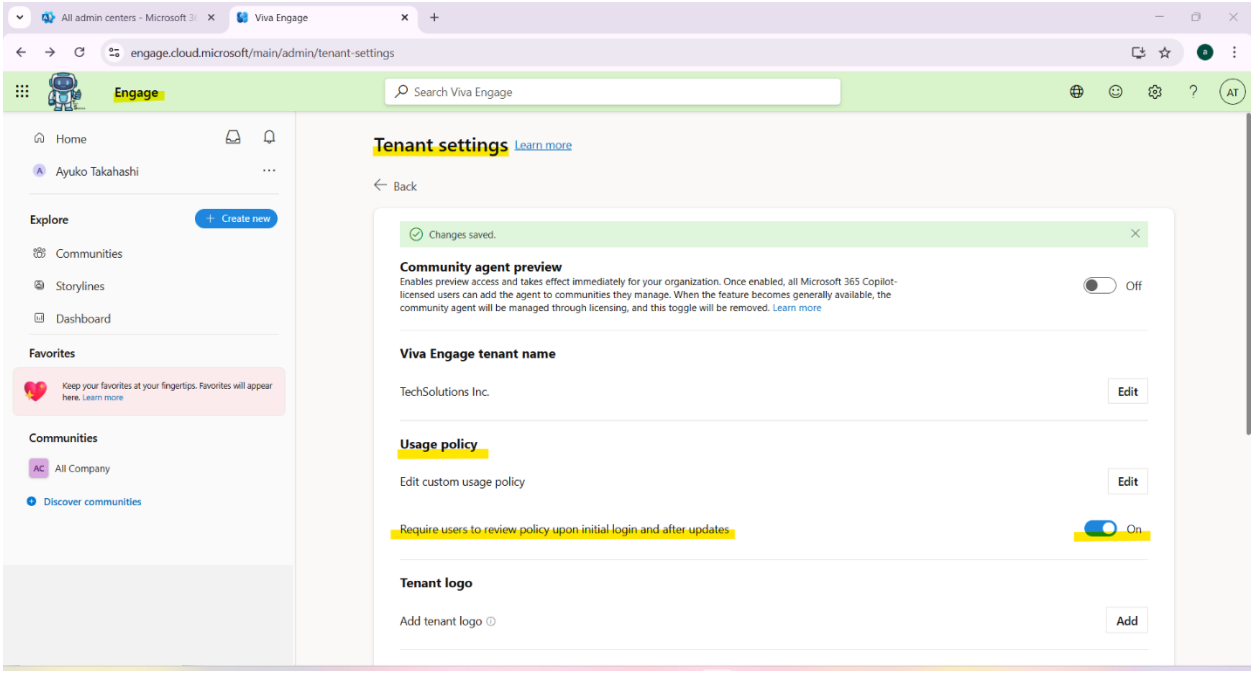
Department-Specific Discussion Groups for Marketing Team. Add Marketing members, set as Private and toggled off for not allowing all network users to move conversations into this community.



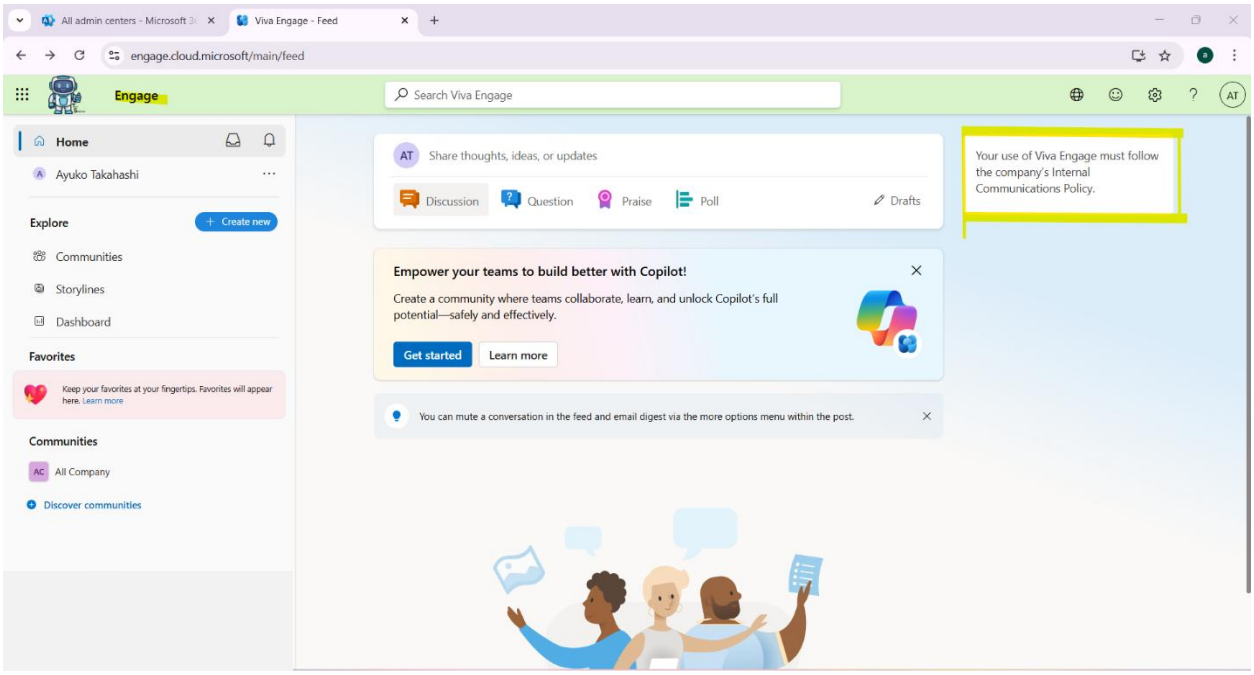
Updated photos, Official badge, and set Global admins and Marketing manager as admin on the community.



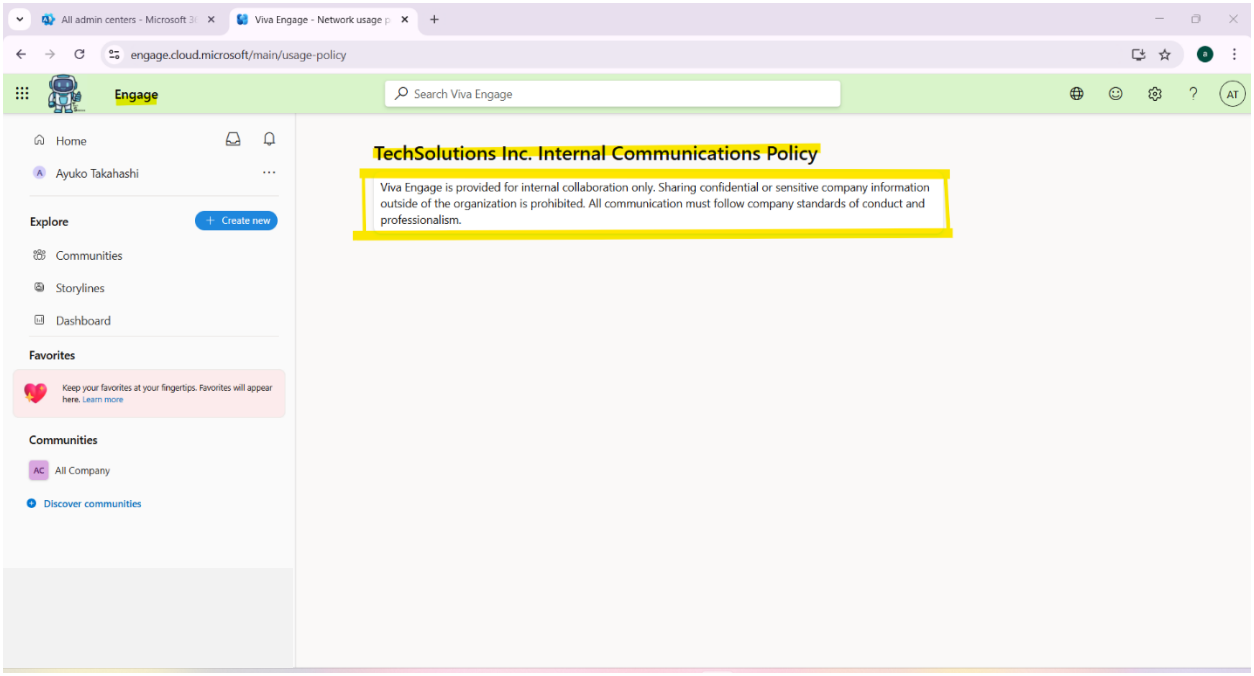
Set Custom usage policy to ensure compliance with the company's social media policy.



Enabled 'Required users to review policy upon initial login and after updates'.



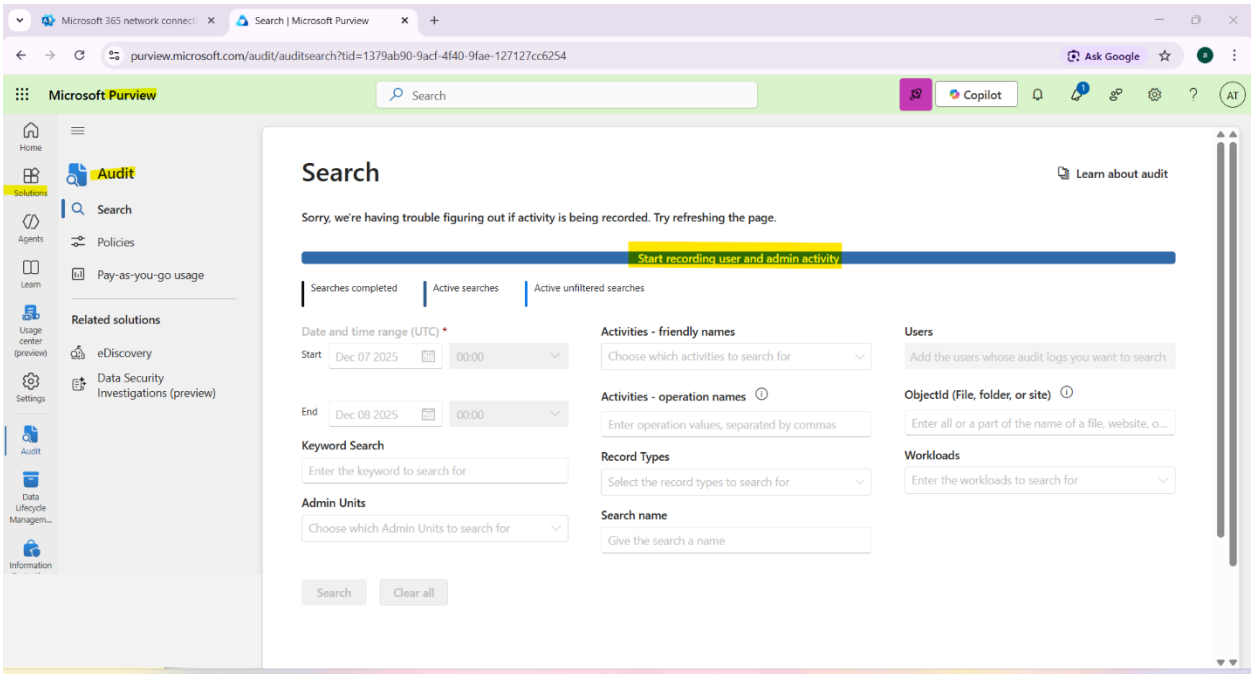
The Viva Engage usage policy was reviewed and confirmed as active for end users.



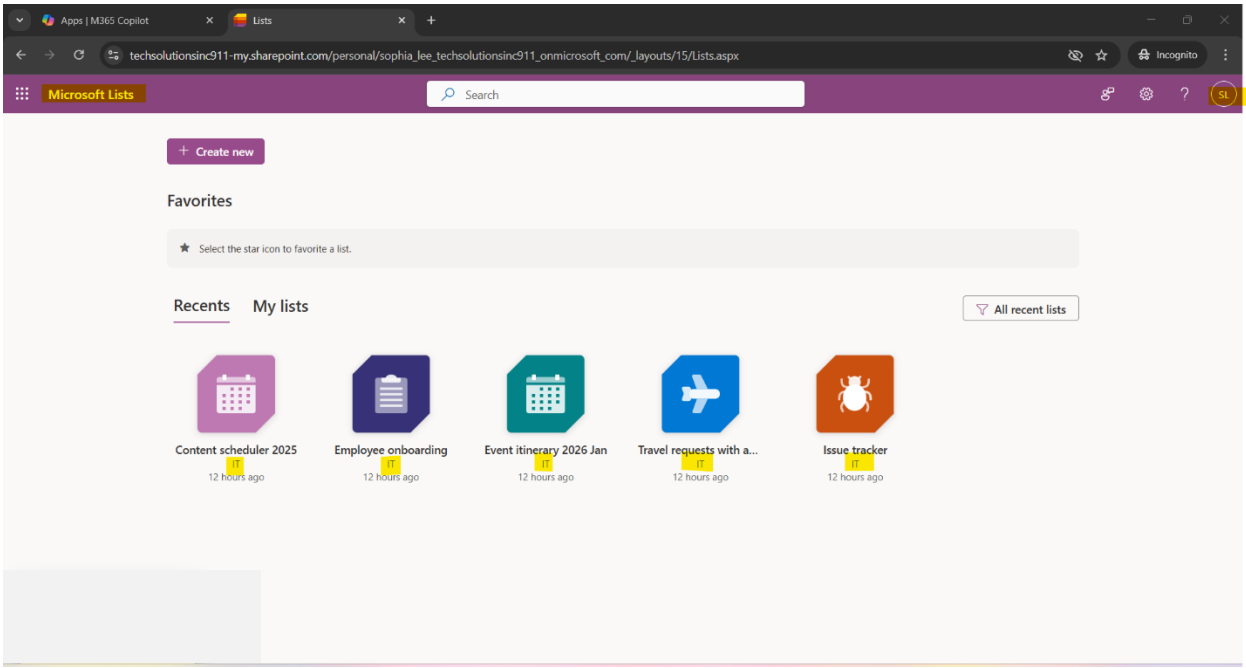
The Viva Engage Social Media Compliance policy was confirmed as active and visible to users.

Monitoring, Audit Logging, and Alerting

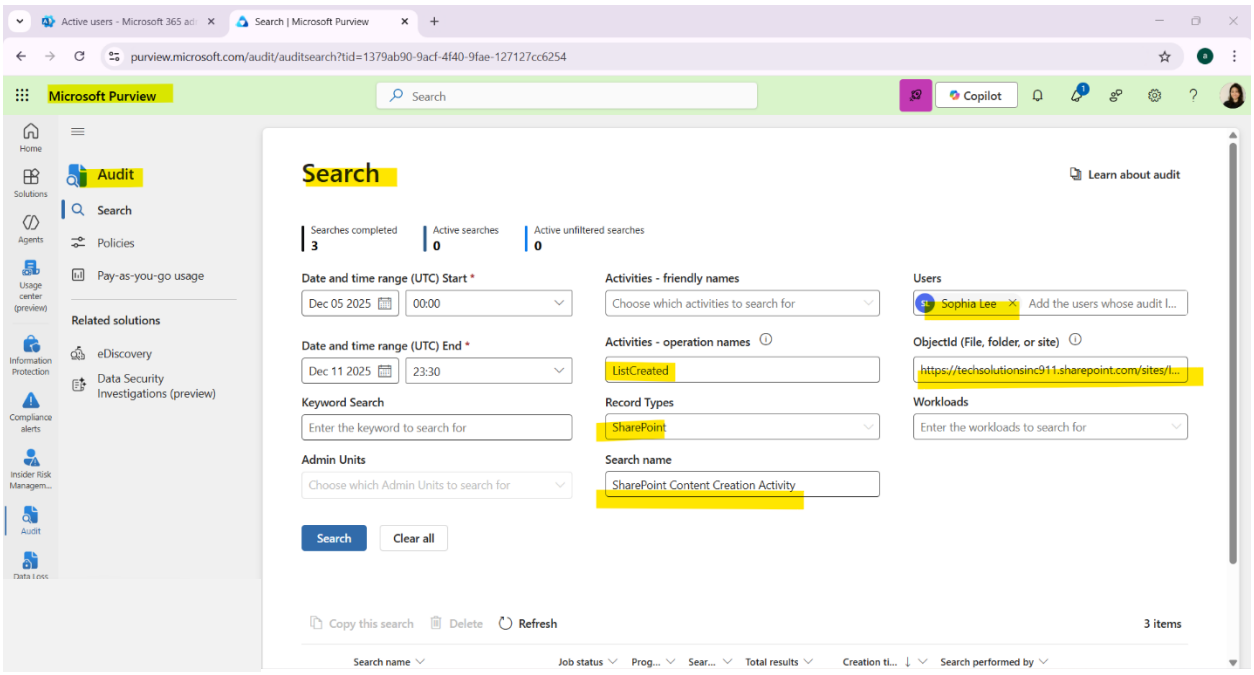
This section demonstrates the configuration of audit logging, alert policies, and usage reporting to provide visibility into user activity and support proactive security monitoring.



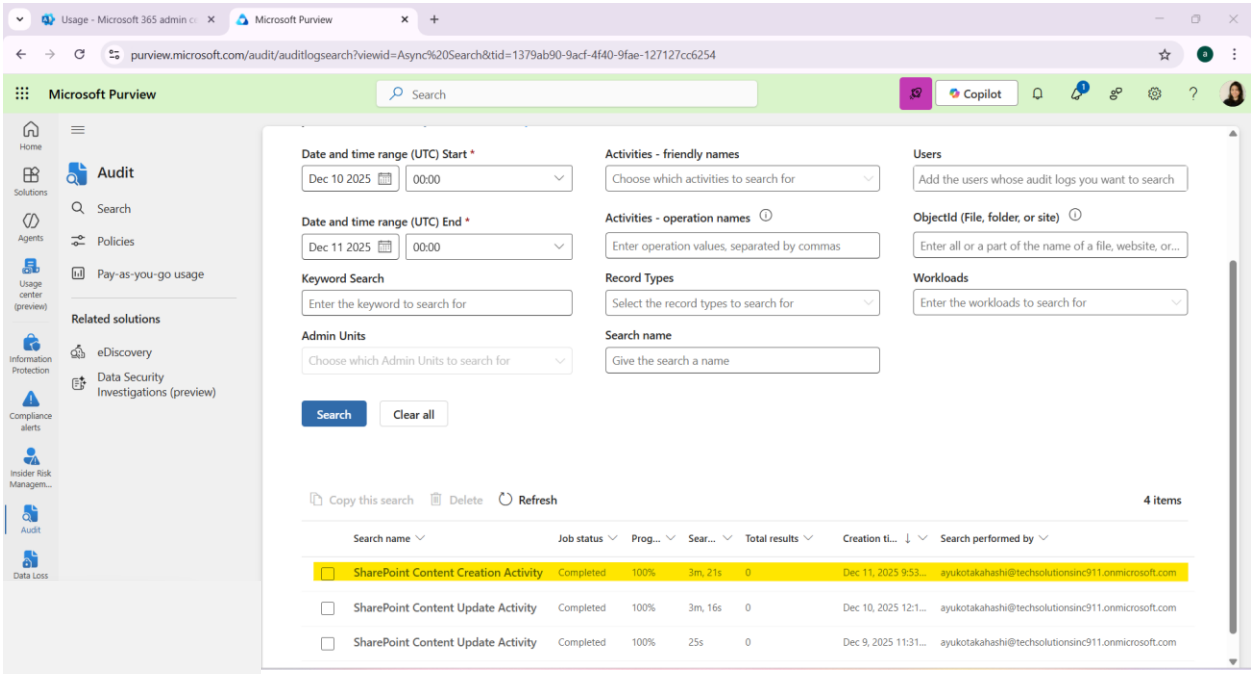
Unified audit logging was enabled to record user and administrative activity across Microsoft 365 services.



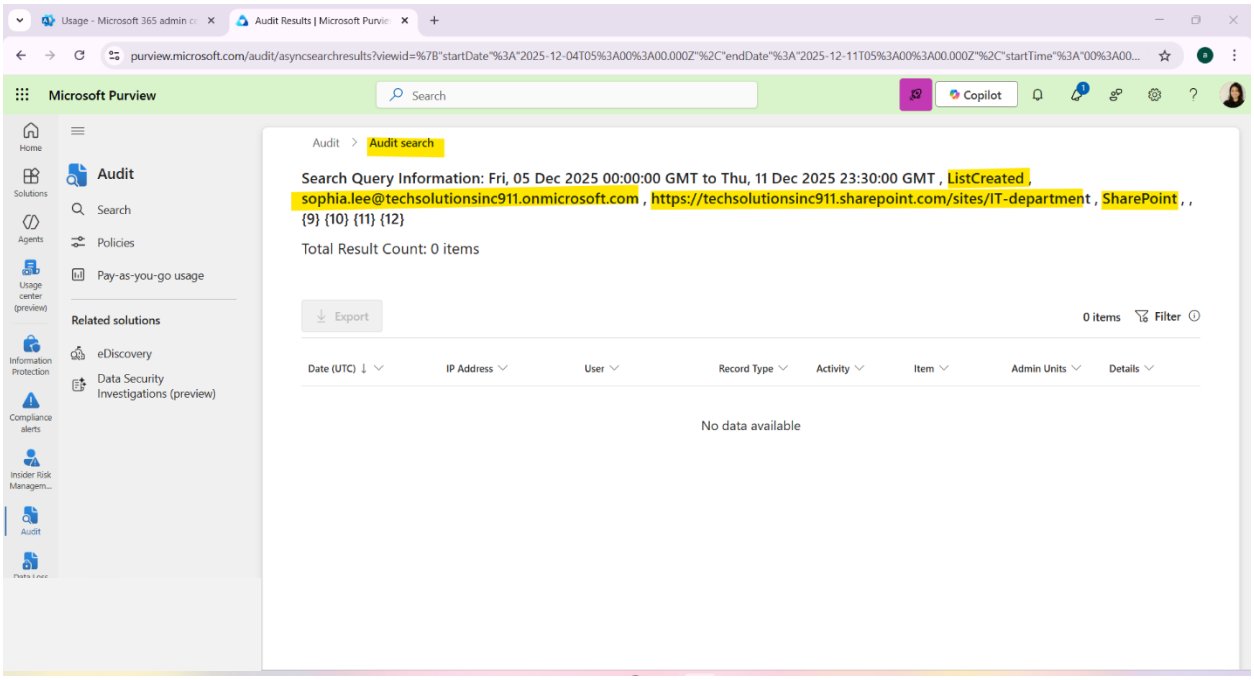
Sophia Lee created Lists on the IT site on SharePoint.



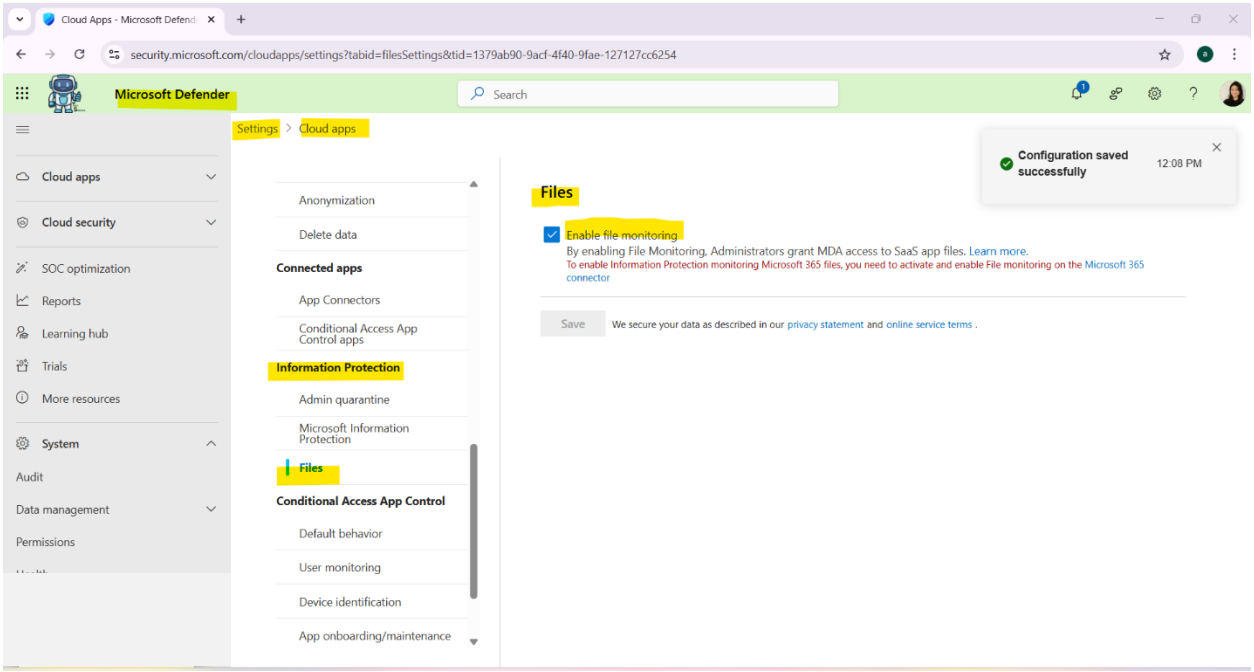
Create a custom audit log search: Sophia Lee, ListCreated, SharePoint, URL: IT site on SharePoint.



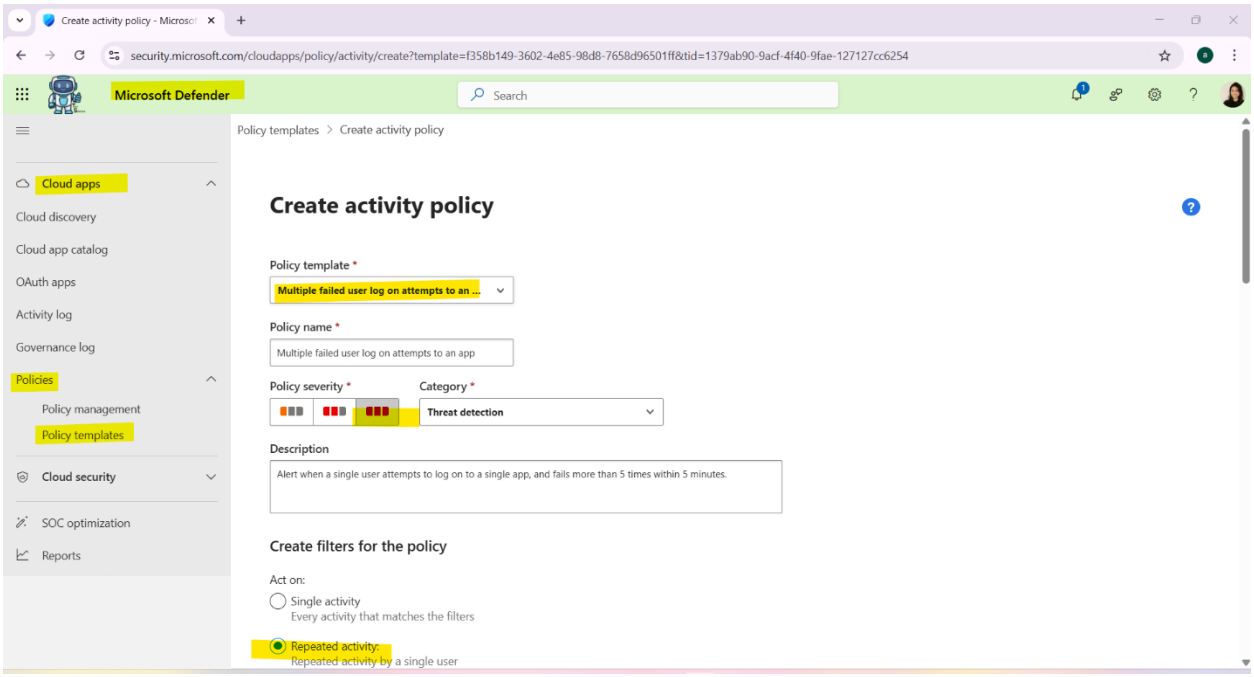
Platform Behavior Note:
Audit log data availability is subject to a standard activation delay of up to seven business days following initial enablement.



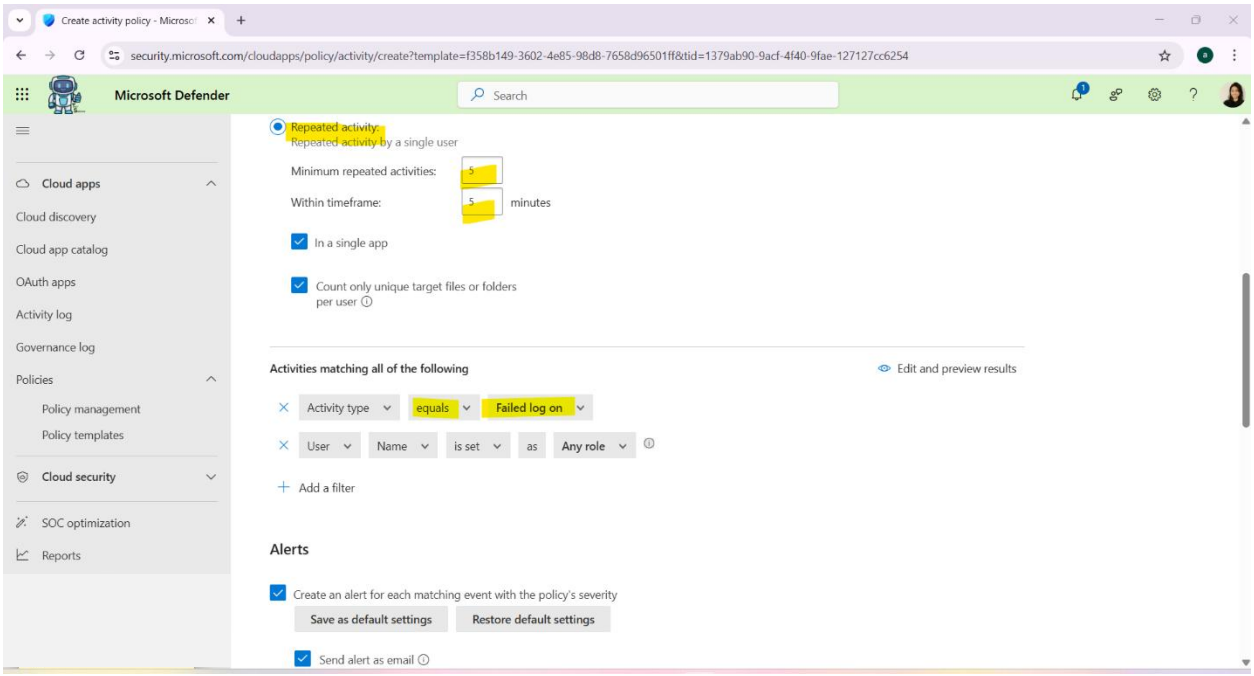
This view is detailed info of the data result page. No data is available yet.



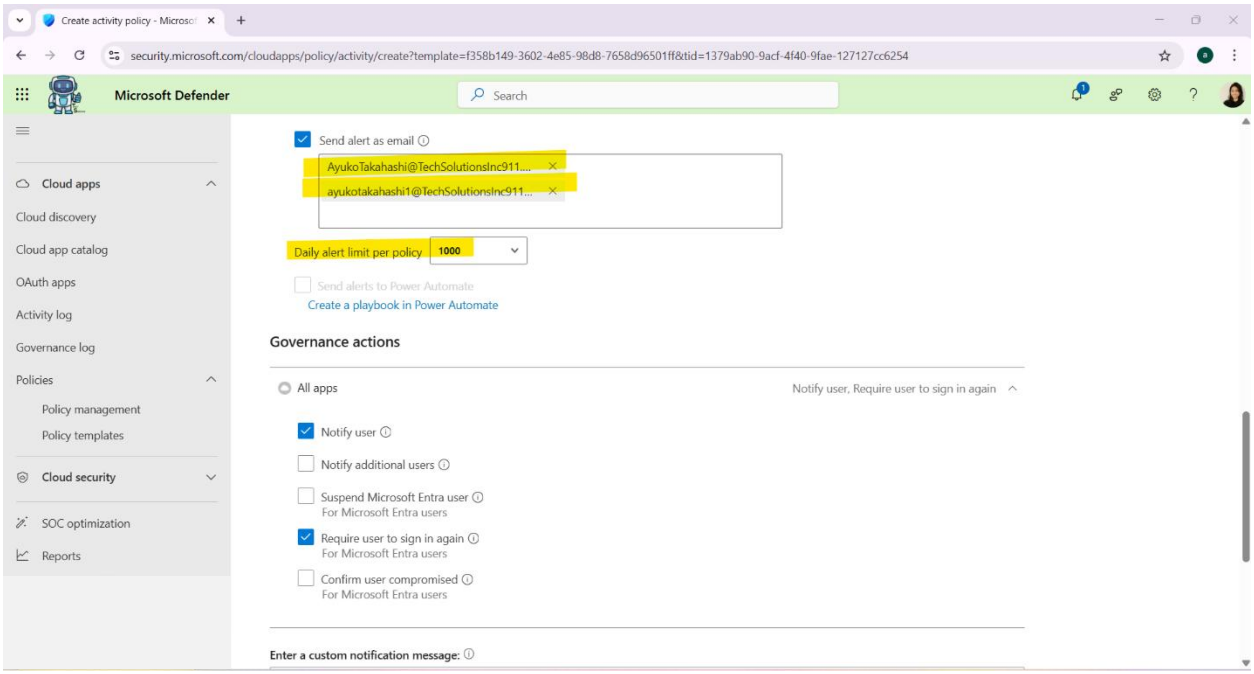
Enabled file monitoring to gain visibility into files stored in SaaS apps.
App Connectors and Cloud Discovery were not configured, as the environment scope was limited to native Microsoft 365 services.



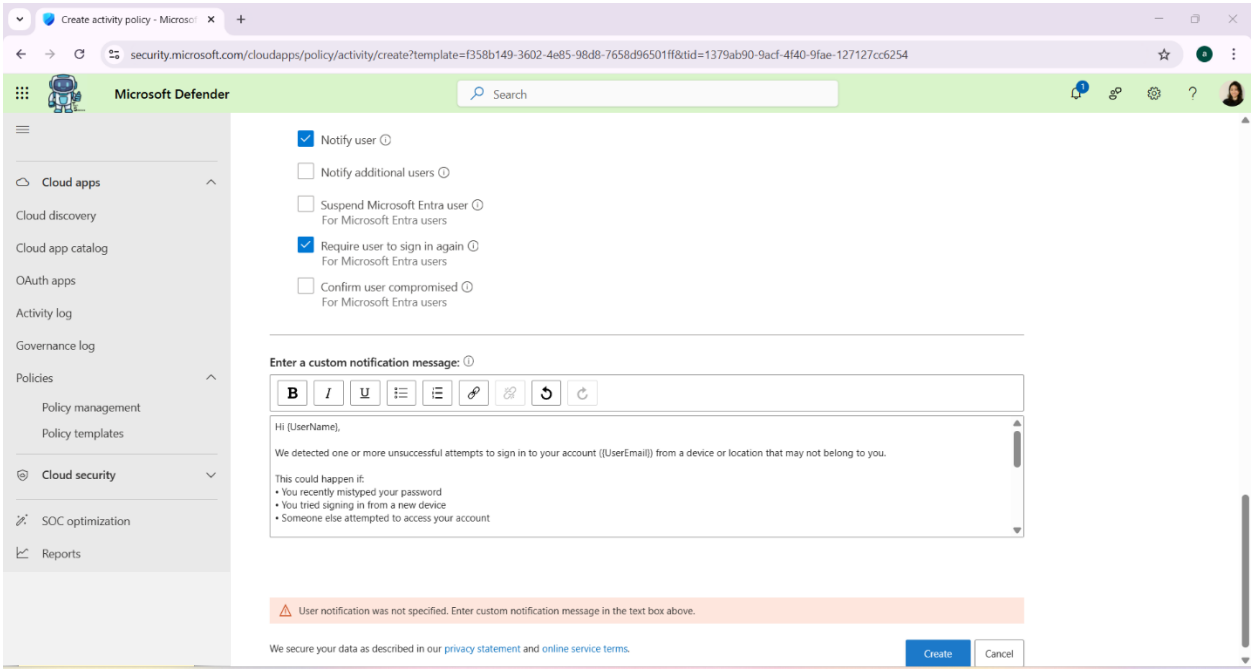
Created activity policy for Multi failed log on attempts to configure alert policy.



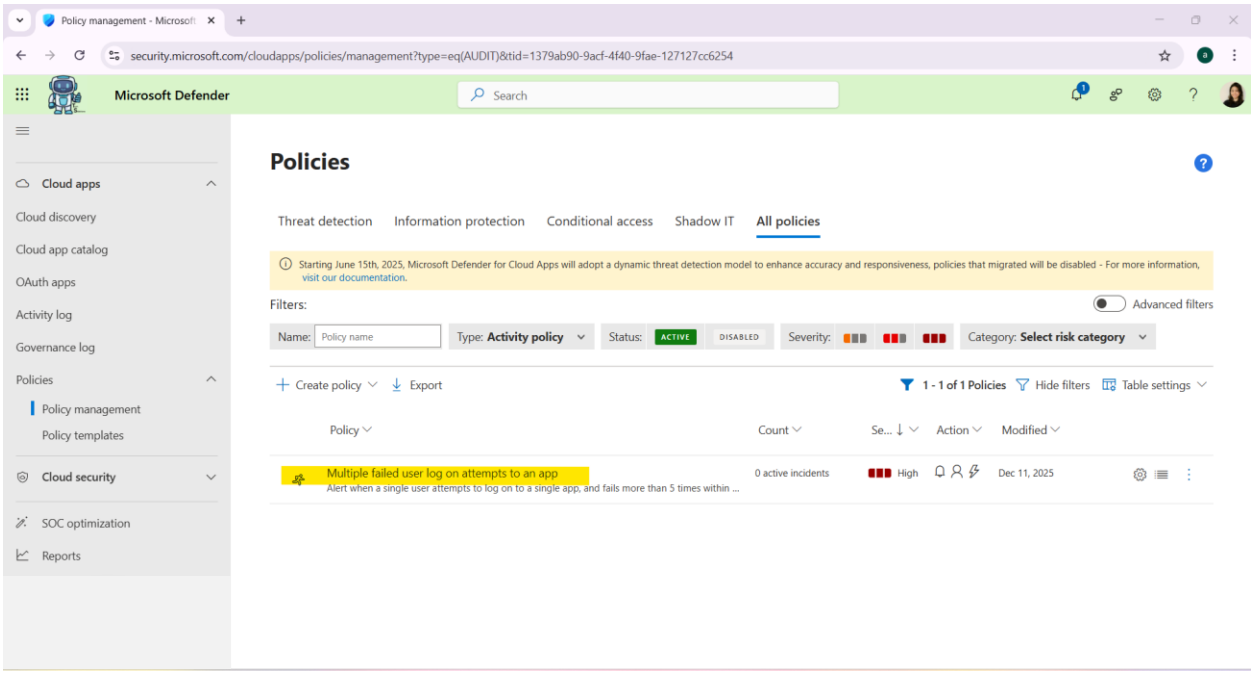
Set failed 5 times repeated activities within 5 minutes.



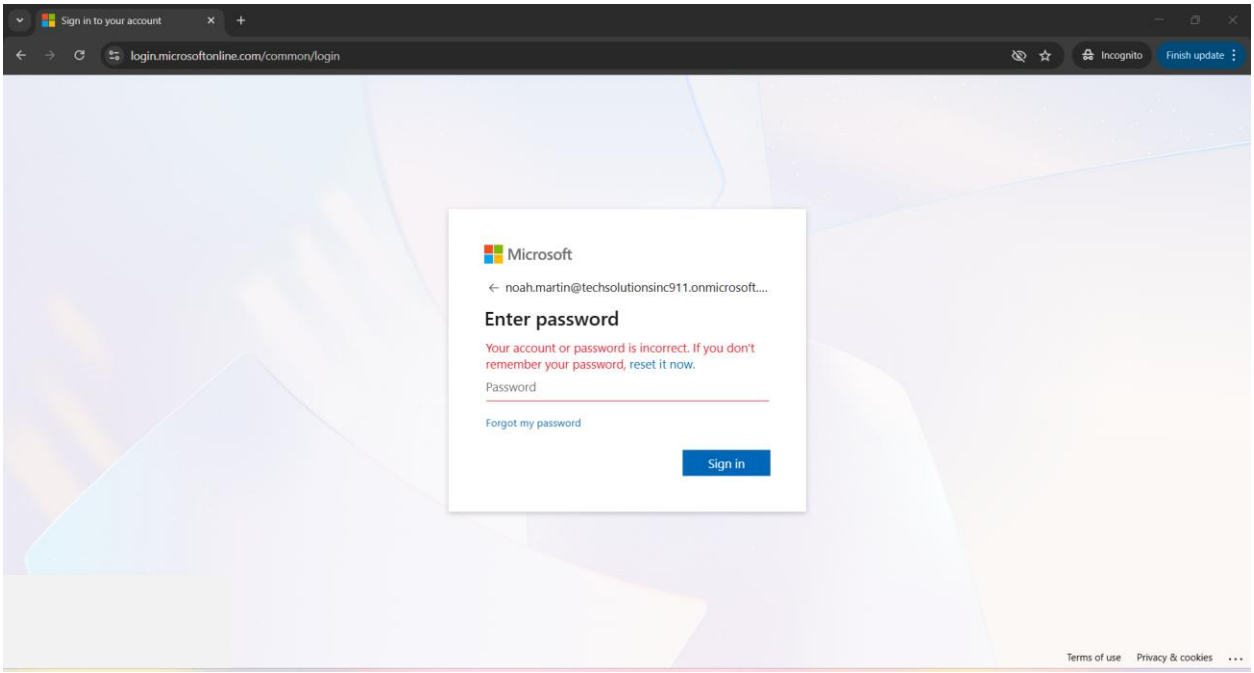
Set recipients to receive alert notification for two global admins and daily alert limit policy maximum since no option as no limit.



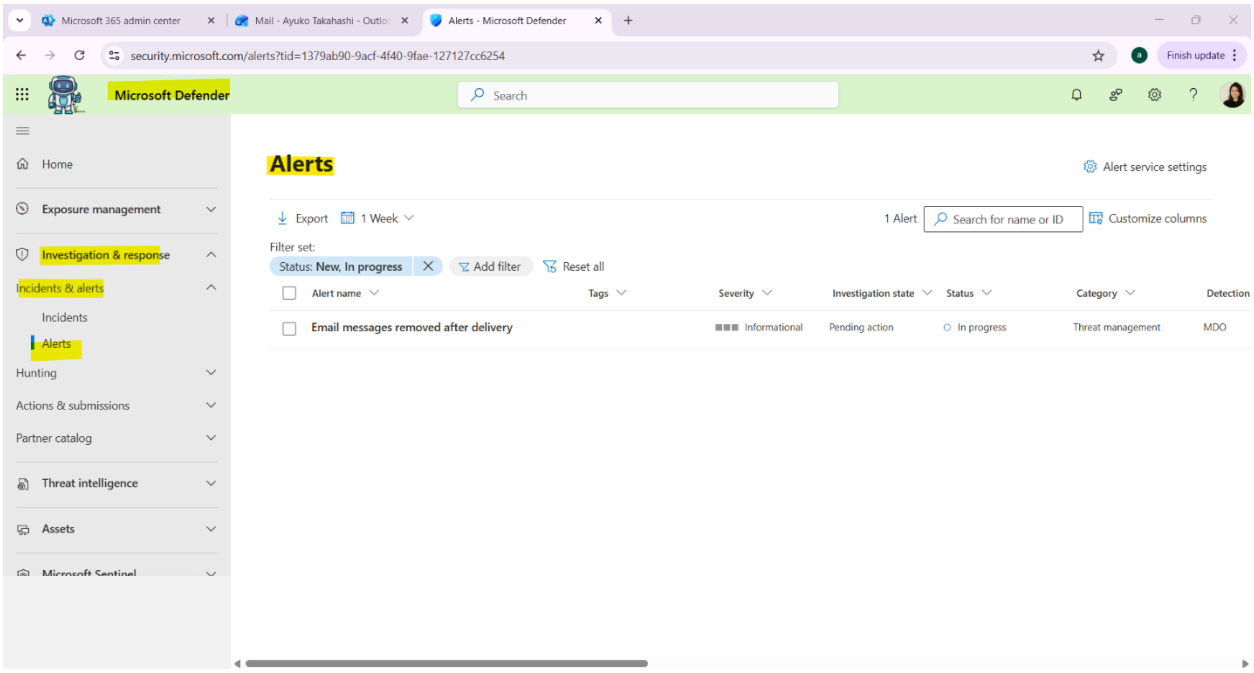
Entered a custom notification message and click Create.



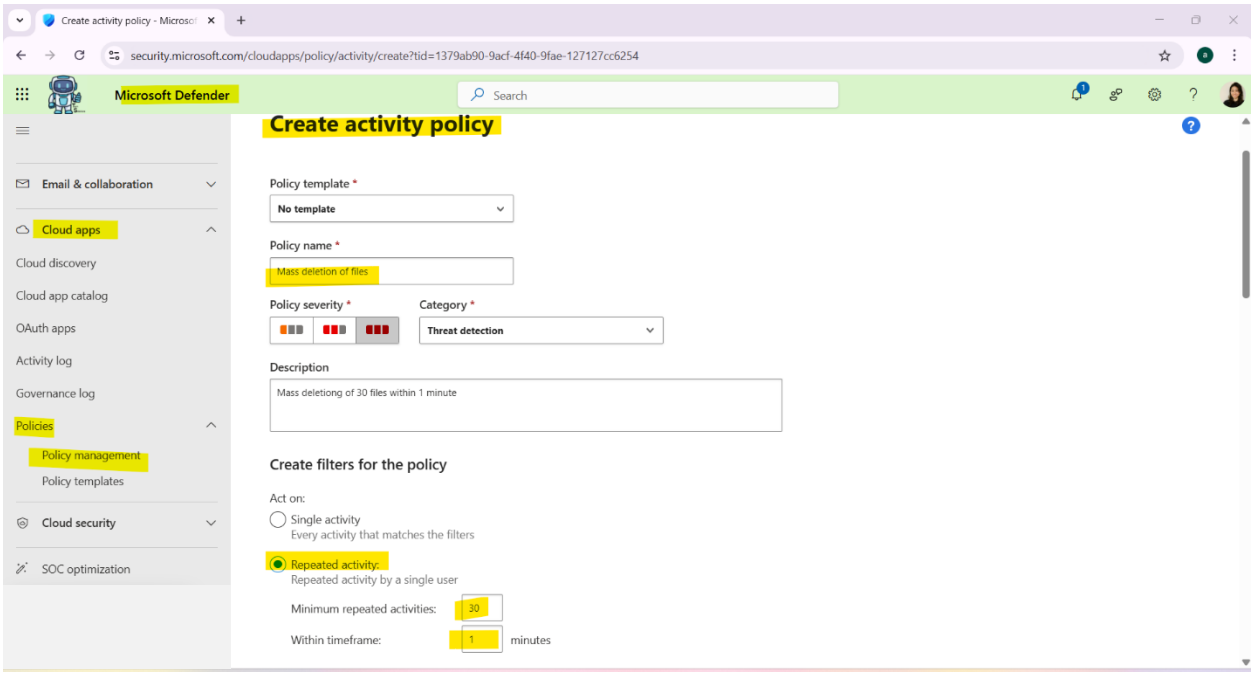
Multiple failed user log on attempts to an app policy has been created.



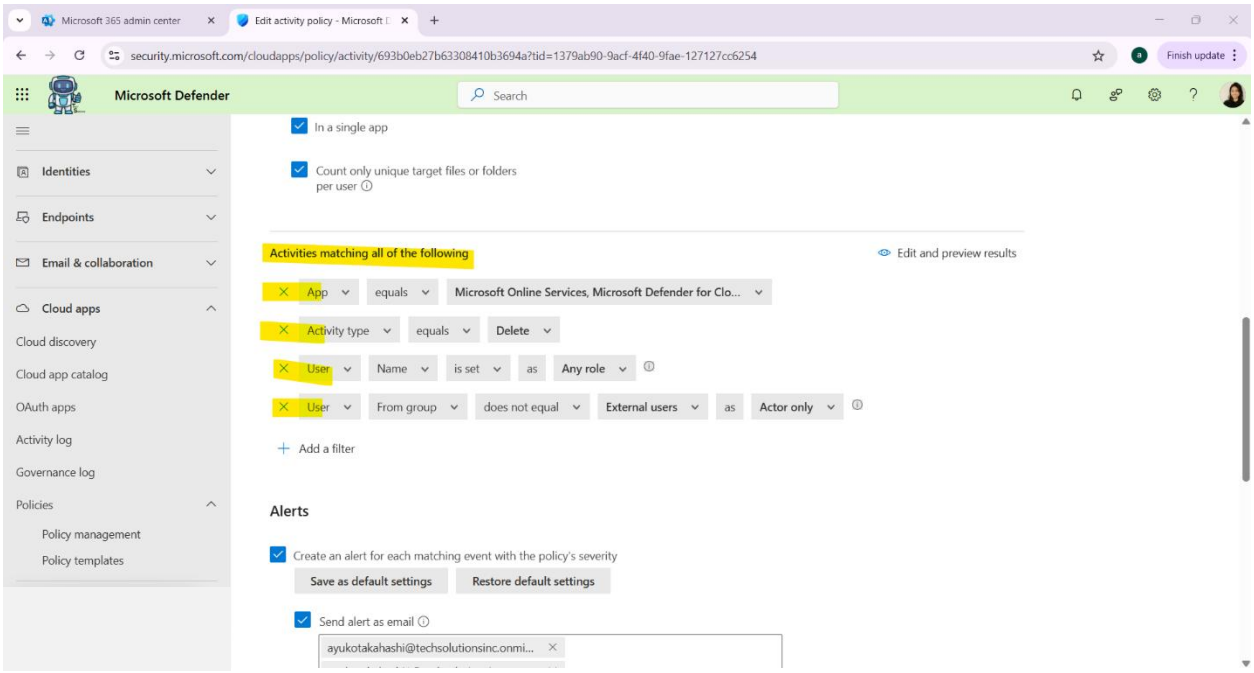
Policy behavior was tested by simulating repeated failed login attempts, confirming alert thresholds and detection logic.



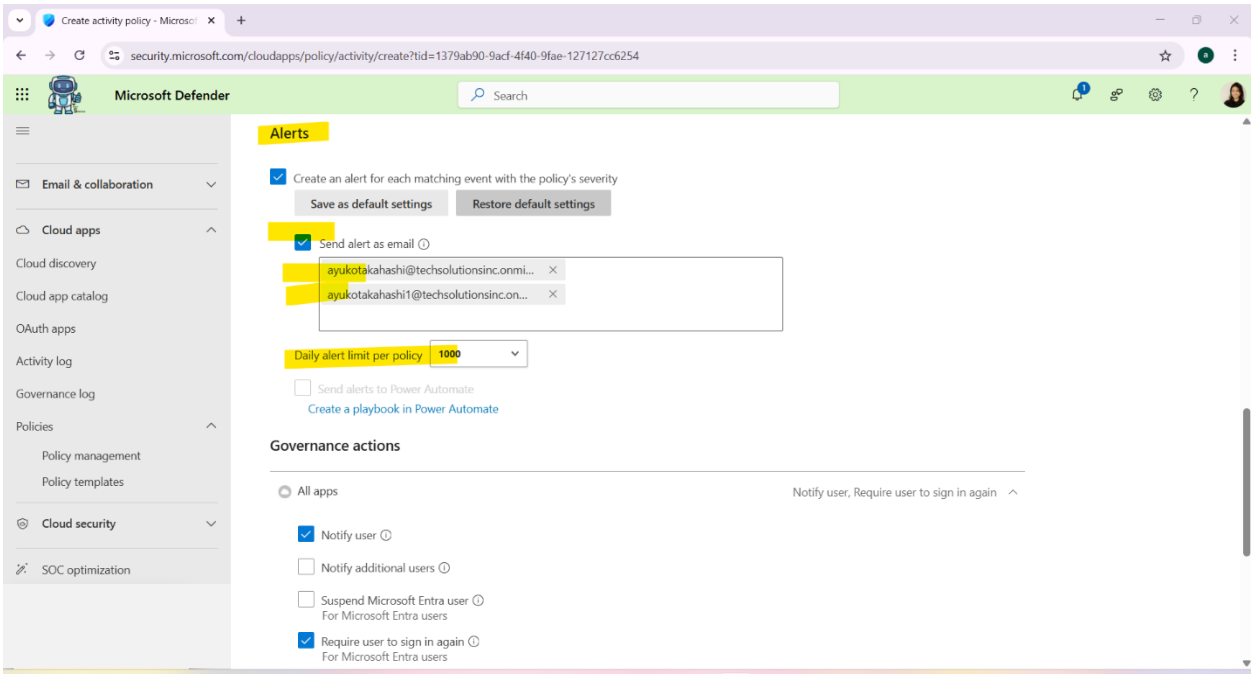
Navigate to Alerts to see the activity report, however, the policy will take an effect 7 business days so no data show yet. Neither Global admins received notification yet.



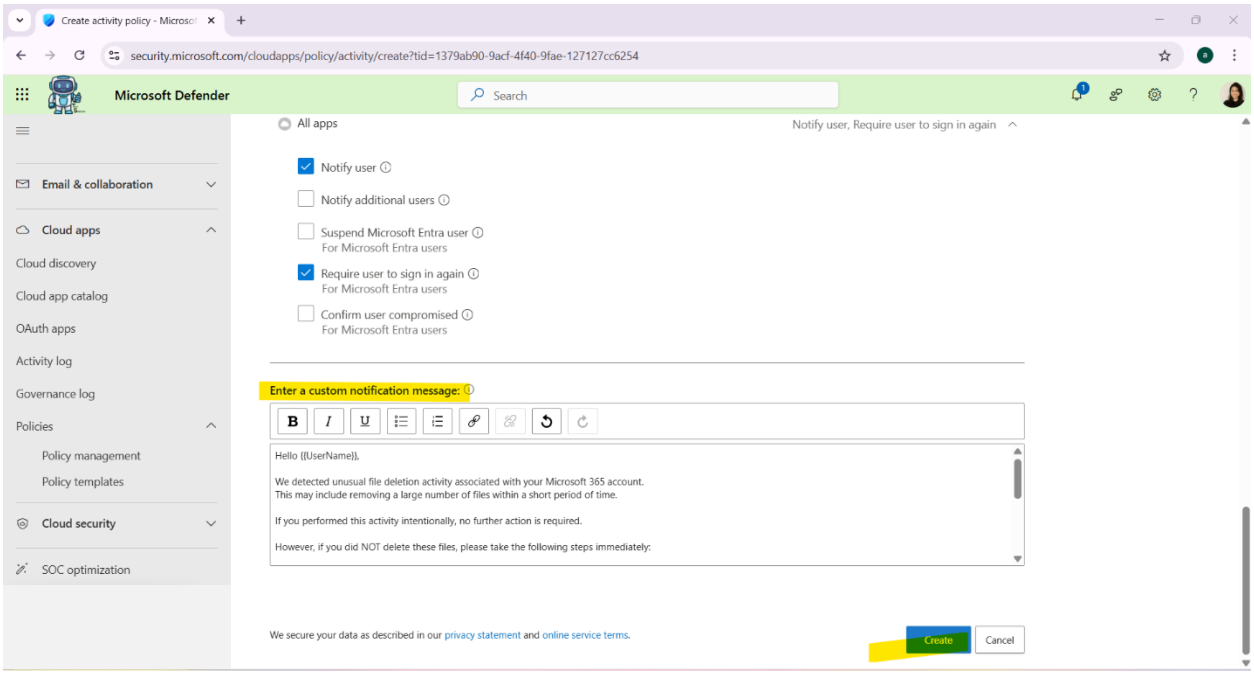
Created Activity policy for Mass deletion of files, set Repeated activity 30 times within 1 minute.



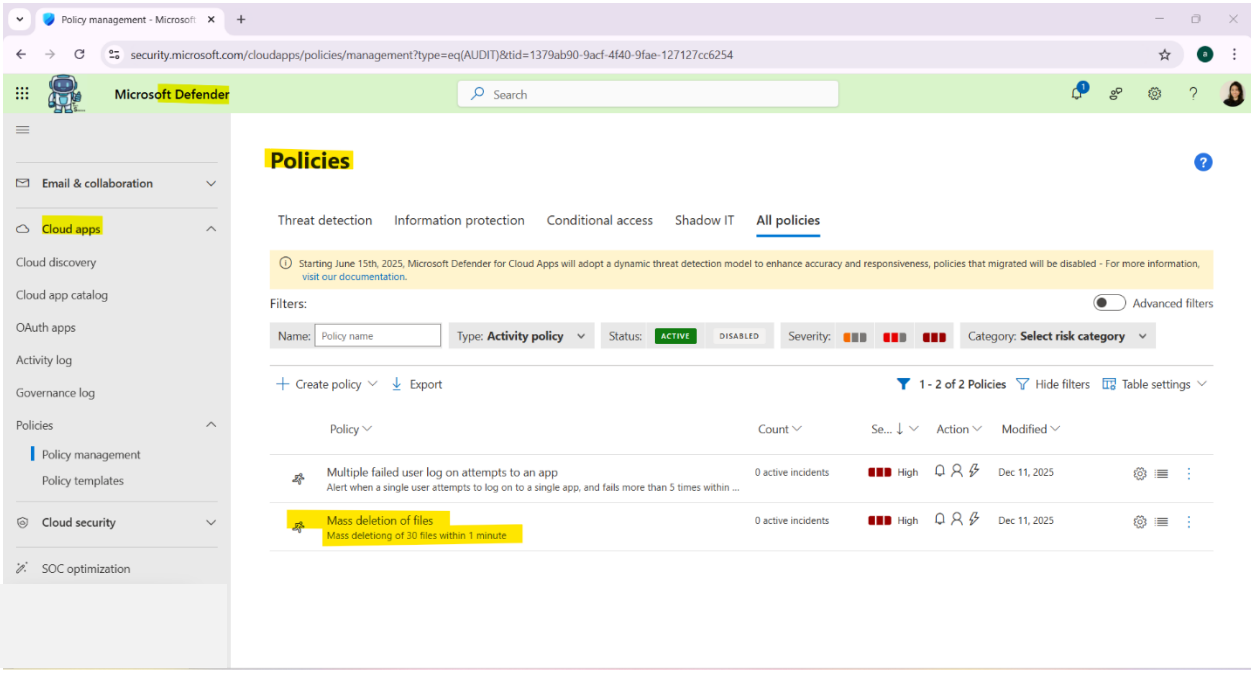
Set Filters to match activities.



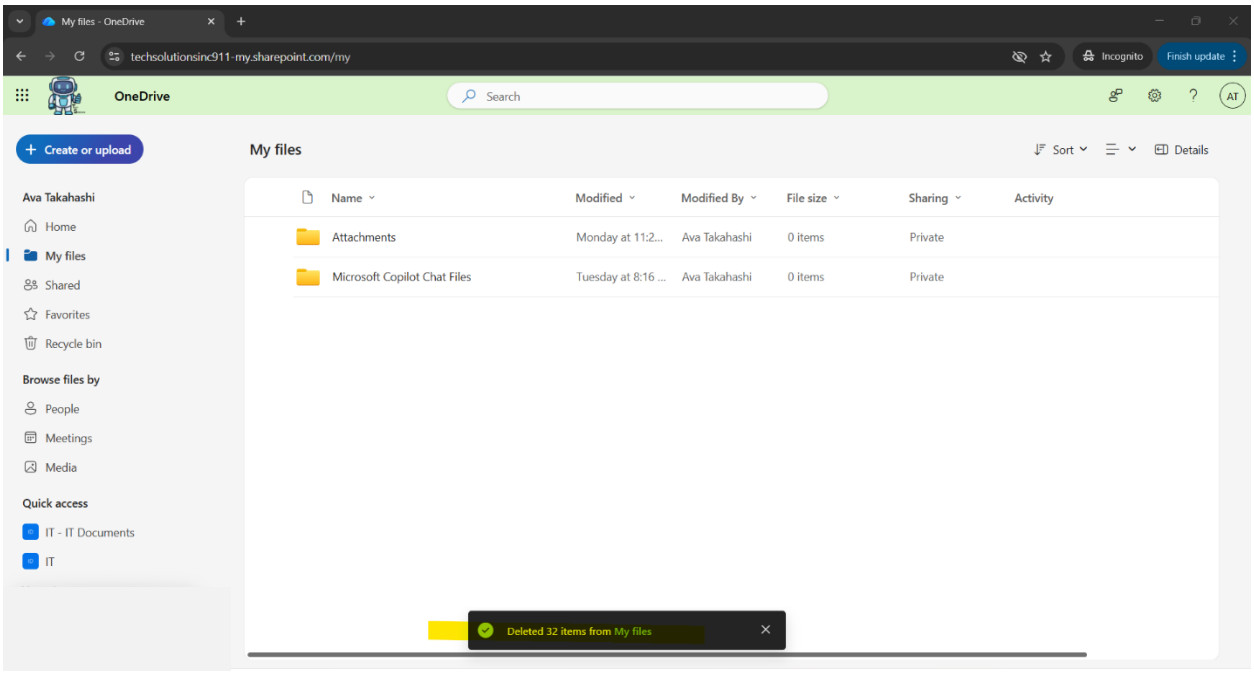
Set recipients to receive alert notification for two global admins and daily alert limit policy maximum since no option as no limit.



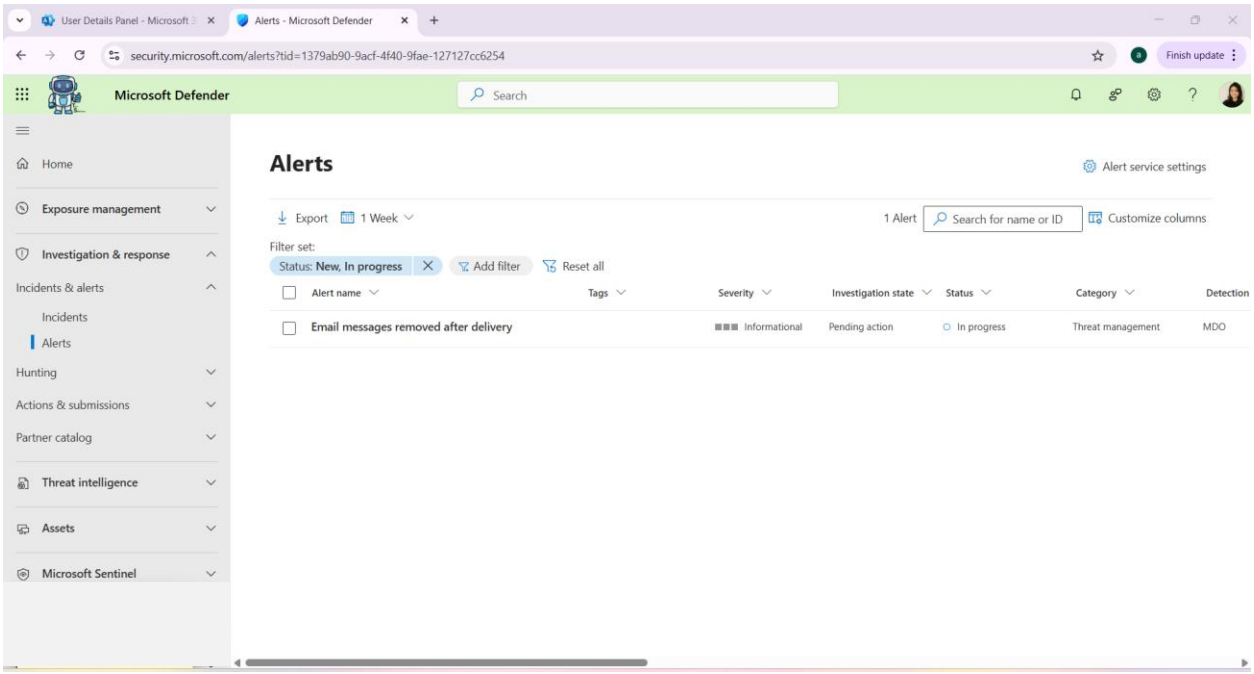
Entered a custom notification message and click Create.



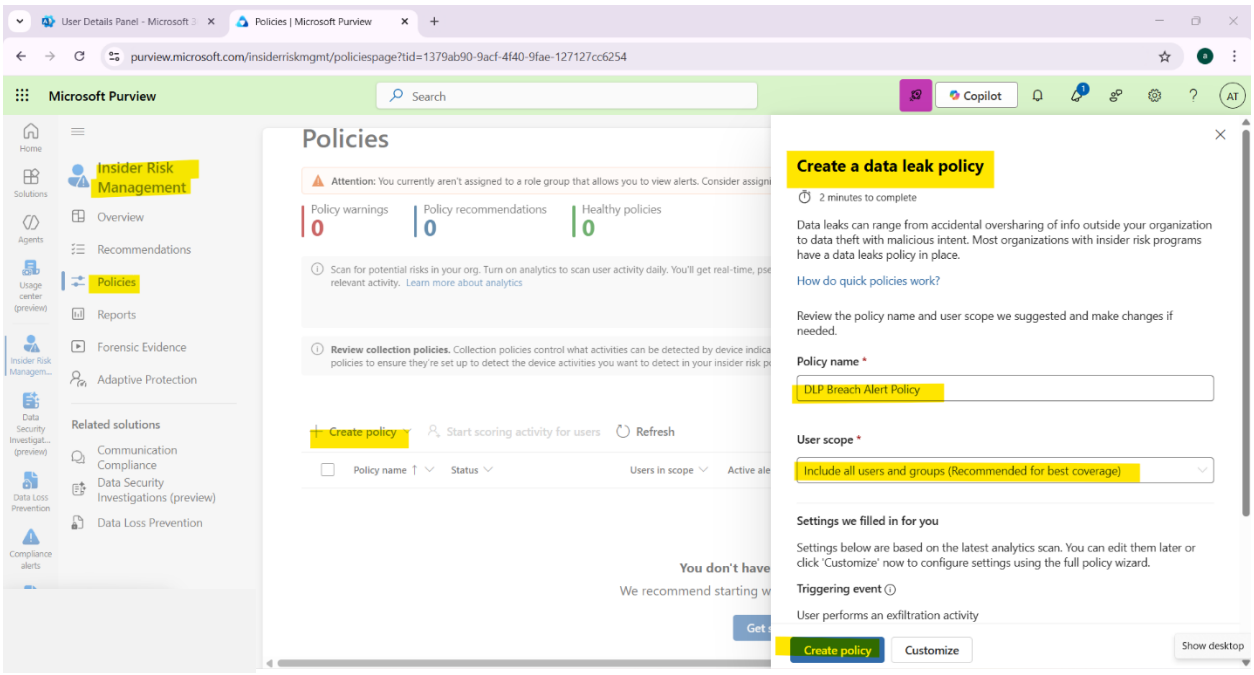
Mass deletion of files policy has been created.



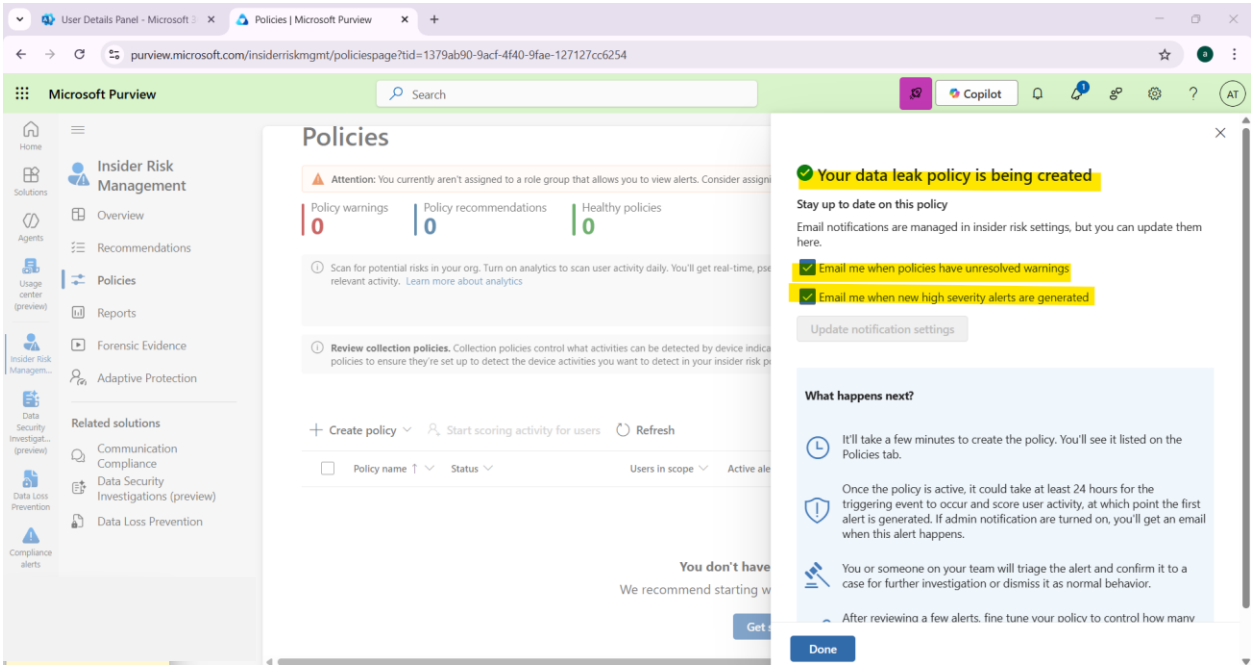
Policy behavior was validated by simulating a mass file deletion event, confirming alert threshold configuration.



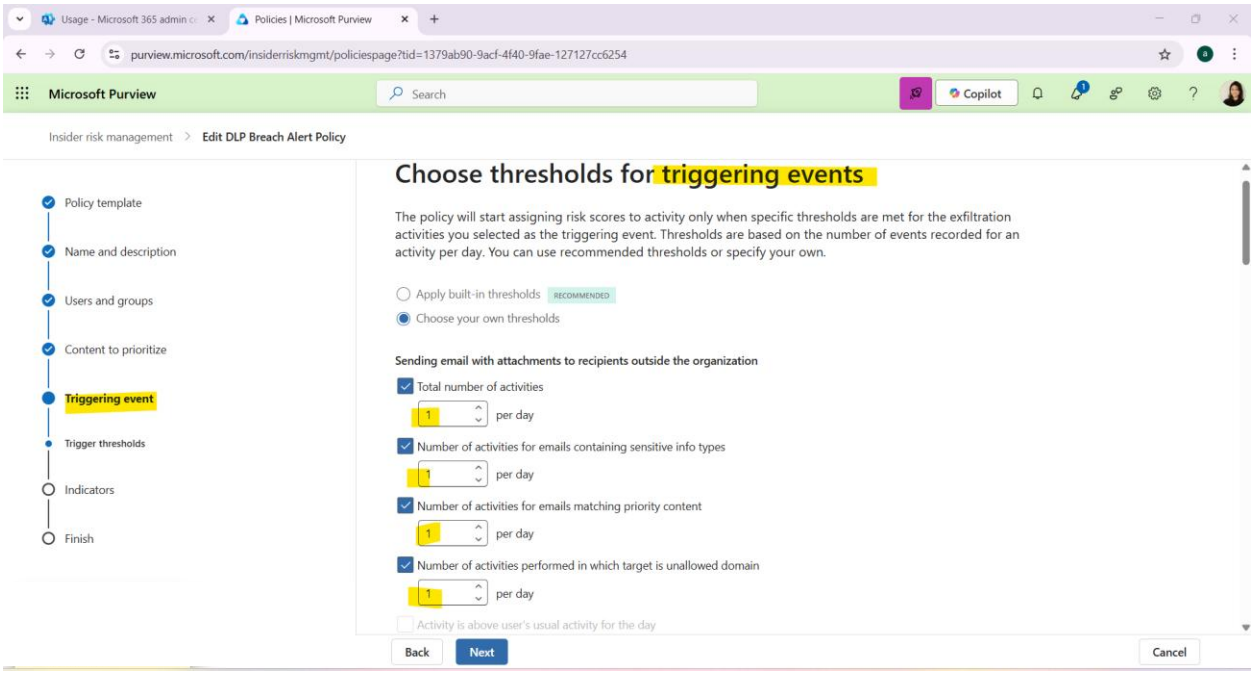
Navigate to Alerts to see the activity report, however, the policy will take an effect 7 business days so no data show yet. Neither Global admins received notification yet.



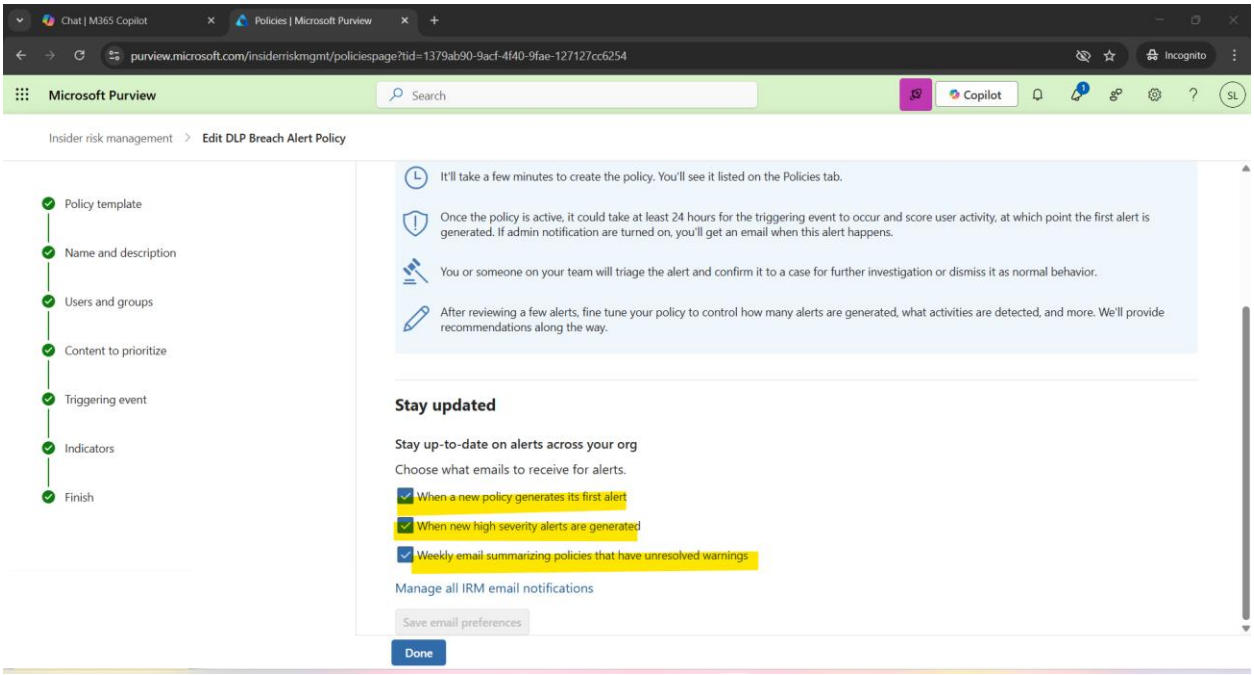
Created a data leak policy. Set Policy name as DLP Breach Alert Policy, User scope as Include all users and groups.



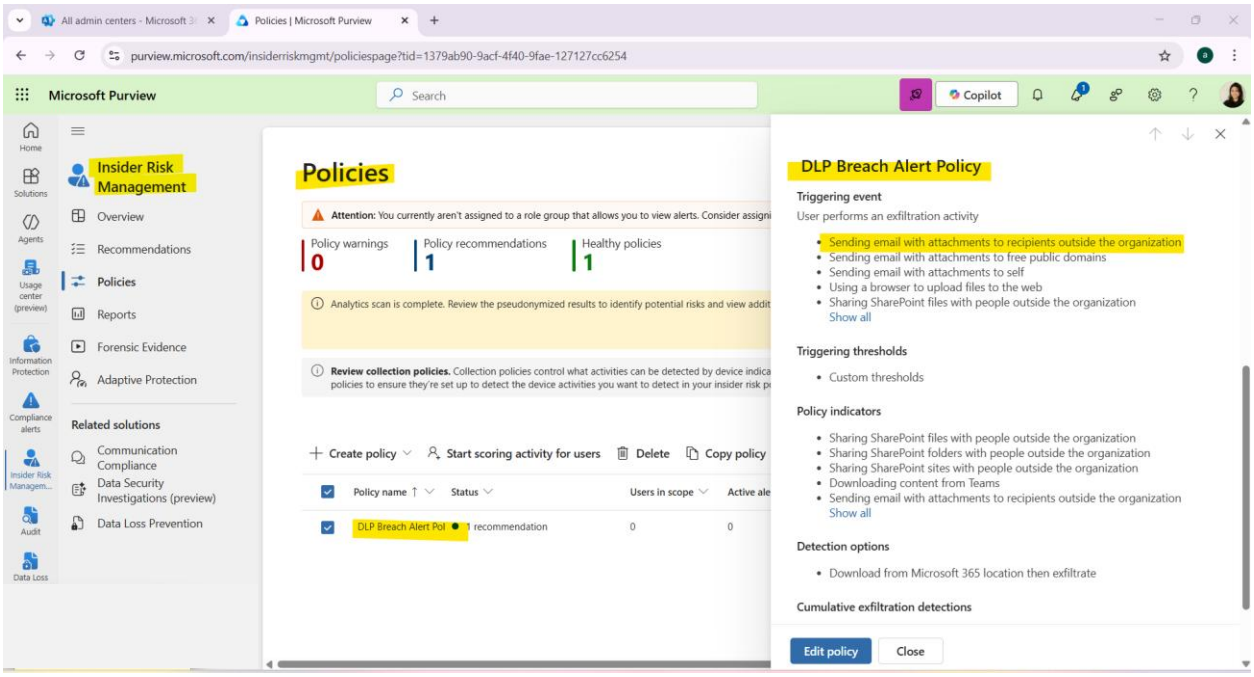
Update both notification settings that Global admin who created the policy receives.



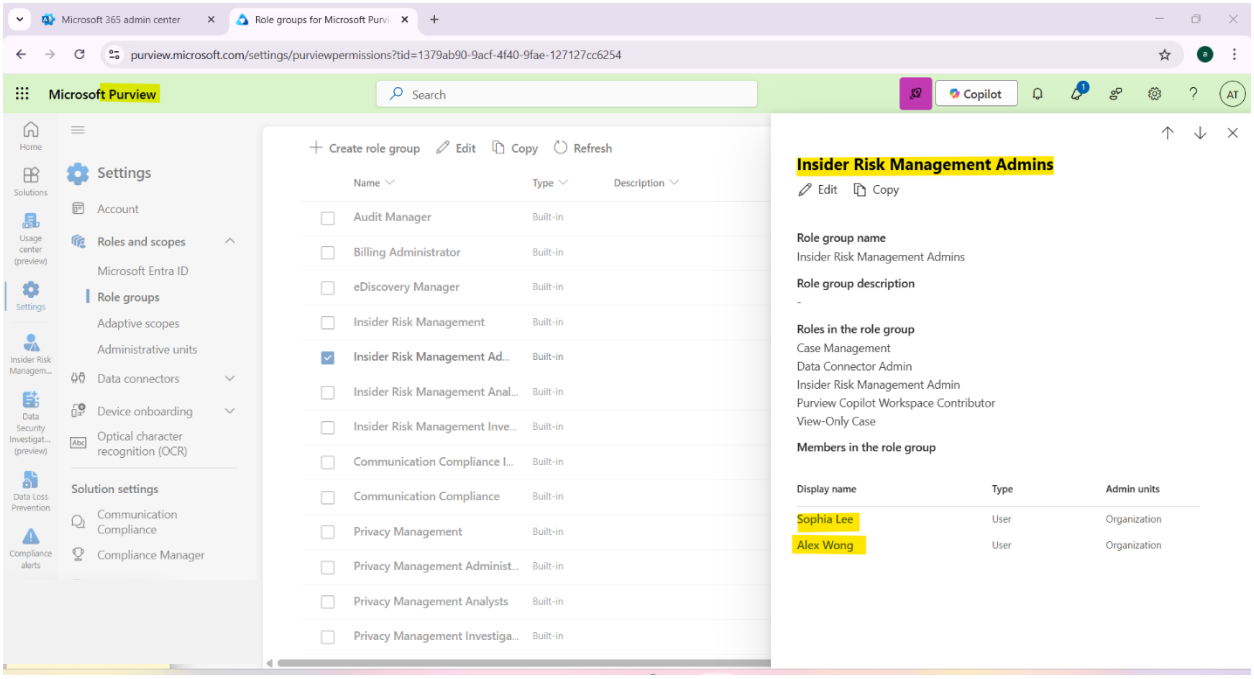
(Edited) Set triggering events to minimum number all sections.



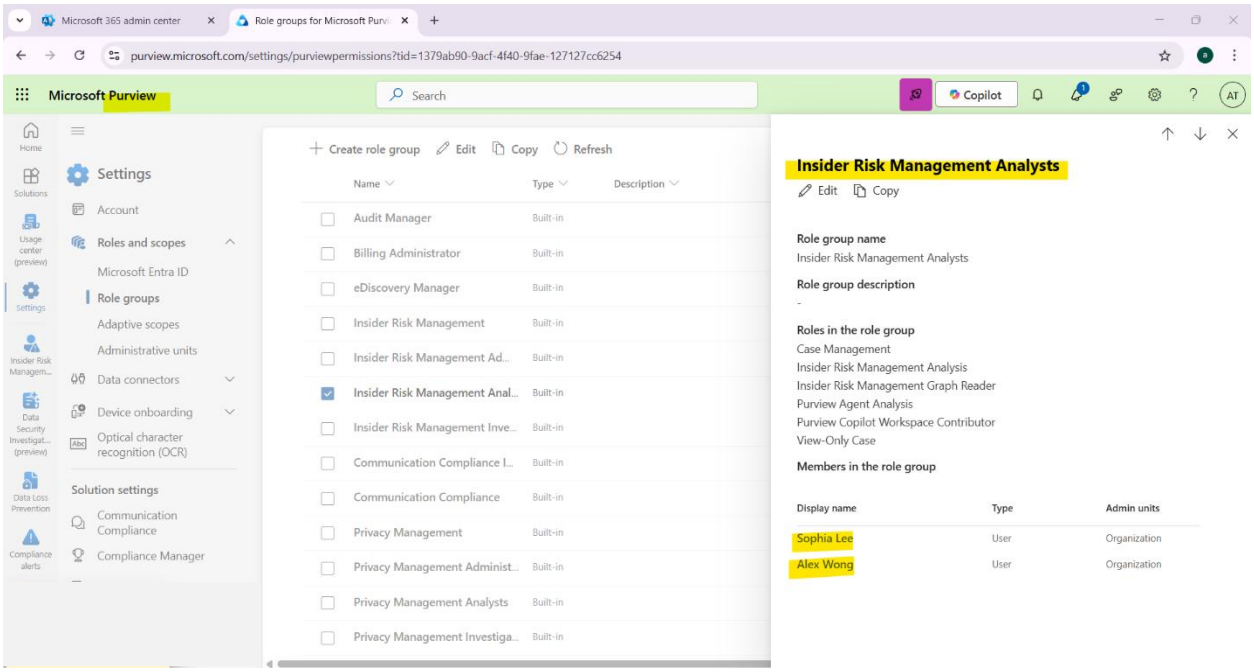
Set notification option.



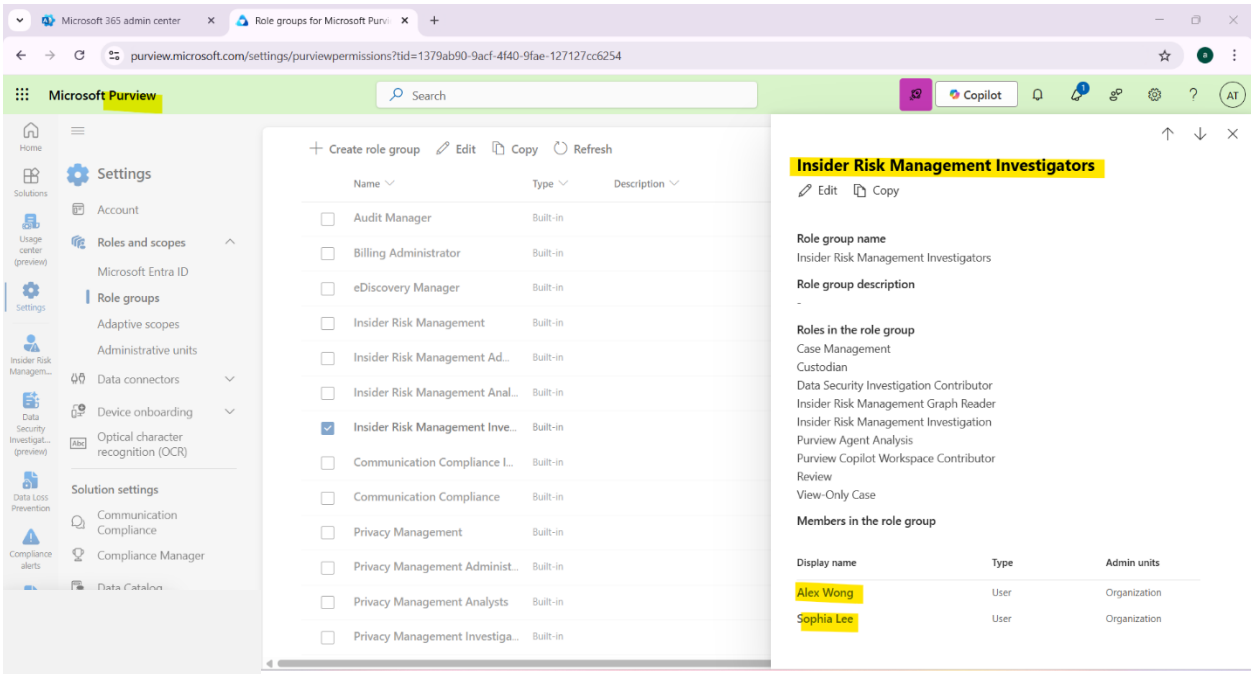
The data leak policy has been created.



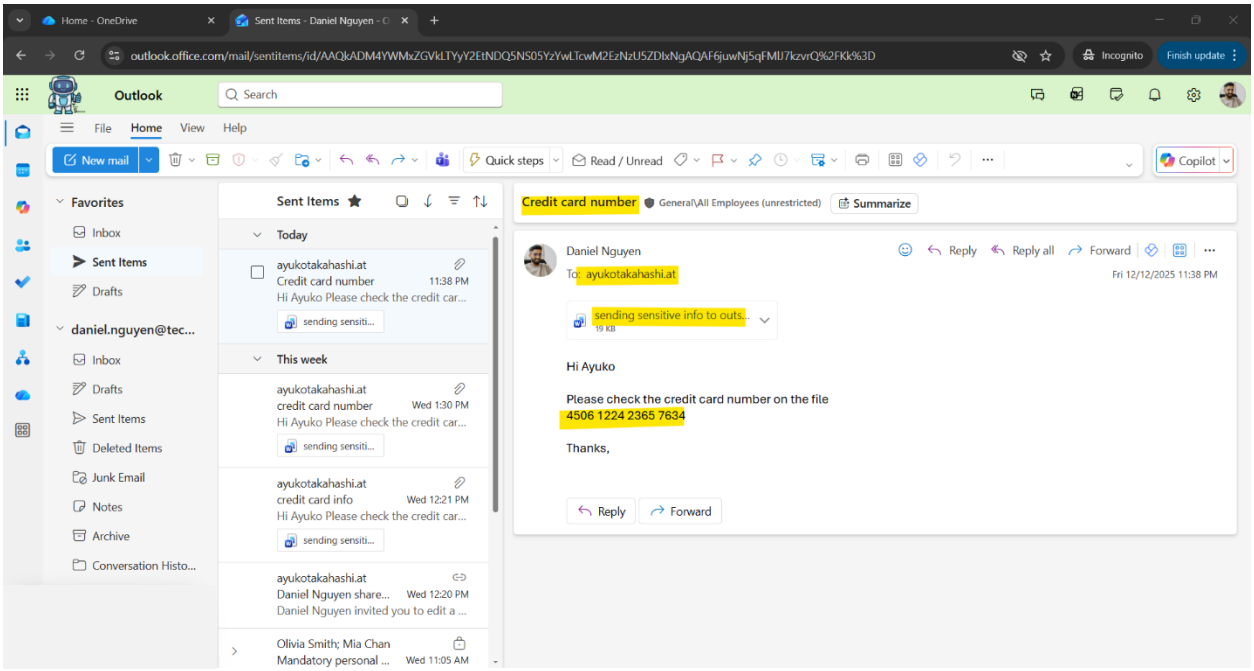
As an option, assign Insider Risk Management Admins role to two IT members to give access Alert check on Purview.



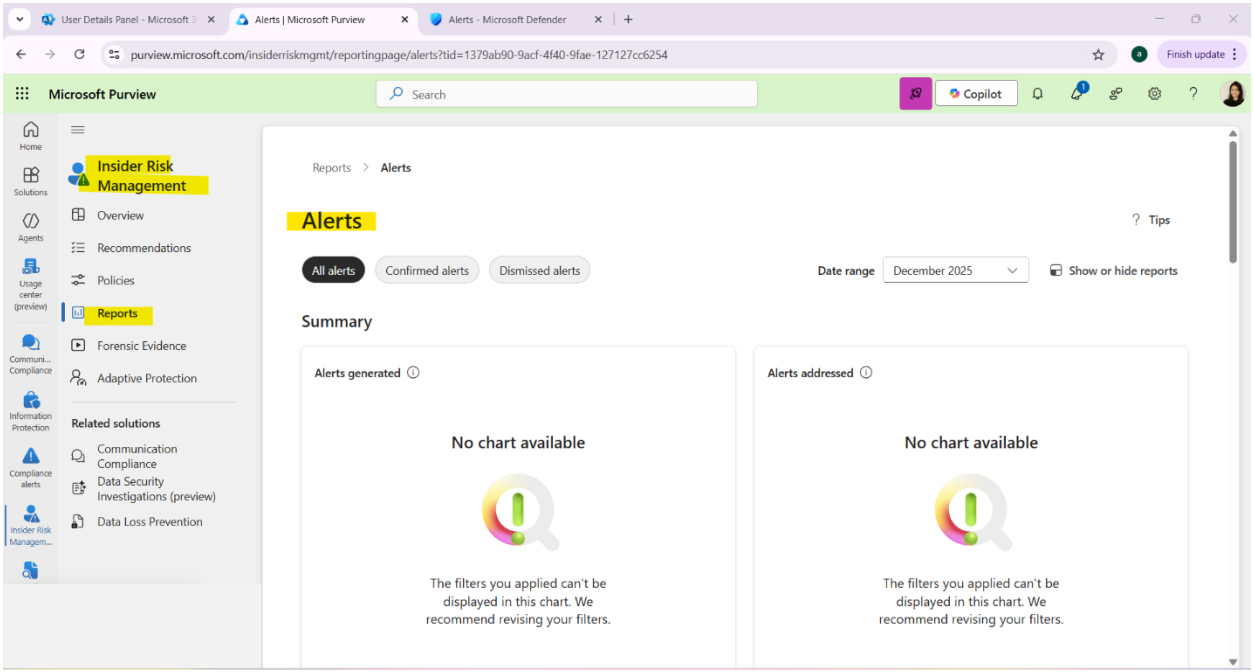
Assign Insider Risk Management Analysts to the same IT members as the admins.



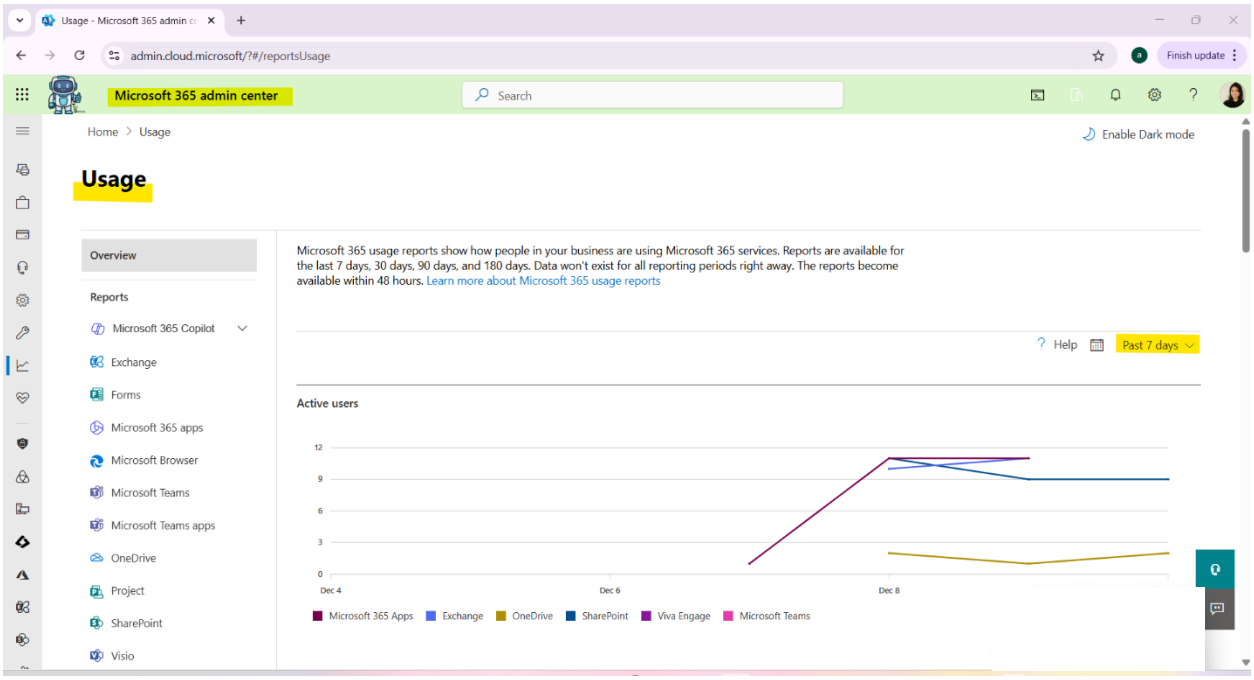
Assign Insider Risk Management investigator roles to the same IT members as the admin for full access of Insider Risk Management.



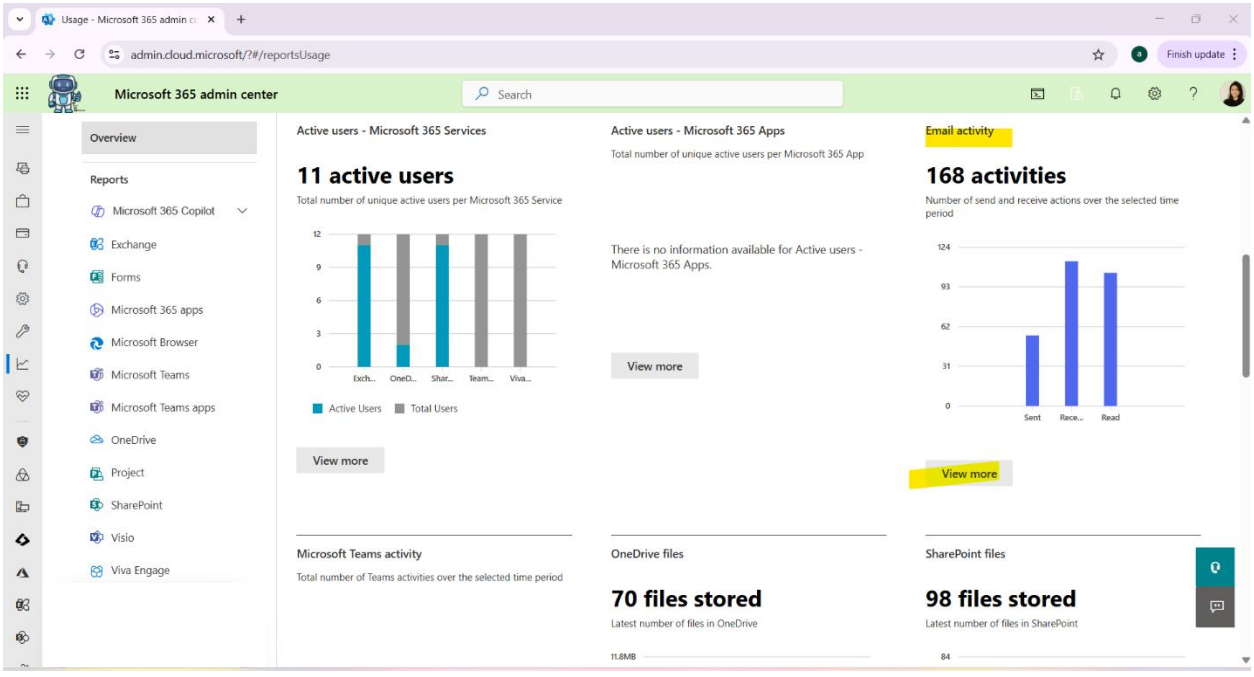
Insider Risk Management alerts were validated by simulating external transmission of sensitive content.

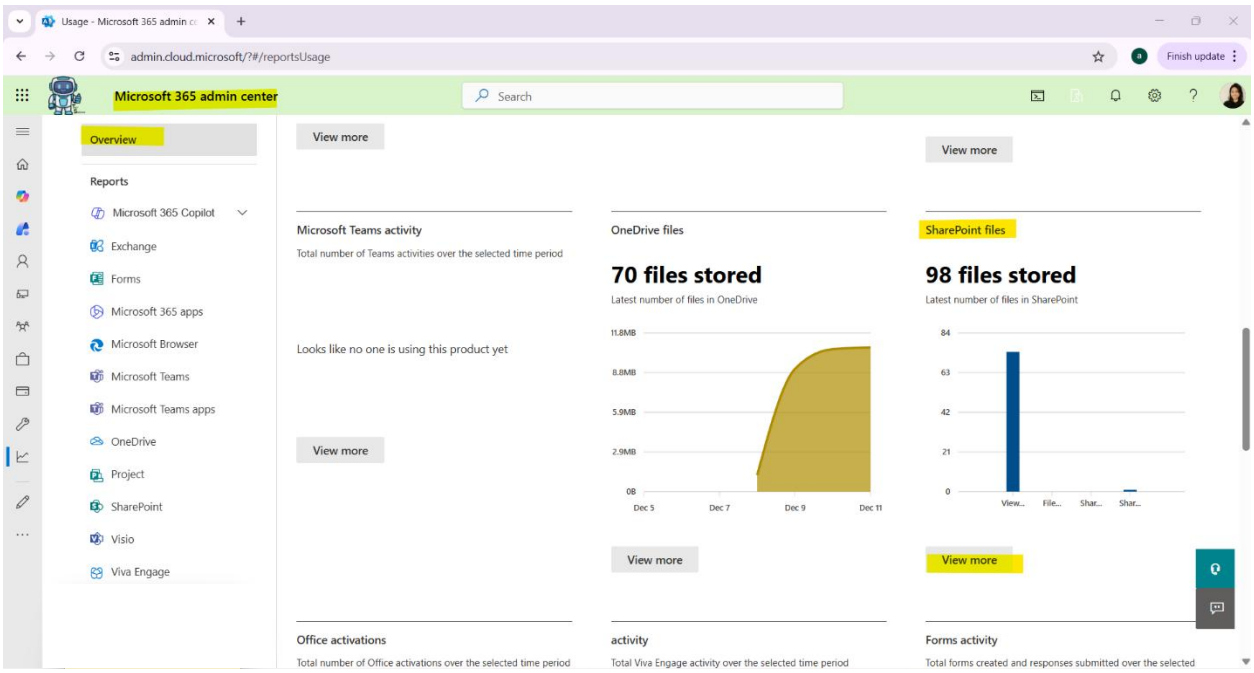


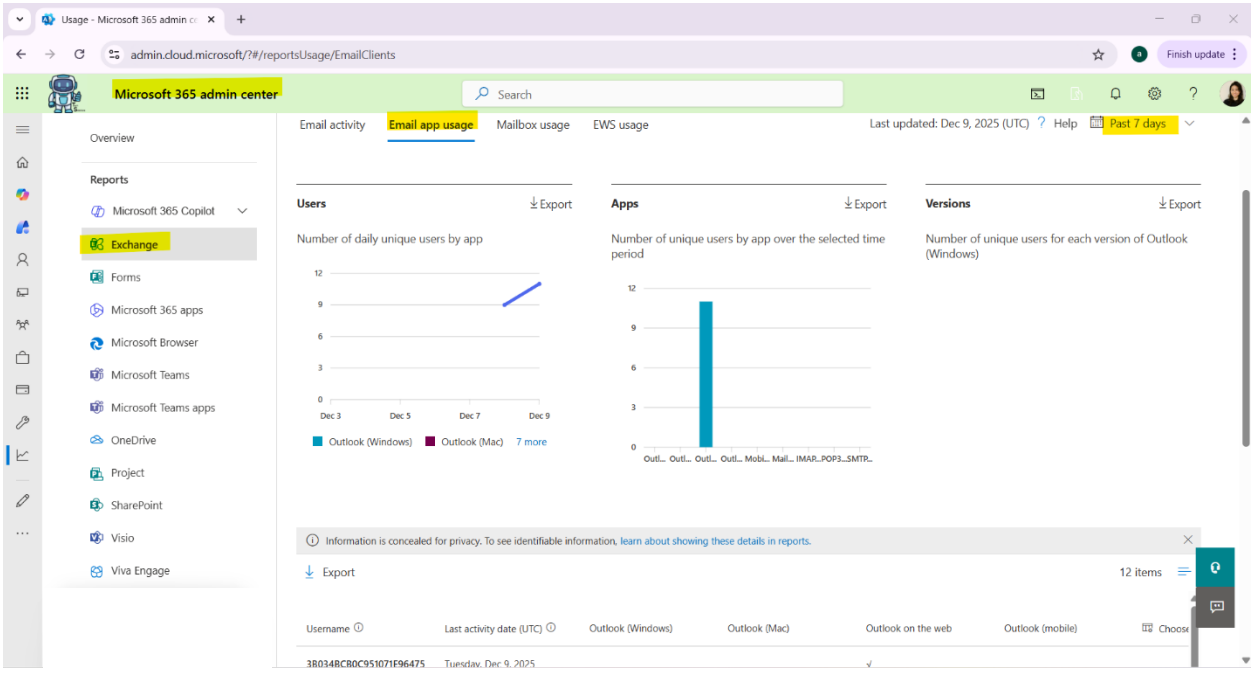
Navigate to Alerts to see the activity report, however, the policy will take an effect 7 business days so no data show yet. Neither Global admins and Daniel (Sender) received notification yet.

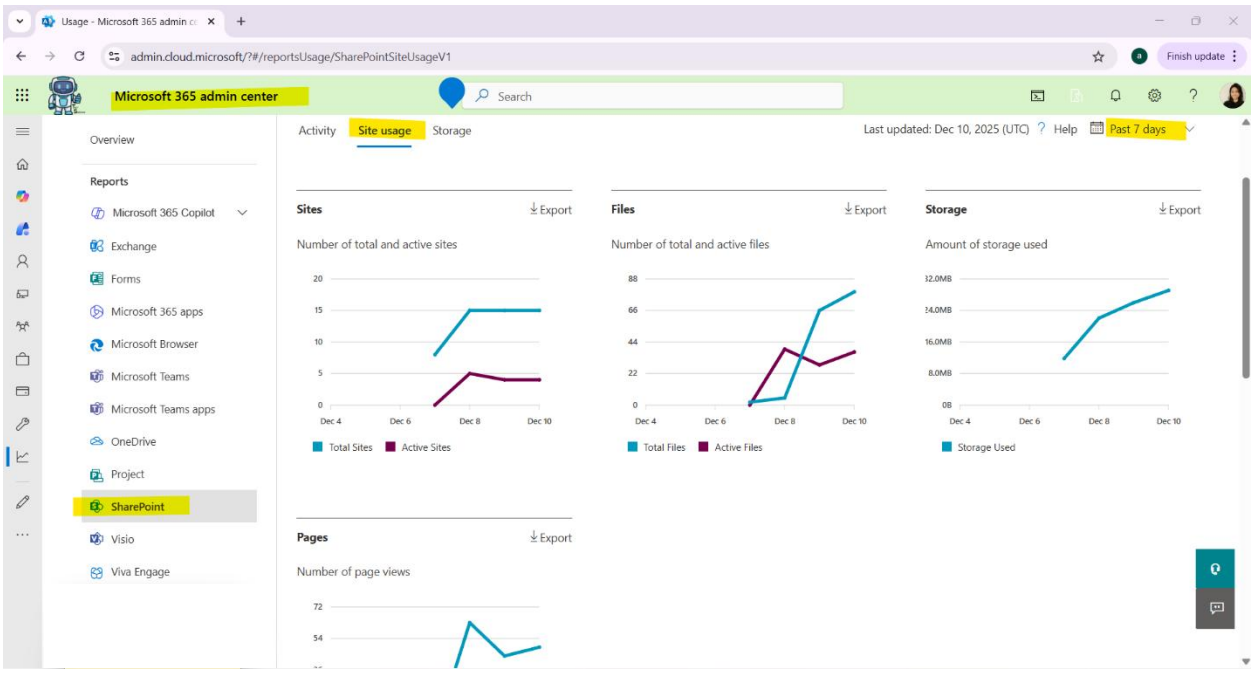


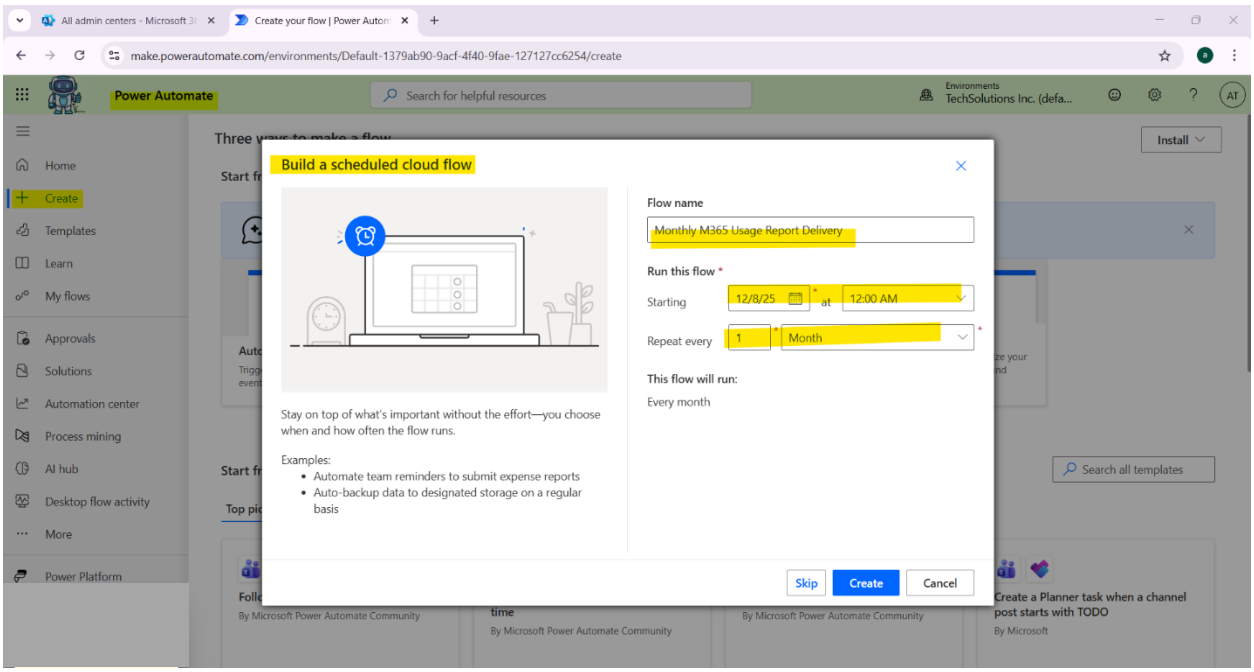
Usage reports were reviewed to assess email and SharePoint activity trends over the previous seven-day period.



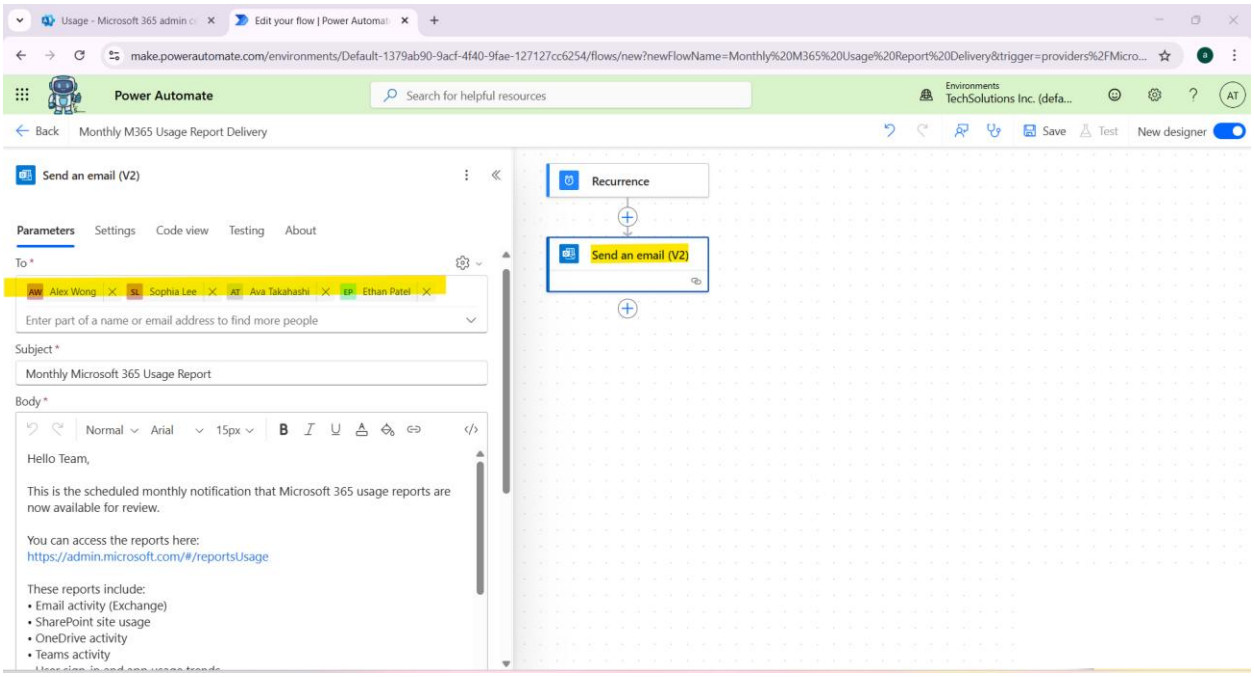

Usage - Microsoft 365 admin
admin.cloud.microsoft/?#/reportsUsage
Finish update
Microsoft 365 admin center
Search
Overview
Reports
Microsoft 365 Copilot
Exchange
Forms
Microsoft 365 apps
Microsoft Browser
Microsoft Teams
Microsoft Teams apps
OneDrive
Project
SharePoint
Visio
Viva Engage
View more
Microsoft Teams activity
Total number of Teams activities over the selected time period
Looks like no one is using this product yet
View more
OneDrive files
70 files stored
Latest number of files in OneDrive
11.8MB
8.8MB
5.9MB
2.9MB
0B
Dec 5
Dec 7
Dec 9
Dec 11
View more
View more
SharePoint files
98 files stored
Latest number of files in SharePoint
84
63
42
21
0
View more
Office activations
Total number of Office activations over the selected time period
activity
Total Viva Engage activity over the selected time period
Forms activity
Total forms created and responses submitted over the selected


Usage - Microsoft 365 admin
admin.cloud.microsoft/?#/reportsUsage/EmailClients
Finish update
Microsoft 365 admin center
Search
Overview
Reports
Microsoft 365 Copilot
Exchange
Forms
Microsoft 365 apps
Microsoft Browser
Microsoft Teams
Microsoft Teams apps
OneDrive
Project
SharePoint
Visio
Viva Engage
Email activity
Email app usage
Mailbox usage
EWS usage
Last updated: Dec 9, 2025 (UTC)
Help
Past 7 days
Users
Export
Number of daily unique users by app
12
9
6
3
0
Dec 3
Dec 5
Dec 7
Dec 9
Outlook (Windows)
Outlook (Mac)
7 more
Apps
Export
Number of unique users by app over the selected time period
12
9
6
3
0
Outl...
Outl...
Outl...
Outl...
Mobi...
Mail...
IMAP...
POP3...
SMTP...
Versions
Export
Number of unique users for each version of Outlook (Windows)
Information is concealed for privacy. To see identifiable information, learn about showing these details in reports.
Export
12 items
Username
Last activity date (UTC)
Outlook (Windows)
Outlook (Mac)
Outlook on the web
Outlook (mobile)
3R034BCB0C951071F96475
Tuesday, Dec 9, 2025

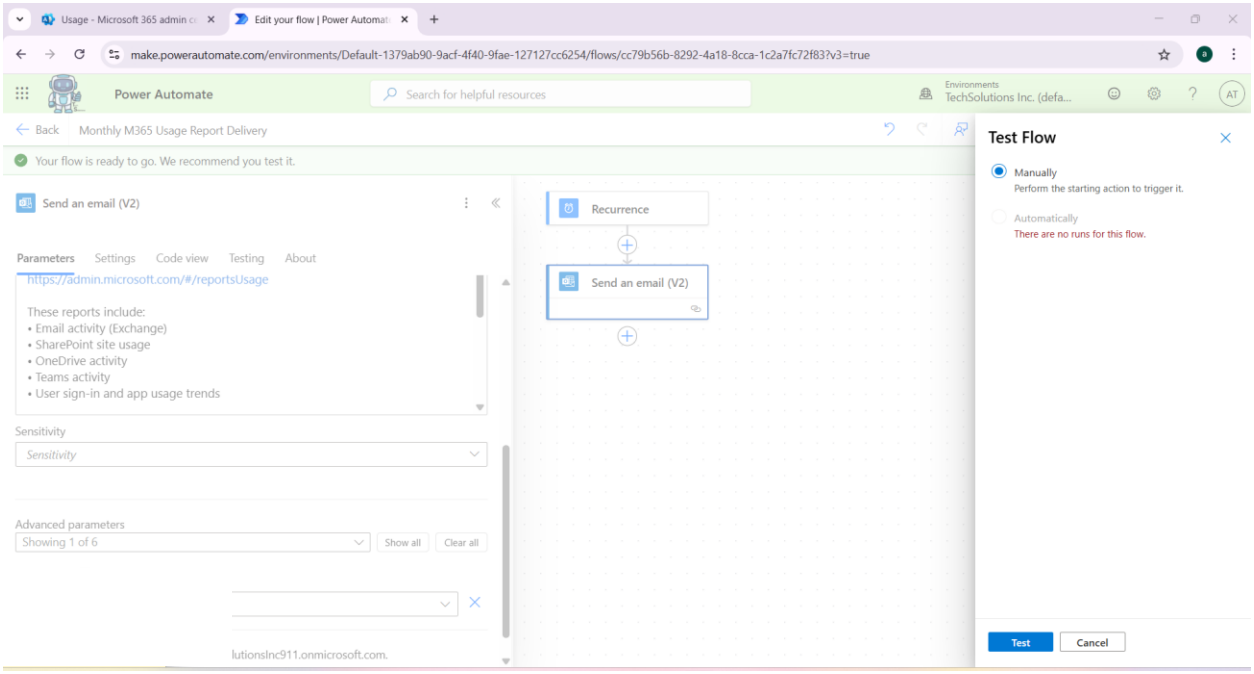




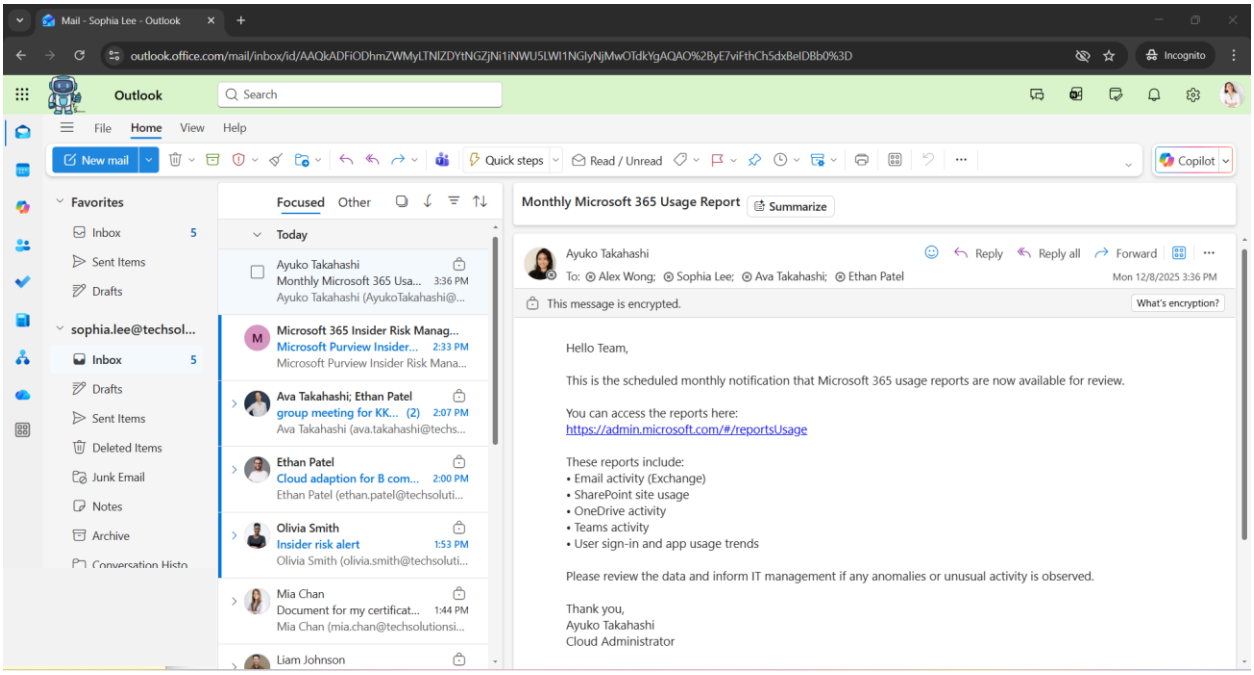
A scheduled Power Automate cloud flow was configured to distribute monthly usage reports to IT members and department leadership.

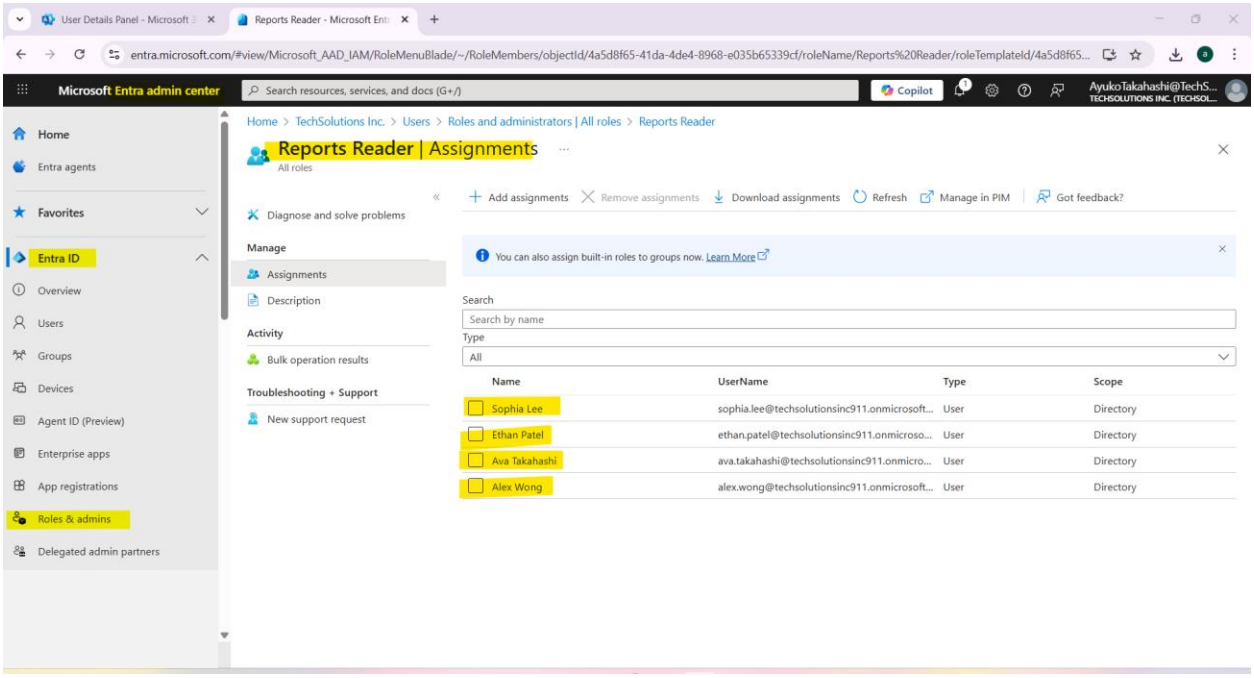


Set IT members and department head to receive the monthly email.

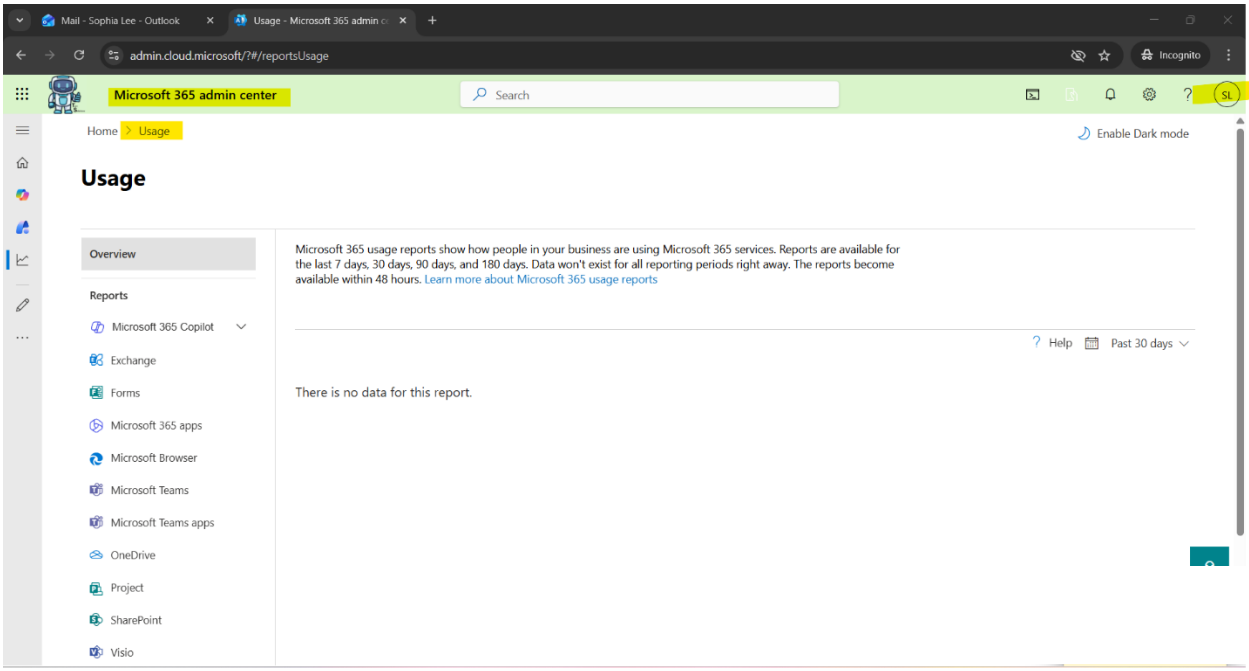


The Power Automate flow was tested successfully, with scheduled usage reports delivered to designated IT recipients.





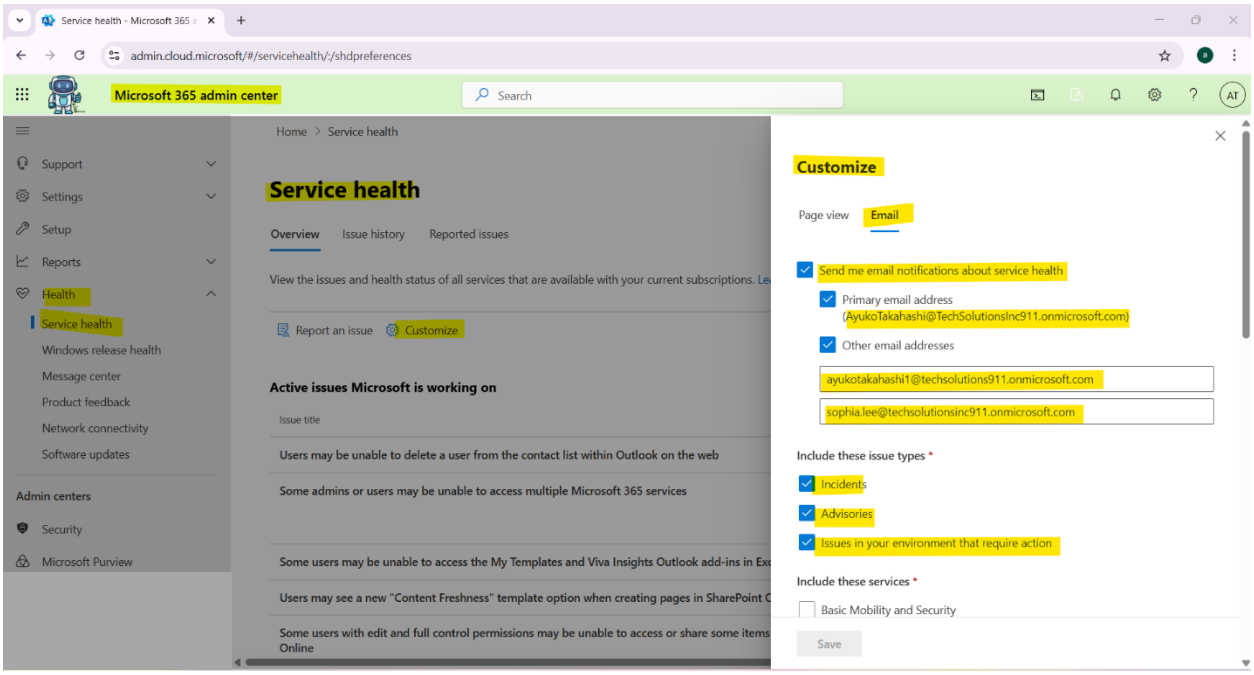
Assign IT members and Department head as Reports Reader role for reading the usage report.



Access to Microsoft 365 usage reports was validated for designated IT members through the Reports Reader role.

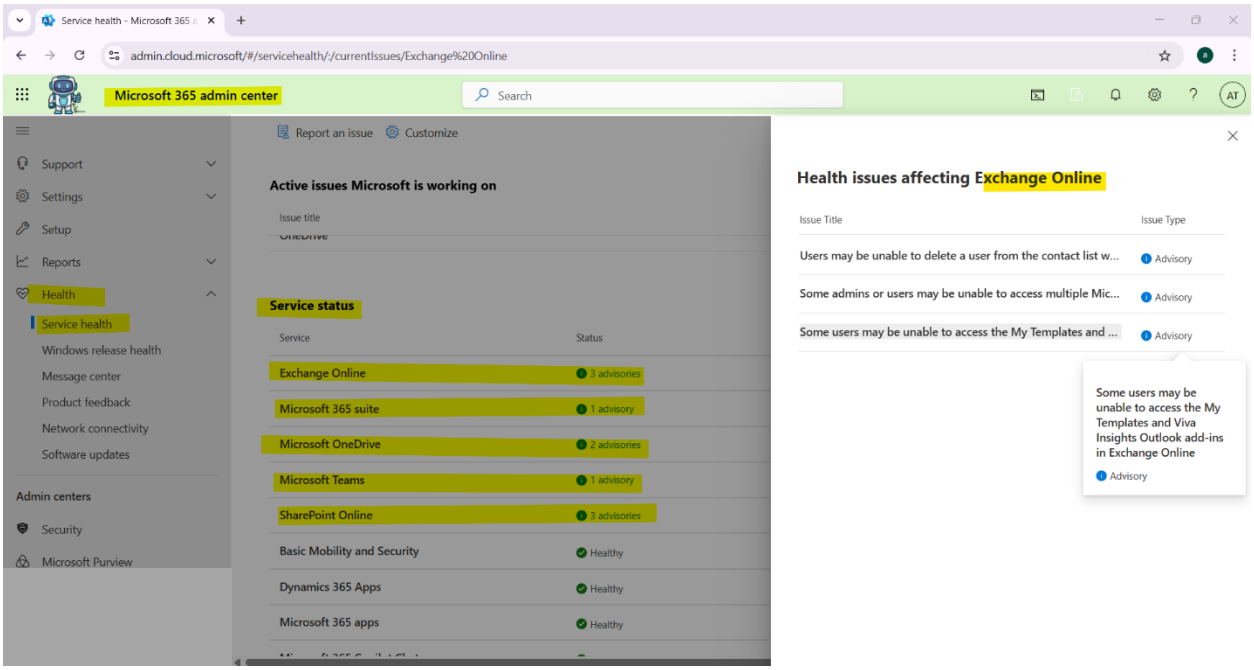
Service Health Monitoring and Operational Oversight

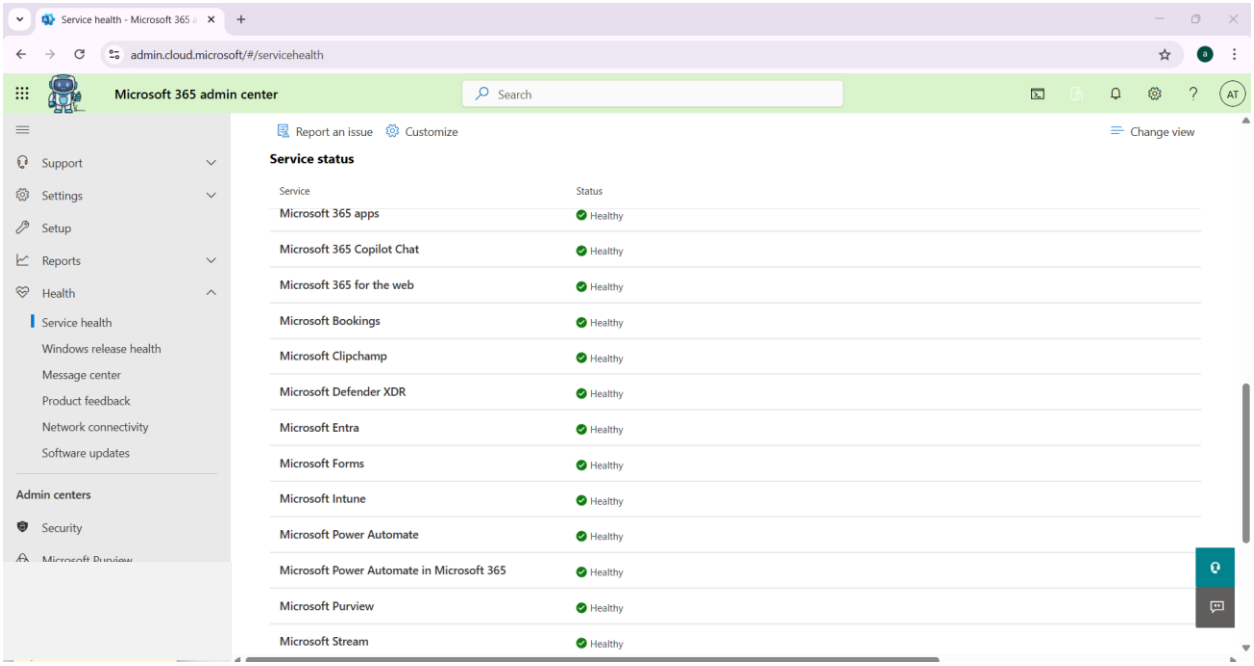
This section highlights service health monitoring practices used to track Microsoft 365 service availability and respond to advisories or incidents affecting business operations.

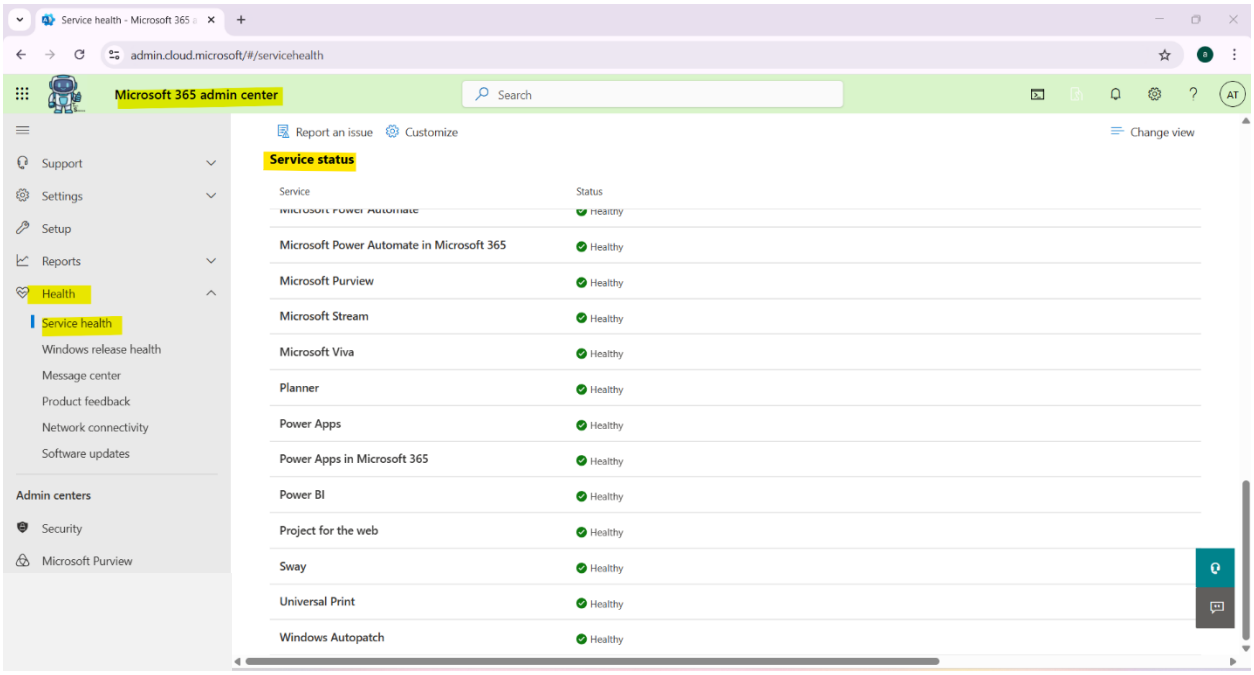


Email notifications were configured in the Service Health dashboard to notify Global Administrators and system administrators of service advisories across key Microsoft 365 workloads.

- Exchange Online
- Microsoft 365 apps
- Microsoft 365 for the web
- Microsoft Defender XDR
- Microsoft Entra
- Microsoft Intune
- Microsoft OneDrive
- Microsoft Power Automate in Microsoft 365
- Microsoft Purview
- Microsoft Teams
- Microsoft Viva
- SharePoint Online


Service health - Microsoft 365
admin.cloud.microsoft/#/servicehealth/:/currentIssues/Exchange%20Online
Microsoft 365 admin center
Search
Report an issue
Customize
Support
Settings
Setup
Reports
Health
Service health
Windows release health
Message center
Product feedback
Network connectivity
Software updates
Admin centers
Security
Microsoft Purview
Active issues Microsoft is working on
Issue title
Service status
Service
Status
Exchange Online
3 advisories
Microsoft 365 suite
1 advisory
Microsoft OneDrive
2 advisories
Microsoft Teams
1 advisory
SharePoint Online
3 advisories
Basic Mobility and Security
Healthy
Dynamics 365 Apps
Healthy
Microsoft 365 apps
Healthy
Health issues affecting Exchange Online
Issue Title
Issue Type
Users may be unable to delete a user from the contact list w...
Advisory
Some admins or users may be unable to access multiple Mic...
Advisory
Some users may be unable to access the My Templates and ...
Advisory
Some users may be unable to access the My Templates and Viva Insights Outlook add-ins in Exchange Online
Advisory


Service health - Microsoft 365
admin.cloud.microsoft/#/servicehealth
Microsoft 365 admin center
Search
Report an issue
Customize
Change view
Support
Settings
Setup
Reports
Health
Service health
Windows release health
Message center
Product feedback
Network connectivity
Software updates
Admin centers
Security
Service status
Service
Status
Microsoft 365 apps
Healthy
Microsoft 365 Copilot Chat
Healthy
Microsoft 365 for the web
Healthy
Microsoft Bookings
Healthy
Microsoft Clipchamp
Healthy
Microsoft Defender XDR
Healthy
Microsoft Entra
Healthy
Microsoft Forms
Healthy
Microsoft Intune
Healthy
Microsoft Power Automate
Healthy
Microsoft Power Automate in Microsoft 365
Healthy
Microsoft Purview
Healthy
Microsoft Stream
Healthy



Ongoing monitoring of the Microsoft 365 Service Health Dashboard was performed to track service availability and advisories. Several services (Exchange Online, OneDrive, SharePoint, Microsoft 365 Suite, and Teams) currently show “Advisory” status, indicating minor issues Microsoft is investigating. All other services are healthy. No critical incidents were found. The Service Health Dashboard is reviewed on an ongoing basis to ensure continued service stability and timely awareness of platform advisories.