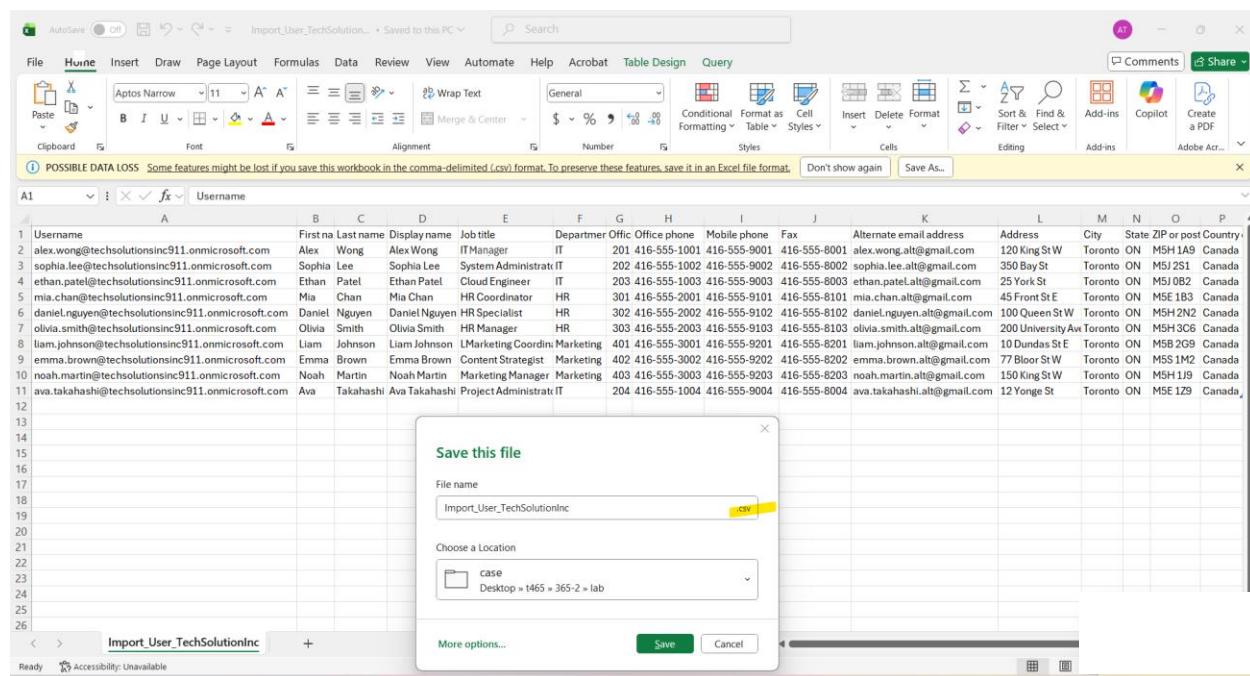


Microsoft 365 Enterprise Security and Operations Project Overview

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.



The screenshot shows a Microsoft Excel spreadsheet titled "Import_User_TechSolutionInc.csv". The spreadsheet contains 11 rows of user data, starting with headers: Username, First name, Last name, Display name, Job title, Department, Office phone, Mobile phone, Fax, Alternate email address, Address, City, State ZIP or post Country. The data includes various users like Alex Wong, Sophia Lee, Ethan Patel, etc., with their respective details such as phone numbers, emails, and addresses. A modal dialog box titled "Save this file" is overlaid on the spreadsheet, prompting the user to save the file with the name "Import_User_TechSolutionInc.csv" to the "Case" folder on the desktop. The dialog also includes "More options..." and "Save" and "Cancel" buttons.

1	Username	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
2	alex.wong@techsolutionsinc911.onmicrosoft.com	Alex	Wong	Alex Wong	IT Manager	IT	201	416-555-1001	416-555-9001	416-555-8001	alex.wong.alt@gmail.com	120 King St W	Toronto	ON	M5H 1A9	Canada
3	sophia.lee@techsolutionsinc911.onmicrosoft.com	Sophia	Lee	Sophia Lee	System Administrat	IT	202	416-555-1002	416-555-9002	416-555-8002	sophia.lee.alt@gmail.com	350 Bay St	Toronto	ON	M5J 2S1	Canada
4	ethan.patel@techsolutionsinc911.onmicrosoft.com	Ethan	Patel	Ethan Patel	Cloud Engineer	IT	202	416-555-1003	416-555-9003	416-555-8003	ethan.patel.alt@gmail.com	25 York St	Toronto	ON	M5J 0B2	Canada
5	mia.chan@techsolutionsinc911.onmicrosoft.com	Mia	Chan	Mia Chan	HR Coordinator	HR	301	416-555-2001	416-555-9101	416-555-8101	mia.chan.alt@gmail.com	45 Front St E	Toronto	ON	M5E 1B3	Canada
6	daniel.nguyen@techsolutionsinc911.onmicrosoft.com	Daniel	Nguyen	Daniel Nguyen	HR Specialist	HR	302	416-555-2002	416-555-9102	416-555-8102	daniel.nguyen.alt@gmail.com	100 Queen St W	Toronto	ON	M5H 2N2	Canada
7	olivia.smith@techsolutionsinc911.onmicrosoft.com	Olivia	Smith	Olivia Smith	HR Manager	HR	303	416-555-2003	416-555-9103	416-555-8103	olivia.smith.alt@gmail.com	200 University Av	Toronto	ON	M5H 3C6	Canada
8	liam.johnson@techsolutionsinc911.onmicrosoft.com	Liam	Johnson	Liam Johnson	Marketing Coordinat	Marketing	401	416-555-3001	416-555-9201	416-555-8201	liam.johnson.alt@gmail.com	10 Dundas St E	Toronto	ON	M5B 2G9	Canada
9	emma.brown@techsolutionsinc911.onmicrosoft.com	Emma	Brown	Emma Brown	Content Strategist	Marketing	402	416-555-3002	416-555-9202	416-555-8202	emma.brown.alt@gmail.com	77 Bloor St W	Toronto	ON	M5S 1M2	Canada
10	noah.martin@techsolutionsinc911.onmicrosoft.com	Noah	Martin	Noah Martin	Marketing Manager	Marketing	403	416-555-3003	416-555-9203	416-555-8203	noah.martin.alt@gmail.com	150 King St W	Toronto	ON	M5H 1J9	Canada
11	ava.takahashi@techsolutionsinc911.onmicrosoft.com	Ava	Takahashi	Ava Takahashi	Project Administrat	IT	204	416-555-1004	416-555-9004	416-555-8004	ava.takahashi.alt@gmail.com	12 Yonge St	Toronto	ON	M5E 1Z9	Canada
12																
13																
14																
15																
16																
17																
18																
19																
20																
21																
22																
23																
24																
25																
26																

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

Active users - Microsoft 365 admin center

Microsoft 365 admin center

Active users > Add multiple users

Basics

Licenses

Finish

First name | Last name | Username | @ TechSolutionsInc9...
First name | Last name | Username | @ TechSolutionsInc9...
First name | Last name | Username | @ TechSolutionsInc9...
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

This screenshot shows the 'Add multiple users' wizard in the Microsoft 365 Admin Center. The 'Basics' step is currently active. It displays four sets of input fields for first name, last name, username, and email domain, all pre-filled with 'TechSolutionsInc9...'. A checkbox for uploading a CSV file is checked. Below the input fields, there are links to download blank or example CSV files. At the bottom, there are 'Next' and 'Cancel' buttons.

Active users - Microsoft 365 admin center

Microsoft 365 admin center

Active users > Add multiple users

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

This screenshot shows the 'Add multiple users' wizard in the Microsoft 365 Admin Center. The 'Finish' step is currently active. It displays a table of 10 users, each with a green checkmark icon next to the 'Basics' and 'Licenses' steps. The table columns are 'Display name', 'Username', and 'Password Show'. The 'Password Show' column contains five asterisks ('*****'). At the bottom, there is a 'Close' button.

The screenshot shows the Microsoft 365 Admin Center interface. The left sidebar includes links for Home, Copilot, Agents, Users (Active users, Contacts, Guest users, Deleted users), Devices, Teams & groups, Marketplace, Billing, Setup, and Customize navigation. The main content area is titled "Microsoft 365 admin center" and shows a table of active users. The columns are "Display name" (sorted by ascending name), "Username", and "Licenses". There are 12 users listed, all of whom are Unlicensed. The users are: Alex Wong, Ava Takahashi, Ayuko Takahashi, Ayuko Takahashi1, Daniel Nguyen, Emma Brown, Ethan Patel, Liam Johnson, Mia Chan, Noah Martin, Olivia Smith, and Sophia Lee. Each user has a search icon and a more options icon (three dots) next to their name.

Display name	Username	Licenses
Alex Wong	alex.wong@techsolutionsinc911.onmicrosoft.com	Unlicensed
Ava Takahashi	ava.takahashi@techsolutionsinc911.onmicrosoft.com	Unlicensed
Ayuko Takahashi	AyukoTakahashi@TechSolutionsInc911.onmicrosoft.com	Microsoft 365 E5
Ayuko Takahashi1	AyukoTakahashi1@TechSolutionsInc911.onmicrosoft.com	Microsoft 365 E5
Daniel Nguyen	daniel.nguyen@techsolutionsinc911.onmicrosoft.com	Unlicensed
Emma Brown	emma.brown@techsolutionsinc911.onmicrosoft.com	Unlicensed
Ethan Patel	ethan.patel@techsolutionsinc911.onmicrosoft.com	Unlicensed
Liam Johnson	liam.johnson@techsolutionsinc911.onmicrosoft.com	Unlicensed
Mia Chan	mia.chan@techsolutionsinc911.onmicrosoft.com	Unlicensed
Noah Martin	noah.martin@techsolutionsinc911.onmicrosoft.com	Unlicensed
Olivia Smith	olivia.smith@techsolutionsinc911.onmicrosoft.com	Unlicensed
Sophia Lee	sophia.lee@techsolutionsinc911.onmicrosoft.com	Unlicensed

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

Display name	Username	Licenses
Alex Wong	alex.wong@techsolutionsinc911.onmicrosoft.com	Microsoft 365 E5
Ava Takahashi	ava.takahashi@techsolutionsinc911.onmicrosoft.com	Microsoft 365 E3
Ayuko Takahashi	ayukoTakahashi@TechSolutionsInc911.onmicrosoft.com	Microsoft 365 E5
Ayuko Takahashi1	AyukoTakahashi1@TechSolutionsInc911.onmicrosoft.com	Microsoft 365 E5
Daniel Nguyen	daniel.nguyen@techsolutionsinc911.onmicrosoft.com	Microsoft 365 E3
Emma Brown	emma.brown@techsolutionsinc911.onmicrosoft.com	Microsoft 365 E3
Ethan Patel	ethan.patel@techsolutionsinc911.onmicrosoft.com	Microsoft 365 E5
Liam Johnson	liam.johnson@techsolutionsinc911.onmicrosoft.com	Microsoft 365 E3
Mia Chan	mia.chan@techsolutionsinc911.onmicrosoft.com	Microsoft 365 E3
Noah Martin	noah.martin@techsolutionsinc911.onmicrosoft.com	Microsoft 365 E5
Olivia Smith	olivia.smith@techsolutionsinc911.onmicrosoft.com	Microsoft 365 E5
Sophia Lee	sophia.lee@techsolutionsinc911.onmicrosoft.com	Microsoft 365 E5

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

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with sections like Home, Entra agents, Favorites, and Entra ID. Under Entra ID, there are links for Overview, Users, Groups, Devices, Agent ID (Preview), Enterprise apps, App registrations, Roles & admins, Delegated admin partners, and Domain services. The main content area is titled 'Alex Wong' and shows the 'Overview' tab selected. It displays basic information such as User principal name (alex.wong@techsolutionsinc911.onmicrosoft.com), Object ID (f78dc884-61ff-4833-ae3b-03d6c1bc50f6), Created date time (Dec 6, 2025, 3:39 PM), User type (Member), and Identities (TechSolutionsInc911.onmicrosoft.com). There are also sections for My Feed, Account status (Enabled), and Sign-ins (Last interactive sign-in: ---, Last non-interactive sign-in: ---). A sidebar on the right provides links for Edit properties, Delete, Refresh, Reset password, Revoke sessions, Manage view, and Got feedback?

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

This screenshot shows the 'Properties' tab for the same user profile. The left sidebar remains the same. The main content area is titled 'Properties' and includes two main sections: 'Identity' and 'Contact Information'. The 'Identity' section lists details like Display name (Alex Wong), First name (Alex), Last name (Wong), User principal name (alex.wong@techsolutionsinc911.onmicrosoft.com), Object ID (f78dc884-61ff-4833-ae3b-03d6c1bc50f6), Identities (TechSolutionsInc911.onmicrosoft.com), User type (Member), Creation type, Created date time (Dec 6, 2025, 3:39 PM), Assigned licenses (View), Preferred language, Sign in sessions valid from date (Dec 6, 2025, 3:39 PM), Last password change date time (Dec 6, 2025, 3:39 PM), and Invitation state. The 'Contact Information' section lists Street address (120 King St W), City (Toronto), State or province (ON), ZIP or postal code (M5H 1A9), Country or region (Canada), Business phone (416-555-1001), Mobile phone (416-555-9001), Email (alex.wong@techsolutionsinc911.onmicrosoft.com), Other emails (View), Proxy addresses (View), Fax number (416-555-8001), IM addresses (View), and Mail nickname (alex.wong). A 'Parental controls' section is also present at the bottom.

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

The screenshot shows the Microsoft Entra admin center interface. On the left, the navigation menu includes Home, Entra agents, Favorites (with Entra ID selected), Overview, Users, Groups, Devices, Agent ID (Preview), Enterprise apps, App registrations, Roles & admins, Delegated admin partners, and Domain services. The main area displays the user profile for "Alex Wong". The "Overview" tab is selected. The "Job Information" section shows the following details:

Job title	IT Manager
Company name	TechSolutions Inc
Department	IT
Employee ID	200001
Employee type	Permanent - Full time
Employee hire date	Jan 12, 2021, 12:00 AM
Employee org data	
Office location	201
Azure role assignments	Manager
Authentication methods	Alex Wong
Sponsors	

The "Settings" section shows the following configuration:

Account enabled	Yes
Usage location	Canada
Preferred data location	
On-premises	
On-premises sync enabled	No
On-premises last sync date time	
On-premises distinguished name	
Extension attributes	
On-premises immutable ID	
On-premises provisioning errors	
On-premises SAM account name	
On-premises security identifier	
On-premises user principal name	
On-premises domain name	

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

The screenshot shows the Microsoft Entra admin center interface. The navigation menu is identical to the previous screenshot. The main area displays the user profile for "Ava Takahashi". The "Overview" tab is selected. The "Basic info" section shows the following details:

User principal name	ava.takahashi@techsolutionsinc911.onmicrosoft.com
Object ID	0132828d-9dd8-4737-90de-382368184f4c
Created date time	Dec 6, 2025, 3:39 PM
User type	Member
Identities	TechSolutionsInc911.onmicrosoft.com

The "My Feed" section shows account status and sign-in activity:

Account status	Enabled
Sign-ins	Last interactive sign-in: --- Last non-interactive sign-in: ---

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

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with sections like Home, Entra agents, Favorites, and Entra ID (Overview, Users, Groups, Devices, Agent ID (Preview), Enterprise apps, App registrations, Roles & admins, Delegated admin partners, Domain services). The main area is titled 'Ava Takahashi' and shows the 'Properties' tab selected under 'Overview'. It displays various user details such as Display name (Ava Takahashi), First name (Ava), Last name (Takahashi), User principal name (ava.takahashi@techsolutionsinc911.onmicrosoft.com), Object ID (0132828d-9dd8-4737-90de-382368184f4c), Identities (TechSolutionsInc911.onmicrosoft.com), User type (Member), and Creation type (Azure AD). It also shows contact information like Street address (12 Yonge St), City (Toronto), State or province (ON), ZIP or postal code (M5E 1Z9), Country or region (Canada), Business phone (416-555-1004), Mobile phone (416-555-9004), Email (ava.takahashi@techsolutionsinc911.onmicrosoft.com), Other emails (View), Proxy addresses (View), Fax number (416-555-8004), IM addresses (View), Mail nickname (ava.takahashi), and Parental controls.

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

The screenshot shows the Microsoft Entra admin center interface. The left sidebar is identical to the previous one. The main area is titled 'Ava Takahashi' and shows the 'Job Information' tab selected under 'Overview'. It displays job details like Job title (Project Administrator), Company name (TechSolutions Inc), Department (IT), Employee ID (200004), Employee type (Permanent - Full time), Employee hire date (Apr 2, 2018, 12:00 AM), Employee org data (Office location 204 Manager Alex Wong Sponsors), and usage location set to Canada. Other tabs visible include Password profile, Authorization info, Settings, and On-premises.

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

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with sections like Home, Entra agents, Favorites (with Overview, Users, Groups, Devices, Agent ID (Preview), Enterprise apps, App registrations, Roles & admins, Delegated admin partners, and Domain services), and Entra ID (with Overview, Audit logs, Sign-in logs, Diagnose and solve problems, Custom security attributes, Assigned roles, Administrative units, Groups, Applications, Licenses, Devices, Azure role assignments, Authentication methods, and New support request). The main content area is titled "Daniel Nguyen" and shows the "Overview" tab selected. It displays basic info such as User principal name (daniel.nguyen@techsolutionsinc911.onmicrosoft.com), Object ID (86f7ae0f-9dce-4bc4-a429-ef941cd8913b), Created date time (Dec 6, 2025, 3:39 PM), User type (Member), and Identities (TechSolutionsInc911.onmicrosoft.com). It also shows account status (Enabled) and sign-in information (Last interactive sign-in: ---, Last non-interactive sign-in: ---). There are tabs for Overview, Monitoring, and Properties.

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

This screenshot shows the "Properties" tab for Daniel Nguyen in the Microsoft Entra admin center. The left sidebar is identical to the previous screenshot. The main content area is titled "Daniel Nguyen" and shows the "Properties" tab selected. It is divided into two columns: "Identity" and "Contact Information". The "Identity" column includes fields for Display name (Daniel Nguyen), First name (Daniel), Last name (Nguyen), User principal name (daniel.nguyen@techsolutionsinc911....), Object ID (86f7ae0f-9dce-4bc4-a429-ef941cd8913b), Identities (TechSolutionsInc911.onmicrosoft.com), User type (Member), Creation type, Created date time (Dec 6, 2025, 3:39 PM), Assigned licenses (View), Preferred language, Sign in sessions valid from date t..., Last password change date time (Dec 6, 2025, 3:39 PM), Invitation state, and External user state change date t... The "Contact Information" column includes fields for Street address (100 Queen St W), City (Toronto), State or province (ON), ZIP or postal code (M5H 2N2), Country or region (Canada), Business phone (416-555-2002), Mobile phone (416-555-9102), Email (daniel.nguyen@techsolutionsinc911....), Other emails (View), Proxy addresses (View), Fax number (416-555-8102), IM addresses (View), Mail nickname (daniel.nguyen), and Parental controls (View). There are tabs for Overview, Monitoring, and Properties.

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

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with various options like Home, Entra agents, Favorites (with Entra ID), Overview, Users, Groups, Devices, Agent ID (Preview), Enterprise apps, App registrations, Roles & admins, Delegated admin partners, and Domain services. The main area is titled "Daniel Nguyen" and shows the "Overview" tab selected. It displays basic user information such as job title (HR Specialist), company name (TechSolutions Inc), department (HR), employee ID (300002), employee type (Contract - Full time), hire date (Jun 23, 2025, 12:00 AM), office location (302), manager (Olivia Smith), and sponsors. There are also sections for "Job Information" and "Settings". Under "Settings", the "Usage location" is highlighted and set to "Canada". Other settings include account enabled (Yes), preferred data location, and various on-premises and extension attributes.

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

The screenshot shows the Microsoft Entra admin center interface, similar to the previous one but for a different user. The navigation sidebar is identical. The main area is titled "Emma Brown" and shows the "Overview" tab selected. It displays basic user information such as user principal name (emma.brown@techsolutionsinc911.onmicrosoft.com), object ID (2eb33dae-7887-4f08-9fcc-fe66064de69b), created date time (Dec 6, 2025, 3:39 PM), user type (Member), identities (TechSolutionsinc911.onmicrosoft.com), and group memberships (1). There are also sections for "My Feed", "Account status" (Enabled), and "Sign-ins" (Last interactive sign-in: -- --, Last non-interactive sign-in: -- --).

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

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with sections like Home, Entra agents, Favorites, and Entra ID (Overview, Users, Groups, Devices, Agent ID (Preview), Enterprise apps, App registrations, Roles & admins, Delegated admin partners, and Domain controllers). The main area is titled 'Emma Brown' under 'User'. It has tabs for Overview, Monitoring, and Properties. The Properties tab is active, showing detailed information in three columns:

	Identity	Contact Information
Display name	Emma Brown	Street address 77 Bloor St W
First name	Emma	City Toronto
Last name	Brown	State or province ON
User principal name	emma.brown@techsolutionsinc911.onmicrosoft.com	ZIP or postal code M5S 1M2
Object ID	2eb33dae-7887-4f08-9fcc-fe66064de69b	Country or region Canada
Groups	Object ID	Business phone 416-555-3002
Applications	Identities	Mobile phone 416-555-9202
Licenses	User type	Email emma.brown@techsolutionsinc911.onmicrosoft.com
Devices	Creation type	Other emails View
Azure role assignments	Created date time	Proxy addresses View
Authentication methods	Assigned licenses	Fax number 416-555-8202
New support request	Preferred language	IM addresses View
	Sign in sessions valid from date to...	Mail nickname emma.brown
	Last password change date time	Invitation state External user state change date ti...
		Parental controls View

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

This screenshot shows the same Microsoft Entra admin center interface as the previous one, but the 'Properties' tab is not selected. Instead, the 'Job Information' tab is active. The main area is titled 'Emma Brown' under 'User'. It has tabs for Overview, Password profile, Authorization info, Job Information, Settings, and On-premises. The Job Information tab is active, showing details in three columns:

	Job Information	Settings
Job title	Content Strategist	Consent provided for minor
Company name	TechSolutions Inc	Legal age group classification
Department	Marketing	
Employee ID	400002	Account enabled Yes
Employee type	Contract - Full-time	Usage location Canada
Employee hire date	Jul 14, 2025, 12:00 AM	Preferred data location
Employee org data		On-premises
Office location	402	On-premises sync enabled No
Manager	Noah Martin	On-premises last sync date time
Sponsors		On-premises distinguished name
		Extension attributes
		On-premises immutable ID
		On-premises provisioning errors
		On-premises SAM account name
		On-premises security identifier
		On-premises user principal name
		On-premises domain name

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

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with categories like Home, Entra agents, Favorites, Entra ID, Overview, Users, Groups, Devices, Agent ID (Preview), Enterprise apps, App registrations, Roles & admins, Delegated admin partners, and Domain services. The main area is titled "Ethan Patel" and shows the "Overview" tab selected. It displays basic user information: User principal name (ethan.patel@techsolutionsinc911.onmicrosoft.com), Object ID (a3303ef4-4817-45ba-aaf0-18c330259c3d), Created date time (Dec 6, 2025, 3:39 PM), User type (Member), and Identities (TechSolutionsInc911.onmicrosoft.com). There are also sections for My Feed, Account status (Enabled), and Sign-ins (Last interactive sign-in: ---, Last non-interactive sign-in: ---).

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

This screenshot shows the "Properties" tab for Ethan Patel. The left sidebar remains the same. The main area is titled "Ethan Patel" and shows the "Properties" tab selected. It lists various contact and administrative details under two main sections: "Identity" and "Contact Information".

Section	Details	Value
Identity	Display name	Ethan Patel
	First name	Ethan
	Last name	Patel
	User principal name	ethan.patel@techsolutionsinc911.on...
	Object ID	a3303ef4-4817-45ba-aaf0-18c330259c3d
Contact Information	Street address	25 York St
	City	Toronto
	State or province	ON
	ZIP or postal code	M5J 0B2
	Country or region	Canada
General	Business phone	416-555-1003
	Mobile phone	416-555-9003
	Email	ethan.patel@techsolutionsinc911.on...
	Other emails	View
	Proxy addresses	View
Administrative	Fax number	416-555-8003
	IM addresses	View
	Mail nickname	ethan.patel
	Invitation state	
	External user state change date ti...	

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

The screenshot shows the Microsoft Entra admin center interface. On the left, the navigation menu includes Home, Entra agents, Favorites (Overview, Entra ID, Users, Groups, Devices, Agent ID (Preview), Enterprise apps, App registrations, Roles & admins, Delegated admin partners, Domain services), and a search bar. The main area displays the user profile for Ethan Patel. The 'Overview' tab is selected. The user's details are shown in the 'Job Information' section:

Job title	Cloud Engineer
Company name	TechSolutions Inc
Department	IT
Employee ID	200003
Employee type	Permanent - Full-time
Employee hire date	Aug 12, 2024, 12:00 AM
Employee org data	
Office location	203
Manager	Alex Wong
Sponsors	

Other tabs include Password profile, Authorization info, and Settings. The 'Usage location' field is highlighted in yellow and set to Canada. The 'On-premises' section shows various attributes like sync status and immutable ID.

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

The screenshot shows the Microsoft Entra admin center interface. The navigation menu is identical to the previous screenshot. The main area displays the user profile for Liam Johnson. The 'Overview' tab is selected. The user's details are shown in the 'Basic info' section:

User principal name	liam.johnson@techsolutionsinc911.onmicrosoft.com	Group memberships	1
Object ID	90ac0464-715e-4a89-a91e-8a12f527427a	Applications	0
Created date time	Dec 6, 2025, 3:39 PM	Assigned roles	0
User type	Member	Assigned licenses	1
Identities	TechSolutionsInc911.onmicrosoft.com		

Below the basic info, there are sections for My Feed, Account status (Enabled), and Sign-ins (Last interactive sign-in: ---, Last non-interactive sign-in: ---).

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

Liam Johnson - Microsoft Entra

Microsoft Entra admin center

Home > Users > Liam Johnson

Properties tab selected.

	Identity	Contact Information
Display name	Liam Johnson	Street address 10 Dundas St E
First name	Liam	City Toronto
Last name	Johnson	State or province ON
User principal name	liam.johnson@techsolutionsinc911.onmicrosoft.com	ZIP or postal code MSB 2G9
Object ID	90ac0464-715e-4a89-a91e-8a12f527427a	Country or region Canada
Groups	TechSolutionsInc911.onmicrosoft.com	Business phone 416-555-3001
Applications		Mobile phone 416-555-9201
Licenses		Email liam.johnson@techsolutionsinc911.onmicrosoft.com
Devices		Other emails View
Azure role assignments	Created date time Dec 6, 2025, 3:39 PM	Proxy addresses View
Authentication methods	Assigned licenses View	Fax number 416-555-8201
New support request	Preferred language	IM addresses View
	Sign in sessions valid from date to... Dec 6, 2025, 3:39 PM	Mail nickname liam.johnson
	Last password change date time Dec 6, 2025, 3:39 PM	
	Invitation state	Parental controls

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

Liam Johnson - Microsoft Entra

Microsoft Entra admin center

Home > Users > Liam Johnson

Job Information tab selected.

	Job Information	Settings
Job title	LMarketing Coordinator	Consent provided for minor Legal age group classification
Company name	TechSolutions Inc	Account enabled Yes
Department	Marketing	Usage location Canada
Employee ID	400001	Preferred data location
Employee type	Permanent - Full time	On-premises
Employee hire date	Oct 4, 2021, 12:00 AM	On-premises sync enabled No
Employee org data		On-premises last sync date time
Office location	401	On-premises distinguished name
Manager	Noah Martin	Extension attributes
Sponsors		On-premises immutable ID
		On-premises provisioning errors
		On-premises SAM account name
		On-premises security identifier
		On-premises user principal name
		On-premises domain name

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

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with sections like Home, Entra agents, Favorites, Entra ID (Overview, Users, Groups, Devices, Agent ID (Preview), Enterprise apps, App registrations, Roles & admins, Delegated admin partners, Domain services), and Copilot. The main area is titled "Mia Chan" and shows the "Overview" tab selected. It displays basic user information: User principal name (mia.chan@techsolutionsinc911.onmicrosoft.com), Object ID (88049524-27c0-4cfb-b268-2992e28af19f), Created date time (Dec 6, 2025, 3:39 PM), User type (Member), and Identities (TechSolutionsInc911.onmicrosoft.com). It also shows account status (Enabled) and sign-in activity (Last interactive sign-in: ---, Last non-interactive sign-in: ---). Other tabs include Monitoring and Properties.

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

This screenshot shows the "Properties" tab for Mia Chan. The left sidebar is identical to the previous screenshot. The main area is titled "Mia Chan" and shows the "Properties" tab selected. It is divided into two columns: "Identity" and "Contact Information". The "Identity" column includes fields for Display name (Mia Chan), First name (Mia), Last name (Chan), User principal name (mia.chan@techsolutionsinc911.onmicrosoft.com), Object ID (88049524-27c0-4cfb-b268-2992e28af19f), Identities (TechSolutionsInc911.onmicrosoft.com), User type (Member), Creation type, Created date time (Dec 6, 2025, 3:39 PM), Assigned licenses (View), Preferred language, Sign in sessions valid from date time (Dec 6, 2025, 3:39 PM), Last password change date time (Dec 6, 2025, 3:39 PM), Invitation state, and External user state change date time. The "Contact Information" column includes fields for Street address (45 Front St E), City (Toronto), State or province (ON), ZIP or postal code (M5E 1B3), Country or region (Canada), Business phone (416-555-2001), Mobile phone (416-555-9101), Email (mia.chan@techsolutionsinc911.onmicrosoft.com), Other emails (View), Proxy addresses (View), Fax number (416-555-8101), IM addresses (View), Mail nickname (mia.chan), and Parental controls (View). A "Copilot" button is visible at the top right of the main content area.

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

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with various options like Home, Entra agents, Favorites, Entra ID, Overview, Users, Groups, Devices, Agent ID (Preview), Enterprise apps, App registrations, Roles & admins, Delegated admin partners, and Domain services. The main area is titled 'Mia Chan' and shows her user profile. The 'Overview' tab is selected. The 'Job Information' section is highlighted with a yellow box. It contains fields such as Job title (HR Coordinator), Company name (TechSolutions Inc), Department (HR), Employee ID (300001), Employee type (Permanent - Part-time), Employee hire date (Sep 20, 2021, 12:00 AM), Employee org data (Office location 301, Manager Olivia Smith, Sponsors), and Usage location (Canada). Other tabs like Audit logs, Sign-in logs, Diagnose and solve problems, Custom security attributes, Assigned roles, Administrative units, Groups, Applications, Licenses, Devices, Azure role assignments, Authentication methods, and New support request are also visible.

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

The screenshot shows the Microsoft Entra admin center interface. The navigation sidebar is identical to the previous one. The main area is titled 'Noah Martin' and shows his user profile. The 'Overview' tab is selected. The 'Basic info' section is highlighted with a yellow box. It includes a profile picture of Noah Martin, his email (noah.martin@techsolutionsinc911.onmicrosoft.com), and his status (Member). Other tabs like Monitoring and Properties are available. Below the basic info, there are sections for User principal name, Object ID, Created date time, User type, Identities, Account status (Enabled), and Sign-ins (Last interactive sign-in: -- --, Last non-interactive sign-in: -- --). The sidebar on the left lists the same categories as the first screenshot.

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

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with sections like Home, Entra agents, Favorites, and Entra ID. Under Entra ID, there are options for Overview, Users, Groups, Devices, Agent ID (Preview), Enterprise apps, App registrations, Roles & admins, Delegated admin partners, and Domain services. The main area displays user details for 'Noah Martin'. The 'Overview' tab is selected. The user's name is Noah Martin. The 'Properties' tab is also visible. The 'Identity' section contains fields like Display name, First name, Last name, User principal name, Object ID, Identities, User type, Creation type, Created date time, Assigned licenses, Preferred language, Sign in sessions valid from date, Last password change date time, and Invitation state. The 'Contact Information' section includes Street address, City, State or province, ZIP or postal code, Country or region, Business phone, Mobile phone, Email, Other emails, Proxy addresses, Fax number, IM addresses, Mail nickname, and Parental controls. A note at the bottom says 'External user state change date t...'. The top right corner shows the user's email (AyukoTakahashi@TechS...), the company name (TECHSOLUTIONS INC (TECHSOL...)), and a Copilot icon.

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

The screenshot shows the Microsoft Entra admin center interface, similar to the previous one but with different tabs selected. The 'Job Information' tab is highlighted. The user's name is Noah Martin. The 'Job Information' section contains fields like Job title (Marketing Manager), Company name (TechSolutions Inc), Department (Marketing), Employee ID (400003), Employee type (Permanent - Full time), Employee hire date (May 6, 2019, 12:00 AM), Employee org data (Noah Martin), Office location (403), Manager (Noah Martin), and Sponsors. The 'Settings' section includes fields like Consent provided for minor, Legal age group classification, Account enabled (Yes), Usage location (Canada), Preferred data location, On-premises sync enabled (No), On-premises last sync date time, On-premises distinguished name, Extension attributes, On-premises immutable ID, On-premises provisioning errors, On-premises SAM account name, On-premises security identifier, On-premises user principal name, and On-premises domain name. The top right corner shows the user's email (AyukoTakahashi@TechS...), the company name (TECHSOLUTIONS INC (TECHSOL...)), and a 'Finish update' button.

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

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with sections like Home, Entra agents, Favorites, Entra ID (Overview, Users, Groups, Devices, Agent ID (Preview), Enterprise apps, App registrations, Roles & admins, Delegated admin partners, Domain services), and Copilot. The main area is titled 'Olivia Smith' and shows the 'Overview' tab selected. It displays basic info such as User principal name (olivia.smith@techsolutionsinc911.onmicrosoft.com), Object ID (72179a01-d089-4661-8916-eb34ecebaa67), Created date time (Dec 6, 2025, 3:39 PM), User type (Member), and Identities (TechSolutionsInc911.onmicrosoft.com). There are also sections for My Feed, Account status (Enabled), and Sign-ins (Last interactive sign-in: ---, Last non-interactive sign-in: ---).

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

This screenshot shows the 'Properties' tab for Olivia Smith. The left sidebar is identical to the previous screenshot. The main area is titled 'Olivia Smith' and shows the 'Properties' tab selected. It is divided into two columns: 'Identity' and 'Contact Information'. The 'Identity' column includes fields like Display name (Olivia Smith), First name (Olivia), Last name (Smith), User principal name (olivia.smith@techsolutionsinc911.on...), Object ID (72179a01-d089-4661-8916-eb34ecebaa67), Identities (TechSolutionsInc911.onmicrosoft.com), User type (Member), Creation type, Created date time (Dec 6, 2025, 3:39 PM), Assigned licenses (View), Preferred language, Sign in sessions valid from date t..., Last password change date time (Dec 6, 2025, 3:39 PM), Invitation state, and External user state change date t... . The 'Contact Information' column includes fields like Street address (200 University Ave), City (Toronto), State or province (ON), ZIP or postal code (M5H 3C6), Country or region (Canada), Business phone (416-555-2003), Mobile phone (416-555-9103), Email (olivia.smith@techsolutionsinc911.on...), Other emails (View), Proxy addresses (View), Fax number (416-555-8103), IM addresses (View), Mail nickname (olivia.smith), and Parental controls (View).

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

The screenshot shows the Microsoft Entra admin center interface. On the left, the navigation menu includes Home, Entra agents, Favorites (with Entra ID selected), Overview, Users, Groups, Devices, Agent ID (Preview), Enterprise apps, App registrations, Roles & admins, Delegated admin partners, and Domain services. The main pane displays the user profile for Olivia Smith. The 'Overview' tab is selected. The 'Job Information' section is highlighted. Key details shown include:

Job title	HR Manager
Company name	TechSolutions Inc
Department	HR
Employee ID	300003
Employee type	Permanent - Full time
Employee hire date	Mar 7, 2022, 12:00 AM
Employee org data	
Office location	303
Azure role assignments	Manager
Authentication methods	Sponsors

The 'Usage location' field is set to Canada. Other settings like Account enabled (Yes) and On-premises sync enabled (No) are also visible.

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

The screenshot shows the Microsoft Entra admin center interface. The navigation menu is identical to the previous screenshot. The main pane displays the user profile for Sophia Lee. The 'Overview' tab is selected. The 'Basic info' section shows:

User principal name	sophia.lee@techsolutionsinc911.onmicrosoft.com
Object ID	faf5d9f2-49d1-410e-b998-cde475653049
Created date time	Dec 6, 2025, 3:39 PM
User type	Member
Identities	TechSolutionsInc911.onmicrosoft.com

Below the basic info, there are sections for My Feed, Account status (Enabled), and Sign-ins (Last interactive sign-in: ---, Last non-interactive sign-in: ---).

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

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a navigation sidebar with sections like Home, Entra agents, Favorites, and Entra ID (Overview, Users, Groups, Devices, Agent ID (Preview), Enterprise apps, App registrations, Roles & admins, Delegated admin partners, Domain services). The main area is titled "Sophia Lee" and shows the "Properties" tab selected under "Overview". The "Identity" section lists details such as Display name (Sophia Lee), First name (Sophia), Last name (Lee), User principal name (sophia.lee@techsolutionsinc911.onmicrosoft.com), Object ID (faf5d9f2-49d1-410e-b998-cde475653049), Identities (TechSolutionsInc911.onmicrosoft.com), User type (Member), Creation type (Normal), Creation date time (Dec 6, 2025, 3:39 PM), and Preferred language (English). The "Contact Information" section includes Street address (350 Bay St), City (Toronto), State or province (ON), ZIP or postal code (M5J 2S1), Country or region (Canada), Business phone (416-555-1002), Mobile phone (416-555-9002), Email (sophia.lee@techsolutionsinc911.onmicrosoft.com), Other emails (View), Proxy addresses (View), Fax number (416-555-8002), IM addresses (View), Mail nickname (sophia.lee), and Parental controls (Edit).

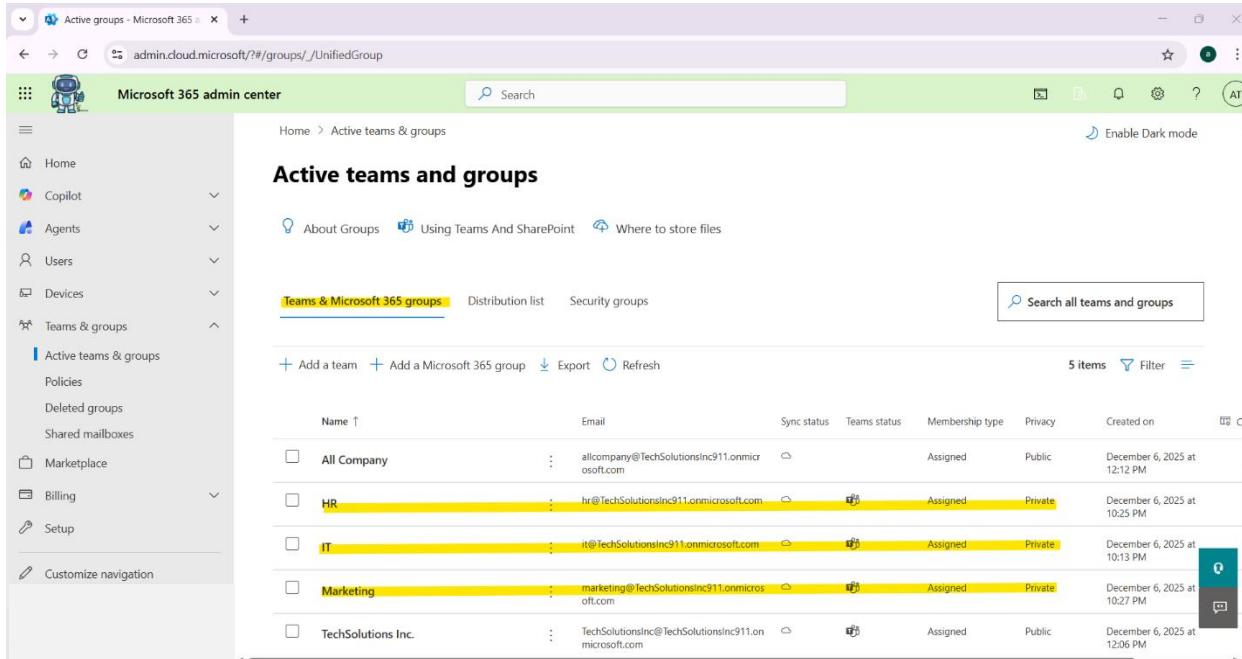
Contact information for Sophia Lee, including office phone, mobile phone, and full mailing address.

This screenshot shows the same Microsoft Entra admin center interface as the previous one, but with the "Job Information" tab selected under "Properties". The "Job Information" section displays details such as Job title (System Administrator), Company name (TechSolutions Inc), Department (IT), Employee ID (200002), Employee type (Permanent - Full-time), Employee hire date (Jul 21, 2025, 12:00 AM), Employee org data (Office location 202 Manager Alex Wong Sponsors), and Usage location (Canada). Other tabs visible include "Overview", "Audit logs", "Sign-in logs", "Diagnose and solve problems", "Custom security attributes", "Assigned roles", "Administrative units", "Groups", "Applications", "Licenses", "Devices", "Azure role assignments", "Authentication methods", and "New support request". The "Settings" section on the right shows Account enabled (Yes), Consent provided for minor, Legal age group classification, and various usage and sync settings.

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

Group, Permission, and Collaboration Governance

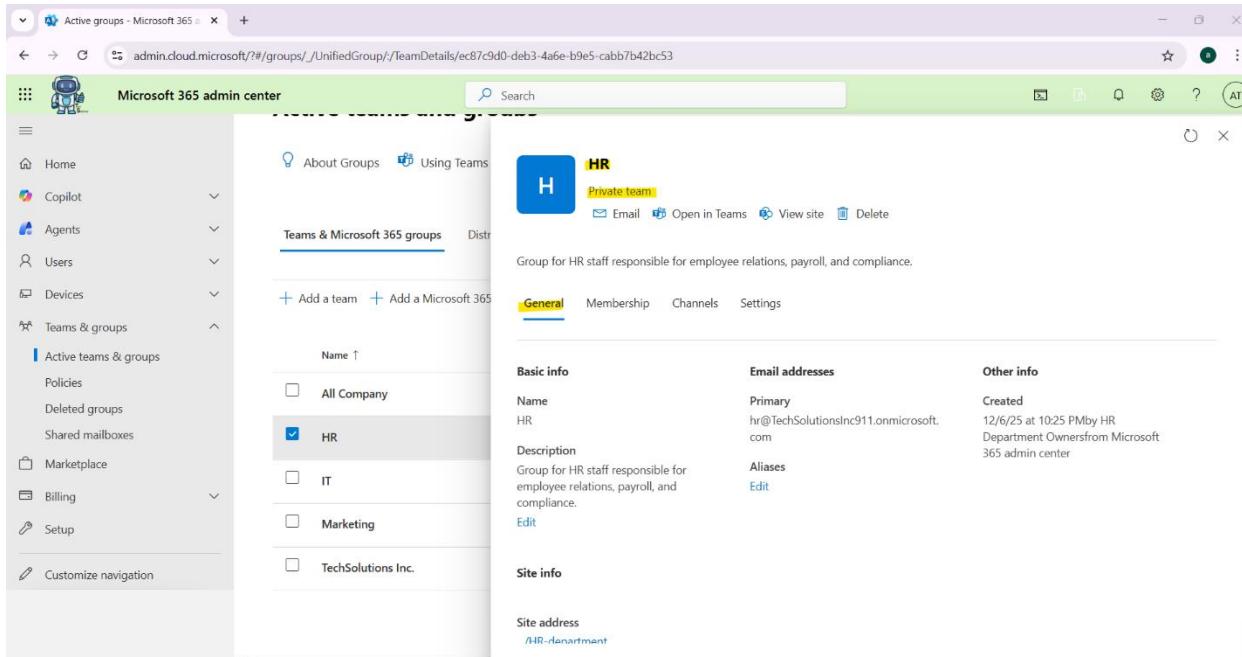
This section demonstrates the creation and governance of Microsoft 365 groups and permissions to support secure departmental collaboration across Teams, SharePoint, and related services.



The screenshot shows the Microsoft 365 Admin Center interface. The left sidebar is collapsed, and the main content area is titled "Active teams and groups". At the top of the main area, there are three tabs: "Teams & Microsoft 365 groups" (which is selected), "Distribution list", and "Security groups". Below the tabs, there are buttons for "Add a team", "Add a Microsoft 365 group", "Export", and "Refresh". A search bar labeled "Search all teams and groups" is located on the right. The main table displays five items, each representing a Microsoft 365 group. The columns include Name, Email, Sync status, Teams status, Membership type, Privacy, and Created on. The "HR" group is highlighted with yellow background and blue text. The table has a header row with filters and sorting options.

Name	Email	Sync status	Teams status	Membership type	Privacy	Created on
All Company	allcompany@TechSolutionsInc911.onmicrosoft.com	Synced	Active	Assigned	Public	December 6, 2025 at 12:12 PM
HR	hr@TechSolutionsInc911.onmicrosoft.com	Synced	Active	Assigned	Private	December 6, 2025 at 10:25 PM
IT	it@TechSolutionsInc911.onmicrosoft.com	Synced	Active	Assigned	Private	December 6, 2025 at 10:13 PM
Marketing	marketing@TechSolutionsInc911.onmicrosoft.com	Synced	Active	Assigned	Private	December 6, 2025 at 10:27 PM
TechSolutions Inc.	TechSolutionsInc@TechSolutionsInc911.onmicrosoft.com	Synced	Active	Assigned	Public	December 6, 2025 at 12:06 PM

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



The screenshot shows the Microsoft 365 Admin Center interface, specifically the "TeamDetails" view for the "HR" group. The left sidebar is collapsed. The main content area shows the "General" tab selected. At the top, there is a large blue square icon with a white letter "H" and the text "HR Private team". Below this, there are buttons for "Email", "Open in Teams", "View site", and "Delete". The main content area contains information about the group, including its name, description, and various settings tabs like General, Membership, Channels, and Settings. The "HR" group is selected in the list on the left. The "Basic info" section shows the group's name, email addresses (Primary: hr@TechSolutionsInc911.onmicrosoft.com), and other info such as created date (12/6/25 at 10:25 PM) and department (Owners from Microsoft 365 admin center). The "Site info" section shows the site address as "/HR-department".

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

The screenshot shows the Microsoft 365 admin center interface. On the left, there's a navigation sidebar with various options like Home, Copilot, Agents, Users, Devices, and Teams & groups. Under 'Teams & groups', 'Active teams & groups' is selected, showing 'HR' as the active team. The main content area displays the 'HR' team details, which is described as a 'Private team' for HR staff responsible for employee relations, payroll, and compliance. The 'Membership' tab is currently selected. In the 'Owners' section, there are two entries: 'All Company' and 'HR'. Under 'HR', 'Ayuko.Takahashi' and 'Ayuko.Takahashi1' are listed as owners. A search bar at the top right allows searching for all members.

Owners of the HR group, including two Global Admins.

This screenshot shows the same Microsoft 365 admin center interface as the previous one, but with a different focus. The 'Members' section is now highlighted. It lists three members: 'Daniel Nguyen' (DN), 'Mia Chan' (MC), and 'Olivia Smith' (OS). Each member is represented by a small profile icon and their name. The rest of the page content remains the same, including the team description and the 'Owners' section.

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

The screenshot shows the Microsoft 365 admin center interface. On the left, there's a navigation sidebar with options like Home, Copilot, Agents, Users, Devices, and Teams & groups. Under Teams & groups, 'Active teams & groups' is selected, showing a list of existing groups: All Company, HR, IT (which is checked), Marketing, and TechSolutions Inc. The main content area displays the 'IT' group details. It's a 'Private team' for IT staff. The 'General' tab is selected, showing the group name 'IT', a description 'Group for IT staff including admins and support personnel.', and a site address '_/IT-department C-AT'. The 'Email addresses' section lists 'Primary' as 'it@TechSolutionsInc911.onmicrosoft.com' and 'Aliases' as 'Edit'. The 'Other info' section shows it was created on '12/6/25 at 10:13 PM by IT Department Owners from Microsoft 365 admin center'. Other tabs include Membership, Channels, and Settings.

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

This screenshot shows the 'Membership' tab for the IT group. The 'Owners' section is highlighted. It lists two owners: Ayuko.Takahashi (email: AyukoTakahashi@TechSolutionsInc911.onmicrosoft.com) and Ayuko.Takahashi1 (email: AyukoTakahashi1@TechSolutionsInc911.onmicrosoft.com). There are buttons to '+ Add owners' and 'Search all membershi...'. The 'Members' section is also visible. The left sidebar remains the same as the previous screenshot.

Owners of the IT group, including two Global Admins.

The screenshot shows the Microsoft 365 admin center interface. On the left, there's a navigation sidebar with options like Home, Copilot, Agents, Users, Devices, and Teams & groups. Under Teams & groups, 'Active teams & groups' is selected, showing a list of groups: All Company, HR, IT (which is checked), Marketing, and TechSolutions Inc. The main content area displays the 'IT' group details. It shows a blue square icon with a white 'I', the name 'IT', and the description 'Private team'. Below this, it says 'Group for IT staff including admins and support personnel.' There are tabs for General, Membership (which is selected), Channels, and Settings. The Membership tab shows a table with columns for Name, Email address, and a search bar. It lists four members: Alex Wong (alex.wong@techsolutionsinc911.onmicrosoft.com), Ava Takahashi (ava.takahashi@techsolutionsinc911.onmicrosoft.com), Ethan Patel (ethan.patel@techsolutionsinc911.onmicrosoft.com), and Sophia Lee (sophia.lee@techsolutionsinc911.onmicrosoft.com). Each member has a small profile picture and their email address.

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

The screenshot shows the Microsoft 365 admin center interface, similar to the previous one but for the Marketing group. The navigation sidebar is identical. In the 'Active teams & groups' section, 'Marketing' is selected. The main content area displays the 'Marketing' group details. It shows a blue square icon with a white 'M', the name 'Marketing', and the description 'Private team'. Below this, it says 'Group for the marketing team responsible for branding, content, and campaigns.' There are tabs for General, Membership (selected), Channels, and Settings. The General tab shows a table with columns for Basic info, Email addresses, and Other info. Under Basic info, it shows the Name 'Marketing', Description 'Group for the marketing team responsible for branding, content, and campaigns.', and a 'Edit' link. Under Email addresses, it shows 'Primary' email as 'marketing@TechSolutionsInc911.onmicrosoft.com'. Under Other info, it shows 'Created' as '12/6/25 at 10:27 PM by Marketing Department Owners from Microsoft 365 admin center'. There are also sections for Site info and Site address.

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

The screenshot shows the Microsoft 365 admin center interface. On the left, there's a navigation sidebar with various options like Home, Copilot, Agents, Users, Devices, and Teams & groups. Under Teams & groups, 'Active teams & groups' is selected, showing options for All Company, HR, IT, Marketing, and TechSolutions Inc. The main content area is titled 'Marketing' and describes it as a 'Private team'. It has tabs for General, Membership (which is selected), Channels, and Settings. The Membership tab shows two owners: Ayuko.Takahashi (email: Ayuko.Takahashi@TechSolutionsInc911.onmicrosoft.com) and Ayuko.Takahashi1 (email: Ayuko.Takahashi1@TechSolutionsInc911.onmicrosoft.com). There's also a search bar for members.

Owners of the Marketing group, including two Global Admins.

This screenshot is similar to the previous one but focuses on the 'Members' tab of the Marketing group. It lists three members: Emma Brown (email: emma.brown@techsolutionsinc911.onmicrosoft.com), Liam Johnson (email: liam.johnson@techsolutionsinc911.onmicrosoft.com), and Noah Martin (email: noah.martin@techsolutionsinc911.onmicrosoft.com). Each member is represented by a small profile icon and their name and email address.

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

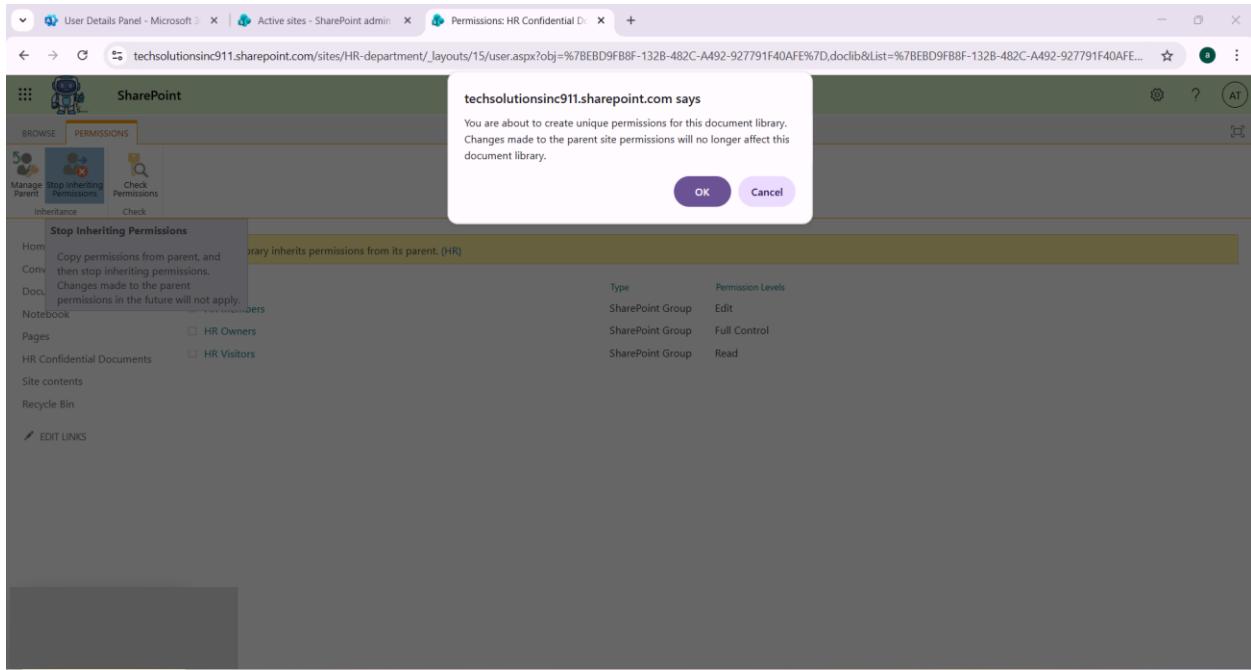
The screenshot shows the SharePoint Admin Center's Active sites page. On the left, there's a navigation menu with options like Home, Sites, Active sites (which is selected), Deleted sites, Containers, Policies, Settings, Content services, Migration, Reports, Advanced, and More features. The main area is titled "Active sites" and contains a table with the following data:

Site name	URL	Teams	Channel sites	Storage u...	Primary admin	Hub	Template	Last
All Company	.../sites/allcompany	-	-	0.00	Group owners	-	Team site	-
Communication site	https://techsolutionsinc911.sharepo...	-	-	0.00	Global Administrator	-	Communication site	-
HR	.../sites/HR-department	HR	-	0.00	Group owners	-	Team site	-
IT	.../sites/IT-department	IT	-	0.00	Group owners	-	Team site	-
Marketing	.../sites/Marketing-department	Marketing	-	0.00	Group owners	-	Team site	-

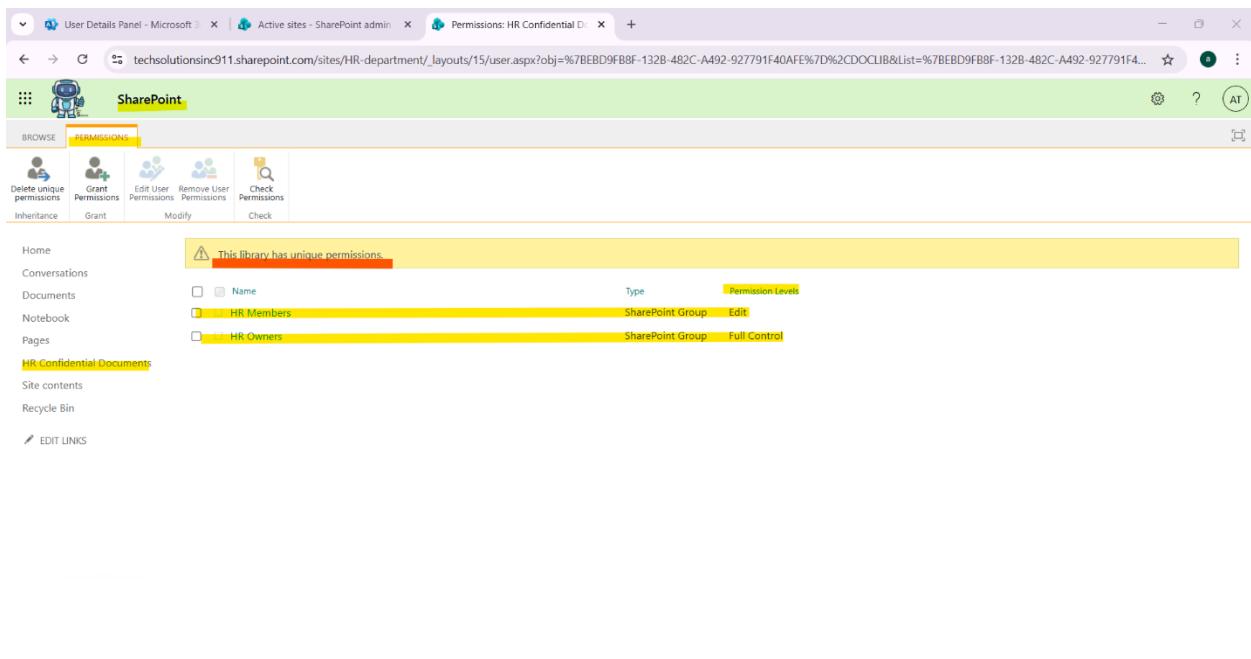
Departmental SharePoint sites were reviewed to confirm successful creation and alignment with corresponding Microsoft 365 groups.

The screenshot shows the HR - Home SharePoint site. The left navigation bar includes Home, Conversations, Documents, Notebook, Pages, Site contents, Recycle bin, and Edit. The main content area displays a news item about the new HR Department group being ready. A modal dialog is open, prompting to create a new library named "HR Confidential Documents". The dialog also includes a description field and a checked checkbox for "Show in site navigation".

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.



The screenshot shows the Microsoft Entra admin center interface. On the left, the navigation menu includes Home, Entra agents, Favorites, Entra ID (Overview, Users, Groups, Devices, Agent ID (Preview), Enterprise apps, App registrations, Roles & admins, Delegated admin partners, Domain services). The main content area is titled 'Marketing-Team-Creators' (Group) and shows the following details:

- Overview:** Shows a green 'M' icon, a 'Delete' button, and a 'Got feedback?' link.
- Manage:** Options include Properties, Members, Owners, Roles and administrators, Administrative units, Group memberships, Applications, Licenses, Azure role assignments, Activity, Privileged Identity Management, Access reviews, Audit logs, and Bulk operation results.
- Marketing-Team-Creators** (highlighted in yellow):
 - Membership type:** Assigned
 - Source:** Cloud
 - Type:** Security (highlighted in yellow)
 - Object ID:** afc62aac-a84d-4ff9-8258-c8a0b838b795 (highlighted in yellow)
 - Created on:** 12/13/2025, 2:38 PM
 - Total direct members:** 3
 - User(s):** 3
 - Group(s):** 0
 - Device(s):** 0
 - Other(s):** 0
- Feed:** Includes sections for Group memberships (0), Owners (2), and Total members (3).

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

```

Administrator: Windows PowerShell
Environment : Global

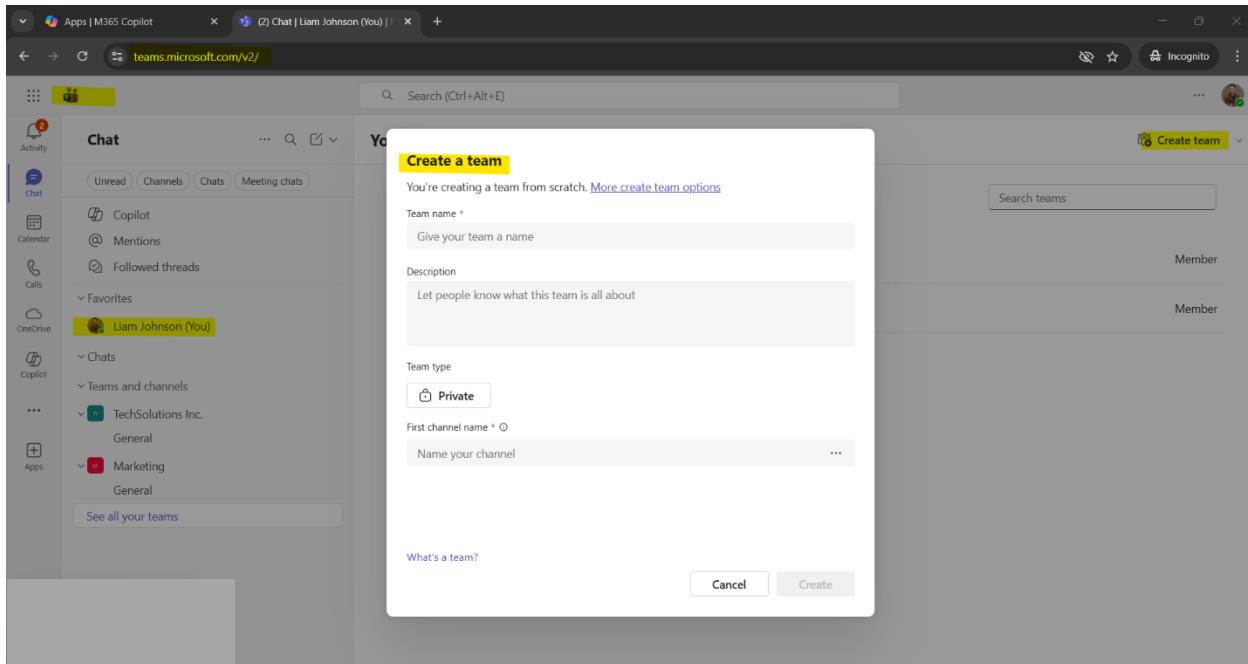
PS C:\WINDOWS\system32> $groupId = "afc62aac-a84d-4ff9-8258-c8a0b838b795"
>>> $setting = Get-MgBetaDirectorySetting |
    Where-Object { $_.DisplayName -eq "Group.Unified" }

$parameters = @{
    Values = @(
        @{
            Name = "EnableGroupCreation"
            Value = "false"
        },
        @{
            Name = "GroupCreationAllowedGroupId"
            Value = $groupId
        }
    )
}

Update-MgBetaDirectorySetting `
    -DirectorySettingId $setting.Id `
    -BodyParameter $parameters

PS C:\WINDOWS\system32> (Get-MgBetaDirectorySetting |
    Where-Object { $_.DisplayName -eq "Group.Unified" }).Values
Name          Value
----          -----
NewUnifiedGroupWritebackDefault true
EnableMTPLabel true
CustomLockedWordsList
EnableSSStandardLockedWords false
ClassificationDescriptions
DefaultClassification
PrefixSuffixNamingRequirement
AllowGuestsToBeGroupOwner false
AllowGuestsToAccessGroups true
GuestUsageGuidelinesUrl
GroupCreationAllowedGroupId afc62aac-a84d-4ff9-8258-c8a0b838b795 ←
AllowToAddGuests true
UsageGuidelinesUrl
ClassificationList
EnableGroupCreation false ←

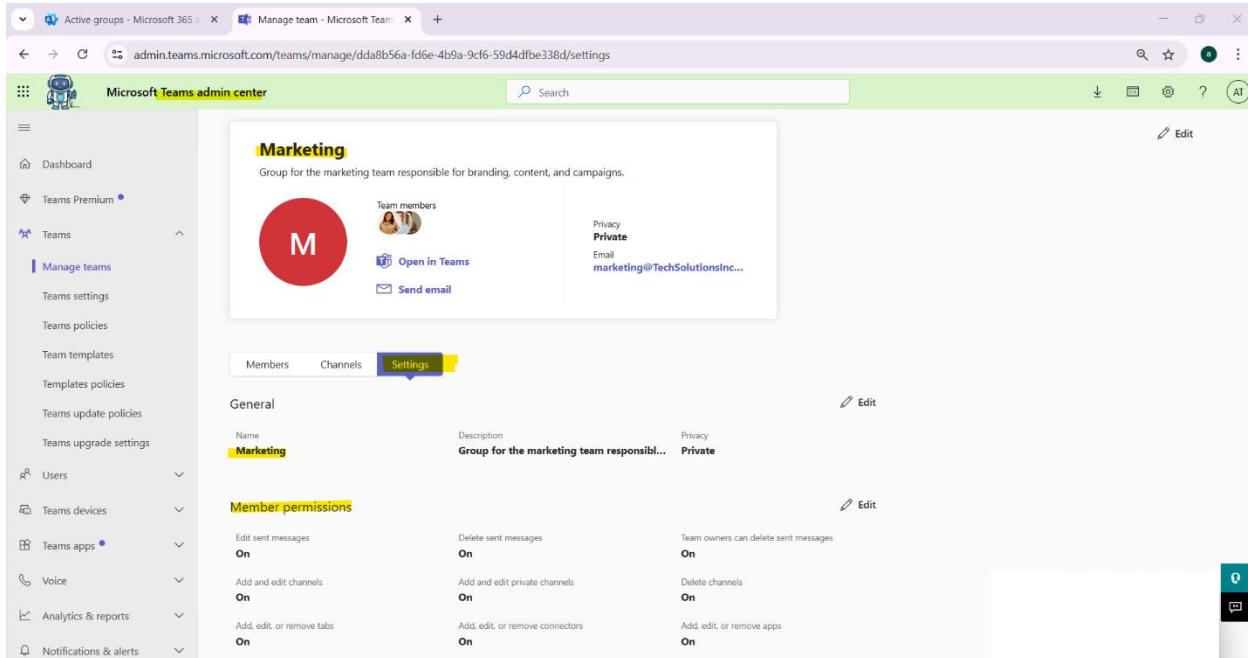
```



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:

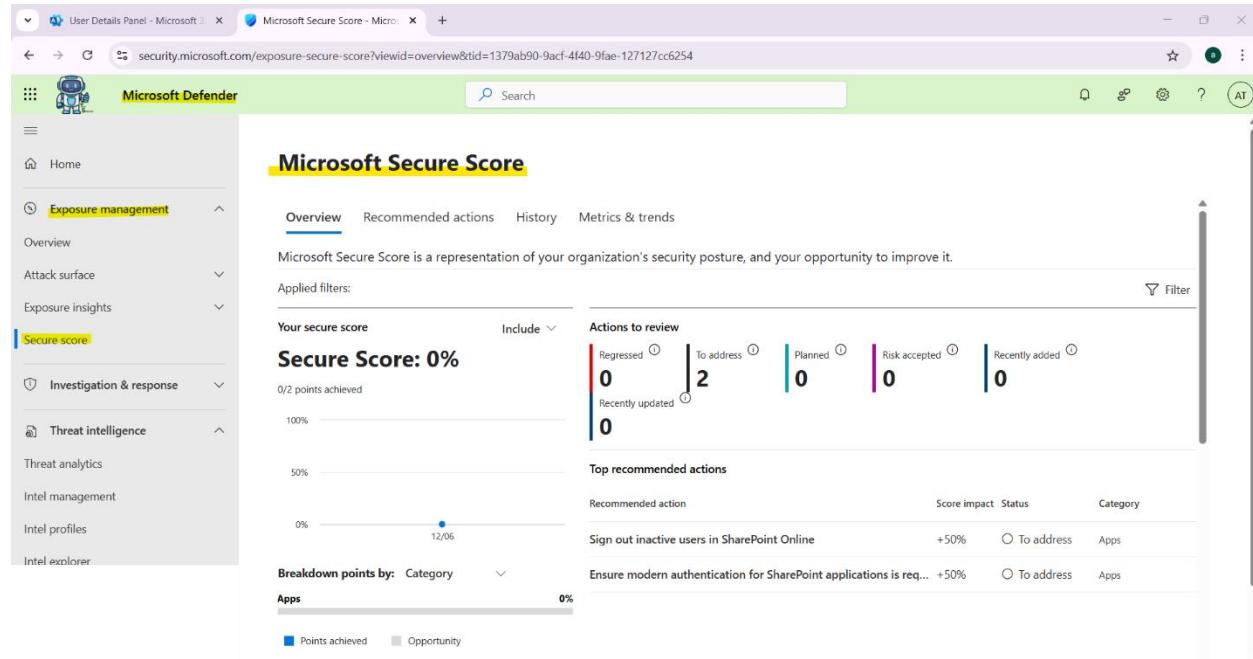
This policy requires a propagation period of up to 48 hours before enforcement is fully reflected in end-user experiences.



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

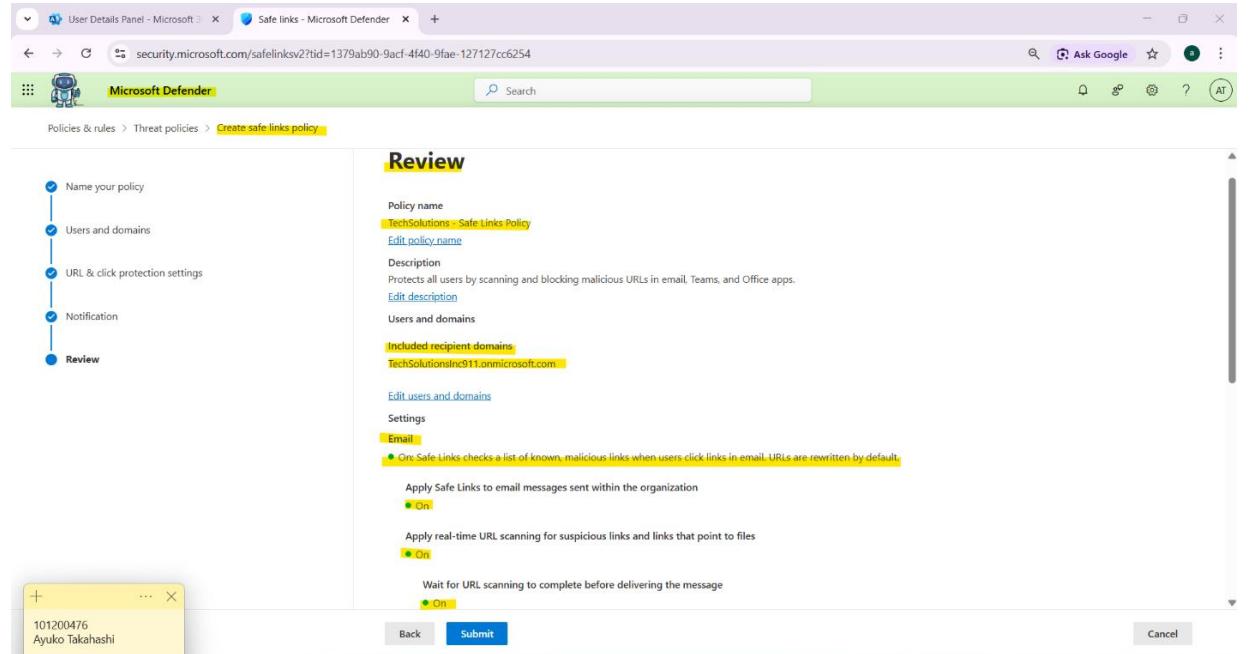
Enterprise Security and Threat Protection

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



The screenshot shows the Microsoft Secure Score dashboard. The left sidebar is titled "Microsoft Defender" and includes sections for Home, Exposure management, Secure score, Investigation & response, Threat intelligence, and Intel explorer. The main area is titled "Microsoft Secure Score" and shows a "Secure Score: 0%" with "0/2 points achieved". It lists two actions to review: "Sign out inactive users in SharePoint Online" and "Ensure modern authentication for SharePoint applications is req...". A breakdown by category shows 0% for Apps.

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



The screenshot shows the "Review" step of creating a safe links policy. The left sidebar shows the navigation path: Policies & rules > Threat policies > Create safe links policy. The right pane displays the policy details: Policy name (TechSolutions - Safe Links Policy), Description (Protects all users by scanning and blocking malicious URLs in email, Teams, and Office apps.), Users and domains (Included recipient domains: TechSolutionsInc511.onmicrosoft.com), Settings (Email: On, Real-time URL scanning: On, Wait for URL scanning to complete before delivering the message: On). At the bottom, there are Back, Submit, and Cancel buttons.

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.

The screenshot shows the Microsoft Defender Safe Links configuration page. On the left, a sidebar lists steps: Name your policy, Users and domains, URL & click protection settings, Notification, and Review. The main area shows configuration for 'Do not rewrite URLs, do checks via Safe Links API only.' under 'On'. It includes sections for Teams (Safe Links checks known malicious links in Microsoft Teams), Office 365 Apps (Safe Links checks known malicious links in Microsoft Office apps), and Track user clicks (lets users click through to original URL). Buttons for Back, Submit, and Cancel are at the bottom.

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 screenshot shows the Microsoft Defender interface for managing security policies. On the left, there's a navigation sidebar with options like Identities, Endpoints, Email & collaboration, and Policies & rules. The main area is titled 'Policies & rules > Threat protection' and 'Apply standard protection'. It lists four selected protection types: Exchange online protection, Defender for Office 365 protection, Impersonation protection, and Policy mode. A note states: 'Note: Built-in protection Microsoft Defender for Office 365 applies to all attachments.' Below this is a 'Review' button. To the right, there's a detailed description of how the policy will be applied to users, groups, and domains. It highlights 'Exchange Online Protection (EOP) applies to all', 'Defender for Office 365 applies to all', and 'Impersonation protection applies to emails from' specific sender email addresses. It also mentions 'Sender domains' and 'Mode' (Policy mode). At the bottom are 'Back', 'Confirm', and 'Cancel' buttons.

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.

This screenshot shows the same Microsoft Defender interface after the policy changes have been applied. The 'Apply standard protection' screen now displays a green checkmark icon next to the title, indicating success. It also includes a 'Learn more' section with links to 'Preset Security Policies' and 'Impersonation settings'. At the bottom is a single 'Done' button.

The screenshot shows the Microsoft Defender for Office 365 interface. On the left, there's a sidebar with navigation options like Overview, Investigations, Explorer, Review, Campaigns, Threat tracker, Exchange message trace, Attack simulation training, Policies & rules, and Cloud apps. The main area is titled "Preset security policies". It shows three protection levels: "Built-in protection", "Standard protection", and "Strict protection". "Standard protection" is currently selected, indicated by a yellow bar at the bottom. The "Standard protection" section includes a note that it's enabled only for paid Microsoft Defender for Office 365 tenants, a list of features (Additional machine learning models, More aggressive detonation evaluation, Visual indication in the experience), and a note about Safe Attachments. A blue button says "Standard protection is on". There are also links to "Add exclusions (Not recommended)" and "Manage protection settings".

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

The screenshot shows the "Apply standard protection" dialog. On the left, there's a sidebar with navigation options like Overview, Investigations, Explorer, Review, Campaigns, Threat tracker, Exchange message trace, Attack simulation training, and Microsoft Defender. The main area has two sections: "Review and confirm your changes" and "Review and confirm your changes". In the first section, there's a list of checked items: Exchange online protection, Defender for Office 365 protection, Impersonation protection, and a "Review" button. In the second section, it says "Exchange Online Protection (EOP) applies to all" and "Defender for Office 365 applies to all". Below that, it says "Impersonation protection applies to emails from" and lists sender email addresses: Ayuko Takahashi, ayukotakahashi@techsolutionsinc911.onmicrosoft.com; Ayuko Takahashi1, ayukotakahashi1@techsolutionsinc911.onmicrosoft.com; Olivia Smith, olivia.smith@techsolutionsinc911.onmicrosoft.com; Alex Wong, alex.wong@techsolutionsinc911.onmicrosoft.com;. It also says "With the exception of the following trusted senders and domains". At the bottom, there are "Back", "Confirm", and "Cancel" buttons.

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

The screenshot shows the Microsoft Defender interface for managing threat policies. The left sidebar is titled 'Email & collaboration' and includes sections for Overview, Investigations, Explorer, Review, Campaigns, Threat tracker, Exchange message trace, Attack simulation training, Policies & rules, and Cloud apps. The main content area is titled 'Safe links' and displays a list of policies. A header bar at the top shows the URL 'security.microsoft.com/safelinks?tid=1379ab90-9acf-4f40-9fae-127127cc6254'. The policy list includes:

Name	Status	Priority
Standard Preset Security Policy	On	..
Built-in protection (Microsoft)	On	Lowest

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

The screenshot shows the Microsoft Defender interface for managing threat policies. The left sidebar is titled 'Email & collaboration' and includes sections for Overview, Investigations, Explorer, Review, Campaigns, Threat tracker, Exchange message trace, Attack simulation training, Policies & rules, and Cloud apps. The main content area is titled 'Safe attachments' and displays a list of policies. A header bar at the top shows the URL 'security.microsoft.com/safeattachmentv2?tid=1379ab90-9acf-4f40-9fae-127127cc6254'. The policy list includes:

Name	Status	Priority
Standard Preset Security Policy	On	..
Built-in protection (Microsoft)	On	Lowest

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

The screenshot shows the Microsoft Defender Anti-phishing policy creation interface. The left sidebar lists steps: Policy name, Users, groups, and domains, Phishing threshold & protection, Actions, and Review. The main area is titled "Policy name" with "Anti-Phishing Protection Policy". Under "Description", it says "Protect users from spoofing and phishing attempts." The "Included recipient domains" field contains "TechSolutionsInc911.onmicrosoft.com". The "Actions" section includes "Mailbox Intelligence" set to "On". Buttons at the bottom are "Back", "Submit", and "Cancel".

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.

The screenshot shows the Microsoft Defender Anti-phishing policy creation interface with more detailed configuration. The "Actions" section is expanded, listing various detection rules and their corresponding quarantine actions. These include:

- If a message is detected as user impersonation: Quarantine the message, DefaultFullAccessPolicy
- If a message is detected as domain impersonation: Quarantine the message, DefaultFullAccessPolicy
- If Mailbox Intelligence detects an impersonated user: Quarantine the message, DefaultFullAccessPolicy
- If the message is detected as spoof and DMARC Policy is set as p=quarantine: Quarantine the message, Default full access policy
- If the message is detected as spoof and DMARC Policy is set as p=reject: Reject the message
- If the message is detected as spoof by spoof intelligence: Move the message to the recipients' Junk Email folders

Buttons at the bottom are "Back", "Submit", and "Cancel".

The screenshot shows the Microsoft Defender Anti-phishing policy creation interface. The left sidebar lists policy components: Policy name, Users, groups, and domains, Phishing threshold & protection, Actions, and Review. The Review step is selected. The main pane displays various detection and response rules. A yellow bar at the bottom indicates 1 of 3 selected actions.

If the message is detected as spoof and DMARC Policy is set as p=quarantine
Quarantine the message
Default full access policy

If the message is detected as spoof and DMARC Policy is set as p=reject
Reject the message

If the message is detected as spoof by spoof intelligence
Move the message to the recipients' Junk Email folders

First contact safety tip
User impersonation safety tip
Domain impersonation safety tip
Unusual characters safety tip
Unauthenticated senders symbol (?) for spoof
Show "via" tag
Honor DMARC record policy when the message is detected as spoof

[Edit actions](#)

Back Submit Cancel

The screenshot shows the Microsoft Defender Anti-phishing policy list interface. The left sidebar includes sections for Identities, Endpoints, Email & collaboration, Overview, Investigations, Explorer, Review, Campaigns, Threat tracker, Exchange message trace, Attack simulation training, Policies & rules, and Cloud apps. The Policies & rules section is expanded, showing sub-options like Threat policies, Anti-phishing, and Identity protection.

Anti-phishing

By default, Microsoft 365 includes built-in features that help protect your users from phishing attacks. Set up anti-phishing policies to increase this protection. For example, you can refining the settings to better detect and prevent impersonation and spoofing attacks. The default policy applies to all users within the organization. You can create custom, higher priority policies for specific users, groups or domains. [Learn more about anti-phishing policies](#)

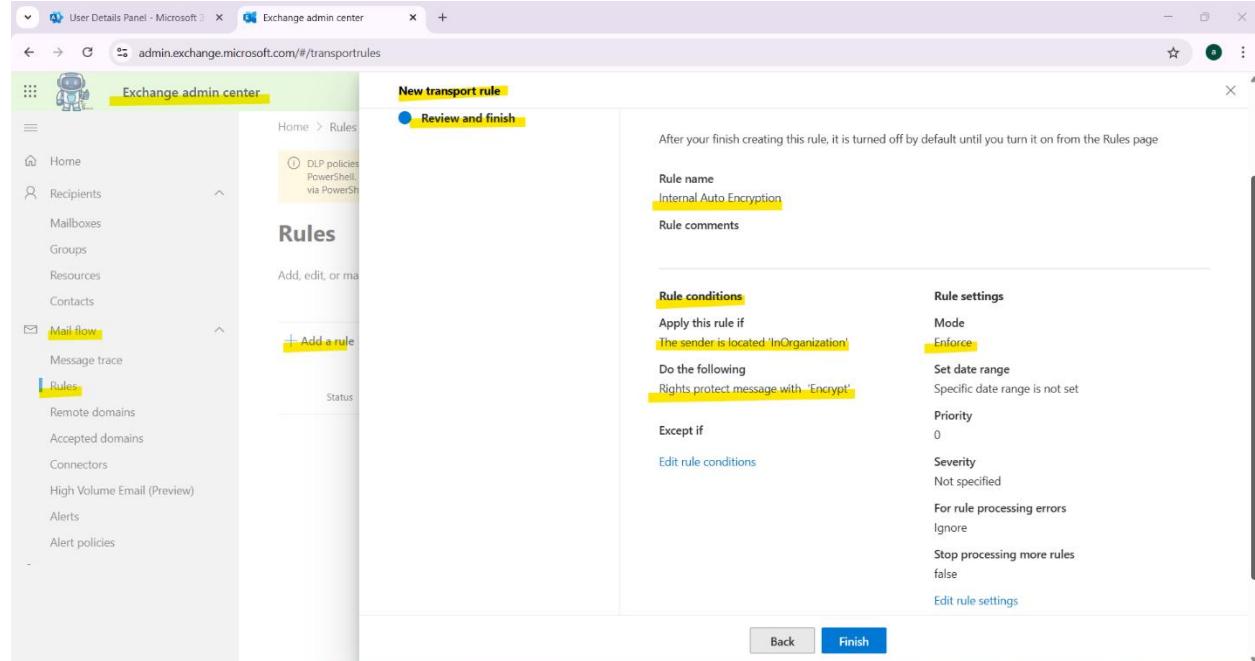
[Create](#) [Export](#) [Refresh](#) [More actions](#)

Name	Status	Priority	Last modified
Standard Preset Security Policy	On	--	Dec 7, 2025
Anti-Phishing Protection Policy	On	0	Dec 7, 2025
Office365 AntiPhish Default (Default)	Always on	Lowest	Dec 7, 2025

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

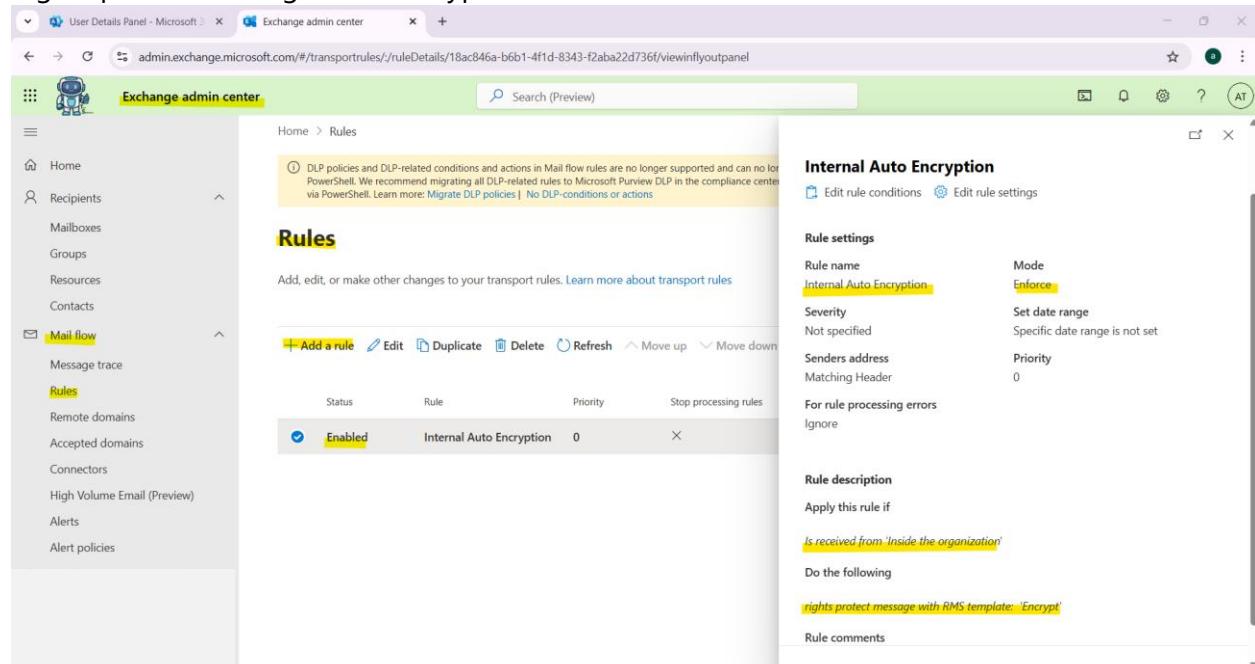
Data Protection and Message Encryption

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



The screenshot shows the Exchange admin center interface. On the left, the navigation pane is open with the 'Mail flow' section selected, specifically the 'Rules' sub-section. The main content area is titled 'New transport rule' and is currently on the 'Review and finish' step. The rule is named 'Internal Auto Encryption'. The 'Rule conditions' section specifies that the rule applies if the sender is located 'InOrganization'. The 'Do the following' section contains the action 'Rights protect message with "Encrypt"'. The 'Rule settings' section includes options like 'Mode: Enforce', 'Set date range' (disabled), 'Priority: 0', 'Severity: Not specified', and 'For rule processing errors: Ignore'. A 'Finish' button is visible at the bottom right of the dialog.

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



The screenshot shows the Exchange admin center interface. The left navigation pane is open with the 'Mail flow' section selected, specifically the 'Rules' sub-section. The main content area displays a list of rules under the heading 'Rules'. One rule is listed: 'Internal Auto Encryption' (Status: Enabled). The right side of the screen provides detailed information about this rule. It shows the rule name 'Internal Auto Encryption', mode 'Enforce', and priority '0'. The 'Rule description' section states 'Apply this rule if Is received from "Inside the organization"'. The 'Do the following' section contains the action 'rights protect message with RMS template: "Encrypt"'. There are also sections for 'Edit rule conditions' and 'Edit rule settings'.

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

The screenshot shows the Microsoft Outlook web interface. On the left, the navigation pane displays 'Favorites' with items like 'Inbox', 'Sent Items', 'Drafts', and 'Deleted Items'. The main pane shows a list of messages under 'Focused' and 'Other'. Two messages are highlighted:

- Emma Brown** (Project A) - Sent on Mon 12/8/2025 12:59 PM. The message body says: "Hello, Noah, Liam. This is regarding to Project A. Thanks, Emma".
- Liam Johnson** (General\All Employees (unrestricted)) - Sent on Mon 12/8/2025 1:03 PM. The message body says: "Hi Emma. I'm working on it by tomorrow. Thanks, Liam".

In both messages, there is a yellow bar at the top stating "This message is encrypted." with a small shield icon.

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

The screenshot shows a browser window for outlook.office365.com. The URL in the address bar is 'outlook.office365.com/encryption/display-message'. The page title is 'new hiring info'. The message details are as follows:

Liam Johnson <liam.johnson@techsolutionsinc911.onmicrosoft.com>
12/8/2025 6:08:58 PM
To: ayukotakahashi.at@gmail.com

The message body contains:

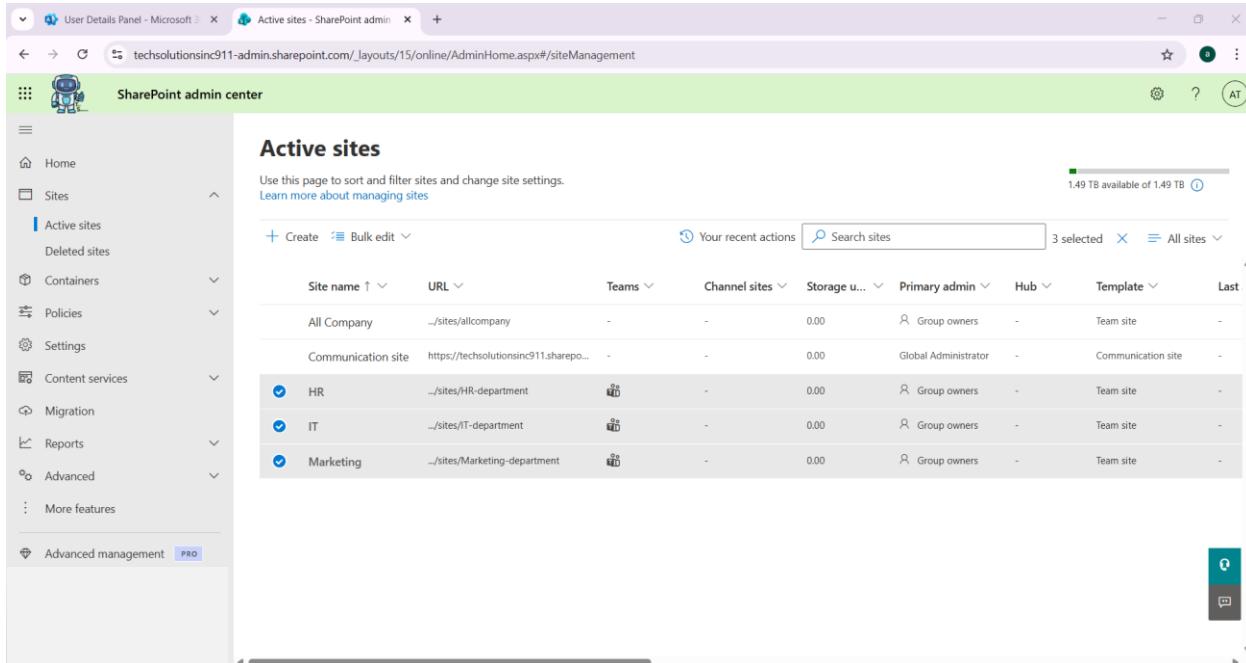
Hi Ayuko,
We're hiring system admin role, if you're interested, let me know.
Thanks,
Liam

A yellow bar at the top of the message area states "Encrypt: This message is encrypted. Recipients can't remove encryption." with a small shield icon.

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

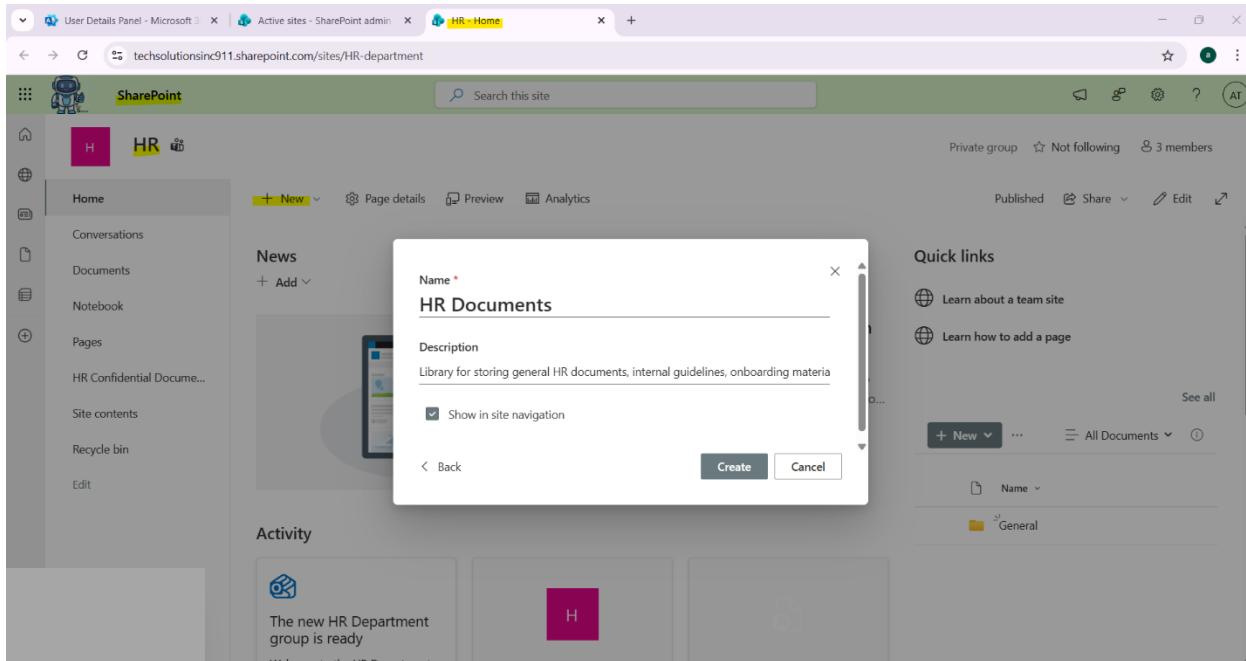
Collaboration Services Configuration and Governance

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.



The screenshot shows the SharePoint Admin Center interface. On the left, there's a navigation menu with options like Home, Sites, Containers, Policies, Settings, Content services, Migration, Reports, Advanced, and More features. The main area is titled "Active sites" and displays a table of existing sites. The table includes columns for Site name, URL, Teams, Channel sites, Storage usage, Primary admin, Hub, Template, and Last modified. There are four entries: "All Company" (Team site), "Communication site" (Communication site), "HR" (Team site), and "IT" (Team site). A search bar at the top right allows filtering by site name.

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



The screenshot shows the SharePoint site for the HR department. The left navigation bar includes Home, Conversations, Documents, Notebook, Pages, HR Confidential Docume..., Site contents, Recycle bin, and Edit. The main content area has a "News" section with a "New" button and a "Create" dialog box open. The dialog box is titled "HR Documents" and asks for a "Name" (with a red asterisk) and a "Description" (Library for storing general HR documents, internal guidelines, onboarding materia...). There's also a checked checkbox for "Show in site navigation". At the bottom of the dialog are "Create" and "Cancel" buttons. To the right of the dialog, there's a "Quick links" section with links to "Learn about a team site" and "Learn how to add a page". Below that is a "See all" section with a "New" button and a "All Documents" list. The footer shows activity items related to the HR department.

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

The screenshot shows the SharePoint Permissions page for the 'HR Documents' library. At the top, there are tabs for 'BROWSE' and 'PERMISSIONS'. Under 'PERMISSIONS', there are five buttons: 'Delete unique permissions', 'Grant Permissions', 'Edit User Permissions', 'Remove User Permissions', and 'Check Permissions'. Below these buttons, there is a section titled 'Inheritance' with options 'Grant', 'Modify', and 'Check'. A yellow warning bar at the top states 'This library has unique permissions.' A table lists the permissions for the library:

Name	Type	Permission Levels
HR Members	SharePoint Group	Edit
HR Owners	SharePoint Group	Full Control

The screenshot shows the SharePoint 'IT Home' site. On the left, the navigation menu includes 'Home', 'Conversations', 'Documents', 'Notebook', 'Pages', 'Site contents', 'Recycle bin', and 'Edit'. In the center, there is a modal dialog for creating a new document library named 'IT Documents'. The dialog fields include 'Name *' (IT Documents), 'Description' (Library for storing and managing IT department documents, including technical ...), and a checked 'Show in site navigation' option. At the bottom of the dialog are 'Back', 'Create', and 'Cancel' buttons. To the right of the dialog, the 'Quick links' sidebar is visible, containing links to 'Learn about a team site' and 'Learn how to add a page'. The main content area shows a news item: 'The new IT Department group is ready'.

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

This screenshot shows the SharePoint Permissions page for the 'IT Documents' library. The browser tabs include 'User Details Panel - Microsoft 365', 'Active sites - SharePoint admin', and 'Permissions: IT.Documents'. The main content area displays the permission settings for the library. A yellow warning bar at the top states 'This library has unique permissions.' Below this, a table lists three entries:

	Type	Permission Levels
<input type="checkbox"/> Name	SharePoint Group	Edit
<input type="checkbox"/> IT Members	SharePoint Group	Edit
<input type="checkbox"/> IT Owners	SharePoint Group	Full Control

The left sidebar shows navigation links: Home, Conversations, Documents, Notebook, Pages, IT Documents (selected), Site contents, and Recycle Bin. At the bottom left is an 'EDIT LINKS' button.

This screenshot shows the creation of a new document library named 'Marketing Documents' within the 'Marketing' site. The browser tabs are identical to the previous screenshot. The main content area shows the 'Marketing' site's home page with a modal dialog open for creating the library. The dialog fields are:

- Name: Marketing Documents
- Description: "Library for storing marketing plans, creative assets, campaign materials, and team"
- Show in site navigation: checked

At the bottom right of the dialog are 'Create' and 'Cancel' buttons. The background shows the 'Marketing' site's navigation bar and a news section.

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

User Details Panel - Microsoft 365 | Active sites - SharePoint admin | Permissions: Marketing Document

techsolutionsinc911.sharepoint.com/sites/Marketing-department/_layouts/15/user.aspx?obj=%7b4A70E8B1-942E-4A49-BE0B-674773ED9460%7d%2cdclib&List=%7b4A70E8B1-942E-4A49-BE0B-6747...

SharePoint

BROWSE PERMISSIONS

Delete unique permissions Grant Permissions Edit User Permissions Remove User Permissions Check Permissions

Inheritance Grant Modify Check

Home Conversations Documents Notebook Pages Marketing Documents Site contents Recycle Bin

EDIT LINKS

This library has unique permissions.

Type	Permission Levels
SharePoint Group	Edit
SharePoint Group	Full Control

Marketing Members Marketing Owners

User Details Panel - Microsoft 365 | Active sites - SharePoint admin | Document Library Settings

techsolutionsinc911.sharepoint.com/sites/HR-department/_layouts/15/listedit.aspx?List=%7B2ff6acc0-9189-457d-9b1d-3e0c4358ad21%7D

SharePoint

EDIT LINKS

HR Documents > Settings

List Information

Name: HR Documents
Web Address: https://techsolutionsinc911.sharepoint.com/sites/HR-department/HR Documents/Forms/AllItems.aspx
Description: Library for storing general HR documents, internal guidelines, onboarding materials, and department resources accessible to the HR team.

General Settings

- List name, description and navigation
- Versioning settings
- Advanced settings
- Validation settings
- Column default value settings
- Audience targeting settings
- Rating settings
- Form settings

Permissions and Management

- Delete this document library
- Permissions for this document library
- Manage files which have no checked in version
- Workflow Settings
- Enterprise Metadata and Keywords Settings

Communications

- RSS settings

Columns

A column stores information about each document in the document library. The following columns are currently available in this document library:

Column	Type	Required
Created	Date and Time	
Modified	Date and Time	
Title	Single line of text	Required

Versioning settings.

The screenshot shows the 'Document Library Versioning' settings page in SharePoint. Under 'Content Approval', the 'Require content approval for submitted items?' section is set to 'Yes'. Under 'Version time limit', the 'No time limit' option is selected, indicating versions won't be deleted based on their age. A note states: 'Versions are deleted over time based on activity and how long ago the file was first created.'

Content Approval
Specify whether new items or changes to existing items should remain in a draft state until they have been approved. Learn about requiring approval.

Require content approval for submitted items?
 Yes No

Create a version each time you edit a file in this document library?
 Create major versions
Example: 1, 2, 3, 4
 Create major and minor (draft) versions
Example: 1.0, 1.1, 1.2, 2.0

What kind of version time limit do you want to set?
 No time limit:
Versions won't be deleted based on their age.
 Automatic
Versions are deleted over time based on activity and how long ago the file was first created.
 Manual
Versions are deleted when they exceed the following number of days.

Version count limit:
Delete the oldest versions when the number of versions exceeds a number you set.

Keep the following number of major versions:
500

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

The screenshot shows the 'Document Library Versioning' settings page in SharePoint. Under 'Draft item security', the 'Who should see draft items in this document library?' section is set to 'Only users who can approve items (and the author of the item)'. Under 'Require Check Out', the 'Require documents to be checked out before they can be edited?' section is set to 'No'. Other visible sections include 'Version count limit' and 'Keep drafts for the following number of major versions'.

Draft item security:
Drafts are minor versions or items which have not been approved. Specify which users should be able to view drafts in this document library. Learn about specifying who can view and edit drafts.

Who should see draft items in this document library?
 Any user who can read items
 Only users who can edit items
 Only users who can approve items (and the author of the item)

Require Check Out:
Specify whether users must check out documents before making changes in this document library. Learn about requiring check out.

Require documents to be checked out before they can be edited?
 Yes No

OK **Cancel**

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.

The screenshot shows the SharePoint admin center's Sharing page. On the left, there's a navigation menu with 'Sharing' selected under 'Policies'. The main content area is titled 'Sharing' and describes how to control sharing at the organization level. It features a horizontal slider for 'Content can be shared with:' between 'SharePoint' (most permissive) and 'OneDrive' (least permissive). The 'OneDrive' side of the slider is highlighted with a yellow circle, indicating the current setting. Below the slider, it says 'Least permissive' and 'Only people in your organization' with 'No external sharing allowed' underneath. There are also sections for 'New and existing guests' and 'Existing guests'. At the bottom, there's a link to 'More external sharing settings'.

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.

The screenshot shows the Microsoft Purview Data Lifecycle Management interface for creating a retention policy. On the left, a vertical progress bar indicates steps completed (Name, Administrative Units, Type, Retention settings) and the current step (Finish). The main area is titled 'Review and finish' and contains the following details:

- Policy name:** OneDrive 5-Year Retention
- Description:** This retention policy ensures all OneDrive files are kept for a minimum of five years to meet organizational data retention and compliance requirements. Items are automatically deleted after the retention period ends.
- 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.

A warning message in an orange box states: "⚠️ Items that are currently older than 5 years will be deleted after you turn on this policy. This is especially important to note for locations scoped to 'All' sources (for example, 'All Teams chats') because all matching items in those locations across your organization will be permanently deleted."

At the bottom are 'Back', 'Submit', and 'Cancel' buttons.

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.

Retention policies

Your users create a lot of content every day, from emails to Teams and Yammer conversations. need. [Learn more about creating retention policies](#)

If your role group permissions are restricted to a specific set of users or groups, you'll only be able to create new policies for those users.

Set up pay-as-you-go to create new AI related policies. To create new policies that include Copilot, first link an Azure subscription for billing. There's no charge for retaining interactions in Microsoft 365.

+ New retention policy Edit Delete Disable policy Export

Name: OneDrive 5-Year Retention

Applies to content in these locations: OneDrive accounts

Admin units (preview): Full directory

Retention period: Keep content, and delete it if it's older than 5 years

Preservation lock: No

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

Review and finish

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

Policy name: OneDrive 1-Year Auto-Cleanup

Description: This policy automatically deletes OneDrive files older than one year, causing them to be moved into the user's Recycle Bin for clean up.

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 years based on when they were created

Items that are currently older than 1 years will be deleted after you turn on this policy. This is especially important to note for locations scoped to 'All' sources (for example, 'All Teams chats') because all matching items in these locations across your organization will be permanently deleted.

Back Submit Cancel

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.

The screenshot shows the Microsoft Purview Data Lifecycle Management Retention policies page. On the left sidebar, under 'Retention policies', the 'OneDrive 1-Year Auto-Cleanup' policy is highlighted. The main content area displays the policy details: Status (Enabled (Success)), Description (This policy automatically deletes OneDrive files older than one year, causing them to be moved into the user's Recycle Bin for clean up.), Admin units (Full directory), Applies to content in these locations (OneDrive accounts), Settings (Retention period: Don't retain content; but delete it if it's older than 1 year), and Preservation lock (No). A note at the top right says 'Set up pay-as-you-go to create new AI related policies. To create new policies that include Copilot, first link an Azure subscription for billing. There's no charge for retaining interactions in Microsoft 365'.

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

```

Administrator: Windows PowerShell
PS C:\WINDOWS\system32> $temp = Get-MgBetaDirectorySettingTemplate | Where-Object {$_DisplayName -eq "Group.Unified"}
>>> $temp | Format-List Id, DisplayName

Id : 62375ab9-6b52-47ed-820b-58e47e0e304b
DisplayName : Group.Unified

PS C:\WINDOWS\system32> $paramsCreate = @{
>     TemplateId = $temp.Id
>     Values = @(
>         @{
>             Name = "EnableMIPLabels"
>             Value = "True"
>         }
>     )
> }
> $newSetting = New-MgBetaDirectorySetting -BodyParameter $paramsCreate
> $newSetting.Id
> $newSetting.Id
> 077a891-a8a0-4ed0-8524-432b612fd9e1
PS C:\WINDOWS\system32> $verify = Get-MgBetaDirectorySetting -DirectorySettingId $newSetting.Id
>>> $verify.Values | Where-Object {$_Name -eq "EnableMIPLabels"}
>>>
Name      Value
----      ---
EnableMIPLabels True

```

The PowerShell session shows the creation of a sensitive label named 'EnableMIPLabels' with a value of 'True' for the 'Group.Unified' Microsoft 365 group. The output table is highlighted with a yellow box.

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](#)

The screenshot shows the Microsoft Purview interface for creating a new sensitivity label. The left sidebar has a tree view with 'Label details' (selected), 'Scope' (selected), 'Items', 'Groups & sites', and 'Finish'. The main area is titled 'Define the scope for this label'. It explains that labels can be applied to data assets and containers like SharePoint sites and Teams. It lists three options: 'Files & other data assets', 'Emails', and 'Meetings'. Below 'Meetings', there's a note about meeting settings. At the bottom, there's a note about applying labels to Azure storage and SQL. A red arrow points to the 'Groups & sites' checkbox, which is currently grayed out.

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

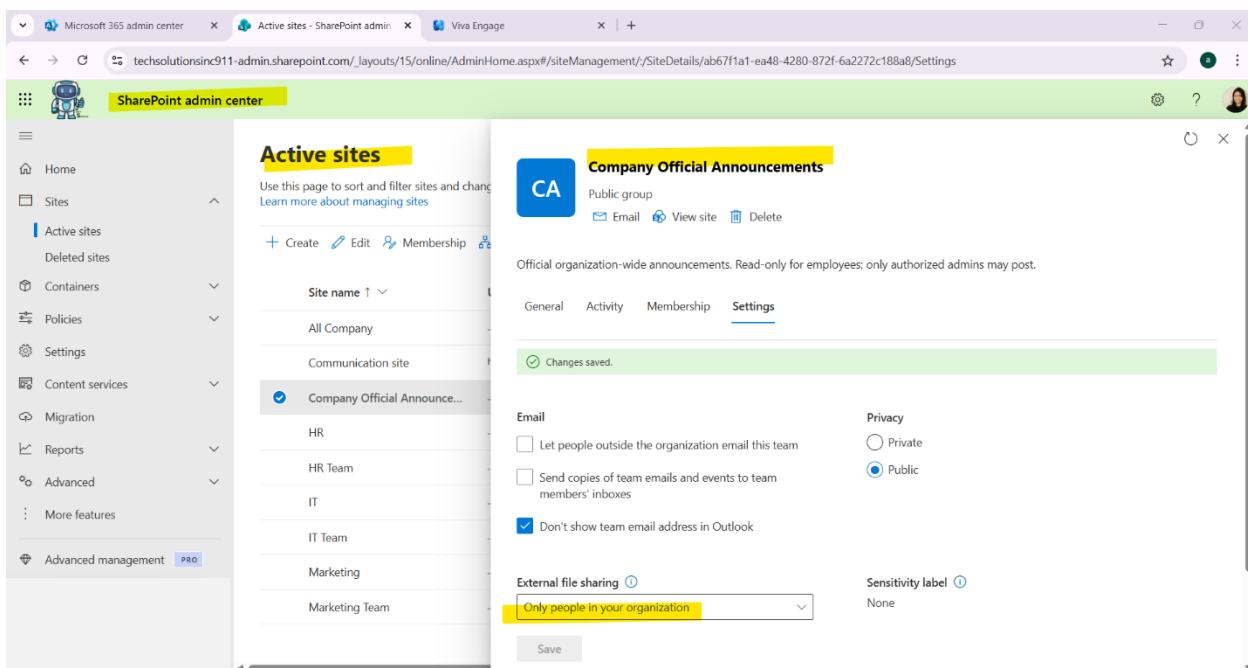
- Skipped
- ◆ Label Publishing
 - Label name: Internal Communications Only
 - The label would be published to users and applied to the Microsoft 365 Group associated with the Viva Engage community.
- ◆ Outcome (Intended)

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

Use this page to sort and filter sites and change Learn more about managing sites

+ Create Edit Membership

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

Home

Sites

Containers

Policies

Settings

Content services

Migration

Reports

Advanced

More features

Advanced management PRO

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

Use this page to sort and filter sites and change Learn more about managing sites

+ Create Edit Membership

HT 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

Home

Sites

Containers

Policies

Settings

Content services

Migration

Reports

Advanced

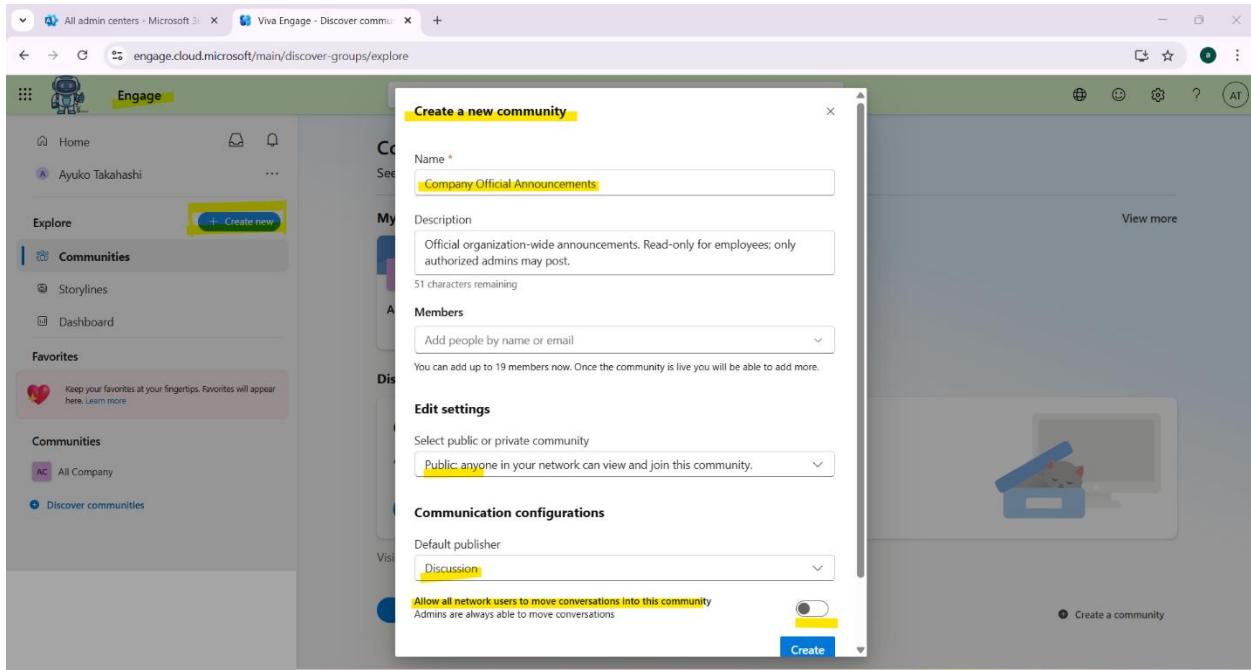
More features

Advanced management PRO

The screenshot shows the SharePoint admin center interface. On the left, the navigation menu includes Home, Sites (Active sites selected), Containers, Policies, Settings, Content services, Migration, Reports, Advanced, and More features. Under Advanced management, there is a PRO button. The main content area is titled "Active sites" and shows a list of sites under the "Marketing Team" private group. The "Marketing Team" site is selected, displaying its settings. The "Settings" tab is active, showing options for Email (including checkboxes for letting people outside the organization email the team, sending copies of team emails to members' inboxes, and a checked option for "Don't show team email address in Outlook"), Privacy (set to Private), External file sharing (set to "Only people in your organization"), and Sensitivity label (None). A green banner at the bottom indicates "Changes saved".

The screenshot shows the Viva Engage Admin center interface. The left sidebar includes Home, Ayuko Takahashi, Explore (Communities, Storylines, Dashboard), Favorites (with a note to keep favorites at your fingertips), Communities (Company Official Announcements, IT Team, Marketing Team), and more. The main content area is titled "Admin center" and includes sections for Setup and configuration (Admin roles, Tenant settings, External net), Engage segmentation, and a callout for Copilot. A Networks section on the right shows "TechSolutions Inc." with "Home network" selected. A search bar at the top right says "Search Viva Engage".

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.

The screenshot shows the Viva Engage platform interface. On the left, there's a sidebar with navigation links like Home, Explore, and Favorites. The main area displays a community feed with posts from 'Company Official Announcements'. A context menu is open over a post, listing options such as 'Mute community in feed', 'Subscribe by email', 'Embed community feed', 'Network admin', 'Mute for network', 'Unmark official community', and 'Leave community'. The right side shows a 'Members' section with one member named 'AT'.

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

The screenshot shows the 'Community settings' page for the 'Company Official' community. It includes sections for 'Community description' (with a note about being a read-only announcement board), 'Community information' (for summarizing details and rules), and 'Configuration' (with privacy set to 'Public: anyone in your organization can view it' and posting permissions set to 'Restricted').

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

The screenshot shows the Microsoft Viva Engage interface for a 'Company Official' community. The main content area features a large red banner with a cartoon character and the text 'Company Official Announcements'. Below the banner, there's a section for 'Community experts' where users can assign members. A prominent yellow 'Restricted' button is visible at the bottom right of the main content area. The sidebar includes sections for Home, Ayuko Takahashi, Explore (Communities, Storylines, Dashboard), Favorites, and Communities (All Company, Discover communities).

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

This screenshot shows the same Viva Engage interface after updates. The main banner now features a larger, more detailed cartoon robot character. The 'Community experts' section has been removed. The yellow 'Restricted' button is still present. The sidebar now includes a 'Company Official Announcements' section under the Communities heading. On the right side, there's a 'Members' panel listing various company members with their roles: Ayuko Takahashi (Admin), Noah Martin (Marketing Manager), Olivia Smith (HR Manager), Alex Wong (Support Specialist), Mia Chan (HR Coordinator), Sophia Lee (System Administrator), Liam Johnson (Marketing Coordinator), Ethan Patel (Cloud Engineer), Emma Brown (Content Strategist), Daniel Nguyen (HR Specialist), Ava Takahashi (Project Administrator), and Ayuko Takahashi (Admin again). The 'Import from CSV' button is also visible in this panel.

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.

User Details Panel - Microsoft 365 | Viva Engage - Company Official

engage.cloud.microsoft/main/groups/eyJfdHlwZSI6Ikdyb3VwliwiaWQjOilyNDQ3NjAxODI3ODQifQ/all

Engage

Name * **IT Team**

Description
A space for the IT team to collaborate, share updates, and discuss projects.
74 characters remaining

Members
Alex Wong, Ethan Patel, Ava Takahashi, Sophia Lee

Add people by name or email

You can add up to 19 members now. Once the community is live you will be able to add more.

Edit settings
Select public or private community
Private: only approved community members can view or participate.

Communication configurations
Default publisher
Discussion

Allow all network users to move conversations into this community
Admins are always able to move conversations

Create

Members • 12

Community experts

Assign members who offer expertise in this community.

Assign

Community summary

Nov 11, 2025 - Dec 8, 2025
We do not have enough data for this community yet.
Only admins can see this summary.

See full community analytics

Info

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.

All admin centers - Microsoft 365 | Viva Engage - IT Team

engage.cloud.microsoft/main/groups/eyJfdHlwZSI6Ikdyb3VwliwiaWQjOilyNDQ3NjE0ODUzMTIifQ/all

Engage

Search Viva Engage

IT Team
A space for the IT team to collaborate, share updates, and discuss projects.

Conversations About Files Events

Share thoughts, ideas, or updates

Discussion Question Praise Poll Drafts

Introducing community experts & verified answers

Admins can now assign experts to enrich the community experience by verifying helpful responses. Verified answers help build credibility and trust across your community.

Members

Invite or search for people by name

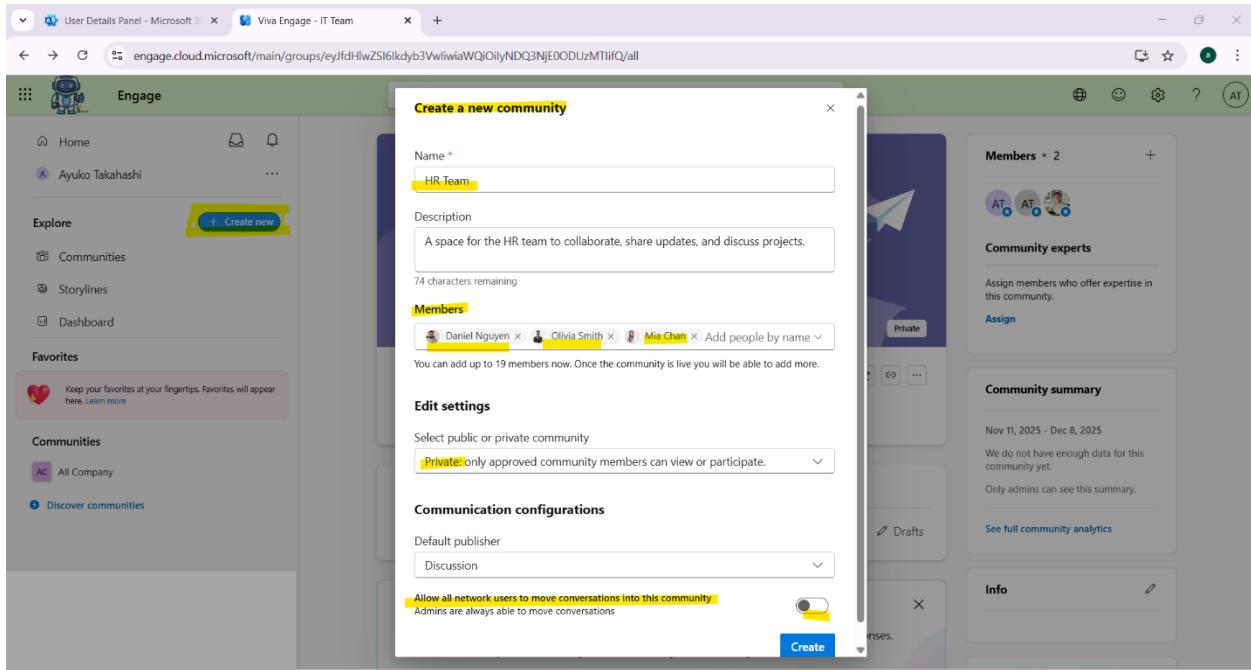
Search

Learn more Import from CSV

Community members

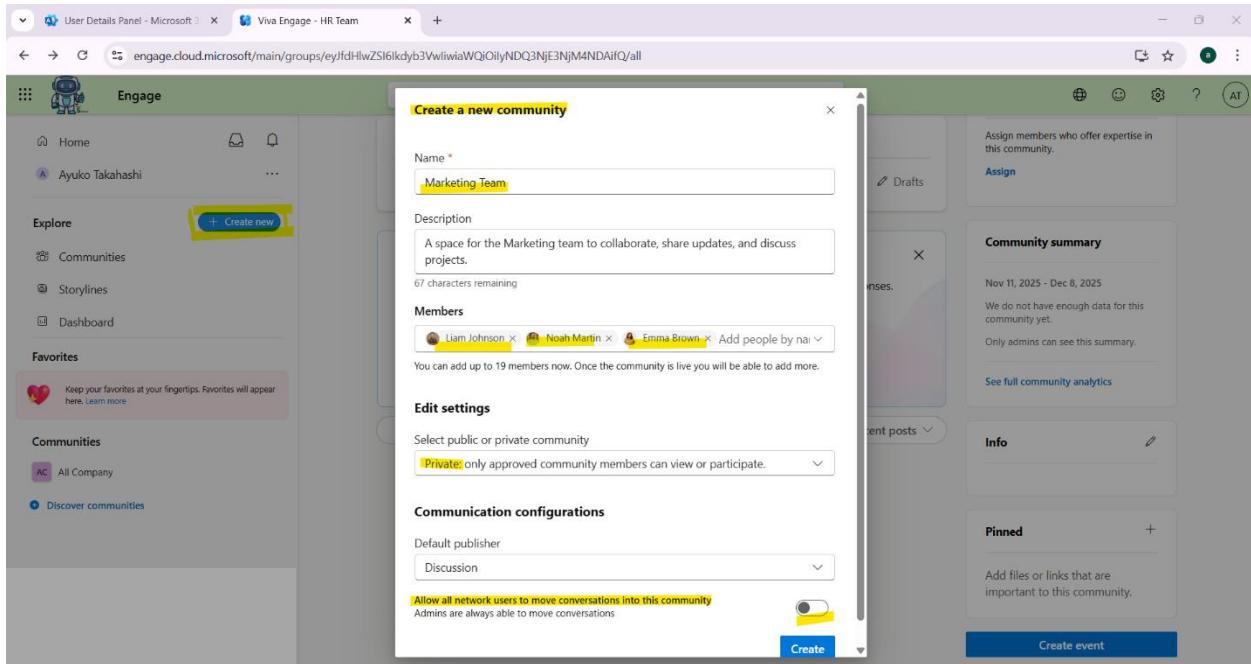
- Ayuko Takahashi (Admin)
- Alex Wong (Admin, IT Support Specialist)
- Ayuko Takahashi1 (Admin)
- Sophia Lee (System Administrator)
- Ava Takahashi (Project Administrator)
- Ethan Patel (Cloud Engineer)

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



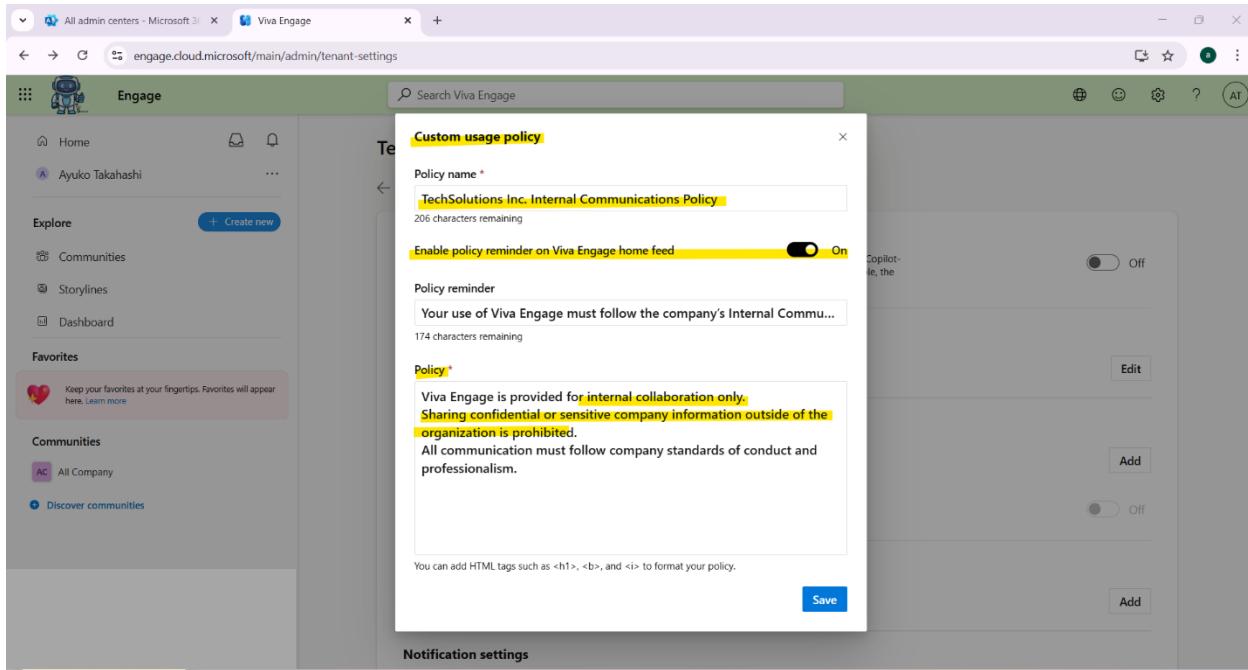
Department-Specific Discussion Groups for HR Team. Add HR members, set as Private and toggled off for not allowing all network users to move conversations into this community.

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

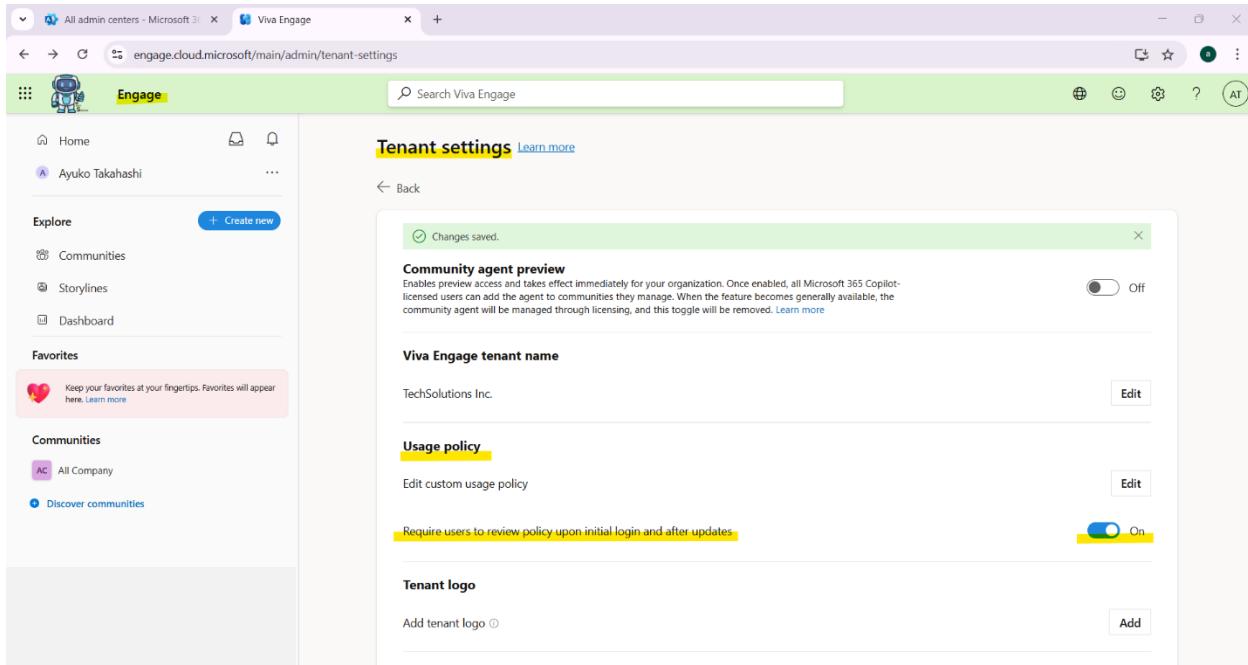


Department-Specific Discussion Groups for Marketing Team. Add Marketing members, set as Private and toggled off for not allowing all network users to move conversations into this community.

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 screenshot shows the Microsoft Viva Engage interface. On the left, there's a sidebar with 'Home', 'Ayuko Takahashi', 'Explore' (Communities, Storylines, Dashboard), and 'Favorites' (with a note about keeping favorites at fingertips). The main area has a search bar 'Search Viva Engage'. It features a 'Share thoughts, ideas, or updates' section with icons for AT, Discussion, Question, Praise, Poll, and Drafts. A yellow box highlights a message: 'Your use of Viva Engage must follow the company's Internal Communications Policy.' Below this is a 'Copilot' promotion and a note about muting conversations. At the bottom is a graphic of three people interacting.

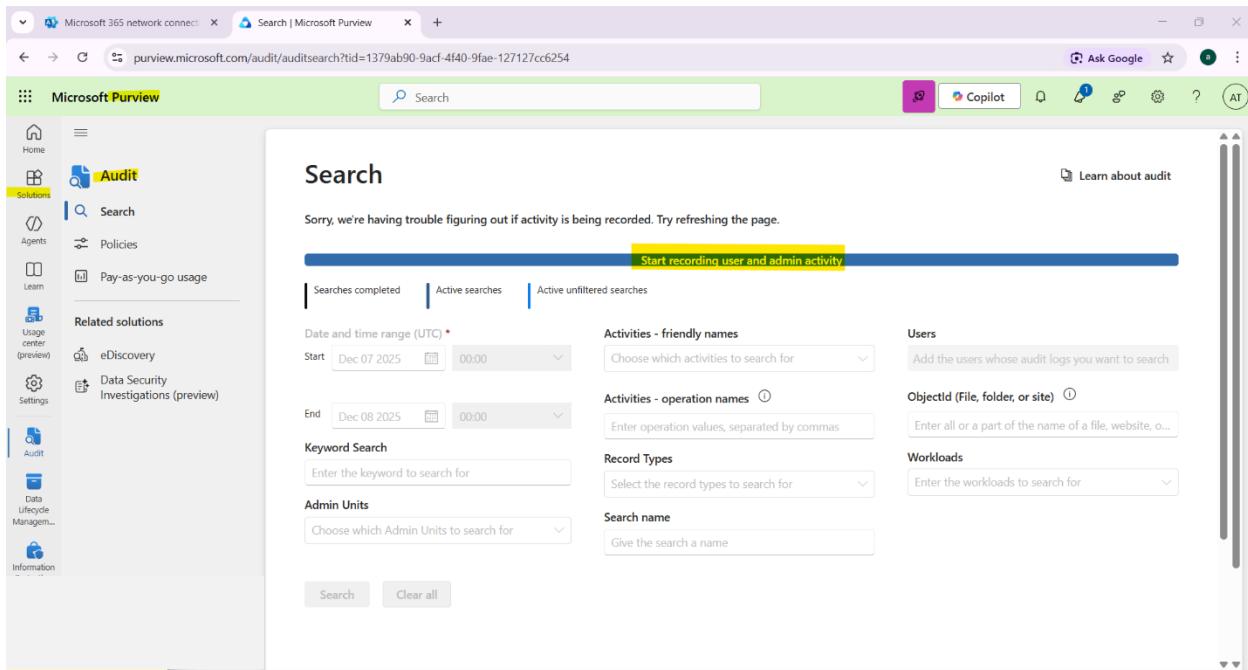
The Viva Engage usage policy was reviewed and confirmed as active for end users.

The screenshot shows the Microsoft Viva Engage interface. The layout is similar to the previous one, with a sidebar for 'Home', 'Ayuko Takahashi', 'Explore', and 'Favorites'. The main area features a prominent yellow box containing the 'TechSolutions Inc. Internal Communications Policy' title and a detailed description: 'Viva Engage is provided for internal collaboration only. Sharing confidential or sensitive company information outside of the organization is prohibited. All communication must follow company standards of conduct and professionalism.'

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

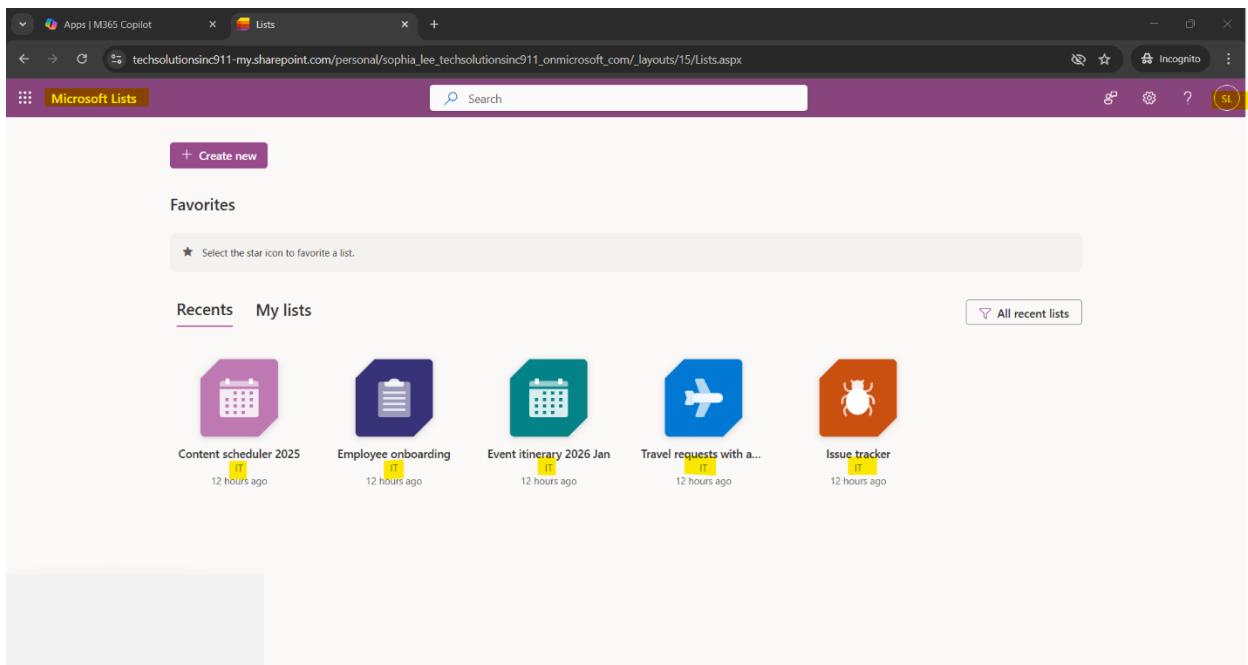
Monitoring, Audit Logging, and Alerting

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



The screenshot shows the Microsoft Purview Audit search interface. On the left, there's a sidebar with various navigation options like Home, Audit (which is selected), Search, Policies, and Pay-as-you-go usage. The main area is titled 'Search' and contains a message: 'Sorry, we're having trouble figuring out if activity is being recorded. Try refreshing the page.' Below this is a prominent yellow button labeled 'Start recording user and admin activity'. The search form includes fields for 'Date and time range (UTC)', 'Activities - friendly names', 'Users', 'Objectid (File, folder, or site)', 'Record Types', 'Workloads', and 'Search name'. There are also sections for 'Keyword Search' and 'Admin Units'. At the bottom are 'Search' and 'Clear all' buttons.

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



The screenshot shows the Microsoft Lists interface. At the top, it says 'Apps | M365 Copilot' and 'Lists'. The main area has a purple header bar with 'Microsoft Lists' and a search bar. Below this is a 'Favorites' section with a note to 'Select the star icon to favorite a list.' Under 'Recents' (which is underlined), there are five list items: 'Content scheduler 2025' (12 hours ago), 'Employee onboarding' (12 hours ago), 'Event itinerary 2026 Jan' (12 hours ago), 'Travel requests with a...' (12 hours ago), and 'Issue tracker' (12 hours ago). There's also a link to 'All recent lists'.

Sophia Lee created Lists on the IT site on SharePoint.

The screenshot shows the Microsoft Purview Audit search interface. The search parameters are set as follows:

- Date and time range (UTC) Start: Dec 05 2025, 00:00
- Date and time range (UTC) End: Dec 11 2025, 23:30
- Activities - friendly names: Choose which activities to search for
- Activities - operation names: ListCreated
- Record Types: SharePoint
- Search name: SharePoint Content Creation Activity
- Users: Sophia Lee
- Objectid (File, folder, or site): https://techsolutionsinc911.sharepoint.com/sites/IT
- Workloads: Enter the workloads to search for

The search results table shows 3 items found:

Search name	Job status	Prog...	Sear...	Total results	Creation ti...	Search performed by
SharePoint Content Creation Activity	Completed	100%	3m, 21s	0	Dec 11, 2025 9:53...	ayukotakahashi@techsolutionsinc911.onmicrosoft.com
SharePoint Content Update Activity	Completed	100%	3m, 16s	0	Dec 10, 2025 12:1...	ayukotakahashi@techsolutionsinc911.onmicrosoft.com
SharePoint Content Update Activity	Completed	100%	25s	0	Dec 9, 2025 11:31...	ayukotakahashi@techsolutionsinc911.onmicrosoft.com

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

The screenshot shows the Microsoft Purview Audit search interface. The search parameters are set as follows:

- Date and time range (UTC) Start: Dec 10 2025, 00:00
- Date and time range (UTC) End: Dec 11 2025, 00:00
- Activities - friendly names: Choose which activities to search for
- Activities - operation names: Enter operation values, separated by commas
- Record Types: Select the record types to search for
- Search name: Give the search a name

The search results table shows 4 items found:

Search name	Job status	Prog...	Sear...	Total results	Creation ti...	Search performed by
SharePoint Content Creation Activity	Completed	100%	3m, 21s	0	Dec 11, 2025 9:53...	ayukotakahashi@techsolutionsinc911.onmicrosoft.com
SharePoint Content Update Activity	Completed	100%	3m, 16s	0	Dec 10, 2025 12:1...	ayukotakahashi@techsolutionsinc911.onmicrosoft.com
SharePoint Content Update Activity	Completed	100%	25s	0	Dec 9, 2025 11:31...	ayukotakahashi@techsolutionsinc911.onmicrosoft.com

Platform Behavior Note:

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

This screenshot shows the Microsoft Purview Audit search interface. The left sidebar includes Home, Audit (selected), Search, Policies, and Pay-as-you-go usage. Under Related solutions, eDiscovery and Data Security Investigations (preview) are listed. The main area displays a search query from Friday, December 5, 2025, to Thursday, December 11, 2025, for ListCreated events. The results show 0 items found. A table header is present with columns for Date (UTC), IP Address, User, Record Type, Activity, Item, Admin Units, and Details. A message at the bottom states 'No data available'.

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

This screenshot shows the Microsoft Defender Cloud Apps Settings page. The left sidebar includes Cloud apps, Cloud security, SOC optimization, Reports, Learning hub, Trials, More resources, System, Audit, Data management, and Permissions. The main area shows the 'Cloud apps' settings under 'Settings'. In the 'Files' section, the 'Enable file monitoring' checkbox is checked. A success message box indicates 'Configuration saved successfully' at 12:08 PM. The 'Save' button is visible at the bottom.

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.

Create activity policy

Policy template *

Multiple failed user log on attempts to an ...

Policy name *

Multiple failed user log on attempts to an app

Policy severity *

Category *

Threat detection

Description

Alert when a single user attempts to log on to a single app, and fails more than 5 times within 5 minutes.

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

Repeated activity

Repeated activity by a single user

Minimum repeated activities: 5

Within timeframe: 5 minutes

In a single app

Count only unique target files or folders per user

Activities matching all of the following

Activity type equals Failed log on

User Name is set as Any role

Alerts

Create an alert for each matching event with the policy's severity

Save as default settings

Restore default settings

Send alert as email

Set failed 5 times repeated activities within 5 minutes.

The screenshot shows the Microsoft Defender interface for creating an activity policy. In the top right, there are tabs for 'Cloud apps', 'Cloud security', and 'Reports'. The left sidebar lists 'Cloud apps' (Cloud discovery, Cloud app catalog), 'OAuth apps', 'Activity log', 'Governance log', 'Policies' (Policy management, Policy templates), 'Cloud security' (selected), 'SOC optimization', and 'Reports'. The main area has a green header bar with a search bar and user profile. Below it, under 'Alerts', 'Send alert as email' is checked, and two recipient entries are shown: 'AyukoTakahashi@TechSolutionsInc911...' and 'ayukotakahashi1@TechSolutionsInc911...'. A yellow box highlights the 'Daily alert limit per policy' input field set to '1000'. Under 'Governance actions', 'All apps' is selected, and 'Notify user' is checked. A note says 'Notify user, Require user to sign in again'. Below this, other options like 'Notify additional users', 'Suspend Microsoft Entra user', 'Require user to sign in again', and 'Confirm user compromised' are listed. A note at the bottom says 'Enter a custom notification message:'. A vertical scrollbar is on the right.

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

This screenshot shows the same Microsoft Defender interface as above, but with a custom notification message entered. The 'Custom notification message' text box contains the following text:

```
Hi [UserName],  
We detected one or more unsuccessful attempts to sign in to your account ([UserEmail]) from a device or location that may not belong to you.  
This could happen if:  
• You recently mistyped your password  
• You tried signing in from a new device  
• Someone else attempted to access your account
```

A red warning message at the bottom says '⚠ User notification was not specified. Enter custom notification message in the text box above.' At the bottom right, there are 'Create' and 'Cancel' buttons. A vertical scrollbar is on the right.

Entered a custom notification message and click Create.

The screenshot shows the Microsoft Defender Policy management interface. The left sidebar includes sections for Cloud apps (Cloud discovery, Cloud app catalog, OAuth apps, Activity log, Governance log), Policies (Policy management, Policy templates), Cloud security, SOC optimization, and Reports. The main area is titled 'Policies' and shows tabs for Threat detection, Information protection, Conditional access, Shadow IT, and All policies (which is selected). A message at the top states: 'Starting June 15th, 2025, Microsoft Defender for Cloud Apps will adopt a dynamic threat detection model to enhance accuracy and responsiveness; policies that migrated will be disabled - For more information, visit our documentation.' Below this are filters for Name, Type (Activity policy), Status (ACTIVE, DISABLED), Severity (High, Medium, Low), and Category (Select risk category). A button for 'Advanced filters' is also present. The table lists one policy: 'Multiple failed user log on attempts to an app' (Alert when a single user attempts to log on to a single app, and fails more than 5 times within ...). The policy has 0 active incidents, is set to High severity, and was modified on Dec 11, 2025.

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

The screenshot shows a Microsoft login page with a 'Sign in to your account' header and a URL of 'login.microsoftonline.com/common/login'. A modal window titled 'Enter password' is displayed, asking for a password. It includes a message: 'Your account or password is incorrect. If you don't remember your password, reset it now.' Below the message is a 'Password' input field, a 'Forgot my password' link, and a 'Sign in' button. At the bottom right of the page, there are links for 'Terms of use', 'Privacy & cookies', and an ellipsis.

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

The screenshot shows the Microsoft Defender interface for 'Alerts'. The left sidebar has 'Investigation & response' selected, with 'Alerts' highlighted. The main area displays a single alert entry:

Alert name	Tags	Severity	Investigation state	Status	Category	Detection
Email messages removed after delivery		Informational	Pending action	In progress	Threat management	MDO

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.

The screenshot shows the 'Create activity policy' page. The left sidebar has 'Policies' selected, with 'Policy management' highlighted. The main form fields are:

- Policy template: No template
- Policy name: Mass deletion of files
- Policy severity: High (3 red bars)
- Category: Threat detection
- Description: Mass deletion of 30 files within 1 minute
- Act on:
 - Single activity: Every activity that matches the filters (radio button)
 - Repeated activity: Repeated activity by a single user (radio button, selected)
- Minimum repeated activities: 30
- Within timeframe: 1 minutes

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

In a single app

Count only unique target files or folders per user

Activities matching all of the following

App equals Microsoft Online Services, Microsoft Defender for Clo...

Activity type equals Delete

User Name is set as Any role

User From group does not equal External users

Add a filter

Alerts

Create an alert for each matching event with the policy's severity

Send alert as email

ayukotakahashi@techsolutionsinc.onmicrosoft.com

Save as default settings

Restore default settings

Set Filters to match activities.

Create an alert for each matching event with the policy's severity

Send alert as email

ayukotakahashi@techsolutionsinc.onmicrosoft.com

ayukotakahashi1@techsolutionsinc.onmicrosoft.com

Save as default settings

Restore default settings

Daily alert limit per policy: 1000

Send alerts to Power Automate

[Create a playbook in Power Automate](#)

Governance actions

Notify user

Notify additional users

Suspend Microsoft Entra user
For Microsoft Entra users

Require user to sign in again
For Microsoft Entra users

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

The screenshot shows the Microsoft Defender interface for creating an activity policy. On the left, a sidebar lists categories like Email & collaboration, Cloud apps, and Policies. The Policies section is expanded, showing Policy management, Policy templates, and Cloud security. Under Cloud security, there is a SOC optimization option. The main pane is titled 'All apps' and contains several policy options with checkboxes: 'Notify user' (checked), 'Notify additional users', 'Suspend Microsoft Entra user', 'Require user to sign in again' (checked), and 'Confirm user compromised'. Below these is a text area labeled 'Enter a custom notification message:' containing a rich text editor and a preview window. The preview window shows a message template with placeholder {{UserName}} and instructions about unusual file deletion activity. At the bottom right are 'Create' and 'Cancel' buttons.

Entered a custom notification message and click Create.

The screenshot shows the Microsoft Defender interface for managing policies. The left sidebar is identical to the previous screen. The main pane is titled 'Policies' and shows a list of existing policies. The 'All policies' tab is selected. A message at the top states: 'Starting June 15th, 2025, Microsoft Defender for Cloud Apps will adopt a dynamic threat detection model to enhance accuracy and responsiveness, policies that migrated will be disabled - For more information, visit our documentation.' Below this, there are filters for Name, Type (Activity policy), Status (ACTIVE), Severity (High), and Category (Select risk category). The table lists two policies: 'Multiple failed user log on attempts to an app' and 'Mass deletion of files'. Both policies are listed as '0 active incidents' and have a 'High' severity level. The 'Mass deletion of files' policy has a note: 'Mass deletion of 30 files within 1 minute.' At the bottom right of the table are 'Hide filters', 'Table settings', and a 'Count' dropdown.

Mass deletion of files policy has been created.

A screenshot of a web browser displaying the OneDrive interface. The left sidebar shows navigation links like Home, My files, Shared, Favorites, and Recycle bin. The main area is titled 'My files' and lists two folders: 'Attachments' (modified Monday at 11:2...) and 'Microsoft Copilot Chat Files' (modified Tuesday at 8:16 ...). At the bottom of the page, a notification bar indicates 'Deleted 32 items from My files'.

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

A screenshot of a web browser displaying the Microsoft Defender Alerts interface. The left sidebar shows navigation links for Exposure management, Investigation & response (Incidents & alerts, Incidents, Alerts), Hunting, Actions & submissions, Partner catalog, Threat intelligence, Assets, and Microsoft Sentinel. The main area is titled 'Alerts' and shows a table of alerts. The table includes columns for Alert name, Tags, Severity, Investigation state, Status, Category, and Detection. A single alert is listed: 'Email messages removed after delivery' (Severity: Informational, Status: Pending action, Category: Threat management, Detection: MDO). The alert status is 'New, In progress'.

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.

The screenshot shows the Microsoft Purview Policies page. On the left, there's a sidebar with various options like Home, Solutions, Agents, Usage center (preview), Forensic Evidence, Adaptive Protection, and related solutions such as Communication Compliance, Data Security Investigations (preview), and Data Loss Prevention. The main area is titled 'Policies' and displays three categories: Policy warnings (0), Policy recommendations (0), and Healthy policies (0). A yellow box at the top right says 'Create a data leak policy'. Below it, there's a note about data leaks and a 'Policy name' field containing 'DLP Breach Alert Policy'. The 'User scope' dropdown is set to 'Include all users and groups (Recommended for best coverage)'. A 'Create policy' button is visible.

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

The screenshot shows the Microsoft Purview Policies page again. The sidebar and main interface are similar to the previous screenshot. A yellow box on the right says 'Your data leak policy is being created'. It includes a note about staying up-to-date and two checked notification settings: 'Email me when policies have unresolved warnings' and 'Email me when new high severity alerts are generated'. There's also a 'Update notification settings' button. Below this, a section titled 'What happens next?' provides information about the creation process and alert handling.

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

Policy template

Name and description

Users and groups

Content to prioritize

Triggering event

Trigger thresholds

Indicators

Finish

Choose thresholds for triggering events

The policy will start assigning risk scores to activity only when specific thresholds are met for the exfiltration activities you selected as the triggering event. Thresholds are based on the number of events recorded for an activity per day. You can use recommended thresholds or specify your own.

Apply built-in thresholds RECOMMENDED

Choose your own thresholds

Sending email with attachments to recipients outside the organization

Total number of activities
1 per day

Number of activities for emails containing sensitive info types
1 per day

Number of activities for emails matching priority content
1 per day

Number of activities performed in which target is unallowed domain
1 per day

Activity is above user's usual activity for the day

Back Next Cancel

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

It'll take a few minutes to create the policy. You'll see it listed on the Policies tab.

Once the policy is active, it could take at least 24 hours for the triggering event to occur and score user activity, at which point the first alert is generated. If admin notification are turned on, you'll get an email when this alert happens.

You or someone on your team will triage the alert and confirm it to a case for further investigation or dismiss it as normal behavior.

After reviewing a few alerts, fine tune your policy to control how many alerts are generated, what activities are detected, and more. We'll provide recommendations along the way.

Stay updated

Stay up-to-date on alerts across your org

Choose what emails to receive for alerts.

When a new policy generates its first alert

When new high severity alerts are generated

Weekly email summarizing policies that have unresolved warnings

Manage all IRM email notifications

Save email preferences

Done

Set notification option.

The screenshot shows the Microsoft Purview Policies page. On the left sidebar under 'Insider Risk Management', the 'Policies' section is selected. In the main content area, a policy named 'DLP Breach Alert Pol' is listed with a status of 'recommendation'. To the right, the details for the 'DLP Breach Alert Policy' are shown, including its triggering event (User performs an exfiltration activity), thresholds (Custom thresholds), indicators (Sharing SharePoint files with people outside the organization, etc.), and detection options.

The data leak policy has been created.

The screenshot shows the Microsoft Purview Settings page. Under 'Role groups', a new role group named 'Insider Risk Management Admins' is being created. The table lists various roles, with 'Insider Risk Management Admin...' checked. The right pane displays the role group's name ('Insider Risk Management Admins'), description (''), and members ('Sophia Lee', 'Alex Wong').

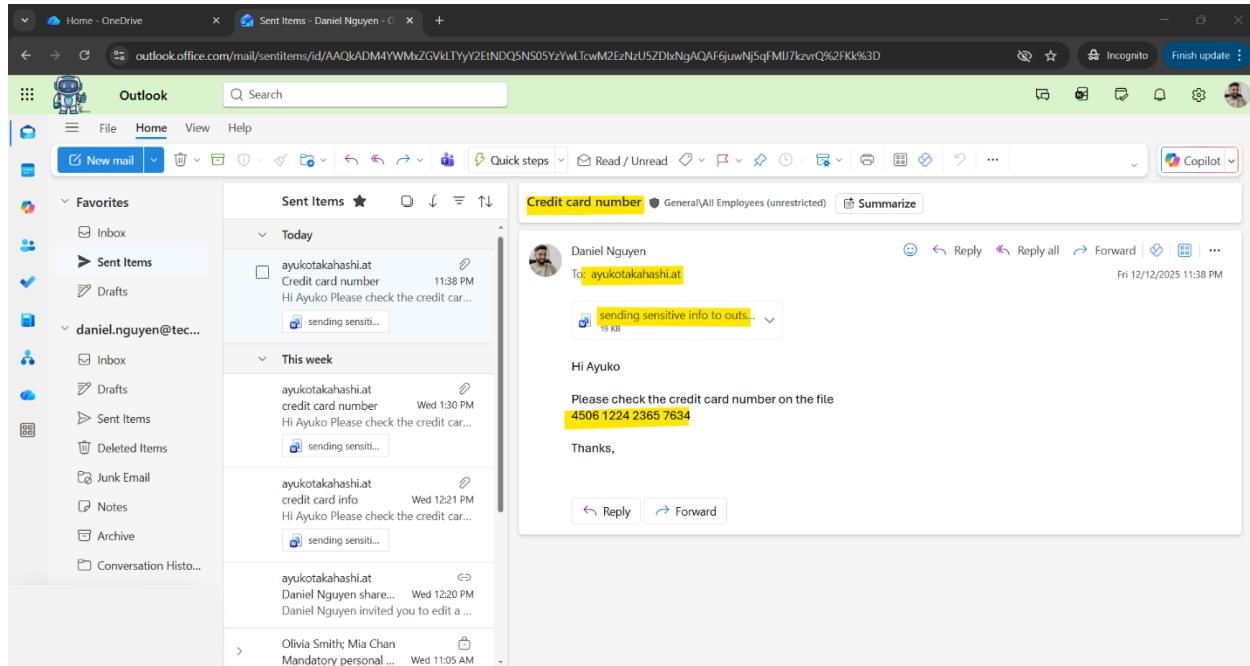
As an option, assign Insider Risk Management Admins role to two IT members to give access Alert check on Purview.

The screenshot shows the Microsoft Purview admin center interface. On the left, the navigation menu includes Home, Solutions, Usage center (preview), Settings, Insider Risk Management (preview), Data Security Investigation (preview), Data Loss Prevention, and Compliance alerts. Under Settings, Roles and scopes is expanded, showing Microsoft Entra ID, Role groups, Adaptive scopes, Administrative units, Data connectors, Device onboarding, Optical character recognition (OCR), Solution settings, Communication Compliance, and Compliance Manager. The main content area displays a list of role groups. A specific role group, "Insider Risk Management Analysts", is selected and detailed on the right. The role group name is "Insider Risk Management Analysts". It includes roles such as Case Management, Insider Risk Management Analysis, Insider Risk Management Graph Reader, Purview Agent Analysis, Purview Copilot Workspace Contributor, and View-Only Case. Members in the role group are listed as Sophia Lee and Alex Wong.

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

This screenshot is similar to the previous one but shows a different role group, "Insider Risk Management Investigators". The structure is identical, with the role group name being "Insider Risk Management Investigators". It includes roles like Case Management, Custodian, Data Security Investigation Contributor, Insider Risk Management Investigation, Purview Agent Analysis, Purview Copilot Workspace Contributor, Review, and View-Only Case. Members listed are Alex Wong and Sophia Lee.

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.

User Details Panel - Microsoft 365 | Alerts | Microsoft Purview | Alerts - Microsoft Defender

Microsoft Purview

Insider Risk Management

Reports > Alerts

Alerts

All alerts Confirmed alerts Dismissed alerts

Date range December 2025 Show or hide reports

Summary

Alerts generated No chart available

The filters you applied can't be displayed in this chart. We recommend revising your filters.

Alerts addressed No chart available

The filters you applied can't be displayed in this chart. We recommend revising your filters.

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.

The screenshot shows the Microsoft 365 Admin Center interface with the 'Usage' section selected. On the left, a sidebar lists various service categories like Microsoft 365 Copilot, Exchange, Forms, etc. The main area displays a chart titled 'Active users' showing the number of unique active users per day from December 4 to December 8. The chart includes data for Microsoft 365 Apps, Exchange, OneDrive, SharePoint, Viva Engage, and Microsoft Teams. The user count starts at 0 on Dec 4, rises to a peak of about 11 on Dec 7, and then stabilizes around 9.

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

The screenshot shows the Microsoft 365 Admin Center interface with the 'Overview' section selected. The left sidebar is identical to the Usage screen. The main area contains several summary cards: 'Active users - Microsoft 365 Services' (11 active users), 'Active users - Microsoft 365 Apps' (Total number of unique active users per Microsoft 365 App, no information available), 'Email activity' (168 activities, showing counts for Sent, Received, and Read actions), 'Microsoft Teams activity' (70 files stored), 'OneDrive files' (Latest number of files in OneDrive, 11.8MB), and 'SharePoint files' (98 files stored). Each card has a 'View more' button.

Usage - Microsoft 365 admin center

admin.cloud.microsoft/?#/reportsUsage

Microsoft 365 admin center

Overview

Reports

- Microsoft 365 Copilot
- Exchange
- Forms
- Microsoft 365 apps
- Microsoft Browser
- Microsoft Teams
- Microsoft Teams apps
- OneDrive
- Project
- SharePoint
- Visio
- Viva Engage

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

Date	Files Stored
Dec 5	0
Dec 6	2.9MB
Dec 7	5.9MB
Dec 8	8.8MB
Dec 9	11.8MB

View more

SharePoint files

98 files stored

Latest number of files in SharePoint

File Type	Count
View...	63
File...	21
Shar...	1

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 time period

Usage - Microsoft 365 admin center

admin.cloud.microsoft/?#/reportsUsage/EmailClients

Microsoft 365 admin center

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

Number of daily unique users by app

Date	Outlook (Windows)	Outlook (Mac)
Dec 3	9	0
Dec 4	9	0
Dec 5	9	0
Dec 6	9	0
Dec 7	9	0
Dec 8	9	0
Dec 9	9	0

Apps

Number of unique users by app over the selected time period

App Type	Count
Outlook (Windows)	10
Outlook (Mac)	2
Outlook on the web	0
Outlook (mobile)	0

Versions

Number of unique users for each version of Outlook (Windows)

Version	Count
Outlook 2021	10
Outlook 2019	0
Outlook 2016	0
Outlook 2013	0
Outlook 2010	0
Outlook 2007	0

Information is concealed for privacy. To see identifiable information, learn about showing these details in reports.

Export

Username

Last activity date (UTC)

Outlook (Windows)

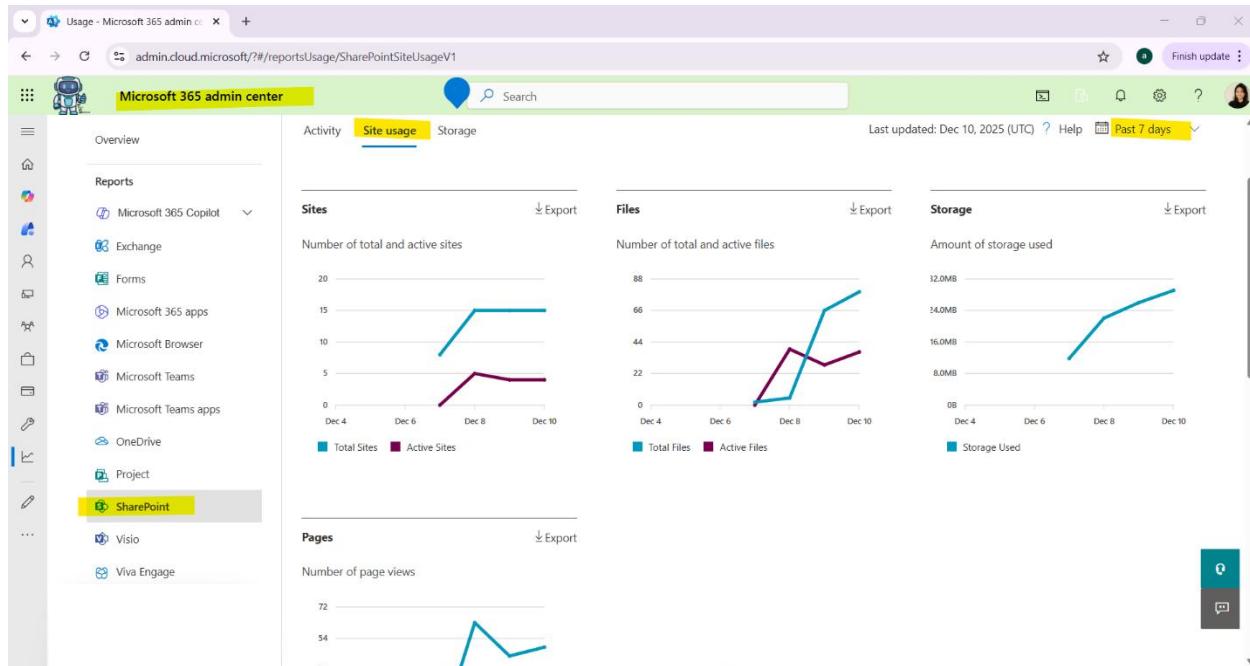
Outlook (Mac)

Outlook on the web

Outlook (mobile)

Choose

3B034BCR0C951071E96475 Tuesday, Dec 9, 2025



The screenshot shows the Power Automate interface with the 'Create' button selected in the sidebar. A modal window titled 'Build a scheduled cloud flow' is open, prompting the user to 'Start from scratch'. The modal includes fields for 'Flow name' (Monthly M365 Usage Report Delivery), 'Run this flow *' (Starting 12/8/25 at 12:00 AM, Repeat every 1 Month), and a note that it will run monthly. Below the modal, there are sections for 'Examples:' (Automate team reminders to submit expense reports, Auto-backup data to designated storage on a regular basis) and 'Top picks' (Folio, time, By Microsoft Power Automate Community).

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

The screenshot shows the Microsoft Power Automate interface for creating a new flow. The flow consists of a 'Recurrence' trigger followed by a 'Send an email (V2)' action. The 'Send an email (V2)' action is configured with the following parameters:

- To ***: A list of recipients including Alex Wong, Sophia Lee, Ava Takahashi, and Ethan Patel.
- Subject ***: Monthly Microsoft 365 Usage Report
- Body ***:
 - Normal font, Arial, 15px.
 - Hello Team,
 - This is the scheduled monthly notification that Microsoft 365 usage reports are now available for review.
 - You can access the reports here: <https://admin.microsoft.com/#/reportsUsage>
 - These reports include:
 - Email activity (Exchange)
 - SharePoint site usage
 - OneDrive activity
 - Teams activity
 - User sign-in and app usage trends

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

The screenshot shows the Microsoft Power Automate interface with the flow successfully tested. The 'Test Flow' pane indicates:

- Test Flow** button
- Manually** radio button selected: Perform the starting action to trigger it.
- Automatically** section: There are no runs for this flow.
- Test** and **Cancel** buttons at the bottom right.

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

The screenshot shows the Microsoft Outlook web interface. On the left, the navigation pane displays 'Favorites' with sections for 'Inbox' (5 items), 'Drafts', and an account section for 'sophia.lee@techsol...'. The main pane shows a 'Focused' inbox with several messages from team members. One message from Ayuko Takahashi is selected, titled 'Monthly Microsoft 365 Usage Report'. The message body contains a summary of the report and a link to access it. The footer of the message includes a note from Ayuko Takahashi as Cloud Administrator.

The screenshot shows the Microsoft Entra admin center. The left sidebar is under 'Entra ID' and has a 'Roles & admins' section highlighted. The main page shows the 'Reports Reader | Assignments' section. It displays a table of users assigned to the 'Reports Reader' role, including Sophia Lee, Ethan Patel, Ava Takahashi, and Alex Wong. Each user's name is preceded by a checkbox.

Name	UserName	Type	Scope
Sophia Lee	sophia.lee@techsolutionsinc911.onmicrosoft...	User	Directory
Ethan Patel	ethan.patel@techsolutionsinc911.onmicrosoft...	User	Directory
Ava Takahashi	ava.takahashi@techsolutionsinc911.onmicrosoft...	User	Directory
Alex Wong	alex.wong@techsolutionsinc911.onmicrosoft...	User	Directory

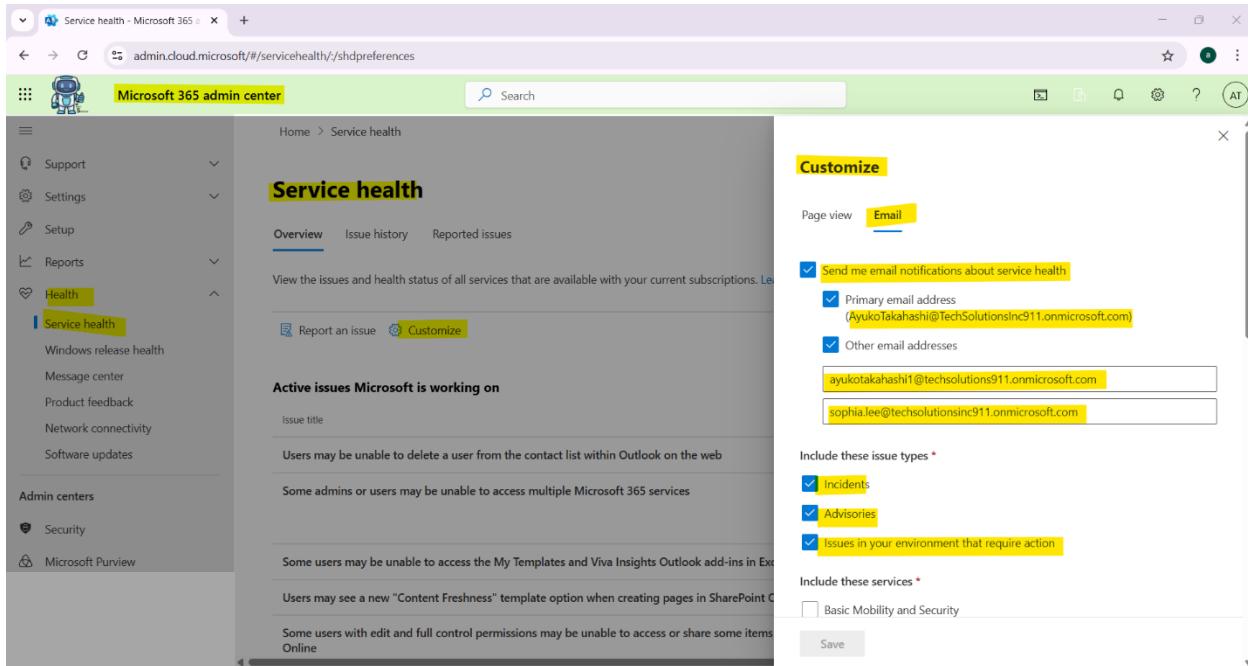
Assign IT members and Department head as Reports Reader role for reading the usage report.

The screenshot shows the Microsoft 365 Admin Center interface. The left sidebar has a 'Reports' section with various service icons. The main content area is titled 'Usage' and displays a message: 'Microsoft 365 usage reports show how people in your business are using Microsoft 365 services. Reports are available for the last 7 days, 30 days, 90 days, and 180 days. Data won't exist for all reporting periods right away. The reports become available within 48 hours.' Below this, a sub-section for 'Microsoft 365 Copilot' is shown with the message 'There is no data for this report.' A 'Past 30 days' button is visible at the bottom of this section.

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.



The screenshot shows the Microsoft 365 Admin Center with the 'Service health' page open. On the left, the navigation menu includes 'Support', 'Settings', 'Setup', 'Reports', 'Health' (which is selected), and 'Service health'. Under 'Service health', there are links for 'Windows release health', 'Message center', 'Product feedback', 'Network connectivity', and 'Software updates'. The main content area displays 'Active issues Microsoft is working on' with several listed items. To the right, a 'Customize' pane is open, showing settings for email notifications. It includes a 'Page view' dropdown set to 'Email', a checked checkbox for 'Send me email notifications about service health', and input fields for 'Primary email address' (ayuko.takahashi@TechSolutionsInc911.onmicrosoft.com) and 'Other email addresses' (ayukotakahashif@techsolutions911.onmicrosoft.com, sophia.lee@techsolutionsinc911.onmicrosoft.com). There are also sections for 'Include these issue types' (Incidents, Advisories, Issues in your environment that require action), 'Include these services' (Basic Mobility and Security), and a 'Save' button.

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

Report an issue Customize

Search

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

This screenshot shows the Microsoft 365 Admin Center's Service Health page. On the left, there's a navigation sidebar with links like Support, Settings, and Health. Under Health, 'Service health' is selected. The main area displays 'Active issues Microsoft is working on' with a search bar and a text input field. Below that is a 'Service status' table showing various Microsoft services and their current status. To the right, a section titled 'Health issues affecting Exchange Online' lists specific problems with Exchange Online, each accompanied by an 'Advisory' icon.

Service health - Microsoft 365

admin.cloud.microsoft/#/servicehealth

Microsoft 365 admin center

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 Microsoft Purview

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

This screenshot shows the Microsoft 365 Admin Center's Service Health page. The navigation sidebar is identical to the previous one. The main area displays a 'Service status' table where every service listed is marked as 'Healthy'. There are no 'advisories' or other issues present.

The screenshot shows the Microsoft 365 admin center with the 'Service health' page selected. The left sidebar has 'Health' highlighted. The main area displays a table titled 'Service status' with two columns: 'Service' and 'Status'. Most services listed are marked as 'Healthy' with green checkmarks. The table includes entries for Microsoft Power Automate, Microsoft Power Automate in Microsoft 365, Microsoft Purview, Microsoft Stream, Microsoft Viva, Planner, Power Apps, Power Apps in Microsoft 365, Power BI, Project for the web, Sway, Universal Print, and Windows Autopatch. A single entry, 'Windows release health', is listed under 'Message center' and is marked as 'Advisory' with a yellow exclamation mark. The top right of the dashboard features a search bar and various navigation icons.

Service	Status
MICROSOFT POWER AUTOMATE	Healthy
Microsoft Power Automate in Microsoft 365	Healthy
Microsoft Purview	Healthy
Microsoft Stream	Healthy
Microsoft Viva	Healthy
Planner	Healthy
Power Apps	Healthy
Power Apps in Microsoft 365	Healthy
Power BI	Healthy
Project for the web	Healthy
Sway	Healthy
Universal Print	Healthy
Windows Autopatch	Healthy
Windows release health	Advisory

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.