NIC Cloud Connect

Oslo Spektrum
November 7 - 9

NIC Cloud Connect

Julian Rasmussen

Are your organization and data Copilot Ready?

POINT:TAKEN

Data governance

Why data governance?

Delve never changes any permissions, so you'll only see documents that you already have access to.

Why data governance?

Real-time intelligent assistance

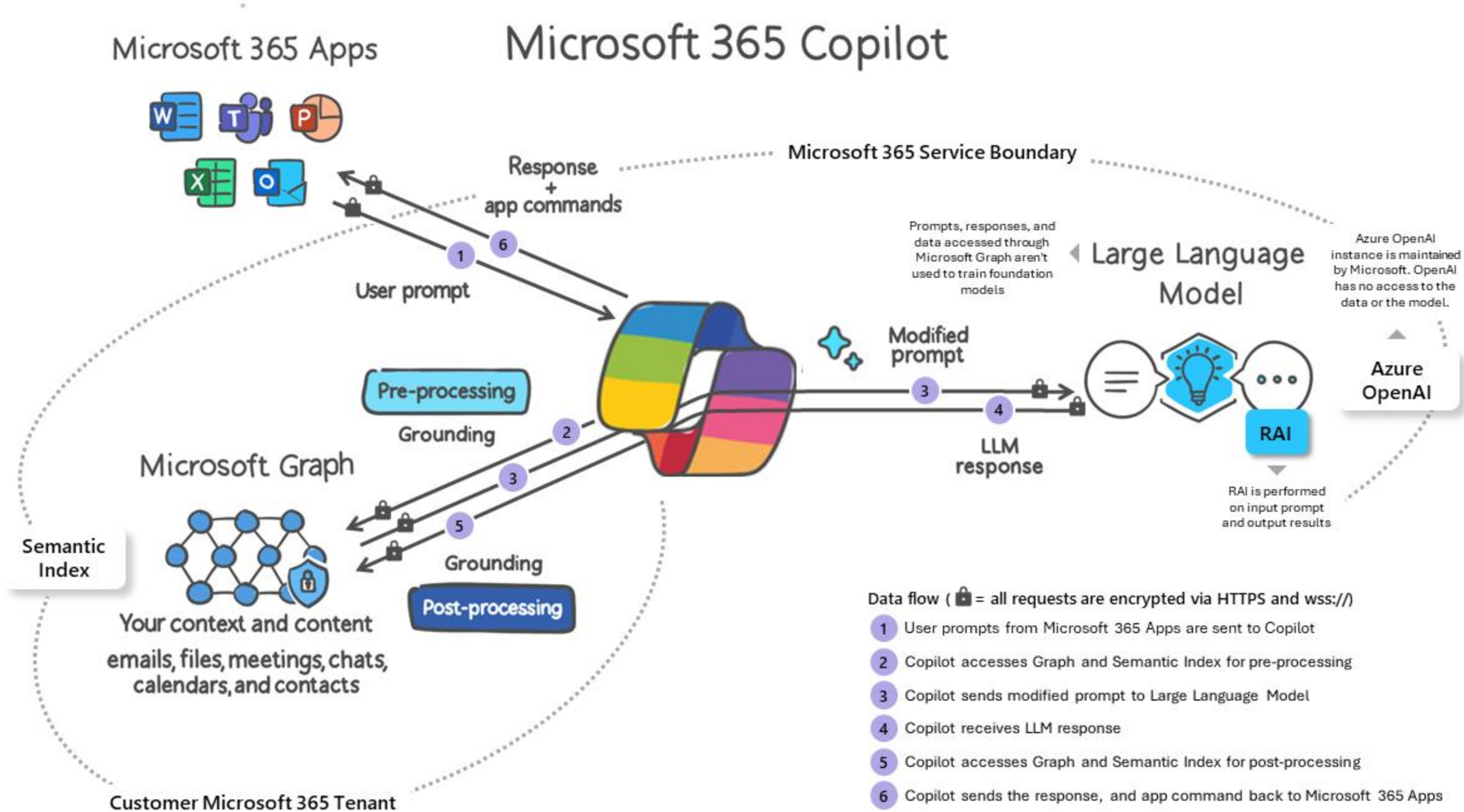
Microsoft 365 Copilot - FAQ

- Copilot is available to users with Business Standard and Premium plans and Microsoft 365 E3 and E5 plans at $30 for a new step-up license
- Only available for Enterprise customers and with a minimum buy in for 300 seats

Microsoft 365 Copilot

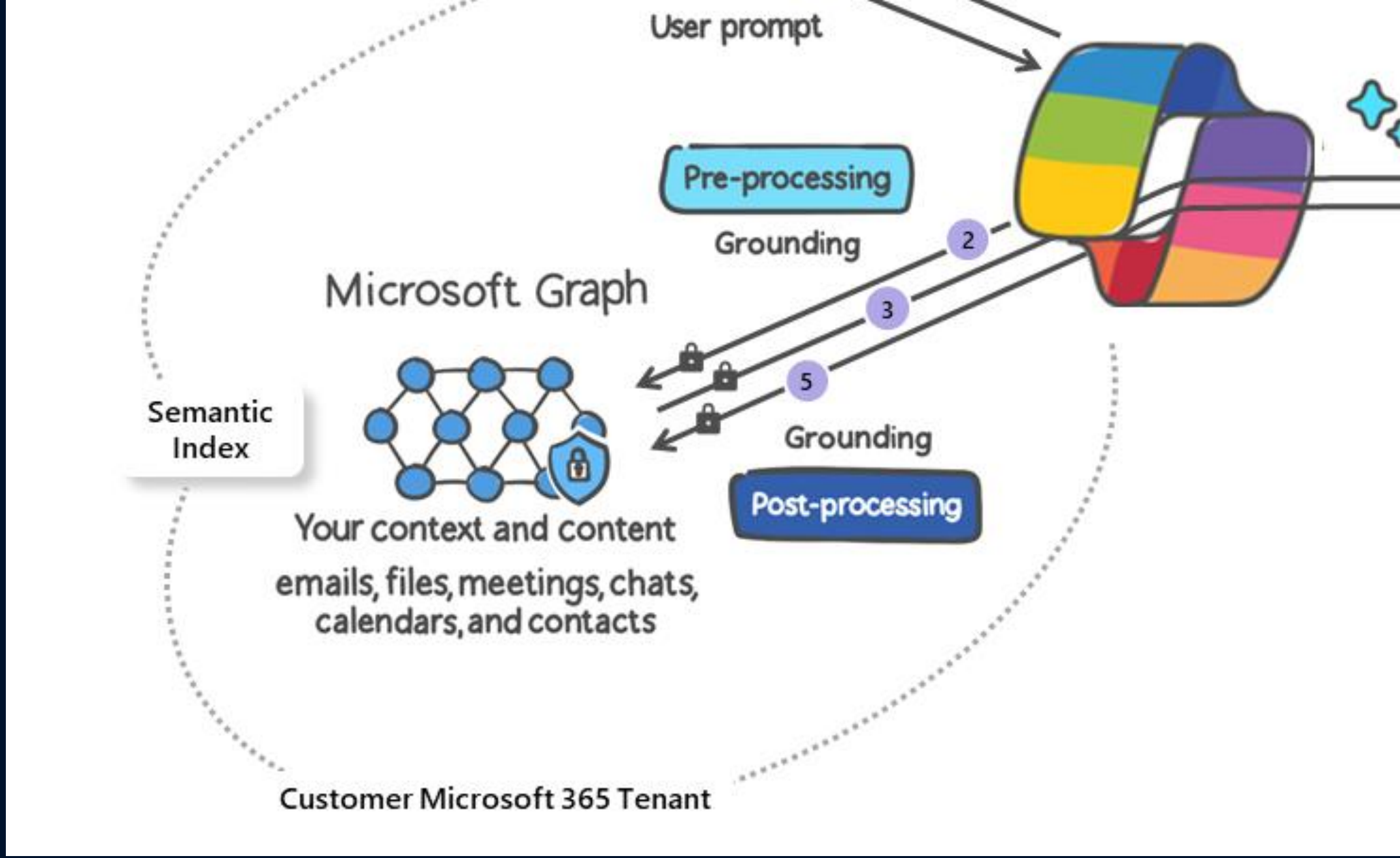
- YOUR data
- NOT used to train the LLM
- Your data is PROTECTED

Microsoft 365 Copilot

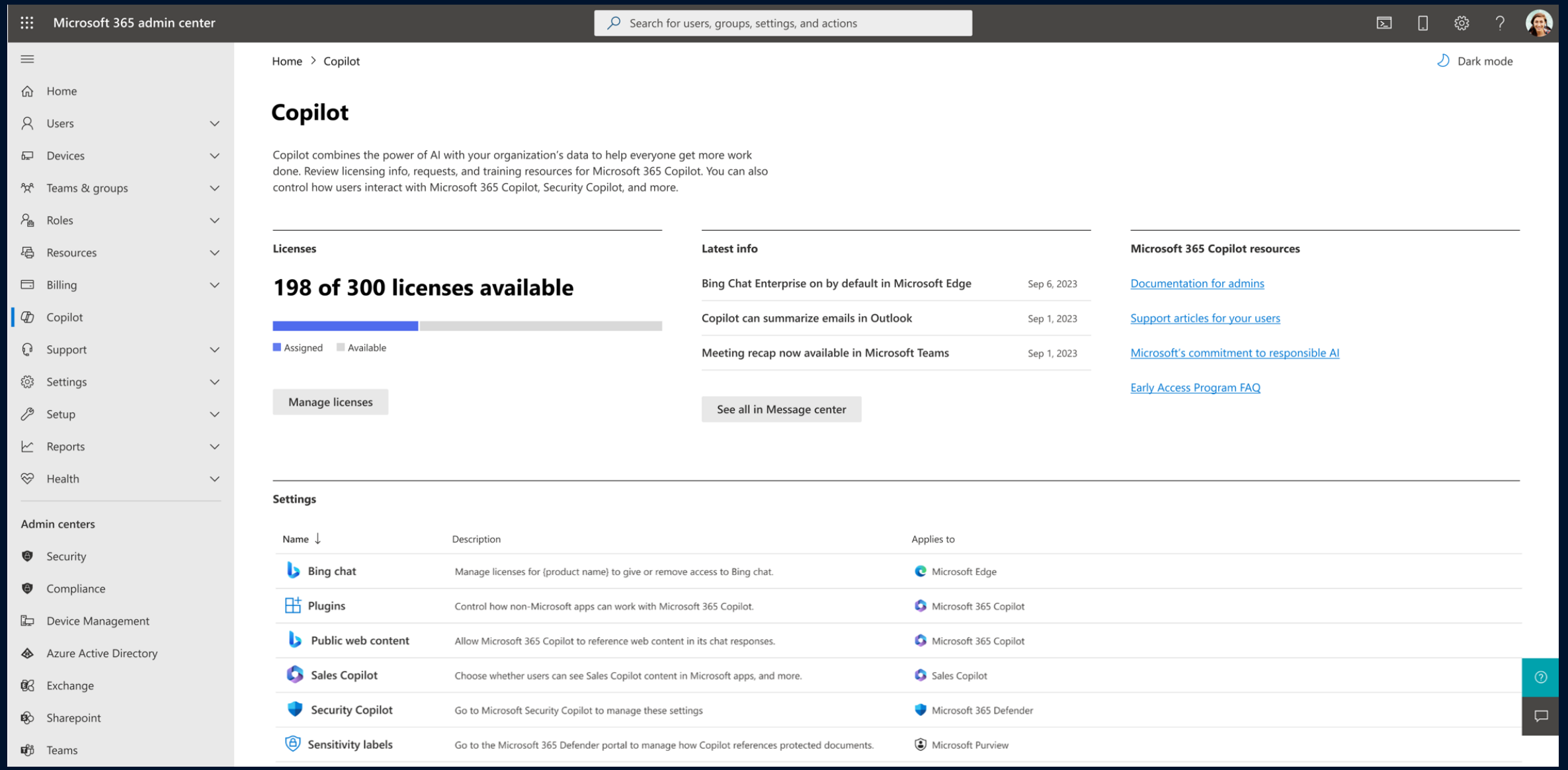


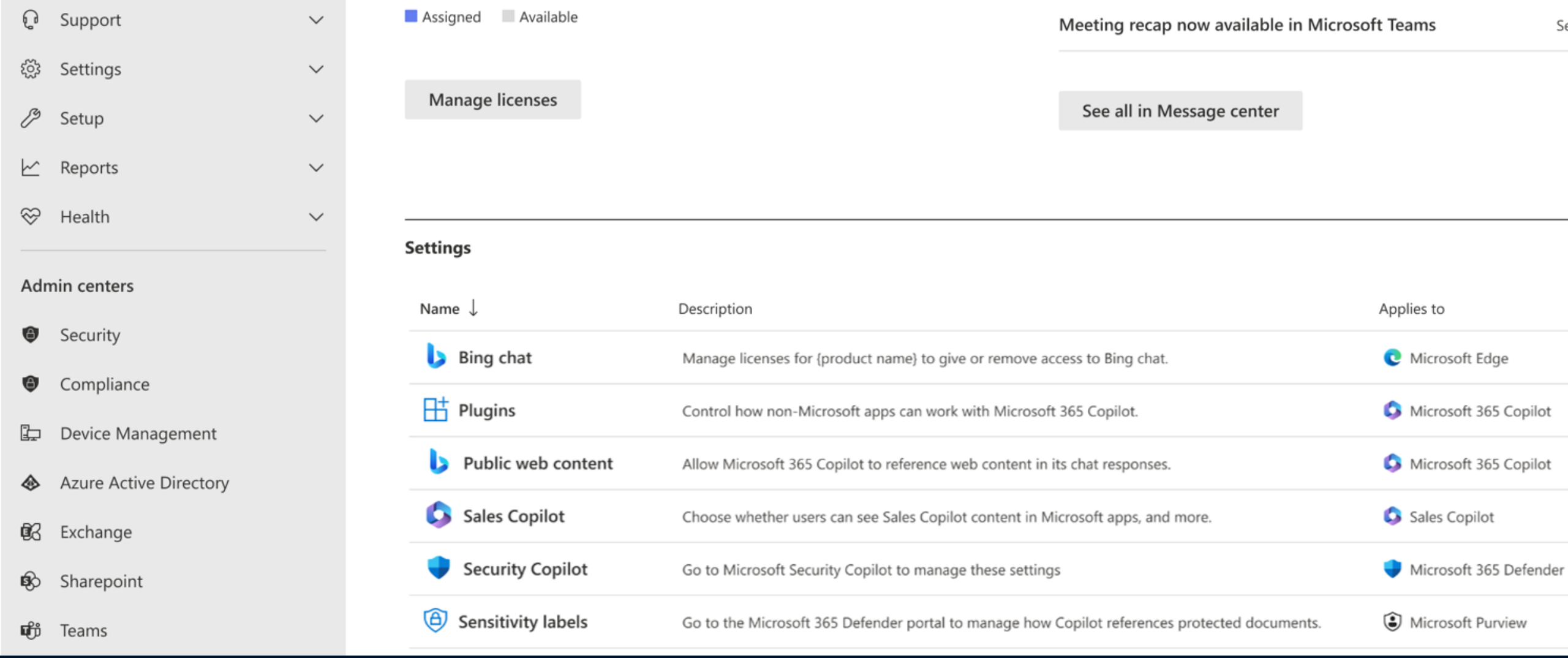
Data flow (= all requests are encrypted via HTTPS and wss://)

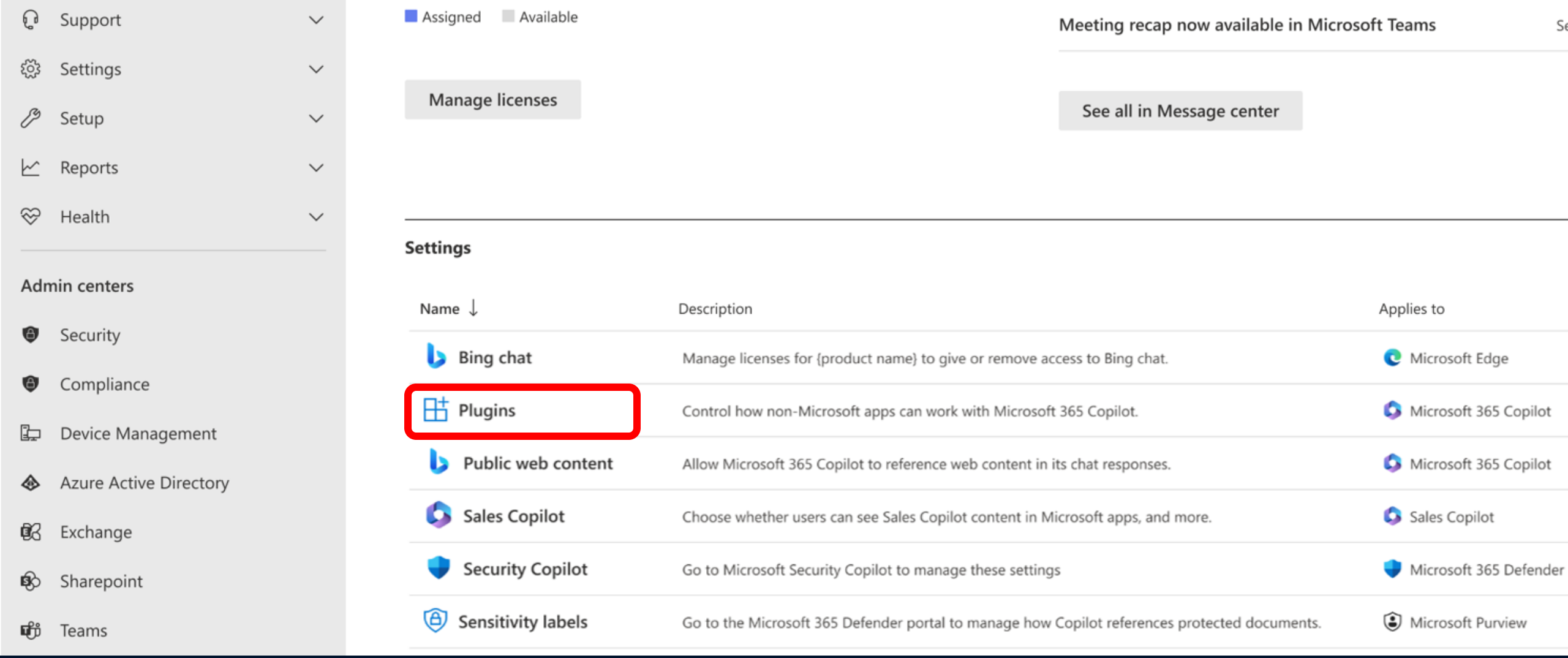
1. User prompts from Microsoft 365 Apps are sent to Copilot
2. Copilot accesses Graph and Semantic Index for pre-processing
3. Copilot sends modified prompt to Large Language Model
4. Copilot receives LLM response
5. Copilot accesses Graph and Semantic Index for post-processing
6. Copilot sends the response, and app command back to Microsoft 365 Apps

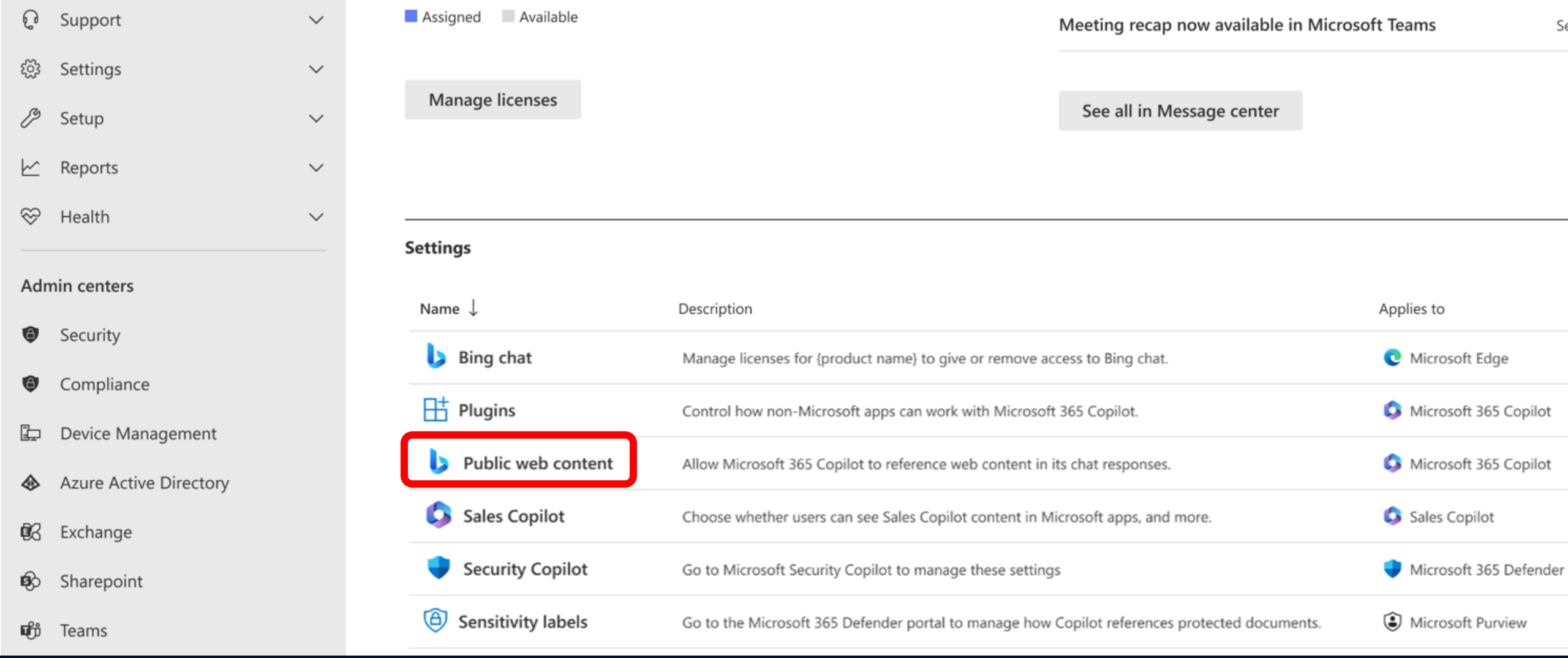

User prompt
Pre-processing
Grounding
2
3
5
Microsoft Graph
Semantic Index
Grounding
Post-processing
Your context and content
emails, files, meetings, chats, calendars, and contacts
Customer Microsoft 365 Tenant

Microsoft 365 Copilot – Admin Center




Support
Settings
Setup
Reports
Health
Admin centers
Security
Compliance
Device Management
Azure Active Directory
Exchange
Sharepoint
Teams
Assigned
Available
Manage licenses
Meeting recap now available in Microsoft Teams
See all in Message center
Settings
Name
Description
Applies to
Bing chat
Manage licenses for {product name} to give or remove access to Bing chat.
Microsoft Edge
Plugins
Control how non-Microsoft apps can work with Microsoft 365 Copilot.
Microsoft 365 Copilot
Public web content
Allow Microsoft 365 Copilot to reference web content in its chat responses.
Microsoft 365 Copilot
Sales Copilot
Choose whether users can see Sales Copilot content in Microsoft apps, and more.
Sales Copilot
Security Copilot
Go to Microsoft Security Copilot to manage these settings
Microsoft 365 Defender
Sensitivity labels
Go to the Microsoft 365 Defender portal to manage how Copilot references protected documents.
Microsoft Purview


Support
Settings
Setup
Reports
Health
Admin centers
Security
Compliance
Device Management
Azure Active Directory
Exchange
Sharepoint
Teams
Assigned
Available
Manage licenses
Meeting recap now available in Microsoft Teams
See all in Message center
Settings
Name
Description
Applies to
Bing chat
Manage licenses for {product name} to give or remove access to Bing chat.
Microsoft Edge
Plugins
Control how non-Microsoft apps can work with Microsoft 365 Copilot.
Microsoft 365 Copilot
Public web content
Allow Microsoft 365 Copilot to reference web content in its chat responses.
Microsoft 365 Copilot
Sales Copilot
Choose whether users can see Sales Copilot content in Microsoft apps, and more.
Sales Copilot
Security Copilot
Go to Microsoft Security Copilot to manage these settings
Microsoft 365 Defender
Sensitivity labels
Go to the Microsoft 365 Defender portal to manage how Copilot references protected documents.
Microsoft Purview


Support
Settings
Setup
Reports
Health
Admin centers
Security
Compliance
Device Management
Azure Active Directory
Exchange
Sharepoint
Teams
Assigned
Available
Manage licenses
Meeting recap now available in Microsoft Teams
See all in Message center
Settings
Name
Description
Applies to
Bing chat
Manage licenses for {product name} to give or remove access to Bing chat.
Microsoft Edge
Plugins
Control how non-Microsoft apps can work with Microsoft 365 Copilot.
Microsoft 365 Copilot
Public web content
Allow Microsoft 365 Copilot to reference web content in its chat responses.
Microsoft 365 Copilot
Sales Copilot
Choose whether users can see Sales Copilot content in Microsoft apps, and more.
Sales Copilot
Security Copilot
Go to Microsoft Security Copilot to manage these settings
Microsoft 365 Defender
Sensitivity labels
Go to the Microsoft 365 Defender portal to manage how Copilot references protected documents.
Microsoft Purview

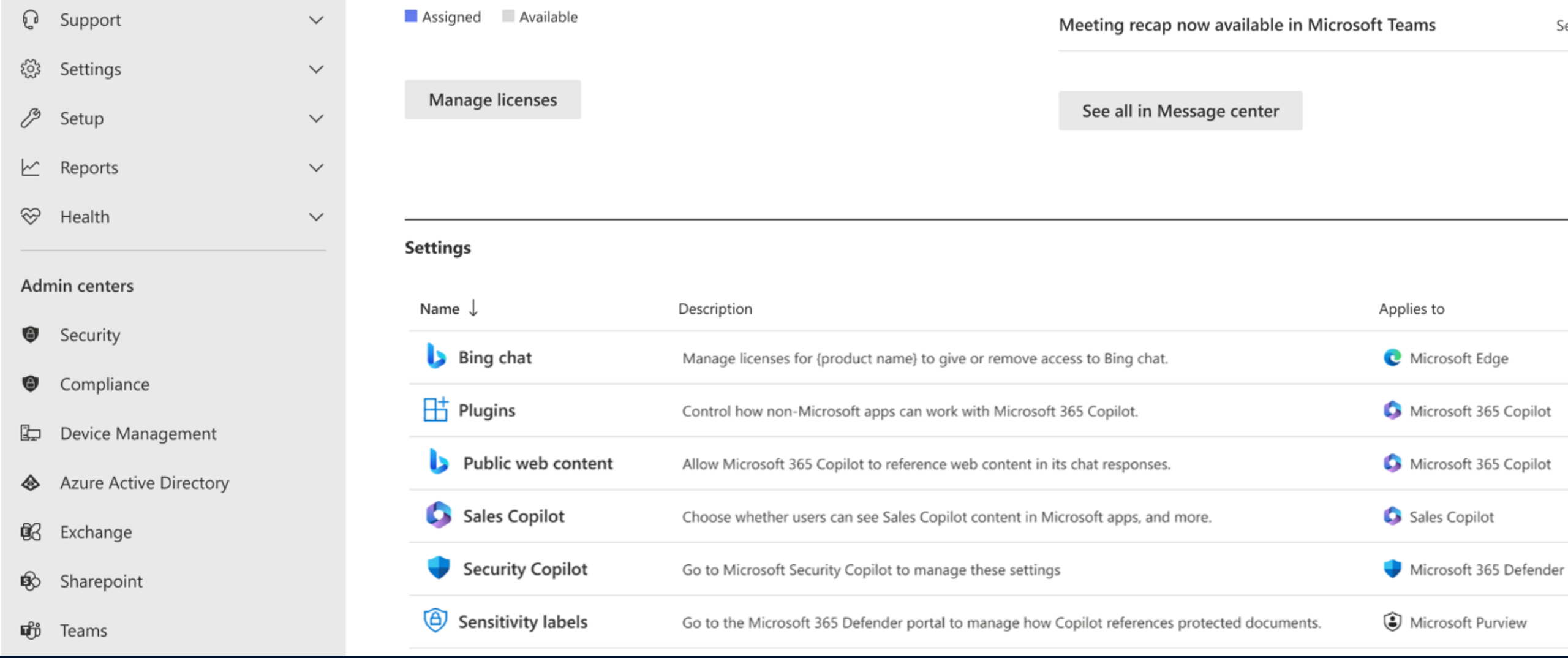
Public web content in Microsoft 365 Copilot

Allow Microsoft 365 Copilot to reference public web content in its chat responses. When allowed, customer content will be sent to Bing outside your tenancy. Your use of Bing is governed by the Microsoft Privacy Statement. The Data Protection Addendum does not apply to your use of Bing. This only affects the Microsoft 365 Copilot App in Teams and the Microsoft 365 Copilot chat experiences in Bing and Edge.

Learn more about Microsoft 365 Copilot

Active

Change


Support
Settings
Setup
Reports
Health
Admin centers
Security
Compliance
Device Management
Azure Active Directory
Exchange
Sharepoint
Teams
Assigned
Available
Manage licenses
Meeting recap now available in Microsoft Teams
See all in Message center
Settings
Name
Description
Applies to
Bing chat
Manage licenses for {product name} to give or remove access to Bing chat.
Microsoft Edge
Plugins
Control how non-Microsoft apps can work with Microsoft 365 Copilot.
Microsoft 365 Copilot
Public web content
Allow Microsoft 365 Copilot to reference web content in its chat responses.
Microsoft 365 Copilot
Sales Copilot
Choose whether users can see Sales Copilot content in Microsoft apps, and more.
Sales Copilot
Security Copilot
Go to Microsoft Security Copilot to manage these settings
Microsoft 365 Defender
Sensitivity labels
Go to the Microsoft 365 Defender portal to manage how Copilot references protected documents.
Microsoft Purview

Reports > Usage

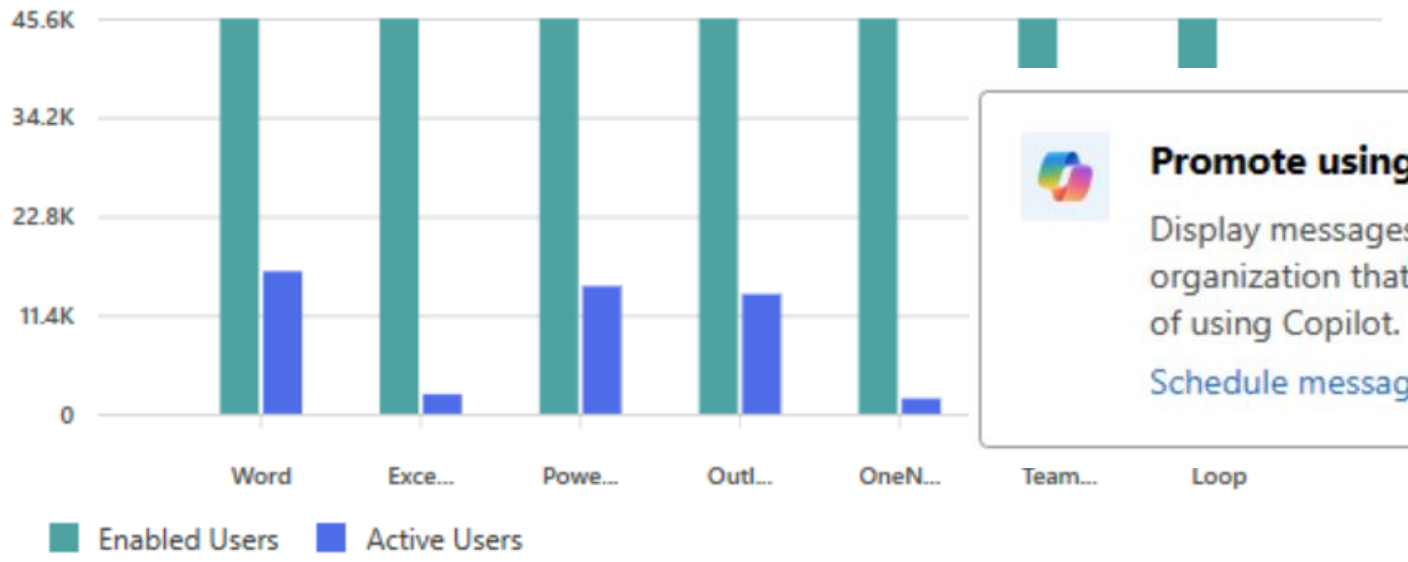
Reports > Usage

Adoption

Microsoft 365 Copilot adoption by product

Current | Trend

Adoption status of Microsoft 365 Copilot over the selected time period



Promote using Microsoft 365 Copilot

Display messages to targeted users in your organization that encourage them to seee the benefits of using Copilot.

Schedule message PREVIEW

Security, privacy, and data residency

Zero trust - principles

"A complete zero trust security posture may never be fully achieved, but specific initiatives can be undertaken today" - Gartner

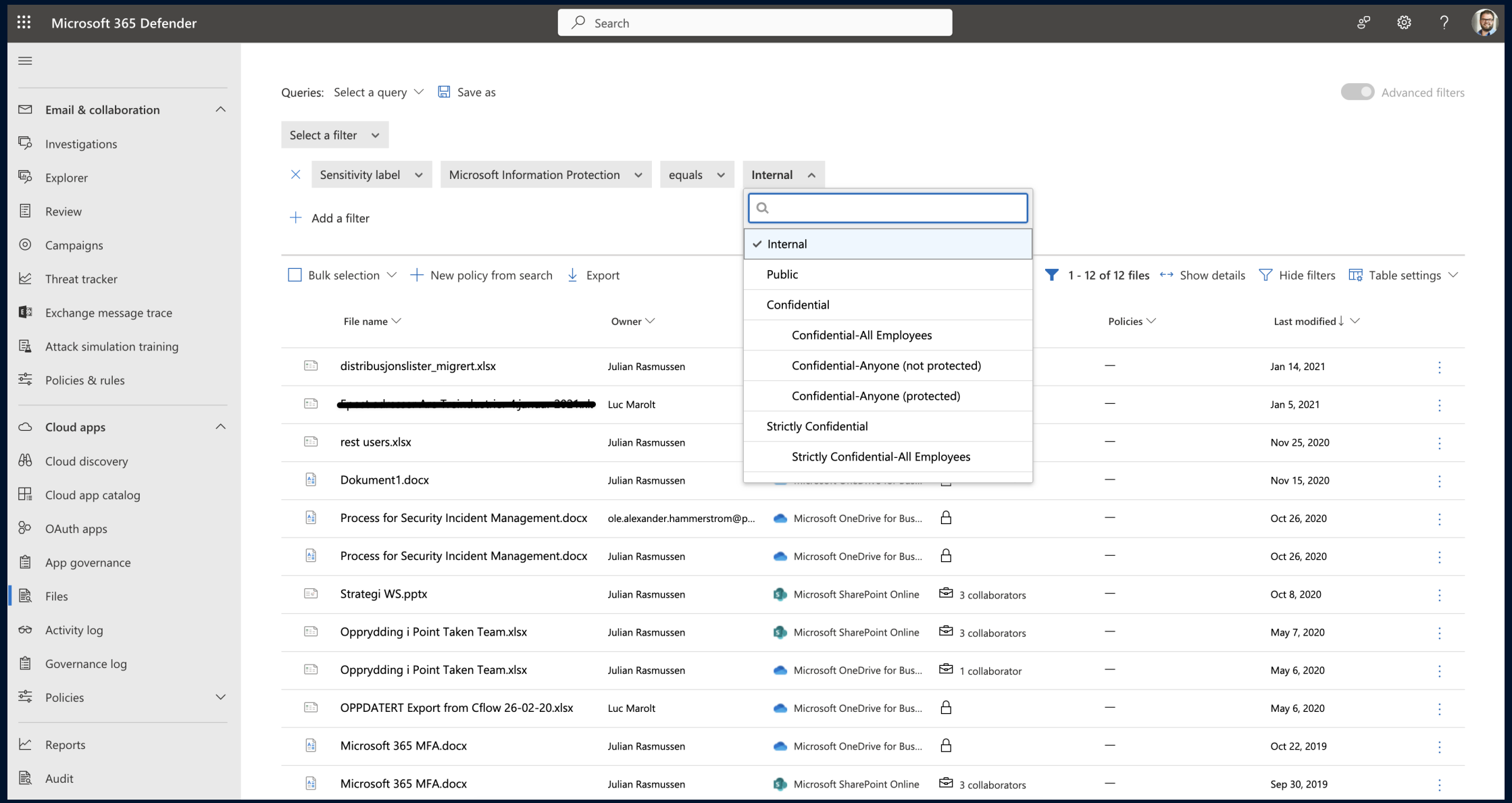
Zero trust!


Identity
Phising resistant
Endpoint
Constantly monitored
Network
Network traffic is encrypted end-to-end
Data
Automated classifications

DEMO

Just enough Access

Defender for Cloud apps



t a filter

Sensitivity label | Microsoft Information Protection | equals | Internal

dd a filter

- Internal
- Public
- Confidential
  - Confidential-All Employees
  - Confidential-Anyone (not protected)
  - Confidential-Anyone (protected)
- Strictly Confidential
  - Strictly Confidential-All Employees

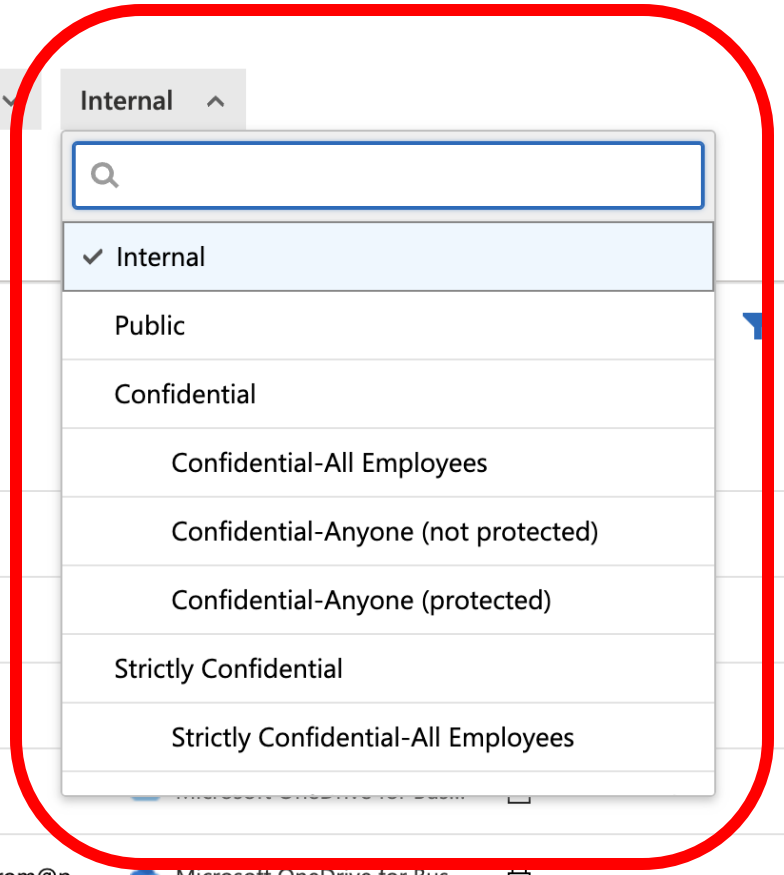
lk selection | New policy from search | Export | 1 - 12 of 12 files | Show details | Hide filters | Table settings

File name	Owner			Policies	Last modified
distribusjonslister_migrert.xlsx	Julian Rasmussen			—	Jan 14, 2021
[redacted]	Luc Marolt			—	Jan 5, 2021
rest users.xlsx	Julian Rasmussen			—	Nov 25, 2020
Dokument1.docx	Julian Rasmussen			—	Nov 15, 2020
Process for Security Incident Management.docx	ole.alexander.hammerstrom@p...	Microsoft OneDrive for Bus...		—	Oct 26, 2020
Process for Security Incident Management.docx	Julian Rasmussen	Microsoft OneDrive for Bus...		—	Oct 26, 2020
Strategi WS.pptx	Julian Rasmussen	Microsoft SharePoint Online	3 collaborators	—	Oct 8, 2020
Opprydding i Point Taken Team.xlsx	Julian Rasmussen	Microsoft SharePoint Online	3 collaborators	—	May 7, 2020
Opprydding i Point Taken Team.xlsx	Julian Rasmussen	Microsoft OneDrive for Bus...	1 collaborator	—	May 6, 2020
OPPDATERT Export from Cflow 26-02-20.xlsx	Luc Marolt	Microsoft OneDrive for Bus...		—	May 6, 2020

t a filter

Sensitivity label | Microsoft Information Protection | equals | Internal

dd a filter



lk selection | New policy from search | Export | 1 - 12 of 12 files | Show details | Hide filters | Table settings

File name	Owner			Policies	Last modified
distribusjonslister_migrert.xlsx	Julian Rasmussen			—	Jan 14, 2021
[redacted]	Luc Marolt			—	Jan 5, 2021
rest users.xlsx	Julian Rasmussen			—	Nov 25, 2020
Dokument1.docx	Julian Rasmussen			—	Nov 15, 2020
Process for Security Incident Management.docx	ole.alexander.hammerstrom@p...	Microsoft OneDrive for Bus...		—	Oct 26, 2020
Process for Security Incident Management.docx	Julian Rasmussen	Microsoft OneDrive for Bus...		—	Oct 26, 2020
Strategi WS.pptx	Julian Rasmussen	Microsoft SharePoint Online	3 collaborators	—	Oct 8, 2020
Opprydding i Point Taken Team.xlsx	Julian Rasmussen	Microsoft SharePoint Online	3 collaborators	—	May 7, 2020
Opprydding i Point Taken Team.xlsx	Julian Rasmussen	Microsoft OneDrive for Bus...	1 collaborator	—	May 6, 2020
OPPDATERT Export from Cflow 26-02-20.xlsx	Luc Marolt	Microsoft OneDrive for Bus...		—	May 6, 2020

t a filter

Sensitivity label | Microsoft Information Protection | equals | Internal

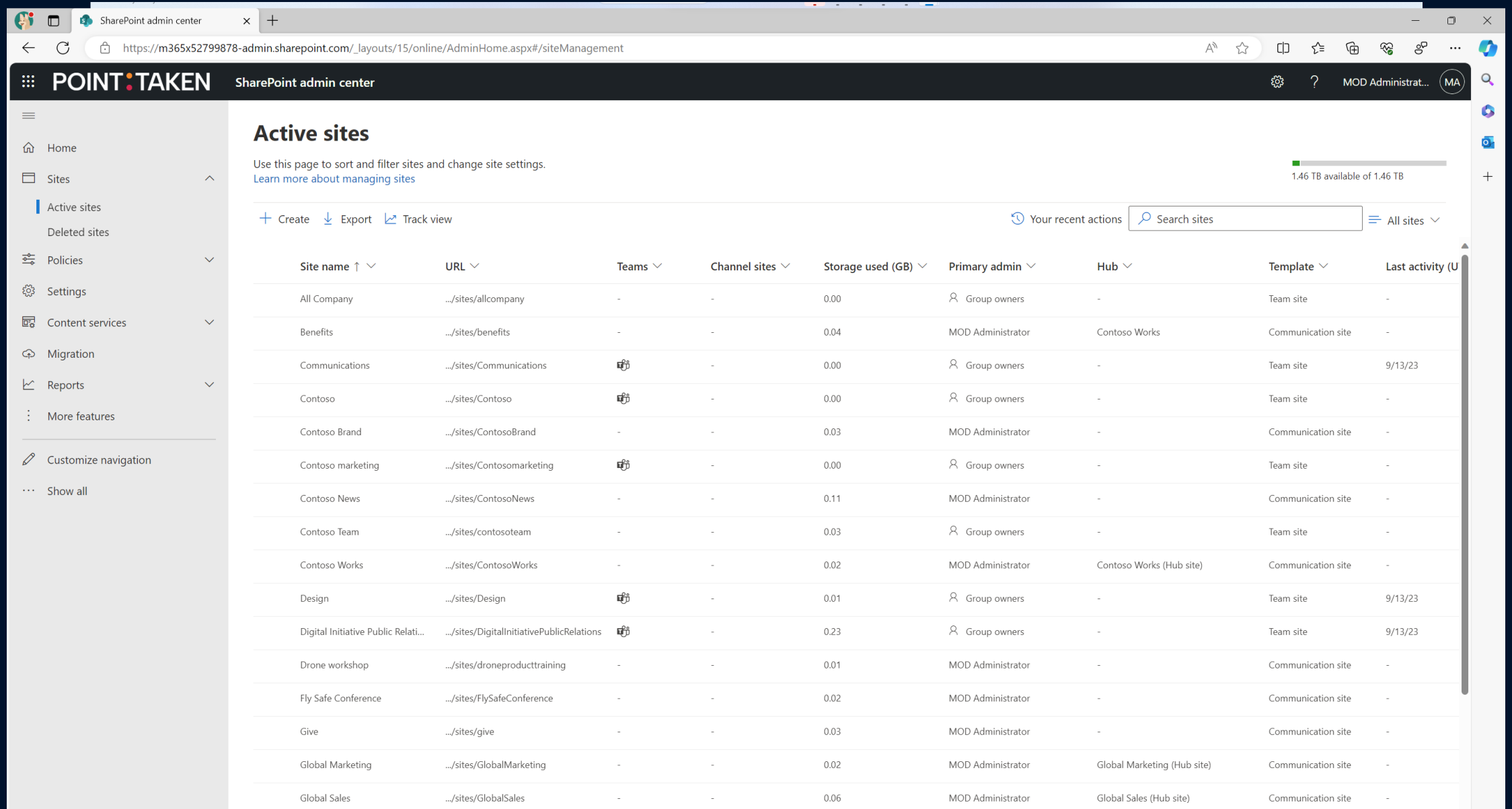
dd a filter

Internal
Public
Confidential
Confidential-All Employees
Confidential-Anyone (not protected)
Confidential-Anyone (protected)
Strictly Confidential
Strictly Confidential-All Employees

lk selection | New policy from search | Export | 1 - 12 of 12 files | Show details | Hide filters | Table settings

File name	Owner			Policies	Last modified
distribusjonslister_migrert.xlsx	Julian Rasmussen			—	Jan 14, 2021
[redacted]	Luc Marolt			—	Jan 5, 2021
rest users.xlsx	Julian Rasmussen			—	Nov 25, 2020
Dokument1.docx	Julian Rasmussen			—	Nov 15, 2020
Process for Security Incident Management.docx	ole.alexander.hammerstrom@p...	Microsoft OneDrive for Bus...		—	Oct 26, 2020
Process for Security Incident Management.docx	Julian Rasmussen	Microsoft OneDrive for Bus...		—	Oct 26, 2020
Strategi WS.pptx	Julian Rasmussen	Microsoft SharePoint Online	3 collaborators	—	Oct 8, 2020
Opprydding i Point Taken Team.xlsx	Julian Rasmussen	Microsoft SharePoint Online	3 collaborators	—	May 7, 2020
Opprydding i Point Taken Team.xlsx	Julian Rasmussen	Microsoft OneDrive for Bus...	1 collaborator	—	May 6, 2020
OPPDATERT Export from Cflow 26-02-20.xlsx	Luc Marolt	Microsoft OneDrive for Bus...		—	May 6, 2020

SharePoint Admin Center



SharePoint admin center

https://m365x52799878-admin.sharepoint.com/_layouts/15/online/AdminHome.aspx#/siteManagement

POINT TAKEN | SharePoint admin center | MOD Administrat... | MA

- Home
- Sites
  - Active sites
  - Deleted sites
- Policies
- Settings
- Content services
- Migration
- Reports
- More features
- Customize navigation
- Show all

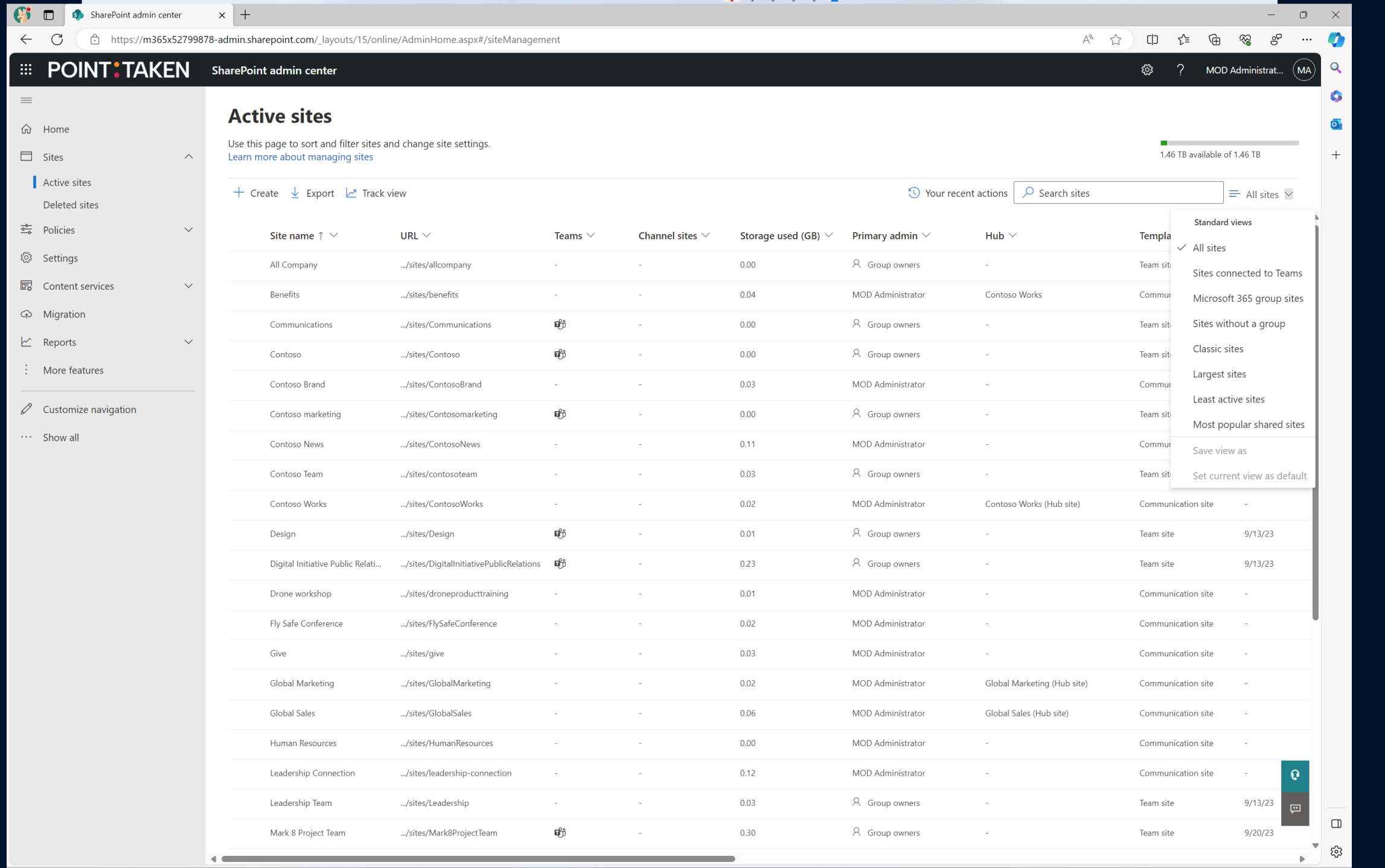
Active sites

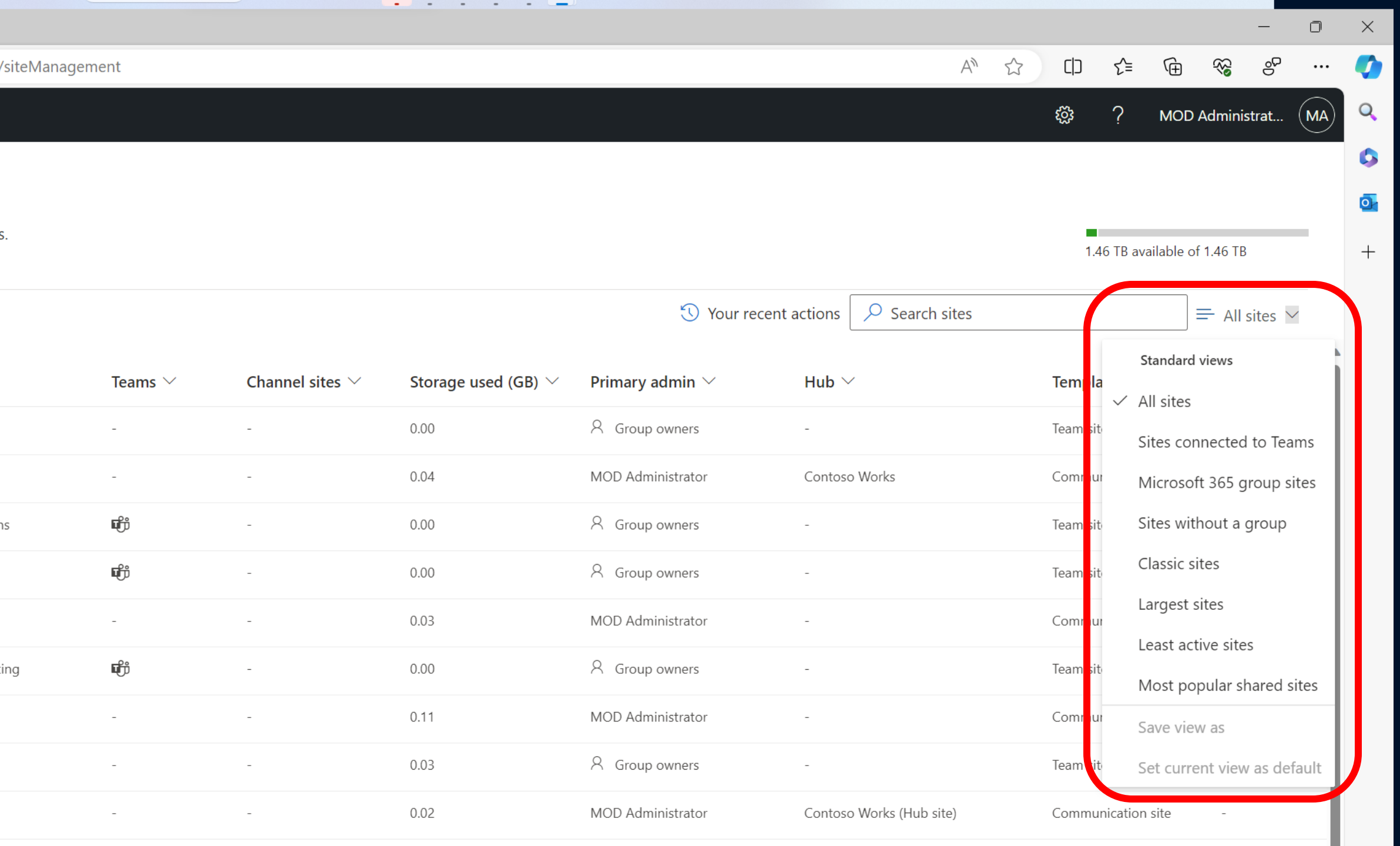
Use this page to sort and filter sites and change site settings.
Learn more about managing sites

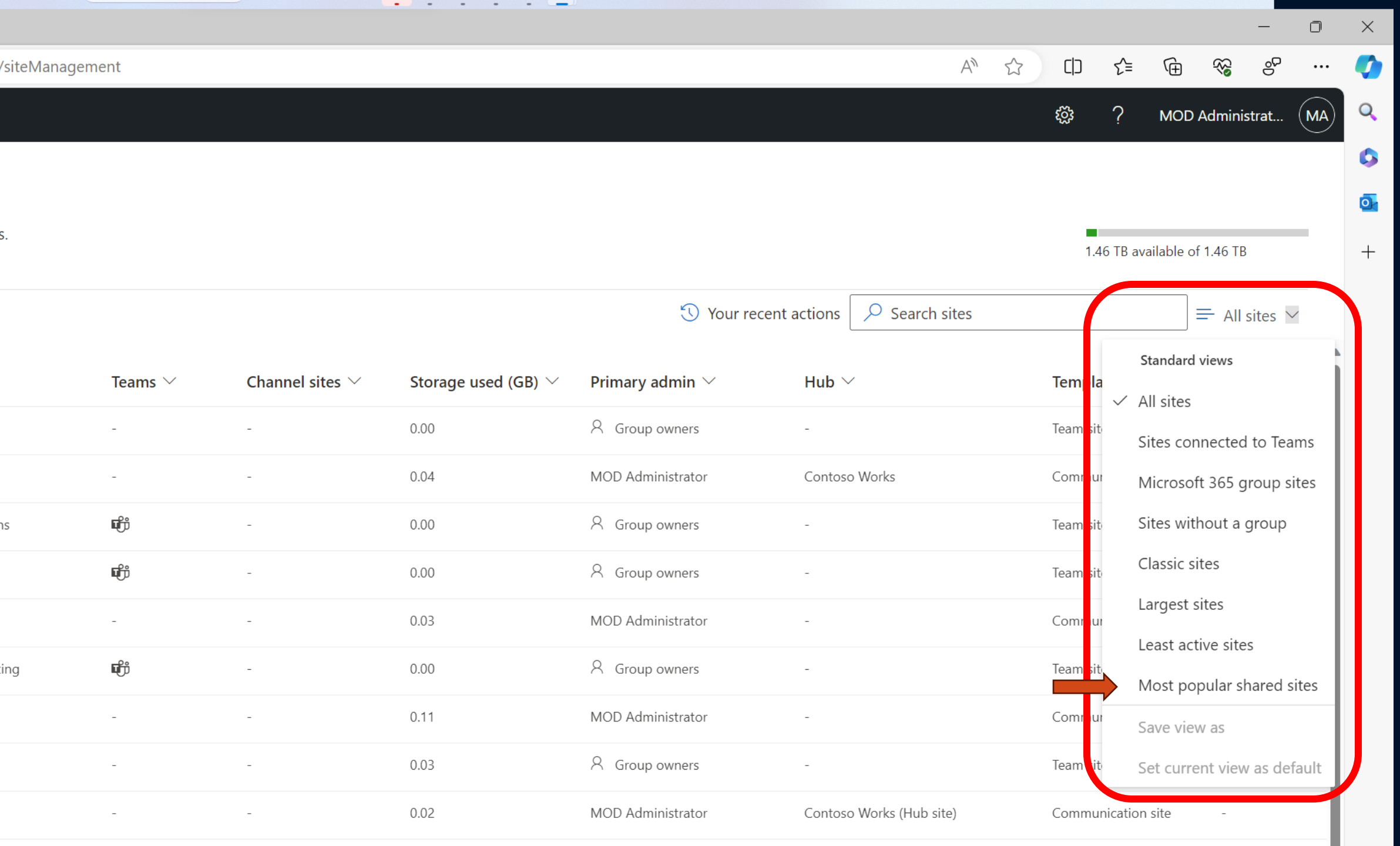
1.46 TB available of 1.46 TB

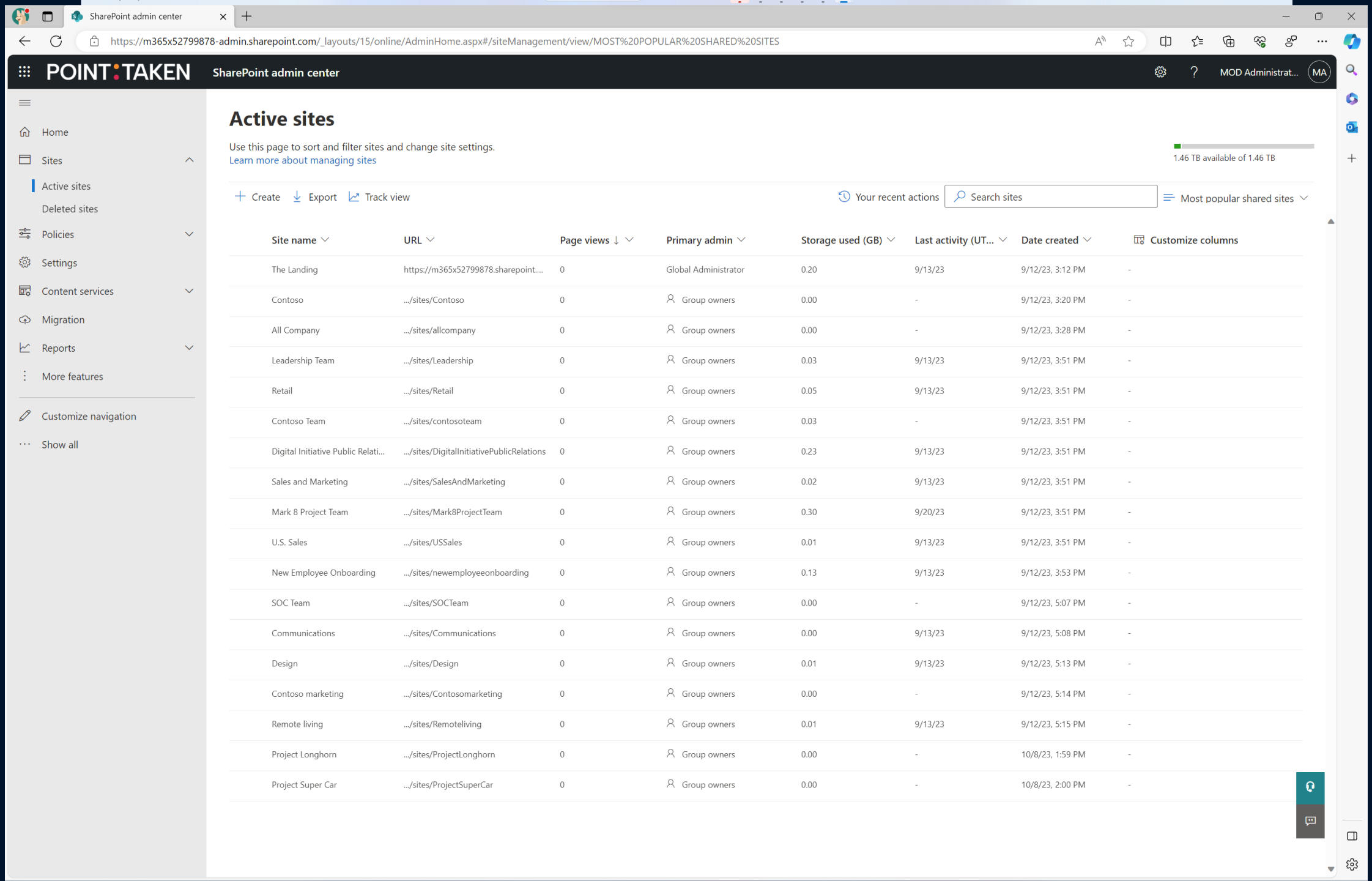
+ Create | Export | Track view | Your recent actions | Search sites | All sites

Site name	URL	Teams	Channel sites	Storage used (GB)	Primary admin	Hub	Template	Last activity (U
All Company	.../sites/allcompany	-	-	0.00	Group owners	-	Team site	-
Benefits	.../sites/benefits	-	-	0.04	MOD Administrator	Contoso Works	Communication site	-
Communications	.../sites/Communications		-	0.00	Group owners	-	Team site	9/13/23
Contoso	.../sites/Contoso		-	0.00	Group owners	-	Team site	-
Contoso Brand	.../sites/ContosoBrand	-	-	0.03	MOD Administrator	-	Communication site	-
Contoso marketing	.../sites/Contosomarketing		-	0.00	Group owners	-	Team site	-
Contoso News	.../sites/ContosoNews	-	-	0.11	MOD Administrator	-	Communication site	-
Contoso Team	.../sites/contosoteam	-	-	0.03	Group owners	-	Team site	-
Contoso Works	.../sites/ContosoWorks	-	-	0.02	MOD Administrator	Contoso Works (Hub site)	Communication site	-
Design	.../sites/Design		-	0.01	Group owners	-	Team site	9/13/23
Digital Initiative Public Relati...	.../sites/DigitalInitiativePublicRelations		-	0.23	Group owners	-	Team site	9/13/23
Drone workshop	.../sites/droneproducttraining	-	-	0.01	MOD Administrator	-	Communication site	-
Fly Safe Conference	.../sites/FlySafeConference	-	-	0.02	MOD Administrator	-	Communication site	-
Give	.../sites/give	-	-	0.03	MOD Administrator	-	Communication site	-
Global Marketing	.../sites/GlobalMarketing	-	-	0.02	MOD Administrator	Global Marketing (Hub site)	Communication site	-
Global Sales	.../sites/GlobalSales	-	-	0.06	MOD Administrator	Global Sales (Hub site)	Communication site	-
Human Resources	.../sites/HumanResources	-	-	0.00	MOD Administrator	-	Communication site	-
Leadership Connection	.../sites/leadership-connection	-	-	0.12	MOD Administrator	-	Communication site	-
Leadership Team	.../sites/Leadership	-	-	0.03	Group owners	-	Team site	9/13/23
Mark 8 Project Team	.../sites/Mark8ProjectTeam		-	0.30	Group owners	-	Team site	9/20/23


SharePoint admin center
https://m365x52799878-admin.sharepoint.com/_layouts/15/online/AdminHome.aspx#/siteManagement
POINT TAKEN
SharePoint admin center
MOD Administrat...
MA
Home
Sites
Active sites
Deleted sites
Policies
Settings
Content services
Migration
Reports
More features
Customize navigation
Show all
Active sites
Use this page to sort and filter sites and change site settings.
Learn more about managing sites
1.46 TB available of 1.46 TB
Create
Export
Track view
Your recent actions
Search sites
All sites
Standard views
All sites
Sites connected to Teams
Microsoft 365 group sites
Sites without a group
Classic sites
Largest sites
Least active sites
Most popular shared sites
Save view as
Set current view as default
Site name
URL
Teams
Channel sites
Storage used (GB)
Primary admin
Hub
Templa
All Company .../sites/allcompany - - 0.00 Group owners - Team sit
Benefits .../sites/benefits - - 0.04 MOD Administrator Contoso Works Commu
Communications .../sites/Communications - 0.00 Group owners - Team sit
Contoso .../sites/Contoso - 0.00 Group owners - Team sit
Contoso Brand .../sites/ContosoBrand - - 0.03 MOD Administrator - Commu
Contoso marketing .../sites/Contosomarketing - 0.00 Group owners - Team sit
Contoso News .../sites/ContosoNews - - 0.11 MOD Administrator - Commu
Contoso Team .../sites/contosoteam - - 0.03 Group owners - Team sit
Contoso Works .../sites/ContosoWorks - - 0.02 MOD Administrator Contoso Works (Hub site) Communication site -
Design .../sites/Design - 0.01 Group owners - Team site 9/13/23
Digital Initiative Public Relati... .../sites/DigitalInitiativePublicRelations - 0.23 Group owners - Team site 9/13/23
Drone workshop .../sites/droneproducttraining - - 0.01 MOD Administrator - Communication site -
Fly Safe Conference .../sites/FlySafeConference - - 0.02 MOD Administrator - Communication site -
Give .../sites/give - - 0.03 MOD Administrator - Communication site -
Global Marketing .../sites/GlobalMarketing - - 0.02 MOD Administrator Global Marketing (Hub site) Communication site -
Global Sales .../sites/GlobalSales - - 0.06 MOD Administrator Global Sales (Hub site) Communication site -
Human Resources .../sites/HumanResources - - 0.00 MOD Administrator - Communication site -
Leadership Connection .../sites/leadership-connection - - 0.12 MOD Administrator - Communication site -
Leadership Team .../sites/Leadership - - 0.03 Group owners - Team site 9/13/23
Mark 8 Project Team .../sites/Mark8ProjectTeam - 0.30 Group owners - Team site 9/20/23

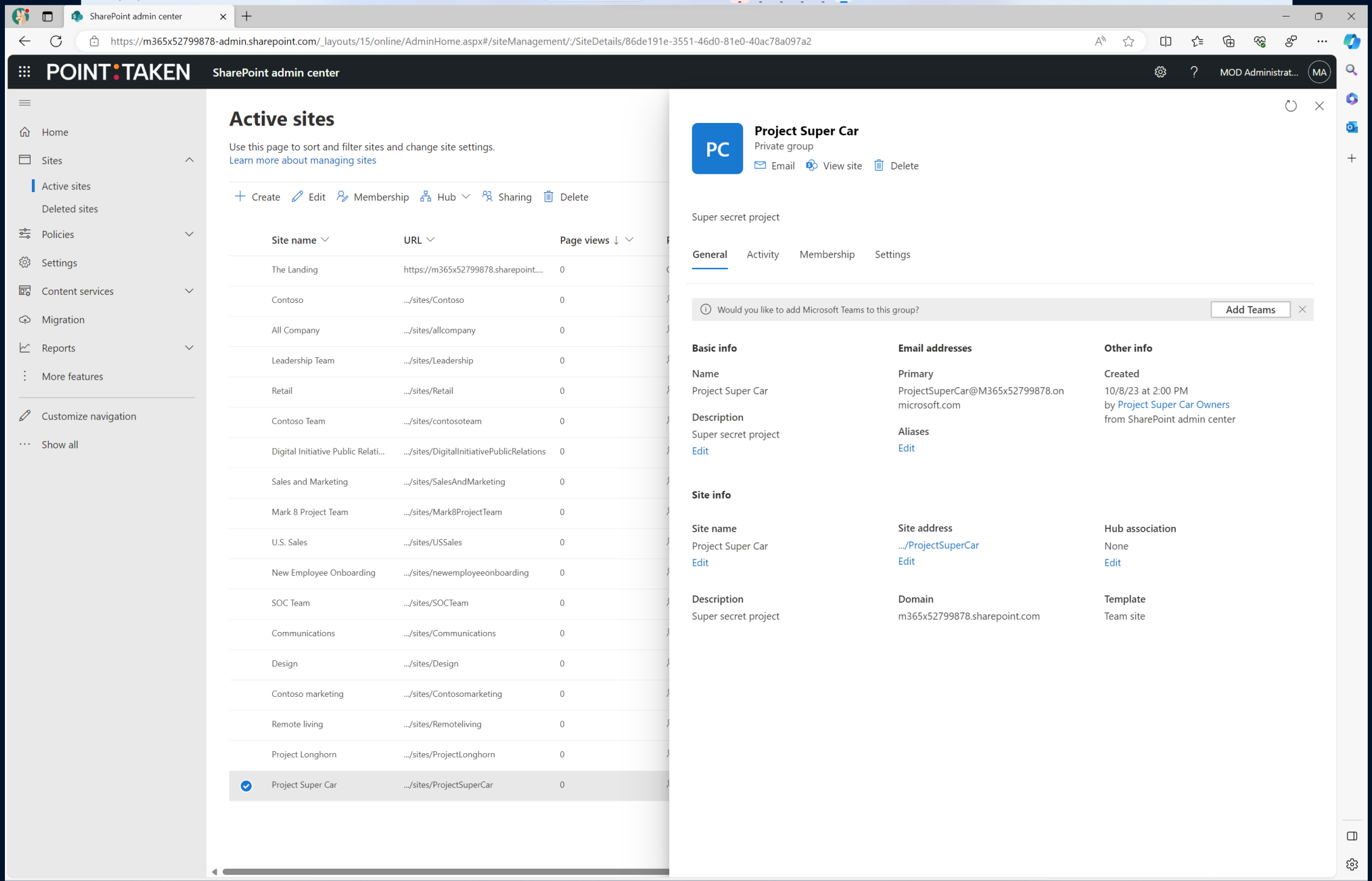

/siteManagement
MOD Administrat...
MA
1.46 TB available of 1.46 TB
Your recent actions
Search sites
All sites
Standard views
All sites
Sites connected to Teams
Microsoft 365 group sites
Sites without a group
Classic sites
Largest sites
Least active sites
Most popular shared sites
Save view as
Set current view as default
Teams
Channel sites
Storage used (GB)
Primary admin
Hub
Group owners
MOD Administrator
Contoso Works
Contoso Works (Hub site)
Communication site
0.00
0.04
0.03
0.11
0.02


/siteManagement
MOD Administrat...
MA
1.46 TB available of 1.46 TB
Your recent actions
Search sites
All sites
Standard views
All sites
Sites connected to Teams
Microsoft 365 group sites
Sites without a group
Classic sites
Largest sites
Least active sites
Most popular shared sites
Save view as
Set current view as default
Teams
Channel sites
Storage used (GB)
Primary admin
Hub
Group owners
MOD Administrator
Contoso Works
Contoso Works (Hub site)
Communication site
0.00
0.04
0.03
0.11
0.02


SharePoint admin center
https://m365x52799878-admin.sharepoint.com/_layouts/15/online/AdminHome.aspx#/siteManagement/view/MOST%20POPULAR%20SHARED%20SITES
POINT TAKEN
SharePoint admin center
MOD Administrat...
MA
Home
Sites
Active sites
Deleted sites
Policies
Settings
Content services
Migration
Reports
More features
Customize navigation
Show all
Active sites
Use this page to sort and filter sites and change site settings.
Learn more about managing sites
1.46 TB available of 1.46 TB
Create
Export
Track view
Your recent actions
Search sites
Most popular shared sites
Site name
URL
Page views
Primary admin
Storage used (GB)
Last activity (UT...
Date created
Customize columns
The Landing https://m365x52799878.sharepoint.... 0 Global Administrator 0.20 9/13/23 9/12/23, 3:12 PM -
Contoso .../sites/Contoso 0 Group owners 0.00 - 9/12/23, 3:20 PM -
All Company .../sites/allcompany 0 Group owners 0.00 - 9/12/23, 3:28 PM -
Leadership Team .../sites/Leadership 0 Group owners 0.03 9/13/23 9/12/23, 3:51 PM -
Retail .../sites/Retail 0 Group owners 0.05 9/13/23 9/12/23, 3:51 PM -
Contoso Team .../sites/contosoteam 0 Group owners 0.03 - 9/12/23, 3:51 PM -
Digital Initiative Public Relati... .../sites/DigitalInitiativePublicRelations 0 Group owners 0.23 9/13/23 9/12/23, 3:51 PM -
Sales and Marketing .../sites/SalesAndMarketing 0 Group owners 0.02 9/13/23 9/12/23, 3:51 PM -
Mark 8 Project Team .../sites/Mark8ProjectTeam 0 Group owners 0.30 9/20/23 9/12/23, 3:51 PM -
U.S. Sales .../sites/USSales 0 Group owners 0.01 9/13/23 9/12/23, 3:51 PM -
New Employee Onboarding .../sites/newemployeeonboarding 0 Group owners 0.13 9/13/23 9/12/23, 3:53 PM -
SOC Team .../sites/SOCTeam 0 Group owners 0.00 - 9/12/23, 5:07 PM -
Communications .../sites/Communications 0 Group owners 0.00 9/13/23 9/12/23, 5:08 PM -
Design .../sites/Design 0 Group owners 0.01 9/13/23 9/12/23, 5:13 PM -
Contoso marketing .../sites/Contosomarketing 0 Group owners 0.00 - 9/12/23, 5:14 PM -
Remote living .../sites/Remoteliving 0 Group owners 0.01 9/13/23 9/12/23, 5:15 PM -
Project Longhorn .../sites/ProjectLonghorn 0 Group owners 0.00 - 10/8/23, 1:59 PM -
Project Super Car .../sites/ProjectSuperCar 0 Group owners 0.00 - 10/8/23, 2:00 PM -

Create | Export | Track view | Your recent actions | Search sites | Most popular

Site name	URL	Page views	Primary admin	Storage used (GB)	Last activity (UT...	Date created	Customize columns
The Landing	https://m365x52799878.sharepoint....	0	Global Administrator	0.20	9/13/23	9/12/23, 3:12 PM	-
Contoso	.../sites/Contoso	0	Group owners	0.00	-	9/12/23, 3:20 PM	-
All Company	.../sites/allcompany	0	Group owners	0.00	-	9/12/23, 3:28 PM	-
Leadership Team	.../sites/Leadership	0	Group owners	0.03	9/13/23	9/12/23, 3:51 PM	-
Retail	.../sites/Retail	0	Group owners	0.05	9/13/23	9/12/23, 3:51 PM	-
Contoso Team	.../sites/contosoteam	0	Group owners	0.03	-	9/12/23, 3:51 PM	-
Digital Initiative Public Relati...	.../sites/DigitalInitiativePublicRelations	0	Group owners	0.23	9/13/23	9/12/23, 3:51 PM	-
Sales and Marketing	.../sites/SalesAndMarketing	0	Group owners	0.02	9/13/23	9/12/23, 3:51 PM	-
Mark 8 Project Team	.../sites/Mark8ProjectTeam	0	Group owners	0.30	9/20/23	9/12/23, 3:51 PM	-
U.S. Sales	.../sites/USSales	0	Group owners	0.01	9/13/23	9/12/23, 3:51 PM	-
New Employee Onboarding	.../sites/newemployeeonboarding	0	Group owners	0.13	9/13/23	9/12/23, 3:53 PM	-
SOC Team	.../sites/SOCTeam	0	Group owners	0.00	-	9/12/23, 5:07 PM	-
Communications	.../sites/Communications	0	Group owners	0.00	9/13/23	9/12/23, 5:08 PM	-
Design	.../sites/Design	0	Group owners	0.01	9/13/23	9/12/23, 5:13 PM	-
Contoso marketing	.../sites/Contosomarketing	0	Group owners	0.00	-	9/12/23, 5:14 PM	-
Remote living	.../sites/Remoteliving	0	Group owners	0.01	9/13/23	9/12/23, 5:15 PM	-
Project Longhorn	.../sites/ProjectLonghorn	0	Group owners	0.00	-	10/8/23, 1:59 PM	-
Project Super Car	.../sites/ProjectSuperCar	0	Group owners	0.00	-	10/8/23, 2:00 PM	-


SharePoint admin center
https://m365x52799878-admin.sharepoint.com/_layouts/15/online/AdminHome.aspx#/siteManagement/:/SiteDetails/86de191e-3551-46d0-81e0-40ac78a097a2
POINT TAKEN
SharePoint admin center
MOD Administrat...
MA
Home
Sites
Active sites
Deleted sites
Policies
Settings
Content services
Migration
Reports
More features
Customize navigation
Show all
Active sites
Use this page to sort and filter sites and change site settings.
Learn more about managing sites
Create
Edit
Membership
Hub
Sharing
Delete
Site name
URL
Page views
The Landing https://m365x52799878.sharepoint.... 0
Contoso .../sites/Contoso 0
All Company .../sites/allcompany 0
Leadership Team .../sites/Leadership 0
Retail .../sites/Retail 0
Contoso Team .../sites/contosoteam 0
Digital Initiative Public Relati... .../sites/DigitalInitiativePublicRelations 0
Sales and Marketing .../sites/SalesAndMarketing 0
Mark 8 Project Team .../sites/Mark8ProjectTeam 0
U.S. Sales .../sites/USSales 0
New Employee Onboarding .../sites/newemployeeonboarding 0
SOC Team .../sites/SOCTeam 0
Communications .../sites/Communications 0
Design .../sites/Design 0
Contoso marketing .../sites/Contosomarketing 0
Remote living .../sites/Remoteliving 0
Project Longhorn .../sites/ProjectLonghorn 0
Project Super Car .../sites/ProjectSuperCar 0
PC
Project Super Car
Private group
Email
View site
Delete
Super secret project
General
Activity
Membership
Settings
Would you like to add Microsoft Teams to this group?
Add Teams
Basic info
Name
Project Super Car
Description
Super secret project
Edit
Email addresses
Primary
ProjectSuperCar@M365x52799878.onmicrosoft.com
Aliases
Edit
Other info
Created
10/8/23 at 2:00 PM
by Project Super Car Owners
from SharePoint admin center
Site info
Site name
Project Super Car
Edit
Site address
.../ProjectSuperCar
Edit
Hub association
None
Edit
Description
Super secret project
Domain
m365x52799878.sharepoint.com
Template
Team site

nHome.aspx#/siteManagement/:/SiteDetails/86de191e-3551-46d0-81e0-40ac78a097a2

MOD Administrat... MA

ge site settings.

Hub Sharing Delete

	Page views
/m365x52799878.sharepoint....	0
/Contoso	0
/allcompany	0
/Leadership	0
/Retail	0
/contosoteam	0
/DigitalInitiativePublicRelations	0
/SalesAndMarketing	0
/Mark8ProjectTeam	0
/USSales	0

PC

Project Super Car

Private group

Email View site Delete

Super secret project

General Activity Membership Settings

Would you like to add Microsoft Teams to this group? Add Teams

Basic info

Name
Project Super Car

Description
Super secret project
Edit

Email addresses

Primary
ProjectSuperCar@M365x52799878.onmicrosoft.com

Aliases
Edit

Other info

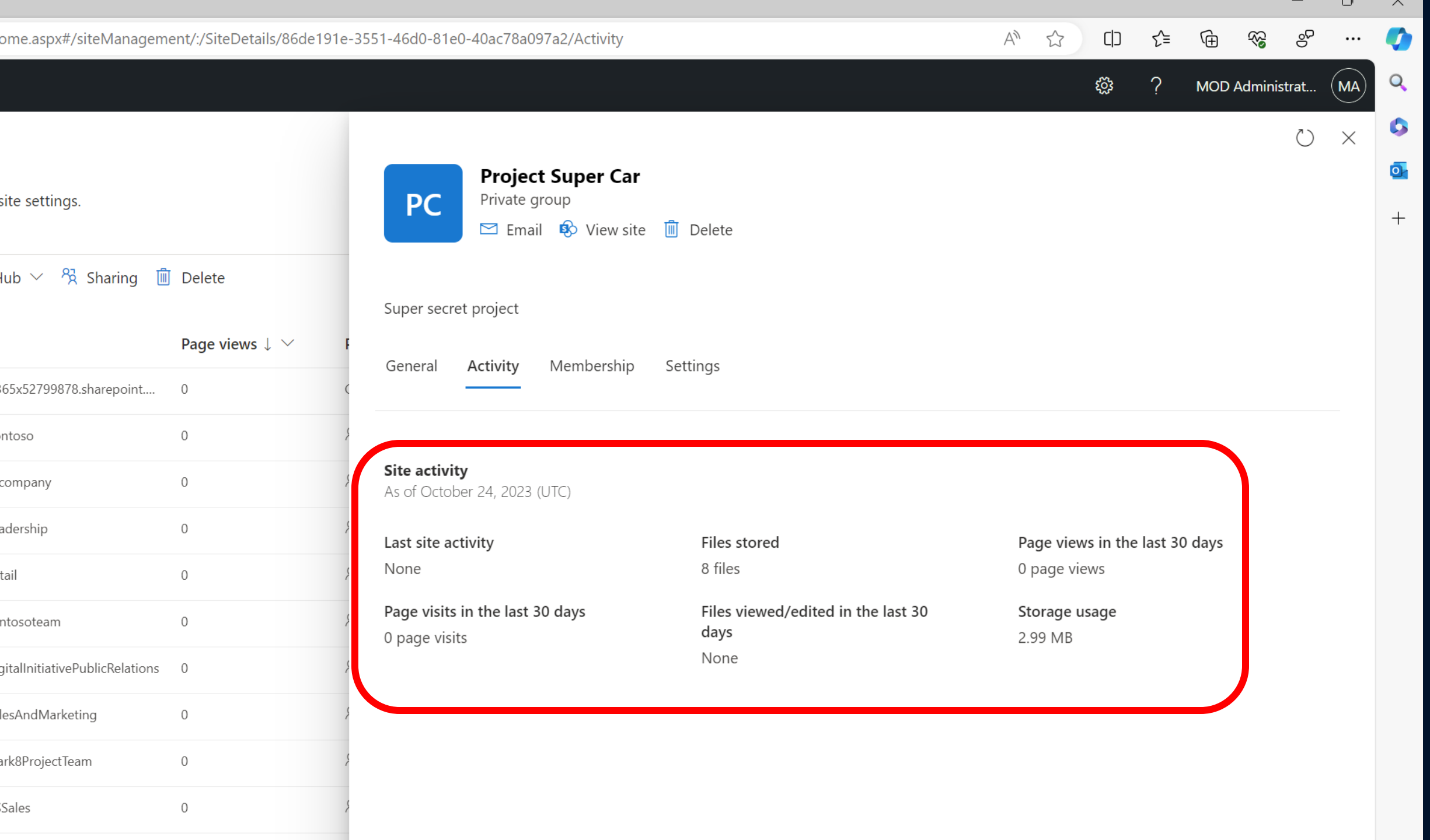
Created
10/8/23 at 2:00 PM
by Project Super Car Owners
from SharePoint admin center

Site info

Site name
Project Super Car
Edit

Site address
.../ProjectSuperCar
Edit

Hub association
None
Edit


ome.aspx#/siteManagement/:/SiteDetails/86de191e-3551-46d0-81e0-40ac78a097a2/Activity
MOD Administrat...
MA
site settings.
Hub
Sharing
Delete
Page views
365x52799878.sharepoint....
0
ntoso
0
company
0
adership
0
tail
0
ntosoteam
0
gitalInitiativePublicRelations
0
lesAndMarketing
0
ark8ProjectTeam
0
Sales
0
PC
Project Super Car
Private group
Email
View site
Delete
Super secret project
General
Activity
Membership
Settings
Site activity
As of October 24, 2023 (UTC)
Last site activity
None
Files stored
8 files
Page views in the last 30 days
0 page views
Page visits in the last 30 days
0 page visits
Files viewed/edited in the last 30 days
None
Storage usage
2.99 MB

ome.aspx#/siteManagement/:/SiteDetails/86de191e-3551-46d0-81e0-40ac78a097a2/Activity

MOD Administrat... MA

site settings.

Hub Sharing Delete

	Page views
365x52799878.sharepoint....	0
ntoso	0
company	0
adership	0
tail	0
ntosoteam	0
gitalInitiativePublicRelations	0
lesAndMarketing	0
ark8ProjectTeam	0
Sales	0

PC

Project Super Car

Private group

Email View site Delete

Super secret project

General Activity Membership Settings

Site activity

As of October 24, 2023 (UTC)

Last site activity
None

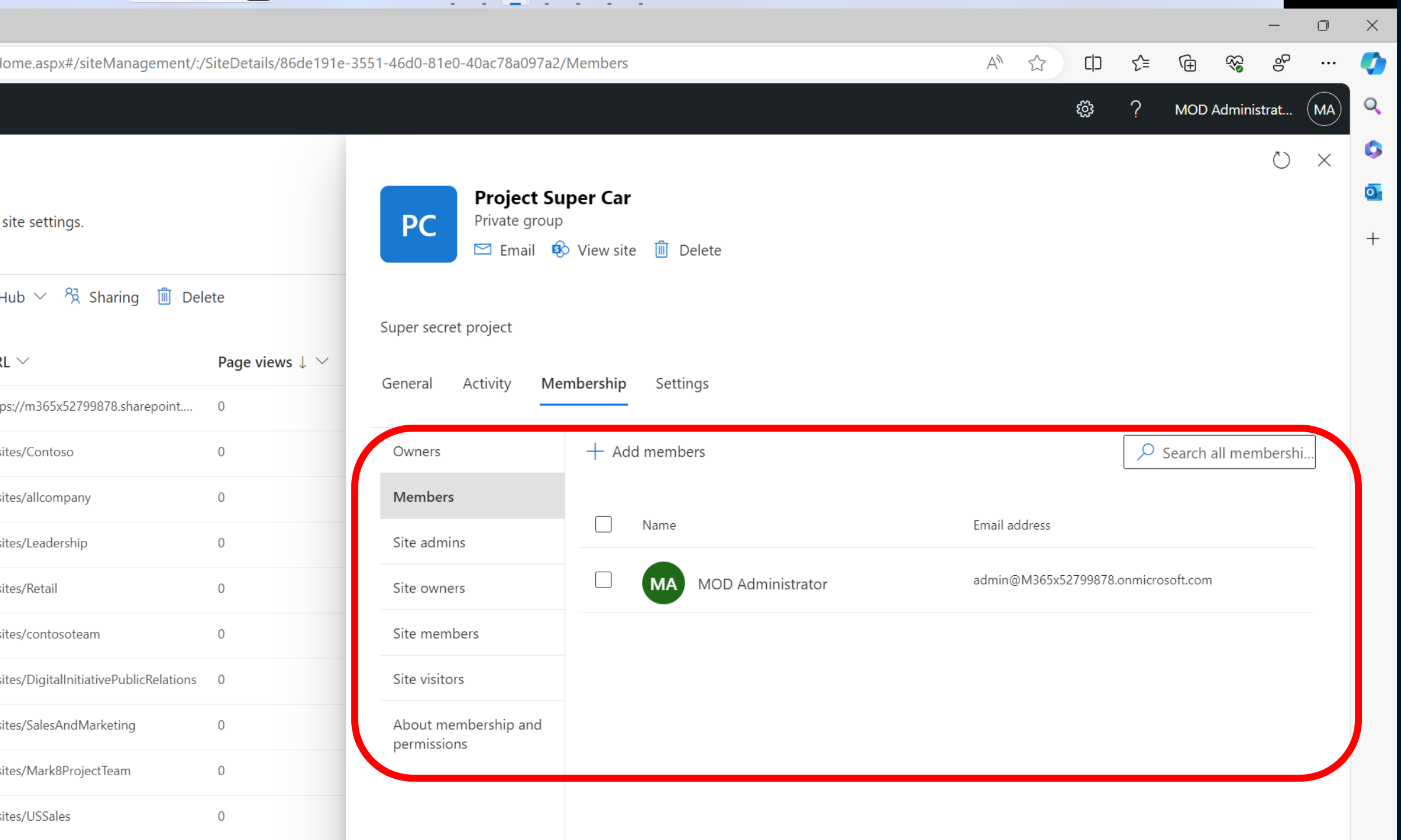
Files stored
8 files

Page views in the last 30 days
0 page views

Page visits in the last 30 days
0 page visits

Files viewed/edited in the last 30 days
None

Storage usage
2.99 MB


Home.aspx#/siteManagement/:/SiteDetails/86de191e-3551-46d0-81e0-40ac78a097a2/Members
MOD Administrat...
MA
site settings.
Hub
Sharing
Delete
RL
Page views
ps://m365x52799878.sharepoint....
0
sites/Contoso
0
sites/allcompany
0
sites/Leadership
0
sites/Retail
0
sites/contosoteam
0
sites/DigitalInitiativePublicRelations
0
sites/SalesAndMarketing
0
sites/Mark8ProjectTeam
0
sites/USSales
0
PC
Project Super Car
Private group
Email
View site
Delete
Super secret project
General
Activity
Membership
Settings
Owners
Members
Site admins
Site owners
Site members
Site visitors
About membership and permissions
Add members
Search all membershi...
Name
Email address
MA
MOD Administrator
admin@M365x52799878.onmicrosoft.com

ome.aspx#/siteManagement/:/SiteDetails/86de191e-3551-46d0-81e0-40ac78a097a2/Activity

MOD Administrat... MA

site settings.

Hub Sharing Delete

	Page views
365x52799878.sharepoint....	0
ntoso	0
company	0
adership	0
tail	0
ntosoteam	0
gitalInitiativePublicRelations	0
lesAndMarketing	0
ark8ProjectTeam	0
Sales	0

PC

Project Super Car

Private group

Email View site Delete

Super secret project

General Activity Membership Settings

Site activity

As of October 24, 2023 (UTC)

Last site activity
None

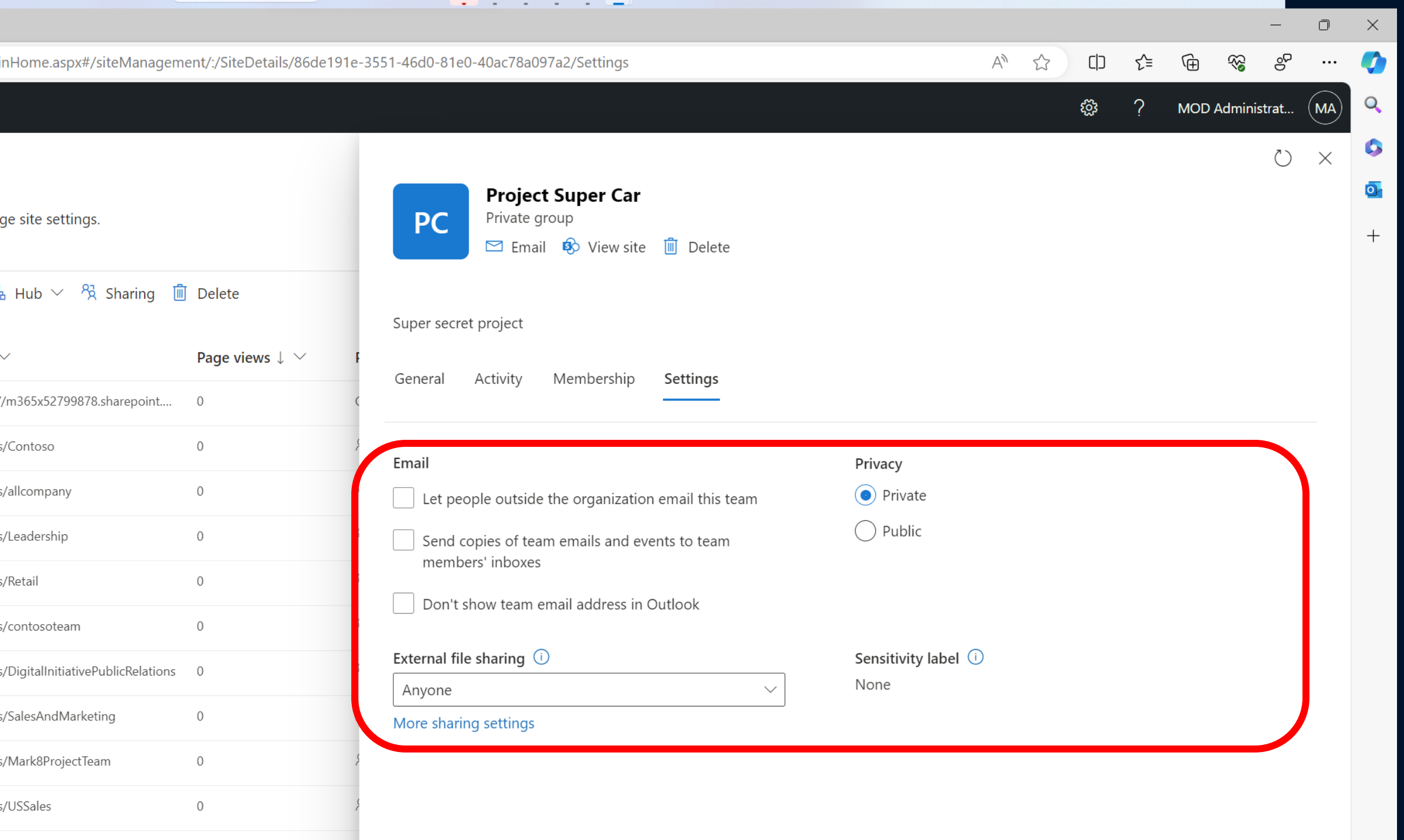
Files stored
8 files

Page views in the last 30 days
0 page views

Page visits in the last 30 days
0 page visits

Files viewed/edited in the last 30 days
None

Storage usage
2.99 MB

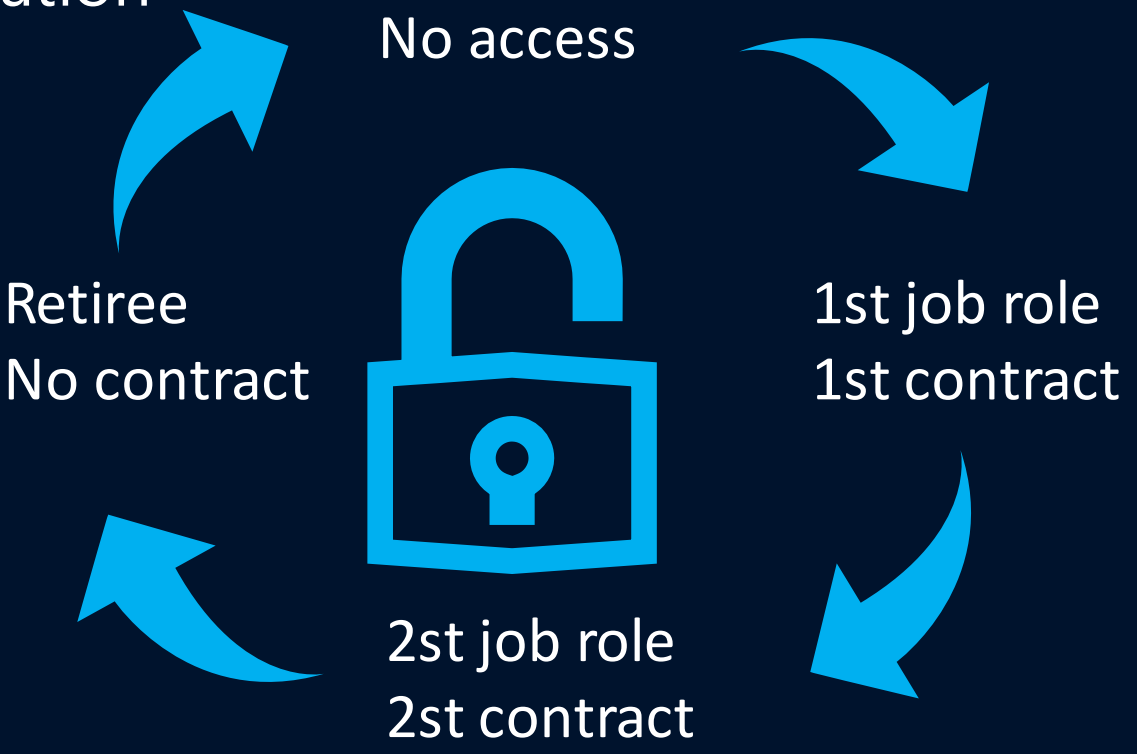

inHome.aspx#/siteManagement/:/SiteDetails/86de191e-3551-46d0-81e0-40ac78a097a2/Settings
MOD Administrat...
MA
ge site settings.
Hub
Sharing
Delete
Page views
/m365x52799878.sharepoint....
0
s/Contoso
0
s/allcompany
0
s/Leadership
0
s/Retail
0
s/contosoteam
0
s/DigitalInitiativePublicRelations
0
s/SalesAndMarketing
0
s/Mark8ProjectTeam
0
s/USSales
0
PC
Project Super Car
Private group
Email
View site
Delete
Super secret project
General
Activity
Membership
Settings
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
External file sharing
Anyone
More sharing settings
Privacy
Private
Public
Sensitivity label
None

Microsoft Entra ID

Manage identity and access lifecycle at scale

Microsoft Entra ID Entitlement Management

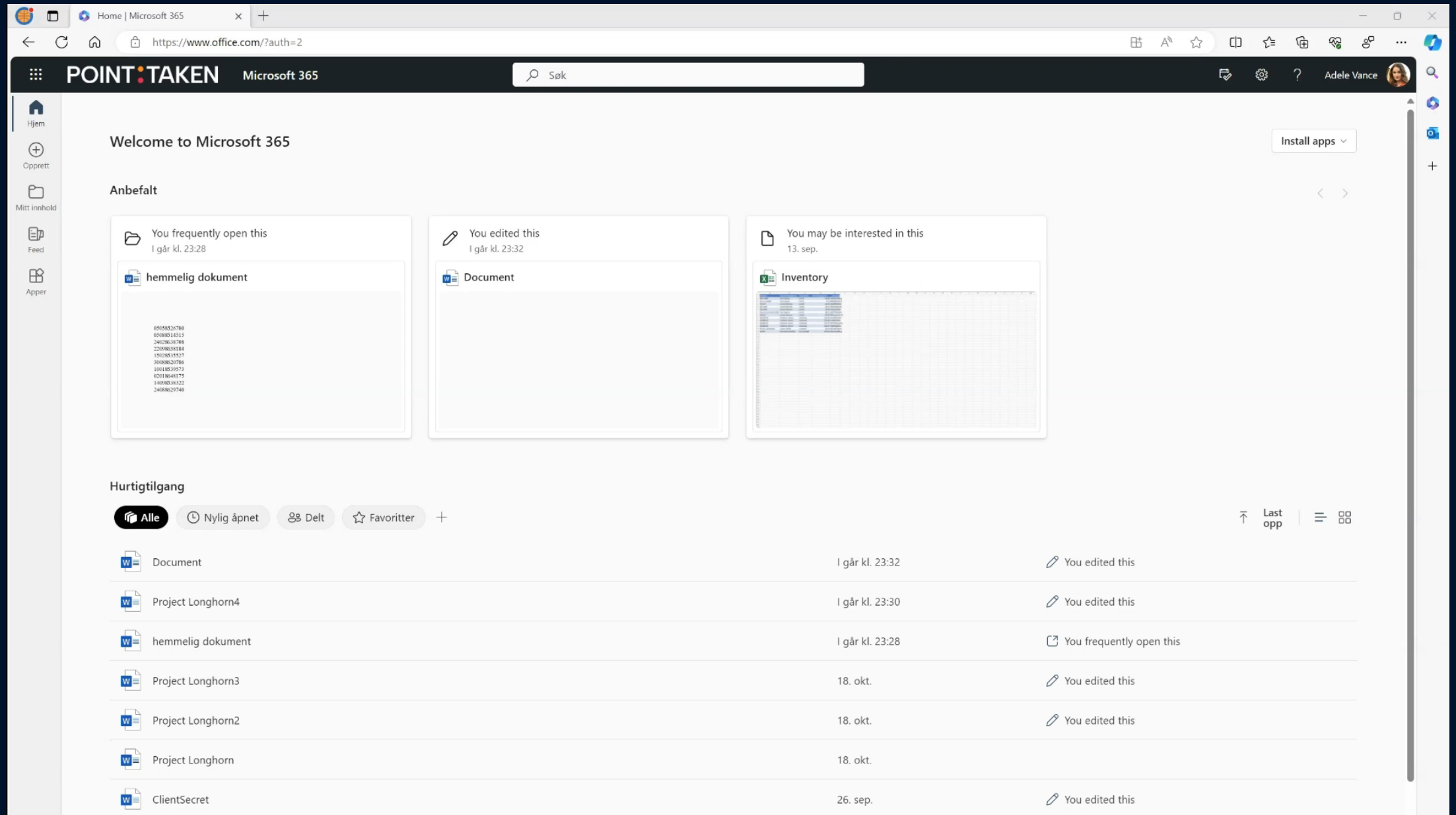
- Govern the identity lifecycle
- Secure privileged access for administration
- Govern access lifecycle



DEMO

Entra ID

Microsoft Entra ID



Home
Favorites
Identity
Overview
Users
Groups
Devices
Applications
Protection
Identity governance
External Identities
Show more
Protection
Identity governance
Verifiable credentials
Permissions Management
Global Secure Access (Preview)
Learn & support

Azure AD is now Microsoft Entra ID. Learn more

Microsoft Entra admin center

Secure access for a connected world with comprehensive multicloud identity and network access solutions.

Learn more

Microsoft Entra ID (Azure AD)

Secure and manage identities to connect them with apps, devices and data.

Go to Microsoft Entra ID

ID Protection

Identify and address identity risks in your organization.

Go to ID Protection

ID Governance

Manage access rights with entitlement management, access reviews and lifecycle workflows.

Go to ID Governance

Verified ID

Create, issue and verify decentralized identity credentials for secure interactions.

Go to Verified ID

Workload ID

Secure identities for apps and services and their access to cloud resources.

Go to Workload ID

Permissions Management

Discover, remediate, and monitor permission risks for any identity or resource.

Go to Permissions Management

Internet Access

Secure access and improve visibility to the Internet, M365 and SaaS apps.

Go to Global Secure Access

Private Access

Secure and modernize access to your private apps and resources.

Go to Global Secure Access

Get started for free

Access free trials for the family of identity and access products from Microsoft.

Try the products

Microsoft Entra ID. Learn more

Microsoft Entra admin center

Secure access for a connected world with comprehensive multicloud identity and network access solutions.

Learn more

Microsoft Entra ID (Azure AD)

Secure and manage identities to connect them with apps, devices and data.

Go to Microsoft Entra ID

ID Protection

Identify and address identity risks in your organization.

Go to ID Protection

ID Governance

Manage access rights with entitlement management, access reviews and lifecycle workflows.

Go to ID Governance

Verified ID

Create, issue and verify decentralized identity credentials for secure interactions.

Workload ID

Secure identities for apps and services and their access to cloud resources.

Permissions Management

Discover, remediate, and monitor permission risks for any identity or resource.

Home
Favorites
Identity
Protection
Identity governance
Dashboard
Entitlement management
Access reviews
Privileged Identity Management
Lifecycle workflows
Verifiable credentials
Permissions Management
Global Secure Access (Preview)
Learn & support

Contoso

Welcome to Identity Governance

Manage identity and access rights across multiple applications and services to meet security and regulatory compliance requirements. With Microsoft Entra ID Governance, balance security and productivity by ensuring that the right people have the right access to the right resources for the right amount of time.

Learn more

Member user lifecycle governance

0 member user accounts recently created

Improve operational efficiency, increase new hire productivity and reduce security risks by automating your employee onboarding and offboarding tasks.

Configure lifecycle workflows | Learn more

Application access governance

4 apps with direct user assignments

Manage how your employees and guests get access to business applications and maintain compliance by configuring request approval workflows and periodic access reviews, and automatically revoke access when it is no longer necessary.

Create access package | Learn more

Guest access governance

1 guest user accounts recently created

Reduce security risk by monitoring inactive guest users at scale with intelligent insights, configure thresholds based on your compliance needs and perform periodic review of guest access to groups and business applications.

View inactive guests | Learn more

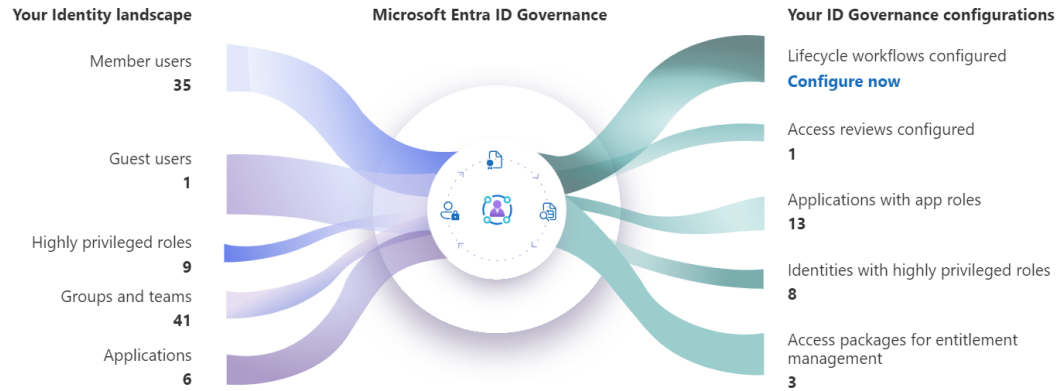
Privileged access governance

7 permanent global administrator assignments

Microsoft recommends you to keep fewer than 5 standing global admins with 2 of them reserved for break glass scenarios

Reduce global administrators | Learn more

Identity Governance status



Home

Favorites

Identity

Protection

Identity governance

Dashboard

Entitlement management

Access reviews

Privileged Identity Management

Lifecycle workflows

Verifiable credentials

Permissions Management

Global Secure Access (Preview)

Contoso ...

Welcome

Manage identity and access r
requirements. With Microsoft
the right access to the right r

Learn more

Member user lifecycle governance

0 member user accounts recently created

Improve operational efficiency, increase new hire productivity and reduce security risks by automating your employee onboarding and offboarding tasks.

Configure lifecycle workflows | Learn more

Application access governance

4 apps with direct user assignments

Manage how your employees and guests get access to business applications ar
maintain compliance by configuring request approval workflows and periodic a
reviews, and automatically revoke access when it is no longer necessary.

Create access package | Learn more

Privileged access governance

Identity Governance status

Home
Favorites
Identity
Protection
Identity governance
Dashboard
Entitlement management
Access reviews
Privileged Identity Management
Lifecycle workflows
Verifiable credentials
Permissions Management
Global Secure Access (Preview)
Learn & support

Identity Governance | Getting started

Got feedback?
Dashboard
Getting started
Entitlement management
Access packages
Catalogs
Connected organizations
Reports
Settings
Lifecycle workflows
Lifecycle workflows
Access reviews
Overview
Access reviews
Programs
Settings
Review History
Privileged Identity Management
Azure AD roles
Azure resources
Terms of use
Terms of use
Activity
Audit logs
Troubleshooting + Support
Troubleshoot
New support request

Get started with Identity Governance

tal identities securely and efficiently with Azure Active Directory (Azure AD) Identity Governance.
Review the ost common use cases and set of capabilities for your governance needs.

Uses | External user lifecycle | Group membership | Role assignments | Auditing and reporting

Control your external user lifecycle

Manage the entire lifecycle of external users: configure onboarding approval flows, set up regular access reviews, and remove external users when they're done collaborating. Remove guests from groups and Teams, and even guest accounts from Azure AD.

Review common use cases

Manage group membership

Secure and enhance your organization's use of group membership. Make groups "self-service," and delegate approvals directly to business decisionmakers. For privileged access groups, enforce owner eligibility with access reviews.

Review common use cases

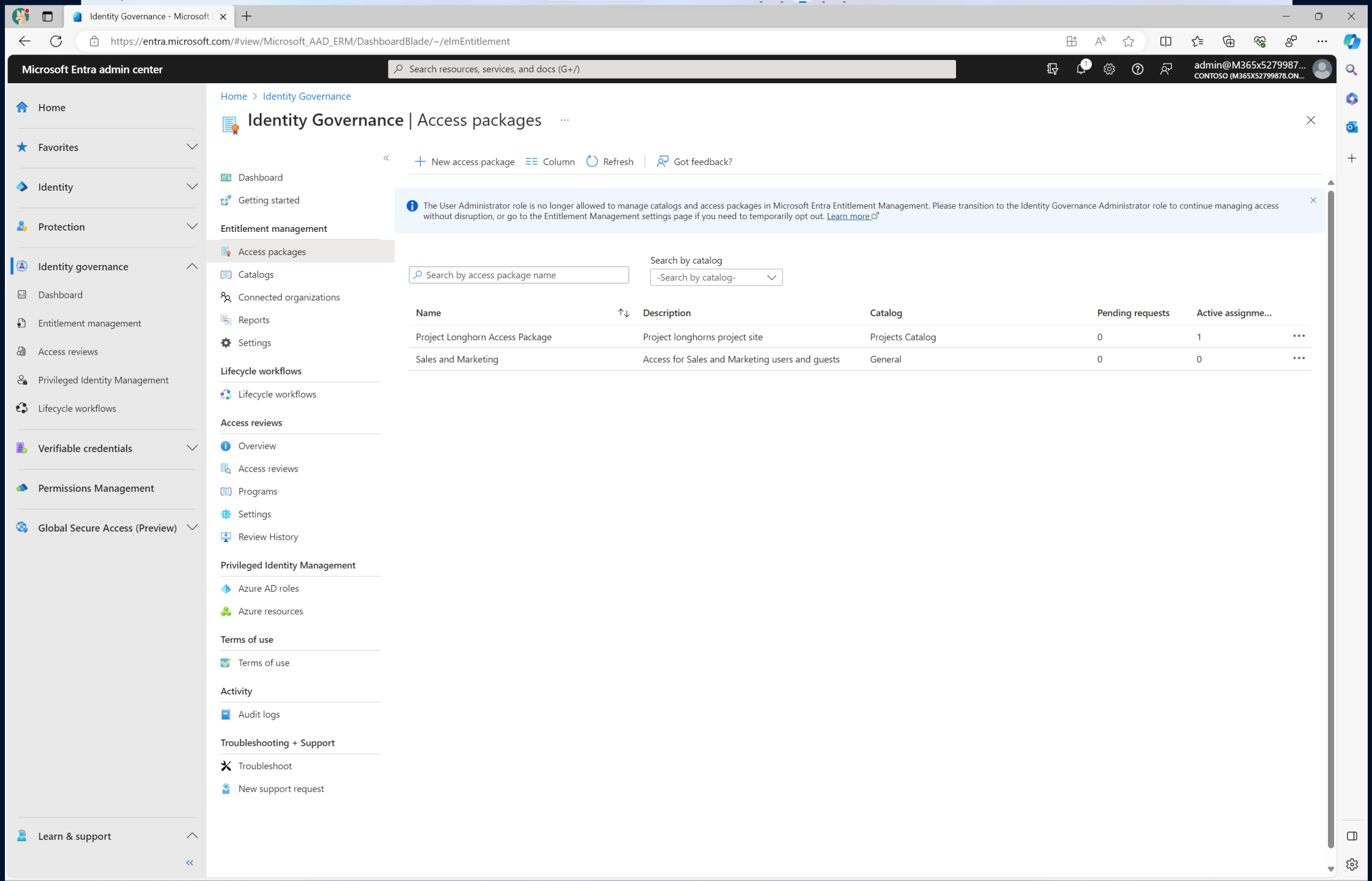
Protect resources with role assignments

Require approvals and multifactor authentication to activate use of Azure AD and Azure resource roles. By reviewing roles and making assignments time-bound, you'll help ensure only the right people have access to secure info and resources.

Review common use cases

Audit and create reports

Audit and generate reports on activity within Azure AD. Learn whether or not people review access, who's getting privileged access, or flag suspicious activity tied to Azure AD or Azure resource roles.


Identity Governance - Microsoft
https://entra.microsoft.com/#view/Microsoft_AAD_ERM/DashboardBlade/~/elmEntitlement
Microsoft Entra admin center
Search resources, services, and docs (G+/)
admin@M365x5279987...
CONTOSO (M365X5279878.ON...
Home
Favorites
Identity
Protection
Identity governance
Dashboard
Entitlement management
Access reviews
Privileged Identity Management
Lifecycle workflows
Verifiable credentials
Permissions Management
Global Secure Access (Preview)
Learn & support
Home > Identity Governance
Identity Governance | Access packages
Dashboard
Getting started
Entitlement management
Access packages
Catalogs
Connected organizations
Reports
Settings
Lifecycle workflows
Lifecycle workflows
Access reviews
Overview
Access reviews
Programs
Settings
Review History
Privileged Identity Management
Azure AD roles
Azure resources
Terms of use
Terms of use
Activity
Audit logs
Troubleshooting + Support
Troubleshoot
New support request
New access package
Column
Refresh
Got feedback?
The User Administrator role is no longer allowed to manage catalogs and access packages in Microsoft Entra Entitlement Management. Please transition to the Identity Governance Administrator role to continue managing access without disruption, or go to the Entitlement Management settings page if you need to temporarily opt out. Learn more
Search by access package name
Search by catalog
-Search by catalog-
Name
Description
Catalog
Pending requests
Active assignme...
Project Longhorn Access Package
Project longhorns project site
Projects Catalog
0
1
Sales and Marketing
Access for Sales and Marketing users and guests
General
0
0

Identity Governance - Microsoft

https://entra.microsoft.com/#view/Microsoft_AAD_ERM/DashboardBlade/~/elmEntitlement

Microsoft Entra admin center

Search resources, services, and docs (G+/)

- Home
- Favorites
- Identity
- Protection
- Identity governance
  - Dashboard
  - Entitlement management
  - Access reviews
  - Privileged Identity Management
  - Lifecycle workflows
- Verifiable credentials

Home > Identity Governance

Identity Governance | Access packages

- Dashboard
- Getting started

Entitlement management

- Access packages
- Catalogs
- Connected organizations
- Reports
- Settings

Lifecycle workflows

- Lifecycle workflows

Access reviews

- Overview
- Access reviews

New access package | Column | Refresh | Got feedback?

The User Administrator role is no longer allowed to manage catalogs and access packages in Microsoft Entra Entit
without disruption, or go to the Entitlement Management settings page if you need to temporarily opt out. Learn

Search by access package name

Search by catalog

-Search by catalog-

Name	Description
Project Longhorn Access Package	Project longhorns project site
Sales and Marketing	Access for Sales and Marketing users and guests

Home
Favorites
Identity
Protection
Identity governance
Dashboard
Entitlement management
Access reviews
Privileged Identity Management
Lifecycle workflows
Verifiable credentials
Permissions Management
Global Secure Access (Preview)
Learn & support

New access package

*Basics | Resource roles | *Requests | Requestor information | *Lifecycle | Custom extensions | Review + create

Access package

Create a collection of resources that users can request access to.

Name *

Description *

Catalog * General

Learn more.

Create new catalog

Review + create

Next: Resource roles >

New access package

* Basics | Resource roles | * Requests | Requestor information | * Lifecycle | Custom extensions | Review + create

Access package

Create a collection of resources that users can request access to.

Name *: Access to Event portal

Description *: This package gives access to our Event portal

Catalog *: General

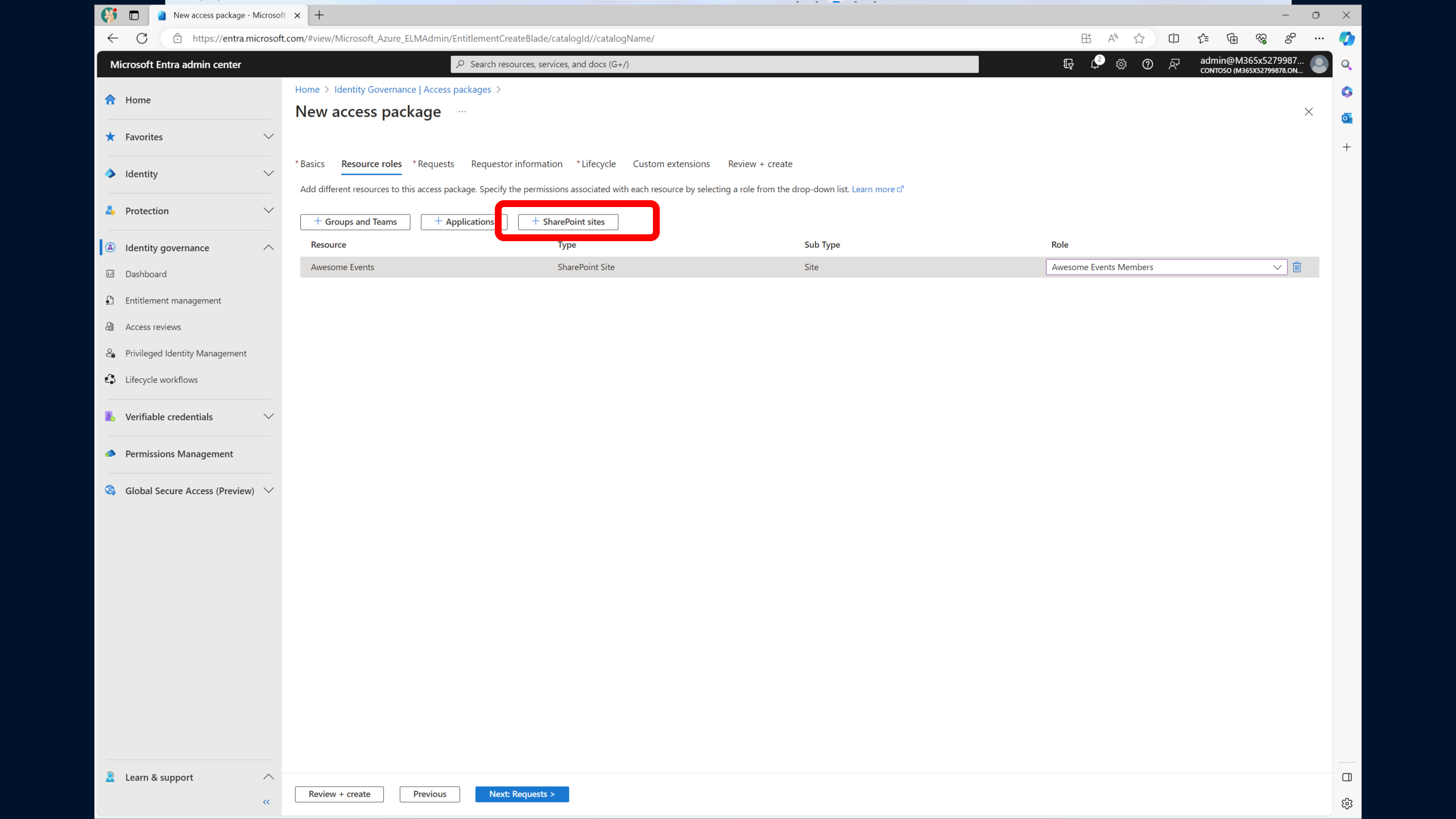
Learn more.

Create ne

Search by catalog-

Projects Catalog

General


New access package - Microsoft
https://entra.microsoft.com/#view/Microsoft_Azure_ELMAdmin/EntitlementCreateBlade/catalogId//catalogName/
Microsoft Entra admin center
Search resources, services, and docs (G+/)
admin@M365x5279987...
CONTOSO (M365X5279878.ON...
Home
Favorites
Identity
Protection
Identity governance
Dashboard
Entitlement management
Access reviews
Privileged Identity Management
Lifecycle workflows
Verifiable credentials
Permissions Management
Global Secure Access (Preview)
Learn & support
Home > Identity Governance | Access packages >
New access package
*Basics
Resource roles
*Requests
Requestor information
*Lifecycle
Custom extensions
Review + create
Add different resources to this access package. Specify the permissions associated with each resource by selecting a role from the drop-down list. Learn more
+ Groups and Teams
+ Applications
+ SharePoint sites
Resource
Type
Sub Type
Role
Awesome Events
SharePoint Site
Site
Awesome Events Members
Review + create
Previous
Next: Requests >

Basics | Resource roles | *Requests | Requestor information | *Lifecycle | Custom extensions | Review + create

Add different resources to this access package. Specify the permissions associated with each resource by selecting a role from the drop-down list. Learn more

+ Groups and Teams | + Applications | + SharePoint sites

Resource	Type	Sub Type	Role
Awesome Events	SharePoint Site	Site	Awesome Events Members

Search role

Awesome Events Members

Awesome Events Owners

Awesome Events Visitors

Home
Favorites
Identity
Protection
Identity governance
Dashboard
Entitlement management
Access reviews
Privileged Identity Management
Lifecycle workflows
Verifiable credentials
Permissions Management
Global Secure Access (Preview)
Learn & support

New access package

*Basics Resource roles *Requests Requestor information *Lifecycle Custom extensions Review + create

Create a policy to specify who can request an access package, who can approve requests, and when access expires. Additional request policies can be created. Learn more

Users who can request access

Users who can request access *

- (●) For users in your directory
  Allow users and groups in your directory to request this access package
- ( ) For users not in your directory
  Allow users in connected organizations (other directories and domains) to request this access package
- ( ) None (administrator direct assignments only)
  Allow administrators to directly assign specific users to this access package. Users cannot request this access package

- ( ) Specific users and groups
- ( ) All members (excluding guests)
- (●) All users (including guests)

Approval

Require approval * ⓘ Yes | No

Enable

Enable new requests * ⓘ Yes | No

Required Verified IDs

Choose whether or not you want users to show Verified IDs for this policy. First add the issuer's identifier and then add type of credential you want to check for. Users will need to present the selected credentials for this policy. Learn more

You'll need to configure your organization for the Verified ID service before you can use this feature.
Configure Verified ID Service

+ Add issuer

Issuer Identifier	Credential types

Review + create Previous Next: Requestor Information >

* Basics Resource roles * Requests Requestor information * Lifecycle Custom extensions Review + create

Create a policy to specify who can request an access package, who can approve requests, and when access expires. Additional request policies can be created. Learn more

Users who can request access

Users who can request access *

- (•) For users in your directory
  Allow users and groups in your directory to request this access package
- ( ) For users not in your directory
  Allow users in connected organizations (other directories and domains) to request this access package
- ( ) None (administrator direct assignments only)
  Allow administrators to directly assign specific users to this access package. Users cannot request this access package

- ( ) Specific users and groups
- ( ) All members (excluding guests)
- (•) All users (including guests)

Approval

Require approval * ⓘ Yes [No]

Enable

Enable new requests * ⓘ [Yes] No

Required Verified IDs

Choose whether or not you want users to show Verified IDs for this policy. First add the issuer's identifier and then add type of credential you want to check for. Users will need to present the selected credentials for this policy. Learn more

ⓘ

You'll need to configure your organization for the Verified ID service before you can use this feature.

Users who can request access

Users who can request access *

- (•) For users in your directory
  Allow users and groups in your directory to request this access package
- ( ) For users not in your directory
  Allow users in connected organizations (other directories and domains) to request this access package
- ( ) None (administrator direct assignments only)
  Allow administrators to directly assign specific users to this access package. Users cannot request this access package

- ( ) Specific users and groups
- ( ) All members (excluding guests)
- (•) All users (including guests)

Approval

Require approval * ⓘ Yes | No

Enable

Enable new requests * ⓘ Yes | No

Required Verified IDs

Choose whether or not you want users to show Verified IDs for this policy. First add the issuer's identifier and then add type of credential you want to check for. Users will need to present the selected credentials for this policy. Learn more

You'll need to configure your organization for the Verified ID service before you can use this feature.
Configure Verified ID Service

+ Add issuer

Users who can request access

Users who can request access *

- (•) For users in your directory
  Allow users and groups in your directory to request this access package
- ( ) For users not in your directory
  Allow users in connected organizations (other directories and domains) to request this access package
- ( ) None (administrator direct assignments only)
  Allow administrators to directly assign specific users to this access package. Users cannot request this access package

- ( ) Specific users and groups
- ( ) All members (excluding guests)
- (•) All users (including guests)

Approval

Require approval * ⓘ [Yes | No]

Enable

Enable new requests * ⓘ [Yes | No]

Required Verified IDs

Choose whether or not you want users to show Verified IDs for this policy. First add the issuer's identifier and then add type of credential you want to check for. Users will need to present the selected credentials for this policy. Learn more

You'll need to configure your organization for the Verified ID service before you can use this feature.
Configure Verified ID Service

+ Add issuer

Users who can request access

Users who can request access *

- (•) For users in your directory
  Allow users and groups in your directory to request this access package
- ( ) For users not in your directory
  Allow users in connected organizations (other directories and domains) to request this access package
- ( ) None (administrator direct assignments only)
  Allow administrators to directly assign specific users to this access package. Users cannot request this access package

- ( ) Specific users and groups
- ( ) All members (excluding guests)
- (•) All users (including guests)

Approval

Require approval * ⓘ Yes | No

Enable

Enable new requests * ⓘ Yes | No

Required Verified IDs

Choose whether or not you want users to show Verified IDs for this policy. First add the issuer's identifier and then add type of credential you want to check for. Users will need to present the selected credentials for this policy. Learn more

You'll need to configure your organization for the Verified ID service before you can use this feature.
Configure Verified ID Service

+ Add issuer

Home
Favorites
Identity
Protection
Identity governance
Dashboard
Entitlement management
Access reviews
Privileged Identity Management
Lifecycle workflows
Verifiable credentials
Permissions Management
Global Secure Access (Preview)
Learn & support

New access package

*Basics Resource roles *Requests Requestor information *Lifecycle Custom extensions Review + create

Collect information and attributes from requestor. Go to Catalogs to add attributes for this access package's catalog resources. Learn more

Questions Attributes

Question	Add localization	Answer format	Multiple choice options	Regex pattern (Preview)	Required
Enter question	add localization	Answer format			

Home
Favorites
Identity
Protection
Identity governance
Dashboard
Entitlement management
Access reviews
Privileged Identity Management
Lifecycle workflows
Verifiable credentials
Permissions Management
Global Secure Access (Preview)
Learn & support

New access package

*Basics Resource roles *Requests Requestor information *Lifecycle Custom extensions Review + create

Expiration

Access package assignments expire: On date | Number of days | Number of hours | Never

Assignments expire after (number of days) *: 365

Users can request specific timeline *: Yes | No

Show advanced expiration settings

Access Reviews

Require access reviews *: Yes | No

New access package ...

* Basics | Resource roles | * Requests | Requestor information | * Lifecycle | Custom extensions | Review + create

Expiration

Access package assignments expire: On date | **Number of days** | Number of hours | Never

Assignments expire after (number of days) *: 365

Users can request specific timeline *: **Yes** | No

Show advanced expiration settings

Access Reviews

Require access reviews *: Yes | No

Home
Favorites
Identity
Protection
Identity governance
Dashboard
Entitlement management
Access reviews
Privileged Identity Management
Lifecycle workflows
Verifiable credentials
Permissions Management
Global Secure Access (Preview)

ome

vorites

entity

otection

entity governance

shboard

titlement management

cess reviews

ivileged Identity Management

ecycle workflows

erifiable credentials

ermissions Management

obal Secure Access (Preview)

New access package ...

* Basics Resource roles * Requests Requestor information * Lifecycle Custom extensions Review + create

Expiration

Access package assignments expire: On date | Number of days | Number of hours | **Never**

Users can request specific timeline *: **Yes** | No

Access Reviews

Require access reviews *: **Yes** | No

Starting on: 31.10.2023

Review frequency: Annually | Bi-annually | **Quarterly** | Monthly | Weekly

Duration (in days) *: 25

Maximum 80

Reviewers:
- (•) Self-review
- ( ) Specific reviewer(s)
- ( ) Manager

Show advanced access review settings

Home
Favorites
Identity
Protection
Identity governance
Dashboard
Entitlement management
Access reviews
Privileged Identity Management
Lifecycle workflows
Verifiable credentials
Permissions Management
Global Secure Access (Preview)
Learn & support

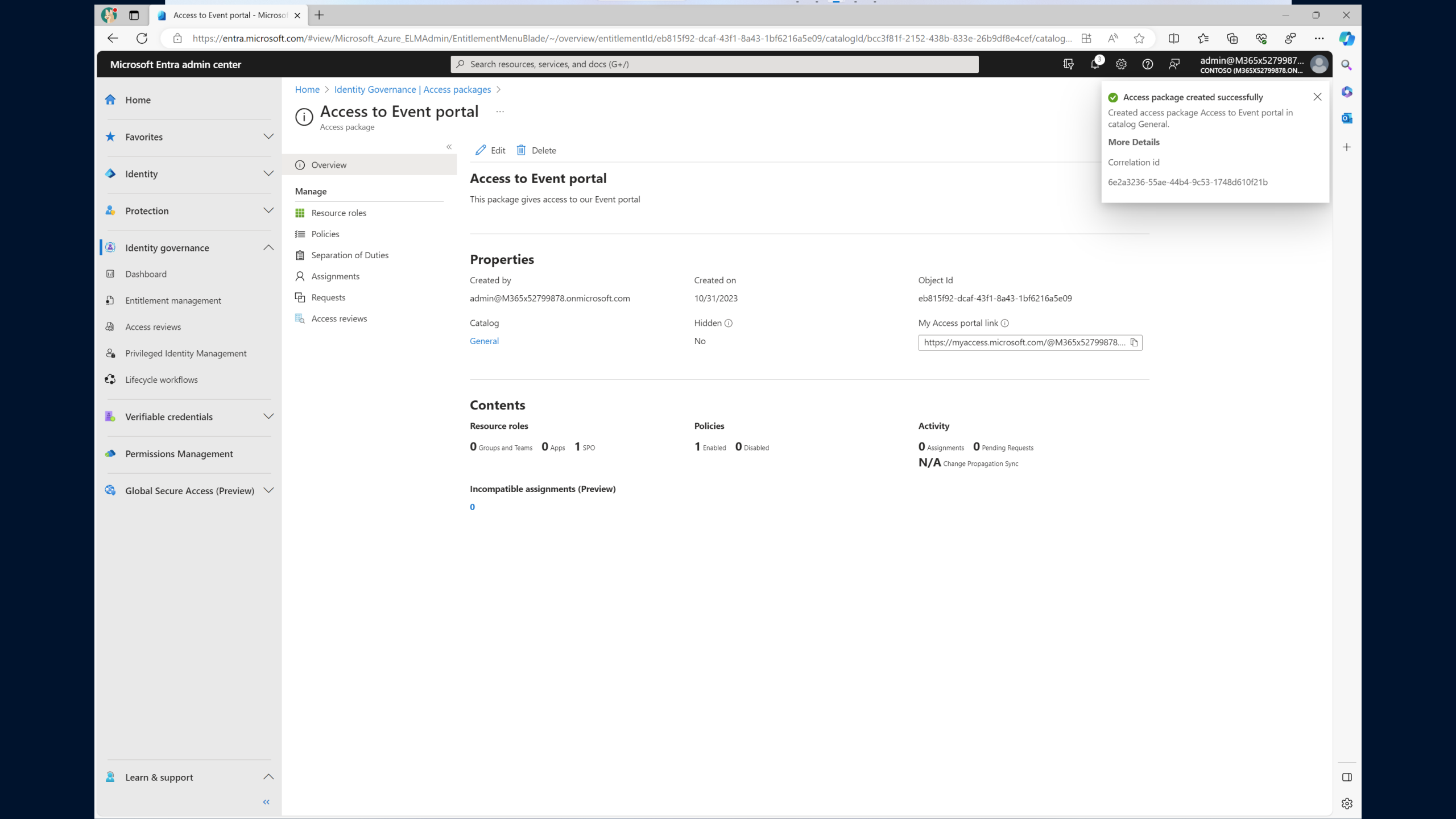
New access package

*Basics Resource roles *Requests Requestor information *Lifecycle Custom extensions Review + create

Configure a rule: If <event>, then do <flow>. A rule contains an event that/and triggers a previously defined custom flow

Stage	Custom Extension
Select stage	Select custom extension

Review + create | Previous | Next: Review + create >


Access to Event portal - Microsof
https://entra.microsoft.com/#view/Microsoft_Azure_ELMAdmin/EntitlementMenuBlade/~/overview/entitlementId/eb815f92-dcaf-43f1-8a43-1bf6216a5e09/catalogId/bcc3f81f-2152-438b-833e-26b9df8e4cef/catalog...
Microsoft Entra admin center
Search resources, services, and docs (G+/)
admin@M365x5279987...
CONTOSO (M365X52799878.ON...
Home
Favorites
Identity
Protection
Identity governance
Dashboard
Entitlement management
Access reviews
Privileged Identity Management
Lifecycle workflows
Verifiable credentials
Permissions Management
Global Secure Access (Preview)
Learn & support
Home > Identity Governance | Access packages >
Access to Event portal
Access package
Overview
Manage
Resource roles
Policies
Separation of Duties
Assignments
Requests
Access reviews
Edit
Delete
Access package created successfully
Created access package Access to Event portal in catalog General.
More Details
Correlation id
6e2a3236-55ae-44b4-9c53-1748d610f21b
Access to Event portal
This package gives access to our Event portal
Properties
Created by
admin@M365x52799878.onmicrosoft.com
Created on
10/31/2023
Object Id
eb815f92-dcaf-43f1-8a43-1bf6216a5e09
Catalog
General
Hidden
No
My Access portal link
https://myaccess.microsoft.com/@M365x52799878....
Contents
Resource roles
0 Groups and Teams 0 Apps 1 SPO
Policies
1 Enabled 0 Disabled
Activity
0 Assignments 0 Pending Requests
N/A Change Propagation Sync
Incompatible assignments (Preview)
0

ortal ...

Edit Delete

Access to Event portal

This package gives access to our Event portal

Properties

Created by
admin@M365x52799878.onmicrosoft.com

Created on
10/31/2023

Object Id
eb815f92-dcaf-43f1-8a43-1bf6216a5e09

Catalog
General

Hidden
No

My Access portal link
https://myaccess.microsoft.com/@M365x52799878....

Contents

Resource roles

0 Groups and Teams **0** Apps **1** SPO

Policies

1 Enabled **0** Disabled

Activity

0 Assignments **0** Pending Requests

N/A Change Propagation Sync

Incompatible assignments (Preview)

0

Access package created succe

Created access package Access to catalog General.

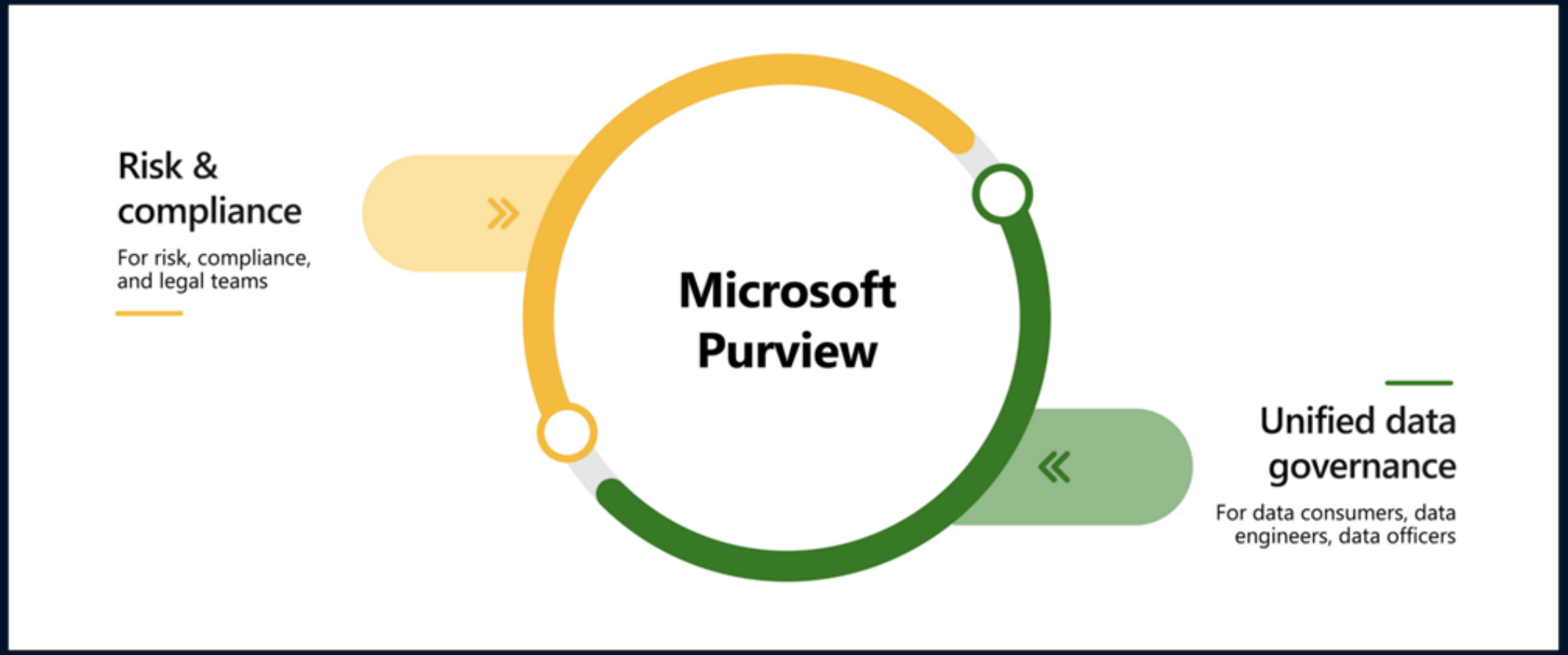
More Details

Correlation id

6e2a3236-55ae-44b4-9c53-1748d

Data governance

Microsoft Purview



Microsoft Purview

Unified data governance

For data consumers, data engineers, data officers

Microsoft Purview – Sensitivity labeling

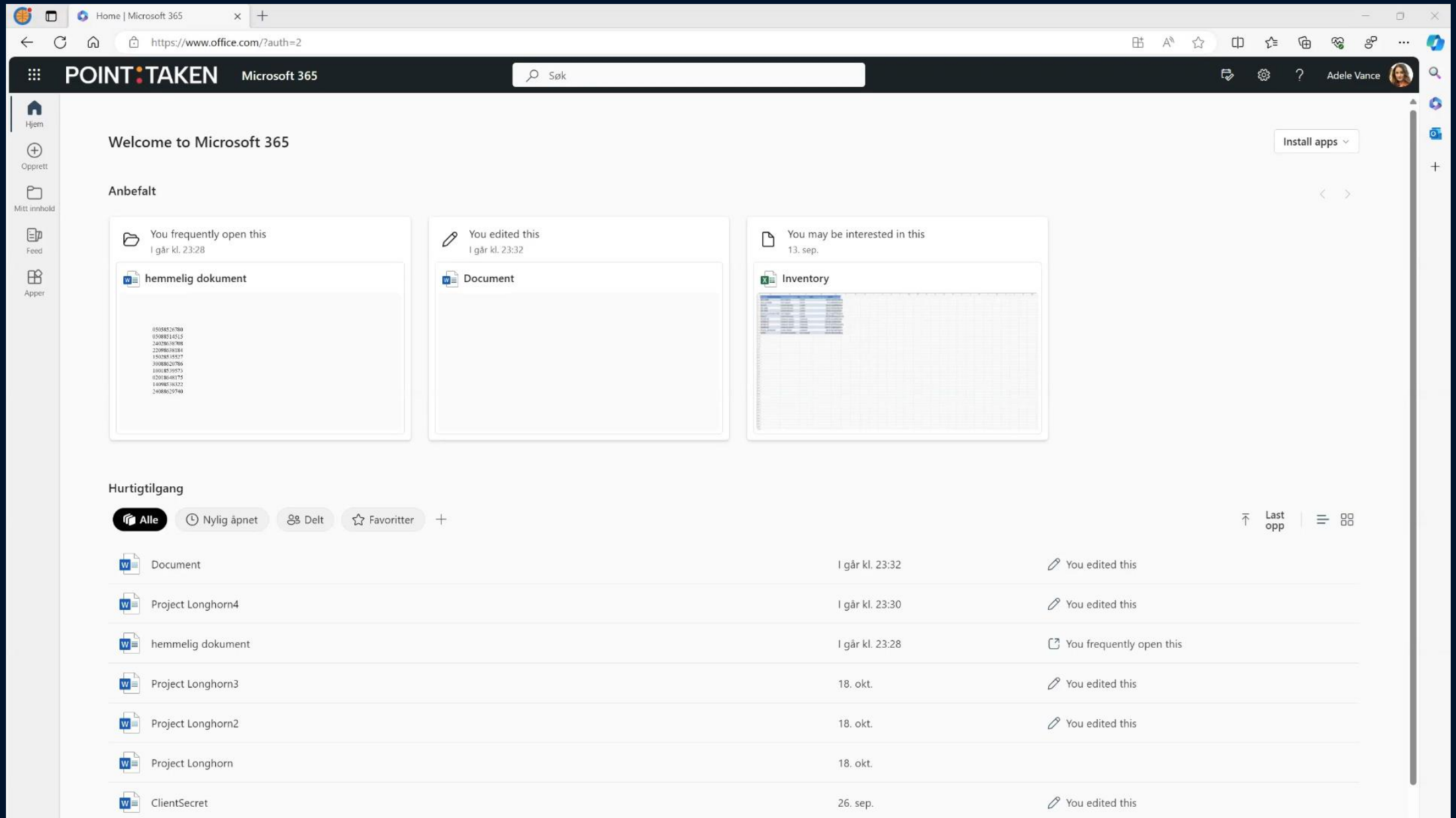
Labeling helps organizations discover, classify and protect sensitive documents, emails and meetings, and groups and sites.

- Microsoft 365 E5/A5/G5/E3/A3/G3/F1/F3/Business Premium/OneDrive for Business (Plan 2)
- Enterprise Mobility + Security E3/E5
- Office 365 E5/A5/E3/A3

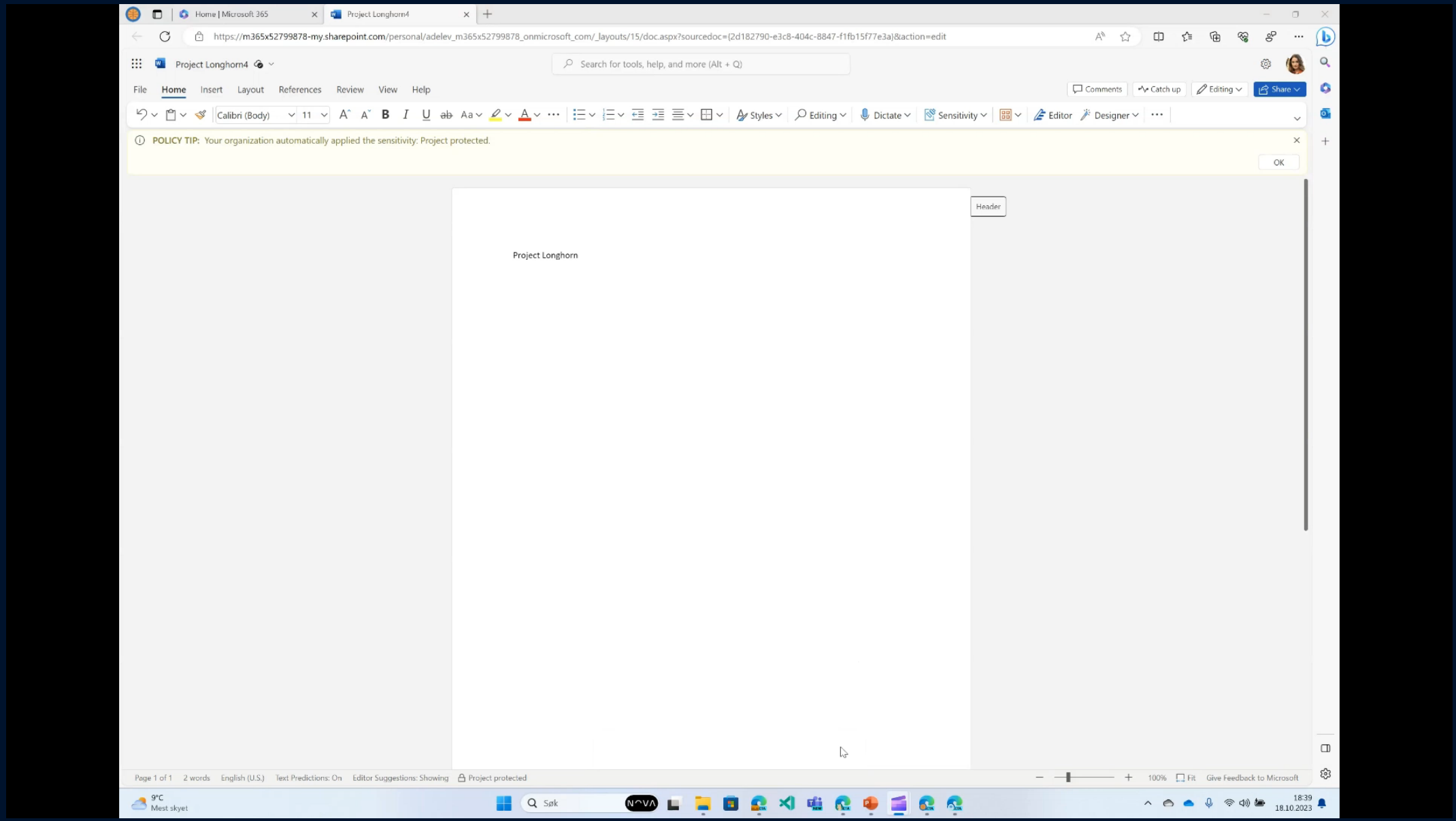
DEMO

Microsoft Purview

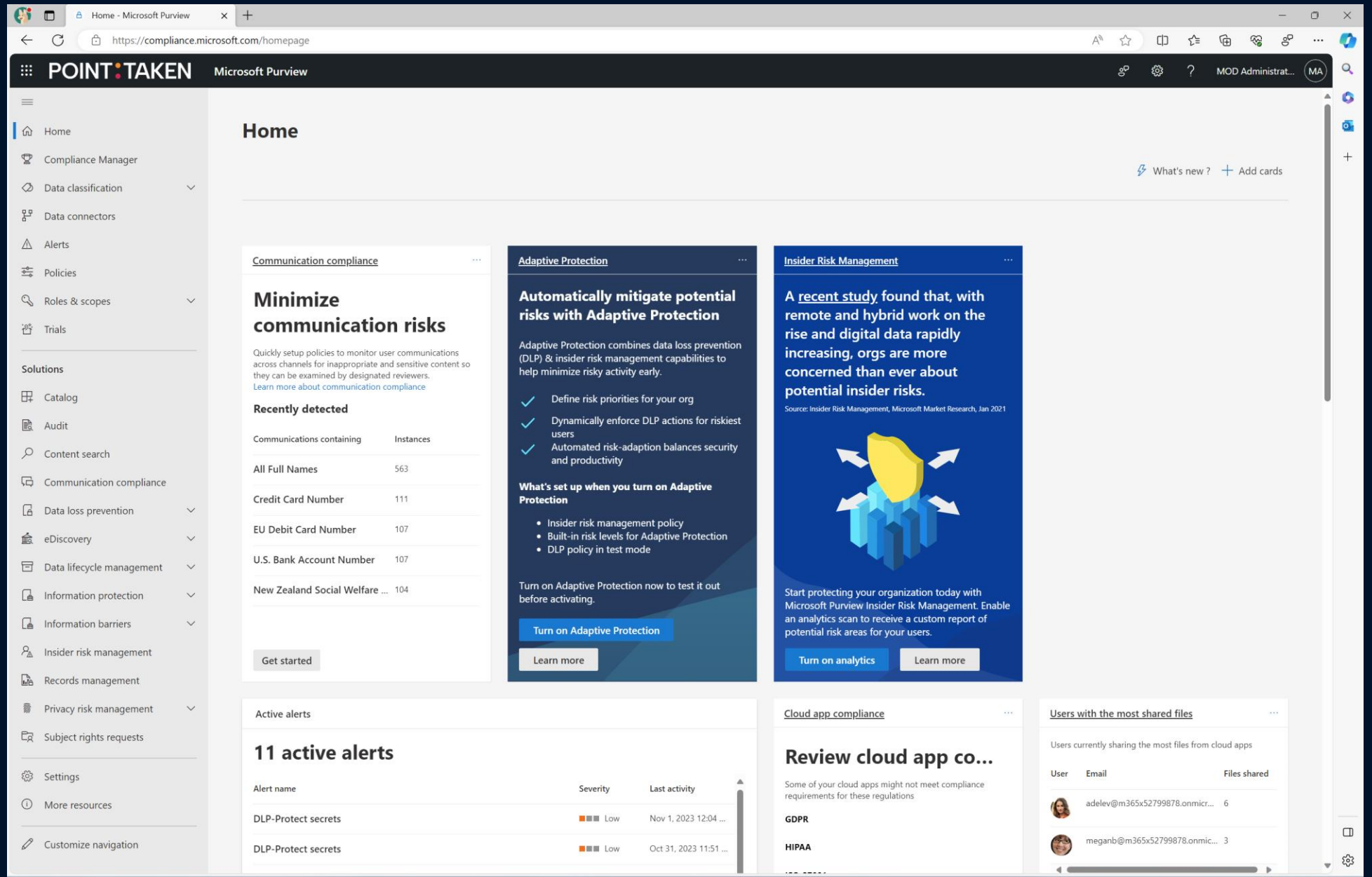
Autolabeling



Watermark


Home | Microsoft 365
Project Longhorn4
https://m365x52799878-my.sharepoint.com/personal/adelev_m365x52799878_onmicrosoft_com/_layouts/15/doc.aspx?sourcedoc={2d182790-e3c8-404c-8847-f1fb15f77e3a}&action=edit
Search for tools, help, and more (Alt + Q)
File
Home
Insert
Layout
References
Review
View
Help
Comments
Catch up
Editing
Share
Calibri (Body)
11
Styles
Editing
Dictate
Sensitivity
Editor
Designer
POLICY TIP: Your organization automatically applied the sensitivity: Project protected.
OK
Header
Project Longhorn
Page 1 of 1
2 words
English (U.S.)
Text Predictions: On
Editor Suggestions: Showing
Project protected
100%
Fit
Give Feedback to Microsoft
9°C
Mest skyet
Søk
18:39
18.10.2023

Sensitivity label



- Compliance Manager
- Data classification
- Data connectors
- Alerts
- Policies
- Roles & scopes
- Trials

Solutions

- Catalog
- Audit
- Content search
- Communication compliance
- Data loss prevention
- eDiscovery
- Data lifecycle management
- Information protection
  - Overview
  - Labels
  - Label policies
  - Auto-labeling
- Information barriers
- Insider risk management

Labels

Communication compliance

Minimize communication risks

Quickly setup policies to monitor user communications across channels for inappropriate and sensitive content so they can be examined by designated reviewers.
Learn more about communication compliance

Recently detected

Communications containing	Instances
All Full Names	563
Credit Card Number	111
EU Debit Card Number	107
U.S. Bank Account Number	107
New Zealand Social Welfare ...	104

Get started

Adaptive Protection

Automatically mitigate potential risks with Adaptive Protection

Adaptive Protection combines data loss prevention (DLP) & insider risk management capabilities to help minimize risky activity early.

- Define risk priorities for your org
- Dynamically enforce DLP actions for riskiest users
- Automated risk-adaption balances security and productivity

What's set up when you turn on Adaptive Protection

- Insider risk management policy
- Built-in risk levels for Adaptive Protection
- DLP policy in test mode

Turn on Adaptive Protection now to test it out before activating.

Turn on Adaptive Protection

Learn more

Insider Risk Management

A recent study found that, with remote and hybrid work on the rise and digital data rapidly increasing, orgs are more concerned than ever about potential insider risks.

Source: Insider Risk Management, Microsoft Market Research, Jan 2021

Start protecting your organization today with Microsoft Purview Insider Risk Management. Enable an analytics scan to receive a custom report of potential risk areas for your users.

Turn on analytics

Learn more

Active alerts

11 active alerts

Cloud app compliance

Review cloud app co...

Users with the m

Users currently shar

Home
Compliance Manager
Data classification
Data connectors
Alerts
Policies
Roles & scopes
Trials

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Data lifecycle management

Labels

You can now create sensitivity labels with privacy and access control settings for Teams, SharePoint sites, and Microsoft 365 Groups. To do this, you must first complete these steps to enable the feature.

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settir encrypt files, add content marking, and control user access to specific sites. Learn more about sensitivity labels

Create a label | Publish labels | Export | Refresh

Name	Priority	Scope	Created by	Last modif
Personal	0 - lowest	File, Email		Sep 13, 20
Public	1	File, Email		Sep 13, 20
General	2	File, Email		Sep 13, 20
Confidential	5	File, Email		Sep 13, 20
Highly Confidential	9	File, Email		Sep 13, 20
Confidential - Finance	13	File, Email	Megan Bowen	Sep 13, 20
Project protected	14	File, Email, Meetings, Schematized dat...	MOD Administrator	Oct 1, 202
super secret label	15 - highest	File, Email, Meetings, Schematized dat...	MOD Administrator	Oct 22, 20

New sensitivity label

- Label details
- Scope
- Items
- Groups & sites
- Schematized data assets (preview)
- Finish

Provide basic details for this label

The protection settings you choose for this label will be immediately enforced on the items or content containers to which it's applied. Labeled files will be protected wherever they go, whether they're saved in the cloud or downloaded to a computer.

Name *

Super secret label

Display name *

Super secret label

Description for users *

Use this label to mark your super secret files in your project

Description for admins

Enter a description that's helpful for admins who will manage this label

Label color

Name and tooltip

The protection settings you choose for this label will be immediately enforced on the items or content containers to which it's applied. Labeled files will be protected wherever they go, whether they're saved in the cloud or downloaded to a computer.

Name *

Super secret label

Display name *

Super secret label

Description for users *

Use this label to mark your super secret files in your project

Description for admins

Enter a description that's helpful for admins who will manage this label

Label color

The color selected below is currently applied to the parent label. As a result, all sublabels of the parent label will inherit the same color. If you want to use a different color, edit the parent label. Learn more about label color

New sensitivity label

- Name and tooltip
- **Scope**
- Items
- Groups & sites
- Schematized data assets (preview)
- Finish

Define the scope for this label

Labels can be applied directly to items (such as files, emails, meetings), containers like SharePoint sites and Teams, Power BI items, schematized data assets, and more. Let us know where you want this label to be used so you can configure the applicable protection settings. Learn more about label scopes

- [x] **Items**

  Be aware that restricting the scope to only files or emails might impact encryption settings and where the label can be applied. Learn more

  - [x] Files

    Protect files created in Word, Excel, PowerPoint, and more.

  - [x] Emails

    Protect messages sent from all versions of Outlook.

  - [x] Meetings

    Protect calendar events and meetings scheduled in Outlook and Teams.

    ⓘ Parent label will automatically inherit meeting scope from sub labels

- [ ] Groups & sites

  Configure privacy, access control, and other settings to protect labeled Teams, Microsoft 365 Groups, and SharePoint sites.

  ⓘ To apply sensitivity labels to Teams, SharePoint sites, and Microsoft 365 Groups, you must first complete these steps to enable the feature.

- [x] **Schematized data assets (preview)**

  Apply labels to files and schematized data assets in Microsoft Purview Data Map. Schematized data assets include SQL, Azure SQL, Azure Synapse, Azure Cosmos, AWS RDS, and more.

New sensitivity label

- Label details
- Scope
- **Items**
- Groups & sites
- Schematized data assets (preview)
- Finish

Choose protection settings for labeled items

Configure encryption and content marking settings to protect labeled items.

- [ ] **Apply or remove encryption**
  Control who can access items that have this label applied.
- [ ] **Apply content marking**
  Add custom headers, footers, and watermarks to items that have this label applied.
- [ ] **Protect Teams meetings and chats**
  Configure protection settings for Teams meetings and chats.

New sensitivity label

- Label details
- Scope
- **Items**
- Groups & sites
- Schematized data assets (preview)
- Finish

Choose protection settings for labeled items

Configure encryption and content marking settings to protect labeled items.

- [x] **Apply or remove encryption**
  Control who can access items that have this label applied.
- [x] **Apply content marking**
  Add custom headers, footers, and watermarks to items that have this label applied.
- [ ] **Protect Teams meetings and chats**
  Configure protection settings for Teams meetings and chats.

New sensitivity label

- Label details
- Scope
- **Items**
- **Encryption**
- Content marking
- Auto-labeling for files and emails
- Groups & sites
- Schematized data assets (preview)
- Finish

Encryption

Control who can access items that have this label applied. Items include emails, Office files, Power BI files, and meeting invites (if you chose to configure meeting settings for this label). Learn more about encryption settings

- ( ) Remove encryption if the file or email or calendar event is encrypted
- (•) Configure encryption settings

Assign permissions now or let users decide?

Assign permissions now

The encryption settings you choose will be automatically enforced when the label is applied to email and Office files.

User access to content expires

Never

Allow offline access

Always

Assign permissions to specific users and groups *

Assign permissions

0 items

Users and groups	Permissions	Edit	Delete
No data available			

☐ Use Double Key Encryption

Labels - Microsoft Purview

https://compliance.microsoft.com/informationprotection/labels

POINT TAKEN Microsoft Purview

MOD Administrat

New sensitivity label

- Label details
- Scope
- **Items**
- **Encryption**
- Content marking
- Auto-labeling for files and emails
- Groups & sites
- Schematized data assets (preview)
- Finish

Encryption

Control who can access items that have this label applied. Items include emails, Office files, Po
to configure meeting settings for this label). Learn more about encryption settings

- ( ) Remove encryption if the file or email or calendar event is encrypted
- (•) Configure encryption settings

Assign permissions now or let users decide?

Assign permissions now

The encryption settings you choose will be automatically enforced when the label is applied to email and O

User access to content expires

Never

Allow offline access

Always

Assign permissions to specific users and groups *

Assign permissions

Users and groups	Permissions
No data available	

[ ] Use Double Key Encryption

Assign permissions

Only the users or groups you choose will be assigned permissions to use the content that this label applied. You can choose from existing permissions (such as Co-Owner, Co-Auth and Reviewer) or customize them to meet your needs.

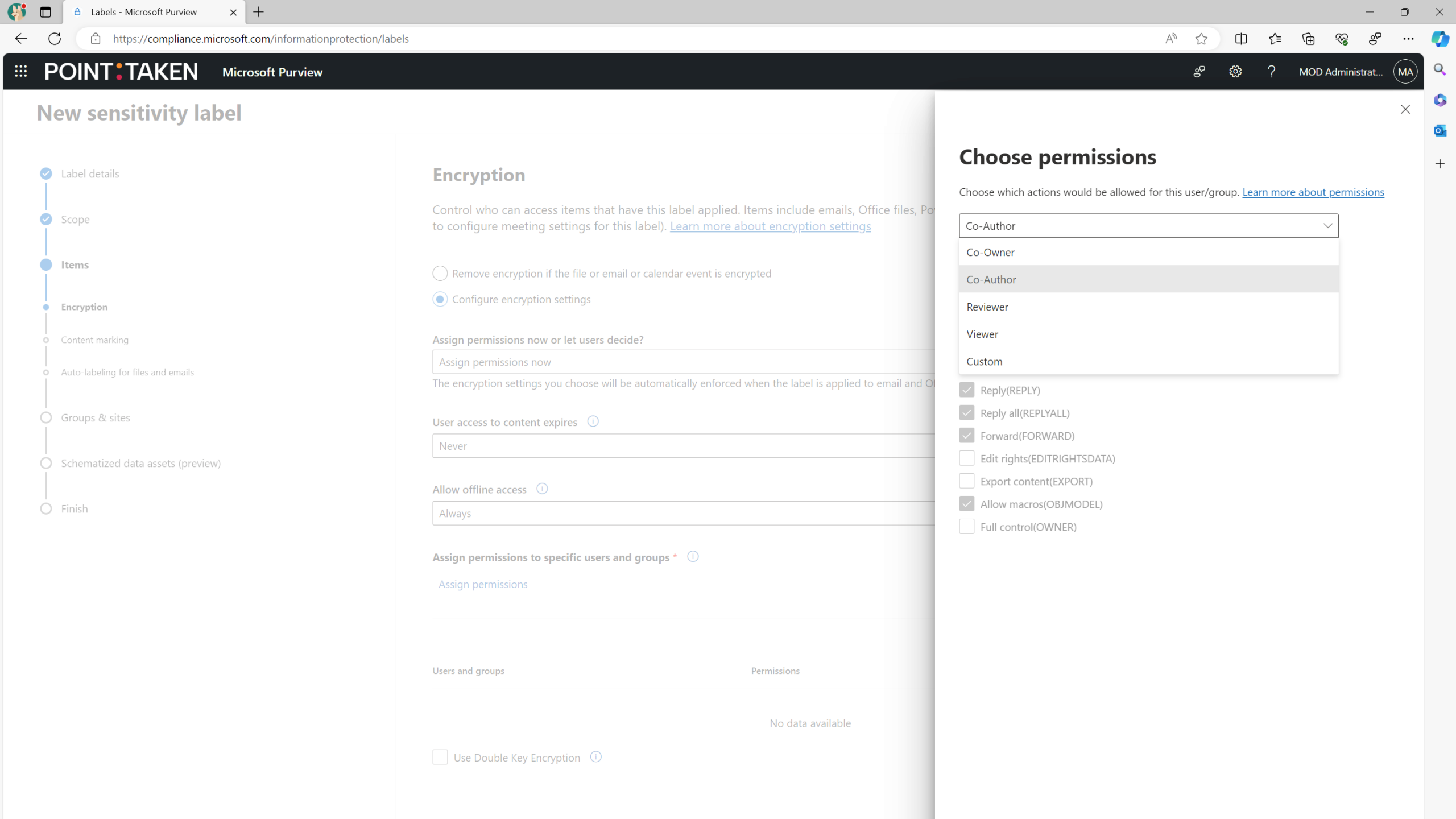
- + Add all users and groups in your organization
- + Add any authenticated users
- + Add users or groups
- + Add specific email addresses or domains

0 ite

Permissions assigned to	Delete
No data available	

Choose permissions

Co-Author
View content,View rights,Edit content,Save,Print,Copy and extract content,Reply,Reply all,Forward,Allow macros


Labels - Microsoft Purview
https://compliance.microsoft.com/informationprotection/labels
POINT:TAKEN
Microsoft Purview
MOD Administrat...
MA
New sensitivity label
Label details
Scope
Items
Encryption
Content marking
Auto-labeling for files and emails
Groups & sites
Schematized data assets (preview)
Finish
Encryption
Control who can access items that have this label applied. Items include emails, Office files, Po
to configure meeting settings for this label). Learn more about encryption settings
Remove encryption if the file or email or calendar event is encrypted
Configure encryption settings
Assign permissions now or let users decide?
Assign permissions now
The encryption settings you choose will be automatically enforced when the label is applied to email and O
User access to content expires
Never
Allow offline access
Always
Assign permissions to specific users and groups *
Assign permissions
Users and groups
Permissions
No data available
Use Double Key Encryption
Choose permissions
Choose which actions would be allowed for this user/group. Learn more about permissions
Co-Author
Co-Owner
Co-Author
Reviewer
Viewer
Custom
Reply(REPLY)
Reply all(REPLYALL)
Forward(FORWARD)
Edit rights(EDITRIGHTSDATA)
Export content(EXPORT)
Allow macros(OBJMODEL)
Full control(OWNER)

ns

yption

ent marking

-labeling for files and emails

ups & sites

ematized data assets (preview)

sh

Remove encryption if the file or email or calendar event is encrypted

Configure encryption settings

Assign permissions now or let users decide?

Assign permissions now

The encryption settings you choose will be automatically enforced when the label is applied to email and Office files.

User access to content expires

Never

Allow offline access

Always

Assign permissions to specific users and groups *

Assign permissions

2 item

Users and groups	Permissions	Edit	Delete
Authenticated users	Co-Author		
M365x52799878.onmicrosoft.com	Co-Author		

Use Double Key Encryption

New sensitivity label

- Label details
- Scope
- **Items**
- Encryption
- **Content marking**
- Auto-labeling for files and emails
- Groups & sites
- Schematized data assets (preview)
- Finish

Content marking

Add custom headers, footers, and watermarks to content that has this label applied. Learn more about content marking

All content marking will be applied to documents but only the header and footer will be applied to email messages. If you chose to configure meeting settings for this label, the header and footer will also be applied to meeting invites.

Content marking

New sensitivity label

- Label details
- Scope
- **Items**
- Encryption
- **Content marking**
- Auto-labeling for files and emails
- Groups & sites
- Schematized data assets (preview)
- Finish

Content marking

Add custom headers, footers, and watermarks to content that has this label applied. Learn more about content marking

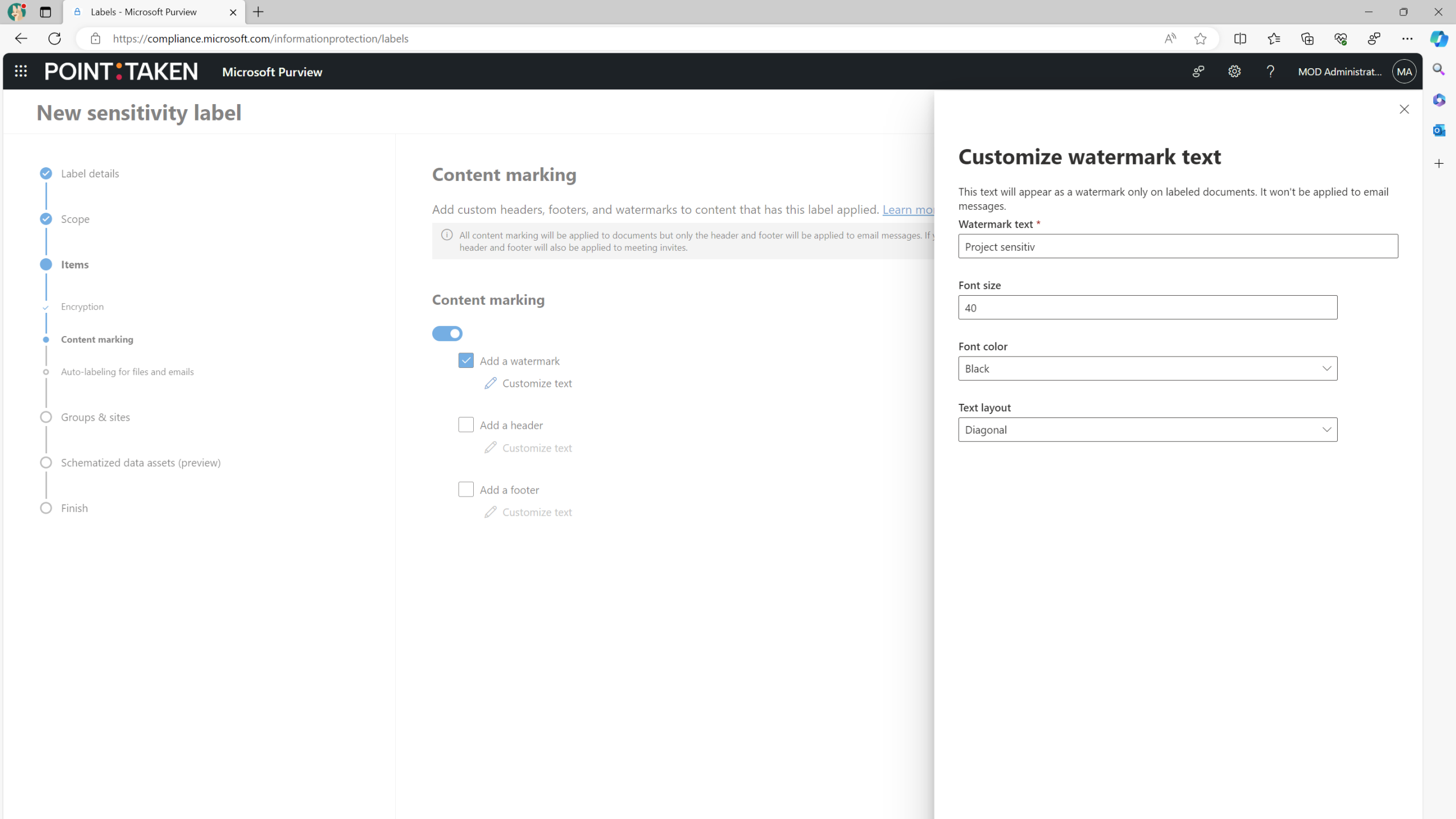
All content marking will be applied to documents but only the header and footer will be applied to email messages. If you chose to configure meeting settings for this label, the header and footer will also be applied to meeting invites.

Content marking

Add a watermark
Customize text

Add a header
Customize text

Add a footer
Customize text


Labels - Microsoft Purview
https://compliance.microsoft.com/informationprotection/labels
POINT:TAKEN
Microsoft Purview
MOD Administrat...
MA
New sensitivity label
Label details
Scope
Items
Encryption
Content marking
Auto-labeling for files and emails
Groups & sites
Schematized data assets (preview)
Finish
Content marking
Add custom headers, footers, and watermarks to content that has this label applied. Learn mo
All content marking will be applied to documents but only the header and footer will be applied to email messages. If
header and footer will also be applied to meeting invites.
Content marking
Add a watermark
Customize text
Add a header
Customize text
Add a footer
Customize text
Customize watermark text
This text will appear as a watermark only on labeled documents. It won't be applied to email messages.
Watermark text *
Project sensitiv
Font size
40
Font color
Black
Text layout
Diagonal

New sensitivity label

- Label details
- Scope
- **Items**
- Encryption
- Content marking
- **Auto-labeling for files and emails**
- Groups & sites
- Schematized data assets (preview)
- Finish

Auto-labeling for files and emails

When users edit Office files or compose, reply to, or forward emails from Outlook that contain content matching the conditions you choose here, we'll automatically apply this label or recommend that they apply it themselves. Learn more about auto-labeling for Microsoft Purview

We'll also apply this label to files that match the same conditions in Azure Blob Storage, Azure Files, Azure Data Lake Storage, and Amazon S3. Learn more about auto-labeling in Microsoft Purview Data Map

To automatically apply this label to files that are already saved (in SharePoint and OneDrive) or emails that are already processed by Exchange, you must create an auto-labeling policy. Learn more about auto-labeling policies

Auto-labeling for files and emails

New sensitivity label

- Label details
- Scope
- Items
- **Groups & sites**
- Schematized data assets (preview)
- Finish

Define protection settings for groups and sites

These settings apply to teams, groups, and sites that have this label applied. They don't apply directly to the files stored in those containers.
Learn more about these settings

- [ ] **Privacy and external user access**
  Control the level of access that internal and external users will have to labeled teams and Microsoft 365 Groups.
- [ ] **External sharing and Conditional Access**
  Control external sharing and configure Conditional Access settings to protect labeled SharePoint sites.

New sensitivity label

- Label details
- Scope
- Items
- Groups & sites
- **Schematized data assets (preview)**
- Finish

Auto-labeling for schematized data assets (preview)

Automatically apply this label to schematized data assets in Microsoft Purview Data Map that contain the sensitive info types you choose here. You can automatically label database columns in SQL, Azure SQL, Azure Synapse, Azure Cosmos, AWS RDS, and various other data sources governed by Microsoft Purview Data Map. Learn more about auto-labeling for schematized data assets

Auto-labeling for schematized data assets (preview)

New sensitivity label

- Label details
- Scope
- Items
- Groups & sites
- Schematized data assets (preview)
- **Finish**

Review your settings and finish

Name
Super secret labelz
Edit

Display name
Super secret label
Edit

Description for users
Use this label to mark your super secret files in your project
Edit

Scope
File, Email, Meetings, Schematized data assets
Edit

Encryption
Encryption
Edit

Content marking
Watermark: Project sensitiv
Edit

Auto-labeling for files and emails
None
Edit

Meetings settings
Edit

Auto-labeling for schematized data assets (preview)
None
Edit

sensitivity label

me and tooltip

pe

ns

ups & sites

ematized data assets (preview)

sh

Your sensitivity label was created

Creating the label is just the first step in classifying and protecting content. To make this label available to users in your organization, you can auto-apply it to specific content and publish it to users' apps.

Next steps

- (●) **Publish label to users' apps**
  Create a label policy to make the label available in Office apps, SharePoint, Teams, and Microsoft 365 Groups. Once published, users will be able to apply it to protect their content. Learn more about publishing labels
- ( ) **Don't create a policy yet**
  You can publish or auto-apply this label later.

Recommended resources based on your settings

Review prerequisites to get the most out of your encryption settings
Review prerequisites for applying sensitivity labels to Power BI content.
Review a Microsoft Purview Data Map tutorial on how to start scanning assets and automatically apply this label

Home
Compliance Manager
Data classification
Data connectors
Alerts
Policies
Roles & scopes
Trials

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Data lifecycle management
Information protection
Overview
Labels
Label policies
Auto-labeling
Information barriers
Insider risk management

Labels

You can now create sensitivity labels with privacy and access control settings for Teams, SharePoint sites, and Microsoft 365 Groups. To do this, you must first complete these steps to enable the feature.

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. Learn more about sensitivity labels

Create sublabel | Create auto-labeling policy | Publish label | Edit label | Reprioritize | Delete label | Refresh

1 of 8 selected

Name	Priority	Scope	Created by	Last modified
Personal	0 - lowest	File, Email		Sep 13, 2023 8:12:18 AM
Public	1	File, Email		Sep 13, 2023 8:12:18 AM
General	2	File, Email		Sep 13, 2023 8:12:19 AM
Confidential	5	File, Email		Sep 13, 2023 8:12:21 AM
Highly Confidential	9	File, Email		Sep 13, 2023 8:12:28 AM
Confidential - Finance	13	File, Email	Megan Bowen	Sep 13, 2023 11:38:34 AM
Project protected	14	File, Email, Meetings, Schematized dat...	MOD Administrator	Oct 1, 2023 9:42:20 PM
super secret label	15 - highest	File, Email, Meetings, Schematized dat...	MOD Administrator	Oct 22, 2023 11:19:42 PM

iance Manager
lassification
onnectors
s
& scopes
g
nt search
unication compliance
oss prevention
very
fecycle management
ation protection
ew
policies

Labels

You can now create sensitivity labels with privacy and access control settings for Teams, SharePoint sites, and Microsoft 365 Groups. To do this, you must first complete these steps to enable the feature.

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For examp
encrypt files, add content marking, and control user access to specific sites. Learn more about sensitivity labels

+ Create sublabel | Create auto-labeling policy | Publish label | Edit label | Reprioritize | Delete label | Refresh

Name	Priority	Scope	Created by	Last modified
Personal	0 - lowest	File, Email		Sep 13, 2023 8:12:18 AM
Public	1	File, Email		Sep 13, 2023 8:12:18 AM
General	2	File, Email		Sep 13, 2023 8:12:19 AM
Confidential	5	File, Email		Sep 13, 2023 8:12:21 AM
Highly Confidential	9	File, Email		Sep 13, 2023 8:12:28 AM
Confidential - Finance	13	File, Email	Megan Bowen	Sep 13, 2023 11:38:34 AM
Project protected	14	File, Email, Meetings, Schematized dat...	MOD Administrator	Oct 1, 2023 9:42:20 PM
super secret label	15 - highest	File, Email, Meetings, Schematized dat...	MOD Administrator	Oct 22, 2023 11:19:42 PM

- Name
- Admin units
- Locations
- Policy rules
- Label
- Policy mode
- Finish

Name your auto-labeling policy

This policy will automatically apply a label to items that match rules and conditions you'll define.

Name *

super secret label auto-labeling policy

Description

Enter a description for your new auto-labeling policy

- Name
- **Admin units**
- Locations
- Policy rules
- Label
- Policy mode
- Finish

Assign admin units

Choose the admin units you'd like to assign this policy to. Admin units are created in Azure Active Directory and restrict the policy to a specific set of users or groups. Your selections will affect the location options available to you in the next step.

If you want to assign this policy to all users and groups, select 'Next' and proceed. Learn more about admin units

+ Add or remove admin units

Admin units

Full directory

Choose locations where you want to apply the label

Exchange will automatically apply the label to unlabeled emails, regardless of which device or platform is used to send and receive the email. OneDrive and SharePoint will automatically apply the label to unlabeled Office documents and PDFs.

Tip Edit the "Auto-labeling" settings for this label to ensure that that it's automatically applied to documents when they're saved and emails when they're sent.

If your role group permissions are restricted to a specific set of users or groups, you'll only be able to apply the label to those users or groups. Learn more about role group permissions.

View role groups

Location	Scope	
Exchange email	All users & groups	Edit
SharePoint sites	All sites	Edit
OneDrive accounts	All users & groups	Edit

- Name
- Admin units
- Locations
- **Policy rules**
- Label
- Policy mode
- Finish

Set up common or advanced rules

Rules are made up of conditions that define what content the label is applied to. Choose common rules to define one set of rules that will apply to all locations you selected or choose advanced rules to define different rules for each location.

(●) **Common rules.** Define one set of common rules for all locations.

ⓘ Common rules consist of conditions for specifying what sensitive info to detect and whether to apply the label to items shared inside or outside your organization. If you selected Exchange and want access to more email conditions, choose advanced rules.

( ) **Advanced rules.** Define specific rules for each location.

- Name
- Admin units
- Locations
- **Policy rules**
- **Common rules**
- Label
- Policy mode
- Finish

Define rules for content in all locations

We'll automatically apply this label to content that matches the rules and related conditions here. These rules will a
locations you specified.

+ New rule

Name	Statu

No rules created

cy

Define rules for content in all locations

We'll automatically apply this label to content that matches the rules and related conditions here. The locations you specified.

+ New rule

Name

No rules created

- Name
- Admin units
- Locations
- **Policy rules**
- Common rules
- Label
- Policy mode
- Finish

New rule

Name *

Project auto protected

Description

Enter a description for this rule

Conditions

We'll apply this policy to content that matches these conditions.

Add condition

- Content contains
- Content is shared
- File extension is
- Document name contains words or phrases
- Document property is
- Document size equals or is greater than
- Document created by

hes any of these exceptions.

ame

dmin units

cations

olicy rules

ommon rules

bel

olicy mode

nish

Name *

Project auto protected

Description

Enter a description for this rule

Conditions

We'll apply this policy to content that matches these conditions.

+ Add condition

Content contains

Content is shared

File extension is

Document name contains words or phrases

Document property is

Document size equals or is greater than

Document created by

hes any of these exceptions.

New rule

Name *

Project auto protected

Description

Enter a description for this rule

Conditions

We'll apply this policy to content that matches these conditions.

Document name contains words or phrases

Applies label to documents where the file name contains any of the words or phrases you specify.

Enter words and then click 'Add'. Separate multiple entries with commas.

Add

Add condition

Exceptions

We won't apply this rule to content that matches any of these exceptions.

Add exception

New rule

Name *

Project auto protected

Description

Enter a description for this rule

Conditions

We'll apply this policy to content that matches these conditions.

Document name contains words or phrases

Applies label to documents where the file name contains any of the words or phrases you specify.

Project

Longhorn

Enter words and then click 'Add'. Separate multiple entries with commas.

Add

Add condition

Exceptions

We won't apply this rule to content that matches any of these exceptions.

Add exception

We'll apply this policy to content that matches these conditions.

Document name contains words or phrases

Applies label to documents where the file name contains any of the words or phrases you specify.

Project

Longhorn

Enter words and then click 'Add'. Separate multiple entries with commas.

Add

Add condition

Exceptions

We won't apply this rule to content that matches any of these exceptions.

Add exception

- Except if file extension is
- Except if attachment or document name contains words or phrases
- Except if document property is
- Except if document size equals or is greater than
- Except if document created by

Define rules for content in all locations

We'll automatically apply this label to content that matches the rules and related conditions here. These rules will apply to content in all locations you specified.

+ New rule

1 item

Name	Status
Project auto protected	

Conditions
Document name contains words or phrases
Project
Longhorn

- Name
- Admin units
- Locations
- Policy rules
- **Label**
- Policy mode
- Finish

Choose a label to auto-apply

Users will see this label applied to files that match the rules and conditions you chose. Where will this label appear?

Label to auto-apply
super secret label

Change

- Name
- Admin units
- Locations
- Policy rules
- **Label**
- **Additional email settings**
- Policy mode
- Finish

Additional settings for email

These settings only apply to email messages.

☑ Automatically replace existing labels that have the same or lower priority

If selected, this label will replace existing labels if their priority is the same or lower than this one, regardless of whether the existing label was applied automatically or manually. Learn about label priority

- Name
- Admin units
- Locations
- Policy rules
- Label
- **Policy mode**
- Finish

Decide if you want to test out the policy now or later

To help you determine whether the label will be applied to the correct items, you'll need to run the policy in simulation mode before turning it on. You can do this right away or wait until later.

(•) **Run policy in simulation mode**
We'll gather items that match the policy but labels won't be applied yet. It's highly recommended that you review these items to decide whether the policy needs to be refined or if it's ready to be turned on.

If your role group permissions are restricted to a specific set of users, you'll only be able to view simulation results for those users. Learn more about role group permissions.

View role groups

☑ Automatically turn on policy if not modified after 7 days in simulation.
The 7-day period will restart each time the policy is modified while in simulation.

( ) **Leave policy turned off**
Your settings will be saved, but the policy will be inactive until you run it in simulation mode and then turn it on.

- Name
- Admin units
- Locations
- Policy rules
- Label
- Policy mode
- **Finish**

Review and finish

Policy name

super secret label auto-labeling policy

Edit

Label and policy settings

Label super secret label
Exchange overwrite label true

Edit

Trainable Classifier

Admin units

None

Apply to content in these locations

Exchange email All
SharePoint sites All
OneDrive accounts All

Edit

Exclude content from these locations

Exchange email None
SharePoint sites None
OneDrive accounts None

Edit

Rules for auto-applying this label

Exchange email 1 rule
SharePoint 1 rule
OneDrive 1 rule

Edit

Mode

Simulation : Automatically turn on policy if not modified after 7 days in simulation.

- Name
- Admin units
- Locations
- Policy rules
- Label
- Policy mode
- Finish

Your auto-labeling policy was created

We're running the policy in simulation mode to detect items that match the policy's conditions.

RECOMMENDATION

You're protecting this sensitive data, now make sure it's deleted when no longer relevant to your organization.

Removing unnecessary or obsolete data can reduce your risk during a security incident. Use auto-labeling policies in Data Lifecycle Management to help minimize your attack surface.

Secure Now

Next steps
Check the policy simulation overview in a few hours to review results. You will get an email notification when simulation completes.

Learn more
Learn about auto-labeling policy simulation

DEMO

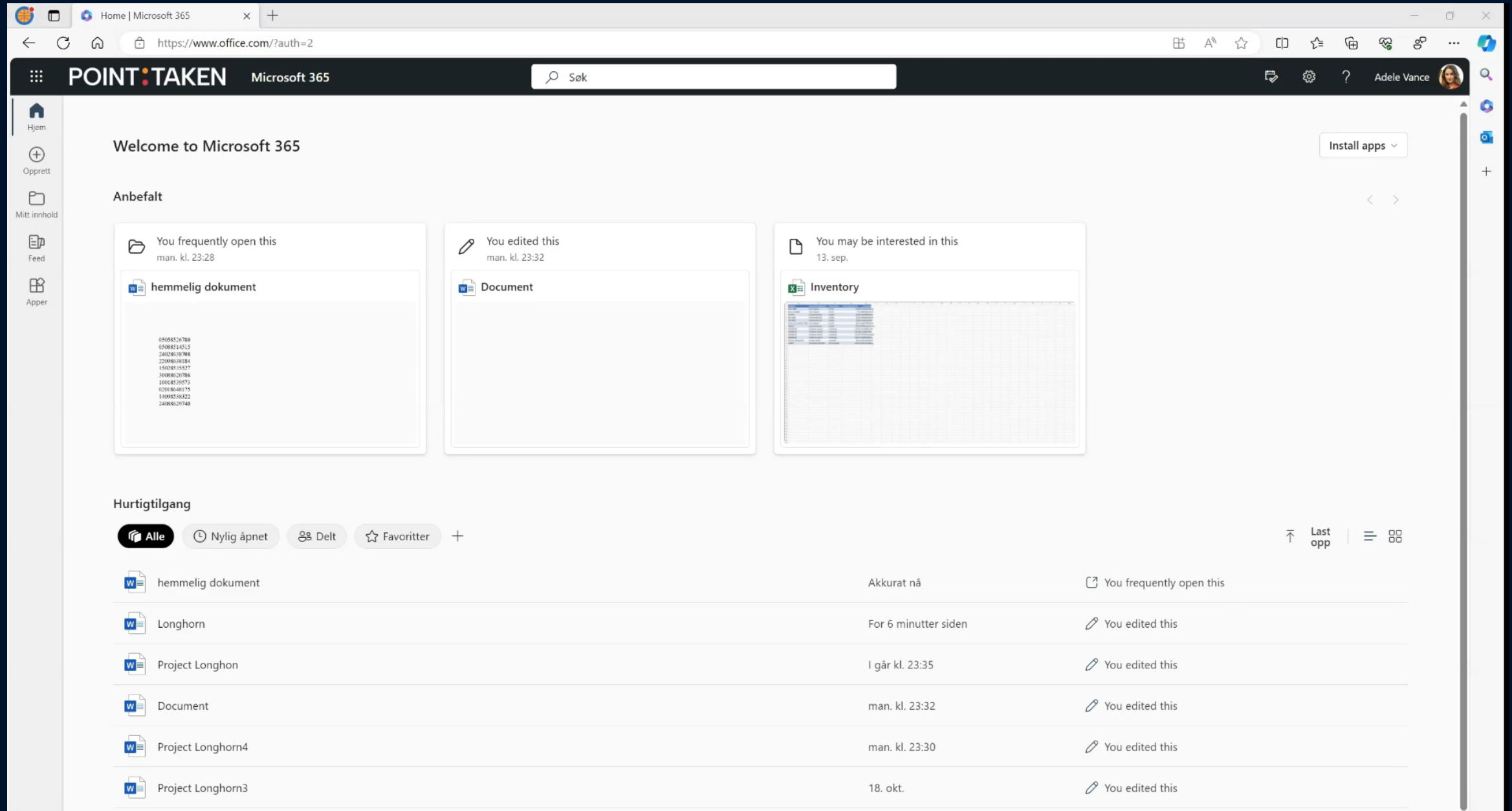
Microsoft Purview

Microsoft Purview – Data loss Prevention

A set of rules that defines how sensitive data should be detected, monitored, and protected in different locations and scenarios.

- Microsoft 365 E5/A5/G5/E3/A3/G3, Microsoft 365 Business Premium, SharePoint Online Plan 2, OneDrive for Business (Plan 2), Exchange Online Plan 2
- Office 365 E5/A5/G5/E3/A3/G3

DLP


Home | Microsoft 365
https://www.office.com/?auth=2
POINT TAKEN
Microsoft 365
Søk
Adele Vance
Hjem
Opprett
Mitt innhold
Feed
Apper
Welcome to Microsoft 365
Install apps
Anbefalt
You frequently open this
man. kl. 23:28
hemmelig dokument
You edited this
man. kl. 23:32
Document
You may be interested in this
13. sep.
Inventory
Hurtigtilgang
Alle
Nylig åpnet
Delt
Favoritter
Last opp
hemmelig dokument
Akkurat nå
You frequently open this
Longhorn
For 6 minutter siden
You edited this
Project Longhon
I går kl. 23:35
You edited this
Document
man. kl. 23:32
You edited this
Project Longhorn4
man. kl. 23:30
You edited this
Project Longhorn3
18. okt.
You edited this

Data loss prevention policy

POINT TAKEN | Microsoft Purview | MOD Administrat... | MA

- Home
- Compliance Manager
- Data classification
- Data connectors
- Alerts
- Policies
- Roles & scopes
- Trials

Solutions

- Catalog
- Audit
- Content search
- Communication compliance
- Data loss prevention
- eDiscovery
- Data lifecycle management
- Information protection
- Information barriers
- Insider risk management
- Records management
- Privacy risk management
- Subject rights requests

Home

What's new ? | Add cards

Communication compliance

Minimize communication risks

Quickly setup policies to monitor user communications across channels for inappropriate and sensitive content so they can be examined by designated reviewers.
Learn more about communication compliance

Recently detected

Communications containing	Instances
All Full Names	560
Credit Card Number	111
EU Debit Card Number	107
U.S. Bank Account Number	107
New Zealand Social Welfare ...	104

Get started

Adaptive Protection

Automatically mitigate potential risks with Adaptive Protection

Adaptive Protection combines data loss prevention (DLP) & insider risk management capabilities to help minimize risky activity early.

- Define risk priorities for your org
- Dynamically enforce DLP actions for riskiest users
- Automated risk-adaption balances security and productivity

What's set up when you turn on Adaptive Protection

- Insider risk management policy
- Built-in risk levels for Adaptive Protection
- DLP policy in test mode

Turn on Adaptive Protection now to test it out before activating.

Turn on Adaptive Protection | Learn more

Insider Risk Management

A recent study found that, with remote and hybrid work on the rise and digital data rapidly increasing, orgs are more concerned than ever about potential insider risks.

Source: Insider Risk Management, Microsoft Market Research, Jan 2021

Start protecting your organization today with Microsoft Purview Insider Risk Management. Enable an analytics scan to receive a custom report of potential risk areas for your users.

Turn on analytics | Learn more

Compliance Manager

Your compliance score: 43%

Compliance Manager helps your org simplify compliance and reduce risks around data protection and regulatory standards. Your score reflects your current compliance posture and helps you see what needs attention.

Learn more about Compliance Manager

Protect information	27 / 81
Control access	81 / 381
Manage devices	0 / 282
Protect against threats	0 / 136
Discover and respond	0 / 69
Manage internal risks	0 / 40
Manage compliance	9500 / 21112

Current score | Remaining score

Updated Today at 11:01 PM

Visit Compliance Manager

Active alerts

12 active alerts

Cloud app compliance

Users with the most shared files

Users currently sharing the most files from cloud apps

Home
Compliance Manager
Data classification
Data connectors
Alerts
Policies
Roles & scopes
Trials

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
eDiscovery
Data lifecycle management
Information protection
Information barriers
Insider risk management
Records management
Privacy risk management
Subject rights requests

Settings

Home

What's new ? Add cards

Communication compliance

Minimize communication risks

Quickly setup policies to monitor user communications across channels for inappropriate and sensitive content so they can be examined by designated reviewers.
Learn more about communication compliance

Recently detected

Communications containing	Instances
All Full Names	560
Credit Card Number	111
EU Debit Card Number	107
U.S. Bank Account Number	107
New Zealand Social Welfare ...	104

Get started

Adaptive Protection

Automatically mitigate potential risks with Adaptive Protection

Adaptive Protection combines data loss prevention (DLP) & insider risk management capabilities to help minimize risky activity early.

- Define risk priorities for your org
- Dynamically enforce DLP actions for riskiest users
- Automated risk-adaption balances security and productivity

What's set up when you turn on Adaptive Protection

- Insider risk management policy
- Built-in risk levels for Adaptive Protection
- DLP policy in test mode

Turn on Adaptive Protection now to test it out before activating.

Turn on Adaptive Protection
Learn more

Insider Risk Management

A recent study found that, with remote and hybrid work on the rise and digital data rapidly increasing, orgs are more concerned than ever about potential insider risks.

Source: Insider Risk Management, Microsoft Market Research, Jan 2021

Start protecting your organization today with Microsoft Purview Insider Risk Management. Enable an analytics scan to receive a custom report of potential risk areas for your users.

Turn on analytics
Learn more

Compliance Manager

Your compliance score: 43%

Compliance Manager helps your org simplify compliance and reduce risks around data protection and regulatory standards. Your score reflects your current compliance posture and helps you see what needs attention.

Learn more about Compliance Manager

Protect information	27 / 81
Control access	81 / 381
Manage devices	0 / 282
Protect against threats	0 / 136
Discover and respond	0 / 69
Manage internal risks	0 / 40
Manage compliance	9500 / 21112

Current score Remaining score

Updated Today at 11:01 PM

Visit Compliance Manager

Active alerts

12 active alerts

Alert name	Severity	Last activity

Cloud app compliance

Review cloud app co...

Some of your cloud apps might not meet compliance

Users with the most shared files

Users currently sharing the most files from cloud apps

User	Email	Files shared

Home
Compliance Manager
Data classification
Data connectors
Alerts
Policies
Roles & scopes
Trials

Solutions

Catalog
Audit
Content search
Communication compliance
Data loss prevention
Overview
Policies
Alerts
Endpoint DLP settings
Activity explorer
eDiscovery
Data lifecycle management
Information protection
Information barriers
Insider risk management
Records management

Policies

Use data loss prevention (DLP) policies to help identify and protect your organization's sensitive info. For example you can set up policies to help make sure information in email and docs isn't shared with the wrong people. Learn more about DLP

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

View role groups

Create policy | Export | Refresh

6 items | Search

Name	Priority	Last modified	Status
U.S. Financial Data	0	Sep 13, 2023 2:44 AM	On
General Data Protection Regulation (GDPR)	1	Sep 13, 2023 2:44 AM	On
Default policy for Teams	2	Sep 13, 2023 8:12 AM	On
Default policy for devices	3	Sep 13, 2023 8:12 AM	On
Block norwegian id	4	Sep 24, 2023 12:11 AM	On
Compant secret project	5	Nov 1, 2023 12:00 AM	Off

Home
Compliance Manager
Data classification
Data connectors
Alerts
Policies
Roles & scopes
Trials

Solutions
Catalog
Audit
Content search
Communication compliance
Data loss prevention
Overview
Policies
Alerts
Endpoint DLP settings
Activity explorer
eDiscovery
Data lifecycle management
Information protection
Information barriers
Insider risk management
Records management

Policies

Use data loss prevention (DLP) policies to help identify and protect your organization's sensitive info. For example you can set up policies to help make sure information in email and docs isn't shared with the wrong people. Learn more about DLP

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

View role groups

+ Create policy | Export | Refresh

6 items | Search

Name	Priority	Last modified	Status
U.S. Financial Data	0	Sep 13, 2023 2:44 AM	On
General Data Protection Regulation (GDPR)	1	Sep 13, 2023 2:44 AM	On
Default policy for Teams	2	Sep 13, 2023 8:12 AM	On
Default policy for devices	3	Sep 13, 2023 8:12 AM	On
Block norwegian id	4	Sep 24, 2023 12:11 AM	On
Compant secret project	5	Nov 1, 2023 12:00 AM	Off

- Template or custom policy
- Name
- Admin units
- Locations
- Policy settings
- Policy mode
- Finish

Start with a template or create a custom policy

Choose an industry regulation to see the DLP policy templates you can use to protect that info or create a custom policy start from scratch. If you need to protect labeled content, you'll be able to choose labels later. Learn more about DLP policy templates

Check out our new enhanced policy templates. These enhanced templates extend several of the original templates by also detecting named entities (such as full names and physical addresses). Just look for the templates labeled 'Enhanced' to start protecting even more personal data.

Search for specific templates

All countries or regions

Categories

- Enhanced
- Financial
- Medical and health
- Privacy
- Custom

- Template or custom policy
- Name
- Admin units
- Locations
- Policy settings
- Policy mode
- Finish

Start with a template or create a custom policy

Choose an industry regulation to see the DLP policy templates you can use to protect that info or create a custom policy start from scratch. If you need to protect labeled content, you'll be able to choose labels later. Learn more about DLP policy templates

Check out our new enhanced policy templates. These enhanced templates extend several of the original templates by also detecting named entities (such as full names and physical addresses). Just look for the templates labeled 'Enhanced' to start protecting even more personal data.

Search for specific templates

All countries or regions

Categories

- Enhanced
- Financial
- Medical and health
- Privacy
- Custom

Templates

Custom policy

Custom policy

Create a custom policy from scratch. You will choose the type of content to protect and how you want to protect it.

- Template or custom policy
- **Name**
- Admin units
- Locations
- Policy settings
- Policy mode
- Finish

Name your DLP policy

Create a DLP policy to detect sensitive data across locations and apply protection actions when the conditions match.

Name *

Block norwegian id

Description

Create a custom policy from scratch. You will choose the type of content to protect and how you want to protect it.

- Template or custom policy
- Name
- **Admin units**
- Locations
- Policy settings
- Policy mode
- Finish

Assign admin units

Choose the admin units you'd like to assign this policy to. Admin units are created in Azure Active Directory and restrict the policy to a specific set of users or groups. Your selections will affect the location options available to you in the next step.

If you want to assign this policy to all users and groups, select 'Next' and proceed. Learn more about admin units

+ Add or remove admin units

Admin units

Full directory

- Template or custom policy
- Name
- Admin units
- **Locations**
- Policy settings
- Policy mode
- Finish

Choose locations to apply the policy

We'll apply the policy to data that's stored in the locations you choose.

If your role group permissions are restricted to a specific set of users or groups, you'll only be able to apply this policy to those users or groups. Learn more about role group permissions.

View role groups

Protecting sensitive info in on-premises repositories (SharePoint sites and file shares) is now in preview. Note that there are prerequisite steps needed to support this new capability. Learn more about the prerequisites

	Location	Scope	
☑	Exchange email	All groups	Edit
☑	SharePoint sites	All sites	Edit
☑	OneDrive accounts	All users & groups	Edit
☑	Teams chat and channel messages	All users & groups	Edit
☑	Devices	All users & groups	Edit
☑	Microsoft Defender for Cloud Apps	All instances	Edit
☑	On-premises repositories	All repositories	Edit
☐	Power BI workspaces	Turn on location to scope	

- Template or custom policy
- Name
- Admin units
- Locations
- **Policy settings**
- Policy mode
- Finish

Define policy settings

Decide if you want to use the default settings from the template you selected to quickly set up a policy or configure custom rules to refine your policy further.

- ○ Review and customize default settings from the template.
- ◉ Create or customize advanced DLP rules

- Template or custom policy
- Name
- Admin units
- Locations
- **Policy settings**
- **Advanced DLP rules**
- Policy mode
- Finish

Customize advanced DLP rules

The rules here are made up of conditions and actions that define the protection requirements for this policy. You can edit existing rules or create new ones.

+ Create rule

0 items

Name	Status

No rules created

Customize advanced DLP rules

The rules here are made up of conditions and actions that define the protection requirements for this policy. You can edit existing rules or create new ones.

+ Create rule

0 items

Name	Status

No rules created

Create rule

Use rules to define the type of sensitive information you data protect. If content matches many rules, the most restrictive one will be enforced. Learn more about rules.

Name *

Block norwegian id

Description

Conditions

We'll apply this policy to content that matches these conditions.

+ Add condition

Exceptions

We won't apply this rule to content that matches any of these exceptions.

+ Add exception

Actions

Use actions to protect content when the conditions are met.

+ Add an action

User notifications

Use notifications to inform your users and help educate them on the proper use of sensitive info.

Off

Notifications won't be used for activity in Exchange, SharePoint, OneDrive, Teams, and On Premises Scanner.

User overrides

Allow overrides from M365 services

Allow overrides from M365 services. Allows users in Power BI, Exchange, SharePoint, OneDrive, and Teams to override policy restrictions.

Incident reports

Use this severity level in admin alerts and reports: Select an option

Send an alert to admins when a rule match occurs.

Save Cancel

Name

Block norwegian id

Description

Conditions

We'll apply this policy to content that matches these conditions.

+ Add condition

Content contains

Exceptions

We won't apply this rule to content that matches any of these exceptions.

+ Add exception

Actions

Use actions to protect content when the conditions are met.

+ Add an action

User notifications

Use notifications to inform your users and help educate them on the proper use of sensitive info.

Off

Notifications won't be used for activity in Exchange, SharePoint, OneDrive, Teams, and On Premises Scanner.

User overrides

Allow overrides from M365 services

Allow overrides from M365 services. Allows users in Power BI, Exchange, SharePoint, OneDrive, and Teams to override policy restrictions.

Incident reports

Create rule

Use rules to define the type of sensitive information you data protect. If content matches many rules, the most restrictive one will be enforced. Learn more about rules.

Name *

Block norwegian id

Description

Conditions

We'll apply this policy to content that matches these conditions.

Content contains

Group name *

Default

Group operator

Any of these

Add

Sensitive info types

Add condition

Exceptions

We won't apply this rule to content that matches any of these exceptions.

Add exception

Actions

Use actions to protect content when the conditions are met.

Add an action

Sensitive info types

Search for Sensitive info types

315 items

Name	Publisher
ABA Routing Number	Microsoft Corporation
All Credential Types	Microsoft Corporation
All Full Names	Microsoft Corporation
All Medical Terms And Conditions	Microsoft Corporation
All Physical Addresses	Microsoft Corporation
Amazon S3 Client Secret Access Key	Microsoft Corporation
Argentina National Identity (DNI) Numb...	Microsoft Corporation
Argentina Unique Tax Identification Key...	Microsoft Corporation

Sensitive info types

Norway

3 items

Name	Publisher
Norway Identity Number	Microsoft Corporation
Norway Identity Number copy	Contoso
Norway Physical Addresses	Microsoft Corporation

Create rule

Use rules to define the type of sensitive information you data protect. If content matches many rules, the most restrictive one will be enforced. Learn more about rules.

Name *

Block norwegian id

Description

Conditions

We'll apply this policy to content that matches these conditions.

Content contains

Group name *

Default

Group operator

Any of these

Sensitive info types

Norway Identity Number	High confidence		Instance count	1 to Any	

Add

Add condition

Exceptions

We won't apply this rule to content that matches any of these exceptions.

Add exception

Actions

Use actions to protect content when the conditions are met.

Add an action

Create rule

Default

Any of these

Sensitive info types

Norway Identity Number | High confidence | Instance count 1 to Any

Add

Add condition

Exceptions

We won't apply this rule to content that matches any of these exceptions.

Add exception

Actions

Use actions to protect content when the conditions are met.

Add an action

- Restrict access or encrypt the content in Microsoft 365 locations
- Audit or restricted activities when users access sensitive sites in Microsoft Edge browser on Windows devices
- Audit or restrict activities on devices
- Restrict Third Party Apps
- Restrict access or remove on-premises files

User overrides

Allow overrides from M365 services

Allow overrides from M365 services. Allows users in Power BI, Exchange, SharePoint, OneDrive, and Teams to override policy restrictions.

Create rule

Default

Any of these

Sensitive info types

Norway Identity Number | High confidence | Instance count 1 to Any

Add

Add condition

Exceptions

We won't apply this rule to content that matches any of these exceptions.

Add exception

Actions

Use actions to protect content when the conditions are met.

Restrict access or encrypt the content in Microsoft 365 locations

- (•) Block users from receiving email or accessing shared SharePoint, OneDrive, and Teams files.

  By default, users are blocked from sending Teams chats and channel messages that contain the type of content you're protecting. But you can choose who is blocked from receiving emails or accessing files shared from SharePoint, OneDrive, and Teams.

  - (•) Block everyone.
  - ( ) Block only people outside your organization.

Add an action

User notifications

Use notifications to inform your users and help educate them on the proper use of sensitive info.

Off

Notifications won't be used for activity in Exchange, SharePoint, OneDrive, Teams, and On Premises Scanner.

Create rule

User notifications

Use notifications to inform your users and help educate them on the proper use of sensitive info.

Off

Notifications won't be used for activity in Exchange, SharePoint, OneDrive, Teams, and On Premises Scanner.

User overrides

Allow overrides from M365 services

Allow overrides from M365 services. Allows users in Power BI, Exchange, SharePoint, OneDrive, and Teams to override policy restrictions.

Incident reports

Use this severity level in admin alerts and reports: High

Send an alert to admins when a rule match occurs.

On

Send email alerts to these people (optional)

Add or remove groups

Collect original file as evidence for all selected file activities on Endpoint Add storage

Send alert every time an activity matches the rule

Send alert when the volume of matched activities reaches a threshold

Instances more than or equal to 15 matched activities

Volume more than or equal to 0 MB

During the last 60 minutes

For All users

Use email incident reports to notify you when a policy match occurs.

Off

Additional options

If there's a match for this rule, stop processing additional DLP policies and rules.

Set the order in which this rule will be selected for evaluation

Priority: 0

Save Cancel

- Template or custom policy
- Name
- Admin units
- Locations
- **Policy settings**
  - **Advanced DLP rules**
- Policy mode
- Finish

Customize advanced DLP rules

The rules here are made up of conditions and actions that define the protection requirements for this policy. You can edit existing rules or create new ones.

+ Create rule

1 item

Name	Status
Block norwegian id	On

Conditions
Content contains any of these sensitive info types:
Norway Identity Number

Actions
Restrict access to the content
Send alerts to Administrator

- Template or custom policy
- Name
- Admin units
- Locations
- Policy settings
- **Policy mode**
- Finish

Policy mode

Decide whether you want to turn the policy on right away or test it out first.

- (●) **Test it out first**
  You'll be able to review alerts to assess the policy's impact. Any restrictions you configured won't be enforced. Learn more about test mode
  - [x] Show policy tips while in test mode
- ( ) **Turn it on right away**
  After the policy is created, it'll take up to an hour for it to take effect.
- ( ) **Keep it off**
  You'll be able to test it out or turn it on later.

- Template or custom policy
- Name
- Admin units
- Locations
- Policy settings
- Policy mode
- **Finish**

Review your policy and create it

Review all settings for your new DLP policy and create it.

The information to protect

Custom policy

Edit

Name

Block norwegian id

Edit

Description

Create a custom policy from scratch. You will choose the type of content to protect and how you want to protect it.

Edit

Locations

Exchange email
SharePoint sites
OneDrive accounts
Teams chat and channel messages
Devices
Microsoft Defender for Cloud Apps
On-premises repositories

Edit

Policy settings

Block norwegian id

Edit

Turn policy on after it's created?

Yes

Edit

What have we done?

- Just enough access
- Created Access Package
- Created Sensitivity label
- Created DLP Policy

Key takeaways

- Have control of your data
- Use Data loss prevention!
- Mark your sensitive data
- Keep an healty security posture