SharePoint Advanced Management

More control, more security, more efficiency

Adrian

Business
-   Microsoft technology for 18 years
-   Focus on collab topics (Teams / SharePoint)
-   Cloud Architect at glueckkanja AG, Offenbach

Community
-   Co-Host Teams User Group Deutschland location Bochum
-   Co-Host Global AI Chapter Bochum
-   Microsoft MVP
-   Cloudkumpel Cast
-   Cloudkumpel Blog
-   Podcast "AI und Du – Copilot in Microsoft 365"
-   Speaker at various conferences/MeetUps

Adrian Ritter
Cloud Architect
glueckkanja AG
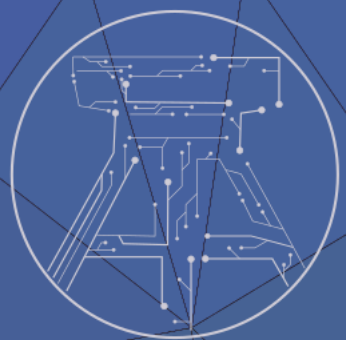
Agenda

Overview / Licensing

Content Sprawl

Lifecycle

Permission and Access

SharePoint Advanced Management

Advanced management

Manage and govern SharePoint and OneDrive with advanced tools and enhanced Microsoft 365 secure collaboration abilities.

Learn more about SharePoint Advanced Management

What's included

Feature ↑	Location	Purpose
Block download policy for SharePoint and OneDrive	Microsoft PowerShell	Prevent download for both external and internal users
Change history	Reports > Change history	Find who made particular site or organization setting changes and when
Conditional access policies for SharePoint and OneDrive	Microsoft Entra conditional access	Control whether users can access sensitive sites based on conditions like location or operating system
Data access governance reports	Reports > Data access governanace	Discover potential oversharing and keep track of sites that have sensitive files
Default sensitivity labels for document libraries	Library settings and Create document library panel	Help make sure sensitive project files are appropriately labeled
OneDrive access restriction	Policies > Access control > OneDrive access restriction	Allow only particular groups of users to use OneDrive
Recent actions	Active sites > Recent actions	Review recent site changes you made
Site lifecycle management	Policies > Site lifecycle management	Automate tasks across the life cycle of your sites
Site-level access restriction	Policies > Access control > Site-level access restriction	Allow admins to restrict access to specific SharePoint sites and their content

SharePoint Advanced Management

✓ Your SharePoint Advanced Management subscription is enabled.

Per-User License
3$ per user / month
Features are currently available with the first licensed user
Since end of May part of the Microsoft 365 Copilot license

Requires a Microsoft 365 / Office 365 license (SharePoint Plan)

Functional

| Content Sprawl	Lifecycle	Permission & Access
Site Owner Policy ✧ Inactive Site Policy Site Attestation Policy	Data Governance Reports ✧ Change History Report Last Admin Actions ✧ Sensitivity Label Report	⌦ Block Download ⌦ Restrict Site Access ⌦ Restrict Site Creation ⌦ Restrict Content Discovery ⌦ Restrict OneDrive Access (one / all) App Insights

✧ AI generated Insights available ⌦ Only available via PowerShell

Content Sprawl
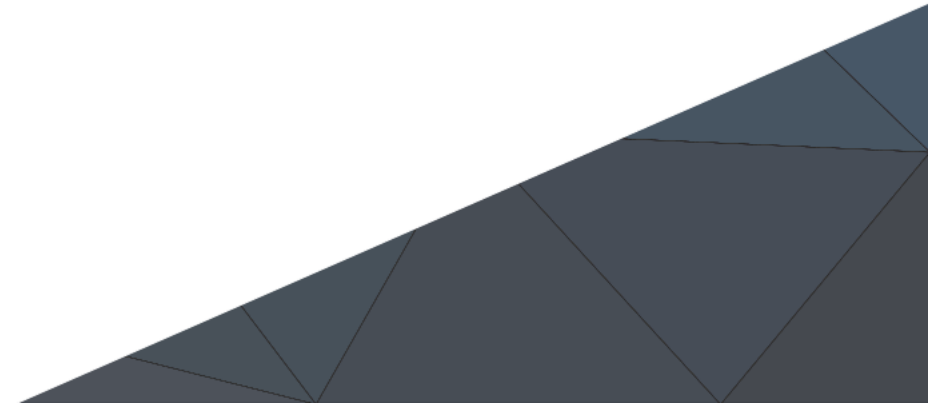
Content Sprawl

Content is available / spreads even though it is outdated and no one is responsible for the permissions.

PREVIEW

Inactive Site Policy

SharePoint Site Collections with no user activity are detected. Owners will be contacted and must confirm that the site collection is still needed.
- Read-Only
- Archive

Owner Policy

If the predefined number of owners is not reached, the remaining owner will be asked to designate another owner.
- Escalation paths available
- Set Read-Only

Site attestation policy

Require the site owners to review site contents, users with access and overall necessity of the site on a regular basis.
- Escalation paths available
- Set Read-Only
- Archive

Inactive Site Policy – Create

Inactive site policy `PRO`

Create and manage your active and simulation policies. Up to 5 policies can be created at one time.
Learn how inactive site policies work

+ Create policy   ○ Refresh

Policy name	Mode	Enforcement type	Last run ↓	Inactive sites	Report
Teams Connected Sites	● Active	Read-only	○ Running (this might take a few days)	-	-

↓ Download

Create an inactive site policy

● Overview
● Scope
○ Configuration
○ Finish

Set policy scope

How long after the last activity should a site be considered inactive?

Includes activity on the site, files, and any connected resources like Microsoft Teams, Viva Engage, or Exchange.

[3 months ▼]

Which sites should be checked for inactivity? *

OneDrive sites are excluded automatically.

[Select site templates ▼]

☐ Filter by sensitivity label
☐ Filter by site creation source
☐ Include sites with retention policies and retention holds

Exclude sites

☐ Exclude specific sites from this policy

Simulation possible
Runs automatically monthly
Sites under "Retention" can be included

Scope based on:
- Period
- Site Template
- Sensitivity Label
- Way of creation
- Explicit exclusion (max. 100)

Action (after 3 notifications):
- Read-Only
- Read-Only Phase, MS Archive

Inactive Site Policy – Results

Teams Connected Sites

⊘ Activate   ✦ Get AI insights   🗑 Delete

ⓘ This policy is in simulation mode, which creates a report of inactive sites and doesn't notify site owners. You can activate the policy later.

Reports   Scope   Configuration   General

Simulation report date: March 17, 2025

Inactive sites found
12

Download report

Next step

Happy with the policy's trial run? **Activate the policy to run it automatically every month and notify site owners.**

Activate policy

Simulation Report

	A	B	C	D	E	F	G	H
1	Site name	URL	Template	Connected to Teams	Sensitivity label	Retention Policy	Site lock state	Last activity date (UTC)
2	PowerAdminCommunity	https://c4a	Team site	WAHR		Not applied	Unlock	05/27/2024
3	CitizenDeveloper	https://c4a	Team site	WAHR		Not applied	Unlock	09/21/2023
4	[EXT] Test Team	https://c4a	Team site	WAHR		Not applied	Unlock	09/05/2022
5	Project Management	https://c4a	Team site	WAHR		Not applied	Unlock	04/04/2024
6	On-Call Duty	https://c4a	Team site	WAHR		Not applied	Unlock	09/19/2023
7	Test Team	https://c4a	Team site	WAHR		Not applied	Unlock	11/15/2024
8	CrisisCommunicationTeam	https://c4a	Team site	WAHR		Not applied	Unlock	09/19/2023
9	Admin Created Team	https://c4a	Team site	WAHR		Not applied	Unlock	09/19/2023
10	Confidential Team	https://c4a	Team site	WAHR	Confidential Label	Not applied	Unlock	09/19/2023
11	Austauch Vertrieb / IT	https://c4a	Team site	WAHR		Not applied	Unlock	06/10/2024
12	c4a8alzoc Org-Wide	https://c4a	Team site	WAHR		Not applied	Unlock	06/12/2024
13	PRJ - Zeiterfassung	https://c4a	Team site	WAHR	Confidential GST	Not applied	Unlock	06/11/2024

Owner Email Notification

■ Microsoft 365

'PRJ - Zeiterfassung' has been inactive for more than a month

PRJ - Zeiterfassung
Connected to Teams

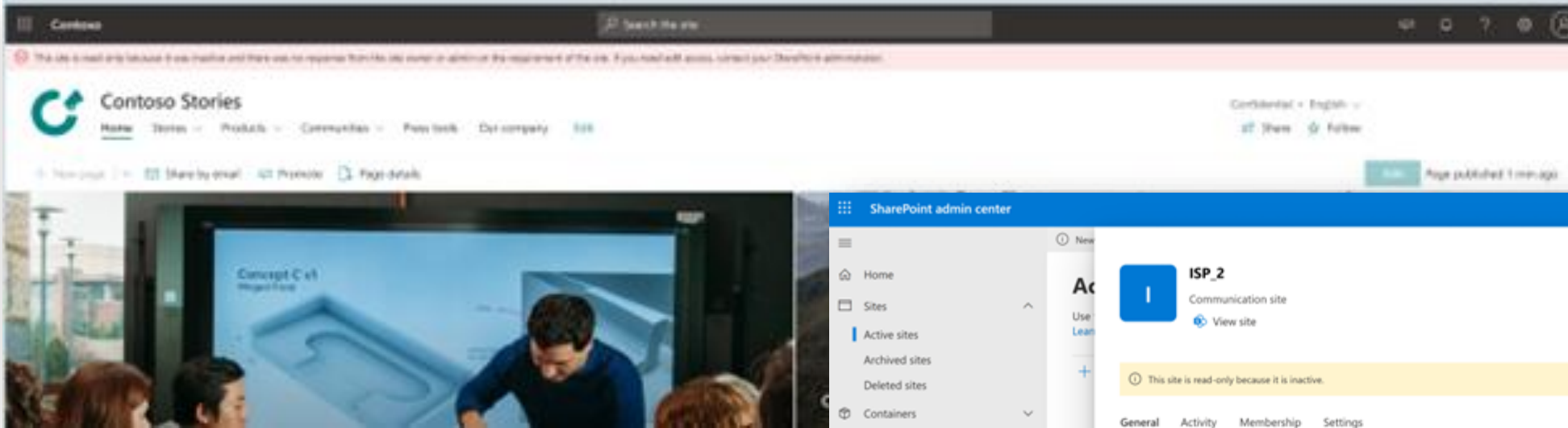⊘ The action completed successfully.   ✕

Select **Certify site** to confirm if it's still in use, or consider deleting it if the site is no longer needed.
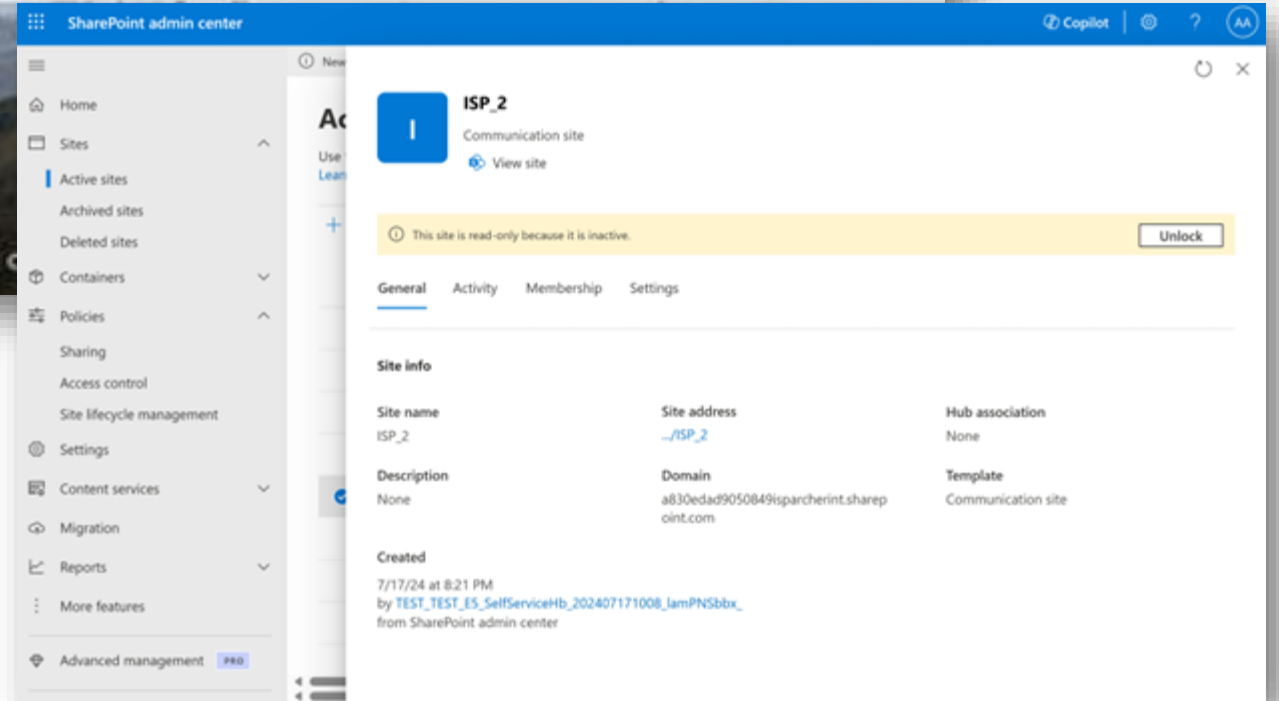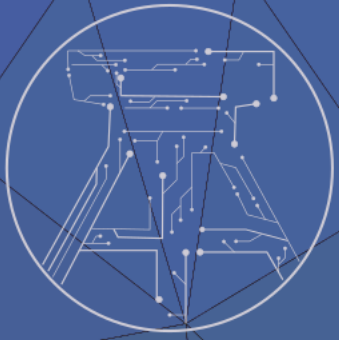
Certify site   Learn how to delete a site

Inactive Site Policy – Results

When a Site is set to read-only mode a banner is added to the site.

A site can be removed from read-only mode only by a SharePoint Admin.

Live Demo

Owner Policy – Create

Create a site ownership policy

- ✓ Overview
- ● **Scope**
- ○ Configuration
- ○ Finish

Set policy scope

Which site templates do you want to check the ownership status for? *

[Select site templates ▼]

☐ Filter by sensitivity label

☐ Filter by site creation source

☐ Include sites with retention policies and retention holds

Exclude sites

☐ Exclude specific sites from this policy

Who should be notified (via email) to assign or claim site responsibility? *

If a site has less than minimum owners or admins, chosen recipients will be notified. It is recommended to ensure at least 3 options are selected to increase likelihood of finding an owner.

☑ Current site owners, if any

☐ Current site admins, if any

☐ Manager of previous site owner or admin ⓘ

☐ Active site members ⓘ

A minimum of 1 or 2 (recommended) owners can be defined.

Owners and/or site administrators can be responsible.

Scope based on:
- Period
- Site Template
- Sensitivity Label
- Way of creation
- Explicit exclusion (max. 100)

Owner Policy – Results

2 Owner Minimum

⊖ Simulation

✓ Activate   🗑 Delete

> ⓘ This policy is in simulation mode which only creates a report of sites. Email notifications and actions on ownerless sites will take effect after the policy is activated.

Report   Scope   Configuration   General

Report date: March 17, 2025

Ownership compliance criteria: 2 site owners

Non-compliant sites
8

For more information on ownerless sites, last activity date, storage used etc., refer to the report

Download detailed report

Next step

Activate the policy to run it monthly and notify site owners and admins, to take action.

Activate policy

Simulation Report

	A	B	C	D	E	F	G	
1	Site name		Template	Sensitivity label	Retention policy	Minimum owners or admins configured	Number of site owners	Email
2	CitizenDeveloper	https://c4a	Team site		Not applied	2	1	Cloud
3	[EXT] Test Team	https://c4a	Team site		Not applied	2	1	Cloud
4	On-Call Duty	https://c4a	Team site		Not applied	2	1	Cloud
5	Test Team	https://c4a	Team site		Not applied	2	1	Cloud
6	CrisisCommunicationTeam	https://c4a	Team site		Not applied	2	1	Cloud
7	Admin Created Team	https://c4a	Team site		Not applied	2	1	Cloud
8	Confidential Team	https://c4a	Team site	Confidential Label	Not applied	2	1	Cloud
9	PRJ - Zeiterfassung	https://c4a	Team site	Confidential GST	Not applied	2	1	Cloud

Attestation Policy – Create

Site owners or admins to check and confirm the accuracy of site information, including the site's necessity, its owners, members, permissions, and sharing settings.

Same scope options as for inactivity or owner policy.

Exclusion of users or groups

Known "action" options

Create a site attestation policy

Create a site attestation policy

- ✓ Overview
- ✓ Scope
- ● **Configuration**
- ○ Finish

Configure policy

How often do you need the sites in your organization to be attested? *

[6 months   ⌄]

Who is responsible for attesting a site? *

☑ Site owners
☐ Site admins

Exclude site owners or admins from receiving attestation requests ⓘ

   𝄜 Exclude users or groups

What action should the policy take on sites that are unattested after 3 monthly notifications? *

> ⓘ Enforcement actions cannot be edited after policy creation

○ Do nothing

◉ Take an enforcement
   Users will be able to access the site content depending on the selected action.

   Select an enforcement type:
   ◉ Read-only access
      Users can view site content, but can't edit it.

   ○ Archive sites after mandatory read-only period `RECOMMENDED`

Attestation Policy – Results

Site attestation policy PREVIEW

Create policies to periodically notify site owners or admins to attest their sites and take actions on unattested sites.
Learn more about site attestation

+ Create policy   ⟳ Refresh

ⓘ This policy is in simulation mode, which creates a report of sites and doesn't send notifications.

Policy name	Mode	Enforcement type	Last run ↓	Sites	Report
Site Attestation Policy	⊖ Simulation	Read-only	6/23/25	0	↓ Download

Content Lifecycle

Lifecycle – Setting Change History

Change history PRO

Create and download custom CSV reports of site actions or organization setting changes within the last 180 days. When you create a report, it might take a few hours for it to run.
Learn more about these reports

+ New report   ◌ Refresh status

Report name	Report type	Report status	Total changes
2024-12 Org Setting Report	Organization settings	✔ Completed	0
Change History	Site settings	✔ Completed	434

At the site or organization level
Limited to the last 180 days
AI Insights for Site Settings

AI insights
Change History

- **Site deletions by Cloud Admin**: Multiple instances of site deletions by the user "Cloud Admin" on 11/23/2023. For example, the sites "TMG-BeiratEinkaufTechnik" and "TMG-ANL" were deleted. This could lead to accidental data loss. Consider reviewing the necessity of these deletions and implementing a review process for site deletions to prevent data loss.

- **Frequent changes to group ownership and membership by cloud▮▮▮▮▮▮▮▮**: Numerous changes to group ownership and membership by the user "clouda▮▮▮▮▮▮▮t" on 11/23/2023. For example, ownership of "Austauch Vertrieb / IT" was changed multiple times. This could lead to confusion and potential security risks. Consider auditing these changes and ensuring that group ownership and membership changes are necessary and documented.

- **IB mode changes to less strict settings**: Instances of IB mode changes from more strict to less strict settings. For example, the site "▮▮▮▮zocOrg-Wide" had its IB mode changed from "Implicit" to "Open" on 1/9/2024. This can lead to oversharing of sensitive content. Review these changes and consider reverting to more secure settings where appropriate to prevent unauthorized access.

⧉ Copy

AI-generated content may be incorrect   👍 👎

Lifecycle – Last Admin Actions

Your recent actions PRO

Review the most recent site changes you made from the SharePoint admin center in the last 30 days.
Learn more about recent actions

✓ **IB settings changed**
  .../sites/Contoso

7:09 AM
✓ **Site members changed**
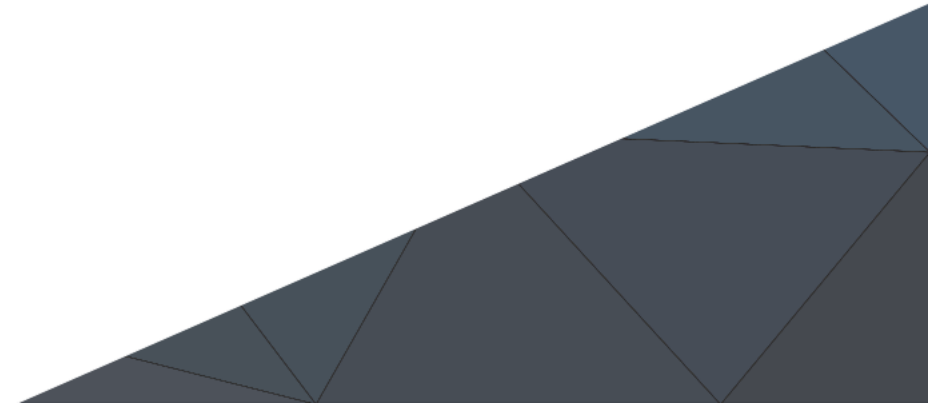 .../sites/Contoso

7:07 AM
✓ **Site created**
  .../sites/Contoso

1:48 AM
✓ **Site admins changed**
  .../sites/1111Comm1111

Permission & Access

Lifecycle – Data Governance

E5 License

SAM License

Welcome to data access governance

These new reports help you maintain the security and compliance of your data in SharePoint.

Next

Sharing links

Identify potential oversharing by monitoring sites where users created new sharing links in SharePoint.

View reports

Sensitivity labels applied to files

Monitor sensitive content by reviewing the sites where sensitive files are stored and the policies applied to these sites.

View reports

Data access governance

Reports   My review requests

These reports help you maintain the security and compliance of your data in SharePoint.

Learn more about data access governance

Sharing links

Identify potential oversharing by monitoring sites where sharing links in SharePoint.

View reports

Sensitivity labels applied to files

Monitor sensitive content by reviewing the sites where s stored and the policies applied to these sites.

View reports

Content shared with 'Everyone except external users'

Discover potential oversharing by reviewing content shared with 'Everyone except external users'. Send site owners requests to review access permissions of their content based on the report.

View reports

Data access governance > Content shared with 'Everyone except external users'

Content shared with 'Everyone except external users'

Use these reports to view sites where 'Everyone except external users' was added as a site member, or view sites with specific content, like files, folders, and lists, shared with 'Everyone except external users'. Reports include data from the last 28 days. To get the latest data, run the report, which may take a few hours.

Learn more about these reports

+ Create report   ▷ Run all   ↻ Refresh status

	Report name	Status	Report type ⓘ
☐	2025-01 EEEU Site Me...	Updated 2 months ago	Site with org-wide membership

Block Download (SharePoint / OneDrive)

Set-SPOSite -Identity <SiteURL> -BlockDownloadPolicy $true

Additional parameters:

Site owners are allowed to download
-ExcludeBlockDownloadPolicySiteOwners $true

Members of the configured groups are allowed to download
-ExcludedBlockDownloadGroupIds <comma separated group IDs>

Members of the configured SharePoint groups are allowed to download
-ExcludeBlockDownloadSharePointGroups <comma separated group names>

Site is additionally read-only
-ReadOnlyForBlockDownloadPolicy $true
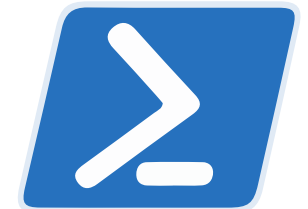
App insights report

Number of non-Microsoft apps found

4

Filters: App name: **All**   Site Permissions: **All**   Site Sensitivity: **All**

Site name	URL	Sensitivity	App ID	App name	App permissions	Requests volume ↓
Contoso Giving	../sites/contosogiv	General	Test AppID1	Test App1	Files.Read, Files.Read.All...	1,970
Contoso HR	.../teams/contosohr	Highly confidential	Test AppID2	Test App2	Sites, Write all	807
Contoso Secure	../sites/contososecu	Top secret	Test AppID3	Test App3	Sites, Read all	500
Contoso IT	../sites/contosoit	Highly confidential	Test AppID4	Test App4	Sites, Write all	340

Report contains:
- Site accessed
- Site sensitivity
- App name
- App permission
- Data volume

App Actions recognized:
- FileAccessed
- FileDownloaded
- FileModified
- FileUploaded

Access Review

Based on the Sharing Link / EEEU Report

OneDrive Access Restriction (All)

Activate/Configure:

OneDrive access restriction ×

Use this setting to allow only users in specific security groups to access OneDrive content. You can add up to 10 security groups. Users not in these security groups will lose access to all OneDrive content.

Learn more about restricting access to OneDrive

☑ Restrict OneDrive access to only users in specified security groups

Add security groups

[Search security groups]

Name (1) ↑

G Germany-Sec ✕

Only members of the configured security groups have OneDrive access.

Max. 10 Group

All other users will lose their OneDrive access

Access Denied

Your organization's policies prevent you from seeing the content on this site.

Here are a few ideas:

⊙ Please contact your organization. Know more about your organization's policies here.

Set-SPOTenant –RestrictedAccessControlForOneDriveErrorHelpLink "<Learn more URL>"

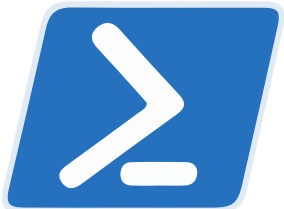# OneDrive Access Restriction (Specific)

Activate:

Set-SPOSite –Identity <siteurl> –RestrictedAccessControl $true

Set-SPOSite –Identity <siteurl> –AddRestrictedAccessControlGroups <comma separated group GUIDS>

Set-SPOSite –Identity <siteurl> –RestrictedAccessControlGroups <comma separated group GUIDS>

Set-SPOSite –Identity <siteurl> –ClearRestrictedAccessControl

⊗ Can't share with one or more people or groups due to your organization's site access restriction policy.

- OneDrive-level control (site)
- Owner of the OneDrive must also be taken into account!
- Maximum 10 groups
- Only group members have access
- All previously granted permissions/links will no longer work.

Site Level Access Restrictions

Activate:

Site-level access restriction

This setting lets you and other Global or SharePoint Administrators restrict access to sites. For sites connected to a group or team, you can restrict access to only the group or team owners and members. For communication sites, you can restrict access to only the groups you specify.

Learn more about Restricted Access Control for SharePoint sites
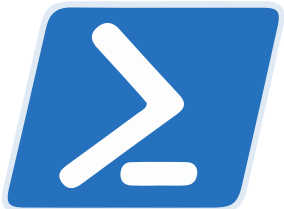
☑ Allow access restriction

Only members of the configured M365 group/security groups have access to the site.

Individually authorized files can still appear in the search, but access is then not possible.

Set-SPOTenant -EnableRestrictedAccessControl $true

Configure (Group Connected):

Set-SPOSite –Identity <siteurl> –RestrictedAccessControl $true

Not Group Conected (Admin Center)

Restricted site access

Use this setting to allow only users in specific groups to access this Sha add up to 10 security groups or Microsoft 365 groups. Users not in the access to this SharePoint site.

Learn more about Restricted Access Control for SharePoint sites

☑ Restrict SharePoint site access to only users in specified groups

Add group

Search groups

Restrict Discovery

Exclusion of certain (sensitive) sites from search (Copilot)

Activate:

Set-SPOSite -identity <site-url> -RestrictContentOrgWideSearch $true

- Not applicable to OneDrive Sites
- Not applied to search in the site context
- Recent still works

⊗ **Caution**

Overuse of Restricted Content Discovery can negatively affect performance across search, SharePoint, and Copilot. Removing sites or files from tenant-wide discovery means that there's less content for search and Copilot to ground on, leading to inaccurate or incomplete results.

Restrict SharePoint Site Creation

Two options:
Certain people are not allowed to create sites (deny mode)
Certain people are allowed to create sites (Allow mode)

Policy controls site type:
All
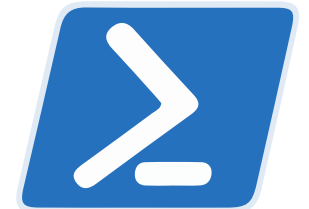SharePoint (nicht OneDrive)
OneDrive
Team
Communication

Activate:

Set-SPORestrictedSiteCreation -Enabled $true
Set-SPORestrictedSiteCreation -Mode Allow
Set-SPORestrictedSiteCreation -SiteType SharePoint -RestrictedSiteCreationGroups <Gruppen ID>

- Max 10 security groups per site type
- Only Entra ID Security Groups

Insights report on SharePoint agents

Create a report

ℹ This report will have the data from May 27, 2025 to June 24, 2025.

Use reports to view and download SharePoint agents across SharePoint sites and OneDrive accounts.

Report name *

Add a name for your report

Report duration *

Select an option ⌄

Last 1 day

Last 7 days

Last 14 days

Last 28 days

Report will contain data from up to last 28 days

| Agents in SharePoint sites	Agents in OneDrive accounts
127	**23**

╋ Initiate site access review ✎ Restrict site access ⧉ Restrict content discovery

Filters: Site template: **All**   Restrict site access enabled **All**   Restrict site discovery enabled **All**

☐	Site name	URL	Template	Site owner	Agents created ↓
☐	Advanced Product Division	../sites/AdvancedProductDivision	Teams connected site	Mona Kane	23
☐	Contoso Finance	.../teams/contosofin	Teams connected site	Brenda Thomas	21
☐	Contoso Secure	../sites/contososecu	Communication site	Jack Becker	18
☐	Chris Smith	../personal/chriss	OneDrive site	Chris Smith	18
☐	Green Energy	../sites/GreenEnergy	Group connected site	Emily Baker	16
☐	Contoso HR	../sites/contosoHR	Group connected site	Mona Kane	12
☐	Contoso Leaders	../sites/contosole	Group connected site	Shikha Verma	11
☐	Contoso Design	../sites/contosodes	Group connected site	Jesse Wallin	9
☐	Contoso in house	../sites/contosoin	Teams connected site	Emily Baker	6
☐	Contoso BI	../sites/contosobi	Communication site	Brenda Thomas	7
☐	Jack Becker	../personal/jackb	OneDrive site	Jack Becker	5
☐	Contoso Give	../sites/contosogiv	Group connected site	Emily Baker	4
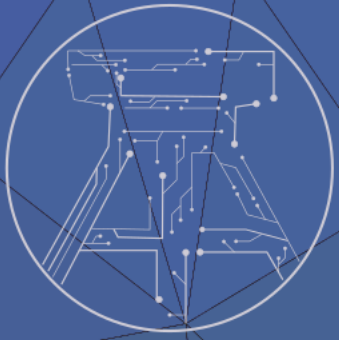
Thank you for your attention!

Questions??