

SharePoint Advanced Management

Mehr Kontrolle, mehr Sicherheit,
mehr Effizienz



Adrian



Adrian Ritter
Cloud Architect
glueckkanja AG

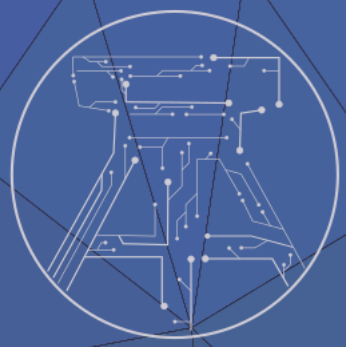
Business

- Microsoft Technologie seit 18 Jahren
- Fokussierung auf Collab Themen (Teams / SharePoint)
- Cloud Architect bei glueckkanja AG, Offenbach

Community

- Co-Host der Teams User Group Deutschland
- Co-Host Global AI Chapter Bochum
- MVP seit Mai 2024
 - o Cloudkumpel Cast
 - o Cloudkumpel Blog
 - o Podcast "AI und Du – Copilot in Microsoft 365"
- Speaker bei verschiedenen Konferenzen/MeetUps





Agenda

Übersicht / Lizenzierung

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 governance	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.

Pro-Benutzer Lizenz

3\$ Pro Benutzer / Monat

Features sind aktuell mit dem ersten Lizenzierten Benutzer Verfügbar

Wird Teil der Microsoft 365 Copilot Lizenz

Setzt eine Microsoft 365 / Office 365 Lizenz (SharePoint Plan) Voraus





Funktionsbereiche

Content Sprawl

Site Owner Policy
❖ Inactive Site Policy

Lifecycle

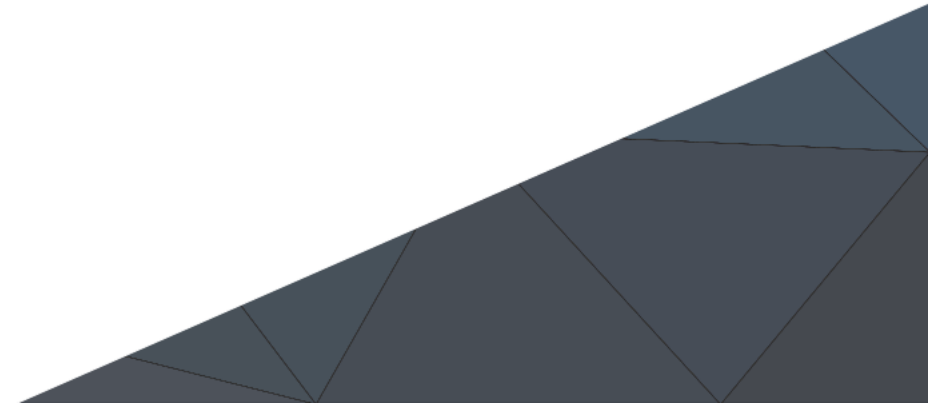
Daten Governance Reports
❖ Change History Report
Last Admin Actions
❖ Sensitivity Label Report

Permission & Access

➤ Block Download
➤ Restrict Site Access
➤ Restrict Site Creation
➤ Restrict Content Discovery
➤ Restrict OneDrive Access
(one / all)
App Insights (Preview)



Content Sprawl





Content Sprawl

Inhalte sind verfügbar / verbreiten sich, obwohl sie veraltet sind und keiner die Berechtigungen verantwortet.

Inactive Site Policy

SharePoint Site Collections ohne Nutzeraktivität werden erkannt. Owner werden kontaktiert und müssen bestätigen, dass die Site Collection noch benötigt wird.

- Read-Only
- Archive

Owner Policy

Wird die vordefinierte Besitzer-Anzahl unterschritten, wird der verbleibende Besitzer aufgefordert, einen weiteren Besitzer zu bestimmen.

- Eskalationspfade verfügbar



Inactive Site Policy – Erstellen

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 möglich
Wird automatisch monatlich ausgeführt
Sites unter „Retention“ können einbezogen werden

Scope basierend auf:

- Zeitraum
- Site Template
- Sensitivity Label
- Weg der Erstellung
- Expliziter Ausschluss (max. 100)

Aktion (nach 3 Benachrichtigungen):

- Read-Only
- Read-Only Phase, MS Archive



Inactive Site Policy – Ergebnisse

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	Austausch 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

Besitzer E-Mail-Benachrichtigung

Microsoft 365

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

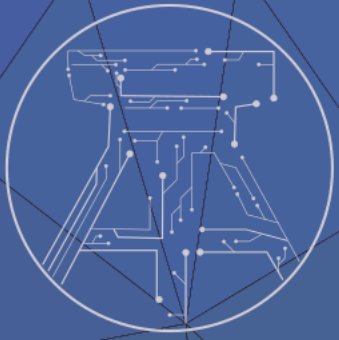
PRJ - Zeiterfassung
Connected to Teams

✓ 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



Live Demo



Owner Policy – Erstellen

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 ⓘ

Spezielle Sites sind ausgenommen z.B.:
OneDrive, App Catalog, Erstellt durch System Account...

Durch Inaktivität schreibgeschützte Sites sind ausgenommen.

Verantwortlich können Besitzer und / oder Site Administratoren sein.

Scope basierend auf:

- Zeitraum
- Site Template
- Sensitivity Label
- Weg der Erstellung
- Expliziter Ausschluss (max. 100)



Owner Policy – Ergebnisse

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.

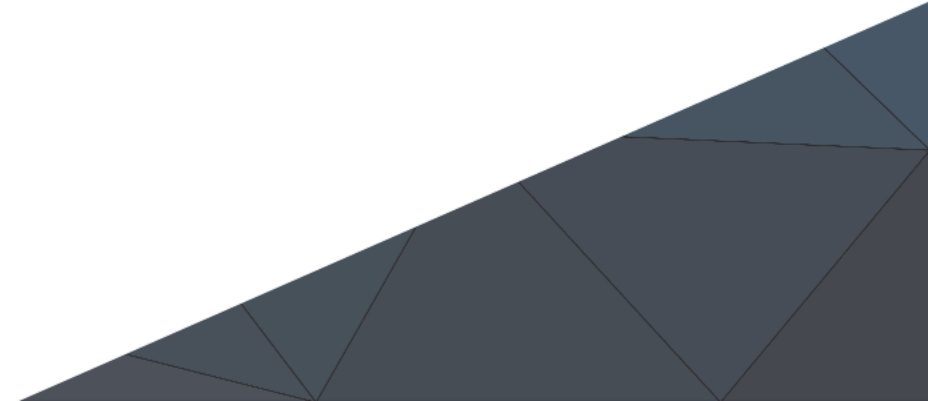
Activate policy

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://c4e Team site		Not applied	2	1	Cloud	
3	[EXT] Test Team	https://c4e Team site		Not applied	2	1	Cloud	
4	On-Call Duty	https://c4e Team site		Not applied	2	1	Cloud	
5	Test Team	https://c4e Team site		Not applied	2	1	Cloud	
6	CrisisCommunication Team	https://c4e Team site		Not applied	2	1	Cloud	
7	Admin Created Team	https://c4e Team site		Not applied	2	1	Cloud	
8	Confidential Team	https://c4e Team site	Confidential Label	Not applied	2	1	Cloud	
9	PRJ - Zeiterfassung	https://c4e Team site	Confidential GST	Not applied	2	1	Cloud	



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

Auf Site oder Organisations Ebene
Beschränkt auf die letzten 180 Tage
AI Insights für 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" on 11/23/2023. For example, ownership of "Austausch 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 Lizenz



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](#)

SAM Lizenz

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 sensitive content is 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](#)

<input type="checkbox"/>	Report name	Status	Report type ⓘ
<input type="checkbox"/>	2025-01 FEEU Site Me...	Updated 2 months ago	Site with org-wide membership





Block Download (SharePoint / OneDrive)

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

Zusätzliche Parameter:

Site Besitzer dürfen herunterladen

```
-ExcludeBlockDownloadPolicySiteOwners $true
```

Mitglieder der konfigurierten Gruppen dürfen herunterladen

```
-ExcludedBlockDownloadGroupIds <comma separated group IDs>
```

Mitglieder der konfigurierten SharePoint Gruppen dürfen herunterladen

```
-ExcludeBlockDownloadSharePointGroups <comma separated group names>
```

Site wird zusätzlich schreibgeschützt

```
-ReadOnlyForBlockDownloadPolicy $true
```





OneDrive Access Restriction (All)

Aktivieren / Konfigurieren:

The screenshot shows the 'OneDrive access restriction' settings window. At the top, it says 'OneDrive access restriction' with a close button. Below is a description: '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.' There is a link 'Learn more about restricting access to OneDrive'. A checkbox is checked with the label 'Restrict OneDrive access to only users in specified security groups'. Below this is a section 'Add security groups' with a search bar labeled 'Search security groups'. Underneath the search bar is a list of added groups, currently showing 'Germany-Sec' with a blue 'G' icon and a close button for that group.

Nur Mitglieder der konfigurierten Sicherheitsgruppen haben OneDrive Zugriff.

Max. 10 Gruppen

Alle anderen Benutzer verlieren ihren OneDrive Zugriff

The screenshot shows an 'Access Denied' message box. It says 'Access Denied' in large text, followed by 'Your organization's policies prevent you from seeing the content on this site.' Below this, it says 'Here are a few ideas:' followed by a link icon and the text 'Please contact your organization. Know more about your organization's policies here.'

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



OneDrive Access Restriction (Specific)

Aktivieren:

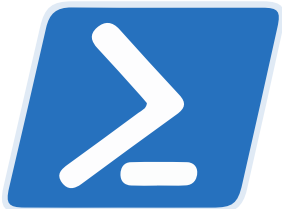
```
Set-SPOSite -Identity <siteurl> -RestrictedAccessControl $true
```

```
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.



- Kontrolle auf OneDrive Ebene (Site)
- Besitzer des OneDrive muss auch berücksichtigt werden!
- Maximal 10 Gruppen
- Nur Gruppenmitglieder haben Zugriff
- Alle vorher erteilten Berechtigungen / Links funktionieren nicht mehr.



Site Level Access Restrictions

Aktivieren:

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

Nur Mitglieder der konfigurierten M365 Gruppe / Sicherheitsgruppen haben Zugriff auf die Site.

Einzelne berechnete Dateien können in der Suche weiterhin auftauchen, Zugriff ist dann aber nicht möglich.

Set-SPOTenant -EnableRestrictedAccessControl \$true

Konfigurieren (Group Connected):

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



01.04.2025

www.cloudkumpel.de

Nicht Group Connected (Admin Center)

Restricted site access

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

Ausschluss bestimmter (Sensibler) Sites aus der Suche (Copilot)

Aktivieren:

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

- Nicht anwendbar auf OneDrive Sites
- Wird nicht auf die Suche im Site Kontext angewendet
- „Zuletzt verwendet“ funktioniert weiterhin

⊗ 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

Zwei Optionen:

Bestimmte Personen dürfen **keine** Sites erstellen (Deny Modus)

Bestimmte Personen dürfen Sites erstellen (Allow Modus)

- Max 10 Sicherheitsgruppen pro Site Typ
- Nur Entra ID Sicherheitsgruppen

Policy steuert Site Typ:

All

SharePoint (nicht OneDrive)

OneDrive

Team

Communication

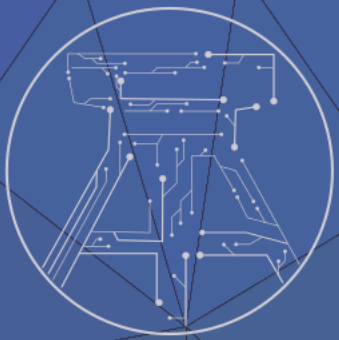
Aktivieren:

`Set-SPORestrictedSiteCreation -Enabled $true`

`Set-SPORestrictedSiteCreation -Mode Allow`

`Set-SPORestrictedSiteCreation -SiteType SharePoint -RestrictedSiteCreationGroups <Gruppen ID>`





Danke für eure
Aufmerksamkeit!

Fragen??