



MK Nepal Solutions

USER GUIDE

M365 Audit & Governance

Find oversharing, inactive and ownerless workspaces and orphaned Power Platform resources – and fix them, step by step.

Home

CONNECT

SharePoint

Tenants

AUDIT

Sharing

Teams & sites

Power Platform

Audits

Actions

License

v1.0.23

Teams, groups & sites > Teams, groups & sites – 2026-10-27

Teams, groups & sites – 2026-10-27

Completed · finished 10/27/2026, 7:30:23 AM

Run again

Edit and run again

Export CSV

5

All findings

2

High risk

2

Medium risk

0

Low risk

3

Inactive

1

No owner

1

Owners disabled

1

One owner

Findings

Changes

Audit log

All findings

0 selected

E-mail owners

Add owners

☐	Risk	Type	Name	Last activity	Owners	Flags
☐	High	Microsoft 365 group	Orphan Group orphangroup@contoso.com	2026-09-27 30 days ago	None	No owner
☐	High	Microsoft 365 group	Leaver Group leavergroup@contoso.com	2025-12-31 300 days ago	None Disabled: gone@contoso.com	Owners disabled Inactive
☐	Medium	Team	Old Project Team oldprojectteam@contoso.com	2025-09-22 400 days ago	ann@contoso.com	One owner Inactive
☐	Medium	SharePoint site	https://contoso.sharepoint.com/sites/archive https://contoso.sharepoint.com/sites/archive	2025-06-14 500 days ago	ben@contoso.com	Inactive
☐	Info	Team	Sales Team salesteam@contoso.com	2026-10-25 2 days ago	ann@contoso.com, ben@contoso.com	

5 of 5 shown

Contents

1 Introduction	2
The audits	2
Three promises	2
How to use this guide	2
2 Install and activate	3
System requirements	3
Install	3
Start the free trial	3
Activate with a serial number	3
Offline activation (no internet on this computer)	4
Renewal and moving to another computer	4
3 Connect	5
3.1 SharePoint connections	5
3.2 Tenant – sign in as an administrator (no app registration)	6
3.3 Tenant – App ID (unattended)	7
3.4 Power Platform with an App ID (once)	8
3.5 Show real names in usage reports	8
4 Permissions & sharing audit	9
Run the audit	9
Read the results	10
The People tab	11
5 User access and copy access	12
Find what someone can open	12
Copy the access to another person	13
Remove someone's access	14
6 Fix oversharing	15
Good practice	16
7 Teams, groups & sites	17
Run the audit	17
E-mail the owners	18
Add owners	19
8 Power Platform	20
Run the audit	20
Assign a new owner	21
9 Results, scheduling and history	22
Working with results	22
Schedule an audit	22
Repeat every week or month, with an e-mailed summary	22
Compare two runs	23
Audits list and Actions log	24
10 A governance routine that works	26
Set up once	26
Recommended cadence	26
Key numbers to track	27
11 Troubleshooting	28
Getting help	28
Appendix – Quick reference	29

CHAPTER 1

1 Introduction

What M365 Audit & Governance does, how it keeps you safe, and how this guide is organised.

M365 Audit & Governance is a Windows desktop app for Microsoft 365 and SharePoint administrators. It answers the governance questions you are asked most often – *who can open this?*, *who owns this team?*, *what did the person who left leave behind?* – and lets you fix what it finds in a few clicks.

The audits

Audit	Answers	Connect with
Permissions & sharing	Anyone and organization sharing links, guests, “Everyone”, site collection administrators and every unique permission – down to single files.	A SharePoint connection
User access	Everything one person can open across sites, subsites, lists, libraries, folders and files – and through what. Copy it to another person.	A SharePoint connection
Teams, groups & sites	Teams, Microsoft 365 groups and SharePoint sites with no activity for a period you choose, no owner, disabled owners or a single owner.	A tenant
Power Platform	Power Automate flows and Power Apps whose owner was deleted or disabled.	A tenant

Three promises

- **Audits only read.** Running an audit never changes anything in SharePoint, Teams or Power Platform.
- **Changes only after you confirm.** Every action – e-mailing owners, adding owners, transferring a flow, removing access – shows what will happen and waits for your confirmation.
- **Everything is logged.** Every action is written to the Actions log with who it affected and the result, so you can prove what was done.

How to use this guide

Chapters 2 and 3 get you installed and connected – do these once. Chapters 4 to 9 explain each audit and action. Chapter 10 is a ready-made governance routine you can adopt as is. Chapter 11 lists the messages you may see and what to do.

TIP

Short on time? Install, connect a tenant by signing in as an administrator (section 3.2), and run a **Teams, groups & sites** audit. You will have useful results in under ten minutes.

CHAPTER 2

2 Install and activate

Install the app, start the free trial or enter your serial number.

System requirements

- Windows 10 or Windows 11 (64-bit).
- Internet access to Microsoft 365 (and to your SharePoint Server farm if you audit on-premises sites).
- A Microsoft 365 administrator account, or an Entra ID app registration (App ID) – see chapter 3.

Install

- 1 Download **M365-Governance-Setup.exe** from mknepalsolutions.com.
- 2 Run it and follow the steps. You can choose the installation folder; a desktop shortcut is created.
- 3 Start **M365 Audit & Governance**. The app checks for updates on start and installs them when you agree.

NOTE

Closing the window keeps the app running in the notification area, so scheduled and repeating audits still run. To quit, right-click the tray icon and choose **Quit**.

Start the free trial

- 1 On the activation screen click **Start free trial**.
- 2 Enter your **work e-mail address**. A verification code is sent to it.
- 3 Enter the **verification code**. The 7-day trial starts on this computer.

The trial has every feature and can audit up to 3 site collections or tenant scans. The License page shows what is left.

Activate with a serial number

- 1 Buy a license at mknepalsolutions.com (\$999 per computer per year). The serial number is e-mailed to you.
- 2 In the app open **License** → **Enter serial number**, paste it and click **Activate**.
- 3 Online serials are bound to this computer by the activation server. The license starts today and replaces the trial.

Offline activation (no internet on this computer)

- 1 Open **License** and click **Copy request for vendor**. This copies the computer's Machine ID, computer name, Windows user and app version.
- 2 Paste it into an e-mail to us. You receive an offline serial number issued for that Machine ID.
- 3 Enter it under **License** → **Enter serial number**. The License page shows *Offline – serial issued for Machine ID*

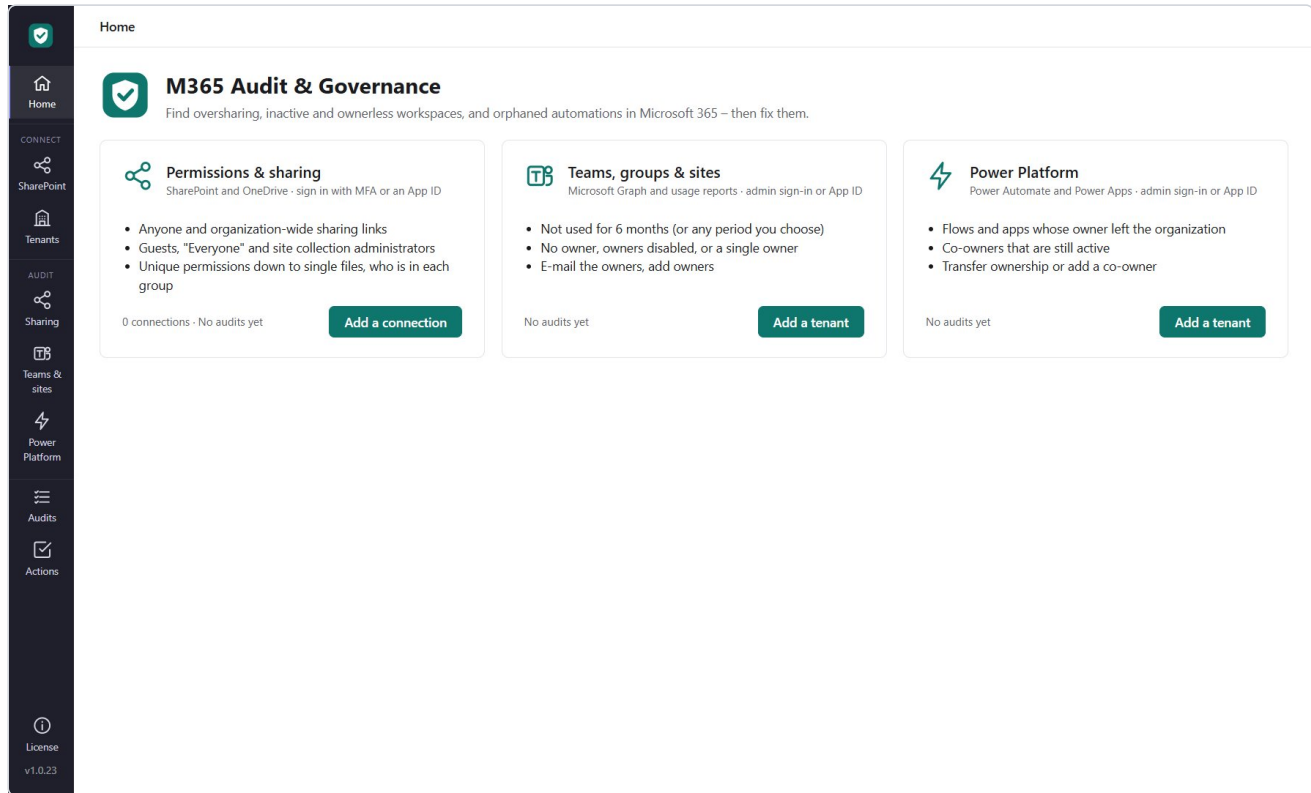
Renewal and moving to another computer

Before the license expires the app reminds you. Enter the renewal serial under **License** → **Enter renewal serial** – the new term continues from the old one. To move a license to another computer, activate it there; the activation server releases it on the old computer after you confirm, and the term continues (it does not restart).

CHAPTER 3

3 Connect

Connect your SharePoint sites (for permission audits) and your Microsoft 365 tenant (for Teams, groups, sites and Power Platform).



Home: the three audit areas. The sidebar groups Connect (SharePoint, Tenants) and Audit (Sharing, Teams & sites, Power Platform, Audits, Actions).

To run	You need
Permissions & sharing, User access	A SharePoint connection (sidebar → SharePoint)
Teams, groups & sites, Power Platform, e-mail summaries	A Tenant (sidebar → Tenants)

3.1 SharePoint connections

- 1 Open **SharePoint** → **Add connection**.
- 2 Enter the **admin center address**, for example `https://contoso-admin.sharepoint.com`. With the admin center the audits can list every site and OneDrive in the tenant. A single site address works too.

- 3 Choose how to sign in: **Microsoft 365 – browser sign-in** (Microsoft's own page; MFA and Conditional Access work as usual – no App ID needed), or an **App ID** with the SharePoint application permission `Sites.FullControl.All` for unattended audits.
- 4 For SharePoint Server (on-premises) enter the site address and use **Windows – user name & password (NTLM)** or **Windows – current user**.
- 5 Click **Connect**. The connection shows **Connected**.

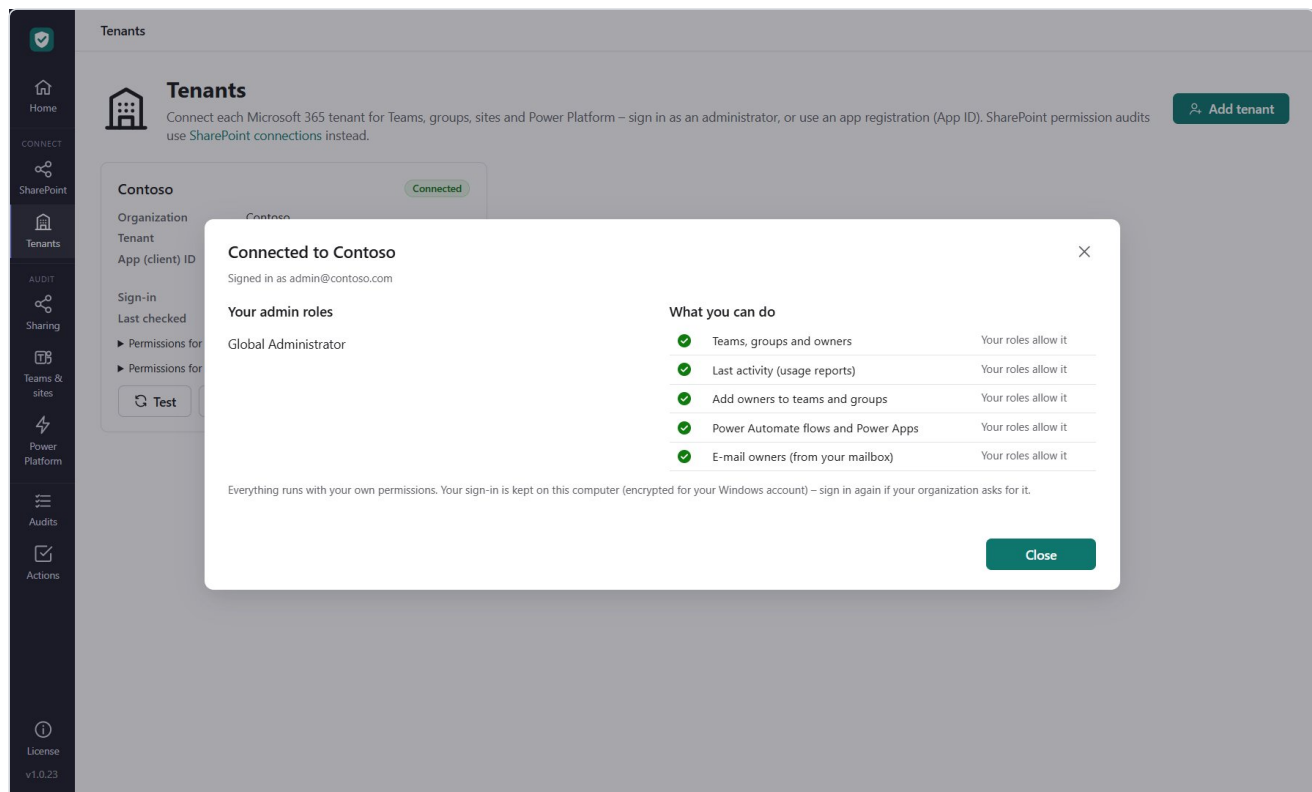
TIP

Sign in as a **SharePoint Administrator** and make sure the account is a site collection administrator of the sites you audit, or the audit cannot read items with unique permissions.

3.2 Tenant – sign in as an administrator (no app registration)

The quickest way. The audits run with your own admin roles – nothing to register in Entra ID.

- 1 Open **Tenants** → **Add tenant** and choose **Sign in as an administrator**.
- 2 Sign in with your work account. MFA and Conditional Access work as usual.
- 3 The first time, Microsoft may ask you to approve *Microsoft Graph Command Line Tools* – Microsoft's own sign-in app, also used by Microsoft Graph PowerShell. A Global Administrator can tick **Consent on behalf of your organization** to approve it for everyone.
- 4 The app shows your admin roles and what they allow you to do.



After signing in: your admin roles and what each one allows.

Which roles you need:

To	Your account needs one of
Teams, groups and their owners	Groups Administrator, Teams Administrator, SharePoint Administrator, Global Reader, Global Administrator
Last activity (usage reports)	Reports Reader, Global Reader, SharePoint / Teams / Exchange Administrator, Global Administrator
Add owners	Groups Administrator, Teams Administrator, SharePoint Administrator, Global Administrator
Power Automate flows and Power Apps	Power Platform Administrator, Dynamics 365 Administrator, Global Administrator
E-mail owners and summaries	Nothing extra – sent from your mailbox, or a shared mailbox you may send as

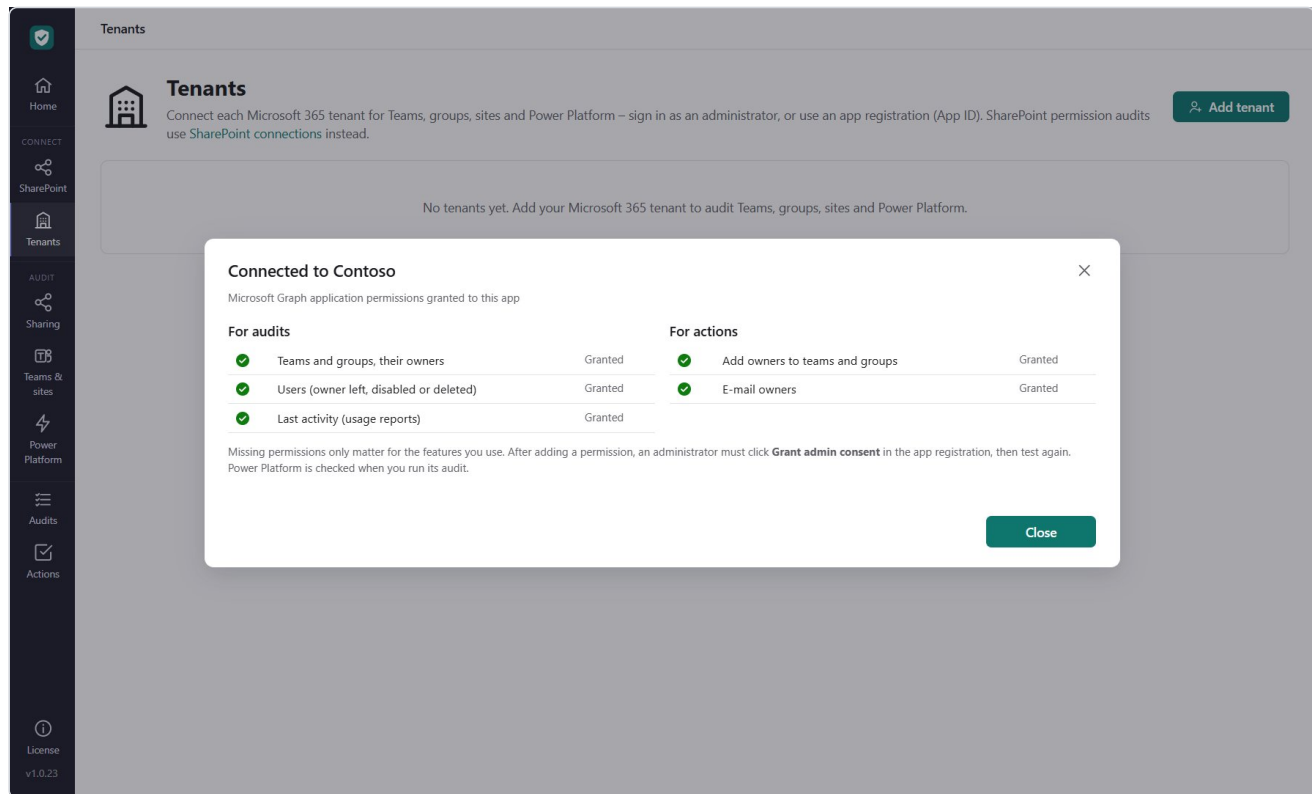
Your sign-in is kept on this computer, encrypted for your Windows account. If your organization asks you to sign in again, click **Sign in again** on the tenant.

3.3 Tenant – App ID (unattended)

Best for scheduled and repeating audits that must never wait for someone to sign in.

- 1 Entra admin center → **App registrations** → **New registration**.
- 2 **API permissions** → **Add a permission** → **Microsoft Graph** → **Application permissions** and add the permissions below.
- 3 Click **Grant admin consent**.
- 4 **Certificates & secrets**: upload a certificate (recommended) or create a client secret.
- 5 In the app: **Tenants** → **Add tenant** → **App ID**. Enter the tenant (for example `contoso.onmicrosoft.com`), the Application (client) ID and the certificate or secret.
- 6 Click **Test**. The app lists which permissions are granted.

Permission (application)	Needed for
Group.Read.All	Teams and groups, their owners and members
User.Read.All	Whether owners are disabled or deleted
Reports.Read.All	Last activity from the Microsoft 365 usage reports
Group.ReadWrite.All	Action: add owners
Mail.Send	Action: e-mail owners, and e-mailed audit summaries



Test shows the permissions granted to the App ID – for audits and for actions.

3.4 Power Platform with an App ID (once)

Signed in as an administrator? Skip this. With an App ID, Power Platform's admin APIs accept the app only after it is registered as a management application. Run once in PowerShell with the Power Platform CLI, as a Power Platform administrator:

```
pac admin application register --application-id <Application (client) ID>
```

3.5 Show real names in usage reports

Activity dates come from the Microsoft 365 usage reports. If your tenant hides names in reports, sites cannot be matched to their owners. Microsoft 365 admin center → **Settings** → **Org settings** → **Reports** → clear **Display concealed user, group, and site names in all reports**.

NOTE

Usage reports are produced by Microsoft once a day, so a team used this morning may still show yesterday's date.

CHAPTER 4

4 Permissions & sharing audit

Find every sharing link, guest, “Everyone” permission, site collection administrator and unique permission in SharePoint sites and OneDrives.

Run the audit

- 1 Open **Sharing** → **New audit**.
- 2 Pick the **SharePoint connection**. With an admin center connection, click **Load sites** to list every site; tick **OneDrives** to include them. Filter, then **Select shown** – or paste site addresses, one per line.
- 3 Choose **How deep** (see below).
- 4 Keep **Read SharePoint group members** ticked to find guests inside groups and see who a *Specific people* link was shared with.
- 5 Optionally set **Repeat** (chapter 9), then click **Start audit** – or **Schedule...** to run later.

The permissions & sharing audit form.

How deep	Reads	Use when
Everything	Sites, lists, libraries, folders, files and items with their own permissions or sharing links	Access reviews and audits – the complete picture (slower on very large sites)

How deep	Reads	Use when
Sites and lists	Sites, subsites, lists and libraries	A quick overview; files and folders shared on their own are not listed
Sites only	Site and subsite permissions, site collection administrators	Checking who administers what across many sites

Read the results

Findings appear while the audit runs, sorted by risk. The tiles at the top count findings by risk and by type – click a tile to filter.

Permissions & sharing > Permissions & sharing – 2026-10-27

Permissions & sharing – 2026-10-27
 Completed · finished 10/27/2026, 7:30:30 AM

Run again Edit and run again Export CSV

13 All findings 0 High risk 0 Medium risk 1 Low risk 0 Anyone links 0 Guests 0 Everyone 1 Organization links

Findings People Changes Audit log

Search name, address, person... All findings 0 selected Remove access Restore inheritance

Risk	Object	Name	Who	Type	Access	Flags
Low	File	Résumé - final (2).pdf Contoso Intranet	Organization link 1 member	Sharing link Organization · View	Read	Organization link
Info	Site collection	Contoso Intranet Contoso Intranet	Migration Admin	User	Site collection administrator	Direct user permission Can edit Site admin
Info	Site	Contoso Intranet Contoso Intranet	Migration Admin	User	Full Control	Direct user permission Can edit
Info	Subsite	Certification Contoso Intranet	Certification Owners 1 member	SharePoint group	Full Control	Can edit
Info	Subsite	Certification Contoso Intranet	Certification Members 2 members	SharePoint group	Contribute	Can edit
Info	Subsite	Certification Contoso Intranet	Auditors 1 member	SharePoint group	Approve Docs	Can edit
Info	Subsite	Certification Contoso Intranet	Carol Chen	User	Read	Direct user permission
Info	Subsite	Certification Contoso Intranet	Finance Team (AD group)	Security group	Read	
Info	Folder	2024 Contoso Intranet	Auditors 1 member	SharePoint group	Read	

13 of 13 shown

Results: tiles, findings sorted by risk, and the Findings, People, Changes and Audit log tabs.

Risk levels

Risk	When
High	An Anyone link; a guest or Everyone who can edit; a guest site collection administrator; a group with guests that can edit
Medium	A guest or Everyone who can read; an organization link that can edit
Low	An organization link that can view
Info	Every other unique permission (groups, people) – useful for access reviews

Flags

Flag	Meaning
Anyone link	Anyone with the link can open it, without signing in
Organization link	Everyone in your organization who has the link
Specific people link	Shared with named people – guests among them are listed
Guest	An external user (#ext#), directly or inside a SharePoint group
Everyone	"Everyone", "Everyone except external users" or all authenticated users
Direct user permission	Given to one person instead of a group – hard to manage over time
Can edit	The permission level allows changes (Contribute, Edit, Design, Full Control...)
Site admin	A site collection administrator

The People tab

One line per person, group or link, with the highest risk and how many objects they can reach – an instant access review. Click a line to see the objects. Sort by count to find the accounts that can open the most.

TIP

Start with the **High risk** tile, then **Anyone links** and **Guests**. Most real exposure is there. Info findings are normal and mostly useful for access reviews.

CHAPTER 5

5 User access and copy access

See everything one person can open – and give a new starter or a replacement the same access.

Find what someone can open

- 1 Open **Sharing** → **User access**.
- 2 Enter the person: `jane@contoso.com`, or `CONTOSO\jane` on-premises.
- 3 Choose the SharePoint connection and the sites – with an admin center connection you can pick every site and OneDrive.
- 4 Click **Start audit**.

The screenshot shows the 'User access – contoso\alice' interface in the Microsoft 365 admin center. The top section displays a summary of access types: 3 All access, 0 Direct, 1 Through groups, 0 Site admin, 0 Everyone, 1 Sharing links, and 1 Entra / M365 groups. Below this, the 'Findings' tab is active, showing a table of access findings. The table has columns for Object, Name, Access, Through, and Flags. Three findings are listed: a File named 'Résumé – final (2).pdf' with Read access through an Organization link; a Subsite named 'Certification Contoso Intranet' with Contribute access through the SharePoint group 'Certification Members'; and another Subsite named 'Certification Contoso Intranet' with Read access through the Security group 'Finance Team (AD group) – membership not checked'. The interface also includes buttons for 'Run again', 'Edit and run again', 'Export CSV', 'Remove access', and 'Copy to another person'.

Object	Name	Access	Through	Flags
File	Résumé – final (2).pdf Contoso Intranet	Read	Organization link	Organization link
Subsite	Certification Contoso Intranet	Contribute	SharePoint group: Certification Members	Can edit
Subsite	Certification Contoso Intranet	Read	Security group: Finance Team (AD group) – membership not checked	

User access: every place the person can open, the permission level and through what.

Through	Meaning
Direct	Permissions given to the person themselves
SharePoint group: ...	They are a member of that SharePoint group
Site collection administrator	Full control of the whole site collection
Everyone / Everyone except external users	Everyone in the organization has this access

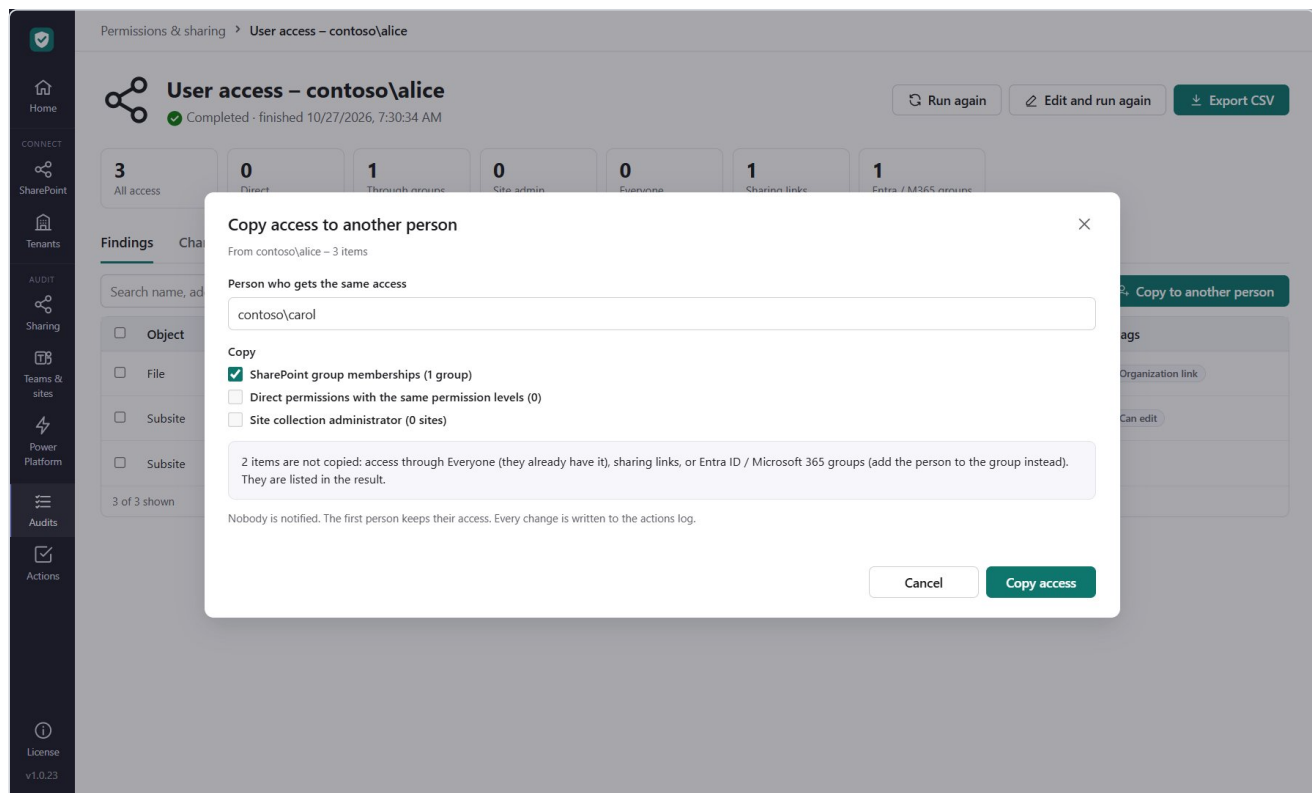
Through	Meaning
... link	A sharing link that was shared with them
Security group / Microsoft 365 group – membership not checked	Access given to an Entra ID or AD group; SharePoint cannot tell whether the person is in it

Access to a site includes everything in it that does not have its own permissions, so only the places with their own permissions are listed separately.

Copy the access to another person

Typical uses: a new starter who needs the same access as a colleague, or a replacement for someone who left.

- 1 In the result select rows – or select none to copy everything shown.
- 2 Click **Copy to another person** and enter the person.
- 3 Choose what to copy: **SharePoint group memberships** (added to the same groups, each once), **Direct permissions** (same levels on the same objects), and – only if you tick it – **Site collection administrator**.
- 4 Click **Copy access**.



Copy access: choose what to copy. Nobody is notified and every change is logged.

Not copied, and listed with the reason: access through **Everyone** (they already have it), **sharing links** (share the item with them instead) and **Entra ID / Microsoft 365 groups** (add them to the group). The first person

keeps their access. Run **User access** for the new person afterwards to check.

Remove someone's access

In a User access result, select rows and click **Remove access**. Direct permissions are removed; access through a SharePoint group is removed by taking the person **out of the group** – the group keeps its permissions for everyone else. Access through Everyone, sharing links or Entra ID groups is not changed.

TIP

Offboarding: run User access for the leaver, **Copy to another person** for their replacement, then **Remove access** for the leaver – all from one result.

CHAPTER 6

6 Fix oversharing

Remove sharing links, guests, “Everyone” and other permissions, or restore inheritance – straight from the results.

In a **Permissions & sharing** result, tick the rows and choose an action:

Action	What happens
Remove access	That permission is removed: a sharing link stops working; a guest, “Everyone”, group or person loses that permission level on that site, list, folder or file. A site collection administrator stops being one.
Restore inheritance	The folder, file, list or subsite goes back to its parent’s permissions. All its own permissions and sharing links are removed – not only the ticked ones. Top-level sites are skipped (they have no parent).

The screenshot shows the 'Permissions & sharing' results for 2026-10-27. The interface includes a sidebar with navigation options like Home, CONNECT, SharePoint, Tenants, AUDIT, Sharing, Teams & sites, Power Platform, Audits, and Actions. The main area displays a summary of findings: 13 All findings, 0 High risk, 0 Medium risk, 1 Low risk, 0 Anyone links, 0 Guests, 0 Everyone, and 1 Organization links. A modal dialog titled 'Remove access' is open, providing a summary of the changes and asking for confirmation. The dialog text states: 'This changes SharePoint – export the results first if you may need to restore them. 1 permission will be removed: 1 sharing link – people who use them lose access, the rest: people and groups with their own permissions. Nobody is notified. Every change is written to the actions log. Run the audit again afterwards to confirm.' The dialog has 'Cancel' and 'Remove access' buttons. The background table shows findings for 'Subsite' and 'Folder' with various permissions and actions.

Remove access summarises what will change and waits for your confirmation.

IMPORTANT

Export CSV before you clean up if you may need to put permissions back. Changes are made in SharePoint immediately, nobody is notified, and every change is written to the Actions log.

Good practice

- Fix **Anyone links** on sensitive content first, then guests who can edit, then “Everyone”.
- Prefer **Restore inheritance** for folders and files that were shared ad hoc – it removes the whole tangle at once.
- Replace “Everyone” with a SharePoint or Microsoft 365 group rather than individual people.
- Tighten the tenant policy too: SharePoint admin center → **Policies** → **Sharing**, and per site under **Active sites** → **Sharing**.
- Run the audit again and check the **Changes** tab: removed findings appear under **Fixed**.

CHAPTER 7

7 Teams, groups & sites

Find inactive and ownerless workspaces – then ask the owners, or add owners where none are left.

Run the audit

- 1 Open **Teams & sites** → **New audit** and choose the tenant.
- 2 Set **Inactive for**: 3 months, 6 months (default, 180 days), 1 year – or any number of days.
- 3 Choose what to include: **Teams, Microsoft 365 groups, SharePoint sites**.
- 4 Click **Start audit**.

Teams, groups & sites > Teams, groups & sites – 2026-10-27

Teams, groups & sites – 2026-10-27
 Completed · finished 10/27/2026, 7:30:23 AM

Run again Edit and run again Export CSV

5 All findings 2 High risk 2 Medium risk 0 Low risk 3 Inactive 1 No owner 1 Owners disabled 1 One owner

Findings Changes Audit log

Search name, address, person... All findings 0 selected E-mail owners Add owners

☐	Risk	Type	Name	Last activity	Owners	Flags
☐	High	Microsoft 365 group	Orphan Group orphangroup@contoso.com	2026-09-27 30 days ago	None	No owner
☐	High	Microsoft 365 group	Leaver Group leavergroup@contoso.com	2025-12-31 300 days ago	None Disabled: gone@contoso.com	Owners disabled Inactive
☐	Medium	Team	Old Project Team oldprojectteam@contoso.com	2025-09-22 400 days ago	ann@contoso.com	One owner Inactive
☐	Medium	SharePoint site	https://contoso.sharepoint.com/sites/archive https://contoso.sharepoint.com/sites/archive	2025-06-14 500 days ago	ben@contoso.com	Inactive
☐	Info	Team	Sales Team salesteam@contoso.com	2026-10-25 2 days ago	ann@contoso.com, ben@contoso.com	

5 of 5 shown

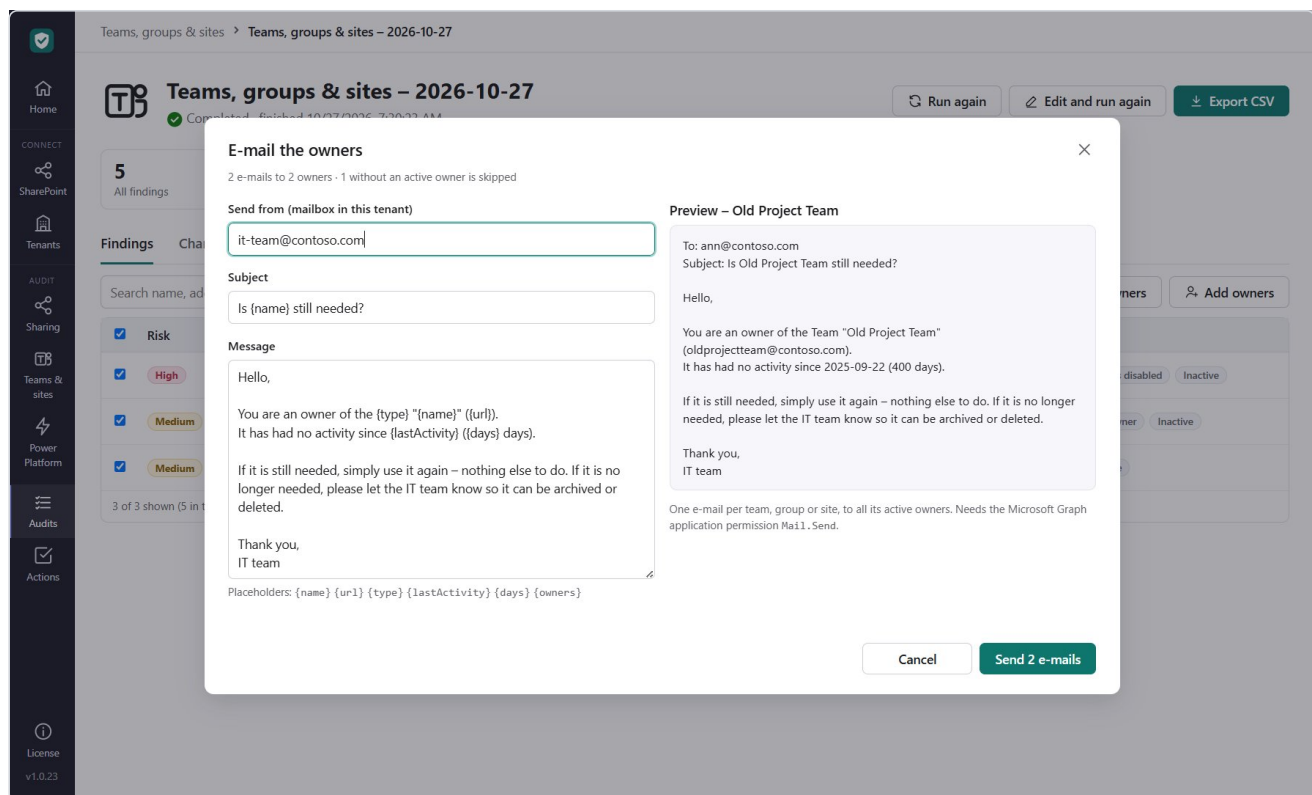
Teams, groups & sites: last activity, owners and flags for every workspace.

Flag	Meaning	Risk
No owner	The team or group has no owner at all	High
Owners disabled	Every owner is disabled or deleted – nobody can manage it	High
Inactive	No activity (files, messages, e-mail, page views) for longer than your period	Medium
One owner	Only one owner – a risk when that person leaves	Low

Flag	Meaning	Risk
Guests	The group has guest members – check they still need access	Info

E-mail the owners

Before archiving or deleting an inactive workspace, ask its owners. Select inactive teams, groups or sites and click **E-mail owners**. One e-mail per workspace goes to all its active owners, from the mailbox you enter – a shared mailbox such as `it-team@contoso.com` works well.



E-mail owners: your own subject and message, with a preview of the first e-mail.

Placeholder	Replaced with
{name}	The team, group or site name
{url}	Its address
{type}	Team, Microsoft 365 group or SharePoint site
{lastActivity}	The date of the last activity
{days}	Days since the last activity
{owners}	The owners' names

Workspaces without an active owner are skipped – add an owner first.

TIP

Example message: *"{name} has not been used since {lastActivity} ({days} days). If it is still needed, reply within 30 days – otherwise it will be archived."*

Add owners

Select teams or groups (typically those flagged **No owner**, **Owners disabled** or **One owner**) and click **Add owners**. Enter one or more people. They are added as owners and members (team owners must be members). People who do not exist or are disabled are refused before anything changes.

CHAPTER 8

8 Power Platform

Find Power Automate flows and Power Apps left behind by people who left – and hand them to a new owner before they break.

Run the audit

- 1 Open **Power Platform** → **New audit** and choose the tenant.
- 2 Choose the environments (all, or pick some) and what to include: **Flows, Apps**.
- 3 Keep **List only flows and apps whose owner left** ticked for a short list of what needs action.
- 4 Click **Start audit**.

Power Platform > Power Platform – 2026-10-27

Power Platform – 2026-10-27
 Completed · finished 10/27/2026, 7:30:27 AM

Run again Edit and run again Export CSV

2 All findings 2 High risk 0 Medium risk 0 Low risk 2 Orphaned 0 Owner left, co-owner active

Findings Changes Audit log

Search name, address, person... All findings 0 selected Assign new owner

☐	Risk	Type	Name	Environment	Owner	Co-owners	Flags
☐	High	Power App	Leave requests CanvasApp · changed 2025-01-02	Contoso (default)	old@contoso.com Deleted	None	Orphaned
☐	High	Flow	Weekly report Started · changed 2025-02-03	Contoso (default)	gone@contoso.com Disabled	None	Orphaned

2 of 2 shown

Power Platform: orphaned apps and flows, with the owner's status and any active co-owners.

Flag	Meaning	Risk
Orphaned	The owner (or the flow's creator) was deleted or disabled and there is no active co-owner. Nobody can edit it.	High
Owner left, co-owner active	The owner left, but an active co-owner can still manage it.	Medium

Assign a new owner

Select the flows and apps and click **Assign new owner**:

- **Power Apps – Transfer ownership** makes the person the owner (the previous owner keeps edit rights), or **Add as co-owner**.
- **Flows** – the person is added as an owner; a flow's creator cannot be changed. The new owner should open the flow and fix connections that used the old account.

IMPORTANT

Connections belong to the person who created them. After a transfer, ask the new owner to open the flow or app, replace connections that used the leaver's account, and test it.

CHAPTER 9

9 Results, scheduling and history

Work with results, run audits on a schedule, repeat them every week or month, and see what changed.

Working with results

Control	What it does
Tiles	Counts by risk and type. Click to filter; click again to clear.
Search and filter	Search by name, address or person; the drop-down filters by flag.
Export CSV	All findings with every column – for auditors, Excel or Power BI. Export before cleaning up.
Run again	Runs the same audit now, as a new run of the same series.
Edit and run again	Opens the form with the same settings so you can change them first.
Changes tab	What is new, fixed and changed compared with an earlier run.
Audit log tab	What the audit read, with warnings (for example an item it was refused).

Schedule an audit

In any audit form click **Schedule...** to choose when it starts. Scheduled audits wait under **Audits** and run while the app is open (minimized to the notification area is fine). Scheduled audits use the saved sign-in; with an administrator sign-in, sign in again if your organization asks.

Repeat every week or month, with an e-mailed summary

- 1 In the audit form, under **Repeat**, choose **Every week** or **Every month**.
- 2 Tick **E-mail a summary of what changed**.
- 3 **Send with tenant:** a tenant from Tenants (admin sign-in, or an App ID with `Mail.Send`).
- 4 **From:** the mailbox it is sent from (your own when signed in as an administrator). **To:** who receives it.
- 5 Start the audit. When a run finishes, the next one is scheduled automatically.

New permissions & sharing audit

Read-only: nothing is changed at the sites

Sites to audit

☐ OneDrives

Click **Load sites**, or paste site addresses below.

1 site selected

How deep

☒ **Everything** – sites, lists, libraries, folders, files and items with their own permissions or sharing links

☐ **Sites and lists** – faster; files and folders shared on their own are not listed

☐ **Sites only** – site and subsite permissions, site collection administrators

☒ Read SharePoint group members (finds guests inside groups and shows who a "Specific people" link was shared with)

Repeat

☐ Once ☒ Every week ☐ Every month

☒ E-mail a summary of what changed since the previous run

Send with tenant

Repeat options in the audit form.

After each run the recipients get the number of findings and what is **new**, **fixed** and **changed** since the previous run. A run missed while the app was closed starts when it opens. To stop, open the audit and click **Stop repeating** – the waiting run is removed.

Compare two runs

Open an audit, click the **Changes** tab and choose the earlier run to compare with:

- **New** – findings that were not there before (a new Anyone link, a new ownerless team).
- **Fixed** – findings that are gone.
- **Changed** – the same finding with a different risk, access level or flags; the *Before* column shows what it was.

Permissions & sharing > Permissions & sharing – 2026-10-27

Permissions & sharing – 2026-10-27

Completed · finished 10/27/2026, 7:30:38 AM

Run again Edit and run again Export CSV

0 All findings

0 High risk

0 Medium risk

0 Low risk

0 Anyone links

0 Guests

0 Everyone

0 Organization links

Findings People **Changes** Audit log

Compare with 10/27/2026, 7:30:29 AM – Permissions & sharing – 2026-10-27 13 findings then, 12 now

0 New (0 high risk)

1 Fixed (0 high risk)

0 Changed

New since then (0)
Nothing new.

Fixed since then (1)

Risk	Object	Name	Who	Access
Low	File	Résumé – final (2).pdf Contoso Intranet	Organization link	Read

Changed (0)
Nothing changed.

Audits v1.0.23

Changes: the removed sharing link shows as Fixed after the audit ran again.

Audits list and Actions log

Audits lists every run – running, scheduled, finished – with its result. **Actions** lists every change the app made: e-mails sent, owners added, ownership transferred, access copied or removed, inheritance restored – with the object, the people affected, who did it and the result. Export it to CSV as evidence for auditors.

✓

Home

CONNECT

SharePoint

Tenants

AUDIT

Sharing

Teams & sites

Power Platform

Audits

Actions

License

v1.0.23

Actions log

✓

Actions log

Every change made from this app: e-mails sent to owners, owners added, ownership transferred – with who, what and the result.

Date	Action	Target	Who	Result
10/27/2026, 7:30:37 AM	Removed access	File: Résumé – final (2).pdf	Organization link Organization link removed (Read)	✓ Done
10/27/2026, 7:30:36 AM	Copied access	Subsite: Certification	contoso\carol added to Certification Members (like contoso\alice)	✓ Done
10/27/2026, 7:30:28 AM	Transferred ownership	Leave requests Power App	nora@contoso.com	✓ Done
10/27/2026, 7:30:26 AM	E-mailed owners	https://contoso.sharepoint.com/sites/archive SharePoint site	ben@contoso.com	✓ Done
10/27/2026, 7:30:26 AM	E-mailed owners	Old Project Team Team	ann@contoso.com	✓ Done
10/27/2026, 7:30:25 AM	Added owner	Orphan Group	nora@contoso.com	✓ Done

The Actions log – your evidence of what was changed, when and with what result.

CHAPTER 10

10 A governance routine that works

A ready-made rhythm for using the app effectively – adopt it as is or adjust it to your organization.

Set up once

- 1 Connect SharePoint through the **admin center** so audits see every site and OneDrive.
- 2 Connect the tenant with an **App ID with a certificate** for repeating audits (no sign-in prompts), and keep an administrator sign-in for ad-hoc work.
- 3 Clear **Display concealed names** in report settings (section 3.5).
- 4 Create a shared mailbox such as `it-governance@contoso.com` for owner e-mails and summaries.
- 5 Run each audit once and **export the CSVs** as your baseline.
- 6 Turn on **Repeat** for the audits below, with the summary e-mailed to the governance team.

Recommended cadence

When	Audit	Act on
Weekly	Permissions & sharing – <i>Sites and lists</i> on sensitive sites (Finance, HR, Legal, Executive)	New Anyone links and guests who can edit – remove them or ask the site owner
Weekly	Power Platform	New Orphaned flows and apps – assign an owner within a week
Monthly	Teams, groups & sites – 180 days	No owner / Owners disabled → add owners. Inactive → e-mail owners; archive what nobody claims after 30 days
Monthly	Permissions & sharing – <i>Everything</i> , all sites and OneDrives	Check the Changes tab: new High and Medium findings
Quarterly	People tab of the full sharing audit	Access review with site owners; export CSV as evidence
Leaver	User access for the person	Copy to the replacement, then remove access. Then check Power Platform for their flows and apps
Joiner / mover	User access for a colleague in the same role	Copy to another person – same groups and permission levels

Key numbers to track

- Anyone links – aim for zero on sensitive sites.
- Guests who can edit – each one should have a named sponsor.
- Teams and groups with no owner or with one owner – aim for at least two active owners everywhere.
- Workspaces inactive for more than a year – archived or deleted.
- Orphaned flows and apps – zero older than one week.

The e-mailed summary and the Changes tab give these numbers run by run; export the CSVs into Excel or Power BI for a trend over time.

TIP

Share the e-mailed summary with your security or compliance lead. A weekly “3 new, 5 fixed” is the simplest proof that governance is working.

CHAPTER 11

11 Troubleshooting

Messages you may see and what to do about them.

Message or symptom	What to do
<i>The app may not read usage reports – add ... Reports.Read.All</i>	Add the Graph application permission <code>Reports.Read.All</code> , grant admin consent and run again. Owners are still checked meanwhile. Signed in as an administrator? You need Reports Reader or one of the roles in 3.2.
<i>The usage reports hide user, group and site names</i>	Clear Display concealed user, group, and site names (section 3.5).
<i>... Add the Microsoft Graph application permission Mail.Send</i>	Add <code>Mail.Send</code> (application) and grant consent. The sender must be a mailbox in the tenant.
<i>... Group.ReadWrite.All</i>	Needed to add owners. Add it and grant consent.
<i>Power Platform refused the app (403)...</i>	Register the App ID as a Power Platform management application once: <code>pac admin application register --application-id <client ID></code> .
<i>No user ... in this tenant / ... is disabled</i>	Check the address. A new owner must be an enabled user in the tenant.
Power Platform shows nothing after admin sign-in	Your account needs Power Platform Administrator, Dynamics 365 Administrator or Global Administrator.
<i>Access denied (401/403) on a site or item</i>	The account is not a site collection administrator there. Add it as site admin (SharePoint admin center → Active sites → Permissions), or use an App ID with <code>Sites.FullControl.All</code> .
Only one site is listed in the sites picker	The connection points at a single site. Connect to the admin center address (https://contoso-admin.sharepoint.com).
A scheduled or repeating audit did not run	Audits run while the app is open (minimized is fine). A missed run starts when the app opens. With admin sign-in, check the tenant does not ask to sign in again.
Sign-in window keeps asking to sign in	Your organization requires a new sign-in (Conditional Access). Click Sign in again on the tenant or connection.
Trial limit reached	The trial audits up to 3 site collections or tenant scans. Enter a serial number under License to continue without limits.

Getting help

- Knowledge base: mknepalsolutions.com/activation/kb.php – search for “governance”.
- Support tickets: sign in at mknepalsolutions.com and open a ticket. Attach the audit’s CSV export or the **Audit log** tab text when reporting a problem.
- When you report a problem, include the app version (bottom of the sidebar) and the exact message.

APPENDIX

Appendix – Quick reference

Everything on one page.

I want to...	Go to
Find Anyone links and guests	Sharing → New audit → filter Anyone links / Guests
See what one person can open	Sharing → User access
Give a new starter the same access as a colleague	User access for the colleague → Copy to another person
Remove a sharing link or permission	Sharing result → select → Remove access
Undo ad-hoc sharing on a folder	Sharing result → select → Restore inheritance
Find ownerless teams	Teams & sites → New audit → tile No owner
Ask owners about inactive teams	Teams & sites result → filter Inactive → E-mail owners
Add owners in bulk	Teams & sites result → select → Add owners
Rescue flows of a leaver	Power Platform → New audit → select → Assign new owner
Get a weekly report by e-mail	Any audit form → Repeat → Every week → E-mail a summary
See what changed since last month	Open the audit → Changes tab
Prove what was changed	Actions → export CSV
Enter a serial number	License → Enter serial number

M365 Audit & Governance 1.0.23 · MK Nepal Solutions · mknepalsolutions.com

Microsoft 365, SharePoint, Teams, Power Automate, Power Apps, Entra ID and Exchange are trademarks of the Microsoft group of companies.