



# Cloud Backup technical investigation and remediation guide

For MSPs customer administrators and incident response teams

October 18, 2026

All event times are UTC

Technical workflow for reviewing Microsoft 365 tenants, preserving evidence, and remediating confirmed unauthorized changes associated with Cloud Backup and related former SkyKick application identities.

## Intended use

Use this guide to investigate potential unauthorized activity associated with ConnectWise Cloud Backup and related former SkyKick application identities, preserve evidence, and remediate confirmed unauthorized changes in your MSP tenant and each customer tenant you manage. **It is intended for authorized Microsoft 365 administrators, security teams, and incident response providers. We recommend that partners complete the suggestions working with their security team and following any relevant Microsoft guidance.** Complete the checks within each tenant, including environments with dormant connections. Keep affected connections disabled until ConnectWise provides formal restoration instructions; completing this workflow does not establish that a tenant was unaffected or authorize service reconnection.

If you supply these services through a reseller, distributor, or marketplace, send this guide to the administrator responsible for every customer tenant. Confirm who will perform the review and record its status. Where you lack delegated access, coordinate with the customer's IT administrator or security provider; reviewing your own tenant does not review the customer's tenant.

Use an account authorized for the tenant under review and involve your security team or incident response provider. Log access, application administration, directory-role changes, policy management, and Exchange investigation require different permissions. The access tables give examples of suitable roles, not a requirement to assign every role or a guarantee of access. Tenant restrictions, role scope, licensing, and the selected API or cmdlet can change what is available. Use existing approved access and confirm permissions before making changes.

The screenshots in sections 3 through 7 are illustrative examples from Microsoft documentation. They do not show ConnectWise, SkyKick, partner, or customer environments. Some show creation dialogs solely to identify controls. Do not add credentials, grant new consent, or create policies or rules as part of this review. Interface labels and navigation may vary.

We will continue to post current status and guidance on the [ConnectWise Trust Center](#).

## Application identities disabled on October 17

At 07:00 UTC on October 17, 2026, ConnectWise disabled the seven application identities listed below and revoked the associated credentials as part of our containment actions. These vendor-side actions do not change the configuration of enterprise applications within individual partner or customer tenants.

Verify the local enterprise-application setting in every tenant you administer. Vendor-side containment and local tenant settings are different controls; this table does not document a local change in every tenant. Previously issued tokens may remain usable until they expire or are otherwise invalidated. Separate unauthorized credentials, grants, or identities require investigation and remediation.

| Application                        | Application client ID                |
|------------------------------------|--------------------------------------|
| ConnectWise Cloud Backup           | 506e08f9-6e9a-4da4-942b-a099a03644ae |
| ConnectWise Cloud Management       | 2399d300-6fca-4e6a-a686-399fefe75b83 |
| Cloud Management - MS Teams        | 24205314-2b89-4e07-a2a4-579e898a5640 |
| Cloud Management - Exchange Online | b78f6a77-d4e5-46fb-87e5-d1648bd02519 |
| Cloud Management - MS Graph        | 0de14c77-b9b0-4137-9360-34878a929827 |

| Application                          | Application client ID                |
|--------------------------------------|--------------------------------------|
| Cloud Management - Partner Center    | 412dcf96-176d-4b3a-a1b0-4981ad66971e |
| Cloud Management - SharePoint Online | b2b55f5b-7758-4719-8d8f-88ae172e6bdb |

Older installations may display SkyKick Cloud Manager names. Match on Application ID rather than display name, and record the local Object ID as well. Do not assume a similarly named application has the same identity or status.

## 1 Verify local status and preserve evidence

- Sign in to <https://entra.microsoft.com/>, select the correct directory, and record its tenant ID.
- Open Entra ID → Enterprise applications → All applications. Find each listed Application ID. For an affected application that remains enabled, open Properties, set Enabled for users to sign-in? to No, and save. Disabling an enterprise application requires appropriate administrative permissions, such as Application Administrator or Cloud Application Administrator, or authorization as an owner of the service principal. Global Administrator is not required for this action.
- Verify the saved state. Record the application and local Object IDs, administrator, and UTC time. Keep affected connections disabled. Do not delete the application as the first response; preserve its configuration and evidence for investigation.
- Open Monitoring & health → Audit logs and download the available records as JSON. Export the available interactive-user, non-interactive-user, service-principal, and managed-identity sign-in records separately. Use smaller date ranges or approved collection tools for large exports.
- In Microsoft Purview → Audit, collect available Microsoft 365 activity covering the investigation period. Preserve relevant SIEM, storage, and previously configured Graph activity records as well.

Preserve evidence promptly, but do not delay urgent containment while waiting for exports. Entra normally retains audit and sign-in records for seven days on Free and 30 days on P1/P2; access and features vary. Exported/SIEM retention may be longer. Note missing records and actual coverage. A license upgrade does not recover expired history.

## 2 Review sign-ins across identities

Review from October 13, 2026, through the current time. For broader scoping, extend sign-in searches back to October 1 where records are available, and investigate earlier activity if identified. Record investigation times in UTC; if a portal displays local time, record the offset and convert it for correlation.

- In each available sign-in category, filter IP address to 144.172.64.128. Inspect successful and failed events separately and note any other user or application involved.
- In Service principal sign-ins, filter each listed Application ID. Review source addresses, results, timestamps, resources, and available correlation IDs. Expand grouped records to inspect individual events.
- Review unfamiliar addresses against the application owner's expected activity. Do not restrict the search to the published IP or assume Microsoft/private addresses establish legitimate use.

| Indicator or context                                 | How to interpret it                                                                                                                |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| 144.172.64.128<br>144.172.64[.]99<br>144.172.64[.]60 | Published suspicious addresses. A matching event requires investigation; its result and subsequent activity determine the finding. |

| Indicator or context                      | How to interpret it                                                                                     |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------|
| Python-urllib/3.12; python-requests; curl | Scripting clients may help identify unusual operations, but are also used by legitimate administrators. |
| kiota-dotnet; Azure private IPv6          | Associated with expected vendor activity. Neither alone establishes that an event was authorized.       |

Treat attempts, successful authentication, configuration changes, and data access as distinct findings. Common tooling or an address match alone does not prove compromise or exfiltration.

### 3 Review directory audit events

#### Access for this section

| Operation                                     | Review access examples                                                                         | Remediation access examples  |
|-----------------------------------------------|------------------------------------------------------------------------------------------------|------------------------------|
| View, filter, and open directory audit events | Reports Reader (Security Reader, Security Operator, or Security Administrator also sufficient) | Not applicable — review only |
| Download audit records as JSON                | Reports Reader                                                                                 | Not applicable — review only |

Audit and sign-in log access does not require Global Administrator. Sources: [Microsoft Entra least privileged roles by task](#)

Open Monitoring & health → Audit logs. Use October 13 through now and inspect the following activities; portal labels can vary slightly.

| Category              | Activity examples                                                                                                                                                                                                                                                                                   |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ApplicationManagement | Update application – Certificates and secrets management; Add service principal credentials; Add application; Add service principal; Add owner to application; Add owner to service principal; Add app role assignment to service principal; Add delegated permission grant; Consent to application |
| RoleManagement        | Add member to role; relevant user/group eligible-role assignment changes.                                                                                                                                                                                                                           |
| Policy                | Conditional Access policy additions, changes or deletions; named-location changes.                                                                                                                                                                                                                  |
| UserManagement        | New users, password resets, and authentication-method registration changes.                                                                                                                                                                                                                         |

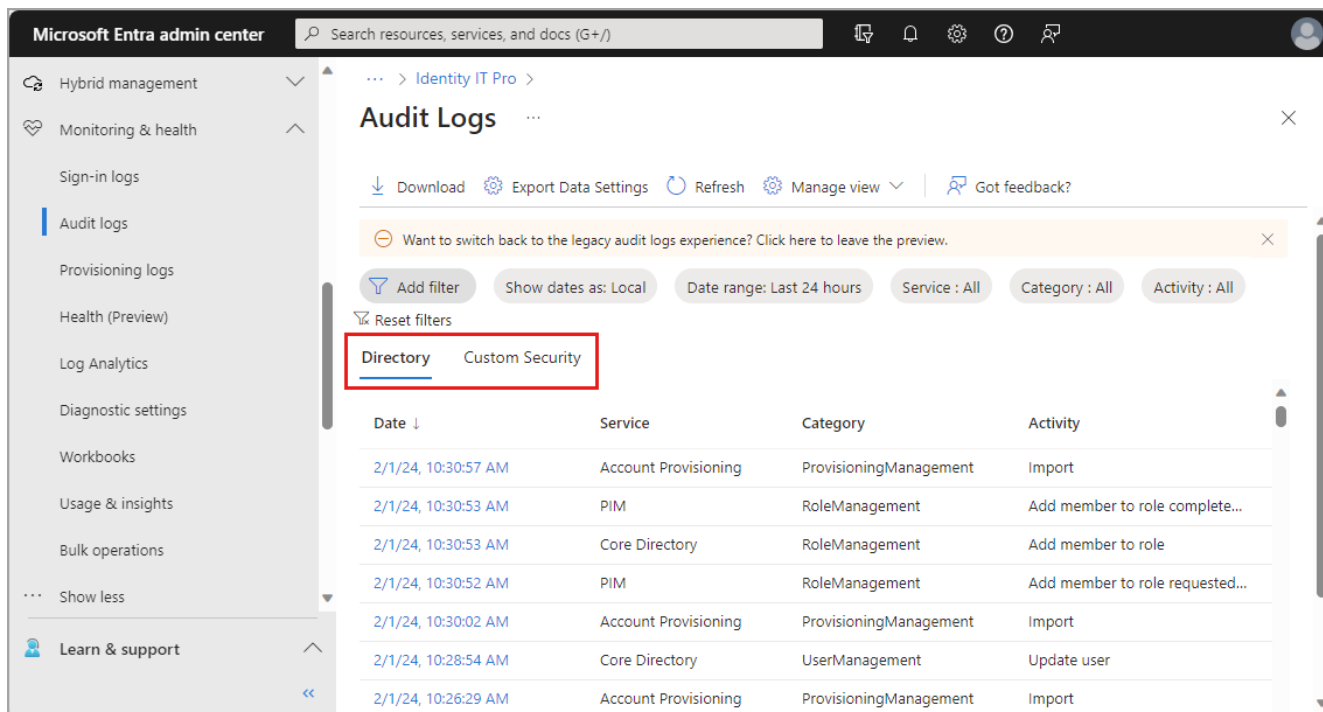


**Figure 1 — Microsoft Entra admin center, Monitoring & health → Audit logs (Directory tab). Filter by Service, Category, and Activity to isolate ApplicationManagement, RoleManagement, Policy, and UserManagement events from October 13 onward, then open individual events to record the initiator, target, outcome, and correlation ID. Source: <https://learn.microsoft.com/en-us/entra/identity/monitoring-health/concept-audit-logs>**

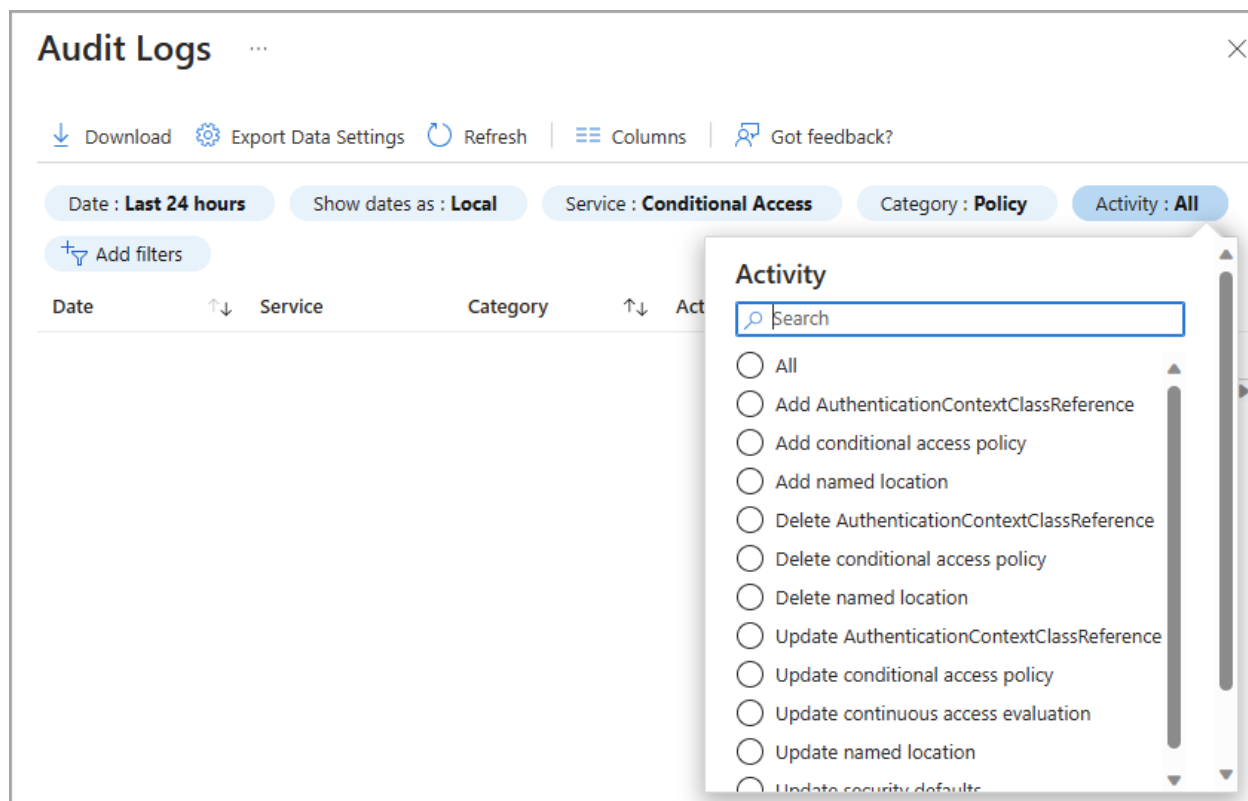


**Figure 2. Audit-log Activity filter. This example shows Conditional Access policy activities. Select the service, category, and activity relevant to each check; it does not illustrate application-credential events. Source: <https://learn.microsoft.com/en-us/entra/identity/monitoring-health/howto-customize-filter-logs>**

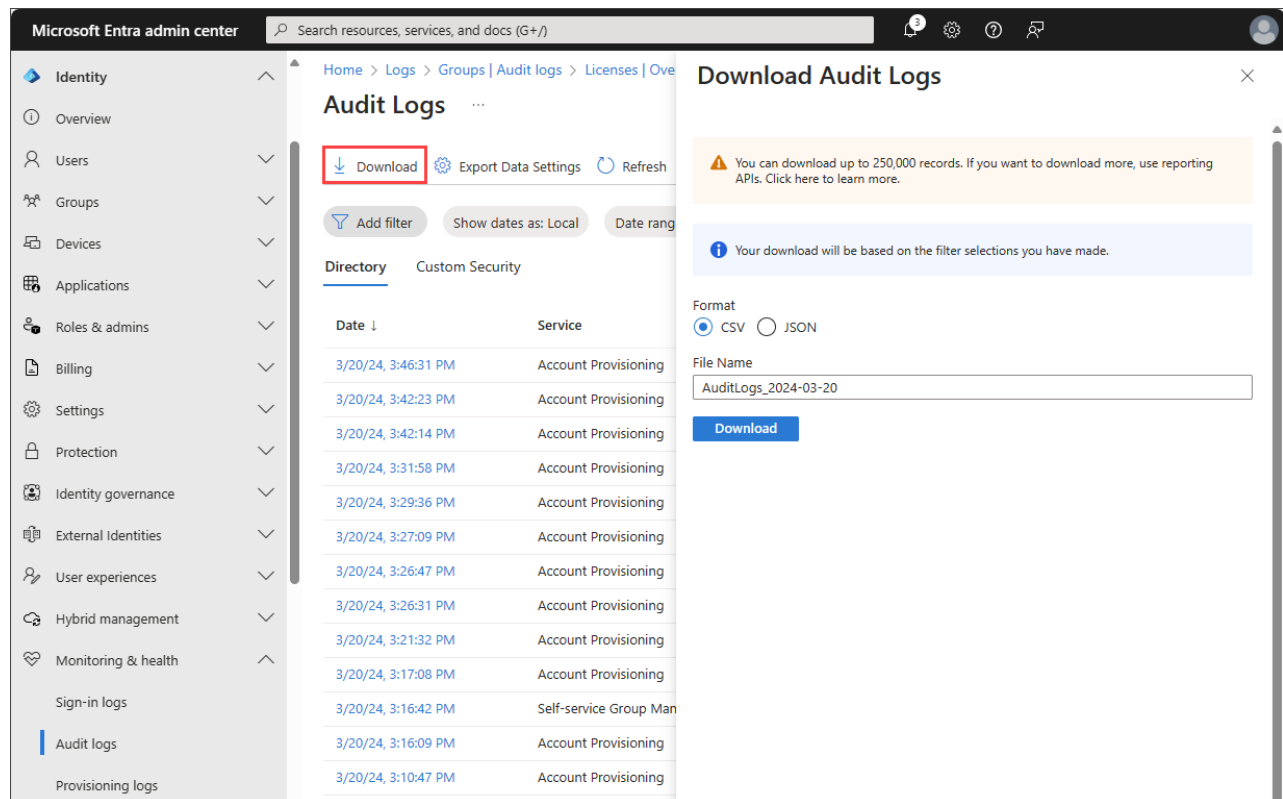


**Figure 3 — Audit-log download dialog (shown with CSV selected; select JSON for this workflow and use smaller date ranges for large exports).** Source: <https://learn.microsoft.com/en-us/entra/identity/monitoring-health/howto-download-logs>

Open relevant events and record the initiator, target, outcome, correlation ID and modified properties. Review the user agent where recorded; not every event contains it. Search listed applications as both initiators and targets. Follow any changes they made to other identities. Confirm authorization against owner and change records before classifying an unfamiliar event as malicious.

## 4 Check credentials and federation trusts

### Access for this section

| Operation                                                                                               | Review access examples                                                                                                                                                                                  | Remediation access examples                                                                                        |
|---------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| View App registrations and Certificates & secrets (client secrets, certificates, federated credentials) | Member users can normally read application properties; tenant restrictions or portal access may require an approved directory reader role. Secret values cannot be retrieved from existing credentials. | Not applicable — review only                                                                                       |
| Remove an unauthorized service-principal or application secret, certificate, or federated credential    | —                                                                                                                                                                                                       | Cloud Application Administrator or Application Administrator (application owners can act on applications they own) |

| Operation                                                                  | Review access examples | Remediation access examples                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------------------------------|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Remove a service-principal secret through Microsoft Graph (removePassword) | —                      | Delegated: Application.ReadWrite.All plus a supported user role, such as Cloud Application Administrator or Application Administrator, or ownership of the target. Application-only: Application.ReadWrite.OwnedBy for an owned target; Application.ReadWrite.All is broader. API permission alone does not establish delegated authority. |

The seven listed ConnectWise applications are vendor-owned multitenant applications. Their application registrations and vendor-managed credentials are maintained in ConnectWise's tenant and are not visible to customer administrators. Partners should review the corresponding enterprise applications and service principals in their own tenants, including locally configured credentials, permissions, owners, and associated audit activity where applicable. Sources: [Microsoft Graph removePassword](#); [Default user permissions](#)

- For locally registered applications, open App registrations → All applications, confirm the Application ID, and inspect Certificates & secrets, including client secrets, certificates and federated credentials.

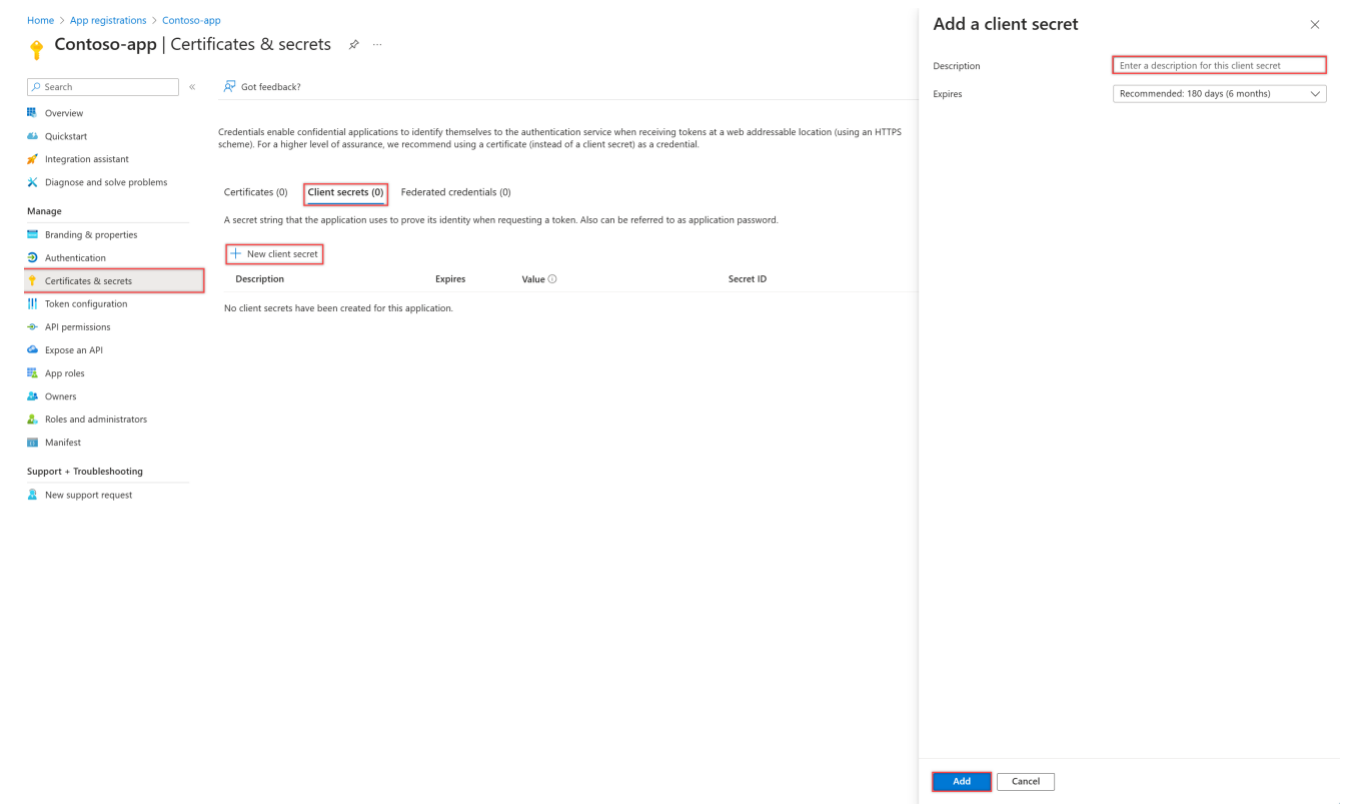


**Figure 4. App registrations and the Client secrets tab. The example shows an Add a client secret dialog; do not create a secret for this review. Inspect existing metadata only for registrations present in the tenant. Source: <https://learn.microsoft.com/en-us/entra/identity-platform/how-to-add-credentials>**

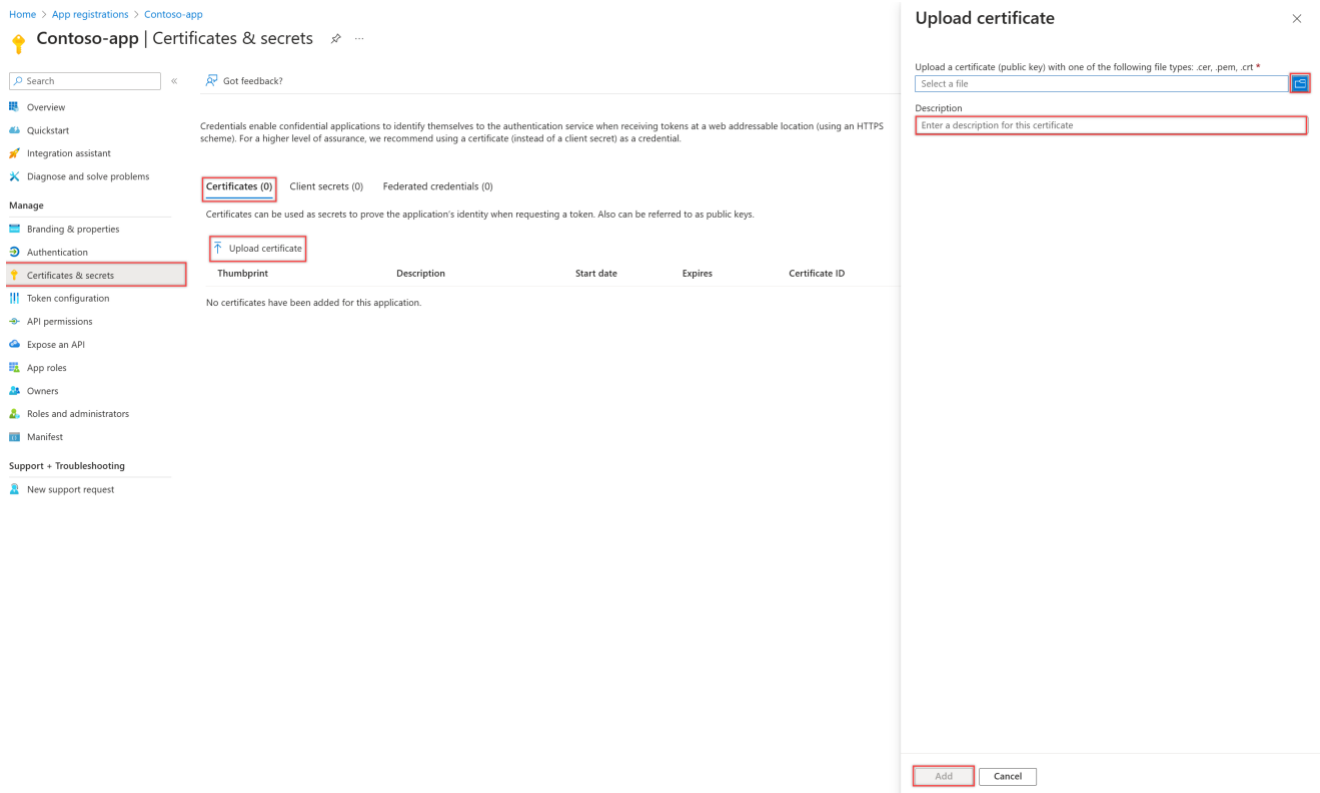


**Figure 5. Certificates tab.** The Upload certificate dialog is an interface reference, not an instruction to upload a certificate. Review existing thumbprints and validity dates and correlate with audit records. Source: <https://learn.microsoft.com/en-us/entra/identity-platform/how-to-add-credentials>

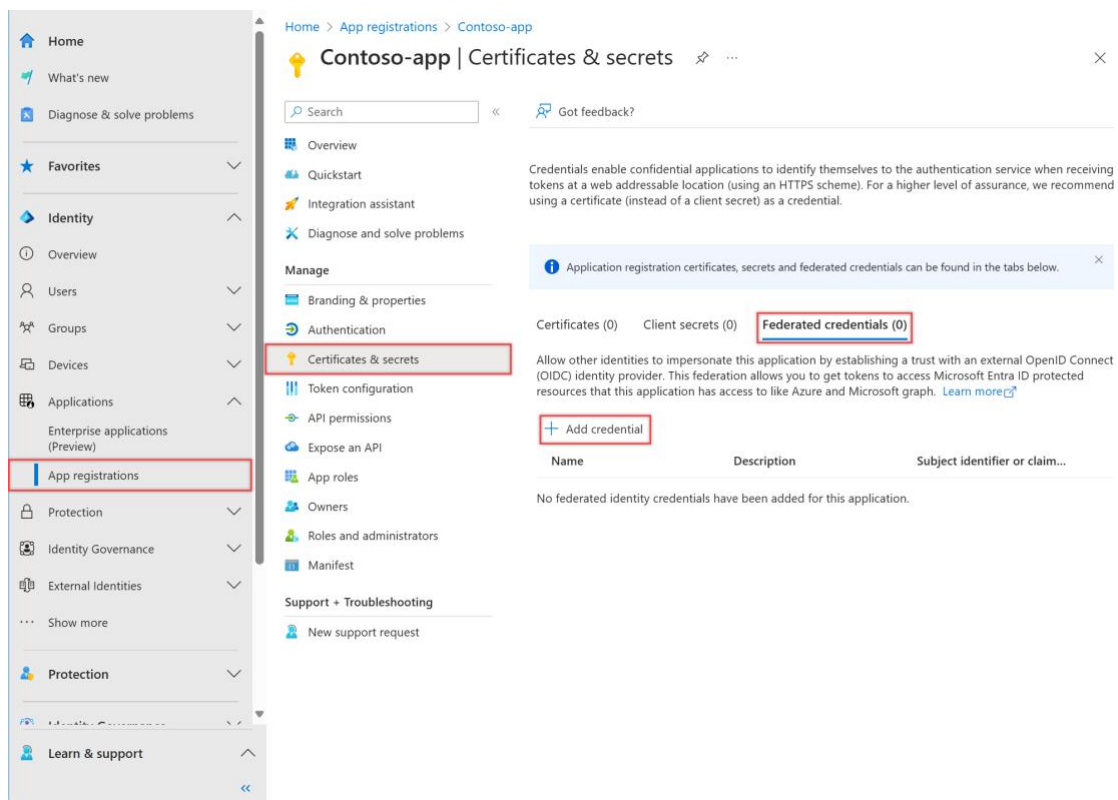


**Figure 6. Federated credentials tab for a locally registered application.** Review existing trusts and their issuer, subject, and audience. An empty tab in this example is not evidence about your tenant. Source: <https://learn.microsoft.com/en-us/entra/identity-platform/how-to-add-credentials>

- Record credential identifiers, thumbprints, validity periods and federation issuer/subject/audience. Compare them with approved configuration and audit events; validity dates alone do not establish when a credential was added.
- Review both the application registration and associated service principal. Vendor registrations may not appear in the customer's App registrations. An authorized responder can inspect service-principal credential metadata through Microsoft Graph.
- Preserve the evidence, then coordinate removal of unauthorized entries with the owner and incident response provider. Review all management and security integrations that could retain access, not just the seven listed applications.

For service-principal secrets, Microsoft Graph provides `removePassword` using the local Object ID and credential keyId; application-registration secrets use the application equivalent. Delegated Graph access requires both the API permission and a supported signed-in user role or ownership scope. Application-only access requires an appropriately consented application permission and ownership where applicable. Certificates and federated credentials use different operations; `removePassword` does not remove them. Preserve metadata, use an authorized responder, and verify removal. ConnectWise cannot be assumed to have permission to make changes inside your tenant.

## 5 Check roles applications owners and consent grants

### Access for this section

| Operation                                                | Review access examples                                                                                                                                  | Remediation access examples                                                                                                                 |
|----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| View role memberships and assignments                    | An authorized directory reader with visibility to the assignments; Security Reader is one example. Verify scope for privileged or eligible assignments. | Privileged Role Administrator (remove or change role assignments)                                                                           |
| View enterprise application owners and permission grants | Member users can normally read application configuration and grants; verify tenant restrictions and portal access.                                      | Cloud Application Administrator or Application Administrator (update owners); existing enterprise application owners can also update owners |

Have an authorized role administrator remediate confirmed unauthorized assignments. This workflow reviews and removes unauthorized access; it does not call for granting new application consent. Consent revocation permissions depend on the grant type and operation. Confirm the required directory role and API permissions before proceeding. Source: Microsoft Entra least privileged roles by task.

- Open Roles and administrators and review active application assignments, prioritizing Global Administrator, Privileged Role Administrator, Privileged Authentication Administrator, Application Administrator, Cloud Application Administrator, Exchange Administrator and SharePoint Administrator.

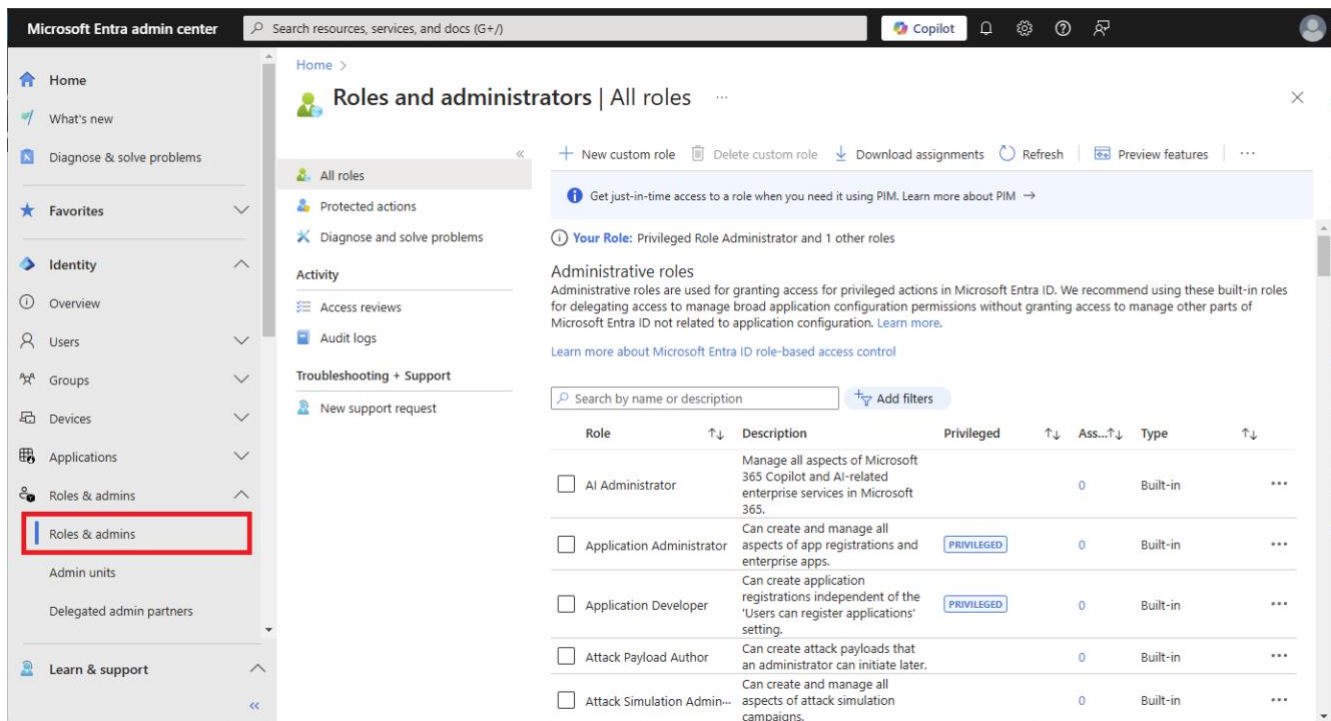


**Figure 7 — Entra ID → Roles & admins. Review active assignments, prioritizing Global Administrator, Privileged Role Administrator, Privileged Authentication Administrator, Application Administrator, Cloud Application Administrator, Exchange Administrator, and SharePoint Administrator; match local Object IDs against audit records. Source: <https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/manage-roles-portal>**

- Match local Object IDs and correlate changes with audit records. Separately inspect privileged user/group changes and applicable eligible assignments; do not assume application identities use the same activation process as people.
- Inspect recently created application registrations and enterprise applications, their Owners, and the enterprise application Permissions grants. Look for unauthorized owners, admin/user consent and elevated API permissions.

## Admin consent      User consent

| Search permissions |    |                      |    |                           |    |             |    |
|--------------------|----|----------------------|----|---------------------------|----|-------------|----|
| API Name           | ↑↓ | Claim value          | ↑↓ | Permission                | ↑↓ | Type        | ↑↓ |
| Microsoft Graph    |    |                      |    |                           |    |             |    |
| Microsoft Graph    |    | offline_access       |    | Maintain access to dat... |    | Delegated   |    |
| Microsoft Graph    |    | openid               |    | Sign users in             |    | Delegated   |    |
| Microsoft Graph    |    | Application.Read.All |    | Read all applications     |    | Application |    |

**Figure 8. Enterprise application Permissions view. Review existing Admin consent and User consent grants; do not grant additional consent during this investigation. Source: <https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/grant-admin-consent>**

- Preserve findings and have the authorized responder remove confirmed unauthorized assignments, owners or grants. For a malicious newly created application, disable it, retain evidence, and decide on deletion after investigation.

Review each access mechanism separately. If an MSP management identity has permissions across customers, assess which other tenants need investigation. A replacement legitimate credential does not remove an attacker-added credential, role, or consent grant.

## 6 Check policy changes

### Access for this section

| Operation                                              | Review access examples | Remediation access examples                                               |
|--------------------------------------------------------|------------------------|---------------------------------------------------------------------------|
| View Conditional Access policies and named locations   | Security Reader        | Not applicable                                                            |
| Correct Conditional Access policies or named locations | —                      | Conditional Access Administrator (Security Administrator also sufficient) |

Assess operational effects before altering legitimate controls. Sources: [Microsoft Entra least privileged roles by task](#)

- Open Protection → Conditional Access → Policies and Named locations. Review recent changes to policy state, assignments, exclusions and trusted locations against approved records.

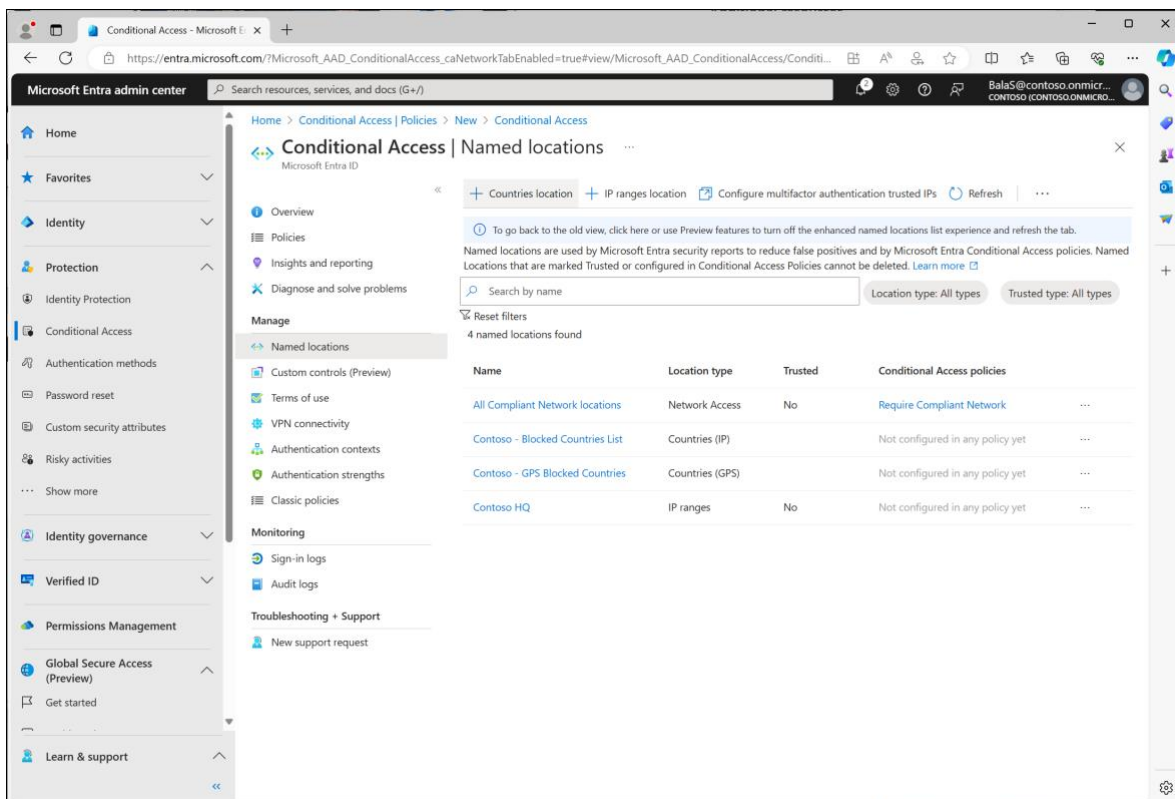


**Figure 9 — Protection → Conditional Access → Named locations.** Review recent additions or changes to locations and trusted locations against approved records. Source: <https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-assignment-network>

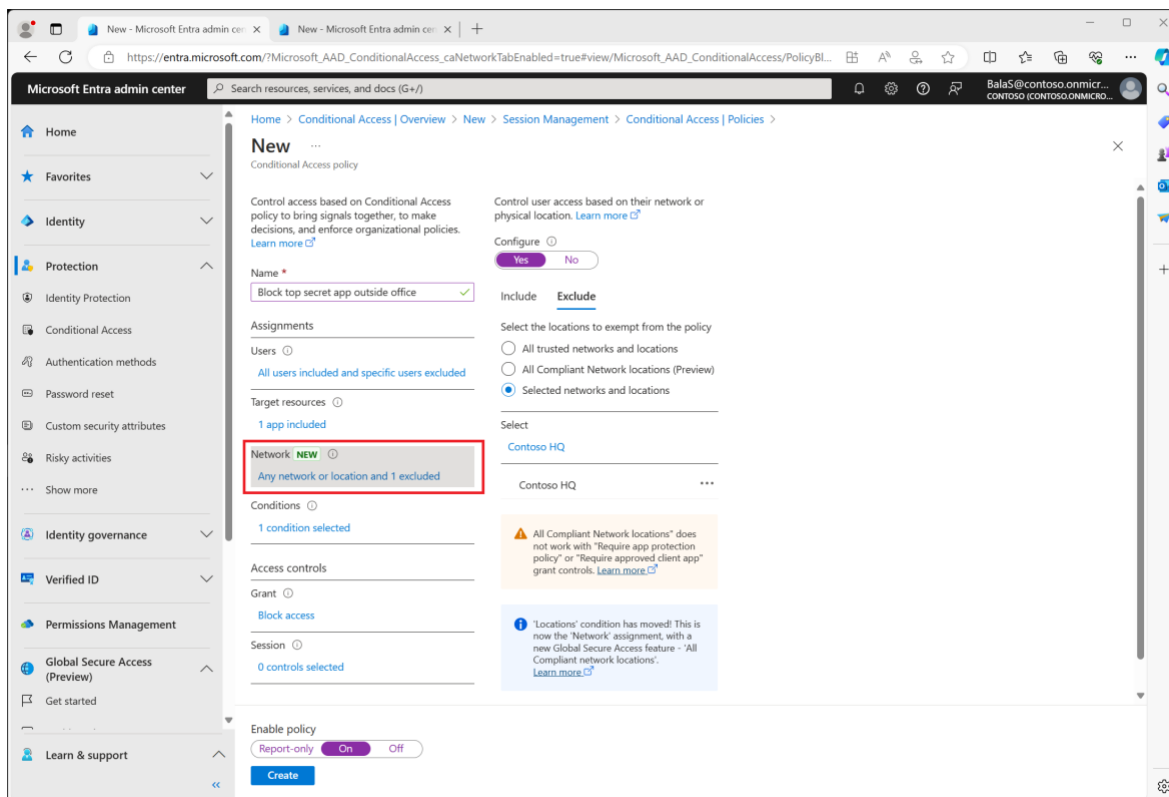


**Figure 10 — Conditional Access policy Network condition (interface reference, shown on policy creation). When reviewing existing policies, inspect state, assignments, exclusions, and selected networks and locations for unexplained changes.**

Source: <https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-assignment-network>

- Escalate unexplained changes and have the policy administrator correct confirmed unauthorized settings. Assess operational effects before altering legitimate controls.

This is a review for additional persistence or weakened controls. User policies do not automatically protect application-only authentication. Conditional Access for workload identities covers supported single-tenant service principals registered in the tenant, not third-party SaaS/multitenant apps. It is not a substitute for disabling affected connections.

## 7 Check Exchange and resource activity

### Access for this section

| Operation                                                                           | Review access examples                                      | Remediation access examples                                               |
|-------------------------------------------------------------------------------------|-------------------------------------------------------------|---------------------------------------------------------------------------|
| Search the audit log in Microsoft Purview Audit                                     | View-Only Audit Logs role (Audit Logs role also sufficient) | Not applicable                                                            |
| View transport rules, mailbox settings, and delegation in the Exchange admin center | View-Only Organization Management role group                | Not applicable                                                            |
| Change or remove mail flow (transport) rules                                        | —                                                           | Organization Management role group                                        |
| Change mailbox forwarding and other mailbox or recipient settings                   | —                                                           | Recipient Management role group (Organization Management also sufficient) |

| Operation                                                  | Review access examples                                                                                                                            | Remediation access examples                                                                                                       |
|------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Remove Full Access or Send As (permissions and delegation) | —                                                                                                                                                 | Organization Management role group                                                                                                |
| Inspect inbox rules with Get-InboxRule -IncludeHidden      | An Exchange role assignment permitting Get-InboxRule for the target mailbox. Ask the Exchange administrator to verify cmdlet and recipient scope. | An authorized assignment permitting Remove-InboxRule or Set-InboxRule for the target mailbox; verify scope before changing rules. |

Purview roles can be added to a custom role group to limit access to audit search. Sources: [Purview audit search](#); [Exchange Online feature permissions](#)

- In Purview Audit, search the investigation period for Exchange activities such as New-InboxRule, Set-InboxRule, Set-Mailbox, Add-MailboxPermission, Add-RecipientPermission, New-TransportRule and Set-TransportRule. Use corresponding friendly names where the search interface requires them.

| Audit > Audit search                                                                       |                |                      |                          |                      |                               |                       |                                    |
|--------------------------------------------------------------------------------------------|----------------|----------------------|--------------------------|----------------------|-------------------------------|-----------------------|------------------------------------|
| Search Query Information: Sun, 04 Jun 2023 00:30:00 GMT to Sun, 11 Jun 2023 02:00:00 GMT , |                |                      |                          |                      |                               |                       |                                    |
| Total Result Count: 2928338 items                                                          |                |                      |                          |                      |                               |                       |                                    |
| ↓ Export                                                                                   |                | 300 items Filter     |                          |                      |                               |                       |                                    |
| Date (UTC) ↓                                                                               | IP Address     | User                 | Record type              | Activity             | Item                          | Admin Units (Preview) | Details                            |
| Jun 11, 2023 1:41 AM                                                                       |                | ADMIN@EDISCO...      | ComplianceDLPSharePoint  | Matched DLP rule     | ffd39aaf-2c77-4ca8-a02f-ed... |                       |                                    |
| Jun 10, 2023 10:33 PM                                                                      |                | SecurityComplianc... | SecurityComplianceAlerts | AlertEntityGenerated | ADMIN@EDISCOF.ONML...         |                       |                                    |
| Jun 10, 2023 10:16 PM                                                                      | 104.42.253.135 | app@sharepoint       | SharePointFileOperation  | Accessed file        | WKC_3_1462060_5.txt           |                       | Accessed from "IPML_WKC_3_185"     |
| Jun 10, 2023 9:49 PM                                                                       |                | SecurityComplianc... | SecurityComplianceAlerts | AlertEntityGenerated | 7af559ce-3c8e-4e1d-b140-f...  |                       |                                    |
| Jun 10, 2023 12:54 PM                                                                      | 104.42.253.135 | app@sharepoint       | SharePointFileOperation  | Accessed file        | WKC_3_131165_6_F1588813-...   |                       | Accessed from "PreservationHold... |
| Jun 10, 2023 11:32 AM                                                                      | 104.42.253.135 | app@sharepoint       | SharePointFileOperation  | Accessed file        | WKC_3_21058_3.txt             |                       | Accessed from "IPML_WKC_3_395"     |
| Jun 10, 2023 11:18 AM                                                                      | 104.42.253.135 | app@sharepoint       | SharePointFileOperation  | Accessed file        | WKC_3_2105044_10.txt          |                       | Accessed from "IPML_WKC_3_395"     |
| Jun 10, 2023 7:12 AM                                                                       |                | SecurityComplianc... | SecurityComplianceAlerts | AlertTriggered       | b9ca924a-fee6-f06c-9400-0...  |                       |                                    |
| Jun 10, 2023 6:58 AM                                                                       | 104.42.253.135 | app@sharepoint       | SharePointFileOperation  | Accessed file        | WKC_3_1701093_37.txt          |                       | Accessed from "IPML_WKC_3_274"     |
| Jun 10, 2023 6:12 AM                                                                       | 104.42.253.135 | app@sharepoint       | SharePointFileOperation  | Accessed file        | WKC_3_17857_4.txt             |                       | Accessed from "IPML_WKC_3_301"     |

**Figure 11 — Microsoft Purview Audit search results.** Search the investigation period for Exchange activities such as New-InboxRule, Set-InboxRule, Set-Mailbox, Add-MailboxPermission, and transport-rule changes, then export findings. Source: <https://learn.microsoft.com/en-us/purview/audit-search>

- Investigate unexpected external forwarding, rules that hide or delete messages, new Full Access or Send As rights, and transport-rule changes. Validate against authorized changes.
- Use Exchange admin center → Mail flow → Rules for transport rules and Recipients → Mailboxes for forwarding/delegation settings. Inspect inbox rules separately with authorized Exchange Online PowerShell where needed, including Get-InboxRule -Mailbox <mailbox> -IncludeHidden for hidden rules.

**Figure 12. Transport-rule creation wizard shown only to identify rule conditions and actions. Inspect existing transport rules in Mail flow and review mailbox inbox rules separately with authorized Exchange Online tools. Do not create a rule for this review. Source: <https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/whats-new-in-updated-mail-flow-rules-ux-in-eac>**

- Where available and licensed, correlate MailItemsAccessed, other Microsoft 365 audit records, security alerts and previously collected Graph activity with suspicious events. Include relevant SharePoint, OneDrive and Teams activity.

Preserve evidence and remediate confirmed unauthorized changes through your response provider. Application authentication alone does not establish data copying. Normal backup reads and limited logging may make attribution difficult. Enabling logging now does not recover events that were never recorded; document that uncertainty.

## 8 Review remaining connections and record the outcome

- Search Enterprise applications for other ConnectWise and SkyKick identities. Record their IDs, owners, permissions and purpose. Assess their legitimacy and risk with your security provider and ConnectWise; do not infer compromise from a name alone.
- Keep affected or suspicious connections disabled while the review continues. Preserve evidence and assess business impact before removing unrelated legitimate integrations.
- For each tenant, record log coverage, findings, containment times, credential/role/consent/policy/mailbox remediation, unresolved questions, and your response owner.
- Check the last successful backup recovery point and assess the protection gap while services are unavailable. Follow formal restoration guidance before reconnecting; after authorized restoration, verify workload connections and successful backup jobs.

Escalate unauthorized credentials, privileged assignments, suspicious successful activity or evidence of data access to your incident response provider immediately. Send relevant findings to

**SecurityPartnerSupport@ConnectWise.com**, including tenant and application identifiers, UTC timestamps, event/correlation IDs and a description. Do not include passwords, private keys, tokens or other secrets.

A completed checklist records the work performed and evidence available. It does not guarantee that a tenant was unaffected. Please use the Trust Center for current status and guidance. Contact Partner Care for service assistance and report suspicious activity to **SecurityPartnerSupport@ConnectWise.com**.

## Microsoft technical references

[Application sign-in disablement](#)

[Entra log download and retention](#)

[Compromised application investigation](#)

[Audit activity reference](#)

[Service principal secret removal](#)

[Workload Conditional Access scope](#)

[Inbox rule investigation](#)