

EXPIRY REPORT

# Executive summary

Tailspin Toys | 10 October 2026 | Internal assessment

OVERALL POSTURE

Expiries require attention

These figures cover the 23 items this run read; 0 ignored items stay out of them and are listed in the technical report, so its totals differ by design.

11

Fine

1

Expired

4

Expiring soon

7

Attention

23

items

1

Already expired

11

Fine on the run date

4

Expire in 30 days

23

Watched items

The leading areas for review are App registration secrets and certificates, Intune certificates and tokens, enterprise application credentials. The run found 1 expired and 4 expiring within 30 days among 23 watched items. Days left are counted from the run date, not from today. The report does not establish that a renewal is under way unless the item was marked handled in the portal.

WHERE TO FOCUS

01

App registration secrets and certificates

2 items due · EXPIRED

02

Intune certificates and tokens

2 items due · SOON

03

Enterprise application credentials

1 item due · SOON

DATED ITEMS BY DAYS LEFT



RUN SNAPSHOT

| COLLECTION                                                                                   | HANDLING                                                  | OWNERS                                              | COVERAGE LIMITS                                    | SINCE LAST RUN                         |
|----------------------------------------------------------------------------------------------|-----------------------------------------------------------|-----------------------------------------------------|----------------------------------------------------|----------------------------------------|
| 212 applications, 488 enterprise applications, 2 domains read<br>Read-only; run from the app | 0 handled / 0 ignored<br>Decisions recorded in the portal | 2 without an owner<br>Assign in Entra or the portal | 1 part not read<br>Grant the permission, run again | First run<br>No earlier run to compare |

THE MANAGEMENT DECISION

Assign an owner to every open item, agree who renews what before each date, and keep the schedule running so the next expiry is a warning, not an outage. Ignored items stay on the report with their reason.

## PRIORITIZED FINDINGS &amp; RECOMMENDATIONS

# Priority workstreams

Ordered by the nearest expiry. Who renews what, and when, remains the owner's review.

## 01 App registration secrets and certificates



EXPIRED

4 items; 1 expired, 1 within 30 days. Legacy ticketing: expired 11 days ago. Payroll sync: 8 days left.

**Action** Add a new secret or certificate in the app registration, update the integration that uses it, then remove the old one. The next run shows the new date.

**Why it matters** When an application's secret expires, every sign-in and integration through it stops at that moment.

**The decision** Ask the owner to add a new secret before the date and confirm it on the next run.

## 02 Intune certificates and tokens



SOON

5 items; 2 within 30 days. Apple MDM push certificate (the certificate Apple requires before devices can be managed): 5 days left. Certificate connector SRV-PKI01: 25 days left.

**Action** Renew in the Intune admin center under Tenant administration, with the same Apple or Google account that created the token.

**Why it matters** When an Apple or Google token expires, phones and laptops stop enrolling and can lose management.

**The decision** Renew with the same Apple or Google account before the date.

## 03 Enterprise application credentials



SOON

2 items; 1 within 30 days. HR portal SSO: 22 days left.

**Action** Renew the certificate in the enterprise application's single sign-on settings and upload the new one on the application's side before the old one ends.

**Why it matters** When a signing certificate expires, staff can no longer sign in to the application that relies on it.

**The decision** Ask the owner to renew it on both sides before the date.

## PRIORITIZED FINDINGS &amp; RECOMMENDATIONS

# Supporting workstreams

Ordered by the nearest expiry. Who renews what, and when, remains the owner's review.

## 04 Applications without an owner

2 items; 2 need attention. HR portal SSO: no owner. Intranet SharePoint connector: no owner.

**ATTENTION**

**Action** Assign an owner in the Entra admin center or in the portal, so that Remind knows whom to warn before the next expiry.

**Why it matters** Nobody is warned about an item without an owner, so its expiry is found when something stops.

**The decision** Name an owner for each one now; it takes a minute in Entra or in the portal.

## 05 Unused applications

2 items; 1 needs attention. Old CRM import: last sign-in 2026-03-02.

**ATTENTION**

**Action** Confirm with the owner that the application is no longer used, then remove its credentials or the application itself.

**Why it matters** A credential nobody uses still opens a door, and if it leaks nobody notices.

**The decision** Ask the owner whether the application is still needed; remove it or its credentials.

## 06 Domains and mail records

7 items; 3 need attention. tailspin-mail.example: DKIM (the signature that proves mail really came from the domain) not enabled. tailspin.example: SPF (the list of servers allowed to send mail for the domain) differs.

**ATTENTION**

**Action** Correct the DNS record at the registrar to what Microsoft publishes and rotate DKIM in the Defender portal; check the next run after DNS has propagated.

**Why it matters** A wrong mail record means the company's mail bounces or lands in spam, often without a warning.

**The decision** Have the DNS host fix the record and check that the next run shows it as fine.

## PRIORITIZED FINDINGS &amp; RECOMMENDATIONS

# Supporting workstreams

Ordered by the nearest expiry. Who renews what, and when, remains the owner's review.

## 07 Entra Connect and cloud sync

ATTENTION

1 item; 1 needs attention. Entra Connect (the service that copies on-premises accounts to Microsoft 365) sync: 2 sync errors.

**Action** Check the Entra Connect or cloud sync server: the service, the connector account and the last completed synchronization.

**Why it matters** If directory sync stalls, password changes and new staff do not reach Microsoft 365.

**The decision** Have IT check the sync server today; it is usually a stopped service or an account.

## 08 Conditional Access references

NOT READ

Not read in this run: This part was not read in this run: the Conditional Access (the sign-in rules of the tenant) permission was not granted. Run again with that permission to include it.

**Action** Grant the permission at the next run; the result is a coverage limit, not a pass.

**Why it matters** This part was not read in this run, so it gives no assurance either way.

**The decision** Grant the missing permission before the next run so that this part is included.

DELIVERY PLAN & ASSESSMENT CONFIDENCE

# From findings to action

Proposed timing starts when the plan is accepted. Owners and exceptions remain to be agreed.

01

## First 30 days

Renew everything already expired or due within 30 days. Assign an owner to every item without one. Record handled or ignored for each decision in the portal.

02

## Days 31-60

Renew the items due within 60 days. Correct the mail records and the directory synchronization. Remove unused applications once their owners confirm.

03

## Days 61-90

Set the schedule: daily runs, warning addresses per tenant and a review of ignored items. Close an item only when the next run shows its new date.

## COVERAGE & DECISIONS

### COLLECTION

Not read in this run: the Conditional Access policies. A part that was not read gives no assurance; grant the permission and run again.

### CONFIDENCE

23 items were read from 212 applications, 488 enterprise applications and 2 domains on 10 October 2026. Days left are counted from that date. No trend is inferred without an earlier run.

### BOUNDARIES

Remind reads the names and dates of credentials, never their values, and never renews anything. Secrets kept outside Microsoft 365, certificates on servers, third-party services and licenses are outside scope. DNS records are read from the computer that ran the app, so a split DNS can differ from what the Internet sees.

### ACCEPTANCE

An ignored item stays on the report with its reason. A handled item returns to open when the next run still finds the old date after the expected date. Require an owner, a date and a note for each exception.

Sample report: fictional organization

This report lists the credentials, certificates, tokens and records read from the Microsoft 365 tenant named in it, at the time shown, within the limits in its coverage section. It is a point-in-time review, not an audit opinion, a certification or a guarantee that nothing else will expire or break. Days left are counted from the run date. Findings and guidance are informational; renewals are made by the customer, and nothing in this report changes a tenant. Parts that could not be read are reported as not read, not as fine. Microsoft behavior can change after the run date. Prepared by GlacierPoint Technologies LLC under the GlacierPoint Remind Terms of Service.

## REPORT NAVIGATION

# Contents

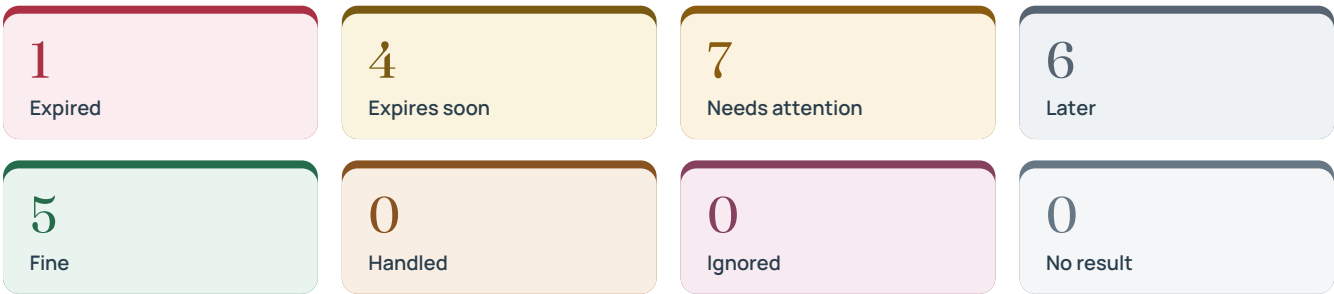
Pages 1-5: executive brief. The entries below link to the technical sections, the findings, the scope sections and the tenant inventory.

|                         |    |
|-------------------------|----|
| Scope & interpretation  | 7  |
| Due within the window   | 8  |
| Item type matrices      | 10 |
| Findings & next actions | 13 |
| App registrations       | 16 |
| Enterprise applications | 17 |
| Domains                 | 18 |
| Intune                  | 19 |
| Directory               | 20 |
| Tenant inventory        | 21 |
| Methodology references  | 23 |

READ THIS FIRST

# Scope & interpretation

Tenant: tailspin.onmicrosoft.com (Tailspin Toys)  
Signed in as: admin@tailspin.example  
Run finished UTC: 2026-10-10T08:02:41Z  
App: 0.1.0 | Technical format: 3.0  
Window: items expiring within 30 days count as due; applications unused for 90 days count as unused  
Sample report: fictional organization  
Not read in this run: conditional access. This is a coverage limit of the run, not a fine result for those parts.



These totals count all 23 items, ignored ones included. The executive brief leaves ignored items out, so its totals differ by design.

|           |                                                                                                                                         |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------|
| EXPIRED   | Expired. The date has passed; whatever depends on this item has stopped or is about to.                                                 |
| SOON      | Expires soon. The date falls within the tenant's window; renew before it.                                                               |
| ATTENTION | Needs attention. No date, but the facts say something is wrong: a missing owner, an unused application, a wrong record, a stalled sync. |
| LATER     | Later. Dated beyond the window; listed so that the owner sees it coming.                                                                |
| FINE      | Fine. Nothing wrong on the run date.                                                                                                    |
| HANDLED   | Handled. Marked in the portal as being renewed, with the date the new value should show up; warnings pause until then.                  |
| IGNORED   | Ignored. Marked in the portal as a decision, with a reason; warnings stop, the row stays on the report.                                 |
| NO RESULT | No result. An absent matrix intersection: nothing of this type lives in that scope, or it was not read.                                 |

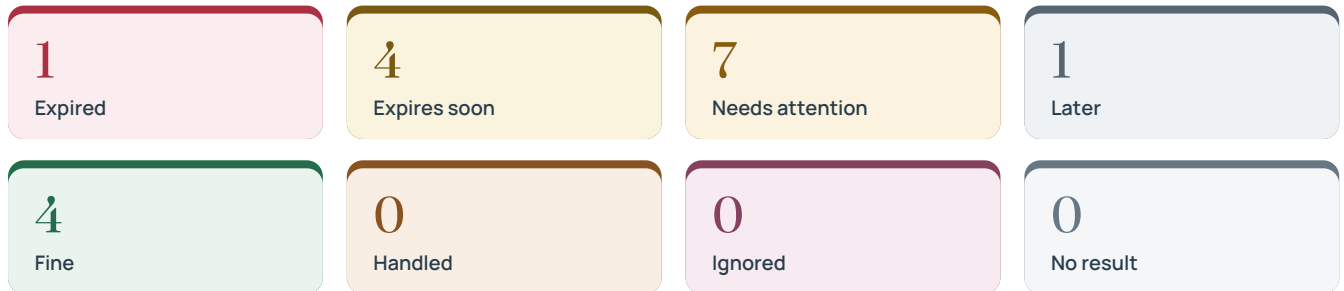
NO RESULT marks an absent matrix intersection; it is not a fine result and is excluded from the counts. Days left are whole days from the run's end to the item's end date; an item without a date is judged on its facts. Every item keeps its row; a handled or ignored item keeps its state in the facts.

Collection is read-only. Remind reads the names and dates of credentials, never their values; it never holds a private key and never renews anything. Owners are the application's owners in Entra, or an owner assigned in the portal. DNS records are read from the computer that ran the app with its system resolver. Items Microsoft does not return (a secret created by a first-party service, a certificate on a server) are outside scope.

## REPORTING WINDOW

## Due within the window

The window of 30 days covers 9 of the 15 item types found (17 of 23 items). The executive brief is computed from the live rows of every type; every item, due or not, appears unchanged in the sections that follow.



## Due item types / scopes 1-4 of 5

App registrations | Enterprise applications | Domains | Intune

| ID         | ITEM TYPE                         | App registrations | Enterprise applications | Domains   | Intune    |
|------------|-----------------------------------|-------------------|-------------------------|-----------|-----------|
| APP - SEC  | App registration secret           | EXPIRED           | NO RESULT               | NO RESULT | NO RESULT |
|            |                                   | SOON              |                         |           |           |
|            |                                   | LATER             |                         |           |           |
| SP - SAML  | SAML signing certificate          | NO RESULT         | SOON                    | NO RESULT | NO RESULT |
| OWN - NONE | Application without an owner      | ATTENTION         | ATTENTION               | NO RESULT | NO RESULT |
| APP - IDLE | Unused application                | NO RESULT         | ATTENTION               | NO RESULT | NO RESULT |
|            |                                   |                   | FINE                    |           |           |
| DOM - DNS  | DNS record (MX, SPF, DKIM, DMARC) | NO RESULT         | NO RESULT               | ATTENTION | NO RESULT |
|            |                                   |                   |                         | 2 items   |           |
|            |                                   |                   |                         | FINE      |           |
| DOM - DKIM | DKIM signing in Exchange Online   | NO RESULT         | NO RESULT               | ATTENTION | NO RESULT |
|            |                                   |                   |                         | FINE      |           |
| INT - APNS | Apple MDM push certificate        | NO RESULT         | NO RESULT               | NO RESULT | SOON      |
| INT - CONN | Certificate connector             | NO RESULT         | NO RESULT               | NO RESULT | SOON      |
| DIR - SYNC | Entra Connect synchronization     | NO RESULT         | NO RESULT               | NO RESULT | NO RESULT |

## Due item types / scopes 5-5 of 5

Directory

| ID         | ITEM TYPE                         | Directory |
|------------|-----------------------------------|-----------|
| APP - SEC  | App registration secret           | NO RESULT |
| SP - SAML  | SAML signing certificate          | NO RESULT |
| OWN - NONE | Application without an owner      | NO RESULT |
| APP - IDLE | Unused application                | NO RESULT |
| DOM - DNS  | DNS record (MX, SPF, DKIM, DMARC) | NO RESULT |
| DOM - DKIM | DKIM signing in Exchange Online   | NO RESULT |
| INT - APNS | Apple MDM push certificate        | NO RESULT |
| INT - CONN | Certificate connector             | NO RESULT |
| DIR - SYNC | Entra Connect synchronization     | ATTENTION |

## COVERAGE AT A GLANCE

# Item type matrices

## App registration secrets and certificates

A secret or certificate has an end date. When it passes, every integration that signs in with it stops, usually without a warning from Microsoft.

Scopes 1-1 of 1: App registrations

| ID        | ITEM TYPE                    | App registrations                                   |
|-----------|------------------------------|-----------------------------------------------------|
| APP - SEC | App registration secret      | <div>EXPIRED</div> <div>SOON</div> <div>LATER</div> |
| APP - CRT | App registration certificate | <div>LATER</div>                                    |

## Enterprise application credentials

Single sign-on to a third-party application relies on a signing certificate with an end date. When it passes, staff can no longer sign in to that application.

Scopes 1-1 of 1: Enterprise applications

| ID        | ITEM TYPE                          | Enterprise applications |
|-----------|------------------------------------|-------------------------|
| SP - CRT  | Enterprise application certificate | <div>LATER</div>        |
| SP - SAML | SAML signing certificate           | <div>SOON</div>         |

## Applications without an owner

Microsoft warns the owners of an application before its credentials expire. An application with no owner warns nobody.

Scopes 1-2 of 2: App registrations | Enterprise applications

| ID         | ITEM TYPE                    | App registrations    | Enterprise applications |
|------------|------------------------------|----------------------|-------------------------|
| OWN - NONE | Application without an owner | <div>ATTENTION</div> | <div>ATTENTION</div>    |

## Unused applications

An application nobody has used in a long time still holds working credentials. If one leaks, nobody notices. Confirm it is still needed or remove it.

Scopes 1-1 of 1: Enterprise applications

| ID         | ITEM TYPE          | Enterprise applications |
|------------|--------------------|-------------------------|
| APP - IDLE | Unused application | ATTENTION<br>FINE       |

## Domains and mail records

DNS records do not expire, but they break. A domain move, a new mail service or a rebuilt website can delete or overwrite them, and nobody notices until mail bounces or lands in spam. Remind reads the MX, SPF, DKIM and DMARC records as the Internet sees them and compares them with what Microsoft 365 expects, so a change shows here before it shows as lost mail.

Scopes 1-1 of 1: Domains

| ID         | ITEM TYPE                         | Domains                                 |
|------------|-----------------------------------|-----------------------------------------|
| DOM - DNS  | DNS record (MX, SPF, DKIM, DMARC) | ATTENTION<br>2 items<br>FINE<br>2 items |
| DOM - DKIM | DKIM signing in Exchange Online   | ATTENTION<br>FINE                       |
| DOM - FED  | Federation signing certificate    | LATER                                   |

## Intune certificates and tokens

Apple and Google require a certificate or token that Microsoft cannot renew for you. When one expires, phones and laptops stop enrolling and can fall out of management.

Scopes 1-1 of 1: Intune

| ID         | ITEM TYPE                    | Intune |
|------------|------------------------------|--------|
| INT - APNS | Apple MDM push certificate   | SOON   |
| INT - DEP  | Apple Business Manager token | LATER  |
| INT - VPP  | Apple VPP token              | LATER  |
| INT - PLAY | Managed Google Play binding  | FINE   |
| INT - CONN | Certificate connector        | SOON   |

## Entra Connect and cloud sync

Directory synchronization copies on-premises accounts and password changes to Microsoft 365. When it stalls, new staff cannot sign in and password changes do not take effect in the cloud.

Scopes 1-1 of 1: Directory

| ID       | ITEM TYPE                     | Directory |
|----------|-------------------------------|-----------|
| DIR-SYNC | Entra Connect synchronization | ATTENTION |

## SHARED GUIDANCE / ITEM-SPECIFIC EVIDENCE

## Findings &amp; next actions

Each item type is explained once. Every expired, due or attention item appears below with where it lives, its owners and what the run recorded; fine, later, handled and ignored items are retained in the scope sections. Handling is separate from the item's state.

|                                                                                             |                                                                                                                                                                                                                                             |
|---------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>APP - SEC</b>                                                                            | <b>App registration secret</b>                                                                                                                                                                                                              |
| <b>GUIDANCE</b>                                                                             | Add a new secret or certificate in the app registration (Microsoft Entra admin center, App registrations, Certificates & secrets), update the integration that uses it, then remove the old one. Remind shows the new date on the next run. |
| <b>NEXT ACTION</b>                                                                          | Add the new secret, update the integration, confirm the sign-ins, then delete the old secret.                                                                                                                                               |
| <b>Legacy ticketing</b><br>App registrations<br><b>EXPIRED</b><br>Owners: IT shared mailbox | Credential "api" (key id ending 44d1). expires 2026-09-30 (expired 11 days ago).<br>Why: sign-ins and API calls through this application stop.                                                                                              |
| <b>Payroll sync</b><br>App registrations<br><b>SOON</b><br>Owners: Ana Ruiz                 | Credential "prod-2024" (key id ending a1f3). expires 2026-10-19 (8 days left).<br>Why: sign-ins and API calls through this application stop.                                                                                                |

|                                                                            |                                                                                                                                                                                                                       |
|----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>INT - APNS</b>                                                          | <b>Apple MDM push certificate</b>                                                                                                                                                                                     |
| <b>GUIDANCE</b>                                                            | Renew in the Microsoft Intune admin center under Tenant administration, Connectors and tokens, with the same Apple ID or Google account that created the token. A renewal with a different account unenrolls devices. |
| <b>NEXT ACTION</b>                                                         | Renew the certificate in the Intune admin center with the same Apple ID; a new Apple ID unenrolls every device.                                                                                                       |
| <b>Apple MDM push certificate</b><br>Intune<br><b>SOON</b><br>Owners: none | Apple MDM push certificate. expires 2026-10-16 (5 days left).<br>Why: device enrollment and management of Apple devices stop.                                                                                         |

|                                                 |                                                                                                                                                                                                                 |
|-------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SP - SAML</b>                                | <b>SAML signing certificate</b>                                                                                                                                                                                 |
| <b>GUIDANCE</b>                                 | Renew the certificate in the enterprise application's single sign-on settings (Microsoft Entra admin center, Enterprise applications) and upload the new one on the application's side before the old one ends. |
| <b>NEXT ACTION</b>                              | Create a new signing certificate, upload it to the application's identity provider settings, then activate it.                                                                                                  |
| <b>SP - SAML</b>                                | <b>SAML signing certificate</b>                                                                                                                                                                                 |
| <b>HR portal SSO</b><br>Enterprise applications | SAML signing certificate. expires 2026-11-02 (22 days left).<br>Why: SAML sign-in to this application stops.                                                                                                    |

## SP - SAML

## SAML signing certificate

SOON

Owners: none

## INT - CONN

## Certificate connector

## GUIDANCE

Renew in the Microsoft Intune admin center under Tenant administration, Connectors and tokens, with the same Apple ID or Google account that created the token. A renewal with a different account unenrolls devices.

## NEXT ACTION

Renew the connector on its server and confirm it reports as active in the Intune admin center.

**Certificate connector  
SRV-PKI01**

Intune

SOON

Owners: none

certificate connector, state active, version 6.2405.0.0. expires 2026-11-05 (25 days left).  
Why: certificates are no longer issued to devices.  
Where: SRV-PKI01

## DOM - DKIM

## DKIM signing in Exchange Online

## GUIDANCE

Update the record at the registrar or DNS host to what Microsoft publishes (Microsoft 365 admin center, Settings, Domains), and rotate DKIM in the Microsoft Defender portal under Email authentication settings. Changes show after DNS has propagated.

## NEXT ACTION

Enable DKIM signing for the domain in the Defender portal and publish the two selector records.

**tailspin-mail.example**

Domains

ATTENTION

Owners: none

DKIM signing not enabled, selector selector1.  
Why: signed mail from this domain fails verification.

## DOM - DNS

## DNS record (MX, SPF, DKIM, DMARC)

## GUIDANCE

Update the record at the registrar or DNS host to what Microsoft publishes (Microsoft 365 admin center, Settings, Domains), and rotate DKIM in the Microsoft Defender portal under Email authentication settings. Changes show after DNS has propagated.

## NEXT ACTION

Set the record at the registrar to the value Microsoft publishes, then check the next run.

**tailspin.example**

Domains

ATTENTION

Owners: none

SPF record differs: found v=spf1 include:spf.protection.outlook.com  
include:\_spf.oldhost.example -all; expected v=spf1 include:spf.protection.outlook.com  
-all.  
Why: mail from this domain may be rejected or marked as spam.

**tailspin.example**

Domains

ATTENTION

Owners: none

DMARC record missing: nothing published.  
Why: mail from this domain may be rejected or marked as spam.

|                                                                            |                                                                                                                                                                                                                         |
|----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>DIR - SYNC</b>                                                          | <b>Entra Connect synchronization</b>                                                                                                                                                                                    |
| <b>GUIDANCE</b>                                                            | Check the Entra Connect or cloud sync server: the service is running, the connector account can sign in, and the last synchronization completed. The Entra admin center, Entra Connect, Connect Sync, shows the errors. |
| <b>NEXT ACTION</b>                                                         | Check the sync service and the connector account on the server; review the errors in the Entra admin center.                                                                                                            |
| <b>Entra Connect sync</b><br>Directory<br><b>ATTENTION</b><br>Owners: none | Last synchronization 2026-10-10 01:12 UTC. 2 sync errors.<br>Why: password changes and new users stop reaching the cloud.<br>Where: Tailspin Toys                                                                       |

|                                                                                               |                                                                                                                                            |
|-----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <b>OWN - NONE</b>                                                                             | <b>Application without an owner</b>                                                                                                        |
| <b>GUIDANCE</b>                                                                               | Assign an owner in the Microsoft Entra admin center (the application's Owners page), or assign one here so that Remind knows whom to warn. |
| <b>NEXT ACTION</b>                                                                            | Assign an owner in Entra, or in the portal so that warnings reach a person.                                                                |
| <b>HR portal SSO</b><br>Enterprise applications<br><b>ATTENTION</b><br>Owners: none           | 1 credential and no owner in Entra.<br>Why: nobody is warned before its credentials expire.                                                |
| <b>Intranet SharePoint connector</b><br>App registrations<br><b>ATTENTION</b><br>Owners: none | 1 credential and no owner in Entra.<br>Why: nobody is warned before its credentials expire.                                                |

|                                                                                            |                                                                                                                                                                                          |
|--------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>APP - IDLE</b>                                                                          | <b>Unused application</b>                                                                                                                                                                |
| <b>GUIDANCE</b>                                                                            | Confirm with the application's owner that it is no longer used, then remove its credentials or the application itself. A credential nobody uses is an exposure, not only an outage risk. |
| <b>NEXT ACTION</b>                                                                         | Confirm with the owner; remove the credentials or the application, or record the decision as ignored with a reason.                                                                      |
| <b>Old CRM import</b><br>Enterprise applications<br><b>ATTENTION</b><br>Owners: Ben Okafor | Last sign-in 2026-03-02.<br>Why: a credential nobody uses is an exposure.                                                                                                                |

## SCOPE SUMMARY / EVIDENCE INDEX

## App registrations

1

Expired

1

Expires soon

1

Needs attention

2

Later

0

Fine

0

Handled

0

Ignored

0

No result

Dated items by days left: 1 expired, 0 within 7 days, 1 within 30 days, 2 later.

## Findings index / click a type to open its card

APP-SEC

EXPIRED

APP-SEC

SOON

OWN-NONE

ATTENTION

## Fine, later, handled and ignored items

| TYPE / OUTCOME   | ITEM                                                                                                                                       |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| APP-CRT<br>LATER | <b>Warehouse scanner API</b><br>Credential "CN=warehouse-api" (key id ending 9c0e). expires 2026-11-28 (48 days left). Owners: Ben Okafor. |
| APP-SEC<br>LATER | <b>Intranet SharePoint connector</b><br>Credential "unnamed" (key id ending b7e2). expires 2027-03-14 (154 days left). Owners: none.       |

## SCOPE SUMMARY / EVIDENCE INDEX

## Enterprise applications

0

Expired

1

Expires soon

2

Needs attention

1

Later

1

Fine

0

Handled

0

Ignored

0

No result

Dated items by days left: 0 expired, 0 within 7 days, 1 within 30 days, 1 later.

## Findings index / click a type to open its card

SP-SAML

SOON

OWN-NONE

ATTENTION

APP-IDLE

ATTENTION

## Fine, later, handled and ignored items

## TYPE / OUTCOME

## ITEM

SP-CRT

LATER

## Expense tool

Credential "CN=expense-tool" (key id ending e8a7). expires 2027-01-20 (101 days left). Owners: Ana Ruiz.

APP-IDLE

FINE

## Event registration bot

Last sign-in 2026-10-01. Owners: none.

## SCOPE SUMMARY / EVIDENCE INDEX

## Domains

0

Expired

0

Expires soon

3

Needs attention

1

Later

3

Fine

0

Handled

0

Ignored

0

No result

Dated items by days left: 0 expired, 0 within 7 days, 0 within 30 days, 1 later.

## Findings index / click a type to open its card

DOM-DKIM

ATTENTION

DOM-DNS

ATTENTION

DOM-DNS

ATTENTION

## Fine, later, handled and ignored items

| TYPE / OUTCOME   | ITEM                                                                                                                           |
|------------------|--------------------------------------------------------------------------------------------------------------------------------|
| DOM-FED<br>LATER | <b>tailspin-mail.example</b><br>Federation signing certificate. expires 2027-06-30 (262 days left). Owners: none.              |
| DOM-DNS<br>FINE  | <b>tailspin.example</b><br>MX record ok: found 0 tailspin-example.mail.protection.outlook.com. Owners: none.                   |
| DOM-DNS<br>FINE  | <b>tailspin.example</b><br>DKIM record ok: found selector2-tailspin-example._domainkey.tailspin.onmicrosoft.com. Owners: none. |
| DOM-DKIM<br>FINE | <b>tailspin.example</b><br>DKIM signing enabled, selector selector2, rotates on 2026-10-31. Owners: none.                      |

## SCOPE SUMMARY / EVIDENCE INDEX

## Intune

0

Expired

2

Expires soon

0

Needs attention

2

Later

1

Fine

0

Handled

0

Ignored

0

No result

Dated items by days left: 0 expired, 1 within 7 days, 1 within 30 days, 2 later.

## Findings index / click a type to open its card

INT-APNS

SOON

INT-CONN

SOON

## Fine, later, handled and ignored items

| TYPE / OUTCOME   | ITEM                                                                                                                   |
|------------------|------------------------------------------------------------------------------------------------------------------------|
| INT-VPP<br>LATER | <b>Apple VPP token</b><br>Token for Tailspin Toys, state valid. expires 2026-12-01 (51 days left). Owners: none.       |
| INT-DEP<br>LATER | <b>Apple Business Manager token</b><br>Apple Business Manager token. expires 2027-02-09 (121 days left). Owners: none. |
| INT-PLAY<br>FINE | <b>Managed Google Play</b><br>Binding boundAndSynced, last app sync 2026-10-09. Owners: none.                          |

SCOPE SUMMARY / EVIDENCE INDEX

# Directory



Dated items by days left: 0 expired, 0 within 7 days, 0 within 30 days, 0 later.

## Findings index / click a type to open its card

DIR-SYNC

ATTENTION

## TENANT INVENTORY

## Tenant inventory

## Tenant identity

|                   |                                                   |
|-------------------|---------------------------------------------------|
| Display name      | Tailspin Toys                                     |
| Initial domain    | tailspin.onmicrosoft.com                          |
| Tenant id         | 4d2f7c1a-9b3e-4e6a-8c1d-2f5b7a9e0c13              |
| Signed-in account | admin@tailspin.example                            |
| Run               | sample-run-2026-10-10-tailspin-0001               |
| Mode              | from the app                                      |
| Started UTC       | 2026-10-10T08:00:00Z                              |
| Finished UTC      | 2026-10-10T08:02:41Z                              |
| App version       | 0.1.0                                             |
| Thresholds        | expires soon within 30 days; unused after 90 days |

## Parts read

| PART                             | STATUS  | NOTE            |
|----------------------------------|---------|-----------------|
| Organization                     | ok      | -               |
| App registrations                | ok      | -               |
| Enterprise applications          | ok      | -               |
| Sign-in activity of applications | ok      | -               |
| Domains                          | ok      | -               |
| DNS lookups                      | ok      | -               |
| DKIM signing (Exchange Online)   | ok      | -               |
| Intune                           | ok      | -               |
| Conditional Access               | skipped | consent_missing |

Totals

|                             |     |
|-----------------------------|-----|
| Applications                | 212 |
| Enterprise applications     | 488 |
| Domains                     | 2   |
| Conditional Access policies | 0   |
| Items watched               | 23  |

Verified domains

|                       |
|-----------------------|
| tailspin.example      |
| tailspin-mail.example |

Collection diagnostics

No collection diagnostics were recorded.

Collection was read-only through Microsoft Graph delegated permissions, the Exchange Online read for DKIM where granted, and DNS lookups from the computer that ran the app. Secret values are never returned by Microsoft and never asked for; no private key leaves the tenant; nothing was renewed.

## REFERENCE MATERIAL

# Methodology references

## Add credentials to an app registration

<https://learn.microsoft.com/en-us/entra/identity-platform/how-to-add-credentials>

## Manage certificates for federated single sign-on

<https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/tutorial-manage-certificates-for-federated-single-sign-on>

## Set up DKIM, SPF and DMARC for Microsoft 365

<https://learn.microsoft.com/en-us/defender-office-365/email-authentication-about>

## Renew the Apple MDM push certificate

<https://learn.microsoft.com/en-us/mem/intune/enrollment/apple-mdm-push-certificate-get>

## Apple Business Manager and VPP tokens in Intune

<https://learn.microsoft.com/en-us/mem/intune/apps/vpp-apps-ios>

## Microsoft Entra Connect Health

<https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/whatis-azure-ad-connect>

## Conditional Access policies

<https://learn.microsoft.com/en-us/entra/identity/conditional-access/overview>

## About this report

This report lists the credentials, certificates, tokens and records read from the Microsoft 365 tenant named in it, at the time shown, within the limits in its coverage section. It is a point-in-time review, not an audit opinion, a certification or a guarantee that nothing else will expire or break. Days left are counted from the run date. Findings and guidance are informational; renewals are made by the customer, and nothing in this report changes a tenant. Parts that could not be read are reported as not read, not as fine. Microsoft behavior can change after the run date. Prepared by GlacierPoint Technologies LLC under the GlacierPoint Remind Terms of Service.