

# Contoso Legal LLP



PREPARED BY

Harbour IT

DATE

14 Oct 2026

DATA COLLECTED

14 Oct 2026, 04:00 UTC

MICROSOFT 365 TENANT

contoso.onmicrosoft.com

Admin roles, Conditional Access, app credentials, consents, domains and account changes from the directory audit log, and who made them.

Filtered view. All admin changes: 22 of 22 rows, 1 column hidden. The headline figures cover every row.

## Changes to review 10 10 to review

Changes in the 120 days since 16 Jun 2026, when Office Sentry started keeping this tenant's audit log that are worth confirming with the client: domain sign-in (federation) changes, new app secrets and certificates, admin roles granted, and Conditional Access policies deleted or switched off. Failed attempts are left out.

| Flag     | When (UTC)         | Change                                                   | By                           | Target                         | Detail                 | Why it matters                                                                           |
|----------|--------------------|----------------------------------------------------------|------------------------------|--------------------------------|------------------------|------------------------------------------------------------------------------------------|
| ● High   | 11 Oct 2026, 16:00 | Set domain authentication                                | mallory.hart@contoso.example | contoso.example                | –                      | Changes how users of a domain sign in; a rogue federation lets someone sign in as anyone |
| ● Medium | 13 Oct 2026, 16:00 | Add service principal credentials                        | Contoso Automation           | Mail Sync Pro                  | Credential added       | New secret or certificate: whoever holds it can sign in as the app                       |
| ● Medium | 12 Oct 2026, 16:00 | Update application – Certificates and secrets management | admin@contoso.example        | Payroll Sync                   | Added certificate      | New secret or certificate: whoever holds it can sign in as the app                       |
| ● Medium | 12 Oct 2026, 04:00 | Add member to role                                       | admin@contoso.example        | bobby.marsh@contoso.example    | Global Administrator   | Admin role granted                                                                       |
| ● Medium | 11 Oct 2026, 04:00 | Add eligible member to role in PIM completed (permanent) | admin@contoso.example        | annabel.fraser@contoso.example | Exchange Administrator | Admin role granted                                                                       |
|          |                    |                                                          |                              |                                |                        |                                                                                          |

| Flag     | When (UTC)         | Change                                                   | By                    | Target                      | Detail               | Why it matters                                                     |
|----------|--------------------|----------------------------------------------------------|-----------------------|-----------------------------|----------------------|--------------------------------------------------------------------|
| ● Medium | 9 Oct 2026, 04:00  | Update conditional access policy                         | admin@contoso.example | Require MFA for all users   | On → Off             | Conditional Access policy no longer enforced                       |
| ● Medium | 7 Oct 2026, 16:00  | Delete conditional access policy                         | admin@contoso.example | Block risky countries       | –                    | Conditional Access policy deleted                                  |
| ● Medium | 2 Oct 2026, 04:00  | Update application – Certificates and secrets management | admin@contoso.example | Payroll Sync                | Added certificate    | New secret or certificate: whoever holds it can sign in as the app |
| ● Medium | 3 Sep 2026, 04:00  | Update conditional access policy                         | admin@contoso.example | Require MFA for all users   | On → Off             | Conditional Access policy no longer enforced                       |
| ● Medium | 11 Aug 2026, 04:00 | Add member to role                                       | admin@contoso.example | bobby.marsh@contoso.example | Global Administrator | Admin role granted                                                 |

## All admin changes 22 10 to review

Every admin role, Conditional Access, policy, app, domain and account change in the 120 days since 16 Jun 2026, when Office Sentry started keeping this tenant's audit log, newest first.

| Flag     | When (UTC)         | Area        | Change                                                   | By                           | Target                       | Detail               | IP address   |
|----------|--------------------|-------------|----------------------------------------------------------|------------------------------|------------------------------|----------------------|--------------|
| ● Medium | 13 Oct 2026, 16:00 | Apps        | Add service principal credentials                        | Contoso Automation           | Mail Sync Pro                | Credential added     | –            |
|          | 13 Oct 2026, 04:00 | Admin roles | Add member to role                                       | mallory.hart@contoso.example | mallory.hart@contoso.example | Global Administrator | 203.0.113.9  |
| ● Medium | 12 Oct 2026, 16:00 | Apps        | Update application – Certificates and secrets management | admin@contoso.example        | Payroll Sync                 | Added certificate    | 203.0.113.40 |
| ● Medium | 12 Oct 2026, 04:00 | Admin roles | Add member to role                                       | admin@contoso.example        | bobby.marsh@contoso.example  | Global Administrator | 203.0.113.40 |
| ● High   | 11 Oct 2026, 16:00 | Domains     | Set domain authentication                                | mallory.hart@contoso.example | contoso.example              | –                    | 203.0.113.9  |

| Flag     | When (UTC)         | Area               | Change                                                   | By                    | Target                                                                                                                                 | Detail                                          | IP address   |
|----------|--------------------|--------------------|----------------------------------------------------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|--------------|
| ● Medium | 11 Oct 2026, 04:00 | Admin roles        | Add eligible member to role in PIM completed (permanent) | admin@contoso.example | annabel.fraser@contoso.example                                                                                                         | Exchange Administrator                          | 203.0.113.40 |
|          | 10 Oct 2026, 16:00 | Accounts           | Reset user password                                      | admin@contoso.example | annabel.fraser@contoso.example                                                                                                         | –                                               | 203.0.113.40 |
|          | 10 Oct 2026, 04:00 | Admin roles        | Remove member from role                                  | admin@contoso.example | old.admin@contoso.example                                                                                                              | Global Administrator                            | 203.0.113.40 |
|          | 9 Oct 2026, 16:00  | Accounts           | Admin registered security info                           | admin@contoso.example | annabel.fraser@contoso.example                                                                                                         | –                                               | 203.0.113.40 |
| ● Medium | 9 Oct 2026, 04:00  | Conditional Access | Update conditional access policy                         | admin@contoso.example | Require MFA for all users                                                                                                              | On → Off                                        | 203.0.113.40 |
|          | 8 Oct 2026, 04:00  | Conditional Access | Add conditional access policy                            | admin@contoso.example | Block legacy authentication                                                                                                            | On                                              | 203.0.113.40 |
| ● Medium | 7 Oct 2026, 16:00  | Conditional Access | Delete conditional access policy                         | admin@contoso.example | Block risky countries                                                                                                                  | –                                               | 203.0.113.40 |
|          | 6 Oct 2026, 04:00  | Apps               | Update application – Certificates and secrets management | admin@contoso.example | Old Integration                                                                                                                        | Removed secret                                  | 203.0.113.40 |
|          | 5 Oct 2026, 04:00  | Apps               | Consent to application                                   | admin@contoso.example | Mail Sync Pro                                                                                                                          | Admin consent for everyone: Mail.Read User.Read | 203.0.113.40 |
|          | 5 Oct 2026, 01:36  | Apps               | Add app role assignment to service principal             | admin@contoso.example | Mail Sync Pro                                                                                                                          | Mail.ReadWrite on Microsoft Graph               | 203.0.113.40 |
|          | 4 Oct 2026, 04:00  | Accounts           | Delete user                                              | admin@contoso.example | leaver0@contoso.example, leaver1@contoso.example, leaver2@contoso.example, leaver3@contoso.example, leaver4@contoso.example and 2 more | –                                               | 203.0.113.40 |
|          | 3 Oct 2026, 04:00  | Partners           | Add partner to company                                   | Partner Center        | Contoso IT Services                                                                                                                    | –                                               | –            |

| Flag     | When (UTC)         | Area               | Change                                                   | By                    | Target                      | Detail               | IP address   |
|----------|--------------------|--------------------|----------------------------------------------------------|-----------------------|-----------------------------|----------------------|--------------|
| ● Medium | 2 Oct 2026, 04:00  | Apps               | Update application – Certificates and secrets management | admin@contoso.example | Payroll Sync                | Added certificate    | 203.0.113.40 |
|          | 2 Oct 2026, 04:00  | Domains            | Verify domain                                            | admin@contoso.example | new.contoso.example         | –                    | 203.0.113.40 |
| ● Medium | 3 Sep 2026, 04:00  | Conditional Access | Update conditional access policy                         | admin@contoso.example | Require MFA for all users   | On → Off             | 203.0.113.40 |
| ● Medium | 11 Aug 2026, 04:00 | Admin roles        | Add member to role                                       | admin@contoso.example | bobby.marsh@contoso.example | Global Administrator | 203.0.113.40 |
|          | 16 Jul 2026, 04:00 | Conditional Access | Add conditional access policy                            | admin@contoso.example | Block legacy authentication | On                   | 203.0.113.40 |

Who made changes 4

Everyone (and every app) that made one of the changes above, most active first.

| Who                          | Type | Changes | Last change (UTC)  |
|------------------------------|------|---------|--------------------|
| admin@contoso.example        | User | 18      | 12 Oct 2026, 16:00 |
| mallory.hart@contoso.example | User | 2       | 13 Oct 2026, 04:00 |
| Contoso Automation           | App  | 1       | 13 Oct 2026, 16:00 |
| Partner Center               | App  | 1       | 3 Oct 2026, 04:00  |