

## Northwind Traders

PREPARED BY  
Harbour ITDATE  
12 Oct 2026DATA COLLECTED  
12 Oct 2026, 06:36 UTCMICROSOFT 365 TENANT  
northwindtraders.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: 1 of 22 rows, Target is mallory.price@northwindtraders.example, 1 column hidden. The headline figures cover every row.

**Changes to review** 10 10 to review

Changes in the 120 days since 14 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   | 9 Oct 2026, 18:36  | Set domain authentication                                | mallory.price@northwindtraders.example | northwindtraders.example               | –                      | Changes how users of a domain sign in; a rogue federation lets someone sign in as anyone |
| ● Medium | 11 Oct 2026, 18:36 | 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 | 10 Oct 2026, 18:36 | Update application – Certificates and secrets management | admin@northwindtraders.example         | Payroll Sync                           | Added certificate      | New secret or certificate: whoever holds it can sign in as the app                       |
| ● Medium | 10 Oct 2026, 06:36 | Add member to role                                       | admin@northwindtraders.example         | robert.hughes@northwindtraders.example | Global Administrator   | Admin role granted                                                                       |
| ● Medium | 9 Oct 2026, 06:36  | Add eligible member to role in PIM completed (permanent) | admin@northwindtraders.example         | ann.patel@northwindtraders.example     | Exchange Administrator | Admin role granted                                                                       |

| Flag     | When (UTC)         | Change                                                   | By                             | Target                                 | Detail               | Why it matters                                                     |
|----------|--------------------|----------------------------------------------------------|--------------------------------|----------------------------------------|----------------------|--------------------------------------------------------------------|
| ● Medium | 7 Oct 2026, 06:36  | Update conditional access policy                         | admin@northwindtraders.example | Require MFA for all users              | On → Off             | Conditional Access policy no longer enforced                       |
| ● Medium | 5 Oct 2026, 18:36  | Delete conditional access policy                         | admin@northwindtraders.example | Block risky countries                  | –                    | Conditional Access policy deleted                                  |
| ● Medium | 30 Sep 2026, 06:36 | Update application – Certificates and secrets management | admin@northwindtraders.example | Payroll Sync                           | Added certificate    | New secret or certificate: whoever holds it can sign in as the app |
| ● Medium | 1 Sep 2026, 06:36  | Update conditional access policy                         | admin@northwindtraders.example | Require MFA for all users              | On → Off             | Conditional Access policy no longer enforced                       |
| ● Medium | 9 Aug 2026, 06:36  | Add member to role                                       | admin@northwindtraders.example | robert.hughes@northwindtraders.example | Global Administrator | Admin role granted                                                 |

All admin changes 1

Every admin role, Conditional Access, policy, app, domain and account change in the 120 days since 14 Jun 2026, when Office Sentry started keeping this tenant's audit log, newest first.

| When (UTC)         | Area        | Change             | By                                     | Target                                 | Result                          | IP address  |
|--------------------|-------------|--------------------|----------------------------------------|----------------------------------------|---------------------------------|-------------|
| 11 Oct 2026, 06:36 | Admin roles | Add member to role | mallory.price@northwindtraders.example | mallory.price@northwindtraders.example | Failed: Insufficient privileges | 203.0.113.9 |

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@northwindtraders.example         | User | 18      | 10 Oct 2026, 18:36 |
| mallory.price@northwindtraders.example | User | 2       | 11 Oct 2026, 06:36 |
| Contoso Automation                     | App  | 1       | 11 Oct 2026, 18:36 |
| Partner Center                         | App  | 1       | 1 Oct 2026, 06:36  |

---

Prepared by Harbour IT (help@harbourit.example · 0161 496 0000). Read from Microsoft 365 with read-only access; nothing was changed. Data collected 12 Oct 2026, 06:36 UTC.