

Contoso Legal LLP

PREPARED BY
Harbour ITDATE
12 Oct 2026DATA COLLECTED
12 Oct 2026, 06:36 UTCMICROSOFT 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. Who made changes: 1 of 4 rows, Changes is 18. 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.hart@contoso.example	contoso.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@contoso.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@contoso.example	bobby.marsh@contoso.example	Global Administrator	Admin role granted
● Medium	9 Oct 2026, 06:36	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	7 Oct 2026, 06:36	Update conditional access policy	admin@contoso.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@contoso.example	Block risky countries	–	Conditional Access policy deleted
● Medium	30 Sep 2026, 06:36	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	1 Sep 2026, 06:36	Update conditional access policy	admin@contoso.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@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 14 Jun 2026, when Office Sentry started keeping this tenant's audit log, newest first.

Flag	Area	Change	By	Target	Detail	Result	IP address
● Medium	Apps	Add service principal credentials	Contoso Automation	Mail Sync Pro	Credential added	Succeeded	–
	Admin roles	Add member to role	mallory.hart@contoso.example	mallory.hart@contoso.example	Global Administrator	Failed: Insufficient privileges	203.0.113.9
● Medium	Apps	Update application – Certificates and secrets management	admin@contoso.example	Payroll Sync	Added certificate	Succeeded	203.0.113.40
● Medium	Admin roles	Add member to role	admin@contoso.example	bobby.marsh@contoso.example	Global Administrator	Succeeded	203.0.113.40
● High	Domains	Set domain authentication	mallory.hart@contoso.example	contoso.example	–	Succeeded	203.0.113.9

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

Flag	Area	Change	By	Target	Detail	Result	IP address
	Domains	Verify domain	admin@contoso.example	new.contoso.example	–	Succeeded	203.0.113.40
● Medium	Conditional Access	Update conditional access policy	admin@contoso.example	Require MFA for all users	On → Off	Succeeded	203.0.113.40
● Medium	Admin roles	Add member to role	admin@contoso.example	bobby.marsh@contoso.example	Global Administrator	Succeeded	203.0.113.40
	Conditional Access	Add conditional access policy	admin@contoso.example	Block legacy authentication	On	Succeeded	203.0.113.40

Who made changes 1

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	10 Oct 2026, 18:36

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.