

PREPARED BY
Harbour IT

DATE
14 Oct 2026

DATA COLLECTED
14 Oct 2026, 04:00 UTC

MICROSOFT 365 TENANT
contoso.onmicrosoft.com

Every policy in plain words, and which accounts each one actually covers.

Filtered view. Policies: 11 of 11 rows, 1 column hidden. Coverage by account: 1 of 20 rows, Admin roles is Exchange Administrator. The headline figures cover every row.

Policies 11 2 to review

Every policy in plain words, enforced ones first.

Flag	Policy	State	Applies to	Apps	Conditions	Requires
	CA001 — Admins: Require phishing-resistant MFA	On	Global Administrator, Security Administrator, SharePoint Administrator, Exchange Administrator, Conditional Access Administrator, Application Administrator, Cloud Application Administrator, Password Administrator, Privileged Authentication Administrator, Privileged Role Administrator, User Administrator	All apps	–	MFA
	CA002 — All users: Require MFA	On	All users	All apps	–	MFA
	CA003 — Block legacy authentication	On	All users	All apps	Clients: ActiveSync, Other legacy	Block
	CA004 — All users: Require compliant or hybrid-joined device	On	All users	All apps	Platforms: windows, macOS	Compliant device or Hybrid joined

Flag	Policy	State	Applies to	Apps	Conditions	Requires
	CA005 — Block sign-ins from disallowed countries	On	All users	All apps	Locations	Block
	CA006 — Require MFA for Azure management	On	All users	1 app	–	MFA
	CA007 — Admins: No persistent browser, 8h sign-in frequency	On	Global Administrator, Security Administrator, SharePoint Administrator, Exchange Administrator, Conditional Access Administrator, Application Administrator, Cloud Application Administrator, Password Administrator, Privileged Authentication Administrator, Privileged Role Administrator, User Administrator	All apps	–	Session controls
	CA008 — All users: 8h sign-in frequency	On	All users	All apps	–	Session controls
	CA009 — Require MFA for device registration	On	All users	User actions	–	MFA
● Medium	CA010 — Insider risk: Step-up MFA	On, but never applies (needs Entra ID P2)	All users	All apps	User risk: high	MFA
● Medium	CA011 — High sign-in risk: Block	On, but never applies (needs Entra ID P2)	All users	All apps	Sign-in risk: high	Block

Coverage by account 1

19 of 20 enabled accounts are covered by an enforced policy that requires MFA for all apps.

Account	Type	Admin roles	MFA required by	Legacy sign-in blocked	Excluded from
g#EXT#@contoso.example	Guest	Exchange Administrator	CA001 — Admins: Require phishing-resistant MFA	Yes	CA002 — All users: Require MFA, CA008 — All users: 8h sign-in frequency

Prepared by Harbour IT (help@harbourit.example · 0161 496 0000). Read from Microsoft 365 with read-only access; nothing was changed. Data collected 14 Oct 2026, 04:00 UTC.