CONDITIONAL ACCESS COVERAGE

Fabrikam Dental Group

Harbour IT

PREPARED BY	DATE	DATA COLLECTED	MICROSOFT 365 TENANT
Harbour IT	29 Nov 2026	29 Nov 2026, 04:00 UTC	fabrikam.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 57 rows, MFA required by is Nothing. The headline figures cover every row.

Policies on
7
2 report-only, 0 off

MFA not required
1
Enabled accounts no enforced policy asks for MFA in every app, including 1 admin

Legacy sign-in allowed
57
Enabled accounts no enforced policy blocks legacy sign-in for

Security Defaults
Off
Conditional Access applies instead

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
	CA005 — Block sign-ins from disallowed countries	On	All users	All apps	Locations	Block

Flag	Policy	State	Applies to	Apps	Conditions	Requires
	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
	CA003 — Block legacy authentication	Report-only	All users	All apps	Clients: ActiveSync, Other legacy	Block
	CA004 — All users: Require compliant or hybrid-joined device	Report-only	All users	All apps	Platforms: windows, macOS	Compliant device or Hybrid joined

Coverage by account 1 1 to review

56 of 57 enabled accounts are covered by an enforced policy that requires MFA for all apps.

Flag	Account	Type	Admin roles	MFA required by	Legacy sign-in blocked	Excluded from
High	breakglass@fabrikam.example	Member	Global Administrator	Nothing	No	CA001 — Admins: Require phishing-resistant MFA, CA002 — All users: Require MFA, CA005 — Block sign-ins from disallowed countries, CA006 — Require MFA for Azure management, CA007 — Admins: No persistent browser, 8h sign-in frequency, CA008 — All users: 8h sign-in frequency, CA009 — Require MFA for device registration, CA010 — Insider risk: Step-up MFA, CA011 — High sign-in risk: Block

Prepared by Harbour IT (help@harbourit.example · 0161 496 0000). Read from Microsoft 365 with read-only access; nothing was changed. Data collected 29 Nov 2026, 04:00 UTC.