

Fabrikam Dental Group



PREPARED BY	DATE	DATA COLLECTED	MICROSOFT 365 TENANT
Harbour IT	12 Oct 2026	12 Oct 2026, 06:36 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: 2 of 55 rows, Admin roles is Global Administrator. The headline figures cover every row.

Policies 11 2 to review

Every policy in plain words, enforced ones first.

Flag	Policy	Applies to	Except	Apps	Conditions	Requires
	CA001 — Admins: Require phishing-resistant MFA	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	breakglass@fabrikam.example	All apps	–	MFA

Flag	Policy	Applies to	Except	Apps	Conditions	Requires
	CA002 — All users: Require MFA	All users	breakglass@fabrikam.example, 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
	CA005 — Block sign-ins from disallowed countries	All users	breakglass@fabrikam.example	All apps	Locations	Block
	CA006 — Require MFA for Azure management	All users	breakglass@fabrikam.example	1 app	–	MFA
	CA007 — Admins: No persistent browser, 8h sign-in frequency	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	breakglass@fabrikam.example	All apps	–	Session controls
	CA008 — All users: 8h sign-in frequency	All users	breakglass@fabrikam.example, 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
	CA009 — Require MFA for device registration	All users	breakglass@fabrikam.example	User actions	–	MFA

Flag	Policy	Applies to	Except	Apps	Conditions	Requires
● Medium	CA010 — Insider risk: Step-up MFA	All users	breakglass@fabrikam.example	All apps	User risk: high	MFA
● Medium	CA011 — High sign-in risk: Block	All users	breakglass@fabrikam.example	All apps	Sign-in risk: high	Block
	CA003 — Block legacy authentication	All users	breakglass@fabrikam.example	All apps	Clients: ActiveSync, Other legacy	Block
	CA004 — All users: Require compliant or hybrid-joined device	All users	breakglass@fabrikam.example, anna.kowalski@fabrikam.example	All apps	Platforms: windows, macOS	Compliant device or Hybrid joined

Coverage by account 2 1 to review

54 of 55 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
	anna.kowalski@fabrikam.example	Member	Global Administrator	CA001 — Admins: Require phishing-resistant MFA	No	CA002 — All users: Require MFA, CA008 — All users: 8h sign-in frequency