

Flag	Policy	State	Applies to	Except	Apps	Conditions	Requires
	CA002 — All users: Require MFA	On	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	On	All users	breakglass@fabrikam.example	All apps	Locations	Block
	CA006 — Require MFA for Azure management	On	All users	breakglass@fabrikam.example	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	breakglass@fabrikam.example	All apps	–	Session controls
	CA008 — All users: 8h sign-in frequency	On	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

Flag	Policy	State	Applies to	Except	Apps	Conditions	Requires
	CA009 — Require MFA for device registration	On	All users	breakglass@fabrikam.example	User actions	–	MFA
● Medium	CA010 — Insider risk: Step-up MFA	On, but never applies (needs Entra ID P2)	All users	breakglass@fabrikam.example	All apps	User risk: high	MFA
● Medium	CA011 — High sign-in risk: Block	On, but never applies (needs Entra ID P2)	All users	breakglass@fabrikam.example	All apps	Sign-in risk: high	Block
	CA003 — Block legacy authentication	Report-only	All users	breakglass@fabrikam.example	All apps	Clients: ActiveSync, Other legacy	Block
	CA004 — All users: Require compliant or hybrid-joined device	Report-only	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	MFA required by	Legacy sign-in blocked	Excluded from
● High	breakglass@fabrikam.example	Member	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	CA001 — Admins: Require phishing-resistant MFA	No	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.