STRONDEX

Microsoft 365 Hardening — Top 10 Controls

The highest-impact controls, pulled from our 80-point Microsoft 365 Hardening checklist.

Start here. These are the controls that block the most risk (and the ones auditors and cyber-insurance carriers ask about first). Work top-down — severity is highest at the top.

1	CRITICAL	**Require multi-factor authentication for every user, not just admins.** **Verify:** In Entra admin center → Protection → Conditional Access → Overview, confirm an MFA policy covers All users.
2	CRITICAL	**Enforce MFA on all Global Administrator accounts.** **Verify:** List Global Admins under Entra → Roles & admins → Global Administrator, then confirm each is in scope of an MFA Conditional Access policy.
3	CRITICAL	**Block legacy (Basic) authentication protocols with Conditional Access.** **Verify:** In Entra → Protection → Conditional Access, create a policy that targets Client apps → Exchange ActiveSync & Other clients and sets Block access.
4	CRITICAL	**Run an active Conditional Access policy that requires MFA for all users.** **Verify:** In Entra → Protection → Conditional Access → Policies, confirm an enabled policy targeting All users and All cloud apps with grant control Require mul…
5	CRITICAL	**Run an active Conditional Access policy that blocks legacy authentication.** **Verify:** Confirm an enabled CA policy with conditions Client apps → Exchange ActiveSync clients and Other clients, grant set to Block access.
6	CRITICAL	**Keep Global Administrator assignments to between two and four accounts.** **Verify:** In Entra → Roles & admins → Global Administrator, count active assignments.
7	CRITICAL	**Make Global Admin accounts cloud-only, not synced from on-prem AD.** **Verify:** In Entra → Users, check each Global Admin's On-premises sync enabled property is No.
8	CRITICAL	**Use dedicated admin accounts — never use Global Admin for day-to-day work.** **Verify:** Confirm admins hold a separate, unlicensed admin identity (no mailbox, no Teams) used only for administration, and a standard account for email and da…
9	CRITICAL	**Publish a DMARC record with a policy of quarantine or reject.** **Verify:** Add a DNS TXT record at _dmarc.yourdomain.com, e.g.
10	CRITICAL	**Restrict external sharing to existing guests or organization-only — not "Anyone".** **Verify:** In SharePoint admin center → Policies → Sharing, set the organization-level slider to Existing guests or Only people in your organization.