



Conditional Access starter checklist

Conditional Access is where Microsoft 365 identity policy becomes real. Tick only what is enforced, not planned.

Work top-down: break-glass, then MFA, then legacy auth, then devices and registration hardening.

Name a break-glass account before you tighten Conditional Access, and exclude it from policies that would lock you out.

BEFORE YOU START

- ☐ At least one break-glass account exists, is monitored, and is excluded from risky Conditional Access policies
- ☐ You know which licences you have (Entra ID P1 / P2, Intune) so you only tick what you can actually enforce
- ☐ A small pilot group is ready (IT first) for any policy that might interrupt sign-in

CORE SIGN-IN POLICIES

- ☐ MFA required for all users (prefer Conditional Access over per-user MFA)
- ☐ MFA required for all admins, with phishing-resistant methods where licensing allows (passkeys / FIDO2 / Windows Hello for Business)
- ☐ Legacy authentication blocked (POP, IMAP, SMTP AUTH, and other basic auth clients)
- ☐ High-risk sign-ins blocked or forced to remediate (where Identity Protection is licensed)
- ☐ Risky users blocked or forced to remediate (where licensed)

DEVICES AND APPS

- ☐ Exchange Online, SharePoint, and OneDrive require a managed / compliant device or a constrained browser session (no download / sync) for unmanaged devices
- ☐ Device code flow blocked unless you have a named business exception
- ☐ Authentication transfer / companion-app style flows blocked unless you have a named exception
- ☐ Persistent browser sessions limited for privileged roles

SECURITY INFO AND REGISTRATION

Helpdesk-style "update your passkey / MFA" lures succeed when registration is wide open. Harden this on purpose.

- ☐ Separate Conditional Access for registering security information (MFA methods / passkeys)
- ☐ Registration requires phishing-resistant strength where you can
- ☐ Registration limited to managed devices and/or trusted locations
- ☐ Registration blocked at high sign-in risk
- ☐ Fresh interactive sign-in required before registering new methods

GUESTS AND EXTERNAL ACCESS

- ☐ Guest users have Conditional Access applied (not left on "we'll do guests later")

Conditional Access starter checklist

- ☐ Guest MFA required
- ☐ Guest access to sensitive apps is deliberate — not the tenant default

PRIVILEGED ROLES

- ☐ Standing Global Administrators kept small and named
- ☐ Privileged roles use just-in-time elevation (PIM) where licensed
- ☐ Privileged role sign-ins require phishing-resistant MFA and, where practical, managed devices

OPERATING RHYTHM

- ☐ Policies have clear names (what they do, who they cover)
- ☐ Exclusions are listed and reviewed on a cadence
- ☐ A named owner reviews Conditional Access after any Entra / identity disclosure or major M365 change
- ☐ Break-glass sign-in is monitored (alert on use)

What good looks like: you can explain every policy in one sentence. Nobody is relying on per-user MFA leftovers. Device-code and MFA registration are not open doors.

zenaossolutions.co.nz contact@zenaossolutions.co.nz