Checklist

Entra ID Conditional Access 2026

The practitioner's guide to building and auditing enterprise-grade CA policies

By Ramón Lotz — February 2026 | access-insights.com

After managing Conditional Access policies for 8,500+ users across 5 timezones, I've seen the same mistakes made over and over. This checklist captures what actually matters — not the checkbox-friendly items from the official docs, but the things that bite you at 3am when a VP is locked out before a board meeting.

Use this to audit an existing environment or build a new one from scratch. Priority labels reflect real-world risk, not theoretical best practices.

> *Priority Legend: ✗ Must Have — your baseline, non-negotiable | Recommended — important for most enterprises | Advanced — mature environments & regulated industries*

1. Foundations & Named Locations

	Policy / Configuration	Priority	Notes
☐	Break-glass / emergency access accounts excluded from all CA policies	**Must Have**	*At least 2 accounts, different MFA methods, monitored*
☐	Named Locations defined for all corporate network ranges (IPv4 + IPv6)	**Must Have**	*Needed for location-based policies to function correctly*
☐	Countries allowlist or blocklist configured	**Recommended**	*Block sign-ins from non-operating regions*
☐	VPN egress IPs included in Named Locations	**Recommended**	*Prevents false positives on compliant device policies*
☐	Trusted Location scope reviewed and not over-permissive	**Must Have**	*Avoid labelling entire internet ranges as trusted*
☐	Named Location naming convention documented and enforced	**Recommended**	*NL-CORP-HQ-DE, NL-VPN-EU, NL-CLOUD-AWS*

2. User & Group Targeting

	Policy / Configuration	Priority	Notes
☐	All policies target specific groups, NOT 'All users' where possible	**Recommended**	*Staged rollout + less blast radius on misconfiguration*
☐	Service accounts excluded via dedicated exclusion group	**Must Have**	*Workload identities break if caught by user policies*
☐	Guest / External users scoped in dedicated policies	**Must Have**	*Default policy gaps frequently exploited*
☐	Directory Sync accounts (Entra Connect) excluded	**Must Have**	*Sync breaks silently and can corrupt directory*
☐	Policy exclusion groups monitored (alert on membership changes)	**Recommended**	*Exclusion groups are a common attack surface*

© 2026 Access Insights | ramonlotz.de
© 2026 Access Insights

	Policy / Configuration	Priority	Notes
☐	Lifecycle policy for excluded accounts (regular access reviews)	Advanced	*ISPM / Identity Governance integration*

3. Authentication Strength & MFA

	Policy / Configuration	Priority	Notes
☐	Authentication Strength policies used instead of 'Require MFA'	Recommended	*Granular control over allowed MFA methods*
☐	Phishing-resistant MFA required for admin roles (FIDO2 or CBA)	Must Have	*Microsoft recommends: no SMS for admins*
☐	Legacy authentication blocked (Exchange ActiveSync, IMAP, POP3, SMTP auth)	Must Have	*Single most impactful policy for reducing account compromise*
☐	SMS / Voice OTP downgraded or removed for privileged accounts	Must Have	*SIM-swap attacks are trivial and increasing*
☐	Windows Hello for Business or FIDO2 deployed for frontline workers	Recommended	*Passwordless reduces phishing exposure significantly*
☐	Temporary Access Pass (TAP) policy scoped tightly with short lifetime	Recommended	*Avoid TAP as permanent fallback for all users*
☐	Combined Registration enabled and enforced for new users	Recommended	*Prevents users skipping MFA registration*

4. Device Compliance & Platform Conditions

	Policy / Configuration	Priority	Notes
☐	Require compliant device OR hybrid Azure AD joined for corporate access	Must Have	*Core Zero Trust control plane*
☐	Compliance policies exist for all platforms (Windows, macOS, iOS, Android)	Must Have	*Policy gap = unmanaged devices get through*
☐	Separate policies for BYOD vs. Corporate devices	Recommended	*BYOD should have stricter session controls*
☐	App Protection Policies (MAM) for BYOD mobile without enrollment	Recommended	*MAM-only is valid for M365 mobile access*
☐	Unsupported device platforms blocked (e.g., Linux if not in scope)	Recommended	*Filter for devices condition can scope precisely*
☐	Grace period for non-compliant devices set to 48h max	Recommended	*Longer grace periods = policy bypass window*
☐	Stale device cleanup process in place (Intune + Entra ID)	Advanced	*Ghost devices cause compliance check failures*

5. Session Controls

© 2026 Access Insights | ramonlotz.de © 2026 Access Insights

	Policy / Configuration	Priority	Notes
☐	Continuous Access Evaluation (CAE) enabled for supported apps	**Must Have**	*Near-real-time token revocation*
☐	Sign-in frequency set for sensitive apps (8h max)	**Recommended**	*Persistent sessions = long token lifetimes*
☐	Persistent browser sessions disabled for unmanaged devices	**Must Have**	*Prevents session persistence on shared/BYOD devices*
☐	App-enforced restrictions for SharePoint and Exchange	**Recommended**	*Block download on unmanaged devices*
☐	Microsoft Defender for Cloud Apps integrated for session inspection	**Advanced**	*Required for advanced DLP and shadow IT controls*
☐	Token protection (binding) enabled for supported scenarios	**Advanced**	*Preview feature — evaluate for high-value workloads*

6. Privileged Access & Admin Roles

	Policy / Configuration	Priority	Notes
☐	All Azure AD / Entra admin roles covered by dedicated CA policies	**Must Have**	*Separate admin policies from user policies*
☐	Admins require phishing-resistant MFA from every location	**Must Have**	*Trusted locations should NOT bypass MFA for admins*
☐	Privileged Identity Management (PIM) enabled for all admin roles	**Must Have**	*Just-in-time access = reduced permanent exposure*
☐	Admin access restricted to SAWs or compliant devices	**Recommended**	*Admin Workstations or PAW concept*
☐	Global Admin activations require approval workflow in PIM	**Recommended**	*Four-eyes principle for highest-privilege roles*
☐	Admin sessions require re-authentication every 4h	**Recommended**	*Reduce session hijack exposure window*

7. Application-Specific Policies

	Policy / Configuration	Priority	Notes
☐	Separate policies for M365 core apps vs. custom / 3rd party apps	**Recommended**	*Avoid over-broad 'All cloud apps' policies*
☐	High-value apps (Finance, HR, ERP) require compliant device + strong MFA	**Must Have**	*Risk-based application tiering*
☐	Guest access to sensitive apps restricted via dedicated policy	**Must Have**	*Guests should never inherit user-level access by default*

© 2026 Access Insights | ramonlotz.de
© 2026 Access Insights

	Policy / Configuration	Priority	Notes
☐	Microsoft Azure Management restricted to IT/admin group	Recommended	*Prevents accidental or malicious Azure resource access*
☐	Intune enrollment excluded from device compliance requirement	Must Have	*Catch-22: device needs to enroll to become compliant*
☐	MCAS / Defender XDR integration apps configured for session proxy	Advanced	*Required for real-time policy enforcement*

8. Sign-In Risk & User Risk Policies

	Policy / Configuration	Priority	Notes
☐	Sign-in risk policy: High risk → block or require strong MFA	Must Have	*Microsoft Entra ID Protection baseline*
☐	User risk policy: High risk → require password change	Must Have	*Compromised credential remediation flow*
☐	Sign-in risk: Medium risk → require MFA	Recommended	*Complements the high-risk block policy*
☐	Risk policies tested in report-only mode before enforcement	Must Have	*Never enforce risk policies without a report-only baseline*
☐	Risk detections reviewed weekly (Entra ID Protection dashboard)	Recommended	*Risk policies are useless without operational review*
☐	Named locations properly configured to reduce false positives	Must Have	*Unfamiliar travel detections from VPN = noise without this*

9. Operations, Naming & Governance

	Policy / Configuration	Priority	Notes
☐	All policies follow a documented naming convention	Must Have	*CA001-GLOBAL-Block-LegacyAuth, CA050-ADMINS-MFA-All*
☐	Policy changes deployed via report-only first (min. 48h observation)	Must Have	*Production-first changes = high blast radius*
☐	CA policy changes tracked via Entra Audit Log + SIEM alerts	Recommended	*Alert on any policy create/update/delete*
☐	Policy owner and review cycle documented (Wiki / CMDB)	Recommended	*Policies without owners become zombie policies*
☐	Quarterly CA policy review scheduled	Advanced	*Business changes render old policies ineffective or risky*
☐	Workbook: CA insights & reporting enabled in Log Analytics	Recommended	*Built-in monitoring for CA sign-in impact*

© 2026 Access Insights | ramonlotz.de © 2026 Access Insights

	Policy / Configuration	Priority	Notes
☐	Policy documentation exported and version-controlled	Advanced	*PowerShell export → Git for change history*

10. Multi-Region & Multi-Timezone Deployments

	Policy / Configuration	Priority	Notes
☐	Rollout windows account for all active timezones	Must Have	*No changes during business hours for any region*
☐	Emergency access accounts available to on-call in all regions	Must Have	*Break-glass usage must be executable from any timezone*
☐	Policy report-only mode extended to cover all region business hours	Must Have	*24h minimum for global orgs; 72h recommended*
☐	Communication plan for MFA changes to cover non-DE regions	Recommended	*Asia-Pacific is always the first to be forgotten*
☐	CA audit log retention aligned to all regional compliance requirements	Advanced	*APAC and US have different retention minimums than EU*

> *Pro Tip: Export your CA policies quarterly via Microsoft Graph PowerShell and version-control them in Git. When something breaks at 3am, you'll know exactly what changed and when.*

About This Checklist

This checklist is based on real-world experience managing Conditional Access at enterprise scale across multiple industries and geographies. It reflects lessons learned from actual incidents, not documentation exercises.

Ramón Lotz is an IT Architect with 7+ years of experience in Microsoft Identity and Cloud Security, specializing in Entra ID, Zero Trust architecture, and M365 Security. He writes at access-insights.com and maintains open-source identity tooling on GitHub.

More resources: access-insights.com — LinkedIn: /in/ramonlotz

© 2026 Access Insights