SOURCEPASS™ MCOE
CENTER OF EXCELLENCE FOR MICROSOFT

Top Conditional Access Policies

A Practical Guide for IT Leaders and Microsoft 365 Administrators

WHY CONDITIONAL ACCESS MATTERS

In today's threat landscape, a username and password alone are no longer sufficient to protect your organization. Microsoft Entra ID Conditional Access is one of the most powerful tools available in Microsoft 365 — acting as a policy engine that evaluates every sign-in attempt and enforces the right controls based on user, device, location, and risk.

Think of Conditional Access as your organization's Zero Trust enforcement layer — it doesn't just ask who you are, it asks where you are, what device you're using, and whether your behavior looks suspicious before granting access.

- **License Requirement:** Conditional Access requires Entra ID P1, which is included in Microsoft 365 Business Premium and Microsoft 365 E3/E5. For risk-based policies (covered in the Extra Credit section), Entra ID P2 is required — available through the Microsoft Defender suite or as a standalone add-on.

THE CORE CONDITIONAL ACCESS POLICIES YOU SHOULD HAVE ENABLED

1. MFA Enforced for All Users: Every user in your organization should be required to complete Multi-Factor Authentication (MFA) when signing in. This single policy alone blocks the overwhelming majority of credential-based attacks. No exceptions — every user, every time.

2. MFA Enforced for All Admins: Administrator accounts are the highest-value targets in any Microsoft 365 environment. A dedicated policy targeting all administrative roles ensures that even if an admin account credential is compromised, an attacker cannot gain elevated access without the second factor.

3. Block Legacy Authentication: Legacy authentication protocols (such as SMTP, IMAP, POP3, and older Office clients) do not support modern MFA, making them a common attack vector. Blocking legacy authentication is one of the highest-impact, lowest-effort policies you can implement. Microsoft reports that over 97% of credential stuffing attacks use legacy authentication protocols.

4. MFA Required for Azure Management: Access to the Azure Portal, Azure CLI, and Azure PowerShell should always require MFA. Azure management access gives users the ability to spin up resources, modify infrastructure, and access sensitive data — making it a critical surface to protect.

SOURCEPASS™ MCOE
CENTER OF EXCELLENCE FOR MICROSOFT

Top Conditional Access Policies

A Practical Guide for IT Leaders and Microsoft 365 Administrators

5. MFA Required to Enroll Devices in Entra ID: Device enrollment is the gateway to your managed environment. Requiring MFA for Entra ID device registration and join operations prevents attackers from enrolling rogue devices into your tenant, even if they have a valid set of credentials.

6. Phishing-Resistant MFA Required for Admins: Standard MFA (SMS, authenticator app push notifications) can still be bypassed via MFA fatigue attacks or real-time phishing proxies. For administrative accounts, enforce phishing-resistant MFA — specifically FIDO2 Passkeys or Windows Hello for Business — to eliminate this risk entirely.

7. MFA Required for Intune Enrollment: Requiring MFA for Microsoft Intune enrollment ensures that only authenticated, legitimate users can bring devices under management. This closes a potential gap where attackers could attempt to enroll devices to bypass compliance policies.

8. Limit Browser Sessions for Privileged Users: Privileged users — such as Global Admins, Security Admins, and other high-value roles — should have persistent browser sessions disabled and sign-in frequency enforced. This ensures that an unattended or compromised browser session cannot be reused by an attacker after the initial authentication window expires.

9. Require Managed Devices for Sign-In: Requiring a compliant or Hybrid Entra ID Joined device for access to corporate resources ensures that only devices meeting your organization's security baseline can reach sensitive applications and data. This is a cornerstone of a Zero Trust device posture and works hand-in-hand with Intune compliance policies.

10. Block Device Code Sign-In Flow: The device code flow is a legitimate OAuth authentication method designed for devices without browsers (like smart TVs or IoT devices) — but it is frequently abused in Business Email Compromise (BEC) and phishing campaigns. Unless you have a specific business need, this flow should be blocked for all users.

EXTRA CREDIT: RISK-BASED POLICIES WITH ENTRA ID P2

License Requirement: These policies require Entra ID P2, which we recommend purchasing through the Microsoft Defender for Business suite or as part of Microsoft 365 E5. Entra ID P2 unlocks Identity Protection, Microsoft's AI-powered risk detection engine.

SOURCEPASS™ MCOE
CENTER OF EXCELLENCE FOR MICROSOFT

Top Conditional Access Policies

A Practical Guide for IT Leaders and Microsoft 365 Administrators

EC1. Block High and Medium Users: When Microsoft's Identity Protection detects that a user account has been compromised — based on leaked credentials, anomalous behavior, or threat intelligence — that account is assigned a risk level. This policy automatically blocks sign-in and forces a password reset for any user flagged at medium or high risk, containing the damage before it spreads.

EC2. Block High and Medium Risk Sign-Ins: Even if a user account itself isn't flagged, an individual sign-in attempt can be evaluated for risk in real time — detecting things like impossible travel, anonymous IP addresses, malware-linked IPs, and atypical sign-in properties. This policy blocks suspicious sign-in sessions before access is granted, regardless of whether MFA was completed.

GETTING STARTED

Implementing these policies doesn't have to happen all at once. A recommended approach:

1. Start in Report-Only mode to understand impact before enforcing.
2. Deploy MFA policies first - highest impact, lowest disruption.
3. Layer in device compliance and session controls once Intune is configured
4. Add risk-based policies last once Entra ID P2 is licensed and Identity Protection is tuned.

Need help designing and deploying your Conditional Access framework? The Sourcepass Microsoft Center of Excellence (MCOE) specializes in security architecture, Entra ID configuration, and Zero Trust deployments. Reach out to learn how we can help your organization build a modern, resilient security posture.

Guide prepared by the Sourcepassa Center of Excellence for Microsoft (MCOE) | May 2026

Schedule an assessment today by contacting us at sourcepassmcoe.com or (916) 787-3223