

Conditional Access Use Cases in Microsoft Entra ID



Top 5 Conditional Access Use Cases

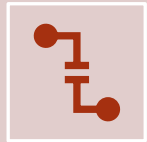


Microsoft Entra ID | Real-World Security Scenarios

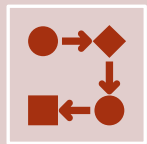


Personal Account-Friendly | Lab-Tested

What is Conditional Access?



Conditional Access lets you enforce **automated access decisions** based on conditions like location, device state, or user risk.



Think of it like:
"If this condition is met → then take this action."



Example:
If the user logs in from an unfamiliar location,
then require multi-factor authentication (MFA).



It's a core part of Zero Trust security in Microsoft Entra ID.

1 – Require MFA for Admin Portals

➤ Use Case:

✓ Require MFA when accessing Azure Portal or Microsoft 365 Admin

🔒 Secures elevated access

💻 Easy to test with personal account

#2 – Sign-in Risk Policy (Entra ID Protection)

➤ Use Case:



Block or challenge users if their sign-in is risky



Based on unusual IP, behavior, or anonymizers

Requires Entra ID P2

#3 – Require Compliant Devices Only

➤ Use Case:

🔒 Allow access only from devices compliant with Intune

📱 Blocks unknown or unmanaged endpoints
Requires Intune setup

#4 – Block Legacy Authentication

➤ Use Case:





- 🚫 Block insecure protocols like IMAP, POP, SMTP
- ⚠️ Legacy apps can bypass MFA — this closes the gap
- ✅ Highly recommended in any tenant

#5 – Require Terms of Use Acceptance

➤ Use Case:

- 📄 Force users to accept a policy doc before access
- ✅ Works for guests & internal users
- 📄 Upload PDF, link to CA policy — no code needed

Summary – Why Conditional Access Rocks

-  Central to Zero Trust
-  Flexible for users, apps, and risks
-  Works in real orgs & personal labs
-  Most powerful free security feature in Entra ID



Want More Labs Like This?

- **Follow for** more Microsoft Entra, Azure Security, and Identity labs
 - 💬 Drop a comment with what you want to see next
#MicrosoftEntra #ConditionalAccess #AzureAD
#ZeroTrust #MFA