# / MAURISEC.DE

FIELD NOTES / CHECKLIST 02

# Conditional Access: sicher planen, testen und einschalten

PRUEFEN. BELEGEN. NACHHALTEN.

Für Administratoren eines Entra-Tenants mit den erforderlichen Berechtigungen und Lizenzen. Jede Änderung benötigt ein klares Schutzziel, definierte Testkonten und einen Wiederherstellungsweg. Quellenstand: 09.11.2026.

Pruefbereich / Team:

Datum:

- [ ] **01 / Schutzziel, betroffene Benutzer, Ressourcen, Clienttypen und Gerätebedingungen je Richtlinie schriftlich festlegen.**

  Nachweis: Richtliniensteckbrief mit Eigentümer, Freigabe und gewünschter Zugriffsentscheidung.

- [ ] **02 / Bestehende Richtlinien und Abhängigkeiten erfassen; alle auf eine Anmeldung zutreffenden Richtlinien gemeinsam berücksichtigen.**

  Nachweis: Konfigurationsexport und Testmatrix mit überlappenden Richtlinien.

- [ ] **03 / Notfallzugriff testen und notwendige Ausnahmen eng, begründet und überprüfbar halten.**

  Nachweis: Notfall-Testprotokoll und Ausnahmeliste mit Zuständigkeit und Prüftermin.

- [ ] **04 / Benutzeranmeldungen und Workload-Identitäten getrennt planen; Benutzer-Richtlinien nicht als Schutz aller Dienstprinzipale ansehen.**

  Nachweis: Getrennte Bestandsliste und dokumentierte Abdeckung je Identitätstyp.

- [ ] **05 / Die Richtlinie zunächst für einen passenden Pilot und, soweit unterstützt, in Report-only prüfen.**

  Nachweis: Richtlinienzustand und protokollierte Report-only-Ergebnisse der vorgesehenen Anmeldungen.

- [ ] **06 / Erlaubte und verbotene Szenarien mit What If vorprüfen und anschließend mit realen Testanmeldungen validieren.**

  Nachweis: Simulationsbericht plus korrespondierende Anmeldeereignisse mit Korrelations-ID.

- [ ] **07 / Auswirkungen auf Geräteaufnahme, Administrationszugang und wichtige Ressourcen gezielt testen.**

  Nachweis: Erfolgreiche Aufnahme und Administration sowie erwartete Ablehnungen im Pilot.

- [ ] **08 / Erst nach dokumentierter Auswertung auf On wechseln; Support, Rücknahme und Nachkontrolle bereitstellen.**

  Nachweis: Freigabe, Änderungsticket, Rücknahmeweg und überprüfte Anmeldeergebnisse nach Aktivierung.

## GEGENPROBE / AUTORISIERTE TESTUMGEBUNG

Vor Erzwingung den dokumentierten Notfallweg testen und erlaubte sowie zu blockierende Anmeldungen mit repräsentativen Testkonten nachstellen.

## GRENZEN UND VORAUSSETZUNGEN

Report-only erzwingt die Richtlinie nicht und unterstützt nicht jeden User-Action-Fall. Geräte-Compliance-Prüfungen können dort trotzdem Zertifikatsdialoge auf macOS, iOS und Android auslösen. What If ist eine Simulation und ersetzt keinen echten Anmeldungstest. Pauschales Blockieren aller Benutzer und Ressourcen oder voreilig erzwungene Geräte-Compliance kann Administration und Geräteaufnahme aussperren.

## PRIMAERQUELLEN / STAND 09.11.2026

**Microsoft Learn: Plan a Conditional Access deployment**
learn.microsoft.com

**Microsoft Learn: Analyze impact with report-only**
learn.microsoft.com

**Microsoft Learn: Troubleshoot Conditional Access**
learn.microsoft.com

**Microsoft Learn: Conditional Access What If**
learn.microsoft.com