

# Conditional Access prüfen und aktualisieren

---

# Christian Decker

---



## Wer bin ich?

- ❖ Seit über 30 Jahren in der IT-Branche
- ❖ Seit 2017 bei ACP als Cloud Architekt
- ❖ Immer mit dem Mehrwert von IT-Lösungen für Menschen beschäftigt
- ❖ Autor von <https://derdecker.at>
- ❖ Moderator der LinkedIn Gruppe [Microsoft Conditional Access](#)
- ❖ Seit März 23 erster Security MVP in Österreich

## Wovon lebe ich?

- ❖ Begleitung von Unternehmen zu M365 in folgenden Bereichen:
  - ❖ Governance
  - ❖ Security
  - ❖ Datenschutz
  - ❖ User Adoption
- ❖ Entwicklung von Standards für M365 innerhalb der ACP-Gruppe

## Und sonst?

CEO (Chief Entertainment Officer) des VIP-Zeltes beim Red Bull Erzberg-Rodeo seit über 10 Jahren



# Neue „Gastoptionen“

**Include**   Exclude

☐ None

☐ All users

☒ Select users and groups

☒ Guest or external users ⓘ

0 selected ▼

- ☐ B2B collaboration guest users
- ☐ B2B collaboration member users
- ☐ B2B direct connect users
- ☐ Local guest users
- ☐ Service provider users
- ☐ Other external users

Specify external Microsoft Entra organizations

☒ All

☐ Select

## B2B collaboration guest users

- Gastaccounts mit Status GAST

## B2B collaboration member users

- Gastaccounts mit Status Member

## B2B direct connect users

- Zugriff über B2B direct connect

## Local guest users

- Lokale Accounts mit Status Gast

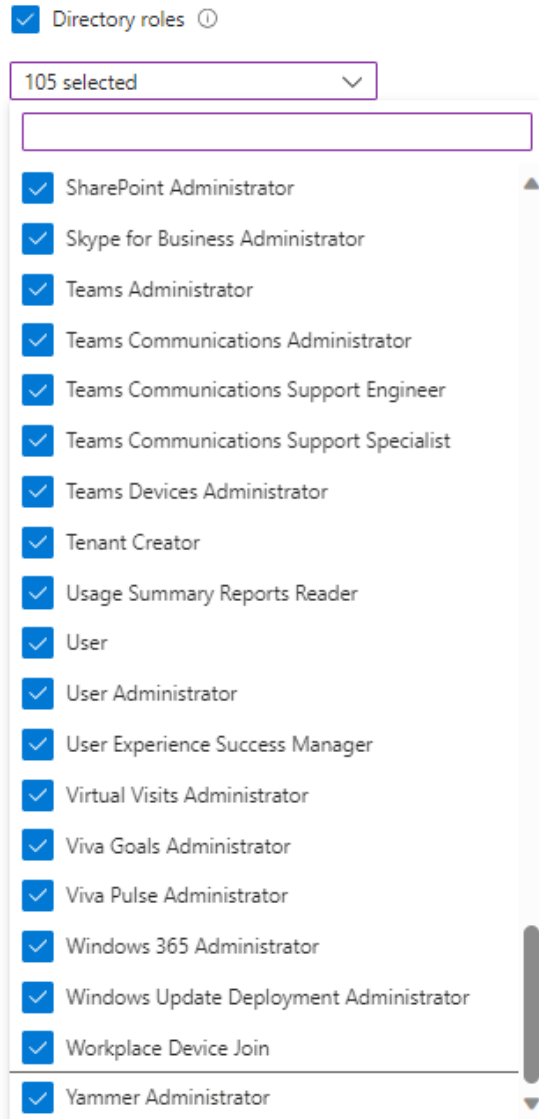
## Service provider users

- User von Service Providern (CSP)

## Other external users

- Externe User, die von den obigen Typen nicht abgedeckt sind

# Viele neue Rollen



Mittlerweile 105 Rollen

„einfache“ Auswahl mit <Pfeil runter>+<Enter>

Achtung bei folgenden Rollen

- Directory Synchronization Account
- Guest User
- Restricted Guest User (?)
- User

# Target resources – User Actions

---

## Register or join devices

Select what this policy applies to

User actions



Select the action this policy will apply to

☐ Register security information

☐ Register or join devices

# Target resources – Microsoft Admin Portals

Select what this policy applies to

Cloud apps

**Include** Exclude

☐ None

☐ All cloud apps

☒ Select apps

---

Edit filter


None

---

Select

Microsoft Admin Portals

---

 Microsoft Admin Portals ⓘ ...

Regelt den Zugriff auf MS Admin Portale

- Azure portal
- Exchange admin center
- Microsoft 365 admin center
- Microsoft 365 Defender portal
- Microsoft Entra admin center
- Microsoft Intune admin center
- Microsoft Purview compliance portal

Regelt interactive SignIns

Microsoft Graph & Azure Resource Manager APIs

- Regeln über „Windows Azure Service Management API“
- Nicht vergessen: In Users / User Settings Access zu Entra admin center wieder aktivieren

# Access Control – Grant

☒ Require authentication strength ⓘ „Require multifactor authentication“ ersetzen durch „Require authentication strength“

Multifactor authentication... ▼

- ☐ Multifactor authentication ⓘ  
Combinations of methods that
- ☐ satisfy strong authentication, such ⓘ  
as Password + SMS
- ☐ Passwordless MFA
- ☐ Passwordless methods that satisfy ⓘ  
strong authentication, such as ⓘ  
Microsoft Authenticator
- ☐ Phishing-resistant MFA
- ☐ Phishing-resistant Passwordless ⓘ  
methods for the strongest
- For r authentication, such as FIDO2
- ☒ Security Key

# Access Control – Grant

„Require device to be marked as compliant“ und „Require Microsoft Entra hybrid joined device“ ersetzen durch Device filter

- ☒ Grant access
- ☐ Require multifactor authentication ⓘ
  - ☐ Require authentication strength ⓘ
  - ☐ Require device to be marked as compliant ⓘ
  - ☐ Require Microsoft Entra hybrid joined device ⓘ

And/Or	Property	Operator	Value	
	TrustType	Equals	Pick a value	
+ Add expression				
Rule syntax ⓘ				
	IsCompliant	Equals	True	

Microsoft Entra joined  
Microsoft Entra hybrid joined  
Microsoft Entra registered

Edi

Achtung: Ersetzt „Require device to be marked as compliant“ und „Require Microsoft Entra hybrid joined device“



# Access Control – Grant - Require approved client app

---

Wird im März 2026 deaktiviert

Sollte migriert werden zu „Require app protection policy“

- ☐ Require approved client app ⓘ  
[See list of approved client apps](#)
- ☐ Require app protection policy ⓘ  
[See list of policy protected client apps](#)

# Empfohlene „Zusatz-Regeln“

---

## Intune Enrollment

- Nur von trusted networks + Ausnahmegruppe

## MFA Registrierung

- Nur von trusted devices + trusted networks + Ausnahmegruppe

## Block legacy Authentication

- Alles ausser Modern Authentication blocken

## Block other countries

- Erlaubte Länderliste (großzügig) konfigurieren

## Admin block countries

- Alle Adminrollen nur von D bzw A

## Admin – Non persistent Session

# Was prüfe ich bei CondAcc Regeln ?

Doku unbedingt in Excel

#	Name	Benutzer einschließen	Benutzer ausschließen	Cloud Apps einschließen	Cloud Apps	Geräteplattformen	Geräteplattformen	Standorte einschließen	Standorte ausschließen	Client-Apps einschließen	Sign-Risk	User Risk Level	Gerätefilter include Or exclude	Gerätefilter Query	Grant	Session	Kommentar
1	Glass Break Admin	Glass Break Admin		Alle Cloud Apps												Anmeldehäufigkeit 2 Stunden Persistent session: never persistent	
2	Internal Admins	Alle Directory-Rollen anhängen (derzeit 101)	Directory Roles: Directory Sync Account Glass Break Admin Gruppe: NoConAcc, Service Accounts, External Admins Guest or external users: Service provider users (nur bei CSP!)	Alle Cloud Apps											MFA UNID Hybrid Joined	Anmeldehäufigkeit 10 Stunden	
3	External Admins	Gruppe: External Admins	Directory Roles: Directory Sync Account Glass Break Admin Gruppe: NoConAcc	Alle Cloud Apps											MFA	Anmeldehäufigkeit 10 Stunden	
4	User Trusted Device	Alle Benutzer	Gastuser Directory Roles: Directory Sync Account Glass Break Admin Gruppe: NoConAcc, Service Accounts, External Admins	Alle Cloud Apps	Microsoft Intune										Hybrid Joined ODER Compliant		Beide Intune Apps nehmen
5	Intune Enrollment and Compliance State	Alle Benutzer	Directory Roles: Directory Sync Account Glass Break Admin Gruppe: NoConAcc, Intune Enrollment Group	Microsoft Intune				Alle Standorte	Trusted Network				Exclude	Exclude Compliant Intune Exclude Hybrid AzureAD	BLOCK ACCESS		Beide Intune Apps nehmen Intune Enrollment Group für Personen, die ausserhalb enrollen müssen - User danach entfernen!
6	Guest Access	Gastuser	Directory Roles: Directory Sync Account Glass Break Admin Gruppe: NoConAcc Guest or external users: Service provider users (nur bei CSP!)	Alle Cloud Apps											MFA UNID ToC	Anmeldehäufigkeit 10 Stunden	
10	Service Accounts	Gruppe: Service Accounts	Directory Roles: Directory Sync Account Glass Break Admin Gruppe: NoConAcc	Alle Cloud Apps				Alle Standorte	Trusted Network						BLOCK ACCESS		
11	CSP Admins	Guest or external users: Service provider users (nur bei CSP!)	Directory Roles: Directory Sync Account Glass Break Admin	Alle Cloud Apps											MFA	Anmeldehäufigkeit 10 Stunden	

# Was sollst du prüfen

---

## Break Glass Admin

- Vorhanden ? In ALLEN Policies ausgenommen ?

## Alle Benutzer brauchen einen zweiten Faktor

- Fido-Key, Authenticator, SMS, Unternehmensgerät, Unternehmensnetzwerk

## Jede Ausnahme hat eine eigene Regel

## Gibt es Regeln mit mehr als einer INCLUDE Condition ?

- Mehrere INCLUDE Optionen sind ODER!
- Beispiel: Device Platform INCLUDE Windows, Locations: INCLUDE trusted locations  
Bedeutet, ein User kann sich von überall anmelden, wenn er ein Windows Device hat UND er kann sich mit allen Betriebssystemen von trusted locations anmelden!

# Wenn EntraID P2

---

Block High User Risk

Block High Risk Sign-In

- ACHTUNG: 2 Regeln! Sonst ist es wieder ein UND

Für Benutzer mit erhöhten Berechtigungen / Rollen

Block Medium User Risk

Block Medium Sign-In Risk

# Meine Empfehlungen

---

## Zugriff nur von Unternehmensgeräten

- Hybrid-EntraID joined Devices bzw Intune Compliant
- „Normale“ Benutzer können Device als zweiten Faktor nutzen
- Benutzer mit einer Rolle benötigen zusätzlich dritten Faktor

## Benutzer mit Rollen

- Phishing resistant MFA
  - FIDO2 Security Key bzw device-bound Passkey (bald auf EntraID)  
[Prepare for device-bound passkeys in Microsoft Entra ID \(changes to FIDO2 and Windows Hello for Business\) - M365 Admin \(handsontek.net\)](#)