
# Break Glass Admin mit FIDO2 Token

Der Break Glass Admin ist ein globaler Administrator und von allen Conditional Access Policies ausgenommen. Dieses Konto hat ein sehr komplexes Passwort und wird zusätzlich mit einem Hardware FIDO2 Token gesichert. Ob Fehlkonfiguration oder verlorener Zugang: Break Glass Admins ermöglichen es, im Notfall blitzschnell einzugreifen und den Betrieb wiederherzustellen.

IT for innovators.

# Break Glass Admins:

## Ihr Notfallzugang zum Microsoft-365-Tenant

### Warum sollte ein Break Glass Admin eingerichtet werden?

Um sich in der Cloud vor Angriffen zu schützen, sind zunehmend strengere Sicherheitsvorkehrungen nötig. Eine wichtige Maßnahme ist die Multi-Faktor-Authentifizierung (MFA) mit Conditional Access. Dabei besteht jedoch das Risiko, dass Admins sich selbst den Zugriff verweigern. Um dies zu verhindern, werden spezielle Break Glass Admins eingerichtet.

### Was ist ein Break Glass Admin?

Break Glass Admins sind von allen Conditional Access-Richtlinien ausgenommen. Sie verwenden ein äußerst komplexes Passwort und sind zusätzlich durch einen FIDO2-Hardware-Token gesichert. Break Glass Admins werden nur in absoluten Notfällen genutzt, wenn andere Admin-Zugänge versagen. Nach jeder Nutzung ist eine Dokumentation erforderlich und das Passwort muss geändert werden.

### Was wird bei diesem ACP Setup eingerichtet?

ACP richtet für Sie zwei Break Glass Admins mit komplexen Passwörtern und FIDO2-Hardware-Token ein. Um den bestmöglichen Sicherheitsstandard zu erreichen, werden Token eingesetzt, die einen physischen Aktivierungsprozess durch eine Person erfordern. Zusätzlich konfigurieren wir für diese Konten eine Ausnahme für die Conditional Access Policies.
Die Zugangsdaten, einschließlich der Passwörter, werden in verschlossenen Umschlägen sicher aufbewahrt und persönlich an die Geschäftsleitung oder eine autorisierte Vertretung ausgehändigt. Dies muss von Ihnen schriftlich bestätigt werden.
Die Übergabe erfolgt standardmäßig in den ACP Räumlichkeiten, kann auf Wunsch allerdings auch bei Ihnen vor Ort erfolgen. Bitte beachten Sie, dass dabei Fahrtkosten anfallen können. In jedem Fall erfolgt die Übergabe persönlich.

### Welche FIDO2-Hardware-Token werden verwendet?

Für die Sicherung der Break Glass Admins verwenden wir zwei Security Keys C NFC (USB-C).

### An wen richtet sich dieses ACP Setup?

- IT Management
- IT-Sicherheitsverantwortliche
- IT Admins
- CISOs

## Ihre Vorteile des ACP Setups

**Notfallzugriff auf Ihren M365-Tenant**
Sollte der Zugang zum Microsoft-365-Tenant durch technische Probleme (z. B. defektes Handy mit Authenticator-App) oder den Verlust von Zugangsdaten scheitern, gewährleistet das Break Glass Konto den Zugriff.

**Sicherheit auf höchstem Niveau**
Der Break Glass Admin hat keine aktiven Logins und ist zusätzlich mit einem FIDO2-Token gesichert, um maximalen Schutz zu bieten. Als Cloud-only-Konto bleibt es unabhängig von externen Systemen wie Active Directory.

**Überwachung**
Um eine unbefugte Nutzung des Break Glass Admins zu verhindern, werden die Aktivitäten des Notfallbenutzers dokumentiert und überwacht.

**Jetzt nur**
**€ 490,–**
**(exkl. USt.)**

**Sie möchten mehr über unsere Security-Lösungen erfahren?**
Dann wenden Sie sich bitte an:

security@acp.at
www.acp-gruppe.com/fido2