

Entra ID Änderungen

- [Übersicht änderungen Entra / Azure](#)
- [MFA Härtung](#)

MFA Härtung

Einschließen Ausschließen

Ziel Alle Benutzer Gruppen auswählen

Name	Typ	Registrierung	Authentifizierungsmodus
Alle Benutzer	Gruppe	Optional	Kennwortlos

****Dezember 18, 2025 08:30 ** Auf Kennwortlos gewechselt**

Authentifizierungsmethoden | Einstellungen ****Dezember 18, 2025 08:30 ****

Microsoft Entra ID-Sicherheit

Suche

Haben Sie Feedback?

Verwalten

- Richtlinien
- Kennwortschutz
- Registrierungskampagne
- Authentifizierungsstärken
- Einstellungen**

Überwachung

- Aktivität
- Details zur Benutzerregistrierung
- Ereignisse registrieren und zurücksetzen
- Ergebnisse von Massenvorgängen

Verdächtige Aktivität melden

Ermöglicht es Benutzern, verdächtige Aktivitäten zu melden, wenn sie eine Authentifizierungsanforderung erhalten, die sie nicht initiiert haben. Diese Kontrolle ist verfügbar, wenn Sie die Microsoft Authenticator-App und Sprachanrufe verwenden. Durch das Melden verdächtiger Aktivitäten wird das Risiko des Benutzers auf „Hoch“ festgelegt. Wenn der Benutzer risikobasierten Richtlinien bedingten Zugriff unterliegt, wird er möglicherweise blockiert.

[Weitere Informationen](#)

Status * **geändert auf** Aktiviert

Ziel * Alle Benutzer Gruppe auswählen

Berichtscode * 0

Vom System bevorzugte Multi-Faktor-Authentifizierung

Diese Einstellung legt fest, ob Benutzern die sicherste Multi-Faktor-Authentifizierungsmethode angezeigt wird. [Weitere Informationen](#)
Hinweis: Wenn der Featurestatus auf „von Microsoft verwaltet“ festgelegt ist, wird er von Microsoft zu einem geeigneten Zeitpunkt aktiviert. [Weitere Informationen](#)

Status * **geändert auf** Aktiviert

Ausschließen

Ziel **geändert auf** -BreakGlass-

Gruppe

Löschen Haben Sie Feedback?

bersicht

Diagnose und Problembehandlung

Gruppen

Gründlegende Informationen

D Deaktivierte_Methoden_Platzhalter

Diese Gruppe darf keine Mitglieder haben. Sie dient bei ausgegrauten Optionen dazu, niemandem zuzuschließen, um die entsprechende Option trotzdem zu aktivieren.

Mitgliedschaftstyp	Zugewiesen	Direkte Mitglieder g...	0
Quelle	Cloud	Benutzer	0
Typ	Sicherheit	Gruppen	0
Objekt-ID	[Redacted]	Gerät(e)	
Erstellt am	[Redacted]	Andere	0

Feed

Privileged Identity Management

Gruppenrichtlinien

Funktioniert nicht.

Gruppe erstellt um Software Oauth token zu deaktivieren und Nutzung der Authenticatorregistrierung mit OTP zu erhalten

“ Diesen Workaround genutzt um Anmeldung mit Telefon für Authenticator nutzen zu können

Funktioniert nicht, scheint blödsinnig zu sein

... > Gruppen | Übersicht > Authentifizierungsmethoden | Richtlinien > Gruppen | Alle Gruppen > Deaktivierte_Methoden_Platzhalter > Authentifizierungsmethoden | Richtlinien >

Software-OATH-Token-Einstellungen

Software-OATH-Token sind Anwendungen, die den OATH-TOTP-Standard und einen geheimen Schlüssel verwenden, um 6-stellige Codes zur Authentifizierung zu generieren. Diese Richtlinieneinstellung verwaltet die Möglichkeit, Authenticator-Apps einschließlich Microsoft Authenticator zu registrieren und zu verwenden, um Software-OATH-Token zu verwalten. Software-OATH-Token können für die Multi-Faktor-Authentifizierung und Self-Service-Kennwortzurücksetzungsflows verwendet werden. [Weitere Informationen](#).

Das Software-OATH-Token kann nicht als Einfaktor-Authentifizierungsmethode verwendet werden.

Aktivieren und Ziel

Aktivieren

Bei deaktivieren soll angeblich Authenticator Registrierung nicht mehr funktionieren mit OTP

Einschließen Ausschließen

Gruppen hinzufügen

Name	Typ
Deaktivierte_Methoden_Platzhalter	Gruppe

leere Gruppe, da verbote eher greifen als freigaben