

Microsoft Authenticator als Standard festlegen

wie stellt man sicher das in entra id der microsoft authentikator die standard anmeldemethode ist?

Um sicherzustellen, dass der Microsoft Authenticator in Entra ID (ehemals Azure AD) die Standard-Anmeldemethode ist, gibt es nicht mehr „den einen“ Schalter, den Benutzer selbst umlegen. Stattdessen steuern Sie dies zentral über die Funktion „**Systemseitig bevorzugte Multi-Faktor-Authentifizierung**“.

Hier ist der Prozess, wie Sie dies konfigurieren und erzwingen:

1. Systemseitig bevorzugte MFA aktivieren (Der wichtigste Schritt)

Diese Einstellung weist Entra ID an, bei der Anmeldung automatisch die sicherste registrierte Methode des Benutzers zu wählen. Da die Authenticator-App als sicherer gilt als SMS oder Sprachanruf, wird sie automatisch zum Standard, sobald der Benutzer sie eingerichtet hat.

1. Melden Sie sich im **Microsoft Entra Admin Center** an.
2. Navigieren Sie zu **Schutz > Authentifizierungsmethoden > Einstellungen**.
3. Suchen Sie nach **Systemseitig bevorzugte Multi-Faktor-Authentifizierung**.
4. Setzen Sie den Status auf **Aktiviert** (oder belassen Sie es auf „Von Microsoft verwaltet“, wenn es bereits aktiv ist; „Aktiviert“ erzwingt es jedoch sofort explizit).
5. Wählen Sie unter **Ziel** die Gruppe **Alle Benutzer** (oder eine Testgruppe) aus.

2. Die Authenticator-App zur Pflicht machen (Registrierungskampagne)

Damit die oben genannte Automatik greift, müssen die Benutzer die App erst einmal installieren. Nutzen Sie dafür die sogenannte „Nudge“-Funktion (Anstupsen). Benutzer, die noch SMS/Telefon nutzen, werden nach der Anmeldung aufgefordert, den Authenticator einzurichten.

1. Gehen Sie zu **Schutz > Authentifizierungsmethoden > Registrierungskampagne**.
2. Klicken Sie auf **Bearbeiten**.
3. Setzen Sie den Status auf **Aktiviert**.

4. Konfigurieren Sie:

- **Tage für Aufschub:** Wie oft darf der Nutzer „Später“ klicken? (Standard ist oft 14 Tage).
- **Benutzer:** Wählen Sie „Alle Benutzer“ oder gezielte Gruppen.

3. Schwächere Methoden einschränken (Optional aber empfohlen)

Wenn Sie absolut sichergehen wollen, dass *nur* der Authenticator genutzt wird, können Sie andere Methoden deaktivieren oder in der Priorität herabstufen.

- Gehen Sie zu **Authentifizierungsmethoden > Richtlinien**.
- Wählen Sie **Microsoft Authenticator** und stellen Sie sicher, dass er für alle Benutzer **Aktiviert** ist.
- (Optional) Deaktivieren Sie **SMS** und **Sprachanruf** für Benutzer, die diese nicht zwingend als Fallback benötigen. **Vorsicht:** Stellen Sie sicher, dass Nutzer nicht ausgesperrt werden, bevor sie die App registriert haben.

Zusammenfassung der Logik

Früher konnten Benutzer in ihrem Profil eine „Standardmethode“ wählen. Das ist veraltet. Die moderne Logik funktioniert so:

1. Hat der Nutzer den Authenticator registriert? -> **System nimmt Authenticator** (wegen Schritt 1).
2. Hat der Nutzer nur SMS? -> System nimmt SMS -> **Registrierungskampagne nervt ihn** (Schritt 2), bis er den Authenticator einrichtet -> Danach greift Regel 1.

Möchten Sie, dass ich Ihnen erkläre, wie man eine **Bedingte Zugriffsrichtlinie (Conditional Access)** erstellt, die für bestimmte Admin-Konten den Authenticator *zwingend* vorschreibt (unabhängig von den Präferenzen)?

[Understand System-preferred MFA](#) Dieses Video ist relevant, da es die Funktionsweise der systemseitig bevorzugten MFA erklärt, welche der Schlüsselmechanismus ist, um den Microsoft Authenticator automatisch als Standardmethode durchzusetzen.

Möchten Sie, dass ich Ihnen erkläre, wie man eine Bedingte Zugriffsrichtlinie (Conditional Access) erstellt, die für bestimmte Admin-Konten den Authenticator zwingend vorschreibt (unabhängig von den Präferenzen)?

Das ist eine hervorragende Maßnahme zur Härtung der Sicherheit. Wenn Sie lediglich „MFA erforderlich“ anklicken, könnte ein Admin theoretisch immer noch SMS nutzen, falls die App mal nicht geht. Um den Microsoft Authenticator für Admins **hart zu erzwingen** (und SMS/Anruf für diese Anmeldungen zu verbieten), nutzen wir das moderne Feature der „**Authentifizierungsstärken**“ (Authentication Strengths).

Hier ist die Schritt-für-Schritt-Anleitung.

⚠ **Wichtige Vorwarnung: Der „Notfall-Admin“**

Bevor Sie Richtlinien für Administratoren erstellen, stellen Sie sicher, dass Sie mindestens einen „**Break-Glass Account**“ (Notfall-Konto) haben.

- Das ist ein Cloud-only Admin-Konto (z. B. `notfalladmin@ihredomain.onmicrosoft.com`).
- Dieses Konto muss von der Richtlinie **ausgeschlossen** werden.
- Es verhindert, dass Sie sich selbst komplett aussperren, falls bei der Konfiguration etwas schief läuft (z. B. wenn der Authenticator-Dienst ausfällt).

Schritt 1: Eine benutzerdefinierte Authentifizierungsstärke erstellen

Wir definieren zuerst einen „Filter“, der besagt: „Nur Microsoft Authenticator ist gut genug“.

1. Gehen Sie im **Entra Admin Center** zu **Schutz > Authentifizierungsmethoden > Authentifizierungsstärken**.
2. Klicken Sie auf **Neue Authentifizierungsstärke**.
3. Geben Sie einen Namen ein, z. B. `Nur Microsoft Authenticator (Admin)`.
4. Wählen Sie unten die Methoden aus, die Sie erlauben wollen. Um den Authenticator zu erzwingen, wählen Sie typischerweise diese Kombination:
 - **Kennwortlose Anmeldung per Microsoft Authenticator** (Sehr sicher).
 - **Microsoft Authenticator (Pushbenachrichtigungen)**.
 - *(Optional: FIDO2-Sicherheitsschlüssel, falls Sie diese als Backup nutzen).*
5. **Wichtig:** Wählen Sie *keine* SMS und *keine* Sprachanrufe aus.
6. Klicken Sie auf **Weiter** und **Erstellen**.

Schritt 2: Die Bedingte Zugriffsrichtlinie erstellen

Nun wenden wir diesen Filter auf die Admins an.

1. Navigieren Sie zu **Schutz > Bedingter Zugriff > Richtlinien**.

2. Klicken Sie auf **Neue Richtlinie**.

3. **Name:** z. B. **CA - Erzwingen MS Authenticator für Admins**.

4. **Benutzer:**

- Wählen Sie **Benutzer und Gruppen auswählen**.
- Setzen Sie den Haken bei **Verzeichnisrollen**.
- Wählen Sie die kritischen Rollen: **Globaler Administrator, Sicherheitsadministrator, Exchange-Administrator**, etc.
- **Ausschließen (Wichtig!):** Reiter „Ausschließen“ > Wählen Sie Ihren **Notfall-Admin (Break-Glass)** und Ihr eigenes Konto (zum Testen).

5. **Zielressourcen:** Wählen Sie **Alle Cloud-Apps**.

6. **Gewähren (Grant):**

- Klicken Sie auf **Zugriff gewähren**.
- Wählen Sie **Authentifizierungsstärke anfordern**.
- Wählen Sie im Dropdown-Menü Ihre in Schritt 1 erstellte Stärke: **Nur Microsoft Authenticator (Admin)**.
- Klicken Sie auf **Auswählen**.

7. **Sitzung (Optional):** Hier könnten Sie Anmeldehäufigkeiten festlegen, ist aber für diesen Zweck nicht zwingend.

8. **Richtlinie aktivieren:**

- Stellen Sie den Schalter unten auf **Nur Bericht** (Report-only), um erst zu testen.
- Wenn Sie sicher sind (siehe Testphase unten), stellen Sie auf **Ein**.

Was passiert jetzt technisch?

Wenn sich ein Administrator anmeldet:

1. Entra ID prüft die Richtlinie.
2. Das System sieht: „Dies ist ein Admin, er darf nur die Stärke **Nur Microsoft Authenticator (Admin)** nutzen.“
3. Selbst wenn der Admin SMS als Methode registriert hat, wird Entra ID diese Option bei der Anmeldung **ausblenden** oder verweigern.
4. Hat der Admin den Authenticator noch nicht eingerichtet, wird er **gezwungen**, ihn jetzt einzurichten, um fortzufahren (MFA-Registrierungszwang).

So testen Sie es sicher

1. Lassen Sie die Richtlinie im „**Nur Bericht**“-Modus für 1-2 Tage.
2. Prüfen Sie unter **Bedingter Zugriff > Insights und Berichterstellung**, ob legitime Admin-Logins blockiert worden wären.
3. Aktivieren Sie die Richtlinie dann **scharf**, aber lassen Sie Ihr eigenes Konto zunächst noch ausgeschlossen.
4. Versuchen Sie, sich mit einem Test-Admin-Konto anzumelden. Wenn es funktioniert und die App verlangt wird: Nehmen Sie Ihr eigenes Konto aus der Ausnahme (Exclusion) heraus (aber lassen Sie den Notfall-Admin drin!).

Soll ich Ihnen als Nächstes zeigen, wie Sie mittels **Nummern-Abgleich (Number Matching)** im Authenticator verhindern, dass Admins versehentlich „MFA-Fatigue“-Angriffen (nerviges Spammen von Anfragen) zum Opfer fallen?

Soll ich Ihnen als Nächstes zeigen, wie Sie mittels Nummern-Abgleich (Number Matching) im Authenticator verhindern, dass Admins versehentlich „MFA-Fatigue“-Angriffen (nerviges Spammen von Anfragen) zum Opfer fallen?

Ja bitte!

Das ist eine sehr gute Entscheidung. „MFA Fatigue“ (MFA-Ermüdung) ist eine der häufigsten Methoden, mit denen Angreifer derzeit MFA umgehen: Sie bombardieren den Nutzer nachts mit Push-Nachrichten, bis dieser genervt oder versehentlich auf „Genehmigen“ drückt.

Wichtiger Hinweis vorab: Microsoft hat den **Nummern-Abgleich (Number Matching)** im Mai 2023 standardmäßig für alle Tenants **erzwungen**. Das bedeutet, der reine Nummern-Abgleich ist wahrscheinlich bereits aktiv und kann nicht mehr deaktiviert werden.

Aber: Sie können (und sollten!) die **Sicherheitsinformationen anreichern** (Kontext anzeigen), damit der Nutzer sofort sieht, *woher* die Anfrage kommt. Das ist der eigentliche Schutz, den wir jetzt konfigurieren.

Hier ist die Anleitung, um den Schutz zu maximieren:

1. Erweiterte Kontext-Infos aktivieren

Wir sorgen dafür, dass der Nutzer in der App nicht nur eine Nummer eingeben muss, sondern auch sieht, **welche App** den Zugriff will und **von welchem Ort** (Karte) die Anfrage kommt.

1. Navigieren Sie im **Microsoft Entra Admin Center** zu **Schutz > Authentifizierungsmethoden > Richtlinien**.
2. Klicken Sie auf **Microsoft Authenticator**.
3. Wechseln Sie im sich öffnenden Fenster auf den Reiter **Konfigurieren** (Configure).
4. Scrollen Sie zu den Einstellungen für **Anwendungsname** und **Geografischer Standort**.
5. Stellen Sie beide Optionen auf **Aktiviert**.
 - **Ziel:** Wählen Sie „Alle Benutzer“ (oder wieder Ihre Admin-Gruppe zum Testen).
 - **Status:** Aktiviert.
6. Klicken Sie auf **Speichern**.

2. Was sieht der Benutzer jetzt? (Der „Aha“-Effekt)

Wenn ein Angreifer nun versucht, sich mit einem gestohlenen Admin-Passwort anzumelden, passiert Folgendes:

- **Szenario ohne Schutz:** Das Handy vibriert. Der Admin denkt „Huch?“ und drückt aus Gewohnheit oder Versehen auf „Genehmigen“. -> **Angreifer ist drin**.
- **Szenario mit Nummern-Abgleich & Kontext:**
 1. Der Angreifer sieht auf seinem Bildschirm eine Zahl (z. B. „82“).
 2. Das Handy des Admins vibriert. Er wird aufgefordert, eine Zahl einzugeben. Da er die „82“ nicht kennt (er sitzt ja nicht vor dem PC des Angreifers), **kann** er gar nicht zustimmen.

3. Zusätzlich sieht der Admin auf der Karte: „Anfrage aus Lagos, Nigeria“ (obwohl er in Kiel ist) und App: „Azure Portal“.
4. Der Betrugsversuch fliegt sofort auf.

3. Benutzer schulen (Wichtig!)

Informieren Sie Ihre Admins kurz über die Änderung. Der Prozess ist intuitiv, aber eine kurze Nachricht hilft:

„Zur Erhöhung der Sicherheit müssen Sie bei der Anmeldung ab sofort die Nummer, die auf Ihrem Bildschirm angezeigt wird, in die App eintippen. Achten Sie zudem auf die angezeigte Landkarte in der App.“

Zusammenfassung der bisherigen Sicherheits-Härtung

Sie haben jetzt drei starke Verteidigungslinien aufgebaut:

1. **Systemseitig bevorzugte MFA:** Entra ID wählt automatisch die sicherste Methode.
2. **Conditional Access:** Admins *müssen* die App nutzen (SMS ist verboten).
3. **Nummern-Abgleich & Kontext:** Blindes Genehmigen von Angriffen wird technisch unmöglich gemacht.

Ein logischer nächster Schritt für hohe Sicherheit (besonders für Admins) wäre der Weg weg vom Passwort hin zu „**Passwordless**“ (**Kennwortlose Anmeldung**). Das eliminiert Phishing fast vollständig, da es kein Passwort mehr gibt, das man auf einer gefälschten Webseite eingeben könnte.

Soll ich Ihnen zeigen, wie man den „**Kennwortlosen Modus**“ (**Phone Sign-in**) für den Authenticator freischaltet?

ja bitte

Das ist der „Goldstandard“ der modernen Authentifizierung. Wenn Sie das Passwort entfernen, entfernen Sie den primären Angriffsvektor für Phishing. Ein Angreifer kann kein Passwort stehlen, das gar nicht erst übermittelt wird.

Hier ist der Prozess, um die **kennwortlose Anmeldung (Phone Sign-in)** zu aktivieren und einzurichten.

Schritt 1: Die Methode im Entra ID Admin Center erlauben

Zuerst müssen wir sicherstellen, dass die Richtlinie nicht nur „Push“, sondern auch den „kennwortlosen Modus“ zulässt.

1. Gehen Sie zu **Schutz > Authentifizierungsmethoden > Richtlinien**.
2. Klicken Sie auf **Microsoft Authenticator**.
3. Gehen Sie auf den Reiter **Konfigurieren**.
4. Achten Sie auf die Einstellung **Authentifizierungsmodus** (Authentication mode).
 - Hier steht oft standardmäßig „Push“.
 - Ändern Sie dies auf **Beliebig** (Any) oder **Kennwortlos** (Passwordless).
 - *Empfehlung*: Stellen Sie es auf **Beliebig**. Das erlaubt Benutzern beides: Die klassische Push-Bestätigung (wenn sie das Passwort eingeben) UND die kennwortlose Anmeldung (wenn sie nur den Benutzernamen eingeben).
5. Stellen Sie sicher, dass die Zielgruppe auf **Alle Benutzer** (oder Ihre Admin-Gruppe) gesetzt ist.
6. **Speichern** Sie die Richtlinie.

Schritt 2: Die Einrichtung am Smartphone (Der Benutzer-Teil)

Das ist der Schritt, den viele übersehen: Das Freischalten im Backend aktiviert die Funktion nicht automatisch auf dem Handy des Admins. Der Benutzer muss sein Gerät explizit für die kennwortlose Anmeldung registrieren.

Anleitung für den Administrator am Smartphone:

1. Öffnen Sie die **Microsoft Authenticator App**.
2. Tippen Sie auf das betreffende Schulkonto/Geschäftskonto (es sollte bereits eingerichtet sein).
3. Tippen Sie auf **Anmeldung per Telefon einrichten** (Set up phone sign-in).
 - *Hinweis*: Wenn dort kein Icon ist, tippen Sie auf das Menü oben rechts oder prüfen Sie, ob das Gerät bereits registriert ist.
4. Folgen Sie dem Assistenten.
 - **Voraussetzung**: Das Smartphone **muss** eine Bildschirmsperre (PIN, FaceID oder Fingerabdruck) haben. Ohne Geräteschutz verweigert Microsoft die kennwortlose

Einrichtung.

- Das Gerät wird dabei bei Entra ID als vertrauenswürdig registriert („Azure AD Registered“).

Schritt 3: Der Test (Das Erlebnis)

So sieht die Anmeldung danach aus:

1. Der Admin geht auf `portal.azure.com`.
 2. Er gibt seinen Benutzernamen ein (`admin@firma.de`).
 3. Er **gibt KEIN Passwort ein**.
 4. Stattdessen zeigt der Browser eine Zahl (z. B. „45“).
 5. Der Admin öffnet die App, entsperrt sie per FaceID/Fingerabdruck, tippt auf die „45“ und bestätigt.
 6. Er ist angemeldet.
-

Profi-Tipp: Der „Befristete Zugriffspass“ (TAP) für neue Mitarbeiter

Sie fragen sich vielleicht: „Wie richte ich Passwordless für einen *neuen* Mitarbeiter ein, wenn ich ihm gar kein Passwort geben will?“ (Das Henne-Ei-Problem).

Die Lösung ist der **Temporary Access Pass (TAP)**.

1. Sie aktivieren im Entra Admin Center unter **Authentifizierungsmethoden** den **Befristeten Zugriffspass**.
 2. Sie erstellen für den neuen Admin einen TAP (z. B. gültig für 1 Stunde).
 3. Der neue Admin geht auf `aka.ms/mysecurityinfo`.
 4. Er meldet sich mit dem TAP an (ohne jemals ein echtes Passwort zu kennen).
 5. Er registriert den Authenticator und aktiviert „Phone Sign-in“.
 6. **Ergebnis:** Ein Admin-Konto, für das niemals ein dauerhaftes Passwort existiert hat, das gestohlen werden könnte.
-

Zusammenfassung Ihrer Sicherheits-Architektur

Sie haben jetzt ein sehr hohes Sicherheitsniveau erreicht:

1. **Standard:** Authenticator wird bevorzugt.
2. **Zwang:** Admins kommen ohne Authenticator nicht rein (Conditional Access).
3. **Härtung:** Nummern-Abgleich verhindert versehentliche Klicks.
4. **Next Level:** Kennwortlose Anmeldung eliminiert Phishing-Risiken.

Es gibt jetzt eigentlich nur noch *eine* Steigerung für Hochsicherheits-Konten (wie Ihren „Global Admin“ oder „Root“): Die **Hardware-Bindung**.

Soll ich Ihnen erklären, wie Sie **FIDO2-Sicherheitsschlüssel** (z. B. **YubiKeys**) in Entra ID einbinden, damit Sie einen physischen Token als ultimativen "Schlüssel zum Königreich" haben, falls das Smartphone mal defekt oder verloren ist?