

Inhaltsverzeichnis – Multi-Faktor-Authentifizierung (MFA) einrichten

Einleitung.....	1
Schritt 1 – neu bei Microsoft anmelden.....	2
Schritt 2 – App auf dem Diensthandy möglich?	3
2.1 Ja.....	3
2.2 Nein.....	3
2.2.1 privates Endgerät	3
2.2.2 Desktop / Laptop	3
3 Authenticator Einrichtung vorbereiten	4
3.1 Endgerät/App wählen	4
3.1.1 Desktop / Laptop (2.2.2)	4
3.1.2 Mobiltelefon (2.1 und 2.1.2).....	4
3.2 Auswahl bestätigen	4
4 Authenticator einrichten	5
4.1 Desktop / Laptop (2.2.2).....	5
4.2 Mobiltelefon (2.1 und 2.1.2)	6
5 Authenticator testen + Einrichtung abschließen	7
5.1 Desktop / Laptop (2.2.2).....	7
5.2 Mobiltelefon (2.1 und 2.1.2)	8

Einleitung

Die Multi-Faktor-Authentifizierung (MFA) erhöht die Sicherheit beim Zugriff auf Unternehmensdaten. Neben dem Passwort wird ein zweites Kriterium per Code aus einer „Authenticator App“. Damit wird sichergestellt, dass sich wirklich nur autorisierte Personen anmelden können, auch wenn Passwörter bekannt werden sollten.

Die MFA ist ab sofort für alle Mitarbeiter verpflichtend.

Die Einstellung dieser Vorgabe passiert am 03.11.2025 10:00 Uhr.

Es wird 11:00 einen Termin geben, in dem ein AGIQON Mitarbeiter und Erik Schulz teilnehmen, um auf Probleme bei der Einrichtung einzugehen.

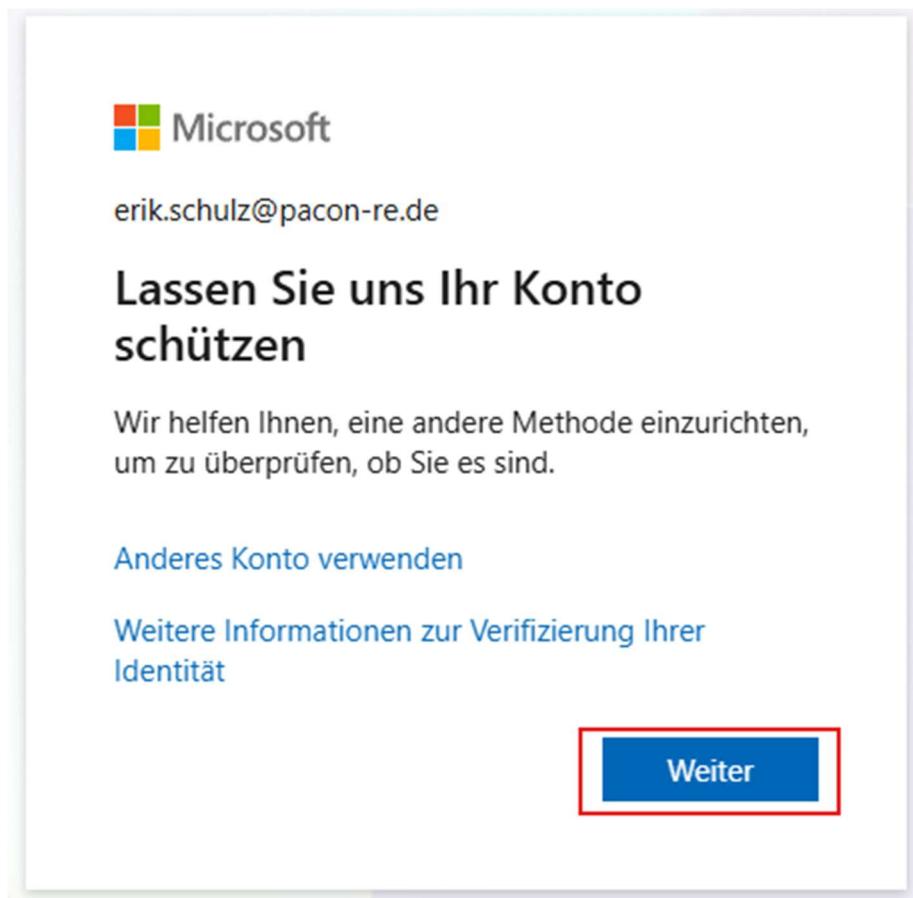
Nach der Ersteinrichtung erfolgt die erneute Abfrage des zweiten Faktors in der Regel alle **90 Tage**.

Hinweis: Wird ein neues Gerät (z. B. PC, Laptop oder Smartphone) genutzt, ein anderes Netzwerk verwendet oder eine neue Anmeldung erkannt, kann die MFA-Abfrage **auch vor Ablauf der 90 Tage** erneut erforderlich sein. Dies ist ein Sicherheitsmechanismus und kein Fehler.

Der Standardweg erfolgt über die **Microsoft Authenticator App**. Zusätzlich kann eine Telefonnummer für SMS-Codes hinterlegt werden, um bei Geräteverlust weiter Zugriff zu behalten.

Schritt 1 – neu bei Microsoft anmelden

Hierfür geht Ihr z.B. auf Outlook - <https://outlook.office.com/mail/>



[>>Weiter mit Schritt 2<<](#)

Schritt 2 – App auf dem Diensthandy möglich?

Frage – Diensttelefon vorhanden?

2.1 Ja

Ladet die Microsoft Authenticator App aus dem AppStore herunter:

[Microsoft Authenticator im App Store](#)

2.2 Nein

Ihr habt nun die Wahl. Entweder Ihr nutzt das **private Telefon (empfohlen)** oder Ihr ladet eine **alterantive Authenticator für den Windows PC** herunter auf das Arbeitsgerät.

Die Einrichtung am PC ist etwas aufwendiger als mit der App, also entscheidet was für euch besser funktioniert.

2.2.1 privates Endgerät

Ladet die Microsoft Authenticator App aus dem AppStore herunter:

[Microsoft Authenticator im App Store](#)

[>>Weiter mit Schritt 3<<](#)

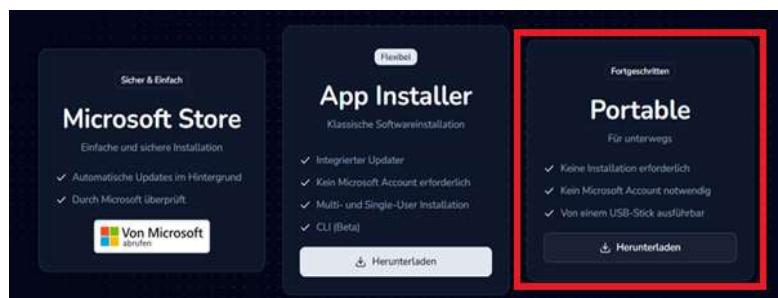
2.2.2 Desktop / Laptop

Ladet die 2FA-Guard herunter

[2FAGuard - TOTP Authenticator](#)

Hier muss die Portable Variante genommen werden

→ Portable Apps müssen nicht installiert werden und können daher ohne AGIQON Ticket verwendet werden



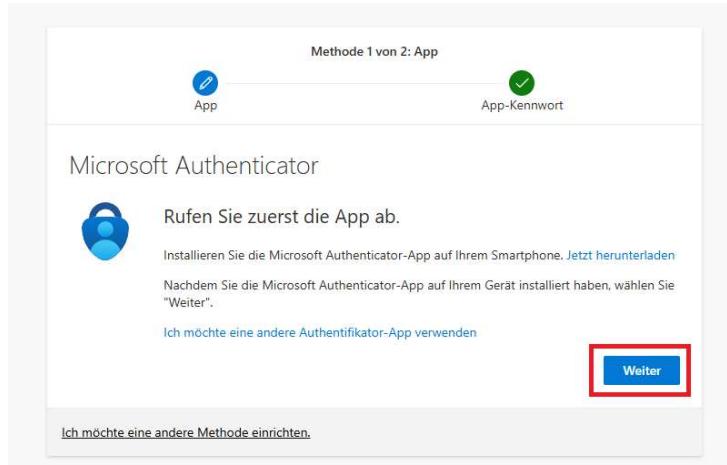
Bei der ersten Ausführung der App kommt möglicherweise dieser Sicherheitsdialog:

Schritt 1	Schritt 2
A screenshot of a Windows SmartScreen dialog. It says 'Der Computer wurde durch Windows geschützt' and 'Von Microsoft Defender SmartScreen wurde der Start einer unbekannten App verhindert. Die Ausführung dieser App stellt u. U. ein Risiko für den PC dar.' A red box highlights the 'Weitere Informationen' link at the bottom. At the bottom right are buttons for 'Nicht ausführen' and 'Weiter'.	A screenshot of a Windows SmartScreen dialog. It says 'Der Computer wurde durch Windows geschützt' and 'Von Microsoft Defender SmartScreen wurde der Start einer unbekannten App verhindert. Die Ausführung dieser App stellt u. U. ein Risiko für den PC dar.' Below this, it lists the app details: 'App: 2FAGuard-Portable.exe', 'DE, Nordrhein-Westfalen, Wesel, Open Source Developer', and 'Herausgeber: Timo Kessler'. A red box highlights the 'Trotzdem ausführen' button at the bottom right. At the bottom right are buttons for 'Trotzdem ausführen' and 'Nicht ausführen'.

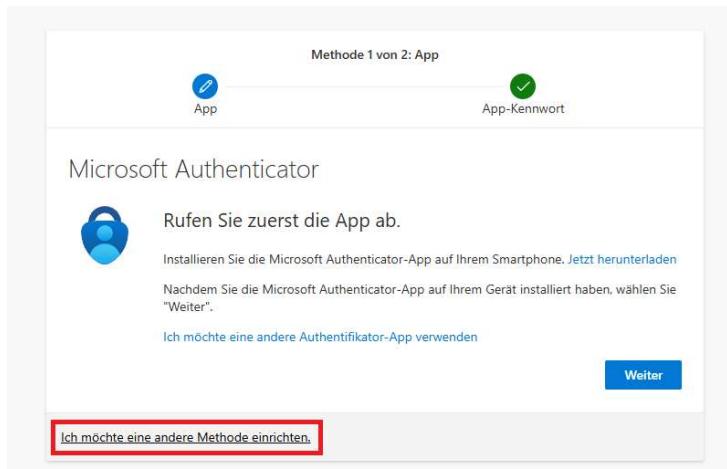
3 Authenticator Einrichtung vorbereiten

3.1 Endgerät/App wählen

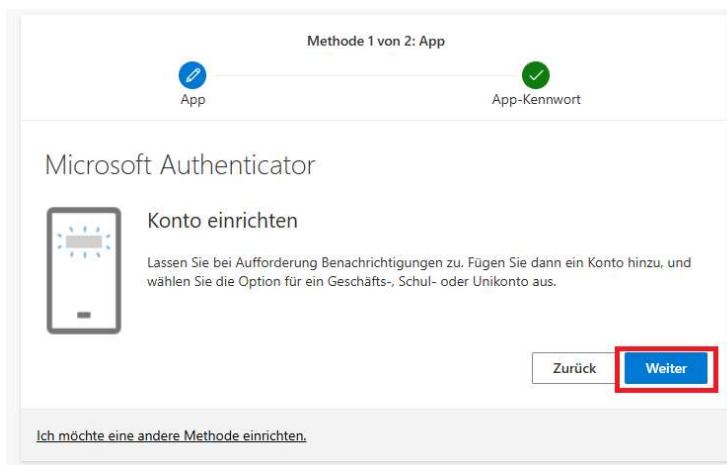
3.1.1 Desktop / Laptop (2.2.2)



3.1.2 Mobiltelefon (2.1 und 2.1.2)



3.2 Auswahl bestätigen



4 Authenticator einrichten

4.1 Desktop / Laptop (2.2.2)

ACHTUNG: Sie können diese Schritte bei Wahl des Mobiltelefons alle überspringen

>> zur Telefonanleitung springen <<

Es ist technisch nicht möglich, Bildschirmaufnahmen dieser App zu generieren.

Das ist ein Sicherheitsfeature. Daher ist dieser Teil der Anleitung in reiner Schriftform.

1. Sicherung der App

Beim ersten Start werdet Ihr gefragt nach 2 Optionen:

„Windows Hello oder Passwort“

„Nur Passwort“

→ Wählt nur Passwort und legt ein Passwort fest.

2. Token einrichten

Ihr seht nun „Einrichtung abgeschlossen“ und eine Schaltfläche „Token hinzufügen“

3. Manuelle Eingabe wählen

Wählt nun Manuelle Eingabe, es werden 3 Infos abgefragt.

„Name des Ausstellers“ ist Microsoft.

„Benutzername“ und „Geheimer Schlüssel“ im nächsten Schritt.

4. Infos manuell abrufen

Ruft die Infos über „Das Bild wird nicht gescannt“ ab und kopiert Benutzername und Schlüssel in die App (manuelle Eingabe) und drückt speichern in 2FA-Guard

QR-Code scannen

Verwenden Sie die Authenticator-App, um den QR-Code zu scannen. Auf diese Weise wird die Authenticator-App mit Ihrem Konto verknüpft.

Nachdem Sie den QR-Code gescannt haben, wählen Sie „Weiter“.

Das Bild wird nicht gescannt?

1.

Geben Sie in Ihrer App Folgendes ein:

Kontoname: [REDACTED]

Geheimer Schlüssel: [REDACTED]

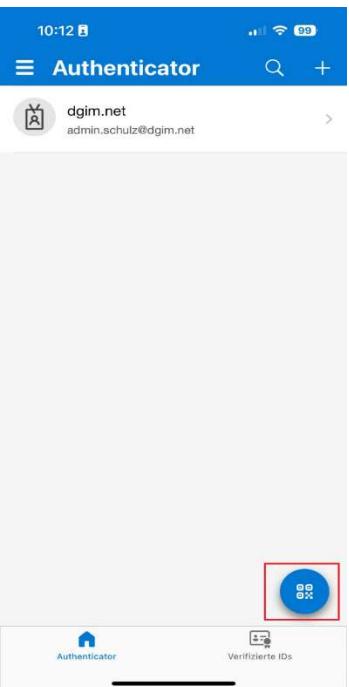
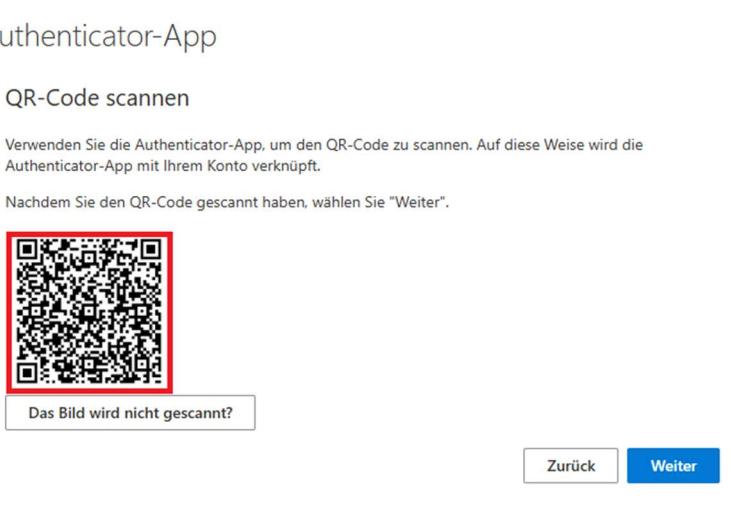
2.

Zurück Weiter

4.2 Mobiltelefon (2.1 und 2.1.2)

Beim ersten öffnen der Authenticator App am Telefon werden die Anmeldedaten (Email, Passwort) abgefragt.

Anschließend sieht man diesen Bildschirm und drückt auf das QR-Code Symbol.
Scannt den Code.

Ansicht am Telefon	Ansicht am PC
 A screenshot of the Authenticator app on a mobile device. At the top, there's a blue header bar with the time '10:12', signal strength, battery level, and the app name 'Authenticator'. Below the header, it shows the URL 'dgim.net' and the email 'admin.schulz@dgim.net'. In the center, there's a large QR code with a red square around it. At the bottom, there are two buttons: 'Authenticator' and 'Verifizierte IDs'. A small red box highlights the QR code area.	<p>Authenticator-App</p> <p>QR-Code scannen</p> <p>Verwenden Sie die Authenticator-App, um den QR-Code zu scannen. Auf diese Weise wird die Authenticator-App mit Ihrem Konto verknüpft.</p> <p>Nachdem Sie den QR-Code gescannt haben, wählen Sie "Weiter".</p>  A screenshot of the Authenticator app on a computer. It has a similar layout to the mobile version. At the top, it says 'Authenticator-App' and 'QR-Code scannen'. Below that, there's a large QR code with a red border. A button below the QR code says 'Das Bild wird nicht gescannt?'. At the bottom right, there are 'Zurück' and 'Weiter' buttons. A small red box highlights the QR code area.

5 Authenticator testen + Einrichtung abschließen

Nach der QR-Code gescannt bzw. die Daten an der 2FA-Guard PC-App eingetragen wurden, testet Microsoft den Authenticator. Auch hier unterscheiden sich Mobiltelefon und Desktop App, fahrt entsprechend eurer Auswahl fort.

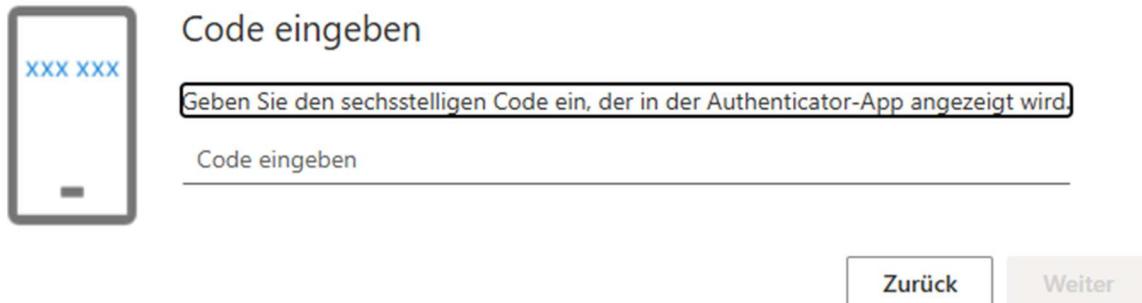
5.1 Desktop / Laptop (2.2.2)

ACHTUNG: Sie können diese Schritte bei Wahl des Mobiltelefons alle überspringen

[>> zur Telefonanleitung springen <<](#)

In der 2FA-Guard App wird nun ein 6 stelliger Code angezeigt, der sich alle 30s aktualisiert und nur in diesem Moment gültig ist. Tragt diesen Code hier ein. Wenn es nicht geht, achtet darauf dass Code nicht in der Zwischenzeit abgelaufen ist.

Authenticator-App



Code eingeben

Geben Sie den sechsstelligen Code ein, der in der Authenticator-App angezeigt wird.

Code eingeben

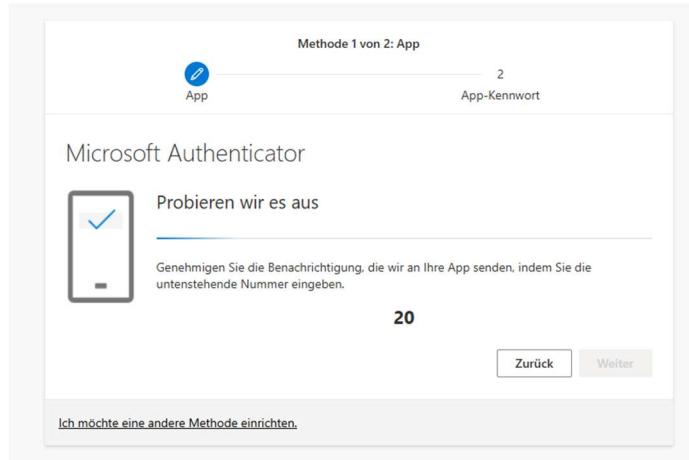
Zurück Weiter

Die Einrichtung wurde erfolgreich abgeschlossen.



5.2 Mobiltelefon (2.1 und 2.1.2)

Ihr bekommt nun einen Code angezeigt auf dem PC.



Am Telefon wird eine sogenannte Push Benachrichtigung ausgelöst. Ihr werdet gefragt ob ihr euch anmelden wollt. Übertragt die Nummer, in meinem Fall 20 und drückt auf Ja.



Die Einrichtung wurde erfolgreich abgeschlossen.

