

Schritt-für-Schritt-Anleitung empfohlene Varianten

I Einrichtung MFA mit der Microsoft Authenticator App

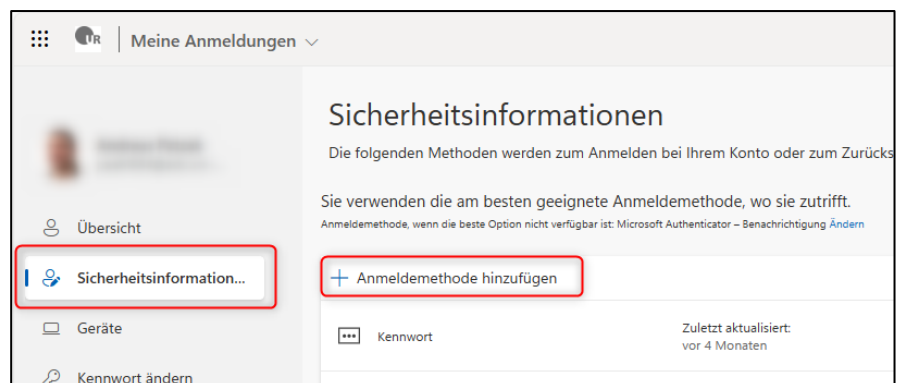
II Einrichtung MFA mit Windows Hello for Business (nur für Beschäftigte)

Wählen Sie **eine der beiden Optionen** I oder II aus und orientieren Sie sich bei der Einrichtung an den in dieser Anleitung beschriebenen Teilschritten.

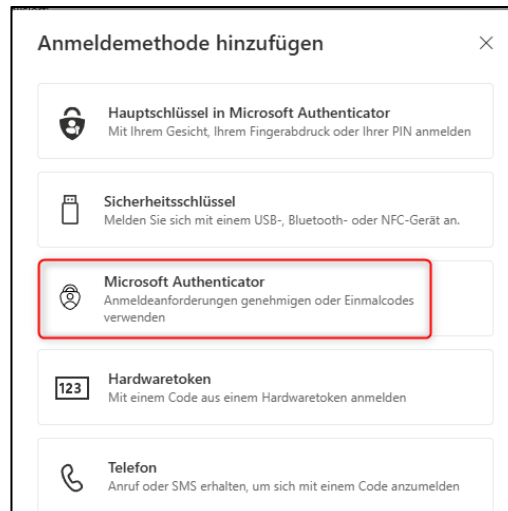
I Einrichtung MFA mit der Microsoft Authenticator App

1. Klicken Sie mit der Maus auf folgenden Link <https://aka.ms/mfasetup> und melden sich mit Ihrem persönlichen Account (RZ-Account@ads.uni-regensburg.de, z. B. „vip12345@ads.uni-regensburg.de“) an.

2. „+ Anmeldemethode hinzufügen“.

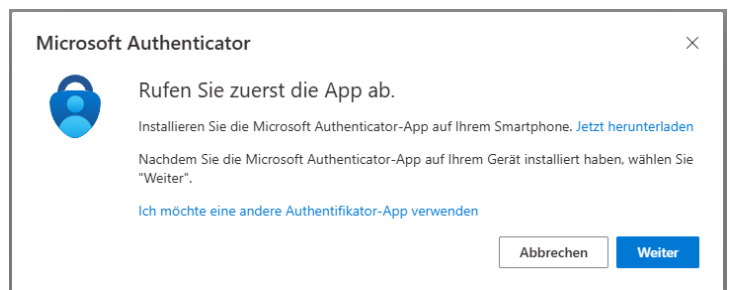


3. Wählen Sie „**Microsoft Authenticator**“.



4. Es erscheint ein Fenster „**Rufen Sie zuerst die App ab**“.

Bleiben Sie auf dieser Website und führen zunächst die Installation der Microsoft Authenticator App auf dem Smartphone durch.



5. Auf dem Smartphone: Installation der Microsoft Authenticator App

Scannen Sie dazu den QR-Code oder suchen Sie im jeweiligen Store nach „Microsoft Authenticator“.

Android: [Google Play Store](#)



iPhone: [App Store](#)



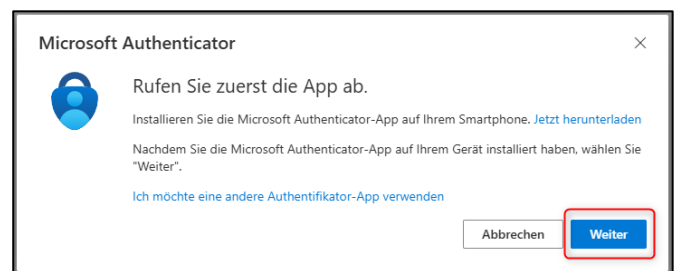
Öffnen Sie nach der Installation die App und bestätigen alle Anfragen, bis Ihnen in einer Anzeige die Option „**QR-Code scannen**“ angeboten wird.

Hinweis:

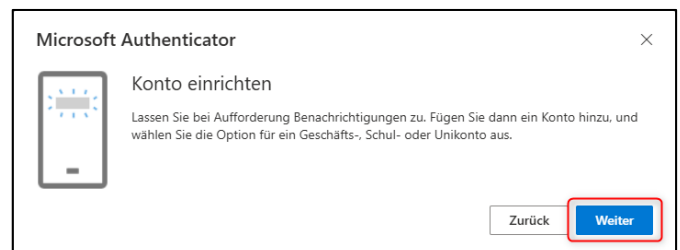
Wenn Sie den Microsoft Authenticator bereits auf Ihrem Smartphone installiert haben, können Sie das UR-Konto hinzufügen, indem Sie oben rechts auf das **[+]** Symbol klicken, **Geschäfts- oder Schulkonto** auswählen und dann den QR-Code scannen.

Fahren Sie mit der Konfiguration **am PC** fort.

6. Setzen Sie die Konfiguration fort, indem Sie die Meldung „Rufen Sie zuerst die App auf“ mit „**Weiter**“ bestätigen.

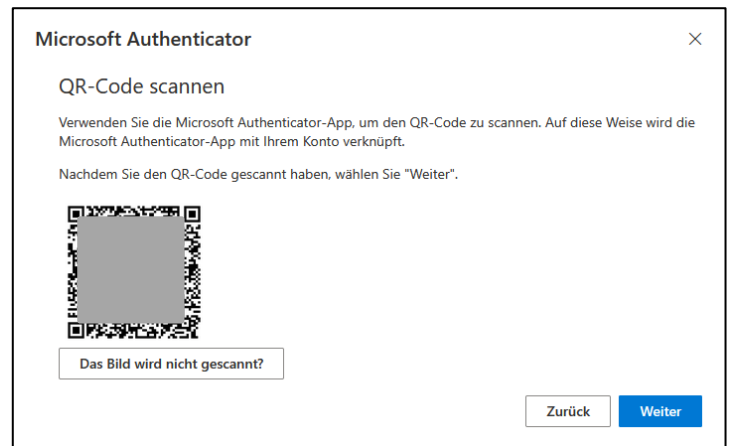


7. Den Hinweis „Konto einrichten“ mit **Weiter** bestätigen.



8. Jetzt kann mittels Authenticator App der angezeigte QR-Code gescannt werden.

Das Microsoft Konto wird dadurch der App hinzugefügt.



9. Klicken Sie auf „**Weiter**“, um die Einrichtung abzuschließen. Zur Bestätigung wird eine **zweistellige Nummer** am PC angezeigt, die Sie in der Microsoft Authenticator App eingeben müssen.



Die Einrichtung ist damit abgeschlossen.

II Einrichtung MFA mit Windows Hello for Business (nur für Beschäftigte)

Windows Hello for Business (WHfB) ist eine Funktion von Windows, mit der Sie sich sicher und bequem an Ihrem PC oder Laptop anmelden können – z. B. mit Ihrem Gesicht, Fingerabdruck oder einer PIN. Diese Methode kann bei der UR als zweiter Faktor bei VPN-Anmeldungen genutzt werden (gerätespezifisch).

Bitte beachten Sie zwei Dinge:

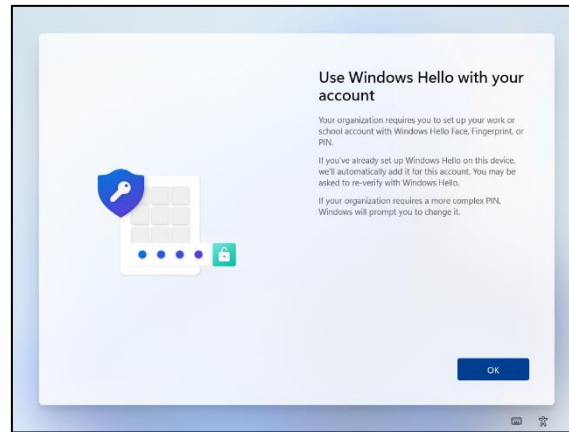
- Windows Hello for Business kann nicht als alleiniger zweiter Faktor genutzt werden! Sollten Sie sich für Windows Hello for Business als Methode entscheiden, bitten wir Sie, zuvor eine andere Methode wie z. B. die Authenticator App zu hinterlegen.
- Windows Hello for Business kann zudem nur an zentral verwalteten Windows-Geräten aktiviert werden.

1. Windows Hello for Business beantragen:

Schreiben Sie eine Mail an servicedesk@ur.de, um Windows Hello for Business freischalten zu lassen.

Wichtig: Geben Sie dabei bitte Ihre **RZ-Gerätenummer** mit an! Diese finden Sie auf einem Aufkleber an Ihrem PC/Laptop.

2. Nach der Freischaltung durch den ServiceDesk und einer gewissen Replikationszeit wird der Einrichtungsassistent von Windows Hello for Business automatisch nach dem Entsperren oder nächstem Neustart des Rechners gestartet.
3. Der Einrichtungsassistent leitet Sie durch die Konfiguration und Sie können in diesem Zuge die Gesichtserkennung oder Fingerabdruck sowie einen PIN hinterlegen.



4. Nach der Einrichtung können Sie Ihren PIN oder die biometrischen Daten zur Anmeldung an Windows und als zweiten Authentifizierungsfaktor am VPN verwenden.