SWITCH edu-ID, MFA Multi-Faktor-Authentifizierung - einrichten

Publiziert it-support@fhnw.ch allgemeine Anleitung Corporate IT Doku

So richten Sie für Ihre SWITCH edu-ID die Multi-Faktor-Authentifizierung ein.

---

english version

Wir bitten Sie, die **Multifactor Authentication in Ihrer SWITCH edu-ID** mit oder ohne der in der blauen Box beschriebenen "Handlungsaufforderung" entlang der untenstehenden Schritte zu **aktivieren**:

Handlungsaufforderung

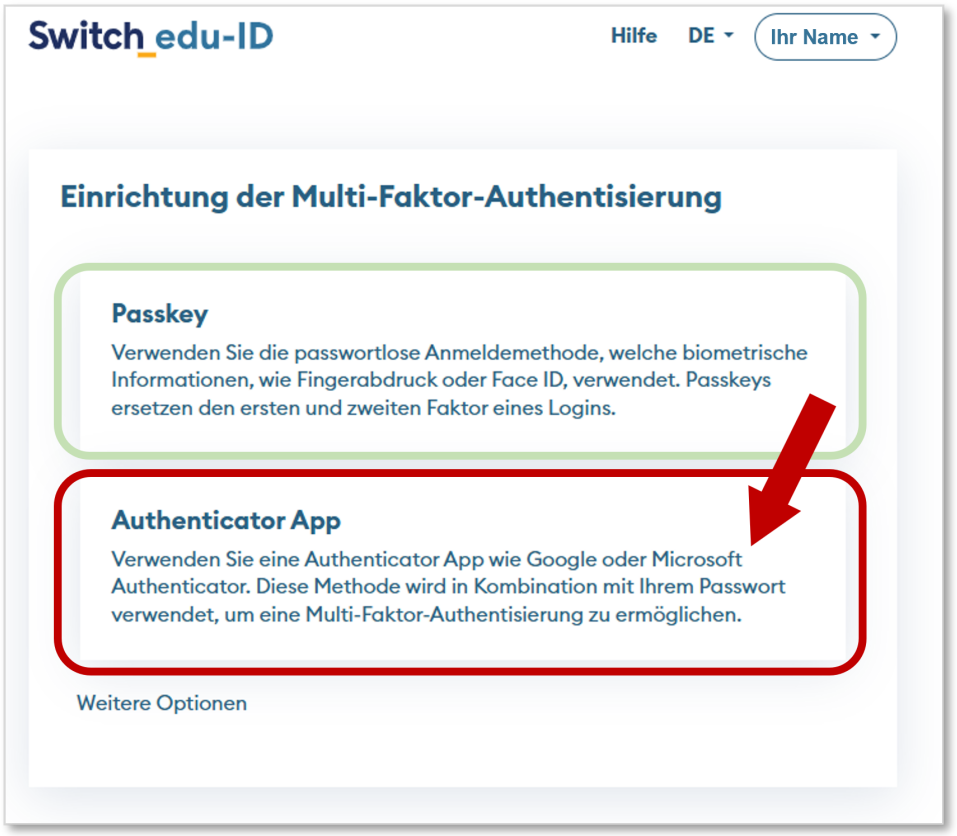
Falls Sie sich bei einem Service anmelden, der MFA verlangt, werden Sie automatisch zum "Handeln" aufgefordert:

In diesem Fall klicken Sie auf weiter, um Ihre Multi-Faktor-Authentisierung einzurichten. Mit klick auf "Weiter" werden Sie schrittweis durch den Einrichtevorgang geführt.

Einrichten der MFA in der SWITCH edu-ID - Schritt für Schritt

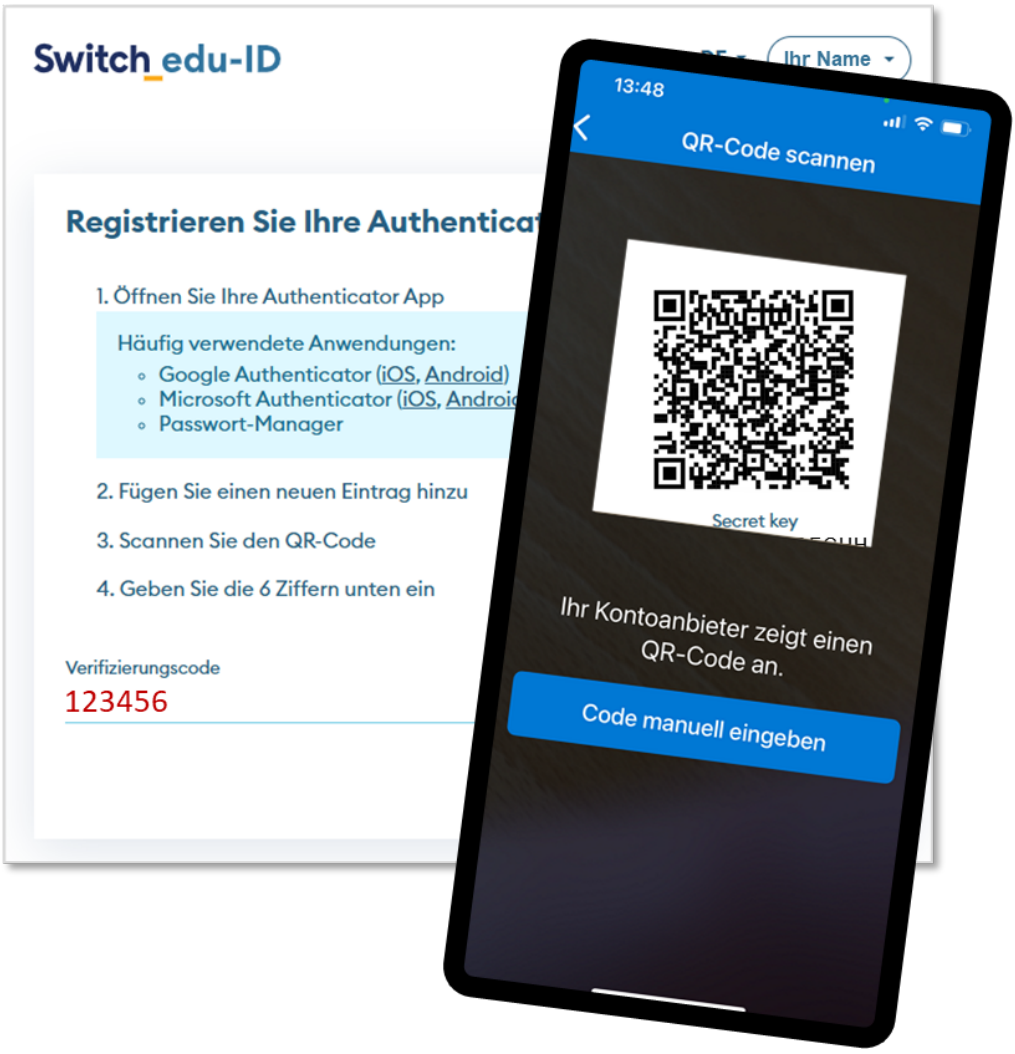
- Loggen Sie sich bei Ihrer persönlichen SWITCH edu-ID ein: Login: SWITCH edu-ID.
- Schieben Sie im Menü "**Sicherheit**" die "Multi-Faktor-Authentisierung (MFA)" auf **On**

- Wählen Sie eine Option für Ihre Multi-Faktor-Authentifizierung.
  Wir empfehlen Ihnen primär die Verwendung einer **Authenticator App**. Sie können jedoch ergänzend oder alternativ auch **Passkey** oder eine "weitere Option" wählen. Nachfolgend ist die Option "Authenticator App" beschrieben. Empfehlungen zur Option "Passkey" sind weiter unten aufgeführt.



Öffnen Sie auf ihrem Smartphone Ihre Authenticator App. Wenn Sie noch keine haben, bitten wir Sie, eine herunterzuladen und einzurichten.
Es gibt diverse Anbieter von Authenticator Apps. Sie können eine der folgenden Apps herunterladen und einrichten:

- Microsoft Authenticator (iOS, Android)
- Google Authenticator (iOS, Android)
- weitere Passwortmanager (LastPass usw.)



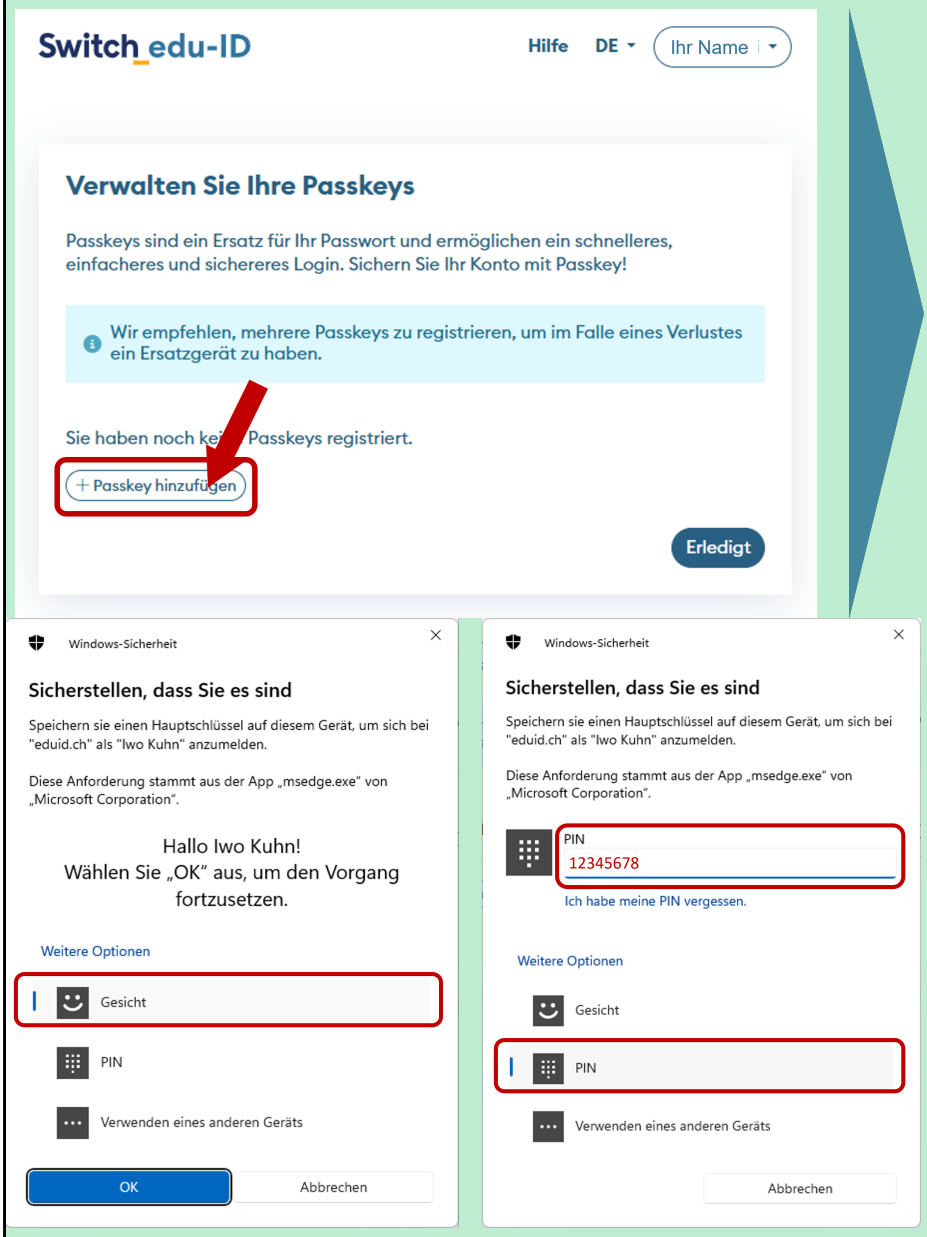
- Fügen Sie einen neuen Eintrag zu Ihrer Authenticator App hinzu (+)
- Wählen Sie, falls Ihre Authenticator App dies zur Auswahl stellt: Geschäfts-oder Schulkonto
- Scannen Sie den QR-Code
- Geben Sie den 6-stelligen Verifizierungscode, welcher in der App angezeigt wird, bei Ihrer SWITCH edu-ID ein.
- Klicken Sie auf Weiter

- Sie erhalten einen neuen Recovery Code, den Sie benötigen, falls Ihr Passwort und Ihre E-Mailadresse nicht mehr zur Verfügung stehen. Bewahren Sie diesen an einem sichern, aber gut auffindbaren Ort auf.
- Klicken Sie auf Weiter

Ihre SWITCH edu-ID ist nun MFA fähig.

Passkey

Beim Einrichten von Passkey für die Multi-Faktor-Authentifizierung empfehlen wir auf Windows-Geräten die Optionen "Gesicht" (Windows Hello) oder "PIN" (Zahlenkombination, wie sie für das Login verwendet wird), mit welchen Sie über Ihren Laptop/Computer authentifiziert werden. Sie können mehrere Passkeys für unterschiedliche Geräte hinterlegen, diese aber nur auf dem jeweiligen Gerät verwenden.



Auf Smartphones, Tablets und Apple-Geräten ist die Passkey-Einrichtung etwas komplexer, da es je nach vorhandenen Apps (z.B. unterschiedliche Passwortmanager) und Gerätekonfiguration verschiedenste Szenarien gibt, die wir zum aktuellen Zeitpunkt nicht im Detail beschreiben können. Auf solchen Geräten empfehlen wir zur Zeit die Verwendung von Passkey nur versierten Nutzenden.

Verwandte Artikel

- Moodle - Zugriff
- Switch edu-ID erstellen
- Einloggen mit FHNW-Account oder SWITCH edu-ID?
- SWITCH edu ID erstellen, verknuepfen und verwalten
- Azure Multi-Factor Authentication (MFA)
- Switch edu-ID Login

publiziert: 2. Juni 2025 16:55 Service: S1309 - IT Infrastruktur Basisdienste (AD | Entra ID | SCEP | Entra Application Proxy) Stichwörter: Security SWITCH edu-ID