

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

Publiziert [it-support@fhnw.ch](mailto:it-support@fhnw.ch) allgemeine Anleitung Corporate IT Doku

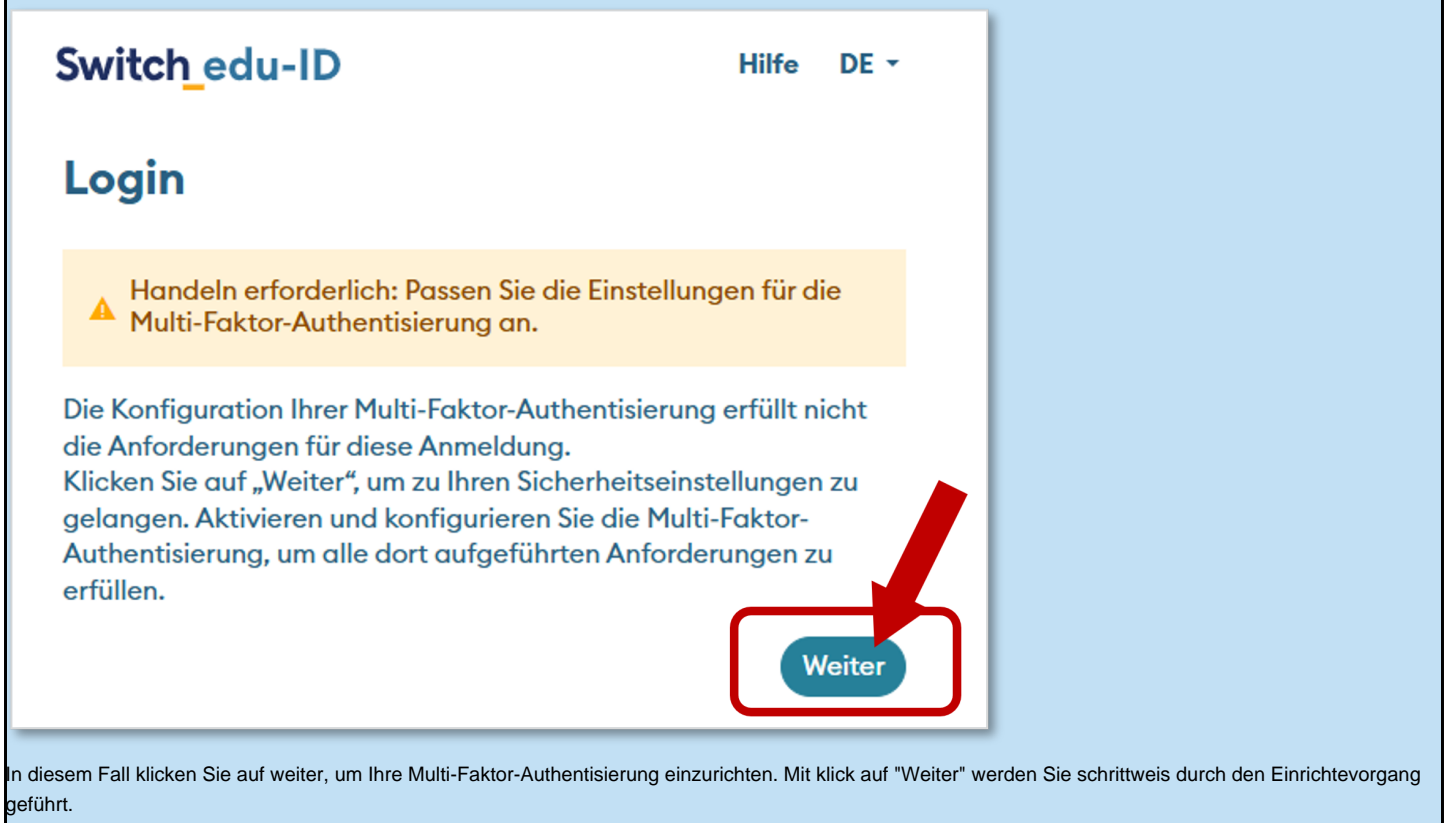
So richten Sie für Ihre SWITCH edu-ID die Multi-Faktor-Authentifizierung ein.

[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:



The screenshot shows the SWITCH edu-ID login interface. At the top left is the logo 'Switch edu-ID' and at the top right are links for 'Hilfe' and 'DE'. Below the logo is the heading 'Login'. A yellow warning box contains the text: '⚠ Handeln erforderlich: Passen Sie die Einstellungen für die Multi-Faktor-Authentisierung an.' Below this, a blue text block states: 'Die Konfiguration Ihrer Multi-Faktor-Authentisierung erfüllt nicht die Anforderungen für diese Anmeldung. Klicken Sie auf „Weiter“, um zu Ihren Sicherheitseinstellungen zu gelangen. Aktivieren und konfigurieren Sie die Multi-Faktor-Authentisierung, um alle dort aufgeführten Anforderungen zu erfüllen.' At the bottom right of this text block, a blue button labeled 'Weiter' is highlighted with a red rounded rectangle and a red arrow pointing to it from the right.

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**

The screenshot shows the 'Switch edu-ID' user interface. At the top, there is a header with the logo, a 'Hilfe' link, a language selector 'DE', and a user profile 'Ihr Name'. Below the header is a navigation bar with four tabs: 'Profil', 'Sicherheit', 'Datenschutz', and 'Organisationen'. The 'Sicherheit' tab is selected and highlighted with a red box. Underneath, there are two main sections: 'Passwort' and 'Multi-Faktor-Authentisierung (MFA)'. The 'Passwort' section shows the current password and a 'Geändert gerade eben' status. The 'MFA' section has a descriptive text and a toggle switch currently set to 'Off'. A red arrow points to the 'On' position of the toggle switch.

- 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 **Paskey** oder eine "weitere Option" wählen. Nachfolgend ist die Option "Authenticator App" beschrieben. Empfehlungen zur Option "Paskey" sind weiter unten aufgeführt.

The screenshot shows the 'Einrichtung der Multi-Faktor-Authentisierung' (Setup of Multi-Factor Authentication) page. It features two main options: 'Paskey' and 'Authenticator App'. The 'Paskey' option is described as a passwordless login method using biometric information. The 'Authenticator App' option is described as using an app like Google or Microsoft Authenticator in combination with a password. A red arrow points to the 'Authenticator App' option. At the bottom, there is a link for 'Weitere Optionen' (More options).

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.)

## Registrieren Sie Ihre Authenticator

### 1. Öffnen Sie Ihre Authenticator App

Häufig verwendete Anwendungen:

- Google Authenticator (iOS, Android)
- Microsoft Authenticator (iOS, Android)
- Passwort-Manager

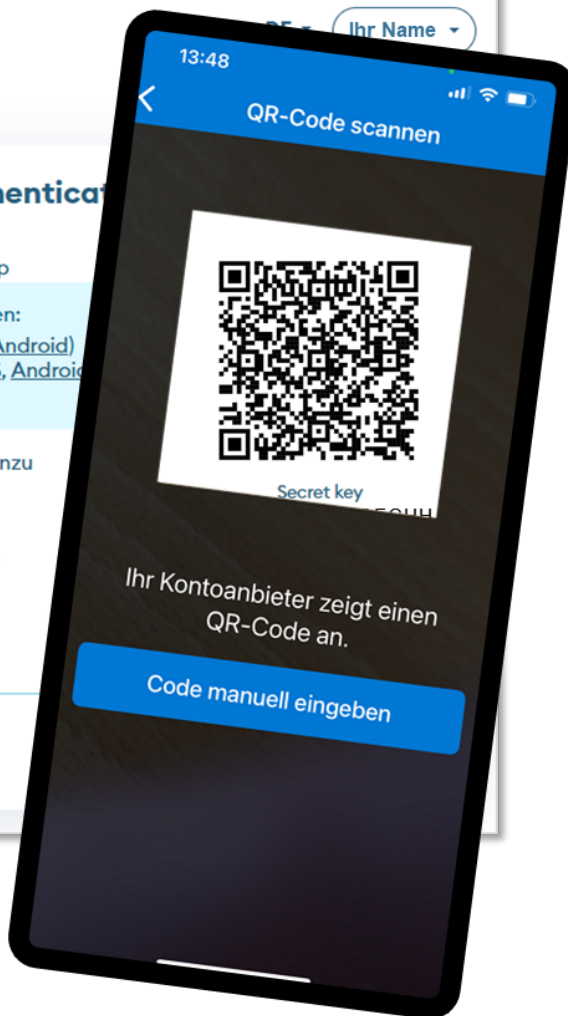
### 2. Fügen Sie einen neuen Eintrag hinzu

### 3. Scannen Sie den QR-Code

### 4. Geben Sie die 6 Ziffern unten ein

Verifizierungscode

**123456**



- 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

## Ihr neuer Recovery Code

Bewahren Sie den Recovery Code an einem **sicheren, aber gut auffindbaren Ort** auf (z.B. Passwortmanager oder Sicherheitsbox).

1234 5678 9123 4567 

Ich habe ihn gespeichert

**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 sicheren, 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.

The image shows a sequence of three screenshots illustrating the Passkey setup process. The top screenshot is the 'Switch edu-ID' web portal, where the user is prompted to 'Verwalten Sie Ihre Passkeys' (Manage your Passkeys). A red arrow points to the '+ Passkey hinzufügen' (Add Passkey) button. The middle screenshot is a Windows Security dialog box titled 'Sicherstellen, dass Sie es sind' (Make sure you're you), showing the user 'Halo Iwo Kuhn!' and offering authentication options: 'Gesicht' (Face), 'PIN', and 'Verwenden eines anderen Geräts' (Use another device). The 'Gesicht' option is highlighted with a red box. The bottom screenshot is another Windows Security dialog box, similar to the middle one, but with the 'PIN' option highlighted by a red box and the PIN '12345678' entered into the input field.

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](#)