

Multi-Faktor-Authentifizierung aktivieren



Nachdem Sie einen YubiKey erhalten haben oder sich einen Softwaretoken eingerichtet haben, können Sie Multi-Faktor Authentifizierung aktivieren. Melden Sie sich mit Ihrer IdM-Kennung unter <https://www.idm.fau.de> im IdM-Portal an.

The screenshot shows the IdM-Portal interface. At the top, there is a navigation bar with 'SELF SERVICE' and 'ANFRAGEN/AUFGABEN' buttons. The 'SELF SERVICE' button is highlighted with a red box and a red arrow labeled '(1)' points to it. Below the navigation bar, the main content area is titled 'Willkommen im IdM'. On the left, a sidebar menu lists 'Profil' (with 'Datenübersicht'), 'Sicherheit' (with 'IdM-Passwort', 'E-Mail-Adresse zur Kontowiederherstellung', 'Multi-Faktor-Authentifizierung' (which is highlighted with a red box and a red arrow labeled '(2)' points to it), 'OpenPGP-Schlüssel', and 'Login-Aktivität').

Klicken Sie im Bereich Self Service (1)
auf Multi-Faktor-Authentifizierung (2)

Setzen Sie sich anschließend bei Einstellungen nacheinander die drei Haken für das IdM-Portal, VPN und WebSSO.

Multi-Faktor-Authentifizierung

 Die Multi-Faktor-Authentifizierung (MFA), auch Multifaktor-Authentisierung, ist eine Verallgemeinerung der Zwei-Faktor-Authentisierung, bei der die Zugangsberechtigung durch mehrere unabhängige Merkmale (Faktoren) überprüft wird.

Token

Der Time-based One-time Password Algorithmus (TOTP) ist ein Verfahren zur Erzeugung von zeitlich limitierten Einmalkennwörtern

[TOTP hinzufügen](#)

Der YubiKey ist ein Security-Token der Firma Yubico, der mit Schnittstellen wie Lighting, Near Field Communication (NFC) oder USB und vielfältigen Protokollen zur Identifizierung und Authentifizierung von Benutzern an Computersystemen verwendet wird

[YubiKey hinzufügen](#)

 Links zu dieser Dienstleistung

- [Anleitung zur Tokenverwaltung](#)
- [FAQs zur Multifaktor-Authentifizierung](#)
- [Empfehlung für Authentifizierungs Anwendungen](#)
 - [Android - FreeOTP+](#)
 - [iOS - Step Two](#)

Einstellungen

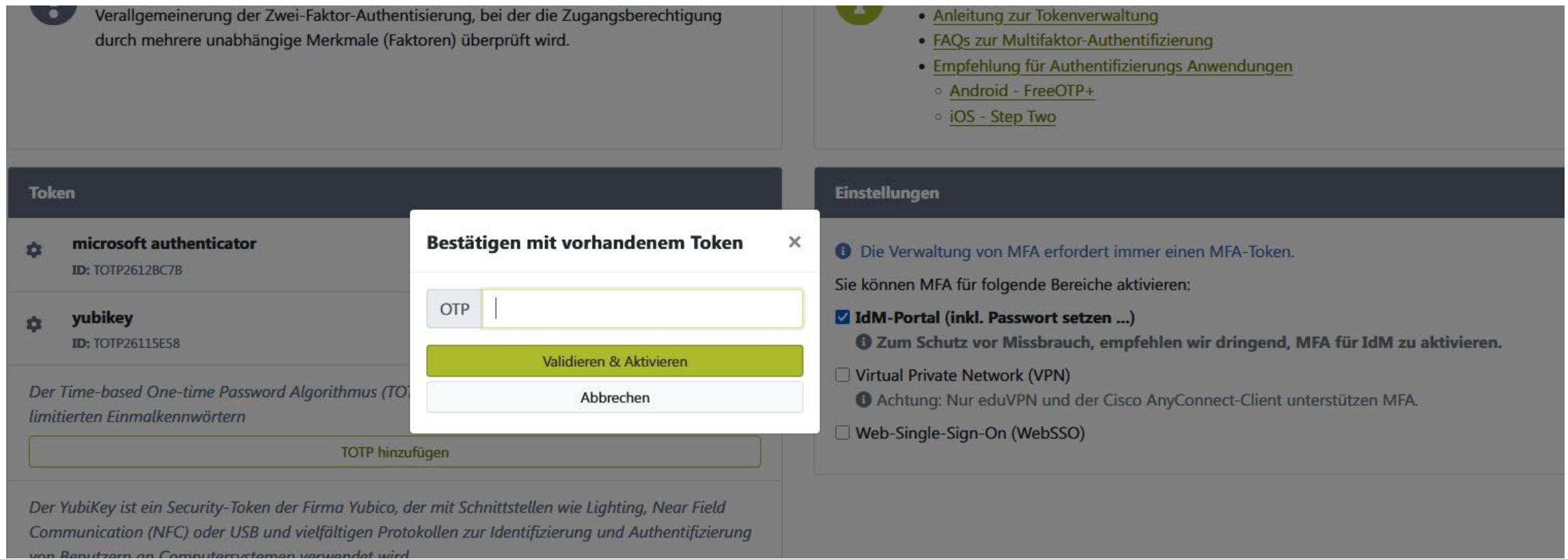
 Bitte fügen Sie mindestens ein Token hinzu
Sie können MFA für folgende Bereiche aktivieren:

IdM-Portal (inkl. Passwort setzen ...)
 • Zum Schutz vor Missbrauch, empfehlen wir dringend, MFA für IdM zu aktivieren.

Virtual Private Network (VPN)

Web-Single-Sign-On (WebSSO)

Bestätigen Sie die Auswahl durch Eingabe Ihres zweiten Faktors im Feld OTP. Drücken sie dazu den Knopf des YubiKey oder geben sie das Einmalpassworts des Softwaretokens ein. Klicken Sie anschließend auf „Validieren und Aktivieren“.



The screenshot shows a user interface for enabling MFA. A central modal dialog box is open, prompting the user to "Bestätigen mit vorhandenem Token" (Confirm with existing token). It contains an "OTP" input field, which is currently empty. Below the input field are two buttons: "Validieren & Aktivieren" (Validate & Activate) in green, and "Abbrechen" (Cancel) in grey. The background of the interface is a dark grey dashboard. On the left, there's a "Tokens" section listing "microsoft authenticator" (ID: TOTP26128C7B) and "yubikey" (ID: TOTP26115E58). A note below these tokens explains the Time-based One-time Password Algorithm (TOTP). On the right, there's an "Einstellungen" (Settings) section with a list of links and checkboxes. The links include "Anleitung zur Tokenverwaltung", "FAQs zur Multifaktor-Authentifizierung", and "Empfehlung für Authentifizierungs Anwendungen" with sub-links for "Android - FreeOTP+" and "iOS - Step Two". The checkboxes are for activating MFA in the "IdM-Portal (inkl. Passwort setzen ...)" (checked), "Virtual Private Network (VPN)" (unchecked), and "Web-Single-Sign-On (WebSSO)" (unchecked). A note next to the IdM checkbox states: "Zum Schutz vor Missbrauch, empfehlen wir dringend, MFA für IdM zu aktivieren." (To protect against misuse, we strongly recommend activating MFA for IdM).

Sobald alle drei Haken gesetzt sind, ist Ihre Multi-Faktor-Authentifizierung fertig eingerichtet.

Einstellungen

i Die Verwaltung von MFA erfordert immer einen MFA-Token.

Sie können MFA für folgende Bereiche aktivieren:

IdM-Portal (inkl. Passwort setzen ...)
i Zum Schutz vor Missbrauch, empfehlen wir dringend, MFA für IdM zu aktivieren.

Virtual Private Network (VPN)

Web-Single-Sign-On (WebSSO)

Mitarbeiter der FAU erhalten, solange der Vorrat reicht, einen fertig eingerichteten YubiKey an den Service-Theken des RRZE.

Eine Anleitung zum „Einrichten des Softwaretokens“ finden Sie auf unserer [MFA-Anleitungsseite](#).