

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.



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

Multi-Faktor-Authentifizierung aktivieren



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.



Links zu dieser Dienstleistung

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

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](#)

Einstellungen

i Bitte fügen Sie mindestens ein Token hinzu

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)

Multi-Faktor-Authentifizierung aktivieren



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 displays the MFA activation interface. A modal dialog titled "Bestätigen mit vorhandenem Token" is centered on the screen. It contains an "OTP" input field, a green "Validieren & Aktivieren" button, and a white "Abbrechen" button. The background interface is dimmed and shows two main sections: "Token" and "Einstellungen".

Token Section:

- microsoft authenticator**
ID: TOTP26128C7B
- yubikey**
ID: TOTP26115E58

Einstellungen Section:

- Die Verwaltung von MFA erfordert immer einen MFA-Token.
- 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)
Achtung: Nur eduVPN und der Cisco AnyConnect-Client unterstützen MFA.
- ☐ Web-Single-Sign-On (WebSSO)

Multi-Faktor-Authentifizierung aktivieren



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](#).