Multi-Faktor-Authentifizierung (MFA)

Kurzanleitung zur MFA

Diese Anleitung dient zur ersten Hilfe und beschreibt nur zwei Methoden (TOTP und Papier-TAN-Liste). Mehr Details über weitere MFA-Methoden und Anmerkungen, z.B. wie Sie Ihre Tokens im Portal verwalten können, finden Sie in der **vollständigen Anleitung**.

Was ist MFA?

MFA schützt Ihr Hochschulkonto zusätzlich. Neben Ihrem Passwort benötigen Sie einen weiteren Sicherheitscode (Token).
Dadurch bleibt Ihr Konto auch geschützt, wenn jemand Ihr Passwort kennt.
Nach der Einrichtung benötigen Sie bei der Anmeldung zusätzlich einen Sicherheitscode aus Ihrer App bzw. aus der TAN-Liste oder einen Hardware-Token.

Was benötige ich für die Einrichtung?

1) Ihre Hochschul-Zugangsdaten (Nutzername (*in Form ab1234*) & Passwort).
2) Eine Authenticator-App auf Ihr Smartphone zum Scannen des QR-Codes ODER die Möglichkeit, die PDF-Datei anzuzeigen oder auszudrucken.

Empfohlene App: PrivacyIDEA Authenticator
Alternativ funktionieren auch: Microsoft-, Google Authenticator, FreeOTP oder 2FAS.

Hier den QR-Code scannen und die App auf Ihr Handy herunterladen.

Laden Sie die Authenticator App für Android.

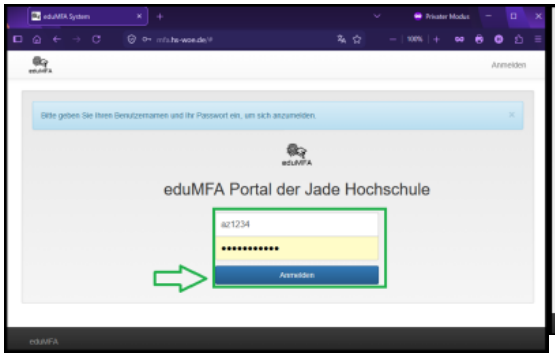
Für Android

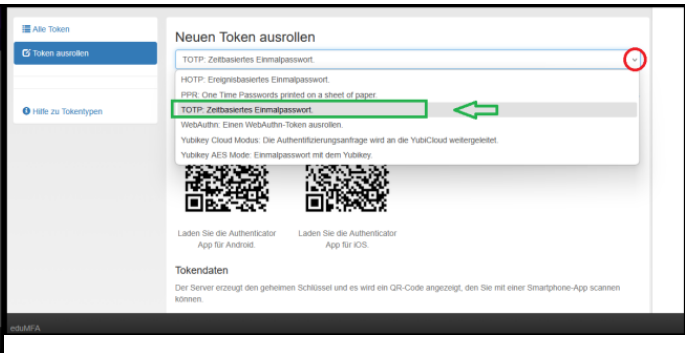
Laden Sie die Authenticator App für iOS.

Für iOS

Wie richte ich mein Token für MFA ein?

1. Öffnen Sie in Ihrem Browser: https://mfa.hs-woe.de/
2. **Melden** Sie sich mit Ihren Hochschuldaten (Nutzername & Passwort) **an**.
3. Klicken Sie links auf : **„Token ausrollen“**, um Ihre MFA-Methode einzurichten.





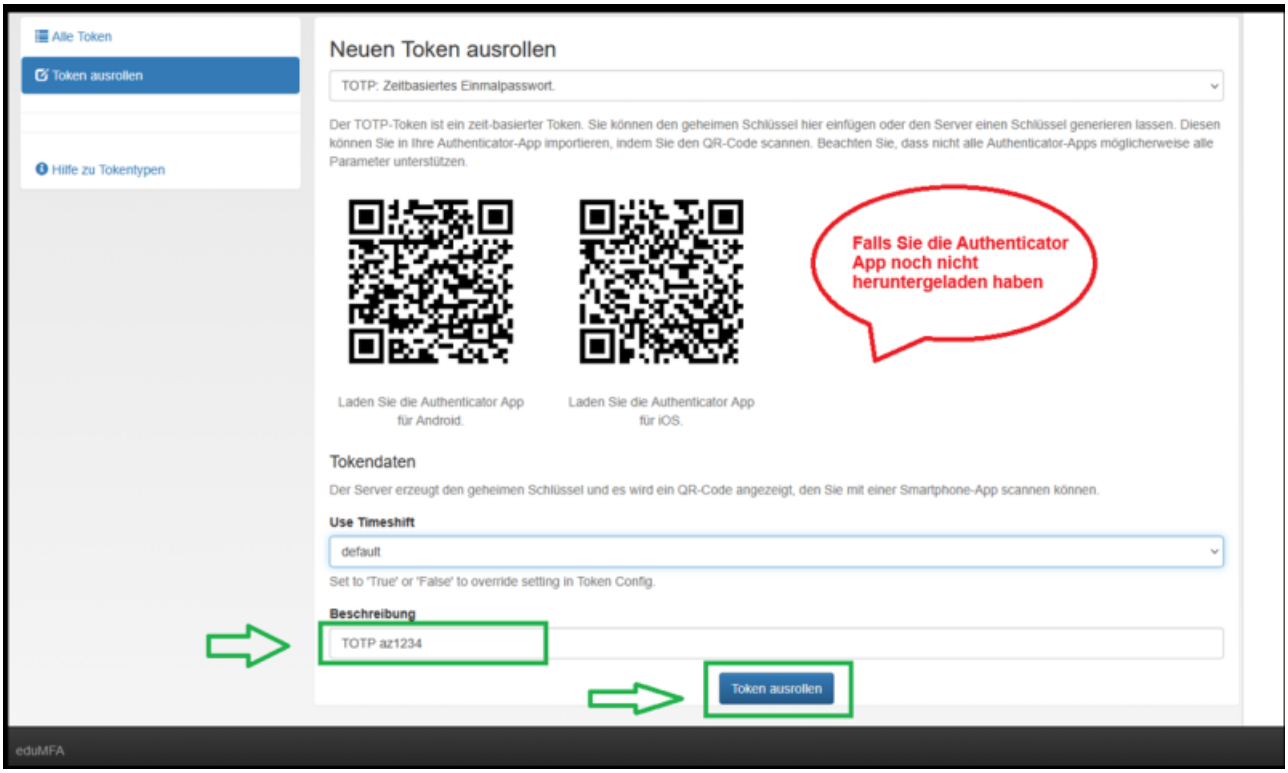
5. **Wählen** Sie den gewünschten Token-Art **aus**.

I. TOTP mit der Authenticator App

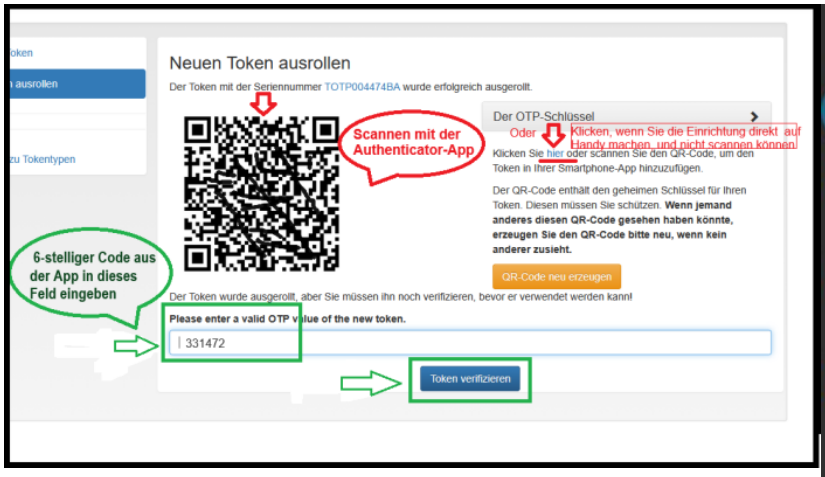
TOTP (Time-based One-Time Password) ist ein zeitbasierter Einmalcode, der alle 30 Sekunden neu generiert wird und zur sicheren Anmeldung als 2FA dient.

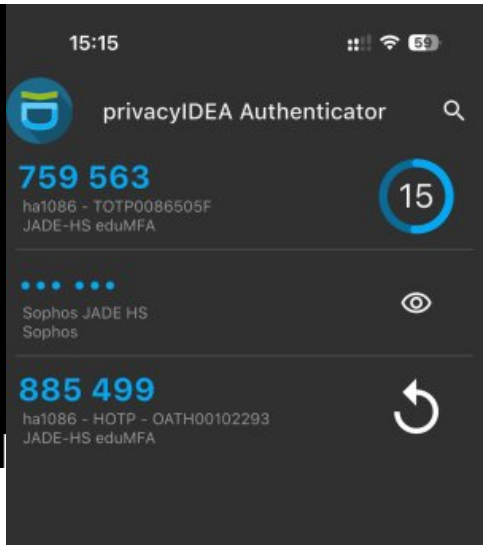
Empfohlen!

- Wählen Sie **TOTP** aus
- Geben Sie eine beliebige Beschreibung für Ihr Token ein. Bsp.: „App - Nutzername“
- Klicken Sie auf **„Token ausrollen“**.



- **Scannen Sie den QR-Code** mit Ihrer Authenticator-App. Die App zeigt einen 6-stelligen Code an.
- Wenn Sie den Vorgang auf dem Handy durchführen und den QR-Code nicht scannen können, klicken Sie auf das blaue Wort „**hier**„





- **wichtig:** Geben Sie diesen Code in das Feld ein und klicken Sie auf: **„Token verifizieren“**.

Wichtig: Ihr Token funktioniert erst nach Klick auf **„Token verifizieren“**.

II. PPR (TAN-Liste) als PDF-Datei

- Wählen Sie **PPR** aus
- Geben Sie eine Beschreibung (Token-Art & Nutzername) ein. Dann klicken Sie auf **„Token ausrollen“**.
- 

- **Speichern** oder drucken Sie die PDF-Datei und bewahren Sie diese sicher auf.
- **wichtig:** Geben Sie den ersten Code (Nr. 0) in das Feld ein und klicken Sie auf: **„Token verifizieren“**.
- 

Wichtig:

- Die Liste kann **nach dem Schließen der Seite NICHT** erneut heruntergeladen werden.
- Ihr Token funktioniert erst nach Klick auf **„Token verifizieren“**.

Wichtiger Sicherheitshinweis:

- Die TAN-Liste ist wie ein Passwort zu behandeln.
- Bewahren Sie sie sicher auf und lassen Sie sie nicht offen auf dem Schreibtisch

oder an anderen frei zugänglichen Orten liegen.
- Geben Sie die Liste nicht an andere Personen weiter.

III. Beschaffung von Sicherheitsschlüsseln als Hardware-Token

Falls Sie kein privates Smartphone für die MFA verwenden möchten oder eine zusätzliche Authentifizierungsmethode benötigen, können Sie über das HRZ einen Hardware-Sicherheitsschlüssel beziehen.

Der Sicherheitsschlüssel dient als zweiter Faktor für die Anmeldung und kann alternativ oder ergänzend zu einer Authenticator-App verwendet werden.

Die Bestellung erfolgt über das Ticketsystem per formloser E-Mail unter Angabe von Kostenstelle, Hardware-Typ und Anschlussart (USB-A oder USB-C).

Aktuell stehen folgende Varianten zur Verfügung:

Kategorie	USB-Version	MFA-Verfahren	Kosten	Modell
Display-Token		TOTP	13 €	
Swissbit iShield2 Key	USB-A oder -C & NFC	WebAuthn / Passkey	24 € / 28 €	
Yubico Security Key	USB-A oder -C &NFC	WebAuthn / Passkey	35 €	

Mehr Details darüber finden Sie hier.

Hinweis:

- Die angegebenen Preise können je nach Angebot und Bestellzeitpunkt geringfügig variieren.
- Nach Erhalt des Sicherheitsschlüssels muss dieser zunächst eingerichtet und

anschließend im eduMFA-Portal registriert werden.

Was ist jetzt neu bei der Anmeldung mit MFA

1. Nach **Anmeldung mit Benutzername und Passwort** *(ganz normal wie vorher)*, wird Ihnen ein neues Anmeldefenster angezeigt.
2. **Öffnen** Sie Ihre Authenticator App oder Ihre TAN-Liste (Papiercode)
3. **Geben** Sie den 6-stelligen Code aus der APP/Liste in das entsprechende Feld ein
4. **Klicken** Sie auf **„überprüfen“**
5. Sie sind anschließend erfolgreich angemeldet.

Tokens im eduMFA-Portal verwalten:

Empfehlung:
Richten Sie nach Möglichkeit **mehr als eine MFA-Methode** ein.
So können Sie sich weiterhin anmelden, falls Ihr Handy verloren geht oder nicht verfügbar ist.

Weitere Anleitungen finden Sie hier:

- MFA mit Microsoft 365 verbinden (Kapitel 10 ab S.30)
- Passkey oder Sicherheitsschlüssel einrichten (Ab S. 15)
- Alle MFA-Funktionen und Verwaltung (Ab S. 36)

Handy oder Token verloren?
Falls möglich: Das verlorene Token im Portal **sofort deaktivieren**.
Falls kein weiteres Token verfügbar ist, kontaktieren Sie bitte sofort den MFA-Service des HRZ.

Support:
Haben Sie Probleme mit Ihrem Token, benötigen Sie Hilfe oder möchten Sie uns Feedback senden?
Dann können Sie ein Ticket über das Ticketsystem oder eine E-Mail unter einer dieser Adressen schreiben:

- hrz-servicedesk@jade-hs.de

- informationssicherheitsmanagement@jade-hs.de