

Multi-Faktor-Authentifizierung (MFA) an der FAU

Regionales Rechenzentrum Erlangen (RRZE)

rrze-mfa@fau.de

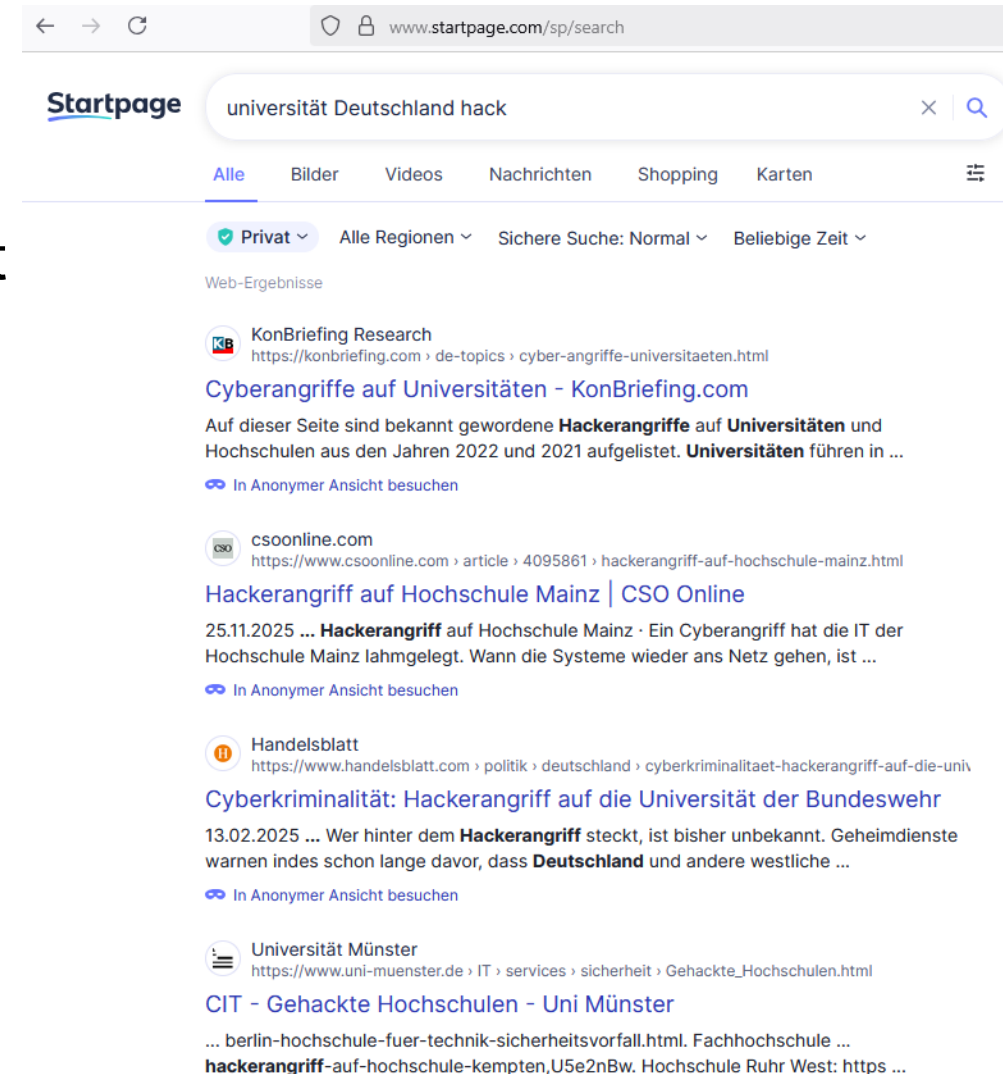
16. Juli 2026

-
- Was ist MFA und warum ist das eine gute Sache?
 - Wie sieht MFA an der FAU praktisch aus?
 - Wie richte ich MFA ein?
 - Tipps und Tricks rund um MFA

Was ist MFA und warum ist das eine gute Sache?



- Universitäten sind mittlerweile ein sehr beliebtes Angriffsziel geworden.
- Benutzername/Passwort alleine reicht nicht mehr als Schutz für die Authentifizierung (Anmeldung).
- Es wird ein zusätzlicher „Faktor“ benötigt, der sich nicht so leicht kopieren oder abhören lässt, weil er nur kurze Zeit gültig ist („Einmal-Passwort“).
- Die meisten kennen das schon länger vom Online-Banking.



Wie sieht MFA an der FAU praktisch aus?



Anmeldung im IdM-Portal

- Schritt 1 (wie ohne MFA):

IdM-Portal Login

Anmeldung
FAU IdM-Portal

ANMELDEN

[Passwort vergessen?](#)

- Schritt 2 (zusätzlich durch MFA):

abmelden.' followed by 'Sie haben noch 5 Versuch(e)'. There is a white input field labeled 'Einmalpasswort' and a green 'ANMELDEN' button."/>

IdM-Portal Login

Multi-Faktor-Authentifizierung
(MFA)

Sie können eine neue Sitzung starten, indem Sie sich [abmelden](#).

Sie haben noch 5 Versuch(e).

Einmalpasswort

ANMELDEN

Wie sieht MFA an der FAU praktisch aus?

Anmeldung bei Diensten mit „SSO-Anmeldung“



- Schritt 1 (wie ohne MFA):

 Zentraler Anmeldeportal

Deutsch ▼

Bitte geben Sie Ihren Benutzernamen und Ihr Passwort ein

Um diesen Dienst zu nutzen, müssen Sie sich authentifizieren. Bitte geben Sie daher unten Benutzernamen und Passwort ein.

Nutzerkennung

Passwort

Anmelden

Passwort vergessen oder die Anmeldung funktioniert nicht?

Bitte überprüfen Sie im IdM-Portal der FAU (idm.fau.de) die Dienstleistung "Web Single Sign-On (WebSSO)". Ist diese nicht vorhanden, abgelaufen oder zeigt einen Fehler an, können Sie diesen Dienst nicht nutzen.

- Schritt 2 (zusätzlich durch MFA):

 Zentraler Anmeldeportal

Multi-Faktor-Authentifizierung (MFA)

Dieser Dienst erfordert MFA. Bitte geben Sie daher unten das Einmalpasswort ein.

Einmalpasswort

Weiter

Keine zweite Authentifizierungsmethode konfiguriert oder verfügbar?

Authentifizierung abbrechen

Die SSO-Anmeldung kommt u. a. zum Einsatz bei:

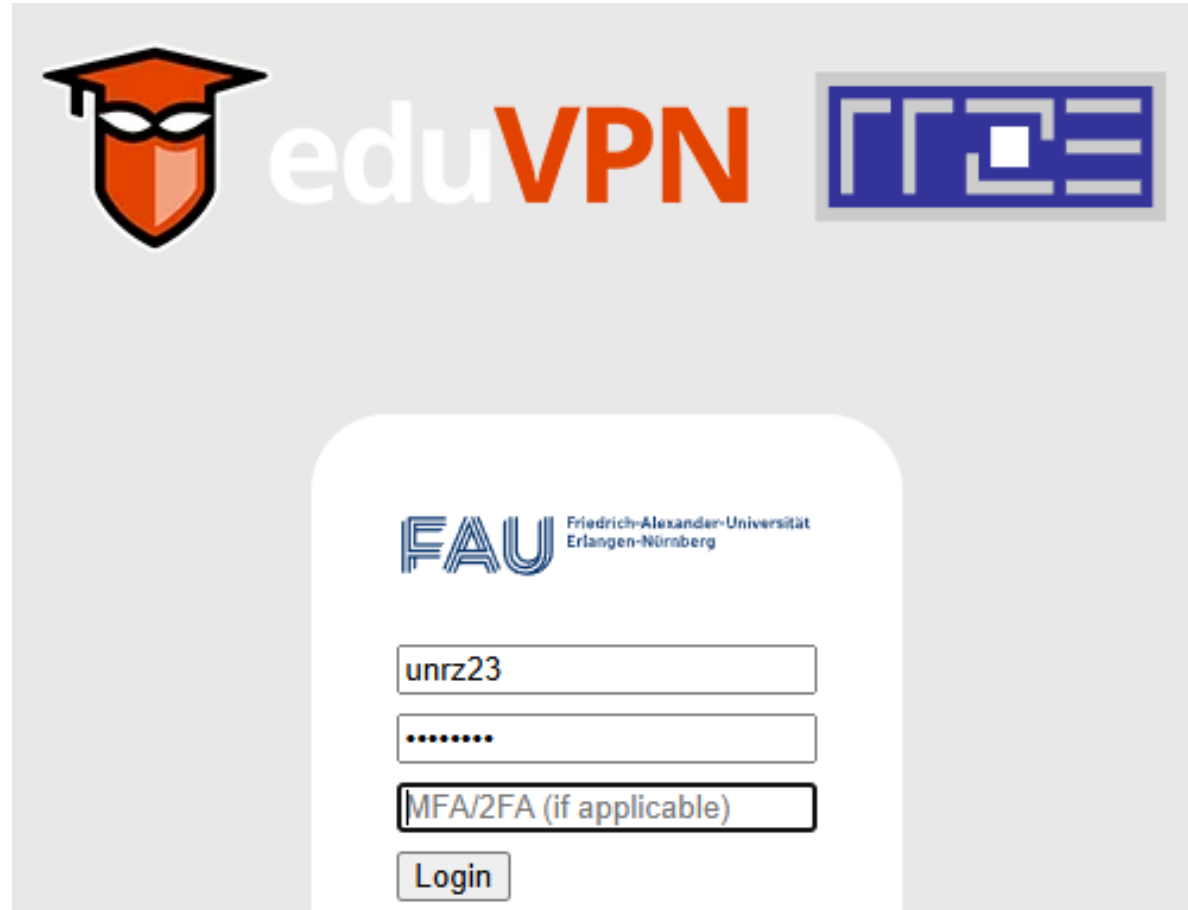
- StudOn
- Campo
- FAUbox
- sdauth.sciencedirect.com
- intern.fau.de
- FAUzoom
- fau.zeitwart.de
- FAUdir
- B-ITE

Wie sieht MFA an der FAU praktisch aus?



Anmeldung am eduVPN

- Schritt 1+2 sind in der gleichen Oberfläche eingebaut:

The image shows the login interface for eduVPN. At the top, there is an orange graduation cap icon, the text 'eduVPN' in white and orange, and the rrze logo. Below this, there is a white rounded rectangle containing the FAU logo and the text 'Friedrich-Alexander-Universität Erlangen-Nürnberg'. Underneath the logo, there are three input fields: the first contains 'unrz23', the second contains a series of dots, and the third contains 'MFA/2FA (if applicable)'. At the bottom of the white rectangle is a 'Login' button.

Die VPN-Verbindung benötigen Sie z. B. für:

- Den Zugriff auf FSV
- Im Homeoffice für den Zugriff auf Netzlaufwerke
- Den Zugriff auf Online-Zeitschriften der Universitätsbibliothek

- Jeder mit einer IdM-Kennung **kann** sein Benutzerkonto mit MFA schützen.
- Besonders wichtige Kennungen **müssen** bereits mit MFA geschützt sein.
- 2026 wird die Verpflichtung, MFA zu nutzen, weiter ausgeweitet:

Nutzergruppe	MFA verpflichtend ab
Hauptberuflich Beschäftigte	20.05.2026 ✓
Weitere Beschäftigte und externe Lehrende	15.07.2026 ✓
Studierende, Promovierende und Sonstige	15.11.2026
Alumni	31.03.2027

- Es gibt mehrere Varianten für MFA an der FAU:
 - Hardware-Token (z. B. „YubiKey“)
 - Software-Token über eine Smartphone-App
 - Software-Token über ein Programm auf dem Arbeitsplatzrechner (z. B. „KeepassXC“)
- Es ist sinnvoll, mehrere Varianten zu nutzen („Zweitschlüssel“).

- Das Hardware-Token wird in einen USB-Anschluss des Notebooks gesteckt.
- Das „Einmalpasswort“ / „OTP“ / „TOTP“ wird durch Drücken auf den Knopf automatisch erzeugt.
- Für hauptberuflich Beschäftigte kann ein YubiKey an einer der Service-Theken des RRZE abgeholt werden (so lange Vorrat reicht). Wichtig: Am besten an den Schlüsselbund, damit man ihn nicht „vergisst“.



- Es gibt sehr viele Apps, die geeignet sind.
- Das RRZE empfiehlt für
 - **Android:** App „FreeOTP+“
(muss heruntergeladen werden)
 - **iOS:** App „Passwörter“
(ist bereits in iOS enthalten).
- Niemand ist gezwungen, ein Smartphone zu verwenden. Es können auch private Smartphones für MFA verwendet werden.
- Anleitungen unter
<https://www.anleitungen.rrze.fau.de/serverdienste/multifaktor-authentifizierung/>



- Auch hier gibt es sehr viele Programme, die geeignet sind.
- Das RRZE empfiehlt das Programm KeepassXC. Es ist für alle gängigen Betriebssysteme (Windows, Linux, macOS) kostenlos verfügbar.
- Das Programm ist auch allgemein als Passwortmanager empfohlen.



- Anleitungen unter <https://www.anleitungen.rrze.fau.de/serverdienste/multifaktor-authentifizierung/>

- Wenn Sie noch nicht zu einer Nutzergruppe gehören, für die MFA verpflichtend ist, können Sie MFA selbst aktivieren oder deaktivieren:

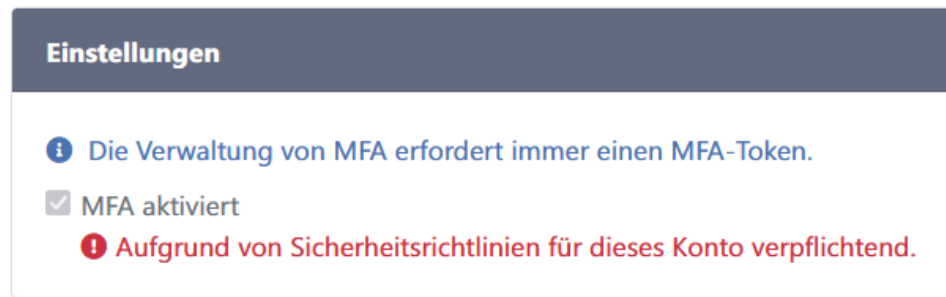


Einstellungen

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

☐ MFA aktivieren

- Andernfalls ist MFA für Sie bereits aktiviert und kann nicht mehr deaktivierbar werden:



Einstellungen

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

☒ MFA aktiviert

! Aufgrund von Sicherheitsrichtlinien für dieses Konto verpflichtend.

Achtung: Die Aktivierung von MFA bedeutet, dass Sie ohne Ihren zweiten Faktor die Dienste nicht mehr nutzen können.

- Keine Angst vor MFA! Man gewöhnt sich sehr schnell daran.
- Legen Sie sich auf jeden Fall einen „Zweitschlüssel“ an.
- Das Programm KeepassXC ist ein vollwertiger Passwortmanager. Die dazugehörige Datenbankdatei können Sie auch mit verschiedenen Smartphone-Apps nutzen und auf verschiedenen Geräten über die FAUBox synchronisieren. Eine Anleitung zu KeepassXC gibt es hier: <https://www.fau.tv/clips/31-it-tipps-aus-dem-cio-office-passwortmanager-w22>
- Das Programm 2FAGuard ist besonders einfach einzurichten und zu bedienen, kann aber nur auf einem Gerät eingesetzt werden und funktioniert nur unter Windows.