

Multi-factor authentication (MFA) at FAU

Erlangen Regional Computing Center (RRZE)

rrze-mfa@fau.de

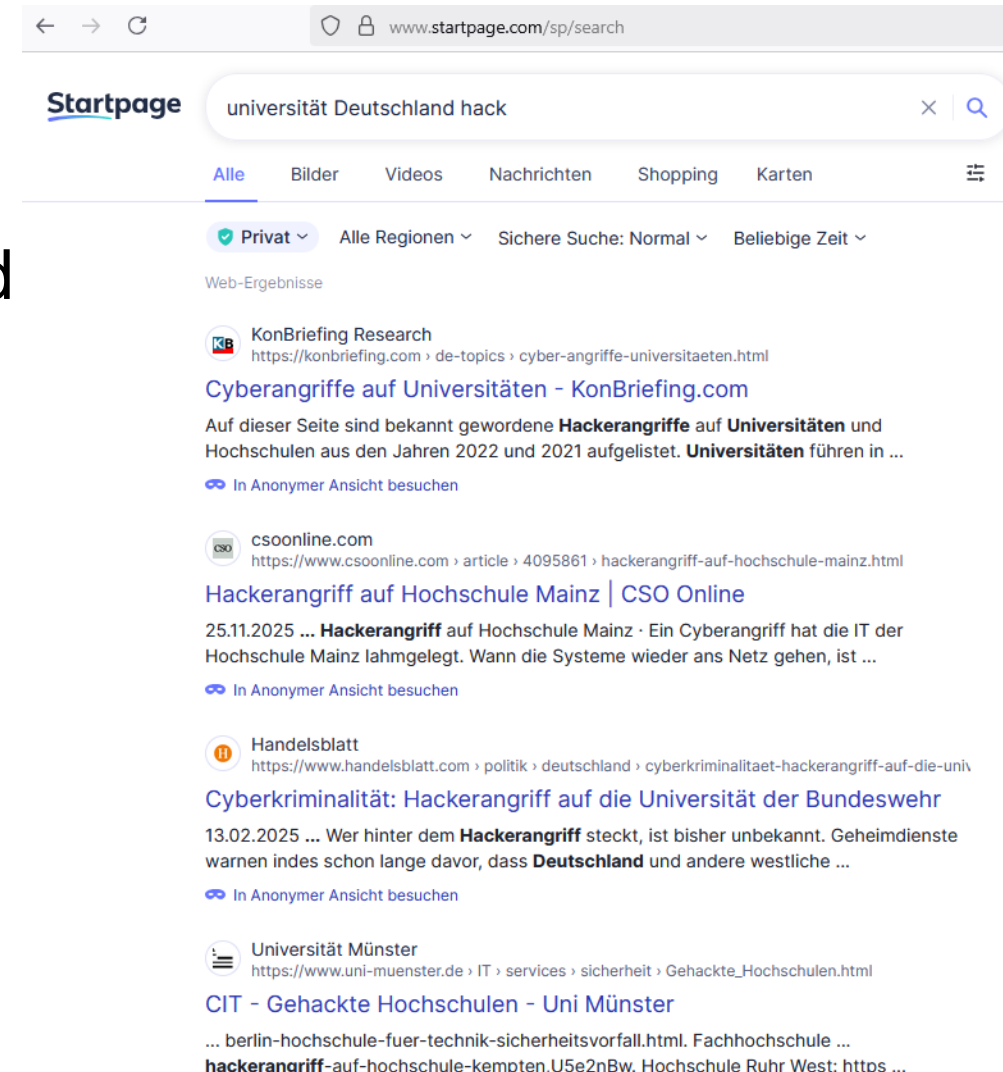
July 16, 2026

-
- What is MFA and what are the benefits?
 - How will FAU implement MFA?
 - How can I set up MFA?
 - Tips and tricks for MFA

What is MFA and what are the benefits?



- Nowadays, universities have become a highly desirable target for attacks.
- The combination of username/password no longer provides sufficient protection for authentication (when logging in).
- An additional “factor” is required that cannot be copied or intercepted as easily.
- Most of us are already familiar with this concept from online banking.



How will FAU implement MFA?



Logging in to the IdM portal

- Step 1 (like without MFA):



IdM-Portal Login



Login
FAU IdM-Portal

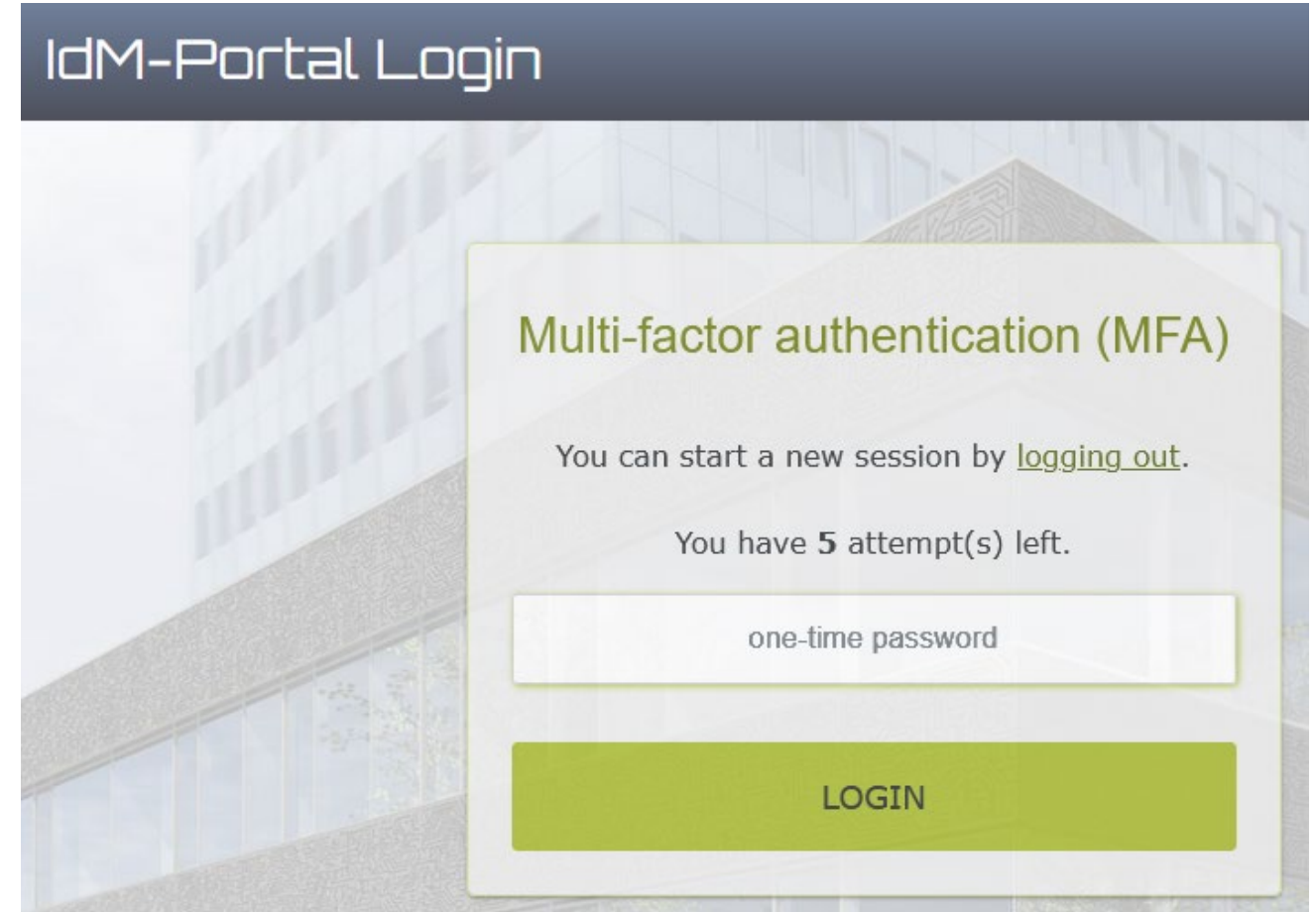
IdM username 

IdM password 

LOGIN

[Forgot your password?](#)

- Step 2 (extra step using MFA):



IdM-Portal Login

Multi-factor authentication (MFA)

You can start a new session by [logging out](#).

You have 5 attempt(s) left.

one-time password

LOGIN

How will FAU implement MFA?

Logging in to services using “SSO login”



- Step 1 (like without MFA):



Central Login Service

Enter your username and password

A service has requested you to authenticate yourself. Please enter your username and password in the form below.

Username

Password

Login

- Step 2 (extra step using MFA):



Central Login Service

Multi-factor authentication (MFA)

This service requires MFA. Please enter one-time password in the form below.

one-time password

Continue

You do not have a second authentication method configured or not available?

Cancel authentication

You will need the SSO-Login, for example, for:

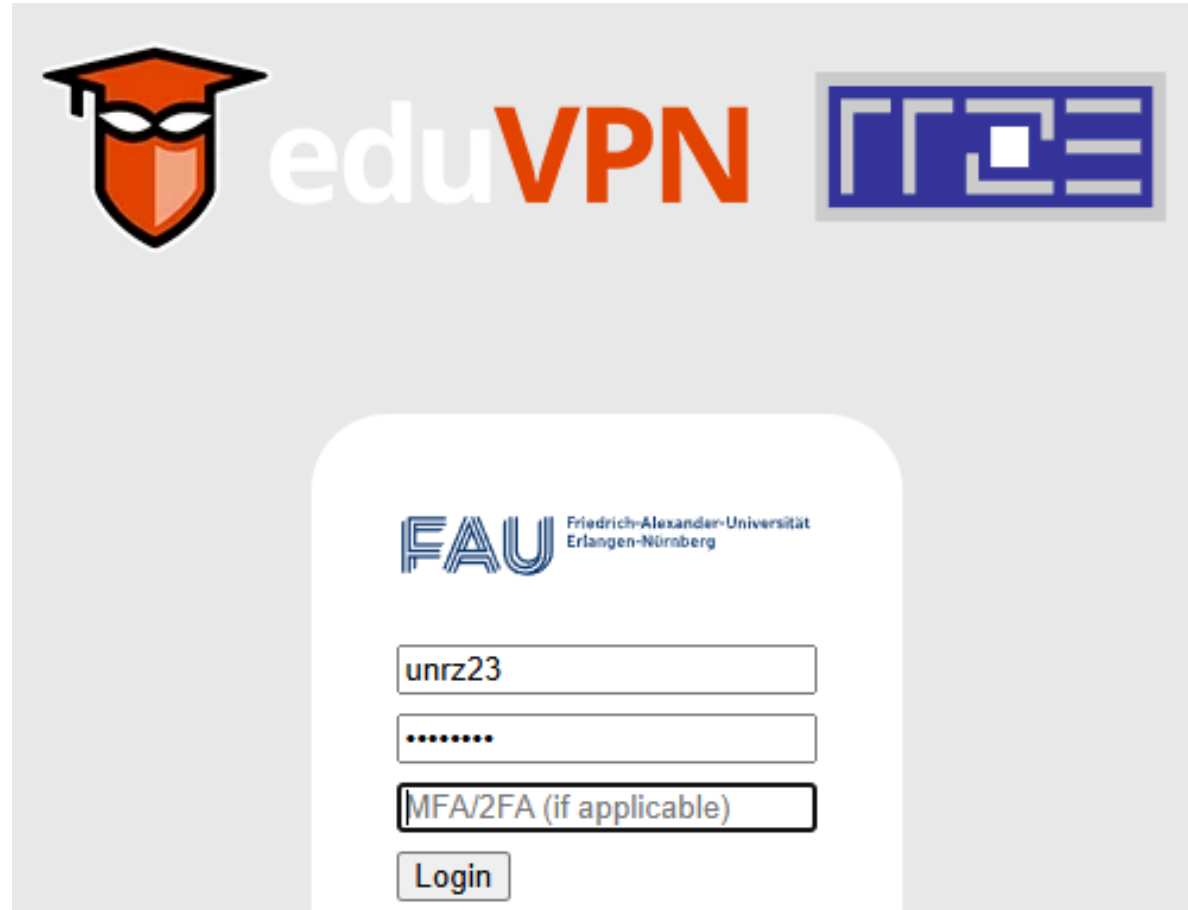
- StudOn
- Campo
- FAUbox
- sdauth.sciencedirect.com
- intern.fau.de
- FAUzoom
- fau.zeitwart.de
- FAUdir
- B-ITE

How will FAU implement MFA?



Logging in to eduVPN

- Steps 1 + 2 are integrated into the same interface:

The image shows a login interface for eduVPN. At the top left is an orange shield logo with a graduation cap. To its right is the text 'eduVPN' in white and orange. Further right is a blue square icon with white geometric shapes. Below these is a white rounded rectangle containing the FAU logo and text 'Friedrich-Alexander-Universität Erlangen-Nürnberg'. Below this are three input fields: the first contains 'unrz23', the second contains seven dots, and the third contains 'MFA/2FA (if applicable)'. At the bottom of the white rectangle is a 'Login' button.

 eduVPN 

 Friedrich-Alexander-Universität
Erlangen-Nürnberg

Login

You will need the VPN connection, for example, for:

- Accessing FSV
- Accessing network drives while working from home
- Accessing online journals from the university library

- Anyone with an IdM username **can** protect their account using MFA.
- Particularly important accounts already **must** be protected using MFA.
- In 2026, the obligation to use MFA will be rolled out further:

User group	MFA compulsory from
Staff in principal employment	May 20, 2026 ✓
Other employees and external lecturers	July 15, 2026 ✓
Students, doctoral candidates and others	November 15, 2026
Alumni	March 31, 2027

-
- There are several different options for MFA at FAU:
 - Hardware tokens (e.g. “YubiKey”)
 - Software tokens using a smartphone app
 - Software tokens using a program on your desktop computer (e.g. “KeepassXC”)
 - It makes sense to use several different options (“second key”)

- The hardware token is inserted into a USB port on your notebook.
- The one-time password / OTP / TOTP is generated automatically when you press the button.
- Staff in principal employment can pick up a Yubikey from one of the RRZE service desks (while supplies last).
Important: We would recommend attaching it to your keyring so as not to forget it.



- There are a number of different apps to choose from.
- RRZE recommends the following:
 - **Android:** “FreeOTP+” app
(must be downloaded)
 - **iOS:** “Passwords” app
(already included in iOS)
- No-one is obliged to use a smartphone. You can also use your private smartphone for MFA.
- Instructions:



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

- Again, there are a number of different programs to choose from.
- RRZE recommends KeepassXC. It is available free of charge for all standard operating systems (Windows, Linux, macOS) .
- The program is generally recommended as a password manager.

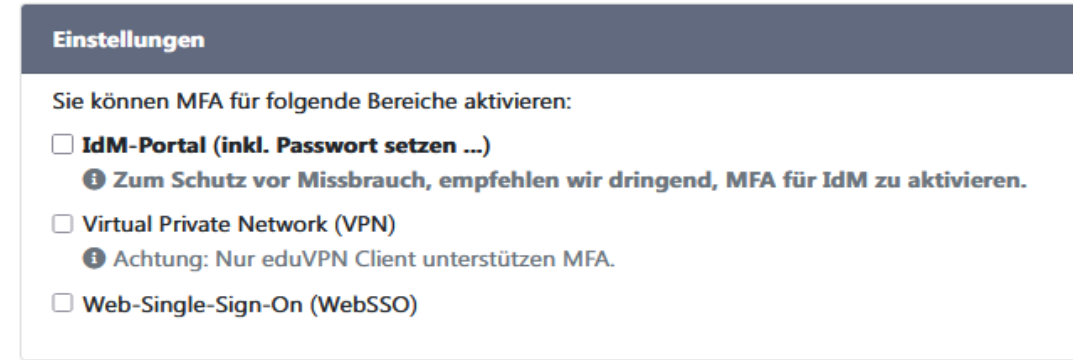


- Instructions:

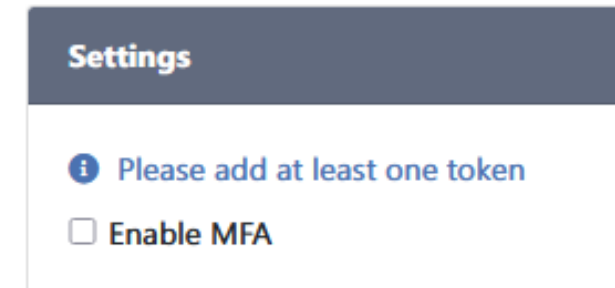
<https://www.anleitungen.rrze.fau.de/serverdienste/multifaktor-authentifizierung/>

- Anyone who set up MFA before March 2026 still has the choice of three checkboxes in the IdM portal:

<https://www.idm.fau.de/go/security/mfa>



- These three options will be merged on May 20, 2025, meaning that enabling MFA will always include all three options. Anyone setting up MFA after March 2026 will now see the following:



- Please note: Enabling MFA means that you will no longer be able to use the services without your second factor.

- MFA is nothing to be afraid of! You get used to it very quickly.
- We would definitely recommend setting up a “second key”.
- The KeepassXC program is an allround password manager. You can also use its file database with various smartphone apps and synchronize it across various devices using the FAUBox. Instructions for KeepassXC: <https://www.fau.tv/clips/31-it-tipps-aus-dem-cio-office-passwortmanager-w22>
- The 2FAGuard programme is particularly easy to set up and use, but it can only be used on one device and runs on Windows only.