

Activating Multi-factor authentication (MFA)

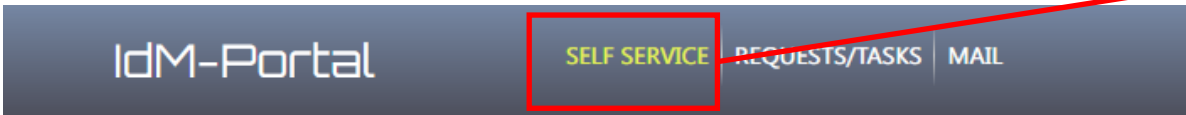


Note: If you have not yet set up an MFA token, please do so by following our instructions:

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

Once you have set up a software token or received a YubiKey, you can enable multi-factor authentication.

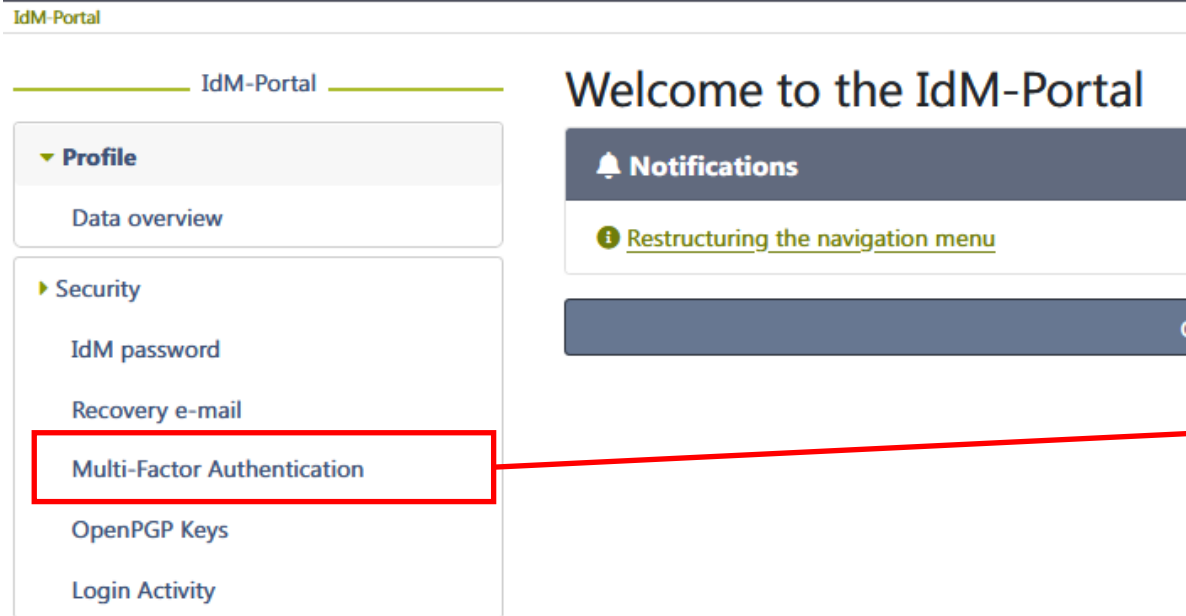
Log in to the IdM portal (<https://www.idm.fau.de/>).



(1)

Click on Self Service (1)

followed by Multi-Factor Authentication (2).



(2)

Activating Multi-factor authentication (MFA)



Please check the box “Enable MFA” in the “Settings” box.

IdM-Portal SELF SERVICE REQUESTS/TASKS MAIL

IdM-Portal / Multi-Factor Authentication

IdM-Portal

Profile
Data overview

Security

IdM password

Recovery e-mail

Multi-Factor Authentication

OpenPGP Keys

Login Activity

Settings & Applications

General settings

Multi-Factor Authentication

? Multi-Factor Authentication (MFA; encompassing Two-factor authentication or 2FA) is an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism: knowledge (something only the user knows), possession (something only the user has), and inherence (something only the user is).

Tokenverwaltung Expert-mode

Software-tokens

[Test-Token](#) Software-token

[+ Add Software-token](#)

Settings

i Links related to this security procedure

- [Multi-Faktor-Authentifizierung](#)
- [Multi-Factor Authentication instructions](#)
- [Multi-Factor Authentication FAQs](#)
- [Recommended applications](#)
 - [Android - FreeOTP+](#)
 - [macOS, iOS und iPadOS - Passwords App](#)

i The management of MFA always requires an MFA token.

Enable MFA

Activating Multi-factor authentication (MFA)



For the OTP (1), either use the code shown in your software token app or press the button on your YubiKey. Then please click on “validate and activate” (2). MFA is then activated for your account.

In order to ensure that you can remain able to work even if you do not have your software token or YubiKey to hand, please create a second software token that is not connected to your first token. Instructions are available at: <https://www.anleitungen.rrze.fau.de/serverdienste/multifaktor-authentifizierung/>

The screenshot displays the IdM-Portal interface for Multi-Factor Authentication. The main content area is titled 'Multi-Faktor-Authentifizierung' and includes a 'Tokenverwaltung' section with 'Software-Token' management. A modal dialog is open, prompting for an OTP code and a 'Validieren & Aktivieren' button. Red annotations (1) and (2) highlight the OTP input field and the activation button, respectively.

Activating Multi-factor authentication (MFA)



Multi-factor authentication is now activated for your account.

IdM-Portal SELF SERVICE | REQUESTS/TASKS | MAIL



IdM-Portal / Multi-Factor Authentication

Multi-Factor Authentication

? Multi-Factor Authentication (MFA; encompassing Two-factor authentication or 2FA) is an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism: knowledge (something only the user knows), possession (something only the user has), and inherence (something only the user is).

Tokenverwaltung Expert-mode

Software-tokens

  [Test-Token](#) Software-token

[+ Add Software-token](#)

Links related to this security procedure

- [Multi-Faktor-Authentifizierung](#)
- [Multi-Factor Authentication instructions](#)
- [Multi-Factor Authentication FAQs](#)
- [Recommended applications](#)
 - [Android - FreeOTP+](#)
 - [macOS, iOS und iPadOS - Passwords App](#)

Settings

i The management of MFA always requires an MFA token.

MFA enabled