

# iOS – Setting up an MFA token in IdM

MFA in iOS 18 with first-party “Passwords” app



Log in to the IdM portal (<https://www.idm.fau.de/>) in order to set up the software token.

The screenshot shows the IdM-Portal interface. At the top, there is a navigation bar with the text 'IdM-Portal' on the left and three menu items: 'SELF SERVICE', 'REQUESTS/TASKS', and 'MAIL'. The 'SELF SERVICE' item is highlighted with a red box and a red arrow pointing to the number '(1)'. Below the navigation bar, the main content area is titled 'Welcome to the IdM-Portal'. On the left side, there is a sidebar menu with the following items: 'Profile' (with a dropdown arrow), 'Data overview', 'Security' (with a right-pointing arrow), 'IdM password', 'Recovery e-mail', 'Multi-Factor Authentication' (highlighted with a red box and a red arrow pointing to the number '(2)'), 'OpenPGP Keys', and 'Login Activity'. On the right side, there is a 'Notifications' section with a bell icon and a message: 'Restructuring the navigation menu'.

Click on Self Service (1)

followed by Multi-Factor Authentication (2).

# iOS – Setting up an MFA token in IdM

MFA in iOS 18 with first-party “Passwords” app



Click on “Add software token”:

The screenshot shows the IdM-Portal interface. At the top, there is a navigation bar with 'IdM-Portal' and links for 'SELF SERVICE', 'REQUESTS/TASKS', and 'MAIL'. Below this, the page title is 'Multi-Factor Authentication'. On the left, a sidebar menu includes 'Profile', 'Security', 'Multi-Factor Authentication', and 'Settings & Applications'. The main content area features a help icon and text explaining MFA. Below this, there is a section for 'Tokenverwaltung' with an 'Expert-mode' link. Underneath, the 'Software-tokens' section contains a button labeled '+ Add Software-token', which is circled in red. To the right, there is an information icon and a list of links related to the security procedure, including 'Multi-Faktor-Authentifizierung', 'Multi-Factor Authentication instructions', 'Multi-Factor Authentication FAQs', and 'Recommended applications' (with sub-links for Android, macOS/iOS/iPadOS). At the bottom right, a 'Settings' section includes a message 'Please add at least one token' and an unchecked checkbox for 'Enable MFA'.

# iOS – Setting up an MFA token in IdM

MFA in iOS 18 with first-party “Passwords” app



Give the token a name (e.g. “iPhone”) (1) to ensure that you can identify the token easily later on, then click on “create” (2).

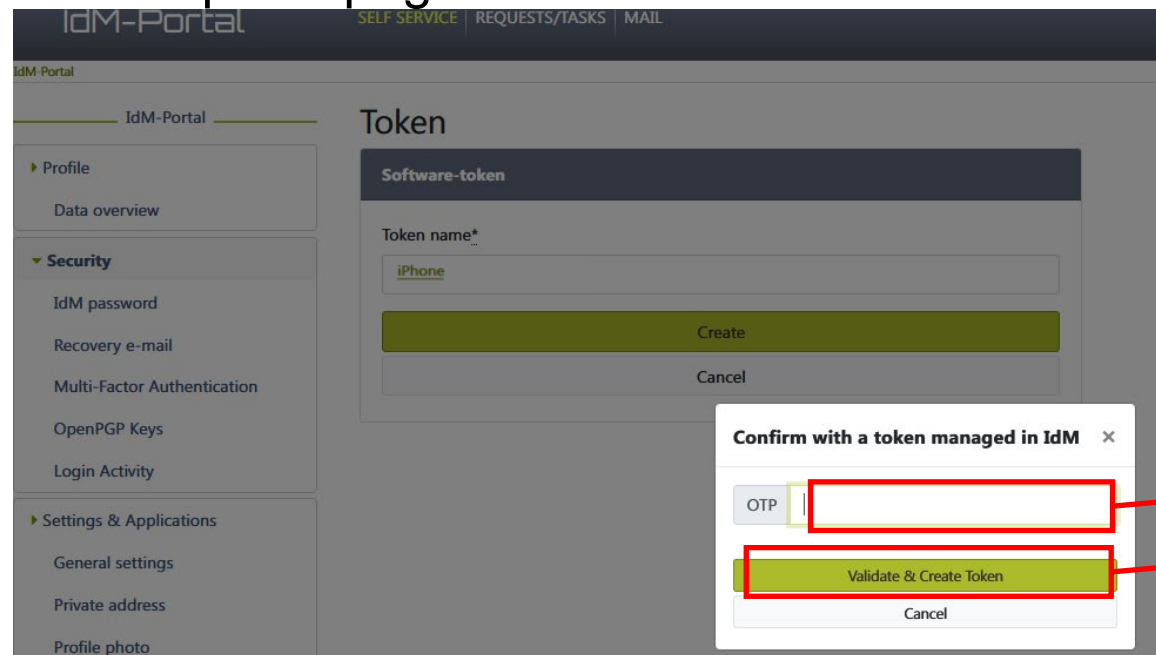
The screenshot shows the IdM-Portal interface. On the left is a navigation menu with 'Profile' and 'Security' sections. The 'Security' section is expanded, showing options like 'IdM password', 'Recovery e-mail', and 'Multi-Factor Authentication'. The main content area is titled 'Token' and contains a 'Software-token' form. The form has a 'Token name\*' field with the text 'iPhone' entered, which is highlighted with a red box and labeled (1). Below the text field are two buttons: 'Create' (highlighted with a red box and labeled (2)) and 'Cancel'.

# iOS – Setting up an MFA token in IdM

MFA in iOS 18 with first-party “Passwords” app



If you have already set up a token—which can be a YubiKey or a software token—this message will appear. Otherwise, you can skip this page.



Enter a one-time password in the “OTP” field (1) to confirm. You can do this either by pressing the button on your YubiKey or by using one of your existing software tokens. Then click “Validate & Create Token” (2).

# iOS – Setting up an MFA token in IdM

MFA in iOS 18 with first-party “Passwords” app



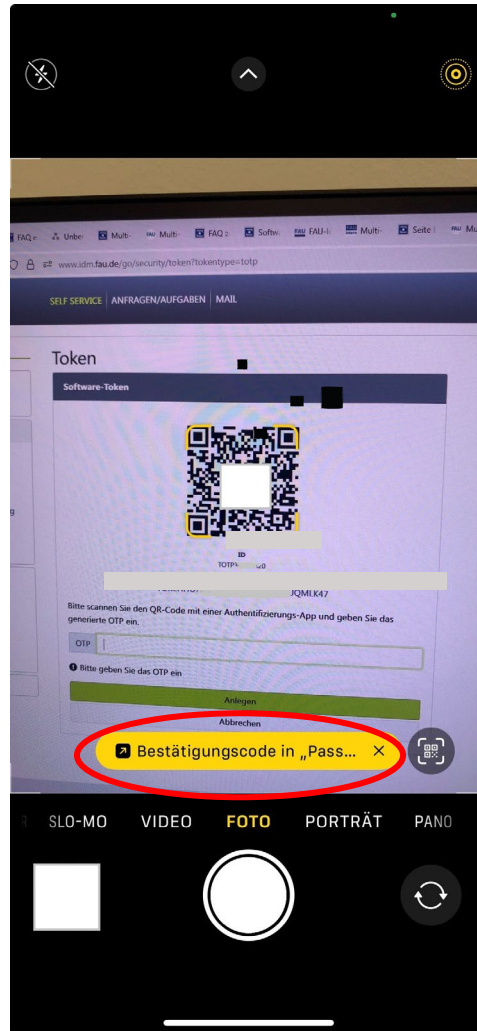
The screenshot shows the IdM-Portal interface. The top navigation bar includes 'IdM-Portal', 'SELF SERVICE', 'REQUESTS/TASKS', and 'MAIL'. The left sidebar contains a menu with categories: Profile (Data overview), Security (IdM password, Recovery e-mail, Multi-Factor Authentication, OpenPGP Keys, Login Activity), Settings & Applications (General settings, Private address, Profile photo, Payment information), and Privacy self disclosure. The main content area is titled 'Token' and shows a 'Software-token' section. A QR code is displayed and circled in red. Below the QR code, the token ID is shown as 'ID TO1-087' and the secret as 'SECRET GLF6P[redacted]/6ESI'. A message instructs the user to scan the QR code with an Authenticator App and enter the generated OTP. An input field for the OTP is provided, along with 'Create' and 'Cancel' buttons.

In the next step, you are shown a QR code.

Open the camera app on your iOS device and hold the camera up to the QR code.

# iOS – Setting up an MFA token in IdM

MFA in iOS 18 with first-party “Passwords” app



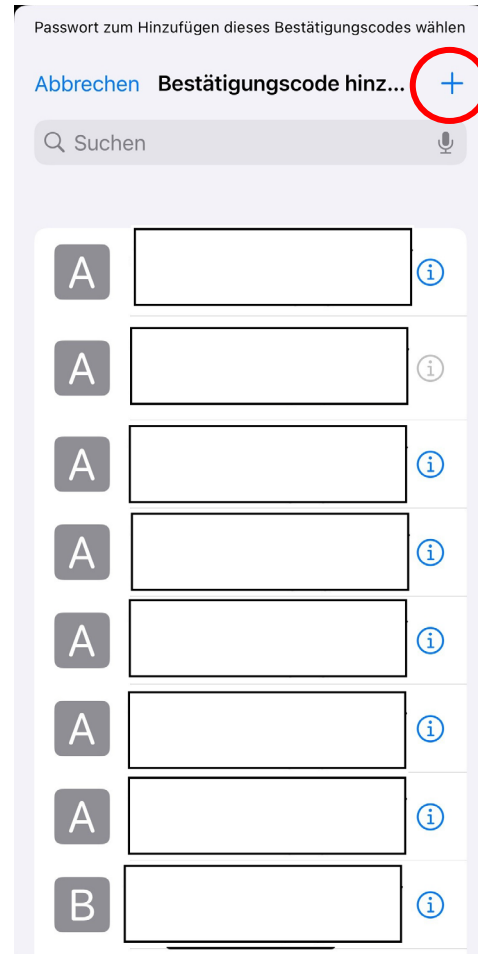
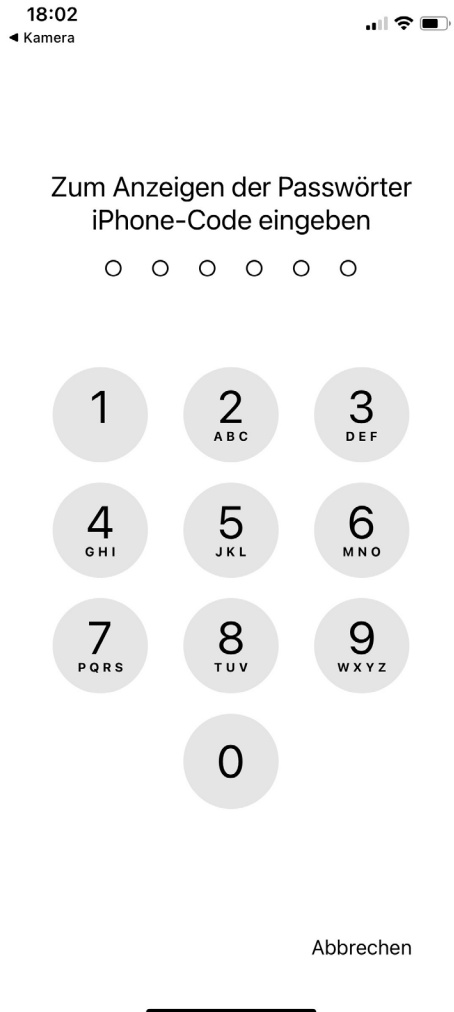
As soon as your device recognizes the code, a button appears: “Add verification code in Passwords”

Click on this button, and the Passwords app opens.

You can create a new entry using the “+” icon.

# iOS – Setting up an MFA token in IdM

MFA in iOS 18 with first-party “Passwords” app

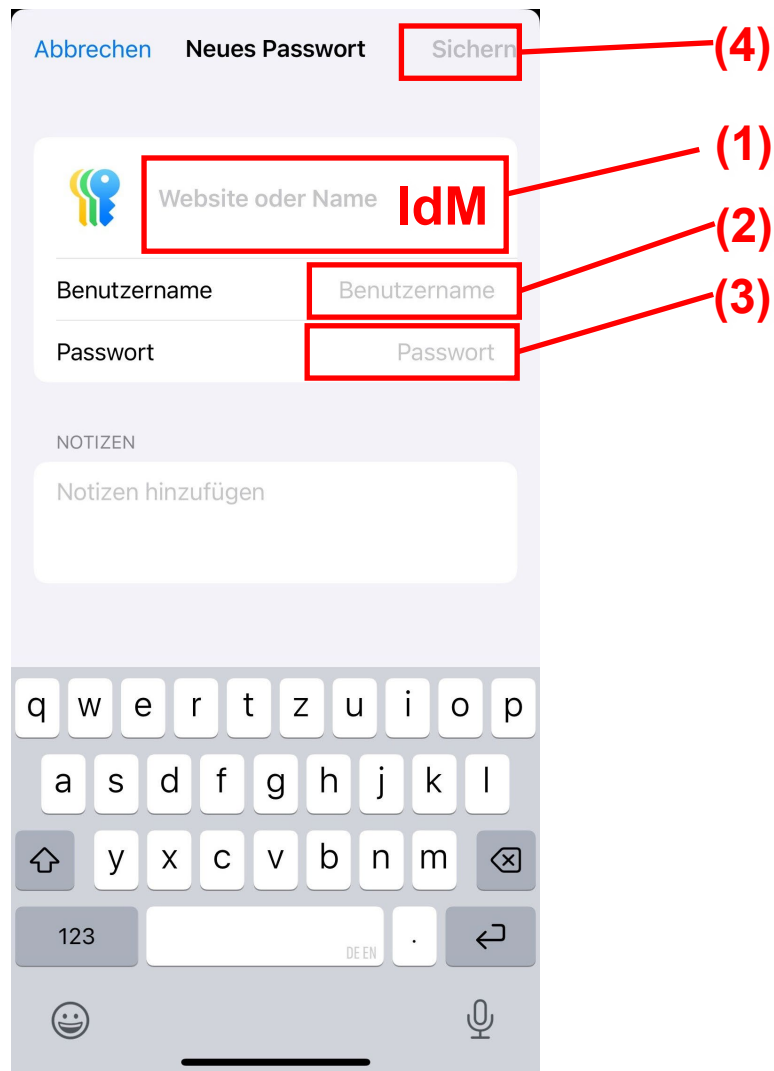


Unlock the Passwords app using your iPhone code.

Tip on the “+” icon to create a new entry.

# iOS – Setting up an MFA token in IdM

MFA in iOS 18 with first-party “Passwords” app

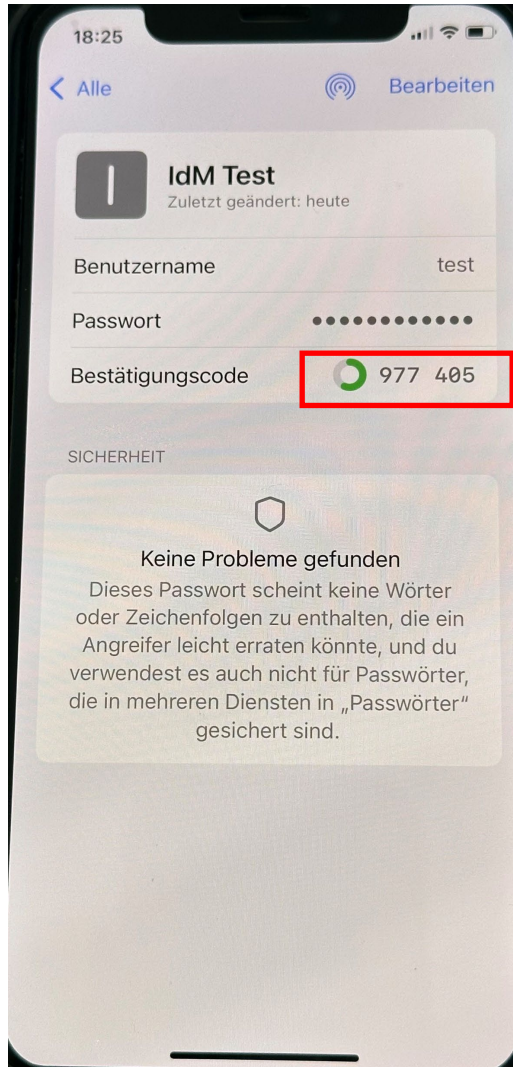


Give this entry a name (e.g. “IdM”) (1), and save your IdM data if applicable (2) or (3). To confirm, tip on “save” (4).

Your one-time password is now visible in the app. Enter the code in the open IdM portal (website) to complete the installation.

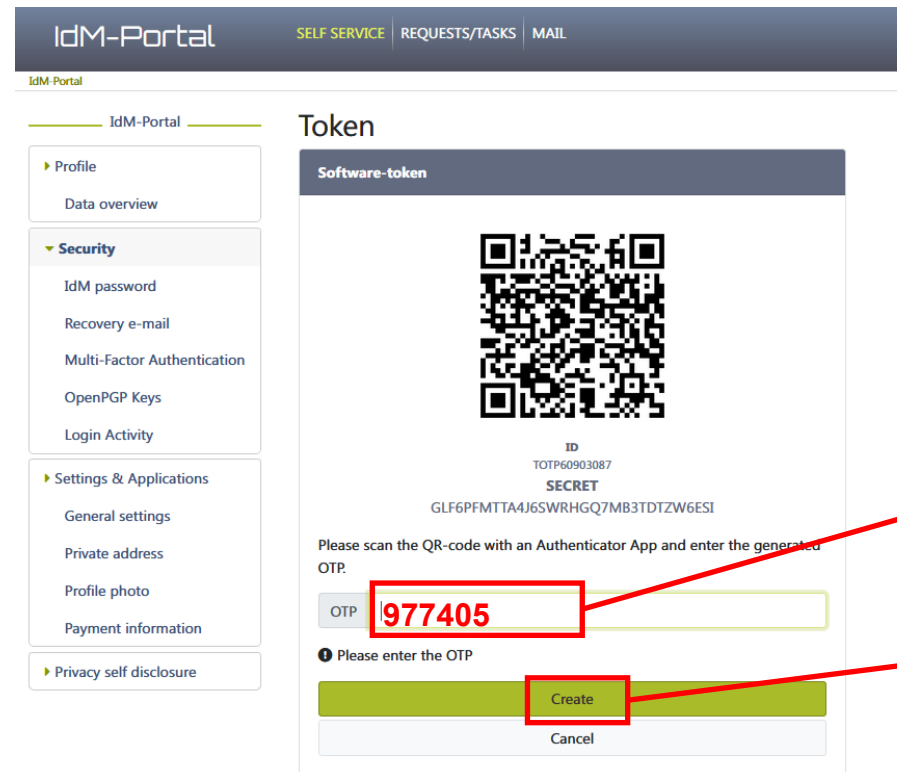
# iOS – Setting up an MFA token in IdM

MFA in iOS 18 with first-party “Passwords” app



Your one-time password is now visible in the app (1).

Enter the code in the open IdM portal (2) to complete the installation by clicking on “create” (3)..

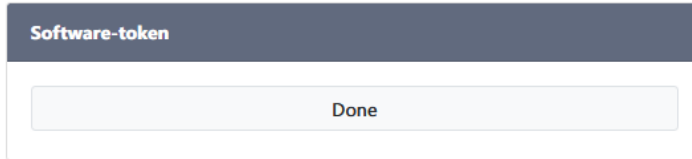


# iOS – Setting up an MFA token in IdM

MFA in iOS 18 with first-party “Passwords” app



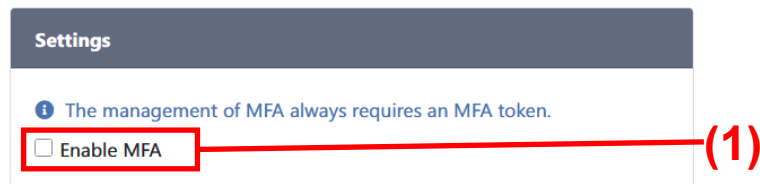
Token



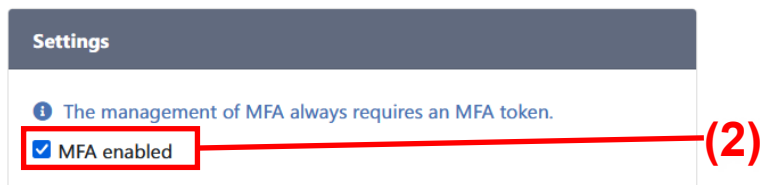
Once you see the message “done”, your MFA token has successfully been installed on your iPhone.

If you have not yet activated MFA, (as in example (1)), follow the instructions at

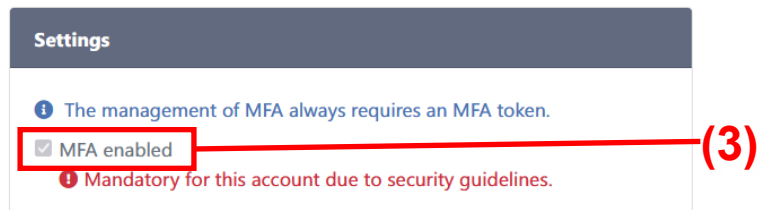
<https://www.anleitungen.rrze.fau.de/serverdienste/multifaktor-authentifizierung/faqs-zur-multifaktor-authentifizierung/#ID-12840>



Once successfully activated, it will look like in example (2) or (3).



In order to ensure that you can remain able to work even if you do not have your iPhone to hand, please create a second software token that is not connected to your iPhone. Instructions are available at:



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