

KeePassXC – Setting up an MFA token in IdM

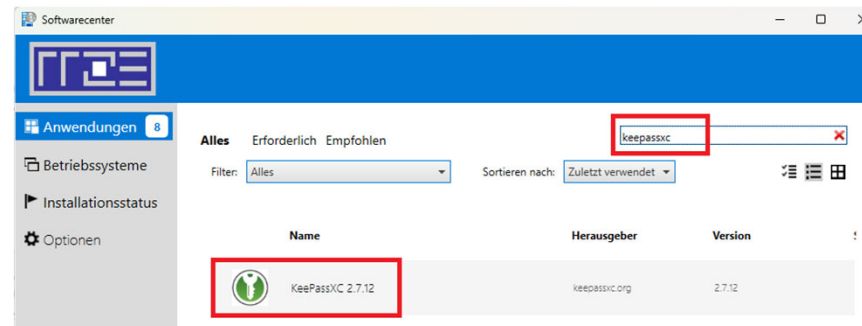
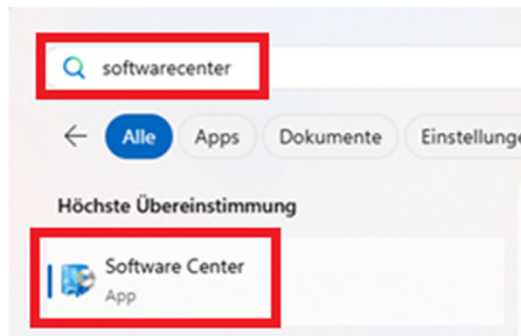
MFA in Windows / macOS / Linux



Note: If you are already using KeePassXC to manage your passwords, you can skip the steps for setting up KeePassXC and go straight to slide 5.

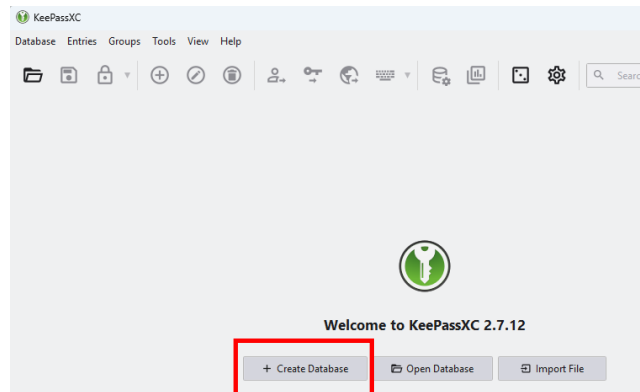
Install the KeePassXC software:

- You can download KeePassXC for Windows, macOS and Linux free of charge:
<https://keepassxc.org/download/>
- On a Windows device managed by RRZE, you will find KeePassXC in the Software Center and can download it without admin rights:

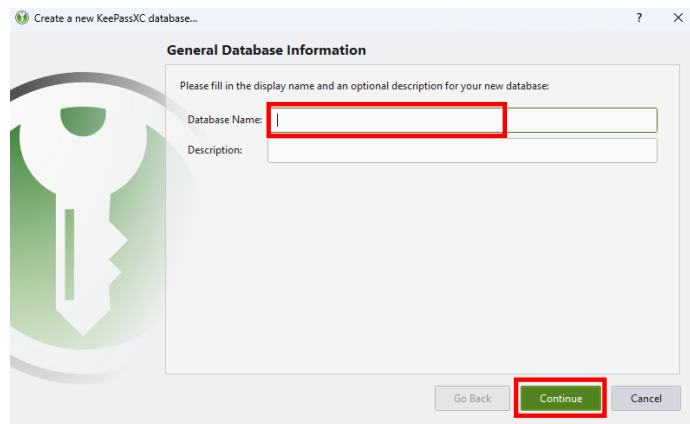


KeePassXC – Setting up an MFA token in IdM

MFA in Windows / macOS / Linux



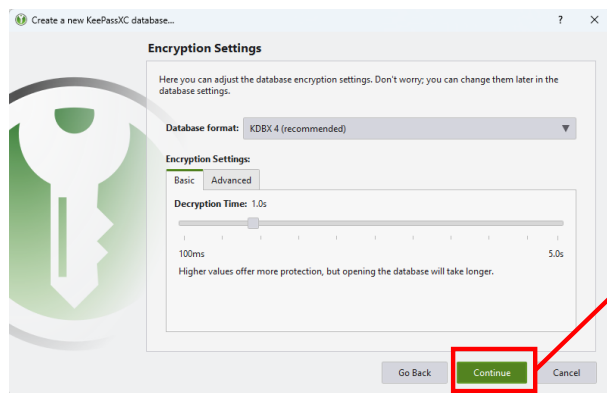
Click on “Create database” if you are not yet using KeePassXC. If you are using it already, open your existing KeePassXC database by clicking on “Open database”.



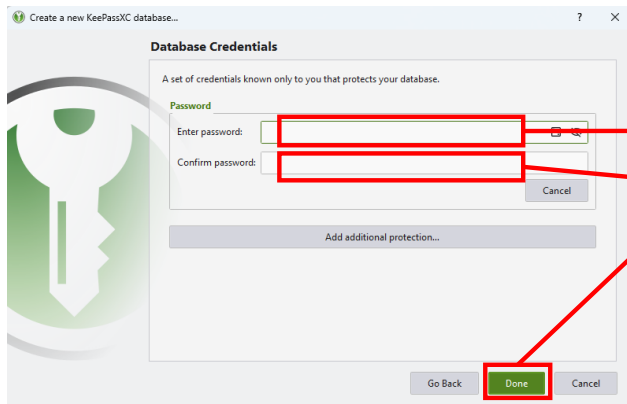
Give the new database a name (e.g. “FAU MFA”) and click on “Continue”.

KeePassXC – Setting up an MFA token in IdM

MFA in Windows / macOS / Linux



You do not need to enter anything under encryption settings and can simply click on “Continue” (1).



Think of a password that is either highly complicated or consists of several words. Enter the password in the boxes (2) and (3) and click “Done” (4).

You will always require this password when using KeePassXC in future. Please make sure you memorize it well.

KeePassXC – Setting up an MFA token in IdM

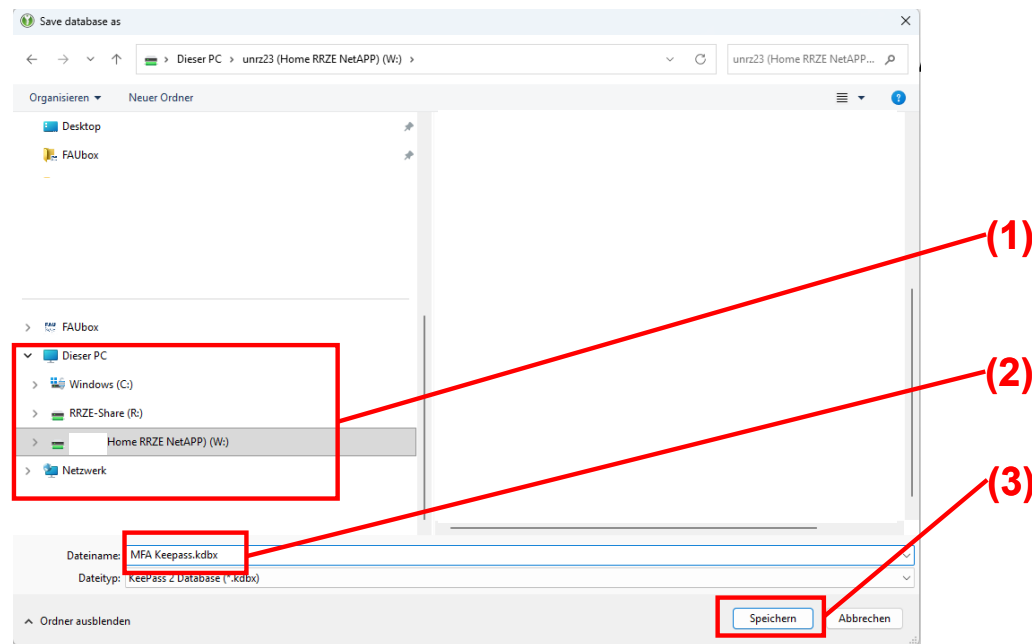
MFA in Windows / macOS / Linux



Choose a suitable location for saving your KeePass file (1).

Give a suitable name (e.g. “FAU MFA.kdbx”) (2) and click on “save” (3).

After saving, KeePassXC will open. You can leave the program open. We will need it in the next step.



KeePassXC – Setting up an MFA token in IdM

MFA in Windows / macOS / Linux



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 following items: 'SELF SERVICE', 'REQUESTS/TASKS', and 'MAIL'. The 'SELF SERVICE' item is highlighted with a red box and labeled (1). Below the navigation bar, there is a 'Welcome to the IdM-Portal' message and a 'Notifications' section. On the left side, there is a 'Profile' section with 'Data overview' and a 'Security' section with 'IdM password', 'Recovery e-mail', 'Multi-Factor Authentication', 'OpenPGP Keys', and 'Login Activity'. The 'Multi-Factor Authentication' option is highlighted with a red box and labeled (2).

Click on Self Service (1)
followed by Multi-Factor Authentication (2).

KeePassXC – Setting up an MFA token in IdM

MFA in Windows / macOS / Linux



Click on “Add software token”:

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

+ Add Software-token

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 A](#)

Settings

i Please add at least one token

Enable MFA

KeePassXC – Setting up an MFA token in IdM

MFA in Windows / macOS / Linux



Give the token a name (e.g. “KeepassXC”) (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 main content area is titled 'Token' and shows a 'Software-token' form. The 'Token name*' field is filled with 'KeepassXC' and is highlighted with a red box and labeled (1). Below the field are 'Create' and 'Cancel' buttons, with the 'Create' button highlighted by a red box and labeled (2).

KeePassXC – Setting up an MFA token in IdM

MFA in Windows / macOS / Linux

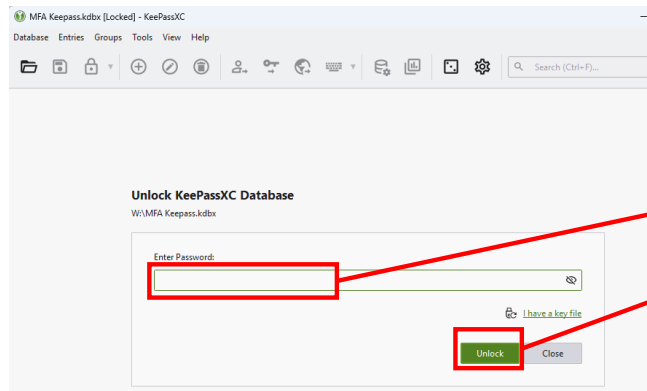


The screenshot shows the IdM-Portal interface. The top navigation bar includes 'IdM-Portal', 'SELF SERVICE', 'REQUESTS/TASKS', and 'MAIL'. The left sidebar contains a menu with categories: Profile (Data overview), Security (IdM password, Recovery e-mail, Multi-Factor Authentication, OpenPGP Keys, Login Activity), Settings & Applications (General settings, Private address, Profile photo, Payment information), and Privacy self disclosure. The main content area is titled 'Token' and contains a 'Software-token' section. It features a QR code for scanning. Below the QR code, the ID is 'TO: [redacted] 087' and the secret is 'SECRET'. A red box highlights the secret code 'GLF6P[redacted]/6ESI'. Below this, there is a text input field for the OTP, a 'Please enter the OTP' message, and 'Create' and 'Cancel' buttons.

- In the next step, you are shown “SECRET”.
- Copy the “SECRET” code to your clipboard.

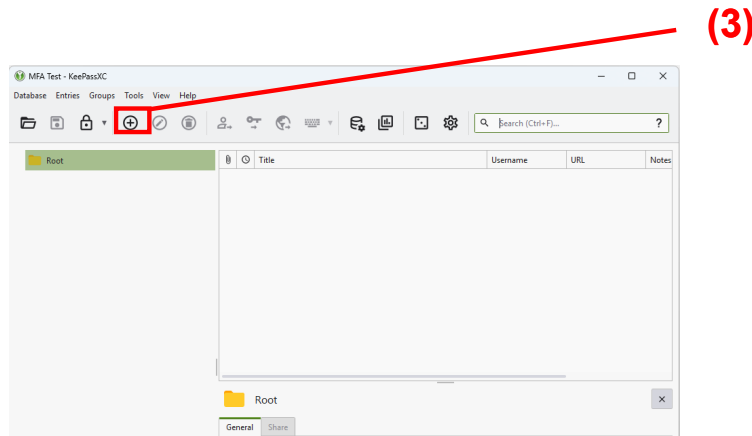
KeePassXC – Setting up an MFA token in IdM

MFA in Windows / macOS / Linux



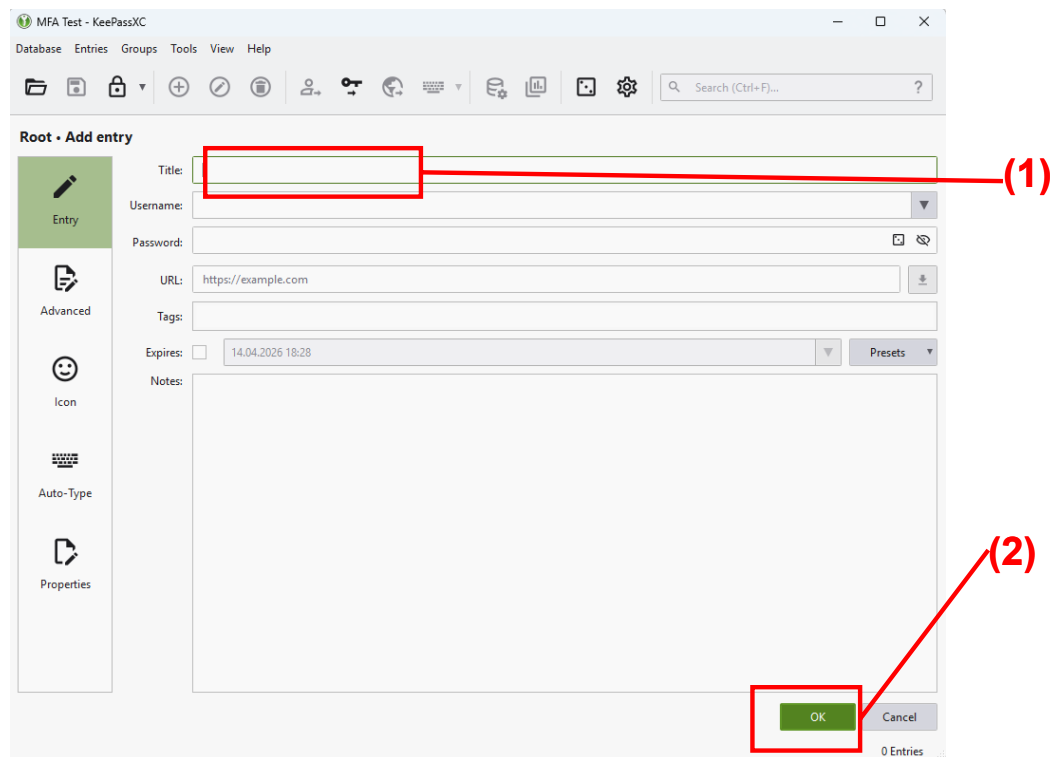
- Open KeePassXC, enter your password (1) and click on “Unlock” (2).

- Next, click on the “+” icon (3) to create a new entry in the database.



KeePassXC – Setting up an MFA token in IdM

MFA in Windows / macOS / Linux



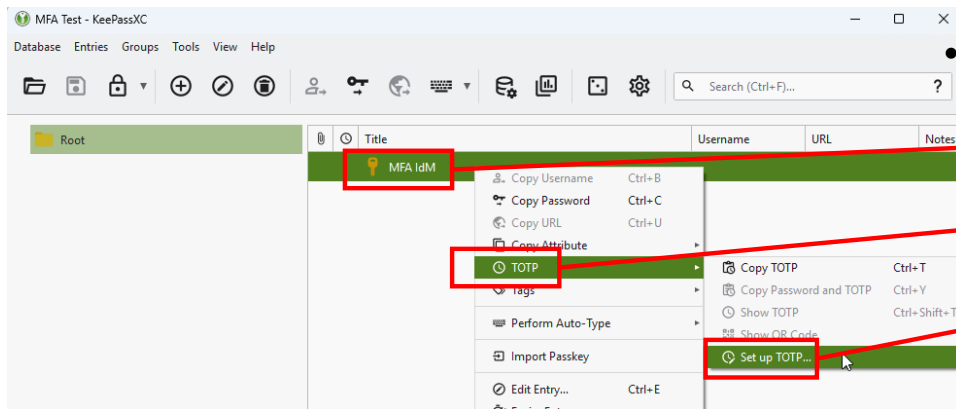
Give the entry a title (e.g. “MFA IDM”) (1) and click on “OK” (2).

KeePassXC – Setting up an MFA token in IdM

MFA in Windows / macOS / Linux

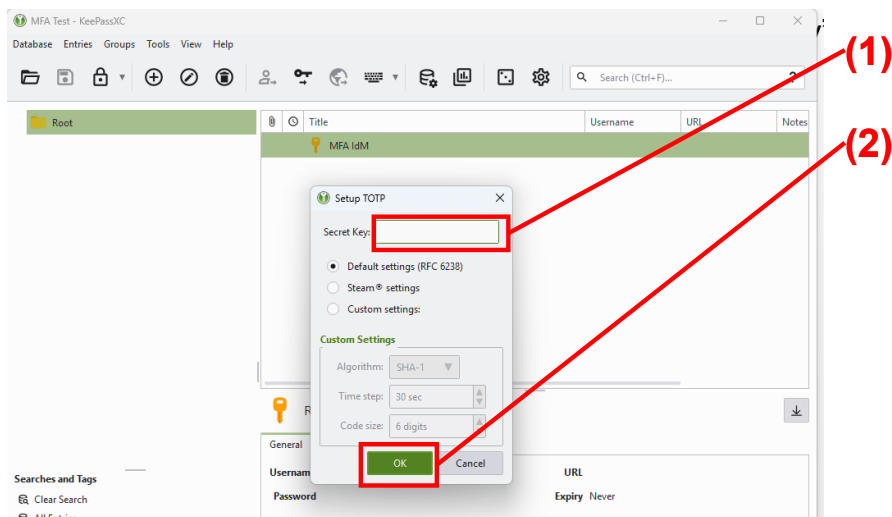


- Right click on your newly created entry (1).
- Select “TOTP” (2) and “Set up TOTP” (3).



KeePassXC – Setting up an MFA token in IdM

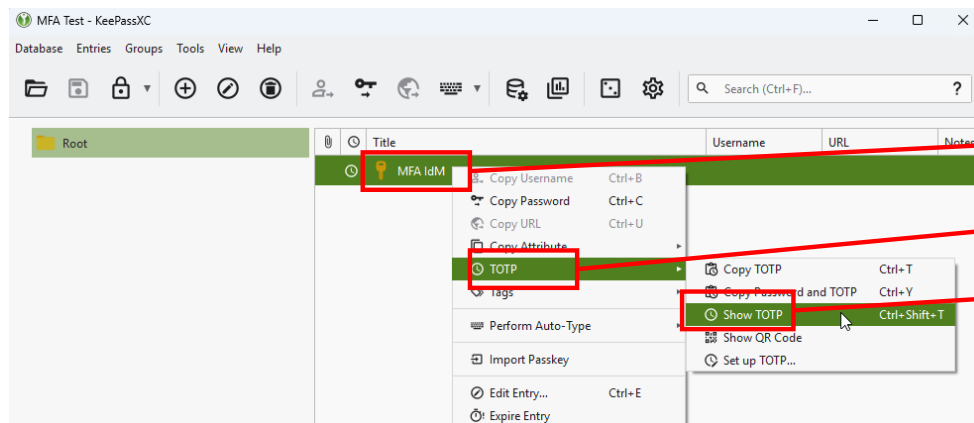
MFA in Windows / macOS / Linux



- Copy the “SECRET” code from the IdM portal into the box “Secret key” (1).
- Confirm with “OK” (2).

KeePassXC – Setting up an MFA token in IdM

MFA in Windows / macOS / Linux



- Right click on your entry (1).
- Select “TOTP” (2) and “Show TOTP” (3).
- Alternatively, you can use the key combination CTRL+shift+T

KeePassXC – Setting up an MFA token in IdM

MFA in Windows / macOS / Linux



The screenshot shows the IdM-Portal interface. At the top, a 'Timed Password' window displays the OTP '295 826' (1). Below it, the IdM-Portal 'Token' page is visible. The page shows a QR code for the 'Software-token' and a 'Create' button (3). The 'Create' button is highlighted with a red box. The 'OTP' input field is also highlighted with a red box (2).

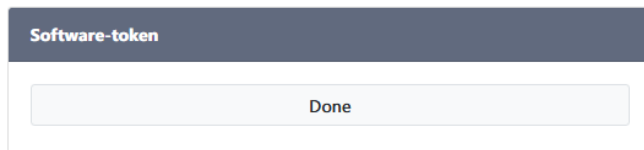
- You can now see the OTP, that changes automatically every 30 seconds (1).
- Enter this OTP in the IdM portal in the box “OTP” (2).
- Click on “Create” (3) to complete the process.

KeePassXC – Setting up an MFA token in IdM

MFA in Windows / macOS / Linux



Token



Once you see the message “done”, your MFA token has successfully been entered in KeePassXC.

If you have not yet activated MFA, please check the box “Enable MFA”.

IdM-Portal SELF SERVICE REQUESTS/TASKS MAIL

IdM-Portal / Multi-Factor Authentication

Multi-Factor Authentication

Profile
Data overview

Security
IdM password
Recovery e-mail

Multi-Factor Authentication
OpenPGP Keys
Login Activity

Settings & Applications
General settings

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).

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

Tokenverwaltung Expert-mode

Software-tokens

Icon	Name	Type
		KeePassXC
		Software-token

[+ Add Software-token](#)

Settings

The management of MFA always requires an MFA token.

Enable MFA

KeePassXC – Setting up an MFA token in IdM

MFA in Windows / macOS / Linux



For the OTP, enter the code shown in KeePass (1) and click on “validate and activate”.

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 KeePass file to hand, please create a second software token that is not connected to your KeePassXC database. Instructions are available at:

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

