What is Cryptomator?

Cryptomator is a free application that allows you to easily store encrypted data in a cloud or a NAS. In the instructions that follow we show you how to use Cryptomator to encrypt your data.

Useful information on Cryptomator

- You need administrator's rights on your device to install Cryptomator. If you do not have administrator's rights, please contact your administrator or the IT Support team in room 364.
- If you want to share a folder you have encrypted with Cryptomator, the other person must also install Cryptomator in order to open the encrypted folder.
- Even if you choose the secure encryption process AES-256, the file is only as secure as your password. Please take this into account when choosing your password! Use at least 20 letter/numbers/special characters.
- You have the option to create a recovery key. If you forget your password, the recovery key is the only option to access your encrypted data. It is very important that you store the key at a secure location which is inaccessible to third parties.
- There is a portable version for Windows and Linux. (A version that does not need installing.)
- You can chose to crypt files in the cloud and you can move the folder I the future if needed.

What are the disadvantages of Cryptomator?

- If you open an encrypted folder, without unlocking it first, you will see the files contained in the folder. However, Cryptomator converts the files into the C9R format so that the original files cannot be traced back. The file format, date of creation and file names are not shown. You only see the number of files.
- If you use a shared encrypted folder (e.g. in OneDrive/Box), it is not possible to simultaneously work on the files in this folder.

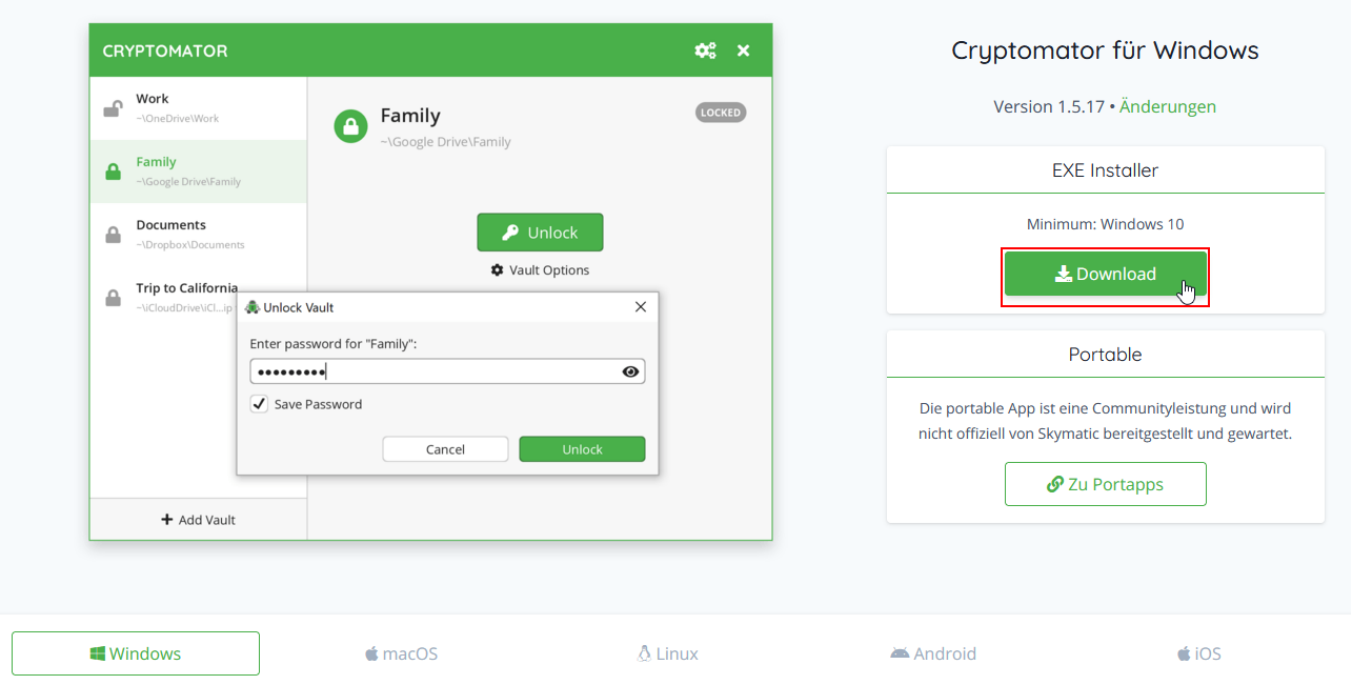
How can I use Cryptomator?

Download & installation

Step 1: Download Cryptomator

Click on the following link to download and install Cryptomator for your operating system: https://cryptomator.org/downloads/

Important information: Please note that you need administrator's rights to install Cryptomator on your device. If you do not have admin rights, please contact your administrator or the IT Support in room 364.



If you click on the link, you will also find versions for other operating systems, such as MacOS or Linux. The Linux version is an appimage and should work as an portable app. There is also a portable version available from the download site at https://cryptomator.org/downloads/

Step 2: Install Cryptomator (Windows/Linux/MacOS)

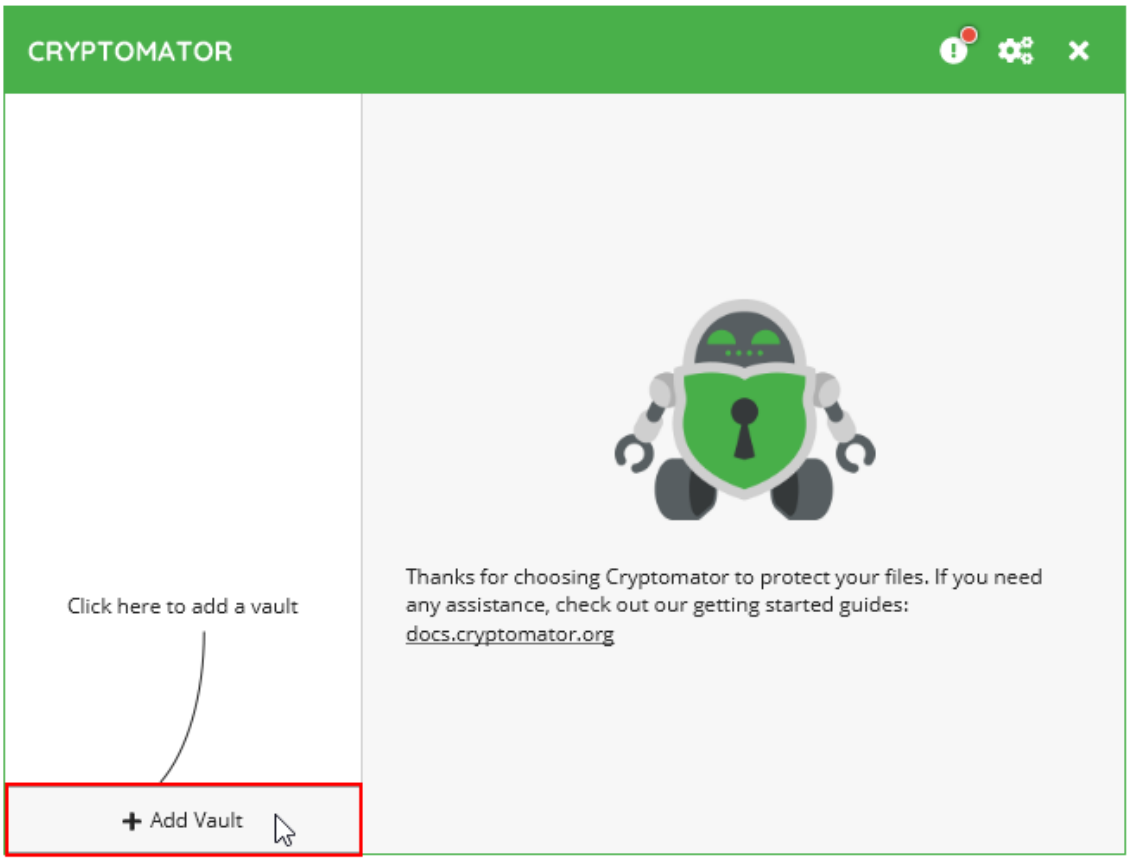
By opening the .exe file that you have downloaded, you start the installation of Cryptomator. After you have installed Cryptomator, you can directly start the program. In Linux make the appimage executable and run it. In MacOS install the dmg file, and run Cryptomator. For Android and iOS download from Google Play and App Store (These versions are not free)

Create a new vault

Step 1: Add vault

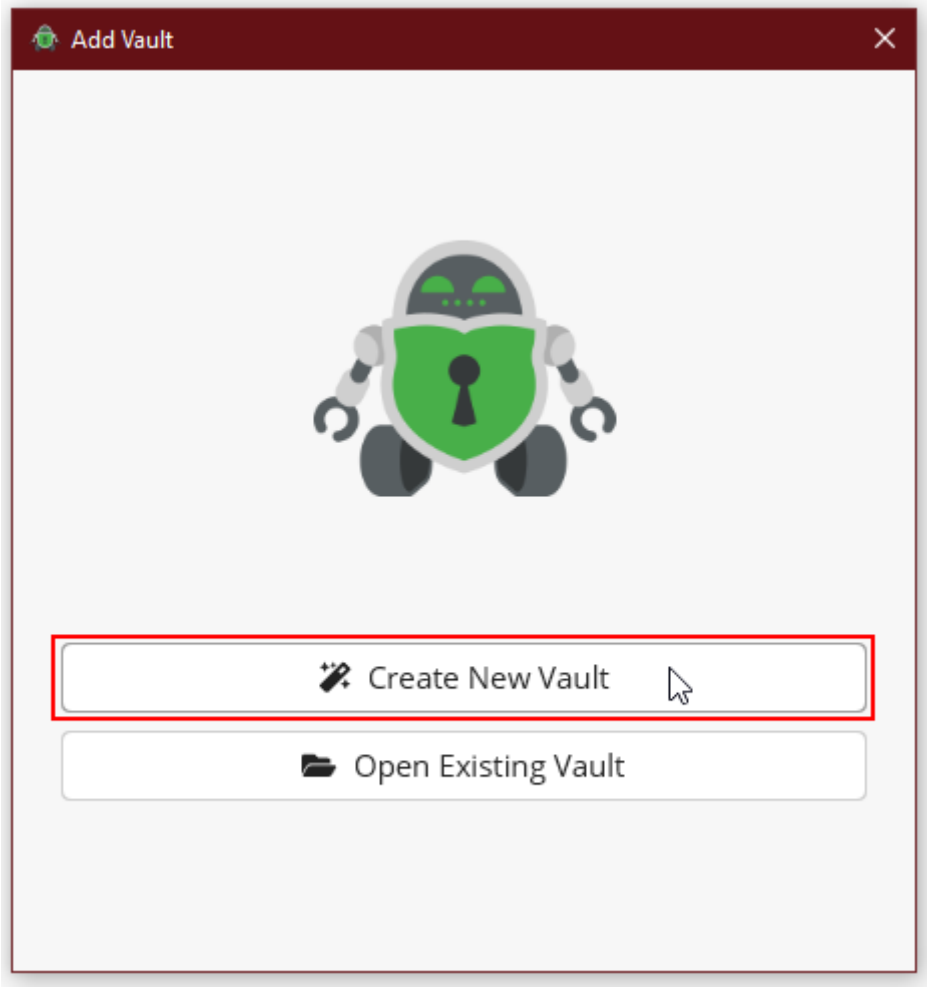
Start Cryptomator.

Select “Add vault”.



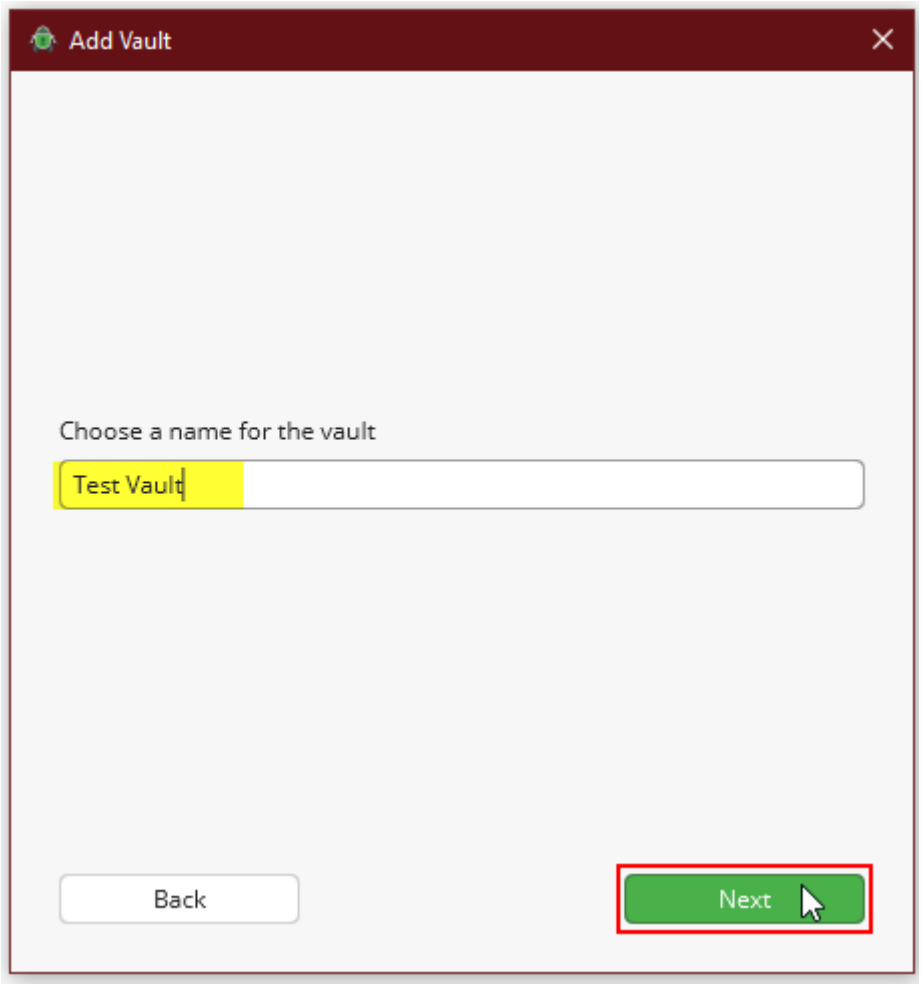
Step 2: Create a new vault

Select “Create New Vault”.



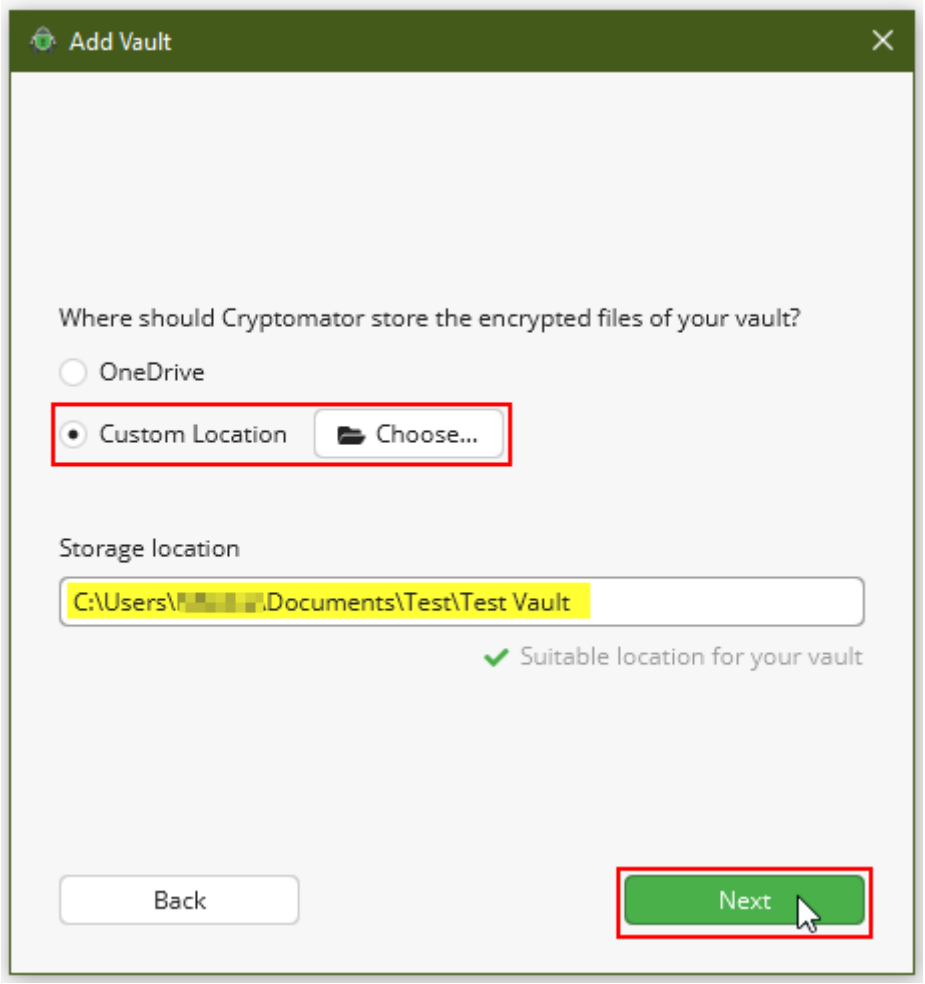
Step 3: Choose a name for the vault

Enter a name for your vault and confirm by clicking “Next”.



Step 4: Choose a storage location

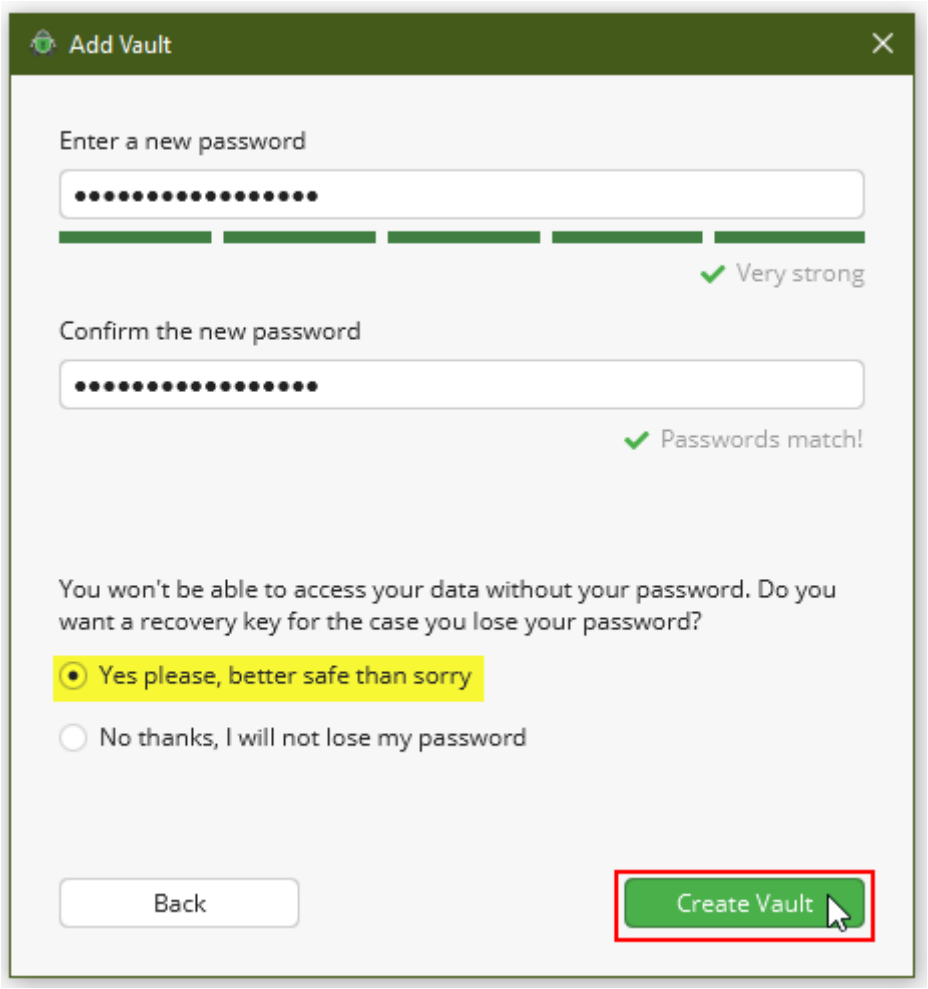
Via “Choose...”, you can select the desired storage location for your vault. Confirm your selection by clicking “Next”.



Step 5: Choose a password

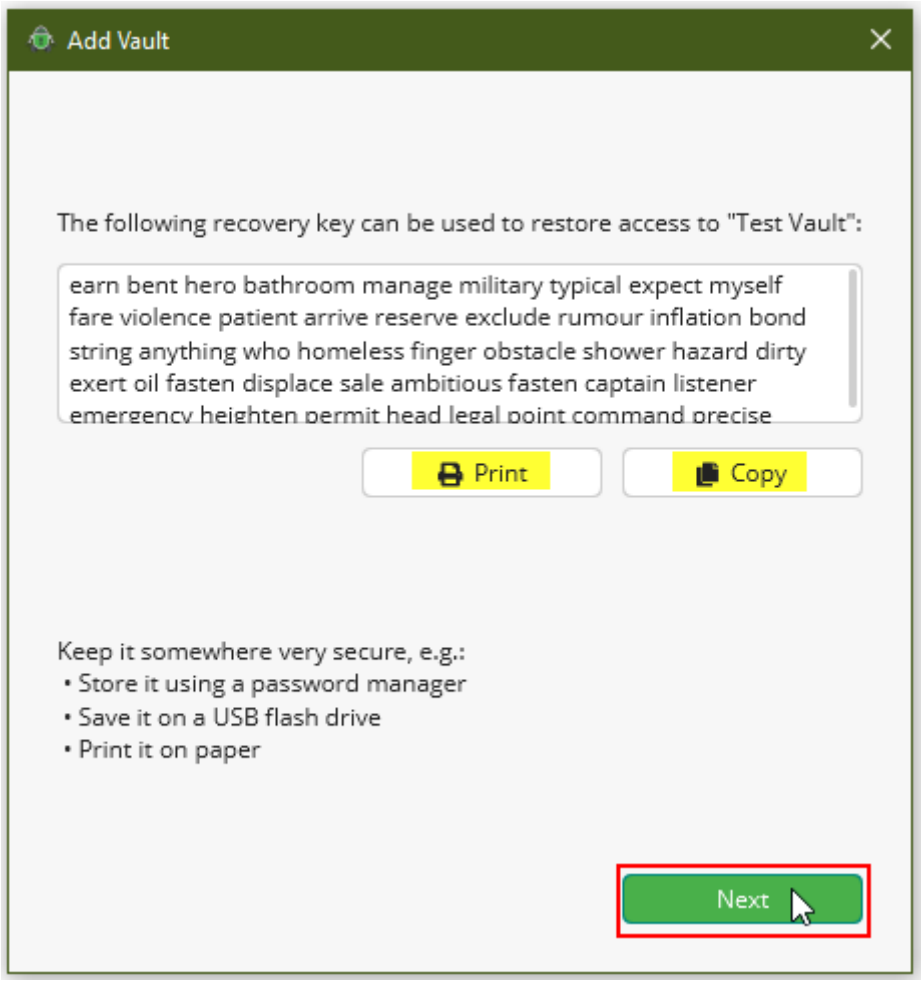
Then you have to choose a password for your vault. Choose a secure password with at least 20 characters.

You also have the possibility to create a recovery key. If you have forgotten your password, the recovery key is the only option to unlock your vault.



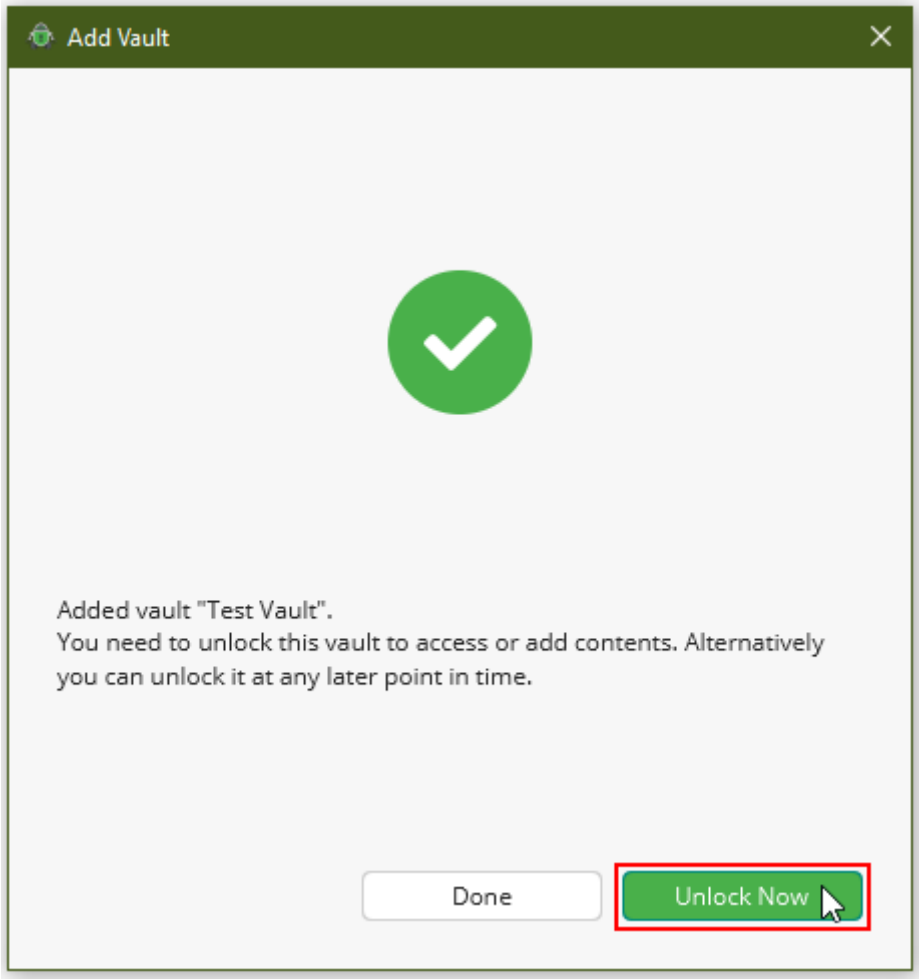
Step 6: Recovery key

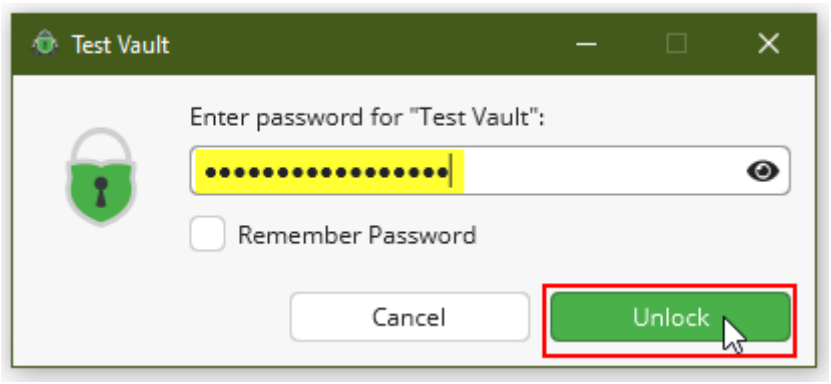
Print your recovery key or copy it to a password management program or on a USB stick. Third parties must not be able to access the key. The key must also not be stored together with the encrypted vault.



Step 7: Unlocking a vault

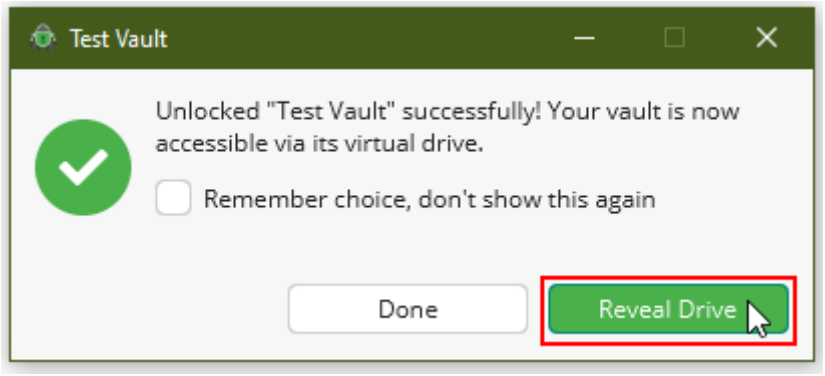
After you have created a new vault, you can unlock the vault by entering your password.

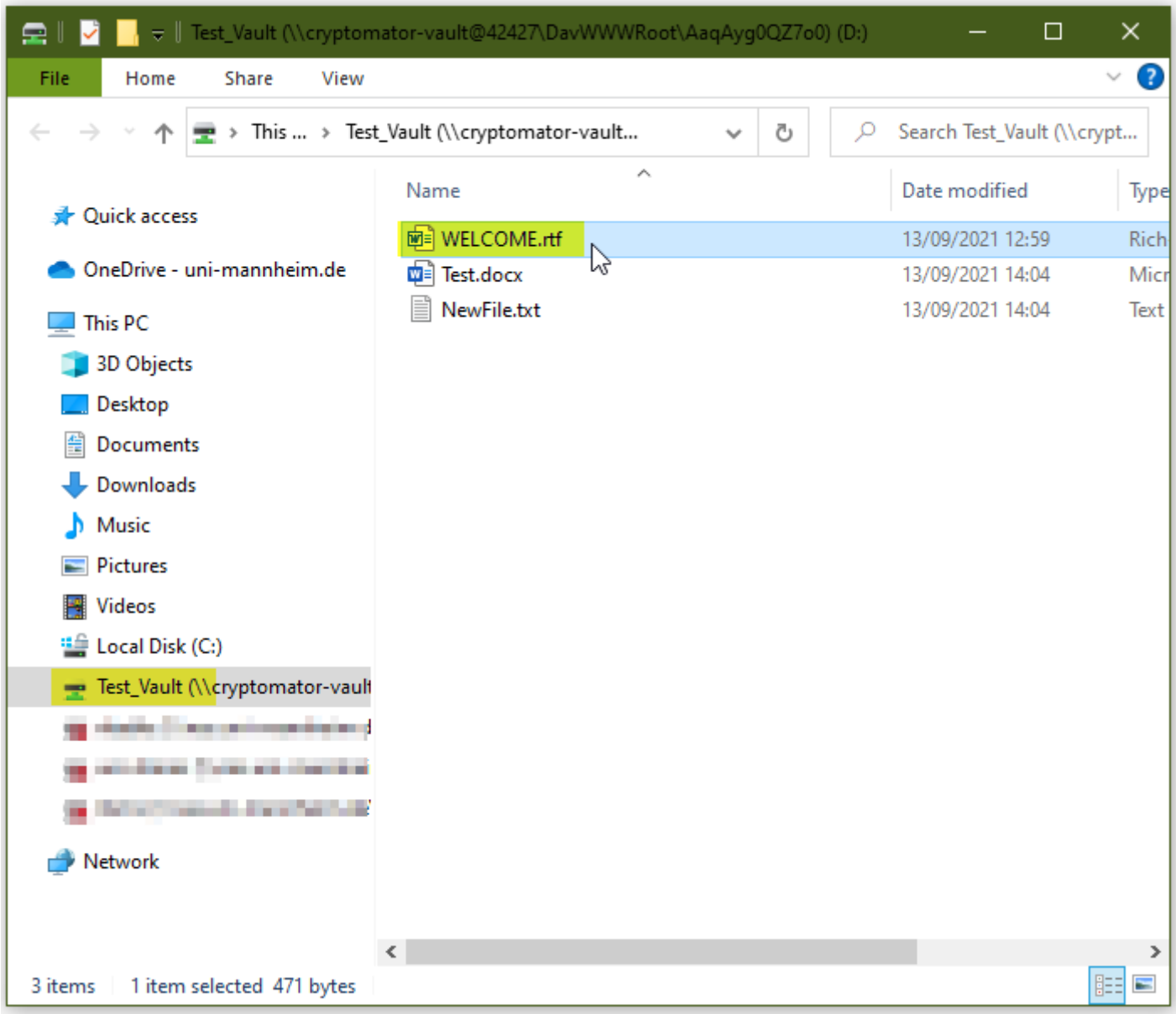




Step 8: Manage files

After you have unlocked the vault, you can see the contents of the vault.



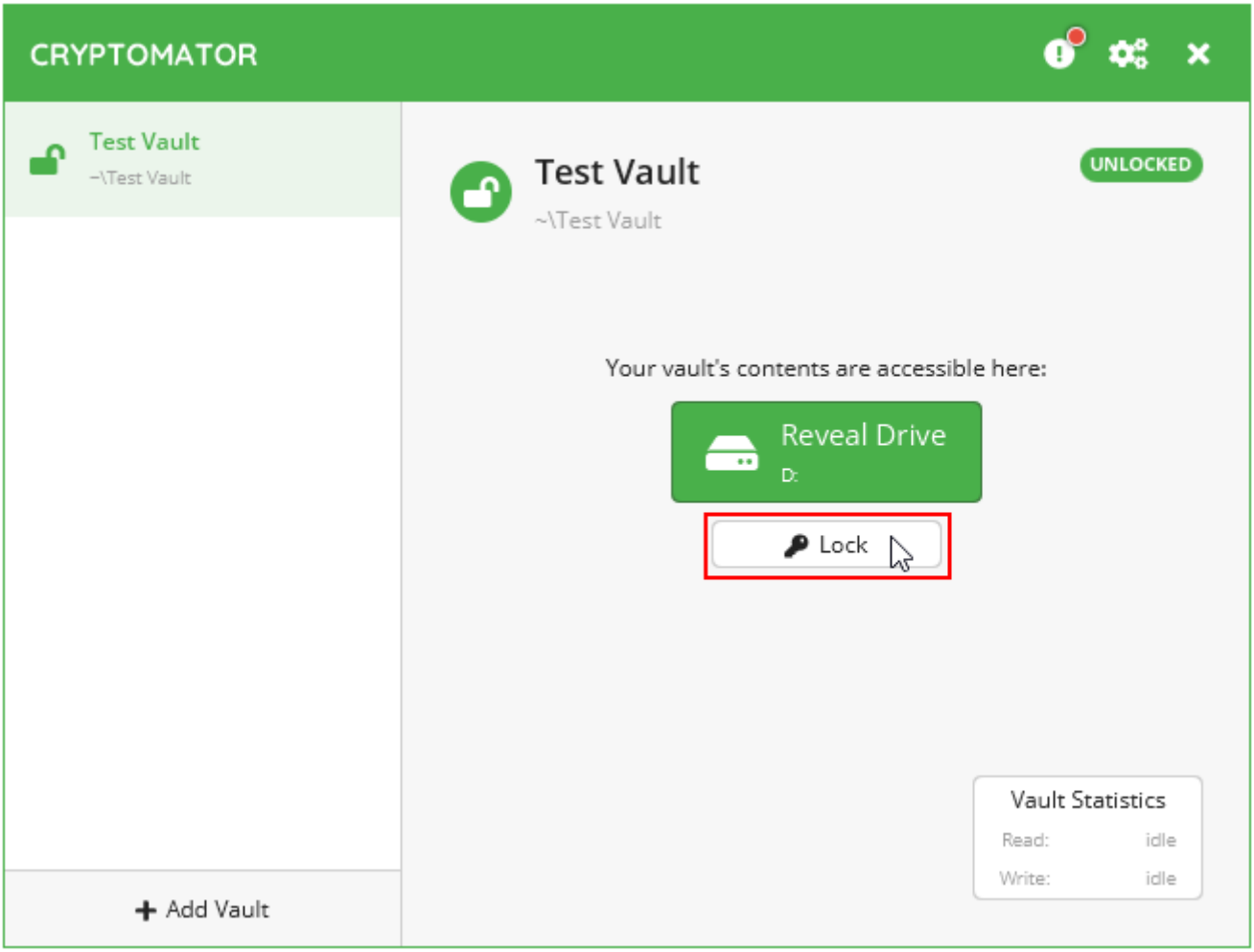


Now you can add, edit or delete files.

The “WELCOME.rtf” file contains some information on the vault. After you have read the file, you can delete it.

Step 9: Lock vault

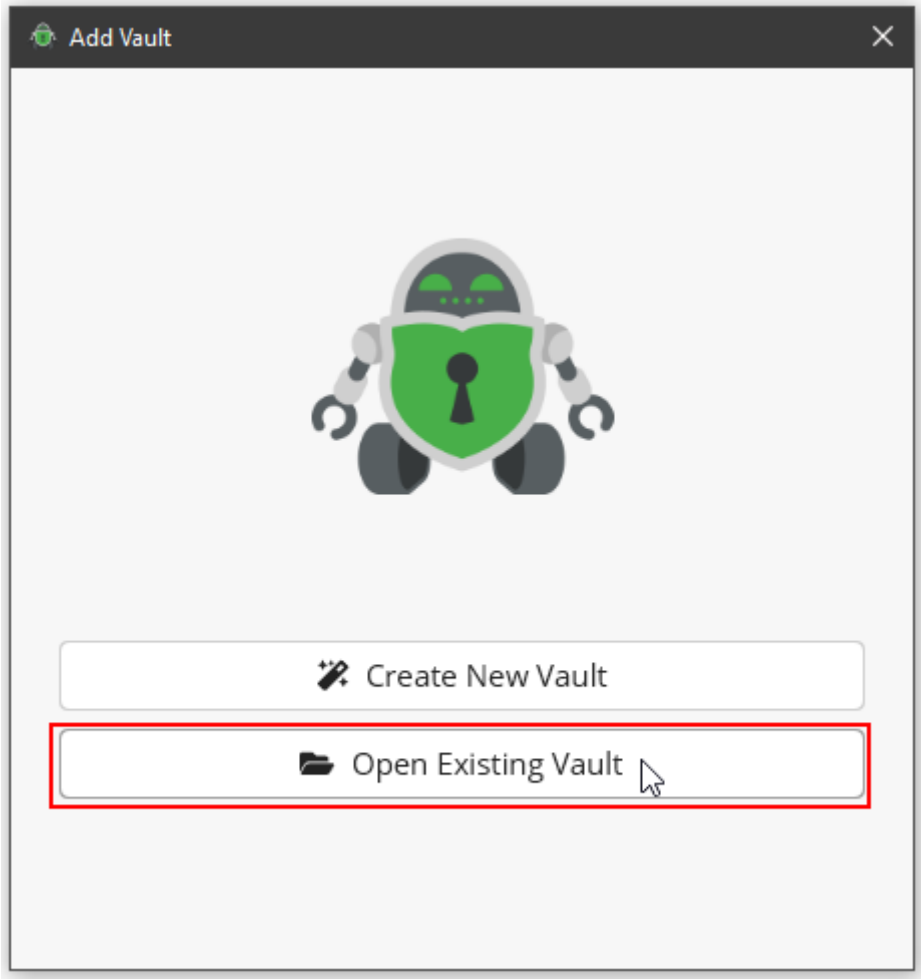
Lock the vault if you have finished editing the files.



Open existing vault

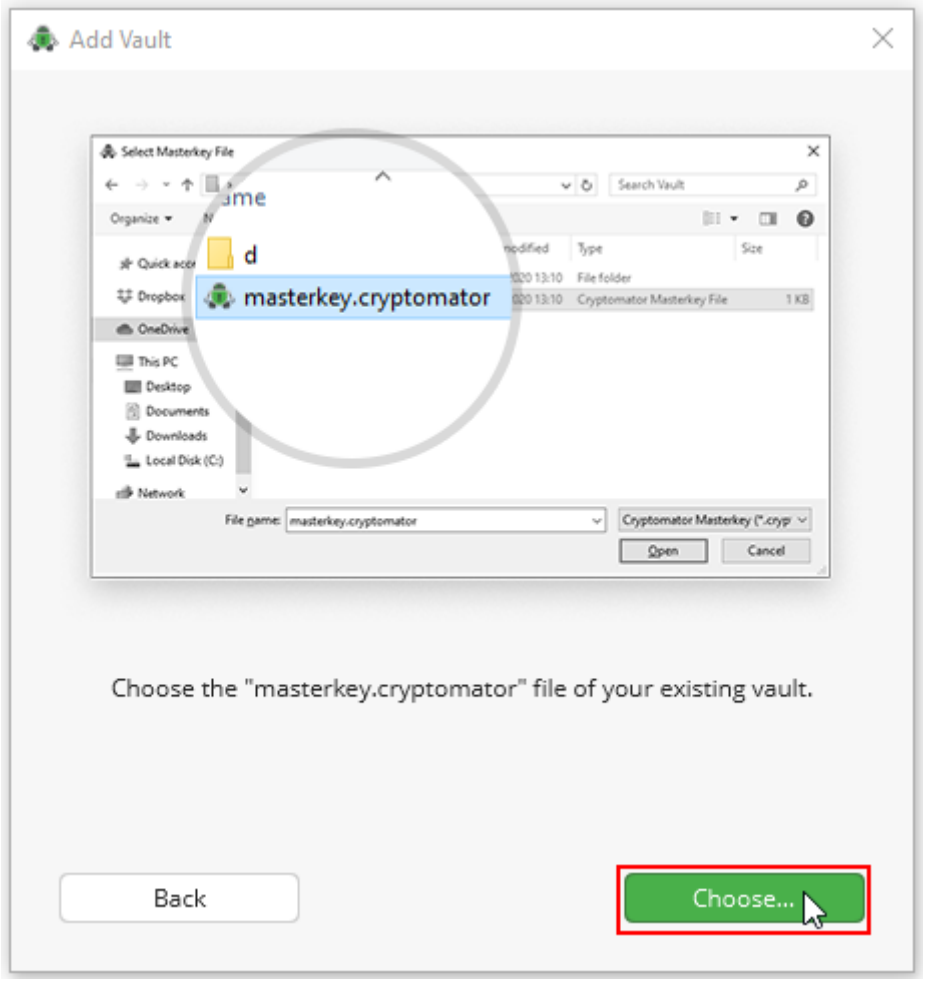
Step 1: Open existing vault

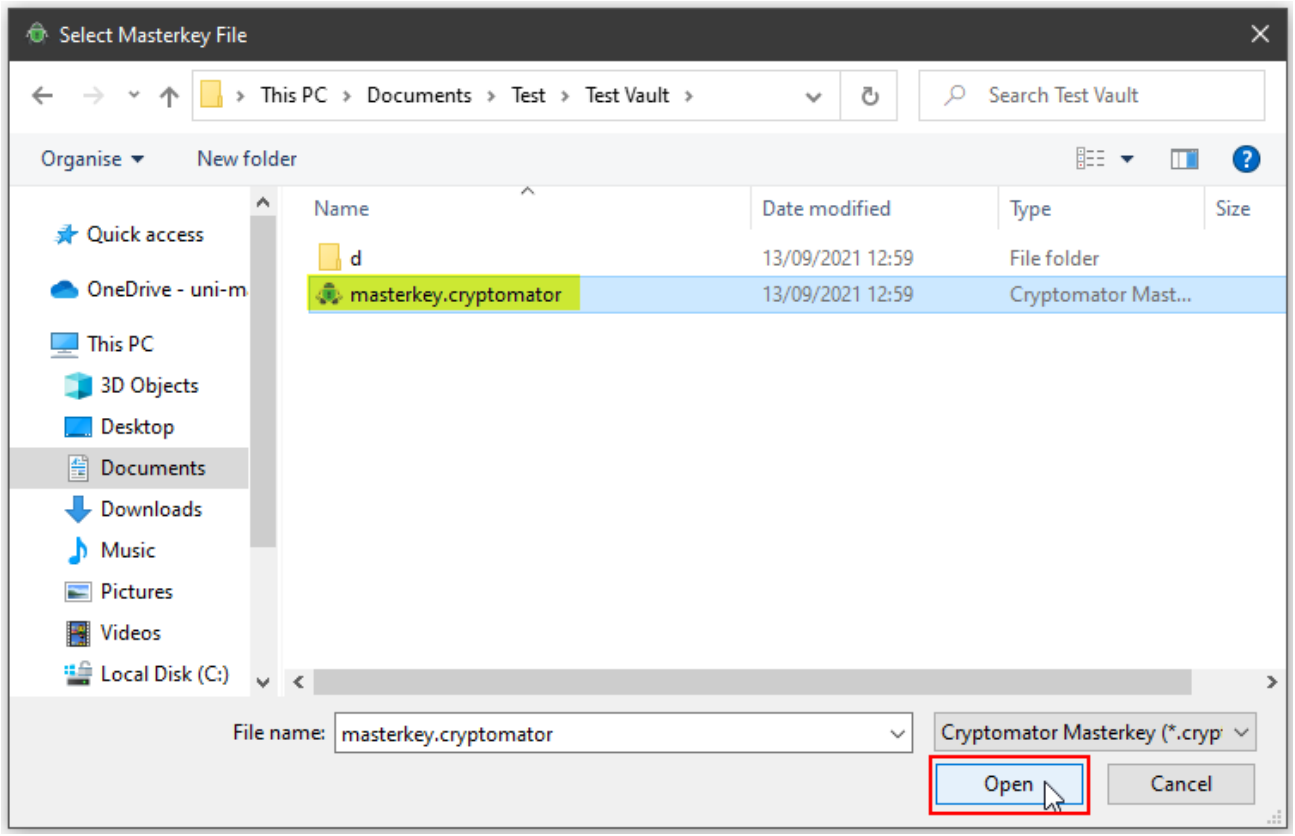
In order to add an existing vault, click “Open Existing Vault”.



Step 2: Select the file “masterkey.cryptomator”

Open the desired vault and select the file “masterkey.cryptomator”.

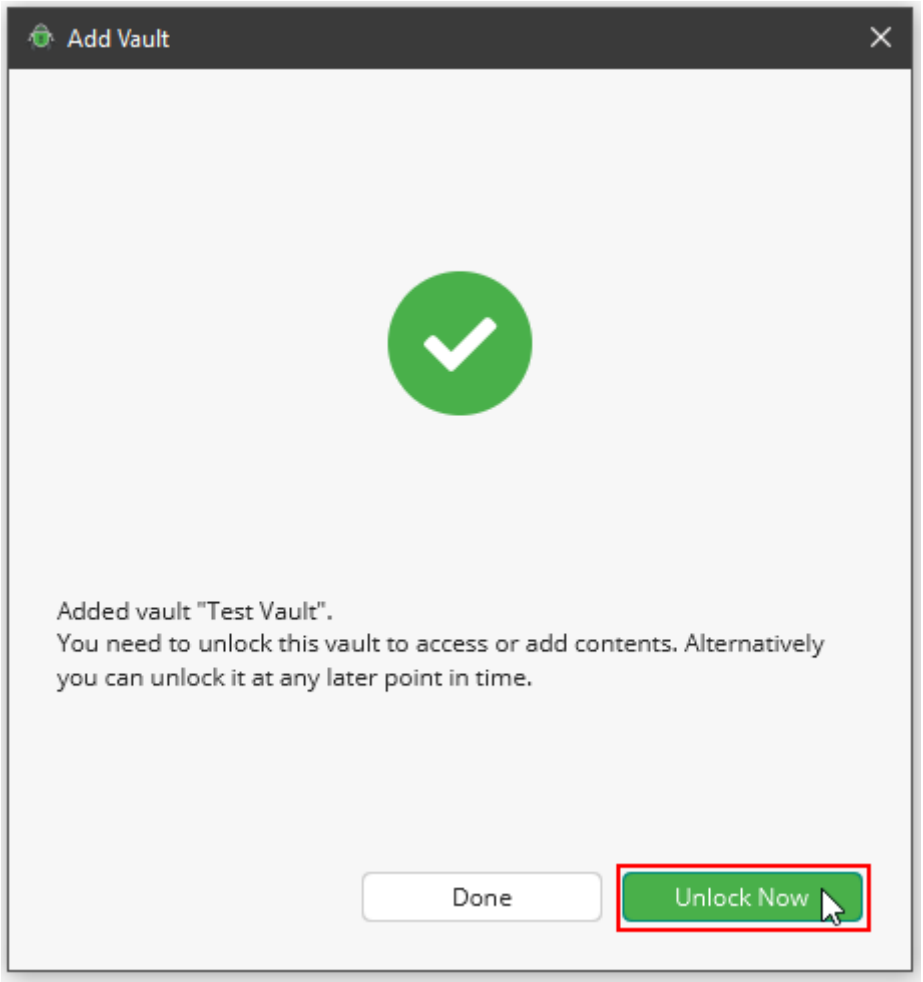




Step 3: Unlocking an existing vault

If you enter your password, you can unlock the vault and see the content.

Then you can open, edit or delete the files in the folder or add new files to the folder.

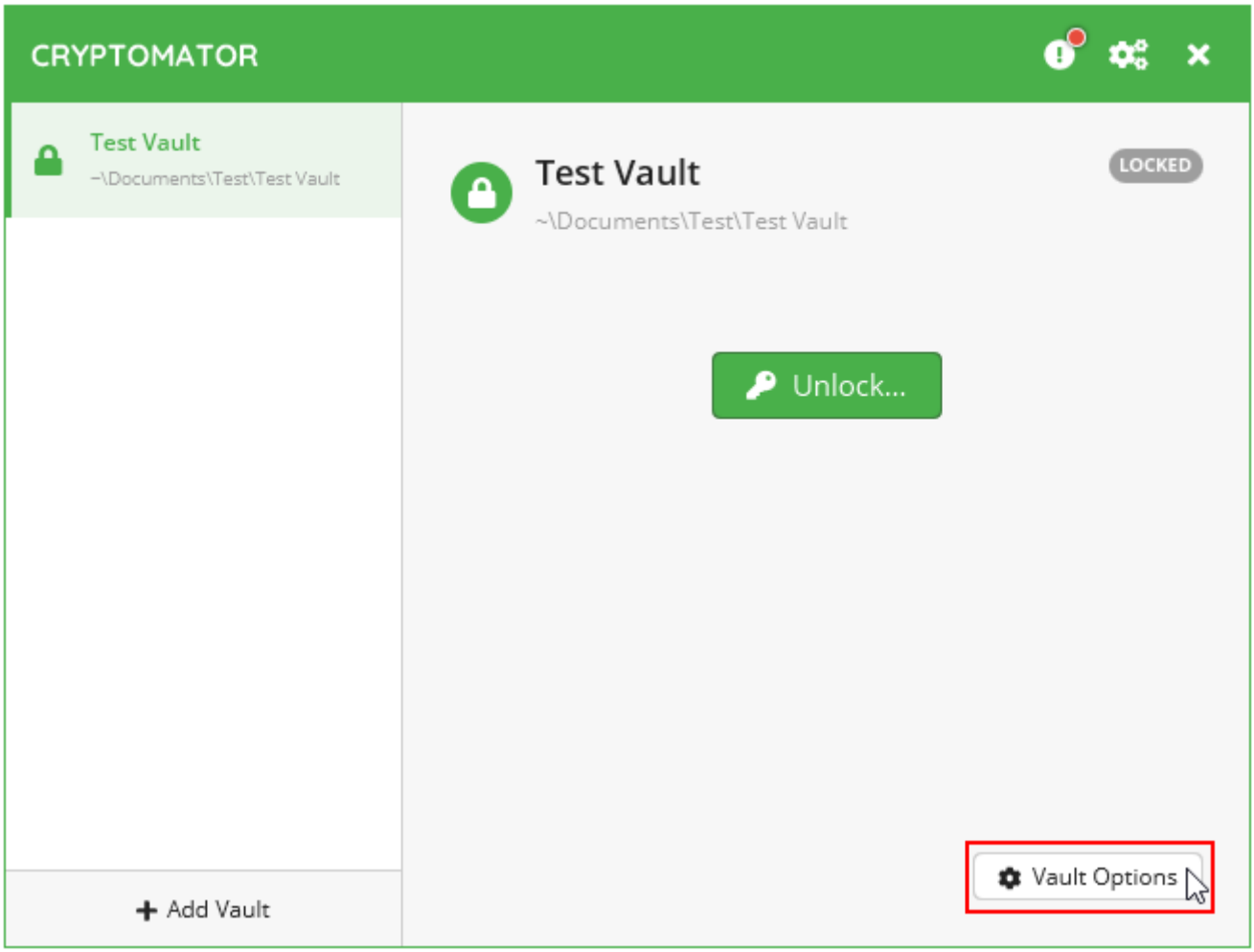


Reset your password

Step 1: Vault options

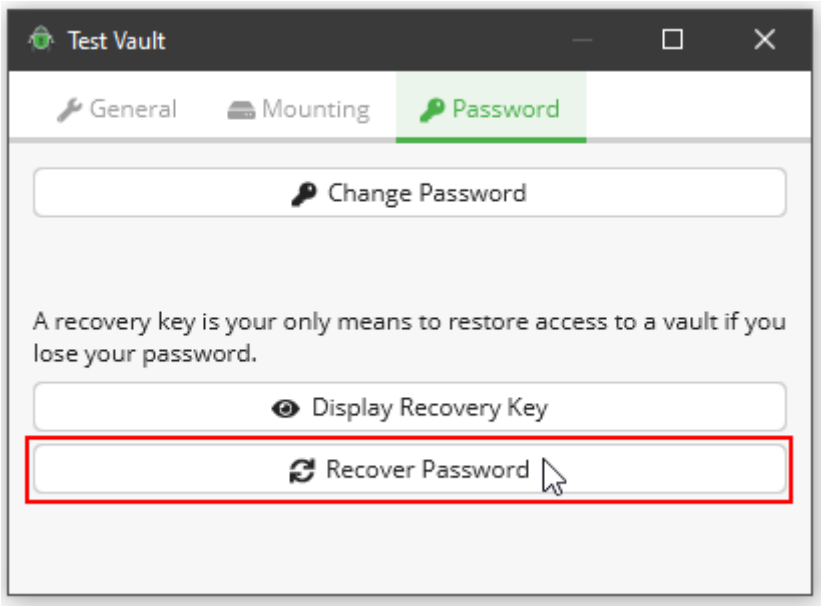
If you have forgotten your password, you need the recovery key to reset your password.

Select “Vault options” in the relevant folder.



Step 2: Recoveryour password

In the “Password” tab, you have the option to recover your password.


Test Vault
General
Mounting
Password
Change Password
A recovery key is your only means to restore access to a vault if you lose your password.
Display Recovery Key
Recover Password