Cryptomator Documentation

Release 1.7.0

Cryptobot

Sep 29, 2023

DESKTOP

Cryptomator encrypts your data quickly and easily, so you can safely upload it to your favourite cloud service.

If you're a first time user, you will probably want to follow *this guide on how to get started*.

If you are interested in the security of Cryptomator, have a look at our *security section*.

CHAPTER

ONE

SETUP

The Desktop version of Cryptomator is currently available for Windows, macOS, and Linux. Download and installation process varies depending on your operating system. Follow the instructions for your operating system. Ensure that your computer's specifications meet the system requirements required to run Cryptomator smoothly.

Note: We maintain archives of all Cryptomator versions along with detailed changelogs on our GitHub releases page.

1.1 Install Cryptomator on Windows

1. Download Cryptomator's `.exe` installer for Windows from our downloads page.
2. Launch the `.exe` installer.
3. Follow the on-screen instructions.

1.2 Install Cryptomator on macOS

1. Download Cryptomator's `.dmg` installer for macOS from our downloads page.
2. Launch the `.dmg` installer.
3. Accept the license.
4. Drag & drop Cryptomator into the Applications folder.

On macOS, Cryptomator will use WebDAV volume type by default if no FUSE driver is installed on the system. But we recommend installing *macFUSE* or *FUSE-T* for a smoother file browsing experience. Install *macFUSE* if your Mac comes with an Intel CPU or install *FUSE-T* if your Mac comes with an Apple Silicon CPU.

Note: Change your Gatekeeper settings if macOS blocks Cryptomator's installation.

1.3 Install Cryptomator on Linux

Cryptomator is available on Linux via `Flatpak`, `PPA` and `AUR` package managers, and as an AppImage (an `.appimage` file).

The easiest and recommended way of installing Cryptomator on Linux is by downloading Cryptomator's AppImage (an `.appimage` file) - as it works on almost all distrubtions. Just remember to make it executable before you try to run it.

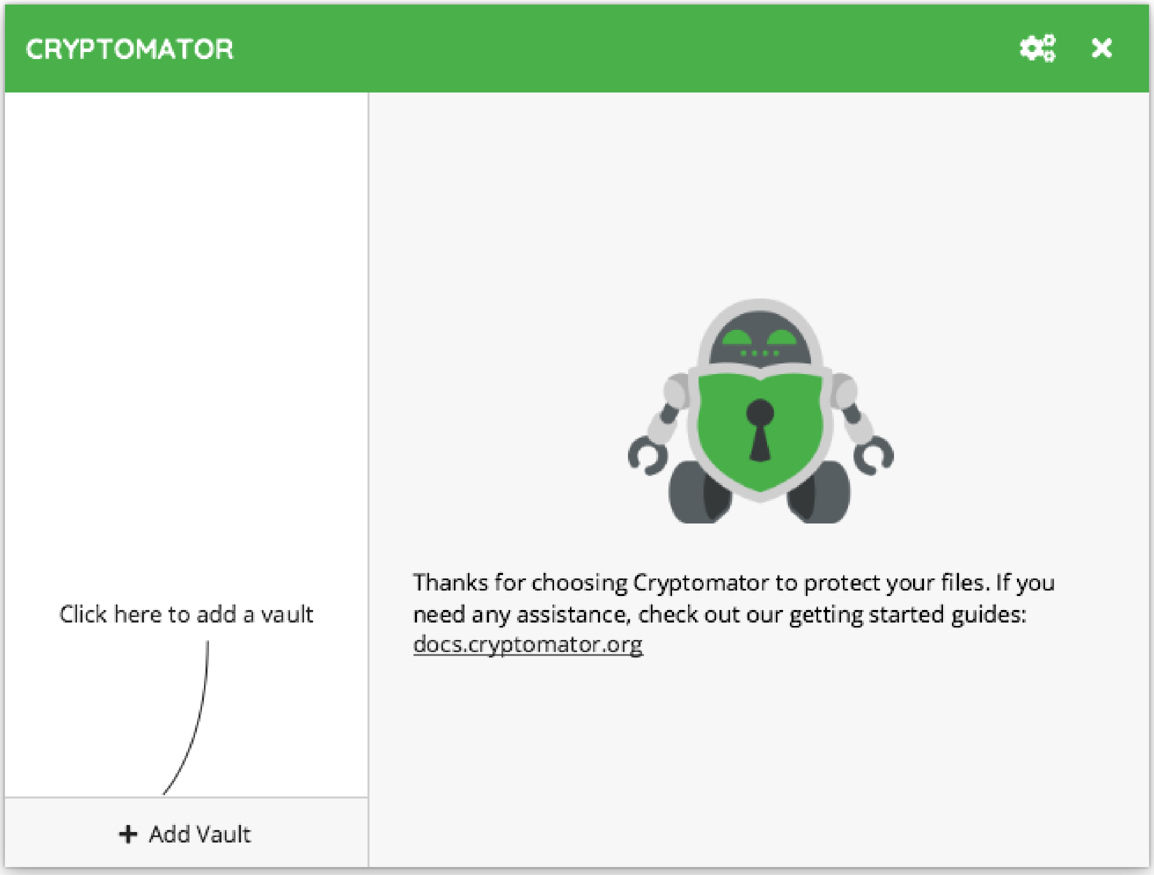
Visit our downloads page to choose your preferred installation method.

CHAPTER

TWO

GETTING STARTED

You will be greeted with the following screen when you start Cryptomator for the first time. You can create new vaults (or add existing ones) using the AddVault button located at the lower left corner.



Thanks for choosing Cryptomator to protect your files. If you need any assistance, check out our getting started guides: docs.cryptomator.org

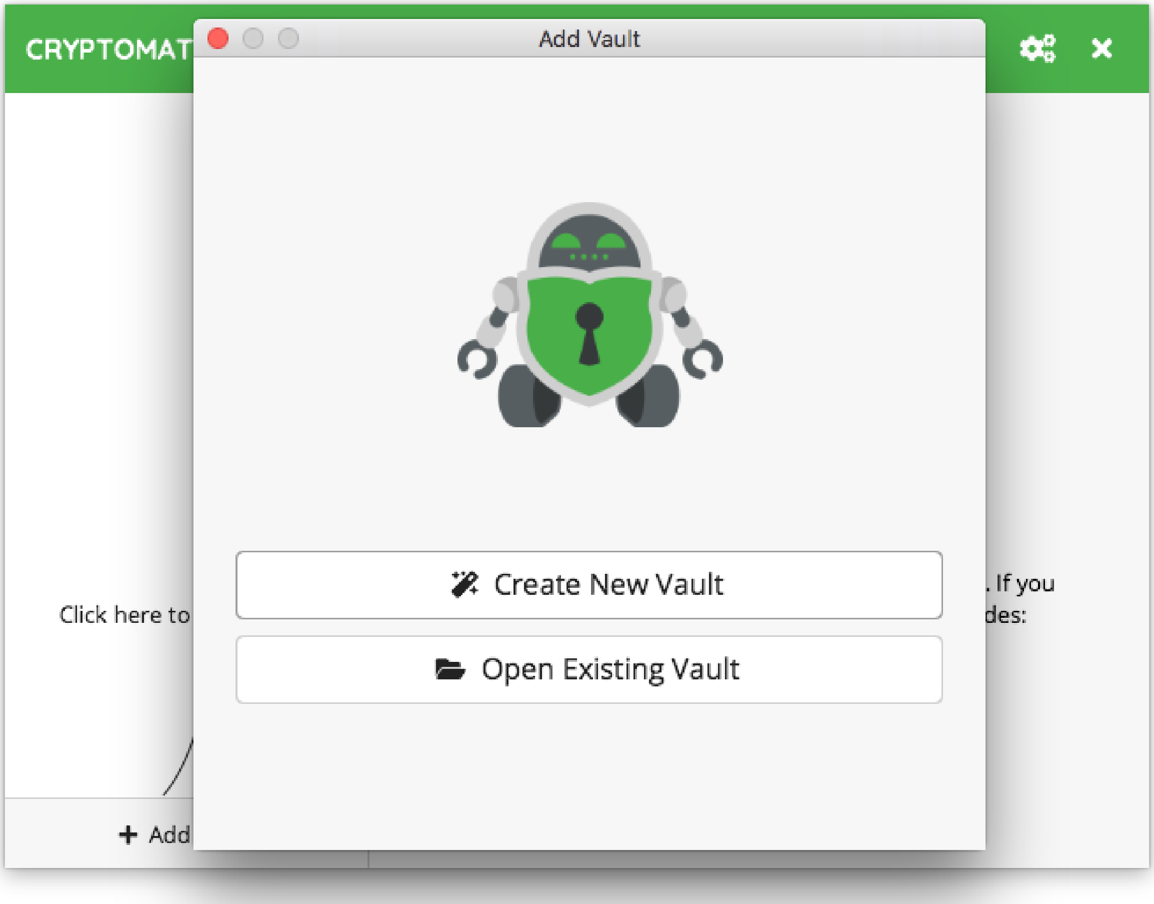
CHAPTER

THREE

ADDING VAULTS

You will be presented with two options when adding a vault:

1. `Create New Vault` - Choose this if you wish to create a new vault.
2. `Open Existing Vault` - Choose this if you already have a vault and wish to open it.

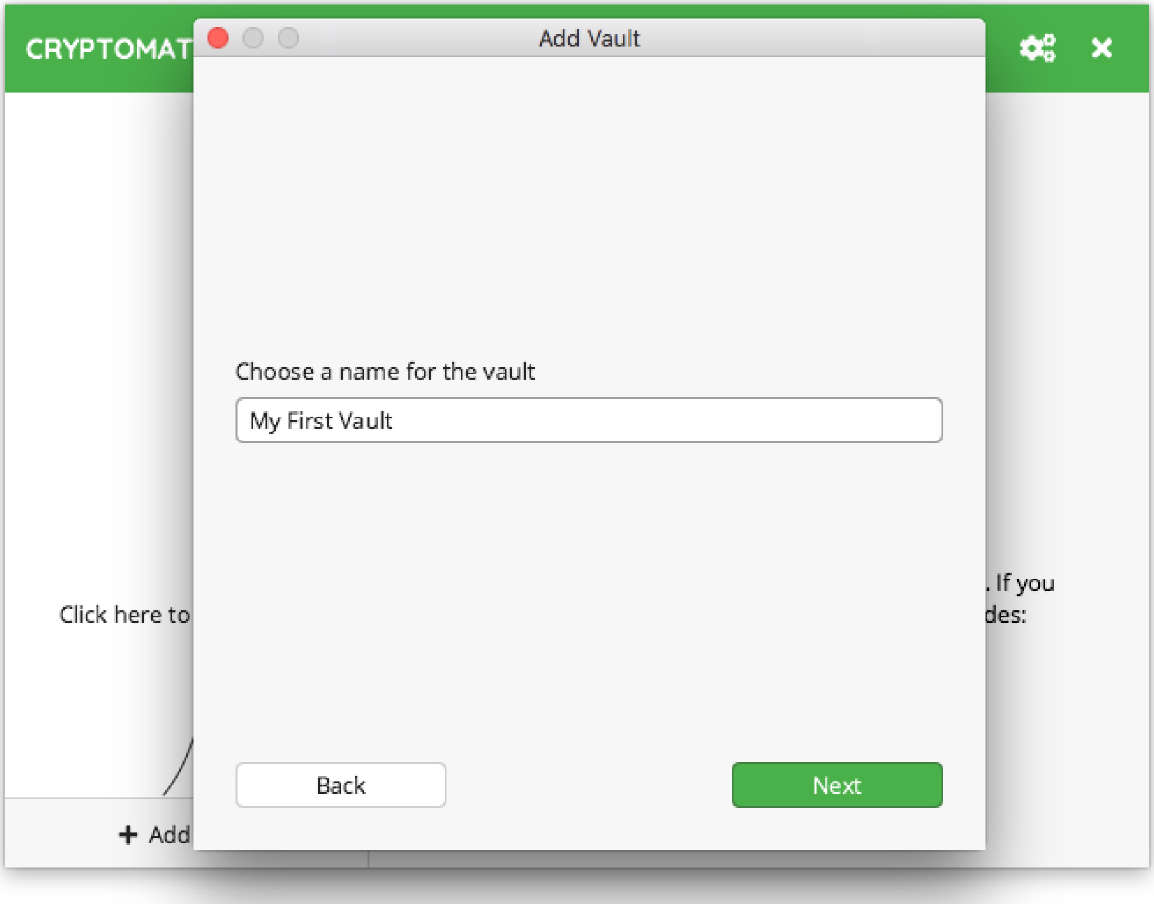


3.1 Create a New Vault

If you chose to create a new vault, the wizard will guide you through a simple 5-step vault creation process.

3.1.1 1. Choose a Name

Start by choosing a name for your vault.



Choose a name for the vault

My First Vault

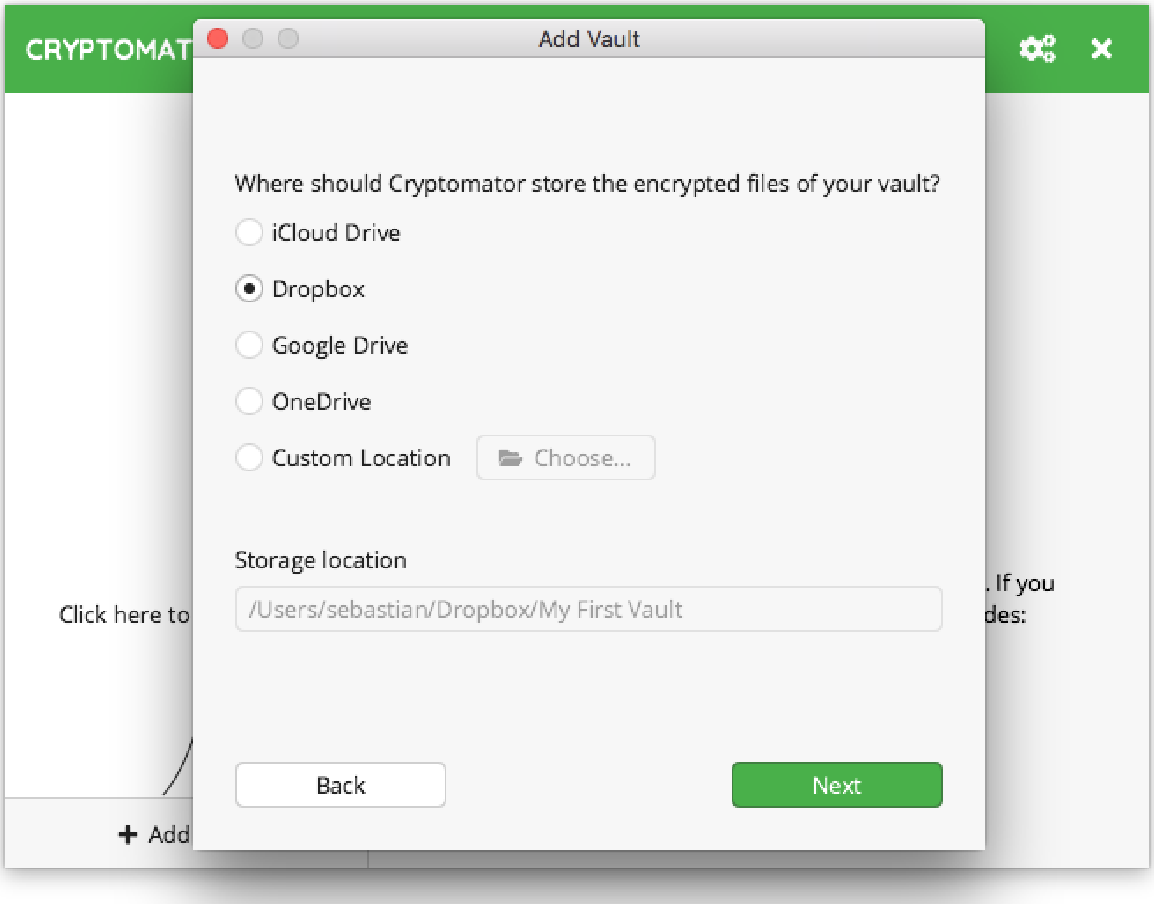
3.1.2 2. Choose a Storage Location

Next, you need to choose a directory on your PC where your vault's encrypted data will be stored. If you wish to sync the encrypted data to your cloud storage, then choose a cloud-synced directory.

Cryptomator is not a sync tool. You need to install the sync software of your cloud storage provider to sync your encrypted data.

Note: Cryptomator tries to detect locations of well-known cloud sync software (see screenshot below).

The screenshot below shows multiple cloud storage locations, because we have multiple sync software installed on our device. You might not see the same options, depending on which cloud services are installed on your PC, but you can always choose `Custom Location` and navigate to your cloud-synced directory manually.



Where should Cryptomator store the encrypted files of your vault?

○ iCloud Drive

● Dropbox

○ Google Drive

○ OneDrive

○ Custom Location   Choose...

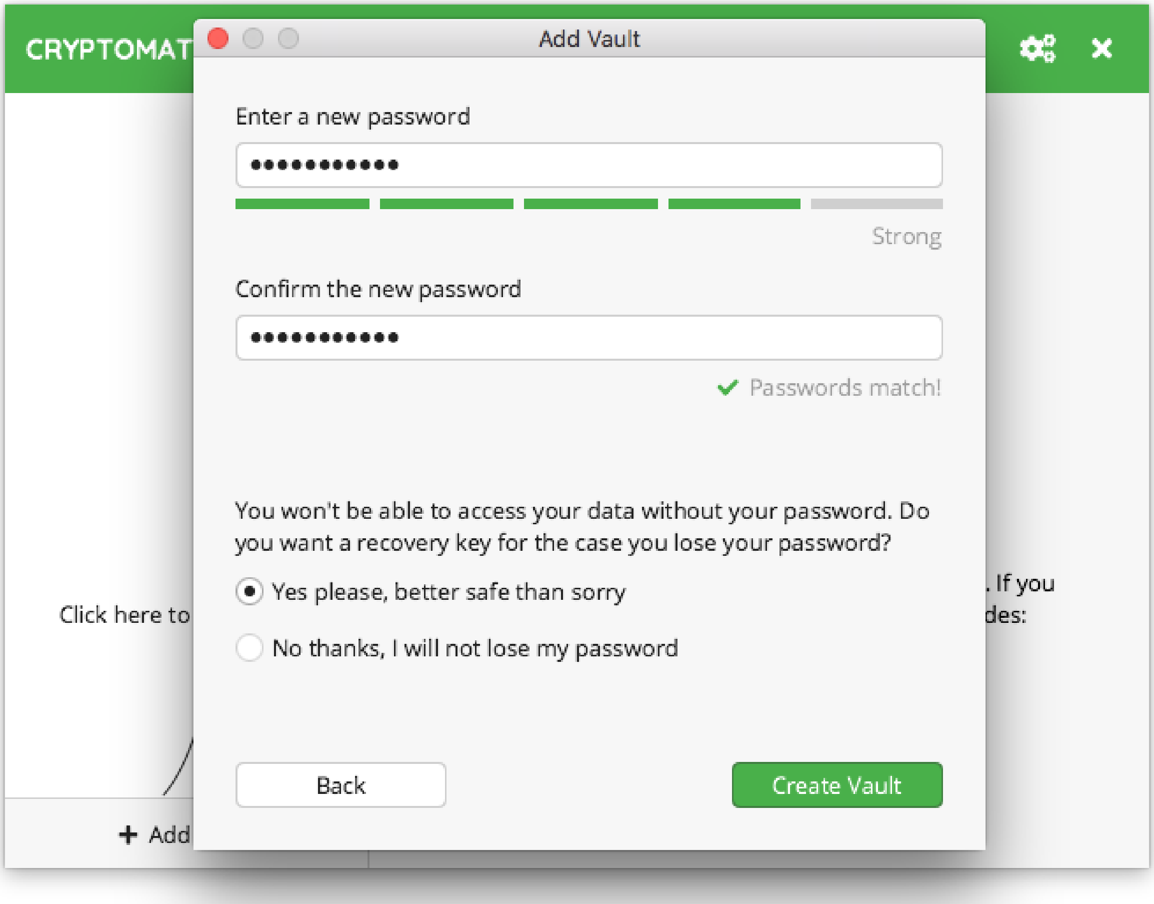
Storage location

/Users/sebastian/Dropbox/My First Vault

3.1.3 3. Choose a Password

Now it is time to choose a *strong password* for your vault. Cryptomator requires at least 8 characters, but we recommend you to use longer phrases such as pass-sentences. The bar below the password field will help you estimate the strength of your password.

Note: Always choose a password that's unique across your vaults and accounts. This is espically important if you plan to share a vault with someone. Additionally, we recommend sharing passwords only over a secure channel, like PGP encypted emails, or end-to-end encrypted chat apps.



Add Vault

Enter a new password

●●●●●●●●●●●

Strong

Confirm the new password

●●●●●●●●●●●

✓ Passwords match!

You won't be able to access your data without your password. Do you want a recovery key for the case you lose your password?

● Yes please, better safe than sorry

○ No thanks, I will not lose my password

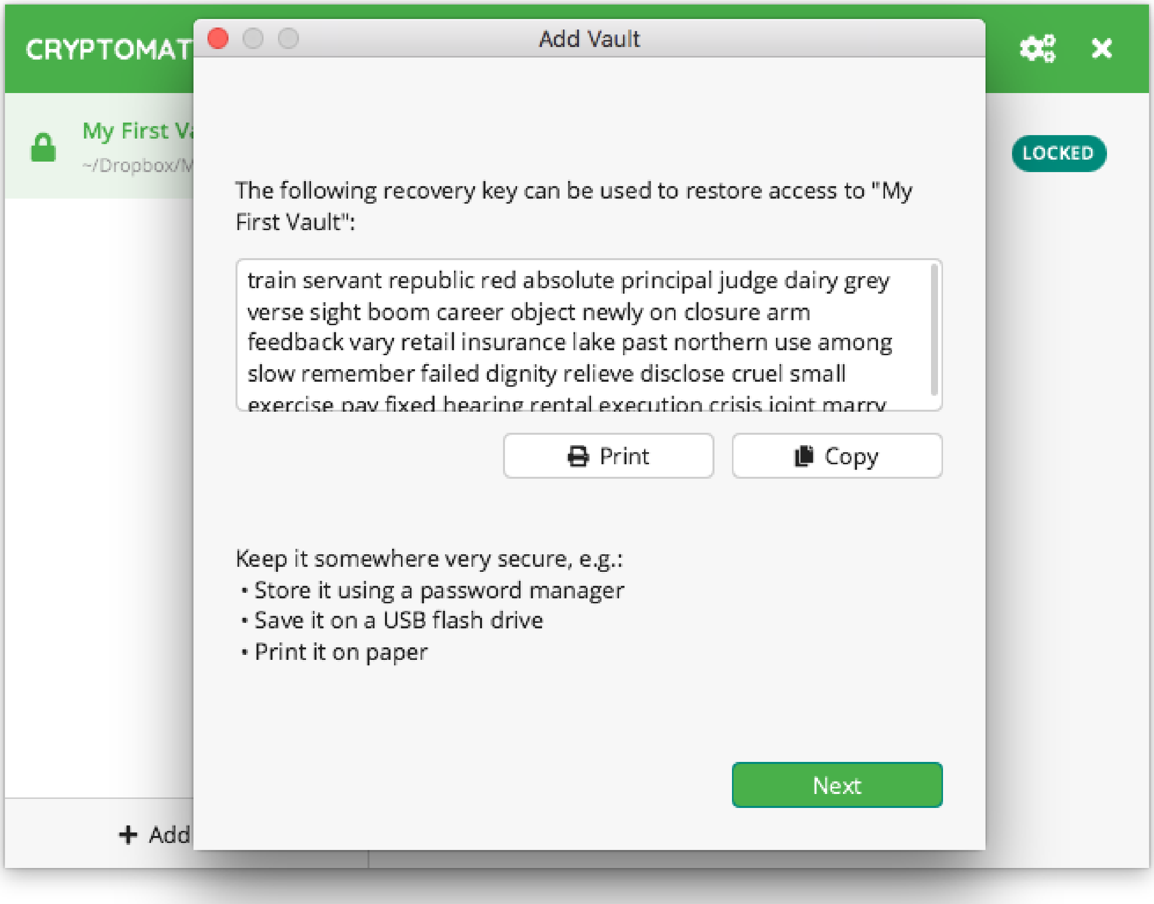
Warning: Nobody except you knows this password, and we also cannot "reset" it for you. Without a vaild password, your files can't be decrypted and will become inaccessible. So, store your password in a secure password manager or just don't forget it.

However, you can reset a vault's password by yourself if you have its *recovery key*.

3.1.4 4. Show Recovery Key (optional step)

A recovery key allows you to reset your password if you ever forget it.

If you chose to create a recovery key in the previous step, it will now be displayed. Make sure not to lose it and ideally make a hard copy of it.



The following recovery key can be used to restore access to "My First Vault":

train servant republic red absolute principal judge dairy grey verse sight boom career object newly on closure arm feedback vary retail insurance lake past northern use among slow remember failed dignity relieve disclose cruel small exercise pay fixed hearing rental execution crisis joint marry

Keep it somewhere very secure, e.g.:
- Store it using a password manager
- Save it on a USB flash drive
- Print it on paper

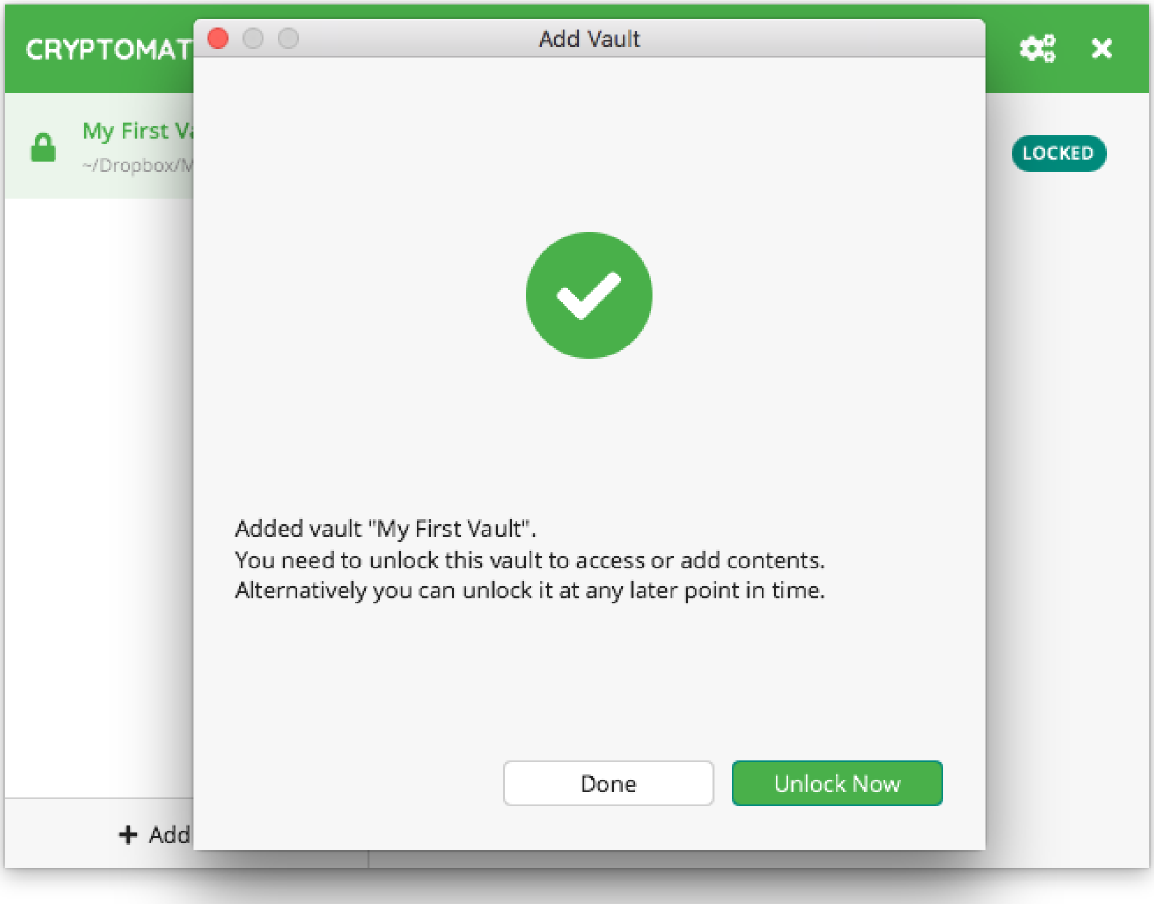
Warning: Remember, a recovery key is just like your password, its purpose is to gain access to your vault! Keep it as safe as your password.

For more details, take a look at *how a recovery key works*.

3.1.5 5. Done

That's it. You have successfully created a new vault.

You can now unlock this vault using your password and start adding files into it.



Added vault "My First Vault".
You need to unlock this vault to access or add contents.
Alternatively you can unlock it at any later point in time.

3.2 Open an Existing Vault

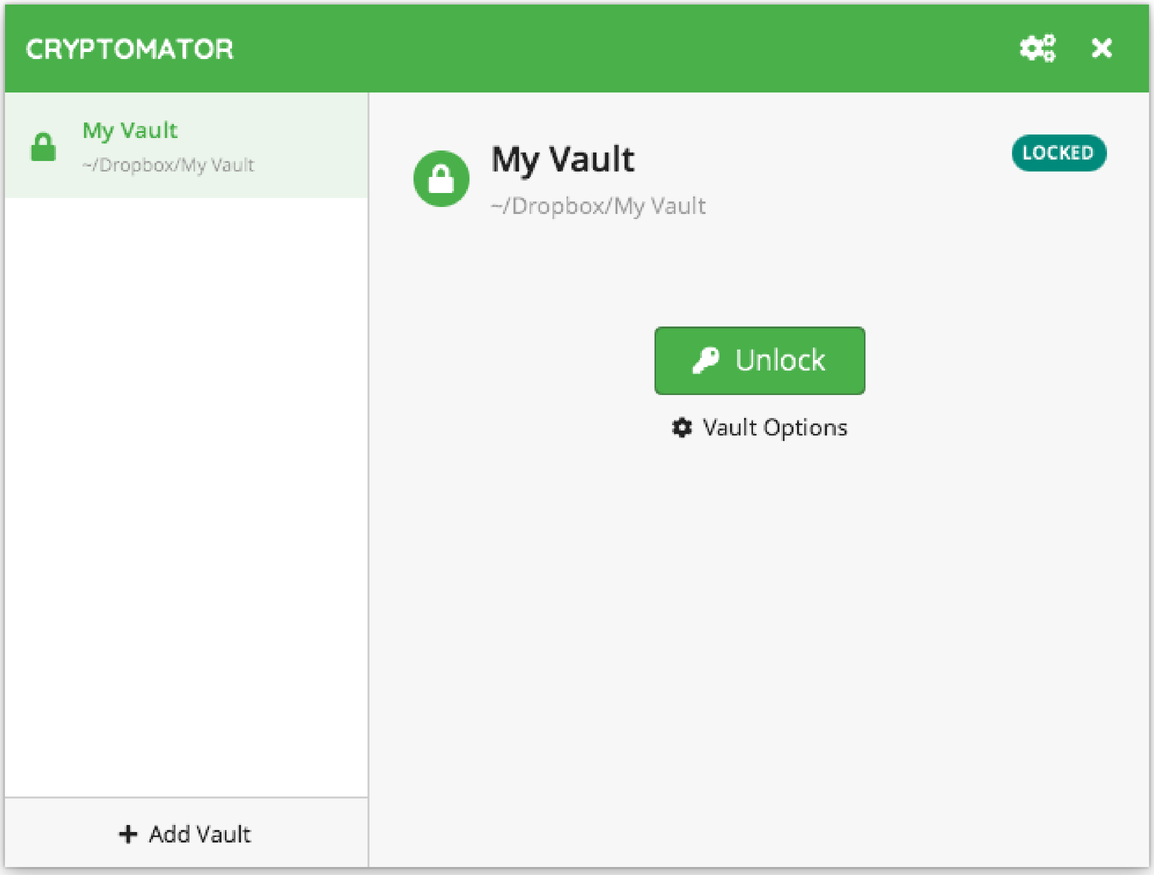
To open an existing vault, you need to locate the `masterkey.cryptomator` file of the vault you wish to open.

Note: If you created the vault on another device and cannot find it or its masterkey file, make sure that the directory containing the vault is properly synchronized and fully accessible on your device.

CHAPTER FOUR

ACCESSING VAULTS

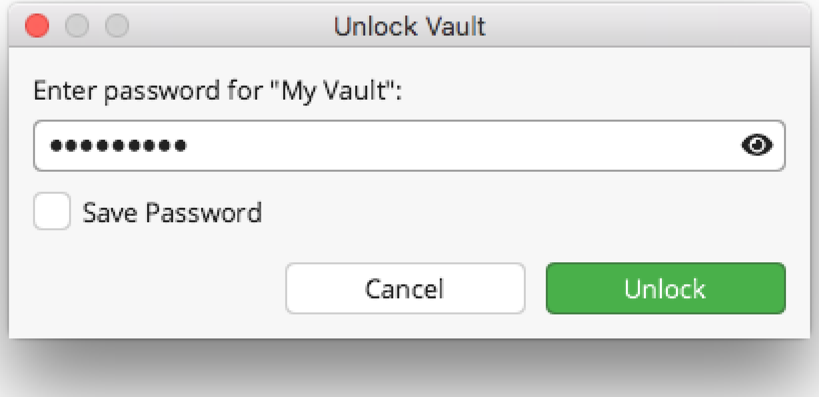
You can only access decrypted files of a vault if you can unlock it. Unlocking a vault is just a two-step process as long as you know the password.



4.1 Unlocking a Vault

1. Select the vault you wish to unlock.
2. Click on the large `Unlock` button located at the center of the Cryptomator window.
3. Enter your vault's password.

A confirmation will be displayed if your password is correct. You can either close the confirmation window by clicking `Done` or click on `Reveal Vault` to show your unlocked vault in your file manager.



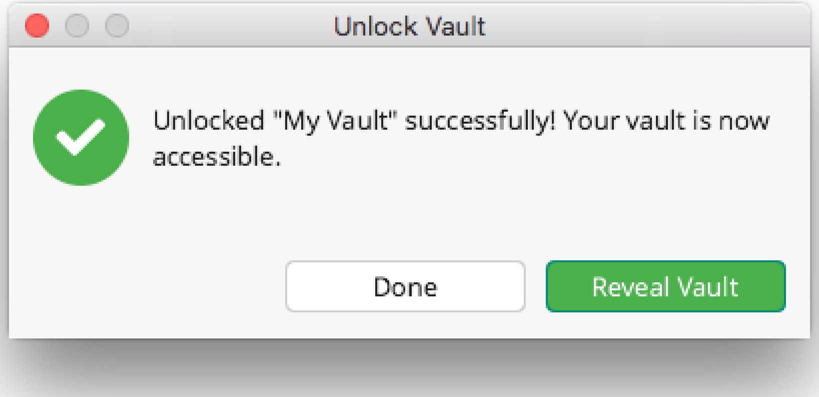
Enter password for "My Vault":

●●●●●●●●●●

□ Save Password

Note: You can store the password in your operating system's keychain by checking the "Save Password" checkbox. There is also a plug-in for Cryptomator, that allows you to store Cryptomator's vault passwords in a KeePassXC database. With a saved password, you can unlock your vaults without typing a password on every unlock. It's faster.

Warning: Only store your password in the system's keychain on trusted devices. Anyone with access to the computer with stored passwords will be able to unlock your vault, and in some cases, even find your password.



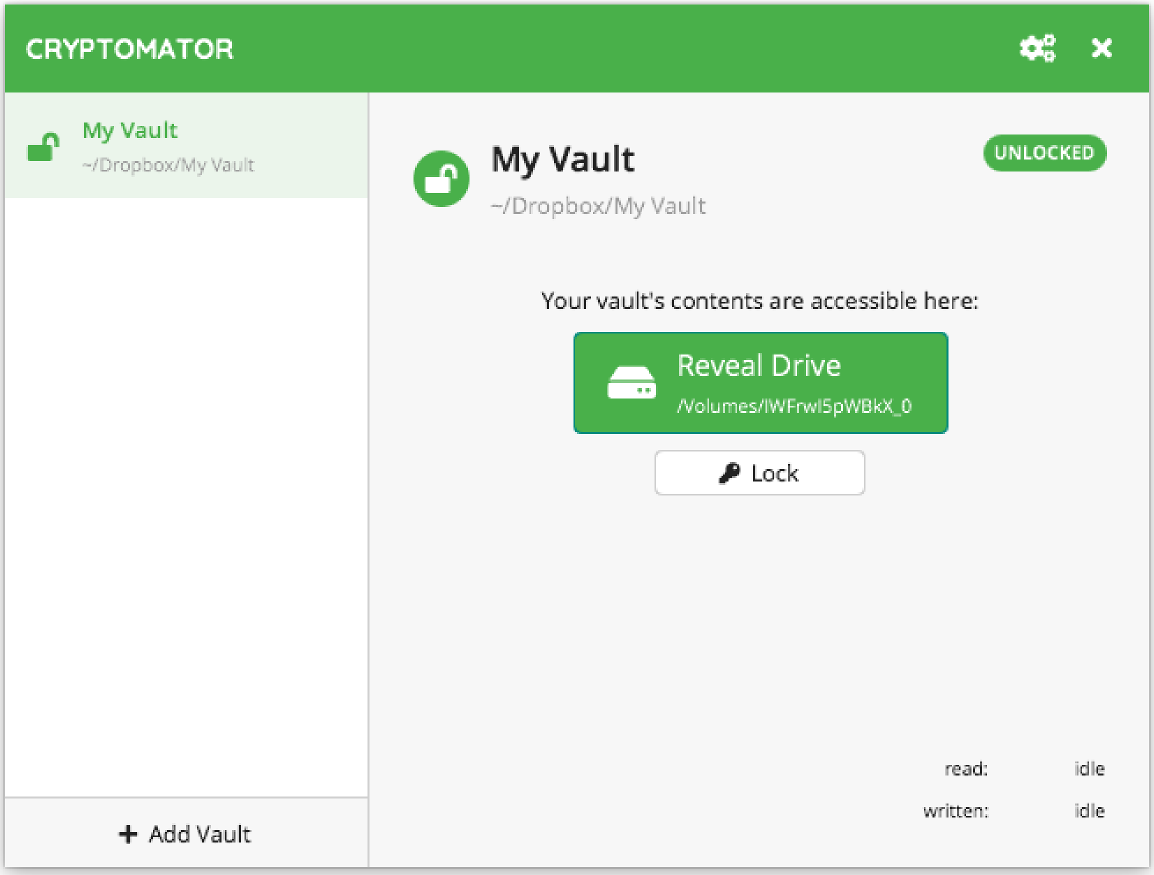
Unlocked "My Vault" successfully! Your vault is now accessible.

4.2 Manage Files and Folders in your Vault

By default, a vault's content will be accessible via an attached virtual drive on your PC. So, you can manage files and folders in your unlocked vault just like you do on any other hard drive or USB drive.

Alternatively, a vault's content can be accessed via a directory or a WebDAV server by changing its *volume type*. Click on `Reveal Drive` in the Cryptomator window to open the mount location using the default file manager (Windows Explorer, Finder, . . .).

Note: Even though your files are shown unencrypted in the virtual drive, they are not stored unencrypted on the hard drive but only in volatile memory



Your vault's contents are accessible here:

/Volumes/IWFrwl5pWBkX_0

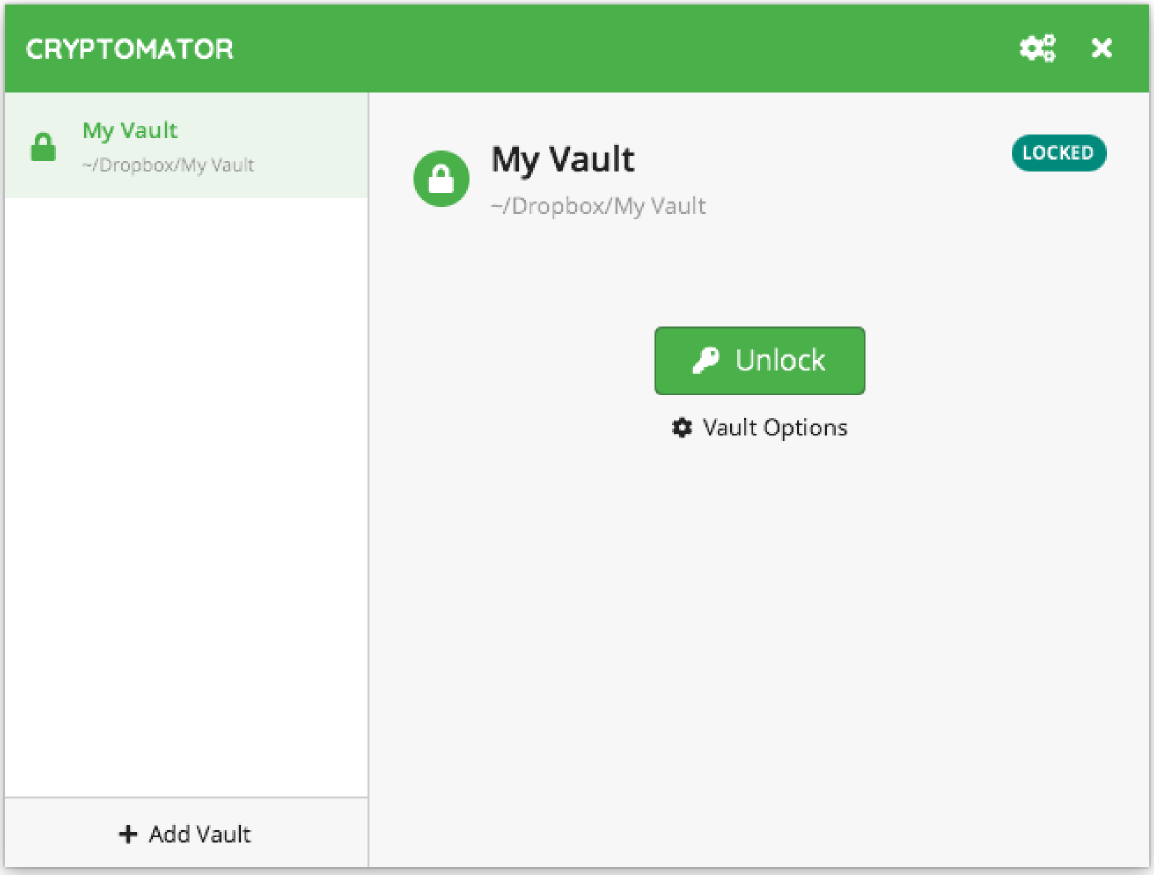
read: idle

written: idle

Note: On Windows, you can choose the drive letter of the virtual drive for each vault using advanced vault options.

4.3 Locking a vault

To lock a vault, simply click `Lock` and the virtual drive will disappear or render empty. Your files remain encrypted at the vault's location.


CRYPTOMATOR
My Vault
~/Dropbox/My Vault
+ Add Vault
My Vault
~/Dropbox/My Vault
LOCKED
Unlock
Vault Options

CHAPTER

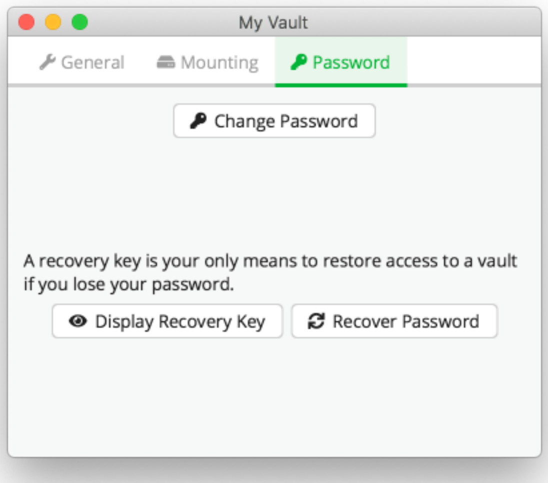
FIVE

PASSWORD AND RECOVERY KEY

This section explains how to change a password for a vault, show its recovery key, and reset a password. But, before that, let's understand how Cryptomator encrypts a vault using a password and what a recovery key is. The security of your vault is only as good as its password because Cryptomator encrypts your vault using a key derived from your password. So, *choosing a strong password* is very important.

Additionally, a unique *recovery key* can be derived for each vault while creating its password or later. A *recovery key* allows you to create a new password if you forget the original one. Do note that the *recovery key* feature does not break encryption in any way. It is a human readable form of your decrypted *masterkey* and therefore independent of the current vault password and highly confidential. Keep it as safe as your password.

All actions can be carried out using the `Password` tab under vault options. You can access it by selecting a vault, lock it if necessary, and click on `Vault Options`.



A recovery key is your only means to restore access to a vault if you lose your password.

5.1 Change Password

To change the password of an existing vault, you need to know its current one or have a recovery key (see reset password section).

Navigate to the `Vault Options` -> `Password` tab, and click on `Change Password`.

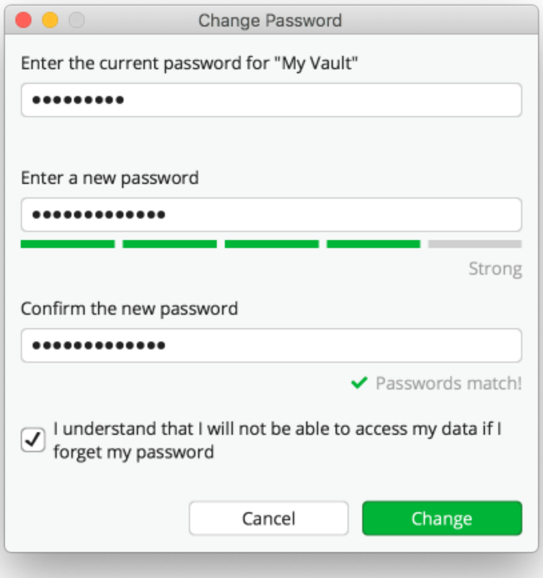
In the opened window, you will be asked for:

1. The vault's current password.
2. A new password. We suggest following our guide on choosing a *strong password*.
3. Enter the new password again.

In order to proceed, you must confirm that you understand your action by selecting a checkbox.

Finally, click on the `Change` button to change the password.

Note: The `Change` button is activated only if the new password fields match and the checkbox is selected.



Change Password

Enter the current password for "My Vault"

•••••••••

Enter a new password

•••••••••••••

Strong

Confirm the new password

•••••••••••••

✓ Passwords match!

☑ I understand that I will not be able to access my data if I forget my password

Note: The password is used to derive a KEK, which is then used to encrypt further keys. The KEK changes, but the keys encrypted with the KEK will stay the same. The actual files will not get re-encrypted, meaning you can not upgrade a weak passphrase to a stronger one once the data has been synced to a service that allows recovery of older versions of the masterkey file.

If you like to encrypt your vault files with a new, stronger password, you need to create a new vault and drag the data from the old to the new one. Make sure to wipe all backups of the old vault afterwards.

5.2 Show Recovery Key

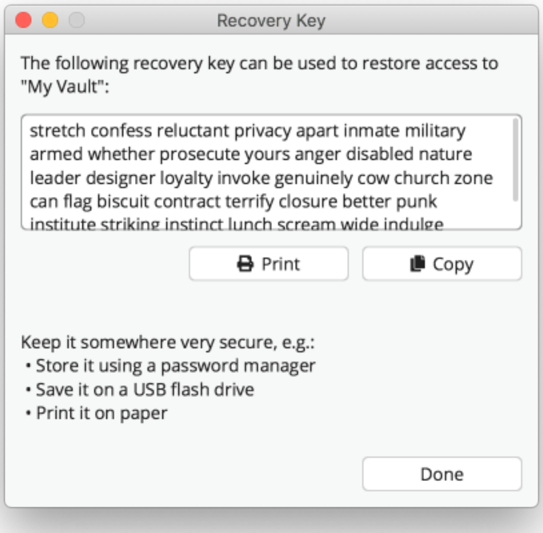
You can derive a recovery key during vault creation or even later as long as you know your vault's password. To increase security, Cryptomator does not store the recovery key on your hard drive and always derives it on the fly.

Warning: A recovery key can reset a vault's current password. So, treat it like a password and ensure only trusted people have access to it.

To derive a recovery key:

1. Navigate to the `Password` tab under `Vault Options`.
2. Click on `Display Recovery Key`.
3. Enter the vault's password.

A new window will open displaying a sequence of words (i.e., the recovery key).



The following recovery key can be used to restore access to "My Vault":

stretch confess reluctant privacy apart inmate military armed whether prosecute yours anger disabled nature leader designer loyalty invoke genuinely cow church zone can flag biscuit contract terrify closure better punk institute striking instinct lunch scream wide indulge

Keep it somewhere very secure, e.g.:
• Store it using a password manager
• Save it on a USB flash drive
• Print it on paper

You can copy it to your clipboard and store it in a secure password manager, or print it on paper.

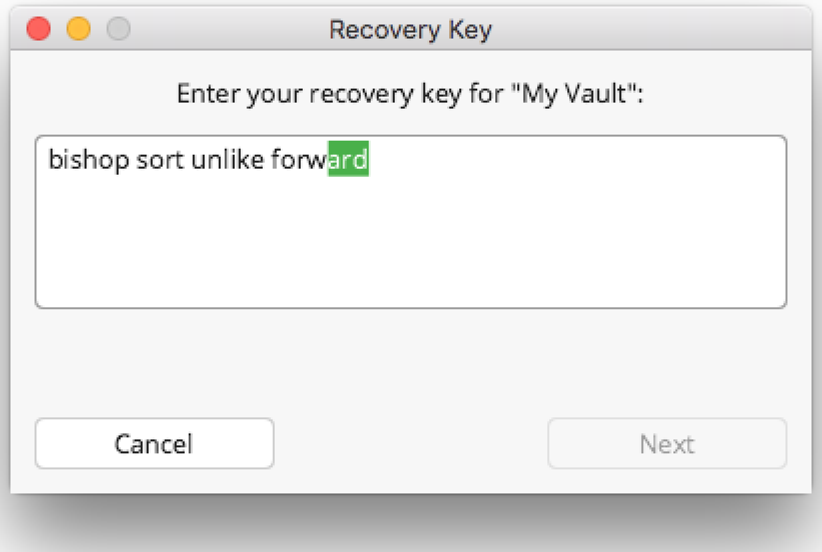
5.3 Reset Password

We cannot reset the password of a vault for you in any way. Only you can reset a vault's password, assuming you have its recovery key. Keep it ready before you proceed.

1. Navigate to the `Password` tab under `Vault Options`.
2. Click on `Recover Password`.

Type or paste your recovery key in the new window.

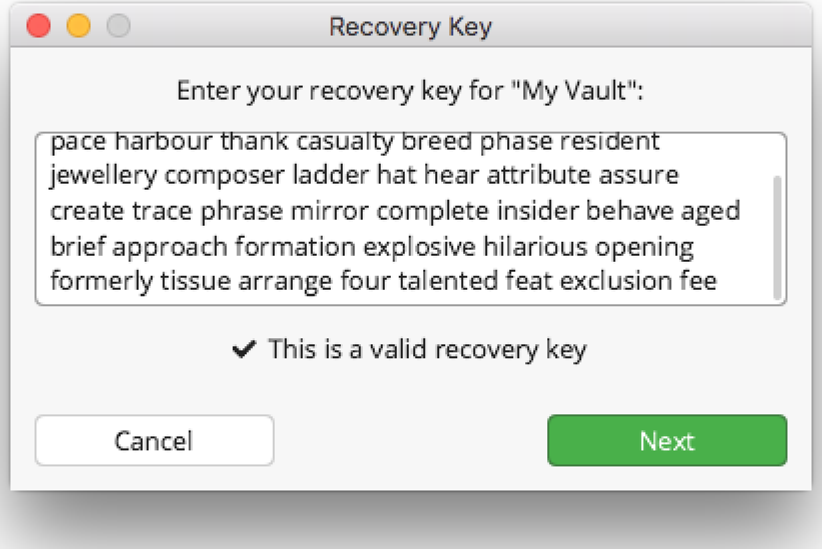
Note: Cryptomator offers an auto completion feature to make things easier when typing a recovery key. It's helpful if your recovery key is printed on paper or stored it somewhere where you cannot copy it. The feature will kick in automatically once you start typing the first few letters of a word.


Recovery Key

Enter your recovery key for "My Vault":

bishop sort unlike forward

If the recovery key is valid, a small message will be displayed below the entered recovery key and the `Next` button will be activated.


Recovery Key

Enter your recovery key for "My Vault":

pace harbour thank casualty breed phase resident
jewellery composer ladder hat hear attribute assure
create trace phrase mirror complete insider behave aged
brief approach formation explosive hilarious opening
formerly tissue arrange four talented feat exclusion fee

✓ This is a valid recovery key

Warning: By design, *only* the correct recovery key is accepted. **A valid but incorrect key won't be accepted to prevent your old data from becoming inaccessible.**

Finally, assign a new password to your vault. It is the same process as the *vault creation*, except that no new recovery key is generated. Again, please choose a *strong password*.

Once changed, you can unlock your vault with the new password.

Note: Don’t discard the recovery key after resetting the password as it will still remain valid.

CHAPTER

SIX

VAULT MANAGEMENT

A *vault* is where your files are stored encrypted. For your operating system or other apps, a vault is a just a normal directory containing some encrypted files. Only Cryptomator can decrypt the vault's contents when you unlock it using a password.

6.1 Remove Vaults

To remove a vault from the vault list, right click on a vault, and click remove. This is only possible if the vault is locked.

Note: The vault is **not** deleted from your PC by removing it from the list. If you wish to permanently delete your encrypted files, you need to delete the vault directory using the file manager.

6.2 Reorder Vaults

You can change the order of the vaults in the list by dragging them.

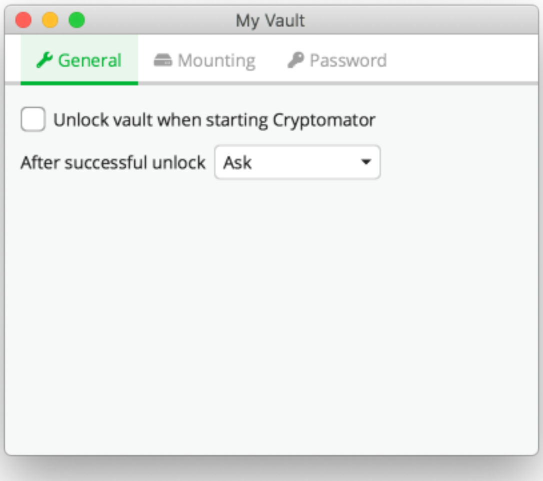
6.3 Vault Options

Each vault has its own settings which can be customized under vault options. To open a vault's settings, select a vault, lock it, and click on `Vault Options`.

The options are divided across three categories:

1. General - Options not fitting in other categories.

You can select this option if the vault is unlocked as soon as Cryptomator starts.

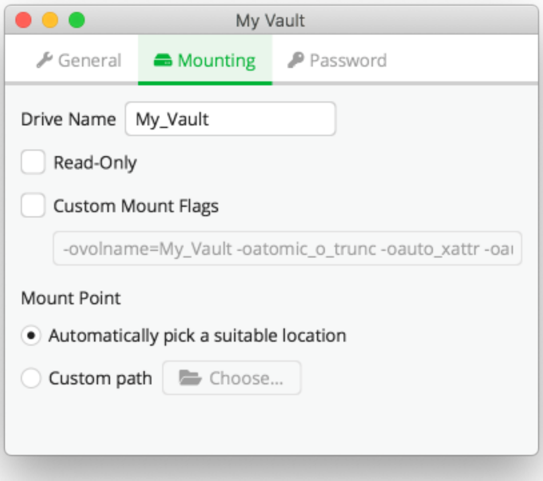


□ Unlock vault when starting Cryptomator

After successful unlock Ask

2. Mounting - Settings that manage how and where a vault is mounted.

Note: The mount options depend on the selected *volume type*



Drive Name My_Vault

□ Read-Only

□ Custom Mount Flags

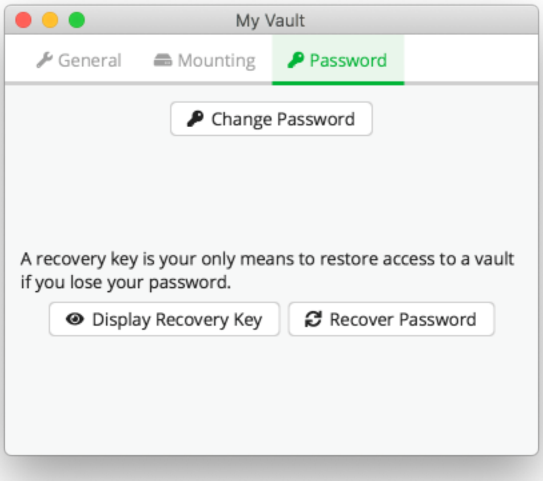
-ovolname=My_Vault -oatomic_o_trunc -oauto_xattr -oai

Mount Point

● Automatically pick a suitable location

○ Custom path

3. Password - Here you can manage the vault’s password and recovery key.



A recovery key is your only means to restore access to a vault if you lose your password.

Take a look at the `Mounting` and `Password` sections to understand how vault mounting and passwords work.

CHAPTER

SEVEN

VOLUME TYPES

Volume types play an important role when handling your files.

When you unlock a vault, Cryptomator makes decrypted files available in your file manager by mounting a virtual drive on your operating system. This mounting of a virtual drive is handled differently depending on the volume type chosen in Cryptomator's preferences.

In general, all volume types Cryptomator offers can be categorized into three categories:

1. *WebDAV*
2. *FUSE*
3. *Other*

7.1 What is a WebDAV volume type?

WebDAV is a standardized communication protocol used to perform operations on resources (files, directories/folders) between a client (you) and a server (your local computer). WebDAV was intended for remote access, but Cryptomator uses it to start a local-only server, which you can use to browse your decrypted files.

You can tweak WebDAV's settings for each vault by navigating to *Cryptomator Preferences* -> *Virtual Drive*.

WebDAV has widespread support and adequate performance, but its implementation differs between operating systems.

7.2 What is a FUSE volume type?

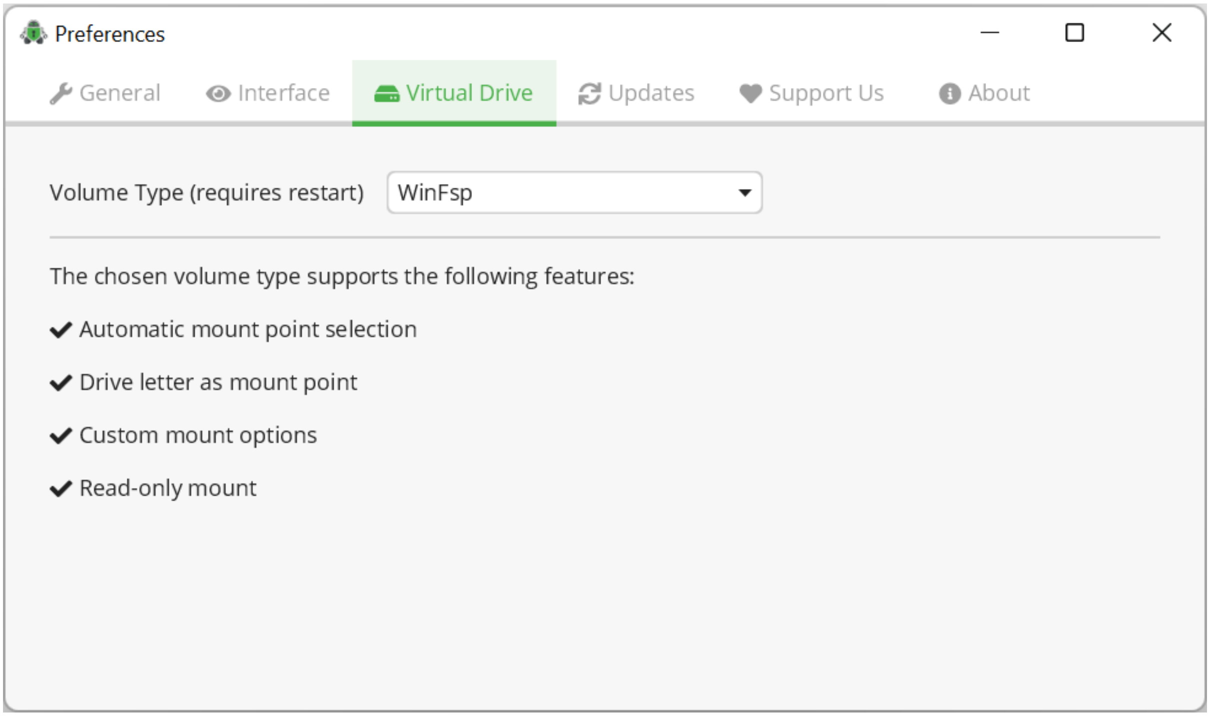
Filesystem in Userspace (FUSE) is a filesystem interface originally developed for Unix operating systems that let non-privileged users create their own file systems without editing kernel code. Which means, FUSE does not require admin privileges and is has good support across all major desktop operating systems. FUSE volume type also delivers good performance when working on files.

All FUSE related volume types support custom mount options, but every option must be prefixed with `-o`. For example, you must enter `-oallow_other` if you want to specify `allow_other` option.

7.3 Choosing a Volume Type

Cryptomator uses the same volume type for all vaults. You can select which volume type to use in the preferences. Every volume type offers fixed set of features for mounting a vault. The feature set is shown when selecting the volume type.

In Cryptomator's window, navigate to `Preferences` (gear icon at top right), then `Virtual Drive` to set the volume type. The availability of volume types depends on your operating system and installed drivers. You might have to restart Cryptomator when changing volume types. A notification will be displayed if a restart is needed.



Volume Type (requires restart): WinFsp

The chosen volume type supports the following features:

✓ Automatic mount point selection

✓ Drive letter as mount point

✓ Custom mount options

✓ Read-only mount

7.4 Windows

7.4.1 WinFsp / WinFsp (Local Drive)

Requirements: Windows, WinFsp installed

The WinFsp project provides FUSE bindings for Windows. WinFsp is automatically installed along Cryptomator when you are using the EXE installer, but there's also a WinFsp standalone installer here if you ever need it.

By default, unlocked vaults are mounted to a random drive letter, either as a network or a local drive. Info on custom mount options is available at WinFsp repository.

Note: Vaults mounted to a drive letter are only accessible to the *current user*. If you want to access the vault as a different/elevated user, you have to use WinFsp (Local Drive) and *mount to a directory*.

7.4.2 WebDAV (Windows Explorer)

Requirements: Windows

WebDAV on Windows uses the net use command to mount/unmount the virtual drive. By default, unlocked vaults are mounted as a network drive and assigned a random drive letter. Using WebDAV on Windows has the following drawbacks:

- The size of transferred files is restricted to a maximum of 4 GB.
- The total space and free space of the network drive are shown to be the same as the total space and free space of the C: drive, which is technically incorrect.

7.4.3 Dokany (v1.5.1)

Warning: Dokany support in Cryptomator is deprecated since version 1.7.0. We suggest switching to *WinFsp / WinFsp (Local Drive)*.

Requirements: Windows, Dokany 1.5.1 installed

The Dokany project aims to achieve the same goals as FUSE, but specific for Windows: Provide an interface to create your own filesystem without requiring to write your own kernel filesystem driver. It has to be installed separately by downloading an installer from Dokany's releases page. By default, unlocked vaults are mounted to a random drive letter.

7.5 macOS

7.5.1 macFUSE

Requirements: macOS, macFUSE installed

Warning: Apple has deprecated the OS APIs used by macFUSE since macOS 12.3 and made installation difficult. We recommend you to use FUSE-T and only fallback to macFUSE, if there are any errors.

macFUSE volume type depends on a library provided by the macFUSE project. It is not included with Cryptomator due to license restrictions. However, you can install the latest version from macFUSE's release page.

By default, unlocked vaults are mounted to */Volumes*. Info on custom mount options is available at macFUSE wiki.

7.5.2 FUSE-T (Experimental)

Requirements: macOS, FUSE-T installed

This volume type depends on a library provided by the new FUSE-T project. You can install it using brew:

```
brew tap macos-fuse-t/homebrew-cask
brew install fuse-t
```

By default, unlocked vaults are mounted to *~/Cryptomator/*. Info on custom mount options is available at wiki of the FUSE-T project.

Note: FUSE-T is a new project, so support for it is currently marked as experimental. Be sure to keep FUSE-T up to date to benefit from the latest improvements.

7.5.3 WebDAV (AppleScript)

Requirements: macOS

WebDAV on macOS utilizes the scripting language *AppleScript* to mount/unmount the virtual drive. By default, unlocked vaults are mounted to */Volumes*.

7.6 Linux based OS

7.6.1 FUSE

Requirements: Linux, `fuse3` installed

FUSE on Linux works only if the *fuse3* package is installed. Luckily, *fuse3* comes pre-installed on many Linux distributions.

By default, unlocked vaults are mounted to *~/.local/share/Cryptomator/mnt*, but you can use custom mount options to change the path. Info on custom mount options is available at man page for mount.fuse.

Note: `allow_root` and `allow_other` cannot be used as *custom mount flags* without enabling (uncommenting) `user_allow_other` option in **/etc/fuse.conf** configuration file.

7.6.2 WebDAV (gio)

Requirements: Linux, `gio` installed

Due to the wide variety of Linux distributions, Cryptomator only supports system integrated WebDAV volume type if gio is installed. You can unlock your vault without `gio` using *WebDAV (HTTP Address)*, but support across distributions is not guaranteed. Also, it's up to yourself to figure out how to integrate WebDAV share with your distro.

7.7 OS Independent

7.7.1 WebDAV (HTTP Address)

Requirements: None - Works on all OS.

This volume type is always present and comes in handy when all other volume types fail to mount. It starts a local-only WebDAV server, which can be manually integrated into the system or accessed using a third-party application, like Cyberduck. Check out the regarding manuals for your OS on how to connect to a WebDAV server. The address of Cryptomators local-only WebDAV server can be copied from the vault detail screen by clicking the green “Copy” button.

CHAPTER

EIGHT

SETUP

You can get Cryptomator for Android on

- Google Play
- APK Store
- Cryptomator F-Droid repository
- Main F-Droid repository

As for the functionality of Cryptomator, the application does not differ using Google Play or the APK Store as installation type. Google Drive is excluded from the F-Droid version because Google Drive needs proprietary dependencies which doesn't fit to the spirit of F-Droid.

The APK Store and F-Droid variant of Cryptomator was created to serve users who do not have Google Play-Store installed on their Android device. If you have a Google PlayStore on your device, we recommend using the PlayStore version of Cryptomator.

Table 1: Cryptomator for Android variants

	Google Play	APK Store	Cryptomator F-Droid repo	Main F-Droid repo
Dropbox				[1]
Google Drive			[2]	[1]
OneDrive				[1]
pCloud				[1]
WebDAV				
S3				
Local Storage				

[1]: Excluded because they require API keys. [2]: Excluded because they contains proprietary dependencies.

8.1 Google PlayStore

If you have installed Cryptomator via the Google PlayStore, you will receive updates as usual via the Google PlayStore.

After buying the app using Google PlayStore, it can be used with any number of devices that you have linked to the google account from your purchase. Furthermore it supports the "Google Play Family Library" function which means that the app can be used by up to 5 people in a family without having to buy it again. The conditions and how to create a "Google Play Family" can be found here: https://support.google.com/googleplay/answer/7007852?hl=en

Sometimes the Google PlayStore has problems to recognize that the app was already bought and asks you to buy again the app, see this topic to recover from this problem: On how many devices can the app be installed using Google Play Store?

8.2 APK Store

The APK store version can be installed from our website https://cryptomator.org/android/. Please verify the *SHA256 Signature* after downloading the APK before installing. The download is a so-called *APK* (Android application package), which is an installation archive. Install the app by simply clicking on the APK.

It is possible that the app in which you clicked on the APK is asking for “Install from Unknown Sources” permission, this is normal and must be activated for a short time (it is recommended to remove the permission afterwards).

This version does include an automatic updater that periodically checks if there is a newer version of this app, and if so, it can be downloaded and installed directly from within the app. Using the *Update Check Interval* in the Cryptomator settings, you can specify how often the update check is executed.

As this version wasn’t bought using Google’s PlayStore you need to buy a license key from our website https://cryptomator.org/android/. After Cryptomator is installed, you have to enter this key. This can be done by copying and pasting the license into the field when asked for it or by clicking on the link starting with *cryptomator://license/YOUR_LICENSE_KEY*.

8.3 Cryptomator F-Droid repository

The Cryptomator F-Droid repository version can be installed after adding our F-Droid repository to the F-Droid app by opening this link on the device or scanning the following QR-Code:

As well as using the APK Store variant because this app version wasn’t bought using Google’s PlayStore you need to buy a license key from our website https://cryptomator.org/android/. After Cryptomator is installed, you have to enter this key. This can be done by copying and pasting the license into the field when asked for it or by clicking on the link starting with *cryptomator://license/YOUR_LICENSE_KEY*.

8.4 Main F-Droid repository

The Main F-Droid repository version can be installed directly from the Main F-Droid repository. Regarding the license key, the same applies as with the *Cryptomator F-Droid repository* variant.

Unlike all other versions of Cryptomator for Android, this version has its own package name: `org.cryptomator.lite`. It means that you cannot, intentionally or unintentionally, simply switch between this and the other versions. It requires to setup the app again. The reason we decided to do this is that other Cryptomator variants already exist in some popular F-Droid repositories, and if we hadn’t decided to do this, there could have been an unwanted variant switch.

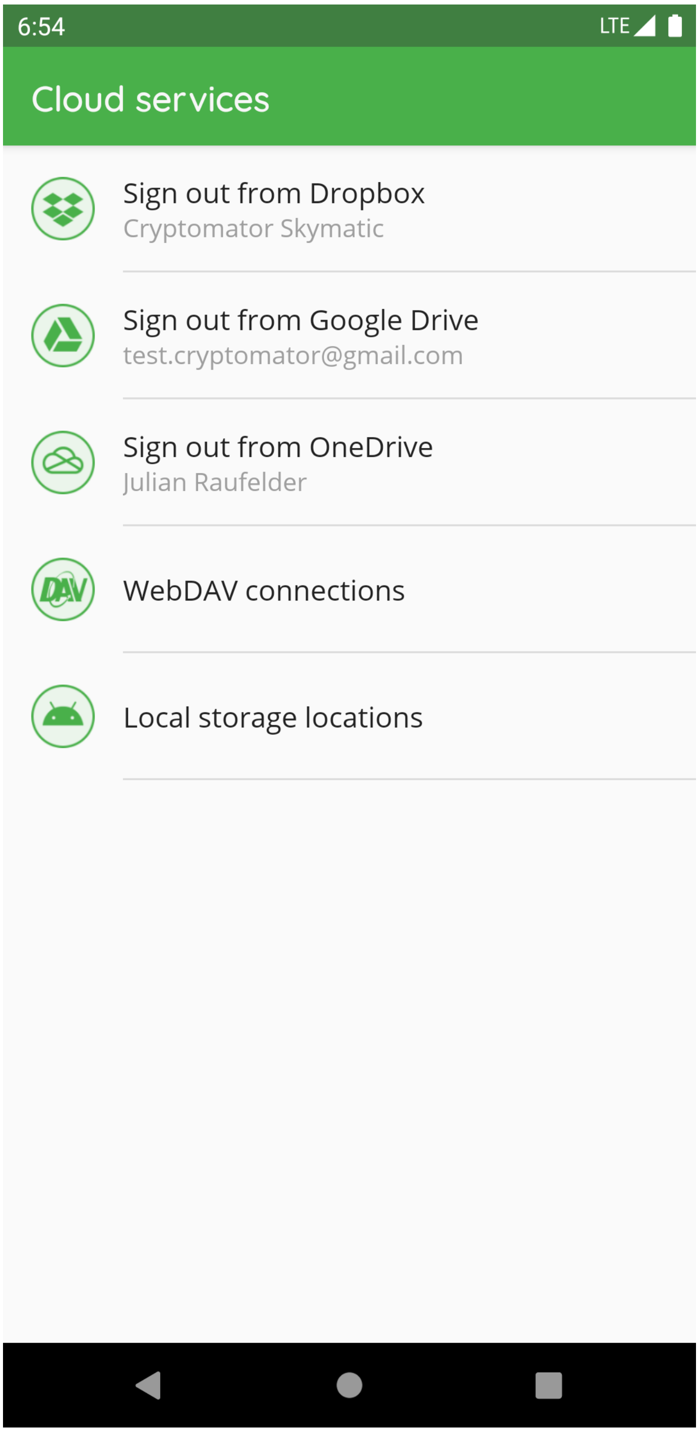
8.5 Requirements

Requires Android 8.0 or later.

CHAPTER

NINE

CLOUD MANAGEMENT



Cloud services

Sign out from Dropbox
Cryptomator Skymatic

Sign out from Google Drive
test.cryptomator@gmail.com

Sign out from OneDrive
Julian Raufelder

WebDAV connections

Local storage locations

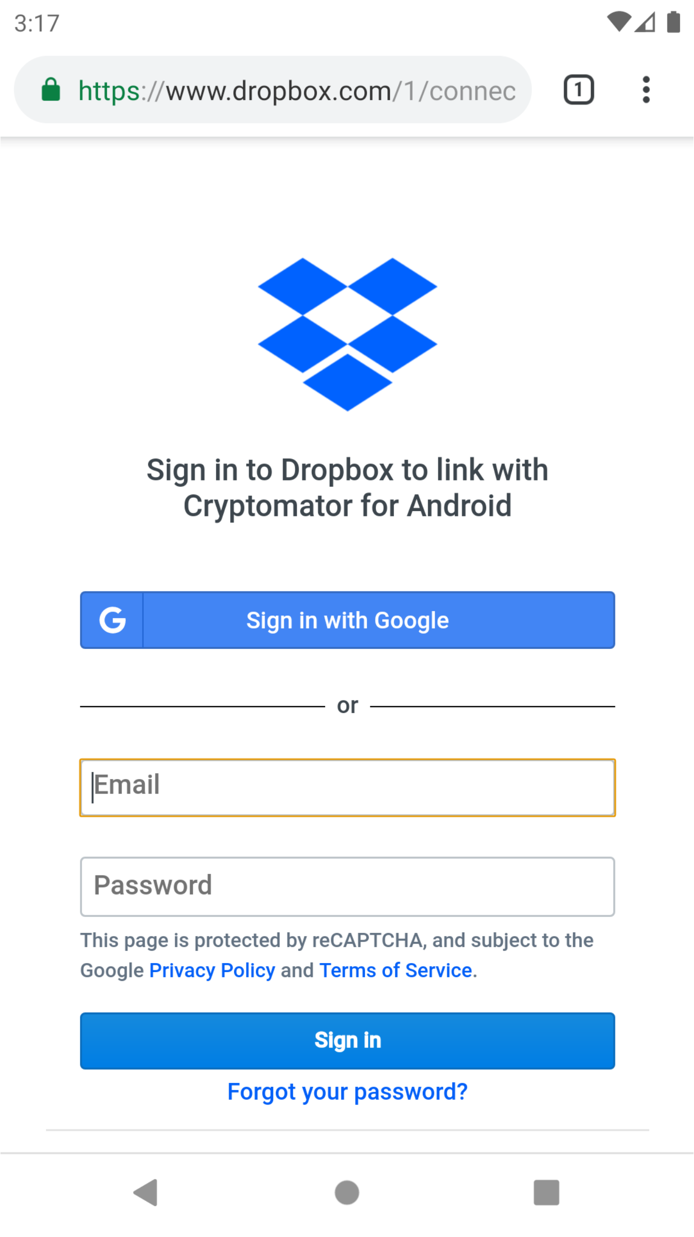
In “Cloud Services”, you can create or edit the connection between the Cryptomator app and your storage provider accounts.

Please enter the credentials for your provider account or in case of Google Drive choose your account. If your authentication was successful, some of the providers might ask you to grant Cryptomator access permission to your online files. Please allow this permission.

In Google Drive, OneDrive and Dropox you can only create one connection between your cloud storage account and the Cryptomator app. You can’t connect to (for example) two different *Dropbox* accounts.

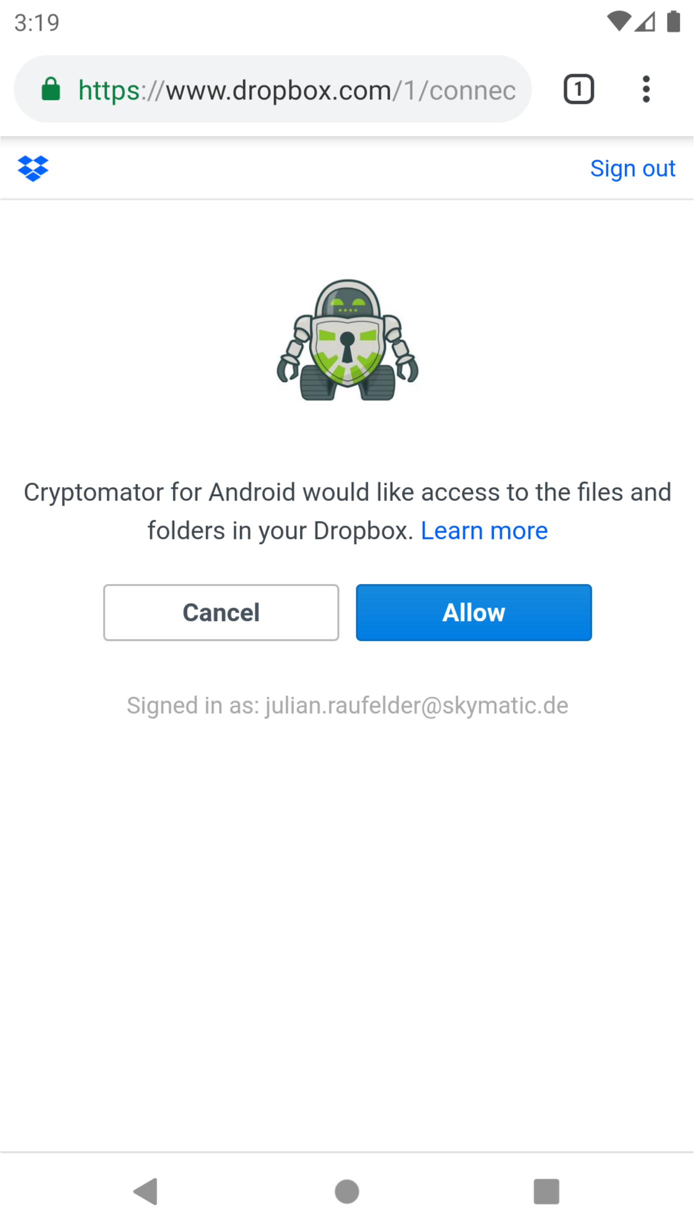
If the provider requested permission to access your online files you can remove Cryptomator permissions from your online storage account at any time. Please keep in mind that Cryptomator then cannot connect to your vault anymore.

9.1 Login Dropbox



Sign in to Dropbox to link with Cryptomator for Android

This page is protected by reCAPTCHA, and subject to the Google Privacy Policy and Terms of Service.



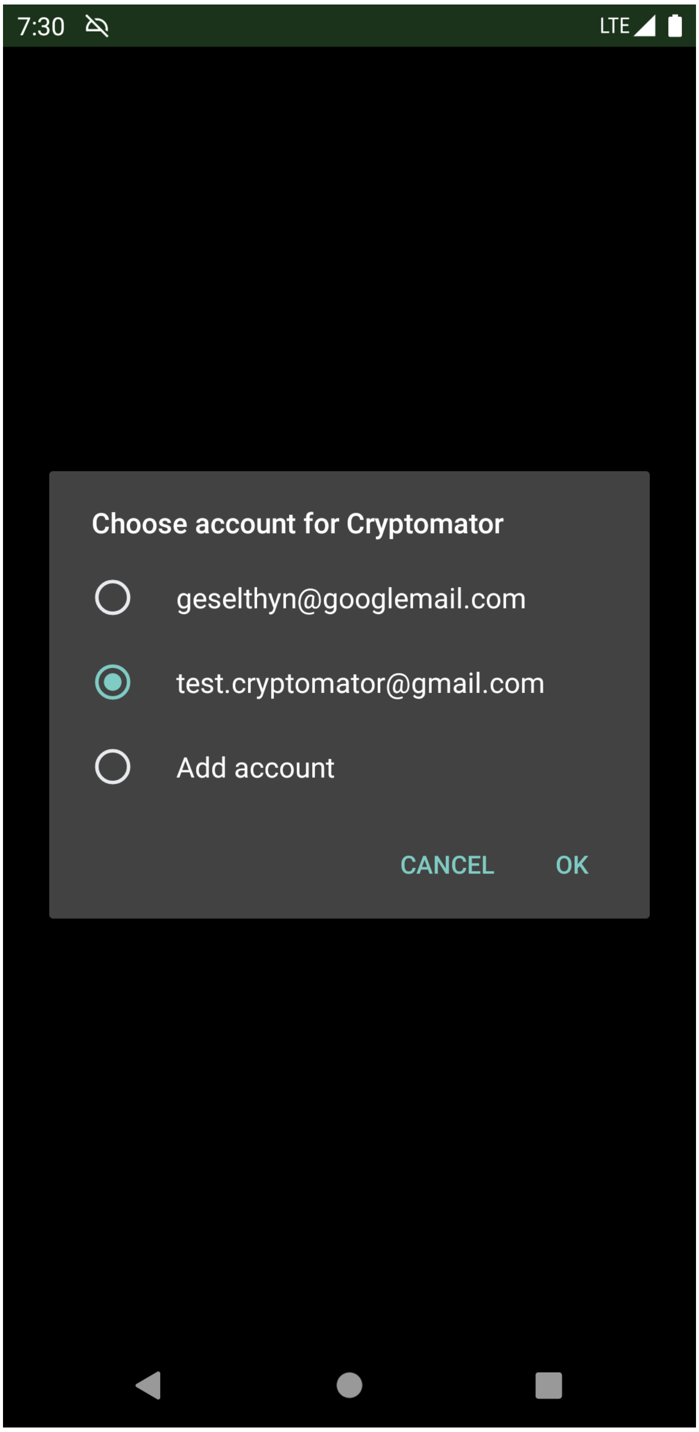
3:19

https://www.dropbox.com/1/connec

Cryptomator for Android would like access to the files and folders in your Dropbox. Learn more

Signed in as: julian.raufelder@skymatic.de

9.2 Login Google Drive



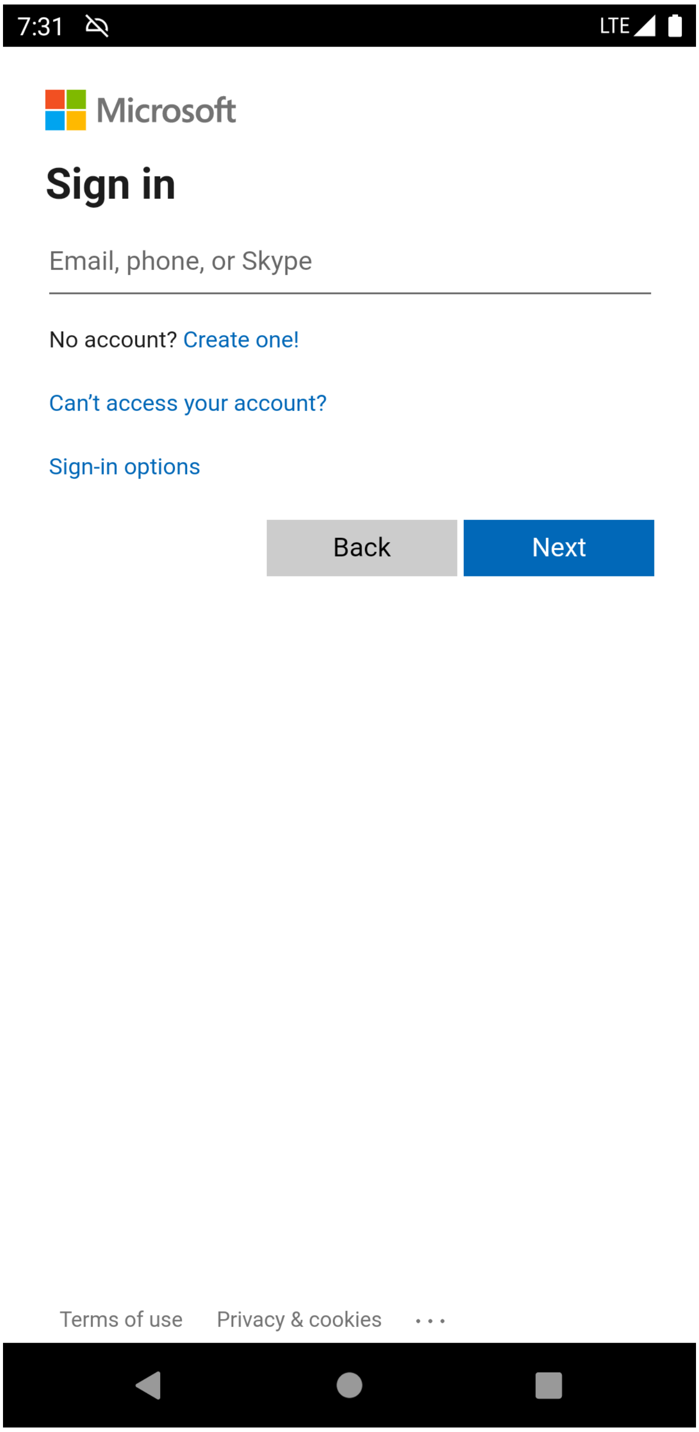
Choose account for Cryptomator

○ geselthyn@googlemail.com

● test.cryptomator@gmail.com

○ Add account

9.3 Login OneDrive



7:31 LTE

Microsoft

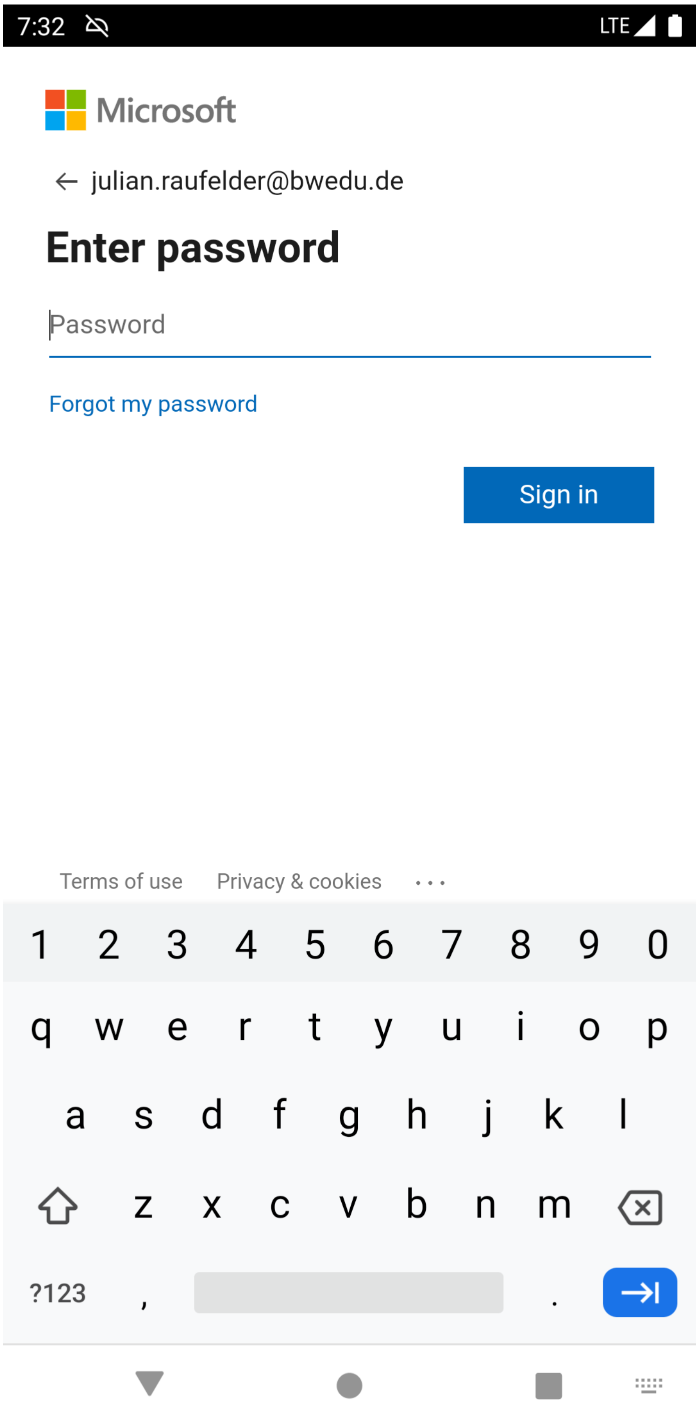
Sign in

Email, phone, or Skype

No account? Create one!

Can’t access your account?

Sign-in options

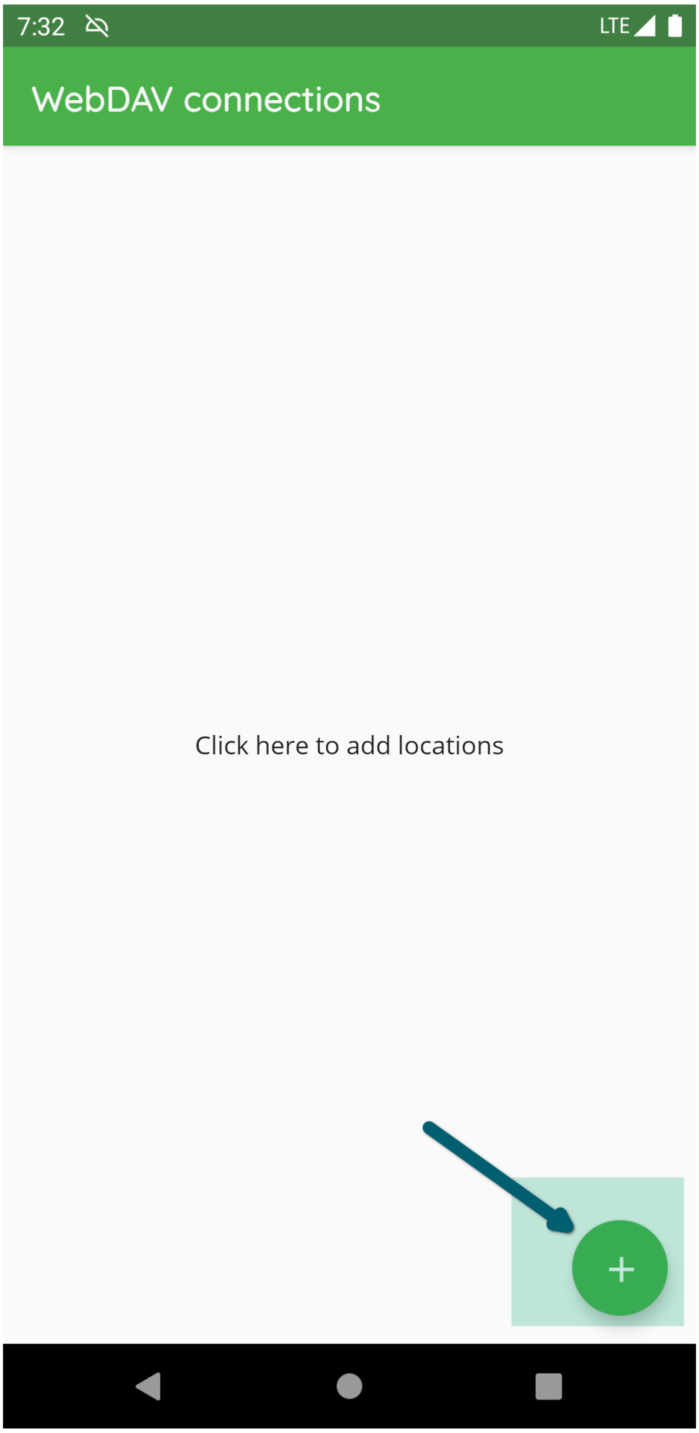


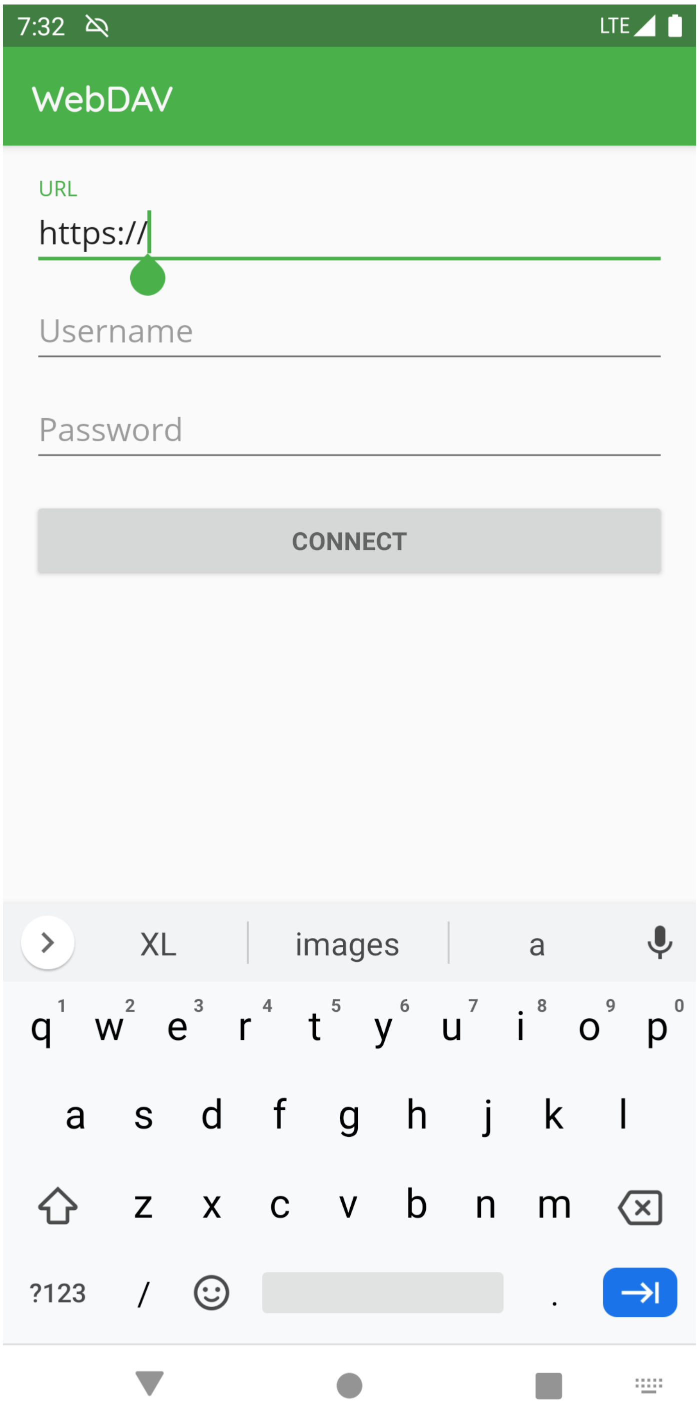
Enter password

Password

9.4 Login WebDAV

You can find here a list of the most common WebDAV URLs.





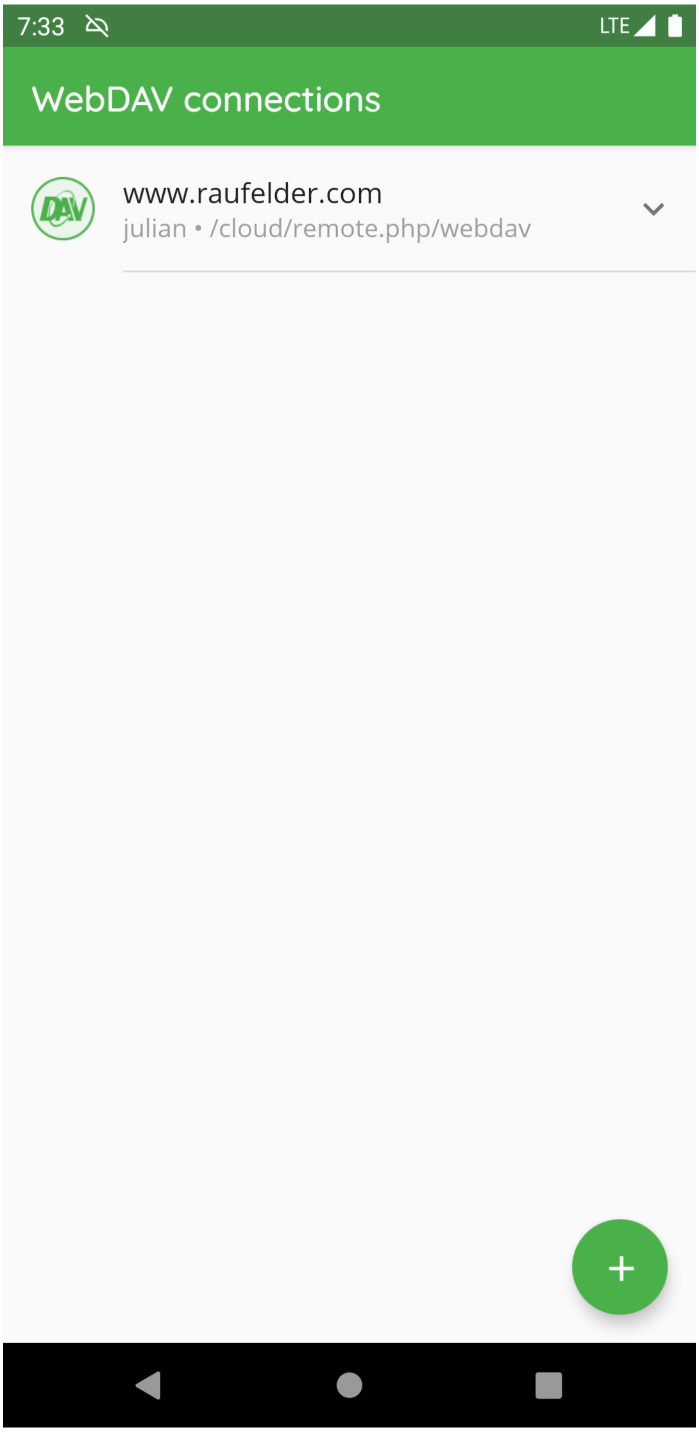
WebDAV

URL

https://

Username

Password



7:33 LTE

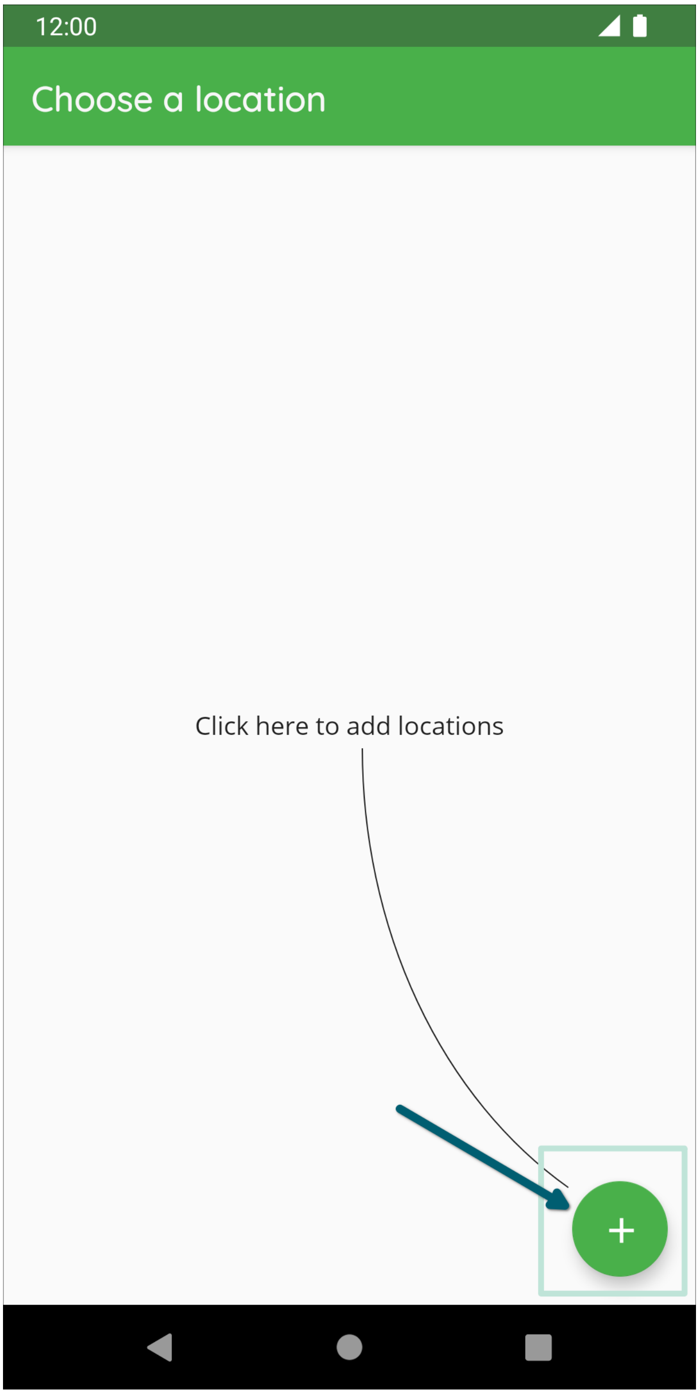
WebDAV connections

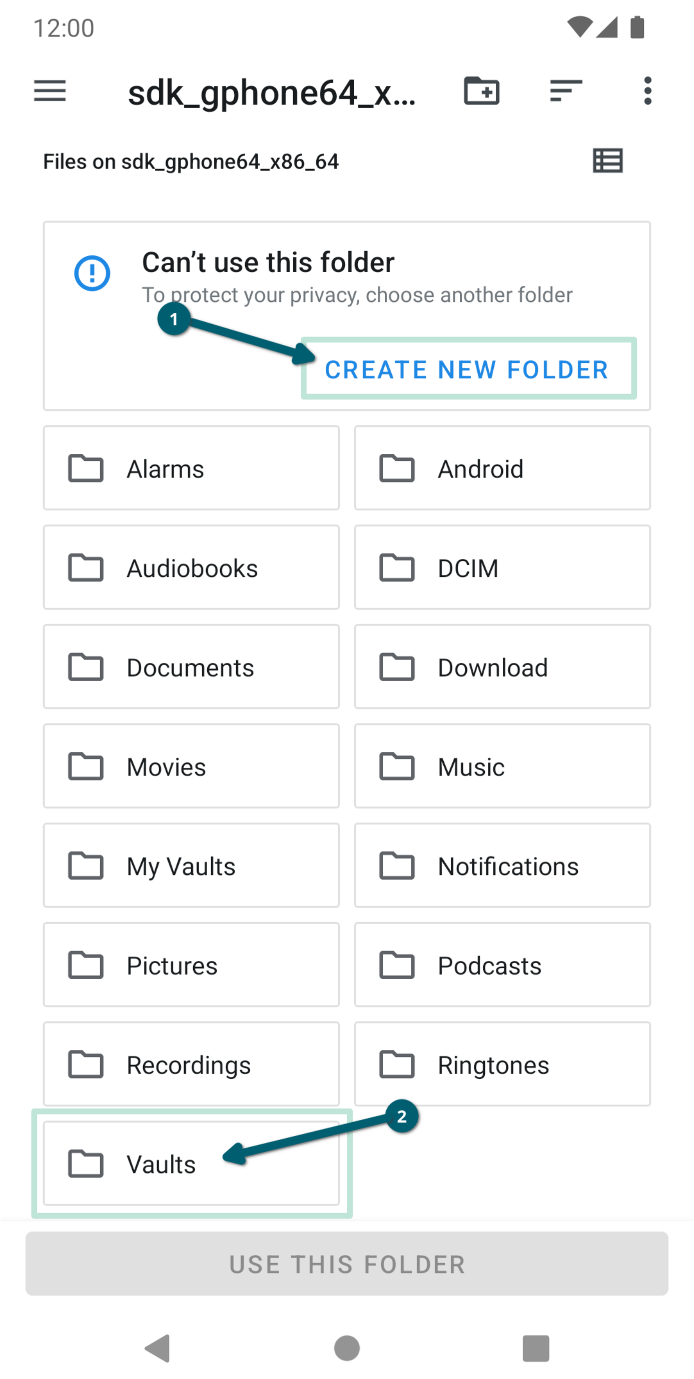
www.raufelder.com
julian • /cloud/remote.php/webdav

Note: While creating the WebDAV connection, please make sure to add the root of the accessible stroge and don't navigate directly into the vault.

9.5 Login Local Storage

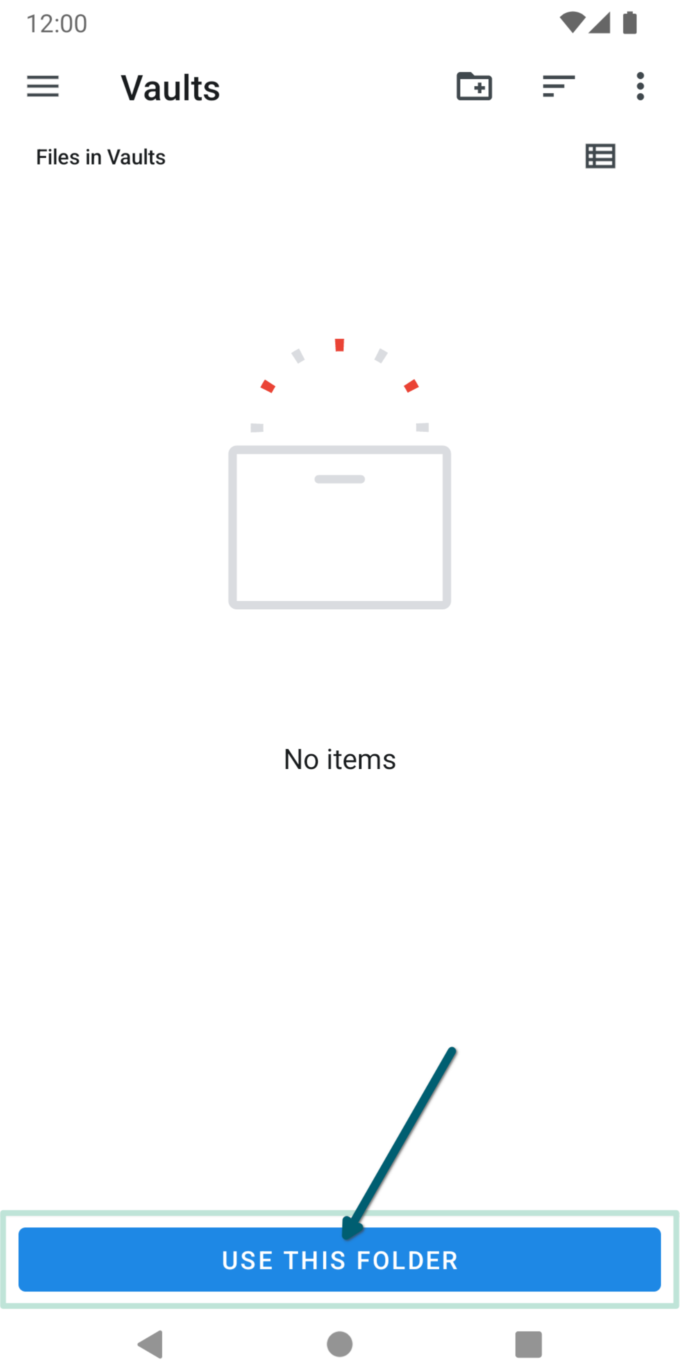
The following pictures describes how to setup a location to access vaults stored on the internal storage of the device (the same applies for vaults located e.g. on a SD card):



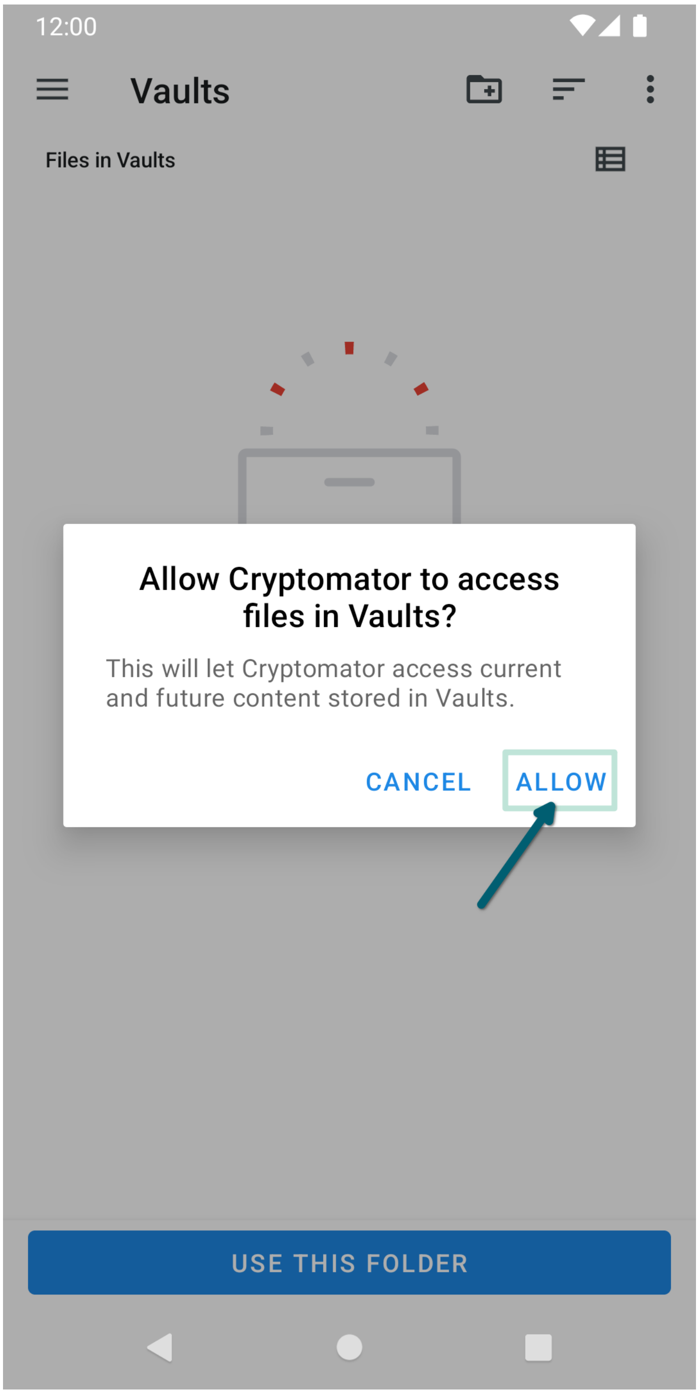


Can't use this folder

To protect your privacy, choose another folder



12:00
Vaults
Files in Vaults
No items
USE THIS FOLDER



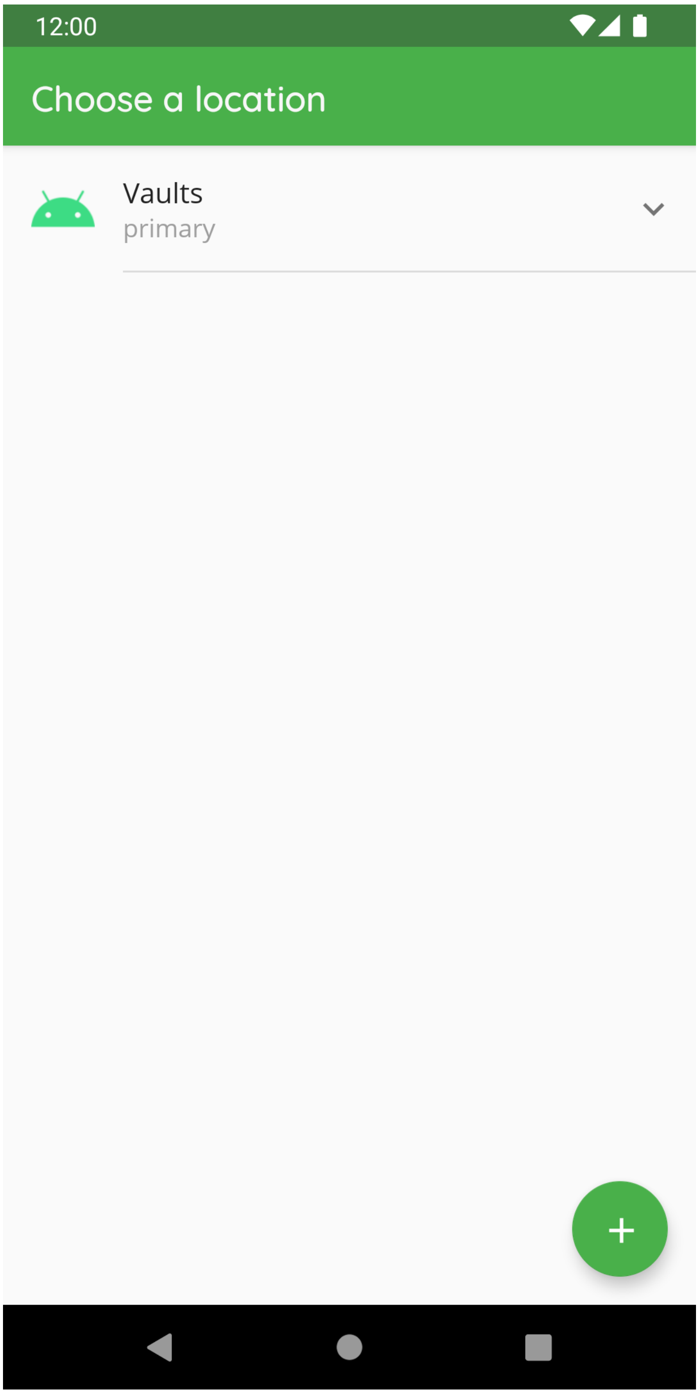
12:00

Vaults

Files in Vaults

Allow Cryptomator to access files in Vaults?

This will let Cryptomator access current and future content stored in Vaults.



After creating the location, you can access it by clicking on the name of the location to add a vault or create a new vault.

Note: If you use a custom location please make sure to add the root folder of the storage like described in the pictures and don't navigate directly into the vault.

CHAPTER

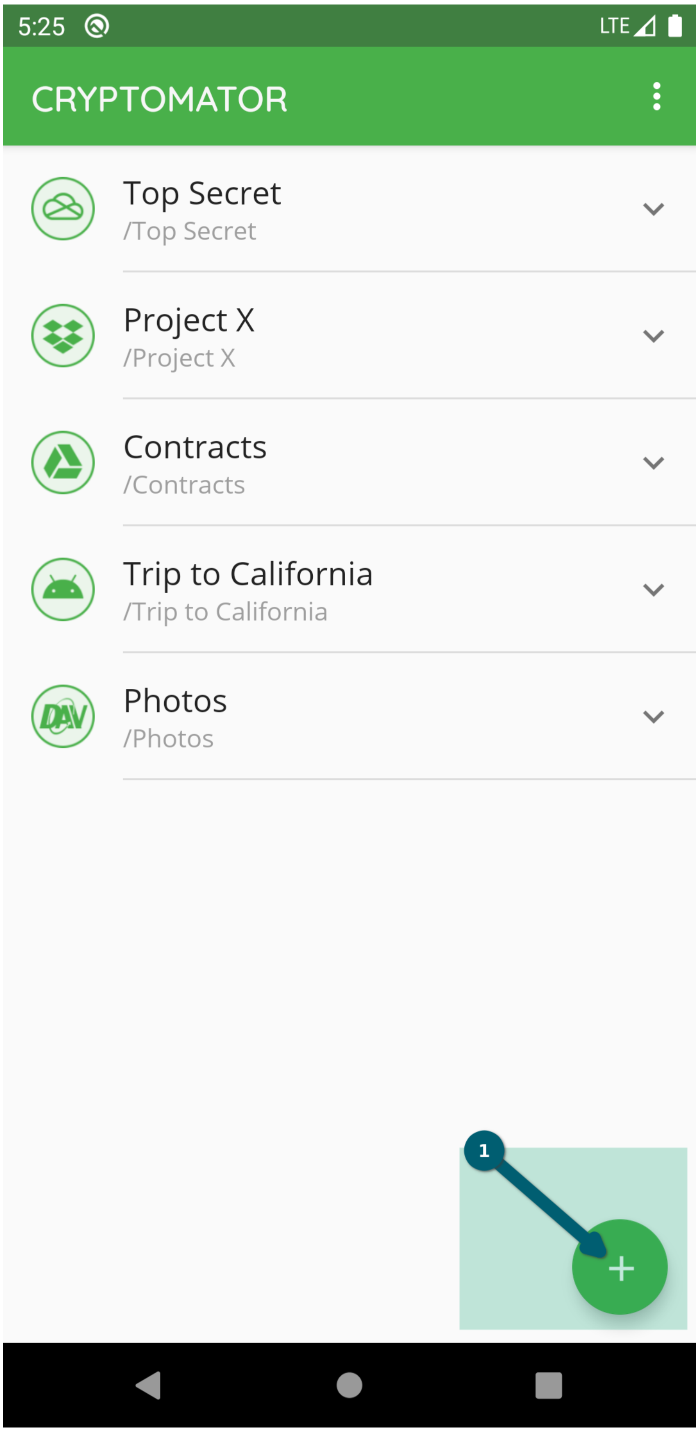
TEN

VAULT MANAGEMENT

TODO.

10.1 Create a New Vault

To create a new vault, click on the plus sign and choose *Create new vault* in the next screen.



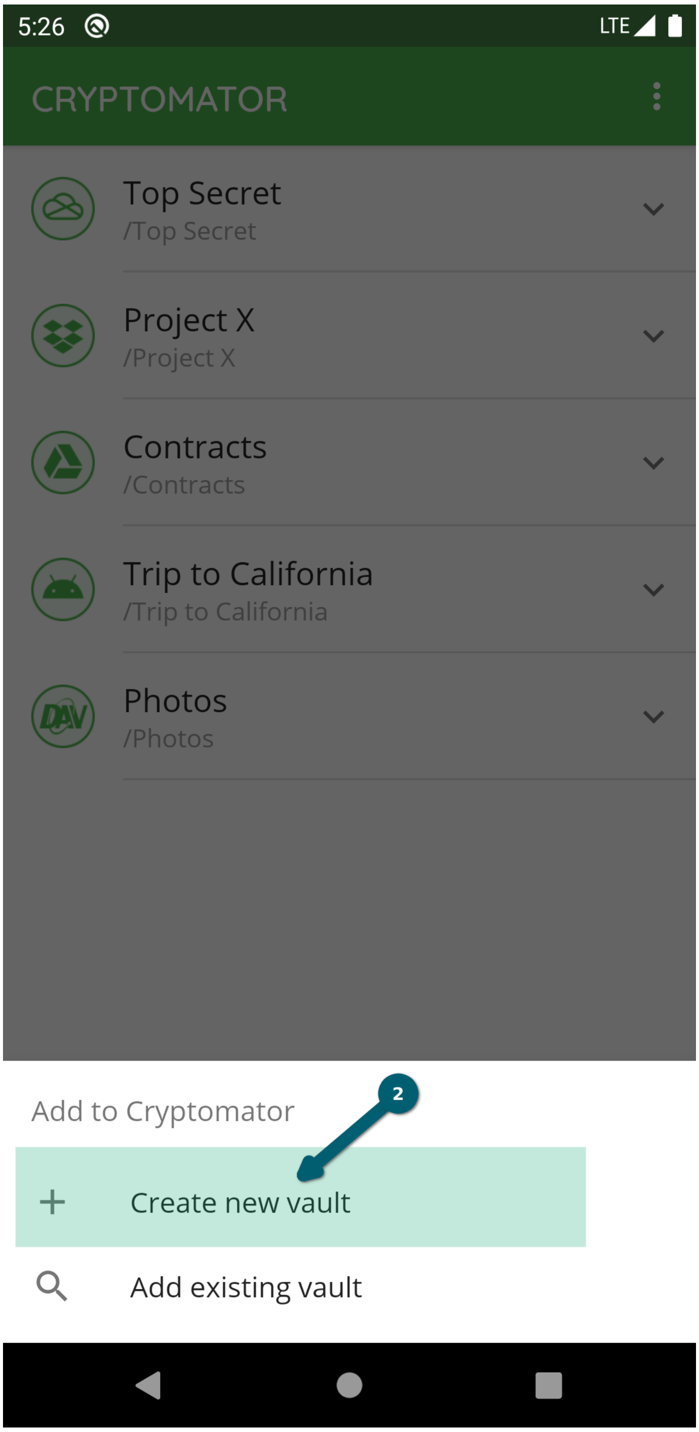
Top Secret
/Top Secret

Project X
/Project X

Contracts
/Contracts

Trip to California
/Trip to California

Photos
/Photos

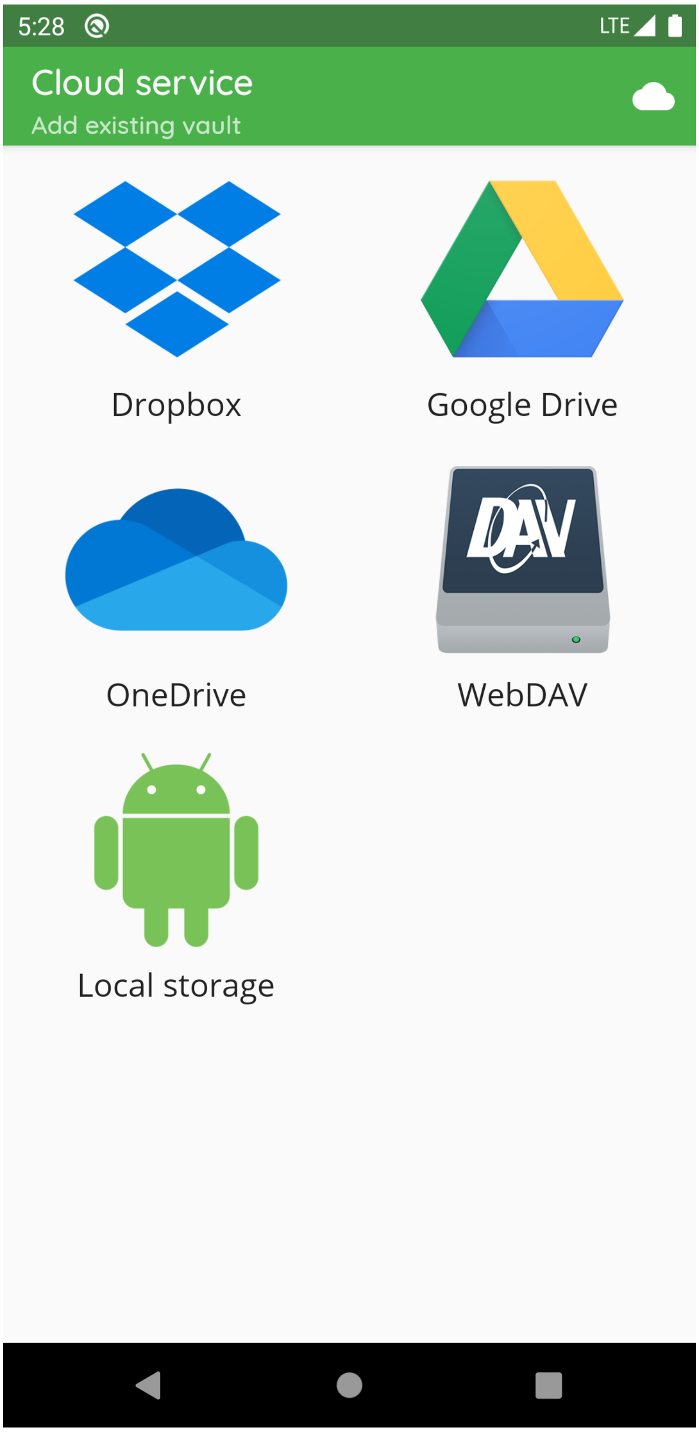


Note: If you already have a vault created with the desktop app and just want to add this vault to your mobile app, please select go to chapter `Add Existing Vaults`.

You will now be prompted to select the cloud provider where you want to store your vault.

Choose between *Dropbox*, *Google Drive*, *OneDrive* (works also with *OneDrive for Business*) or *Local storage* (which means your local device with all attached devices).

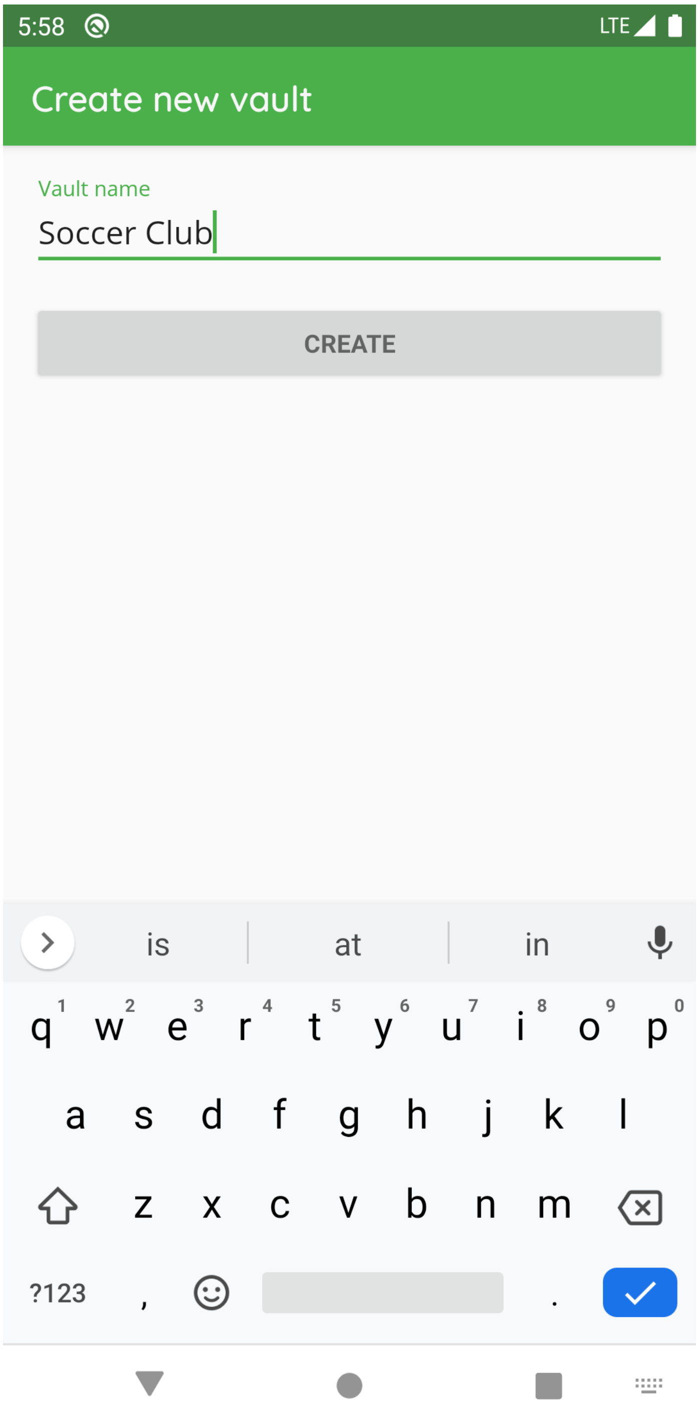
If your desired provider is not listed and offers WebDAV access, please select *WebDAV* as the storage location of your vault. Here you can find WebDAV URLs of Common Cloud Storage Services.



If not already done, you have to create the connection between the Cryptomator app and your storage provider account. Please follow the instructions in the *Cloud Management* chapter and contiune later here.

Now that you've established a connection, you'll add the existing vault.

In the first step, please enter a name for your new vault. This name will also be the folder name of your vault files in your online storage.

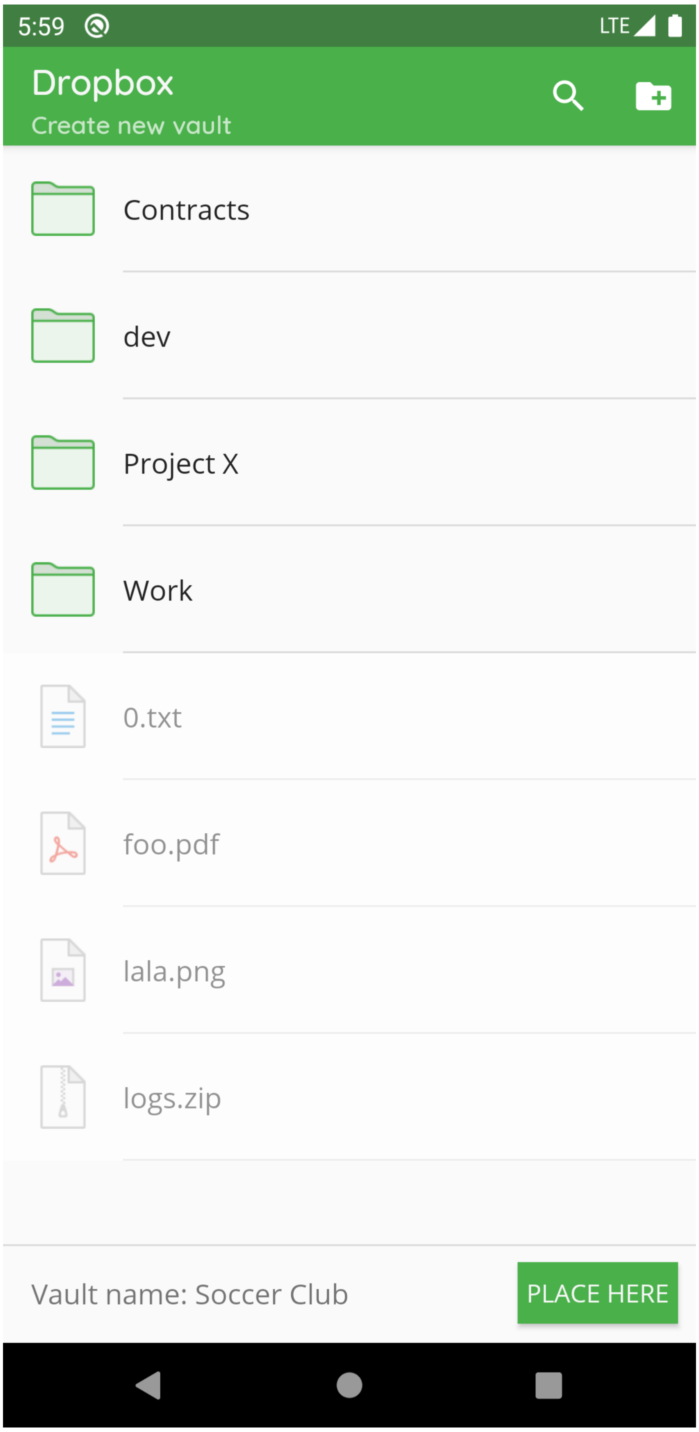


Create new vault

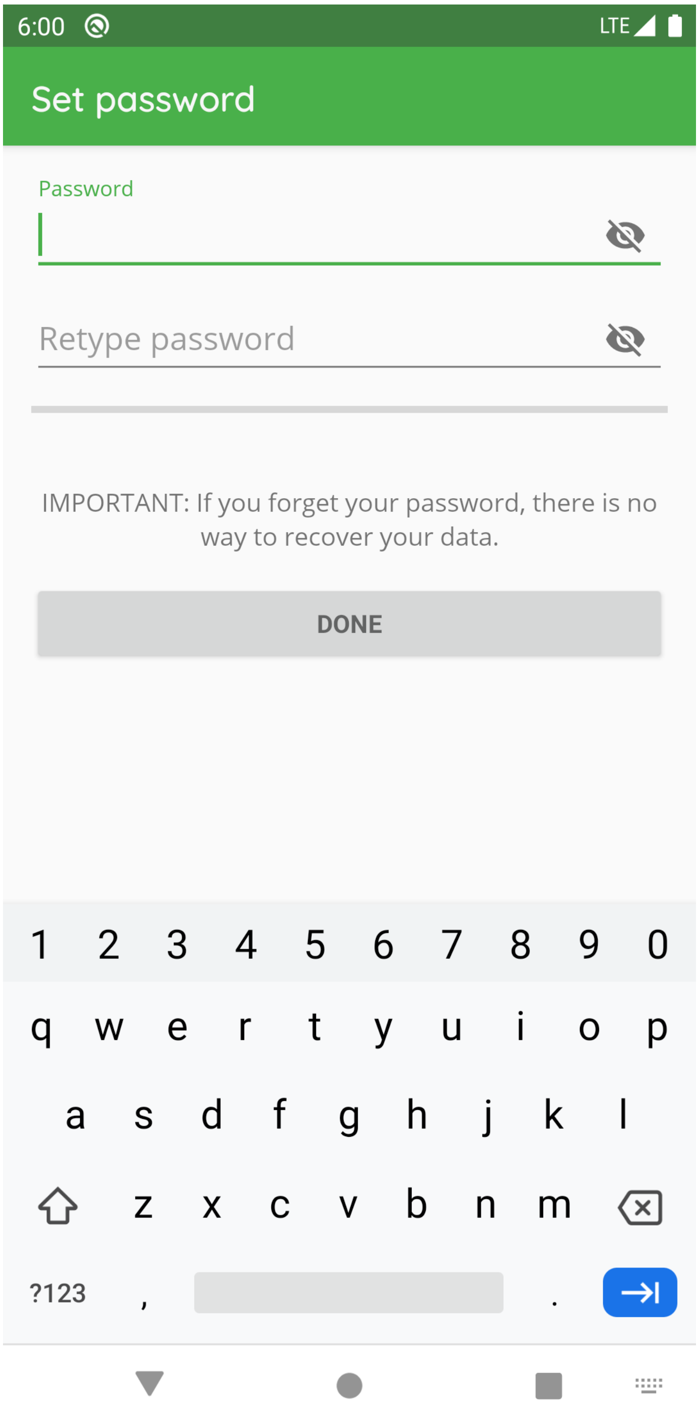
Vault name

Soccer Club

Then choose the location on your cloud storage where you want to have your encrypted vault files stored.



And last but not least, create a **secure** password for your vault. Basically, you have the whole Unicode for choosing a password including non-printable characters.


6:00

Set password

Password

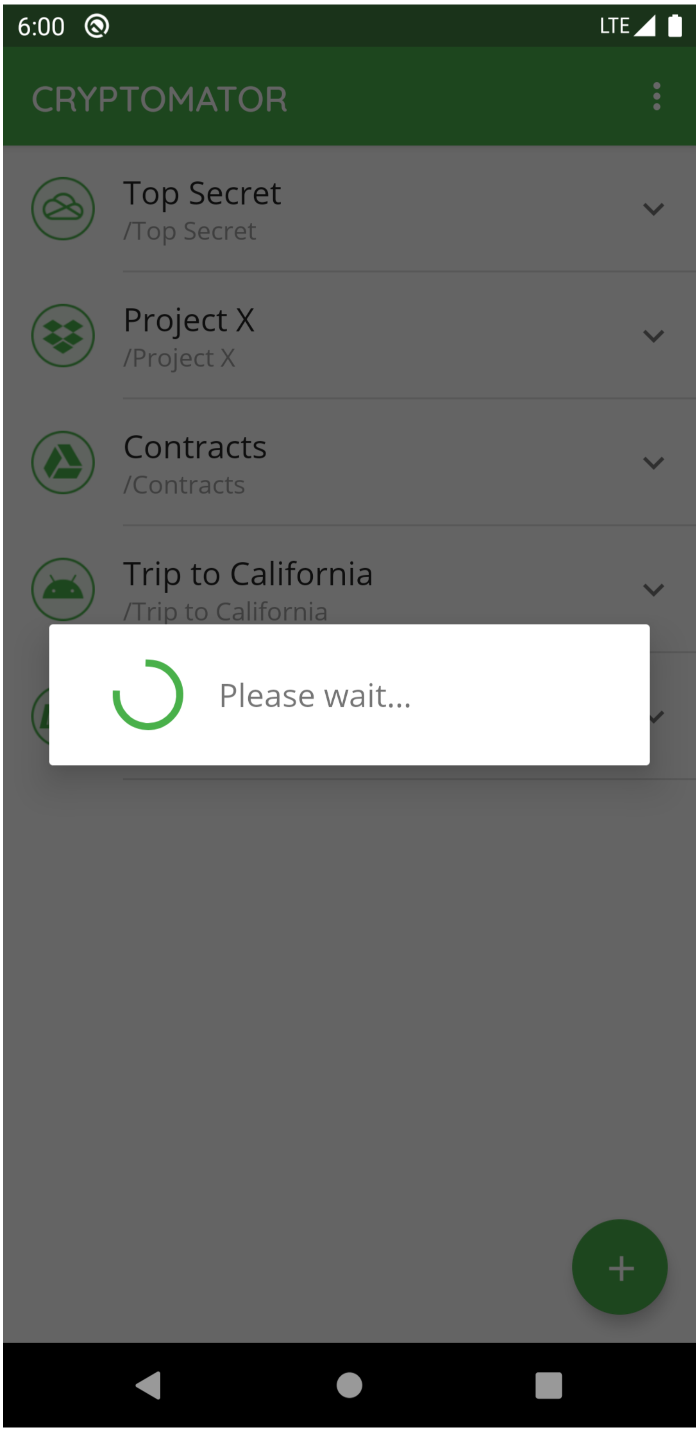
Retype password

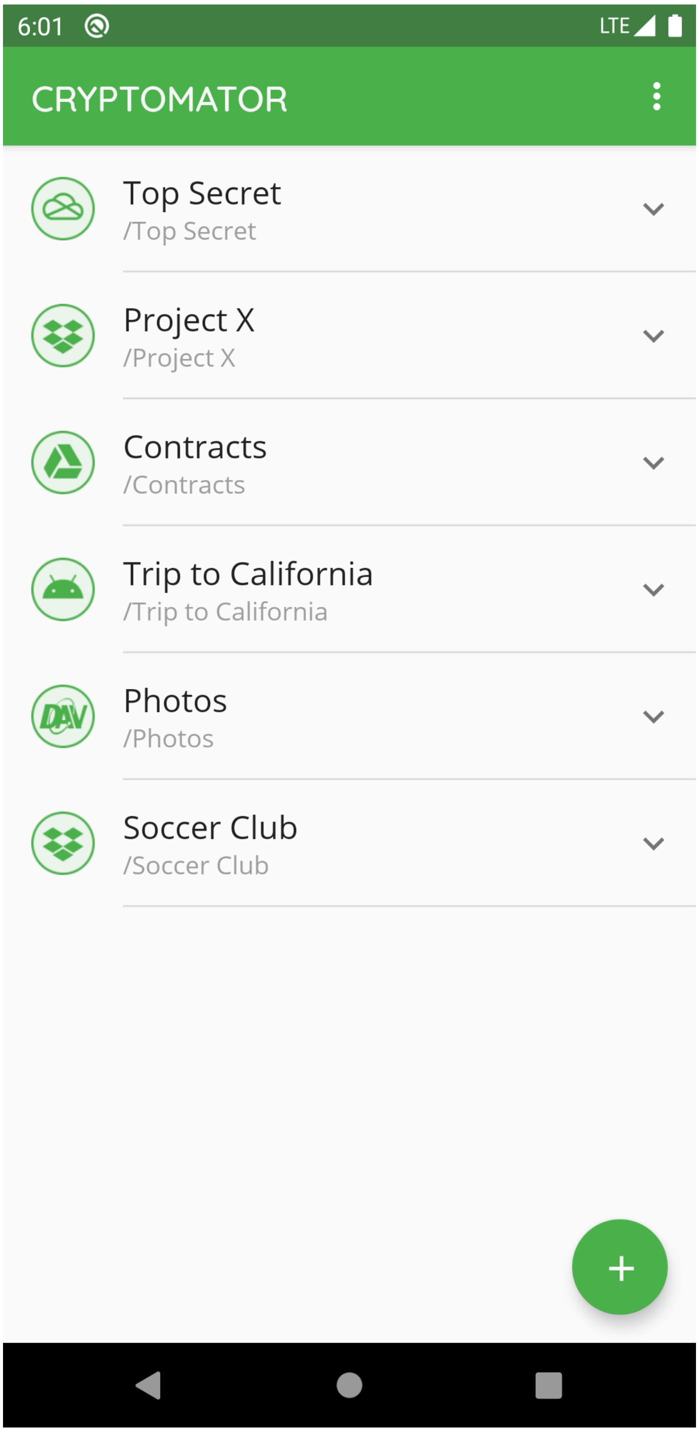
IMPORTANT: If you forget your password, there is no way to recover your data.

DONE

Warning: You have to remember this password at all times because there is **no way to access your data if you forget your password**. Choose a *good password* to make your data secure.

After you have confirmed your password, the vault is created. You will find it now on the start page of your Cryptomator app, where you can open your vault and optionally change settings. [documentation will follow]


6:00
LTE
CRYPTOMATOR
Top Secret
/Top Secret
Project X
/Project X
Contracts
/Contracts
Trip to California
/Trip to California
Please wait...
+



6:01

CRYPTOMATOR

Top Secret
/Top Secret

Project X
/Project X

Contracts
/Contracts

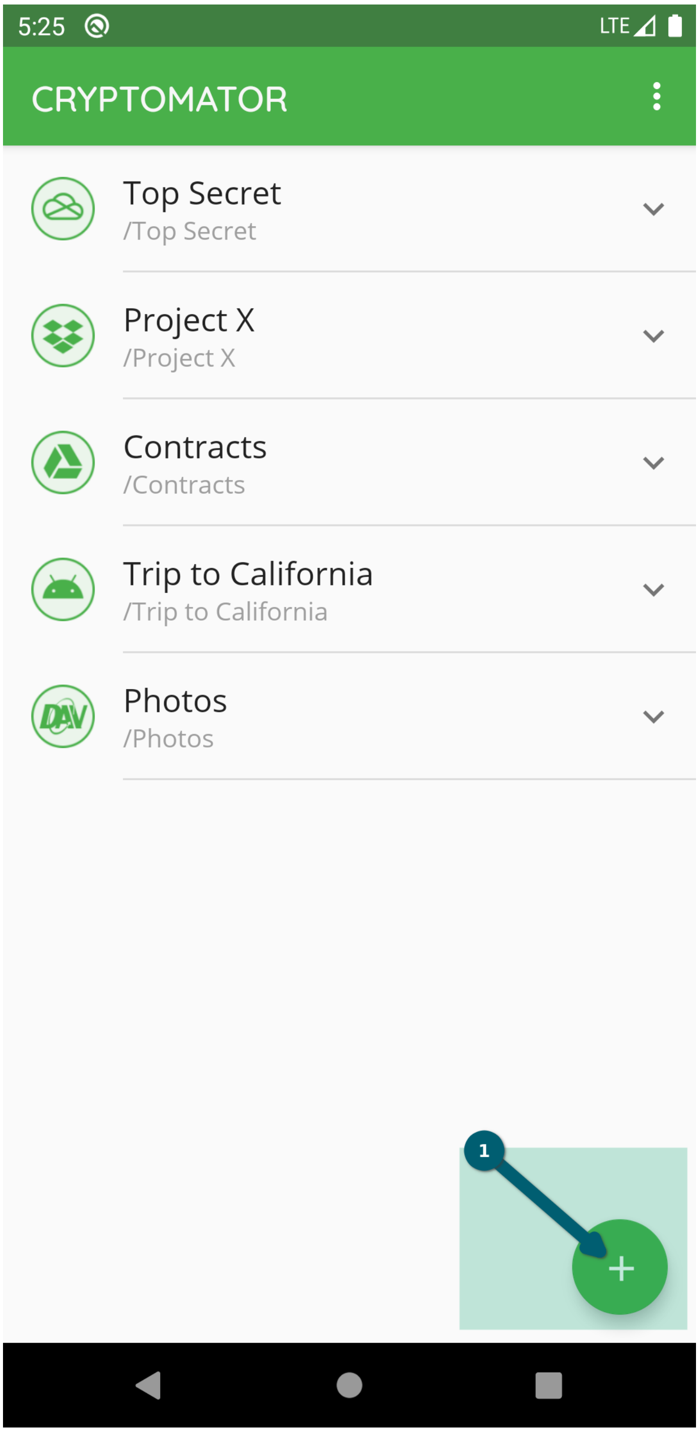
Trip to California
/Trip to California

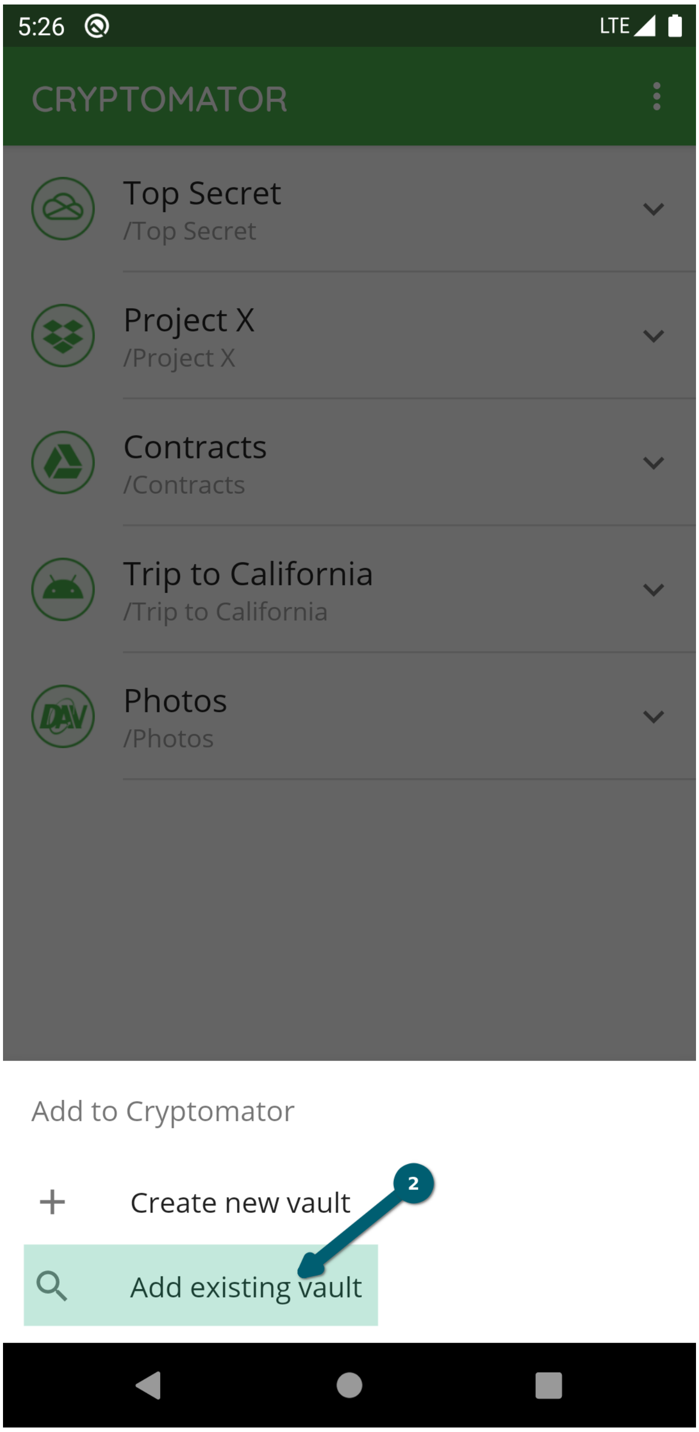
Photos
/Photos

Soccer Club
/Soccer Club

10.2 Add Existing Vaults

To add an existing vault, click on the plus sign and choose *Add existing vault* in the next screen.

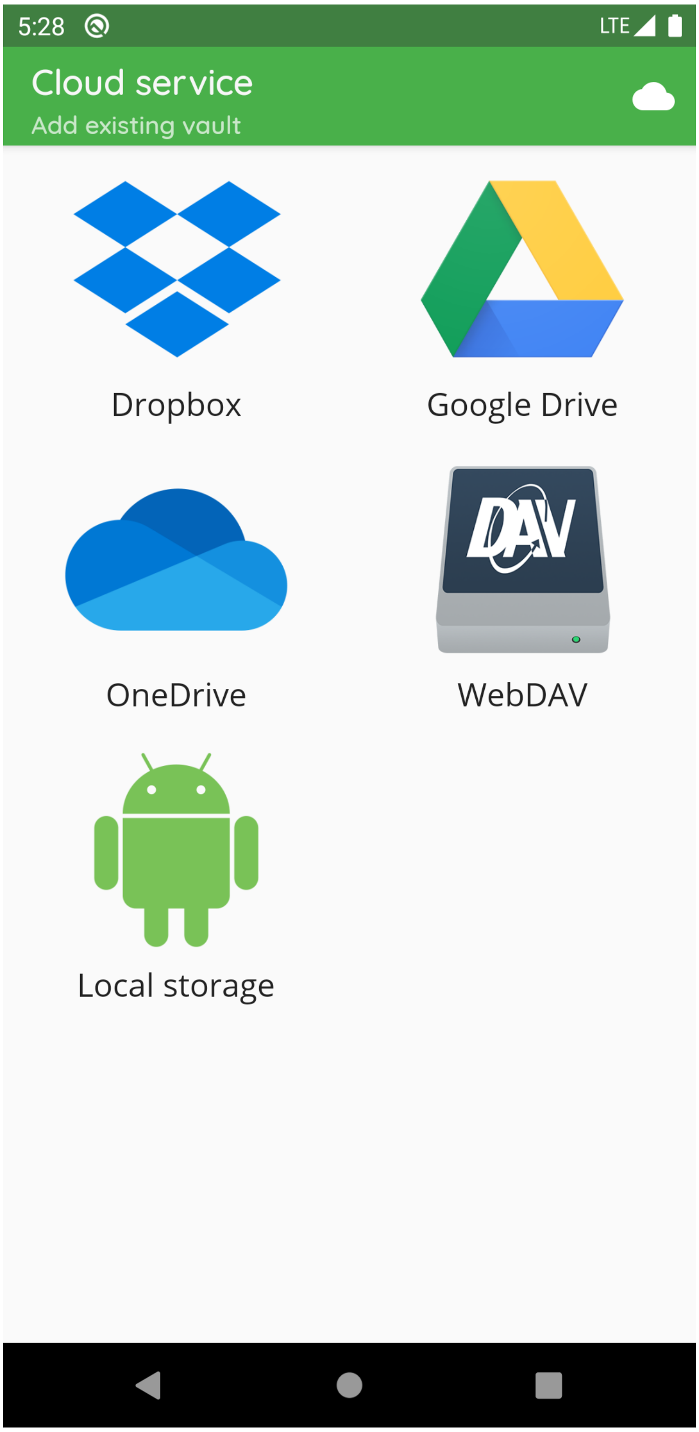




You will now be prompted to select the cloud provider where the vault is located.

Choose between *Dropbox*, *Google Drive*, *OneDrive* (works also with *OneDrive for Business*) or *Local storage* (which means your local device with all attached devices).

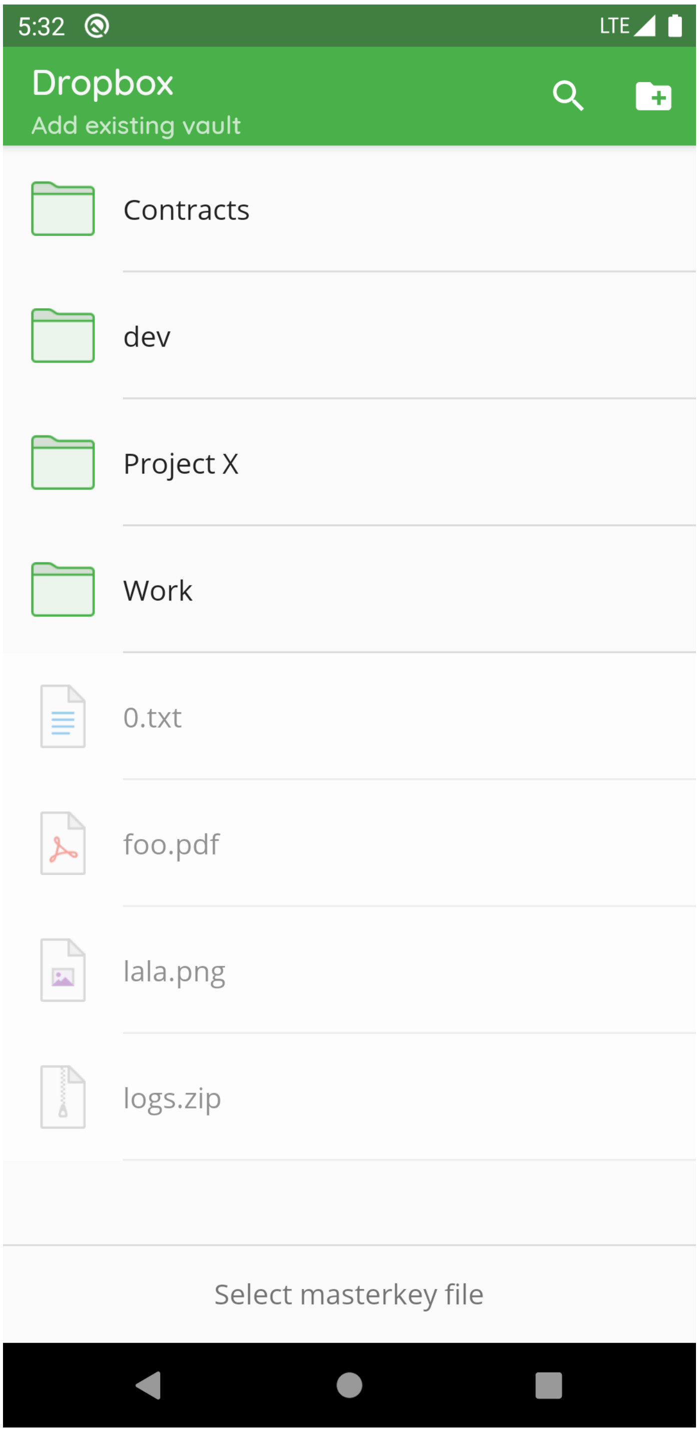
If your desired provider is not listed and offers WebDAV access, please select *WebDAV* as the storage location of your vault. Here you can find WebDAV URLs of Common Cloud Storage Services.



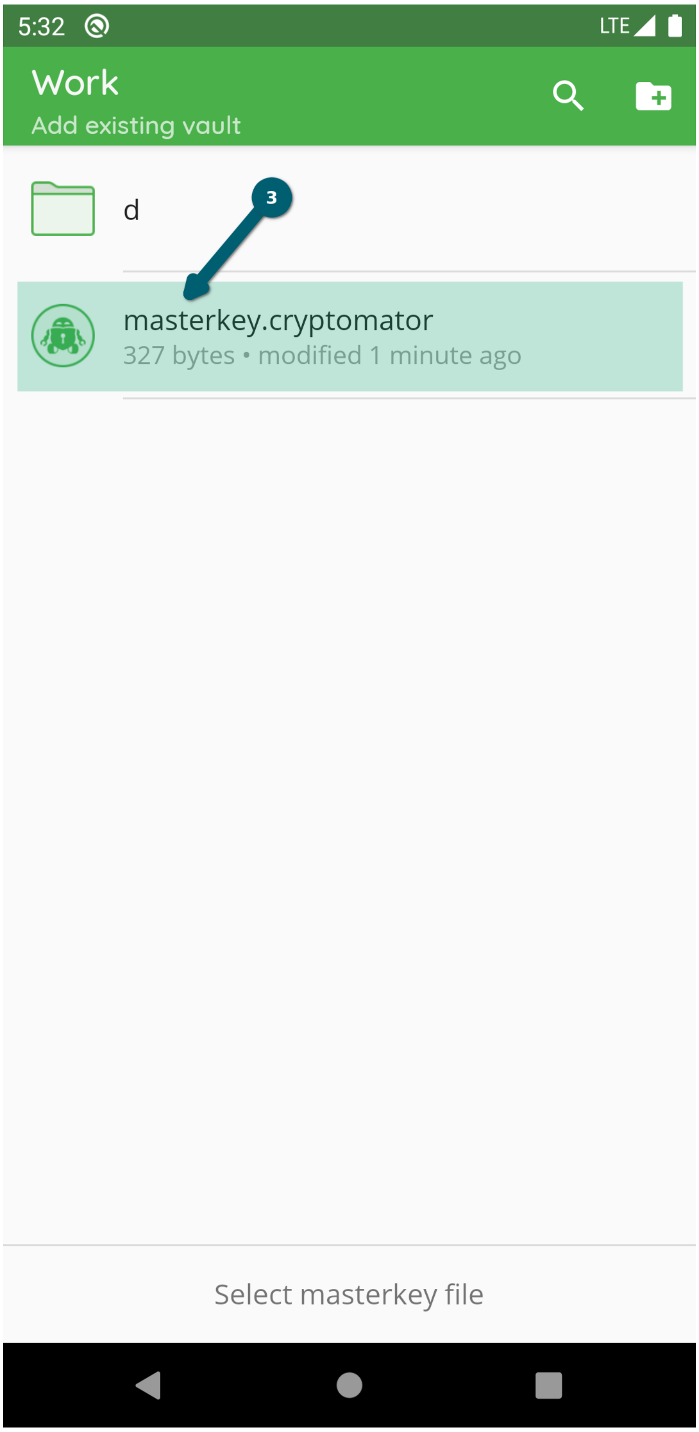
If not already done, you have to create the connection between the Cryptomator app and your storage provider account. Please follow the instructions in the *Cloud Management* chapter and contiune later here.

Now that you've established a connection, you'll add the existing vault.

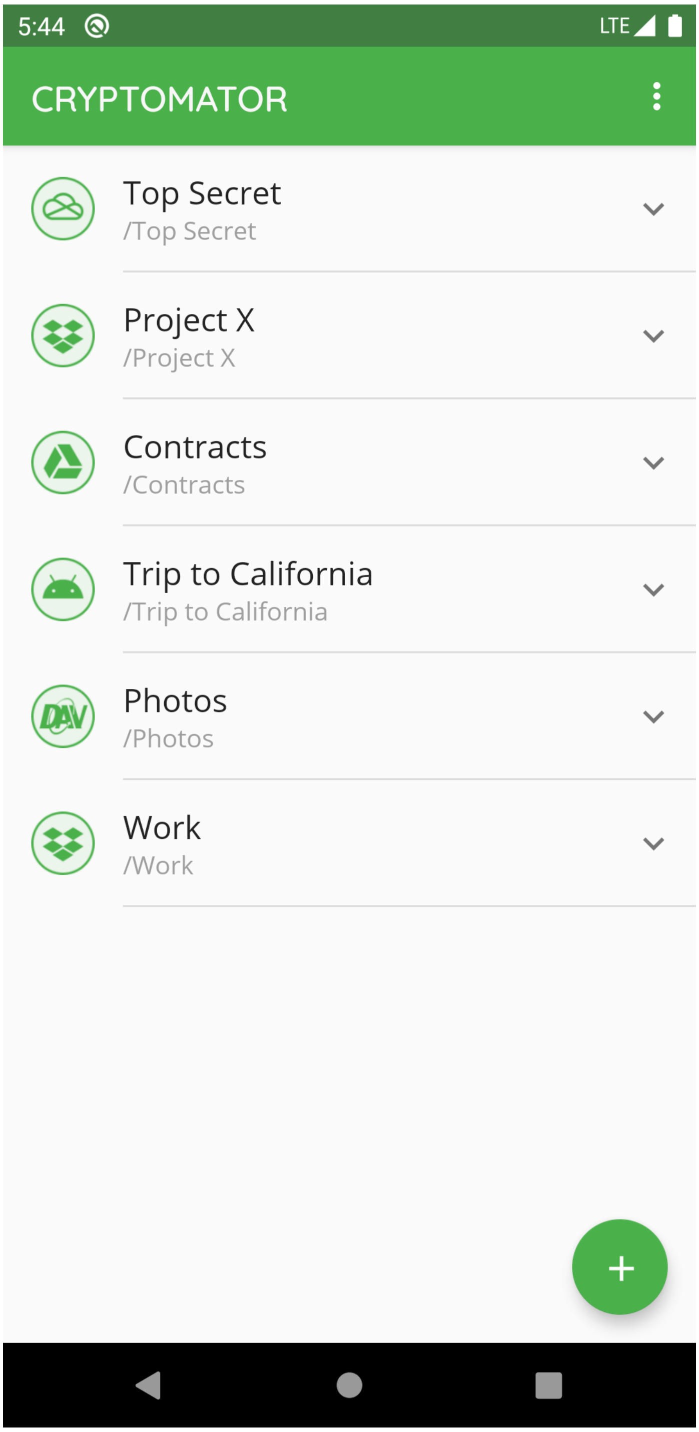
In the first step, please choose the folder in which the vault is located. This folder name is the same as the vault name (in this example, our vault name is *test vault* so we select this folder).



Then choose the `masterkey.cryptomator` file.



Now the vault is added to the list of vaults. You will find it now on the start page of your Cryptomator app, where you can open your vault and optionally change settings. [documentation will follow]



Top Secret
/Top Secret

Project X
/Project X

Contracts
/Contracts

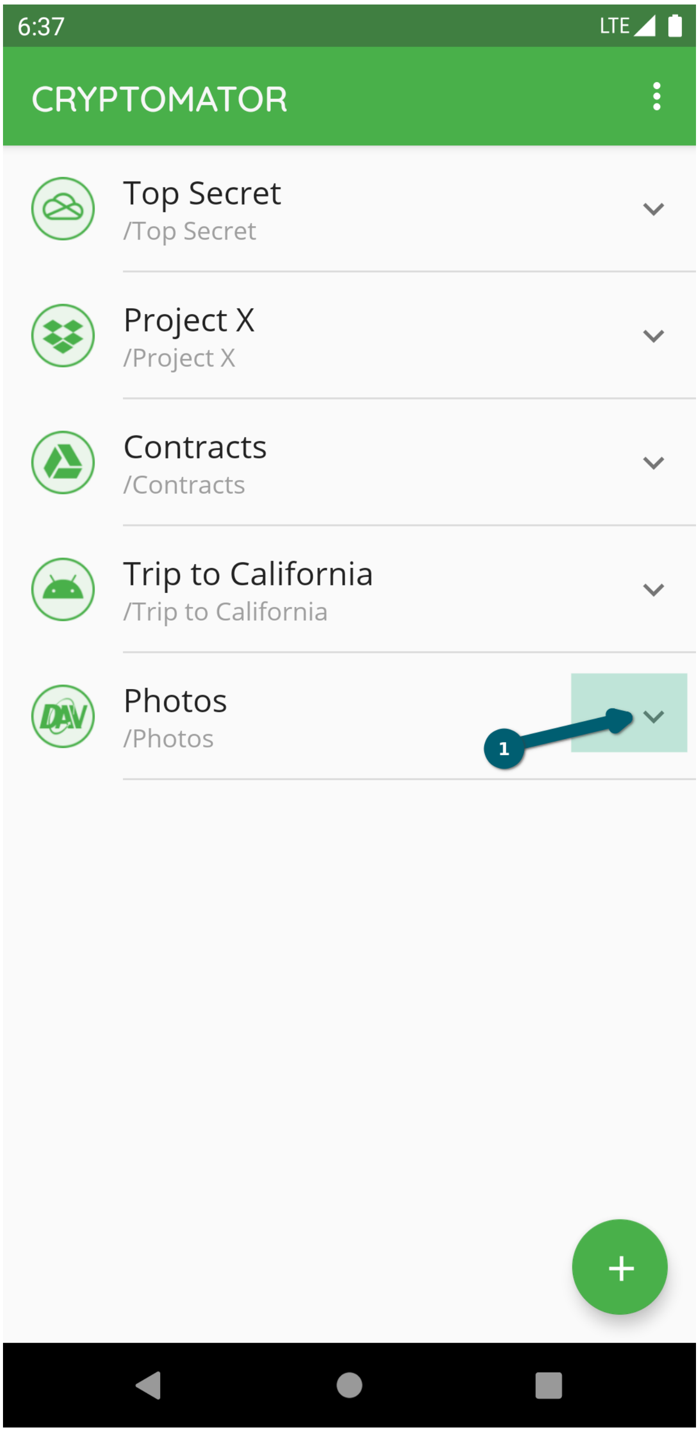
Trip to California
/Trip to California

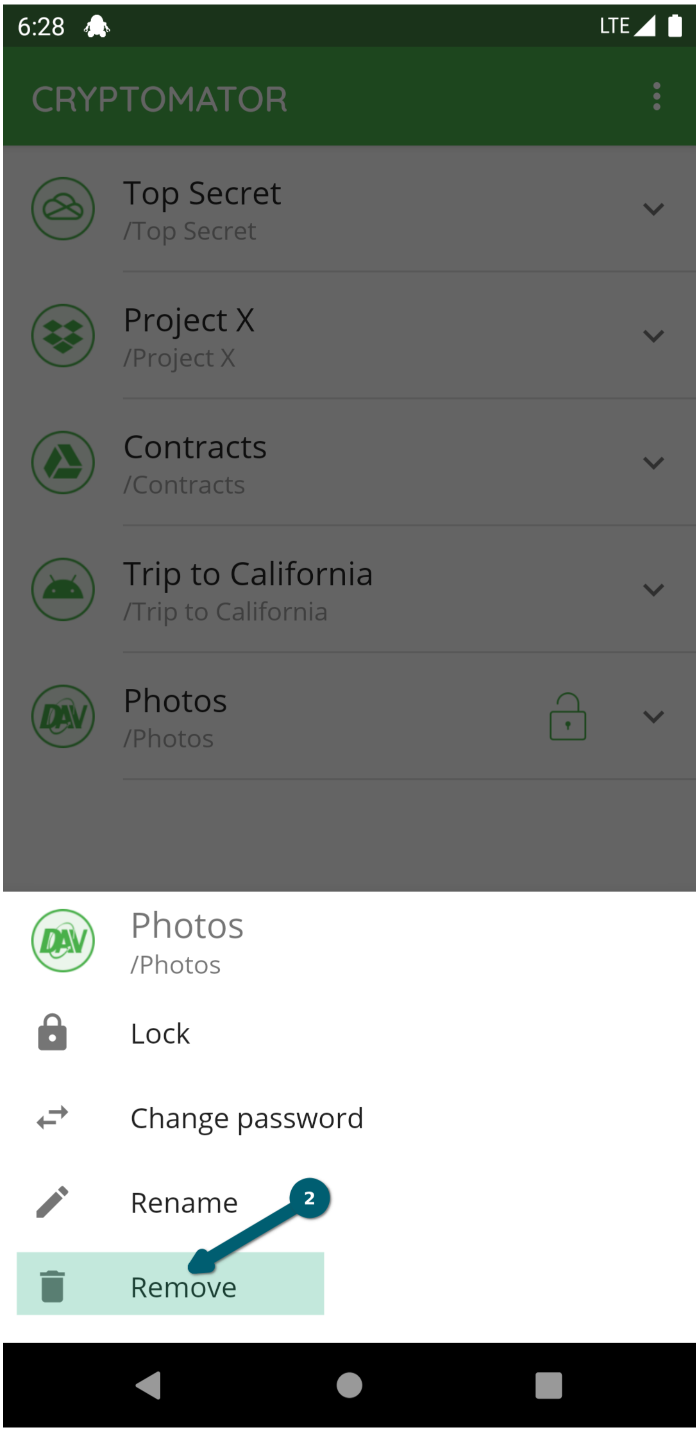
Photos
/Photos

Work
/Work

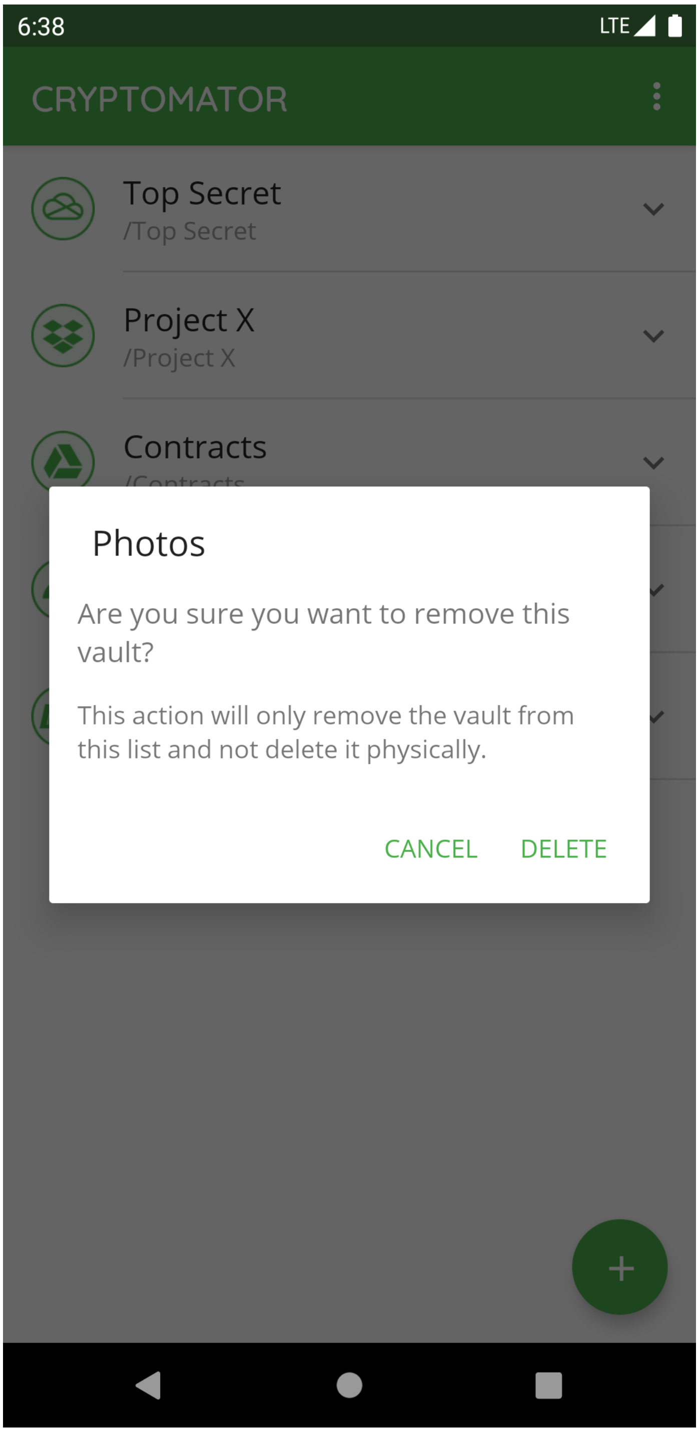
10.3 Remove Vaults

If you want a specific vault to stop being displayed in Cryptomator, you select the V next to the vault and choose *Remove* .





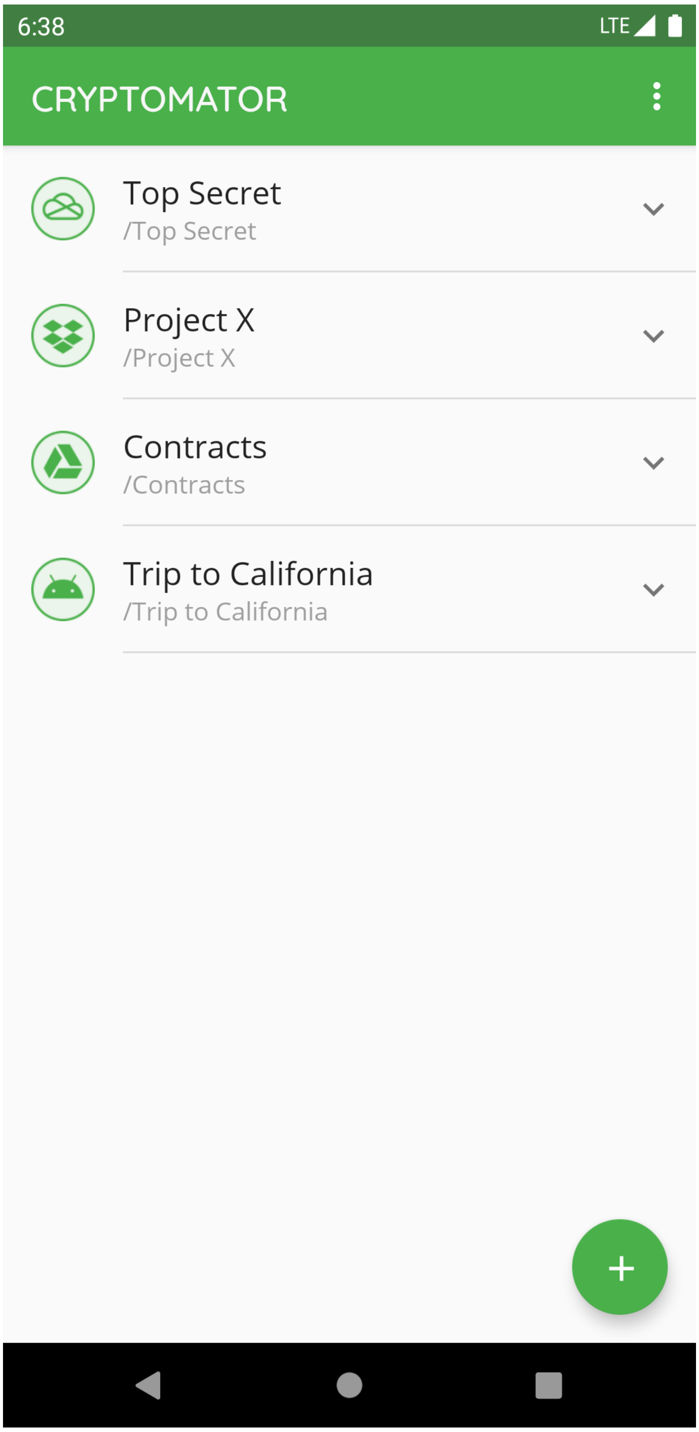
Confirm the deletion process using the `Delete` button.



Photos

Are you sure you want to remove this vault?

This action will only remove the vault from this list and not delete it physically.



6:38

CRYPTOMATOR

Top Secret
/Top Secret

Project X
/Project X

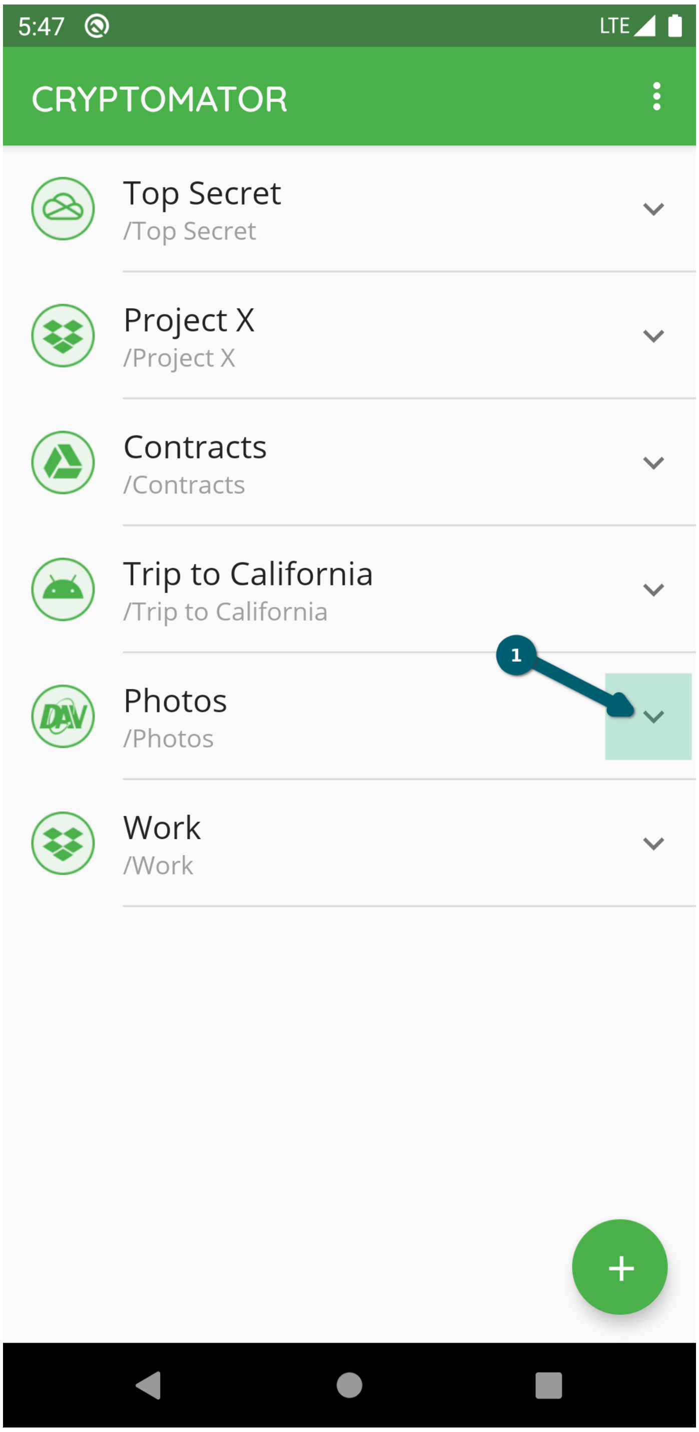
Contracts
/Contracts

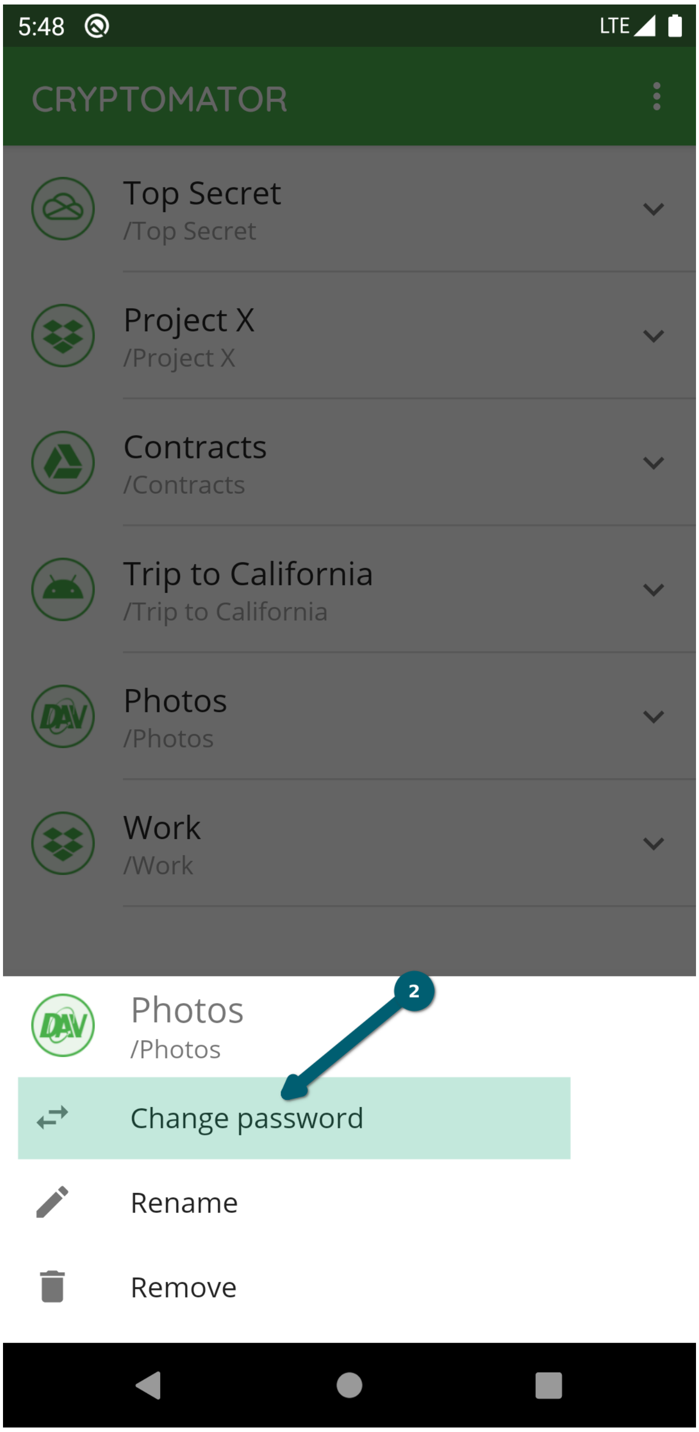
Trip to California
/Trip to California

Note: By removing a vault, it is only removed from the list but not deleted in the cloud. You can re-add the vault afterwards.

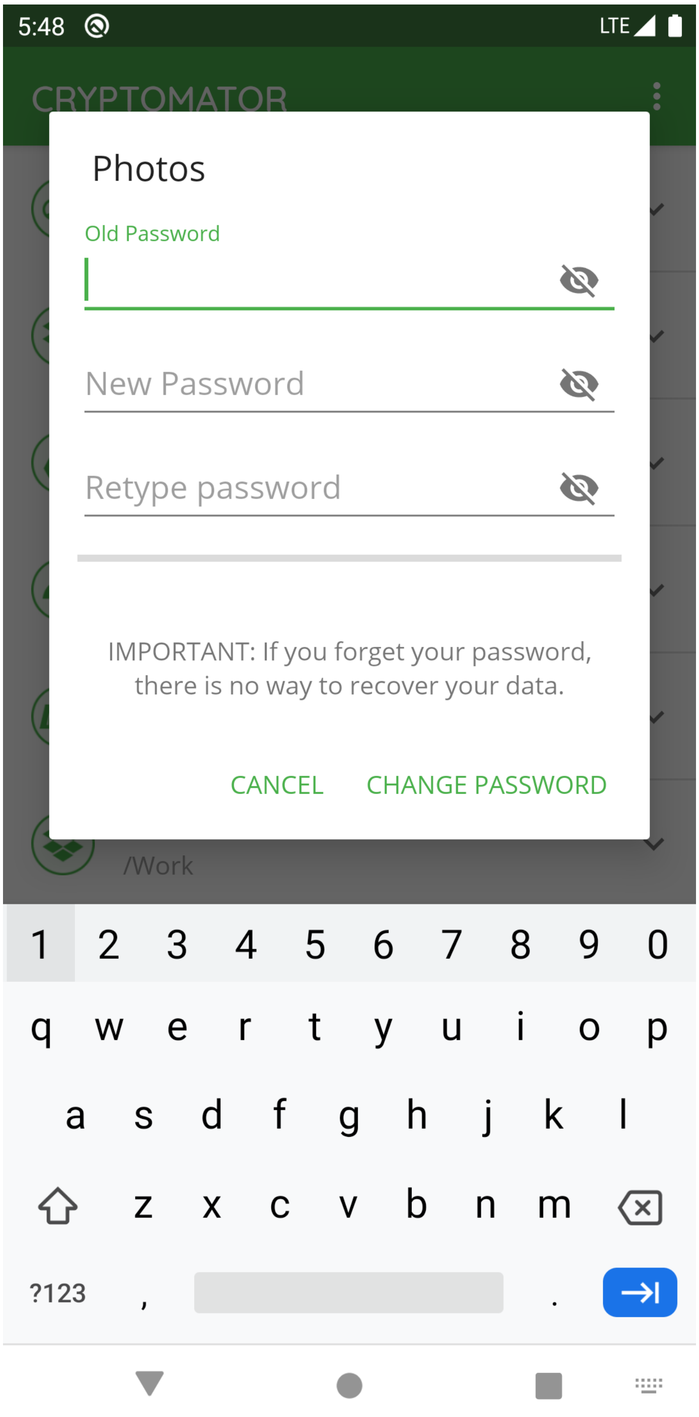
10.4 Change Vault Password

If you want change the password of a specific vault in Cryptomator, you select the V next to the vault and choose *Change password* .





Enter the old password and choose a **secure** new one. Basically, you have the whole Unicode for choosing a password including non-printable characters.



Photos

Old Password

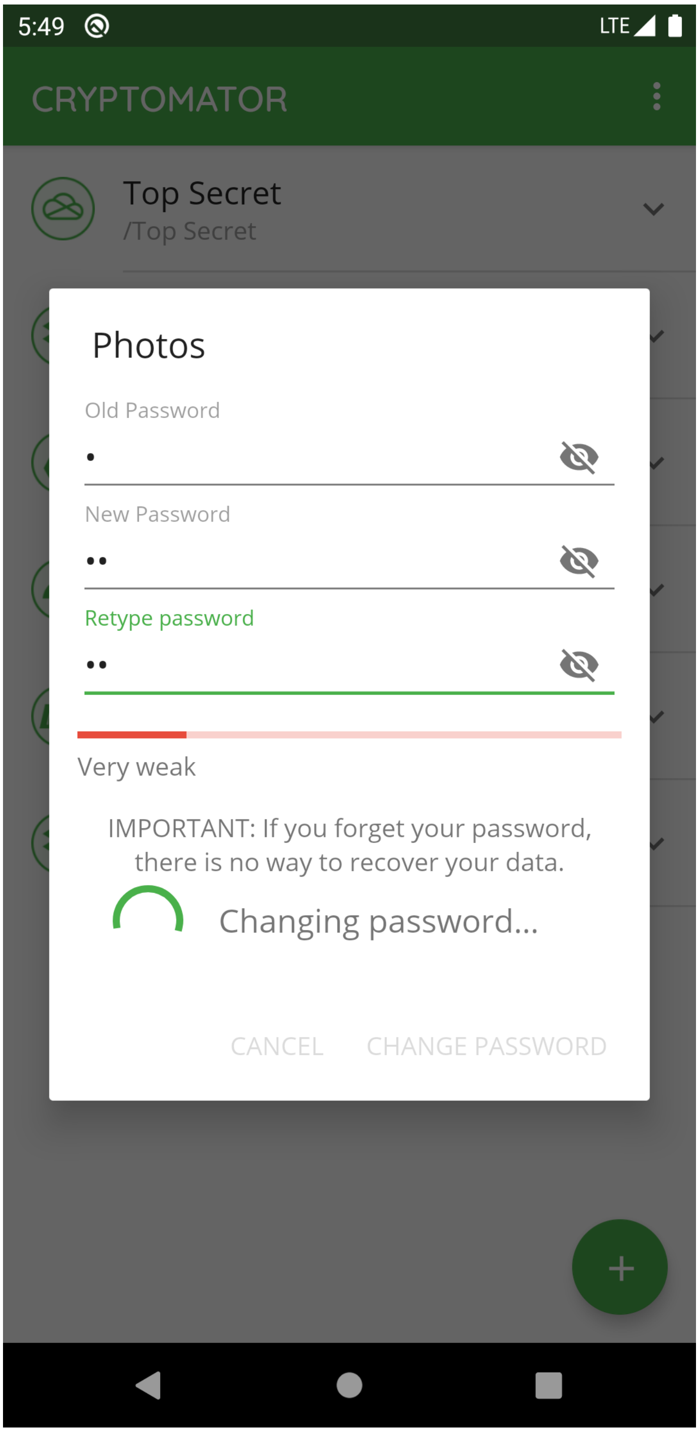
New Password

Retype password

IMPORTANT: If you forget your password, there is no way to recover your data.

Warning: You have to remember this password at all times because there is **no way to access your data if you forget your password**. Choose a *good password* to make your data secure.

Start the process using the `CHANGE PASSWORD` button.



Photos

Old Password: •

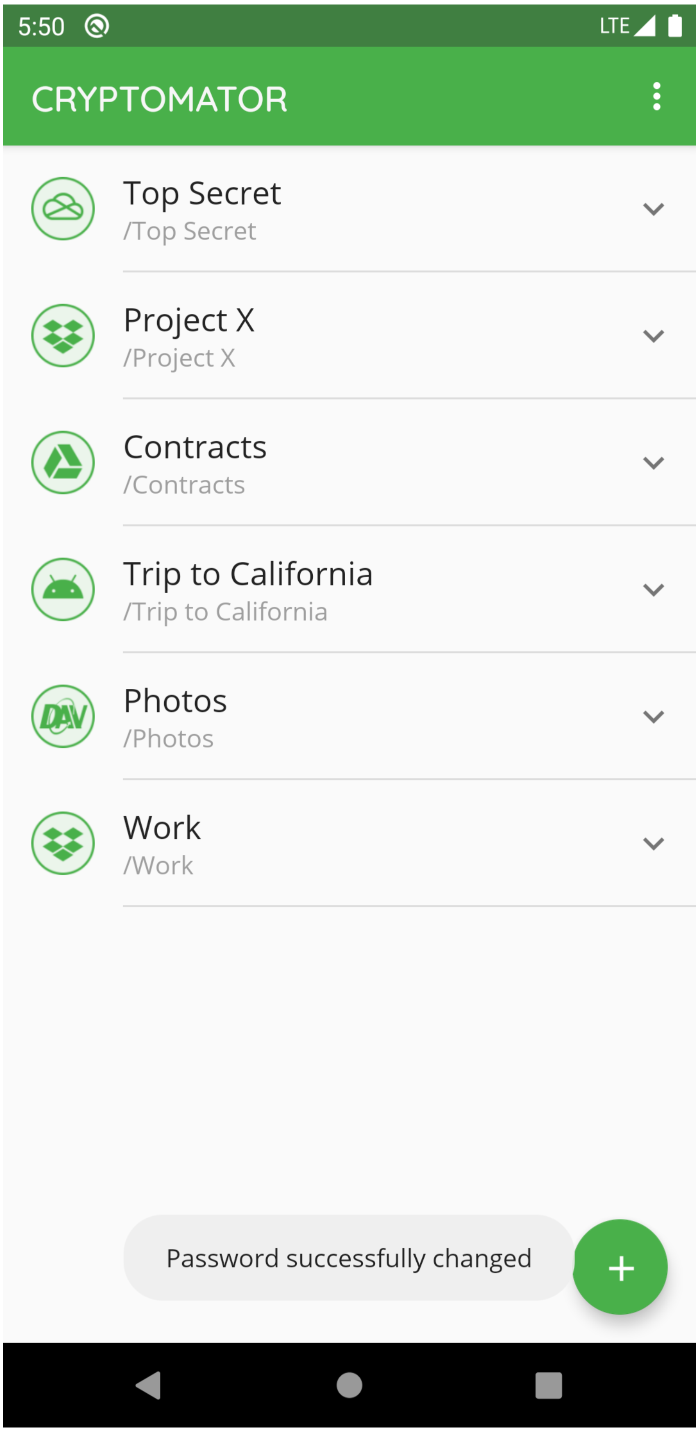
New Password: ••

Retype password: ••

Very weak

IMPORTANT: If you forget your password, there is no way to recover your data.

Changing password...



Top Secret
/Top Secret

Project X
/Project X

Contracts
/Contracts

Trip to California
/Trip to California

Photos
/Photos

Work
/Work

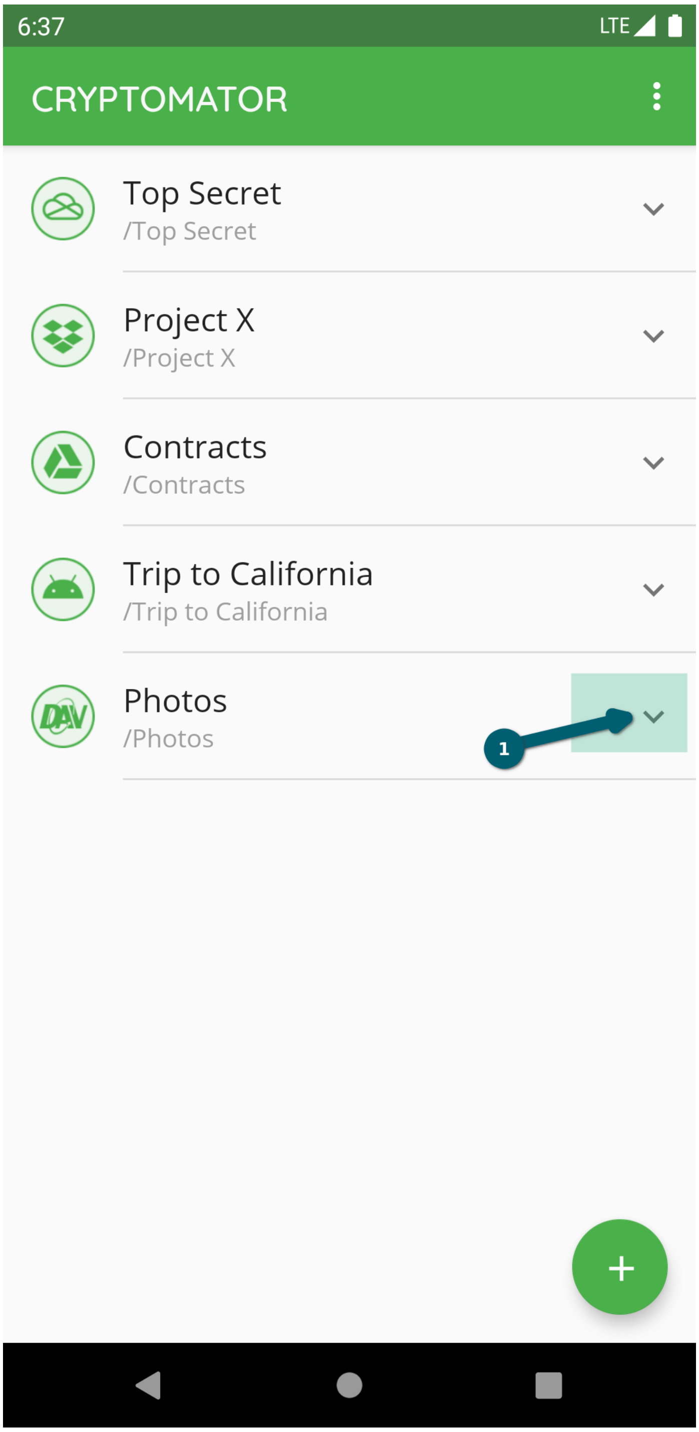
Password successfully changed

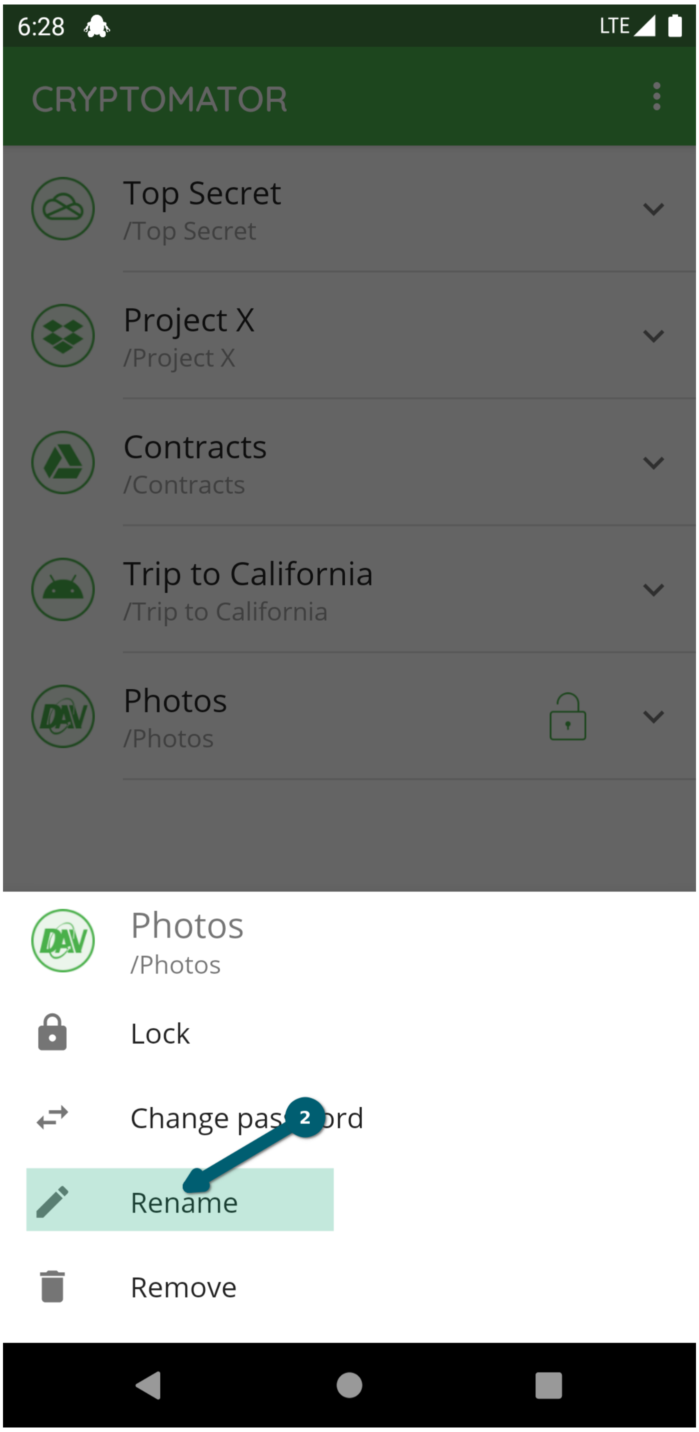
Note: The password is used to derive a KEK, which is then used to encrypt futher keys. The KEK changes, but the keys encrypted with the KEK will stay the same. The actual files will not get re-encrypted, meaning you can not upgrade a weak passphrase to a stronger one once the data has been synced to a service that allows recovery of older versions of the masterkey file.

If you like to encrypt your vault files with a new, stronger password, you need to create a new vault and copy the data from the old to the new one. Make sure to wipe all backups of the old vault afterwards.

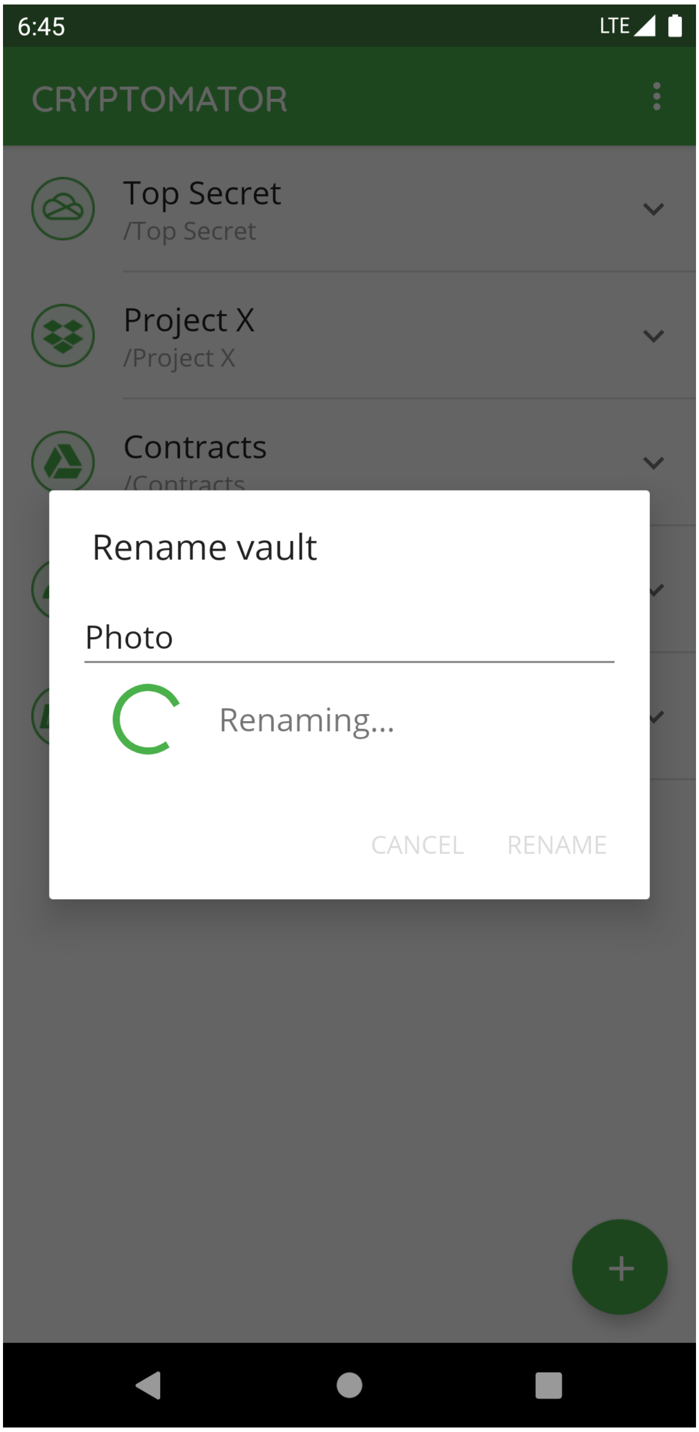
10.5 Rename Vault

If you want to change the name of a specific vault in Cryptomator, you select the `V` next to the vault and choose *Rename* .





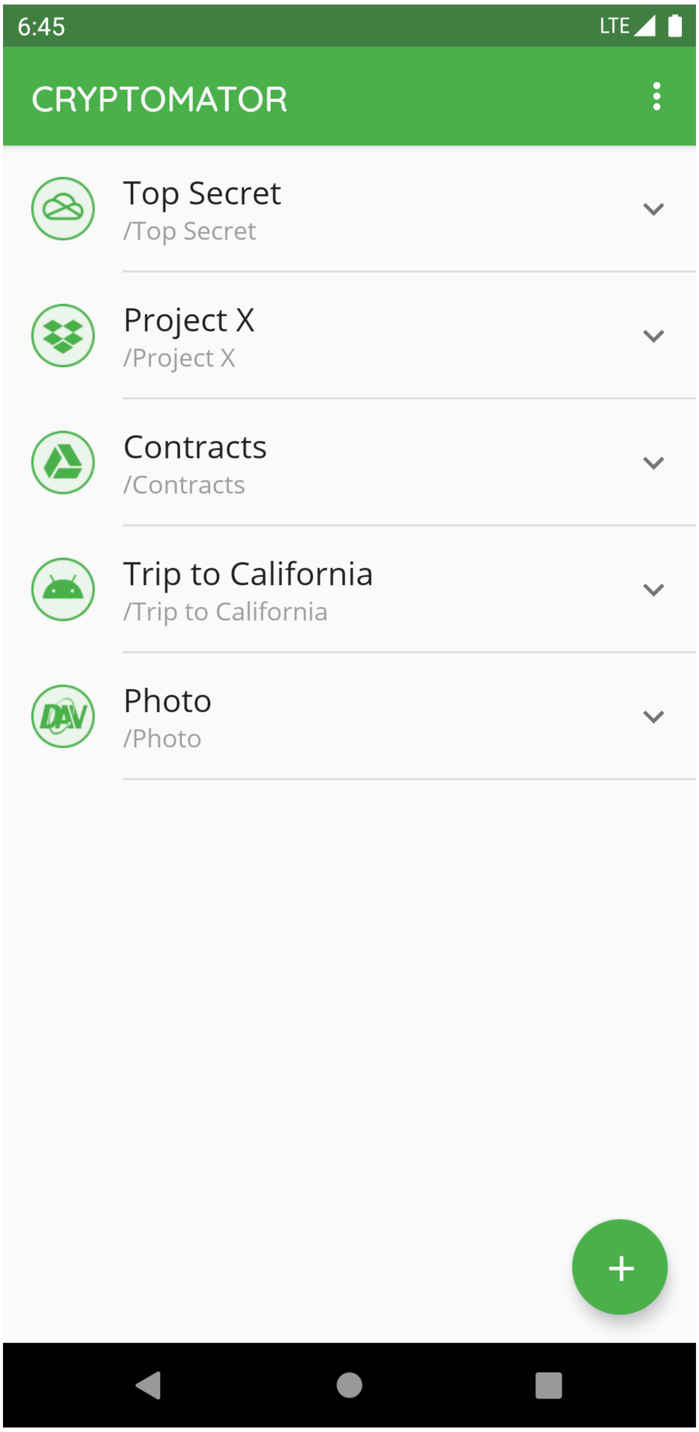
Choose a new name and confirm using the RENAME button.



Rename vault

Photo

Renaming...



Top Secret
/Top Secret

Project X
/Project X

Contracts
/Contracts

Trip to California
/Trip to California

Photo
/Photo

10.6 Change Vault Position

If you want to change the position of a specific vault in the vault list in Cryptomator, long-press on the vault and drag it to the desired position in the pressed state:

CHAPTER

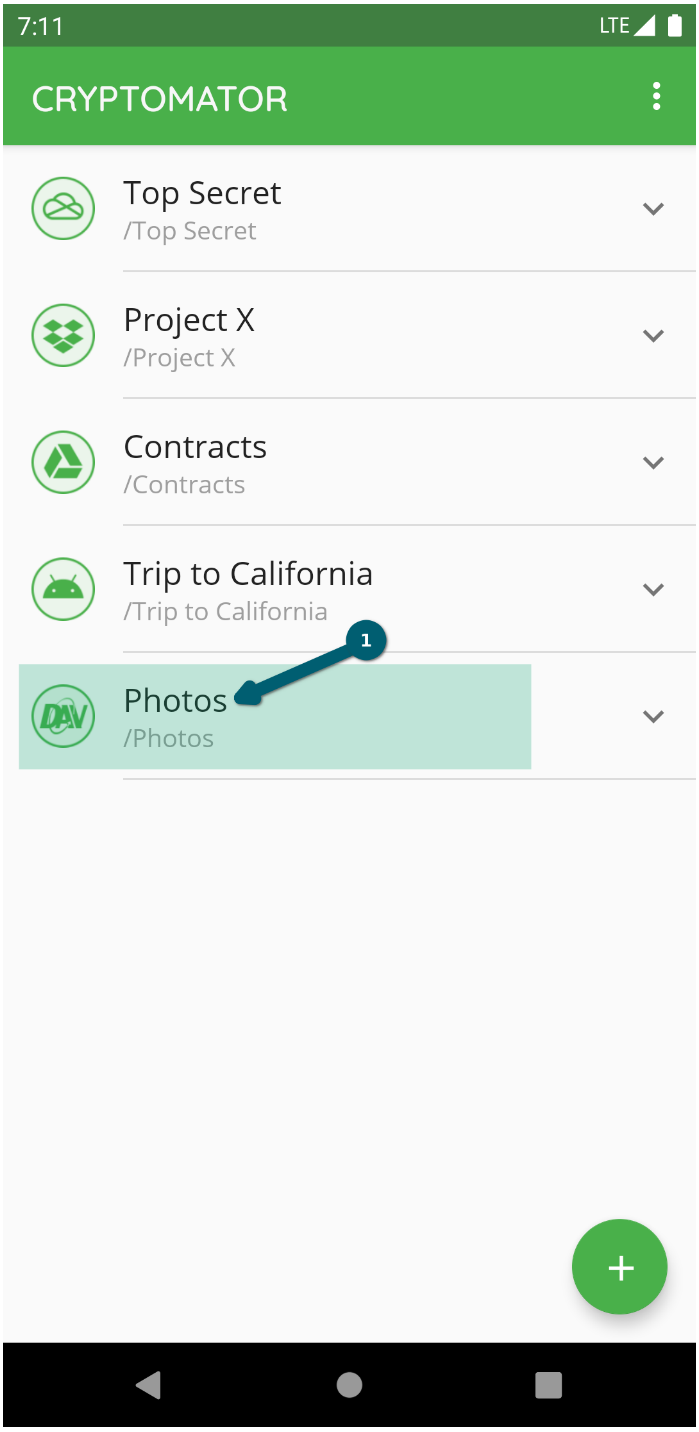
ELEVEN

WORKING WITH VAULTS

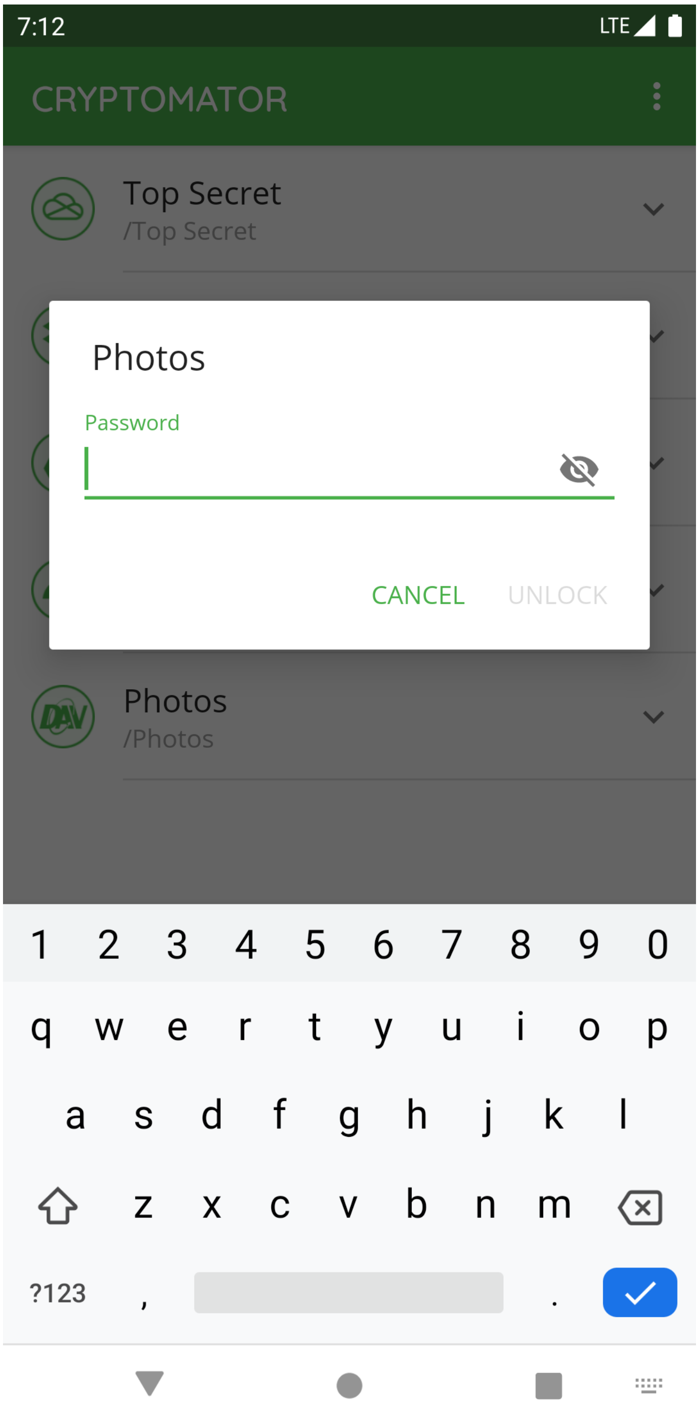
This section shows you how to work with a vault like view its content, move files or access it with other applications.

11.1 Unlock Vault

If you want to access the data inside a vault, you have to unlock it by selecting it.



In the next step, you have to unlock the vault using the password. If the device supports fingerprint authentication and you've activated it in the settings for this vault, you will be prompted to unlock using fingerprint. How to setup fingerprint authentication will be documented in a separate chapter.



7:12

CRYPTOMATOR

Top Secret

/Top Secret

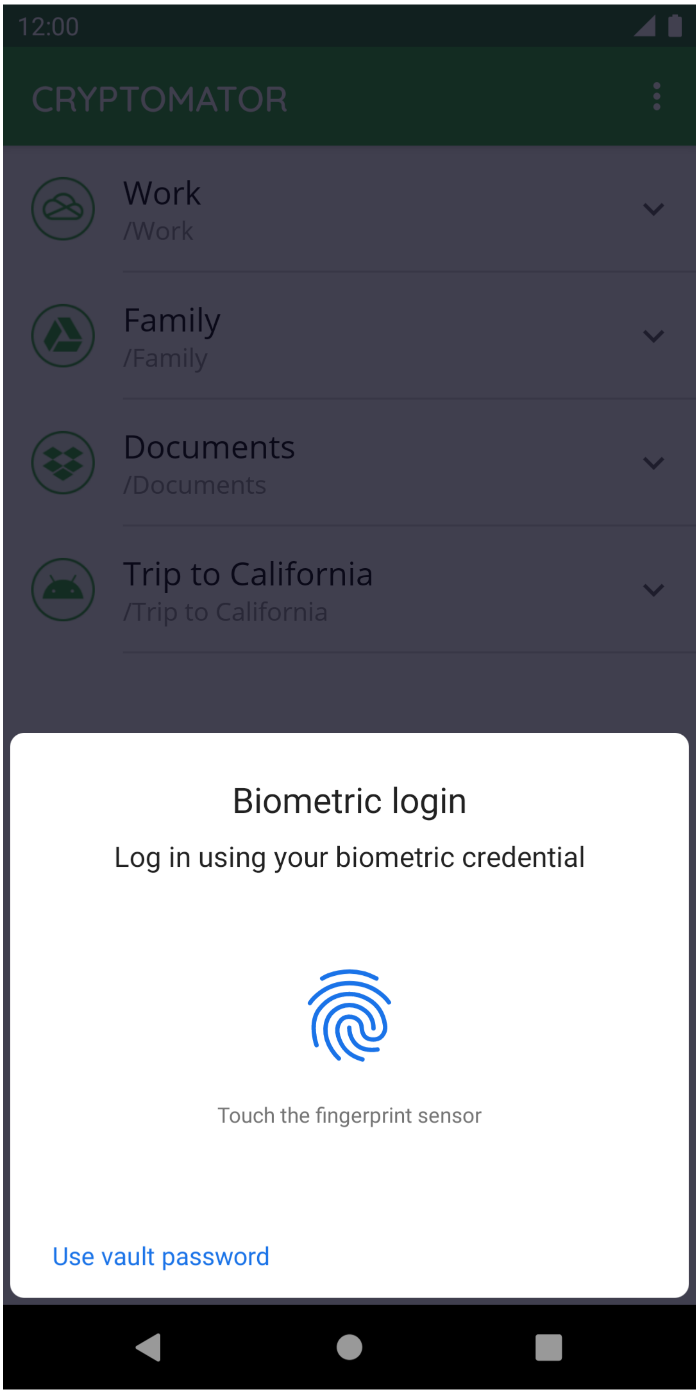
Photos

Password

CANCEL UNLOCK

Photos

/Photos



12:00

CRYPTOMATOR

Work
/Work

Family
/Family

Documents
/Documents

Trip to California
/Trip to California

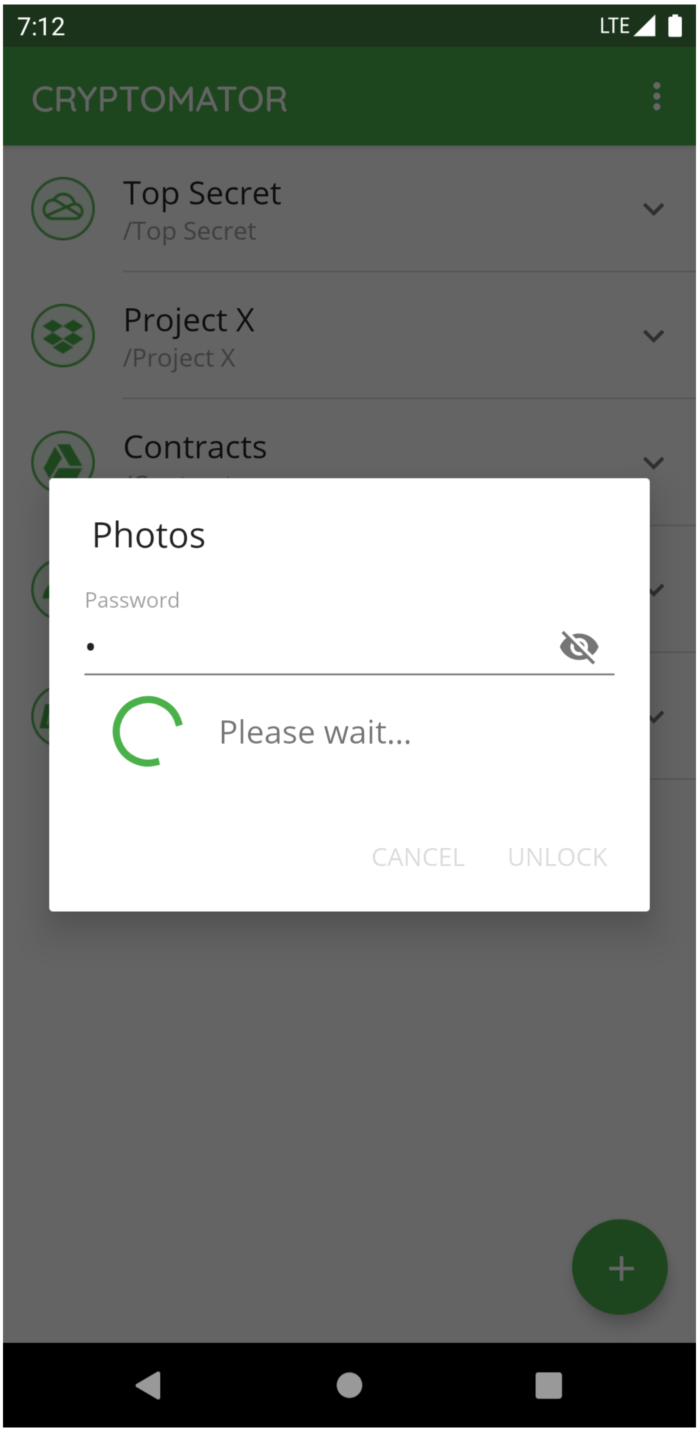
Biometric login

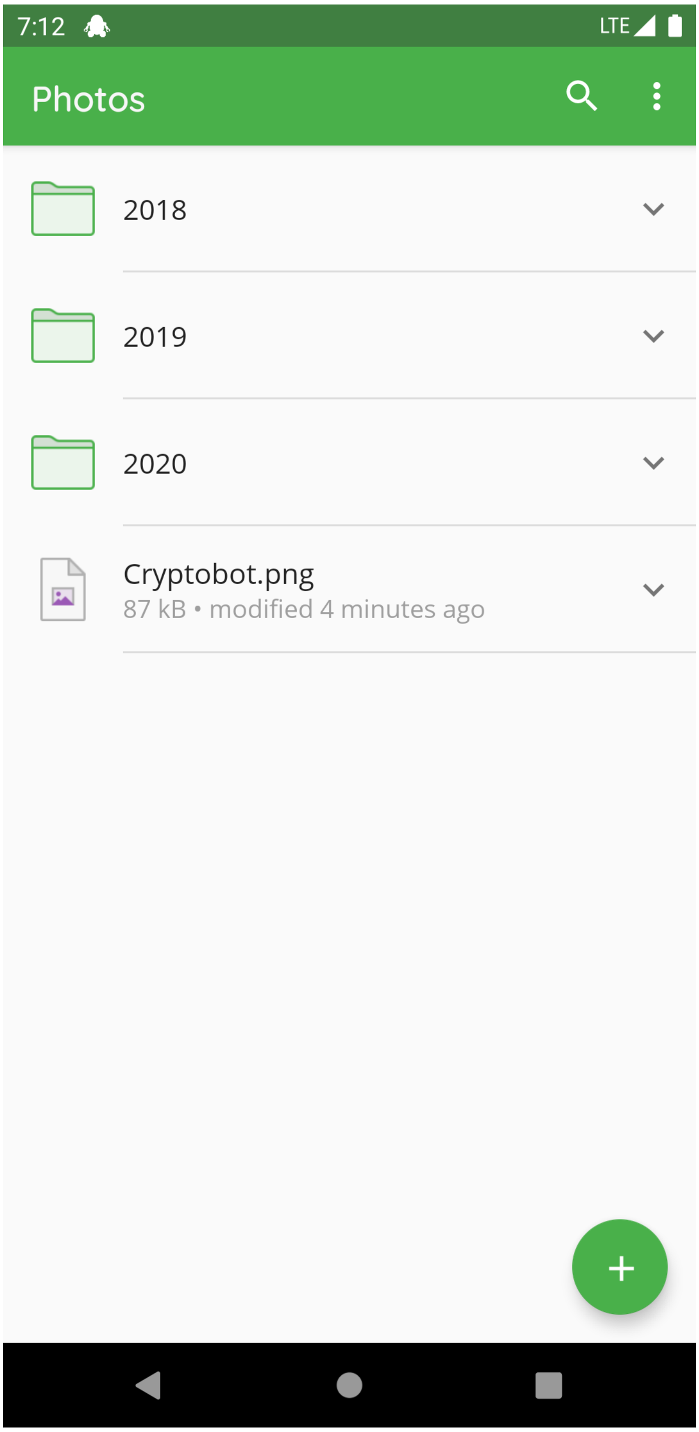
Log in using your biometric credential

Touch the fingerprint sensor

Use vault password

After providing the credentials, the vault gets unlocked and opened.


7:12
LTE
CRYPTOMATOR
Top Secret
/Top Secret
Project X
/Project X
Contracts
Photos
Password
•
Please wait...
CANCEL
UNLOCK

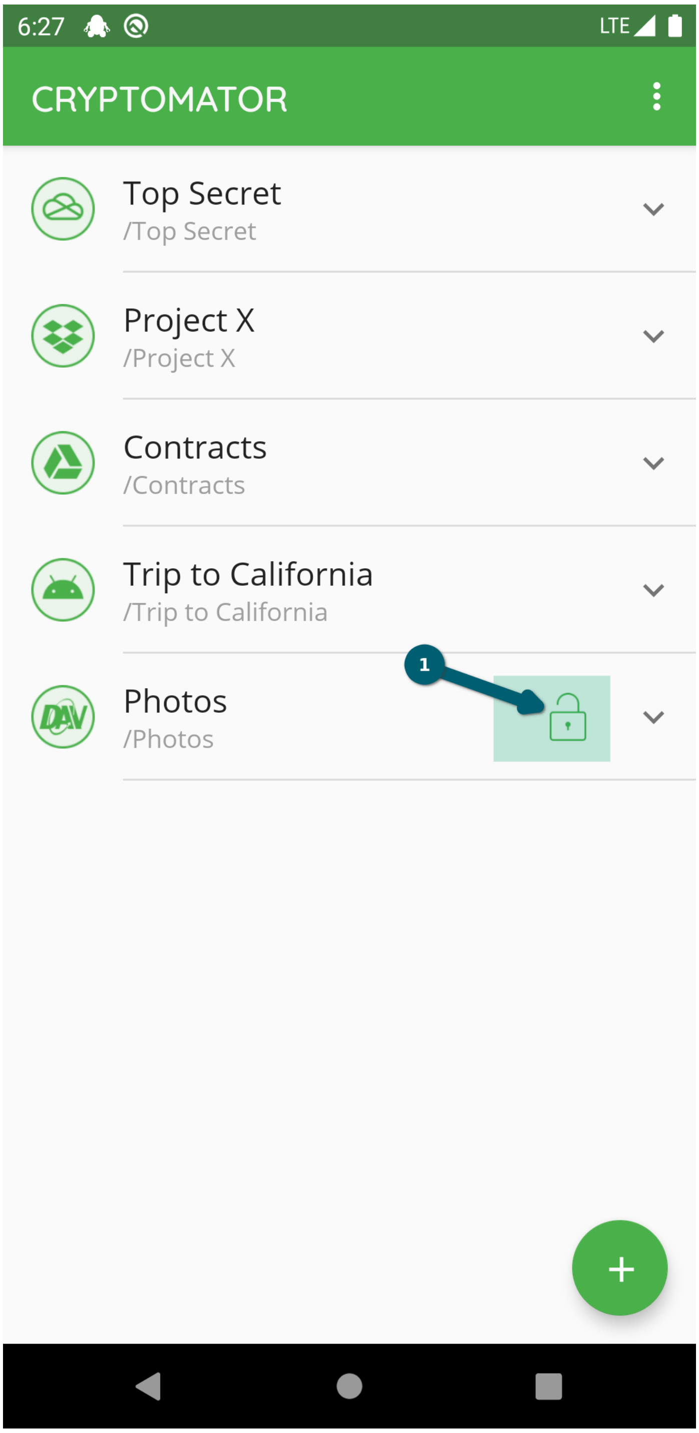


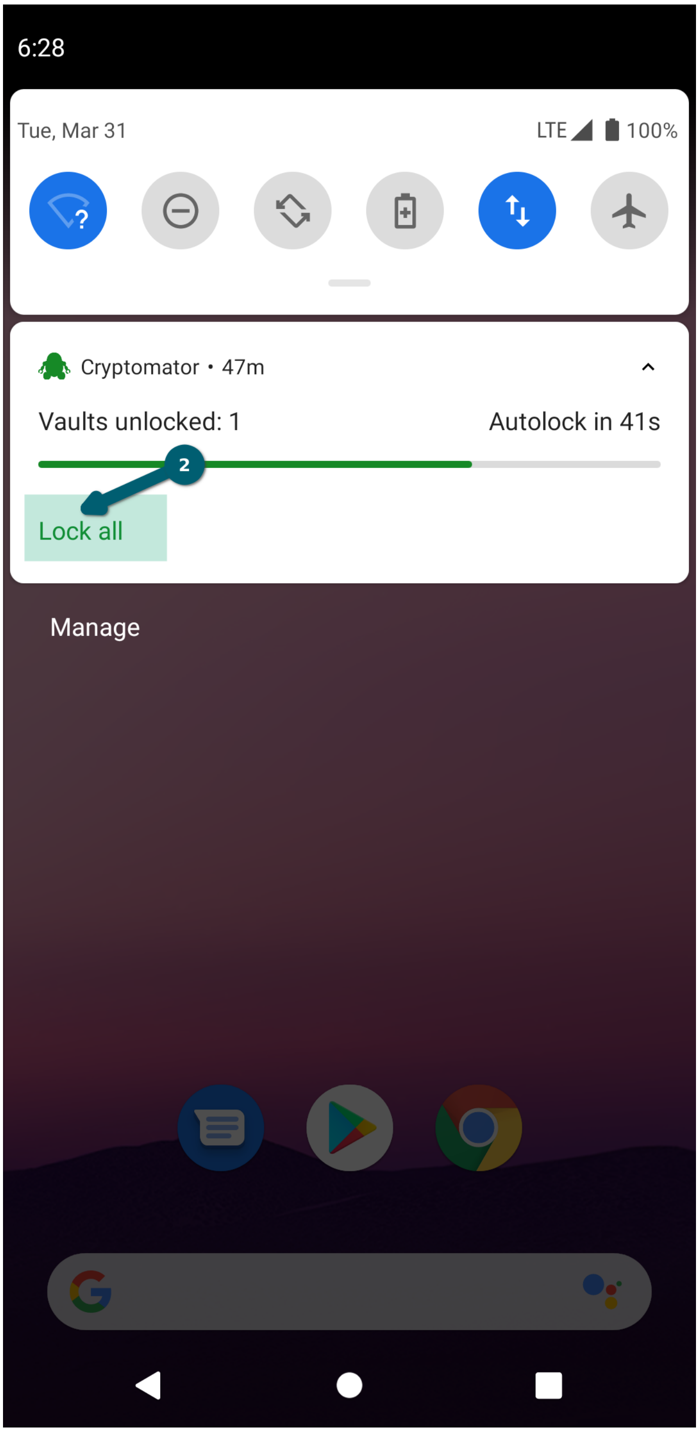
You’re now able to edit the content of the vault.

11.2 Lock Vault

To lock an unlocked vault, there are several ways to do this:

- use the lock button in the vault list
- use the lock button in the notification
- use the lock button in the vault actions and





6:28

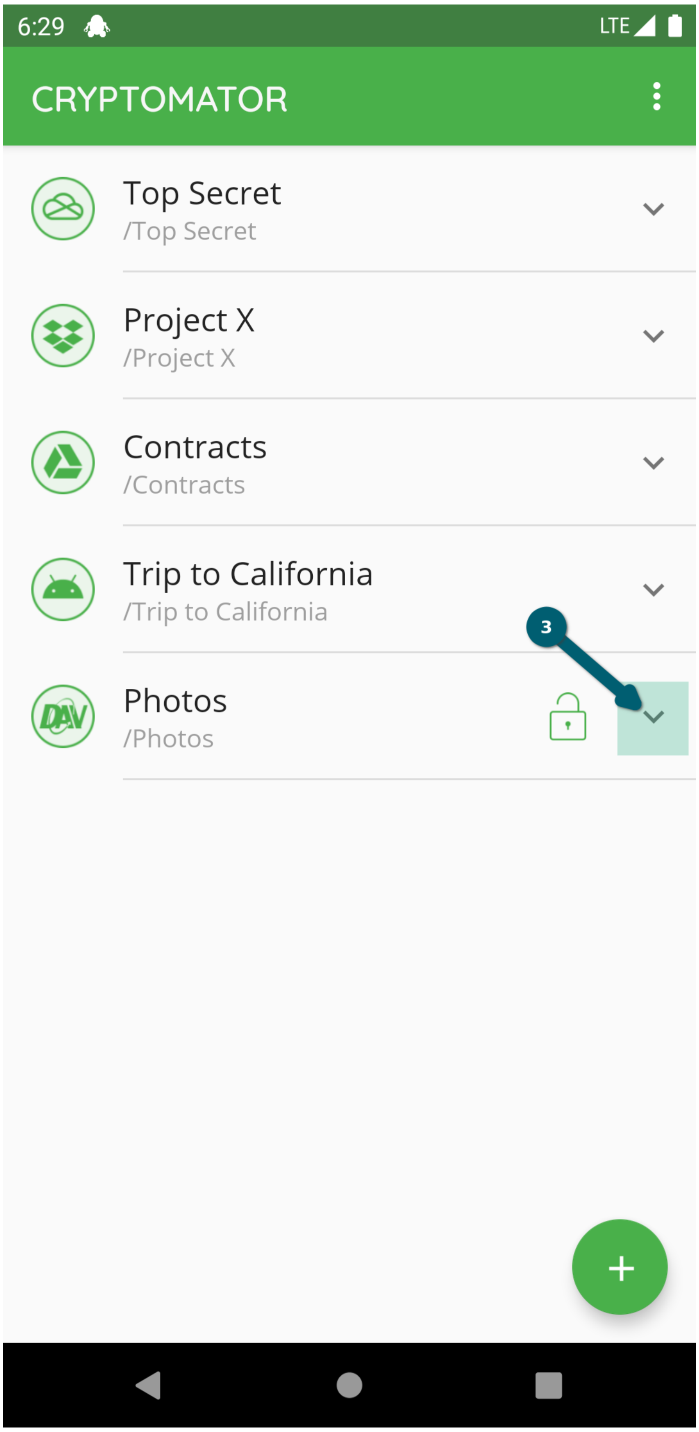
Tue, Mar 31

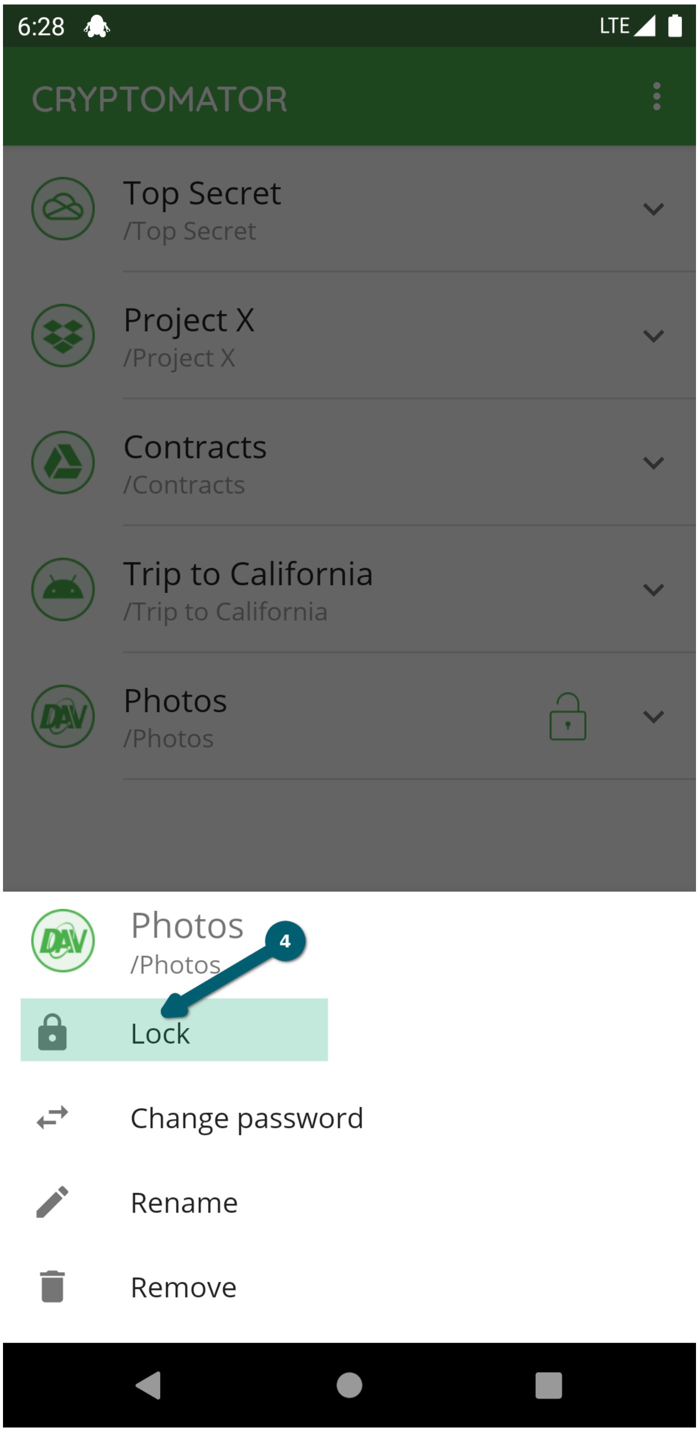
LTE 100%

Cryptomator • 47m

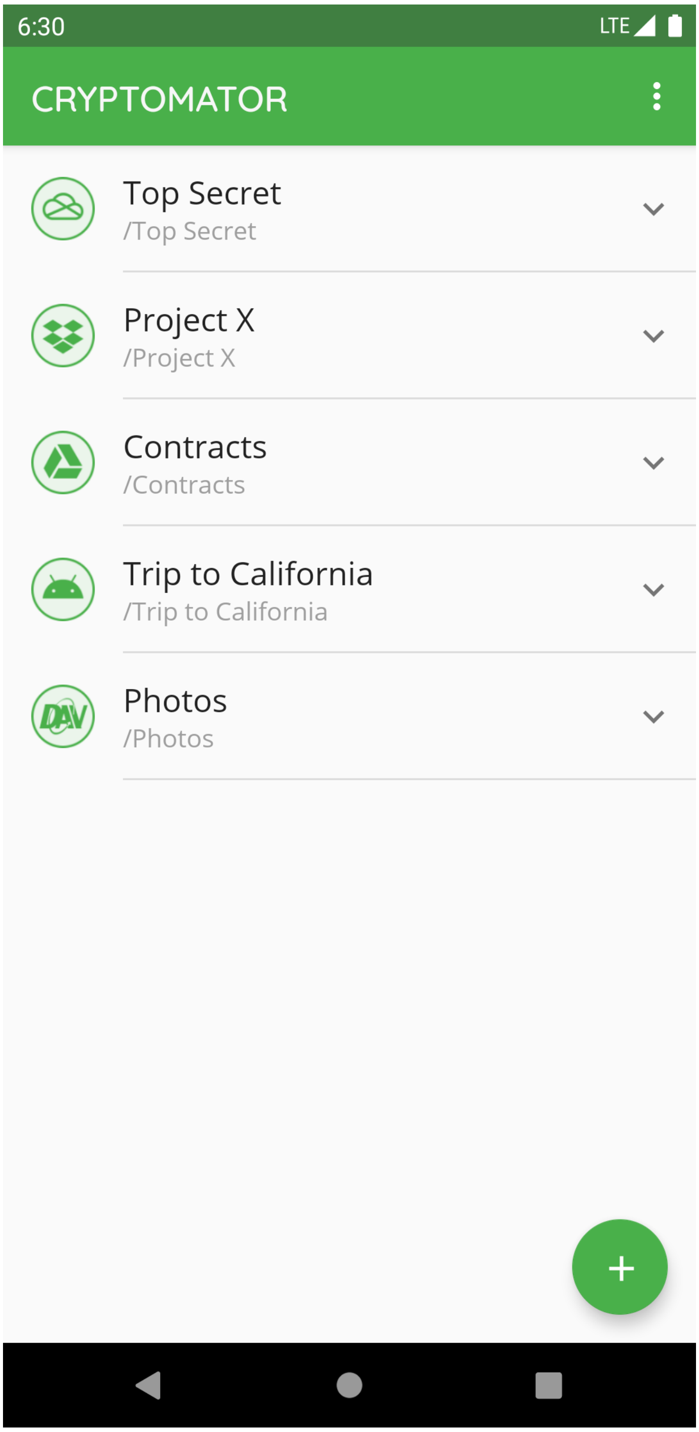
Vaults unlocked: 1

Autolock in 41s


6:29
LTE
CRYPTOMATOR
Top Secret
/Top Secret
Project X
/Project X
Contracts
/Contracts
Trip to California
/Trip to California
3
Photos
/Photos
+



All of the possibilities will result in the locked vault.



6:30 LTE

CRYPTOMATOR

Top Secret
/Top Secret

Project X
/Project X

Contracts
/Contracts

Trip to California
/Trip to California

Photos
/Photos

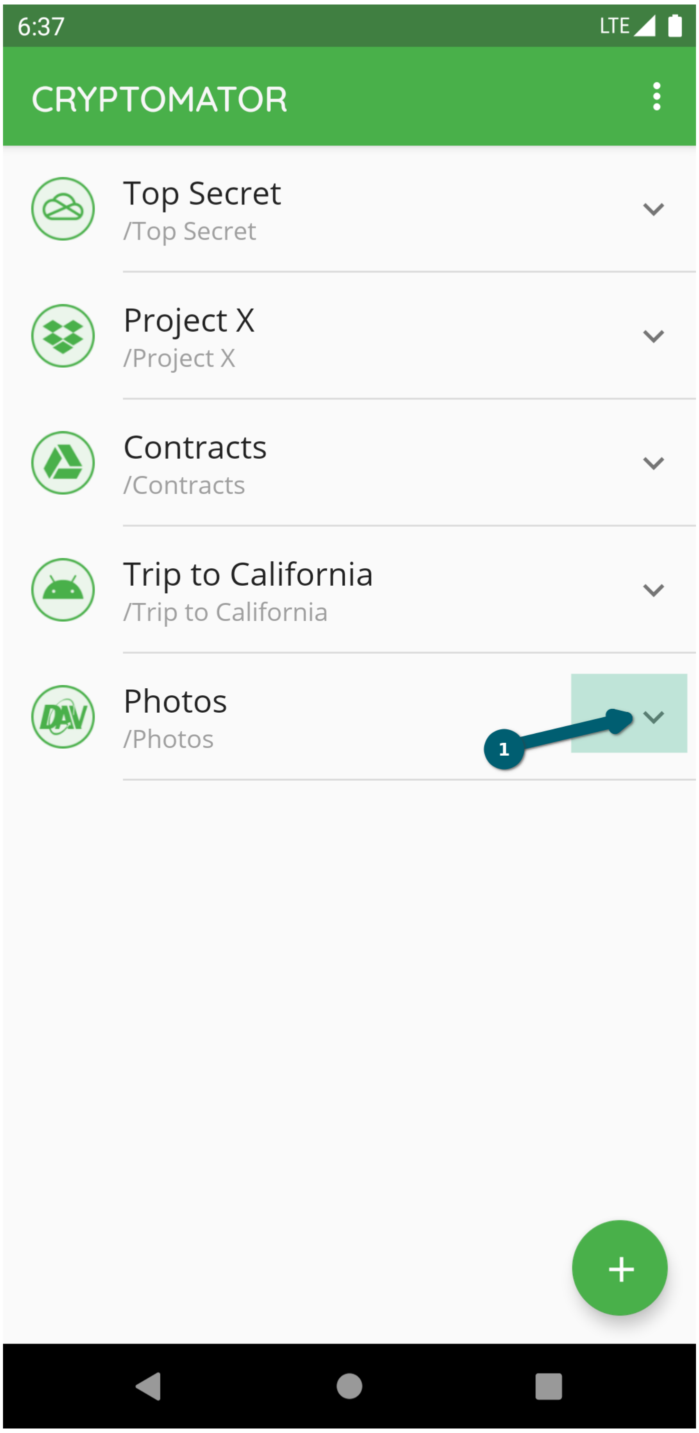
Note: The auto-lock timeout specified in the settings will lock the vault if Cryptomator is in background. Furthermore if not changed in settings, the vault gets locked if the screen turns off.

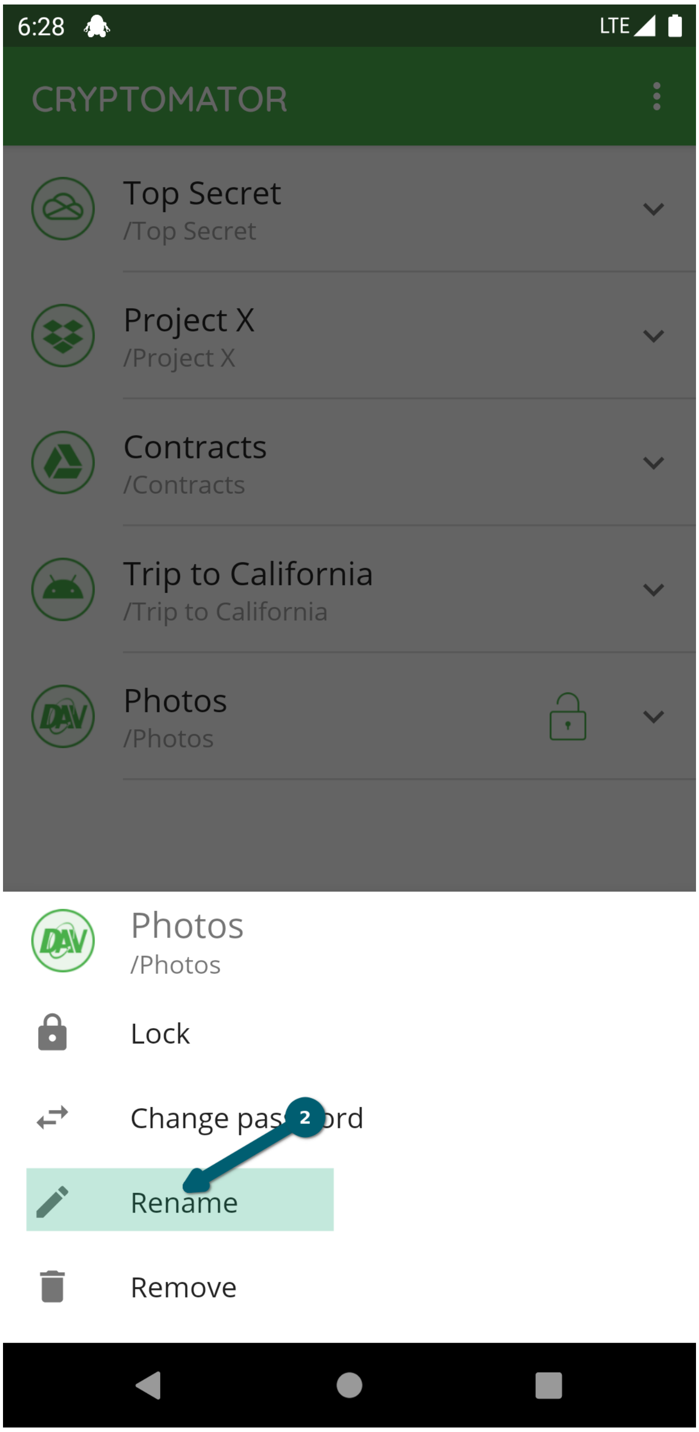
11.3 View and Edit File

Start the view and edit process by clicking on a file. Finish the editing or viewing using the back button of the device until you're back in Cryptomator. If the content has changed, the upload process starts.

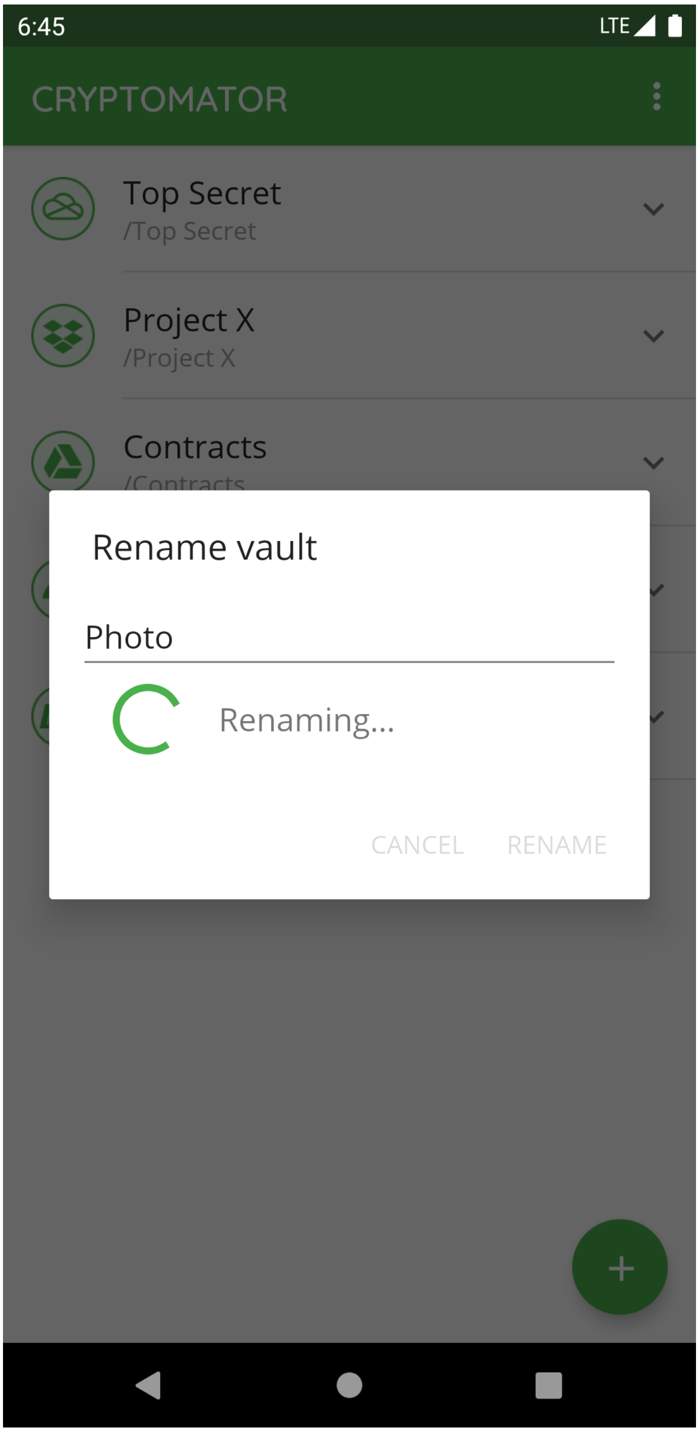
11.4 Rename File or Folder

To change the name of a specific file or folder in Cryptomator, you select the `V` next to the file or folder and choose *Rename* .





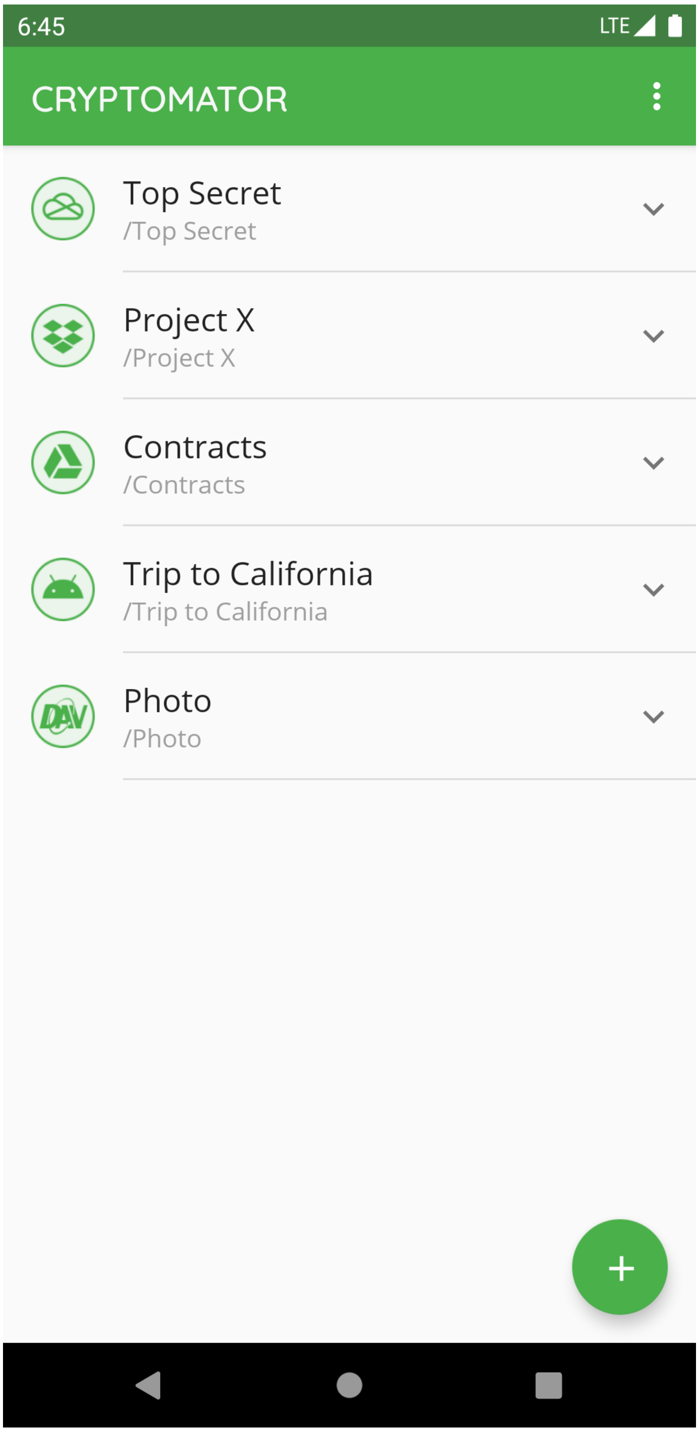
Choose a new name and confirm using the `RENAME` button.



Rename vault

Photo

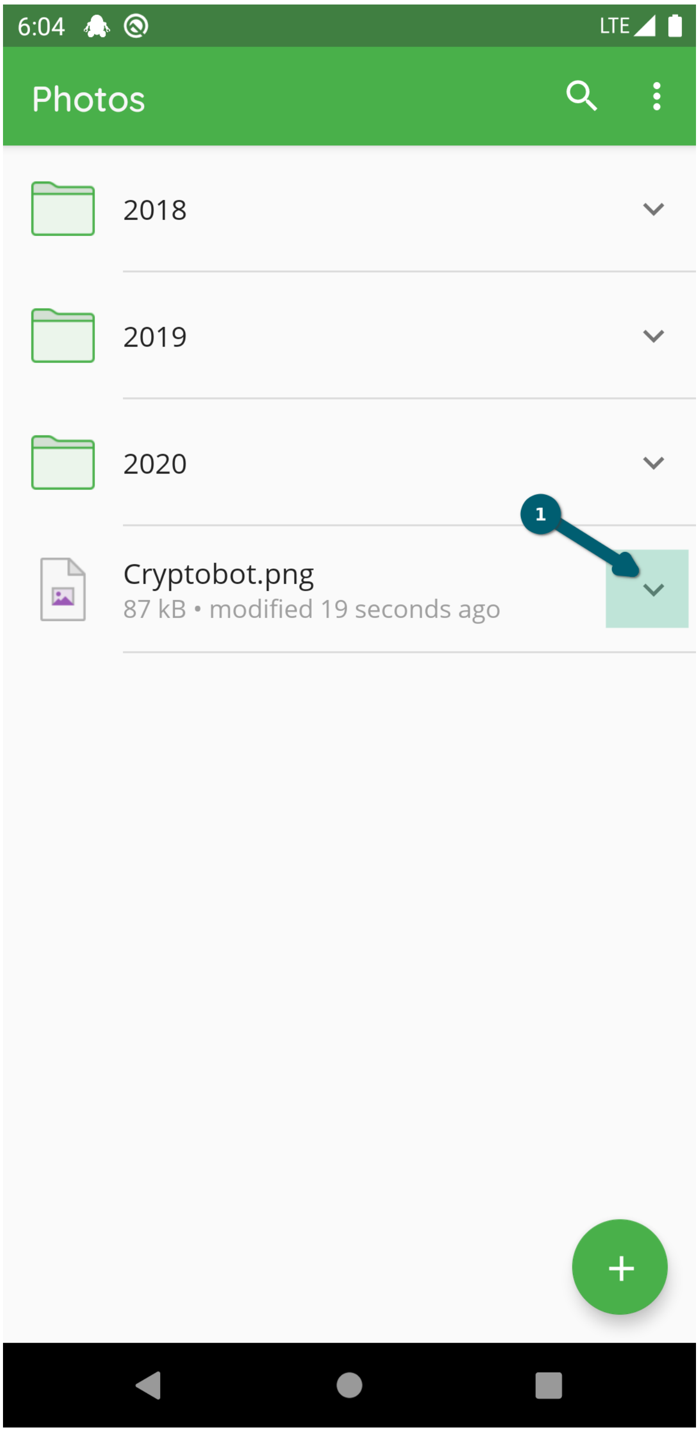
Renaming...

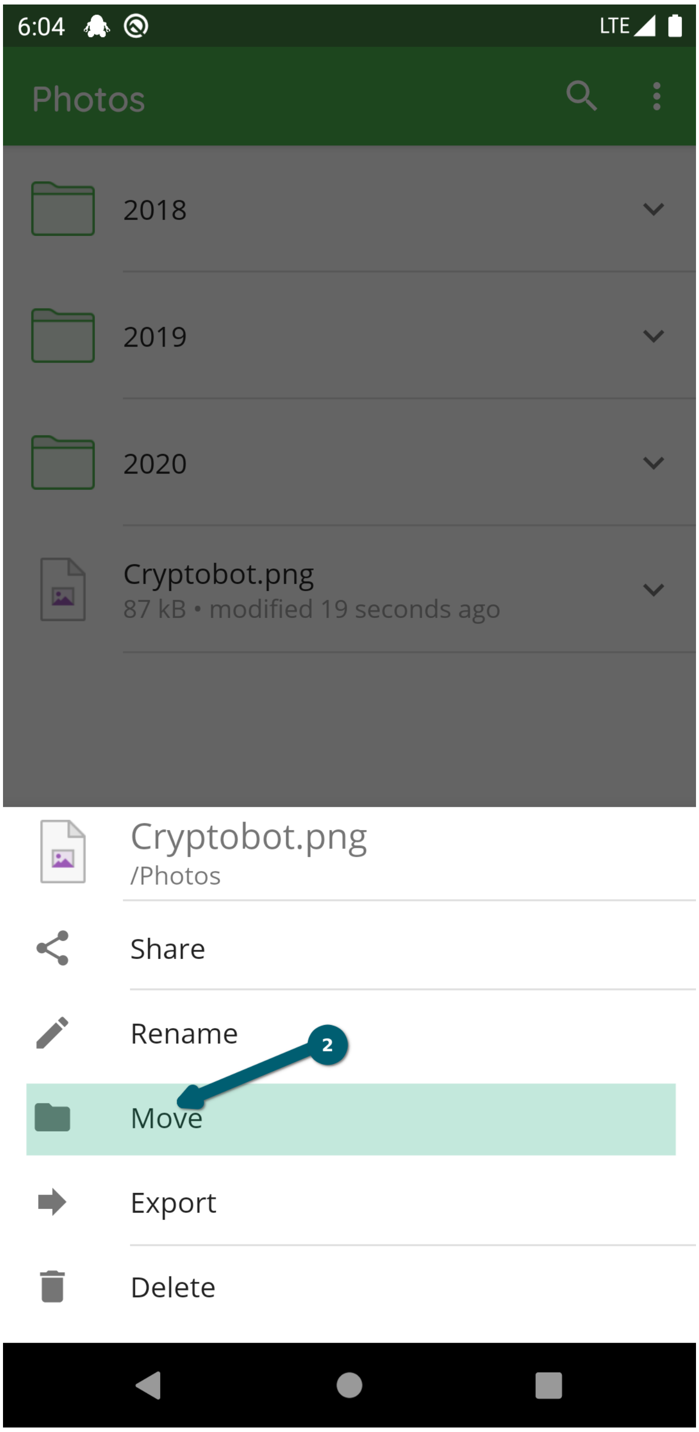


6:45
LTE
CRYPTOMATOR
Top Secret
/Top Secret
Project X
/Project X
Contracts
/Contracts
Trip to California
/Trip to California
Photo
/Photo
+

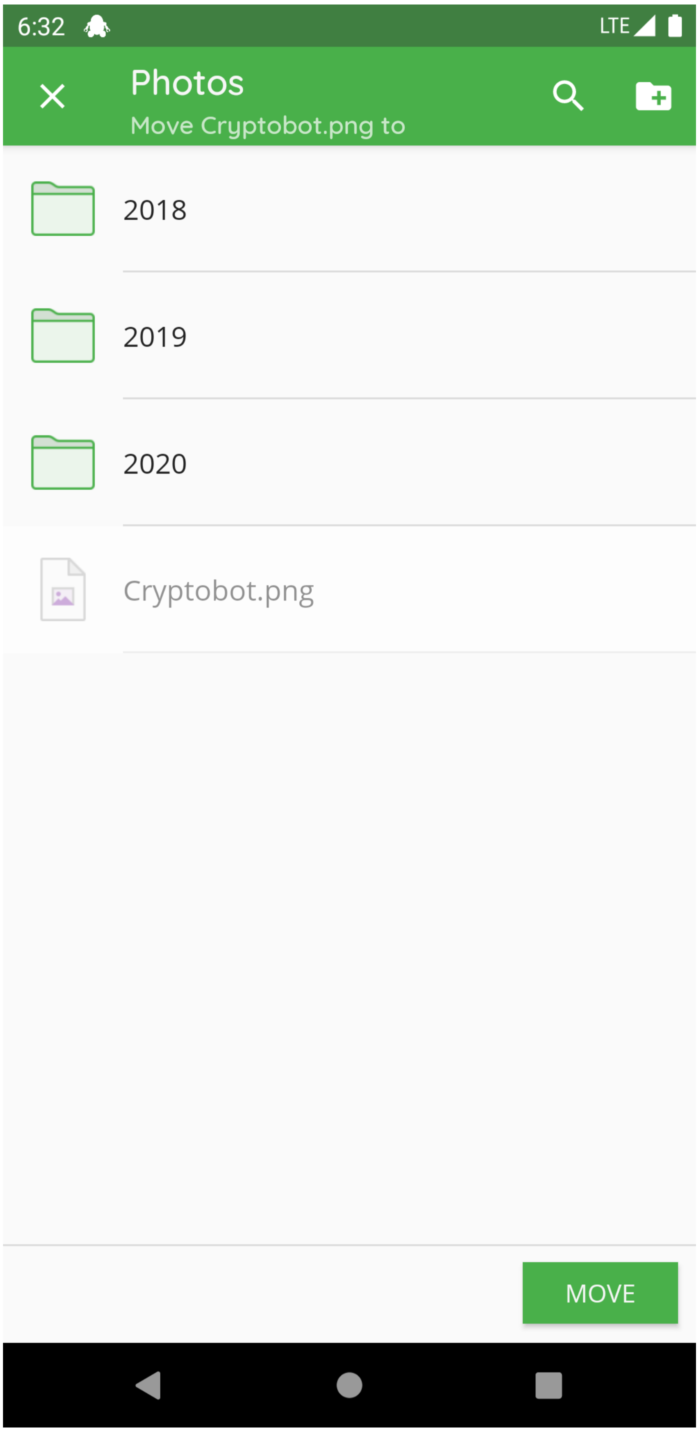
11.5 Move File or Folder

To move a file or a folder into another folder, you select the V next to the file or folder and choose *Move* .

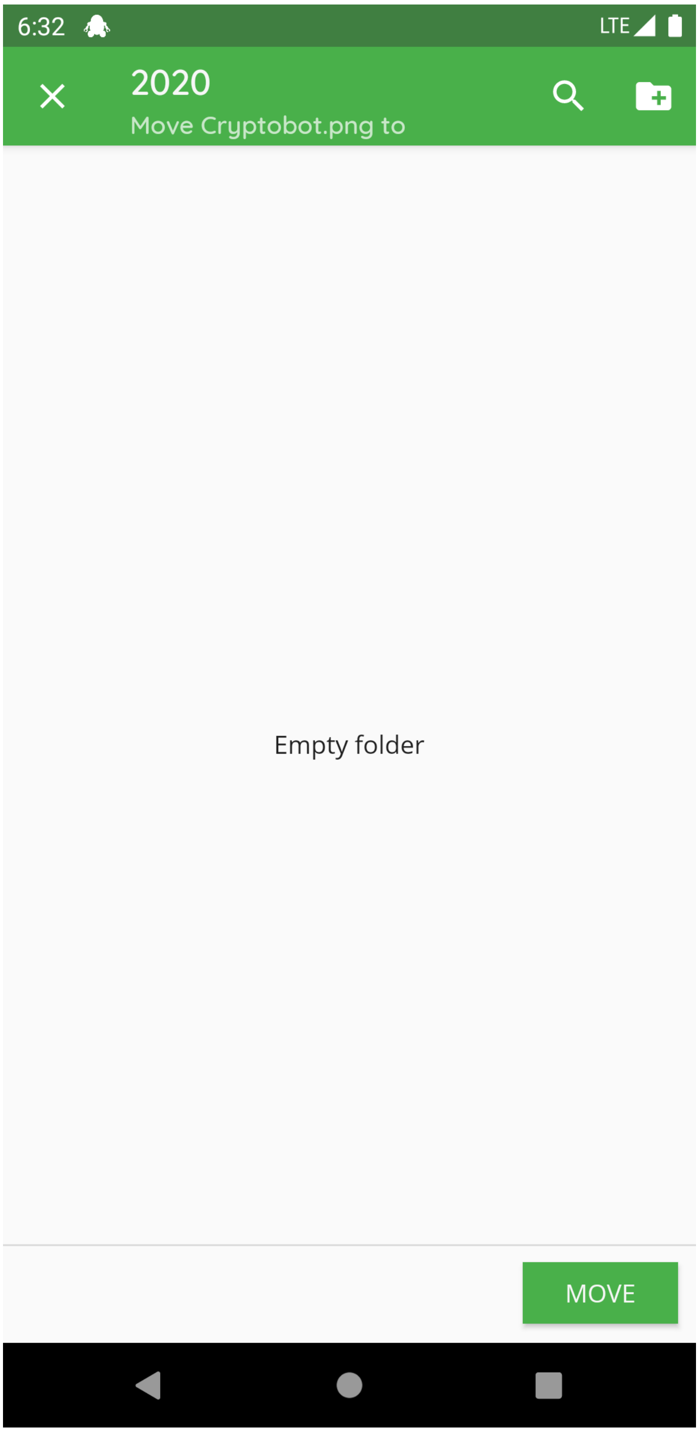




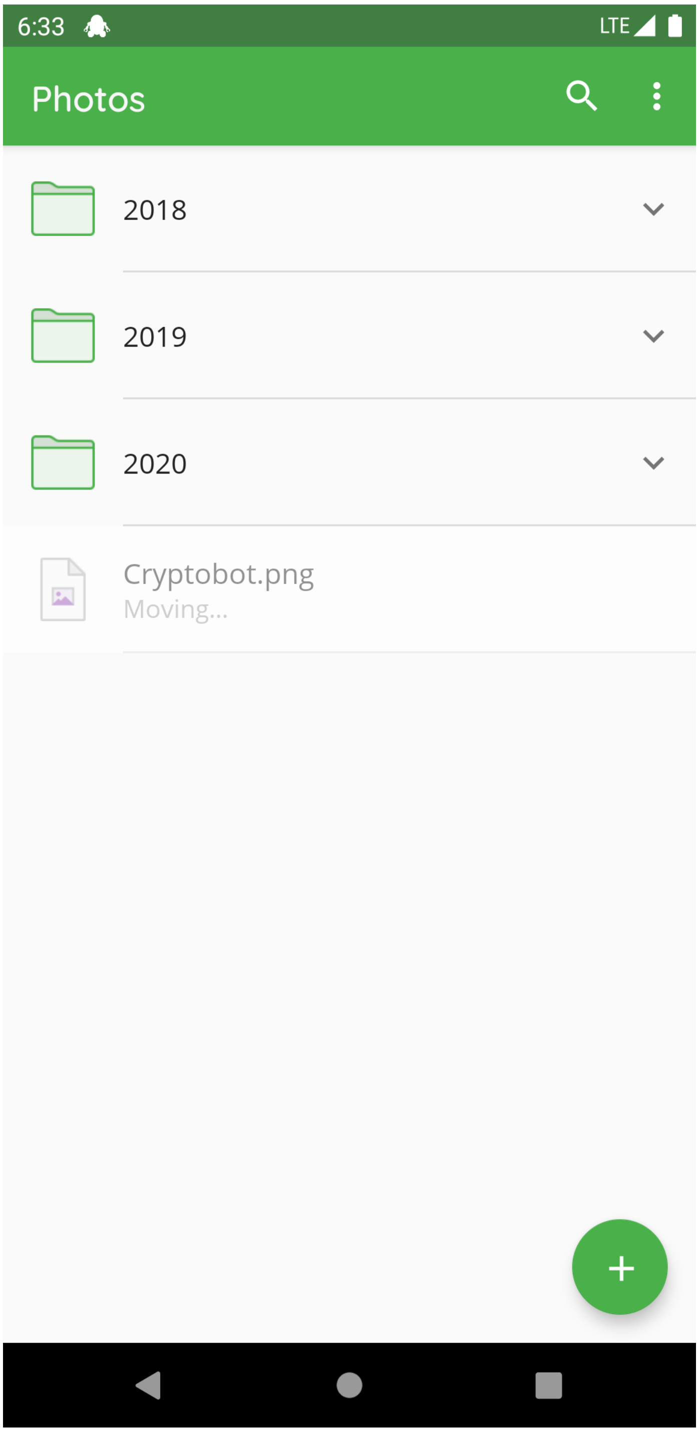
Choose a new location by selecting a folder or by pressing the back button of your phone to navigate to the parent folder.



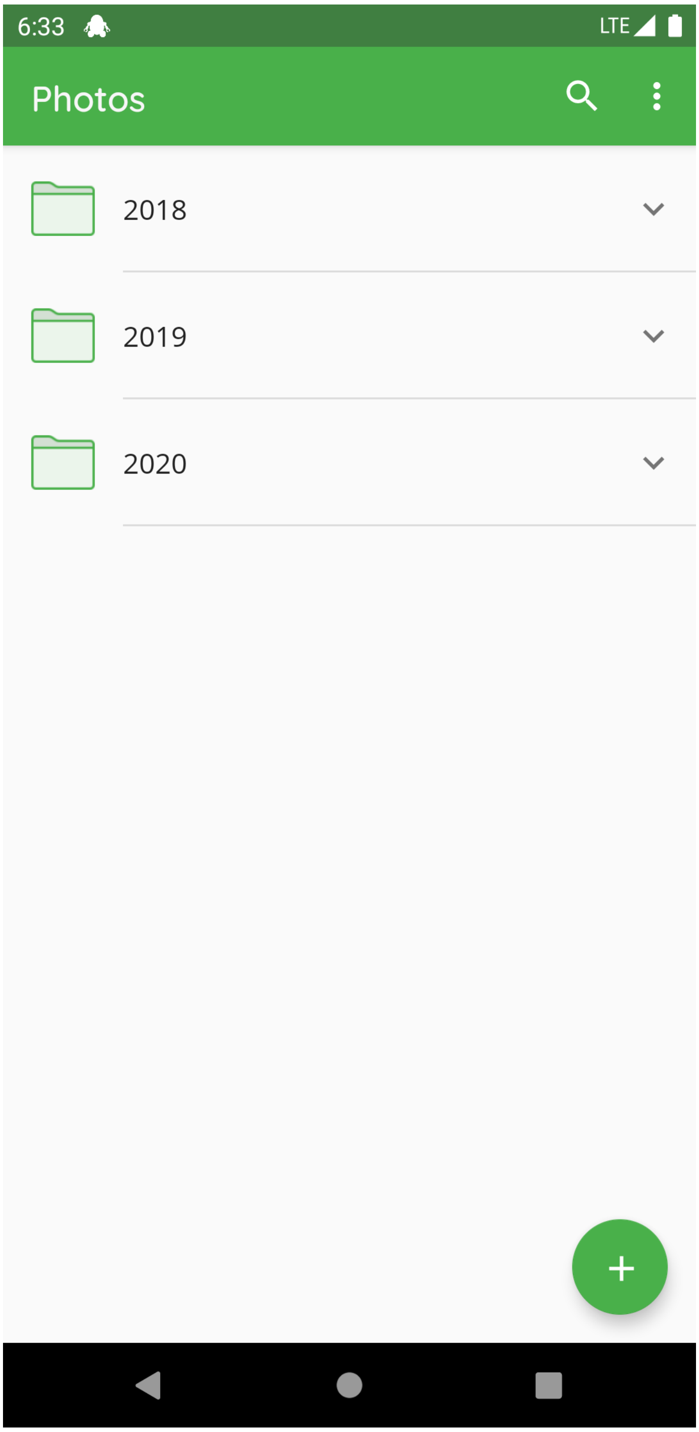
6:32
LTE
Photos
Move Cryptobot.png to
2018
2019
2020
Cryptobot.png
MOVE



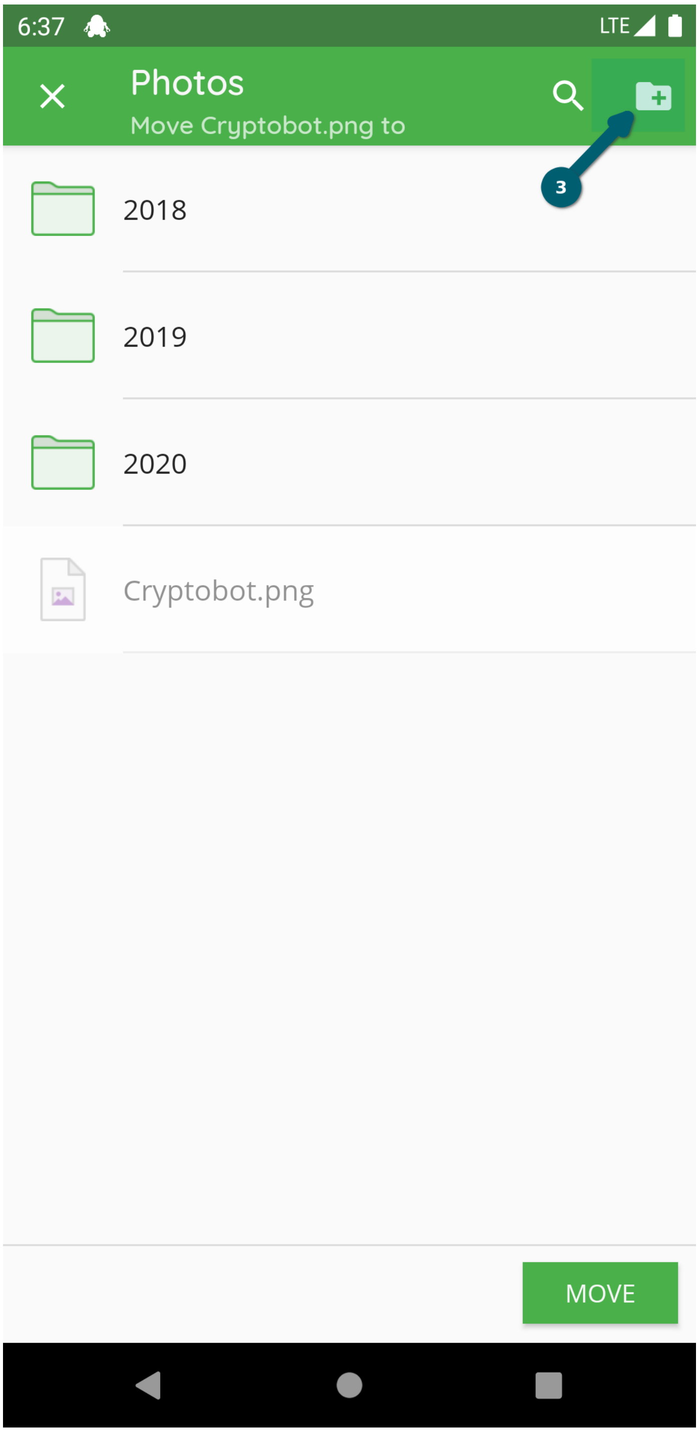
Confirm using the `MOVE` button.



6:33
LTE
Photos
2018
2019
2020
Cryptobot.png
Moving...
+



While moving, you can use the button to create a new folder in the current folder.



Move Cryptobot.png to

2018

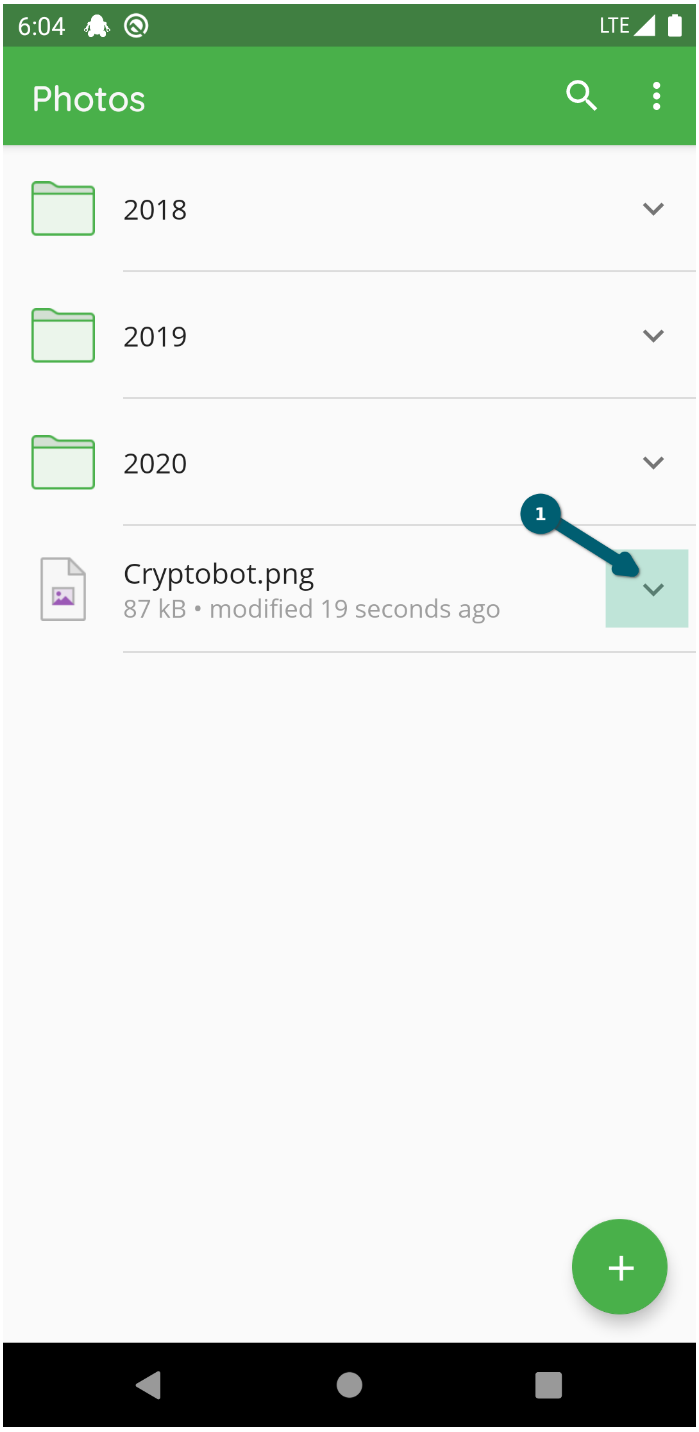
2019

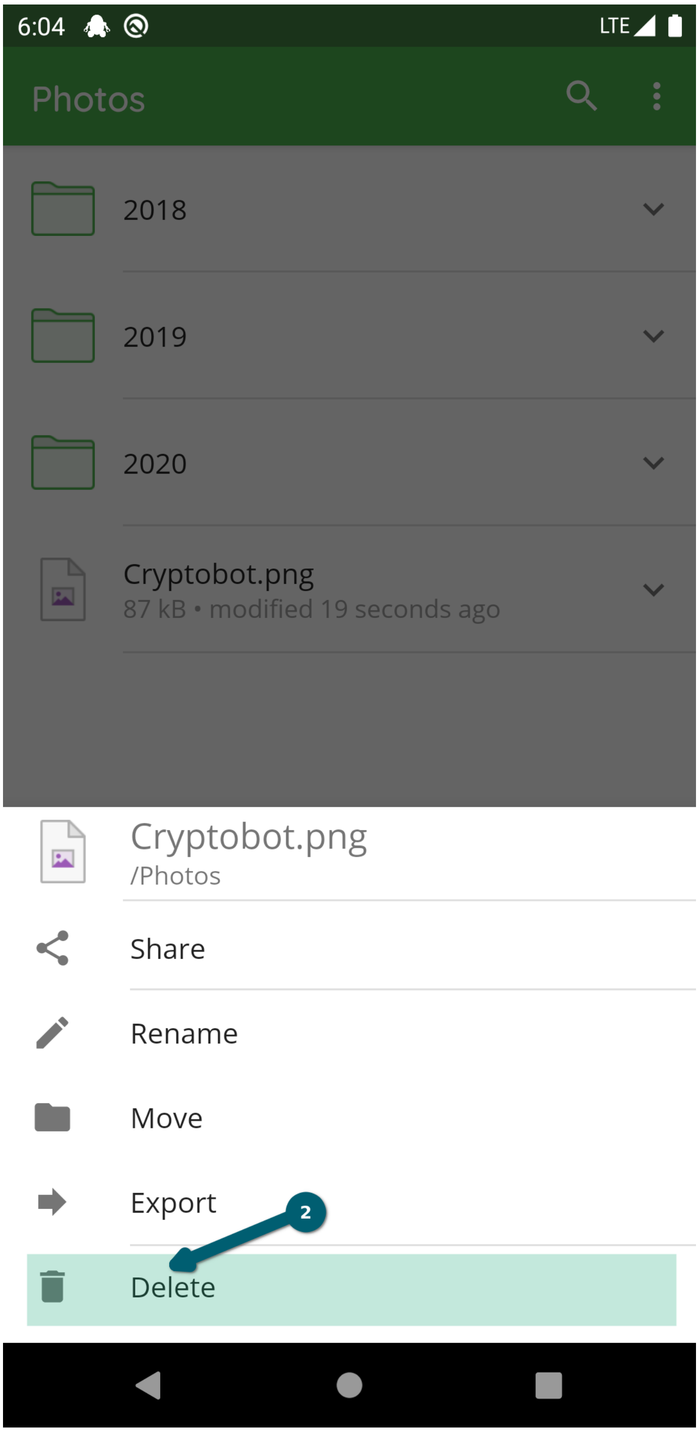
2020

Cryptobot.png

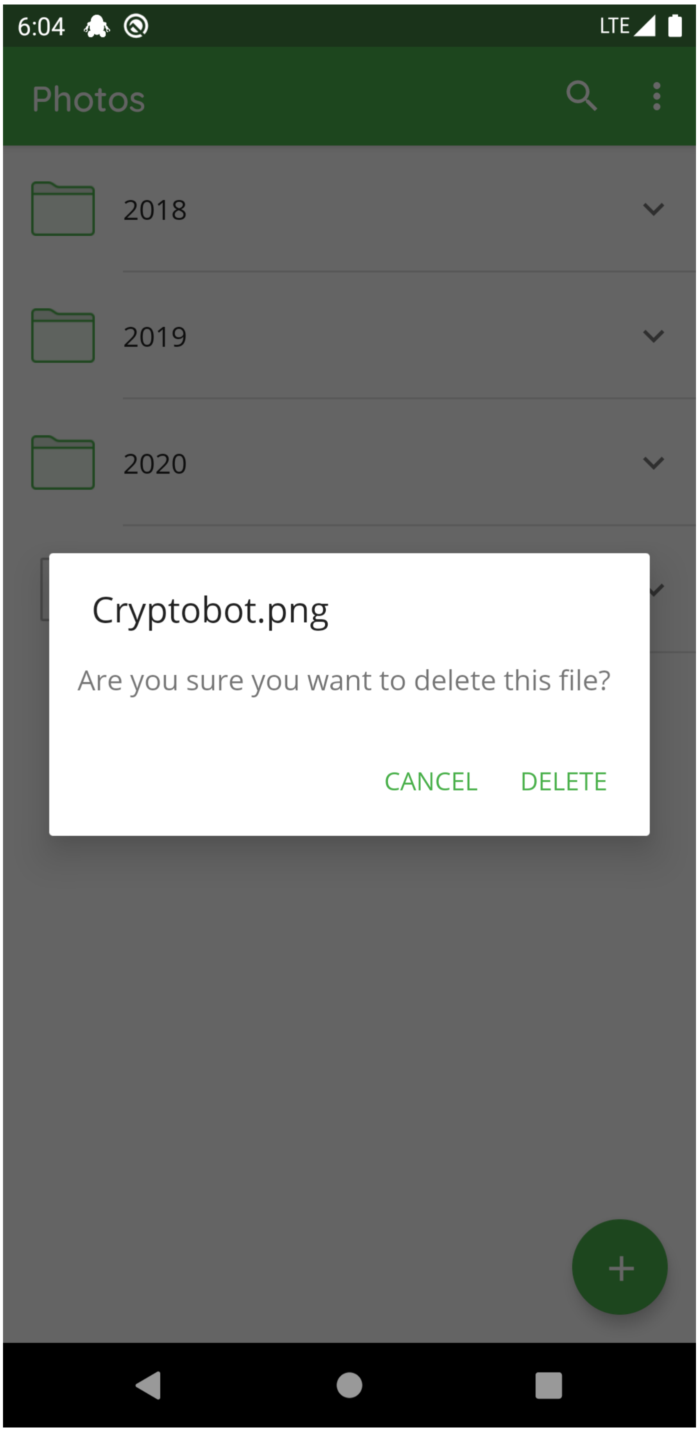
11.6 Delete File or Folder

To delete a specific file or folder in Cryptomator, you select the V next to the file or folder and choose *Delete* .



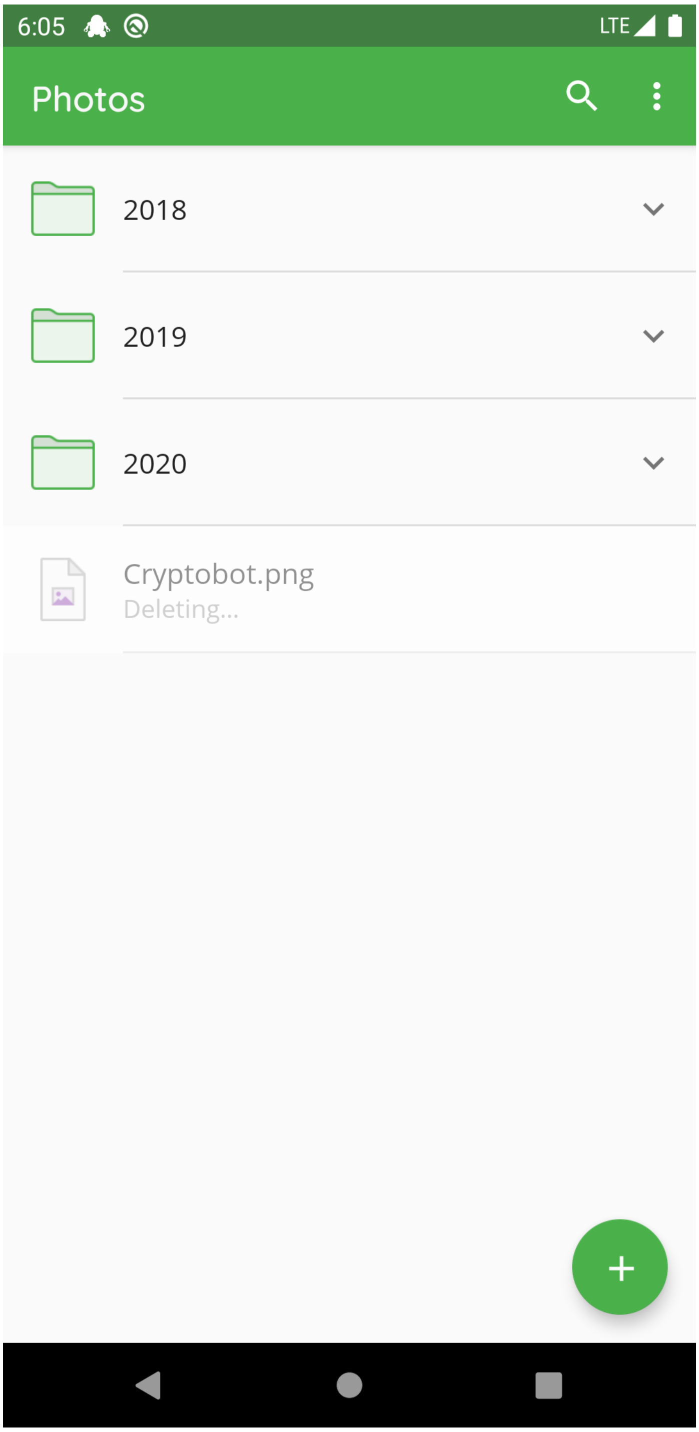


Confirm the deletion process using the DELETE button.



Cryptobot.png

Are you sure you want to delete this file?



6:05

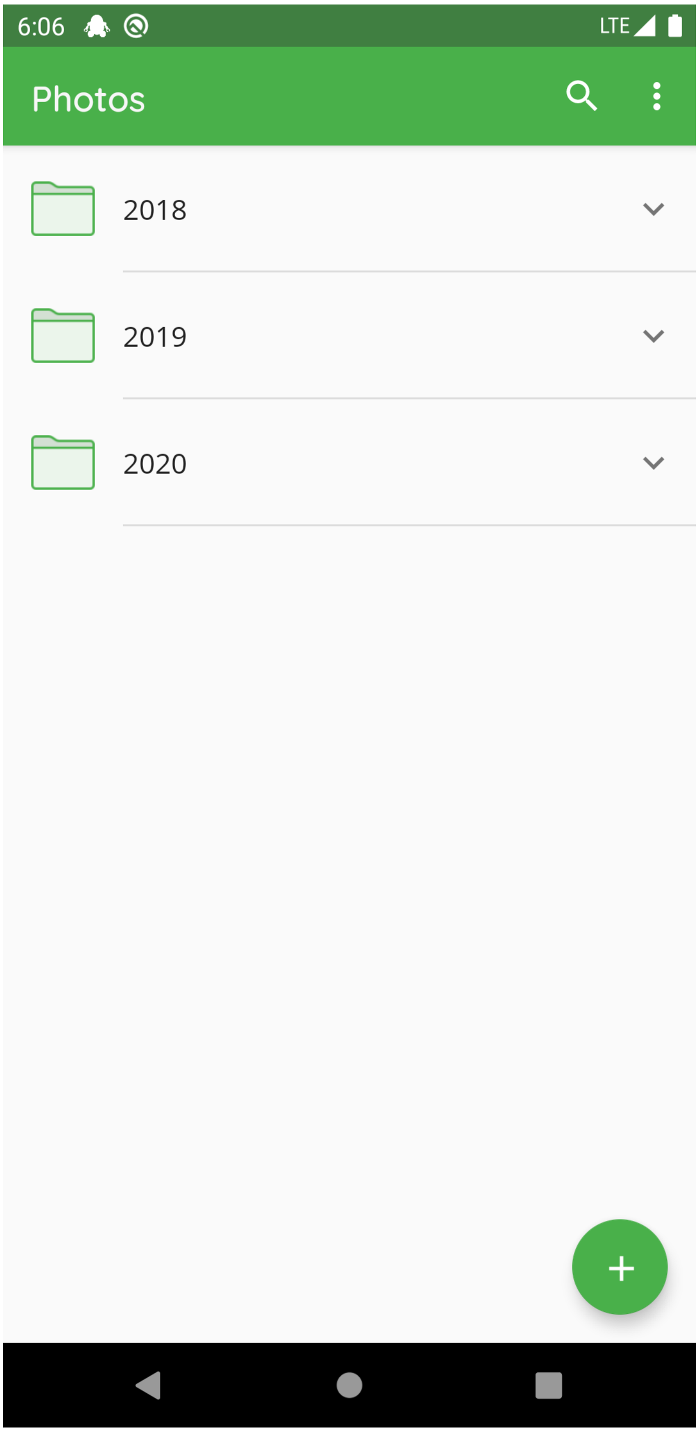
Photos

2018

2019

2020

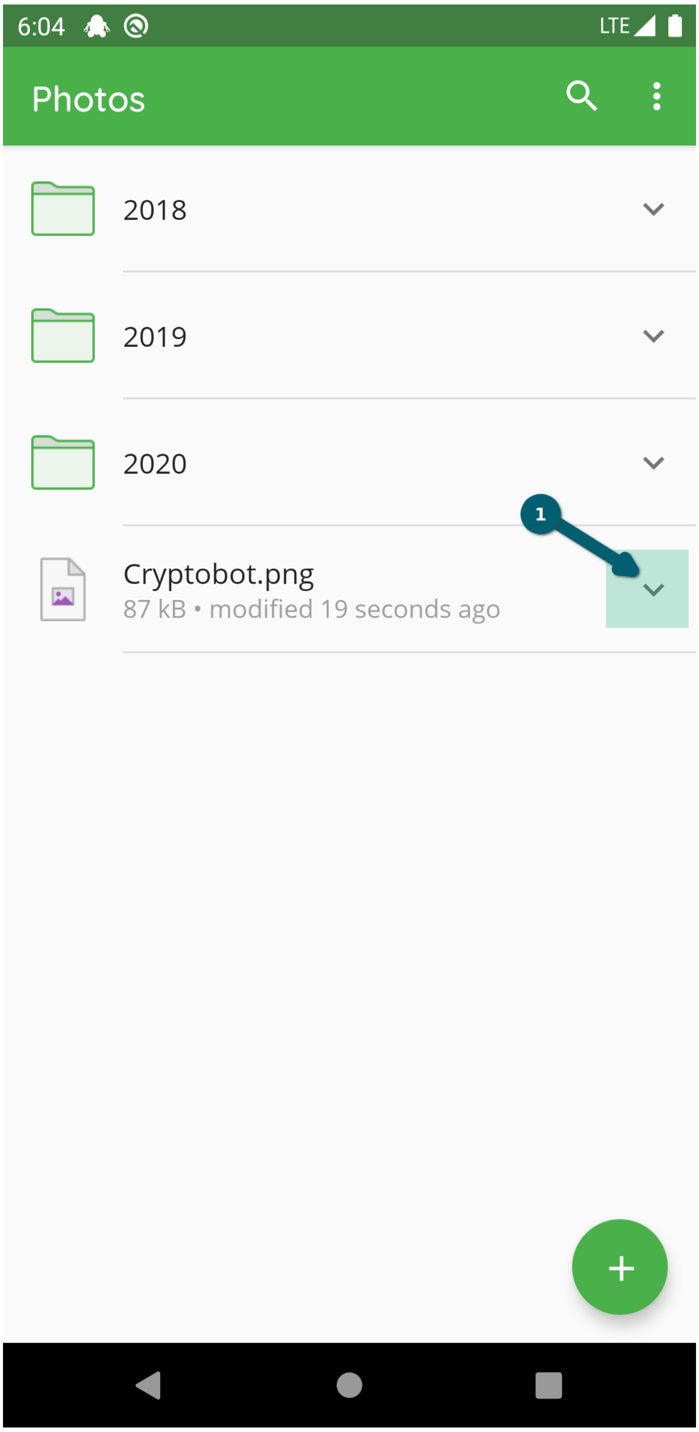
Cryptobot.png
Deleting...

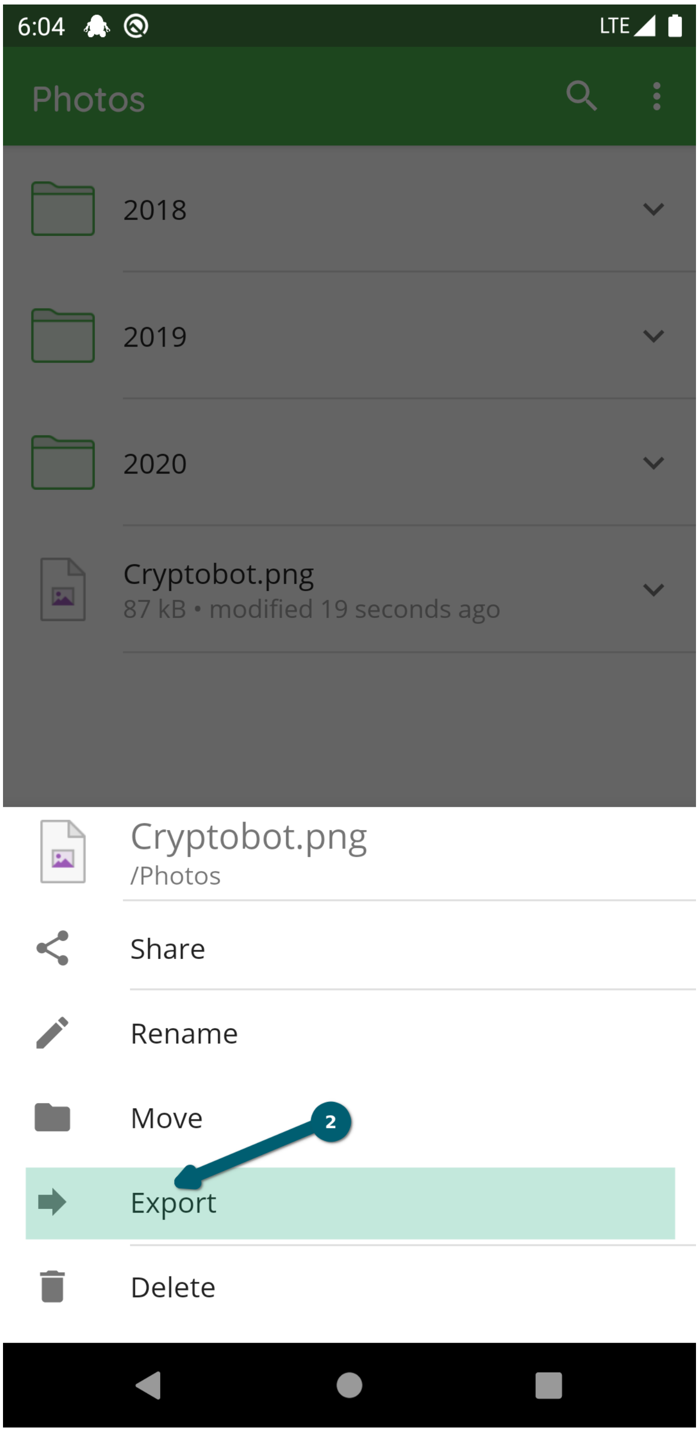


Note: By deleting a folder, all subfolders and files inside are deleted recursively.

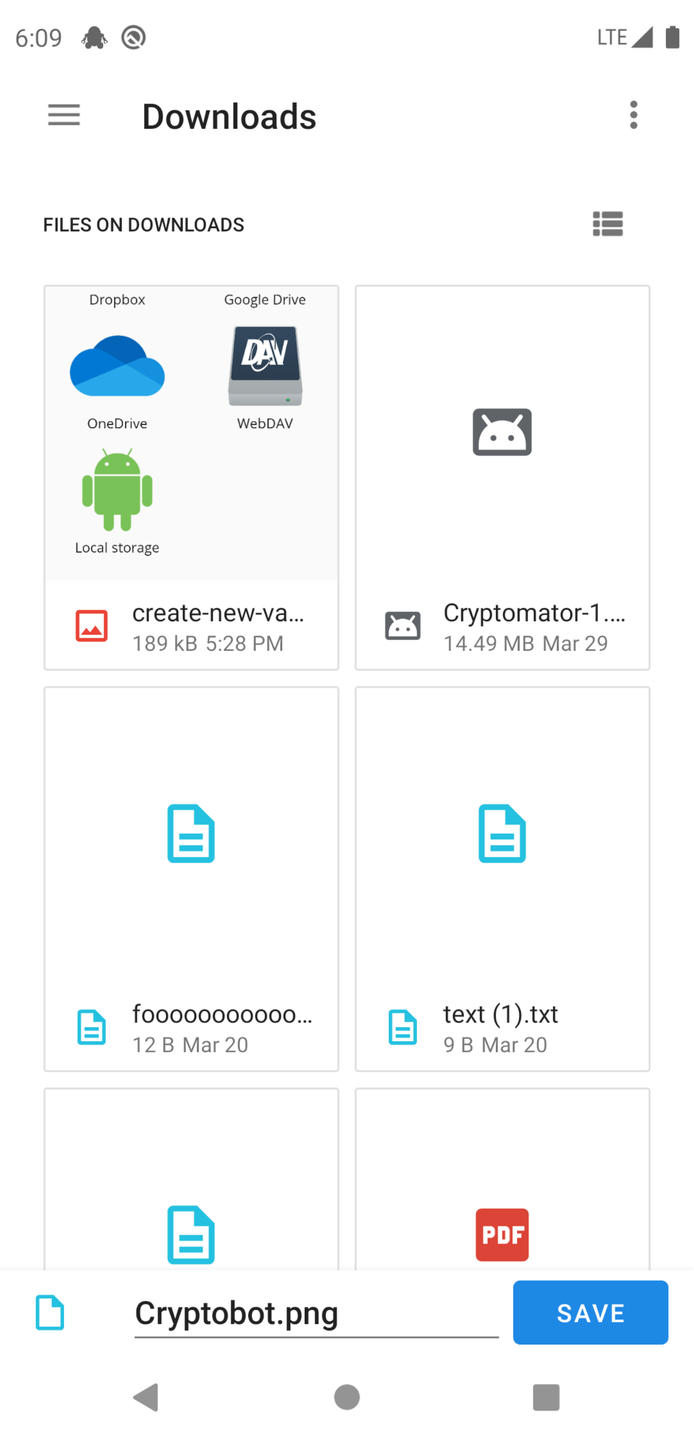
11.7 Export File or Folder

To export a specific file or folder in Cryptomator, you select the V next to the file or folder and choose *Export* .

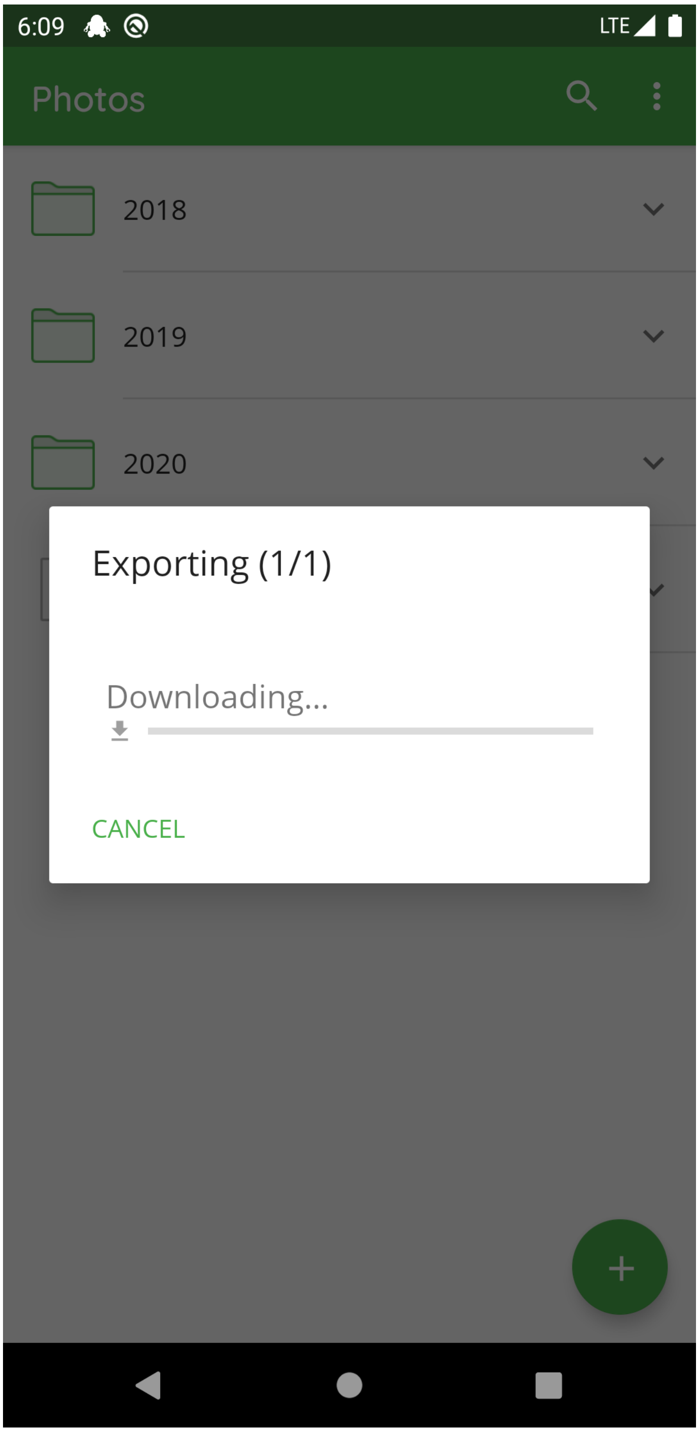




Chose the target location where the file or folder should be exported to.

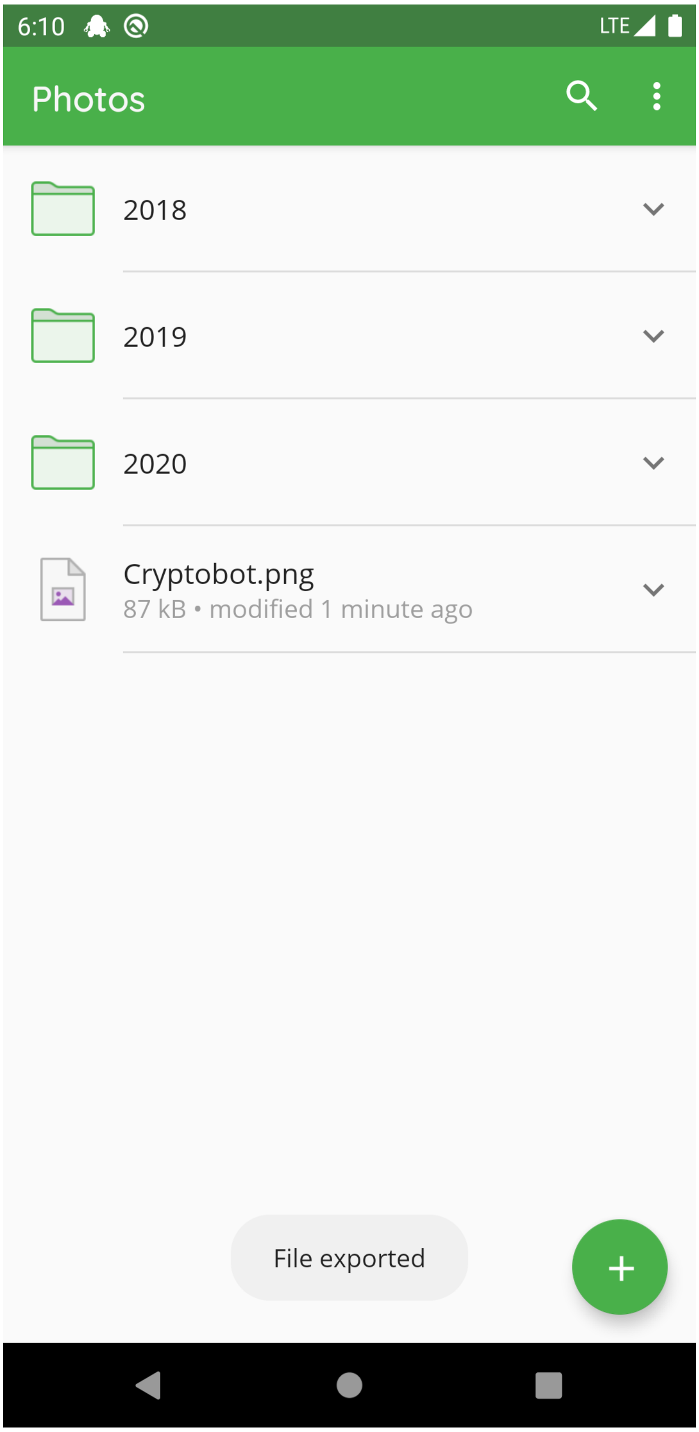


Cryptobot.png



Exporting (1/1)

Downloading...



2018

2019

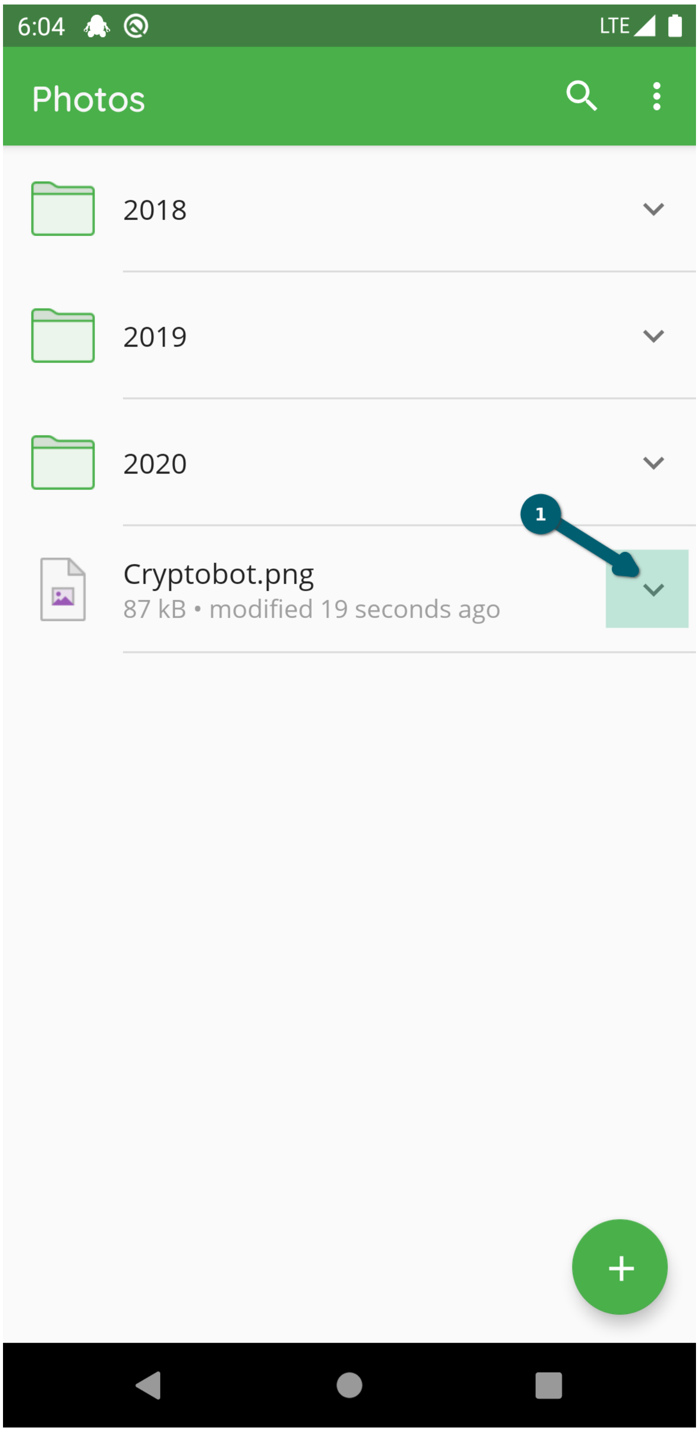
2020

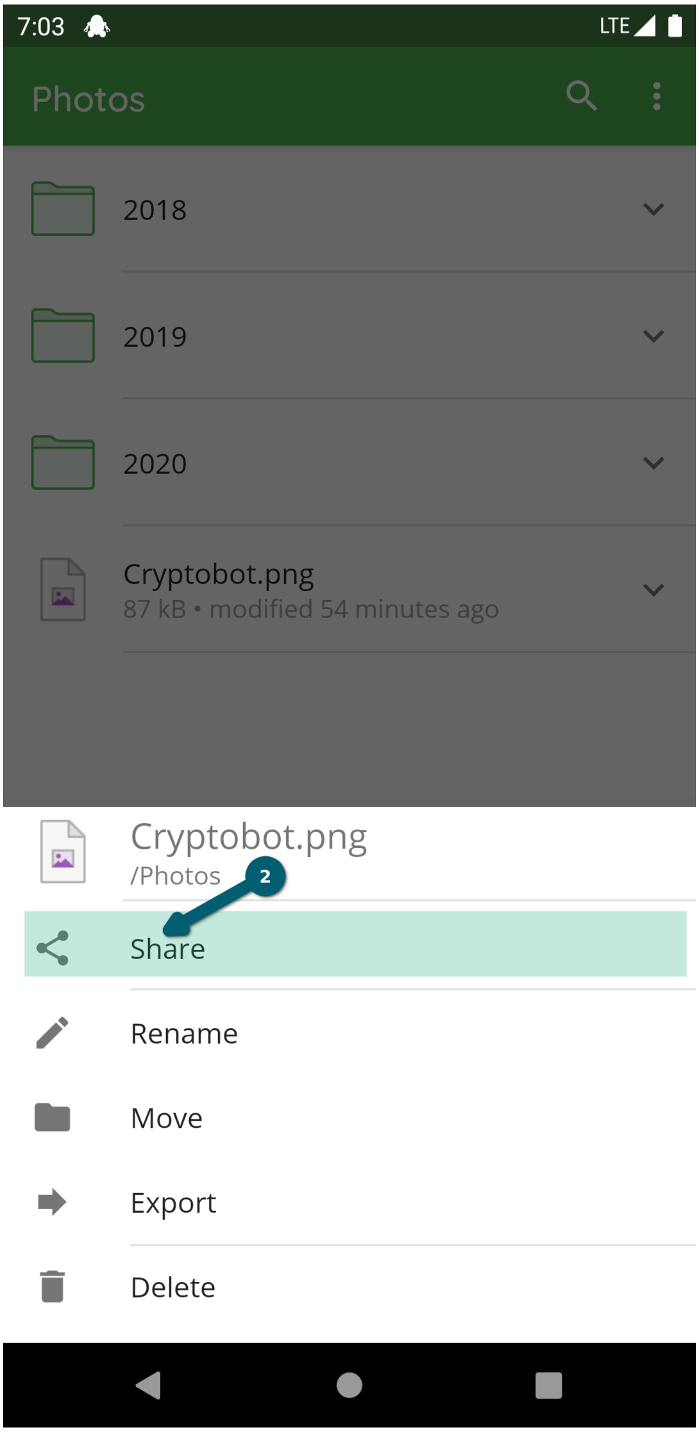
Cryptobot.png
87 kB • modified 1 minute ago

File exported

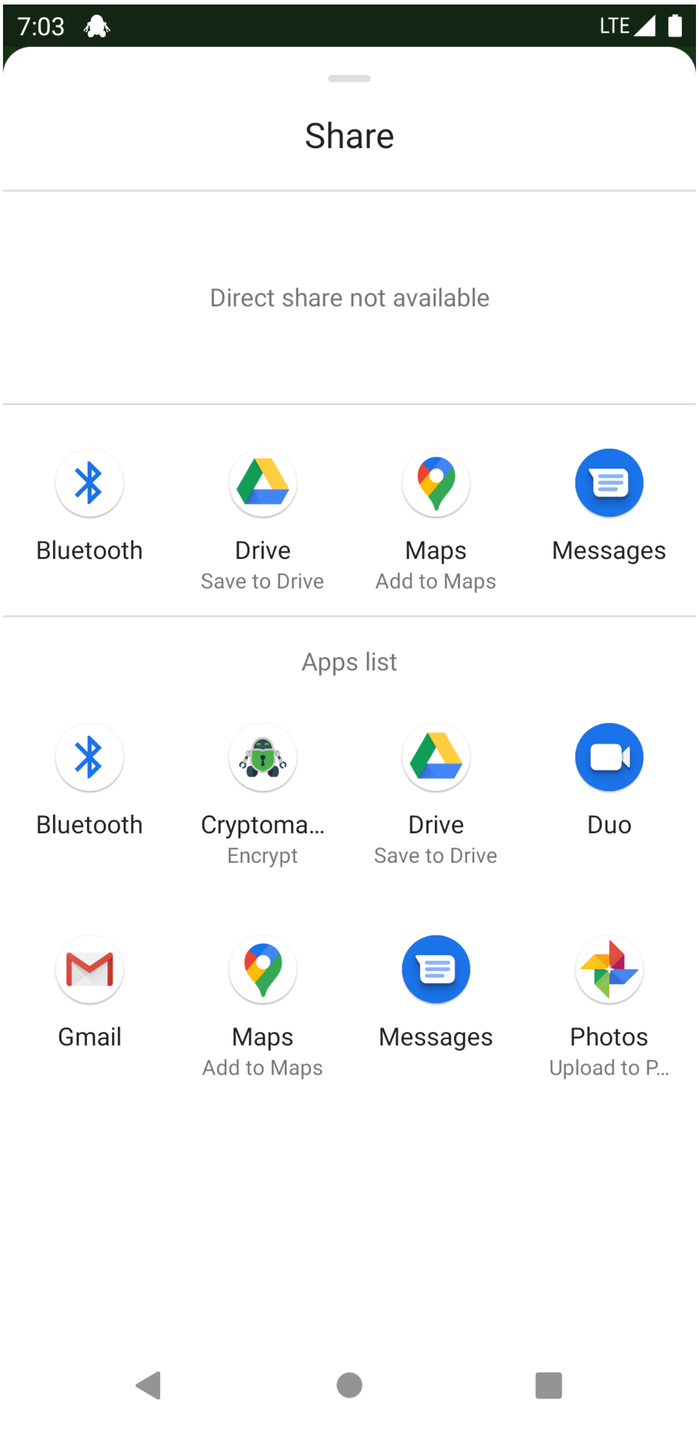
11.8 Share File with Other App

To share a specific file or folder in Cryptomator with another app, you select the V next to the file or folder and choose Share .





Choose the target app in which you will use the file or folder.



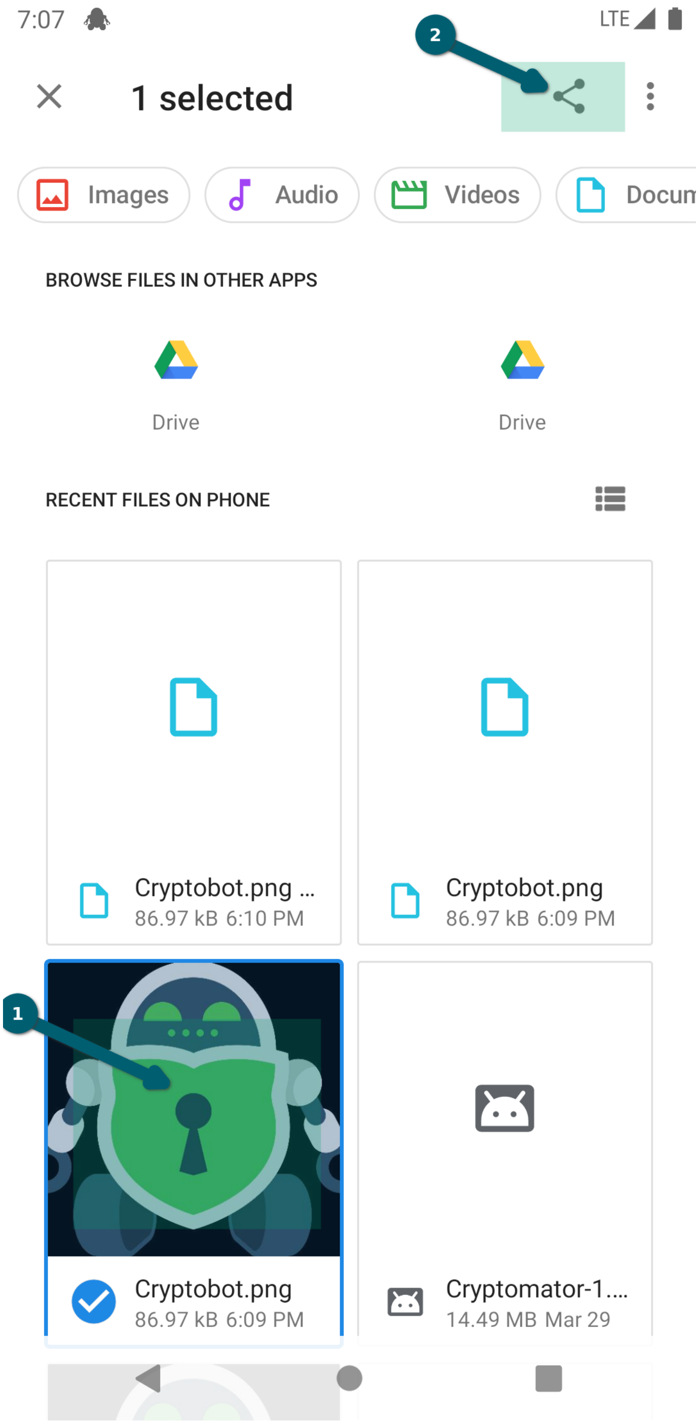
Direct share not available

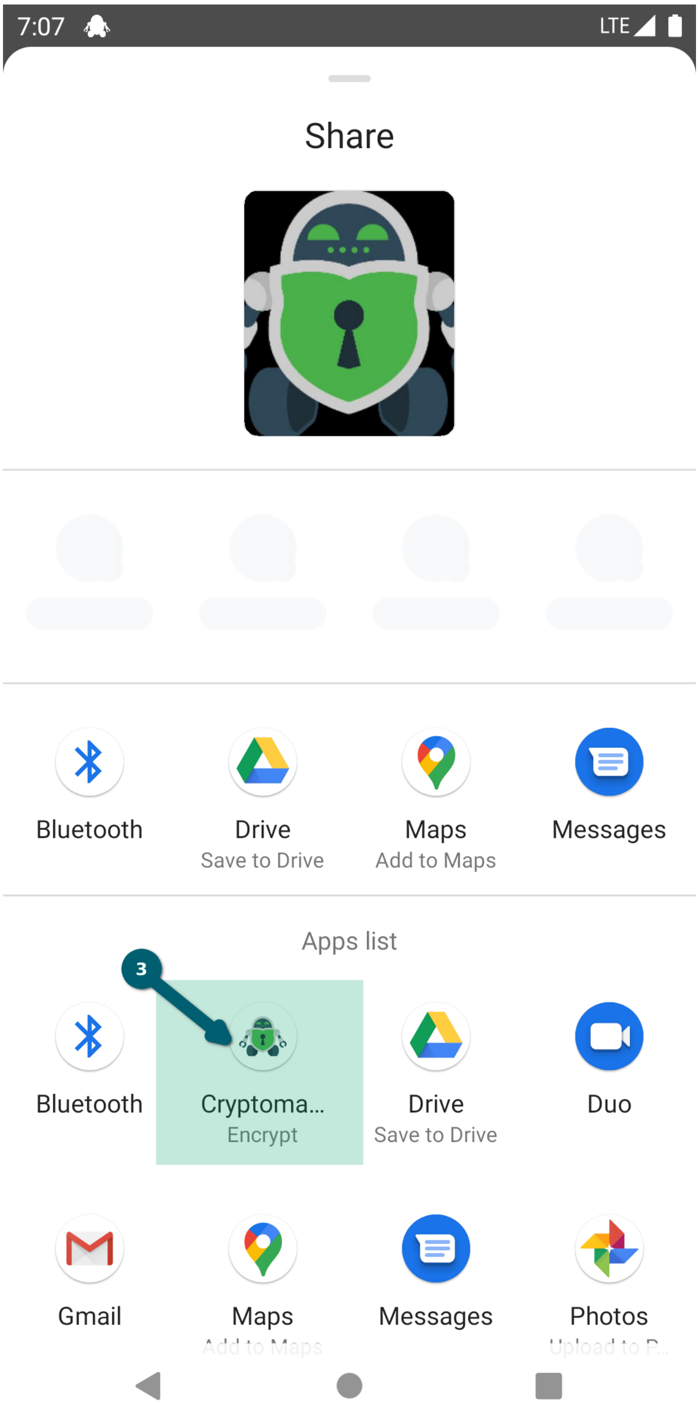
Note: By sharing a file or folder from Cryptomator with Cryptomator, you can copy content from one vault to another one.

11.9 Share File with Cryptomator

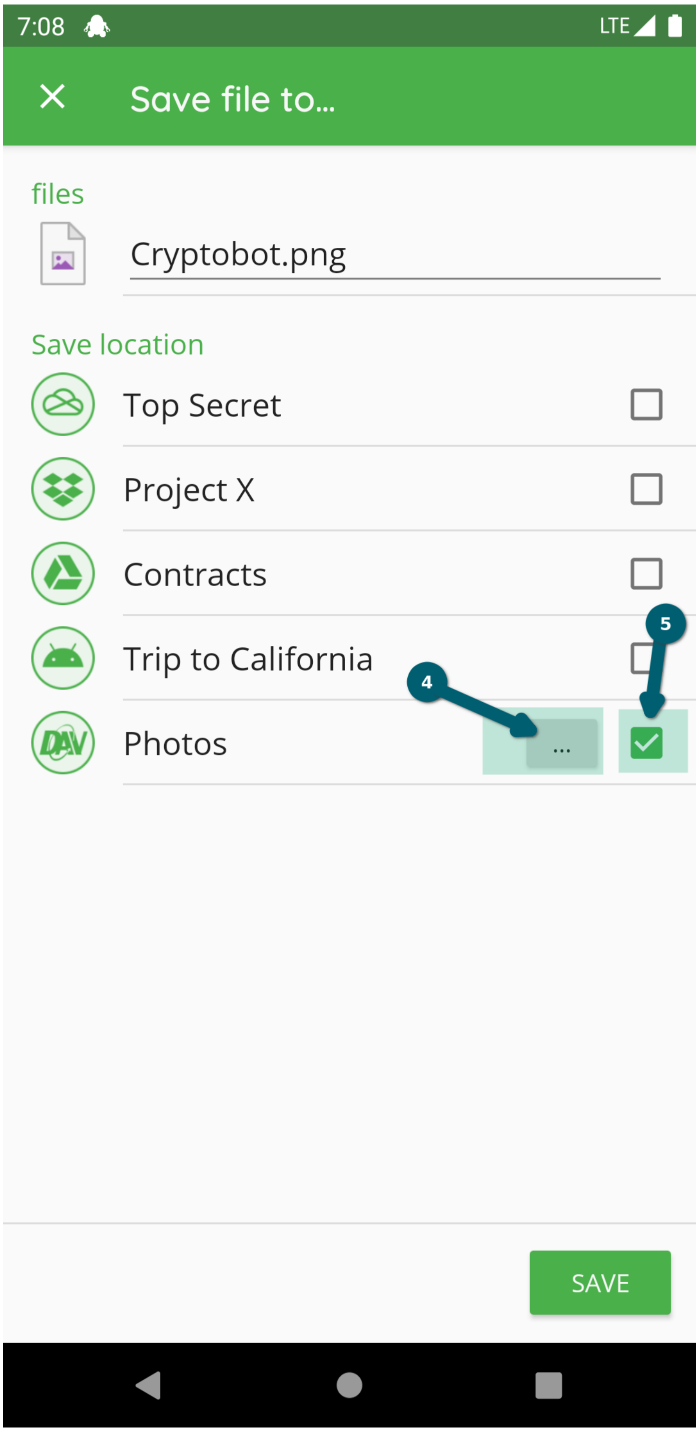
You can share files from another app with Cryptomator. We use as example the Files app from Android.

You select the file(s) to share by long clicking on it . Press the share button to choose to share these file(s) and select *Cryptomator* .

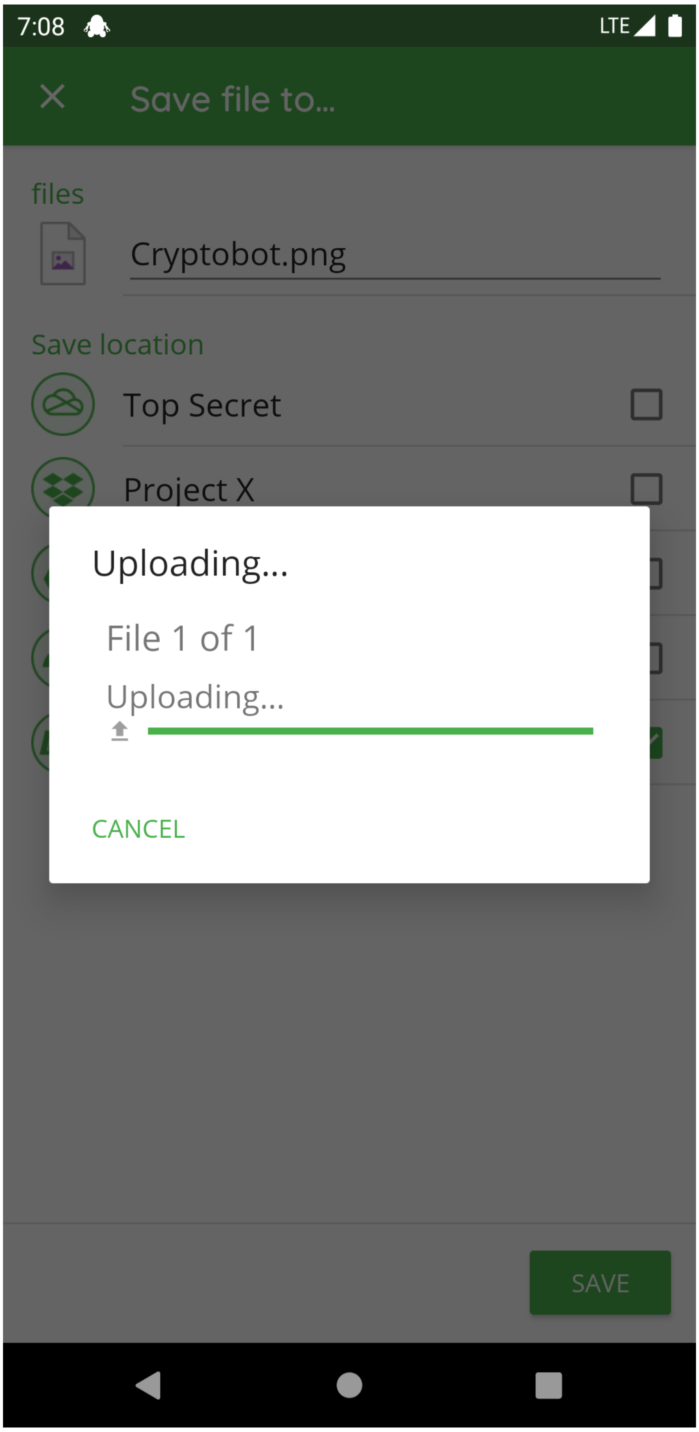




Choose the vault and optionally specify the target folder in the vault (default is the root).



Then the encryption and upload starts.

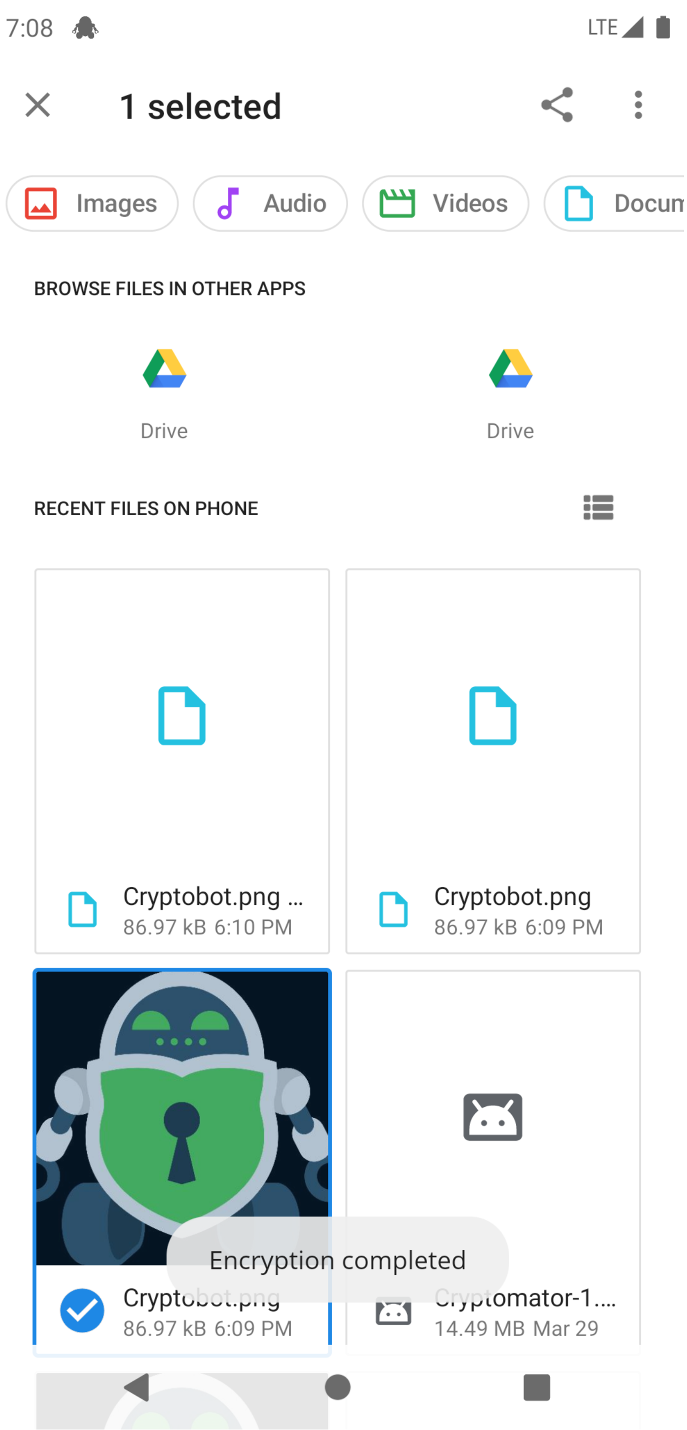


Uploading...

File 1 of 1

Uploading...

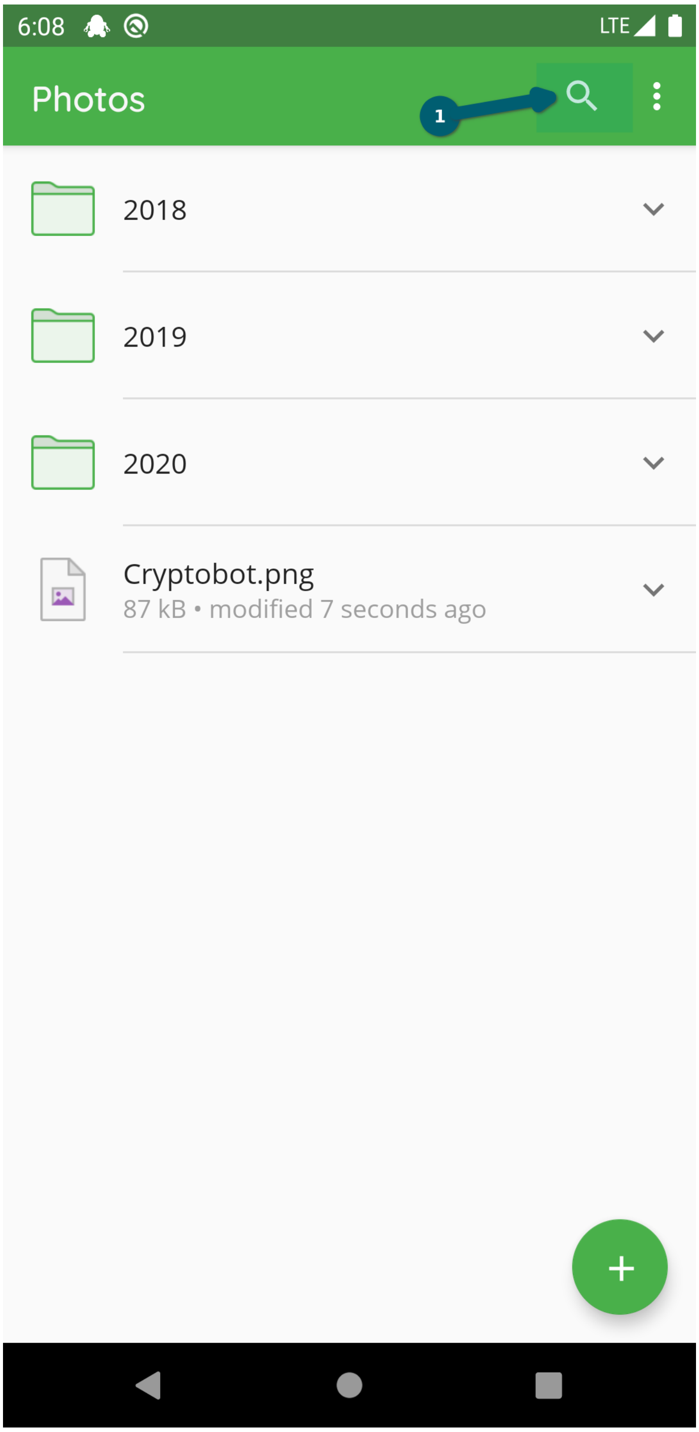
CANCEL



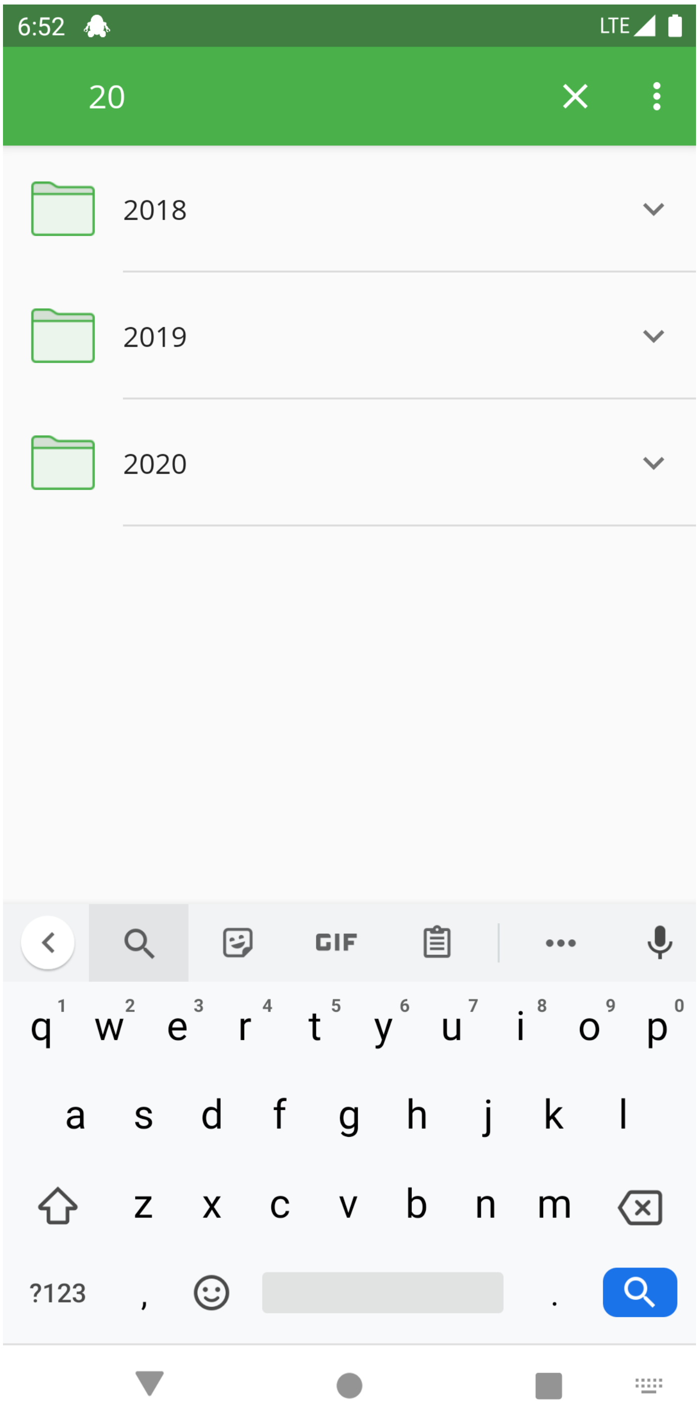
Encryption completed

11.10 Search in Folder

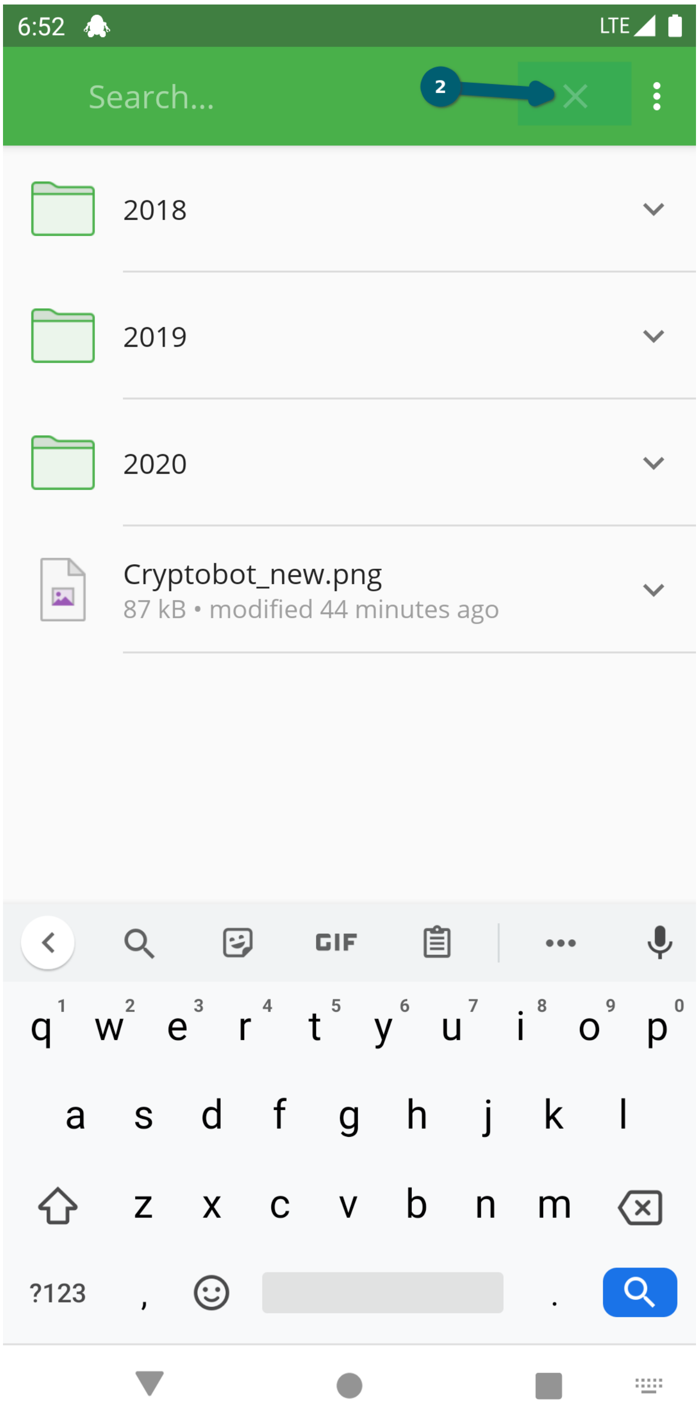
Search for files or folders within the same folder using the magnifier .



Now you can enter the pattern after which you want to search in this folder.



Using the *X* you can clear the pattern and after pressing it again, the filter mode is finished.



In the settings there are two options that influence the behavior of the search:

- Live search (disbaled by default)
- Search using glob pattern matching (disbaled by default)

For more information, see the Settings chapter.

11.11 Sort Folder by…

11.12 Fast scroll

If the folder contents are sorted by file size, the preview will show the file sizes accordingly. The same applies to the modification date.

CHAPTER

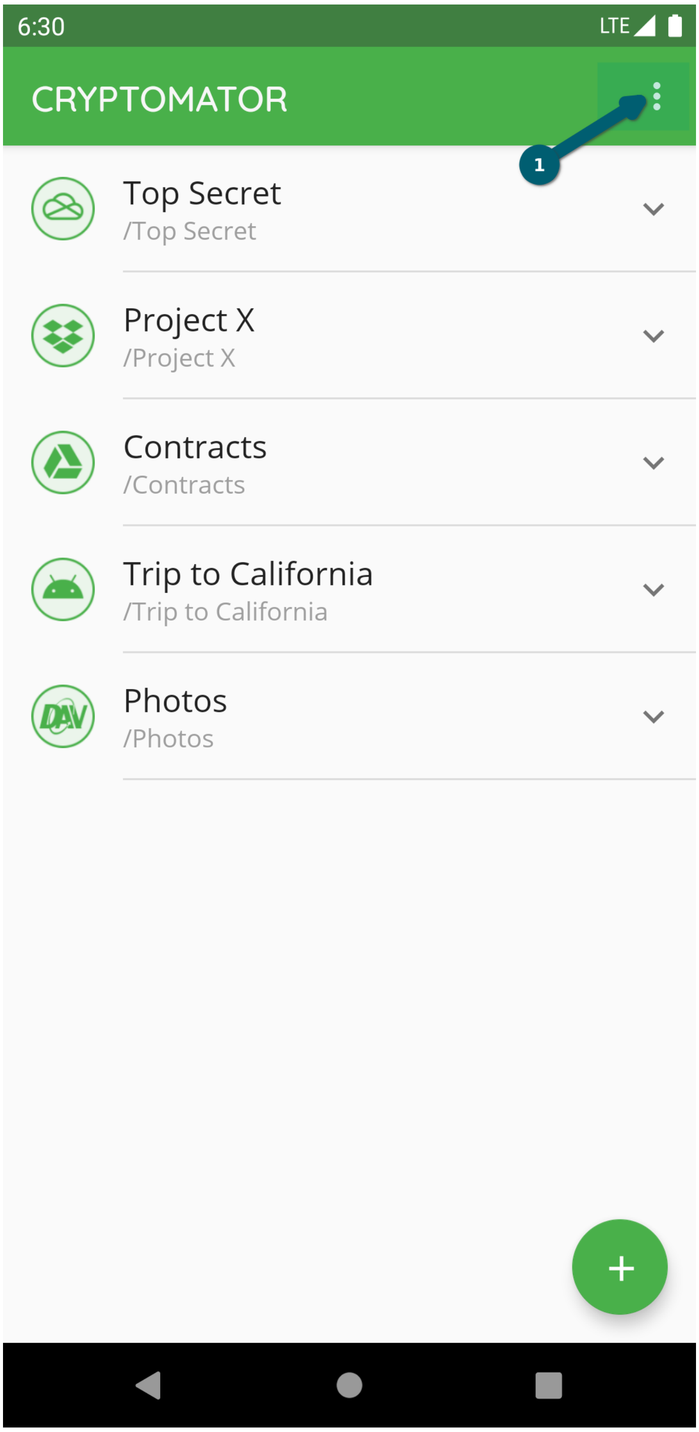
TWELVE

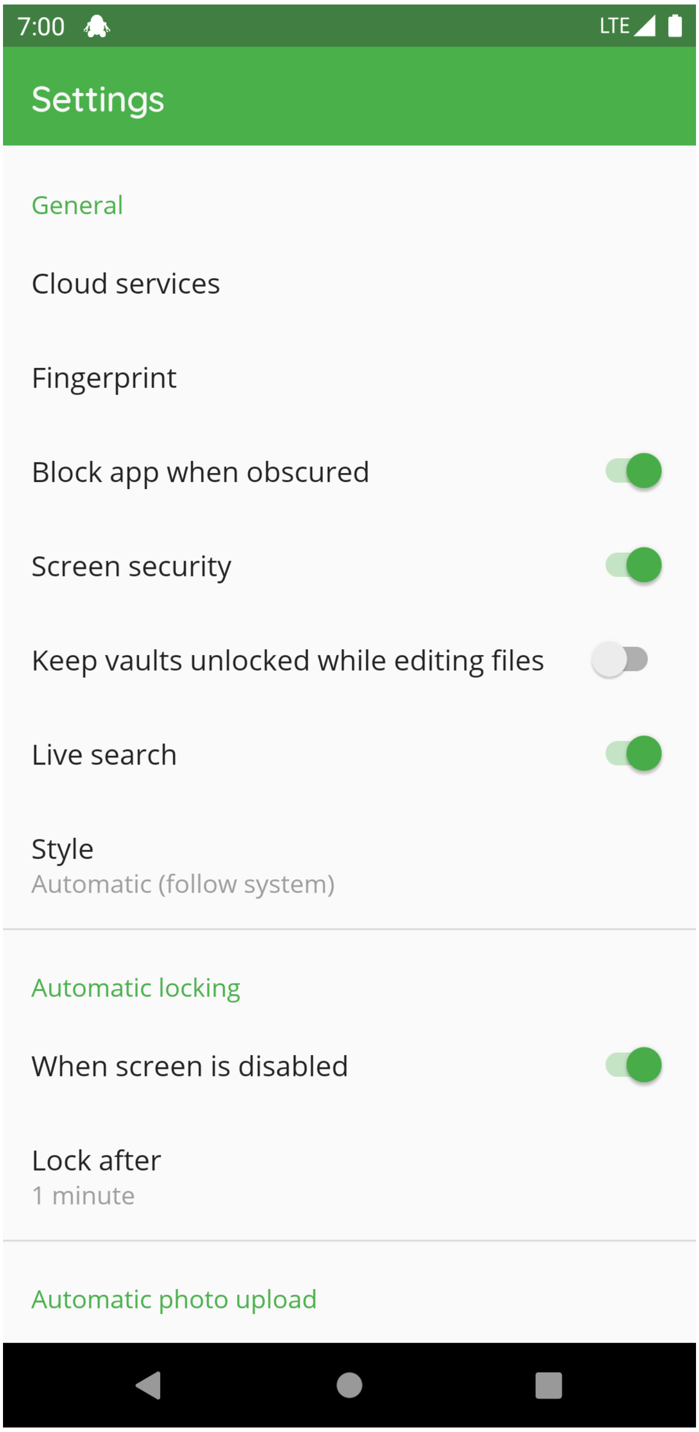
SETTINGS

You can configure Cryptomator to your needs. This section provides an overview of the different settings.

12.1 General Settings

After pressing the three dots and clicking on `Settings`, you will find options to customize Cryptomator.


6:30
LTE
CRYPTOMATOR
1
Top Secret
/Top Secret
Project X
/Project X
Contracts
/Contracts
Trip to California
/Trip to California
Photos
/Photos
+



Settings

General

Cloud services

Fingerprint

Block app when obscured ●

Screen security ●

Keep vaults unlocked while editing files ○

Live search ●

Style
Automatic (follow system)

Automatic locking

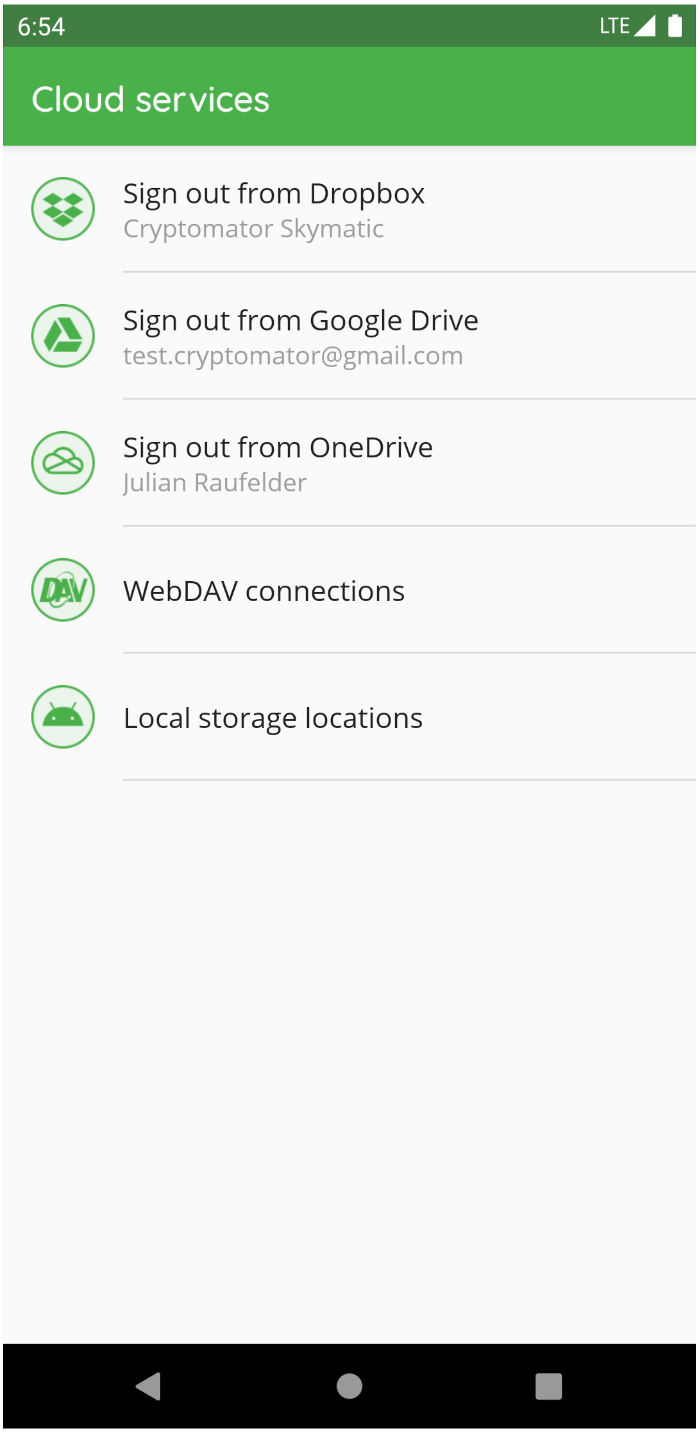
When screen is disabled ●

Lock after
1 minute

Automatic photo upload

12.1.1 Cloud Services

This setting lists all cloud services. When pressing on a service, the authentication starts or if you're already authenticated, you will be logged out.



Sign out from Dropbox
Cryptomator Skymatic

Sign out from Google Drive
test.cryptomator@gmail.com

Sign out from OneDrive
Julian Raufelder

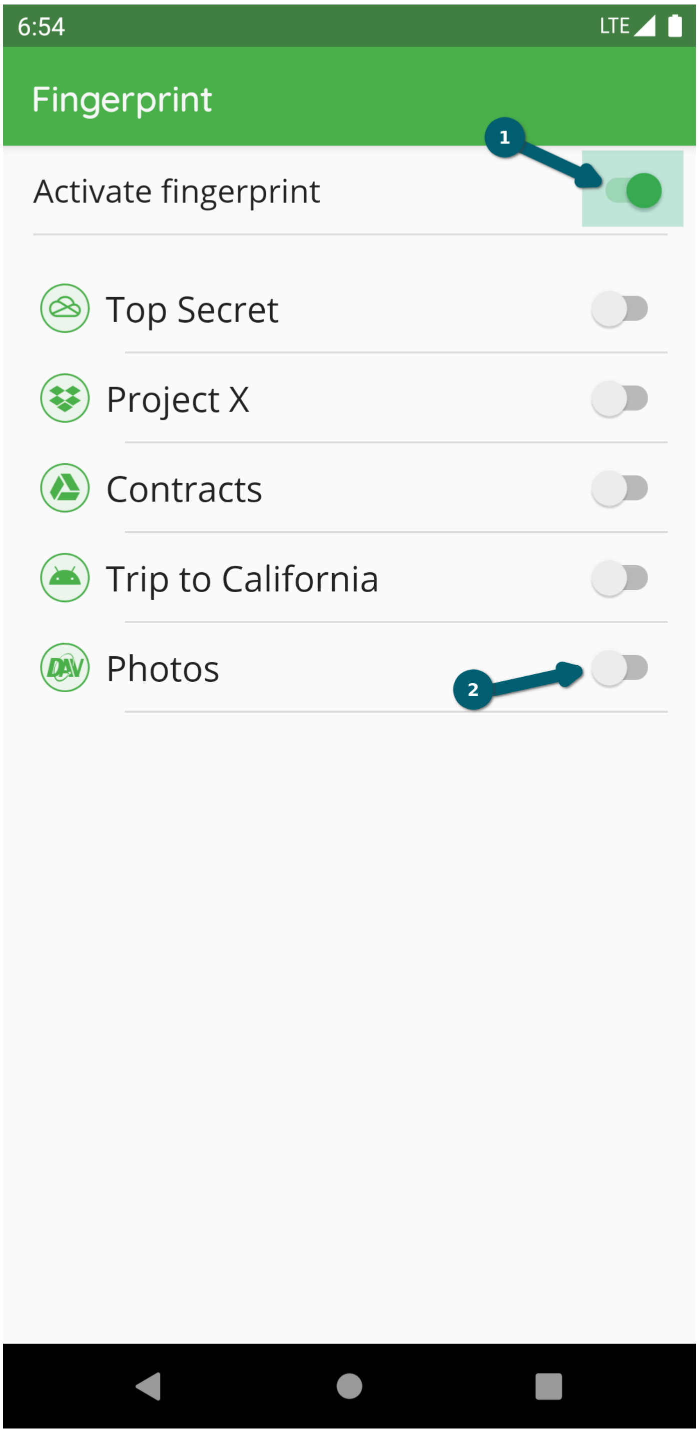
WebDAV connections

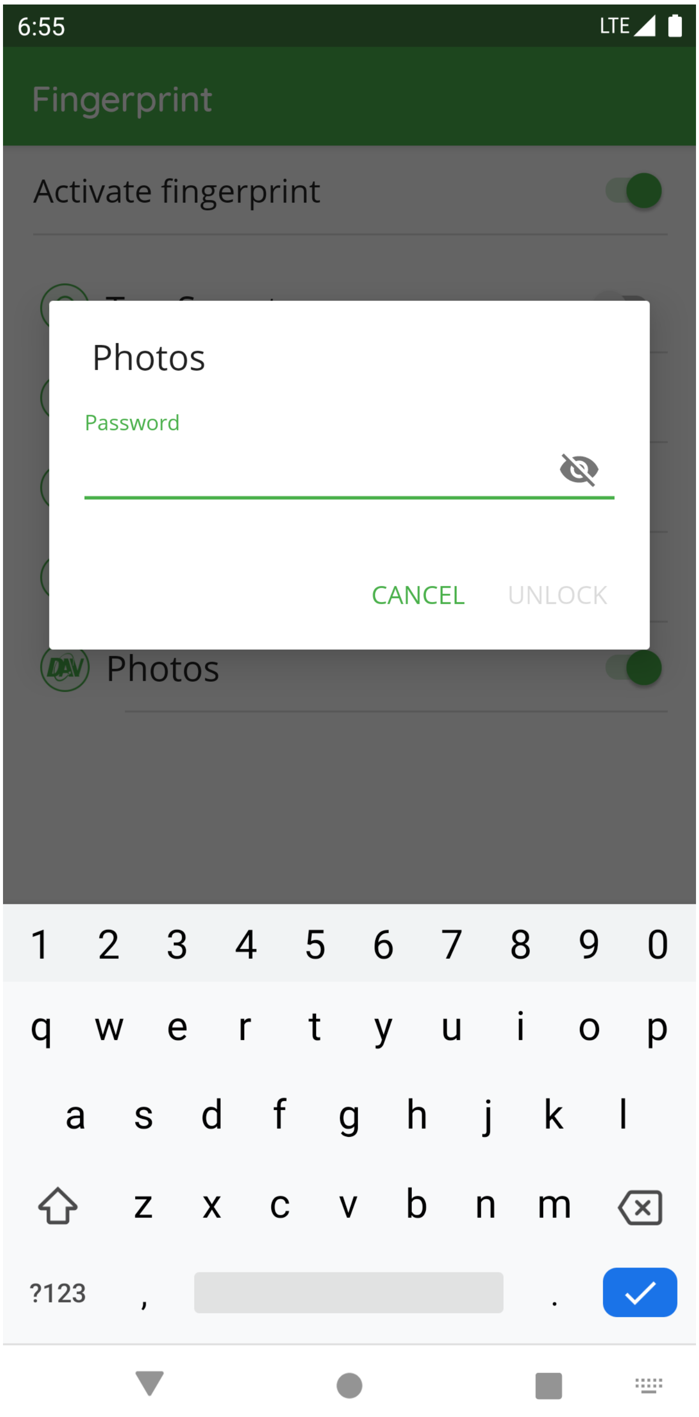
Local storage locations

12.1.2 Fingerprint

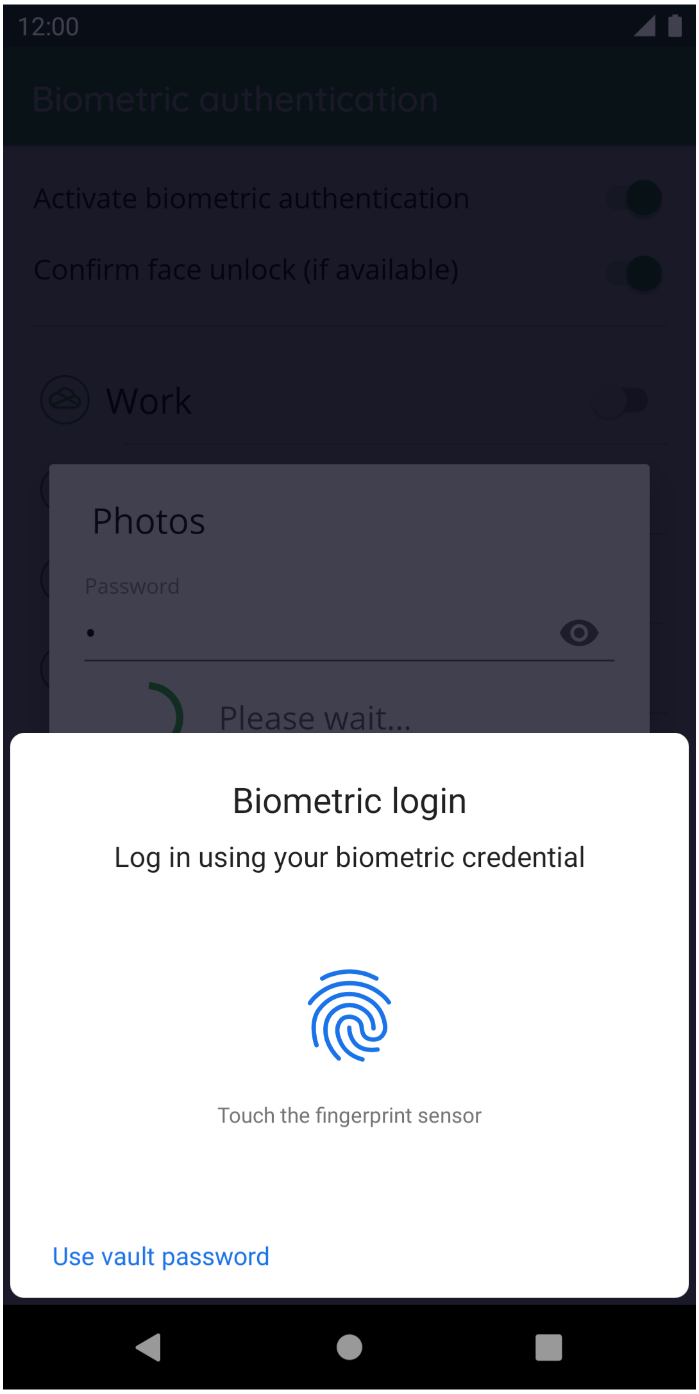
Note: This setting is only available if your device supports the fingerprint authentication.

With the toggle button in the right upper corner , the fingerprint will be generally enabled/disabled. Using the toggle button next to the vault, it will be enabled/disabled for this vault .





After enabling, you have to unlock the vault using the password.



12:00

Biometric authentication

Activate biometric authentication

Confirm face unlock (if available)

Work

Photos

Password

•

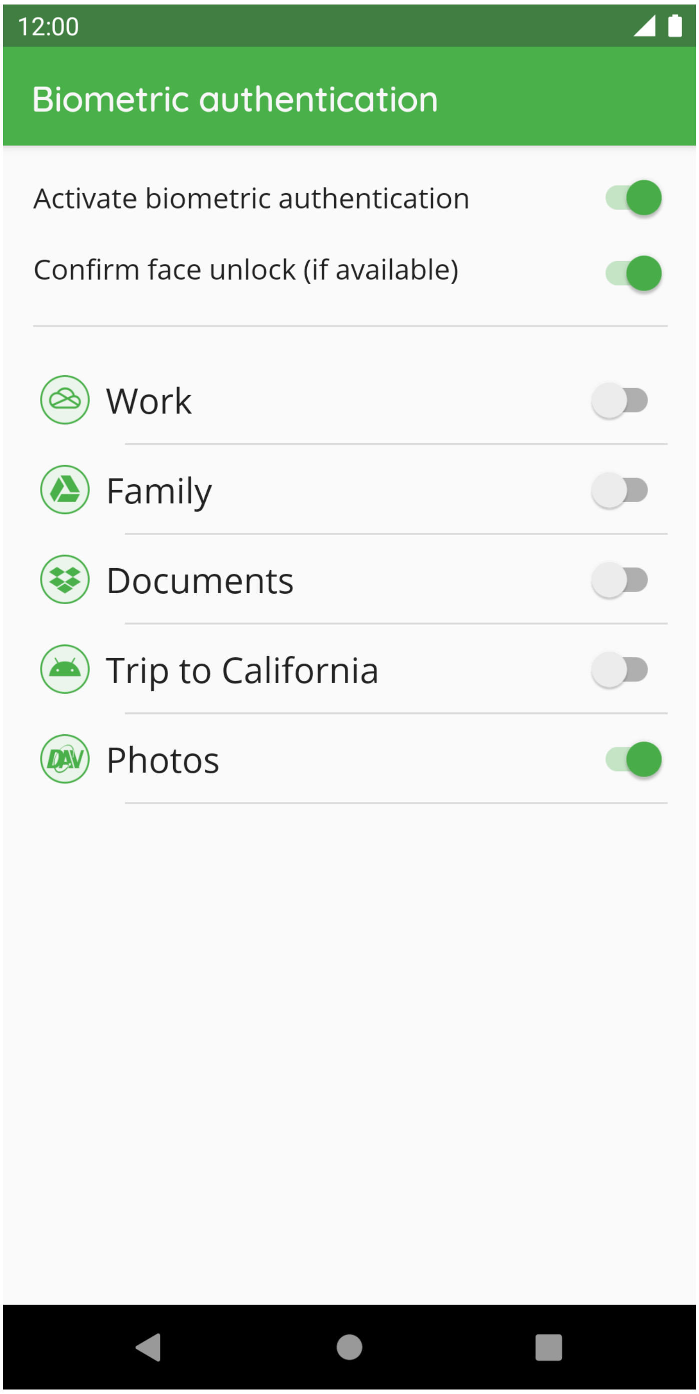
Please wait...

Biometric login

Log in using your biometric credential

Touch the fingerprint sensor

Use vault password



12:00

Biometric authentication

Activate biometric authentication ●

Confirm face unlock (if available) ●

Work ○

Family ○

Documents ○

Trip to California ○

Photos ●

To have access to the key stored in the keystore, you have to authenticate against the system using the fingerprint.

12.1.3 Block App When Obscured

Under certain circumstances, Cryptomator for Android may not respond to touches.

This is most often caused by apps which apply a color filter to the device. Examples are the apps Twilight or Blue Light Filter. When disabling or uninstalling such apps, Cryptomator will work again.

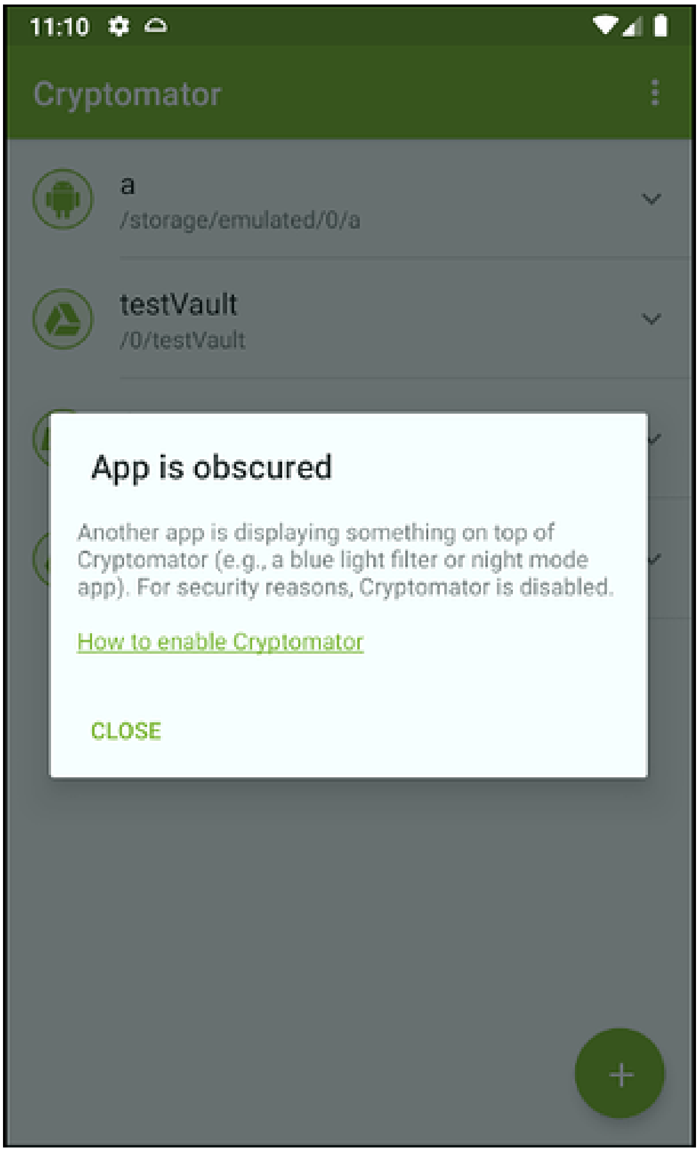
The reason for Cryptomator not working is that the user interface of Cryptomator is obscured. Whenever another app obscures Cryptomator, it could intercept the input done to Cryptomator or display a false UI tricking the user into doing stuff he does not want to do. For security reasons, Cryptomator is disabled by default when obscured. The Android documentation contains some more details.

Starting from version 1.3.0, this protection can be disabled in the settings. We rather recommend to use the app without a blue light filter because this is more secure.

If you want to disable protection, the blue light filter or any app obscuring Cryptomator has to be disabled one time. Afterwards, the settings can be opened and the option “Disable app when obscured” can be disabled. And then the relevant apps can be reenabled again.

To identify apps which could cause this, open the Android settings and navigate to **Settings - Apps - Advanced (gear icon) - Draw over other apps**. This will list the installed Apps and will show you which ones are allowed to draw over other apps. You can disable this for most apps (but not for system apps like the keyboard but this should not cause any problems).

If you see this dialog, some app is able to draw over Cryptomator:



App is obscured

Another app is displaying something on top of Cryptomator (e.g., a blue light filter or night mode app). For security reasons, Cryptomator is disabled.

How to enable Cryptomator

12.1.4 Screen Security

Android provides the possibility to prevent the system and other apps from doing screenshots, screen recordings etc. while Cryptomator is active. This feature is very important because it prevents other apps from reading data across the screen.

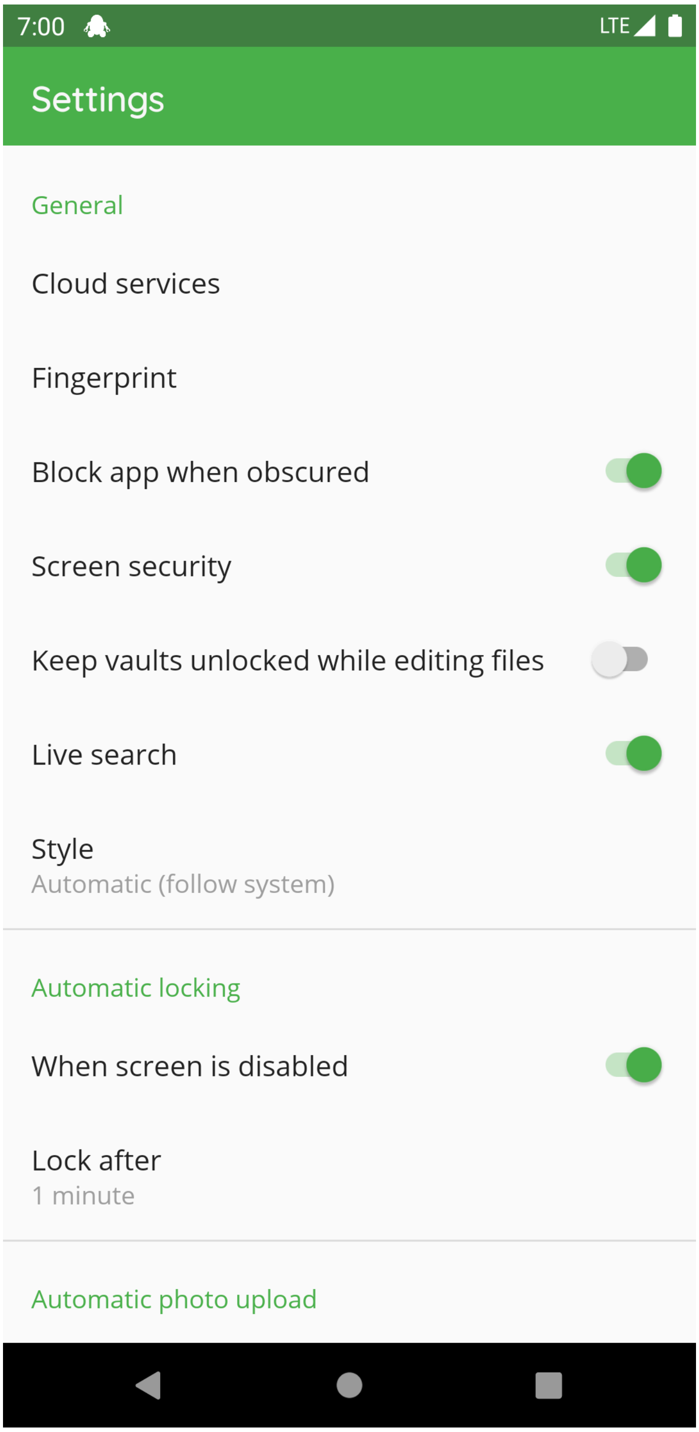
This feature is enabled for all our views. For some devices, e.g. a Chromebook with a second display or to create a screenshot and disable it again, we made this option since the 1.3.9 configurable.

Read more: FLAG*SECURE

12.1.5 Style

You can choose between the following three styles:

- Automatic (follow system): Follows the system specified in the Android settings
- Light: App shows in light mode
- Dark: App shows in dark mode



Settings

General

Cloud services

Fingerprint

Block app when obscured: on

Screen security: on

Keep vaults unlocked while editing files: off

Live search: on

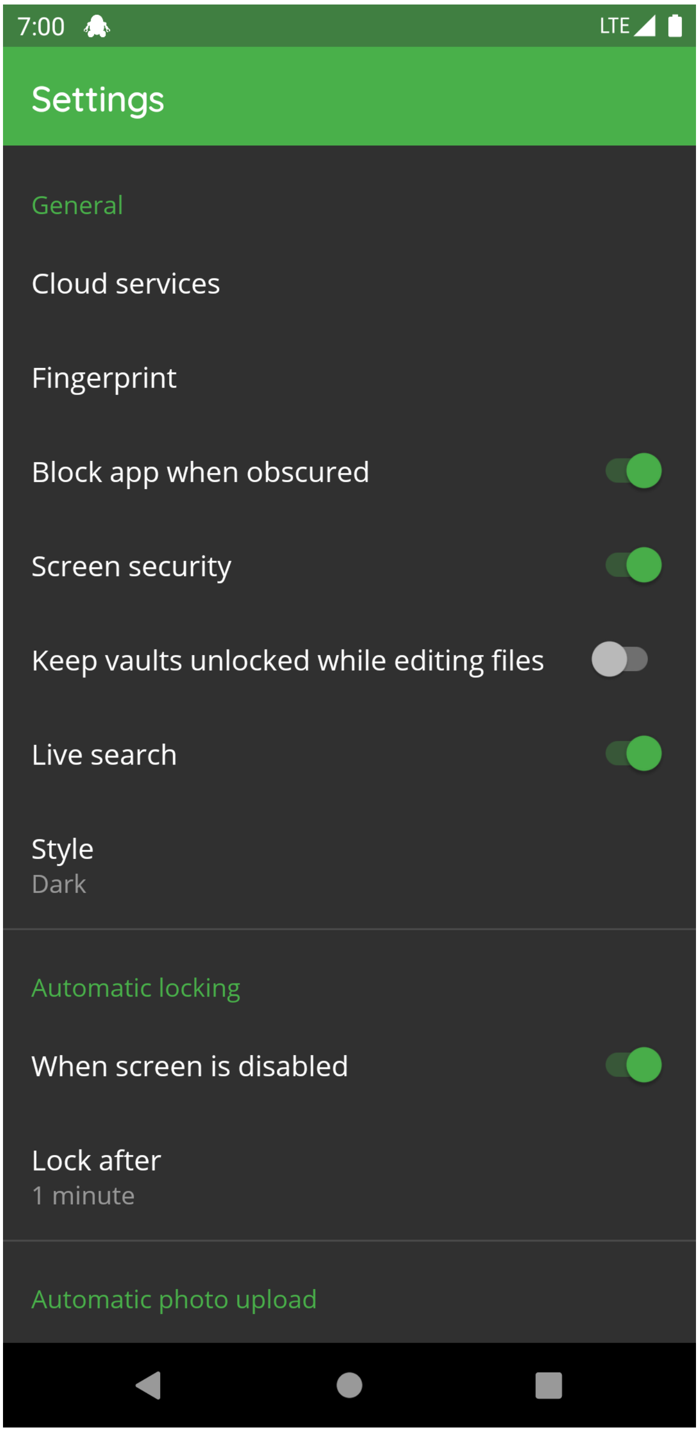
Style
Automatic (follow system)

Automatic locking

When screen is disabled: on

Lock after
1 minute

Automatic photo upload



Settings

General

Cloud services

Fingerprint

Block app when obscured ☑

Screen security ☑

Keep vaults unlocked while editing files ☐

Live search ☑

Style
Dark

Automatic locking

When screen is disabled ☑

Lock after
1 minute

Automatic photo upload

12.2 Search

You can use the magnifier inside the cloud node list to search for specific nodes. Thereby there are two settings:

- Live search (disabled by default)
- Search using glob pattern matching (disabled by default)

both are described in the following chapters.

12.2.1 Live Search

If this setting is enabled, the search mode is `live`. That means, the search starts immediately after entering the search pattern.

If it is disabled, you have to use the magnifier or the enter button in your keyboard to start the search.

12.2.2 Search using glob pattern matching

If this setting is enabled, you have to enter a glob pattern into the search bar.

If it is disabled, the beginning of the cloud node names must match the entered text. Upper and lower case is not relevant in this option.

12.3 Automatic Locking

If a vault is unlocked and Cryptomator isn't active, the automatic locking timeout is counting down. After the timeout expires, all vaults get locked. You can choose between:

- 1 minute
- 2 minutes
- 5 minutes
- 10 minutes
- Never

`When screen is disabled` can be deactivated so that the vaults don't get locked when the screen locks.

12.4 Automatic Photo Upload

If the `Automatic photo upload` is enabled, all photos taken will be marked for upload and after the specified vault gets unlocked again, the upload starts.

Under the setting `Choose vault for upload`, you can specify the target vault and folder in the vault where the images will be placed.

Which pictures will be tracked, depends on the Android version on your phone:

- Nougat (API level 24 or 7.x) and later: All images which Android adds to the gallery will be uploaded to the vault
- Pre-Nougat: Only the images created with the camera will be uploaded to the vault

12.5 Cache

Introduced in version 1.5.0, if enbaled, all downloaded files will be cached (encrypted) on the file system. Further downloads will only verify with the server, that the cached file is still the latest version. If so it will not be downloaded again but directly retrieved from the file system. The cache is implemented using a least recently used mechanism, that means, the oldest entry will be overwritten if the max cache size is reached.

12.5.1 Cache Size Per Cloud

Using this setting, you can specify the total max cache size per cloud provider.

You can choose between the following options:

- 50 MB
- 100 MB
- 250 MB
- 500 MB
- 1 GB
- 5 GB

Note: The more memory is given to caching, the greater the convenience factor. However, this memory can be used up to the maximum on the system and is then no longer available.

12.5.2 Clear Cache

This setting will flush all cached files.

12.6 Support

If you have problems with the app you can enable the `Debug mode`. After reproducing the problem, you can disable the `Debug mode` again and `Send log file`.

12.7 Advanced Settings

12.7.1 Workaround opening Microsoft files

With this setting enabled, files are opened in Microsoft applications with write permission.

Due to a bug in Microsoft apps, the file to be edited must be shared with these apps in a public media folder on the device. After Cryptomator is resumed, the publicly accessible file is deleted again but Cryptomator cannot influence what has happened to this file in the meantime. Make sure that you are aware of this behavior when activating this option. This will only apply to Microsoft file types.

12.7.2 Keep unlocked

With this setting enabled, all vaults remain unlocked when a file is opened by a third-party application, which can be useful in combination with the "Workaround opening Microsoft files".

12.7.3 Accelerate Unlock

Download files to unlock the vault in the background while prompted to enter the password or biometric authentication. Keep it activated unless unlocking the vault does not work.

12.8 Version

This setting displays the current version of this app.

The following sub settings are only available, if you're using the APK-Store version of Cryptomator and not the PlayStore one.

12.8.1 Update Check Interval

Using the specified interval below, the app checks if the latest version is installed.

You can choose between the following options:

- Once a day
- Once a week
- Once a month
- Never

12.8.2 Check For Updates

This setting displays the timestamp of the latest update check. You can click on this setting to trigger a update check.

CHAPTER

THIRTEEN

SETUP

You can get Cryptomator for iOS on the App Store.

13.1 Requirements

Requires iOS 13.0 or later. Compatible with iPhone, iPad, and iPod touch.

CHAPTER

FOURTEEN

CLOUD MANAGEMENT

14.1 Other File Provider

This option allows you to add a vault from any supported file provider. Default implementations by Apple are iCloud Drive and On My iPhone/iPad. Inside the Files app, you can also add custom connections to SMB-compatible servers.

If you have a lot of apps installed that include a file provider, you may notice that most of them are grayed out. This is because third-party file providers usually don't support "picking folders". To our best of knowledge, this is unsupported by Apple. You can find a technical discussion here.

CHAPTER

FIFTEEN

VAULT MANAGEMENT

15.1 Unlock Duration

With the vault setting “Unlock Duration”, you can specify for how long you want your vault to stay unlocked when idle. The following options are:

- Let iOS Decide Automatically
- 5 Minutes
- 10 Minutes
- 30 Minutes
- 1 Hour
- Indefinite

The default option is “Let iOS Decide Automatically”. Accessing Cryptomator via the Files app is possible via a so-called File Provider Extension. This extension has limited capabilities, e.g., it has a lower memory limit than regular apps. To free up memory, iOS may terminate Cryptomator at any time, which is basically the same as locking the vault since the key is held in memory.

This option has two consequences:

- There is no guarantee for how long your vault stays unlocked. Of course, while you’re accessing your vault, it’s highly unlikely that Cryptomator gets terminated.
- You’re responsible for locking your vault manually. Or if that’s not a concern of yours, you can just let iOS decide when Cryptomator is getting terminated.

In order to have a guarantee that your vault stays unlocked for a certain amount of time, the other options are available. By using one of these options, a copy of your key needs to be stored in the iOS keychain, as long as your vault is unlocked.

E.g., if you choose “1 Hour” and Cryptomator gets terminated by iOS within that time frame, your vault can automatically be unlocked again using the key from the iOS keychain. If the selected time frame has passed, the key will be removed from the iOS keychain and your vault will get automatically locked.

If you choose the “Indefinite” option, your vault will be kept unlocked until you have manually locked it.

CHAPTER

SIXTEEN

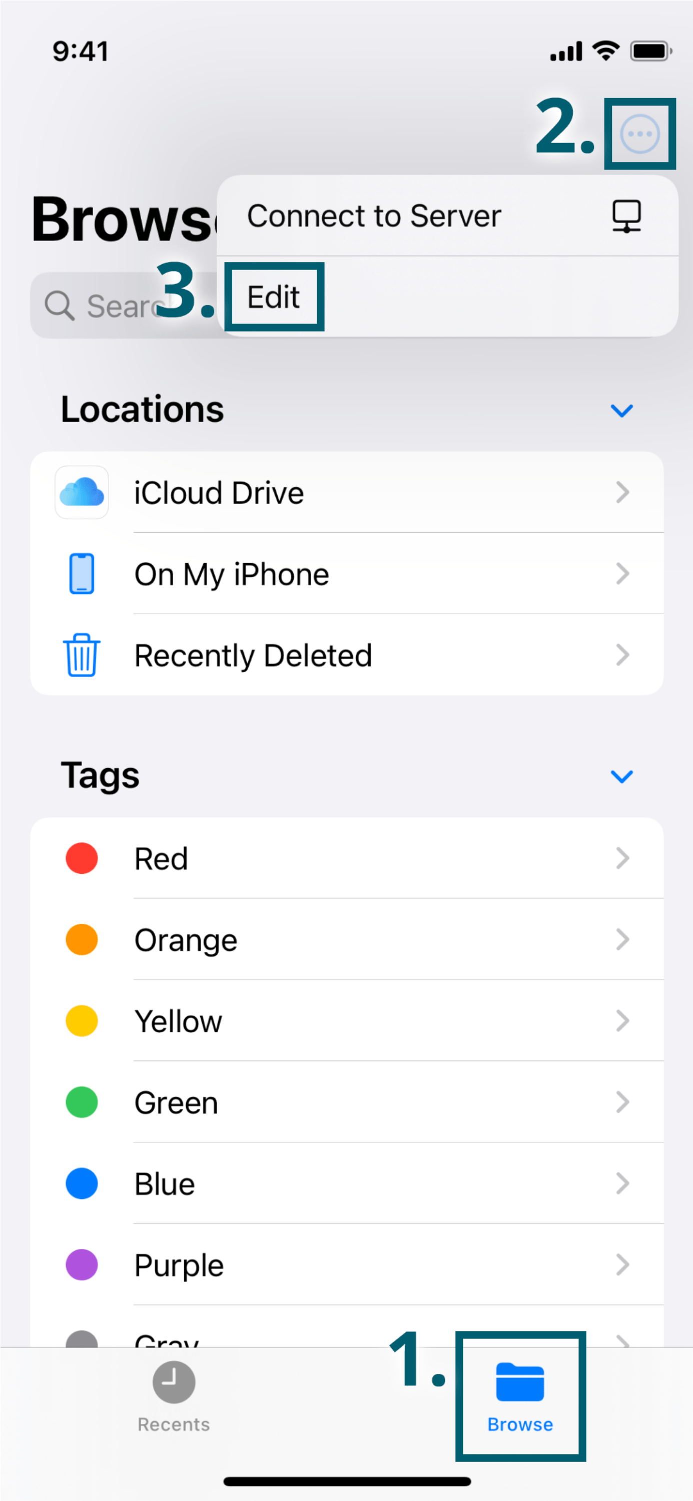
WORKING WITH VAULTS

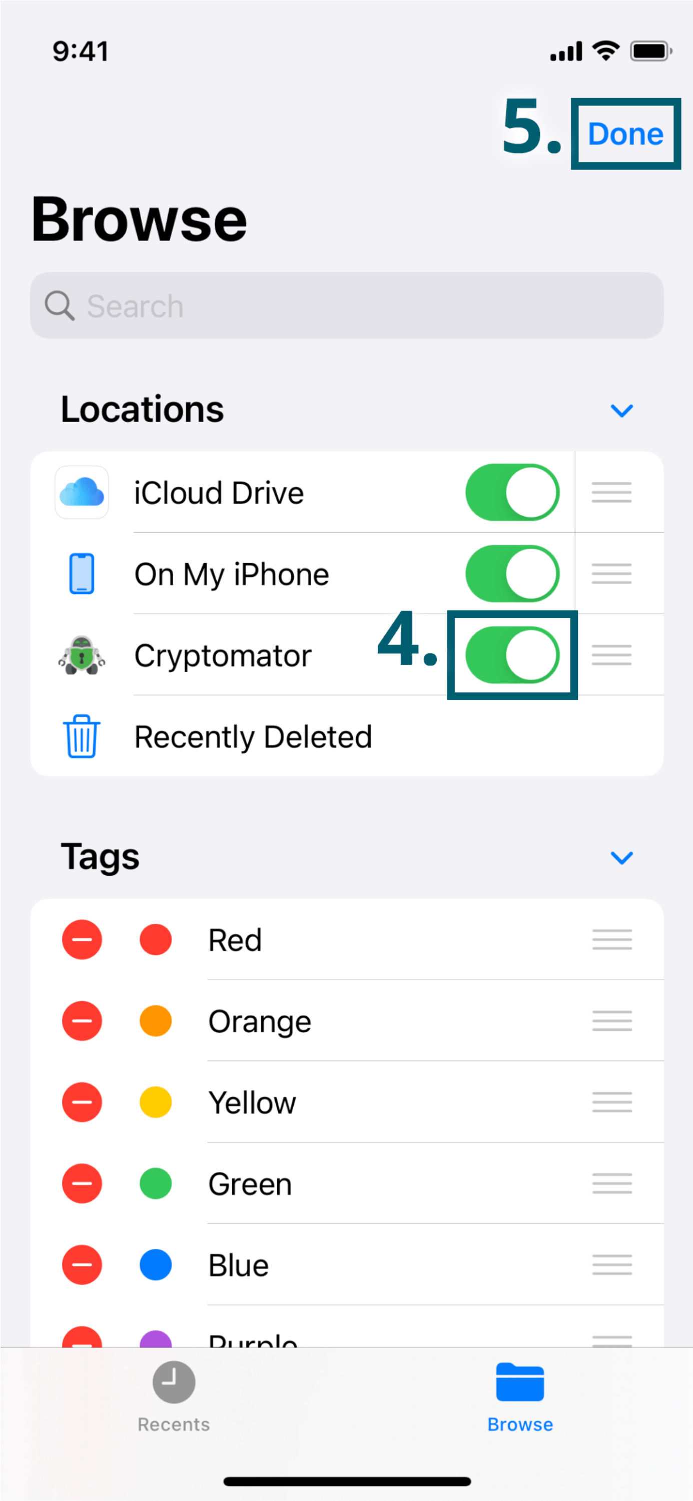
Cryptomator for iOS is fully integrated into the Files app of iOS. In order to access your encrypted data, you have to use the Files app.

16.1 Enable Cryptomator in Files App

In order for Cryptomator to be listed in the Files app under “Locations”, you may have to enable Cryptomator first. Open the Files app and then:

1. Tap on the **Browse** tab in the lower right corner.
2. Tap on the **(...)** button in the upper right corner.
3. Tap on **Edit**.
4. Enable **Cryptomator**.
5. Tap on **Done** in the upper right corner.


9:41
2.
Browse
Connect to Server
3.
Edit
Search
Locations
iCloud Drive
On My iPhone
Recently Deleted
Tags
Red
Orange
Yellow
Green
Blue
Purple
Gray
1.
Recents
Browse


9:41
5.
Done
Browse
Search
Locations
iCloud Drive
On My iPhone
Cryptomator
4.
Recently Deleted
Tags
Red
Orange
Yellow
Green
Blue
Purple
Recents
Browse

CHAPTER

SEVENTEEN

SETTINGS

You can configure Cryptomator to your needs. Access the settings by tapping the gear icon in the top left corner.

17.1 Support

If you have problems with the app, you can enable `Debug Mode`. After reproducing the problem, you should disable `Debug Mode` again and then `Send Log File`.

CHAPTER

EIGHTEEN

SHORTCUTS GUIDE

The Shortcuts integration of Cryptomator allows you to build different automations in the Shortcuts app. With that, you can automate recurring tasks quickly and easily.

For a shortcut to run smoothly, the vault must be unlocked during the execution of the shortcut. For automations, you should set the unlock duration to "Indefinite" in the *settings of your vault*.

In addition, you should know that some Cryptomator shortcut actions build on each other. For example, the "Save File" action requires a folder inside a vault as an input, which can be obtained using the "Get Folder" action.

18.1 Automatic Photo Upload

With Cryptomator's integration in Shortcuts, you can build an action to automatically upload your photos to a Cryptomator vault. You can either follow these step-by-step instructions or use the following shortcut to get started:

https://www.icloud.com/shortcuts/90ae0e36dda44da3a39c9070ae097a92

Step 1: Create new shortcut

- Open the Shortcuts app on your iOS device.
- Tap on the "+" at the top right to create a new shortcut.

If the Shortcuts app is not installed, download it from the App Store.

Step 2: Add "Find Photos" action

- Select the search field at the bottom to add an action.
- Under the tab "Apps", select "Photos".
- Select the action "Find Photos".

You can customize this action to your needs by adding various filters or to limit the number of photos to be selected.

Step 3: Add "Get Folder" action

- Add the "Get Folder" action from Cryptomator.
- Specify the vault and the path of the folder where your photos should be stored.

Important: It will check if the folder exists in your vault. If it doesn't exist, the action will fail and no photos will be uploaded.

Step 4: Add "Save File" action

We're going to add the "Save File" action from Cryptomator. But since this action only saves a single file (or in this case, photo), we need to add wrap this action around a different action first.

- Add the "Repeat with Each" action, which you can find under the "Categories" tab and then under "Scripting".
- Add the "Save File" action from Cryptomator.

- Make sure that the two variables are correctly set: The image you want to save and the folder from the "Get Folder" action in step 3.

In order to set these variables, you may have to tap on the "File" field, then "Select Magic Variable", and tap on "Repeat Item".

Congratulations, you have just created your first shortcut with Cryptomator actions!

Hints:

1. To fully automate your photo upload, you should run a shortcut using an automation. To do this, create a new automation in the Shortcuts app. You don't have to create the whole shortcut again. You can just add the action "Execute Shortcut" and select the previously created shortcut.
2. Executing a shortcut with a lot of photos (>1,000) can take much longer than executing it with 2x500 photos. To our knowledge, this seems to be a limitation of the Shortcuts app. Therefore, try to limit the number of photos using the available filters. One possible filter is to consider only the photos of the last 2-7 days for a shortcut that is executed daily.

18.2 Photo to PDF (Advanced Example)

Another example, inspired by community member JB, is to convert the latest photo to a PDF and save it in a vault under a chosen path. This example is a bit more advanced, but it shows how you can combine different actions to create a more complex automation. You can either follow these step-by-step instructions or use the following shortcut to get started:

https://www.icloud.com/shortcuts/3d8e20cbfe26452486f3629a2f104c94

We assume that you have already installed Shortcuts, see step 1 of the previous example.

Step 1: Add "Is Vault Unlocked" action

- Add the "Is Vault Unlocked" action from Cryptomator.
- Specify the vault you want to use.
- Add the "If" action from the "Scripting" category.
- Set the condition to "is" and the number to "0".

This makes sure that your vault is unlocked. If it is not, the shortcut will ask you to unlock it, see step 2.

Step 2: Add "Open Vault" action

- Add the "Open Vault" action from Cryptomator.
- Drag this action below the "If" action (and above "Otherwise").
- Specify the same vault you used before.
- Add the "Show Alert" action from the "Scripting" category.
- Drag this action below the "Open Vault" action (and above "Otherwise").
- Replace the informational message with something like "Unlock this vault and run this shortcut again".

This completes the "If" block. Now we can be certain that the vault is unlocked for the "Otherwise" block.

Step 3: Add "List" action

If you only want to save the PDF in one specific path, you can skip this step and go to step 4. Otherwise, you can add a list of paths to choose from.

- Add the "List" action from the "Scripting" category.
- Drag this action below the "Otherise" action (and above "End If").
- Customize this list to your needs by specifying paths of the folders where your PDFs could potentially be stored, something like a "favorites" list.

- Add the “Choose from List” action from the “Scripting” category.

Don’t worry about dragging these actions inside the “Otherwise” block of the “If” action, we’ll do that in the very end.

Step 4: Add “Get Latest Photos” + “Make PDF” actions

- Add the “Get Latest Photos” action from the “Media” category.
- Add the “Make PDF” action from the “Documents” category.

This is just an example. Shortcuts offer you many other ways to get the file or media that you could use as an input for encryption.

Step 5: Add “Get Folder” action

- Add the “Get Folder” action from Cryptomator.
- Select the variable “Chosen Item” for the path (or enter a specific path if you skipped step 3) and specify the same vault you used before.

Important: It will check if the folder exists in your vault. If it doesn’t exist, the action will fail and no PDF will be uploaded.

Step 6: Add “Save File” action

- Add the “Save File” action from Cryptomator.
- Make sure that the two variables are correctly set: The PDF you want to save and the folder from the “Get Folder” action in step 5.

Step 7: Finish “Otherwise” block

- Drag the “End If” action to the very bottom, which will enclose all actions that you have created between the steps 3 and 6 into the “Otherwise” block.

Congratulations, you have just created a more advanced shortcut with Cryptomator actions!

CHAPTER

NINETEEN

SETUP

Cryptomator Hub is a zero-knowledge key management solution that allows you to manage access to your vaults from a central component deployed on your own infrastructure.

19.1 Quickstart

1. Decide, on which web addresses you want to deploy Hub and Keycloak (and set up DNS and TLS termination, if required)
2. Use the Setup Wizard to generate a deployment descriptor template
3. Customize the template if needed (e.g., adjust the Ingress settings) and deploy the software stack to your cluster
4. Log in to Keycloak to
    - adjust authentication settings
    - set up users/groups or LDAP/AD
5. Log in to Cryptomator Hub and start creating Hub-managed vaults

19.2 More Details

To get started, use the Setup Wizard to generate the necessary configuration files.

Cryptomator Hub depends on Keycloak, an open-source identity and access management solution. That means, Hub manages access to your vaults whereas Keycloak manages users, groups, and authentication. In the Setup Wizard, you will have the option to choose between deploying Keycloak alongside Hub or specifying an URL to an existing Keycloak installation.

19.3 Reverse Proxy

Cryptomator Hub must be used behind a reverse proxy such as Traefik or Nginx. In the Setup Wizard you can already add rules for some reverse proxies like Traefik. As mentioned there, you will still need a running Traefik deployment.

If you don't have a running Traefik deployment and want to use Docker Compose to run Hub, you can use the following as starting point:

```
networks:
  srv:
    name: srv

services:
```

(continues on next page)

(continued from previous page)

```
  traefik:
    image: traefik:v2.9
    command:
      # Provider
      - '--providers.docker'
      - '--providers.docker.exposedbydefault=false'
      - '--providers.docker.network=srv'
      # Entrypoints
      - '--entrypoints.web.address=:80'
      - '--entrypoints.web.http.redirections.entrypoint.to=websecure'
      - '--entrypoints.websecure.address=:443'
      # Let's Encrypt
      - '--certificatesresolvers.myresolver.acme.email=TODO' # TODO change
      - '--certificatesresolvers.myresolver.acme.httpchallenge.entrypoint=web'
      - '--certificatesresolvers.myresolver.acme.httpchallenge=true'
      - '--certificatesresolvers.myresolver.acme.storage=/letsencrypt/acme.json'
      # Uncomment to use staging for testing
      # - '--certificatesresolvers.myresolver.acme.caserver=https://acme-staging-v02.
↪api.letsencrypt.org/directory'
      - '--entrypoints.websecure.http.tls.certresolver=myresolver'
      # Logs
      - '--accesslog.filepath=/logs/access.log'
      - '--accesslog.format=json'
      - '--log.filepath=/logs/traefik.log'
      - '--log.format=json'
      - '--log.level=ERROR'
      # Misc
      - '--api.dashboard=false'
      - '--global.checknewversion=false'
      - '--global.sendanonymoususage=false'
      - '--ping'
    ports:
      - '80:80'
      - '443:443'
    networks:
      - 'srv'
    restart: always
    healthcheck:
      test: ['CMD', 'traefik', 'healthcheck', '--ping']
      interval: 10s
      timeout: 10s
      retries: 5
    volumes:
      - '/var/run/docker.sock:/var/run/docker.sock'
      - './logs:/logs'
      - './letsencrypt:/letsencrypt'
    labels:
      - 'traefik.enable=false'
```

Some remarks

1. There are a lot of other features of Traefik like Promeheus metrics generation, API frontend, … but we wanted to keep the deployment as simple as possible
2. This deployment uses Let's encrypt in HTTP challenge mode to create and update a TLS certificate for Hub/Keycloak. There are other methods available such as DNS or TCP challenge, see https://doc.traefik.io/traefik/https/overview/ for more information

3. Make sure you add `logs/access.log` to your log rotation, otherwise this file can grow very quickly

Before running this deployment

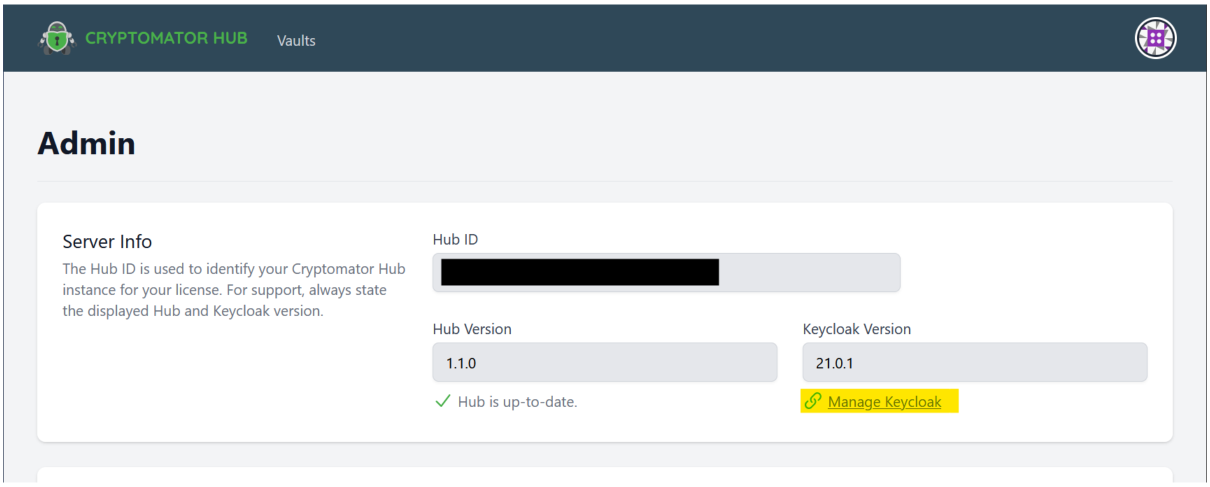
1. You must set a valid email address in `TODO`
2. You must have ports 80 and 443 open on the host machine
3. You need to create for Hub and optionally Keycloak DNS entries (`CNAME`, or `A` record) for the domain entered in the Setup Wizard of Hub
4. Create a Hub deployment using the Setup Wizard with `include Traeffik` selected and merge the content with this file:

1. Copy the `hub-internal: {}` section of the Setup Wizard to this `networks`
2. Copy all services of the Setup Wizard under the `services` section to this `services`
3. Copy the `volumes` from the Setup Wizard to this file

Troubleshooting: If you encounter problems, check the log files in `logs/traffik.log` and `logs/access.log`. Make sure you entered `srv` as `Public Network` in the Setup Wizard of Hub.

19.4 Keycloak Administration

User and group management is done via Keycloak. You can access the Keycloak management interface over the admin section of Hub.



Admin

Server Info

The Hub ID is used to identify your Cryptomator Hub instance for your license. For support, always state the displayed Hub and Keycloak version.

Hub ID: [redacted]

Hub Version: 1.1.0

✓ Hub is up-to-date.

Keycloak Version: 21.0.1

Manage Keycloak

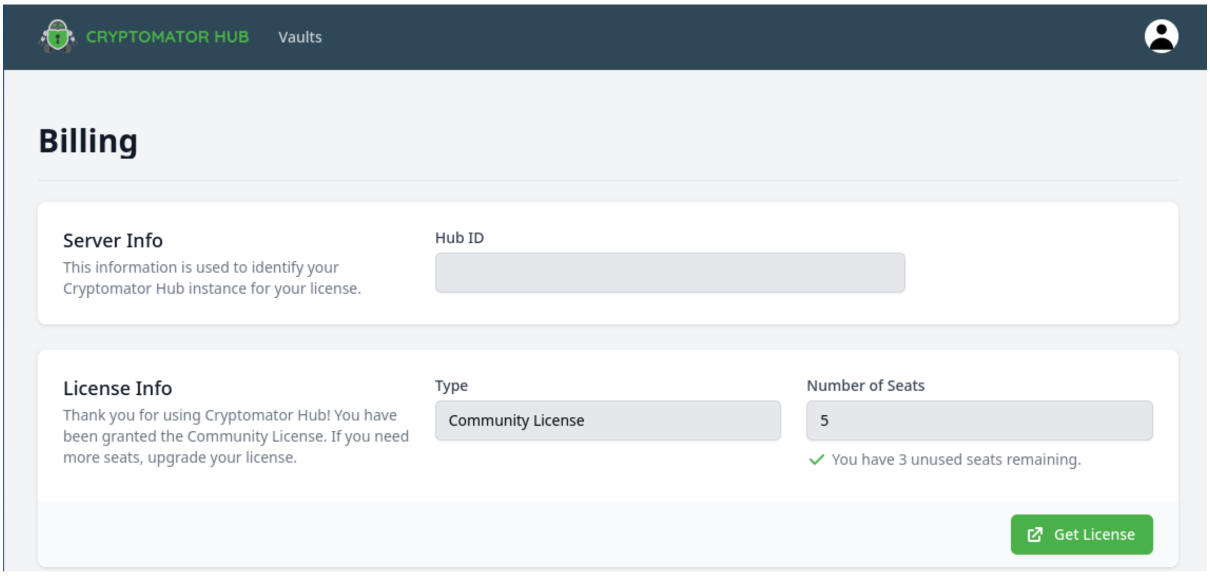
There you can create users, delete users, manage groups, and optionally also synchronize users/groups to Keycloak using LDAP to whom you can then give access to vaults in Hub. Other identity providers such as `OpenID Connect` or `SAML` can also be used. However, they work slightly differently: With `LDAP`, all users and groups are imported and synchronised with Keycloak, so they are available immediately after setup. With `OpenID Connect` or `SAML`, users are unknown to Keycloak and Hub until they log in. This is why we strongly recommend using `LDAP`.

In Keycloak you will find a user called `syncer`. It is used to synchronise all users and groups from Keycloak to Hub, so please do not delete or change it.

Note: Subgroups are not supported at this time.

19.5 Billing

When Cryptomator Hub is freshly installed, it comes with a community license.



Billing

Server Info

This information is used to identify your Cryptomator Hub instance for your license.

Hub ID:

License Info

Thank you for using Cryptomator Hub! You have been granted the Community License. If you need more seats, upgrade your license.

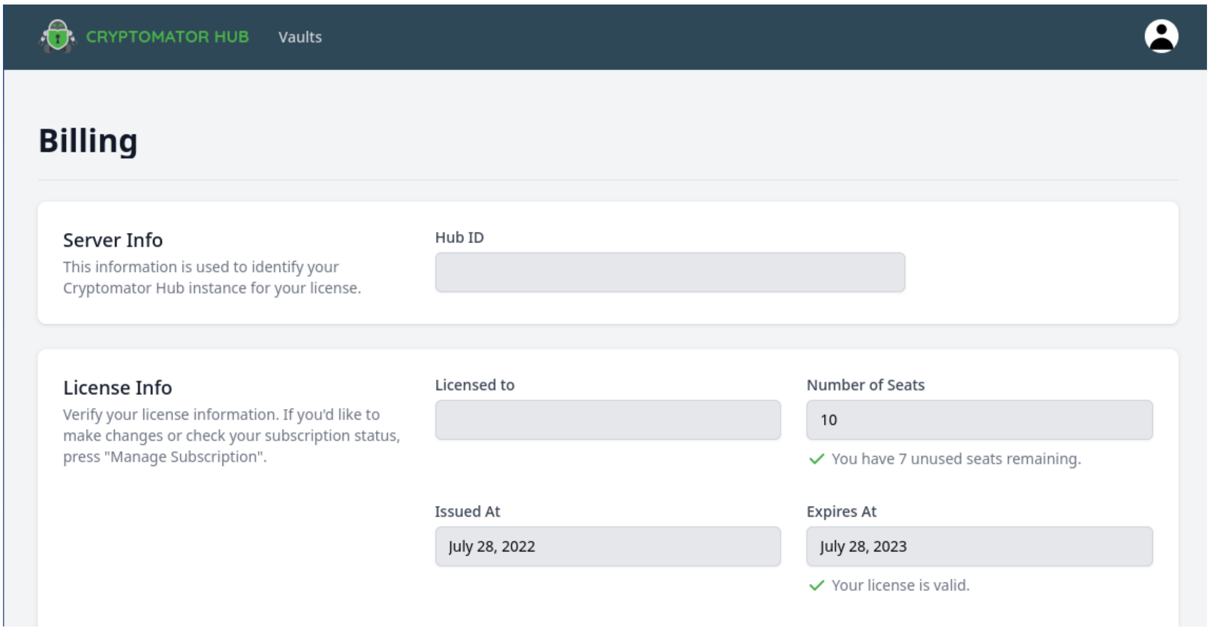
Type: Community License

Number of Seats: 5

✓ You have 3 unused seats remaining.

This license is valid for 5 seats. Only users assigned to a vault will occupy a seat.

The `Get License` button will direct you to an external website at cryptomator.org where you can buy a license for this instance. If successful, you will be automatically redirected back to your Hub instance.



Billing

Server Info

This information is used to identify your Cryptomator Hub instance for your license.

Hub ID:

License Info

Verify your license information. If you'd like to make changes or check your subscription status, press "Manage Subscription".

Licensed to:

Number of Seats: 10

✓ You have 7 unused seats remaining.

Issued At: July 28, 2022

Expires At: July 28, 2023

✓ Your license is valid.

19.6 Requirements

Currently, we are evaluating the system requirements for Cryptomator Hub. If you can provide data, please send us an email to hub@cryptomator.org.

19.7 Backup

Cryptomator Hub and Keycloak both write to the connected Postgres database. So the best and easiest way is to backup it cyclically using e.g. a Cron Job. Depending on your deployment, here is a sample command that you can run on the host system to backup the entire databases to a file using the Postgres container, which you than could import in a similar way:

```
Docker:
docker exec -u postgres -it postgres /bin/bash -c /usr/local/bin/pg_dumpall \
    > "$(date +%F)-hub-backup"

Kubernetes:
kubectl exec -it deployments/postgres -n NAMESPACE \
    -- /usr/local/bin/pg_dumpall -U postgres > "$(date +%F)-hub-backup"
```

See https://www.postgresql.org/docs/current/app-pg-dumpall.html for more information on the *pg_dumpall* command. The command will create a file on the host with a name like “2023-02-06-hub-backup”.

Besides *pg_dumpall* Postgres offers with *psql -f PATH_TO_FILE* a command to restore the database from this file and a new system is completely at the state of this file.

If you also back up the deployment script, you can restore the entire solution to production in minutes.

Note: Make sure this backup is moved to another secure location.

CHAPTER

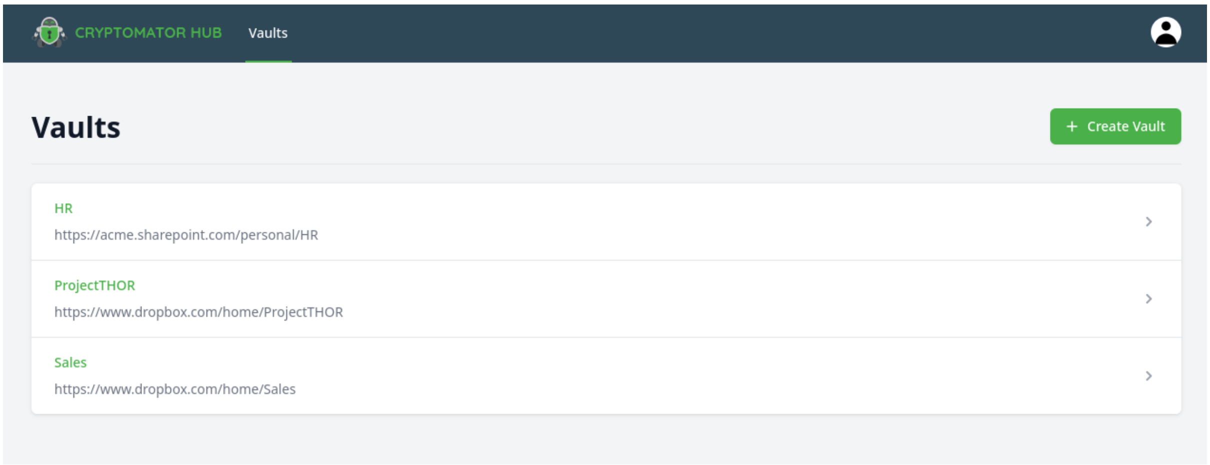
TWENTY

VAULT MANAGEMENT

This section contains instructions to manage vaults in Cryptomator Hub.

20.1 Vault List

The vault list is the main page of Cryptomator Hub. Here, all vaults which are shared with you, are listed. After signing in, Hub redirects you to this list. Alternatively, you can also access the list by clicking on the `Vaults` tab in the navigation bar.



HR
https://acme.sharepoint.com/personal/HR

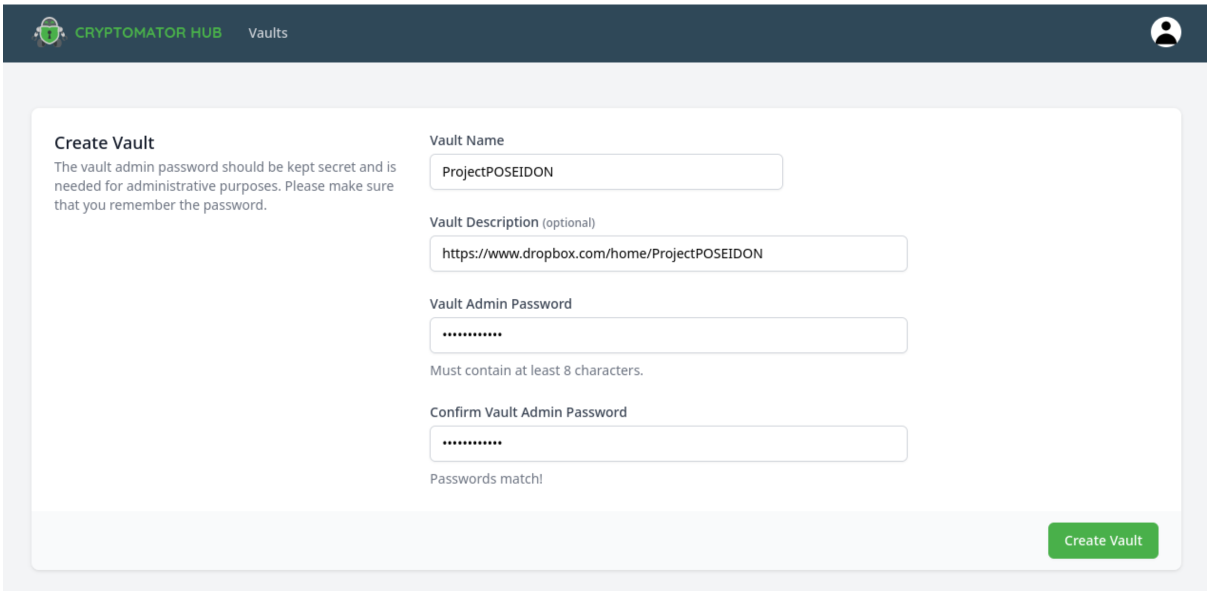
ProjectTHOR
https://www.dropbox.com/home/ProjectTHOR

Sales
https://www.dropbox.com/home/Sales

Note: Even if you are an administrator of the Hub instance, only vaults which are shared with you are listed.

20.2 Create a Vault

To create a vault in Hub, navigate to the vault list and click on the `Create Vault` button in the top right corner. Every vault has a name and an admin password. Fill out the form and continue the process by clicking the `Create Vault` button in the right corner.



Create Vault

The vault admin password should be kept secret and is needed for administrative purposes. Please make sure that you remember the password.

Vault Name: ProjectPOSEIDON

Vault Description (optional): https://www.dropbox.com/home/ProjectPOSEIDON

Vault Admin Password: ••••••••••••

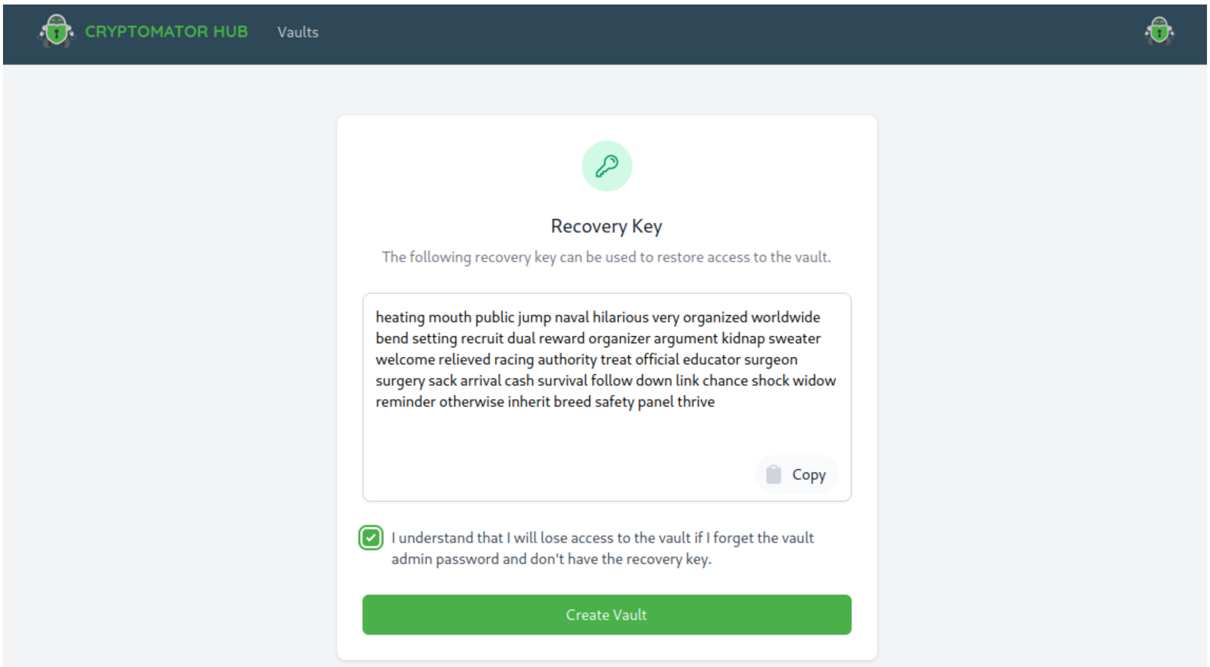
Must contain at least 8 characters.

Confirm Vault Admin Password: ••••••••••••

Passwords match!

Note: The vault admin password is needed to grant or revoke access to the vault. It is not used to unlock the vault in Cryptomator apps.

In the next step, the vault *recovery key* is displayed. It can *restore access to the vault data* in case of an emergency, e.g. if the vault administrator password is lost or Cryptomator Hub is down. Store it at a safe location, tick the checkbox and complete the setup by clicking the `Create Vault` button at the bottom



Recovery Key

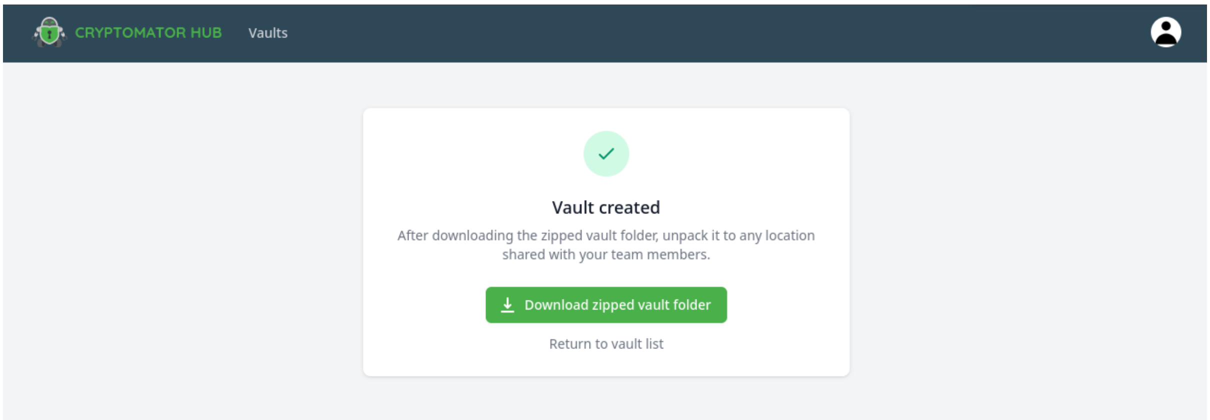
The following recovery key can be used to restore access to the vault.

heating mouth public jump naval hilarious very organized worldwide bend setting recruit dual reward organizer argument kidnap sweater welcome relieved racing authority treat official educator surgeon surgery sack arrival cash survival follow down link chance shock widow reminder otherwise inherit breed safety panel thrive

☑ I understand that I will lose access to the vault if I forget the vault admin password and don't have the recovery key.

Warning: The recovery key is **highly confidential**. It is a human readable form of the vault *masterkey*, which is used to encrypt your data and independent of the key management in Cryptomator Hub.

When the setup is finished, you have the opportunity to download the initial vault template and place it in your desired cloud storage location. You can unlock the vault and place data inside with Cryptomator. If you skip this step, you can download the template *later*.

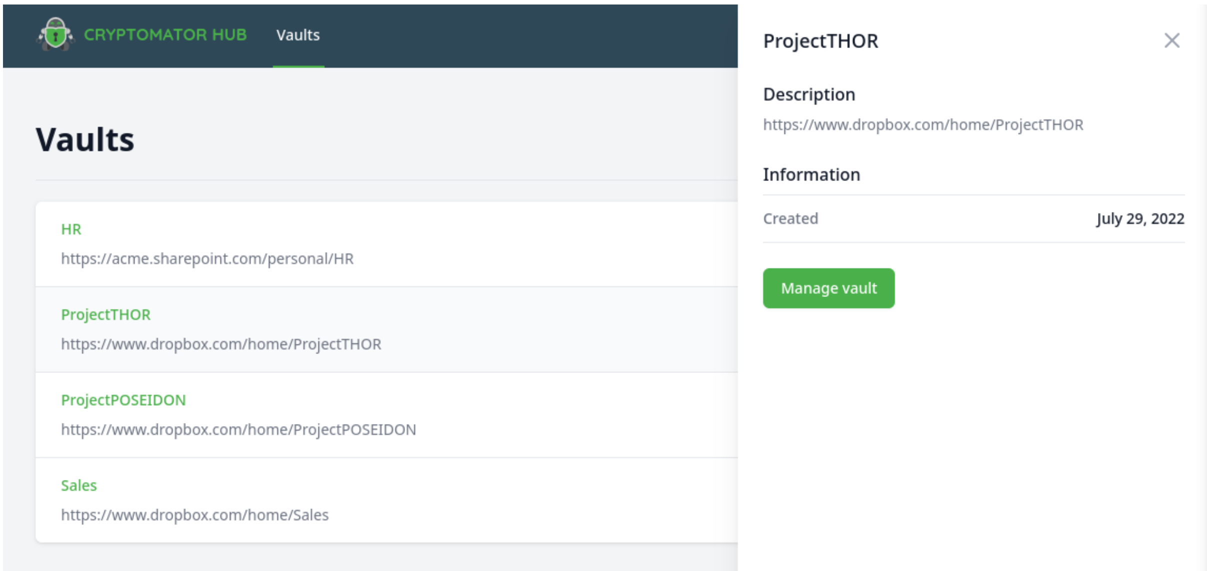


Vault created

After downloading the zipped vault folder, unpack it to any location shared with your team members.

20.3 Vault Details

The vault details page shows metadata of a vault (e.g. creation date) and contains the management section of the vault (e.g. grant a user access). To open it, navigate to the vault list and click on entry in the list. The details are displayed on the right side.



Vaults

HR
https://acme.sharepoint.com/personal/HR

ProjectTHOR
https://www.dropbox.com/home/ProjectTHOR

ProjectPOSEIDON
https://www.dropbox.com/home/ProjectPOSEIDON

Sales
https://www.dropbox.com/home/Sales

ProjectTHOR

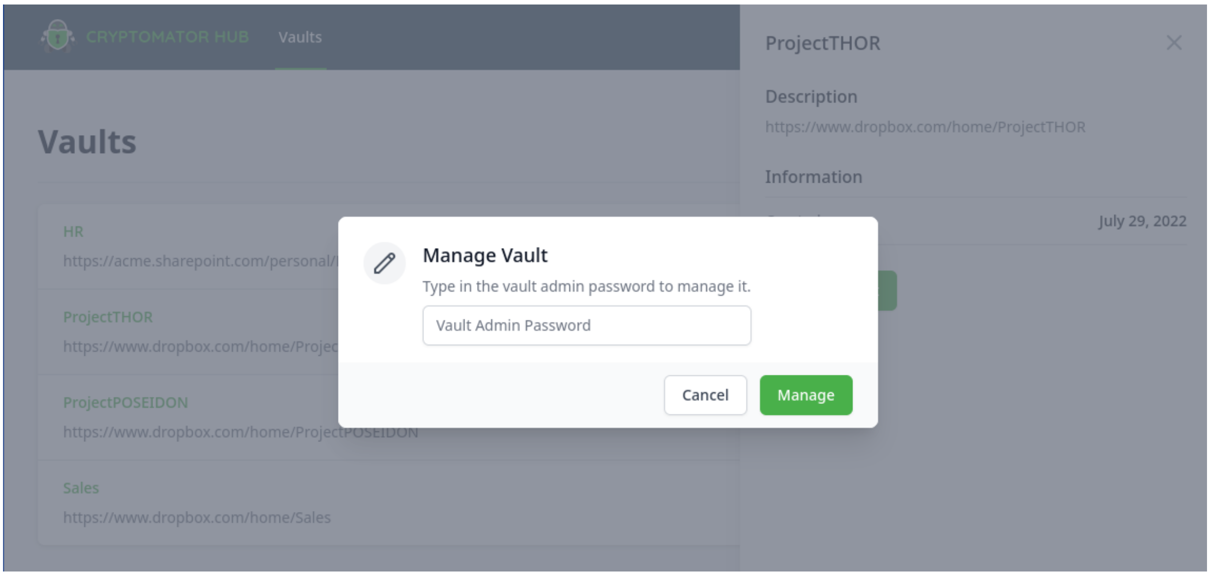
Description
https://www.dropbox.com/home/ProjectTHOR

Information

Created	July 29, 2022

20.3.1 Manage Vault

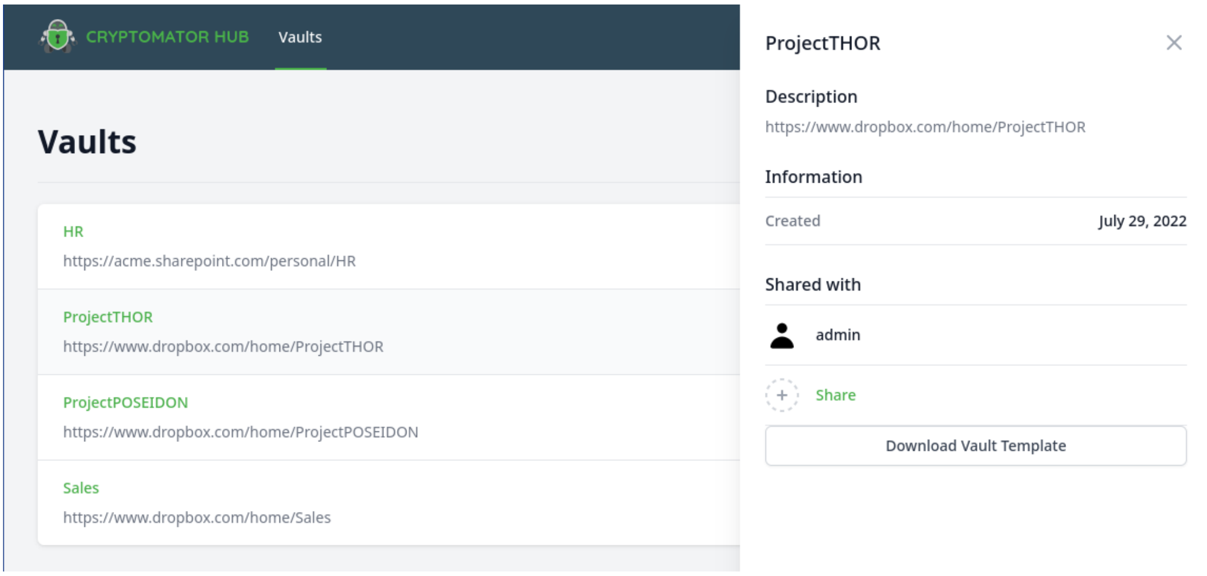
To add a user, grant devices access, or view the members list, you have to enable the management section in the vault details. Open the vault details and click the `Manage Vault` button. In the dialog, enter the vault admin password.


CRYPTOMATOR HUB
Vaults
Vaults
HR
https://acme.sharepoint.com/personal/
ProjectTHOR
https://www.dropbox.com/home/Projec
ProjectPOSEIDON
https://www.dropbox.com/home/ProjectPOSEIDON
Sales
https://www.dropbox.com/home/Sales
ProjectTHOR
Description
https://www.dropbox.com/home/ProjectTHOR
Information
July 29, 2022
Manage Vault
Vault Admin Password
Cancel
Manage

Type in the vault admin password to manage it.

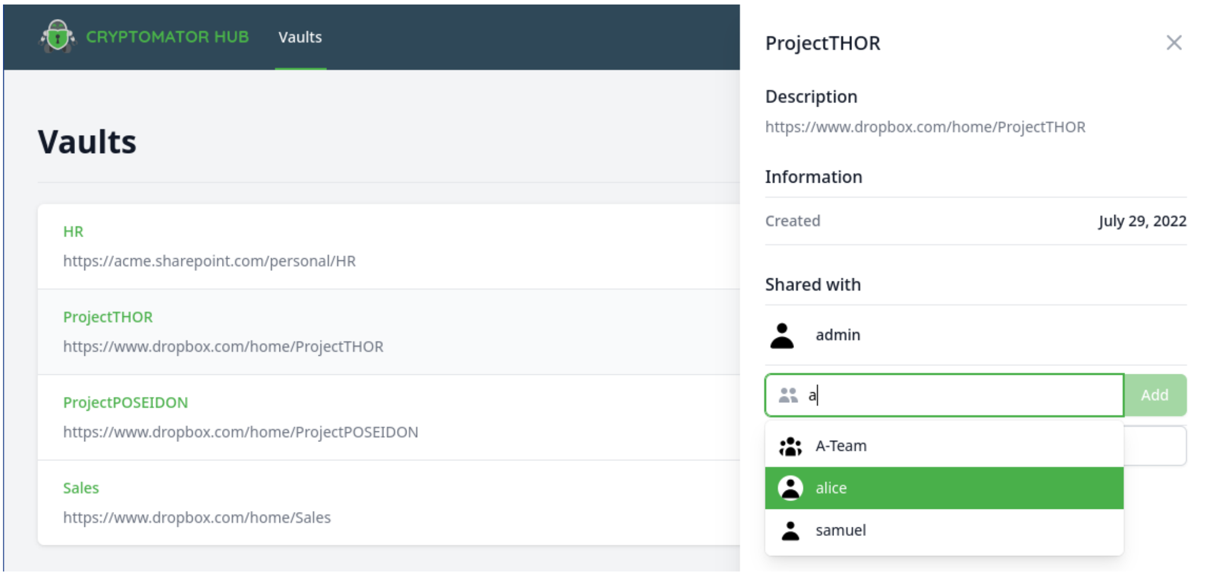
If the password is correct, the vault details view is enriched with more elements:

- `Shared with` members list
- `Download Vault Template` button
- `Update Permissions` button (only shown if necessary)


CRYPTOMATOR HUB
Vaults
Vaults
HR
https://acme.sharepoint.com/personal/HR
ProjectTHOR
https://www.dropbox.com/home/ProjectTHOR
ProjectPOSEIDON
https://www.dropbox.com/home/ProjectPOSEIDON
Sales
https://www.dropbox.com/home/Sales
ProjectTHOR
Description
https://www.dropbox.com/home/ProjectTHOR
Information
Created
July 29, 2022
Shared with
admin
Share
Download Vault Template

Add a User

If a user should have access to this vault, you need to share it with the user. Click on the `Share` button in the `Shared with` list. A search field opens up where you can search for users and groups.

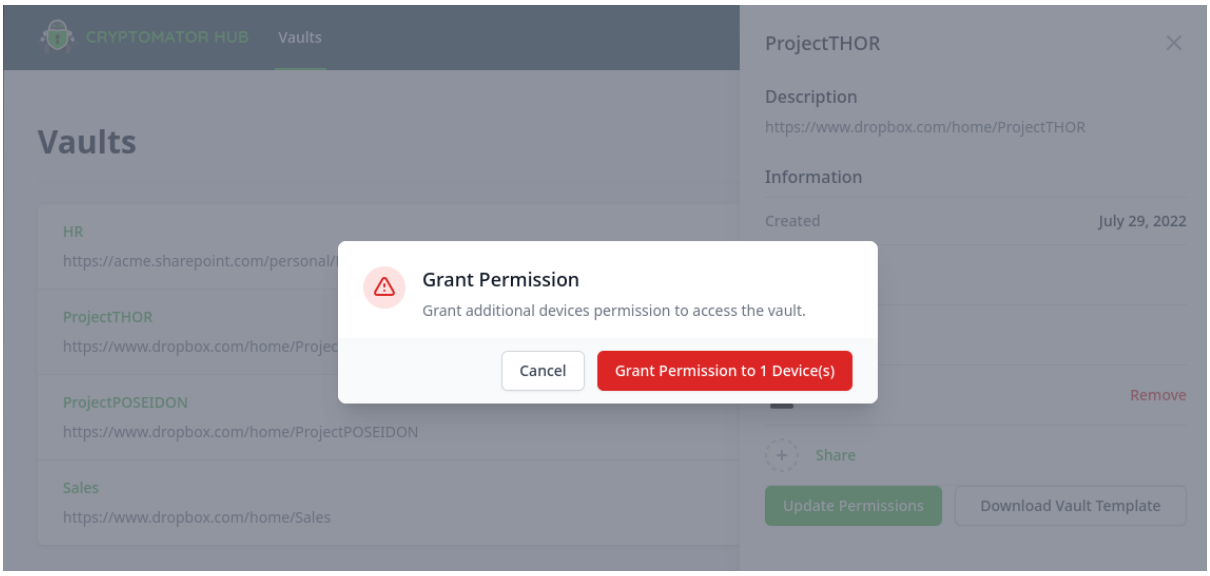

CRYPTOMATOR HUB
Vaults
Vaults
HR
https://acme.sharepoint.com/personal/HR
ProjectTHOR
https://www.dropbox.com/home/ProjectTHOR
ProjectPOSEIDON
https://www.dropbox.com/home/ProjectPOSEIDON
Sales
https://www.dropbox.com/home/Sales
ProjectTHOR
Description
https://www.dropbox.com/home/ProjectTHOR
Information
Created
July 29, 2022
Shared with
admin
a
Add
A-Team
alice
samuel

To add a user or group, select it from the results list and click the `Add` button.

Note: Currently, users and groups can only be *managed via Keyloak*.

Update Permissions

If a member of this vault registers a new device or still has unauthorized devices, an admin of the vault has to grant access to these devices explicitly. Only then, the user can unlock the vault with the device. As a vault admin, you can see that an update is necessary when an `Update Permissions` button appears.


Grant Permission

Grant additional devices permission to access the vault.

CRYPTOMATOR HUB
Vaults
Vaults
HR
https://acme.sharepoint.com/personal/
ProjectTHOR
https://www.dropbox.com/home/Projec
ProjectPOSEIDON
https://www.dropbox.com/home/ProjectPOSEIDON
Sales
https://www.dropbox.com/home/Sales
ProjectTHOR
Description
https://www.dropbox.com/home/ProjectTHOR
Information
Created
July 29, 2022
Cancel
Grant Permission to 1 Device(s)
Remove
Share
Update Permissions
Download Vault Template

20.4 Import a Vault

If you have a existing, password-based Cryptomator vault and want to switch to centralized, password-less user access management, you can import the vault in Cryptomator Hub. For a successful import, the *recovery key* of the vault and write access to its storage location is needed

The import is done via the Hub vault recovery feature. Follow the *vault online recovery guide* and use the recovery key of the password-based vault in the process. Don't forget to replace the vault config file `vault.cryptomator` at the vault storage location at the end. Finally, to ensure that the vault cannot be unlocked with its old password anymore, remove the file `masterkey.cryptomator` and all backup files (ending with `.bkup`).

CHAPTER

TWENTYONE

WORKING WITH VAULTS

Note: Vaults created with Hub are unlocked with the regular Cryptomator apps for desktop, Android and iOS. They can be downloaded here.

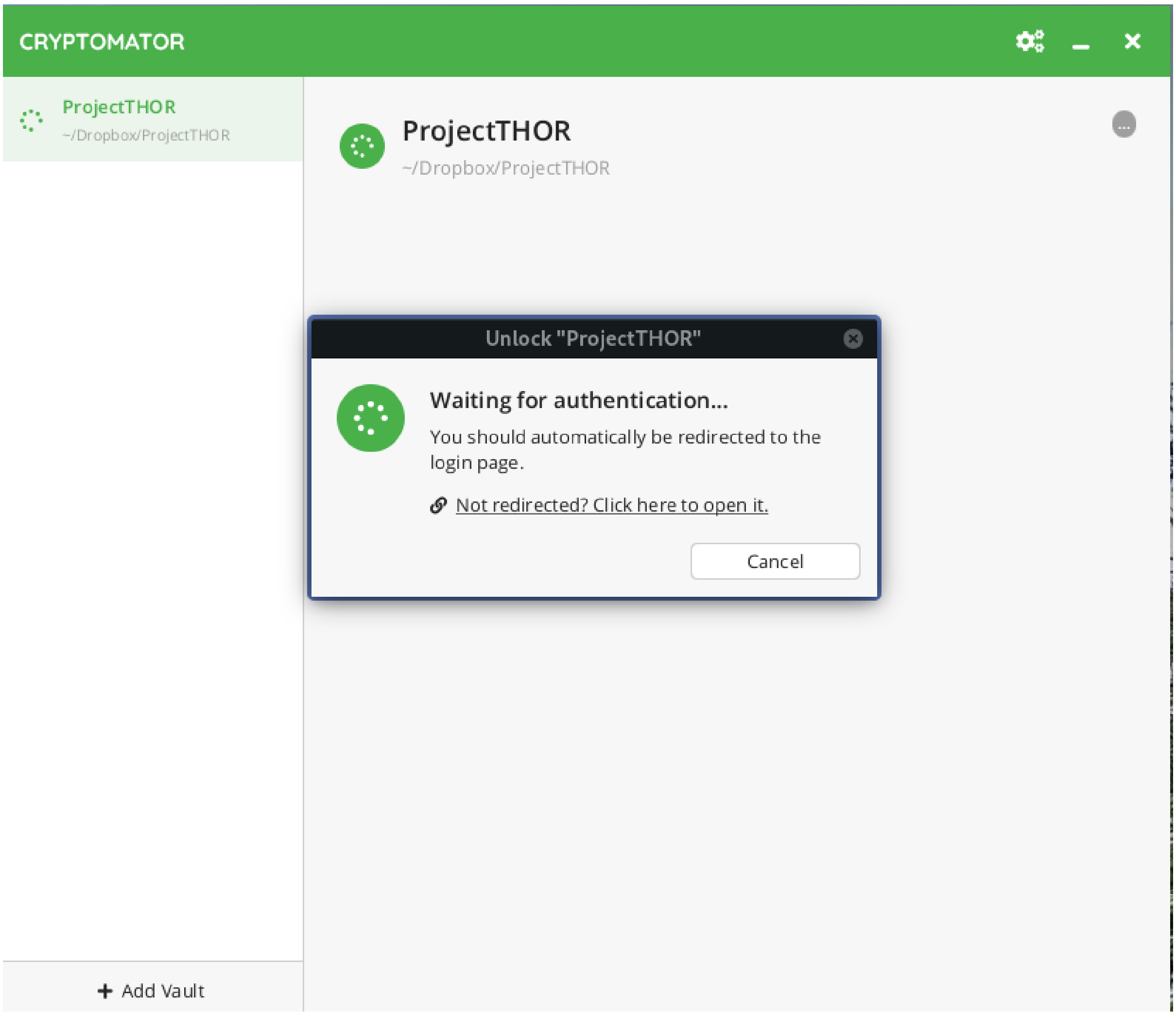
This section describes exemplarily how to unlock a vault in the Desktop app. Android and iOS work analogously.

As described in *open an existing vault*, you should have already added the vault to the vault list, e.g., by selecting the *vault.cryptomator* file.

21.1 Unlocking a Vault

21.1.1 1. Click Unlock

To unlock the vault, click on the large `Unlock` button in the center of Cryptomator's main window.

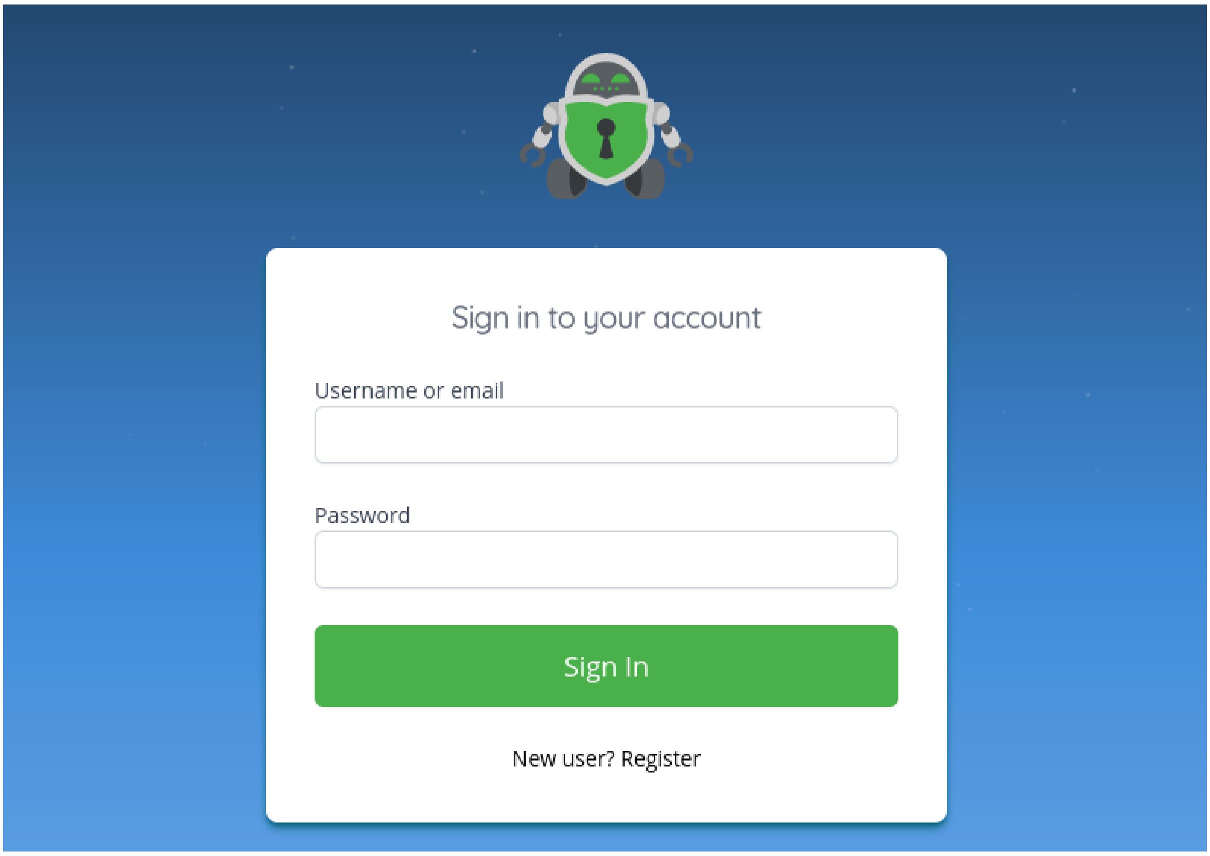


Waiting for authentication...

You should automatically be redirected to the login page.

21.1.2 2. Authenticate

Cryptomator should open your default browser for authentication. If you're not already logged in, you need to provide your user credentials, e.g., by entering your username and password or by inserting your key when WebAuthn is enabled.



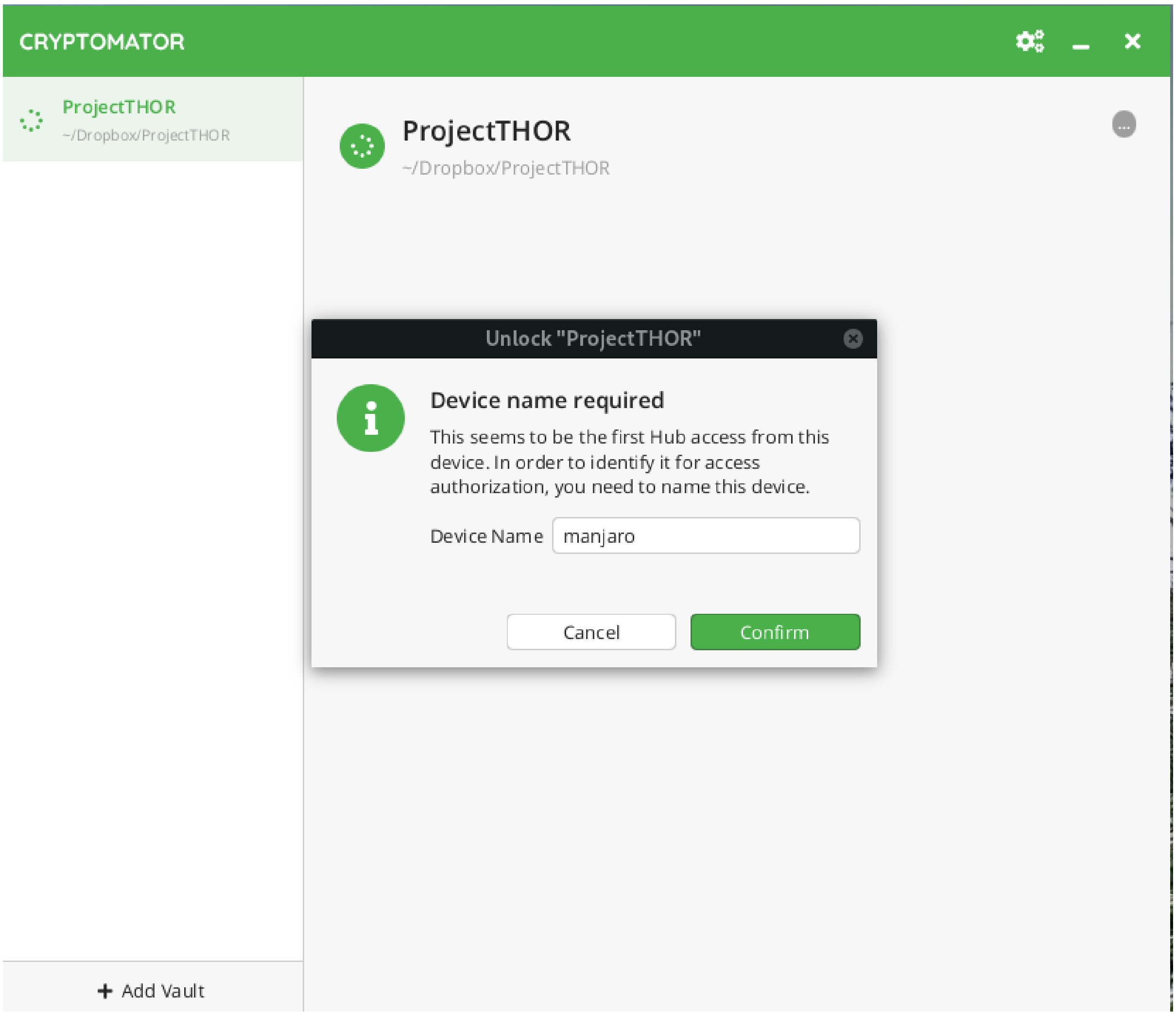
Sign in to your account

Username or email

Password

21.1.3 3. Register Device

If you connect to Hub with this device for the first time, you need to enter a unique name for this device.

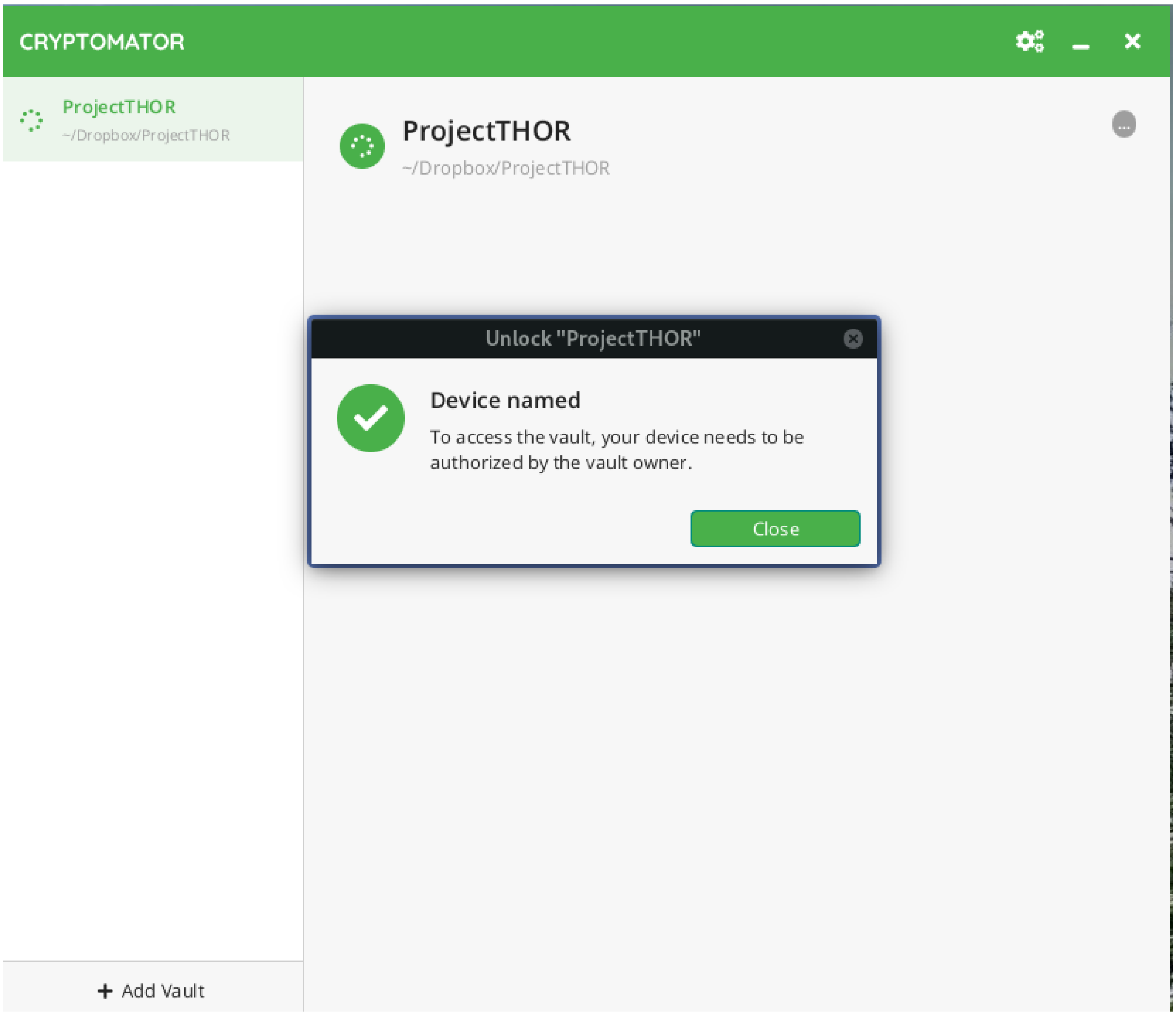


Device name required

This seems to be the first Hub access from this device. In order to identify it for access authorization, you need to name this device.

Device Name: manjaro

After that, you will see the following confirmation dialog.

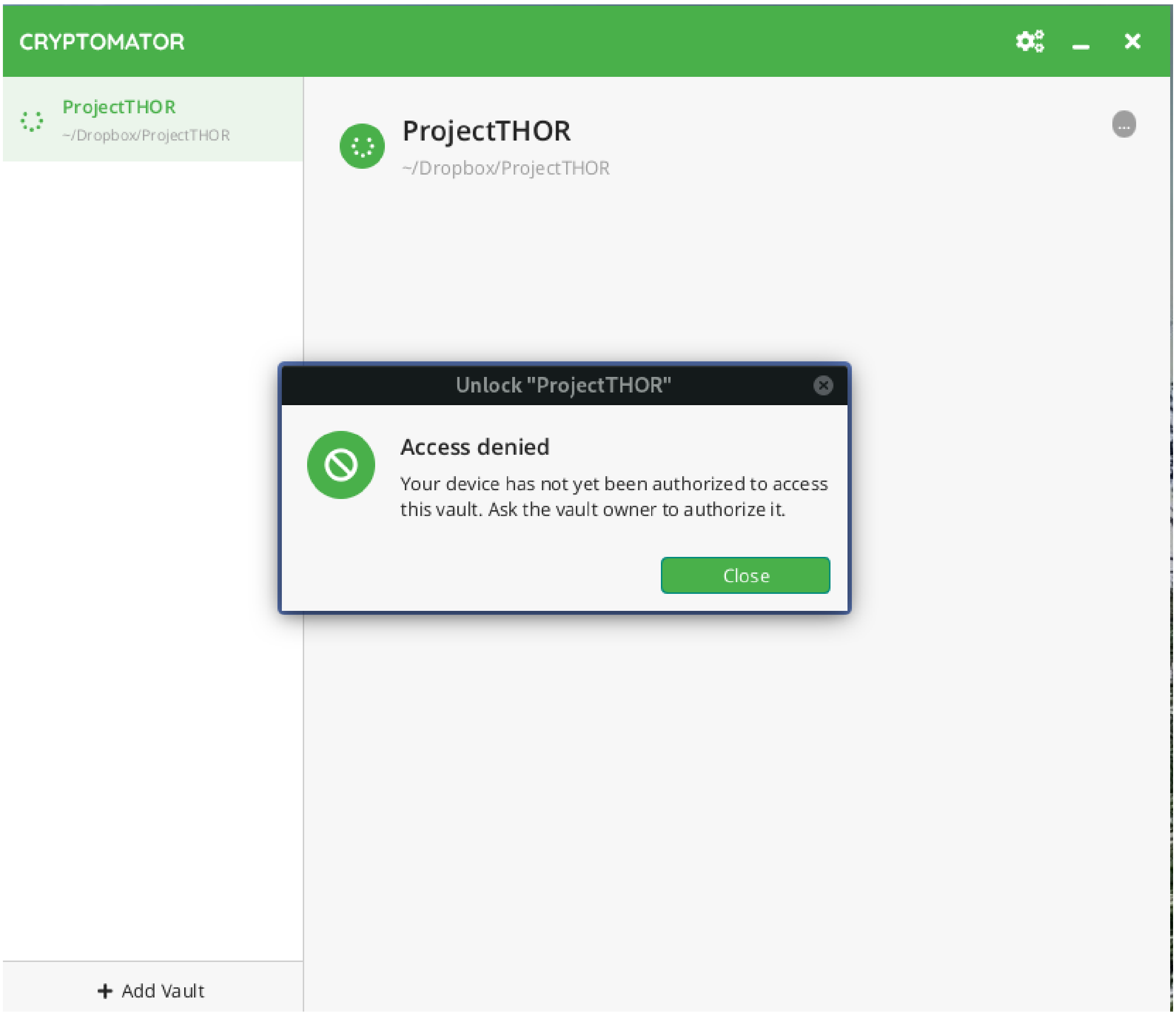


Device named

To access the vault, your device needs to be authorized by the vault owner.

21.1.4 4. Vault Unlocked

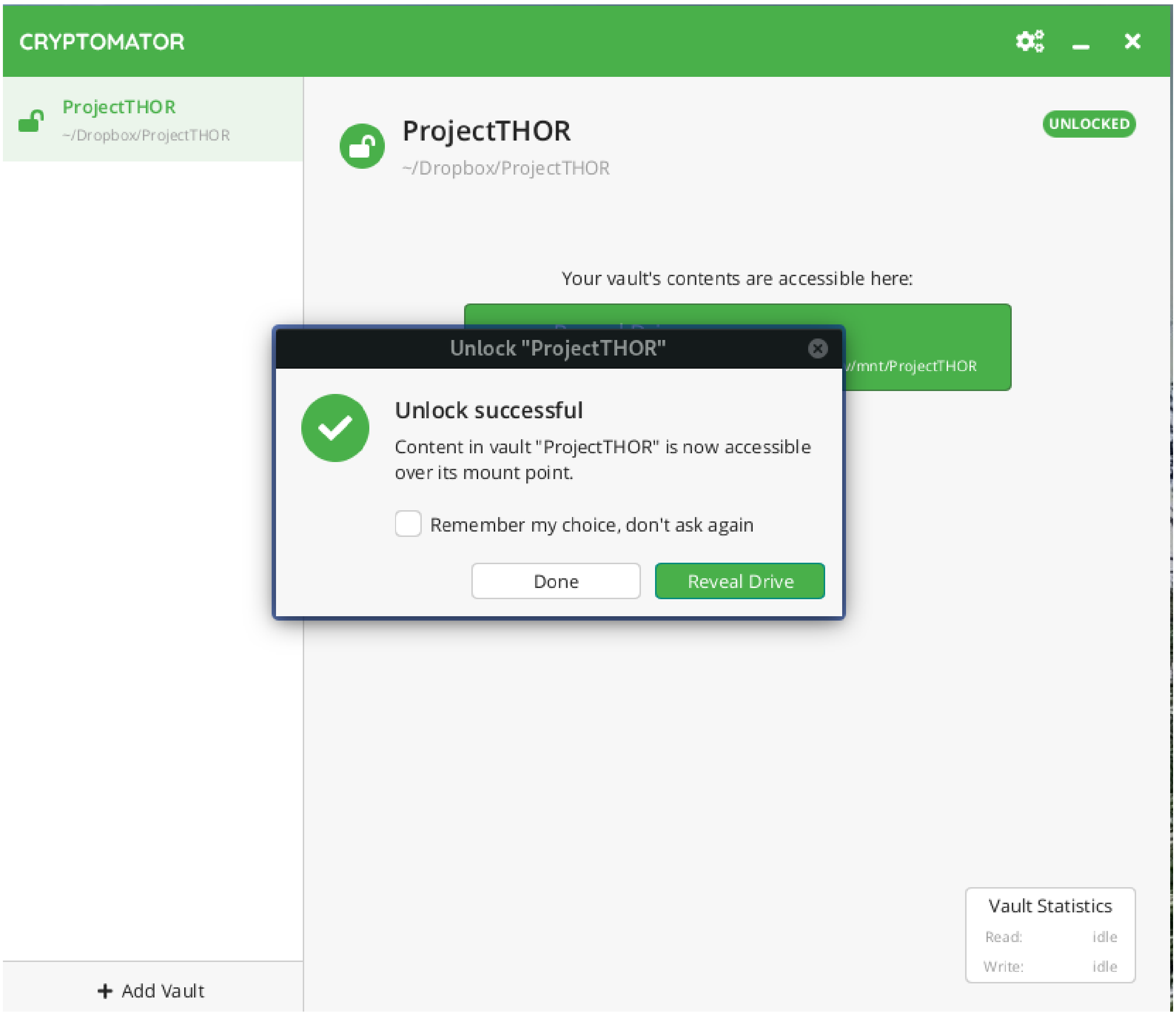
If you just registered the new device, a vault administrator needs to grant you access explicitly for the requested vault as described *here*, otherwise you will see the following dialog.



Access denied

Your device has not yet been authorized to access this vault. Ask the vault owner to authorize it.

After a vault administrator has granted you access, you are all set up and an unlock should be successful from now on. You can then reveal the vault's contents as usual.



ProjectTHOR

~/Dropbox/ProjectTHOR

Your vault's contents are accessible here:

Unlock successful

Content in vault "ProjectTHOR" is now accessible over its mount point.

□ Remember my choice, don't ask again

Vault Statistics

Read: idle

Write: idle

CHAPTER TWENTYTWO

VAULT RECOVERY

This section contains instructions for recovering Cryptomator Hub vaults using the vault recovery key.

Cryptomator Hub vaults can be recovered in two different ways:

1. *Online Recovery* - Reestablishes Hub controlled access management for a vault in case the vault admin password got lost
2. *Offline Recovery* - Restores vault data access of a hub managed vault in case of a disaster (e.g. Cryptomator Hub is down and immediate data access is needed)

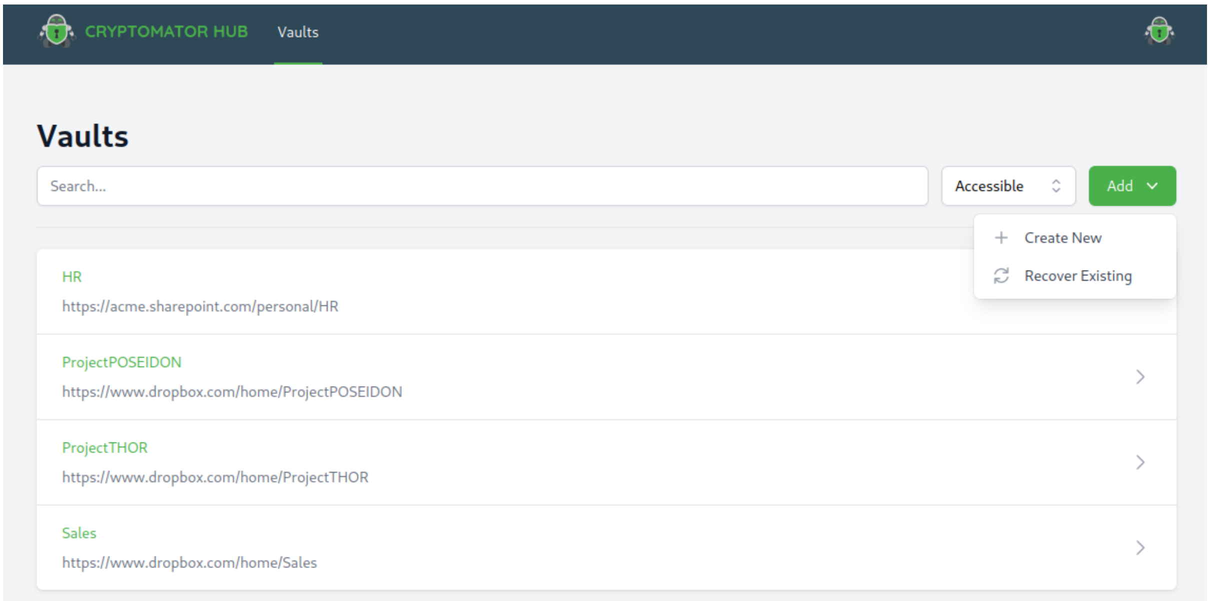
22.1 Online Recovery

This recovery method should be used, if the vault admin password got lost. In the process, a new Hub vault with the same key material as the "to-be-recovered" vault is created. The membership information of the old vault cannot be migrated, hence all users/groups need to be added manually afterwards.

Requirements:

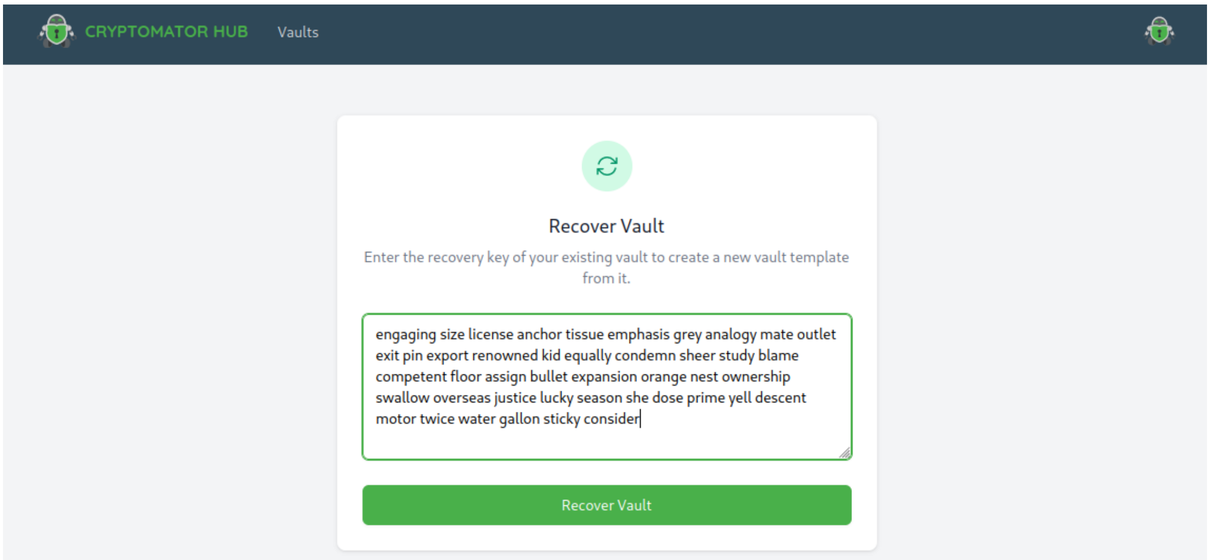
- Access to Cryptomator Hub
- Write access to the storage location of the vault
- Access to the recovery key of the vault

In Cryptomator Hub navigate to the vault list, click `Add` and `Recover Existing`


CRYPTOMATOR HUB
Vaults
Vaults
Search...
Accessible
Add
Create New
Recover Existing
HR
https://acme.sharepoint.com/personal/HR
ProjectPOSEIDON
https://www.dropbox.com/home/ProjectPOSEIDON
ProjectTHOR
https://www.dropbox.com/home/ProjectTHOR
Sales
https://www.dropbox.com/home/Sales

Enter the recovery key for the vault you want to restore. If you enter a recovery key from a different vault, the recovery will not work.

Proceed with `Restore Vault`.

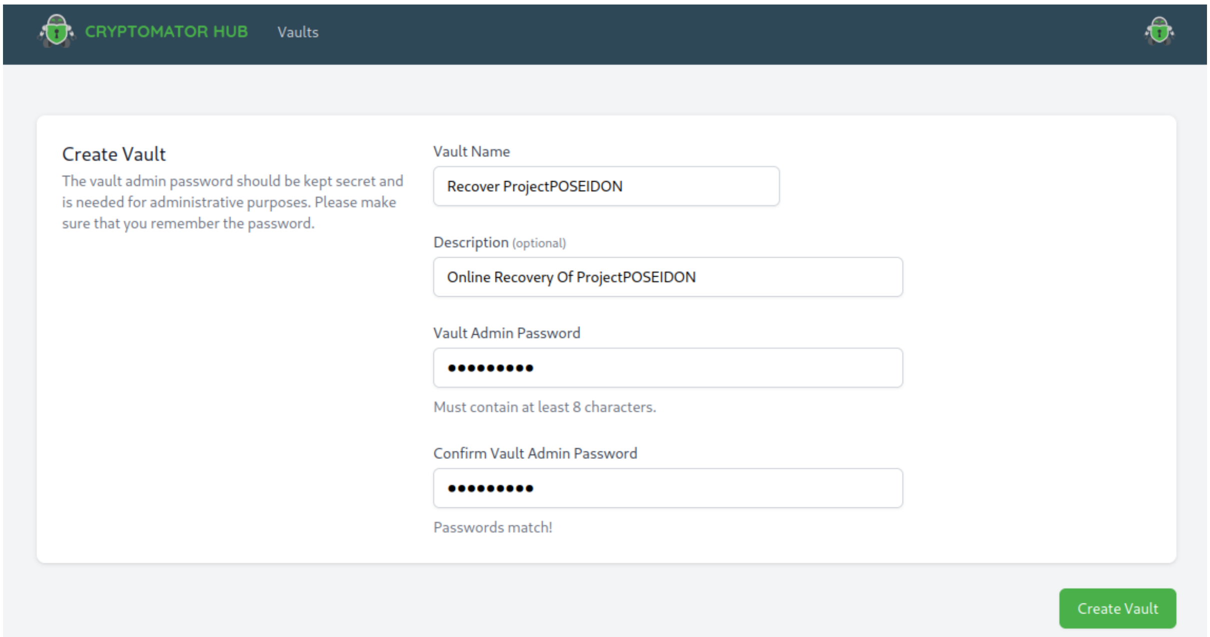


Recover Vault

Enter the recovery key of your existing vault to create a new vault template from it.

engaging size license anchor tissue emphasis grey analogy mate outlet exit pin export renowned kid equally condemn sheer study blame competent floor assign bullet expansion orange nest ownership swallow overseas justice lucky season she dose prime yell descent motor twice water gallon sticky consider

Enter a new vault name, description and vault admin password. The new vault admin password is required to grant or revoke access to the vault.



Create Vault

The vault admin password should be kept secret and is needed for administrative purposes. Please make sure that you remember the password.

Vault Name: Recover ProjectPOSEIDON

Description (optional): Online Recovery Of ProjectPOSEIDON

Vault Admin Password: •••••••••

Must contain at least 8 characters.

Confirm Vault Admin Password: •••••••••

Passwords match!

If successful, a new vault has been created. Proceed as follows:

1. Click on `Download zipped vault folder` of the new created vault
2. Unzip the downloaded folder
3. Copy the file `vault.cryptomator` of the unzipped folder
4. Browse locally on the device, directly in the cloud or network storage to the location of the vault folder. In that folder, replace the existing `vault.cryptomator` file with the one you just copied.

Afterwards, you can manage vault data access over the newly created vault in Hub. You will need to regrant permission to the vault members, and then the vault can be unlocked by the team.

22.2 Offline Recovery

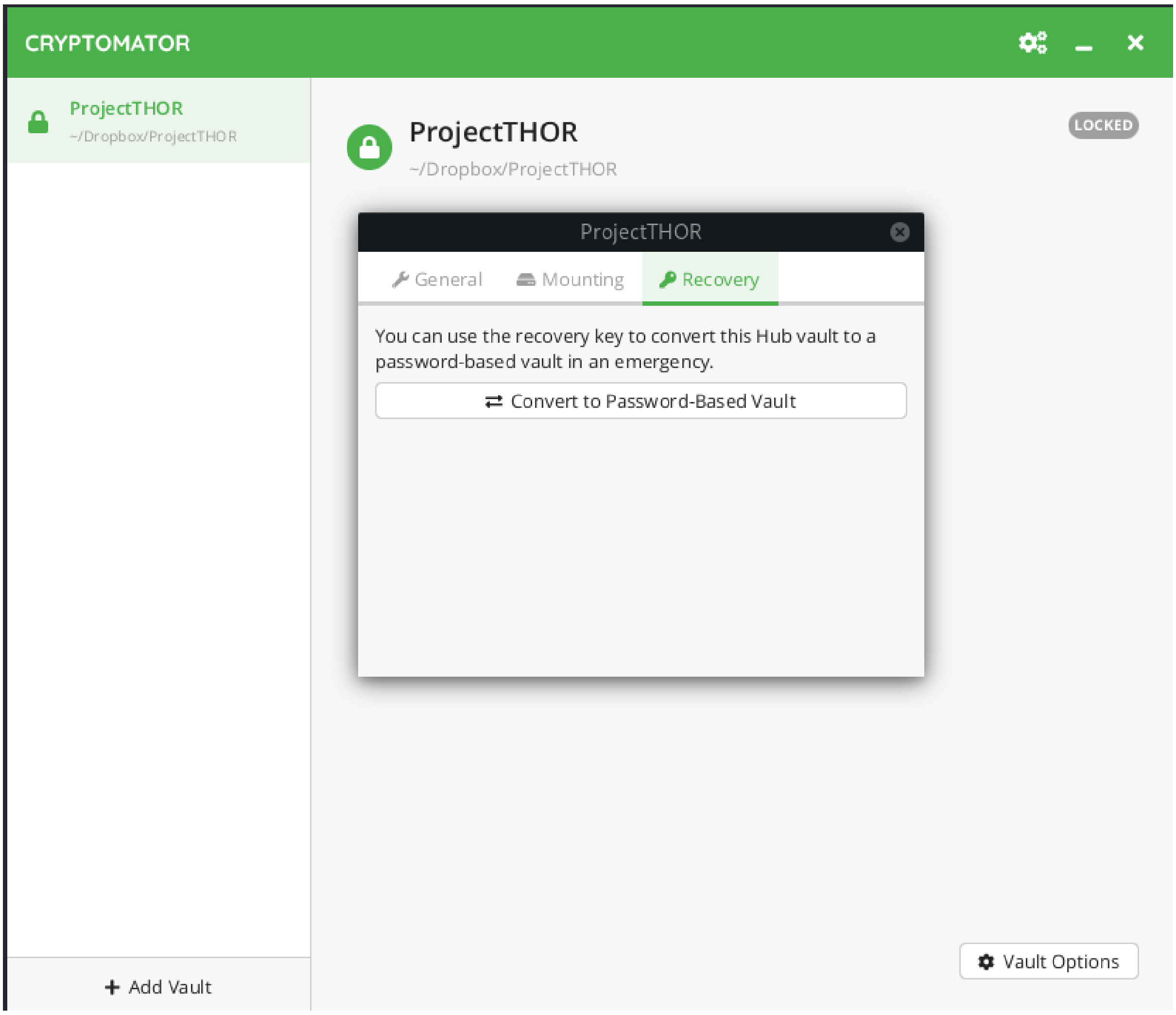
This recovery method should only be used in an emergency, i.e. immediate data access is needed but Cryptomator Hub not reachable. In the process, the authentication needed to unlock the vault is changed from Hub- to password-based by creating/changing vault configuration files. If these changes are synchronized to the online storage, everyone with the chosen password can unlock and access the vault data without requiring a connection to Cryptomator Hub. If you don't want that, ensure that the vault is stored at an offline location without any kind of synchronization.

Note: This process is reversible. See the *end of this section*.

Requirements:

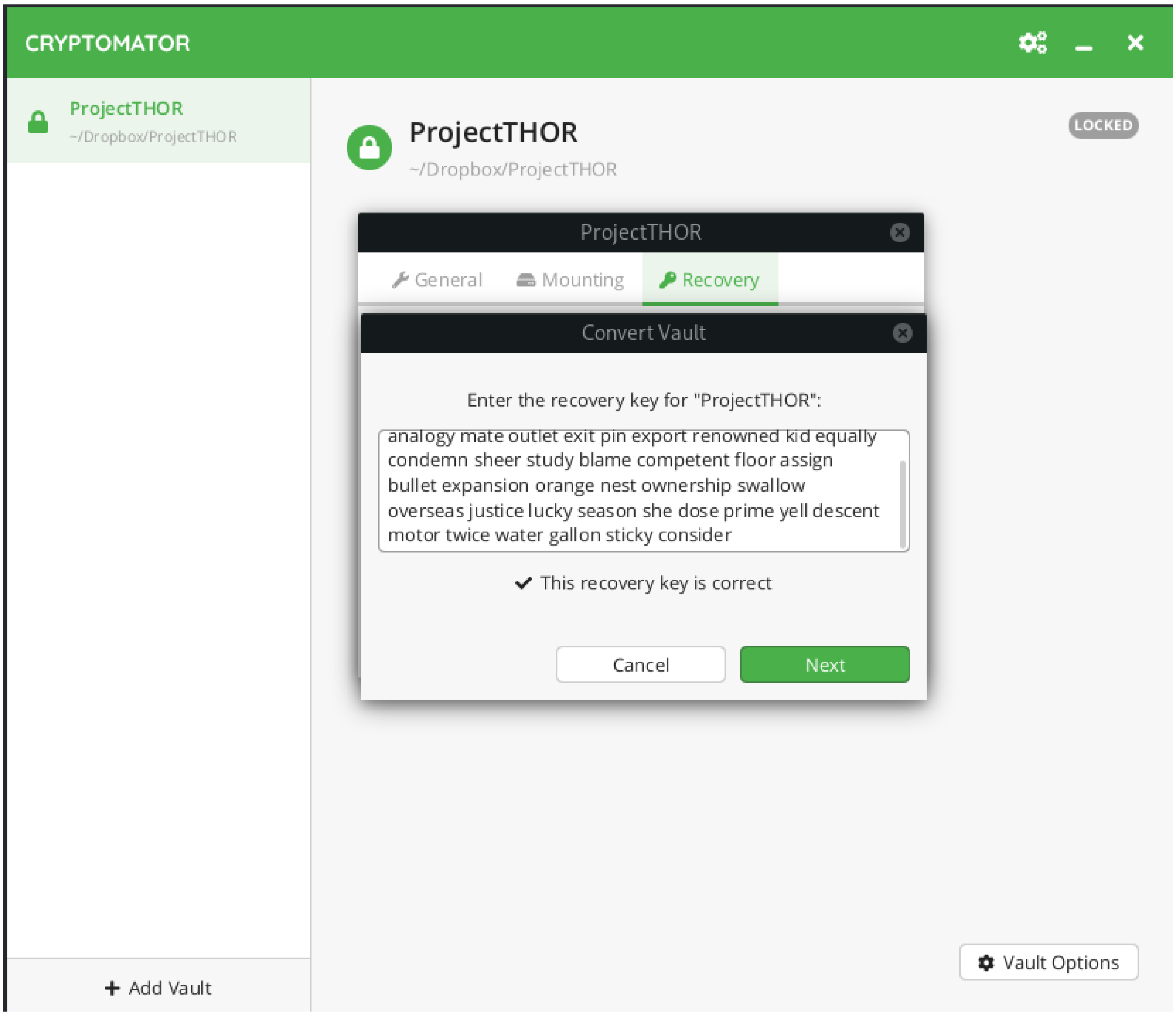
- Access to the Cryptomator desktop application
- Write access to the storage location of the vault
- Access to the recovery key of the vault

Open the Cryptomator desktop app, right-click on the vault you want to restore in the vault list, click `Show vault options` in the opened context menu. In the opening window, select the `Recovery`, read the label description and click the `Convert to Password-Based Vault` button.



You can use the recovery key to convert this Hub vault to a password-based vault in an emergency.

Enter the recovery key for the vault you want to restore. If you enter a recovery key from a different vault, the recovery will not work. Proceed with `Next`.

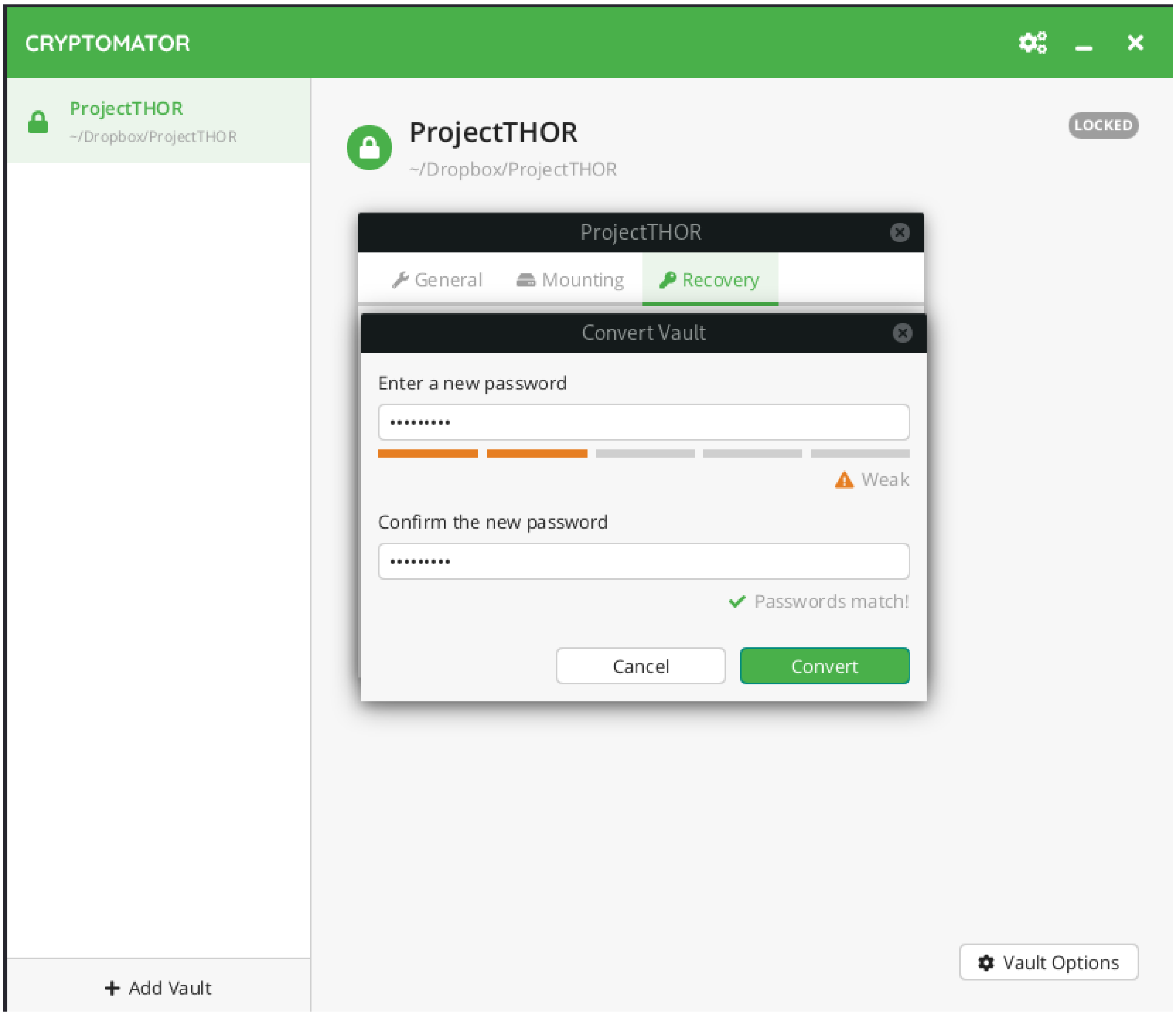


Enter the recovery key for "ProjectTHOR":

analogy mate outlet exit pin export renowned kid equally condemn sheer study blame competent floor assign bullet expansion orange nest ownership swallow overseas justice lucky season she dose prime yell descent motor twice water gallon sticky consider

✓ This recovery key is correct

In the next step choose a *good password* used for unlocking the vault. Cryptomator requires at least 8 characters but we recommend you to use a longer phrases such as pass-sentences. The bar below the password field estimates the strength of your password.



Enter a new password

•••••••••

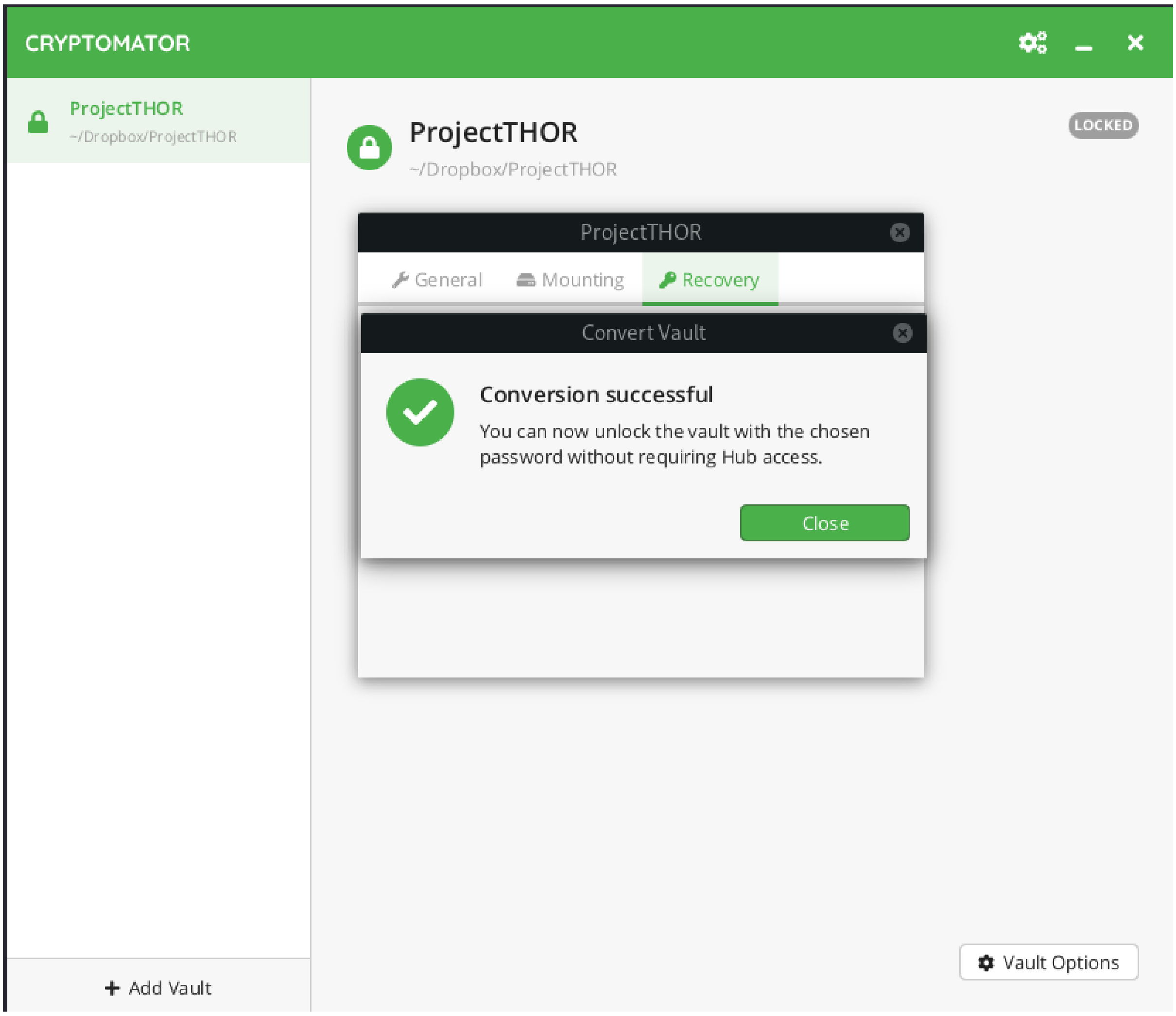
Weak

Confirm the new password

•••••••••

✓ Passwords match!

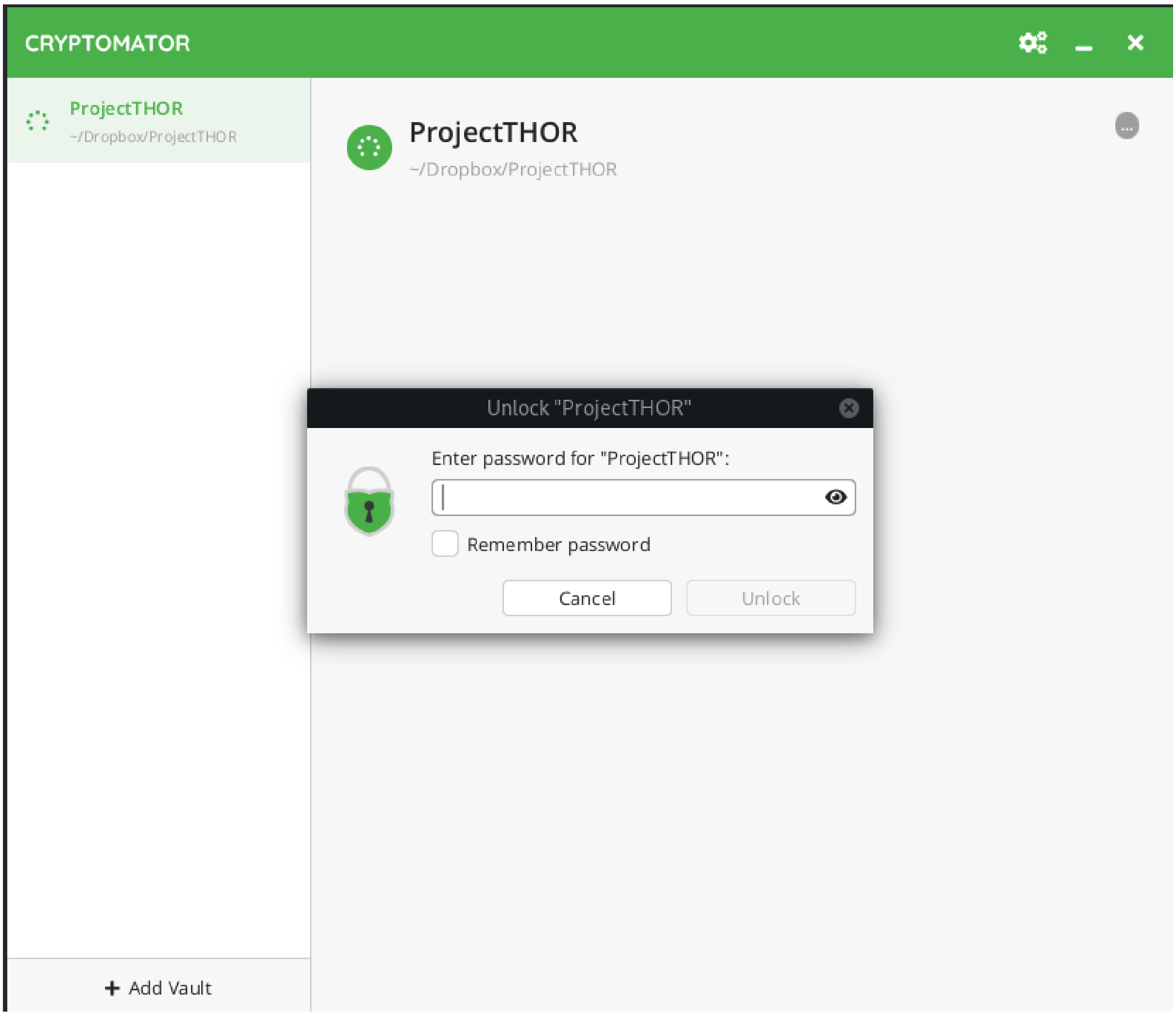
If the conversion was successful, a success message is shown. You can close the dialog box. This vault is now converted to a password-based vault.



Conversion successful

You can now unlock the vault with the chosen password without requiring Hub access.

After the conversion, when unlocking the vault, you are prompted for a password and only the one chosen in the previous step leads to a successful unlock.



Enter password for "ProjectTHOR":

□ Remember password

You can reverse the offline conversion. In order to do that, remove the following files:

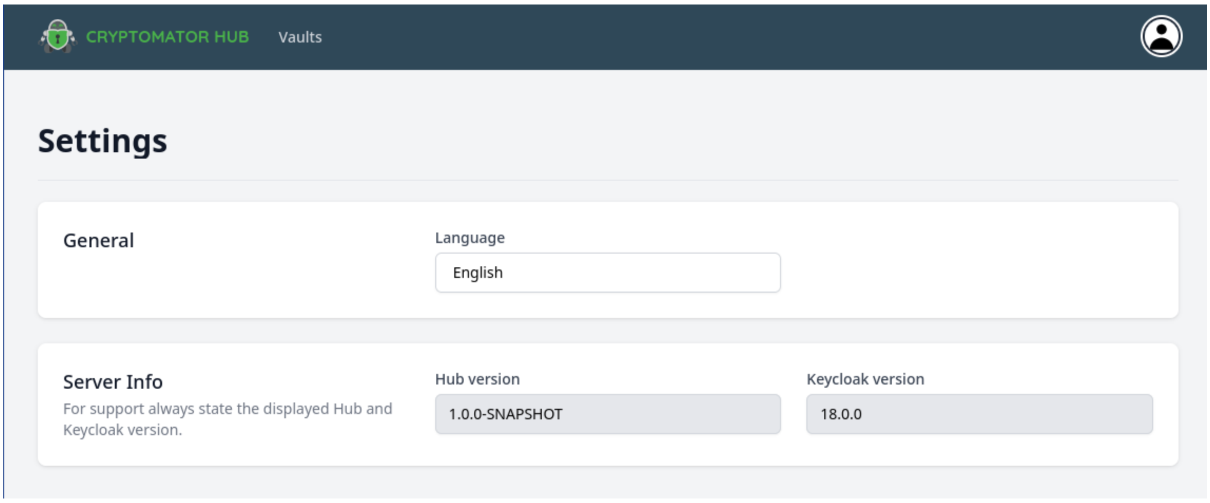
- all files named or starting with `masterkey.cryptomator`
- `vault.cryptomator`
- the *most recent* `vault.cryptomator.XXXXXXXX.bkup`

Then restore the original config by renaming `vault.cryptomator.XXXXXXXX.bkup` to `vault.cryptomator`. You can then unlock the vault again using the Cryptomator Hub.

CHAPTER TWENTYTHREE

SETTINGS

Access the settings of Cryptomator Hub by tapping the profile icon in the top right corner.



Settings

General

Language: English

Server Info

For support always state the displayed Hub and Keycloak version.

Hub version: 1.0.0-SNAPSHOT

Keycloak version: 18.0.0

23.1 Version

The section `Server Info` shows the current running Hub and Keycloak version. Providing those values is required when you ask for support.

The following versions are compatible with each other:

Hub	Keycloak	Cryptomator Desktop	Cryptomator Android	Cryptomator iOS
1.0.0	18, 19, 20	1.6.11	N/A	N/A

CHAPTER

TWENTYFOUR

SECURITY TARGET

Cryptomator was designed to solve privacy issues when saving files to cloud storages.

The risk that the cloud provider or third parties access the data stored in the cloud without permission is mitigated. Only people who know the vault password are able to read the files in the vault or change the file contents undetected. This is true for file contents as well as for filenames.

To allow a working synchronization with the cloud, there are some meta information that Cryptomator does not encrypt. These are:

- access, modification, and creation timestamp of files and folders,
- number of files and folders in a vault and in the folders, and
- size of the stored files.

In addition, you have to keep in mind what Cryptomator is not. Protection of the files on the local computer is not the focus of Cryptomator. Cryptomator is not a complete replacement for other encryption tools based on container files if the aforementioned meta information should be encrypted. Cryptomator does not provide protection if programs create backup copies of the encrypted files when working with them. Such files are not detected by Cryptomator and may remain on the computer even after unlocking a vault. Cryptomator cannot provide protection if the local computer is infected with malware which reads entered passwords and file contents (e.g., files in an unlocked vault).

To protect against such risks, other methods, like complete disk encryption, immediate installation of system and software updates, and the use of applicable antivirus software, is required.

CHAPTER

TWENTYFIVE

SECURITY ARCHITECTURE

25.1 Virtual Filesystem

Cryptomator provides a virtual drive. Add, edit, remove files as you're used to with just any disk drive.

Files are transparently en- and decrypted. There are no unencrypted copies on your hard disk drive. With every access on your files inside the virtual drive, Cryptomator will en- and decrypt these files on-the-fly.

Currently WinFsp (on Windows) and macFUSE (on macOS) and FUSE (Linux) are our frontends of choice. If they're not available on your system, Cryptomator will fall back on WebDAV, as it is supported on every major operating system. WebDAV is an HTTP-based protocol and Cryptomator acts as a WebDAV server accepting so-called loopback connections on your local machine only.

Whenever your file manager accesses files through this virtual drive, Cryptomator will process this request via the following layers.

25.2 Vault Configuration

Every vault must have a vault configuration file named `vault.cryptomator` in the root directory of the vault. It is a JWT containing basic information about the vault and specification what key to use. The JWT is signed using the 512 bit raw masterkey.

This is an example of an encoded vault configuration file:

```
eyJraWQiOiJtYXN0ZXJrZXlmaWxlOm1hc3RlcmtleS5jcnlwdG9tYXRvciIsInR5cCI6IkpXVCIsImFsZyI6IkhTMjU2In0.
↪eyJmb3JtYXQiOjgsInNob3J0ZW5pbmdUaHJlc2hvbGQiOjIyMCwianRpIjoiY2U5NzZmN2EtN2I5Mi00Y2MwLWI0YzEtYzc0YT
↪IJlu4dHb3fqB2fAk9lf8G8zyEXc7OLB-5m9aNxOEXIQ
```

The decoded header:

```
{
  "kid": "masterkeyfile:masterkey.cryptomator", /* URI of where to get the key */
  "typ": "JWT",
  "alg": "HS256" /* current implementations also support HS384 and HS512 */
}
```

The decoded payload:

```
{
  "format": 8, /* vault format for checking software compatibility */
  "shorteningThreshold": 220, /* how many characters in ciphertext filenames before␣
↪shortening */
  "jti": "ce976f7a-7b92-4cc0-b4c1-c74a6aa17cf5", /* random UUID to uniquely identify␣
↪the vault */
  "cipherCombo": "SIV_GCM" /* mode of operation for the block cipher. Other possible␣
```

(continues on next page)

(continued from previous page)

```
↪values are "SIV_CTRMAC" */
}
```

When opening a vault, the following steps have to be followed:

1. Decode `vault.cryptomator` without verification.
2. Read `kid` header and, depending on its value, retrieve the masterkey from the specified location.
3. Verify the JWT signature using the masterkey.
4. Make sure `format` and `cipherCombo` are supported.

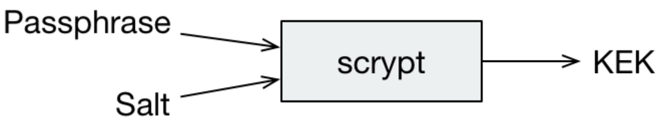
25.3 Masterkey Derivation

Each vault has its own 256 bit encryption as well as MAC masterkey used for encryption of file specific keys and file authentication, respectively.

These keys are random sequences generated by a CSPRNG (Cryptographically secure pseudorandom number generator). We use SecureRandom with SHA1PRNG, seeded with 440 bits from `SecureRandom.getInstanceStrong()`.

Both keys are encrypted using RFC 3394 key wrapping with a KEK (Key-encryption key) derived from the user's password using scrypt.

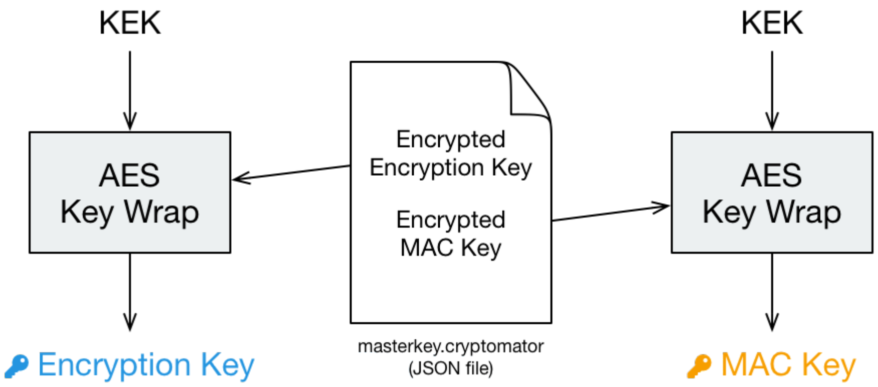
```
encryptionMasterKey := createRandomBytes(32)
macMasterKey := createRandomBytes(32)
kek := scrypt(password, scryptSalt, scryptCostParam, scryptBlockSize)
wrappedEncryptionMasterKey := aesKeyWrap(encryptionMasterKey, kek)
wrappedMacMasterKey := aesKeyWrap(macMasterKey, kek)
```



The wrapped keys and the parameters needed to derive the KEK are then stored as integers or Base64-encoded strings in a JSON file named `masterkey.cryptomator`, which is located in the root directory of the vault.

```
{
    "version": 999, /* deprecated, vault format is now specified in the vault␣
↪configuration */
    "scryptSalt": "QGk...jY=",
    "scryptCostParam": 16384,
    "scryptBlockSize": 8,
    "primaryMasterKey": "QDi...Q==", /* wrappedEncryptionMasterKey */
    "hmacMasterKey": "L83...Q==", /* wrappedMacMasterKey */
    "versionMac": "3/U...9Q=" /* HMAC-256 of vault version to prevent undetected␣
↪downgrade attacks */
}
```

When unlocking a vault the KEK is used to unwrap (i.e. decrypt) the stored masterkeys.



25.4 File Header Encryption

Note: The following section only applies to vaults with the cipher combo `SIV_GCM` in the decoded JWT payload. For vaults with `SIV_CTRMAC`, have a look at our 1.6 documentation.

The file header stores certain metadata, which is needed for file content encryption. It consists of 68 bytes.

- 12 bytes nonce used during header payload encryption.
- 40 bytes AES-GCM encrypted payload consisting of:
  - 8 bytes filled with 1 for future use (formerly used for file size) and
  - 32 bytes file content key.
- 16 bytes tag of the encrypted payload.

```
headerNonce := createRandomBytes(12)
contentKey := createRandomBytes(32)
cleartextPayload := 0xFFFFFFFFFFFFFFFF . contentKey
ciphertextPayload, tag := aesGcm(cleartextPayload, encryptionMasterKey, headerNonce)
```

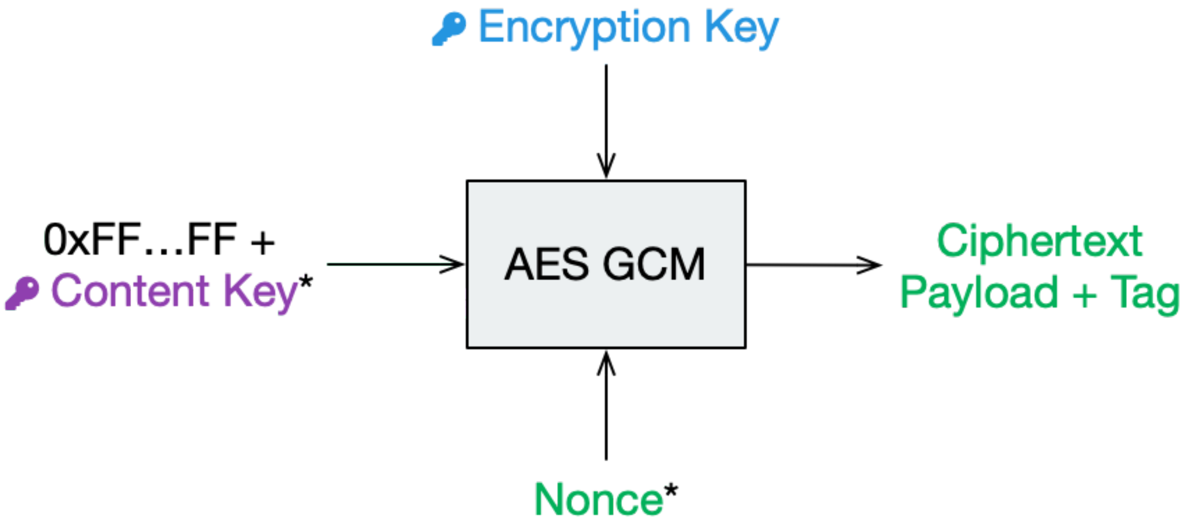


Fig. 1: *Random per file change

25.5 File Content Encryption

This is where your actual file contents get encrypted.

The cleartext is broken down into multiple chunks, each up to 32 KiB + 28 bytes consisting of:

- 12 bytes nonce,
- up to 32 KiB encrypted payload using AES-GCM with the file content key, and
- 16 bytes tag computed by GCM with the following AAD:
  - chunk number as 32 bit big endian integer (to prevent undetected reordering),
  - file header nonce (to bind this chunk to the file header),

Afterwards, the encrypted chunks are joined preserving the order of the cleartext chunks. The payload of the last chunk may be smaller than 32 KiB.

```
cleartextChunks[] := split(cleartext, 32KiB)
for (int i = 0; i < length(cleartextChunks); i++) {
    chunkNonce := createRandomBytes(12)
    aad := [bigEndian(i), headerNonce]
    ciphertextPayload, tag := aesGcm(cleartextChunks[i], contentKey, chunkNonce, aad)
    ciphertextChunks[i] := chunkNonce . ciphertextPayload . tag
}
ciphertextFileContent := join(ciphertextChunks[])
```

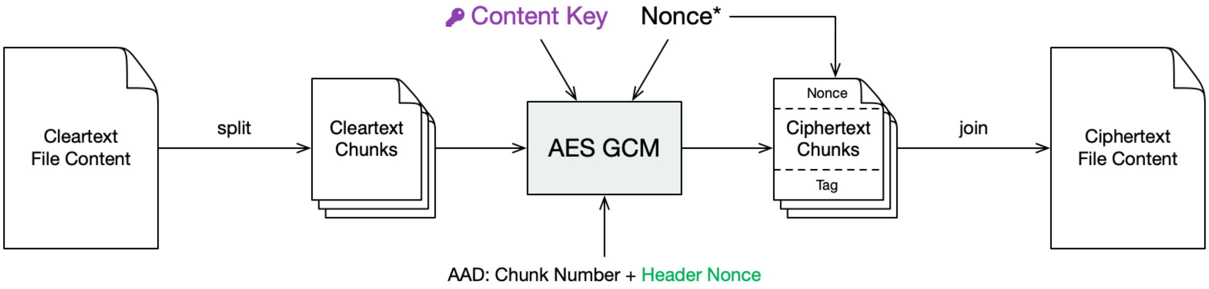


Fig. 2: *Random per chunk change

25.6 Directory IDs

Each directory has a unique ID that is required during filename encryption. For historical reasons, the directory ID is a string, even though any byte sequence would do the job.

The directory ID for the root directory is the empty string. For all other directories, it is a random sequence of at most 36 ASCII chars. We recommend using random UUID (Universally unique identifier).

```
dirId := createUuid()
```

When traversing directories, the directory ID of a given subdirectory is processed in four steps to determine the storage path inside the vault:

1. Encrypting the directory ID using AES-SIV in order to encrypt directory hierarchies.
2. Creating a SHA1 hash of the encrypted directory ID in order to get a uniform length.
3. Encoding the hash with Base32 to get a string of printable chars.
4. Constructing the directory path out of the Base32-encoded hash.

```
dirIdHash := base32(sha1(aesSiv(dirId, null, encryptionMasterKey, macMasterKey)))
dirPath := vaultRoot + '/d/' + substr(dirIdHash, 0, 2) + '/' + substr(dirIdHash, 2,␣
↪30)
```

Regardless of the hierarchy of cleartext paths, ciphertext directories are always stored in a flattened structure. All directories will therefore effectively be siblings (or cousins, to be precise).

25.7 Filename Encryption

The cleartext name of a file gets encoded using UTF-8 in Normalization Form C to get a unique binary representation.

Cryptomator uses AES-SIV to encrypt names. The directory ID of the parent folder is passed as associated data. This prevents undetected movement of files between directories.

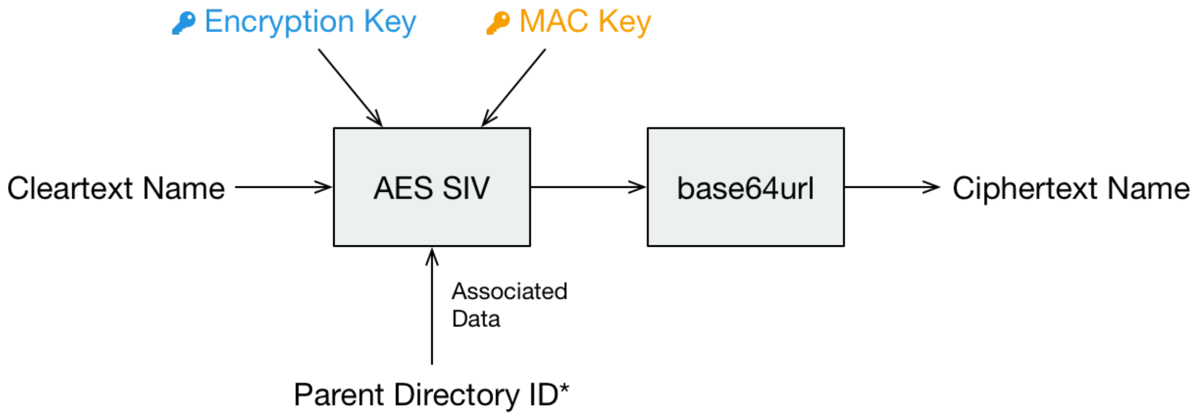


Fig. 3: *Unencrypted directory ID of the partent dir as described above

```
ciphertextName := base64url(aesSiv(cleartextName, parentDirId, encryptionMasterKey,␣
↪macMasterKey)) + '.c9r'
```

Depending on the kind of node, the encrypted name is then either used to create a file or a directory.

- Files are stored as files.
- Non-files are stored as directories. The type of the node then depends on the directory content.
  - Directories are denoted by a file called `dir.c9r` containing aforementioned directory ID.
  - Symlinks are denoted by a file called `symlink.c9r` containing the encrypted link target.
  - Further types may be appended in future releases.

Thus, a cleartext directory structure like this:

```
.
├─ File.txt
├─ SymlinkToFile.txt
├─ Subdirectory
│  └─ ...
└─ ...
```

Becomes a ciphertext directory structure like this:

```
.
├─ d
│  ├─ BZ
│  │  └─ R4VZSS5PEF7TU3PMFIMON5GJRNBDWA
│  │     ├─ 5TyvCyF255sRtfrIv**83ucADQ==.c9r  # File.txt
│  │     ├─ FHTa55bH*sUfVDbEb0gTL9hZ8nho.c9r  # Subdirectory
│  │     │  └─ dir.c9r  # contains dirId
│  │     └─ gLeOGMCN358*UBf2Qk9cWCQl.c9r  # SymlinkToFile.txt
│  │        └─ symlink.c9r  # contains link target
│  └─ FC
│     └─ ZKZRLZUODUUYTYA4457CSBPZXB5A77  # contains contents of Subdirectory
│        └─ ...
├─ masterkey.cryptomator
├─ masterkey.cryptomator.DFD9B248.bkup
└─ vault.cryptomator
```

25.8 Name Shortening

Note: This layer doesn't provide any additional security. Its sole purpose is to maximize compatibility.

To maximize compatibility, we need to make sure the ciphertext names don't exceed a length of 255 chars. As some cloud sync services might want to add a suffix to a file in case of conflicts, we decided to use at most 220 chars.

If an encrypted name (including its `.c9r` extension) exceeds these 220 chars, we will instead create a directory named after its much shorter SHA-1 hash and the `.c9s` extension. Additionally we will create a reverse-mapping file named `name.c9s` containing the original file inside of this directory.

```
if (length(ciphertextName) > 220) {
    deflatedName := base64url(sha1(ciphertextName)) + '.c9s'
    inflatedNameFilePath := deflatedName + '/name.c9s'
    fileContentsPath := deflatedName + '/contents.c9r'
    symlinkFilePath := deflatedName + '/symlink.c9r'
    dirIdFilePath := deflatedName + '/dir.c9r'
}
```

Again, we have to distinguish the kind of a node.

- Non-files (such as symlinks or directories) are stored as a directory anyway. Nothing changes for them.
- Files, on the other hand, need a different place to store their contents. Therefore, we introduce the `contents.c9r` file inside the `.c9s` directory.

A vault containing several nodes with very long names might result in a ciphertext structure like this:

```
.
├─ d
│  ├─ BZ
│  │  └─ R4VZSS5PEF7TU3PMFIMON5GJRNBDWA
│  │     ├─ 5TyvCyF255sRtfrIv**83ucADQ==.c9r
│  │     ├─ FHTa55bH*sUfVDbEb0gTL9hZ8nho.c9r
│  │     │  └─ dir.c9r
│  │     ├─ gLeOGMCN358*UBf2Qk9cWCQl.c9r
│  │     │  └─ symlink.c9r
│  │     ├─ IjTsXtReTy6bAAuxzLPV9T0k2vg=.c9s  # shortened name...
│  │     │  ├─ contents.c9r  # ...node is a regular file
```

(continues on next page)

(continued from previous page)

```
│  │     │  └─ name.c9s  # ...mapping to this full name
│  │     ├─ q2nx5XeNCenHyQvkFD4mxYNrWpQ=.c9s  # shortened name...
│  │     │  ├─ dir.c9r  # ...node is a directory
│  │     │  └─ name.c9s  # ...mapping to this full name
│  │     └─ u*JJCJE-T4IH-EBYASUp1u3p7mA=.c9s  # shortened name...
│  │        ├─ name.c9s  # ...mapping to this full name
│  │        └─ symlink.c9r  # ...node is a symlink
│  └─ FC
│     └─ ZKZRLZUODUUYTYA4457CSBPZXB5A77
│        └─ ...
├─ masterkey.cryptomator
├─ masterkey.cryptomator.DFD9B248.bkup
└─ vault.cryptomator
```

25.9 Backup Directory IDs

Note: This layer is optional and not required for a complete implementation of the Cryptomator Encryption Scheme. It doesn't provide any additional security. Its sole purpose is to increase data recoverability in case of missing or damaged directory files.

By obfuscating the hierarchy of cleartext paths using `dir.c9r` files, which contain *directory IDs*, the directory structure is more vulnerable to problems like incomplete synchronization or bit rotting.

When a directory file is missing or damaged, the `dirPath` cannot be computed, which effectively makes the directory content inaccessible in the *virtual filesystem*. In theory, the contents of the encrypted content of these files can be recovered. But since the *filename encryption* is dependent on the directory ID of the parent folder, which is only stored in the directory file, names of all items (files, directories, or symlinks) are lost.

To alleviate this issue, a backup directory file will be stored during the creation of a directory. Inside the ciphertext directory, a file named `dirid.c9r` will be created, which contains the directory ID of its parent folder. It is *encrypted* like a regular ciphertext file.

CHAPTER

TWENTYSIX

BEST PRACTICES

26.1 Sharing of Vaults

Always be careful when sharing your vault with other people.

In general, keep your vault password secret. Nobody except yourself should know the vault password. Only when you use a vault together with other people, they may know your vault password. Keep in mind that other people could pass on – with or without intent – the vault password. Only share your vaults with people you trust.

If you share a vault with others, do not communicate the vault password on an insecure channel. Tell the password in person, use encrypted email or messengers or other similar secure means.

Are you working in a team and do not want to share vault passwords? Consider using Cryptomator Hub. It adds access management for your vaults and allows you to unlock vaults with your own account.

26.2 Good Passwords

Bad passwords can be cracked easily when using computers. Plenty of recommendations exist for secure passwords. Some of these are:

- A password should not contain public or personal information like the name of your pet, date of birth, or username.
- A password should be long.
- A password should not be an existing word or a combination of few words. It should be a combination of characters or words that is as random as possible.
- For each purpose, a unique password without similarities to other passwords should be used.

If you fulfill these requirements, you quickly reach a point where remembering the passwords gets impossible. Thus, we recommend to use a password manager to generate and store the passwords. By doing so, you only have to remember a few or a single secure password. Otherwise, we recommend to use at least 10 characters, ideally use sentences instead of words.

CHAPTER

TWENTYSEVEN

MANUAL MIGRATION

Under some circumstances, Cryptomator refuses to automatically migrate a vault to a newer format. In this case, your vault will remain untouched, so you can continue using it with the previous version.

To upgrade to the latest version, you can perform a migration manually:

1. Unlock the vault with the previous version of Cryptomator that you have used. You can find downloads of older versions on our GitHub site.
2. Copy all files from this vault onto a temporary storage location on your computer. Be aware that these files are decrypted.
3. Once finished, lock your vault and quit Cryptomator. Now install the latest version of Cryptomator.
4. Create new vault with the latest version of Cryptomator and unlock it.
5. Copy all files from step 2 into the new vault.

Note: One reason why automatic migration is impossible might be the fact that your vault is stored in a location that limits filename or path lengths, such as:

- Network drives on Windows, such as WebDAV mounts
- eCryptfs-encrypted volumes on Linux

In this case, during step 5, you may encounter warnings indicating that you can not encrypt files due to such length limitations. Feel free to simply change the name of any affected files.

CHAPTER

TWENTYEIGHT

CONTRIBUTE

28.1 How Can You Help Us?

Cryptomator is an open source project and wouldn't be possible without contributions from users who support the idea.

There are several ways you can help us:

- By reporting bugs or feature requests on GitHub,
- By discussing solutions in our community,
- By contributing patches or features via pull requests,
- By helping us with the localization of Cryptomator,
- By improving this documentation,
- By becoming a sponsor,
- Or by donating to the maintainers.

28.2 Before You Start

If you plan to help, please stick to our Code of Conduct.

Our code is licensed under GPLv3 and this documentation under CC-BY-SA 4.0. If you contribute either, your grant us the rights to publish your contributions under those licenses. Also you have to digitally sign a Contributor License Agreement (CLA). This is required to protect the maintainers of Cryptomator from legal problems with patent or copyright infringement. The CLA signature process is triggered by your first pull request automatically. You will be asked to authenticate with your GitHub account and your username will be stored even if you revoke any activity on GitHub.

CHAPTER

TWENTYNINE

VAULT FORMAT HISTORY

Cryptomator vaults need to adhere to a structure and format (as described in *Security Architecture*) that may change over time. In order to identify the correct format, the masterkey file contains a version number, which represents the vault format.

29.1 Format 8

Introduced in Cryptomator 1.6.0 on 2021-10-19. The following changes are:

- Decoupled vault configuration from key derivation by introducing new vault configuration file named `vault.cryptomator`. It is a JWT containing basic information about the vault and specification what key to use.
- `version` inside `masterkey.cryptomator` is now deprecated.

29.2 Format 7

Introduced in Cryptomator 1.5.0 on 2020-04-16. The following changes are:

- Added file extension (`*.c9r` and `*.c9s`) to all encrypted files and directories. Certain cloud storage services have issues with files without an extension.
- Encrypted directories are now actually directories. Directory file is now inside of that with the fixed name `dir.c9r`.
- Encrypted symlinks are now directories. Symlink file is now inside of that with the fixed name `symlink.c9r`.
- Files and directories with shortened filenames are now directories (identifiable by the `.c9s` suffix). Mapping file with the long filename is now inside of that with the fixed name `name.c9s`. If it's a regular file, the content file has the fixed name `contents.c9r`.
- Removed directory `m` because mapping files for shortened filenames are now in `d` as well.
- Filenames are encoded with base64url so that name shortenings are less likely.
- Increased ciphertext filename threshold to 220 characters.

This is an example of the vault structure:

```
.
├─ d
│  ├─ BZ
│  │  └─ R4VZSS5PEF7TU3PMFIMON5GJRNBDWA
│  │     ├─ 5TyvCyF255sRtfrIv__83ucADQ==.c9r  # regular file
│  │     ├─ FHTa55bH_sUfVDbEb0gTL9hZ8nho.c9r  # irregular file...
│  │     │  └─ dir.c9r  # ...which is a directory
```

(continues on next page)

(continued from previous page)

```
│  │     ├─ gLeOGMCN358_UBf2Qk9cWCQl.c9r  # irregular file...
│  │     │  └─ symlink.c9r  # ...which is a symlink
│  │     ├─ IjTsXtReTy6bAAuxzLPV9T0k2vg=.c9s  # shortened name...
│  │     │  ├─ contents.c9r  # ...which is a regular file
│  │     │  └─ name.c9s  # ...mapping to this full name
│  │     ├─ q2nx5XeNCenHyQvkFD4mxYNrWpQ=.c9s  # shortened name...
│  │     │  ├─ dir.c9r  # ...which is a directory
│  │     │  └─ name.c9s  # ...mapping to this full name
│  │     ├─ u_JJCJE-T4IH-EBYASUp1u3p7mA=.c9s  # shortened name...
│  │     │  ├─ name.c9s  # ...mapping to this full name
│  │     │  └─ symlink.c9r  # ...which is a symlink
│  │     └─ ...
│  └─ FC
│     └─ ZKZRLZUODUUYTYA4457CSBPZXB5A77
│        └─ ...
├─ masterkey.cryptomator
└─ masterkey.cryptomator.DFD9B248.bkup
```

29.3 Format 6

Introduced in Cryptomator 1.3.0 on 2017-07-01. The following changes are:

- Password is normalized in NFC.

29.4 Format 5

Introduced in Cryptomator 1.2.0 on 2016-09-19. The following changes are:

- Dropped file size obfuscation support.

File sizes can be determined in O(1) instead of having to read and decrypt the file header. This allows showing file sizes in the directory listing without having to download each file first. The file size in the header is now unused and filled with 0xFFFFFFFFFFFFFFFF.

29.5 Format 4

Introduced in Cryptomator 1.1.1 on 2016-07-08. The following changes are:

- Directories now have 0 (zero) prefix instead of a _ (underscore) suffix.

Directories are now stored with different names to avoid conflicts with the naming scheme of certain cloud storage services in case of synchronization conflicts.

This is an example of the vault structure:

```
.
├─ d
│  ├─ BZ
│  │  └─ R4VZSS5PEF7TU3PMFIMON5GJRNBDWA
│  │     ├─ 0USJ7VD36K7YU2RARYJMEFTABZOGN6LUH63VRH5MADVOZ433VZ7EPSM2PLJPHTBL6
│  │     ├─ 0YWVRCCROEC3ZECD2UTJR7BGYERU3LG6R7QODBGMZ7EQ3BXGY24======
│  │     ├─ ...
│  │     ├─ YWBBP7RC6FFX6ZN4YBLN4WXD6IIBTMKXHFFDQEZNYTQLNZWOGDT22EY=
│  │     └─ ZTNHMICOWU6ZSNIR72ESLQSGDMLQYQ42XEKGOWSYYX5II===
│  │
```

(continues on next page)

(continued from previous page)

```
│  └─ FC
│     └─ ZKZRLZUODUUYTYA4457CSBPZXB5A77
│        └─ ...
├─ m
│  └─ ...
├─ masterkey.cryptomator
└─ masterkey.cryptomator.bkup
```

29.6 Format 3

Introduced in Cryptomator 1.0.0 on 2016-03-09.

Vault format 3 is basically the official “first” version. To be exact, it was actually introduced in Cryptomator Beta 0.11 on 2016-03-03. Vault formats 1 and 2 were only used in beta versions of Cryptomator.

This is an example of the vault structure:

```
.
├─ d
│  ├─ BZ
│  │  └─ R4VZSS5PEF7TU3PMFIMON5GJRNBDWA
│  │     ├─ USJ7VD36K7YU2RARYJMEFTABZOGN6LUH63VRH5MADVOZ433VZ7EPSM2PLJPHTBL6_
│  │     ├─ YWBBP7RC6FFX6ZN4YBLN4WXD6IIBTMKXHFFDQEZNYTQLNZWOGDT22EY=
│  │     ├─ ...
│  │     ├─ YWVRCCROEC3ZECD2UTJR7BGYERU3LG6R7QODBGMZ7EQ3BXGY24======_
│  │     └─ ZTNHMICOWU6ZSNIR72ESLQSGDMLQYQ42XEKGOWSYYX5II===
│  └─ FC
│     └─ ZKZRLZUODUUYTYA4457CSBPZXB5A77
│        └─ ...
├─ m
│  └─ ...
├─ masterkey.cryptomator
└─ masterkey.cryptomator.bkup
```