Cryptomator

In this article we will describe how to set up Cryptomator. We highly recommend Cryptomator if you want to synchronize encrypted files to/from the cloud, as it is much faster than using VeraCrypt containers.

Installation

First install Cryptomator. If you use anything other than Linux, simply follow the instructions for your operating system. If you are using Linux you may want to use the Cryptomator flatpak package. Depending on your distribution, you could also use your package manager repository, such as `apt` on Ubuntu/Debian or download the ApImage.

Setup

> [!tip] **Cryptomator has pretty good documentation!** Go ahead and check it out for more detailed instructions on lots of other functionalities.

Follow these steps to create your first vault:

- Click the `+` symbol in the lower-left corner and select `Create New Vault` if you don't have one already.

fresh cryptomator install

- Choose a name for the new vault and click `Next`
- Choose the location where your vault should be stored. This will be the place where you will access all your files later. Click `Next`
- Don't change the "expert settings", just click `Next`
- Enter your new password. It is important to choose a strong password to have solid encryption.

>

> [!warning] Recovery Key
>
> A recovery key can decrypt your data, without knowing your password. This raises the question where to store the recovery key. As you hopefully know, passwords should be stored in a good password manager. As long as your password is stored in a password manager and you have backups of your cryptomator vault and password database, you won't need a recovery key.
>
> We often experienced that people simply stored the recovery key file on their desktop, although they secured all their passwords in a password manager. Doing this defeats the purpose of the password manager, so if you don't have a good strategy for securing your recovery key - just don't save it and make regular backups.

- Finish creating your new vault.

Usage

After opening Cryptomator, press `Unlock` and enter your password. It also asks you whether to remember your password. If you use one of the built-in password managers of your operating system you can check that. Otherwise, leave it blank.

Now you see the general interface. With `Reveal Drive` you can directly open your decrypted vault, just as you can find it with your file manager.

screenshot: cryptomator interface

With `Lock` you will "close" the vault again, so that you will have to enter your password again.

Use Cryptomator in the Cloud

The huge benefit of Cryptomator is, that it can sync your encrypted vault to a cloud very efficiently.

> [!tip] To do this, simply move your vault into your sync cloud directory. See our example on setting up the sync client for Nextcloud.

Version #4
Erstellt: 2026-03-20 17:59:51 UTC von ESC-IT Migration Bot
Zuletzt aktualisiert: 2026-05-23 14:48:55 UTC von ESC-IT Migration Bot