Cryptomator - How to set up data encryption

04.07.2025 12:35:23

FAQ-Artikel-Ausdruck

Kategorie:	IT-Sicherheit & Anmeldung an Diensten::Datenverschlüsselung	**Bewertungen:**	0
Status:	öffentlich (Alle)	**Ergebnis:**	0.00 %
Sprache:	en	**Letzte Aktualisierung:**	11:41:08 - 29.01.2025

Schlüsselwörter

Boxcryptor Cryptomator Datensicherheit Verschlüsselung

Lösung (öffentlich)

This guide outlines how to set up the free version of Cryptomator, especially with regard to its use by a single user. For use in small groups/teams, please refer to the following [1]link.

Cryptomator use and features
-

Data encryption is possible with all common cloud providers (no restriction when using the desktop app; mobile apps compatible with Dropbox, Google Drive, OneDrive, pCloud, iCloud Drive when using iOS and every cloud via WebDAV and S3)

-

Encrypted storage of files on network drives (no restriction when using the desktop app)

-

End-to-end and zero-knowledge encryption

-

Password recovery using recovery keys

-

Software "Made in Germany"

Setting up Cryptomator

To set up Cryptomator to encrypt your files and folders, you must first install the client.
There are corresponding downloads for MacOS, Windows, Linux, Android and iOS at: [2]https://cryptomator.org/downloads/

-

To begin the set up process, open Cryptomator and click on "Add"to add a new safe. Enter a name for the safe and click on "Next."

Screenshot of Cryptomator: Input screen for new vault

-

Specify the folder in which the encrypted data is to be stored. These can be local folders on your computer or folders from cloud storage providers. The folders must be unencrypted. For example, they must not be located within a folder encrypted with Boxcryptor.

-

A password must then be assigned for the encryption. Make sure you create a recovery key (important)! Save the recovery key so that you can access it at any time (save a copy or print it out). Without this key, your data cannot be recovered if you forget your password.

Screenshot of Cryptomator: Set password and create recovery key

-

After completing this process, you can unlock the safe with the assigned password. You can display your encrypted drive on your desktop or open the folder in your file manager (e.g. Windows Explorer) as usual. It is displayed as an additional drive.

Screenshot of Cryptomator: Display after decrypting a vault

-

Now, you can store your sensitive data there.

If you have any further questions or queries, you can find [3]detailed instructions on the manufacturer's website.

[1] https://tickets.tu-dresden.de/otrs/public.pl?Action=PublicFAQZoom;ItemID=1263
[2] https://cryptomator.org/downloads/
[3] https://docs.cryptomator.org/en/latest/desktop/adding-vaults/