

Encrypted-Files-In-Cloud

“ [!toc] Table of Contents

Using a cloud to synchronize your files over devices or to collaboratively work on them as a group is very useful. The main downside is that no cloud solution offers secure, working end-to-end encryption per default, at least until now (2026).

Therefore, the easiest and safest method is to synchronize your cloud files with your device and to put your sensitive files inside an encrypted container inside the synced folder.

“ [!tip]

1. Setup the [Nextcloud Sync-Client](#)
2. Setup [group permissions](#) in Nextcloud
3. Setup a [Cryptomator vault](#) inside your Nextcloud folder

Now that everyone of you has access to the encrypted folder you will have to share the password through a secure channel.

Potential issues

There may be issues, when two or more of you try to open, edit and save a file at the same time. If that happens so called "conflicts" appear, because the server doesn't know which changes to accept first, or in which order.

“ [!technical] Technical

When you open a file in LibreOffice for example, there will be a file with the ending `.lock` right next to the file you just opened. This small file will get synced to the cloud and from there to your friends devices. When they try to open the same file now, their program sees the `.lock` file and knows, that another program (on your device) is currently editing this file and therefore "locked" it up. The actual problems may arise, when the first person opens the

file and before the `.lock` file is being synced to you friends device, they open the file, too. So now both of you opened the file in editing mode. While this is completely fine in the browser, when using encrypted folders this can become part the issue described above.

Version #1

Erstellt: 2026-08-07 17:04:51 UTC von ESC-IT Migration Bot

Zuletzt aktualisiert: 2026-08-07 17:04:51 UTC von ESC-IT Migration Bot