Nextcloud data encryption with Server Side Encryption

While we of course can't (and don't want to) prevent you from enabling, we would like to caution you to take into consideration the following:

Server Side Encryption provides protection for data on 'external storage' (using external storage app) as the files are encrypted before being uploaded to external storage, and the keys never leave the Nextcloud server. When external storage is not used and a server-wide key is used (which is often the case in our configurations), server side encryption would only cause additional overhead, not just in terms of performance, but also size, as encryption adds more data to files and therefore makes them bigger. In addition, we've also observed some pretty nasty cases of the encryption feature breaking down, and it usually isn't that pretty because in one of our experiences, it has caused a week of downtime. So, unless you're using external storage for Nextcloud, we'd recommend leaving it off.

If what you're looking for is more towards end-to-end encryption (meaning files are encrypted before even being uploaded to Nextcloud), while there is https://apps.nextcloud.com/apps/end_to_end_encryption, its reviews are ... not positive. Some of our subscribers have had success using https://cryptomator.org/ though!

Documentation how to enable E2EE: https://docs.cloud68.co/books/open-source-software-instances-faqs/page/nextcloud-data-encryption-with-e2ee
Documentation how to enable Cryptomator: https://docs.cloud68.co/books/open-source-software-instances-faqs/page/nextcloud-data-encryption-with-cryptomator

---

Revision #2
Created 2026-01-30 10:56:16 CET by Irdi
Updated 2026-02-03 08:50:59 CET by Irdi