Using server-side encryption

- Encryption FAQ
  - How can encryption be disabled?
  - Is it possible to disable encryption with the recovery key?
  - Can encryption be disabled without the user's password?
  - Is it planned to move this to the next user login or a background job?
  - Is group sharing possible with the recovery key?
- Using encryption
- Sharing encrypted files
  - Recovery key password
- Files not encrypted
  - Change private key password

Nextcloud includes a server-side encryption app, and when it is enabled by your Nextcloud administrator all of your Nextcloud data files are automatically encrypted on the server. Encryption is server-wide, so when it is enabled you cannot choose to keep your files unencrypted. You don't have to do anything special, as it uses your Nextcloud login as the password for your unique private encryption key. Just log out and in and manage and share your files as you normally do, and you can still change your password whenever you want.

Its main purpose is to encrypt files on remote storage services that are connected to your Nextcloud server. This is an easy and seamless way to protect your files on remote storage. You can share your remote files through Nextcloud in the usual way, however you cannot share your encrypted files directly from the remote service you are using, because the encryption keys are stored on your Nextcloud server, and are never exposed to outside service providers.

If your Nextcloud server is not connected to any remote storage services, then it is better to use some other form of encryption such as file-level or whole disk encryption. Because the keys are kept on your Nextcloud server, it is possible for your Nextcloud administrator to access your unencrypted files, and if the server is compromised the intruder may get access to your files. (Read Encryption in Nextcloud to learn more.)

Encryption FAQ

How can encryption be disabled?

The only way to disable encryption is to run the "decrypt all" script, which decrypts all files and disables encryption.

Is it possible to disable encryption with the recovery key?

Yes, *if* every user uses the file recovery key, "decrypt all" will use it to decrypt all files.

Can encryption be disabled without the user's password?

If you don't have the users password or file recovery key, then there is no way to decrypt all files. What's more, running it on login would be dangerous, because you would most likely run into timeouts.

Is it planned to move this to the next user login or a background job?

If we did that, then we would need to store your login password in the database. This could be seen as a security issue, so nothing like that is planned.

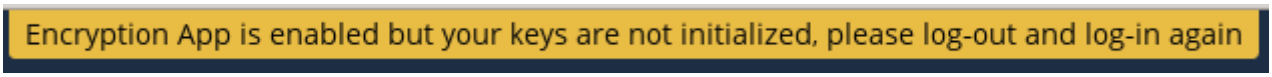
Is group sharing possible with the recovery key?

If you mean adding users to groups and make it magically work? No. This only works with the master key.

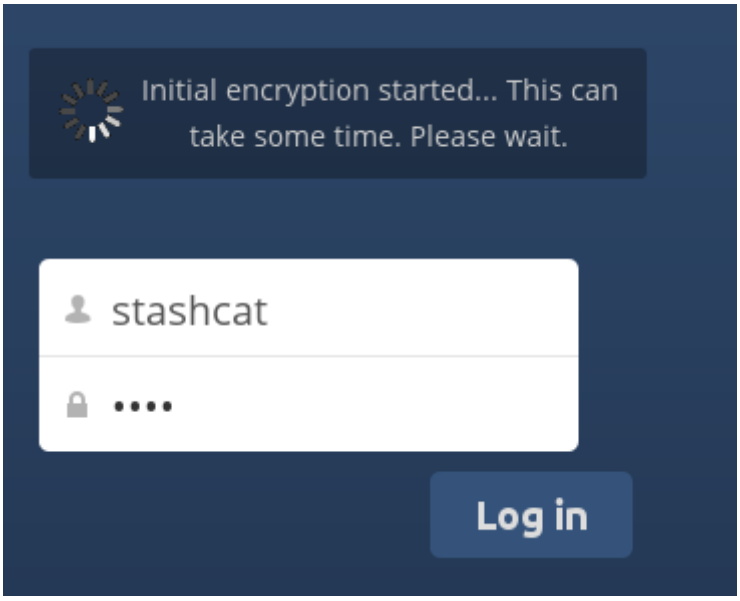
Using encryption

Nextcloud encryption is pretty much set it and forget it, but you have a few options you can use.

When your Nextcloud administrator enables encryption for the first time, you must log out and then log back in to create your encryption keys and encrypt your files. When encryption has been enabled on your Nextcloud server you will see a yellow banner on your Files page warning you to log out and then log back in:



When you log back in it takes a few minutes to work, depending on how many files you have, and then you are returned to your default Nextcloud page.



> You must never lose your Nextcloud password, because you will lose access to your files. Though there is an optional recovery option that your Nextcloud administrator may enable; see the Recovery Key Password section (below) to learn about this.

Sharing encrypted files

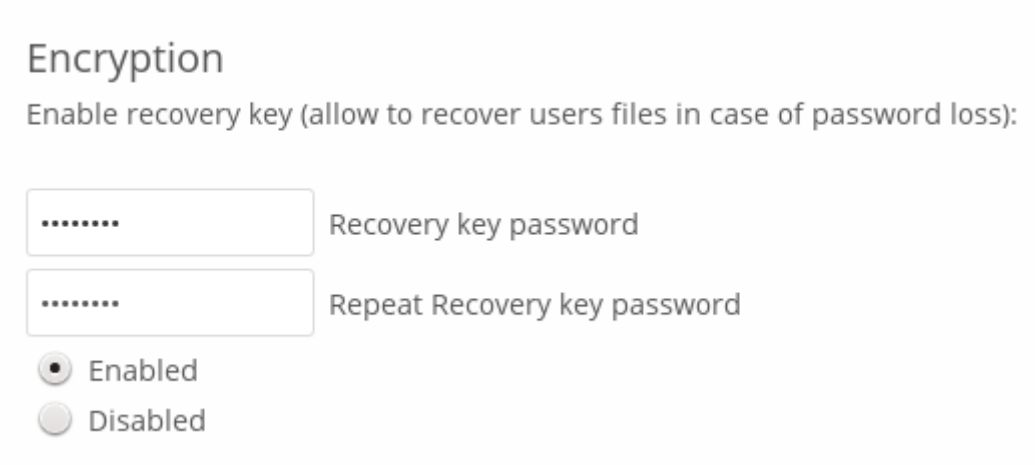
Only users who have private encryption keys have access to shared encrypted files and folders. Users who have not yet created their private encryption keys will not have access to encrypted

shared files; they will see folders and filenames, but will not be able to open or download the files. They will see a yellow warning banner that says "Encryption App is enabled but your keys are not initialized, please log-out and log-in again."

Share owners may need to re-share files after encryption is enabled; users trying to access the share will see a message advising them to ask the share owner to re-share the file with them. For individual shares, un-share and re-share the file. For group shares, share with any individuals who can't access the share. This updates the encryption, and then the share owner can remove the individual shares.

Recovery key password

If your Nextcloud administrator has enabled the recovery key feature, you can choose to use this feature for your account. If you enable "Password recovery" the administrator can read your data with a special password. This feature enables the administrator to recover your files in the event you lose your Nextcloud password. If the recovery key is not enabled, then there is no way to restore your files if you lose your login password.



Files not encrypted

Only the data in your files is encrypted, and not the filenames or folder structures. These files are never encrypted:

- Old files in the trash bin.
- Image thumbnails from the Gallery app.
- Previews from the Files app.
- The search index from the full text search app.
- Third-party app data

Change private key password

This option is only available if the encryption password has not been changed by the administrator, but only the log-in password. This can occur if your Nextcloud provider uses an external user back-end (for example, LDAP) and changed your login password using that back-end configuration. In this case, you can set your encryption password to your new login password by providing your old and new login password. The Encryption app works only if your login password and your encryption password are identical.

□□□ #2

□ cocobook-sync □□□ 2026-10-28 16:22:13 UTC

□ cocobook-sync □□□ 2026-10-29 01:09:08 UTC