

9.3 Two-Factor Authentication

Two-factor authentication requires a second confirmation after the password.

Open **Settings** → **Security**. LightDrive offers:

- **Authenticator app** — time-based codes that work offline and provide the best general-purpose 2FA option.
- **Mobile app approval** — approve requests in the official Nextcloud mobile app.
- **Email verification codes** — receive a one-time code at the verified recovery address.



Security



Protect your LightDrive account by choosing one or more sign-in protections. The strongest options are **Paskeys** and an **Authenticator app**.



Two-factor authentication is not enabled.

We strongly recommend turning it on to protect your account.

To turn on stronger sign-in protection, add a passkey (strongest), an authenticator app, mobile approval, or email verification codes.

Password & sign-in

Change your account password.

[Change password](#)

Paskeys (recommended) Off

Sign in using your device's secure unlock (Face ID, Touch ID, Windows Hello, or a security key).

[Add passkey](#)

[Manage passkeys](#)

Two-factor authentication

Two-factor authentication (2FA) adds an extra layer of protection. After entering your password, you'll confirm sign-in with a trusted device or code.

Authenticator app Off

Works offline · best overall.

[Set up authenticator app](#)

Mobile app approval Off

Easy · requires a signed-in mobile app.

Approve sign-in requests from a compatible mobile app on your phone.

Security settings list the sign-in and two-factor methods available for the account.

Add at least one method, test it in a separate private browser window, and generate backup codes. Do not remove the last working method until its replacement has been tested.

Current online article: <https://help.lightdrive.one/security-and-privacy/two-factor-authentication>

Generated September 1, 2026