LIGHTDRIVE HELP CENTER

LightDrive User Manual

Chapter 9 - Security and Privacy

Generated September 30, 2026

Contents

9.1 How LightDrive Protects Your Account

9.2 Your Password

9.3 Two-Factor Authentication

9.4 Email Verification Codes

9.5 Passkeys

9.6 Backup Codes

9.7 Vault App Passwords and Client Passwords

9.8 Reviewing Account Security

9.9 Recovery Email Security

9.10 Privacy in LightDrive

Chapter 9 - Security and Privacy

9.1 How LightDrive Protects Your Account

LightDrive protects accounts with encrypted HTTPS connections, password controls, optional passkeys and two-factor methods, separately revocable Vault app passwords and LightDrive client passwords for email, contacts, and calendars, active-session review, recovery-email verification, and coordinated account-status enforcement.

Security also depends on your choices. Use a unique password, enable a passkey or authenticator app, store backup codes outside LightDrive, protect connected devices with a screen lock, and revoke sessions, Vault app passwords, or client passwords you do not recognize or no longer use.

LightDrive cannot make a deliberately shared public link private after another person has copied its contents. Review shares, connected apps, and account notices as part of routine security maintenance.

Current online article: https://help.lightdrive.one/security-and-privacy/how-lightdrive-protects-your-account

9.2 Your Password

Your main password signs you in to the Vault and can authenticate compatible Files and Calendar clients. It does not authenticate external email or contacts clients.

Use a long, unique password that is not used for any other site. A password manager can create and store it. Do not send it by email or enter it on a site other than an expected LightDrive sign-in page.

Change the password under **Settings → Security → Password & sign-in**. A Files or Calendar client that stores the main password must be updated afterward. Vault app passwords and LightDrive client passwords remain separate and do not change when you change the main password.

For third-party apps, a separately revocable client password is usually preferable when one is available because it can be limited to the services that app needs.

If you forget the password, use the recovery link on the Vault sign-in page. Instructions go to the verified recovery email address.

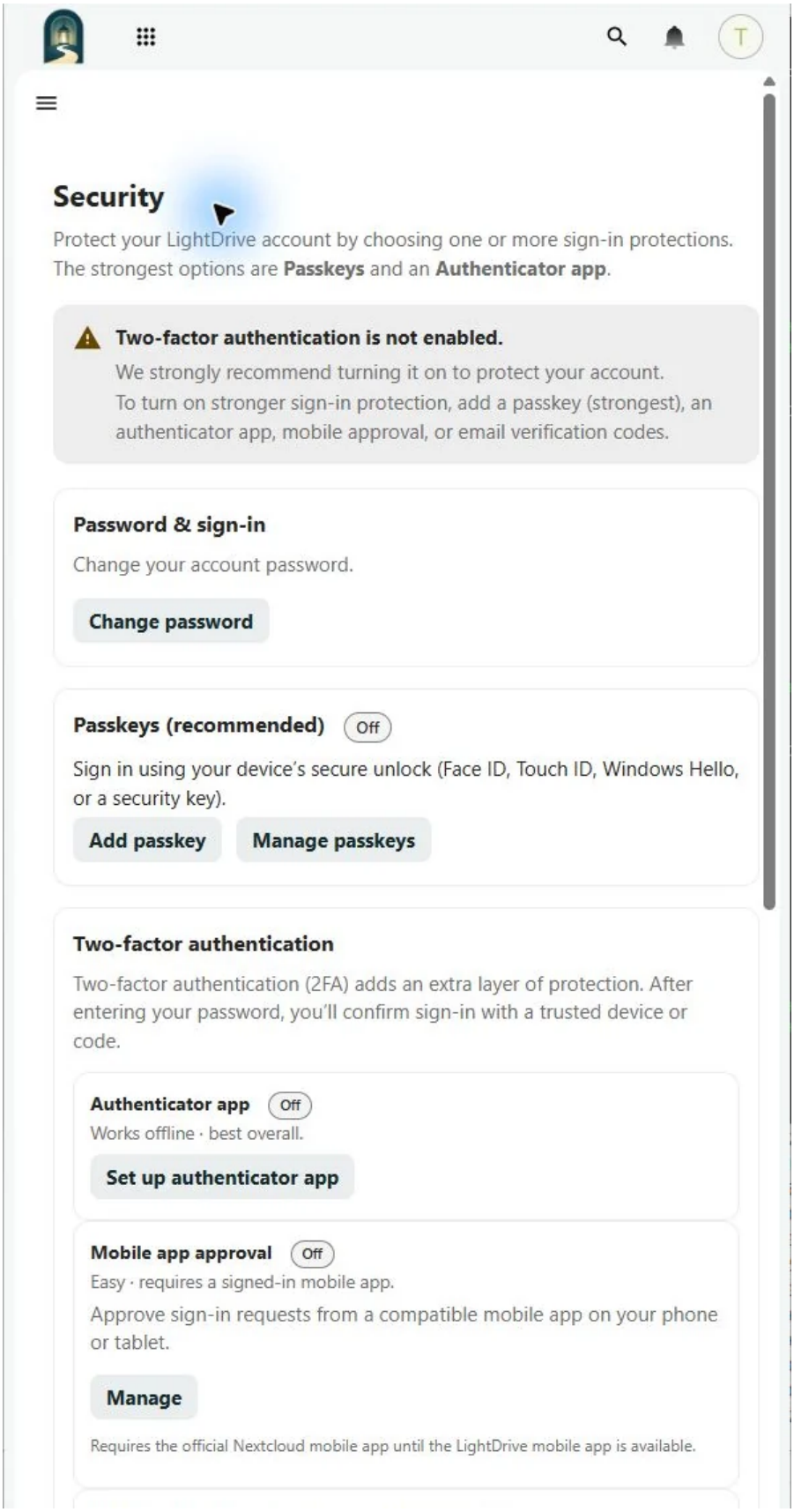
Current online article: https://help.lightdrive.one/security-and-privacy/your-password

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 Passkeys 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
Passkeys (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 or tablet.
Manage
Requires the official Nextcloud mobile app until the LightDrive mobile app is available.

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

9.4 Email Verification Codes

Email verification codes are LightDrive’s basic two-factor option. After you enter the password, LightDrive sends a one-time code to the verified recovery email address.

Open **Settings → Security → Two-factor authentication**, then use **Manage** under **Email verification codes** to enable or disable the method.

This option is convenient but depends on the security and availability of the recovery mailbox. A passkey or authenticator app provides stronger protection. Keep the recovery email password different from the LightDrive password and enable strong sign-in protection on that mailbox too.

Current online article: https://help.lightdrive.one/security-and-privacy/email-verification-codes

9.5 Passkeys

A passkey uses a device’s secure unlock—such as Face ID, Touch ID, Windows Hello, an Android screen lock, or a hardware security key—to confirm sign-in.

Open **Settings → Security → Passkeys** and select **Add passkey**. Follow the browser or operating-system prompt, then give the credential a name that identifies the device. Use **Manage passkeys** to review or remove registered credentials.

Add more than one passkey or keep another tested 2FA method and backup codes. Removing a passkey from LightDrive does not erase credentials stored for other sites, and removing it from a device does not automatically remove its LightDrive registration.

Current online article: https://help.lightdrive.one/security-and-privacy/passkeys

9.6 Backup Codes

Backup codes are one-time recovery codes for a sign-in where your normal passkey, authenticator app, mobile approval, or email code is unavailable.

Open **Settings → Security → Backup codes** and select **Manage**. Generate the codes, save them outside LightDrive, and keep them where another person cannot read them.

Each code works once. Mark a used code or remove it from your saved copy. Generating a new set invalidates the previous set, so replace every stored copy.

Backup codes do not replace the account password and should not be used as an everyday sign-in method.

Current online article: https://help.lightdrive.one/security-and-privacy/backup-codes

9.7 Vault App Passwords and Client Passwords

LightDrive provides separately revocable credentials for connected apps and devices. Use a separate credential for each app or device when practical, and choose only the services that app needs.

Vault app passwords

Use a Vault app password with Files, Calendar, and other Vault services when a client cannot complete browser sign-in or two-factor authentication.

1. Open **Settings → Security → App & device access**.
2. Under **Vault app passwords**, enter a name that identifies the app and device.
3. Select **Create Vault app password** and copy the value immediately.
4. Enter it in the compatible Vault client in place of your main password.

A Vault app password does not provide access to LightDrive Email or CardDAV Contacts.

LightDrive client passwords

For external email, contacts, calendar, and task apps, LightDrive can create a LightDrive client password limited to the services that app needs. It does not grant Files access. Available access combinations include:

- **Email only**
- **Contacts only**
- **Calendars only**
- **Email & contacts**
- **Email & calendars**
- **Contacts & calendars**

- **Email, contacts & calendars**

For example, an email app that only uses IMAP and SMTP should normally receive an **Email only** password. An app such as Thunderbird that uses email, contacts, and calendars can use one **Email, contacts & calendars** password for all three services.

1. Open **Settings → Security → App & device access**.
2. Enter a name that identifies the app or device.
3. Choose the narrowest service combination the app requires.
4. Select **Create client password** and copy the value immediately.
5. Enter that client password into each enabled LightDrive service used by the app.

External email clients require a client password that includes **Email**; your main LightDrive password and Vault app passwords do not authenticate to IMAP or SMTP.

Calendar clients may use your main LightDrive password, a Vault app password, or a LightDrive client password that includes **Calendars**. Compatible Tasks/CalDAV clients also use the **Calendars** scope. For third-party calendar and task apps, a separately revocable client password is generally preferable.

Contacts clients require a LightDrive client password that includes **Contacts**. Your main LightDrive password and Vault app passwords do not authenticate to the LightDrive CardDAV service.

Each client-password value is shown only when it is created. If you lose it, revoke it and create another. Naming each credential for one app and device makes it easier to remove access later without interrupting other connections.

Revoking a Vault app password or client password does not change your main LightDrive password. Treat every credential as a secret and use it only for the access shown when it was created.

9.8 Reviewing Account Security

Review your main Security settings regularly and remove access you no longer recognize or use.

Settings → Security

- Confirm that your main password is unique and current.
- Review passkeys and remove credentials for devices you no longer control.
- Confirm that at least one strong two-factor method works.
- Generate current backup codes and store them outside LightDrive.
- Review active sessions and end any session you do not recognize.
- Review Vault app passwords and revoke any that are no longer needed.
- Review LightDrive client passwords for email, contacts, and calendars, and revoke credentials for apps or devices you no longer use or recognize.

Also review the recovery email under **Settings → Account** and file shares in Files. Contact Support immediately if you see access you cannot explain.

Current online article: https://help.lightdrive.one/security-and-privacy/reviewing-account-security

9.9 Recovery Email Security

The recovery email can receive password-reset links, verification codes, and important account notices. Protect it as carefully as the LightDrive account.

- Use an address you control continuously.
- Use a password different from the LightDrive password.
- Enable strong two-factor authentication on the recovery mailbox.
- Keep its recovery methods current.

A recovery-email change remains pending until the new address is verified. If you receive an unexpected change message, sign in to the Vault directly, cancel the pending change from the banner, change your password, and review active sessions.

Current online article: https://help.lightdrive.one/security-and-privacy/recovery-email-security

9.10 Privacy in LightDrive

LightDrive is designed to store and organize personal data without turning account activity into an advertising profile.

Your files, email, calendars, contacts, reading library, and settings are private to the account unless you choose a sharing feature. Public links and shares intentionally disclose the selected content to the people or audience you authorize.

LightDrive processes account and service information needed to authenticate users, deliver messages and files, synchronize data, bill plans, prevent abuse, support users, and meet legal obligations. The current Privacy Policy describes those purposes, retention rules, and rights in full.

Review **Settings → Legal** for the policy versions associated with your account and use the canonical policy links in Chapter 14.

Current online article: https://help.lightdrive.one/security-and-privacy/privacy-in-lightdrive