

9.7 Vault, Email, and Contacts

Client Passwords

LightDrive provides separately revocable credentials for connected apps. Choose the narrowest access that fits the app. One Email & contacts password may be used for both services by a compatible app; other credential types remain limited to their named services.

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 Vault client in place of your main password.

Email client passwords

Use an Email client password with LightDrive IMAP and authenticated SMTP clients such as Thunderbird, Outlook, Apple Mail, or an Android mail app. External email clients require this credential; the main Vault password and Vault app passwords do not authenticate to email.

1. Under **Email client passwords** in **Settings** → **Security** → **App & device access**, enter a name that identifies the app and device.
2. Choose **Email & contacts** when the app also supports CardDAV, or **Email only** when it does not need contacts.
3. Select **Create client password** and copy the value immediately.

4. Enter it as the normal password for both incoming and outgoing mail. An Email & contacts password can also be entered for CardDAV.

Contacts-only client passwords

Use a Contacts-only client password with a phone, contacts synchronization app, or another CardDAV client that does not need email access.

1. Open the Vault **Contacts** app and select **Mobile & app connections**.
2. Enter a name that identifies the contacts app and device.
3. Create the password and copy the value immediately.
4. Enter it as the CardDAV password with your full LightDrive email address as the username.



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.

Email verification codes (basic protection) Off

Convenient · depends on email security.

Receive a one-time code at your recovery email address.

Manage

Less secure than a passkey or authenticator app, but better than a password alone.

Backup codes (2FA recovery) Available

Use if you cannot access your normal 2FA method.

Backup codes are one-time sign-in codes. Use them when you cannot access your authenticator app, passkey, mobile approval, or email verification code. Store them somewhere safe.

Manage

App & device access

Some apps and devices can't use 2FA directly. Create an app password for each connected device that needs one. App passwords are for desktop/mobile clients and third-party apps. They do not replace your main password.

e.g. iPhone Mail or Thunderbird

Create app password

You can revoke app passwords at any time. Revoke an app password by removing it from the Sessions list.

Vault app passwords and Email client passwords are managed in Security settings.
Contacts-only client passwords are managed inside the Contacts app.

Each value is shown only when created. If it is lost, revoke it and create another. Name each credential for one app and device so you can revoke access without interrupting another connection.

Each credential can be revoked without changing the main password. Treat every credential as a secret and use it only for the access shown when it was created.

Current online article: <https://help.lightdrive.one/security-and-privacy/app-passwords>

Generated September 9, 2026