

Own your passwords.

Replace LastPass with KeePassXC — a local vault, no server.

Your passwords in a single encrypted file that lives on your devices — no cloud account, no subscription, and no company to get breached on your behalf.

Who this is for

Anyone leaving LastPass who wants the simplest possible setup: no server to run, just an encrypted file you keep and sync yourself. Comfortable managing a file across devices.

Pay Once — the offline & one-time-purchase app directory · payoncehq.com

Free guide · pay what you want · share freely

Why KeePassXC

LastPass limits its free plan to one device type and has a rocky security history. **KeePassXC** takes a different approach: your passwords live in a single encrypted `.kdbx` file on your own machine, protected by a master password. No account, no cloud, no subscription — free and open source.

KeePassXC or Vaultwarden?

KeePassXC is a local file you sync yourself — simplest, nothing to host. Vaultwarden is a small server you run for live sync across devices and users. Pick KeePassXC if you'd rather not run a server; Vaultwarden if you want Bitwarden-style always-on sync.

1 · Install KeePassXC

KeePassXC runs on Windows, macOS and Linux. On phones, use a compatible app that opens the same `.kdbx` file (KeePassDX on Android, Strongbox on iOS).

2 · Create your vault

Create a new database and choose a **strong master password** — this is the one password you must remember, and it's the only key to everything. Save the `.kdbx` file somewhere you'll sync (see step 5).

3 · Export from LastPass

In LastPass: Account Options → Advanced → Export → **LastPass CSV File**. Enter your master password to authorize, and save the CSV to your drive.

The CSV is plain text — delete it after

The export contains every password unencrypted. As soon as the import succeeds, securely delete it — on Linux/macOS use `shred -u lastpass_export.csv`. Never leave it in Downloads or a synced folder.

4 · Import into KeePassXC

In KeePassXC: **Database** → **Import** → **CSV File**, select your export, and map the columns so each CSV column lands in the right field (URL, username, password, notes).

Watch the & characters

LastPass encodes an ampersand in a password as `'&'`. KeePassXC takes it literally, which breaks those logins. After importing, do a find/replace to turn `'&'` back into `'&'` in affected entries.

5 · Browser autofill & sync

- Install the KeePassXC browser extension for autofill just like LastPass had.
- To use the vault on several devices, sync the `.kdbx` file with a tool you trust — Syncthing, Nextcloud, Dropbox or similar. The file is encrypted, so the sync provider can't read it.

- Keep a backup copy of the file somewhere safe — lose it and there's no reset.

6 · Verify, then cancel

- Spot-check several logins, including any with special characters, and fix & issues.
- Confirm the browser extension autofills.
- Confirm the vault opens on your second device after sync.
- Only then delete your LastPass vault and close the account.

Common snags

Symptom	Fix
Some logins fail	Ampersand encoding: replace '&' with '&' in those entries.
Columns imported wrong	Redo the import and re-map the CSV columns carefully.
Vault out of date on a device	Your sync hasn't run; the .kdbx file must be the same copy.

Found this useful?

This guide is free — pay what you want if it saved you time. More offline & one-time-purchase alternatives to subscription apps, plus other migration guides, at payoncehq.com.

Sources: official KeePassXC and LastPass export documentation. Steps current as of 2026; check the projects for the latest. Independent guide, not affiliated with KeePassXC or LastPass.