

Sigillum for macOS

User manual · version 4.8.1 · macOS 14 (Sonoma) or later · Apple Silicon & Intel

Contents

- | | |
|----------------------------|--------------------------|
| 1. Install | 6. Add an existing vault |
| 2. Create your first vault | 7. Settings & languages |
| 3. Unlock & mount | 8. Sync vault to cloud |
| 4. Browse in Finder | 9. Troubleshooting |
| 5. Lock & auto-lock | 10. Security model |

1. Install

Open the **Mac App Store**, search for *Sigillum*, and click *Get*. macOS handles the install, the code-signature check, and the first-launch entitlement prompts.

Anti-tamper, by Apple. Mac App Store installs are signed by Apple's deployment key, notarized, and shipped under the *Hardened Runtime* + *App Sandbox*. The binary on your Mac is bit-identical to the one Apple reviewed — nothing in between can swap it out for a tampered build, exfiltrate your passwords, or copy your TOTP secret. Equivalent guarantee to Android's Play Integrity API.

2. Create your first vault

1. Click the **+** button in the toolbar, then choose *New Vault...*
2. Pick a **backend** — a folder anywhere on disk where Sigillum will store the encrypted blobs. iCloud Drive, Dropbox, Google Drive, and any synced folder all work.
3. Pick a **config location** — where the small `.cbor` config file lives. Keep this separate from the backend for an extra layer of paranoia (config carries the wrapped keys).

4. Choose a **cipher suite**. Default: *AES-256-GCM-SIV + ML-KEM-768 + ML-DSA-65*. This is the recommended hybrid post-quantum profile.
5. Set passwords:
 - **FS password** — unlocks the file system.
 - **Config password** — unlocks the config file (defence in depth).
 - Optional **TOTP** — pair with 1Password or Authy.
6. Click *Create vault*. Argon2id key derivation takes ~3-8 seconds on modern Macs — this is intentional.

3. Unlock & mount

Select a vault in the sidebar, click **Unlock**, enter your FS & config passwords (and TOTP if enrolled). Sigillum mounts the vault at `~/Volumes/<vault-name>` via fuse-t.

You can also **unlock with Touch ID** after the first manual unlock. Toggle this in Settings → Convenience.

4. Browse in Finder

Click **Open in Finder** on the unlocked vault, or just navigate to `~/Volumes/<vault-name>`. The mount behaves like any folder — drag files in to encrypt, drag out to decrypt, double-click documents to edit them in-place. Every app you already use just sees regular files.

5. Lock & auto-lock

Click **Lock** on the vault to unmount and zero the in-memory keys. Sigillum also locks automatically after the timeout configured in Settings (default: 5 minutes idle).

6. Add an existing vault

Have a vault created on another device (Android, iOS, Linux)? Click **+** → *Add Existing Vault...*, point at the backend folder, and Sigillum reads the config in place.

encfs import is disabled in 4.8.1. Migrating from a legacy encfs vault required heavier dependencies than we wanted to ship for this release. Re-enabled in 4.9.0.

7. Settings & languages

Open **Sigillum** → **Settings** (⌘, ,):

- **Language** — 16 locales (English, French, German, Spanish, Italian, Dutch, Polish, Ukrainian, Russian, Korean, Chinese-Traditional, Swedish, Norwegian, Finnish, Danish, Portuguese).
- **Color theme** — 4 system-respecting themes.
- **Auto-lock** — 1, 5, 15, 60 minutes, or off.
- **Touch ID** — toggle biometric unlock.

8. Sync your vault to the cloud

Sigillum doesn't sync; it lets your existing cloud client do it.

1. Choose a backend folder that's already inside iCloud Drive, Dropbox, Google Drive, OneDrive, or Nextcloud's sync root.
2. That's it. Encrypted blobs sync exactly like any other files; whichever client you use sees opaque ciphertext.

For multi-device, repeat *Add Existing Vault...* on each device pointing at the synced folder. The same vault opens everywhere with the same passwords.

9. Troubleshooting

"fuse-t is not running"

Open **System Settings** → **Privacy & Security**, scroll to *Allow system software from developer "FUSE for macOS"*, click *Allow*. Reboot if requested. Then re-launch Sigillum.

Vault mount disappears after sleep

macOS unmounts fuse-t volumes when the laptop sleeps for too long. Re-unlock the vault when you wake the Mac. Auto-lock-on-sleep is the secure default.

“Wrong password” but I’m sure it’s right

Check Caps Lock and your keyboard layout (the FS password and config password may have been set with a different layout). Try unlocking on another device to confirm the password works.

I lost my config password

Sigillum is zero-knowledge: **we cannot recover it**. This is the feature you’re paying for. Restore from your password manager, paper backup, or recovery shares (Pro tier).

10. Security model in 30 seconds

- Every vault has its own **master key** wrapped with hybrid **X25519 + ML-KEM-768**.
- The config blob is signed with **ML-DSA-65** — tampering is detected on unlock.
- File content is encrypted with **AES-256-GCM-SIV** per 64 KiB block; filenames are HMAC-name-sealed with a per-vault key.
- Master keys live in **Apple Keychain**; secrets are zeroed on lock; the app makes **no network calls** on its own.