

# Sigillum for Android

User manual · version 2.6.1 · Android 9 (API 28) or later · arm64 / armv7 / x86\_64

## Contents

- |                                 |                                 |
|---------------------------------|---------------------------------|
| 1. Install                      | 7. Quick-note from launcher     |
| 2. Create your first vault      | 8. Cloud sync (any provider)    |
| 3. Pick a storage backend (SAF) | 9. Settings, themes & languages |
| 4. Unlock with biometrics       | 10. Troubleshooting             |
| 5. Browse files                 | 11. Security model              |
| 6. Share-into-vault             |                                 |

## 1. Install

---

Install **Sigillum** from [Google Play](#). Play handles the install, the signature check, and tamper-attestation enrolment automatically.

**Play Integrity API protects every install.** On launch, Sigillum asks Google Play to attest that (a) the running binary is the exact one Play distributed, (b) the device is genuine and not running in an emulator or root-modified state, and (c) no other process has injected code into Sigillum. If any check fails, a red banner appears and unlock is blocked. In practical terms: **your vault passwords, TOTP secrets, and decrypted file content cannot be exfiltrated by a tampered or repackaged copy** — that copy will refuse to run before it ever sees them.

## 2. Create your first vault

---

1. Tap the **+** button.
2. Pick the storage backend — see [SAF backends](#) below.
3. Choose the cipher suite (default: AES-256-GCM-SIV + ML-KEM-768 + ML-DSA-65).

4. Set FS password, config password, and (optional) TOTP.
5. Enrol biometric unlock.
6. Tap *Create vault*. Argon2id key derivation takes ~5-10 seconds on a Pixel-class phone.

### 3. Pick a storage backend

---

Sigillum uses Android's **Storage Access Framework (SAF)** for every backend — that's how it talks to your cloud apps without baking provider-specific SDKs into the binary.

- **Local folder** — SD card, internal storage.
- **Nextcloud** — install the Nextcloud Android app first; Sigillum picks the cloud root through SAF.
- **Google Drive** — via the Drive app + SAF.
- **Dropbox, OneDrive, Box** — same pattern, install the official app then pick through SAF.
- **WebDAV / SMB** — install a SAF provider like RCX or MaterialFiles, then pick the share through SAF.

### 4. Unlock with biometrics

---

After the first manual unlock with passwords, enrol Class 3 biometrics (fingerprint or face). Subsequent unlocks need just the biometric prompt; the wrapped keys live in Android Keystore.

### 5. Browse files

---

The in-app browser shows decrypted filenames, sizes, modified times. Tap to open with your installed apps (PDF readers, viewers, Markdown editors); long-press to share, rename, or delete.

### 6. Share-into-vault

---

Sigillum registers as a system **share target**. From any app — Photos, browser, camera, Files — tap *Share*, pick *Sigillum*, choose a vault, and the file lands encrypted.

## 7. Quick-note from the launcher

---

Long-press the Sigillum icon on your launcher → *New note*. Type, tap save, and the note lands in your default vault as an encrypted `.md` file.

## 8. Cloud sync (any provider)

---

Sigillum doesn't implement sync — your cloud provider's app does. Configure the backend as a SAF-mounted cloud folder; whatever app owns that folder uploads ciphertext blobs in the background.

For mirror backups across multiple clouds, point a Sigillum-managed backup at a second SAF root. The encrypted blobs are safe to mirror anywhere — none of the providers can read each other's copy.

## 9. Settings, themes & languages

---

- **16 languages** — English, French, German, Spanish, Italian, Dutch, Polish, Ukrainian, Russian, Korean, Chinese (Traditional), Swedish, Norwegian, Finnish, Danish, Portuguese.
- **Color themes** — respects Android Material You.
- **Auto-lock** — configurable timeout, plus lock-on-screen-off and lock-on-background.
- **Backup sync** — pick a secondary SAF root to mirror encrypted blobs to.

## 10. Troubleshooting

---

### Backup sync didn't copy a subfolder

Confirm the SAF provider grants *persisted* write permission to the parent folder you picked. Some cloud apps drop permission across reboots — re-pick the folder if Sigillum shows a permission warning.

### Sigillum doesn't appear in the share sheet

Android caches share targets aggressively. Open Sigillum once, then re-open the share sheet — it should now list Sigillum.

## I forgot my config password

Sigillum is zero-knowledge. We cannot recover it. Restore from your password manager, paper backup, or recovery shares (Pro).

## 11. Security model in 30 seconds

---

- Master key wrapped with hybrid **X25519 + ML-KEM-768**.
- Config signed with **ML-DSA-65**.
- File content: **AES-256-GCM-SIV** per block (configurable to XChaCha20-Poly1305).
- Master keys in **Android Keystore**, Class-3 biometric bound. Secrets zeroed on lock.
- App makes **no network calls** on its own — only the cloud apps you SAF-mount.