

# KluisAPP

---

## *EXTENDED USER MANUAL*

Version 0.3.1 • Android • English edition • October 2026

Jeffrey Haimé | Jeffrey-Apps

Important: the names of interface controls are descriptive translations; check the exact wording in your installed app.

## **Contents**

1. Reading guide
2. What is KluisAPP?
3. Installation and first-time setup
4. Unlocking and locking
5. Adding and moving files
6. Viewing photos, videos and documents
7. Exporting and deleting
8. Settings and access credentials
9. Creating a complete encrypted backup
10. Restoring from a backup
11. Internal storage and SD card
12. Security and privacy
13. Troubleshooting
14. Frequently asked questions
15. Glossary
16. Safe-use checklist

## **1. Reading guide**

This manual describes the regular KluisAPP 0.3.1 based on the stable source-code inventory and practical tests. Menu wording may vary slightly by device and app language.

**IMPORTANT: Keep your password or PIN and your recovery code securely outside the vault. If all valid access credentials are lost, encrypted files may be permanently inaccessible.**

## 2. What is KluisAPP?

KluisAPP is an Android application for storing photos, videos and other files in an encrypted vault. Storage can be app-private internal storage or a selected folder on a removable SD card.

The app imports files, displays photos, plays videos, opens documents in an external app, exports and deletes files, and supports encrypted backups and recovery.

It is not a cloud synchronization service. An SD card is not a substitute for an independent backup.

## 3. Installation and first-time setup

Before starting, decide whether to use internal storage or a removable SD card and prepare a secure place to keep your recovery code.

1. Open KluisAPP and choose Use internal storage or Select SD card folder. For an SD card, choose a suitable empty folder in the Android system picker.
2. Select Password (at least 10 characters) or PIN (at least 8 digits). Enter it twice and continue. A password must contain at least four different characters; trivial PIN patterns are rejected.
3. The 32-character recovery code appears once. Write it down accurately and store it outside the device. Confirm that you have saved it.
4. Re-enter the complete recovery code for verification and create the vault.

The recovery code is based on 160 random bits and cannot be displayed or changed later in version 0.3.1.

To restore an existing vault instead of creating one, use Restore from backup on the setup screen; do not overwrite an existing vault.

## 4. Unlocking and locking

1. Open KluisAPP and check the Active storage location.
2. Enter your password or PIN and tap Unlock.
3. If necessary, select Recover with recovery code and enter the complete code to unlock through recovery mode.

Use the lock icon in the vault overview to lock manually. Turning off the screen locks immediately; leaving the app triggers the configured auto-lock delay.

Repeated incorrect attempts result in progressively longer delays, up to five minutes. A delay does not mean the files have been deleted.

## 5. Adding and moving files

Inside KluisAPP: unlock the vault, tap Move to vault, select one or more files in the Android file picker and wait for import, encryption and verification.

When asked to finish moving, choose Delete original or Keep original.

From Gallery or My Files: select files, use Android Share, choose KluisAPP and confirm the transfer.

The app encrypts imported data and checks size and SHA-256. Android may require separate confirmation to delete originals or may refuse deletion.

If the app reports Copied; original could not be deleted, a readable source copy may remain outside the vault. Verify this yourself before considering the transfer complete.

## 6. Viewing photos, videos and documents

The vault overview displays file counts and tiles with Export and Delete actions.

Tap a photo to view it full-screen; the viewer also offers close, export and delete.

When opening a video, choose Play in KluisAPP or Choose another video player. The internal player offers play/pause, ten-second skip and full-screen mode; controls hide after a short delay.

An external player requires confirmation and receives temporary read access to a decrypted temporary copy. Only use external apps you trust.

Documents open through an external compatible application after confirmation. This may expose the document outside the direct control of KluisAPP.

## 7. Exporting and deleting

To export: tap Export on the relevant item, choose destination and filename in the Android picker and wait for Export completed.

Then decide whether to Keep in vault (the safer default) or Remove from vault. Cancelled or failed exports leave the vault item intact.

**WARNING: Exported files are readable at the destination and are no longer protected by vault encryption.**

To delete: tap Delete, read the confirmation and choose Permanently delete only when certain. This removes the vault item, not arbitrary files elsewhere on the device.

## 8. Settings and access credentials

Open Settings from the vault overview.

Auto-lock options: immediately when leaving, 15 seconds, 30 seconds, 1 minute, 5 minutes or 15 minutes. Screen-off locking is immediate.

Storage options: use internal storage or select an SD-card folder; migration to SD is available when using internal storage.

Other settings include Create full backup, Restore from backup, Change password or PIN, and preferred video player (internal, external or ask each time).

Credential management may include Set PIN, Change password and Remove PIN, depending on the current configuration.

Keep the recovery code separately from your password or PIN. A backup without valid access credentials may be impossible to decrypt.

## **9. Creating a complete encrypted backup**

1. Unlock the vault and open Settings.
2. Select Create full backup.
3. Choose a safe destination and a recognizable ZIP filename in the Android file picker.
4. Wait for the success message and check that the ZIP file exists.
5. Copy the backup to another device or external drive.

The encrypted ZIP contains kluisapp-backup.properties, kluis.props, index.enc and encrypted files in data/. It is not a ZIP of readable photos.

Check file size and, where possible, ZIP integrity and SHA-256 after copying. ZIP integrity alone does not prove that recovery and decryption will succeed.

A backup stored only on the same tablet does not protect against loss, theft or device failure.

## **10. Restoring from a backup**

Restoration requires an appropriate empty destination; KluisAPP refuses to overwrite an existing vault.

1. Make sure you have the backup and the correct password or recovery code.
2. Select an empty suitable storage location, never your active vault.
3. Select Restore from backup on the setup screen or in Settings, as appropriate.
4. Choose the ZIP file and allow validation and restoration to complete.
5. Unlock the restored vault and verify the expected files are present and readable.

Test recovery only on a separate empty destination. Do not risk your only working vault.

## **11. Internal storage and SD card**

Internal storage uses the app-private filesDir/kluis folder. Do not edit its contents manually.

For SD storage, Android's folder picker grants access; KluisAPP verifies the removable volume identity and vault identity. If the card or folder is unavailable or different, stop and check the correct media.

To migrate: open Settings while the internal vault is active, select Migrate to SD card, choose a suitable folder, provide the credential if requested, and allow the app to copy and verify the encrypted files.

After migration, verify the SD vault is active and readable. The internal vault remains according to the documented implementation; do not delete it before checking backups and the active storage location.

Never select or erase an unfamiliar folder merely because its name looks right.

## 12. Security and privacy

Password-based key derivation: Argon2id with 64 MiB memory, 3 iterations and parallelism 4.

Master-key protection: AES-256-GCM. Encrypted files and index: streaming authenticated encryption with AES-256-GCM/HKDF-SHA256.

Recovery code: 160 random bits displayed as 32 characters. Incorrect unlock attempts cause delays up to five minutes.

FLAG\_SECURE blocks ordinary screenshots; Android automatic app backup is disabled and the app requests no network permission.

File metadata, including names, types, sizes and hashes, is held in the encrypted index. External viewing may use temporary decrypted files.

No Android Keystore binding is used for the portable vault key, allowing transfer with the right credentials but making their secure storage essential.

## 13. Troubleshooting

Wrong password or PIN: check keyboard input and avoid repeated guessing.

Invalid recovery code: compare all 32 characters with your original record.

Too many failed attempts: wait until the enforced delay expires.

SD card or selected folder unavailable: check the correct card, folder permissions and accessibility.

Folder belongs to a different vault: stop and verify vault identity; do not choose random folders.

Selected folder not empty: choose another empty folder; do not delete unknown contents.

Insufficient SD-card space: free space outside the vault without removing unknown encrypted files.

Copied but original not deleted: check Gallery or My Files for the readable source.

Export failed: check destination, permissions and free space; the vault original is retained.

A vault already exists at this location: restore to an empty destination only.

No external video player found: use the internal player or install a trusted compatible player.

## 14. Frequently asked questions

Can I display my recovery code later? No, version 0.3.1 displays it once during setup.

Can I use a PIN? Yes, at least eight digits, subject to security rules.

Does importing always delete the original? No. You choose, and Android may refuse deletion.

Can I play a video outside KluisAPP? Yes, after a warning; a temporary decrypted copy is shared with the player.

Are exported files encrypted? No, exported copies are readable.

Can a backup overwrite an existing vault? No, the documented restore flow refuses that.

Do I need internet? The app has no network permission and the described local functions work offline.

Can I move an SD-card vault to another device? The design supports portability, but verify compatibility, storage selection and credentials; back up first.

## 15. Glossary

Vault: encrypted storage containing files and an index.

Recovery code: one-time displayed code for recovering access to the vault key.

Backup: ZIP containing the necessary encrypted vault artifacts.

Export: save a readable copy outside the vault.

Migration: verified transfer to a different storage location.

SAF: Android Storage Access Framework, including system file and folder pickers.

SHA-256: checksum for byte-for-byte comparison.

Argon2id: password-based key derivation algorithm.

AES-256-GCM: authenticated encryption algorithm.

Vault ID: unique identifier of a vault.

## 16. Safe-use checklist

Store the recovery code and password or PIN safely and separately.

After import, verify that files can be opened inside the vault.

After moving, verify that any readable original outside the vault has actually been deleted.

Create encrypted full backups regularly and keep at least one current copy outside the Android device.

Verify copied backups with SHA-256 when possible.

Test recovery only on a separate empty destination.

Never delete unfamiliar vault folders, index files or old backups without checking.

Use only trusted external video players and document apps.

© 2026 Jeffrey Haimé — Jeffrey-Apps