HOW-TO

The encrypted Vault & recovery key

Applies to: Shield Vault only

Shield Vault's built-in SSD is encrypted, so your files stay private even if the drive is removed from the device. This is where you set the passphrase, save your recovery key, and lock or unlock the Vault.

Before you put any data on the Vault

> **CAUTION:** Encryption can **only be enabled at Format time**. If you start using the Vault before turning encryption on, you'll need to **back up your data, format with encryption enabled, then restore it**. Enable **Enable Encryption on Format** on a fresh Vault **before** you move any files onto it.

Passphrase & auto-unlock

Set a Vault **passphrase** that protects the encrypted storage. **Auto Unlock on Reboot** lets the Vault unlock itself when the device restarts; turn it off if you'd rather enter the passphrase each time. **Enable Encryption on Format** is the switch that turns encryption on the next time the disk is formatted — see the caution above.

Your recovery key

The recovery key can unlock the Vault if the passphrase or auto-unlock ever becomes unavailable. Use **Reveal Recovery Key**, then **Copy Key**, store it somewhere safe, and confirm with **I Have Saved This Key**.

Save the recovery key somewhere safe and separate from the device. Without the passphrase or recovery key, encrypted data cannot be unlocked — by anyone, including us.

Locking & unlocking

- **Unlock Storage** with the passphrase makes your files available.
- **Lock Storage** secures them again — useful before travelling or lending the device.

Tips & troubleshooting

- Store the recovery key offline — a password manager, or a printed copy in a safe place.
- This is genuine encryption with no backdoor, so the recovery key is your only fallback if you forget the passphrase.

Need a hand? As a founding member you have a direct line to the people building Shield — email hello@wombatss.com.