



MountGuard

User Guide

One button. Total silence.

Korerium LLC

www.korerium.com

Table of Contents

This guide covers everything MountGuard does and how to get the most out of it. Use the sections below to find what you need.

What is MountGuard	2
How MountGuard Works	2
System Requirements	3
Getting Started	4
The MountGuard Popover	4
Guard Tab	4
Timer Tab	5
Log Tab	6
Notifications	7
Settings	7
License Activation	8
Privacy Statement	9

What is MountGuard

MountGuard is a native macOS security tool that blocks removable storage devices from mounting on your Mac. When protection is enabled, USB drives, external SSDs, SD cards, and Thunderbolt storage are prevented from connecting. The moment you step away from your desk, MountGuard closes the physical access gap that network security software cannot see.

MountGuard lives in your menu bar. It has no dock icon, no main window, and no cloud dependency. It is a one-time purchase with no subscription.

Who is MountGuard for?

- Security-conscious professionals who work in shared spaces, open offices, or travel frequently.
- Anyone who steps away from their Mac and wants physical storage access closed while they are gone.
- Organizations that need a lightweight policy enforcement tool to prevent unauthorized data transfer.
- Privacy-focused users who want full control over what can connect to their Mac at the hardware level.

How MountGuard Works

MountGuard uses Apple's DiskArbitration framework to intercept mount approval requests at the system level. When a removable storage device attempts to connect, DiskArbitration asks MountGuard for permission. If protection is enabled, MountGuard denies the request before the drive mounts.

Two-Layer Defense

macOS may display an Accessory Security prompt asking whether to allow a device to connect. This prompt is a hardware-level gate controlled by macOS, not MountGuard. If a drive passes that prompt, MountGuard's second layer activates: it detects the successful mount and immediately force-ejects the device. In both cases the drive does not remain connected. When the Accessory Security prompt appears and protection is enabled,

clicking Don't Allow is the recommended action. MountGuard will catch and eject any drive that gets through regardless.

What MountGuard Blocks

- USB drives and flash storage
- External HDDs and SSDs
- SD cards and card readers
- Thunderbolt storage devices

What MountGuard Does Not Block

- Keyboards and mice
- Audio interfaces and webcams
- Thunderbolt displays and docks (display function only)
- iPhone and iPad connections
- USB charging cables with no storage capability

System Requirements

Requirement	Minimum
macOS	macOS 26 or later
Architecture	Apple Silicon (M1 or later)
Storage	15 MB for the application
Memory	50 MB or less during normal use
Internet	Not required for use

Getting Started

On first launch MountGuard places a shield icon in your menu bar. There is no dock icon and no main window. Click the menu bar icon at any time to open the MountGuard popover. A Welcome screen walks you through the key concepts on first launch.

License Activation

MountGuard includes a five-use trial so you can verify it works before activating. A trial use counter appears in the popover while in trial mode. To activate, open Settings from the popover footer, scroll to the License Information section, enter your name, email address, and license key, then click Activate License.

First Run Checklist

- Click the MountGuard icon in the menu bar to open the popover.
- Review the Guard tab and toggle Block Storage to enable protection.
- Enable Launch at Login in Settings so protection is active after every restart.
- Enable notifications in System Settings so you are alerted when a drive is blocked.
- Open Settings to configure a PIN and activate your license.

The MountGuard Popover

The popover is MountGuard's entire interface. Click the menu bar icon to open it. It is organized into three tabs -- Guard, Timer, and Log -- with a status footer and a gear icon to access Settings. The popover color language is consistent throughout. Blue indicates protection is active. Amber indicates storage is currently allowed.

Guard Tab

The Guard tab is the primary control surface. It contains the storage toggle, a status card showing the current protection state, and a threat summary card explaining what MountGuard prevents.

Storage Toggle

The Block Storage toggle enables or disables removable storage blocking. When enabled, the toggle and status card turn blue and the menu bar icon updates to reflect the protected state. When disabled, both turn amber.

Status Card

The status card shows the current protection state at a glance using a lock icon and a bold state label. Blue with a closed lock means storage is blocked. Amber with an open lock means storage is allowed.

Block Storage Now Button

The full-width button at the bottom of the Guard tab toggles protection on or off. Its label and color update to reflect the current state.

Timer Tab

The Timer tab lets you schedule automatic re-enabling of storage after a set period. This is useful when you need to allow a device temporarily and want protection to restore automatically without remembering to re-enable it.

Timer Presets

- 5 minutes
- 10 minutes
- 15 minutes
- 30 minutes
- 1 hour
- 2 hours
- Custom -- enter any duration in the input field.

How the Timer Works

Select a preset or enter a custom duration, then start the timer. The active countdown appears in the popover footer and continues running while the popover is closed. When the timer expires, storage blocking re-enables automatically and the state is logged. If a drive is already connected when the timer expires and storage re-enables, MountGuard will not eject it automatically. Only new mount attempts after re-enabling are blocked.

Log Tab

The Log tab shows a timestamped session history of every MountGuard event. Each entry includes the time and a plain English description of what occurred.

Log Entry Types

Entry	Meaning
Mount attempt blocked: [name]	DiskArbitration denied the mount request.
Mount detected and ejected: [name]	Drive passed the macOS prompt and was force-ejected.
Removable storage blocked	Protection was enabled by the user.
Removable storage allowed	Protection was disabled by the user.

Export and Clear

Tap Export Log to save the current session log as a plain text file. Tap Clear to erase all entries. The log holds a maximum of 100 entries. Older entries are removed automatically when the limit is reached.

Notifications

MountGuard sends a system notification whenever a removable drive is detected and ejected. The notification appears in the top right corner of your screen and is stored in Notification Center.

Enabling Notifications

On first launch MountGuard requests permission to send notifications. If you missed that prompt or notifications are not appearing, enable them manually:

- Open System Settings on your Mac.
- Click Notifications in the sidebar.
- Scroll down and click MountGuard in the app list.
- Toggle Allow Notifications on.

Notifications are optional. MountGuard blocks and ejects drives regardless of whether notifications are enabled. The popover banner and session log always record eject events.

Settings

Open Settings by clicking the gear icon in the popover footer. Settings replace the popover content in place. Click the gear icon again to return to the popover.

General

- Launch at Login: Start MountGuard automatically when you log in to your Mac.
Recommended for continuous protection.

PIN Protection

PIN Protection requires a numeric PIN to disable storage blocking or quit MountGuard. This prevents someone with brief physical access from simply turning off protection.

- Set PIN: Choose a numeric PIN. The PIN is stored as a salted PBKDF2 hash, never as plain text.
- Change PIN: Replace the current PIN with a new one.

- Disable PIN: Remove PIN requirement. Requires entering the current PIN to confirm.

License Information

The License Information section shows your current activation status. If activated, it shows your name, email, and a confirmation message. If in trial mode, it shows how many trial uses remain and provides fields to enter your license key.

About

The About section shows the current MountGuard version and build number, with links to korerium.com and support.

Danger

Reset All Settings clears your license activation, PIN, and all preferences. This cannot be undone. You can also reset preferences manually by running the following command in Terminal:

```
defaults delete com.korerium.MountGuard
```

License Activation

MountGuard includes a five-use trial. After five uses you will need to activate a license to continue using the app.

How to Activate

- Click the MountGuard menu bar icon to open the popover.
- Click the gear icon in the footer to open Settings.
- Scroll to the License Information section.
- Enter your first and last name.
- Enter the email address you used to purchase MountGuard.
- Enter your license key exactly as it was delivered -- including the dashes.
- Click Activate License.

Activation is verified entirely offline using a cryptographic key derived from your email address. No internet connection is required.

License Key Format

License keys are 35 characters in the format:

XXXXXXXX-XXXXXXXX-XXXXXXXX-XXXXXXXX

Support

If you have trouble activating, contact support@korerium.com with your order confirmation and the email address used to purchase.

Privacy Statement

MountGuard is a local-first application. It does not collect, transmit, or store any data about you, your devices, or your usage.

What MountGuard Does Not Do

- Does not connect to the internet for any purpose during normal operation.
- Does not send usage analytics or telemetry.
- Does not log device identifiers, serial numbers, or hardware details.
- Does not require an account, email address, or login for normal use.
- Does not retain any session log between launches.

What MountGuard Stores Locally

MountGuard stores your preferences -- protection state, PIN hash, launch at login setting, and license activation -- in your Mac's standard preferences system (NSUserDefaults). This data never leaves your Mac. You can reset it at any time in Settings under Danger, or by running the Terminal command above.

License Verification

License key validation is performed entirely offline using HMAC-SHA256 cryptography. Your email address and license key are never transmitted to Korarium or any third party. Validation happens on your Mac using a locally computed cryptographic signature.

Contact

Questions about MountGuard's privacy practices can be directed to support@korarium.com