

How to manage settings in Trojan Scanner for Android

Gridinsoft Help Center

Trojan Scanner's Settings let you control scans, updates, storage, and alerts. Most defaults are safe, but a few tweaks can save data or battery, or make protection more proactive.

Open Settings

- Open Trojan Scanner.
- Tap the menu (three lines) in the top-left.
- Tap Settings.

All settings explained

1) Scan after reboot

What it does: Runs a fast check when your phone restarts, catching threats that try to load early. Good for: Extra safety after OS updates or app installs. Impact: Adds a few seconds after boot; minimal battery use. Recommendation: On for most phones. Turn off only on very low-end devices or if boot speed is critical.

2) Update threats list

What it does: Keeps detection rules current so the app recognizes the latest malware. Modes:

- Download automatically - updates in the background when available.
- On request - you update manually from the app.

When to choose manual: If you're often offline or want strict control of data use.
Recommendation: Automatic for best protection.

3) Download threats list (network rule)

What it does: Tells Trojan Scanner when it's allowed to fetch updates. Options:

- Wi-Fi only - uses no mobile data.
- Always - Wi-Fi or mobile data.

Who should use Wi-Fi only: Users on limited data plans. Recommendation: Wi-Fi only if data is tight; Always if you want updates anywhere.

4) Scan Type

What it does: Chooses depth/speed of checks. Options (typical):

- Quick - fast scan of common risk areas; best for daily use.

- Deep - thorough scan of storage and apps; use weekly or when something feels off.

5) Quarantine - Remove files after

What it does: Auto-cleans old quarantined items so they don't take space. Choices: e.g., 1 week, 2 weeks, 1 month. How it works: Items remain isolated (can't run) until the timer deletes them. Recommendation: 2 weeks is a good balance; extend if you often review items.

6) Keep Reports

What it does: How long to keep scan reports (history + logs). Why it matters: Helpful for troubleshooting patterns or sharing with Support. Recommendation: 1-3 months. Shorten to save space; extend if Support asks.

7) Sounds

What it does: Plays sound cues for detections and scan completion. Tip: If you silence sounds, ensure Android notifications remain on so you still see alerts. Recommendation: On unless you prefer silent mode.

8) Language

What it does: Changes the app interface language. Note: Scans and protection work the same in any language.

Examples: choose a setup that fits you

Battery saver (older phone):

- Scan after reboot: Off
- Scan type: Quick (run Deep weekly)
- Updates: Automatic + Wi-Fi only
- Quarantine cleanup: 2 weeks
- Keep reports: 1 month
- Sounds: Off

Travel / limited data:

- Updates: On request + Wi-Fi only
- Run Deep before you travel; Quick on the road

Paranoid mode (high-risk user):

- Scan after reboot: On
- Scan type: Deep (weekly)

- Updates: Automatic + Always
- Quarantine cleanup: 1 month
- Keep reports: 3 months

Tips & quick fixes

- An option is greyed out or updates fail: Check internet, free storage, and time/date accuracy.
- No detections but the phone acts weird: Update threats list -> run a Deep scan -> review recent installs.
- Can't update on mobile data: Ensure Download threats list -> Always is selected and system Data Saver isn't blocking Play Services.
- Storage tight: Shorten Keep Reports and Quarantine retention; remove large downloads/media.
- Permissions changed by mistake: Android Settings -> Apps -> Trojan Scanner -> Permissions -> allow Files & media.

Privacy note

- Usage data (like last launch time in Apps Usage Statistics) is read locally to generate lists; personal files and browsing content are not collected.

Restore defaults (manual)

If you want to revert quickly:

- Scan after reboot: On
- Update threats list: Automatic
- Download threats list: Wi-Fi only
- Scan type: Quick
- Quarantine: 2 weeks
- Keep reports: 1 month
- Sounds: On
- Language: your preference