Installation

Post-Installation Configuration

Complete the essential Gridinsoft Anti-Malware setup after installation: activate, update, scan, enable protection, schedule checks, and review support tools.

PUBLISHER
Gridinsoft Support

UPDATED
Jul 10, 2026

READ TIME
2 min

CONTENTS

In this guide

01 1. Confirm the installation and version
02 2. Activate the license or trial
03 3. Update the Threat List
04 4. Run an initial scan
05 5. Review real-time protection
06 6. Create a scan schedule
07 7. Check quarantine, exclusions, and logs

After installing Gridinsoft Anti-Malware, complete these checks before relying on it for regular protection. They confirm that the license, Threat List, scan settings, and background modules are working.

01 1. Confirm the installation and version

1. Open the app from the Start menu or desktop shortcut.
2. Select **Info** and confirm that the application reports the current version and an active status.
3. If Windows displays an administrator prompt, approve it only for the signed Gridinsoft application.

02 2. Activate the license or trial

On the **Info** page, choose the option for an existing license and enter the activation key exactly as issued. Activation needs an internet connection. See How to Activate Gridinsoft Anti-Malware for error-specific help.

03 3. Update the Threat List

1. Select **Update**.
2. Check for updates and wait for the completion message.
3. Confirm that the status bar says the Threat List is up to date.

Do not start the initial scan with stale threat data. If the update fails, follow Threat database updates fail.

04 4. Run an initial scan

Run a **Standard** scan for a balanced first check. Use a **Full** scan if the PC has symptoms of infection or was recently cleaned. Review detections before applying permanent actions. The complete scan guide explains every scan type and result action.

05 5. Review real-time protection

Open **Protect** and review the modules available for the licensed system:

- **Internet Security** checks web destinations and dangerous downloads.
- **Suspicious Activity Shield**, formerly On-Run Protection, monitors suspicious application behavior.
- **USB Device Control** monitors connected removable storage.

Keep the layers you need enabled unless Support asks you to turn one off temporarily. See Gridinsoft Anti-Malware Protection Features.

06 6. Create a scan schedule

Open **Settings → Scheduled scan**. A weekly Standard scan is a practical baseline; use Full scans when deeper verification is needed. Ensure the PC will be powered on and awake at the selected time.

07 7. Check quarantine, exclusions, and logs

- Use quarantine when you are uncertain about a detected file.
- Keep the Ignore list limited to objects you have independently verified as safe.
- Open **Tools** to find scan, protection, and application logs.

If a problem remains after setup, contact Support with the app version, license status, error message, and relevant log.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com