GRIDINSOFT
HELP CENTER

OFFICIAL SUPPORT GUIDE

Installation

Additional Configuration Options

Review useful optional settings for startup, scheduled scans, updates, Windows integration, reports, and carefully limited exclusions.

PUBLISHER	UPDATED	READ TIME
Gridinsoft Support	Jul 10, 2026	2 min

CONTENTS

In this guide

01 Startup and scheduled scans

02 Windows integration and updates

03 Reports, quarantine, and exclusions

Gridinsoft Anti-Malware works with its default settings, but a few optional changes can make routine checks more convenient. Change only settings that solve a specific need, and keep protection and updates enabled.

01 Startup and scheduled scans

Open **Settings** to choose whether the app starts with Windows. Use **Scheduled scan** to create a recurring or one-time scan, select the scan type, and set the start time. Enable the option to check for updates before a scheduled scan. The computer must be powered on and awake when the task is due.

02 Windows integration and updates

If available in your installation, enable the Windows context-menu option to scan a selected file or folder from File Explorer. Keep Threat List updates automatic. Configure a proxy only when your network requires one; an incorrect proxy can prevent activation and updates.

03 Reports, quarantine, and exclusions

Review stored scan, protection, and application logs under **Tools**. Quarantine is safer than immediate deletion when you are unsure about a detection. Add an exclusion only after verifying the object and prefer one exact file, folder, or URL over a broad location. Broad exclusions can hide future threats.

After changing protection settings, confirm that the main status remains **Active** and the Threat List is current.

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