GRIDINSOFT
HELP CENTER

OFFICIAL SUPPORT GUIDE

Detections, Quarantine, False Positives

The app detected something — should I delete it?

Choose Quarantine when uncertain, delete confirmed malware after review, and preserve evidence when a detection may be a false positive.

PUBLISHER	UPDATED	READ TIME
Gridinsoft Support	Jul 10, 2026	1 min

CONTENTS

In this guide

01 When to quarantine

02 When deletion is appropriate

03 If the file might be legitimate

Do not choose an action based only on the filename. When you are uncertain, **Quarantine** is the safest first step: it blocks the item from running while keeping it available for review.

01 When to quarantine

- The file is unfamiliar, unsigned, or located in an unusual temporary or startup folder.
- The path looks important to Windows or to a work application.
- You may need to report a false positive or preserve evidence for Support.

02 When deletion is appropriate

Delete or permanently remove an item when it is confirmed malware, no investigation is needed, and the system works normally after isolation and restart. Some active threats are removed during a reboot. Run a follow-up scan afterward to confirm that related files and persistence entries are gone.

03 If the file might be legitimate

1. Leave it quarantined.
2. Record the detection name, original path, publisher, and scan time.
3. Use the in-app false-positive option or send a Support request.

Do not restore and permanently ignore an item merely to stop an alert. If Support confirms it is safe, update the Threat List before restoring it and create only the narrowest necessary exception.

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