GRIDINSOFT
HELP CENTER

OFFICIAL SUPPORT GUIDE

Detections, Quarantine, False Positives

I think this is a false positive. What should I do?

Send file and app false positives to Gridinsoft Support, but submit website and domain reputation cases only through Gridinsoft Portal.

PUBLISHER	UPDATED	READ TIME
Gridinsoft Support	Jul 17, 2026	3 min

CONTENTS

In this guide

01 Keep the item safe while it is reviewed

02 For a file or app detection: use Gridinsoft Support

03 For a website or domain: use Gridinsoft Portal

04 Information that helps the review

05 Act only after the review

A false positive is a safe file, app, website, or domain classified as dangerous. Treat an unexpected detection as potentially real until its origin and behavior have been verified. The correct review channel depends on what was detected.

> **Choose the correct route:** send a file or app detection to Gridinsoft Support. For a website, URL, or domain reputation case, do not open a Support ticket; use the Gridinsoft Portal false-positive form.

01 Keep the item safe while it is reviewed

1. Choose **Quarantine** when possible. This prevents the item from running without permanently deleting it.
2. Do not upload confidential files to public multi-scanner services.
3. Do not add the file, folder, or entire disk to the Ignore list merely to make an alert disappear.

02 For a file or app detection: use Gridinsoft Support

- On the Scan Result screen, use **Let us know** and follow the prompts to send the relevant diagnostic information.
- From elsewhere in the app, select **Get help**, choose the false-positive topic, and describe the detection.
- If the in-app submission does not work, open a Support request and include the file name, detection name, and relevant logs.

03 For a website or domain: use Gridinsoft Portal

Website reputation, blocked URL, and domain classification cases are reviewed through Gridinsoft Portal, not through the Support ticket system. Open the website and domain false-positive form and submit the complete affected URL or domain there.

Remove passwords, access tokens, session identifiers, and private query data before submitting a URL. Include the current classification, the reason you believe it is incorrect, and any evidence that the site has been cleaned or secured.

04 Information that helps the review

- For a file or app: detection name, exact file path, publisher, version, and source.
- For a website or domain: the complete sanitized URL, current classification, and remediation details.
- Gridinsoft app version, Threat List status, and scan time.
- A scan or protection log and a screenshot of the result.

05 Act only after the review

For a file or app, if Support confirms the detection is incorrect, update the Threat List before restoring the quarantined item. Add the narrowest possible exclusion only if it is still required. If the file is unsigned, unexpectedly changed, or obtained from an unofficial source, replace it with a fresh copy from the publisher instead.

For a website or domain, follow the result of the Portal review. Do not create a Support ticket for the same reputation case.

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