GRIDINSOFT
HELP CENTER

OFFICIAL SUPPORT GUIDE

How-To Guides

On-Run Protection: Real-Time Threat Detection

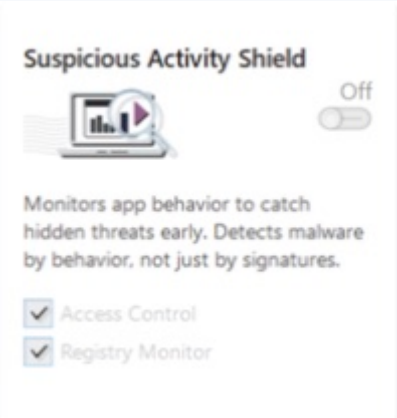
Learn how Suspicious Activity Shield, formerly On-Run Protection, monitors program behavior, records detections, and helps you respond safely.

PUBLISHER	UPDATED	READ TIME
Gridinsoft Support	Jul 10, 2026	3 min

CONTENTS

In this guide

On-Run Protection is the name used in older Gridinsoft documentation. In the current interface, the corresponding real-time module is named **Suspicious Activity Shield**. It monitors app behavior to identify hidden threats, including activity that may not yet match a known signature.



Suspicious Activity Shield module in Gridinsoft Anti-Malware

01 What Suspicious Activity Shield monitors

- Application behavior that resembles malware activity.
- Attempts by programs to make suspicious system changes.
- Access-control and registry activity covered by the module's monitors.
- Behavioral signals that complement the current Threat List.

The module complements scheduled and on-demand scans. It does not replace regular scans or Threat List updates.

02 Turn the protection on or off

1. Open Gridinsoft Anti-Malware.
2. Select **Protection** in the app navigation.
3. Find **Suspicious Activity Shield** and use its switch to turn it on.
4. Confirm that the protection status is active. If Windows asks for administrator approval, allow the change only when the app is the genuine Gridinsoft installation.

Keep this layer enabled unless Gridinsoft Support asks you to disable it temporarily for troubleshooting. If it will not stay enabled, update the app, restart Windows, and check whether another security product is blocking the protection service.

03 What happens when a threat is detected

When the module detects suspicious behavior, Gridinsoft Anti-Malware records the event and may show an in-app or Windows notification. Open the alert or Protection logs to review the affected object and available actions. The exact action labels depend on the detection.

- **Quarantine or Block:** the safest choice when you do not recognize the file. It prevents the item from running while preserving the option to review it.
- **Remove:** deletes or schedules removal of the detected item. Use it when you are confident the file is malicious.
- **Allow once:** permits only the current launch. Do not use it merely to dismiss an alert.
- **Ignore or Always allow:** creates a lasting exception. Use it only for a file you have independently verified as safe.

04 If you think the detection is a false positive

1. Keep the file blocked or quarantined.
2. Do not add a permanent exception yet.
3. Record the detection name and file path.
4. Submit a support request and attach the requested diagnostic information. Do not send confidential files unless Support specifically asks for them.

05 Review protection activity

Open **Tools** and select **Protection logs**, or use **View log** on the Protection page. Review the date, relevant protection log, app version, object, detection, and action. For a full guide to log types and sharing diagnostics, see Gridinsoft Anti-Malware Log Files.

06 Safe operating recommendations

- Keep threat databases and the application current.

- Prefer quarantine when you are uncertain.
- Review permanent exceptions periodically.
- Run a full scan after a confirmed real-time detection, especially if related files may already be present.

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