

Trojan Scanner

Sign in for free cloud checks of apps and files

Add optional free cloud file and app-domain checks with a Gridinsoft account, and understand the information sent with your consent.

PUBLISHER

Gridinsoft Support

UPDATED

Oct 15, 2026

READ TIME

3 min

CONTENTS

In this guide

01 Connect your account**02** Enable Cloud file check**03** Enable analysis of app domains**04** Stay in control

A Gridinsoft account adds optional cloud checks to Trojan Scanner Free and Pro. File checks can compare fingerprints with the cloud threat database, while app analysis can review domains embedded in APKs. These features offer more information for your decision without uploading the files themselves. Local scanning remains available without signing in.

01 Connect your account

1. Open the menu and tap **Sign in**.
2. On the Gridinsoft account screen, tap **Sign in or create account**. Read the connection information and choose **Continue sign-in**.
3. Complete the sign-in in your browser and approve linking this installation.
4. Return to Trojan Scanner and confirm that the account is connected.

Connecting gives the app your name and email and registers this installation with its device name. Scan history and scan results are not synchronized to your member account. No Pro subscription is required for the cloud checks described here.

 Gridinsoft account

Gridinsoft account

Sign in to link your device and unlock free cloud analysis of apps. On-device scanning works without an account.

Not signed in

You can continue using the scanner without signing in.

[SIGN IN OR CREATE ACCOUNT](#)

[PRIVACY POLICY](#)

[DELETE ACCOUNT OR DATA](#)

Sign-in is optional. Local scanning remains available without an account.

02 Enable Cloud file check

1. Open **Menu** → **Settings** → **Detection management**.
2. Turn on **Cloud file check**.
3. Read and accept the consent prompt if you want the feature enabled.
4. Run a manual scan or use [Check a file](#). Review the cloud status alongside the local result.

With your consent, Scanner sends file fingerprints and sizes to compare against the cloud database. A fingerprint can identify a file; the file, its name and its path are not uploaded. If the cloud check cannot finish, the local result is preserved. Check your connection/account and retry rather than interpreting an unavailable layer as clean.

03 Enable analysis of app domains

In **Settings** → **Detection management**, enable **Advanced app analysis** and review its separate consent prompt. With automatic app checks enabled, Scanner can check domains found in new or updated non-system apps. It can also include this analysis in Pro scheduled installed-app checks.

For a selected APK, use **Check APK domains** when the file result offers it. Only the domains found inside the APK are sent; the APK file and app name stay on the device. A domain found as text is a risk signal, not proof that the app contacted it. Hidden or generated links may not be found.

Advanced app-domain analysis is separate from the manual Start scan and from the [Pro checker for shared or pasted links](#).

04 Stay in control

Cloud checks need a connected account, internet access and consent. You can turn each option off in Settings. To disconnect the installation, open the Gridinsoft account screen and choose **Sign out and disconnect**; local scanning remains available.

Use the account screen's **Privacy Policy** and **Delete account or data** links for the published data information and deletion flow. For help reading a result, see [scan results and Protection history](#).

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](https://support.gridinsoft.com)