



WEBROOT®

by **opentext**™

**Mobile Security for Android
User Guide**

Copyright

Copyright 2023 Webroot, an OpenText company. All rights reserved.

Mobile Security for Android User Guide

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of *Webroot, an OpenText company*.

Table of Contents

Notices	<i>ii</i>
Mobile Security for Android	<i>iii</i>
Using Secure Browser	<i>v</i>
Enabling Webroot for Chrome	<i>vii</i>
Password management with LastPass	<i>viii</i>
Viewing your Activity Report	<i>x</i>
Managing threats with Mobile Security for Android	<i>xii</i>
Technical Support	<i>xiii</i>

Notices

Mobile Security for Android User Guide revision *Wednesday, November 8, 2023*

Information in this document is for the following product:

- Webroot Mobile Security for Android

One or more patents may cover this product. For more information, please visit

<https://www.opentext.com/patents>.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Webroot.

© 2004-2023 Webroot. All rights reserved.

Mobile Security for Android

Just as Webroot provides protection for Windows and Mac computers, Webroot Mobile Security for Android delivers protection against viruses, spyware, and other online threats. Once installed, Webroot Mobile Security scans your device and mitigates threats. While shopping and banking online, Webroot keeps your identity and data safe by blocking phishing sites, spam sites, malware sites, and other malicious activities.

The Webroot Mobile Security license is transferrable for upgrades or changed devices.

Installing Mobile Security on your Android device

Confirm the system requirements at <https://www.webroot.com/us/en/support/system-requirements>.

An active internet connection is required.

1. From the Google Play store, download and install the Webroot Mobile Security app.
2. Tap the Webroot app icon to launch the app.
3. If you upgraded from a previous version, tap **Log In** and use your existing credentials.
4. For new users, under **Create Account**, enter your product keycode.
 - You can find the keycode in the receipt email for online purchases, or on a card for retail purchases. It will look something like this: **WSAM-ZZZZ-0000-YYYY-1111**
 - If you don't have a keycode, tap **Trial Here** to create an account for a 14-day trial period.
5. Enter your email address or phone number to be used as your username.
6. Create a password, following the strong password guidelines that are displayed.
7. To review how Webroot processes your personal data, tap **Privacy Policy**.
8. Tap **Create Account**. The **Webroot Subscription Terms** screen appears.

9. Tap **Solution Agreement**, read the terms, and tap **AGREE** to continue.
10. On the welcome screen, tap **SCAN NOW**.
11. When prompted, tap **Allow** to grant the permissions necessary for the app to function properly.
12. For Android OS 11 and newer, from the **All files access** screen, turn on the **Allow access to manage all files** switch.

After installation, Webroot immediately runs a first-time scan of the device.

Even though the app scans continuously, you can always trigger a manual scan by tapping **SCAN NOW**.

Once the scan is complete it will show a status:


- **Safe** means that your phone is protected.
- **Attention Needed** means that there is a security risk. You can take action to manage the risk.

Once Webroot determines that the device is safe, the **Webroot Mobile Security Dashboard** displays:

- Tap **SCAN NOW** to run a manual scan.
- **Secure Browser** lets you explore the Web safely using our secure browser.
- Activate **Webroot for Chrome** to monitor threats while using the Google Chrome browser.
- **Password Manager** enables you to create and manage strong passwords using our included third-party software. Password Manager is included with Webroot Internet Security Plus subscriptions and above.
- **Activity Report** displays a 30-day summary of detected, blocked, removed threats and malware.

Using Secure Browser

From the Webroot Mobile Security Dashboard, tap **Secure Browser** to open the Webroot Mobile Secure Browser. This browser has similar functionality to any other web browser, with the added safety and security of Mobile Security for Android.

Tap the **Settings** button  to set Secure Browser options:

- **Forward** opens the last webpage that you browsed before going **Back**.
- **Favorite** saves the currently open webpage to your **Bookmarks**.
- **Download** saves a copy of the currently open webpage you can view offline.
- **Information** provides security information about the currently open webpage and allows you to configure **Site Settings**.
- **Reload** refreshes the current webpage.
- **New Tab** opens a new browser tab.
- **New Private Tab** opens a new private browser tab. Mobile Security for Android does not save your browsing history, cookies, site data or any information entered in web forms on private tabs.
- **Bookmarks** opens a list of favorite sites.
- **Recent tabs** opens a list of all recently closed webpages.
- **History** opens browsing history in the Mobile Security for Android browser. Web history can be cleared on this screen.
- **Downloads** enables access to the files and articles previously downloaded.
- **Share** enables you to share a loaded page with others.

- **Find in page** enables you to search for text on the loaded page.
- **Settings** opens all settings for Mobile Security for Android.
- **Support** provides a link to get help with Mobile Security for Android.
- **Exit Secure Browser** closes the browser and returns you to the Dashboard.

Enabling Webroot for Chrome

By default, Webroot for Chrome is disabled, as indicated by a red “X” icon.

To enable Webroot for Chrome:

1. From the Dashboard screen, tap **Enable Webroot for Chrome**.
2. Turn on the **Google Chrome Security** switch.
3. Open the notification that appears and tap **Yes**.
4. Tap **Open Settings**.
5. From the Accessibility Settings screen that appears, go to **Installed Services > Webroot**.
6. Turn the switch **On**.
7. Tap **Allow**.
8. Continue tapping the **Back** button until you are back on the Dashboard screen.

Password management with LastPass

With LastPass, you can create and save strong passwords in an encrypted vault using the Carbonite/Webroot My Account portal. Once you create your LastPass account and start saving your credentials, you will be able to automatically log in to your favorite websites and auto-fill web forms. This saves you the hassle of manually entering your credentials, personal information, and credit card numbers.

LastPass Password Manager is included with your subscription of Webroot Mobile Security and is available only for Internet Security Plus and above licenses. If your subscription does not include Password Manager, contact Webroot Support or your administrator to upgrade your subscription.

To start using LastPass:

1. From the Webroot Mobile Security Dashboard, tap **Password Manager**.
2. If you are a new user and do not have an account with **My Account**:
 - a. Tap **Get keycode** and **Copy** an available keycode.
 - b. Tap **Go to My Account Portal**. In the browser tab that opens, enter the required information, including the keycode that you copied.
3. If you are an existing **My Account** user, but do not have a LastPass account:
 - a. Tap **Go to My Account Portal**.
 - b. Follow the steps on the **My Account** page to log in.
 - c. On the navigation pane, go to the **Downloads** tab.
 - d. Scroll down to **LastPass Password Manager** and click **Account Setup**.
 - e. Follow the steps to sign up for a LastPass account.

4. If you already have a LastPass account:
 - a. Tap **Open LastPass App**. The app opens in the Google Play store.
 - b. Tap **Install**. When it finishes installing, open the LastPass Password Manager app and log in.

For more information about LastPass, see the [LastPass Reference Guide](#).


Viewing your Activity Report

Activity Report allows you to see how Webroot Mobile Security is protecting your device from malware threats and malicious websites. You can view your device's activity from the last 30 days and resolve any detected threats.

Note that Activity Report is included with your subscription of Webroot Mobile Security and is available only for Internet Security Complete and above licenses. If your subscription does not include Activity Report, contact Webroot Support or your administrator to upgrade your subscription.


From the Webroot Mobile Security Dashboard, tap **Activity Report** to view a summary of malware and website threats that Webroot Mobile Security detected over the last 30 days. For malware threats, this summary includes the total number of apps scanned and number of new threats detected, as well as threats that are resolved, ignored, and under review. For website threats, this summary includes the total number of websites visited and the number of new threats detected, as well as websites that are blocked, dismissed, and under review.

To view malware threats:

1. From the Activity Summary Report page, tap the **VIEW DETAILS** button.
2. To only display active threats, on the **Activity Details** page, turn on the **Show only active threats** switch.
3. Tap the three-dot icon  next to a **Pending** or **In Review** threat from the list and choose one of three possible actions:
 - **Remove** uninstalls the app from your device and prevents the malware from attacking your device.
 - **Request a Review** sends a request to Webroot's threat experts to review and verify the app. Webroot recommends removing the threat in the meantime to keep your device safe.
 - **Ignore** (not recommended) ignores the malware threat and adds that app to your allow list.

If you trust a website that Webroot Mobile Security flagged as a threat, or no longer want to see it listed, you can remove it from your Activity Details list.

To remove a website from your Activity Details list:

1. From the Activity Summary Report page, tap the **VIEW DETAILS** button. The **Website Threats** tab of the **Activity Details** page displays.
2. To only display previously dismissed threats, turn on the **Show only dismissed threats** switch.
3. Tap the **Delete** button  next to a website from the list. Tap **CONFIRM** to remove that website from the Activity Details list. Note that this only removes the website from appearing in your Activity Details list and does not change the threat status of that website.

Managing threats with Mobile Security for Android

When Webroot detects a threat to the security of your device, or finds unhandled malware that needs to be managed, a notification is displayed on the app's home screen. Tap the notification, or tap **Take Action** while on the Dashboard, and respond with one of the following options:

- **Remove** removes the security risk and prevents the malware from attacking your device.
- **Request a Review** sends a request to Webroot's threat researchers to review and verify the site. Webroot recommends removing the threat in the meantime to keep your device safe.
- **Ignore** (not recommended) ignores the high-risk threat the app discovered and adds it to your allow list.

Webroot displays a warning before loading high-risk websites. The warning page provides the following options:

- **Go Back to Safety** redirects you to the last visited page, or a safe blank page to continue browsing. This is the best option for websites that you have not visited before.
- **Request a Review** sends a request to Webroot's threat experts to review and verify the site.
- **Unblock** (not recommended) removes the block and opens the high-risk website. Only unblock sites if you are familiar with them or if you have verified that they are not threatening to your personal information or security.

Technical Support

Webroot offers a variety of support options. You can do any of the following:

- [Is your Webroot subscription through Best Buy? Click here for additional support options.](#)
 - [Submit a help request.](#)
 - [Look for the answer in our online documentation.](#)
 - [Look for the answer in our knowledgebase and FAQs.](#)
 - [Connect to the Webroot Community.](#)
-