Mobile Security for Android v3
Product Guide

Malwarebytes™

2026

Table of Contents

Get Started

System requirements

This article lists minimum system requirements for Malwarebytes Mobile Security version 3 for Android and ChromeOS. These requirements do not factor in other functions your device is responsible for.

System requirements:

- Operating System: Android 9, 10, 11, 12, 13, 14 or ChromeOS with Google Play.

Mobile Security for ChromeOS features and limitations

The Malwarebytes Mobile Security version 3 app is compatible with Android devices and devices running ChromeOS, such as Google Chromebook. However, Malwarebytes is slightly different on Chromebook devices versus Android devices. This article details those differences and lists which ChromeOS devices support Malwarebytes.

Differences between Android and ChromeOS

- Malwarebytes on ChromeOS devices features larger font size and scaling than the Android version.
- Features related to making and receiving phone calls are not supported on current ChromeOS devices.
- Due to restrictions on ChromeOS, Safe Browsing Scanner does not work with the Chrome browser. Download Malwarebytes Browser Guard to stay protected while browsing online.
- Device Pin, Pattern, and Password are not supported on ChromeOS for the Security Audit feature.
- Battery optimization and the ability to add individual applications to the allow list are not supported on ChromeOS.

ChromeOS devices that support Malwarebytes

ChromeOS devices fall into two categories: those that support Google Play and those that do not.

Devices which support Google Play
These devices can download and run Android apps from the Google Play Store. See Google's support article Install Android apps on your Chromebook to learn which ChromeOS devices support Google Play.

Devices which do not support Google Play
These devices cannot download apps from Google Play. ChromeOS devices without Google Play cannot be infected by malicious applications, but they can still be protected against malicious sites by the Malwarebytes Browser Guard extension. See the Browser Guard product page for more information.

Install Mobile Security for Android v3

Malwarebytes for Android version 3 is designed to protect Android devices from viruses and malware, and is available to install from the Google Play Store. To check if your device is compatible with the latest version of Malwarebytes, see "System requirements."

Follow the instructions below to download and install the app.

1. On your Android device, open the Play Store.
2. In the search bar, enter Malwarebytes, then tap Malwarebytes Mobile Security in the list of results.

3. Tap **Install**.
4. Tap **Open** after the installation is complete.
5. Tap **Get started**.
6. The first time the app launches, Malwarebytes requests security permissions on your device. Follow the prompts on your screen to enable the permissions required. For details on Malwarebytes for Android permissions, refer to "Required functions on Android device."
    - **Note:** On Android 13 devices, you will be requested to provide Notification permissions, when reaching the Dashboard screen.
7. In the Premium screen, you're presented with subscription activation and trial options:
    - **Start free trial:** start a trial with a Google Play subscription. The subscription is charged post the 7-day trial period.
    - **Already have a subscription:** you can activate the Premium features using a purchase from the Malwarebytes online Store, or restore a previous Google Play purchase.
    - **SKIP:** Tap this option to use the free version.

Install Mobile Security v3 on ChromeOS

To use Malwarebytes Mobile Security v3 on a ChromeOS device, download and install the latest version from the Google Play Store app. To learn more about how Malwarebytes works on ChromeOS devices, see "Mobile Security features and limitations on ChromeOS."

Notice: Malwarebytes can only be downloaded from the Google Play Store app. It can't be downloaded from the Google Play website.

1. Open the Google Play Store app. Refer to Google's support article Install Android apps on your Chromebook if you do not see the Google Play Store app on your device.
2. Search for Malwarebytes Mobile Security in the search bar.
3. Click **Install**.
4. Once Malwarebytes installation completes, click **Open**.
5. The first time the app launches, Malwarebytes requests system permissions on your device. Follow the prompts on your screen to enable the permissions required.
6. Malwarebytes setup is now complete. If this is your first time installing Malwarebytes on your ChromeOS device, enjoy a free 7-day trial of the Premium features.

To activate a Malwarebytes subscription, refer to "Activate Premium features on Chromebook device."

Activate Premium features on Android

Your Malwarebytes subscription allows you to activate Premium features such as Real-Time Protection, additional Scan modes and automatic updates in Malwarebytes for Android version 3. If you purchased a subscription for multiple devices, find instructions on how to install and activate on different devices here: Install and activate Malwarebytes products.

Activate using your Malwarebytes Account

To use this method, you need to have an active Malwarebytes account. If you haven't set up your My Account login, see Create your Malwarebytes Account.

1. Open the Malwarebytes app on your Android device.
2. In the upper-left corner of your screen, tap the **Menu** icon.
3. Tap **Settings**.
4. Tap **Already have a subscription**.
5. Enter the credentials and tap **Sign In**.

Activate using a license key

To locate your a license key, see Find my Malwarebytes license key.

1. Open the Malwarebytes app from your Android device.
2. In the upper-left corner of your screen, tap the **Menu** icon.
3. Tap **Premium features**.
4. Tap **Already have a subscription** at the bottom of the screen.
5. Tap **I have a license key**.
6. Enter your provided license key.
7. Tap **Activate**.
8. After you have activated your license key, Malwarebytes shows **Your license has been activated** and the Premium features are turned on automatically.

Activate Premium features on ChromeOS

Your Malwarebytes subscription allows you to activate Premium features such as Real-Time Protection, additional Scan modes and automatic updates.

To activate your subscription, install Malwarebytes Mobile Security version 3 on your Chromebook device. For installation instructions, see "Install Mobile Security v3 on Chromebook devices."

Activate using your Malwarebytes Account

To use this method, you need to have an active Malwarebytes account. If you haven't set up your My Account login, see Create your Malwarebytes Account.

1. Open the Malwarebytes app on your Android device.
2. In the upper-left corner of your screen, tap the **Menu** icon.
3. Tap **Settings**.
4. Tap **Already have a subscription**.
5. Enter the credentials and tap **Sign In**.

Activate using a license key

To locate your a license key, see Find my Malwarebytes license key.

1. Open the Malwarebytes app from your Android device.
2. In the upper-left corner of your screen, tap the **Menu** icon.
3. Tap **Premium features**.
4. Tap **Already have a subscription** at the bottom of the screen.
5. Tap **I have a license key**.
6. Enter your provided license key.
7. Tap **Activate**.
8. After you have activated your license key, Malwarebytes shows **Your license has been activated** and the Premium features are turned on automatically.

Edit Settings

Required Permissions in Settings

Malwarebytes for Android version 3 devices offers several protection layers which require user permission to function. Below are descriptions for each different permission and how Malwarebytes uses them.

Device Administrator
This setting gives Malwarebytes full permissions on your device. This allows us to protect you from ransomware, to enable Real-Time Protection features and to safeguard against the possibility of malware uninstalling Malwarebytes. This setting is only available to Premium and Trial users. Note that Malwarebytes for Android is not capable of performing some of the actions listed in the Android confirmation prompt, such as wiping your phone without notice.

Usage Access
This permission provides additional meta-information on Apps installed which may require this information, such as Real-Time protection or Your apps screen.

Accessibility
This permission is required for monitoring all HTTP/HTTPS calls as part of the Safe Browsing feature. When activated, Safe Browsing Service monitors text on screen, paying special attention to web URLs and email links. When it finds a potentially malicious link, it scans the link against known phishing URLs to find a match and block. The user is notified if anything suspicious is found.

Access Storage
Malwarebytes' Real-Time Protection requires Storage access to perform any manual or scheduled scanning operations.

Draw Over Other Apps
Malwarebytes for Android requires this permission to display anti-ransomware recovery steps. In case ransomware manages to block a user's screen the user can still bring up ransomware recovery instructions on top of the screen using this volume button combination: Up, up, down, down, up, down.

Before it will work, start volume control by tapping any of the buttons up or down, followed by the combination.

Draw over other apps is required to overcome block of the screen which could have been made by ransomware.

Background exclusion required
Background exclusion required is a non-critical issue indicating that Malwarebytes is enabled for Battery Optimization in the device's Settings or any 3rd party optimization apps.

If enabled in Battery Optimization, this could cause functionality issues with Malwarebytes such as preventing the Malwarebytes app from running in the background.

To disable Malwarebytes from Battery Optimization in Settings, see Android OS disabling Malwarebytes Safe Browsing Scanner.

Settings - About

The About screen in Malwarebytes for Android and ChromeOS version 3 allows you to learn about the Malwarebytes program, contact Malwarebytes, and other details surrounding the use of this app. To view this screen in the app, tap the Menu icon at the top-left, then tap About.

An explanation of each option on this screen is as follows:

- **App version:** This shows the version of Malwarebytes on your device. This can be tapped and expanded to show more detailed information.
- **Malware database:** This is the collection of threat signatures which keep you safe. It is updated regularly.

- **Phishing database:** This is a database of known phishing methods that you may need protection against. It is updated regularly.
- **Help Center:** Tap this option to open the Malwarebytes Support website in your browser.
- **Send feedback:** Tap this option to let us know what you like or don't like about Malwarebytes. We want to know what you think!
- **License Agreement:** Tap this option to open the Malwarebytes License Agreement in your web browser.
- **Privacy policy:** Tap this option to open the Malwarebytes Privacy Policy in your web browser.
- **Rate the App:** This connect you to the Google Play Store so you can leave a rating for Malwarebytes.

Settings - Other

Malwarebytes for Android and ChromeOS version 3 has many features to customize your protection. The Other settings contains miscellaneous settings primarily related to database updates and user notifications. To view this screen in the Malwarebytes app, tap the Menu icon at the top-left corner, then tap Settings, then Other. This article describes each setting found on this screen.

Memory Caching
This setting is enabled by default, and allows Malwarebytes to use additional system resources to increase performance. Disabling this setting reduces memory usage of the program, but results in longer scan times.

Database Updates
These settings determine how and when your device receives updates. A description of each setting is as follows:

- **Auto updates enabled:** Determines whether your device receives threat protection updates automatically. If this setting is disabled, the setting for Update frequency is also disabled. We recommend keeping this setting enabled to keep your device protected.
- **Auto update over Wi-Fi:** Allows you to specify whether you receive protection updates using Wi-Fi networks only, or using cellular data. Enabling this setting allows you to conserve your cellular data.
- **Update frequency:** The interval between checks for protection updates. You can choose an interval of 1, 3, or 6 hours between checks. This setting is disabled if Auto updates enabled has been turned off.
- **Force update:** This message displays when the database last updated. The date and time of the most recent update check is shown here whether you actually download a database update. If your signature is already current, there is no need to update again. You can tap this item to force Malwarebytes to check for updates.

Security Audit Overview

The Security Audit screen allows you to enhance your privacy and security in Malwarebytes for Android and ChromeOS version 3. In the app, tap the Menu icon, then tap Security Audit to view the different features. All features display as either Secure Settings or Insecure Settings, indicating if any feature's current state poses a security risk. This article details features found on this screen.

Development mode
This feature maps to the Android Developer Options screen, which allows the device to be used as a development platform. This mode disables many security features and allows developers to control these features through code rather than the user interface. Presence of this feature depends on your device's hardware and software.

Device PIN, Pattern, or Password
This feature determines what additional information is needed to unlock your device. Only one option may be selected at a time.

Device encryption
This feature allows you to safeguard your data by enabling encryption on your device.

NFC
This feature maps to the Android Wireless/Networks screen, which allows communication with another device using Near Field Communication (NFC). Presence of this feature depends on your device's hardware and software.

Android Beam
This feature maps to the Android Wireless/Networks screen, which allows a device to transfer information to or from another Android device if Near Field Communication (NFC) is enabled. Presence of this feature depends on your device's hardware and software.

Google Play Protect
Android 8 (Oreo) introduced this optional feature to test apps and assure they are not malicious. We recommend enabling this feature for additional protection.

Check your Real-Time Protection Status

Real-Time Protection is a Premium feature available in Malwarebytes for Android and ChromeOS version 3. Depending on your operating system, Real-Time Protection can block malware, exploits, or malicious websites. To confirm Real-Time Protection is on or off, open the Malwarebytes application on your Android or Chromebook device and view your Dashboard or refer to the instructions below.

How to check Real-Time Protection status

When activated, Malwarebytes Premium on Android or Chromebook automatically enables malware protection.

1. From your Android or Google Play supporting Chromebook device, open **Malwarebytes**.
2. Tap the **menu** icon, scroll down, then tap **Settings**.
3. Tap **Protection**.
4. Confirm there's a checkbox next to Real-time protection (RTP) and Anti-Ransomware protection (ARP).

Real-Time Protection is more effective with all protection layers turned on. If any Real-Time Protection layers are turned off, we recommend turning them on as soon as possible. For help protecting your devices, refer to "Enable or disable Real-Time Protection."

Enable or disable device administrator permissions

Device administrator is a feature that grants administrator privileges at the operating system level to an app on your Android or Chrome OS device. When enabling Malwarebytes for Android version 3 as a device administrator, an Android OS message is shown, indicating the operations the app is allowed to perform, such as erase all data, or update device settings.

Malwarebytes only uses permissions for the actions specified below:

- automatically enable Anti-Ransomware remediation
- enable Real-Time Protection through file monitoring
- prevent malware from uninstalling the Malwarebytes app

For your protection, do not disable Malwarebytes for Android or Chromebook as a device administrator unless you need to uninstall the app.

These instructions also apply to Chromebooks with Google Play app support.

1. Open Malwarebytes for Android.
2. Tap the **Menu** icon on the top left.
3. Scroll down, then tap **Settings**.
4. Under Security settings, tap **Other**.
5. Tap **Device Administrator**.
   - If you are enabling device administrator, continue to step 6.
   - If you are disabling device administrator, no further action is required.
6. When the About Administration window appears, tap **DO IT NOW**.
7. Scroll down and tap **Activate**.

Enable or disable Protection settings

Protection features can be turned on or off in the paid subscription version of Malwarebytes for Android version 3. These features include Real-time Protection (RTP), Anti-Ransomware Protection (ARP), and Safe Browser Scanning.

Real-Time Protection

Open Malwarebytes for Android.

1. Tap the **menu** icon.
2. Tap **Settings**.
3. Tap **Protection**.
4. Tap the checkbox next to Real-time protection and Anti-Ransomware protection to turn these features on or off. Disabling Real-Time Protection automatically disables Anti-Ransomware protection. When enabling Real-time protection, the About Administration window displays.
5. Tap **DO IT NOW** to enable Device Administrator permissions. For more information, see "Enable or disable device administrator permissions."

If you've turned off Real-Time Protection on your device, turn protection back on as soon as possible to keep your device protected from malware.

Safe Browsing Scanner

1. Open Malwarebytes for Android.
2. Tap the **menu** icon.
3. Tap **Settings**.
4. Tap **Protection**.
5. Tap **Safe Browsing scanner**.
6. The Accessibility Services window displays. Tap **Allow**.
7. The device's Accessibility menu displays. Enable Accessibility Services to turn on Safe Browsing scanner. Tap **Allow**.

Note: The Android OS notification for activating Accessibility Services is shown by default. Malwarebytes only uses this permission to read the URLs you enter and determine if the sites you visit are malicious, and to display notifications over

other apps.

8. Turn off Safe Browsing scanner by disabling Accessibility Services.

Note: Safe Browser scanning is only available when using Chrome browser on phones and tablets. For Chromebook devices, see Install Malwarebytes Browser Guard on Google Chrome browser.

Set background exclusion

Android devices may recommend enabling battery optimization for some apps to reduce battery drain. Setting a background exclusion for Malwarebytes for Android version 3, by disabling battery optimization for the app, is required for Malwarebytes to run in the background and protect your device when the app is not open. For more information on required functions and permissions, see "Required permissions in Settings."

To set a background exclusion by disabling battery optimization:

1. On your Android device, open **Settings**.
2. Tap **Apps**.
3. Select **Malwarebytes**.
4. Tap **Battery Usage**.
5. Select **Don't optimize or Allow background activity**.

Note: Different devices may have different options to disable battery optimization.

Manage Malwarebytes

Deactivate device

When using the Premium version of Malwarebytes for Android version 3, you can deactivate one device to transfer the subscription to another device, or to change subscription details from one subscription to another, for example, from a Google Play subscription to a subscription purchased via the Malwarebytes Online Store.

To deactivate a device:

1. Open the Malwarebytes app on your Android device.
2. In the upper-left corner of your screen, tap the **Menu** icon.
3. Tap **Settings**.
4. Scroll to the bottom and tap **Deactivate this device**.
5. A confirmation window displays, click **DEACTIVATE**.
6. Your device is now deactivated.

You can now activate your subscription on another device, or activate a different subscription on the current device.

To install on another device, see Install & activate Malwarebytes personal products.

Locate license key details

Subscriptions purchased from the Malwarebytes Web store include a license key. You can view your subscription details in the Malwarebytes for Android version 3 app.

1. Open Malwarebytes.
2. Tap the **Menu** icon in the upper-left on the Dashboard.
3. Tap **Settings**.
4. Your license key will display under the Subscription section.

Note: Subscriptions purchased through the Google Play Store do not display a license key in the app.

Malwarebytes for Android v3 Widget

You can create one or more Malwarebytes for Android version 3 widgets on your Android Home screen. The Malwarebytes widget lets you see your device status at a glance. They can be configured to show 1-4 information items. After a widget has been created, press the widget and drag one of its edges to expand or compress it. This article provides information that can be viewed in each widget.

Manually update database

Malwarebytes Premium for Android version 3 automatically performs database updates periodically. If using the Malwarebytes Free version, you must manually check for database updates to ensure your protection definitions are current. On the Dashboard, the Database Version area displays it's current status.

Manually check for database updates

1. Open Malwarebytes on your Android device.
2. Tap the **Menu** icon in the upper left-hand corner.
3. Tap **Settings**.

Uninstall Mobile Security for Android v3

You can uninstall Malwarebytes for Android version 3 from the Malwarebytes app, the device's settings, or the Google Play Store. This article explains how to uninstall through Google Play Store, or within the app itself.

Before you uninstall Malwarebytes for Android, you may need to deactivate the app as a device administrator. Device administrator is an Android feature that grants an app administrator privileges and prevents the app from being uninstalled.

Uninstall from Google Play

1. Open the Google Play Store app.
2. In the search bar, type "**Malwarebytes**".
3. From the results, tap **Malwarebytes Mobile Security**.
4. Tap **Uninstall**.
5. Confirm that you want to uninstall Malwarebytes. Tap **OK** to uninstall the app.

Uninstall from the app

1. Open Malwarebytes on your Android device.
2. Tap the **Menu** icon in the top-left of the screen.
3. Under General, tap **Uninstall Malwarebytes**.
4. Tap the box which best describes why you wish to uninstall Malwarebytes.
5. Tap **Uninstall**.
6. Confirm that you want to uninstall Malwarebytes. Tap **OK** to uninstall the app.

If you have uninstalled Malwarebytes for Android Premium and need to transfer your subscription to a new device, see "Install Mobile Security for Android v3."

Uninstall Mobile Security v3 for ChromeOS

This article guides you through uninstalling Malwarebytes Mobile Security version 3 on your Chromebook.

1. Open the Malwarebytes app on your Chromebook.
2. Click the **menu** button on the upper left side of the window.

3. In the left menu pane, scroll down and click **Uninstall Malwarebytes**. You will be asked why you want to uninstall.
4. Check the checkbox that applies to your reason.
5. Click the **Uninstall** button at the bottom right part of your window.
6. In the confirmation pop-up window, click **OK**.

If you have uninstalled Malwarebytes Premium on Chromebook and need to transfer your subscription to a new Chrome OS device, see "Install Mobile Security v3 for ChromeOS."

Run Scans

Run a Scan

Malwarebytes for Android and ChromeOS version 3 offers a scanner to detect ransomware, malware, adware, spyware, and potentially unwanted programs on your device. You can scan your device on demand whether you have Malwarebytes Free or Malwarebytes Premium versions. This article describes how to initiate a scan, and how to interpret the results of your scan.

To run a scan:

1. Open Malwarebytes for Android or Malwarebytes for Chromebook.
2. In the upper-left corner, tap the **Menu** icon.
3. Tap **Scanner**.
4. Tap **Run a scan**. Malwarebytes may take a few seconds or minutes to scan your device.

Malwarebytes provides a counter of how many threats were detected if any were found. If no malware was found, your device is safe for now.

Interpreting scan results

On the Scanner page, you can scroll down to see Previous scans. These listed items show information on previous scan times, number of items scanned, the time taken, and when new apps were installed. Each item appears with different color bullets in front of the text. Green is good, orange represents a non-critical issue, and red is critical. The following is a list of different items that may appear in your Previous scans list, and what each color means for each item.

On-demand scan

- Green: An on-demand scan completed with no issues detected. Scans that were stopped before completion are not recorded.
- Orange: Potentially unwanted programs were detected during an on-demand scan. Scans that were stopped before completion are not recorded. You must allow, ignore or delete files causing this alert.
- Red: Malware was detected during an on-demand scan. Scans that were stopped before completion are not recorded. You must allow, ignore or delete files causing this alert.

Scheduled scan

- Green: A scheduled completed with no issues detected.
- Orange: Potentially unwanted programs were detected during a scheduled scan. You must allow, ignore or delete files causing this alert.
- Red: Malware was detected during a scheduled scan. You must allow, ignore or delete files causing this alert.

Scan after update

- Orange: Potentially unwanted programs were detected during a scan after the signature database updated. You must allow, ignore or delete files causing this alert.
- Red: Malware was detected during a scan after the signature database updated. Potentially unwanted programs may also have been found. You must allow, ignore or delete files causing this alert.

SD-card scanner

- Orange: Potentially unwanted programs were detected during an SD memory card scan.
- Red: Malware was detected during an SD memory card scan. Potentially unwanted programs may also have been found.

Reboot scan

1. Orange: Potentially unwanted programs were detected during a scan that occurred after a device reboot.
2. Red: Malware was detected during a scan that occurred after a device reboot. Potentially unwanted programs may also have been found.

File monitor

- Orange: Real-Time Protection detected potentially unwanted programs during a file transfer. You must allow, ignore or delete files causing this alert.
- Red: Real-Time Protection detected malware during a file transfer. Potentially unwanted programs may also have been found. You must allow, ignore or delete files causing this alert.

App installation

- Orange: Real-Time Protection was triggered by installation of a potentially unwanted program. You must allow, ignore or delete files causing this alert.
- Red: Real-Time Protection was triggered by installation of a file identified as malware. You must allow, ignore or delete files causing this alert.

App execution

- Orange: Real-Time Protection was triggered by execution of a potentially unwanted program. You must allow, ignore or delete files causing this alert.
- Red: Real-Time Protection was triggered by execution of a file identified as malware. You must allow, ignore or delete files causing this alert.

Act on scan results

If you run a scan in Malwarebytes for Android and ChromeOS version 3 and no threats are detected, your device is safe for now. If malware is detected, it needs to be dealt with. You can act on detections in the following ways:

- **Delete:** The threat will be deleted from your device.
- **Ignore Always:** The file detection will be added to the Allow List, and excluded from future scans. Legitimate files are sometimes detected as malware. We recommend reviewing scan results and adding files to Ignore Always that you know are safe and want to keep.
- **Ignore Once:** A file has been detected as a threat, but you are not sure whether to add it to your Allow List or delete. This option will ignore the detection this time only. It will be detected as malware on your next scan.

To learn how to perform a scan on your Android or Chromebook device, see "Run a scan."

Ignore or delete detections

1. If you want to add any detections to the Allow List, scroll to the detection you want to ignore, tap the **Ignore action** drop down menu, then tap either **Ignore Once** or **Ignore Always**.
2. For detections you want deleted, tap the checkbox next to each item to highlight them for removal. If you want to delete all detections found on the scan results screen, tap the checkbox next to **Select all threats**.
3. Tap **Remove selected**.
4. In the Confirmation window, tap **OK**.

All detections should now be dealt with on your Android or Chrome OS device.

If a file cannot be deleted after a scan

If you find some files cannot be deleted after a scan, this may occur for the following reasons:

- Files may be located in system folders.
- Files may be locked or in use by other apps.
- Malwarebytes was not given storage permissions, or the permissions were revoked.
- Files are bloatware installed on the device by the vendor.

If this situation happens, you will see an error notification when you try to delete a file of this type. To find the location of the file, tap on the Menu icon, then tap Scanner to view Previous scans. This screen displays all files and apps detected for that particular scan.

Scan settings overview

The Scanning settings in Malwarebytes for Android and ChromeOS version 3 allow you to enable or disable certain types of scan, and to schedule scans. To view this screen in the Malwarebytes app, tap the Menu icon in the top-left corner of the screen, then tap Settings, then Scanning. Features relating to schedule scans found on this screen only apply to Malwarebytes Premium subscribers.

Explanation of each setting is as follows:

- **Scan after reboot:** If checked, Malwarebytes performs a full scan immediately after your device is rebooted. If unchecked, no scan occurs on device reboot.
- **Scan after update:** If checked, a full system scan occurs after each protection update. If unchecked, protection updates won't trigger scans.
- **Use deep scanning during full scan:** If checked, full scans use additional deep scanning rules. Scan times will increase, but scans will be able to detect additional items.
- **Power saving scans:** If checked, Malwarebytes will not run scheduled scans if your device battery is low or if the device is in power save mode.
- **Perform scans during charge only:** If checked, Malwarebytes only runs scheduled scans when your device is charging.
- **Scheduled scans:** If checked, Malwarebytes automatically scans your device based on the following settings:
- **Scan frequency:** Chooses whether scans occur daily or weekly.
- **The days of the week:** If Scan frequency is set to Weekly, this option allows you to select which day(s) a scan occurs on.
- **Time:** Allows you to select the exact time when a scan begins. If scans are scheduled to run on multiple days, all cans occur at the same time of day.

If Scheduled scans is unchecked, non-scheduled scans still occur at an on-demand basis.

Manage Threats

Privacy Checker overview

The Privacy Checker screen in Malwarebytes for Android and ChromeOS version 3 helps you maintain a more secure environment on your device. To view this screen, tap the Menu icon hamburger-menu.png in the top-left corner of the app, then tap Privacy Checker. When you load this screen, all of your device's apps are scanned with regard to privacy settings. When the scan completes, you see a breakdown of how your privacy may be effected by each installed app. Categories listed below do not indicate what permissions have been given, only what the app is capable of performing.

Categories which may appear on the Privacy Checker results are:

- **have network access:** These apps can access the Internet.
- **can read your personal info:** These apps can access your contacts, phone number and web history.
- **can access storage:** These apps can read and write files from your phone's memory.
- **can publish shortcuts to the main screen:** These apps can automatically create shortcuts on the main screen, a tactic often used by aggressive ad networks.
- **can download files silently:** These apps can download files without notification.
- **can block screen:** These apps can "steal your screen," taking control of your phone away from you.
- **can cost you money:** These apps can send SMS messages and make calls.
- **can make calls:** These apps can make calls without user confirmation.
- **can track location:** These apps can access your location.
- **can access secure settings:** These apps can change your PINs and lock patterns.
- **can access calendar:** These apps can access your calendar.
- **can be Device Administrator:** These apps can be Device Administrator.
- **uses accessibility service:** These apps can see your activities.
- **can monitor calls:** These apps can record your calls.
- **can access text messages:** These apps can read your text messages.
- **can access accounts:** These apps can access your added system accounts. These accounts include (but are not limited to) your Google account.
- **can control hardware:** These apps can access your hardware, including (but not limited to) camera and NFC adapters.

Tap an any category with apps listed to find out which apps are part of the list. Tap on the vertical ellipses button next to any app for more information about the app and the resources it uses.

Your apps overview

The Your apps screen in Malwarebytes for Android and ChromeOS version 3 allows you to view a list of apps on your device, their app info, and other options. In Malwarebytes, tap the Menu icon, then tap Your apps to view app info. We can only provide usage information if you have granted Malwarebytes usage permission.

Your apps is divided into three sections:

- **System Apps:** This section lists apps installed by Google as part of the operating system.

- **Installed:** This section lists apps installed by you.
- **Recently Used:** This section lists apps that have been used recently, and may be either System apps or Installed apps.

To sort the way apps are listed, tap the three bars at the top-right of the Your apps screen. Tap the three dots next to any app to uninstall, view App info, or open it in the Play Store. You can also view App info by tapping the app itself. The App info screen shows app memory usage characteristics, and provides options affecting app operation. These options can include:

- Force stop
- Clear data
- App info
- Clear cache
- Uninstall

The App info screens for each app are at the system level. We do not recommend tapping Force stop, Clear data, or Clear cache as these may adversely affect app processes or delete app configurations.

View Allow List

If a file or app appears on the Allow List, it is considered safe only because you chose Ignore Always for the detection after a scan. Files and apps can only be added to the Allow List on the Scan results screen of Malwarebytes for Android and ChromeOS version 3. To learn how to allow detections after scans, see "Act on scan results."

View excluded items

1. In Malwarebytes, tap the **Menu** icon in the top-left corner of the screen.
2. Tap **Scanner**.
3. Tap the **Allow List** icon in the top-right of the screen.

If you added a file or app to the Allow List and later decide that you don't want to exclude it from scans, check the box next to the file and tap Remove from Allow List. It will be removed immediately. To remove all files and apps from the Allow List, tap **Select all** at the top-right of the Allow List screen, then tap **Remove from Allow List**.

Once a file has been added to the Allow List, it remains there until you remove it, or if Malwarebytes determines that the file has changed. This may be because its signature has changed, or because the file has been updated.

Remove threats from external storage

Malwarebytes for Android version 3 can remove malware from external storage, such as SD cards, on various Android versions. This article provides instructions on removing threats from your Android device. These instructions do not apply to devices using Chrome OS.

Remove threats from SD card with Android version 4.4

To remove a malicious file from external SD card storage on an Android version 4.4 (Kit Kat) device, you must grant Malwarebytes access to the file, using a special file selection window. You will encounter this window once you have confirmed removal of malware on your Android device.

1. After scanning your device, select the threats you want to delete and tap **Remove selected**.
2. A window displays to ask for your confirmation. Tap **OK**.
3. Another window displays if malware is present of the SD card. The folder containing malware and the malicious files are listed. You must manually find the files on your device.
4. Look for the malicious files in your device's list of apps. Only files identified in the Confirmation windows can be deleted. Long tap on the malicious file or files for the option to manually delete them from your SD card.

Remove threats from SD card with Android version 5.0 and higher

To enable Malwarebytes to remove malware from SD card on Android version 5.0 and higher, you must provide the app access to the whole external storage manually. This access needs to be given once, unless you reinstall Malwarebytes of clear data. You must select the root folder of the SD card in your Android interface which provides Malwarebytes the permission it needs to remove malicious files from your SD card.

1. After scanning your device, select the threats you want to delete and tap **Remove selected**.
2. A window displays to ask for your confirmation. Tap **OK**.
3. Another window displays to guide you to grant permission for Malwarebytes to access your SD card. Tap **OK** after reading the instructions.
4. Locate and select your SD card on your Android device.
5. In the SD card's root folder, tap **SELECT "SD card"** at the bottom of your screen. The name of your SD card may differ from the screenshot shown.

Tapping SELECT "SD card" grants Malwarebytes access to remove malicious files from the entire SD card. Files will be deleted immediately after access is granted. Permission to access the SD card stays active until Malwarebytes is uninstalled, or its data cleared.

Fix device issues

After installing Malwarebytes for Android and ChromeOS version 3, you may see Critical and Non-critical issue notices on the app's Dashboard. Each of these detail issues identified by Malwarebytes on your device. Depending on the amount of messages, you may need to scroll down to view all of them. These issue messages are color coded to signal their severity:

- Orange: Issues which may affect your security but are non-critical.
- Red: Critical issues which require your attention.

Under each issue, you'll see a blue call-to-action button that recommends the next steps. Click the button and follow the prompts to fix the issue. There is also a checkbox to the right of each item. Check any of these boxes if you want to hide non-critical issues from view on the Dashboard. Critical issues cannot be hidden. The following is a selection of issues which may appear on your Dashboard, their severity, and our recommendation for correcting each of them.

Last Scan Performed

- Non-Critical: Last scan has been performed more than a week ago
- Critical: Full scan has never been performed
- Critical: Last scan has been performed more than 2 weeks ago
- Resolution: Perform a full scan

Last Scan Ignore Malware (not deleted or added to Allow List)

- Non-Critical: After last scan you've ignored some unwanted malware
- Non-Critical: After last scan you've ignored some adware
- Critical: After last scan you've ignored some dangerous malware
- Critical: After last scan you've ignored some dangerous RANSOMWARE
- Resolution: Perform a full scan and/or review Allow List entries

Unscanned Apps

- Non-Critical: You have new apps that haven't been scanned yet
- Resolution: Perform a full scan
- Old/Missing Malware Database
- Non-Critical: Last database update has been performed more than a week ago
- Critical: Database has not been updated yet
- Critical: Last database update has been performed more than 2 weeks ago
- Resolution: Update your database

Allow List Cleared

In cases where a user removed items from the Allow List, Malwarebytes may need to scan to ensure previously excluded items are not present on your device.

- Non-Critical: Allow List that contained adware has been cleared
- Non-Critical: Allow List that contained unwanted malware has been cleared
- Critical: Allow List that contained dangerous malware has been cleared
- Critical: Allow List that contained dangerous ransomware has been cleared
- Resolution: Perform a full scan

Scans Disabled

- Non-Critical: Scan after update is disabled
- Resolution: Enable this setting to assure you are protected with the newest threat information
- Real-Time Protection Disabled
- Non-Critical: Real-Time Protection is disabled
- Resolution: Enable Real-Time Protection

Security Audit Issues

- Non-Critical: Security Audit detected some issues
- Resolution: Reviewing Security Audit is highly recommended

Draw over other apps disabled

- Critical: This permission is required to show remediation instructions in Anti-Ransomware protection.
- Resolution: Allow permission for the Malwarebytes app to draw over other apps under device's Accessibility settings.

Background exclusion required

- Non-Critical: Malwarebytes is enabled for Battery Optimization in device Settings or 3rd party app which could cause functionality issues.
- Resolution: Disable Battery Optimization

Other permissions
Malwarebytes on Android devices offers several other protection layers which require user permission to function. Learn more about "Required Permissions in Settings."

Troubleshoot

Collect Diagnostic Data

When you submit a ticket about a Malwarebytes for Android version 3 issue, you'll be contacted by a Malwarebytes Support agent through email. Depending on your issue, you may need to collect diagnostic data for the support agent to investigate and resolve the problem.

Follow the steps below to collect and reply with diagnostic data:

1. Open the Malwarebytes app on your Android device.
2. Tap the **Menu** icon on the top left.
3. Scroll down to the GENERAL section and tap **Settings**.
4. Select the **Enable diagnostic mode** checkbox.
5. Repeat the steps that led to the issue. Once you experience the issue, diagnostic mode logs the incident.
6. Tap **Settings > Export diagnostic data.** Save the file to your device's storage.
7. Locate and open your existing email with Malwarebytes Support.
8. In your email reply, attach the file that you've saved in Step 6.
9. Uncheck the **Enable diagnostic mode** box after you send the email reply to your Malwarebytes Support agent. If you turn off the setting before sending the reply, the diagnostic data file saved to your device may get deleted.

Error Messages

Malwarebytes for Android version 3 provides error codes and messages for connection, activation and authentication issues. This article describes the error messages including error codes, description, and recommended resolution for the error encountered.

Connection errors

Code	Message	Resolution
MB991	Registration error. We are having trouble reaching our registration server. Try again later or contact Support.	Check your internet connection and try again. If the issue persists, submit a ticket with Support.
	There was an issue deactivating Malwarebytes.	An active internet connection is needed to complete this action. Check your internet connection and try again. If the issue persists, submit a ticket with Support.

Activation errors

Code	Message	Resolution
MB403100	There's a problem with your license key and we are unable to activate your license.	Submit a ticket with Support.
MB403101	There's an issue with your license key. Please contact Support.	Submit a ticket with Support.
MB403101	There's an issue with your license key. Please contact Support.	Submit a ticket with Support.

Code	Message	Resolution
MB403102	The license key is expired. Enter another key or purchase a new one.	Purchase a valid subscription. You can make an in-app purchase from the Google Play store or visit our Pricing page, and activate after creating your Malwarebytes Account.
MB403103	This license does not match the product your are trying to activate. Enter another key or purchase a new one.	Purchase a valid subscription. You can make an in-app purchase from the Google Play store or visit our Pricing page, and activate after creating your Malwarebytes Account.
MB403104	This license key was already used to activate the maximum seats available.	Deactivate devices or purchase another subscription. See how to deactivate a device, make an in-app purchase from the App store or visit our Pricing page, and activate after creating your Malwarebytes Account.
MB403105	The license key has been refunded. Enter another key or purchase a new one.	Purchase a valid subscription. You can make an in-app purchase from the Google Play store or visit our Pricing page, and activate after creating your Malwarebytes Account.
MB404102	License key not found. Make sure that it's correct.	Check your license details and try again. If the issue persists, contact Support.
MB404100	This subscription is cancelled. Use another subscription or purchase a new one.	Purchase a valid subscription. You can make an in-app purchase from the Google Play store or visit our Pricing page, and activate after creating your Malwarebytes Account.

Authentication errors

Message	Resolution
Your account does not include Malwarebytes Mobile Security. To get started, add a Malwarebytes Mobile Security subscription.	Purchase a valid subscription. You can make an in-app purchase from the Google Play store or visit our Pricing page, and activate after creating your Malwarebytes Account.
Verify your email and password are correct and try again.	Check your sign in credentials, then try to sign in again. If the issue persists, submit a ticket with Support.
Your email and/or password is incorrect. You have x more attempts in total before your account is locked.	Check your sign in credentials, then try to sign in again. If the issue persists, submit a ticket with Support.
You have reached the maximum number of invalid attempts. For security reasons, your account has been temporarily locked. Please try again in 10 minutes.	RTProtectionDaemon Wait the recommended period of time, then try to sign in again. If the issue persists, submit a ticket with Support.

Report a problem

If you're experiencing an issue with Malwarebytes for Android version 3, send an issue report using the app. Sending an issue report creates a ticket for you.

Send Issue Report from the app

Follow the steps below if you're able to navigate through the app:

1. Open the Malwarebytes for Android app.
2. Tap the **Menu** icon in the upper left-hand corner.
3. Tap **Your apps**. Please wait until your installed apps list populates before continuing.
4. Tap the **Menu** icon in the upper right-hand corner.
5. Tap **Send to support**.
6. Choose an email application under Send email to report a problem to Malwarebytes Support.
7. Your email app opens with all of the needed information automatically included. Do not change any of the information in your email. Tap the **Send button** for your email app.

Send Issue Report when the app's unresponsive

If Malwarebytes for Android doesn't open or becomes unresponsive, follow these steps:

1. From your Android device, go to the home screen or the app list.
2. Find the **Malwarebytes** icon.
3. Press and hold the icon until the dropdown list appears.
4. Select **Contact support** in the list.
5. Select your email application. An email is generated with the issue report.
6. If you have an open support ticket for this issue, add the ticket number at the top of the email body.
7. Tap **Send**.

Start Android in safe mode

Safe mode is a startup method that allows you to troubleshoot issues with your Android device. Use the instructions in this article to start your device in safe mode.

For Google Pixel and stock Android devices

1. Press and hold the Power button until your device turns off.
2. Press and hold the Power button.
3. When the device's logo appears, release the Power button, then press and hold the Volume Down button.

4. Once the words safe mode appear in the bottom-left corner of your screen, release the Volume Down button.

Samsung devices

1. Press and hold the Power button until your device turns off.
2. Press and hold the Power button.
3. When the Samsung logo appears, release the Power button, then press and hold the Volume Down button.
4. Once the words safe mode appear in the bottom-left corner of your screen, release the Volume Down button.

OnePlus devices

1. Press and hold the Power button until your device turns off.
2. Press and hold the Power button.
3. When the OnePlus logo appears, release the Power button, then press and hold the Volume Up and Volume Down buttons.
4. Once the words safe mode appear in the bottom-left corner of your screen, release the Volume buttons.

To quit safe mode, hold down the Power button and tap **Restart**.

Notifications overview

Malwarebytes for Android and ChromeOS version 3 displays notifications related to Scan results, Real-Time Protection, and program or device issues. This article details the notification information and what actions are expected for each.

Scan Result notifications

Message	Description	Action needed
On-demand scan in progress. Scanning...	While a scan is in progress, this notification displays the status of the scan, including the number of items scanned and the number of Malware items detected.	While a scan is in progress, tap the notification to open the app and see additional scan details.
Scan in progress. Scanning...	While a scan is in progress, this notification displays the status of the scan, including the number of items scanned and the number of Malware items detected.	While a scan is in progress, tap the notification to open the app and see additional scan details.
x Infection(s) found	A Scan detected an infection in the device. This is shown every time a malicious item is found.	Tap the notification to take action on the item(s) found. For more information, see “Act on scan results.”
Your device is now safe.	Displays after action has been taken on a previously detected infection.	No action needed. You can access the Scanner page to review previously completed scan results.

Message	Description	Action needed
Possible ransomware detected! [ransomware_name] might be a ransomware application. If you are unsure about this app, we recommend you to remove it immediately.	Displays when a possible ransomware threat is detected. The notification includes action buttons for “Ignore” and “Remove now”	Click the “Ignore” action button to disregard the detection, and keep the app. Click “Remove now” to remove the app from the device. For more information, see “Act on scan.”
Anti-ransomware Protection:... is safe to use	Displays when an app suspected of being ransomware is considered safe to use.	No action needed.

Real-Time Protection notifcations

Message	Description	Action needed
Real time protection is active.	Indicates Real-Time Protection features are enabled.	No resolution required. For more information, see “Enable or disable Real-Time Protection.”

General and Product issues notifcations

Message	Description	Action needed
Your device has issues!	Indicates there are situations that need your attention regarding product or device settings.	Tap the notification to navigate to the app’s Dashboard and resolve the issues presented.

Clear app data

Sometimes bad app data causes an error in Malwarebytes for Android version 3. Clearing app data will help solve issues with Malwarebytes. This article will show you how to clear app data on your Android device.

1. Uninstall and reinstall the Malwarebytes app on your Android device.
2. Once installed, go to the device **Settings > General tab > Apps > Malwarebytes > Storage** and tap the **Clear Data** button.
3. Reboot the device.
4. Launch Malwarebytes and go to the Settings screen by tapping the icon of the 3 stacked horizontal lines located in the top left corner.
5. Tap the **Settings** menu option.
6. Tap **Other**.
7. Tap **Force Update** to download the latest updates. A prompt will appear if the database is already up-to-date.
8. Exit out of Settings and run a new scan in Malwarebytes.

Activation not available when running a trial

Starting a Premium Trial on Malwarebytes for Android version 3 links your Google account to your subscription, hiding the options to activate the Premium features. This article describes how to resolve this issue and allow activation with existing subscription details.

Symptoms
Unable to view activation options while running a Google Play Premium Trial.

Product
Malwarebytes for Android.

Cause
Once the Premium Trial is enabled, the product behaves as if a Premium subscription is in place, not displaying activation options.

Resolution
Cancel the Premium Trial. Once the Trial is cancelled, your app returns to the Free status, and the Activation options will display.

To cancel the Trial via the Google Play store:

1. Open the Google Play app Google Play.
2. At the top right, tap the **profile** icon.
3. Tap **Payments & subscriptions** and then **Subscriptions**.
4. Select the subscription you want to cancel.
5. Tap **Cancel subscription**.
6. Follow the instructions.