



Webroot Home Products User Guide

Webroot® AntiVirus

Webroot® Internet Security Plus

Webroot® Internet Security Complete

Webroot® Premium

Webroot® Security for Chromebook™

Notices

Webroot Home Products User Guide revision Wednesday, May 15, 2024

Information in this document is for the following products:

- Webroot® AntiVirus
- Webroot® Internet Security Plus
- Webroot® Internet Security Complete
- Webroot® Premium
- Webroot® Security for Chromebook™

One or more patents may cover these products. 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 Open Text.

© 2004-2024 Open Text. All rights reserved.

Contents

Getting Started	3
Installing Webroot on your Windows computer	4
Installing Webroot on your Mac	6
Navigating Webroot on your Windows computer	8
Navigating Webroot on your Mac	9
Setting up a Webroot account	10
Scanning for threats	11
Managing detected threats	13
Scheduling scans	15
Changing scan settings	17
Shielding your computer	19
Viewing and disabling shields	21
Changing shield settings (Windows)	22
Using Web Threat Shield	23
Changing Realtime shield settings (Mac)	25
Receiving and reviewing web threats (Mac)	26
Protecting personal information	27
Security recommendations (Mac)	29
Using firewall and web shield protection (Windows)	33
Quarantining items	35
Managing quarantined items	38
Blocking or allowing files	39
Using antimalware tools (PC)	40
Setting preferences on your Windows computer	41
Setting preferences on your Mac	44
Using system control tools	46
Using System Optimizer	48
Changing System Optimizer settings	50
Using Secure Erase	54
Security for Chromebook™	55
Using Secure Browser	57
Enabling Webroot for Chrome	58
Password management with LastPass	59
Viewing your Activity Report	60
Support	61

Getting Started

Webroot home office software delivers protection against viruses, spyware, and other online threats without slowing down performance or disrupting your normal activities. With its fast scans and threat removal, malware is eliminated quickly and easily. Webroot software enables you to surf, share, shop, and bank online with confidence that your computer and your identity will be kept safe.

Information in this document is for the following products:

- Webroot® AntiVirus
- Webroot® Internet Security Plus
- Webroot® Internet Security Complete
- Webroot® Premium
- Webroot® Security for Chromebook™

Note that an earlier name for this software was *SecureAnywhere*. You may see this name in the product and in screenshots within this User Guide. To strive for consistency, the current product edition names are used whenever possible. However, procedures that refer to screen elements labeled *SecureAnywhere* match the user interface to avoid undue confusion.

Screenshots in this User Guide may be from a prior version and differ from what is displayed on your screen.

Prior releases of Webroot software used an online console called the *Management Website*, which is no longer supported. Much of the functionality previously available on the *Management Website* is now available on the MyAccount portal. If you are still using *Management Website*, a User Guide is available at <https://docs.webroot.com/us/en/home>. Some of the information in that Management Website User Guide may be obsolete or inaccurate.

Installing Webroot on your Windows computer

Before you begin:

- Confirm the system requirements at <https://www.webroot.com/us/en/support/system-requirements>.
- Confirm you have all appropriate browser extensions if you intend to turn on Web Threat protection.
- Read the license agreement at <https://www.webroot.com/us/en/legal/service-terms-and-conditions>.
- Make sure you have the 20-character license keycode that identifies your Webroot account.
 - Your keycode comes in an email message or is listed inside the retail box.
 - If you purchased a multi-user license, you can use the same keycode to install the software on up to three or five devices.
 - If you don't know your keycode, click Help me find my keycode on the installation screen.
 - **Note:** The keycode does not include any information related to your computer or its configuration. Webroot does not use the keycode in any way to track individual use of its products.
- Close all programs.

To install Webroot:

1. Install Webroot from either a downloaded file or a CD.
 - Double-click the downloaded installation file to start the installation. Click **Run** to begin.
 - By request, Webroot support can send you an installation CD.
 - If installing from a CD, insert the CD and click a link on the installation dialog to begin.
 - If the installation dialog does not open, use Windows Explorer to navigate to your CD drive and double-click the Webroot installation file.
2. When the Webroot installation dialog appears, enter your keycode in the field.
 - If you don't know your keycode, click **Help me find my keycode**.
3. If required, click **Installation options** to:
 - Change the installation location.
 - Create a desktop shortcut.
 - Randomize the installed filename. Selecting the option prevents malware from detecting and blocking Webroot's installation file.
 - Protect Webroot files, processes, and memory (selected by default). This option enables self-protection and CAPTCHA prompts. CAPTCHA requires reading distorted text on the screen and entering the text in a field before performing any critical actions. For more information, see [Setting access controls](#).

- Change the default language. This setting can only be changed during installation.
- Set proxy settings. If you don't know what these settings should be, leave the default.

When done reviewing installation options, click the **Back** arrow to return to the main installation dialog.

4. On the main Installation dialog, click **Agree and Install**. If prompted, enter an email address and click **Continue**.
5. To exit the installation dialog, click **X**. If you purchased a multi-user license, you can install Webroot on other devices.
6. To view the product, click **Start using SecureAnywhere**. See [Navigating Webroot on your Windows computer](#).

Unless you want to modify your settings, that's all you need to do. Webroot begins scanning and configuring the application immediately.

- If your system is clean, a status screen displays confirmation of the scan.
- If threats are detected, the problematic items are moved to quarantine where they are rendered inoperable. For more information, see [Quarantining items](#).

After the initial scan, Webroot automatically scans your computer daily and constantly monitors your Internet activity in the background. You do not need to launch a scan yourself or schedule scans.

To verify that Webroot is running, look for the Webroot "W" icon in your system tray.

If an important message requires your attention, the icon turns yellow or red. Click the icon to see additional information.

Uninstalling Webroot on your Windows computer:

1. Click **Start** in the system tray and open the **Control Panel**.
2. Select **Programs and Features**. A list of all installed programs appears.
3. Right-click on **Webroot SecureAnywhere** and select **Uninstall**.

Installing Webroot on your Mac

Before you begin:

- Confirm the system requirements at <https://www.webroot.com/us/en/support/system-requirements>.
 - To upgrade to Webroot SecureAnywhere 9.5.10 or later, you must be running macOS 11 (Big Sur®) or later versions. If you are running macOS 10.15 (Catalina®) or older versions of macOS, you will no longer receive any upgrades to the agent beyond version 9.5.8. Consider upgrading your operating system to macOS 11 (Big Sur®) or later to increase product functionality and feature availability.
- Confirm you have all appropriate browser extensions if you intend to turn on Web Threat protection.
- Read the license agreement at <https://www.webroot.com/us/en/legal/service-terms-and-conditions>.
- Make sure you have the 20-character license keycode that identifies your Webroot account.
 - Your keycode comes in an email message or is listed inside the retail box.
 - If you purchased a multi-user license, you can use the same keycode to install the software on up to three or five devices.
 - If you don't know your keycode, click Help me find my keycode on the installation screen.
 - **Note:** The keycode does not include any information related to your computer or its configuration. Webroot does not use the keycode in any way to track individual use of its products.
- Close all programs.

To install Webroot:

1. Click the **Webroot SecureAnywhere installer** for your Mac, then click **Download Now** to begin the installation process.
2. Upon purchase, you should receive an email containing a download link. Open this link on the device you want to protect and follow the installation instructions for that device's operating system.
3. Follow the installation instructions for your device's operating system. When done with the installation, click **Close**. Webroot launches.
4. Enter your keycode in the **Activation** dialog and click **Activate Software**. If you don't know your keycode, click **Help me find my keycode**.
5. Webroot needs full disk access to protect your computer. If the **Full Disk Access** dialog appears:
 - Click **Open System Preferences**
 - Click **Security and Privacy**
 - Navigate to the **Privacy** tab and select **Full Disk Access**. If locked, enter your computer username and password and click **Unlock**.
 - In the **Security and Privacy** window, click **Add an application**.

- Navigate to your Mac's **Applications** tab, select **Webroot Secure Anywhere**, and click **Open**.
 - When prompted, click **Quit & Reopen**. Webroot SecureAnywhere now appears in the **Full Disk Access** list of allowed applications.
6. The **Webroot** window turns blue as it scans your Mac. If the scan does not find any threats, the window turns green when the scan completes. If it detects threats, the window changes to red and it prompts you to move the infected items to quarantine. In quarantine, these items are rendered inoperable. For more information, see [Managing detected threats](#) and [Managing quarantined items](#).

Navigating Webroot on your Windows computer

The main page of Webroot is your access point to all functions and settings.

To open Webroot, double click the Webroot icon on the desktop.

The main page displays.

- The Protected panel displays information about system scans and the status of your subscription to Webroot. You can manually scan the system any time by clicking **Scan My Computer**. The default scan schedule is set to run daily at the time you installed the software. To change the schedule, select **Advanced Settings > Scheduler**.
- The **Message** panel displays virus alerts and other information from Webroot.
- The Webroot features panel is your main navigation area to the product functionalities. Clicking a feature name expands it.
 - Click the gear icon following each feature to view Webroot settings and options.
 - Green circles with a checkmark indicate that this feature is included in your license. Blue circles with a plus sign indicate that this feature is not included in your license.
- You can always return to the main page by clicking on the **Webroot** logo.

Options for the main window include:

- **Advanced settings** define how you want the product to operate.
- **PC Security** options manage shield, firewall, and quarantine settings.
- **Identity Protection** settings protect sensitive data that may be exposed during your online transactions.
- **Password Manager** creates a secure password generator and profile storage facility.
- Use **Utilities** to optimize your system, manage processes and files, view reports, and create a SafeStart Sandbox.
- **My Account** provides account information and access to the web console.
- **Support/Community** provides customer support information and enables you to search for and discuss issues with the Webroot community.

Using the system tray:

- Right-click the Webroot icon in the system tray to launch common Webroot tasks. The popup menu displays different selections, depending on the Webroot edition you purchased.
- Alerts may also show in the system tray.
- If the icon does not display in the system tray, open the Webroot main page, select **Advanced Settings > Install Settings**, and select **Show a system tray icon**.

Navigating Webroot on your Mac

The main page of Webroot is your access point to all functions and settings.

To open Webroot, click the Webroot icon on the menu bar.

The main page displays.

- The Protected panel displays information about system scans and the status of your subscription to Webroot. You can manually scan the system any time by clicking **Scan My Computer**. The default scan schedule is set to run daily at the time you installed the software. To change the schedule, select **Advanced Settings > Scheduler**.
- The **Message** panel displays virus alerts and other information from Webroot.
- The Webroot features panel is your main navigation area to the product functionalities. Clicking a feature name expands it.
 - Click the gear icon next to each feature to view Webroot settings and options.
 - Green circles with a checkmark indicate that this feature is included in your license. Blue circles with a plus sign indicate that this feature is not included in your license.
- You can always return to the main page by clicking on the **Webroot** logo.

Options for the main window include:

- **Advanced settings** define how you want the product to operate.
- **Mac Security** options manage shield, firewall, and quarantine settings.
- **Identity Protection** settings protect sensitive data that may be exposed during your online transactions.
- **Password Manager** creates a secure password generator and profile storage facility.
- Use **Utilities** to optimize your system, manage processes and files, view reports, and create a SafeStart Sandbox.
- **My Account** provides account information and access to the web console.
- **Support/Community** provides customer support information and enables you to search for and discuss issues with the Webroot community.

Click **Webroot SecureAnywhere** on the menu bar to launch common Webroot tasks.

- **About SecureAnywhere** displays the product version number
- **Preferences** allows you to change the system preferences, scan schedules, and other settings
- **My SecureAnywhere Account** displays your keycode and other account details
- **Check for Updates** downloads and applies the latest program updates
- **Hide Webroot SecureAnywhere** hides the main window but does not shut down protection. To shut down protection, click the Webroot icon in the menu bar and select **Shut Down SecureAnywhere**.

Setting up a Webroot account

A Webroot account enables you to view and manage the security status of your supported computers from any device with an internet connection.

1. From the main page, click **My Account**. The area expands to display high-level account information.
2. Click the **My Account** button. The Carbonite/Webroot portal at myaccount.carbonite.com opens.
3. Follow the prompts to create an account.

Scanning for threats

Your computer's overall protection status causes the Windows system tray icon and the main interface to change colors:

- **Green** means your computer is secure
- **Yellow** indicates that one or more potential threats require your attention
- **Red** means one or more critical items require your intervention.

On your Windows computer, you can view details about the current status and settings by right-clicking on the Webroot icon in the system tray, then selecting **View Status**.

Scans automatically run every day at about the same time you installed Webroot. For example, if you installed the product at 8 p.m., Webroot always launches a scan around 8 p.m. It will not disrupt your work, nor will it launch while you play games or watch a movie.

The default deep scan searches all areas where potential threats can hide, including drives, files, and system memory. It looks for items that match Webroot threat definitions, match descriptions in the Webroot community database, or exhibit suspicious behavior.

- If Webroot detects a potential threat, it prompts you to decide whether you want to allow or block the item. If you aren't sure, we recommend that you block the item. See [Managing detected threats](#).
- If Webroot detects a known threat, it moves the item to quarantine where it can no longer harm your system or steal personal data.

Running a scan manually

An immediate scan might be necessary after browsing high-risk websites such as networking, music, or adult entertainment, downloading high-risk items such as screen savers, music, or games, or accidentally clicking on a suspicious pop-up advertisement. Immediate scans can be launched at any time.

To launch an immediate scan, open Webroot and click **Scan My Computer** on the main page.

Viewing scans

On your Windows scans, from the system tray, double-click the **Webroot** icon. The Webroot main page displays the latest scan results in the main panel.

Open Webroot by clicking the **Webroot** icon in the menu bar and selecting Open **Webroot SecureAnywhere**.

On your Mac, the scan statistics display in the middle of the Protected window.

Saving scan logs

If you want to investigate what Webroot scanned and what it found, you can save a scan log. Use this log when working with Webroot Support to determine the cause of a problem.

1. From the main window, click the **Utilities** gear icon and open the **Reports** tab.
2. Click **Save scan log**.

The system prompts you for a location to save the log, saves the most recent scan data to a text file, and displays the file.

Viewing protection statistics on your Windows computer

Protection Statistics allow you to view the background processes that Webroot is currently monitoring.

1. From the main window, click the **Utilities** gear icon and open the **Reports** tab.
2. Under **Event Viewers**, click **View Statistics**. The **Protection Statistics** panel displays.
3. Double-click on an event to view additional details. The **Events** pane displays.
4. Open the **Details** tab to view the additional information.
5. When done, click **Close**.

Managing detected threats

In most cases, Webroot automatically detects threats and quarantines the items for you. However, if it detects a potential threat or an item it does not recognize, it prompts you to decide whether to quarantine the questionable items.

- Clear the checkbox by any filename you recognize and want to keep. It will be restored to its original location and not be placed in quarantine. Do not restore the file unless you are certain that it is legitimate.
- Keep the checkbox selected for any filename you do not recognize. It will be placed in quarantine, where it is rendered inoperable.

Before executing the threat removal, we recommend that you:

- Save all open documents
- Close all open programs
- Safely remove any USB devices
- Remove CD and DVD disks from their drives
- Temporarily disable other security products (strongly recommended)

When you click **Next**, Webroot moves the selected items to quarantine, where they are rendered inoperable. You do not need to delete them or do anything else. If you determine later that you need a file, you can restore it to its original location.

After Webroot moves the threat to quarantine, it launches another scan to make sure your system is clean.

Saving threat logs

You can save a log of all threats removed on your system since installation. Threat logs can be used when investigating an infection with Webroot support.

To save a threat log using your Windows computer:

1. From the main window, click the **Utilities** gear icon.
2. Open the **Reports** tab.
3. Click **Save threat log**. The system prompts you for a location to save the log, gathers threat data saved since installation to a text file, and displays the file.

To save a threat log using your Mac:

1. From the main window, click the **Mac Security** gear icon.
2. Open the **Quarantine** tab.
3. Click **Save Threat Log**.
4. Select a folder location for the threat log and click **Save**.

Viewing execution histories on your Windows computer

The Execution History allows you to see when and where a virus entered the system.

1. From the main window, click the **Utilities** gear icon and open the **Reports** tab.
2. Click **View History**. The Protection Statistics panel displays. The **Execution History** panel displays.
3. For details about a specific program, highlight the name, and click **More Information**. The **Events** pane displays.
4. Open the **Details** tab to view the additional information.
5. When done, click **Close**.

Viewing active processes on your Mac

1. From the main window, click the **Utilities** gear icon.
2. The **System Control** tab displays all active processes.

Scheduling scans

Webroot launches scans automatically every day, at about the same time you installed the software.

To change the scan schedule on your Windows computer:

1. From the Webroot main page, click **Advanced Settings**. The **Settings** pane appears.
2. Click **Scheduler**. In the Scan Schedule tab:
 - When **Enable scheduled scans** is selected you can enter scan frequency and time in the next fields. If this checkbox is cleared, scheduled scanning is disabled.
 - Use the **Scan Frequency** drop down to modify how often to perform a scan.
 - Use the **Time** drop down to select a time for the scans. If you choose to scan when resources are available, the scan will launch as soon as possible, generally within an hour of the time you select.
 - Select **Enable Scheduled System Optimization** to determine the frequency and timing of system optimization.
 - Use the **Scan Frequency** drop down to modify how often to perform a system optimization.
 - Use the **Time** drop down to select a time for the optimizations.
 - **Scan on bootup if the computer is off at the scheduled time** launches a scheduled scan within an hour after you turn on your computer. When cleared, Webroot ignores missed scans.
 - **Hide the scan progress window** runs scans silently in the background. When cleared, a window displays the scan progress.
 - **Do not perform scheduled scans when on battery power** helps conserve battery power. When cleared, scheduled scans launch when you are on battery power.
 - **Do not perform scheduled scans when a full screen application or game is open** ignores scheduled scans when you are viewing a full-screen application, such as a movie or a game. When cleared, scheduled scans run anyway.
 - **Randomize the time of scheduled scans up to one hour for faster scanning** determines the best time for scanning, based on available system resources, and runs the scan within an hour of the scheduled time. When cleared, the scan runs at the exact time scheduled.
 - **Perform a scheduled Quick Scan instead of a Deep Scan** runs a quick scan of memory. When cleared (recommended), deep scans run for all types of malware in all locations.
3. Click **Reset to defaults** to revert to the original options.
4. When done, click **Save**.

To change the scan schedule on your Mac:

1. From the Webroot main page, click **Advanced Settings**. The **Settings** pane appears.
2. Click **Schedule**

- When **Enable scheduled scans** is selected you can enter scan frequency and time in the next fields. If this checkbox is cleared, scheduled scanning is disabled.
 - Use the **Frequency** drop down to modify how often to perform a scan.
 - Use the **Time** drop down to select a time for the scans.
 - Select **Enable Scheduled System Optimization** to determine the frequency and timing of system optimization.
 - Use the **Scan Frequency** drop down to modify how often to perform a system optimization.
 - Use the **Time** drop down to select a time for the optimizations.
 - **Run immediately at startup if SecureAnywhere misses a scheduled activity** launches a scheduled scan within an hour after you turn on your computer. When cleared, Webroot ignores missed scans.
 - **Don't perform scheduled activity when on battery power** helps conserve battery power. When cleared, scheduled scans launch when you are on battery power.
 - **Don't perform scheduled activity when a full screen application or game is open** ignores scheduled scans when you are viewing a full-screen application, such as a movie or a game. When cleared, scheduled scans run anyway.
3. Click **Reset Schedule** to revert to the original schedule.
 4. Click **Reset All** to reset all options to the original default.
 5. When done, click Close.

Changing scan settings

You can modify certain scanning functions using scan settings.

To change scan settings on your Windows computer:

1. From the Webroot main page, click **Advanced Settings**. The Settings pane appears.
2. Open the **Scan Settings** tab, then select your options:
 - **Enable rootkit detection** checks for rootkits and other malicious software hidden on your disk or in protected areas. Spyware developers often use rootkits to avoid detection and removal. We recommend keeping this option selected. It adds only a small amount of time to the scan.
 - **Scan the Master Boot Record** protects your computer against master boot record (MBR) infections. An MBR infection can modify core areas of the system so that they load before the operating system and can infect the computer. We recommend keeping this option selected. It adds only a small amount of time to the scan.
 - **Scan archived files** scans compressed files in zip, rar, cab, and 7-zip archives.
 - **Detect Potentially Unwanted Applications** looks for programs that aren't necessarily malicious but contain adware, toolbars, or other unwanted additions to your system.
 - **Enable rightclick scanning in Windows Explorer** enables you to run a full, file-by-file scan of the currently selected file or folder in the Windows Explorer right-click menu. This option is helpful if you downloaded a file and want to quickly scan it.
 - **Allow files to be submitted for threat research** allows potentially malicious files that our systems have not yet classified to be automatically uploaded to Webroot.
3. Click **Reset to defaults** to revert to the original options.
4. When done, click **Save**.

Creating custom scans on your Windows computer

1. From the main window, click the **PC Security** gear icon. The Scan & Shields tab appears.
2. Click the **Custom Scan** button. The Customized Scan window appears.
 - **Quick** performs a surface scan of files in active memory.
 - **Full** performs a scan of local hard drives.
 - **Deep** performs a scan for rootkits, trojans, and other threats.
 - **Custom** enables you to specify which files and folders to scan.
 - Click **Add File/Folder** then click **Add** to select the folders and files you want to scan.
 - To delete a file or folder, highlight it and click **Remove**.
3. When done, click **Start Scan**.

To change scan settings on your Mac:

1. From the Webroot main page, click **Advanced Settings**. The Settings pane appears.
2. Open the **Scan Settings** tab, then select your options:
 - **Automatically scan removable media** scans any removable media upon insertion. Scan mounted drives includes USB flash drives, external hard drives, disk image files, and other types of mounted drives in the scan.
 - **Scan mounted drives** scans any drives that were not automatically mounted.
 - **Also scan for Windows threats** (selected by default) scans for threats that may be carried on the Mac, but that are designed to attack Windows machines.
 - **Scan only Windows file extensions** only scans files with Windows file extension types such as .exe, .dll, etc.
 - **Scan archived files** (selected by default) determines that archived files such as .ZIP are included in the scan.
 - **Full scan** (selected by default) automatically performs a thorough search for all types of threats in all areas.
 - **Quick scan** performs a surface scan of locations where threats are commonly found. This scan runs quickly but may miss some types of inactive malware that launch after a system reboot.
3. Click **Reset Scan Settings** to revert to the original settings.
4. Click **Reset All** to reset all options to the original default.
5. When done, click **Close**.

Shielding your computer

Shields constantly monitor activity while you work both online and locally, protecting your computer from malware and viruses. Shields run in the background without disrupting your work.

If a shield detects an item that it classifies as a potential threat or does not recognize, it displays an alert. The alert asks if you want to continue or block the site.

- If you recognize the file name and you are purposely downloading it, for example, you were in the process of downloading a new toolbar for your browser, click **Unblock page and continue**.
- If you were not trying to download anything, you should click **Go back to safety**.
- If you feel that the shield is alerting you to a page that is not high risk, then you can click the **Request Review** button.

If you aren't sure what to do, we recommend blocking the file.

Types of shields

Webroot includes the following types of shields:

- **Realtime Shield** monitors unknown programs to determine whether they contain threats. Blocks known threats from running on your computer that are listed in Webroot's threat definitions and in our community database. You should never disable this shield.
- **Rootkit Shield** blocks rootkits from being installed on your computer and removes any that are present.
- **Web Shield** blocks known threats encountered on the internet and displays a warning. The Web shield maintains information on more than 200 million URLs and IP addresses.
- **USB Shield** monitors an installed USB flash drive for threats, blocks and removes any threats that it finds.
- **Offline Shield** protects your system from threats while your computer is not connected to the internet.
- **Script Shield** protects your system from malicious scripts.

The shields are pre-configured based on our recommended settings. Advanced users can change settings if required.

Internet search indicators

Webroot shields run when you run internet queries such as a Google search. Safety information is indicated by icons before each website name in the list of query results.



A dark green circle with a checkmark icon indicates well known sites with strong security practices that rarely exhibit characteristics that expose you to security risks. There is a very low probability that you will be exposed to malicious links or payloads from these sites.



A light green circle with a checkmark icon indicates benign sites that rarely exhibit characteristics that expose you to security risks. There is a low probability that you will be exposed to malicious links or payloads from these sites.



A yellow circle with a dash mark icon indicates generally benign sites but have exhibited some characteristics that suggest security risk. There is some probability that you will be exposed to malicious links or payloads from these sites.



An orange circle with an exclamation mark icon indicates suspicious sites. There is a higher-than-average probability that you will be exposed to malicious links or payloads from these sites.



A red circle with an exclamation mark icon indicates high risk sites. There is a high probability that you will be exposed to malicious links or payloads.



A white circle with a grey icon indicates that ratings are temporarily unavailable or the Webroot agent is shut down. Wait for service to be restored or check to be sure the Webroot agent is running.

Infrared shielding

Webroot can detect threats even when not running a scan using Infrared, a multi-layer defense technology that blocks threats very early in their lifecycle.

Infrared employs multiple engines that work together to determine the level of threat, assessing several factors:

- The safety level of websites.
- The reputation and behavior of newly introduced applications.
- By interpreting user behavior with an overall assessment of the safety level of the system. For example, if a user is classified as a higher risk, based on a combined view of the security of their operating system, applications, and prior threats which have been observed, Infrared dynamically tunes its heuristics and background processing, flexing within the configuration options the user has set, but increasing their effectiveness while preventing false positives for most users.

This risk assessment affects every protection module, from the firewall to behavior monitoring to real time protection, and eventually to website blocking as well. The result is a set of protections customized to the user's specific circumstances.

When possible, Webroot takes care of any detected threat automatically. For less severe cases, you are prompted to decide whether you want to continue.

Low, medium, and high-risk warning dialogs appear on your screen when a threat is detected.

- Low and medium-risk warning dialogs provide information about the detected threat and give you an option to block, allow once, or always allow the program or event.
- High-risk dialogs enable you to remove the threat immediately.

Viewing and disabling shields

We recommend you keep all shields enabled. Disabling a shield makes your computer vulnerable.

To view shield status or to disable shields on your Windows computer:

1. On the main window, in the **PC Security** section, two types of shields appear:
 - **Realtime shield** controls how threats are blocked and quarantined.
 - **Web shield** protects your system as you surf the internet.

We recommend that you keep all shields enabled; however, you can disable a shield by turning its switch off.

2. Click the **PC Security** gear icon to display a full list of shields and their status on the **Scan & Shields** panel.
3. To disable a shield, turn off its switch.
 - For most shields, the window color scheme goes brown, indicating that your computer is not completely protected.
 - For the Realtime Shield, the color scheme goes red, indicating that you are vulnerable to threats and should re-enable the shield.
4. Restart your browser for website shield changes to take effect.

To view shield status or to disable shields on your Mac:

1. On the main window, in the **Mac Security** section, two types of shields appear:
 - **Realtime shield** controls how threats are blocked and quarantined.
 - **Web Threat shield** protects your system as you surf the internet.

We recommend that you keep all shields enabled; however, you can disable a shield by turning its switch off.

2. To disable a shield, turn off its switch.
 - For most shields, the window color scheme goes brown, indicating that your computer is not completely protected.
 - For the Realtime Shield, the color scheme goes red, indicating that you are vulnerable to threats and should re-enable the shield.
3. Restart your browser for website shield changes to take effect.

Changing shield settings (Windows)

Shields are preconfigured, based on our recommended settings. You do not need to configure any settings yourself unless you are an advanced user and would like to modify shield behavior.

1. From the Webroot main page, click **Advanced Settings**. The Settings pane appears.
2. Open the **Shields** tab, then select your options:
 - **Prevent interruption by intelligently suppressing warnings** uses built-in intelligence to suppress warnings if they will interfere with operations.
 - **Automatically quarantine previously blocked files** remembers whether you allowed or blocked a file when previously alerted. If the file is encountered again, it will take the same action as before, without alerting you, including sending it to quarantine if appropriate.
 - If you want to restore the file, you can retrieve it from quarantine.
 - When cleared, Webroot triggers an alert every time it encounters this file in the future.
 - **Check files for threats when written or modified** scans any new or modified files that you save to disk. When cleared, the system ignores new file installations; however, it still alerts you if a threat tries to launch.
 - **Check files for threats when written or modified** scans any new or modified files that you save to disk. When cleared, the system ignores new file installations. It still alerts you if a threat tries to launch.
 - **Block threats automatically if no user is logged in** stops threats from executing even when you are logged off. Threats are sent to quarantine without notification.
 - **Warn if untrusted programs make core system changes when offline** displays a warning if an untrusted program tried to change core system settings while you were offline.
 - **Verify the integrity of the operating system** checks the operating system for problems.
 - **Silently and automatically block untrusted access to user data** automatically prevents unknown programs from accessing user data.
 - **Allow trusted programs to access protected data without warning** allows access to user data for trusted programs.
 - **Prevent any program from modifying the HOSTs file** prevents any program from modifying your HOSTs file.
3. When you're done, click the **Save** button.

Using Web Threat Shield

Web Threat Shield protects your computer as you surf the internet. If it detects a website that may be a threat, it blocks the page and asks if you want to continue despite the warning. This shield analyzes all the links on a search results page. It displays an image next to each link that signifies whether it's a trusted site or a potential risk.

Web Threat Shield is available in two modes: Integrated and Standalone.

- Integrated mode means that Web Threat Shield is installed as part of the Windows or Mac installation and uses the license that was used to install the agent.
- Standalone mode means the Web Threat Shield browser extension is installed without the WSA Windows or Mac agent installed. Standalone mode is used primarily to provide protection on platforms where there is no integrated support.

The standalone browser extensions can be obtained by going to your browser's extension store and searching for Web Threat Shield.

- For Chrome™, go to the [Chrome Web Store](#).
- For Edge, go to [Microsoft Edge Add-ons](#).
- For Firefox, go to [Firefox Add-ons](#).

When installing the extensions you will be prompted to provide a valid Webroot license. You cannot use Web Threat shield if you do not have the appropriate browser extensions installed. If you did not install these extensions when you installed Webroot, you are prompted to install them when you first try to turn on Web Threat protection.

For more information on Web Threat Shield, see the [Web Threat Shield User Guide](#).

Mac users must manually install the extensions on their browser(s) to get this functionality. Webroot for Mac does not automatically install browser extensions.

To change Web Threat shield settings for Mac:

1. From the Webroot main page, click **Advanced Settings**. The **Settings** pane appears.
2. Open the **Web Threat Shield** tab, then select your options:
 - **Enable Web Shield** (recommended) turns Web Shield protection on or off. When selected, you can modify the protection. This checkbox is selected by default.
 - **Block malicious websites** (recommended) checks any URLs and IPs you enter in a browser and creates a block page for known malicious sites. This checkbox is selected by default.
3. Click **Edit Website Overrides** to allow or block specific websites.
 - In the dialog that opens when you click the button, enter a full website name in the field (i.e., www.sitename.com) and click **Add Website**.
 - Specify whether to allow or block the site, then click **Close**.
 - You must restart your browser for website overrides to take effect.

4. **Select Monitor hosts file for changes** to shield the Mac's hosts files.
 - To return the Hosts file to its factory state and remove changes malware may have made to the file, click the **Reset Hosts File** button.
5. To revert Web Threat Shield back to the default settings, click **Reset Web Threat Shield**.
6. Click **Close**.

Changing Realtime shield settings (Mac)

The Realtime shield controls how threats are blocked and quarantined on your Mac. Webroot already configured this shield with our recommended settings, but you can adjust them as needed.

To change Realtime shield settings:

1. From the Webroot main page, click **Advanced Settings**. The **Settings** pane appears.
2. Open the **Realtime Shield** tab, then select your options:
 - **Automatically quarantine previously blocked files** sends an application file to quarantine if you had blocked and quarantined that file before. Clearing this option launches a scan if the file is detected again.
 - **Automatically block suspected threats when detected on execution** opens a notification if you attempt to launch an application that might be a threat. Webroot scans the directory where the application resides, then gives you the option of quarantining the items or allowing them to remain in their current locations.
 - **Scan files when written or modified** scans any new or modified files that you save to disk. When cleared, new file installations are ignored.
 - **Block threats automatically if no user is logged in** stops threats from executing, even when you are logged off. Threats are sent to quarantine without notification.
 - **Secure keyboard entry mode** prevents keyloggers on websites from capturing keystrokes. A keylogger is a type of system monitor that can record all keystrokes in your browser. Keyloggers may be used for legitimate purposes but can also be installed without your knowledge and used to record sensitive information.
 - **Monitor services running on the system** monitors the folders of system services running on your Mac and protects against unwanted activity. System services are programs that load automatically either as part of an application's startup process or the operating system startup process. Services are often a target for malware developers. If Webroot detects changes in the folders, it opens an alert.

Receiving and reviewing web threats (Mac)

On a Mac, the W button in the browser taskbar indicates that Web Threat protection is enabled.

When a threat is detected, Webroot alerts you to the suspicious nature of a website, such as whether it's a phishing attack, a key logger attack, a malicious attack, or something else.

When Webroot displays a Web threat message, stop and review the threat.

After reviewing the information on the page, you need to decide what to do about the threat.

- Click **Go back to safety** when you don't know the website, and don't want to expose your computer to malicious links or payloads. You are navigated away from the currently blocked content and moved to a safe blank page.
- Click **Request Review** when you know the website, are comfortable with the contents, and believe the classification of this URL should be changed to make sure the warning message does not display in future.
 - When you request a review, the dialog expands to display fields where you can enter comments and your email address. To contract the fields, click Request Review again.
 - For more information about the categorization of the website you would like to have changed, see the BrightCloud [URL Categorization Change Request](#).
 - When done, click **Submit**. Change requests are usually processed in 48-72 hours. If, after this period, you do not see the change you requested, [open a ticket with Webroot Support](#).
- Click **Unblock page and continue** when you know the website, are comfortable with the contents, and want to visit the site. When you select this option, Webroot bypasses this URL, and will not block it again.

Protecting personal information

Webroot protects you from identity theft and financial loss. It ensures that your sensitive data is protected, while safe-guarding you from keyloggers, screen-grabbers, phishing schemes, and other information stealing techniques.

Additional identity protection functionality can be purchased either as Webroot Premium with Allstate Identity Protection or as an add-on to Webroot AntiVirus, Webroot Internet Security Plus, or Webroot Internet Security Complete products. The Allstate Identity Protection features include:

- Up to \$550K in expense reimbursement
- Dark Web with social security trace
- Financial monitoring with proactive alerts
- Identity monitoring with Identity Health Status updates
- Bureau credit monitoring
- 24/7 US-based customer support with full-service remediation.

Protecting identity using shields (Windows)

Identity and phishing shields are available when using Webroot AntiVirus, Internet Security Plus, and Internet Security Complete.

Webroot Premium provides additional protections using Allstate Identity Protection.

1. From the main window, click the **Identity Protection** gear icon. The Online Protection pane displays.
 - We recommend that you keep Identity Shield and Phishing Shield enabled.
2. To disable a shield, turn the switch off. You may be prompted to confirm that you are a real user.

Protecting applications (Windows)

You can provide additional security for software applications that may contain confidential information, such as Instant Messaging clients, financial management software, or tax preparation software. By protecting these applications, you secure them against information-stealing Trojans like keyloggers, man-in-the-middle attacks, and clipboard stealers. You can add any applications to the Protected Applications list.

As you work on your computer, Webroot automatically adds web browsers to the Protected Applications list and assigns them to the protected status.

1. From the main window, click the **Identity Protection** gear icon.
2. Open the **Application Protection** tab.
3. For each application you want to modify, select one option:
 - **Protect** secures applications against information-stealing malware, but also allows full access to data on the system. When you run a protected application, the Webroot icon in the system tray displays a padlock.

- **Allow** does not secure applications against information-stealing malware, and allows full access to protected data on the system. Many applications unintentionally access protected screen contents or keyboard data without malicious intent when running in the background. If you trust an application that is currently marked as Deny, you can change it to Allow.
 - Applications flagged with **Deny** cannot view or capture protected data on the system but can otherwise run normally.
 - Turn the switches on or off to enable or disable each level of protection.
4. To include another application in this list, click **Add Application**, then select an executable file.

Security recommendations (Mac)

To keep your Mac safe from security threats and vulnerabilities, consider the following security recommendations outlined in this section when using Webroot SecureAnywhere for Mac. Please note that this list might not be fully comprehensive. You should consider your own specific requirements before making any modifications to your security settings.

To detect any active potential threats, it is a good practice to regularly click **Scan My Computer**.

Under **Mac Security**, turn on the **Realtime Shield** and **Web Threat Shield** switches.

Under **Identity Protection**, turn on the **Phishing Shield** switch.

To review and manage threats, as well as perform other security-related actions, on the main window, click the **Mac Security** gear icon. Consider the following security recommendations for each tab:

- **Threats** – Any detected threats will appear here. Take immediate action to prevent security issues.
- **Quarantine** – Items that are quarantined will appear here. Take appropriate action to protect your device. For more information, see *Quarantining items* on page 35.
- **Block / Allow Files** – You can define detection rules for an individual file using the settings on this tab. Only allow files that you trust. For more information, see *Blocking or allowing files* on page 39.

To adjust system-related settings, click the **Utilities** gear icon. Consider the following security recommendations for each tab:

- **System Control** – You can adjust the threat-detection settings for all programs and processes running on your computer. You can also terminate any untrusted processes, which might be necessary if a regular scan did not remove all traces of a malware program. For more information, see *Using system control tools* on page 46.
- **Reports** – To help Webroot researchers and customer support, you can **Save Scan Log** or **Submit a File** for review if you think that it might be malicious.
- **System Analyzer** – Run the System Analyzer regularly. The System Analyzer will provide recommendations on how you can keep your computer safe from security threats. For more information, see *Running System Analyzer (Webroot Internet Security Complete and above)*.
- **System Optimizer** – Using System Optimizer, you can protect your privacy by removing traces of your activity. For more information, see *Using System Optimizer* on page 48.

To review account-related settings, click the **My Account** gear icon. Consider the following security recommendations for each tab:

- **Keycode** – To ensure active security protection, upgrade/renew your keycode before it expires.
- **About SecureAnywhere** – Frequently check for software updates. Software releases include the latest features and security updates that patch various vulnerabilities to protect your device.

To configure more advanced settings, click the **Advanced Settings** button. For optimal security, consider the following recommended settings for each tab:

- **General**

- Select the **Automatically download and apply updates** check box. Failure to run on the latest version of the product might result in exploitations of the software.
- Clear the **Reduce resource use when intensive applications or games are detected** check box. With less resources dedicated to the agent, it might take longer to identify threats and react accordingly.
- Clear the **Allow SecureAnywhere to be shut down manually** check box. Attackers could potentially shut down the application manually without your consent, leaving your device open to security attacks.
- Clear the **Fade out warning messages automatically** check box so that you do not miss important messages related to the security of your device.
- Clear the **Save disk space by saving fewer details in log files** check box. Critical data that might help with troubleshooting could be contained in the log files.
- Select the **Hide the Webroot license keycode onscreen** check box. Exposing your keycode could put your device at risk.
- Select the **Operate background functions using fewer CPU resources** check box. This allows your computer to dedicate more resources to the agent, giving potential attackers less time for malicious activity.

- **Scan Settings**

- Select the **Automatically scan removable media** check box. Removable media, such as portable storage devices, could potentially contain malware or malicious content.
- Select the **Scan mounted drives** check box. Mounted drives could potentially contain malware or malicious content.
- Select the **Also scan for Windows threats** check box. There might be threats on your device that could potentially harm Windows devices.
- Clear the **Scan only Windows file extensions** check box as the scan might omit malicious files.
- To scan the entire system for threats, click the **Full scan** option rather than the **Quick scan** option.

- **Schedule**

- Select the **Enable Scheduled Scans** check box. Devices that are not scanned frequently might expose you to security threats.
- Select the **Enable Scheduled System Optimization** check box. This ensures that your device is running optimally.
- Select the **Run immediately at startup if SecureAnywhere misses a scheduled activity** check box to ensure that the agent does not miss any scheduled security checkup activities.

- Clear the **Don't perform scheduled activity when on battery power** check box to ensure that the agent does not miss any scheduled security checkup activities.
- Clear the **Don't perform scheduled activity when a full screen application or game is open** check box to ensure that the agent does not miss any scheduled security checkup activities.
- **Realtime Shield**
 - Select the **Automatically quarantine previously blocked files** check box.
 - Select the **Automatically block suspected threats when detected on execution** check box.
 - Select the **Scan files when written or modified** check box. New threats could be present within newly written or modified files.
 - Select the **Block threats automatically if no user is logged in** check box. Threats can run on your device even when a user is not logged in.
 - Select the **Secure keyboard entry mode** check box. This feature protects your inputs from potential unauthorized access and keyloggers.
 - Select the **Monitor services running on the system** check box to detect potential threats running on your system in real-time.
- **Web Threat Shield**
 - Select the **Enable Web Shield** check box to protect your device from web threats.
 - Select the **Block malicious websites** check box.
 - Select the **Enable realtime anti-phishing** check box.
 - Select the **Show safety ratings when using search engines** check box to protect yourself from potentially navigating to unsafe websites.
 - Select the **Monitor hosts file for changes** check box.
 - Take caution when editing a website override. If you add an incorrect override, you could be redirected to a malicious website.
- **Proxy Settings**
 - To prevent exposing your IP address to potential attackers, use a proxy server.
- **Secure Erase**
 - To prevent attackers from recovering deleted files, move the slider to **Maximum**.
- **System Optimizer**
 - Select the **Run system maintenance scripts** check box. Running these scripts is essential for optimal system performance.
 - Select the **Remove temporary files** check box. Removing temporary files prevents an attacker from stealing them.

- Select the **Remove cache files** check box to prevent the files from potentially becoming compromised and used for social engineering attacks.
- Select the **Remove log files** check box to prevent the files from potentially becoming compromised and used for social engineering attacks.
- Select the **Empty trash** check box. Confidential files in the trash could be compromised.
- Select the **Remove diagnostic files** check box to prevent the files from potentially becoming compromised and used for social engineering attacks.

Using firewall and web shield protection (Windows)

The Webroot firewall works with the Windows firewall to monitor data traffic coming both into and out of your computer ports. It looks for untrusted processes that try to connect to the internet and steal your personal information.

With both the Webroot and Windows firewall turned on, your data has complete inbound and outbound protection.

You should not turn off either the Windows firewall or the Webroot firewall. If they are disabled, your system is open to many types of threats whenever you connect to the internet or to a network. These firewalls can block malware, hacking attempts, and other online threats before they can cause damage to your system or compromise your security.

The Webroot firewall is pre-configured to filter traffic on your computer. It works in the background without disrupting your normal activities. If the firewall detects any unrecognized traffic, it opens an alert where you can block the traffic or allow it to proceed.

To view or disable the firewall:

The firewall status displays on the main page under **PC Security**.

- The green button indicates the firewall is enabled.
- To disable the firewall, click the white portion of the button.

Webroot displays a warning that your firewall is disabled and recommends you re-enable it.

Changing firewall and web shield settings

You can adjust how the firewall manages processes and whether it should open an alert when it does not recognize a process.

1. From the Webroot main page, click **Advanced Settings**. The **Settings** pane appears.
2. Open the **Firewall / Web Shield** tab, then select your options:
 - **Enable Web Shield** (recommended) turns the Web Shield on or off. This checkbox is selected by default.
 - **Activate browser extensions** (recommended) blocks malicious websites, realtime anti-phishing protection, and safety ratings when using search engines. Each function can be enabled or disabled separately using the controls below. When cleared, extensions are disabled and removed from each supported browser. This checkbox is selected by default.
 - **Block malicious websites** (recommended) checks any URLs and IPs you enter in a browser and creates a block page for known malicious sites. This checkbox is selected by default.
 - **Enable realtime anti-phishing** (recommended) protects against zero day phishing sites, which are sites that have not been seen before, and whose related viruses do not yet have a definition. This checkbox is selected by default.

- **Show safety ratings when using search engines** (recommended) annotates search results with an icon and tooltip that indicate how likely a site is malicious. This checkbox is selected by default.
- **Suppress the user's ability to bypass blocked websites (Business versions only)** (recommended) prevents users from bypassing blocked websites when a malicious website is detected. This checkbox is selected by default.
- **Suppress the user's ability to request website reviews (Business versions only)** (recommended) prevents users from submitting website reviews from the block page when a malicious website is detected. This checkbox is selected by default.

Select one of the following firewall options:

- **Allow all processes to connect to the Internet unless explicitly blocked** allows all processes to access the internet, unless the process is specifically blocked in the active connections list.
- **Warn if any new, untrusted processes connect to the Internet if the computer is infected** (recommended) warns if the computer is infected and any new untrusted process connects to the internet. This radio button is selected by default.
- **Warn if any new, untrusted process connects to the Internet** warns when any new untrusted process connects to the internet.
- **Warn if any process connects to the Internet unless explicitly allowed** warns if any process connects to the internet, unless the process is explicitly allowed in the active connections list.

3. When done, click **Save**.

Managing active connections

To protect your computer from hackers and other threats, the firewall monitors processes that attempt to access the internet. It also monitors the ports used for communicating with the internet. Advanced users have control over whether SecureAnywhere will allow or block certain processes and port communications.

1. From the main window, click the **PC Security** gear icon. The Scan & Shields tab appears.
2. Click **View Active Connections**. The Active Connections window displays any processes with currently active connections to the internet and the status of your system ports.
3. Use the radio buttons to allow or block specific processes.
4. Use the radio buttons to allow or close specific ports.
5. When done, click **Close**.

Quarantining items

As Webroot software scans and shields your computer, it removes all items associated with threats. It then disables their operation and moves them to a holding area, called quarantine. While in quarantine, threats can no longer harm your computer or steal your information. Once items are moved to quarantine, they are disabled and cannot harm your computer.

To conserve disk space, you can delete the items permanently.

If a program is not working correctly without the quarantined item, you can restore it. In rare cases, a piece of spyware is an integral part of a legitimate program and is required to run that program.

To manage a quarantined item:

1. From the main window, click the **PC Security** or **Mac Security** gear icon.
2. Open the **Quarantine** tab.
 - If the system has detected a threat that has not yet been quarantined, the Quarantine panel displays in red.
 - If the threat has been quarantined, the Quarantine panel displays in green, with the threat listed.

You can leave the item in quarantine, or you can delete or restore it.

- Click **Delete Permanently** to erase the item permanently. After erasing it, you can never restore the item.
- Click **Restore** to move the item back to its original location. When an item is restored, Webroot no longer detects it during scans. If you want the item to be detected again in the future, you can change its detection rules.

Blocking or allowing files

You can change the detection rules for an individual file using Block/Allow Files settings. These settings override Webroot default scanning and shielding behavior.

1. From the main window, click the **PC Security** or **Mac Security** gear icon.
2. Open the **Block/Allow** tab. Any items that were previously quarantined are listed in the pane.
 - Turn the switches on or off to enable or disable each level of protection.
3. To add files to be blocked or allowed, click **Add File** and browse to the file. You can also drag and drop a file from Explorer. The file name displays in the File column.
 - You can add executable files to this list (for example, .exe, .dll, .drv, .com).
 - If Webroot detects other copies of this file with different file names, it only displays the file name that it last detected.
4. For the file that you have just added, select any of the following radio buttons:
 - **Allow** ignores a file during scans and shielding.
 - **Block** stops a file from executing or being written to your computer.

- **Monitor** watches the program to determine if it is legitimate or related to malware.

5. To clear all files from the list, click **Remove All**.

Allowing scripts (Windows)

Typically, Webroot adds scripts to the Allow List for you when it restores a file from Quarantine. However, you can add allowed scripts yourself.

1. From the main window, click the **PC Security** gear icon.
2. Open the **Allow Scripts** tab. Any items that were restored from quarantine are listed in the pane.
3. Click **Allow a file**.
4. Browse to the script file you want to be allowed and click **Open**. The script is now listed on the **Allowed Scripts** tab.

To remove an allowed script:

1. From the main window, click the **PC Security** gear icon.
2. Open the **Allow Scripts** tab. Any items that were restored from quarantine are listed in the pane.
3. Right-click the entry for the script you want to remove then click **Remove this entry**.
4. To clear the entire list, click **Clear list** and confirm when prompted.

Using Antimalware tools (Windows)

Webroot provides tools for advanced Windows users to manually remove threats and perform actions associated with threat removal. You can:

- Target a file for scanning and removal, while also removing its associate registry links, if any.
- Launch a removal script with the assistance of Webroot Support.
- Reboot after removing a threat yourself or using a removal script.
- Reset your wallpaper, screen savers, and system policies.

To use antimalware tools:

1. From the main window, click the **Utilities** gear icon. The **Antimalware Tools** tab opens by default.
2. Under **Tools**, select any of the following options and click **Run Tools**.
 - Select **Reset desktop wallpaper** if your computer was recently infected with malware that changed your wallpaper.
 - Select **Reset screensaver** if your computer was recently infected with malware that changed your screensaver.
 - Select **Set system policies to defaults** if your computer was recently infected with malware that corrupted your system policies.
 - Select **Reboot into Safe Mode** if Webroot Support instructs you to reboot your computer in Safe

Mode.

- Select **Perform an immediate system reboot** to reboot your system after threat removal.
3. Under **Manual Threat Removal**, click **Select File** to scan a specific file for threats. In the Windows Explorer dialog, select a file and click **Open**. Webroot launches a scan. When done, reboot your system.
 4. Under **Removal Script**, click **Select Script** if Webroot support has sent you a removal script. Save the script to your computer and then open it when prompted.

Managing quarantined items

As Webroot software scans and shields your computer, it removes all items associated with threats. It then disables their operation and moves them to a holding area, called quarantine. While in quarantine, threats can no longer harm your computer or steal your information. Once items are moved to quarantine, they are disabled and cannot harm your computer.

To conserve disk space, you can delete the items permanently.

If a program is not working correctly without the quarantined item, you can restore it. In rare cases, a piece of spyware is an integral part of a legitimate program and is required to run that program.

To manage a quarantined item:

1. From the main window, click the **PC Security** or **Mac Security** gear icon.
2. Open the **Quarantine** tab.
 - If the system has detected a threat that has not yet been quarantined, the Quarantine panel displays in red.
 - If the threat has been quarantined, the Quarantine panel displays in green, with the threat listed.

You can leave the item in quarantine, or you can delete or restore it

- Click **Delete Permanently** to erase the item permanently. After erasing it, you can never restore the item.
- Click **Restore** to move the item back to its original location. When an item is restored, Webroot [edition] no longer detects it during scans. If you want the item to be detected again in the future, you can change its detection rules.

Blocking or allowing files

You can change the detection rules for an individual file using Block/Allow Files settings. These settings override Webroot software default scanning and shielding behavior.

To block or allow a file:

1. From the main window, click the **PC Security** or **Mac Security** gear icon.
2. Open the **Block/Allow** tab. Any items that were previously quarantined are listed in the pane.
 - The gray button indicates the level of protection is enabled.
 - The white button indicates the level of protection is disabled.
3. To add files to be blocked or allowed, click **Add File** and browse to the file. You can also drag and drop a file from Explorer. The file name displays in the File column.
 - You can add executable files to this list (for example, .exe, .dll, .drv, .com).
 - If Webroot software detects other copies of this file with different file names, it only displays the file name that it last detected.
4. For the file that you have just added, select any of the following radio buttons:
 - **Allow** ignores a file during scans and shielding
 - **Block** stops a file from executing or being written to your computer
 - **Monitor** watches the program to determine if it is legitimate or related to malware
5. To clear all files from the list, click **Remove All**.

Using antimalware tools (PC)

Webroot software provides tools for advanced users to manually remove threats and perform actions associated with threat removal. You can:

- Target a file for scanning and removal, while also removing its associate registry links, if any.
- Launch a removal script with the assistance of Webroot Support.
- Reboot after removing a threat yourself or using a removal script.
- Reset your wallpaper, screen savers, and system policies.

To use antimalware tools:

1. From the main window, click the **Utilities** gear icon. The **Antimalware Tools** tab opens by default.
2. Under **Tools**, select any of the following options and click **Run Tools**.
 - Select **Reset desktop wallpaper** if your computer was recently infected with malware that changed your wallpaper.
 - Select **Reset screensaver** if your computer was recently infected with malware that changed your screensaver.
 - Select **Set system policies to defaults** if your computer was recently infected with malware that corrupted your system policies.
 - Select **Reboot into Safe Mode** if Webroot Support instructs you to reboot your computer in Safe Mode.
 - Select **Perform an immediate system reboot** to reboot your system after threat removal.
3. Under **Manual Threat Removal**, click **Select File** to scan a specific file for threats. In the Windows Explorer dialog, select a file and click **Open**. Webroot software launches a scan. When done, reboot your system.
4. Under **Removal Script**, click **Select Script** if Webroot support has sent you a removal script. Save the script to your computer and then open it when prompted.

Setting preferences on your Windows computer

Setting installation preferences

You can change basic preferences for your Windows computer using the Install Settings panel.

1. From the Webroot main page, click **Advanced Settings**. The **Settings** pane opens, with **Install Settings** open by default.
 - **Automatically download and apply updates** downloads product updates automatically without alerting you.
 - **Show a shortcut on the desktop** provides double-click access to the main interface by placing the shortcut icon on your desktop. To add or remove the Webroot desktop icon from your desktop, you must enable it or disable it using this setting. You cannot add or delete it directly from the desktop.
 - **Show a system tray icon** provides quick access to Webroot functions by placing the Webroot icon on your desktop. You can double-click the icon to open the main interface or right-click to open a menu of common functions.
 - **Show a status notification screen on bootup** displays Webroot status when you boot up your computer.
 - **Show a Start Menu Shortcut** adds Webroot to the **Start Menu**.
 - **Allow SecureAnywhere** to be shut down manually allows the user to close Webroot.
2. When done, click **Save**

Setting access controls

If multiple people use your computer, you can set some permissions that provide or deny access to certain functions. These access controls also protect your computer from malware that tries to change settings in Webroot.

1. From the Webroot main page, click **Advanced Settings**. The **Settings** pane appears.
2. Open the **Access Control** tab, then select your options:
 - **Enable Password Protection** requires users enter a password for any configuration changes or critical actions. If this is selected, enter and repeat the password for this page.
 - **Protect against process termination** prevents users and programs from terminating any process.
 - **Protect against process tampering** prevents users and programs from modifying the behavior of any process.
 - **Require the completion of a CAPTCHA when changing critical features** opens a CAPTCHA dialog that requires you to enter text in a field before performing any critical actions such as changing shields, importing configuration settings, uninstalling the program, and shutting down the agent.

- **Require the completion of a CAPTCHA when changing any configuration option** opens a CAPTCHA dialog that requires you to enter text in a field before performing any configuration changes.
- **Allow users to remove threats without a password** allows you to remove threats, even if password protection is enabled.
- **Allow non-administrative users to modify configuration options** enables you to modify configuration options, whether you are logged in as an administrative user or not.
- **Allow uninstallation by non-administrative users** allows anyone to uninstall Webroot.
- **Allow access to advanced features by non-administrative users** allows anyone to access advanced features, whether logged in as an administrative user or not. Advanced features include all options in the Settings panels and the antimalware tools under quarantine.
- **Hide the keycode on screen** hides the license keycode when entered or displayed on screen.

3. When done, click **Save**.

Adjusting heuristics

With heuristics settings, you can adjust the level of threat analysis that Webroot performs when scanning your computer. Unless you are an advanced user and understand how changing settings impacts threat detection, we recommend you keep heuristics at their default setting.

1. From the Webroot main page, click **Advanced Settings**. The **Settings** pane appears.
2. Open the **Heuristics** tab, then select your options.
 - **Disable heuristics** (not recommended) turns off heuristic analysis.
 - **Enable standard heuristics** lowers your recommended level of security.
 - **Enable enhanced heuristics based on the behavior, origin, age, and popularity of files** (recommended) is the default security level.
 - **Enable maximum heuristics** could cause unexpected behavior, prevent the use of lesser-known applications, or prevent the installation of rarely-used programs. Use with caution.
 - **Warn when any new program executes that is not specifically whitelisted** Issues a warning for any program not specifically included in the Webroot database of applications that are known to be okay.
 - **Enable Webroot Infrared** enables Webroot to detect threats even when not running a scan a multi-layer defense technology that blocks threats very early in their lifecycle.

3. When you're done, click the **Save** button.

Defining proxy server settings

A proxy server is a computer system or router that acts as a relay between your computer and another server. If you use a proxy server to connect to the Internet, you must define the proxy connection data so Webroot can send updates to your computer.

For more information about your proxy environment, contact your proxy server's administrator.

1. From the Webroot main page, click **Advanced Settings**. The **Settings** pane appears.
2. Open the **Proxy** tab, then select your options:
 - From the **Proxy Type** drop-down menu, select **HTTP Proxy**.
 - From the **Authentication Method** drop-down menu, select one of these authentication methods:
 - Any authentication
 - Basic
 - Digest
 - Negotiate
 - NTLM
 - **Host** is the fully qualified domain name of the server (for example, proxy.company.com).
 - **Port** is the port number the server uses.
 - **Username** is the username of the server, if used.
 - **Password** is the password of the server, if used.
3. When done, click **Save**.

Exporting and importing settings

If you changed the settings configuration, you can back up those new settings using the export function. Making a backup of your configuration is helpful if you ever need to reinstall the software or transfer your configuration to another computer.

1. From the Webroot main page, click **Advanced Settings**. The **Settings** pane appears.
2. Open the **Import/Export** tab.
3. To transfer your settings to another computer:
 - a. Click **Export**
 - b. Enter a name for the file.
 - c. Click **Save**
4. To import settings from another installation:
 - a. Copy the file to be exported from the original machine.
 - b. Click **Import**
 - c. Select the file.
 - d. Click **Save**

Setting preferences on your Mac

Defining general preferences

1. From the Webroot main page, click **Advanced Settings**. The **Settings** pane appears.
2. Open the **General** tab, then select your options:
 - **Automatically download and apply updates** downloads product updates automatically without alerting you.
 - **Reduce resource use when intensive applications or games are detected** suppresses Webroot functions while you are gaming, watching videos, or using other intensive applications.
 - **Allow Webroot SecureAnywhere to be shut down manually** displays a Shutdown command in the system tray menu. When this option is cleared, the Shutdown command is removed from the menu.
 - **Fade out warning messages automatically** closes warning dialogs in the system tray after a few seconds. When this option is cleared, you must manually click on a message to close it.
 - **Save disk space by saving fewer details in log files** saves disk resources by saving only the last four log items.
 - **Hide the Webroot license keycode on screen** blocks your license keycode from displaying on the My Account panel.
 - **Operate background functions using fewer CPU resources** optimizes the system functions to maximize performance while doing other tasks.

Defining proxy server settings

A proxy server is a computer system or router that acts as a relay between your computer and another server. If you use a proxy server to connect to the Internet, you must define the proxy connection data so Webroot can send updates to your computer.

For more information about your proxy environment, contact your proxy server's administrator.

1. From the Webroot main page, click **Advanced Settings**. The **Settings** pane appears.
2. Open the **Proxy** tab, then select your options:
 - From the **Proxy Type** drop-down menu, select **HTTP Proxy**.
 - From the **Authentication Method** drop-down menu, select one of these authentication methods:
 - Any authentication
 - Basic
 - Digest
 - Negotiate
 - NTLM

- **Host** is the fully qualified domain name of the server (for example, proxy.company.com).
- **Port** is the port number the server uses.
- **Username** is the username of the server, if used.
- **Password** is the password of the server, if used.

3. When done, click **Save**.

Using system control tools

There are several tools you can use to monitor system activity:

Active process control

By controlling Active Processes, advanced users can adjust the threat-detection settings for all programs and processes running on your computer. You can also terminate any untrusted processes, which might be necessary if a regular scan did not remove all traces of a malware program.

1. From the main window, click the **Utilities** gear icon and open the **System Control** tab.
2. Click **Start**. The Active Processes panel displays all the processes running on your system.
3. For each process, select one of the following options:
 - **Allow** enables the process to run on your system.
 - **Monitor** watches the process and opens an alert on suspicious activity. Any process flagged as monitored displays at the top of the list.
 - **Block** prevents the process from running on your system. Do NOT block a process unless you have been advised to do so by Webroot Support.
4. To terminate all untrusted processes, click **Stop Untrusted Processes** (Windows) or **Kill Untrusted Processes** (Mac). Do not use this function unless directed by Webroot Support.
5. If you are working on a Windows computer and want details about a specific program, highlight the name, and click **More Info**. The **Events** pane displays. Open the **Details** tab to view additional information.
6. When done, click **Close**.

SafeStart Sandbox (Windows)

To check a program you believe is malware, advanced users can test the program in a protected area called the SafeStart Sandbox. This sandbox allows you to isolate the actions of the malware program and observe its behavior.

The SafeStart Sandbox is not intended for testing legitimate programs.

1. From the main window, click the **Utilities** gear icon and open the **System Control** tab.
2. Click **Run SafeStart Sandbox**. The **SafeStart Sandbox** window displays.
3. Select a file or type in the path and filename for the command you want to start.
4. Select or clear the options you want to control from the scrolling list.
5. When done, click **Start**.

System analyzer - Webroot Internet Security Complete and above

1. From the main window, click the **Utilities** gear icon and open the **System Control** tab.
2. Click **Run System Analyzer**. The analyzer launches, displaying a progress report. A list of results is displayed when the analysis is complete.
 - To view the **report summary**, click the button with three lines.
 - To view the **full report**, click the button with two columns of lines.
 - To **save** the report, click the button with the disk icon.

Using System Optimizer

As you work on your computer and browse the internet, you leave behind traces. These traces may be in the form of temporary files placed on your hard drive, lists of recently used files in programs, lists of recently visited websites, or cookies that websites placed on your hard drive. Anyone who has access to your computer can view what you have done and where you have been. Using System Optimizer, you can protect your privacy by removing traces of your activity, including the internet history, address bar history, internet temporary files (cache), and cookie files.

You can also use the System Optimizer to delete unnecessary files that Windows OS-X stores on your computer. Certain files can consume valuable space on your computer. Even with today's large hard drives, these unnecessary files can impair your computer's performance.

Optimizations remove unnecessary files and traces, not malware threats. Malware such as spyware and viruses are removed during scans. Think of the System Optimizer as the housekeeper for your computer, while the scanner serves as the security guard.

System Optimizer is available when you purchase Webroot Internet Security Complete or Webroot Premium packages.

Running System Optimizer

You can run System Optimizer manually at any time. You can also schedule the System Optimizer to run automatically on a pre-defined schedule.

To run System Optimizer manually on your Windows computer:

1. From the main window, click **Utilities** to expand the Utilities options.
2. Click **Optimize Now**. The system optimization progress pane opens. When optimization is complete, the system displays how much disk space was recovered and when the last optimization was completed.
3. To view more information and run a log about what was deleted, click the **Utilities** gear menu, select the **System Optimizer** tab, and click the **View Log** button.

To run System Optimizer manually on your Mac:

1. From the main window, click **Utilities** to expand the Utilities options.
2. Click **Optimize Now**. The system optimization progress pane opens. When optimization is complete, the system displays how much disk space was recovered and when the last optimization was completed.
3. To view more information, click the **Utilities** gear menu and select the **System Optimizer** tab.
 - **Optimize Now** runs an optimization immediately.
 - **Delete Files Security** ensures data in deleted files cannot be recovered.
 - **Verify Disk** confirms your operating system disk is operating without errors.
 - **Repair Disk** repairs any broken files that may be found

To schedule system optimization on your Windows computer:

1. From the Webroot main page, click **Advanced Settings**. The **Settings** pane appears.
2. Open the **Scheduler** tab, then open the **System Optimizer** tab.
3. Select **Enable scheduled optimization** to turn on automatic scheduling. If this box is cleared, all frequency settings are disabled.
4. If automatic scheduling is enabled:
 - Select **Optimize only on the following days** and select which day(s) of the week to run the optimization. If this checkbox is cleared, and automatic scheduling is enabled, system optimization runs every day.
 - Select **Optimize at specific time of day** to run optimizations at a certain time on the day(s) you have selected.
 - If you want to optimize multiple times per day, select **Optimize every** and enter the hourly interval between optimizations.
5. Select **Run on bootup if the system was off at the scheduled** to run the optimization next time the machine boots up if the optimization was missed while the system was off.
6. To cancel all changes and revert to the original settings, click **Reset to defaults**.
7. When done, click **Save**.

To schedule system optimization on your Mac:

1. From the Webroot main page, click **Advanced Settings**. The **Advanced Settings** pane appears.
2. Open the **Schedule** tab.
3. Select **Enable Scheduled System Optimization** to turn on scheduled system optimization.
 - Use the **Frequency** dropdown to select how often you want to run the system optimization.
 - Use the **Time** dropdown to select what time you want it to run.
4. Click **Reset Schedule** to revert to the original schedule.
5. Click **Reset system optimizer settings** to revert all options to the original default.
6. When done, click **Close**.

Changing System Optimizer settings

You can customize what the System Optimizer cleans up from your system by enabling or disabling the settings. The options on the settings list may change depending on what browsers and other applications you currently have installed.

To change System Optimizer settings on your Windows computer:

1. From the Webroot main page, click **Advanced Settings**. The **Settings** pane appears.
2. Open the **System Optimizer** tab, then select your options from the scrollable list:
 - **Clipboard contents** clears the contents from the clipboard, where Windows stores data when you use either the copy or cut function from any Windows program.
 - **Windows Temporary Folder** deletes all files and folders in the Windows temporary folder, but not files that are in use by an open program.
 - This folder is usually located at `C:\Windows\Temp`
 - Do not put any files here that you need to keep. The files in this folder can consume a lot of space on your hard drive.
 - **System Temporary folder** deletes all files and folders in the system temporary folder, but not files that are in use by an open program.
 - This folder is usually located at: `C:\Documents and Settings\[username]\Local Settings\Temp`
 - Do not put any files here that you need to keep. The files in this folder can consume a lot of space on your hard drive.
 - **Windows Update Temporary folder** deletes all files and subfolders in this folder, but not files that are in use by an open program. Windows uses these files when you run Windows Update. After you install the updates, you no longer need these files.
 - These files are located at `C:\Windows\Software\Distribution\Download`
 - Do not put any files here that you need to keep. The files in this folder can consume a lot of space on your hard drive.
 - **Windows Registry Streams** clears the history of recent changes you made to the Windows registry. This option does not delete the registration changes themselves.
 - **Default logon user history** deletes the Windows registry entry that stores the last name used to log on to your computer.
 - When the registry entry is deleted, you must enter your username each time you turn on or restart your computer.
 - This cleanup option does not affect computers that use the default Welcome screen.
 - **Memory dump files** deletes the memory dump file (`memory.dmp`) that Windows creates when you receive certain Windows errors. The file contains information about what happened when the error occurred.

- **CD burning storage folder** deletes the Windows project files, created when you use the Windows built-in function to copy files to a CD.
 - These project files are typically stored in one of the following directories:
 - C:\Documents and Settings\[username]\Local Settings\Application Data\Microsoft\CDBurning
 - C:\Users\[username]\AppData\Local\Microsoft\Windows\Burn\Burn
- **Flash Cookies** deletes bits of data created by Adobe Flash, which can be a privacy concern because they track user preferences.
 - Flash cookies are not actually cookies and are not controlled through the cookie privacy controls in a browser.
- **Recycle Bin** removes all files from your Recycle Bin, which contains files you have deleted using Windows Explorer.
 - When you delete a file, it is stored in the Recycle Bin until you empty it.
 - You should periodically empty the Recycle Bin to preserve valuable disk space on your computer.
- **Recent document history** clears the history of recently opened files, which is accessible from the Windows Start menu. The cleanup does not delete the actual files.
- **Start Menu click history** clears the history of shortcuts to programs that you recently opened using the Start menu.
- **Run history** clears the history of commands that you recently entered in the Run dialog, which is accessible from the Start menu.
 - After the cleanup, you may need to restart your computer to completely remove items from the Run dialog.
- **Search history** clears the history of files or other information that you searched for on your computer.
 - Your computer stores recent searches and displays them when you start entering a new search that starts with the same characters.
 - You access the search, also called find, from Windows Explorer or from your Start button.
 - The cleanup does not delete the actual files.
- **Start Menu order history** reverts the list of programs and documents in the Start menu back to alphabetical order, which is the default setting.
 - After you run the cleanup, you must reboot your system for the list to revert to alphabetical order.
- **Internet Explorer - Address bar history** removes the list of recently visited websites, which is stored as part of Internet Explorer's AutoComplete feature.
 - You see this list when you click the arrow following the Address drop-down list.

- **Internet Explorer Cookies** deletes all cookies from your computer.
 - Cookies are small files that store information about your interaction with a website and may reveal what sites you visited.
 - Be aware that if you remove all cookie files, some websites will not remember you. This means that you may need to re-enter passwords, shopping cart items, and other entries that these cookies stored.
- **Internet Explorer Temporary Internet Files** deletes copies of stored webpages that you visited recently.
 - This cache improves performance by helping webpages open faster the next time you visit them, but also reveals your visited sites to other people using your computer and can consume a lot of space on your hard drive.
- **Internet Explorer URL history** deletes the list of recently visited websites.
 - You see this list when you click History on the Internet Explorer toolbar.
 - While this history can be helpful, it also reveals your visited sites to other people using your computer.
- **Internet Explorer Setup Log** deletes log files created when you update Internet Explorer. After you install the updates, you no longer need these files.
- **Microsoft Download Folder** deletes the contents in the folder that stores files you last downloaded using Internet Explorer. After downloading, you no longer need these files unless you want to save downloaded software installation files.
- **MediaPlayer Bar History** removes the list of audio and video files recently opened with the media player in Internet Explorer, which plays audio and video files that you access on websites.
 - The cleanup does not delete the files, just the Windows memory that you opened them or searched for them.
- **Autocompleteform information** deletes data that Internet Explorer stores when you enter information into fields on websites.
 - This function is part of Internet Explorer's AutoComplete feature, which predicts a word or phrase based on the characters you begin to type, for example, your email address or password.
- **Clean index.dat (cleaned on reboot)** marks files in the index.dat file for deletion, then clears those files after you reboot the system.
 - The `index.dat` file is a growing Windows repository of web addresses, search queries, and recently opened files.
 - `Index.dat` functions like an active database. It is only cleaned after you reboot Windows.
 - This option works when you also select one or more of the following options:
 - Cookies

- Temporary Internet files
 - URL History
 - **Mozilla Firefox Cached Files** removes temporary files, such as recently visited webpages, stored by Mozilla Firefox.
 - **Google Chrome Cached Files** removes temporary files, such as recently visited webpages, stored by Google Chrome.
 - **Adobe Acrobat Pro Recent Files** Removes the cache of recently opened PDF files stored by Adobe Acrobat. This does not remove any actual PDF files.
 - **Adobe Acrobat Pro User Preferences** removes the cache of user preferences stored by Adobe Acrobat.
 - **Microsoft Management Console – Recent Files** removes the cache of user preferences stored by Adobe Acrobat.
 - **Windows DirectInput – Recent File List** removes the cache of recently opened files stored by Windows DirectInput.
 - **Windows WBEM Log Files** removes log files created by Windows WBEM.
3. To cancel all changes and revert to the original settings, click **Reset to defaults**.
 4. When done, click **Save**.

To change the System Optimizer settings on your Mac:

1. From the Webroot main page, click **Advanced Settings**. The **Settings** pane appears.
2. Open the **System Optimizer** tab, then select your options from the scrollable list:
 - **Run system maintenance scripts** runs a variety of scripts to update and maintain the system.
 - **Remove temporary files** removes temporary files.
 - **Remove cache files** removes files that have been cached.
 - **Remove log files** removes log files.
 - **Empty trash** completely removes items that have been deleted.
 - **Remove diagnostic files** removes files that were used in troubleshooting.
3. To cancel all changes and revert to the original settings, click **Reset system optimizer settings**.
4. When done, click **Close**.

Using Secure Erase

The Secure Erase feature allows you to specify how thoroughly the System Optimizer deletes files when it runs. When working on a Windows computer, you can also use this feature to enable a Secure Erase option on the Windows Explorer right-click menu, as described below.

Normally, when you delete a file, you are moving it to the **Recycle Bin** (Windows) or **Trash** (Mac), where anyone can access it. Even when you empty the **Recycle Bin** (Windows) or **Trash** (Mac), you are not actually deleting the files; you are only deleting the operating system's pointers to the files. The actual data still exists on your hard drive and, unless it is overwritten by other data, it could be resurrected using special recovery tools.

When working on a Windows computer, the setting on the Secure Erase panel can tell the System Optimizer and the Windows Explorer right-click menu option to permanently remove files in a shredding process, which overwrites the data with random characters. This shredding feature is a convenient way to make sure no one can ever access your files with a recovery tool.

To use Secure Erase in Windows Explorer:

1. From the Webroot main page, click **Advanced Settings**. The **Settings** pane appears.
2. Open the **Secure Erase** tab.
3. Select **Enable Windows Explorer right click secure file erasing**.
4. Open Windows Explorer.
5. Right-click on the file or folder you want to permanently erase.
6. From the drop-down menu, select **Permanently erase with Webroot**. After confirmation, the system deletes the file using the level of security you have configured.

To control the security level of Secure Erase:

1. From the Webroot main page, click **Advanced Settings**. The **Settings** pane appears.
2. Select **Secure Erase**, then move the slider to the right to select any of the following options:
 - **Normal** deletes the files without overwriting them.
 - **Medium** overwrites the data with three passes.
 - **Maximum** overwrites the data with seven passes.

These settings may directly impact how long it takes to run a system optimization.

3. When done, click **Save**.

Security for Chromebook™

Webroot® for Chromebook™ is available when you purchase Webroot® Security for Chromebook™ or Webroot Internet Security Plus, Webroot Internet Security Complete, or Webroot Premium packages.

For Chromebook system requirements, see <https://www.webroot.com/us/en/support/system-requirements>.

To install Webroot Security for Chromebook:

1. From the Google Play store, install the Webroot® for Chromebook app on your compatible ChromeOS device.
2. Select the Webroot app icon.
3. Select **Install**.
4. If prompted whether you want to install, select **Yes**. If you upgraded from a previous version select **Log In** and use your existing credentials.
5. If you are a new user, complete the form on the **Login** tab.
 - Enter your product keycode.
 - The keycode can be found in the receipt email for online purchases, or on a card for retail purchases and will look something like this: **WSAM-ZZZZ-0000-YYYY-1111**
 - If you don't have a keycode yet, select **Trial here** for temporary access.
 - Enter your email address or phone number.
 - Phone numbers are used solely as a username and to send requested information.
 - Create a password following the rules on the screen.
 - When done, select **Create Account**. The **Webroot Subscription Terms** screen appears.
 - Click **Solution Agreement**, read the terms, and select **AGREE** to continue.
 - On the Welcome screen, select **Go**.
 - When prompted, select **Allow** to enable Webroot to access and protect your device fully. Webroot recommends allowing accepting all permissions for scanning the entire device.

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

Once the scan is complete it will show a status:

- **Safe** means that your device 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:

- Select **SCAN NOW** to run a manual scan.
- **Secure Browser** lets you explore the Web safely using our secure browser.

- Enable **Webroot for Chrome** to monitor threats while using the Google Chrome browser using the Web Threat Shield extension.
- **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.

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.

Depending on your device, you can view Webroot® for Chromebook in 3 different layout formats:

- **Split** view is best suited for mobile devices.
- **Partial** view is best suited for tablets.
- **Full** view is best suited for computer devices.

To change your view, select the **Maximize** button in the Webroot Security for Chromebook toolbar. You can also drag the edges of the app to reize your view.

Using Secure Browser

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

Select 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. Secure Browser does not save your browsing history, cookies, site data or any information entered in web forms on private tabs.
- **History** opens a list of your browsing history. You can clear your web history on this screen.
- **Downloads** enables access to the files and articles previously downloaded.
- **Bookmarks** opens a list of favorite sites.
- **Recent tabs** opens a list of all recently closed webpages.
- **Share** enables you to share a loaded page with others.

Enabling Webroot for Chrome

The Web Threat Shield extension for Chrome provides additional security by checking websites for malicious or suspicious content and warning you before you visit them.

By default, Web Threat Shield for Chrome is disabled, as indicated by an “X” icon on the Dashboard screen.

To download and enable Web Threat Shield for Chrome:

1. From the Dashboard screen, select **Webroot for Chrome**.
2. Follow the steps shown on the **Secure your Chrome Browser** screen.

For more information on Web Threat Shield, see the [Web Threat Shield User Guide](#).

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 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 Dashboard, select **Password Manager**.
2. If you are a new user and do not have an account with **My Account**:
 - a. Select **Get keycode** and **Copy** an available keycode.
 - b. Select **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. Select **Open LastPass App**. The app opens in the Google Play store.
 - b. Select **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® for Chromebook 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 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 Dashboard, select **Activity Report** to view a summary of malware and website threats that Webroot® for Chromebook 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, select the **VIEW DETAILS** button.
2. To only display active threats, on the **Activity Details** page, turn on the **Show only active threats** switch.
3. Select 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® for Chromebook 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, select 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. Select the **Delete** button  next to a website from the list. Select **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.

Support

Resources

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

Submitting a file

If a file on your system is causing problems or if you know a file is safe and want it reclassified, you can send the file to Webroot support for analysis. You may also be asked to submit a file for troubleshooting.

1. From the main window, click the **Utilities** gear icon and open the **Reports** tab.
2. Click **Submit a file**. You are prompted to select a file and provide a reason for submitting it.
3. Click **Submit File**.

