Copyright

Copyright 2019 Webroot. All rights reserved.

WSA PC User Guide

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

Chapter 1: WSA PC User Guide .................................................................................. 1
  PC User Guide Overview ......................................................................................... 2

Chapter 2: Getting Started ....................................................................................... 3
  Installing SecureAnywhere ...................................................................................... 4
  System Requirements for Windows .......................................................................... 14
    Operating Systems ............................................................................................... 14
    RAM .................................................................................................................... 14
    Hard Disk Space ................................................................................................. 14
    Internet/Browser ................................................................................................. 14
  Creating Webroot Accounts ................................................................................... 15
  Using the SecureAnywhere Interface .................................................................... 21
  Using the System Tray ........................................................................................... 24
  Viewing Protection Statuses .................................................................................. 26

Chapter 3: Scanning For Malware .......................................................................... 27
  Running Scans ....................................................................................................... 28
    Running Scans Immediately ................................................................................ 29
  Managing Detected Threats .................................................................................... 31
  Changing Scan Schedules ..................................................................................... 32
  Changing Scan Settings ......................................................................................... 43
  Creating Custom Scans ......................................................................................... 50

Chapter 4: Shielding Your PC ............................................................................... 55
  PC Shields Overview .............................................................................................. 56
    Types of Shields .................................................................................................. 56
    Indicators Displayed With Query Results .......................................................... 57
    Infrared Shielding and Warning Messages ......................................................... 58
  Changing Shield Settings ....................................................................................... 61
  Managing Web Threats ......................................................................................... 71

Chapter 5: Using Firewall/WebShield Protection ..................................................... 74
  Managing Firewalls ............................................................................................... 75
  Changing Firewall/Web Shield Settings .............................................................. 78
  Managing Active Connections ............................................................................. 86

Chapter 6: Managing Quarantine ........................................................................... 92
  Managing Quarantined Items ............................................................................... 93
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blocking or Allowing Files</td>
<td>96</td>
</tr>
<tr>
<td>Removing Whitelist Entries</td>
<td>100</td>
</tr>
<tr>
<td>Adding Whitelisted Scripts</td>
<td>106</td>
</tr>
<tr>
<td>Using Antimalware Tools</td>
<td>111</td>
</tr>
<tr>
<td>Chapter 7: Using Identity Protection</td>
<td>115</td>
</tr>
<tr>
<td>Managing Identity Protection</td>
<td>116</td>
</tr>
<tr>
<td>Managing Protected Applications</td>
<td>119</td>
</tr>
<tr>
<td>Chapter 8: Managing Passwords</td>
<td>122</td>
</tr>
<tr>
<td>About Managing Passwords</td>
<td>123</td>
</tr>
<tr>
<td>Chapter 9: Managing Backup &amp; Sync</td>
<td>124</td>
</tr>
<tr>
<td>Backup &amp; Sync Overview</td>
<td>125</td>
</tr>
<tr>
<td>Backing Up Files</td>
<td>125</td>
</tr>
<tr>
<td>Downloading Backup &amp; Sync</td>
<td>126</td>
</tr>
<tr>
<td>Synchronizing Files</td>
<td>133</td>
</tr>
<tr>
<td>Adding Sync Folders</td>
<td>139</td>
</tr>
<tr>
<td>Syncing Folders Between Computers</td>
<td>143</td>
</tr>
<tr>
<td>Removing Synced Folders</td>
<td>146</td>
</tr>
<tr>
<td>Backing Up Files</td>
<td>149</td>
</tr>
<tr>
<td>Creating Backup Schedules</td>
<td>156</td>
</tr>
<tr>
<td>Checking File Statuses</td>
<td>165</td>
</tr>
<tr>
<td>Changing Backup &amp; Sync Settings</td>
<td>171</td>
</tr>
<tr>
<td>Adding More Storage</td>
<td>179</td>
</tr>
<tr>
<td>Chapter 10: Using System Optimizer</td>
<td>181</td>
</tr>
<tr>
<td>Changing System Optimizer Settings</td>
<td>182</td>
</tr>
<tr>
<td>Running Scheduled Optimizations</td>
<td>195</td>
</tr>
<tr>
<td>Running System Optimizer Manually</td>
<td>206</td>
</tr>
<tr>
<td>Using Secure Erase</td>
<td>211</td>
</tr>
<tr>
<td>Chapter 11: Using System Control</td>
<td>218</td>
</tr>
<tr>
<td>Running System Analyzer</td>
<td>219</td>
</tr>
<tr>
<td>Controlling Active Processes</td>
<td>223</td>
</tr>
<tr>
<td>Using the SafeStart Sandbox</td>
<td>227</td>
</tr>
<tr>
<td>Chapter 12: Using Reports and Viewers</td>
<td>232</td>
</tr>
<tr>
<td>Saving Scan Logs</td>
<td>233</td>
</tr>
<tr>
<td>Saving Threat Logs</td>
<td>237</td>
</tr>
<tr>
<td>Viewing Protection Statistics</td>
<td>241</td>
</tr>
</tbody>
</table>
Chapter 1: WSA PC User Guide

To get started using the PC User Guide, see the following topic:

<table>
<thead>
<tr>
<th>PC User Guide Overview</th>
<th>2</th>
</tr>
</thead>
</table>

- / -
PC User Guide Overview

Webroot SecureAnywhere™ delivers complete protection against viruses, spyware, and other online threats without slowing down PC performance or disrupting your normal activities. With its fast scans and threat removal, you can rest assured that malware is eliminated quickly and easily. SecureAnywhere gives you the freedom to surf, share, shop, and bank online — all with the confidence that your PC and your identity will be kept safe.

**Note:** This user guide describes the features of all SecureAnywhere editions: AntiVirus, Internet Security Plus, Internet Security Complete, or Endpoint. Your edition may not include all of the features.
Chapter 2: Getting Started

To get started using SecureAnywhere, see the following topics:

- Installing SecureAnywhere ................................................................. 4
- System Requirements for Windows ...................................................... 14
- Creating Webroot Accounts ................................................................. 15
- Using the SecureAnywhere Interface ................................................. 21
- Using the System Tray ......................................................................... 24
- Viewing Protection Statuses ................................................................. 26
Installing SecureAnywhere

SecureAnywhere is available in several editions, described in the table below. If you aren't certain which edition you purchased, do one of the following to determine which edition you have:

- If you purchased SecureAnywhere online, look at the email from Webroot.
- If you purchased SecureAnywhere from a store, look at the product packaging.

<table>
<thead>
<tr>
<th>EDITION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>AntiVirus</td>
<td>Provides protection from viruses, spyware, and phishing. Also includes a firewall and features for safe web searching.</td>
</tr>
<tr>
<td></td>
<td>This edition is available with:</td>
</tr>
<tr>
<td></td>
<td>• Licenses for 1 or 3 devices, PC or Mac</td>
</tr>
<tr>
<td></td>
<td>• Subscriptions for 1 or 2 years</td>
</tr>
<tr>
<td>Internet Security Plus</td>
<td>Provides all the features of the AntiVirus edition, plus a password management feature and protection for mobile devices.</td>
</tr>
<tr>
<td></td>
<td>This edition is available with:</td>
</tr>
<tr>
<td></td>
<td>• Licenses for 3 or 5 devices for PC, Mac, or mobile</td>
</tr>
<tr>
<td></td>
<td>• Subscriptions for 1 or 2 years</td>
</tr>
<tr>
<td>EDITION</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Complete</td>
<td>Provides all the features of the Internet Security Plus edition, along with a system cleaner that removes traces of Internet activity and a feature for backing up and synchronizing your data. This edition is available with:</td>
</tr>
<tr>
<td></td>
<td>• Licenses for 5 devices, PC, Mac, or mobile</td>
</tr>
<tr>
<td></td>
<td>• Subscriptions for 1, 2, or 3 years</td>
</tr>
<tr>
<td>Endpoint</td>
<td>Provides all the features of the AntiVirus edition, plus the system cleaner. This product is available only with the Endpoint Protection business version of SecureAnywhere.</td>
</tr>
</tbody>
</table>

You can install SecureAnywhere on a device with one of the following operating systems:
<table>
<thead>
<tr>
<th>OPERATING SYSTEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| PCs              | Compatible with the following operating systems:  
|                  |   • Windows 10 (32-bit and 64-bit)  
|                  |   • Windows 8 and 8.1 (32-bit and 64-bit)  
|                  |   • Windows 7 (32-bit and 64-bit), Windows 7 SP1 (32-bit and 64-bit)  
|                  |   • Windows Vista® (32-bit), Windows Vista SP1, SP2 (32-bit and 64-bit)  
|                  | Minimum system requirements:  
|                  |   • Intel Pentium®/Celeron® family, or AMD® K6™/Athlon®/AMD Duron™ family, or other compatible processor  
|                  |   • 128 MB RAM (minimum)  
|                  |   • 15 MB Hard Disk Space  
|                  | Internet access with one of the following browsers:  
|                  |   • Internet Explorer® 9.0 and higher (32-bit and 64-bit)  
|                  |   • Mozilla Firefox® (32-bit and 64-bit) - current and most recent versions  
|                  |   • Google Chrome® (32-bit and 64-bit) - current and most recent versions  

## OPERATING SYSTEM

<table>
<thead>
<tr>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>

### Macs

Compatible with the following operating systems:
- Mac OS® X v. 10.7 - Lion
- Mac OS X v. 10.8 - Mountain Lion

For more information on Mac requirements and installation, see the [WSA Mac User Guide](http://example.com). You will also need a separate installer file for Mac. You can download the file from: [http://anywhere.webrootcloudav.com/zerol/wsamac.dmg](http://anywhere.webrootcloudav.com/zerol/wsamac.dmg).

### Mobile

Compatible with the following operating systems:
- Android operating system version 4.0 (Ice Cream Sandwich) or higher
- Apple® devices with iOS version 4.2 or later, compatible with iPhone®, iPod touch®, and iPad® mobile digital devices

Compatible with the following devices:
- Android-compatible phones and tablets, including Kindle and Nook.

Mobile apps are available with the purchase of Internet Security Plus or Complete editions. You can also purchase them separately. To download and install mobile apps, see the [Download Instructions](http://example.com).

### To install SecureAnywhere:

2. Close all programs that are open on your computer.
3. Make sure you have the keycode, which is a 20-character license 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.

**Note:** The keycode is associated only with SecureAnywhere and 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.

4. Start the installation routine either from a CD or from a downloaded file:
   - If you are installing from a CD, insert the CD into the CD drive. An installation dialog opens where you can click a link to begin. If the installation dialog does not open, use Windows Explorer to navigate to your CD drive and double-click the software's installation file.
   - If you are installing from a downloaded file, navigate to where you downloaded the file in Windows Explorer and double-click the file to start the installation. Click **Run** to begin.

5. When the Webroot installer dialog displays, enter your keycode in the field.
   - If your keycode came in an email, you can cut and paste the code into this field.
   - If you don't know where to find your keycode, click the **Help me find my keycode** button.
6. As needed, click the **Installation Options** link at the bottom right to modify these settings.

A new window displays several options.
- Install location — Enter a different folder for the SecureAnywhere installation files.

- Create a desktop shortcut — To place a shortcut icon on your desktop for Webroot SecureAnywhere, select this checkbox.

- Randomize the installed filename to bypass certain infections — To change the Webroot installation filename to a random name, for example, QrXC251G.exe, select this checkbox. Doing so prevents malware from detecting and blocking Webroot's installation file.

- Protect the SecureAnywhere files, processes, and memory from modification — To enable self protection and the CAPTCHA prompts, select this checkbox. CAPTCHA requires that you read distorted text on the screen and enter the text in a field before performing any critical actions. For more information, see Setting Access Controls on page 270.

- Change Language — To change the language displayed in SecureAnywhere, click the Change Language button and select from the supported languages. You can only change the displayed language during installation, not after.

- Proxy Settings — To customize proxy settings, click the Proxy settings button. If you don't know what these settings should be, leave the default.
7. To return to the install screen when you're done, click the **Back** arrow to the left of the title bar.

8. At the main Installation dialog, click **Agree and Install** to begin installation.

9. If prompted, enter an email address and click the **Continue** button.

   SecureAnywhere begins scanning and configuring the application.

   If your system is clean, SecureAnywhere displays a status screen similar to the following example.
Note: If SecureAnywhere detects threats during the scan, it moves the items to quarantine where they are rendered inoperable and can no longer harm your system or steal data. For more information, see Managing Quarantined Items on page 93.

10. As needed, do either of the following:
   - To exit from SecureAnywhere, click X to close the window.
   - To view the main interface, click the Start using SecureAnywhere button.

   For more information, see Using the SecureAnywhere Interface on page 21.

   You do not need to do anything further, unless you want to adjust settings. After the initial scan, SecureAnywhere automatically scans your computer daily and constantly monitors activity as you surf the Internet. You do not need to launch a scan yourself or schedule scans. SecureAnywhere does all the work for you in the background.

11. To verify that SecureAnywhere is running, look for the Webroot icon in your system tray.
• If an important message requires your attention, the icon turns yellow or red.
• A dialog displays with additional information.
• If you purchased a multi-user license, you can install SecureAnywhere on other devices.

Note: To uninstall the program later, go to the Windows Start menu by clicking Start in the system tray, select All Programs > Webroot SecureAnywhere > Tools > Uninstall Webroot. At the prompt, click Yes to continue.
System Requirements for Windows

The following describes the system requirements for using SecureAnywhere functionality on Windows.

Operating Systems

- Windows 10 (32-bit and 64-bit).
- Windows 8 and 8.1 (32-bit and 64-bit).
- Windows 7 (32-bit and 64-bit), Windows 7 SP1 (32-bit and 64-bit).
- Windows Vista® (32-bit), Windows Vista SP1, SP2 (32-bit and 64-bit).

RAM

- Intel Pentium®/Celeron® family, or AMD® K6™/Athlon®/AMD Duron™ family, or other compatible processor.
- 128 MB RAM (minimum).
- 2 GB RAM recommended (minimum).

Hard Disk Space

- 15 MB

Internet/Browser

Internet access is required:

- Internet Explorer® 9.0 and higher (32-bit and 64-bit).
- Mozilla Firefox® (32-bit and 64-bit); current and most recent versions.
- Google Chrome® (32-bit and 64-bit); current and most recent versions.
Creating Webroot Accounts

By creating a Webroot account, you can view and manage the security status of your PC from any device with an Internet connection. This status information is available at the SecureAnywhere website, at my.webrootanywhere.com. From here, you can manage security across multiple devices from a single location, making it easier to determine if all your devices are protected or if any need attention.

For more information, see Creating Accounts in the WSA Management Website User Guide.

Before you begin, do the following:

- Have available the license keycode you used to install SecureAnywhere.
  
  To find your keycode, click the My Account gear icon, select the Keycode tab, and then click the Copy keycode to clipboard button. You can then paste your keycode in the keycode field when creating your account.

- Internet access is required; make sure you are using one of the following browsers:
  - Internet Explorer® 9.0 and higher (32-bit and 64-bit).
  - Mozilla Firefox® (32-bit and 64-bit) - current and most recent versions
  - Google Chrome® (32-bit and 64-bit) - current and most recent versions

  For more information, see System Requirements for Windows on page 14.

To create an account:

1. Do either of the following to access Webroot online:
   - From the main panel, select My Account > Access Web Console.
   - Open your browser and go to my.webrootanywhere.com.
2. Click the **Sign up now** button.

The Create an account window displays.
Enter your information using the following table.

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Webroot Product Keycode</td>
<td>Enter the license keycode you received when you purchased the product.</td>
</tr>
<tr>
<td></td>
<td>To find your keycode, go to My Account Keycode and click Copy keycode to clipboard, then paste it into this field.</td>
</tr>
<tr>
<td>Email Address</td>
<td>Enter your email address, which will also be used for your login name. Your account activation confirmation will be sent to this address.</td>
</tr>
<tr>
<td>Password</td>
<td>Your password must contain at least 6 alphabetic characters and 3 numeric characters.</td>
</tr>
<tr>
<td></td>
<td>Enter a minimum of 9 characters; your password can be longer than the required 9 characters.</td>
</tr>
<tr>
<td></td>
<td>Your password can include special characters, except for angle brackets: &lt; and &gt;.</td>
</tr>
<tr>
<td></td>
<td>Your password is case sensitive.</td>
</tr>
<tr>
<td></td>
<td>As you type, the Strength meter displays how secure your password is. For optimum security, you should make your password as strong as possible.</td>
</tr>
<tr>
<td>FIELD</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Your Personal Security Code</td>
<td>Enter a word or number, which will be used for an extra security step after you enter the password during login.</td>
</tr>
<tr>
<td></td>
<td>Use a code that is easy to remember, using a minimum of six characters.</td>
</tr>
<tr>
<td></td>
<td>Every time you log in, you must also enter two random characters of this code.</td>
</tr>
<tr>
<td></td>
<td>For example, if your code is 123456 and it prompts you for the fourth and sixth character, you would enter 4 and 6.</td>
</tr>
<tr>
<td></td>
<td>Your Personal Security Code is case sensitive.</td>
</tr>
<tr>
<td>Security Question</td>
<td>Select a question from the drop-down list. If you later forget the details of your login, you need to provide the answer to this question to retrieve the information.</td>
</tr>
<tr>
<td>Security Answer</td>
<td>Type an answer to your security question. The Security Answer is case-sensitive.</td>
</tr>
<tr>
<td>Please select your storage region</td>
<td>If your SecureAnywhere edition includes the Backup &amp; Sync feature, another field displays that prompts you to select a storage region. Select the region closest to you, which is U.S., Europe, or Japan.</td>
</tr>
</tbody>
</table>

4. After you enter account details, click the **Register Now** button. SecureAnywhere displays a confirmation message and sends an email to the address you specified. This may take a few minutes.

5. From your email system, open the confirmation email from Webroot and click the link. Your account will not be created until you click this link.
6. When SecureAnywhere prompts you to enter two characters from the Personal Security Code, type the requested characters and click the **Confirm Registration Now** button.

For example, if your code is 123456 and the system prompts you for the fourth and sixth characters, you would enter 4 and 6.

The SecureAnywhere website opens, similar to the following example. The options that display depend on which SecureAnywhere editions you purchased, for example, **AntiVirus**, **Internet Security Plus**, or **Complete**.

---

**Note:** When you install SecureAnywhere on multiple computers using the same multi-license keycode, their status information automatically displays in this website. For example, if you installed SecureAnywhere on five PCs, the PC Security panel displays 5 PCs Protected.
7. Click the **Go to PC Security** button to access status information for your computer.

For more information about using the website to manage your devices, see *Managing Your Account* in the *WSA Management Website User Guide*. 
Using the SecureAnywhere Interface

The SecureAnywhere interface provides access to all functions and settings.

**Note:** Some options may not be available in your edition depending on whether you purchased AntiVirus, Internet Security Plus, or Internet Security Complete.

To use the interface:

1. Do any of the following:
   - On your desktop, double-click the **Webroot** icon.
   - From the system tray menu, right-click on the **Webroot** icon, then select **View Status**.
   - If you cannot locate the system tray icon, from the Windows Start menu, select **All Programs** > **Webroot SecureAnywhere** > **Webroot SecureAnywhere**.
     
     The main interface displays with the Overview panel.
2. The following options are available:

- **Returning to main page** — No matter where you are within the interface, you can return to the main page by clicking on the SecureAnywhere logo in the upper left of the screen.

- **Protected panel** — This panel displays information about system scans and the status of your subscription to SecureAnywhere. You can manually scan the system any time by clicking the Scan My Computer button. The default scan schedule is set to run daily at the time you installed the software. To change the schedule, select Advanced Settings > Scheduler.

- **Message window** — The panel at the bottom left displays changing messages about virus alerts and other important information from Webroot.

- **SecureAnywhere features** — The right side of the main window provides links to SecureAnywhere features. To expand a section of the panel, click the name.

3. To view options related to each feature, click the relevant gear icon.

4. To return to the main window, click the Left arrow on the tab bar, or click the SecureAnywhere logo at the top left.
The green circle with a checkmark indicates that your license includes this feature. A plus sign on blue indicates a feature that is not installed.

5. The following table describes the options on the main interface.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Settings</td>
<td>Define how you want your installation of SecureAnywhere to operate.</td>
</tr>
<tr>
<td>PC Security</td>
<td>Change shield settings, and manage your firewall and quarantine.</td>
</tr>
<tr>
<td>Identity Protections</td>
<td>Protect sensitive data that may be exposed during your online transactions.</td>
</tr>
<tr>
<td>Backup &amp; Sync</td>
<td>Protect your files by uploading them to Webroot's online repository.</td>
</tr>
<tr>
<td>Password Manager</td>
<td>Create a secure password generator and profile storage facility. For more information, see Last Pass Overview.</td>
</tr>
<tr>
<td>Utilities</td>
<td>Use utilities to optimize your system, manage processes and files, view reports, and create a SafeStart Sandbox.</td>
</tr>
<tr>
<td>My Account</td>
<td>View your SecureAnywhere account information and access the web console.</td>
</tr>
<tr>
<td>Support/Community</td>
<td>Contact customer support or search for and discuss issues with the Webroot community.</td>
</tr>
</tbody>
</table>
Using the System Tray

The Webroot icon in the system tray, which is on the toolbar along the bottom of your screen, provides quick access to some common SecureAnywhere tasks. By right-clicking on the Webroot icon, you can view the system tray menu. This menu displays different selections, depending on the SecureAnywhere edition you purchased.

![System Tray Menu]

**Note:** If the icon does not display in the system tray, open the main interface, select Advanced Settings > Install Settings, and select the Show a system tray icon checkbox.

If a threat is detected, SecureAnywhere may also open an alert in the system tray. SecureAnywhere takes the appropriate action to quarantine the items. It may also prompt you to take action yourself.

![Threats Detected]

For more information, see Running Scans on page 28 and Managing Quarantined Items on page 93.
Viewing Protection Statuses

To indicate your computer's overall protection status, the system tray icon and the main interface change colors, as follows:

- **Green** — Your computer is secure.
- **Yellow** — One or more messages require your attention.
- **Red** — One or more critical items require your intervention.

To view details about the current status and settings, open the main interface by right-clicking on the Webroot icon from the system tray menu, then select **View Status**.
Chapter 3: Scanning For Malware

To learn more about scanning your PC for malware, see the following topics:

Running Scans ................................................................. 28
Managing Detected Threats .................................................. 31
Changing Scan Schedules ..................................................... 32
Changing Scan Settings ....................................................... 43
Creating Custom Scans ....................................................... 50
Running Scans

By default, scans run automatically every day, at about the same time you installed SecureAnywhere. For example, if you installed SecureAnywhere at 8 p.m., it always launches a scan around 8 p.m. Depending on the selections in your schedule, it will not disrupt your work, nor will it launch while you play games or watch a movie.

The default scan is referred to as a deep scan, which checks your entire computer for rootkits, trojans and other threats. During the scan, SecureAnywhere searches all areas where potential threats can hide, including drives, files, and system memory. It looks for items that match our threat definitions, match descriptions in our community database, or exhibit suspicious behavior. If SecureAnywhere detects a threat, it moves the item to quarantine where it is rendered inoperable. In quarantine, it can no longer harm your system or steal personal data.

If SecureAnywhere detects a potential threat, it displays an alert that prompts you to make a decision on whether you want to allow or block the item. If you aren't sure, we recommend that you block the item. For more information, see Managing Detected Threats on page 31.

This procedure describes the following:

- How to view the latest scan results.
- How to run a scan immediately.

Note: You can also run a scan from a remote location. For more information, see Scanning PCs Remotely in the WSA Management Website User Guide.

To view the latest scan results:

1. From the system tray, double-click the Webroot icon.

The main interface displays with the latest scan results in the main panel.
Running Scans Immediately

Although scans run automatically, you can launch a scan at any time. An immediate scan might be necessary if you surfed a high-risk website such as networking, music, or adult entertainment, downloaded high-risk items such as screen savers, music, or games, or accidentally clicked on a suspicious pop-up advertisement. You can run a scan in one of two ways:

- From the main panel.
- From the system tray.

**To use the main panel:**

1. Open SecureAnywhere.
2. On the main panel, click the **Scan My Computer** button.

**To use the system tray:**
1. From the system tray, right-click on the **Webroot** icon.

2. From the pop-up menu, select **Scan Now**.

If SecureAnywhere locates threats, it displays a window that guides you through the quarantine process. Items moved to quarantine are rendered inoperable. You do not need to delete them or do anything else. For more information, see *Managing Quarantined Items on page 93*. 
Managing Detected Threats

In most cases, SecureAnywhere 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 manage the item.

For more information, see Managing Quarantined Items on page 93.

To manage a detected threat:

1. Do one of the following:
   - If you recognize the filename, next to the item name, deselect the Remove checkbox.
     
     Do not restore the file unless you are absolutely sure that it is legitimate.
   - If you do not recognize the filename, select the Remove checkbox.

     SecureAnywhere moves the threat to quarantine, where it is rendered inoperable. You do not need to delete it or do anything else.

     After SecureAnywhere moves the threat to quarantine, it launches another scan to make sure your system is clean.
Changing Scan Schedules

SecureAnywhere launches scans automatically every day, at about the same time you installed the software. You can do any of the following:

- Change the scan schedule to run at different times.
- Change the scanning behavior.
- Turn off automatic scanning.

To change the scan schedule:

1. From the system tray, double-click the Webroot icon.

The main interface displays.
2. In the upper right corner, click the **Advanced Settings** button.

The Settings pane displays with the Install Settings sub-pane active.
3. Click **Scheduler**.

The Scheduler pane displays with the Scan Schedule sub-pane active.
Chapter 3: Scanning For Malware

- 37 -
4. To disable automatic scanning, deselect the **Enable scheduled scans** checkbox.

![Scheduling settings](image)

5. To change the scanning frequency, from the **Scan Frequency** drop-down menu, select one of the following:
   - **Scan every day**
   - **Scan on bootup scan**
   - **Scan every Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday**
Chapter 3: Scanning For Malware

Settings

Scan Schedule

Enable scheduled scans

Scan Frequency: Scan every day

Time: Scan at 1:00 pm when resources are available

- Scan on bootup if the computer is off at the scheduled time
- Hide the scan progress window
- Do not perform scheduled scans when on battery power
- Do not perform scheduled scans when a full screen application or game is open
- Randomize the time of scheduled scans up to one hour for faster scanning
- Perform a scheduled Quick Scan instead of a Deep Scan

Reset to defaults Save Cancel
6. To change the time of the scan, from the **Time** drop-down menu, select one of the time options.

If you select one of the when resources available options, the scan will launch when computer resources are available, generally within an hour of the time you select.
7. Select any of the following checkboxes:

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan on bootup if the computer is off at the scheduled time</td>
<td>Launches a scheduled scan within an hour after you turn on your computer. If you deselect this checkbox, SecureAnywhere ignores missed scans.</td>
</tr>
<tr>
<td>Hide the scan progress window</td>
<td>Runs scans silently in the background. If you deselect this checkbox, a window displays the scan progress.</td>
</tr>
<tr>
<td>Do not perform scheduled scans when on battery power</td>
<td>Helps conserve battery power. If you want SecureAnywhere to launch scheduled scans when you are on battery power, deselect this checkbox.</td>
</tr>
<tr>
<td>Do not perform scheduled scans when a full screen application or game is open</td>
<td>Ignores scheduled scans when you are viewing a full-screen application, such as a movie or a game. If you want to run scheduled scans anyway, deselect this checkbox.</td>
</tr>
<tr>
<td>Randomize the time of scheduled scans up to one hour for faster scanning</td>
<td>Determines the best time for scanning, based on available system resources, and runs the scan within an hour of the scheduled time. If you want to force the scan to run at the exact time scheduled, deselect this checkbox.</td>
</tr>
<tr>
<td>Perform a scheduled Quick Scan instead of a Deep Scan</td>
<td>Runs a quick scan of memory. We recommend that you keep this checkbox deselected, so that deep scans run for all types of malware in all locations.</td>
</tr>
</tbody>
</table>

8. When you're done, click Save.
Changing Scan Settings

Scan settings provide advanced users with a little more control over scanning functions.

To change scan settings:

1. From the system tray, double-click the Webroot icon.

The main interface displays.
2. In the upper right corner, click **Advanced Settings**.

The Settings pane displays with the Install Settings sub-pane active.
Chapter 3: Scanning For Malware

![Image of settings interface](image_url)
3. Select **Scan Settings**.

The Scan Settings pane displays.
4. Do either of the following:
   - To enable a setting, select the checkbox.
   - To disable a setting, deselect the checkbox.

The following table describes the settings:
<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable rootkit detection</td>
<td>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 that you keep this option selected. It adds only a small amount of time to the scan.</td>
</tr>
<tr>
<td>Scan the Master Boot Record</td>
<td>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 that you keep this option selected. It adds only a small amount of time to the scan.</td>
</tr>
<tr>
<td>Scan archived files</td>
<td>Scans compressed files in zip, rar, cab, and 7-zip archives.</td>
</tr>
<tr>
<td>Detect Potentially Unwanted Applications</td>
<td>Potentially unwanted applications are programs that aren't necessarily malicious but contain adware, toolbars, or other unwanted additions to your system.</td>
</tr>
<tr>
<td>Enable right-click scanning in Windows Explorer</td>
<td>Enables an option for running 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.</td>
</tr>
<tr>
<td>Allow files to be submitted for threat research</td>
<td>Allows potentially malicious files that our systems have not yet classified to be automatically uploaded to Webroot.</td>
</tr>
</tbody>
</table>
5. When you’re done, click the *Save* button.
Creating Custom Scans

You can create a customized scan that you run manually.

To create a custom scan:

1. From the system tray, double-click the **Webroot** icon.

The main interface displays.
2. Click the **PC Security** gear icon.

The Scan & Shields panel displays.
3. Click the **Custom Scan** button. The Customized Scan window displays.

   ![Customized Scan Window]

4. Select any of the following options:
   - To perform a surface scan of files in active memory, select the **Quick** radio button.
   - To perform a scan of local hard drives, select the **Full** radio button.
   - To perform a scan for rootkits, trojans, and other threats, select the **Deep** radio button.
   - To limit the scan to certain folders and files, click the **Custom** radio button, click the **Add File/Folder** button, and click the **Add** button to select the folders and files you want to scan.
   - To delete a file or folder, highlight it and click the **Remove** button.
5. When you’re done, click the **Start Scan** button.
Chapter 4: Shielding Your PC

To learn more about shielding your PC, see the following topics:

- PC Shields Overview ................................................................. 56
- Changing Shield Settings ....................................................... 61
- Managing Web Threats ............................................................ 71
PC Shields Overview

Shields constantly monitor activity while you surf the Internet and work on your computer, protecting your computer from malware and viruses. As you surf Internet sites, you could be targeted for a drive-by download, where an unwanted program launches and silently installs on your computer as you view pages. We recommend you keep all shields enabled. For more information, see Changing Shield Settings on page 61.

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. Do one of the following:
  - 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.

For more information on all of these options, see Managing Web Threats on page 71.

Types of Shields

SecureAnywhere includes the following types of shields:

- **Realtime Shield** — Monitors unknown programs to determine whether or not 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 to comprise the most accurate and comprehensive data available for classifying content and detecting malicious sites.
- **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. You do not need to configure any settings yourself unless you are an advanced user and would like to change the settings. For more information, see Changing Shield Settings on page 61.
Indicators Displayed With Query Results

When you run an Internet query such as a Google search, SecureAnywhere shields modify the results display with icons that give you safety information about each website returned as a result of the search. The icon displays to the left of each website name in the list of query results. The table below describes the meaning of each icon.

<table>
<thead>
<tr>
<th>ICON</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>These are well known sites with strong security practices, and 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.</td>
</tr>
<tr>
<td>✓</td>
<td>These are benign sites, and rarely exhibit characteristics that expose you to security risks. There is a low probability that you will be exposed to malicious links or payloads.</td>
</tr>
<tr>
<td>☹</td>
<td>These are 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.</td>
</tr>
<tr>
<td>!</td>
<td>These are suspicious sites. There is a higher than average probability that you will be exposed to malicious links or payloads.</td>
</tr>
<tr>
<td>!</td>
<td>These are high risk sites. There is a high probability that you will be exposed to malicious links or payloads.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>
Infrared Shielding and Warning Messages

SecureAnywhere might display warnings to you even if you are not currently running a scan. There could be an unauthorized access to your computer even if you are working elsewhere on your computer and not currently surfing the Internet.

In some cases, SecureAnywhere takes care of the problem automatically; for less severe cases, you are prompted to make a decision about whether or not you want to continue.

To make a determination about what level of warning to display, SecureAnywhere uses a technology called Infrared. Infrared is a multi-layer defense that blocks threats very early in their lifecycle. This is accomplished through a number of engines that work together, considering 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. 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 the vast majority users.

This risk assessment affects every protection module, from the firewall to behavior monitoring to realtime protection, and eventually to website blocking as well. The end result is a set of protections that is custom-tailored to the user's specific circumstances.

The following are samples of warnings that may display on your screen.
Low-Risk Warning

Medium-Risk Warning
High-Risk Warning

SecureAnywhere has identified threats on your system. It will be able to remove these threats without harming your files.

Remove Threat Infection
malware.exe in C:\windows\temp Win32.RHear.1

Cleanup later (not recommended) Continue
Changing Shield Settings

Shield settings provide advanced users with a little more control over shielding functions.

This topic contains the following procedures:

- [Disable Shield Settings](#)
- [Change Shield Settings](#)

**To disable shields:**

1. From the system tray, double-click the **Webroot** icon.

The main interface displays.
2. Click the **PC Security** gear icon.

The Scan & Shields panel displays.
Note the following:

- A green button next to the shield name indicates the shield is enabled. We recommend that you keep all shields enabled; however, you can disable a shield by clicking the green button.
- 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 enable the shield.

To change shield settings:

1. From the system tray, double-click the Webroot icon.
The main interface displays.
2. In the upper right corner, click the **Advanced Settings** button.

The Settings pane displays with the Install Settings sub-pane active.
WSA PC User Guide

Settings

- Automatically download and apply updates
- Show a shortcut on the desktop
- Show a system tray icon
- Show a status notification screen on bootup
- Show a Start Menu shortcut
- Allow SecureAnywhere to be shut down manually

Reset to defaults  Save  Cancel
3. Select **Shields**.

The Shield Settings panel displays.
4. Do either of the following:
   - To enable a setting, select the checkbox.
   - To disable a setting, deselect the checkbox.

The following table describes shield settings.
<table>
<thead>
<tr>
<th><strong>SETTING</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevent interruption by intelligently suppressing warnings</td>
<td>Uses built-in intelligence to suppress warnings if they will interfere with operations.</td>
</tr>
</tbody>
</table>
| Automatically quarantine previously blocked files          | Remembers how you responded to an alert, that is, whether you allowed a file or blocked it. It won’t prompt you again when it encounters the same file but will take the same action as before, including sending it to quarantine if appropriate.  
If you deselect this checkbox, SecureAnywhere opens an alert every time it encounters the file in the future. 
If you blocked a file and want it restored, you can retrieve it from quarantine. |
<p>| Check files for threats when written or modified           | Scans any new or modified files that you save to disk.                                                                                                                                                   |
|                                                           | If you deselect this checkbox, the system ignores new file installations; however, 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.                                                                                         |</p>
<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warn if untrusted programs make core system changes when offline</td>
<td>Displays a warning if an untrusted program tried to change core system settings while you were offline.</td>
</tr>
<tr>
<td>Verify the integrity of the operating system</td>
<td>Checks the operating system for problems.</td>
</tr>
<tr>
<td>Silently and automatically block untrusted access to user data</td>
<td>Automatically prevents unknown programs from accessing user data.</td>
</tr>
<tr>
<td>Allow trusted programs to access protected data without warning</td>
<td>Allows access to user data for trusted programs.</td>
</tr>
<tr>
<td>Prevent any program from modifying the HOSTs file</td>
<td>Prevents any program from modifying your HOSTs file.</td>
</tr>
</tbody>
</table>

5. When you’re done, click the **Save** button.
Managing Web Threats

When you are surfing the web and Webroot alerts you to the suspicious nature of a website, for example a phishing attack, a key logger attack, or a malicious attack, follow this procedure to manage the threat.

To manage a web threat:

1. If when you are surfing the web, and Webroot displays a message similar to the following, stop and review the threat.

![Image of a Webroot alert]

2. After you review information on the page, such as the URL or the type of threat that has been detected, click one of the following buttons:
   - Go back to safety — Click this button when you don't know the website, and do not want to expose your computer to malicious links or payloads. When you click this button, you are navigated away from the currently blocked content to a blank page to keep you safe.
   - Request Review — Click this button when you know the website, are comfortable with the contents, but believe the classification provided by Webroot of this URL needs to be changed to make sure the
warning message does not display in future.

When you click this button, the page expands to display a field where you can enter information about the site. Enter any comments, your email, and enter your email address, if you would like to receive follow-up regarding your request. For more information about the categorization of the website you would like to have changed, see URL Categorization Change Request.

When you're done, click the Submit button. Change requests are usually processed in 48-72 hours. If, after this period, you do not see the change you requested, you can open a ticket with Webroot Support.

Note: To close the Request Review area, click the Request Review button again.
- Unblock page and continue — Click this button 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.
Chapter 5: Using Firewall/WebShield Protection

To learn more about firewall and webshield protection, see the following topics:

- Managing Firewalls ................................................................. 75
- Changing Firewall /Web Shield Settings .................................. 78
- Managing Active Connections .................................................. 86
Managing Firewalls

The SecureAnywhere firewall monitors data traffic traveling out of your computer ports. It looks for untrusted processes that try to connect to the Internet and steal your personal information. It works with the Windows firewall, which monitors data traffic coming into your computer. With both the SecureAnywhere and Windows firewall turned on, your data has complete inbound and outbound protection.

You should not turn off either the Windows firewall or the SecureAnywhere 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 SecureAnywhere firewall is preconfigured 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:

1. From the system tray, double-click the Webroot icon.

The main interface displays.
- The firewall status displays on the main page under PC Security.
- The green button indicates the firewall is enabled.

2. To disable the firewall, click the white portion of the button. The system might prompt you to complete a CAPTCHA screen.

SecureAnywhere displays a warning that your firewall is disabled and recommends you re-enable it.
3. To enable the firewall, do one of the following:
   - Click the **Enable Now** button.
   - Click the red portion of the **Firewall** button.
Changing Firewall /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.

To change firewall / web shield settings:

1. From the system tray, double-click the Webroot icon.

The main interface displays.
2. Click **Advanced Settings**.

The Settings pane displays, with the Instal Settings pane active.
WSA PC User Guide
3. Select **Firewall / Web Shield**.

The Firewall / Web Shield pane displays.
4. Do either of the following:
   - To enable a setting, select the checkbox or radio button.
   - To disable a setting, deselect the checkbox or radio button.

The following table describes Web Shield settings.
## Chapter 5: Using Firewall/WebShield Protection

<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| Enable Web Shield        | Enable or disable the Web Shield.  
This checkbox is selected by default, which is the setting we recommend. |
| Activate browser extensions | Browser extensions provide blocking protection against malicious websites, realtime anti-phishing protection, and safety ratings when using search engines.  
Each function can be enabled or disabled separately using the individual controls for each function described below. To completely disable and remove extensions from each supported browser, deselect this checkbox.  
This checkbox is selected by default, which is the setting we recommend. |
| Block malicious websites | Any URLs and IPs you enter in a browser are checked and a block page is presented for known malicious sites.  
This checkbox is selected by default, which is the setting we recommend. |
| Enable realtime anti-phishing | Protects against zero day phishing sites. Zero day phishing sites are sites that have never been seen before, and their related viruses do not yet have a definition.  
This checkbox is selected by default, which is the setting we recommend. |
The following table describes Firewall settings.

<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| Show safety ratings when using search engines                          | Search result are annotated with an icon and tooltip, indicating the likelihood that a site is malicious.  
This checkbox is selected by default, which is the setting we recommend. |
| Enable Web Filtering driver                                            | Provides additional protection against malicious connections and in cases where the browser extensions are disabled.  
This checkbox is selected by default, which is the setting we recommend. |
| Suppress the user’s ability to bypass blocked websites (Business versions only) | Prevents users from bypassing blocked websites when a malicious website is detected.  
This checkbox is selected by default, which is the setting we recommend. |
| Suppress the user’s ability to request website reviews (Business versions only) | Prevents users from submitting website reviews from the block page when a malicious website is detected.  
This checkbox is selected by default, which is the setting we recommend. |
<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| Allow all processes to connect to the Internet unless explicitly blocked | Allows all processes, including potentially malicious connections to access the internet, unless the process is specifically blocked in the active connections list.  
For more information, see *Managing Active Connections on page 86*. |
| Warn if any new, untrusted processes connect to the Internet if the computer is infected | If the computer is infected and any new untrusted process connects to the internet, the system provides a warning. This radio button is selected by default, which is the setting we recommend. |
| Warn if any new, untrusted process connects to the Internet     | When any new untrusted process connects to the internet, the system displays a warning.                                                      |
| Warn if any process connects to the Internet unless explicitly allowed | If any process connects to the Internet, unless the process is explicitly allowed in the active connections list, the system displays a warning.  
For more information, see *Managing Active Connections on page 86*. |

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

To manage active connections:

1. From the system tray, double-click the Webroot icon.

The main interface displays.
2. Click the **PC Security** gear icon.

The Scan & Shields panel displays.
3. Click the **View Active Connections** button.

The Active Connections window displays any processes with currently active connections to the Internet and the status of your system ports.
4. Select a radio button to do any of the following:
   - To allow or block a process.
   - To allow or close a port.
5. When you're done, click the **Close** button.
Chapter 6: Managing Quarantine

To learn more about managing quarantine, see the following topics:

- Managing Quarantined Items ................................................................. 93
- Blocking or Allowing Files ................................................................. 96
- Removing Whitelist Entries ............................................................... 100
- Adding Whitelisted Scripts ............................................................... 106
- Using Antimalware Tools ................................................................. 111
Managing Quarantined Items

Once items are moved to quarantine, they are disabled and cannot harm your computer. However, you may want to delete or restore quarantined items in the following circumstances:

- 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 system tray, double-click the Webroot icon.

The main interface displays.
2. Click the **PC Security** gear icon.

3. Click the **Quarantine** tab.

   If the system has detected a threat that has not yet been quarantined, the Quarantine panel displays in red.

   ![Quarantine panel](image)

   If the threat has been quarantined, the Quarantine panel displays in green, with the threat listed.
4. You can leave the item in quarantine, or you can delete or restore it:
   - To delete the item permanently, highlight the item and click the **Delete Permanently** button. Be aware that after erasing it, you can never restore the item.
   - To move the item back to its original location, highlight the item and click the **Restore** button. When an item is restored, SecureAnywhere will no longer detect it during scans. If you want the item to be detected again in the future, you can change its detection rules. For more information see *Blocking or Allowing Files on page 96*. 
Blocking or Allowing Files

Block/Allow Files settings override SecureAnywhere’s default scanning and shielding behavior.

To control scanning and shielding behavior related to specific files, you can use the Block/Allow Files tab to specify one of the following actions:

- **Allow** — Ignore a file during scans and shielding.
- **Block** — Stop a file from executing or being written to your computer.
- **Monitor** — Watch the program to determine if it is legitimate or related to malware.

**To block or allow a file:**

1. From the system tray, double-click the **Webroot** icon.

   The main interface displays.
2. Click the **PC Security** gear icon.
3. Click the **Block/Allow Files** tab.

   Any items that were previously quarantined are listed in the pane.
Note the following:

- The gray button indicates the level or protection is enabled.
- The white button indicates the level of protection is disabled.

**Note:** You can add executable files to this list. Executable files typically have an extension of exe, dll, sys, drv, or com.

4. To add files, click the **Add File** button and browse to the file. You can also drag and drop a file from Explorer.

   The file name displays in the File column.
Note: If SecureAnywhere detected other copies of this file with different file names, it only displays the file name that it last detected.

5. For the file that you have just added, select any of the following radio buttons:
   - **Allow** — Ignore a file during scans and shielding.
   - **Block** — Stop a file from executing or being written to your computer.
   - **Monitor** — Watch the program to determine if it is legitimate or related to malware.

6. To clear all files from the list, click the Remove All button.
Removing Whitelist Entries

Follow this procedure to remove whitelisted entries. You can:

- Remove an individual script
- Remove multiple scripts

To remove a whitelist entry:

1. From the system tray, double-click the Webroot icon.

The main interface displays.

2. Click the PC Security gear icon.
3. Click the **Whitelisted Scripts** tab.

The Whitelisted Scripts tab displays.
4. For the script you want to remove, right-click the entry, then click **Remove this entry**.

![Image of Webroot SecureAnywhere interface](image)

The system removes the script.

**To remove multiple whitelist entries:**

1. From the system tray, double-click the **Webroot** icon.

![Image of Windows Start menu with Webroot icon](image)

The main interface displays.
2. Click the **PC Security** gear icon.

3. Click the **Whitelisted Scripts** tab.

   The Whitelisted Scripts tab displays.
4. Click the **Clear whitelist** button.

5. Click the **Yes** button on the confirmation message to confirm.

   The system removes the scripts.
Adding Whitelisted Scripts

Typically, Webroot whitelists scripts for you when it restores a file from Quarantine, as described in Managing Quarantined Items on page 93. However, you can add whitelist scripts yourself, as described in this procedure.

To add a whitelist script:

1. From the system tray, double-click the Webroot icon.

The main interface displays.

2. Click the PC Security gear icon.
3. Click the **Whitelisted Scripts** tab.

   The Whitelisted Scripts tab displays.
4. Click the **Whitelist a file** button.
5. On your computer, select the script you want to restore.

Webroot whitelists the script, which is now listed on the Whitelisted Scripts tab.
Using Antimalware Tools

SecureAnywhere provides tools for manually removing threats and for performing actions associated with threat removal. You should only use these tools if you are an advanced user. These tools allow you to:

- 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 system tray, double-click the Webroot icon.

![System tray icons](image)

The main interface displays.
WSA PC User Guide
2. Click the **Utilities** gear icon.

3. Click the **Antimalware Tools** tab.

Use any of the following options:

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tools</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Reset desktop wallpaper</strong></td>
<td>If your computer was recently infected with malware that changed your wallpaper, select the checkbox and click the <strong>Run Tools</strong> button.</td>
</tr>
<tr>
<td>OPTION</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Reset screensaver</td>
<td>If your computer was recently infected with malware that changed your screensaver, select the checkbox and click the <strong>Run Tools</strong> button.</td>
</tr>
<tr>
<td>Set system policies to</td>
<td>If your computer was recently infected with malware that corrupted your system policies, click the checkbox and click the <strong>Run Tools</strong> button.</td>
</tr>
<tr>
<td>defaults</td>
<td></td>
</tr>
<tr>
<td>Reboot into Safe Mode</td>
<td>If Webroot Support instructs you to reboot your computer in Safe Mode, click the checkbox and click the <strong>Run Tools</strong> button.</td>
</tr>
<tr>
<td>Perform an immediate</td>
<td>To reboot your system after threat removal, select the checkbox and click the <strong>Run Tools</strong> button.</td>
</tr>
<tr>
<td>system reboot</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Manual Threat Removal</td>
<td></td>
</tr>
<tr>
<td>Select File</td>
<td>To scan a specific file for threats, click the Select File button. In the Windows Explorer dialog, select a file and click the <strong>Open</strong> button. SecureAnywhere launches a scan. When it’s complete, reboot your system.</td>
</tr>
<tr>
<td>Removal Script</td>
<td></td>
</tr>
<tr>
<td>Select Script</td>
<td>After Webroot Support sends you a removal script, save it to your computer. Click the <strong>Select Script</strong> button to browse to and launch the tool.</td>
</tr>
</tbody>
</table>
Chapter 7: Using Identity Protection

To manage identity protection, see the following topics:

- Managing Identity Protection ................................................................. 116
- Managing Protected Applications .......................................................... 119
Managing Identity Protection

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

Follow this procedure to view and disable your identity protection status.

To manage identity protection:

1. From the system tray, double-click the Webroot icon.

The main interface displays.
2. Click the **Identity Protection** gear icon.

The Online Protection pane displays.
Identity Protection consists of two shields:

- Identity shield
- Phishing shield.

The green buttons indicate the shields are on. We recommend that you keep them enabled; however, you can disable them by clicking the green button. You may be prompted to type characters into a CAPTCHA window to confirm you are a real user.
Managing Protected Applications

You can provide additional security for software applications that may contain confidential information, such as Instant Messaging clients 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 and assign them to one of the following protection levels:

- **Protect** — Protected applications are secured against information-stealing malware, but also have full access to data on the system. You might want to add financial management software to the category. When you run a protected application, the Webroot icon in the system tray displays a padlock:

- **Allow** — Allowed applications are not secured against information-stealing malware, and also have 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.

- **Deny** — Denied applications cannot view or capture protected data on the system, but can otherwise run normally.

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

**To manage protected applications:**

1. From the system tray, double-click the Webroot icon.

   ![Webroot icons]

   The main interface displays.
SecureAnywhere is protecting your computer. No active threats have been detected.

Stay informed. Join the discussion.

For security news, product questions, and expert advice, please visit the Webroot Community.
2. Click the **Identity Protection** gear icon.

3. Click the **Application Protection** tab.

4. In the row for the application you want to modify, click one of the following radio buttons:
   - **Protect**
   - **Allow**
   - **Deny**

   Note the following:
   - The gray button indicates the level or protection is enabled.
   - The white button indicates the level of protection is disabled.

5. To include another application in this list, click **Add Application**, then select an executable file.
Chapter 8: Managing Passwords

To learn more about password management, see the following topic:

About Managing Passwords ................................................................. 123
About Managing Passwords

If you purchased a SecureAnywhere edition that includes password management, you can use an additional component for managing passwords and profiles online.

Once you define your personal information and passwords in SecureAnywhere, you can automatically log in to websites or populate fields in web forms, saving you the hassle of manually entering your personal data and credit card numbers.

All Password Management features are managed from your account's web interface. You can access that page by clicking the Manage Passwords button under Password Manager. For step-by-step instructions covering all features, see Working With Passwords in the Management Website User Guide.

For more information about LastPass, see the LastPass Reference Guide.
Chapter 9: Managing Backup & Sync

To learn more about Backup & Sync, see the following topics:

- Backup & Sync Overview ................................................................. 125
- Downloading Backup & Sync ............................................................ 126
- Synchronizing Files ................................................................. 133
- Adding Sync Folders ................................................................. 139
- Syncing Folders Between Computers ............................................. 143
- Removing Synced Folders ......................................................... 146
- Backing Up Files ................................................................. 149
- Creating Backup Schedules ...................................................... 156
- Checking File Statuses ................................................................. 165
- Changing Backup & Sync Settings .............................................. 171
- Adding More Storage ................................................................. 179
Backup & Sync Overview

You can use Webroot's preconfigured folder called the Webroot Anywhere folder or you can create your own sync folders. Any files you place in these folders are automatically synchronized to any other computers with shared folders associated with your account, and to mobile devices with the Backup & Sync app installed.

SecureAnywhere constantly monitors the Anywhere folder and other sync folders. If the system detects a change, such as an edited file, a new file, or a deleted file, it immediately makes the same change to your online backups, to shared folders on other computers, and to mobile devices with the Backup & Sync app installed. If you are working offline, SecureAnywhere automatically picks up changes the next time you connect to the Internet.

If SecureAnywhere detects an edited file, it does not overwrite the original version stored in your account. Instead, it uploads the latest version and makes a copy of the original file. If necessary, you can revert back to previous versions, up to five. If you save changes a sixth time, your most recent version is saved and the oldest version is removed.

- For more information, see Backup & Sync Overview in the WSA Management Website User Guide.
- For more information on the preconfigured Anywhere folder, see Synchronizing Files on page 133.
- For more information on how to create sync folders of your own, see Adding Sync Folders on page 139.

Backing Up Files

Instead of synchronizing files with multiple devices, you can simply back them up. For example, you may want to back up tax returns, old photos, and a scanned copy of your passport. These types of documents won’t change and don’t need to be kept in synchronization with other computers. For more information on backups, see Backing Up Files on page 149.
Downloading Backup & Sync

Downloading the component is the first step in using Backup & Sync. This procedure contains the instructions on how to do that. Once you have downloaded Backup & Sync, you must:

- Configure which folders and files you want synchronized. For more information, see Synchronizing Files on page 133.
- Configure which folders and files you want backed up. For more information, see Backing Up Files on page 149.

**Note:** Once installed, Backup & Sync functions are enabled by default. However, nothing is synchronized or backed up until you specify which folders and files you want included.

To download Backup & Sync:

1. If you have not yet created a Webroot account, create one. For more information, see Creating Webroot Accounts on page 15.

   This is where you will access your files stored in the cloud.

2. From the system tray, double-click the **Webroot** icon.

   ![Icons](image)

   The main interface displays.
Chapter 9: Managing Backup & Sync

![Webroot SecureAnywhere interface showing protected status and scan results]

Protected

SecureAnywhere is protecting your computer. No active threats have been detected.

- Last scan: < 5 minutes ago
- Last scan duration: 40 seconds
- Next scan: Starts in 3 hours
- Total scans: 24
- Threats removed: 55
- Active threats: 0
- Subscription: 746 days

Stay informed. Join the discussion.

For security news, product questions, and expert advice, please visit the Webroot Community.

Read Now
3. Click **Backup & Sync**, which displays a plus sign next to it.

The system displays the Log In window.
4. If prompted, enter your Webroot account credentials.
5. Click the **Log In** button.

The system validates your Backup & Sync license and downloads the software.

6. When the setup completes, click the **Start using Backup & Sync** button.

   For subsequent visits, you can access Backup & Sync by clicking the **Backup & Sync** gear icon from the main panel.
The Backup & Sync panel displays.

- By default, synchronization of the Anywhere folder is turned on, but you must first select files for synchronization. For more information, see *Synchronizing Files on page 133*.
- Backups are also turned on by default, but you must first select folders and files for backup. For more information, see *Backing Up Files on page 149*. 

-132-
Synchronizing Files

Webroot includes one preconfigured folder for synchronization, called the Webroot Anywhere folder. It resides under your personal User folder in Windows.

Any files you put in the Webroot Anywhere folder are automatically synchronized with your online account at my.webrootanywhere.com and with shared folders on other computers or mobile devices in your account.

To synchronize files:

1. From the system tray, double-click the Webroot icon.

The main interface displays.
2. Click the **Backup & Sync** gear icon.

3. Click the **Backup & Sync** tab.
4. Click the **Open Anywhere Folder** button.

![Webroot SecureAnywhere Interface](image)

Windows Explorer opens to the Webroot Anywhere folder.

5. In Windows Explorer, copy files or folders into the Webroot Anywhere folder.
   - The files are instantly synchronized to your online SecureAnywhere account and to other shared folders on other computers, if you configured them.
   - In Windows Explorer, icons next to the files and folders indicate the status of the synchronization.
Note: Some files may fail to synchronize because their storage size is larger than the upload limit. You can adjust the limit up to 2000 MB in the Do not upload files larger than field in the Backup & Sync Settings panel. For more information, see Changing Backup & Sync Settings on page 171.

6. Do either of the following:
   - To see the amount of used storage in your account, look at the Storage indicator in the Backup & Sync panel.
   - To check that your files were successfully copied, access your online account by clicking the Visit the Webroot Cloud button.
7. When your browser opens to my.webrootanywhere.com, log in to your account, click the Go to Backup & Sync tab, then select the Anywhere panel.
For more information about using Backup & Sync in your online account, see the SecureAnywhere Management Website User’s Guide.
Adding Sync Folders

Webroot already configured one synchronization folder called the Webroot Anywhere folder. However, you can designate more folders for synchronization if you like. For more information, see *Synchronizing Files on page 133.*

To add a sync folder:

1. From the system tray, double-click the Webroot icon.

The main interface displays.
2. Click the **Backup & Sync** gear icon.

3. Click the **Folders** tab.
4. At the bottom of the panel, click the **Add Folder** button.

5. Browse to and select the folder you want to add and click the **OK** button.

6. Click the **Sync** radio button to indicate you want this folder to be synchronized.

7. Optionally, give the folder a new name that will be used in your Synchronization account.

8. Click the **Save** button. The system adds this folder to your account.

9. To change the settings for the folder, do any of the following:
   - To keep the folder in your Synchronization account but disable synchronization, select the **Enabled** checkbox.
   - To open the folder, double-click the folder name.
   - To remove the folder, click the red **Remove** button.
Syncing Folders Between Computers

If you installed SecureAnywhere on multiple computers, you can create shared, synchronized folders between them. Whenever you update data in one of these shared folders, for example, when you add, edit, move, or delete files, SecureAnywhere automatically makes the same changes in your online account and to all shared folders. This automatic synchronization can be beneficial when you frequently use multiple computers and need access to the most recent files.

Unless you disable synchronization on the Webroot Anywhere folder, it is always synchronized with all computers on the same SecureAnywhere account. The procedure below describes how to create additional synchronization folders.

**Note:** Be aware that when you make changes to a folder on one computer, the changes are propagated across the synchronized folders on all computers in the account. For example, if you delete a synchronized folder from one computer, it is removed from all the computers. However, you can still access a deleted folder or file from the Recycle Bin in your SecureAnywhere account. For more information, see [Restoring Files From the Recycle Bin](#) in the [WSA Management Website User Guide](#).

To sync folders between computers:

1. Configure a new sync folder on the first computer. For more information, see [Adding Sync Folders on page 139](#).
2. On the second computer, if you have not already done so, follow the [Downloading Backup & Sync on page 126](#) procedure to install Backup & Sync.
3. Log in with the same online account you created for the first computer.
   The new computer will be added to that account.

   **Note:** Your license must include multiple devices.

When you log in on the second computer, the Backup & Sync tab displays automatically.

4. While on the second computer, in the Folders tab of Backup & Sync, click the **Link to an existing Cloud Folder** button.
The Link to an Existing Cloud Folder window displays, listing all the synchronized folders that have been added to this account.

5. Highlight the folder you want to synchronize with the second computer.
6. Click **Browse** and select the local folder you want linked to the selected folder. The folder names do not
have to be the same.

7. Click the **Save** button.

The folder you selected is synchronized and now displays in the Backup & Sync panel.
Removing Synced Folders

You can stop synchronizing the contents in a folder either by disabling it from the automatic synchronization process or removing the folder from the list.

**Note:** Disabling folder synchronization or deleting a folder from the list does not delete it from your computer.

To remove a synced folder:

1. From the system tray, double-click the **Webroot** icon.

   The main interface displays.
2. Click the **Backup & Sync** gear icon.
3. Click the **Folders** tab.
4. Locate the folder you want to remove from synchronization and do either of the following:
   - Deselect the **Enabled** checkbox
   - Click the **Remove** radio button.

**Note:** In the Folders panel, you can disable the Anywhere folder but cannot remove it.
**Backing Up Files**

Instead of synchronizing files, you can archive them instead. For example, you may want to back up tax returns, old photos, and a scanned copy of your passport. These types of documents won't change and don't need to be kept in synchronization with other computers. Your backed-up files are uploaded to secure Webroot servers, which are accessible from your SecureAnywhere account.

*Note:* Once installed, Backup & Sync functions are enabled by default. However, your folders and files are not synchronized or backed up until you specify which folders and files you want included.

Use this procedure to run a manual backup. To create an automatic backup schedule, follow the *Creating Backup Schedules on page 156* procedure.

**To back up files:**

1. From the system tray, double-click the Webroot icon.

The main interface displays.
2. Click the **Backup & Sync** gear icon.

3. Click the **Folders** tab.

4. Click the **Add Folder** button.

   The Add Folder window displays.
5. Click the **Browse** button and select the folder you want to back up.

6. Under Folder Type, select the **Backup** radio button, and click the **Save** button.

The system displays the Change Backup Filter pane.
7. Set backup filter settings using the following table.

The default setting in the window is to back up all files in the selected folder.

<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory</td>
<td>To change the directory you already selected, use the <strong>Browse</strong> button to select a new directory.</td>
</tr>
<tr>
<td>Name</td>
<td>The default is the name of the directory you selected; you can change this name.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>File types selected</td>
<td>This field determines which files are selected for backup from the directory. The default, *, selects all files. To narrow the backup selection criteria to certain file types, click the Change button. When the Filter Settings window displays, enable one or more selections. You can also enable Custom filter and type in a comma-separated list of filters. You can specify strings or partial strings; for example, you could specify <em>RPT</em>.doc as a custom backup string. Click the Save button to save your filters.</td>
</tr>
<tr>
<td>Back up files from subdirectories</td>
<td>Select this checkbox if you want all subdirectories backed up as well.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Exclude files from backup that match this filter</td>
<td>Select this checkbox if you want the selections made in the Filter Settings panel to exclude files rather than include them.</td>
</tr>
</tbody>
</table>

8. To run a backup immediately, click the Run Backup Now button.

   On the Folders tab, the Shared Across column indicates that this is a backup folder.

9. Do either of the following:
   - To edit the filter, click the Edit gear icon, make your changes and click the Save button.
   - To delete this filter, click the Remove button.
Creating Backup Schedules

You can change the automatic backup schedule or turn off automatic backups. The default backup schedule is every day at 9 o’clock a.m.

To create a backup schedule:

1. From the system tray, double-click the Webroot icon.

The main interface displays.
2. From the main panel, select **Advanced Settings**.

The Settings panel displays with the Install Settings sub-pane active.
WSA PC User Guide

Settings

- Install Settings
  - Automatically download and apply updates
  - Show a shortcut on the desktop
  - Show a system tray icon
  - Show a status notification screen on boot up
  - Show a Start Menu shortcut
  - Allow SecureAnywhere to be shut down manually

- Scheduler

- Scan Settings

- Shields

- Firewall / Web Shield

- Access Control

- Proxy

- Heuristics

- Import / Export

- System Optimizer

- Secure Erase

Reset to defaults

Save

Cancel
3. Select **Scheduler**.

The Scheduler pane displays with the Scan Schedule sub-pane active.
4. Click the **Backup** tab.

The Backup Schedule pane displays.
5. Set up your backup schedule based on the information in the following table.

<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable scheduled archiving</td>
<td>Do either of the following:</td>
</tr>
<tr>
<td></td>
<td>• To enable automatic backups, select the checkbox</td>
</tr>
<tr>
<td></td>
<td>• To disable automatic backups, deselect the checkbox</td>
</tr>
<tr>
<td>Back up only on the following days</td>
<td>The default backup schedule is every day. If you select the Back up only on the following days checkbox and select one or more days, the backup will only be performed on those days.</td>
</tr>
<tr>
<td>Back up at specific time of day</td>
<td>To set a specific time for back ups, select the radio button and select the time.</td>
</tr>
<tr>
<td>Back up every X hours</td>
<td>To set repeating back ups at intervals less than 24 hours, select the radio button and enter a number for the hourly interval. For example, to run back ups every 8 hours, select 8.</td>
</tr>
<tr>
<td>Run immediately if Backup was inactive at the scheduled time</td>
<td>To run a backup immediately after a missed scheduled backup, select the checkbox.</td>
</tr>
<tr>
<td></td>
<td>A backup might be skipped if you disabled backups, if you shut down SecureAnywhere, or if you logged off your computer.</td>
</tr>
<tr>
<td>Randomize the time of a scheduled archive up to one hour</td>
<td>To run a scheduled backup within an hour of the scheduled time, based on resource availability, select the checkbox This selection makes better use of network resources.</td>
</tr>
</tbody>
</table>
6. When you're done, click the Save button.
Checking File Statuses

You can check the status of synchronization and backup from the main interface or from your account on the SecureAnywhere website.

Note: In Windows Explorer, icons indicate backup status, as they do for synchronized files. For more information, see Synchronizing Files on page 133.

This topic contains the following procedures:

- Checking File Statuses.
- Checking File Statuses From the SecureAnywhere Website.

To check file status:

1. From the system tray, double-click the Webroot icon.

The main interface displays.
WSA PC User Guide
2. Click the **Backup & Sync** gear icon.

3. Click the **File Transfers** tab.

The system displays any backups or synchronizations that are in progress, including the percent complete.

**To check file status from the SecureAnywhere website:**

1. Log in to the SecureAnywhere website at [my.webrootanywhere.com](http://my.webrootanywhere.com).
2. Click **Backup & Sync > Visit the Webroot Cloud**.

   The browser interface to your online account opens.

3. If prompted, log in, and then click the **Backup & Sync** tab.
   - The Files and Folders tab lists storage folders on the left with their contents in the right panel.
   - The Up and Down arrow icons next to the folder name indicates this is a synchronization folder.
   - The Clock icon indicates this is a backup folder.
The Activity Log tab lists a summary of backup and synchronization activity.
The Devices tab displays all the devices associated with this account.
4. For more information about Backup & Sync in your online account, see the SecureAnywhere Management Website User Guide.
Changing Backup & Sync Settings

Backup & Sync comes preconfigured with default settings, but you can adjust the settings if you want. For example, you can adjust the size limit of files to upload or allow a file upload to run while your computer is on battery power. These settings apply both to synchronization and backups.

To change Backup & Sync settings:

1. From the system tray, double-click the Webroot icon.

The main interface displays.
2. In the upper right corner, click **Advanced Settings**.

The Settings pane displays with the Install Settings sub-pane active.
3. Select **Backup & Sync**.

The Backup & Sync pane displays.
4. Do one of the following:
   - To enable a setting, select the checkbox.
   - To disable a setting, deselect the checkbox.

   **Note:** We recommend that you keep Webroot's default settings. If you make changes and decide you want to return to the recommended settings, click the **Reset to defaults** button.

The following table describes the settings.
<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ignore hidden files and directories</td>
<td>If you select this checkbox, files and directories that Windows has hidden in Explorer are not included in the upload. Hidden files are typically system files that do not need to be synchronized or backed up. They can also consume a lot of storage space.</td>
</tr>
<tr>
<td>Ignore system files and directories</td>
<td>If you select this checkbox, Windows system files and directories are not included in the upload. Typically, system files do not need to be synchronized or backed up. They can also consume a lot of storage space.</td>
</tr>
<tr>
<td>Show Windows Explorer overlay icons</td>
<td>If you select this checkbox, the Webroot icons next to files and folders display in Windows Explorer to show whether they are uploaded, whether backed up or synchronized, are in the process of uploading, or did not get uploaded. For more information about these icons, see <em>Synchronizing Files on page 133</em>.</td>
</tr>
<tr>
<td>Do not archive while running on battery power</td>
<td>If you select this checkbox, SecureAnywhere does not run a sync or backup when your computer is unplugged and running on the battery.</td>
</tr>
<tr>
<td>Do not archive when a full-screen application or game is running</td>
<td>If you select this checkbox, SecureAnywhere does not run a sync or backup when you are watching a movie in full-screen mode or running a gaming application.</td>
</tr>
<tr>
<td>FIELD</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable access to the Webroot Cloud from Windows Explorer</td>
<td>If you select this checkbox, the system adds a link within Windows Explorer to the contents of your SecureAnywhere Backup &amp; Sync page in your Webroot account.</td>
</tr>
<tr>
<td></td>
<td>- From there, you can right-click folders to open them.</td>
</tr>
<tr>
<td></td>
<td>- You can right-click files to open, delete, rename them or view their properties, or download them as an archive or specify the program to open them.</td>
</tr>
<tr>
<td></td>
<td>- Any changes you make to a folder here are saved to the folders and files in the Webroot account and, if it's in a sync folder, to any synchronized devices.</td>
</tr>
<tr>
<td></td>
<td>![Image of a link to Webroot Backup &amp; Sync in Windows Explorer]</td>
</tr>
<tr>
<td>Warn when quota usage exceeds</td>
<td>The number in this field determines when SecureAnywhere displays a warning that you are about to exceed your storage limit.</td>
</tr>
<tr>
<td></td>
<td>You can adjust the percentage by entering a new number and clicking the <strong>Save</strong> button.</td>
</tr>
<tr>
<td>Do not upload files larger than</td>
<td>The number in this field determines the size of files to include in synchronization and backup.</td>
</tr>
<tr>
<td></td>
<td>If the file size exceeds the displayed limit, it will not be uploaded. You can adjust the size limit by entering a new number in megabytes, and clicking the <strong>Save</strong> button. The limit is 2000 MB.</td>
</tr>
</tbody>
</table>
5. When you're done, click the Save button.
Adding More Storage

If you need more storage space for your synchronization and backup files, you can purchase storage space online.

To add more storage:

1. From the system tray, double-click the Webroot icon.

   ![Webroot Icon](image)

   The main interface displays.

   ![Webroot Interface](image)
2. Go to the Backup & Sync pane and click the **Get more storage** button.

   The system opens a browser page where you can purchase additional storage space.
Chapter 10: Using System Optimizer

To learn more about Webroot's System Optimizer, see the following topics:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Changing System Optimizer Settings</td>
<td>182</td>
</tr>
<tr>
<td>Running Scheduled Optimizations</td>
<td>195</td>
</tr>
<tr>
<td>Running System Optimizer Manually</td>
<td>206</td>
</tr>
<tr>
<td>Using Secure Erase</td>
<td>211</td>
</tr>
</tbody>
</table>
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:

1. From the system tray, double-click the Webroot icon.

The main interface displays.
2. Click **Advanced Settings**.

The Settings window displays with the Install Settings sub-pane active.
3. Select **System Optimizer**.

![System Optimizer pane](image)

The System Optimizer pane displays.
Note: To view all the settings, use the scroll bar on the right side of the screen.
Select or deselect any of the options, described in the following table:

<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clipboard contents</td>
<td>Clears the contents from the Clipboard, where Windows stores data when you</td>
</tr>
<tr>
<td></td>
<td>use either the Copy or Cut function from any Windows program.</td>
</tr>
<tr>
<td>Windows Temporary Folder</td>
<td>Deletes all files and folders in the Windows temporary folder, but not files</td>
</tr>
<tr>
<td></td>
<td>that are in use by an open program.</td>
</tr>
<tr>
<td></td>
<td>This folder is usually located at:</td>
</tr>
<tr>
<td></td>
<td>C:\Windows\Temp</td>
</tr>
<tr>
<td></td>
<td>You should not put any files here that you need to keep. The files in this</td>
</tr>
<tr>
<td></td>
<td>folder can consume a lot of space on your hard drive.</td>
</tr>
<tr>
<td>System Temporary folder</td>
<td>Deletes all files and folders in the system temporary folder, but not files</td>
</tr>
<tr>
<td></td>
<td>that are in use by an open program.</td>
</tr>
<tr>
<td></td>
<td>This folder is usually located at:</td>
</tr>
<tr>
<td></td>
<td>C:\Documents and Settings[username]\Local Settings\Temp</td>
</tr>
<tr>
<td></td>
<td>You should not put any files here that you need to keep. The files in this</td>
</tr>
<tr>
<td></td>
<td>folder can consume a lot of space on your hard drive.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Windows Update Temporary folder</strong></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>These files are located at:</td>
</tr>
<tr>
<td></td>
<td>C:\Windows\Software\Distribution\Download</td>
</tr>
<tr>
<td></td>
<td>You should 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.</td>
</tr>
<tr>
<td><strong>Windows Registry Streams</strong></td>
<td>Clears the history of recent changes you made to the Windows registry.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This option does not delete the registry changes themselves.</td>
</tr>
<tr>
<td><strong>Default logon user history</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Memory dump files</strong></td>
<td>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.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 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\CD Burning  
  - 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. |
<p>| Start Menu click history      | Clears the history of shortcuts to programs that you recently opened using the Start menu. |</p>
<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run history</td>
<td>Clears the history of commands that you recently entered into the Run dialog, which is accessible from the Start menu.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> After the cleanup, you may need to restart your computer to completely remove items from the Run dialog.</td>
</tr>
<tr>
<td>Search history</td>
<td>Clears the history of files or other information that you searched for on your computer.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>The cleanup does not delete the actual files.</td>
</tr>
<tr>
<td>Start Menu order history</td>
<td>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 back to alphabetical order.</td>
</tr>
<tr>
<td>Internet Explorer - Address bar history</td>
<td>Removes the list of recently visited websites, which is stored as part of Internet Explorer’s AutoComplete feature.</td>
</tr>
<tr>
<td></td>
<td>You see this list when you click the arrow on the right side of the Address drop-down list at the top of the Internet Explorer browser.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Internet Explorer - Cookies</strong></td>
<td>Deletes all cookies from your computer.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Internet Explorer - Temporary Internet Files</strong></td>
<td>Deletes copies of stored web pages that you visited recently.</td>
</tr>
<tr>
<td></td>
<td>This cache improves performance by helping web pages 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.</td>
</tr>
<tr>
<td><strong>Internet Explorer - URL history</strong></td>
<td>Deletes the list of recently visited websites.</td>
</tr>
<tr>
<td></td>
<td>You see this list when you click <strong>History</strong> on the Internet Explorer toolbar. While this history can be helpful, it also reveals your visited sites to other people using your computer.</td>
</tr>
<tr>
<td><strong>Internet Explorer - Setup Log</strong></td>
<td>Deletes log files created when you update Internet Explorer.</td>
</tr>
<tr>
<td></td>
<td>After you install the updates, you no longer need these files.</td>
</tr>
<tr>
<td><strong>Microsoft Download Folder</strong></td>
<td>Deletes the contents in the folder that stores files you last downloaded using Internet Explorer.</td>
</tr>
<tr>
<td></td>
<td>After downloading, you no longer need these files unless you want to save downloaded software installation files.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>MediaPlayer Bar History</strong></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>The cleanup does not delete the files, just the Windows memory that you opened them or searched for them.</td>
</tr>
<tr>
<td><strong>Autocomplete for m information</strong></td>
<td>Deletes data that Internet Explorer stores when you enter information into fields on websites.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Clean index.dat (cleaned on reboot)</strong></td>
<td>Marks files in the index.dat file for deletion, then clears those files after you reboot the system.</td>
</tr>
<tr>
<td></td>
<td>The index.dat file is a growing Windows repository of web addresses, search queries, and recently opened files. This option works when you also select one or more of the following options:</td>
</tr>
<tr>
<td></td>
<td>• Cookies</td>
</tr>
<tr>
<td></td>
<td>• Temporary Internet Files</td>
</tr>
<tr>
<td></td>
<td>• URL History</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>Index.dat functions like an active database. It is only cleaned after you reboot Windows.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>--------------------------------------------------------------</td>
</tr>
<tr>
<td>Mozilla Firefox - Cached Files</td>
<td>Removes temporary files, such as recently visited web pages, stored by Mozilla Firefox.</td>
</tr>
<tr>
<td>Google Chrome - Cached Files</td>
<td>Removes temporary files, such as recently visited web pages, stored by Google Chrome.</td>
</tr>
<tr>
<td>Adobe Acrobat Pro - Recent Files</td>
<td>Removes the cache of recently opened PDF files stored by Adobe Acrobat. Does not remove any actual PDF files.</td>
</tr>
<tr>
<td>Adobe Acrobat Pro - User Preferences</td>
<td>Removes the cache of user preferences stored by Adobe Acrobat.</td>
</tr>
<tr>
<td>Microsoft Management Console - Recent Files</td>
<td>Removes the cache of recently opened files stored by Microsoft Management Console.</td>
</tr>
<tr>
<td>Windows DirectInput - Recent File List</td>
<td>Removes the cache of recently opened files stored by Windows DirectInput.</td>
</tr>
<tr>
<td>Windows WBEM Log Files</td>
<td>Removes log files created by Windows WBEM.</td>
</tr>
</tbody>
</table>
5. Do any of the following:

- To save your settings, click the **Save** button.
- To leave the Settings pane without making changes, click the **Cancel** button.
- To reset to default settings, click the **Reset to defaults** button.
Running Scheduled Optimizations

You can configure the System Optimizer to run automatically on a schedule.

To run a scheduled optimization:

1. From the system tray, double-click the Webroot icon.

The main interface displays.
2. Click **Advanced Settings**.

The Settings pane displays, with the Install Settings sub-pane active.
3. Select **Scheduler**.

The Scheduler pane displays, with the Scan Schedule tab active.
4. Click the **System Optimizer** tab.

The System Optimizer sub-pane displays.
5. Select the **Enable scheduled optimization** checkbox.

6. Do one of the following:
   - Select the **Optimize only on the following days** checkbox and select a day of the week to run the optimization.
   - Deselect the **Optimize only on the following days** checkbox to run the optimization by default every
7. Do one of the following:
   - Select the **Optimize at specific time of day** radio button, then from the drop-down menu, select a time of day.
Select the **Optimize every** radio button and in the hours field, enter the hourly interval.

8. To specify whether the optimization will run on bootup if it was missed while the system was turned off, select or deselect the **Run on bootup** checkbox.
9. Do any of the following:
   - If you're done, click the **Save** button.
   - Click the **Rest to defaults** button to reset all fields to their default values.
   - Click the **Cancel** button to exit without saving your changes.
   - To return to the main window, in the upper right corner, click the **X**.
**Running System Optimizer Manually**

If you purchased a SecureAnywhere edition that includes the System Optimizer, you can remove all traces of your web browsing history, files that indicate your computer use, and other files that reveal your activity.

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 the System Optimizer, you can protect your privacy by removing all 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 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.

**Note:** 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. For more information about scans, see *Running Scans on page 28.*

Before running the optimizer, you can customize it using any of the following procedures:

- To set up a schedule for automatic system optimization — *Running Scheduled Optimizations on page 195.*
- To select what files you want erased — *Changing System Optimizer Settings on page 182.*
- To specify how recoverable you want the erased files to be — *Using Secure Erase on page 211.*

**To run the System Optimizer manually:**

1. From the system tray, double-click the **Webroot** icon.

   ![Windows Icon](image)

   The main interface displays.
2. Click Utilities to expand the Utilities drop-down menu.

![Utilities drop-down menu](image)

3. Do either of the following:
   - From the Utilities drop-down menu, select Optimize Now.
   - Click the Utilities gear icon, then select the System Optimizer tab and click Optimize Now.

The optimizer displays a progress bar as it runs.
When the optimizer completes, the system displays how much disk space was recovered and when the last optimization was completed.

4. To get details about what was deleted, from Utilities, select the **System Optimizer** tab, click the **View Log** button.
The log displays in the default text editor.

5. When you're done, close the file.
Using Secure Erase

The Secure Erase feature described here allows you to specify how thoroughly the System Optimizer deletes files when it runs. 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, where anyone can access it. Even when you empty the Recycle Bin, 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.

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.

This topic includes procedures for the following:

- Specify Secure Erase Settings
- Use Secure Erase in Windows Explorer

To specify Secure Erase settings:

1. From the system tray, double-click the Webroot icon.

The main interface displays.
SecureAnywhere is protecting your computer. No active threats have been detected.

Stay informed. Join the discussion.

For security news, product questions, and expert advice, please visit the Webroot Community.

Scan My Computer

Learn More

PC Security
- On
- On
- On

Identity Protection
- 

Utilities
- 

My Account
- 

Support / Community
- 

Advanced Settings
2. In the upper right corner, click the **Advanced Settings** button.

The Settings pane displays with the Install Settings sub-pane active.
3. Select **Secure Erase**.

The Secure Erase pane displays.
4. 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.

   **Note:** These settings may have a significant impact on the amount of time it takes to run a system optimization.

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

**To use Secure Erase in Windows Explorer:**

1. In the Advanced Settings > **Secure Erase** panel, select the **Enable Windows Explorer right click secure file erasing** checkbox.
2. Open Windows Explorer.
3. Right-click on the file or folder you want to permanently erase.
4. From the drop-down menu, select **Permanently erase with Webroot**.

![Image of drop-down menu with selection highlighted]

The system uses one of the following configuration options to erase the selected file or folder:

- Normal
- Medium
- Maximum
**Chapter 11: Using System Control**

To learn more about system control, see the following topics:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Running System Analyzer</td>
<td>219</td>
</tr>
<tr>
<td>Controlling Active Processes</td>
<td>223</td>
</tr>
<tr>
<td>Using the SafeStart Sandbox</td>
<td>227</td>
</tr>
</tbody>
</table>
Running System Analyzer

If you purchased a SecureAnywhere edition that includes System Analyzer, you can use this simple utility to quickly scan for threats, security vulnerabilities, and other computer problems. After the scan, it displays a report that describes any vulnerabilities it found. It also provides recommendations about enhancements that can increase system performance, privacy, and protection.

To run System Analyzer:

1. From the system tray, double-click the Webroot icon.

![System Analyzer Interface]

The main interface displays.
2. Click the **Utilities** gear icon.

![Utilities gear icon](image)

3. Click the **System Control** tab.

4. Click the **Run System Analyzer** button.

   The analyzer launches, displaying a progress report that describes what it is doing.
When the analysis is complete, System Analyzer displays a report similar to the following example.
5. Do any of the following:
   • To view more detailed information, click the **View Report Details** button.
   • To save the report, click the **Save Results** button.
   • To exit the report, click the **Close** button.
Controlling Active Processes

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

To control an active process:

1. From the system tray, double-click the Webroot icon.

The main interface displays.
2. Click the **Utilities** gear icon.

3. Click the **System Control** tab.
4. Under Control Active Processes, click the **Start** button.

A new panel displays, listing all active processes on your system.
5. For each process, select one of the following radio buttons:
   - **Allow** — The process is allowed to run on your system.
   - **Monitor** — Webroot SecureAnywhere will watch the process and open an alert on suspicious activity. Any process flagged as monitored displays at the top of the list.
   - **Block** — The process is blocked from running on your system. Do NOT block a process unless you are absolutely certain it is non-essential.

6. Do either of the following:
   - To display more information about a particular process, click the process name, click the **More Info** button and then click the **Details** tab.
   - To terminate all untrusted processes, click the **Stop Untrusted Processes** button.

**Note:** Do not click the **Stop Untrusted Processes** button unless you understand the implications or have been told to do so by Webroot Technical Support.
Using the SafeStart Sandbox

If you are an advanced user and want to check a program you believe is malware, you can first 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.

**Note:** The SafeStart Sandbox is intended for testing malware, not for testing legitimate programs.

**To use the SafeStart sandbox:**

1. From the system tray, double-click the Webroot icon.

The main interface displays.
2. Click the **Utilities** gear icon.

![Utilities gear icon](image)

3. Click the **System Control** tab.
4. Under SafeStart Sandbox, click the **Run SafeStart Sandbox** button.

The SafeStart Sandbox window displays.
5. Browse to and select the filename or type in the path and filename for the command you want to start.

6. To control how the program is allowed to execute, select or deselect any of the following checkboxes:

   ![SafeStart Sandbox](image)

   **Note:** The list of commands is in a scrolling window.

7. When you're done, click the **Start** button.
Chapter 12: Using Reports and Viewers

To learn more about reports and views, see the following topics:

- Saving Scan Logs ................................................................. 233
- Saving Threat Logs ........................................................... 237
- Viewing Protection Statistics .............................................. 241
- Viewing Execution Histories ............................................. 249
Saving Scan Logs

If you want to investigate what SecureAnywhere scanned and what it found, you can save a scan log. This log might be helpful if you are working with Webroot Support to determine the cause of a problem.

To save a scan log:

1. From the system tray, double-click the Webroot icon.

The main interface displays.

![Webroot SecureAnywhere Main Interface](image-url)
2. Click the Utilities gear icon.

The Utilities panel displays.
3. Click the **Reports** tab.

The Reports panel displays.
4. Click the **Save scan log** button.

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.
Saving Threat Logs

To save a threat log:

1. From the system tray, double-click the **Webroot** icon.

The main interface displays.
2. Click the **Utilities** gear icon.

The **Utilities** panel displays.
3. Click the **Reports** tab.

The Reports panel displays.
4. Click the **Save threat log** button.

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.
Viewing Protection Statistics

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

To view protection statistics:

1. From the system tray, double-click the Webroot icon.

The main interface displays.
2. Click the Utilities gear icon.

The Utilities panel displays.
3. Click the **Reports** tab.

The Reports panel displays.
4. Under Event Viewers, click the **View Statistics** button.

![SecureAnywhere](image)

The Protection Statistics panel displays.
Protection Statistics allow you to view individual events taking place across the system. You can double click on an individual line to view additional information on the granular changes taking place.

<table>
<thead>
<tr>
<th>Inspected System Events</th>
<th>Session</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Events</td>
<td>10,355,927</td>
<td>214,625,644</td>
</tr>
<tr>
<td>Registry Events</td>
<td>259,679,399</td>
<td>5,701,180,075</td>
</tr>
<tr>
<td>Code Events</td>
<td>161,826</td>
<td>4,337,938</td>
</tr>
<tr>
<td>Network/Internet Events</td>
<td>5,171,940</td>
<td>83,152,015</td>
</tr>
<tr>
<td>Process/Thread Events</td>
<td>227,906,825</td>
<td>4,938,935,779</td>
</tr>
<tr>
<td>Window/GDI Events</td>
<td>7,531,365,396</td>
<td>935,464,177,944</td>
</tr>
<tr>
<td>Input Events</td>
<td>67,462</td>
<td>1,551,456</td>
</tr>
<tr>
<td><strong>Total Events</strong></td>
<td>8,035,209,775</td>
<td>946,407,860,779</td>
</tr>
</tbody>
</table>

SecureAnywhere has used 0.02% of your CPU since installation and 0.001% disk space. Average scan time is 48.3 seconds.
5. To view more detailed information, in the left column, click on an event.

The Events panel displays.
6. Click the **Details** tab.

The Details panel displays.
7. When you are done viewing the information, click the **Close** button to exit the panel.
Viewing Execution Histories

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

To view an execution history:

1. From the system tray, double-click the Webroot icon.

The main interface displays.
2. Click the **Utilities** gear icon.

The Utilities panel displays.
3. Click the **Reports** tab.

The Reports panel displays.

4. Under Event Viewers, click the **View History** button.

The Execution History panel displays.
5. To display details about a specific program, highlight the name, and click the **More Information** button.

The Events panel displays.
6. Click the **Details** tab.

The Details panel displays.
7. When you're done viewing the information, click the **Close** button to exit the panel.
Chapter 13: Using Your Account

To learn more about using your SecureAnywhere account, see the following topics:

- Viewing Account Details ................................................................. 256
- Activating Keycodes ...................................................................... 259
- Checking For Updates .................................................................... 262
- Renewing Your Subscription ......................................................... 266
**Viewing Account Details**

You can view your keycode and the time remaining on your subscription from the My Account section of the main panel.

To view account details:

1. From the system tray, double-click the **Webroot** icon.

The main interface displays.
2. Click the **My Account** link.

Your account information displays.
Stay informed. Join the discussion.

For security news, product questions, and expert advice, please visit the Webroot Community.

Read Now
Activating Keycodes

If you receive a new keycode from Webroot, you can activate it in the My Account panel.

To activate a new keycode:

1. From the system tray, double-click the Webroot icon.

The main interface displays.
2. Click the **My Account** gear icon.

Your **My Subscription** panel displays with the **Keycode** tab active.
3. In the Activate a new keycode field, enter the keycode you want to add and click the **Activate** button.
Checking For Updates

If you deactivated automatic updates from Install Settings, you can manually check for updates yourself.

For more information about setting automatic updates, see Setting Install Preferences on page 297.

To check for updates:

1. From the system tray, double-click the Webroot icon.

![Webroot Icon]

The main interface displays.
2. In the upper right corner, click the **My Account** gear icon.

The My Account panel displays with the Keycode tab active.
3. Click the **About SecureAnywhere** tab.

The **About SecureAnywhere** panel displays.
4. Click the **Check for software updates** button.

The system does one of the following:

- If you're using the most current version of Webroot, the system displays a message. Click **OK** to close the message.

- If a newer version exists, Webroot downloads the updates to your system.
Renewing Your Subscription

You can renew your subscription from the My Account window.

To renew your subscription:

1. From the system tray, double-click the Webroot icon.

The main interface displays.
2. Click the My Account gear icon.

Your My Subscription panel displays.
3. Click the Upgrade/Renew button.

4. The Webroot website opens, where you can purchase an upgrade to your software.
Chapter 14: Setting Preferences

To learn more about setting preferences, see the following topics:

- Setting Access Controls ............................................................. 270
- Defining Proxy Server Settings ..................................................... 278
- Adjusting Heuristics .................................................................. 284
- Exporting and Importing Settings .................................................. 291
- Setting Install Preferences ............................................................. 297
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 SecureAnywhere.

To set access controls:

1. From the system tray, double-click the Webroot icon.

The main interface displays.
2. In the upper right corner, click the **Advanced Settings** button.

The Settings panel displays with the Install Settings sub-pane active.
3. In the left pane, select **Access Control**.

The Access Control pane displays.
WSA PC User Guide
4. Set access control using the information in the following table.

<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Password Protection</td>
<td>Requires that users enter a password for any configuration changes or critical actions.</td>
</tr>
<tr>
<td>Password</td>
<td>If Password Protection is enabled, type the password.</td>
</tr>
<tr>
<td>Repeat Password</td>
<td>If Password Protection is enabled, repeat the password.</td>
</tr>
<tr>
<td>Protect against process termination</td>
<td>Prevents users and programs from terminating any process.</td>
</tr>
<tr>
<td>Protect against process tampering</td>
<td>Prevents users and programs from modifying the behavior of any process.</td>
</tr>
<tr>
<td>Require the completion of a CAPTCHA when changing critical features</td>
<td>Opens a CAPTCHA dialog that requires you to read distorted text on the screen and enter the text in a field before performing any critical actions. These actions include changing shields, importing configuration settings, uninstalling the program, and shutting down the agent.</td>
</tr>
<tr>
<td>Require the completion of a CAPTCHA when changing any configuration option</td>
<td>Opens a CAPTCHA dialog that requires you to read distorted text on the screen and enter the text in a field before performing any configuration changes.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Allow users to remove threats without a password</td>
<td>Allows you to remove threats, even if password protection is enabled.</td>
</tr>
<tr>
<td>Allow non-administrative users to modify configuration options</td>
<td>Enables you to modify configuration options, whether you are logged in as an administrative user or not.</td>
</tr>
<tr>
<td>Allow uninstallation by non-administrative users</td>
<td>Allows anyone to uninstall SecureAnywhere.</td>
</tr>
<tr>
<td>Allow access to advanced features by non-administrative users</td>
<td>Enables you to access the advanced features, whether you are logged in as an administrative user or not. Advanced features include all options in the Settings panels and the Antimalware tools under Quarantine.</td>
</tr>
<tr>
<td>Hide the keycode on screen</td>
<td>Hides the license keycode when entered or displayed on screen.</td>
</tr>
</tbody>
</table>
5. When you're done, click the **Save** button.
Defining Proxy Server Settings

If you use a proxy server to connect to the Internet, you must define the proxy connection data; otherwise, Webroot cannot send updates to your computer. A proxy server is a computer system or router that acts as a relay between your computer and another server.

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

To define proxy server settings:

1. From the system tray, double-click the Webroot icon.

The main interface displays.
2. In the upper right corner, click **Advanced Settings**.

The Settings pane displays with the Install Settings sub-pane active.
3. Select **Proxy**.

The Proxy pane displays.
4. Enter the proxy settings, using the information in the following table.

<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Type</td>
<td>From the drop-down menu, select the HTTP Proxy.</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>From the drop-down menu, select an authentication method.</td>
</tr>
<tr>
<td>Host</td>
<td>Enter the fully qualified domain name of the server, for example, enter proxy.company.com.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port number the server uses.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the user name of the server, if used.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password of the server, if used.</td>
</tr>
</tbody>
</table>

5. When you're done, click the Save button.


**Adjusting Heuristics**

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

**To adjust heuristics:**

1. From the system tray, double-click the **Webroot** icon.

The main interface displays.
2. In the upper right corner, click **Advanced Settings**.

![SecureAnywhere settings panel](image)

The Settings pane displays with the Install Settings sub-pane active.
3. Select **Heuristics**.

The Heuristic pane displays.
WSA PC User Guide
4. Adjust heuristics using the information in the following table.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable heuristics</td>
<td>Turns off heuristic analysis. Not recommended.</td>
</tr>
<tr>
<td>Enable standard heuristics</td>
<td>This setting could lower your level of security.</td>
</tr>
<tr>
<td>Enable enhanced heuristics based on the behavior, origin, age, and popularity of files</td>
<td>Default; recommended setting.</td>
</tr>
<tr>
<td>Enable maximum heuristics</td>
<td>Use with caution; this could cause unexpected behavior, prevent the use of lesser known applications, or prevent the installation of rarely-used programs.</td>
</tr>
<tr>
<td>Warn when any new program executes that is not specifically whitelisted</td>
<td>Issues a warning for any program not specifically included in the Webroot database of websites that are known to be okay.</td>
</tr>
<tr>
<td>Enable Webroot Infrared</td>
<td>For information, see <a href="#">PC Shields Overview on page 56</a>.</td>
</tr>
</tbody>
</table>
5. When you're done, click the **Save** button.
Exporting and Importing Settings

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

To export and import settings:

1. From the system tray, double-click the Webroot icon.

The main interface displays.
2. In the upper right corner, click **Advanced Settings**.

The Settings pane displays with the Install Settings sub-pane active.
Chapter 14: Setting Preferences

![Setting Preferences](image-url)

- Automatically download and apply updates
- Show a shortcut on the desktop
- Show a system tray icon
- Show a status notification screen on boot up
- Show a Start Menu shortcut
- Allow SecureAnywhere to be shut down manually
3. Select **Import / Export**.

The Import / Export pane displays.
4. Do one of the following:
   - To transfer your settings to another computer, click **Export**, enter a name for the file and click the **Save** button.
   - To import settings from another installation, access the new computer, copy the exported file, click
the **Import** button, select the file, and click the **Save** button.
Setting Install Preferences

You can change basic preferences for SecureAnywhere using the Install Settings panel.

To set install preferences:

1. From the system tray, double-click the Webroot icon.

The main interface displays.
2. In the upper right corner, click the **Advanced Settings** button.

The Settings pane displays with the Install Settings sub-pane active.
Chapter 14: Setting Preferences

![Settings Menu]

- Automatically download and apply updates
- Show a shortcut on the desktop
- Show a system tray icon
- Show a status notification screen on bootup
- Show a Start Menu shortcut
- Allow SecureAnywhere to be shut down manually

[Reset to defaults] [Save] [Cancel]
3. Set install preferences using the information in the following table.

<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatically download and apply updates</td>
<td>Downloads product updates automatically without alerting you.</td>
</tr>
<tr>
<td>Show a shortcut on the desktop</td>
<td>Provides quick, double-click access to the main interface by placing the shortcut icon on your desktop. To add or remove the Webroot SecureAnywhere 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.</td>
</tr>
<tr>
<td>Show a system tray icon</td>
<td>Provides quick access to SecureAnywhere 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, like scanning.</td>
</tr>
<tr>
<td>Show a status notification screen on bootup</td>
<td>Displays SecureAnywhere status when you boot up your computer.</td>
</tr>
<tr>
<td>Show a Start Menu shortcut</td>
<td>Adds SecureAnywhere to the Start Menu.</td>
</tr>
<tr>
<td>Allow SecureAnywhere to be shut down manually</td>
<td>Allows the user to close SecureAnywhere.</td>
</tr>
</tbody>
</table>

4. When you're done, do any of the following:
   - Click the Save button.
   - Click the Cancel button to escape the Install settings without making any changes.
   - Click the Reset to defaults button to reset all settings.
Chapter 15: WSA PC Support

To learn more about Webroot's support options and other resources, see the following topics:

- Accessing Technical Support ................................................................. 302
- Submitting Files to Webroot For Analysis ........................................... 303
Accessing Technical Support

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

- Is your Webroot subscription through Best Buy? Click here for additional support options.
- Look for the answer in our knowledgebase and FAQs.
- Look for the answer in our online documentation.
- Enter a help ticket.
- Connect to the Webroot Security for Android forum.
Submitting Files to Webroot For Analysis

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 for analysis. For best results when encountering such issues, contact Webroot Technical Support.

To submit a file:

1. From the system tray, double-click the Webroot icon.

The main interface displays.
2. Click the **Utilities** gear icon.

The **Utilities** panel displays with the **Antimalware Tools** tab active.
3. Click the **Reports** tab.

The Reports panel displays.
4. Click the **Submit a File** button.

A browser page opens where you can submit a file.
5. In the select a file field, click the **Browse** button, and select the file you want to send to Webroot.

6. From the reason for submission drop-down menu, select one of the following:
   - **Malicious file** — I think this file is malicious and is a threat, but Webroot SecureAnywhere is not detecting it as a threat.
   - **False positive detection** — This file was detected as a threat by Webroot SecureAnywhere, but I think that it is incorrect and would like to report this as a false positive detection.
   - **Monitored file** — This file is being monitored under Control Active Processes in Webroot SecureAnywhere, and this monitoring seems to be impacting the file functionality.
   - **Safe file** — I know this file is safe, and would like it to be reviewed further by Webroot.
7. In the Enter the characters in the image field, enter the CAPTCHA images.

8. Select the **Terms and Conditions** checkbox.
9. When you're done, click the **Submit File** button.

The system sends the file to Webroot; tech support will contact you to follow up with their analysis of your issue.
Index

A
access controls, setting 270
accessing technical support 302
account details, viewing 256
activating keycodes 259
active
    connections, managing 86
    processes, controlling 223
adding
    more storage 179
    sync folders 139
    whitelisted scripts 106
adjusting heuristics 284
allowing files 96
antimalware tools, using 111

B
backing up files 149
Backup & Sync
    downloading 126
    overview 125
    settings, changing 171
backup schedules, creating 156
blocking files 96

C
changing
    Backup & Sync settings 171
    firewall settings 78
    scan schedules 32
    scan settings 43
    shield settings 61
    System Optimizer settings 182
    web shield settings 78
checking
    file statuses 165
    checking for updates 262
    controlling active processes 223
creating
  backup schedules 156
  custom scans 50
  Webroot accounts 15
custom scans, creating 50

D

defining proxy server settings 278
description, shields 56
detected threats, managing 31
downloading Backup & Sync 126

E

execution histories, viewing 249
exporting settings 291

F

file statuses, checking 165
files
  allowing 96
  backing up 149
  blocking 96
  submitting to Webroot 303
  synchronizing 133
firewall settings, changing 78
firewalls, managing 75
folders, syncing between computers 143

H

heuristics, adjusting 284

I

identity protection, managing 116
importing settings 291
indicators, query results 57
install preferences, setting 297
installing SecureAnywhere 4

K

keycodes, activating 259
Index

M

managing
  active connections 86
  detected threats 31
  firewalls 75
  identity protection 116
  passwords 123
  protected applications 119
  quarantined items 93
  web threats 71
messages, warning 58

O

overview
  Backup & Sync 125
  PC shields 56

P

passwords, managing 123
PC
  shields overview 56
protected applications, managing 119
protection statistics, viewing 241
protection statuses, using 26
proxy server settings, defining 278

Q

quarantined items, managing 93
query result indicators 57

R

removing synced folders 146
removing, whitelist entries 100
renewing subscriptions 266
running
  scans 28
  scheduled optimizations 195
  System Analyzer 219
  System Optimizer manually 206
SafeStart Sandbox, using 227
safety
  scan logs 233
  threat logs 237
scan logs, saving 233
scan schedules, changing 32
scan settings, changing 43
scans, running 28
scheduled optimizations, running 195
Secure Erase, using 211
SecureAnywhere
  installing 4
  using 21
setting
  access controls 270
  install preferences 297
settings
  exporting 291
  importing 291
shield settings, changing 61
shield types 56
storage, adding 179
submitting files to Webroot 303
subscriptions, renewing 266
sync folders
  adding 139
synced folders, removing 146
synchronizing files 133
syncing folders between computers 143
System Analyzer, running 219
System Optimizer
  running manually 206
  settings, changing 182
system tray, using 24

technical support, accessing 302
threat logs, saving 237

Updates 262
updates, checking for 262
using
  antimalware tools 111
  SafeStart Sandbox 227
  Secure Erase 211
  SecureAnywhere 21
  system tray 24

V
viewing
  account details 256
  execution histories 249
  protection statistics 241
  protection statuses 26

W
warning messages 58
web shield settings, changing 78
web threats, managing 71
Webroot accounts, creating 15
whitelist entries, removing 100
whitelisted scripts
  adding 106