## Contents

1: **Getting Started** .......................................................... 1
   - Installing the software .............................................. 2
   - Using the main interface .......................................... 5
     - Using the system tray menu .................................... 6
     - Viewing the protection status ................................ 7
   - Creating a Webroot account ....................................... 9
   - Viewing the PC security status online ....................... 11

2: **Scans** ........................................................................ 13
   - About scans ........................................................... 14
   - Running an immediate scan ....................................... 15
   - Running a custom scan ............................................ 17
   - Changing the scan schedule ..................................... 19
   - Changing scan settings ........................................... 21

3: **Shields** ...................................................................... 23
   - About shields ....................................................... 24
   - Changing Realtime shield settings ............................ 25
   - Changing Behavior shield settings ............................. 27
   - Changing Core System shield settings .................... 29
   - Changing Web Threat shield settings ....................... 31

4: **Firewall** .................................................................... 33
   - About the firewall ............................................... 34
   - Changing firewall alert settings ............................. 35
   - Managing network applications ............................... 36

5: **Quarantine** ................................................................ 39
   - About quarantine .................................................. 40
   - Managing quarantined items ................................... 41
   - Managing file detection .......................................... 43
   - Using antimalware tools ......................................... 45
   - Saving a threat log ................................................ 47

6: **Identity Protection** .................................................... 49
   - About the Identity shield ......................................... 50
   - Changing Identity shield settings ......................... 51
   - Managing protected applications ............................ 53
   - Managing protected websites ................................. 55

7: **Password Management** .............................................. 59
   - About Password Management ................................ 60
   - Downloading the Passwords component .................. 61
   - Capturing login credentials in a website ................. 63
   - Logging in to websites ......................................... 65
   - Populating fields in web forms ............................. 66
8: Backup & Sync ................................................. 69
   About Backup & Sync ...................................... 70
   Downloading the Backup & Sync component ............... 71
   Configuring synchronized folders ......................... 73
   Using the Magic Briefcase ................................ 75
   Copying files to the Web Archive .......................... 76
   Managing files in the Webroot File Manager .............. 77
   Managing files in the Backups page ....................... 78

9: System Cleaner ............................................. 81
   About cleanups ............................................. 82
   Running a cleanup ........................................ 83
   Changing Windows Desktop settings ....................... 85
   Changing Windows System settings ....................... 87
   Changing Application settings ............................ 89
   Changing Internet Explorer settings ..................... 91
   Using Secure File Removal ................................ 93
   Viewing the Cleanup log .................................  95

10: System Control ........................................... 97
    Controlling active processes ............................ 98
    Using SafeStart Sandbox ................................ 99

11: Reports .................................................. 101
    Saving a scan log ....................................... 102
    Viewing the protection statistics ....................... 103
    Viewing the execution history ........................... 104
    Submitting a file ....................................... 105

12: My Account .............................................. 107
    About My Account ....................................... 108
    Activating a new keycode ................................ 109
    Upgrading or renewing the software ..................... 110
    Checking for software updates ........................... 111

13: Settings ................................................ 113
    Setting basic configuration ................................ 114
    Setting self protection ................................ 116
    Setting access control ................................ 117
    Defining proxy settings ................................ 118
    Setting heuristics ...................................... 120
    Importing or exporting settings ......................... 123

A: Webroot Support ......................................... 125

B: Uninstalling the program ............................... 127

C: License agreement ....................................... 129

Index .................................................................... 131
Webroot® SecureAnywhere™ delivers complete protection against viruses, spyware, and other online threats without slowing down computer performance or disrupting your normal activities. With its fast scans and one-click threat removal, you can rest assured that malware is eliminated quickly and easily. Webroot SecureAnywhere gives you the freedom to surf, share, shop, and bank online—all with the confidence that your computer and your identity will be kept safe.

This guide describes how to use all features and functions of the Webroot SecureAnywhere software, which includes the following editions:

<table>
<thead>
<tr>
<th>Edition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Webroot SecureAnywhere AntiVirus</td>
<td>Standard edition that provides protection against viruses, spyware, and other threats.</td>
</tr>
<tr>
<td>Webroot SecureAnywhere Essentials</td>
<td>All the protection of the AntiVirus edition, plus:</td>
</tr>
<tr>
<td></td>
<td>• Firewall protection</td>
</tr>
<tr>
<td></td>
<td>• System cleaner</td>
</tr>
<tr>
<td></td>
<td>• Identity protection</td>
</tr>
<tr>
<td></td>
<td>• Backups</td>
</tr>
<tr>
<td>Webroot SecureAnywhere Complete</td>
<td>All the protection of the AntiVirus edition and the Essentials edition, plus:</td>
</tr>
<tr>
<td></td>
<td>• Password management</td>
</tr>
</tbody>
</table>

To get started with Webroot SecureAnywhere, see the following topics:

- Installing the software ................................ page 2
- Using the main interface ................................. page 5
- Creating a Webroot account ............................. page 9
- Viewing the PC security status online .......... page 11
Installing the software

Webroot SecureAnywhere can be installed on a Windows® 7, Vista®, or XP computer with an Internet connection. If you purchased a multi-user license, you can use the same keycode to install the software on up to three computers (for 3-seat licenses) or five computers (for 5-seat licenses).

To install the program:

1  Before you begin:
   • Read the license agreement.
   • Make sure your system meets these minimum requirements:

<table>
<thead>
<tr>
<th>Minimum system requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Windows operating system:</strong> Webroot SecureAnywhere can be installed on a computer with one of the following operating systems:</td>
</tr>
<tr>
<td>• Windows XP 32-bit and 64-bit SP2, SP3</td>
</tr>
<tr>
<td>• Windows Vista 32-bit (all Editions), Windows Vista SP1, SP2 32-bit and 64-bit (all Editions)</td>
</tr>
<tr>
<td>• Windows 7 32-bit and 64-bit (all Editions), Windows 7 SP1 32-bit and 64-bit (all Editions)</td>
</tr>
<tr>
<td><strong>RAM:</strong> 128 MB (minimum); 2 GB recommended on Windows Vista and Windows 7</td>
</tr>
<tr>
<td><strong>Hard disk space:</strong> 10 MB</td>
</tr>
<tr>
<td><strong>Internet/Browser:</strong> Internet access is required.</td>
</tr>
<tr>
<td>Browser:</td>
</tr>
<tr>
<td>• Internet Explorer 7.0 and higher (32-bit only)</td>
</tr>
<tr>
<td>• Mozilla Firefox 3.6 and higher (32-bit only)</td>
</tr>
<tr>
<td><strong>Note:</strong> The Identity shield also supports Google Chrome 11 and higher, and Opera 9 and higher (32-bit only).</td>
</tr>
</tbody>
</table>

2  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.
The Webroot Installer dialog opens:

3 Enter your keycode in the field. (If your keycode came in an email, you can cut and paste the code into this field.)

4 If desired, you can click **Change installation options** at the bottom of the dialog to modify these settings:
   - **Create a shortcut to Webroot on the desktop.** This option places a shortcut icon on your Windows Desktop for Webroot SecureAnywhere.
   - **Randomize the installed filename to bypass certain infections.** This option changes the Webroot installation filename to a random name (for example, “QrXC251G.exe”), which prevents malware from detecting and blocking Webroot’s installation file.
   - **Protect the Webroot files, processes, and memory from modification.** This option enables self protection and the CAPTCHA prompts. (CAPTCHA requires you to read distorted text on the screen and enter the text in a field before performing any critical actions.) For more information, see “Setting self protection” on page 116 and “Setting access control” on page 117.

Click **Close** when you’re done.

5 In the main installation dialog, click **Agree and Install.**
If you are prompted to enter an email address, enter your address and click **Continue**. Webroot SecureAnywhere launches a scan.

![Webroot SecureAnywhere scan in progress](image)

When the scan completes, the main interface of Webroot SecureAnywhere opens (see “Using the main interface” on page 5).

If Webroot 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 “About scans” on page 14 and “About quarantine” on page 40.

After the initial scan, Webroot 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. Webroot SecureAnywhere does all the work for you in the background.

To verify that SecureAnywhere is running, look for the Webroot icon in the system tray:

![Webroot SecureAnywhere icon](image)

If an important message requires your attention, the icon turns yellow or red, and a dialog opens with further details.
Using the main interface

The main interface provides access to all Webroot SecureAnywhere functions and settings. To open the main interface, you can either:

- Double-click the Webroot icon in the system tray.
- Open the Windows Start menu, click All Programs (or Programs), Webroot SecureAnywhere, then Webroot SecureAnywhere again.

The main interface opens and displays the Overview panel. The example below shows the Complete edition. Depending on the edition you purchased (either AntiVirus, Essentials, or Complete), some features may not appear.

On the left side of the panel, the main interface includes the following navigation buttons and links:

<table>
<thead>
<tr>
<th>Navigation buttons and links</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>View your system status and manually scan your computer.</td>
</tr>
<tr>
<td>PC Security</td>
<td>Run custom scans, change shield settings, and manage the quarantine. If you have the Essentials or Complete editions, PC Security also includes Firewall functions.</td>
</tr>
<tr>
<td>Identity &amp; Privacy</td>
<td>Protect sensitive data that may be exposed during your online transactions and automatically fill in user names and passwords. <strong>Note:</strong> The Identity shield is only available in the Essentials and Complete editions. Password Management is only available in the Complete edition.</td>
</tr>
<tr>
<td>Backup &amp; Sync</td>
<td>Protect your files by uploading them to Webroot’s online repository. <strong>Note:</strong> Backup &amp; Sync is only available in the Essentials and Complete editions.</td>
</tr>
</tbody>
</table>

Note: The Identity shield is only available in the Essentials and Complete editions. Password Management is only available in the Complete edition.
Using the system tray menu

The system tray menu provides access to system status and some common Webroot SecureAnywhere functions. To open the system tray menu, right-click on the Webroot icon, which is usually located in the bottom right of your computer desktop:

![System Tray Menu](image)

**Note**: If the icon does not appear in the system tray, open the main interface, go to **Settings, Basic Configuration**, and click in the box for **Show a system tray icon**.

The system tray menu provides the following selections:

<table>
<thead>
<tr>
<th>System Tray Menu</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Status</td>
<td>Opens the main interface and displays your computer’s security status. (This selection is only available when the main interface is closed.)</td>
</tr>
<tr>
<td>Scan Now</td>
<td>Scans your computer for spyware, viruses, and other types of malware.</td>
</tr>
<tr>
<td>Check for updates</td>
<td>Checks for the latest software version and downloads it.</td>
</tr>
<tr>
<td>Save a Scan Log</td>
<td>Saves a log of scanning activity that you can send to Webroot Support for diagnostics.</td>
</tr>
<tr>
<td>Shut down Webroot</td>
<td>Closes the main interface and stops all protection operations. Be aware that if you shut down Webroot SecureAnywhere, your computer is not protected.</td>
</tr>
</tbody>
</table>
Viewing the protection status

To show 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. Right-click on the Webroot icon from the system tray menu, then click **View Status**:

If your system is secure, the main interface is green and displays a message that you are protected.
If an issue requires your attention, the main interface describes the problem, as shown in the following example:

SecureAnywhere also opens an alert in the system tray, similar to the following example.

SecureAnywhere takes the appropriate action to quarantine the items. It may also prompt you to take action yourself (see “Running an immediate scan” on page 15 and “Managing quarantined items” on page 41).
Creating a Webroot account

Creating a Webroot account enables you to manage security across multiple devices from the Webroot SecureAnywhere website, so that all your devices are protected against viruses, spyware, and other online threats. When you create an account, Webroot SecureAnywhere generates a master account record for you and associates the license keycode with that record.

**Note:** The first user created for an account is the administrator for that account. The account administrator can create additional users and specify their access levels for each Webroot SecureAnywhere product that is licensed and associated with this account. The administrator has access to the SecureAnywhere consoles, license keycodes, users, and account settings.

**To create an account:**

1. Open your browser and go to [my.webrootanywhere.com](http://my.webrootanywhere.com).
2. Click **Sign up now** in the **Create an account** panel of the SecureAnywhere website.
3. Complete the registration information and click **Register Now**. (For more information, see the Help for the SecureAnywhere website.)

   Webroot SecureAnywhere sends a confirmation message to the email address you specified.
4. Open your email application. Click the link in the confirmation email message to open the Confirm Registration page.

   **Note:** Until you click the link in the confirmation email and validate your account, you won’t be able to log in to the Webroot SecureAnywhere website.
5. SecureAnywhere requests two randomly selected characters of the security code you specified when you created the account. Type the requested characters and click **Confirm Registration Now**.

   The SecureAnywhere website opens, similar to the example below for the **Complete** edition.
You can manage additional devices and features, as follows:

- If you purchased the AntiVirus edition of SecureAnywhere, you can add smartphones and tablets to the Mobile Security panel for central management. Webroot apps are available for Android and iPhone/iPad devices at [Webroot Mobile & Tablet Security](#).

- If you purchased the Essentials edition of SecureAnywhere, click **Set Up Account Now** in the Backups panel. You can also add smartphones and tablets to the Mobile Security panel for central management. Webroot apps are available for Android and iPhone/iPad devices at [Webroot Mobile & Tablet Security](#).

- If you purchased the Complete edition of SecureAnywhere, click **Set Up Account Now** in both the Backups and Passwords panels. Your Complete subscription also includes SecureAnywhere apps for your mobile phones and tablets. For download instructions, see [Downloading SecureAnywhere Mobile Complete](#).
Viewing the PC security status online

The SecureAnywhere website contains your license and status information for all computers managed in your SecureAnywhere account. If you have not yet created an account, see “Creating a Webroot account” on page 9.

To view PC status online:

2. Click either the PC Security tab or the Go to PC Security button.

The PC Security page opens and shows each computer managed in your account.

3. Click on the desired PC.

A dialog opens that provides license information and status of previous scans on this device.
4. For easier viewing, you can change the display name for your PC. To do this, click the **Edit** link at the top of the dialog. Enter a new name and click the **✓**.

5. If you are an advanced user, you may want to adjust the security settings for each PC managed in your account. To do this, click the drop-down arrow in the **Security Setting** field, select a new setting from the drop-down menu, and click the **✓**.

   **Note**: “Medium” is the recommended setting for normal use. You should only change the setting to “High” or “Maximum” if you suspect that your computer is infected.

By default, Webroot SecureAnywhere uses the settings that you configured in the desktop application (“User Configuration”). To learn more about the settings, click the **❓** button next to the field. A panel opens that describes the type of protection available. To learn more about heuristics, see “Setting heuristics” on page 120.
When Webroot SecureAnywhere scans your computer, it searches for spyware, viruses, any other threats that may infect your computer or compromise your privacy. If it detects a known threat, it moves the item to quarantine, where it is rendered inoperable and can no longer run on your computer.

Scans run daily without disrupting your work. If you want to change the automatic scanning behavior, see the following topics:

- About scans ................................. page 14
- Running an immediate scan ................. page 15
- Running a custom scan ..................... page 17
- Changing the scan schedule ................ page 19
- Changing scan settings ..................... page 21
About scans

During a scan, Webroot SecureAnywhere searches all areas of your computer where potential threats can hide, including drives, files, the Windows registry, and system memory. To detect threats, it looks for any items that match our threat definitions, items listed in our online community database, or items that exhibit suspicious behavior.

You can check the scan statistics by clicking **PC Security**, then the **Scan** tab:

Scans run automatically every day, at about the same time you installed the software. For example, if you installed the software at 8 p.m., Webroot SecureAnywhere always launches a scan around 8 p.m. It will not disrupt your work, nor will it launch while you are gaming or watching a movie. If any threats are removed during scans, Webroot SecureAnywhere will launch a follow-up scan to make sure your system is clean.

If desired, you can view scan results online for all your computers (see “Viewing the PC security status online” on page 11). This Scan Information tab shows the last 10 scans performed.
Running an immediate scan

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 (networking, music, or adult entertainment), downloaded high-risk items (screen savers, music, or games), or accidentally clicked on a suspicious pop-up advertisement.

You can scan for threats by doing either of the following:

- If the main interface is closed, right-click the System Tray icon and select Scan Now.

- If the main interface is open, click Scan My Computer from the Overview panel.

This launches a Deep scan, which looks for all types of malware in every area of your computer. (You can also run a quick memory scan or a scan on a selected area. For instructions, see “Running a custom scan” on page 17.)
If Webroot SecureAnywhere locates a threat, it displays information about what it found. To remove a threat, make sure its checkbox is selected and click **Next** to continue.

![Image of a scan result showing one threat found](image)

Threats are moved to quarantine, where they are rendered inoperable. You do not need to delete them or do anything else. If you want to view quarantined items, click **PC Security**, the **Quarantine** tab, then the **View Quarantine** button. For more information, see “Managing quarantined items” on page 41.

When a threat is removed, Webroot SecureAnywhere launches a follow-up scan to make sure your system is clean.
Running a custom scan

Webroot SecureAnywhere allows you to select several types of scans:

- **Quick.** A surface scan of files loaded in memory. This scan runs quickly, but may miss some types of inactive malware that launch after a system reboot. **Note:** If the Quick scan misses an infection, the main interface remains red until you run a Full or Deep scan.

- **Full.** A scan of all hard drives. This type of scan is helpful if you frequently switch between system partitions or you have several programs that have never been scanned before.

- **Deep.** An analytical scan that searches for all types of threats, including rootkits and inactive malware. This is the default scan that runs from the main panel or system tray.

- **Custom.** A customized scan of files and folders (see the instructions below).

To run a custom scan:

1. Open the main interface (see “Using the main interface” on page 5).
2. Click PC Security.
3. From the Scan tab, click **Custom scan**.
4 In the Customized Scan dialog, select the radio button for the type of scan you want to perform. If you want to select specific files or drives, choose Custom. Then you can either drag/drop files into this dialog or click the Add File/Folder button to select the directories and files you want.

![Customized Scan dialog](image)

5 Click the Scan button to launch the scan.
Changing the scan schedule

Webroot SecureAnywhere launches scans automatically every day, at about the same time you installed the software. If desired, you can change the scan schedule to run at different times.

To change the scan schedule:

1. Open the main interface (see “Using the main interface” on page 5).
2. At the bottom left, click Settings.
3. In the Settings dialog, click Scan Schedule.
4. Make sure the Enable Scheduled Scans checkbox is selected.
5. In the Scan Frequency field, select one of the following options: every day, a day of the week, or when you boot up (turn on your computer).
6. In the Time field, select an approximate time for the scan to launch.
   Note: The scan will launch when computer resources are available, generally within an hour of the time you select.
7. If you want to change one of the schedule settings, select its checkbox to disable it (uncheck the box) or activate it (check the box). When you’re done, click Save All.
The settings are described in the table below.

<table>
<thead>
<tr>
<th>Scan schedule options</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 this option is disabled, Webroot SecureAnywhere ignores missed scans.</td>
</tr>
<tr>
<td>Hide the scan progress window during scheduled scans</td>
<td>Runs scans silently in the background. If this option is disabled, a window opens and shows the scan progress.</td>
</tr>
<tr>
<td>Only notify me if an infection is found during a scheduled scan</td>
<td>Opens an alert only if it finds a threat. If this option is disabled, a small status window opens when the scan completes, whether a threat was found or not.</td>
</tr>
<tr>
<td>Do not perform scheduled scans when on battery power</td>
<td>Helps conserve battery power. If you want Webroot SecureAnywhere to launch scheduled scans when you are on battery power, deselect this option.</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. Deselect this option if you want scheduled scans to run anyway.</td>
</tr>
<tr>
<td>Randomize the time of scheduled scans up to one hour for distributed 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 option.</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 option deselected, so that deep scans run for all types of malware in all locations.</td>
</tr>
</tbody>
</table>
Changing scan settings

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

To change the scan settings:

1. Open the main interface (see “Using the main interface” on page 5).
2. At the bottom left, click Settings.
3. In the Settings dialog, click Scan Settings.
4. If you want to change a setting, select its checkbox to disable it (uncheck the box) or activate it (check the box). When you’re done, click Save All.

The settings are described in the table below.

<table>
<thead>
<tr>
<th>Scan settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Realtime Master Boot Record (MBR) Scanning</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>Enable Enhanced 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 settings <strong>(continued)</strong></td>
<td></td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable “right-click” scanning in Windows Explorer</td>
<td>Enables an option for scanning the currently selected file or folder in the Windows Explorer right-click menu, as shown in the example below. This option is helpful if you downloaded a file and want to quickly scan it.</td>
</tr>
<tr>
<td>Update the currently scanned folder immediately as scanned</td>
<td>Displays a full list of files as Webroot SecureAnywhere scans each one. If you want to increase scan performance slightly, deselect this option so that file names only update once per second on the panel. Webroot SecureAnywhere will still scan all files, just not take the time to show each one on the screen.</td>
</tr>
<tr>
<td>Favor low memory usage over fast scanning</td>
<td>Reduces RAM usage in the background by using less memory during scans, but scans will also run a bit slower. Deselect this option to run faster scans and use more memory.</td>
</tr>
<tr>
<td>Favor low CPU usage over fast scanning</td>
<td>Reduces CPU usage during scans, but scans will also run a bit slower. Deselect this option to run faster scans.</td>
</tr>
<tr>
<td>Save non-executable file details to scan logs</td>
<td>Saves all file data to the scan log, resulting in a much larger log file. Keep this option deselected to save only executable file details to the log.</td>
</tr>
<tr>
<td>Show the “Authenticating Files” pop-up when a new file is scanned on-execution</td>
<td>Opens a small dialog whenever you run a program for the first time. Keep this option deselected if you do not want to see this dialog.</td>
</tr>
<tr>
<td>Scan archived files</td>
<td>Scans compressed files in zip, rar, cab, and 7-zip archives.</td>
</tr>
</tbody>
</table>
Shields monitor functions related to web browsing and system activity. If a suspicious item tries downloading or running on your computer, the shields automatically block and quarantine the item. For some types of shields, an alert asks if you want to continue the download or block it.

**Note:** If an alert opens and you aren’t certain whether to allow or block the detected item, your safest action is to block it. The file name is displayed in the alert box. Write down the file name and do an Internet search on that file or contact Webroot support at https://www.webrootanywhere.com/support.

If you want to change the shielding actions, see the following topics:

- About shields ........................................ page 24
- Changing Realtime shield settings ............... page 25
- Changing Behavior shield settings ............... page 27
- Changing Core System shield settings .......... page 29
- Changing Web Threat shield settings ........... page 31
About shields

Shields constantly monitor activity while you surf the Internet and while you work on your computer. The shields protect your computer from malware and viruses, as well as settings for your browser and the Windows system. Webroot has preconfigured the shields for you, based on our recommended settings. You do not need to configure any settings yourself.

To view the shield status, click **PC Security** and the **Shields** tab. A green button indicates the shield is on. We recommend that you keep all shields enabled; however, you can disable a shield by clicking the green button.

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 opens an alert. The alert asks if you want to allow the item to run or you want to block it, similar to the example below:

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 **Allow** to continue. If you were not trying to download anything, you should click **Block**. 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.
Changing Realtime shield settings

The Realtime shield blocks known threats that are listed in Webroot’s threat definitions and community database. If the shield detects a suspicious file, it opens an alert and prompts you to block or allow the item. If it detects a known threat, it immediately blocks and quarantines the item before it causes damage to your computer or steals your information.

To change shield settings:

1. Open the main interface (see “Using the main interface” on page 5).
2. At the bottom left, click Settings.
3. From the Settings dialog, click Realtime Shield.
4. If you want to change a setting, select its checkbox to disable it (uncheck the box) or activate it (check the box). When you’re done, click the Save All button.

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 settings are described in the table below.

<table>
<thead>
<tr>
<th><strong>Realtime shield settings</strong></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Predictive Offline Protection from the central Webroot database</td>
<td>Downloads a small threat definition file to your computer, which protects your computer even when it’s offline. We recommend that you keep this option selected.</td>
</tr>
<tr>
<td>Remember actions on blocked files</td>
<td>Remembers how you responded in an alert (allowed a file or blocked it) and won’t prompt you again when it encounters the same file. If this option is deselected, Webroot 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.)</td>
</tr>
<tr>
<td>Automatically quarantine previously blocked files</td>
<td>Opens an alert when it encounters a threat and gives you the option of blocking it and sending it to quarantine. If this option is deselected, you must run a scan manually to remove a threat.</td>
</tr>
<tr>
<td>Automatically block files when detected on execution</td>
<td>Automatically blocks threats and sends them to quarantine. If this option is deselected, you must respond to alerts about detected threats.</td>
</tr>
<tr>
<td>Scan files when written or modified</td>
<td>Scans any new or modified files that you save to disk. If this option is deselected, it ignores new file installations (however, it will still alert you if a threat tries to launch).</td>
</tr>
<tr>
<td>Block threats automatically if no user is logged in</td>
<td>Stops threats from executing even when you are logged off. Threats are sent to quarantine without notification.</td>
</tr>
</tbody>
</table>
Changing Behavior shield settings

The Behavior shield analyzes the applications and processes running on your computer. If it detects a suspicious file, it opens an alert and prompts you to block or allow the item. If it detects a known threat, it immediately blocks and quarantines the item before it causes damage to your computer or steals your information.

To change shield settings:

1. Open the main interface (see “Using the main interface” on page 5).
2. At the bottom left, click **Settings**.

3. From the Settings dialog, click **Behavior Shield**.

4. If you want to change a setting, select its checkbox to disable it (uncheck the box) or activate it (check the box). When you’re done, click the **Save All** button.

   **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 settings are described in the table below.

<table>
<thead>
<tr>
<th>Behavior shield settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assess the intent of new programs before allowing them to execute</td>
<td>Watches the program’s activity before allowing it to execute. If it appears okay, Webroot SecureAnywhere allows it to launch and continues to monitor its activity.</td>
</tr>
<tr>
<td>Enable advanced behavior interpretation to identify complex threats</td>
<td>Employs a thorough analysis of a program to examine its intent. (For example, a malware program might perform suspicious activities like modifying a registry entry, then sending an email.)</td>
</tr>
<tr>
<td>Track the behavior of untrusted programs for advanced threat removal</td>
<td>Watches programs that have not yet been classified as legitimate or as malware.</td>
</tr>
<tr>
<td>Automatically perform the recommended action instead of showing warning messages</td>
<td>Does not prompt you to allow or block a potential threat. Webroot SecureAnywhere will determine how to manage the item.</td>
</tr>
<tr>
<td>Warn if untrusted programs attempt low-level system modifications when offline</td>
<td>Opens an alert if an unclassified program attempts to make changes to your system when you are offline. (Webroot SecureAnywhere cannot check its online threat database if you are disconnected from the Internet.)</td>
</tr>
</tbody>
</table>
Changing Core System shield settings

The Core System shield monitors the computer system structures and makes sure malware has not tampered with them. If it detects a suspicious file trying to make changes, it opens an alert and prompts you to block or allow the item. If it detects a known threat, it immediately blocks and quarantines the item before it causes damage to your computer or steals your information.

To change shield settings:

1. Open the main interface (see “Using the main interface” on page 5).
2. At the bottom left, click Settings.
3. From the Settings dialog, click Core System Shield.
4. If you want to change a setting, select its checkbox to disable it (uncheck the box) or activate it (check the box). When you’re done, click the Save All button.

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 settings are described in the table below.

<table>
<thead>
<tr>
<th>Core System shield settings</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Assess system modifications before they are allowed to</td>
<td>Intercepts any activity that attempts to make system changes,</td>
</tr>
<tr>
<td>take place</td>
<td>such as a new service installation.</td>
</tr>
<tr>
<td>Detect and repair broken system components</td>
<td>Locates corrupted components, such as a broken Layered Service</td>
</tr>
<tr>
<td></td>
<td>Provider (LSP) chain or a virus-infected file, then restores the</td>
</tr>
<tr>
<td></td>
<td>component or file to its original state.</td>
</tr>
<tr>
<td>Prevent untrusted programs from modifying kernel memory</td>
<td>Stops unclassified programs from changing the kernel memory.</td>
</tr>
<tr>
<td></td>
<td>The kernel is the central component of most computer operating</td>
</tr>
<tr>
<td></td>
<td>systems. It acts as a bridge between applications and data</td>
</tr>
<tr>
<td></td>
<td>processing done at the hardware level.</td>
</tr>
<tr>
<td>Prevent untrusted programs from modifying system</td>
<td>Stops unclassified programs from changing the system processes.</td>
</tr>
<tr>
<td>processes</td>
<td></td>
</tr>
<tr>
<td>Verify the integrity of the LSP chain and other system</td>
<td>Monitors the Layered Service Provider (LSP) chain and other</td>
</tr>
<tr>
<td>structures</td>
<td>system structures to make sure malware does not corrupt them.</td>
</tr>
<tr>
<td>Prevent any program from modifying the HOSTS file</td>
<td>Stops spyware from attempting to add or change the IP address</td>
</tr>
<tr>
<td></td>
<td>for a website in the hosts file. It opens an alert where you can</td>
</tr>
<tr>
<td></td>
<td>block or allow the changes. The hosts file is a Windows file that</td>
</tr>
<tr>
<td></td>
<td>helps direct your computer to a website using Internet Protocol</td>
</tr>
<tr>
<td></td>
<td>(IP) addresses.</td>
</tr>
</tbody>
</table>
Changing Web Threat shield settings

The Web Threat shield protects your system as you surf the Internet. If it detects a website that may be a threat, it opens an alert that allows you to decide whether you want to block the site or continue despite the warning. When you use a search engine, this shield analyzes all the links on the search results page and then displays an image next to each link that signifies whether it’s a trusted site (green checkmark) or a potential risk (red X).

To change shield settings:

1. Open the main interface (see “Using the main interface” on page 5).
2. At the bottom left, click Settings.
3. In the Settings dialog, click Web Threat Shield.
4. If you want to change a setting, select its checkbox to disable it (uncheck the box) or activate it (check the box).

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 settings are described in the following table.

<table>
<thead>
<tr>
<th>Web Threat shield settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analyze search engine results and identify malicious websites before visitation</td>
<td>When you use a search engine, Webroot SecureAnywhere analyzes all links displayed on the search results page by running the URLs through its malware-identification engine. It then displays an image next to each link that signifies its risk level. For example, if a site is known for spreading malware infections, it displays a “Known Threat” image next to the link.</td>
</tr>
<tr>
<td>Enable deep content analysis</td>
<td>Analyzes all data traffic on your computer as you visit websites. If threats try to install, it blocks their activity.</td>
</tr>
<tr>
<td>Look for malware on websites before visitation</td>
<td>When you enter the URL for a website in your browser’s address bar or click on a link to a site, Webroot SecureAnywhere runs the URL through its malware-identification engine. If the site is associated with malware, it blocks it from loading in your browser.</td>
</tr>
<tr>
<td>Look for exploits in website content before visitation</td>
<td>Looks for cross-site scripting attacks that may try to redirect you to a different website.</td>
</tr>
</tbody>
</table>

5 If you want to create a list of websites to always block or always allow, click **View Websites**. In the dialog (shown below), enter a website name in the field (in the form of www.sitename.com) and click **Add Website**. In the table, select whether you want to allow this website (click the **Allow** radio button) or you want to block it (click the **Block** radio button). When you’re done, click **Close**.

6 When you’re done with Web Threat settings, click the **Save All** button.
4: Firewall

If you have the Essentials or Complete editions of Webroot SecureAnywhere, you can use the Webroot firewall to monitor data traffic and block potential threats. The Webroot firewall, when used with the your computer’s built-in Windows firewall, provides thorough protection for your computer system and your security.

The Webroot firewall is already configured with our recommended settings. However, if you would like to change the firewall options, see the following topics:

- About the firewall ......................... page 34
- Changing firewall alert settings ........ page 35
- Managing network applications .......... page 36

Webroot Subscription Information!

Firewall protection is available only in the Essentials and Complete editions. To upgrade, see “Upgrading or renewing the software” on page 110.
About the firewall

The Webroot 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 Webroot and Windows firewall turned on, your data has complete inbound and outbound protection.

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

The Webroot firewall is 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.

We recommend that you keep the firewall enabled. However, you can disable it by clicking PC Security and the Firewall tab. Click the green button to turn it off. (A green button indicates the shield is on; a gray button indicates the shield is off.)
Changing firewall alert 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 alert settings:

1. Open the main interface (see “Using the main interface” on page 5).
2. Click PC Security.
3. Click the Firewall tab.
   
   The Firewall settings in the application are shown below.

   ![Firewall Settings Screen]

4. Click a radio button to select an alerting method.
Managing network applications

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. You have control over whether Webroot SecureAnywhere will allow or block certain processes and port communications.

To change settings for active connections:

1. Open the main interface (see “Using the main interface” on page 5).
2. From the main interface, click PC Security.
3. Click the Firewall tab.
4. At the bottom of the panel, click View Network Applications.

The Network Applications dialog opens.
Click on a radio button to allow or block a process, or to allow or close a port.
The Webroot quarantine is a holding area for potential threats found during scan and shielding activities. Items in quarantine are rendered inoperable and cannot harm your computer. You do not need to delete them, unless you want to conserve disk space. You can also restore items from quarantine, if necessary.

To manage file detection and perform some advanced quarantining functions, see the following topics:

- About quarantine ........................................ page 40
- Managing quarantined items ......................... page 41
- Managing file detection ................................. page 43
- Using antimalware tools .............................. page 45
- Saving a threat log ..................................... page 47
About quarantine

As Webroot SecureAnywhere scans and shields your computer, it removes all items associated with threats from their current locations. It then disables their operation and moves them to a holding area, called quarantine. While in quarantine, threats can no longer harm your computer or steal your information.

Your safest action is to keep items in quarantine until you have a chance to test your computer and determine if all programs still work properly after the scan. If you discover that some legitimate programs cannot function after an item was moved to quarantine, you can restore the item to its original location.

To view and manage quarantined items, click **PC Security** and the **Quarantine** tab.
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:

- If you want to conserve disk space, you can delete the items permanently.
- If you discover that 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 view and manage items in quarantine:

1. Open the main interface (see “Using the main interface” on page 5).
2. Click PC Security, then click the Quarantine tab.
3. Click the View Quarantine button.

The Quarantine panel shows the name of the item, its original location, and the date and time it was quarantined.
4 If you want to delete or restore the item, click in its checkbox to select it. Then do either of the following:

- If you want to remove the item permanently, click **Erase**. Be aware that after erasing it, you can never restore the item.

- If you want to move the item back to its original location, click **Restore**. When an item is restored, Webroot 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 (see “Managing file detection” on page 43).
Managing file detection

If you want more control over scans and shielding when Webroot SecureAnywhere encounters a specific executable file, you can use Detection Configuration to specify one of the following actions:

- **Allow**: Ignore the 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.

Detection configuration acts as an override to Webroot SecureAnywhere’s default scanning and shielding behavior.

To use Detection Configuration:

1. Open the main interface (see “Using the main interface” on page 5).
2. Click **PC Security**, then click the **Quarantine** tab.
3. Under Detection Configuration, click the **Configure** button.

![Image of Webroot SecureAnywhere interface with Detection Configuration highlighted](image-url)
The Detection Configuration panel opens.

4 You can add executable files to this list. (Executable files typically have an extension of exe, dll, sys, drv, or com.) To add files, click the **Add File** button. You can also drag and drop a file from Explorer.

The file name appears in the Threat column. (If Webroot SecureAnywhere detected other copies of this file with different file names, it only shows the file name that it last detected.)

5 In the right column, select the radio button for either **Allow**, **Block**, or **Monitor**.

If you want to clear the list, click the **Remove all** button.
Using antimalware tools

Webroot 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 or if Webroot Support is assisting you. 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, screensavers, and system policies.

To access and use these tools:

1. Open the main interface (see “Using the main interface” on page 5).
2. Click **PC Security**, then click the **Quarantine** tab.
3. Under Antimalware Tools, click the **View Tools** button.

The Antimalware Tools panel opens.
See the table below for descriptions and instructions.

<table>
<thead>
<tr>
<th><strong>Antimalware tools</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reset desktop wallpaper</strong></td>
<td>If your computer was recently infected with malware that changed your wallpaper, click the checkbox and click <strong>Run Tools</strong>.</td>
</tr>
<tr>
<td><strong>Reset screensaver</strong></td>
<td>If your computer was recently infected with malware that changed your screensaver, click the checkbox and click <strong>Run Tools</strong>.</td>
</tr>
<tr>
<td><strong>Reset system policies</strong></td>
<td>If your computer was recently infected with malware that changed your system policies, click the checkbox and click <strong>Run Tools</strong>.</td>
</tr>
<tr>
<td><strong>Reboot in Safe Mode</strong></td>
<td>If Webroot Support instructs you to reboot your computer in Safe Mode, click the checkbox and click <strong>Run Tools</strong>.</td>
</tr>
<tr>
<td><strong>Perform an immediate system reboot</strong></td>
<td>To reboot your system after threat removal, click the checkbox and click <strong>Run Tools</strong>.</td>
</tr>
<tr>
<td><strong>Manual Threat Removal</strong></td>
<td>To scan a specific file for threats, click <strong>Select a file</strong>. In the Windows Explorer dialog, select a file and click <strong>Save</strong>. Webroot SecureAnywhere launches a scan. When it’s complete, reboot your system.</td>
</tr>
<tr>
<td><strong>Removal Script</strong></td>
<td>After Webroot Support sends you a removal script, save it to your computer. Click <strong>Select Script...</strong> to launch the tool.</td>
</tr>
</tbody>
</table>
Saving a threat log

If you want to investigate an infection with Webroot Support, you can save a threat log and send it to Webroot. The threat log shows details about threats removed from your computer.

To save a threat log:

1. Open the main interface (see “Using the main interface” on page 5).
2. Click **PC Security**, then click the **Quarantine** tab.
3. Under **View Quarantine**, click the **Save Threat Log** button.
4. In the dialog, select a folder location for the log and click **Save**.
If you have the Essentials or Complete editions of SecureAnywhere, you can use the Identity shield to safely surf the Internet and enter sensitive data in applications. The Identity shield watches for any suspicious activity that may indicate an outside program is attempting to steal information from your computer.

To configure advanced Identity shield protection, see the following topics:

- About the Identity shield ....................... page 50
- Changing Identity shield settings ................. page 51
- Managing protected applications .................. page 53
- Managing protected websites ..................... page 55
About the Identity shield

The Identity shield protects you from identity theft and financial loss. It ensures that your sensitive data is protected, while guarding you from keyloggers, screen-grabbers and other information-stealing techniques typically employed by financial malware.

Webroot has already configured the Identity shield for you. However, you can adjust the security levels if you want. (Click Identity & Privacy to access the Identity Shield panel.)
Changing Identity shield settings

The Identity shield protects sensitive data that may be exposed during your online transactions. If desired, you can change the behavior of the Identity shield and control what it blocks.

To change Identity shield settings:

1. Open the main interface (see “Using the main interface” on page 5).
2. At the bottom left, click Settings.
3. In the Settings dialog, click Identity Shield.
4. If you want to change a setting, select its checkbox to disable it (uncheck the box) or activate it (check the box). When you’re done, click the Save All button.

**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 settings are described in the table below.

<table>
<thead>
<tr>
<th>Identity shield settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Look for identity threats online</td>
<td>Analyzes websites as you browse the Internet or open links. If the shield detects any malicious content, it blocks the site and opens an alert.</td>
</tr>
</tbody>
</table>
### Identity shield settings *(continued)*

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analyze websites for phishing threats</td>
<td>Analyzes websites for phishing threats as you browse the Internet or open links. If the shield detects a phishing threat, it blocks the site and opens an alert. Phishing is a fraudulent method used by criminals to steal personal information. Typical scams might include websites designed to resemble legitimate sites, such as PayPal or a banking organization, which trick you into entering your credit card number.</td>
</tr>
<tr>
<td>Verify websites when visited to determine legitimacy</td>
<td>Analyzes the IP address of each website to determine if it has been redirected or is on our blacklist. If the shield detects an illegitimate website, it blocks the site and opens an alert.</td>
</tr>
<tr>
<td>Verify the DNS/IP resolution of websites to detect Man-in-the-Middle attacks</td>
<td>Looks for servers that could be redirecting you to a malicious website (man-in-the-middle attack). If the shield detects a man-in-the-middle attack, it blocks the threat and opens an alert.</td>
</tr>
<tr>
<td>Block websites from creating high risk tracking information</td>
<td>Blocks third-party cookies from installing on your computer if the cookies originate from malicious tracking websites. Cookies are small bits of text generated by a web server and then stored on your computer for future use. Cookies can contain everything from tracking information to your personal preferences.</td>
</tr>
<tr>
<td>Prevent programs from accessing protected credentials</td>
<td>Blocks programs from accessing your login credentials (for example, when you type your name and password or when you request a website to remember them).</td>
</tr>
<tr>
<td>Warn before blocking untrusted programs from accessing protected data</td>
<td>Opens an alert any time malware attempts to access data, instead of blocking known malware automatically. (This option is for technical users only; we recommend that you keep this option disabled so the program does not open numerous alerts.)</td>
</tr>
<tr>
<td>Allow trusted screen capture programs access to protected screen contents</td>
<td>Allows you to use legitimate screen capture programs, no matter what content is displayed on your screen.</td>
</tr>
</tbody>
</table>
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.

As you work on your computer, Webroot SecureAnywhere automatically adds web browsers and applications to the Protected Applications list. It assigns applications to one of these levels of protection:

- **Protect.** “Protected applications” are secured against information-stealing malware, but also have full access to data on the system. By default, web browsers are assigned to the “protected” status. If desired, you might also want to add other software applications to “protected,” such as financial management software. 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.

To manage the application list and specify levels of protection:

1. Open the main interface (see “Using the main interface” on page 5).
2. Click **Identity & Privacy**.
3. From the Identity Shield tab, click **View/Edit Protected Applications**.

![Webroot SecureAnywhere Interface](image-url)
The Protected Applications panel opens. This panel shows the web browsers on your system and any other applications that you run on the computer.

4 In the row for the application you want to modify, click the radio button for Protect, Allow, or Deny. (To include another application in this list, click Add Application, then select an executable file.)

5 When you’re done, click Close.
Managing protected websites

The Identity shield already includes the recommended security settings for specific types of websites. If desired, you can adjust security for a website to one of the following levels:

- **None.** Provides unfiltered access to all potentially malicious content. (Not recommended.)
- **Low.** Protects stored data and identifies malware in real time. You may want to use this setting if you have an application that does not work properly when the security level is set to Medium or higher.
- **Medium.** Protects your stored data while also providing software compatibility. You may want to use this setting if you have an application that does not work properly when the security level is set to High or Maximum.
- **High.** Provides strong protection against threats, while still enabling screen accessibility for impaired users (for example, allows text-to-speech programs to run normally).
- **Maximum.** Provides maximum protection against threats, but blocks screen accessibility for impaired users.

When you load a “protected” website, the Webroot icon in the system tray displays a padlock: 🛡️. If the Identity shield encounters a website that may be a threat, it opens an alert similar to the following example. You can decide whether you want to stay secure (click **Block**) or continue despite the warning (click **Allow**).

![Warning alert example](image.png)

To manage settings for protected websites:

1. Open the main interface (see “Using the main interface” on page 5).
2. Click **Identity & Privacy**.
3. From the Identity Shield tab, click **View/Edit Protected Websites**.
The Protected Websites panel opens. Webroot has already applied protection policies to HTTP/HTTPS websites and some social networking sites. If you add individual websites to this list and select custom security options, Webroot first applies the HTTPS or HTTP policies, then layers your user-defined policies on top.

4 In the Protected Websites table, click in the row for the type of website you want to adjust. To include an individual site, enter the address in the field at the top of the dialog, then click Add Website.
Adjust the slider for minimum to maximum protection configuration. As an alternative, you can also select the individual protection options by clicking on the green checkmark or red X. (A green checkmark indicates the option is on; a red X indicates the option is off.) When you’re done, click **Save**.

Each protection option is described below:

<table>
<thead>
<tr>
<th><strong>Website protection options</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Block phishing and known malicious websites</strong></td>
</tr>
<tr>
<td><strong>Protect cookies and saved website data</strong></td>
</tr>
<tr>
<td><strong>Detect and prevent man-in-the-middle attacks</strong></td>
</tr>
<tr>
<td><strong>Protect against keyloggers</strong></td>
</tr>
<tr>
<td><strong>Protect sensitive clipboard data</strong></td>
</tr>
<tr>
<td><strong>Protect against URL grabbing attacks</strong></td>
</tr>
<tr>
<td><strong>Protect browser components from external access</strong></td>
</tr>
<tr>
<td><strong>Protect against Man-in-the-Browser attacks</strong></td>
</tr>
<tr>
<td><strong>Isolate untrusted browser add-ons from data</strong></td>
</tr>
<tr>
<td><strong>Block browser process modification attempts</strong></td>
</tr>
<tr>
<td><strong>Protect against screen grabbing attacks</strong></td>
</tr>
<tr>
<td><strong>Block suspicious access to browser windows</strong></td>
</tr>
</tbody>
</table>
If you have the *Complete* edition of SecureAnywhere, you can use the Password Manager to automatically log in to websites that require a user name and password. The Password Manager works from your computer or mobile devices. You can also use the Password Manager to populate fields in web forms, saving you the hassle of manually entering your personal data and credit card number in fields.

**Note:** This section provides a quick overview of the Password Manager. For further instructions, see the *Passwords User Guide* at Webroot’s [SecureAnywhere Help and Product Guides](#) page.

To get started with the Password Manager, see the following topics:

- About Password Management ........................ page 60
- Downloading the Passwords component .......... page 61
- Capturing login credentials in a website ........... page 63
- Logging in to websites .............................. page 65
- Populating fields in web forms .................... page 66
- Managing credentials in the Passwords page .... page 68
About Password Management

The Password Manager allows you to create a secure password for all your website transactions, automatically remember your user names and passwords, and automatically fill in web forms. By using the Password Manager, you never need to remember multiple login names and passwords again.

To keep your data safe from hackers, the Password Manager encrypts all your login and password data on your local computer. Webroot uses the same encryption method employed by the US Government for Top Secret data. The encrypted data is meaningless to Webroot and to anyone else without the decryption key. This key is stored on your own computer and is created from your email address and master password. Your personal data is never sent over the Internet and is never stored on Webroot servers.

You can use the Password Manager, as follows:

1. **Log in to your Webroot account from the browser toolbar.** After the Passwords component downloads (see “Downloading the Passwords component” on page 61), you can log in to your Webroot account from a browser toolbar. When logged in, the Password Manager detects any information you enter in web forms and prompts you to save the data for future use.

2. **Define or capture login credentials and personal information.** You can either allow the Password Manager to capture data as you enter it in a website or you can manually define the data in the SecureAnywhere website. (See “Capturing login credentials in a website” on page 63 and “Populating fields in web forms” on page 66.)

3. **Access a website that requires a login or personal data in web forms.** After defining login credentials and personal information, you can log in to your Webroot account from the toolbar each time you open a browser. When you are logged in, the Password Manager automatically detects fields in a form and can log in to the website automatically. The Webroot icon appears at the end of the fields to indicate that the login information is stored in the Password Manager. (See “Logging in to websites” on page 65.)

4. **Manage your website information in the SecureAnywhere website.** If you want to change your login credentials for any website, you can open your SecureAnywhere account (my.webrootanywhere.com), click Go to Passwords, and edit the information. (See “Managing credentials in the Passwords page” on page 68.)
**Downloading the Passwords component**

To begin using the Password Manager, you must first download the Passwords component.

**To get started with the Password Manager:**

1. From your computer, open the SecureAnywhere main interface (see “Using the main interface” on page 5). Click **Identity & Privacy**, then click the **Password Management** tab. If a **Download and Install** button appears, click the button to install the components.

*Note:* This button may not appear if the Passwords component installed along with the SecureAnywhere installation.

When the download completes, the Passwords panel displays the following:
2 You can click Manage My Identity to open my.webrootanywhere.com and begin managing your passwords online.

If you have not yet created a Webroot account and enabled Passwords, see “Creating a Webroot account” on page 9. When you log in to my.webrootanywhere.com for the first time, be sure to click Set Up Account Now in the Passwords panel.

Once the Passwords component downloads, a Webroot icon appears in the toolbar of your Internet Explorer or Firefox browsers. To access Password Manager functions, click on the drop-down arrow and log in to your Webroot account (use your SecureAnywhere website login credentials). The Password Manager works mainly with Internet Explorer and Firefox browsers. However, you can use some limited functions with other browsers by using bookmarklets. You can define bookmarklets in my.webrootanywhere.com.

For further instructions, see the Passwords User Guide at Webroot’s SecureAnywhere Help and Product Guides page.
Capturing login credentials in a website

To use the Password Manager, you must first define login credentials (for example, your user name and password for each website). The easiest method of capturing login credentials is to open a website and then allow the Password Manager to capture the information as you type. (You can also manually define login credentials in my.webrootanywhere.com.)

To capture login credentials from a website:

1. Open Internet Explorer or Firefox. Log in to your SecureAnywhere account by clicking the Webroot icon in your browser’s toolbar, then entering your SecureAnywhere user name and password.

2. Open a website that requires you to log in, such as a banking site or social media site.

3. Enter your user name and password for the site and log in.

The Password Manager detects the user name, password, and URL, then prompts you to save the login information from a green toolbar near the top of your browser.

4. From the Webroot prompt, click Save Site.

The Add Webroot Site dialog opens with the web address already displayed in the Name field, such as “my.bank.com.” (The user name, password, and URL have been saved automatically and do not appear on this dialog.)
5 You can specify more information about the site and how you want to access it in the future, as described in the following table:

<table>
<thead>
<tr>
<th>Add Webroot Site dialog</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong> The web address will be used for the site name, unless you want to change it to something simple, such as “My Credit Union.”</td>
</tr>
<tr>
<td><strong>Group</strong> You can define a name for a group or select one from the list (if you already defined groups). By defining a group, you can organize sites by categories in the Passwords page of the SecureAnywhere website, such as Banking and Shopping. If you do not enter a group, the site is categorized in a Default group.</td>
</tr>
<tr>
<td><strong>Make This a Favorite</strong> If you access this site frequently, select the checkbox. You can then use the Open all Favorites option from the Passwords page.</td>
</tr>
<tr>
<td><strong>Require Password Reprompt</strong> Click this checkbox if you don’t want your password automatically filled in the field, and instead, want to manually enter the password yourself. This setting also requires that you enter your SecureAnywhere master password before editing the site information.</td>
</tr>
<tr>
<td><strong>AutoLogin</strong> If you want to bypass the password prompt and log in automatically, select the checkbox.</td>
</tr>
</tbody>
</table>

6 Click the **Save Site** button.

Your password-managed sites are displayed in your online SecureAnywhere account. See “Managing credentials in the Passwords page” on page 68.

**Note:** For further instructions, see the *Passwords User Guide* at Webroot’s [SecureAnywhere Help and Product Guides](#) page.
Logging in to websites

The next time you open a browser, make sure you are signed in to your SecureAnywhere account. When you’re signed in, the Password Manager can automatically fill in the user name and password for you.

To log in to a website using Password Manager:

1. Open Internet Explorer or Firefox. Log in to your SecureAnywhere account by clicking the Webroot icon in your browser’s toolbar, then entering your SecureAnywhere user name and password.

   Internet Explorer:
   ![](image1)

   Firefox:
   ![](image2)

2. Open a website where you previously saved login credentials with the Password Manager. The Password Manager remembers the login credentials for you. The Webroot icon appears at the end of the fields to indicate that the login information is stored in the Password Manager. The user name and password fields are automatically filled in, unless you selected Require Password Reprompt in the Add Webroot Site dialog.

   ![User Name: JoieGallagher](image3)
   ![Password: ********](image4)

   ![Log In](image5)

   Note: For further instructions, see the Passwords User Guide at Webroot’s SecureAnywhere Help and Product Guides page.
Populating fields in web forms

You can use the Password Manager to automatically populate web forms with form-fill profiles. These profiles contain personal information that you commonly enter in fields, including your name, address, and credit card information.

To create form-fill profiles:

1. Open Internet Explorer or Firefox. Log in to your SecureAnywhere account by clicking the Webroot icon in your browser’s toolbar, then entering your SecureAnywhere user name and password.

2. From the Webroot drop-down menu, select Fill Forms, then Add Profile.

The Edit Form Fill Profile dialog opens.

3. In the Profile Name field, enter a name that defines this profile, such as Personal Info or My Visa.
4. Enter as much information as you want in each field. (Click on the tabs for Personal Information, Contact Information, Credit Card Information, Bank Account Information, Custom Fields, and Notes to move between panels.)

The Custom Fields tab can be used to create fields that aren’t listed in this Form Fill dialog. In Text, enter the text from a field on a web page. In Value, enter the information you want automatically filled into that field. (Multiple lines are allowed, but keep in mind that multiple lines can only be filled into a multi-line text box, not a single-line text box.)

If you want to require a SecureAnywhere master password before editing the form fill information, click the checkbox for Require Password Reprompt.

5. When you’re done, click OK.

You can now use the profile to automatically fill your personal data in web fields.

Note: You can also view and edit form-fill profiles in the SecureAnywhere website. Log in to my.webrootanywhere.com and click Go to Passwords.

6. Access a website that requires you to enter personal information into fields (name, address, credit card, and so on).

The yellow Password Manager toolbar opens.

7. Click the Fill Form button and select the profile from the pop-up menu. (If you want to fill only specific fields, use your mouse to highlight the fields before you select the form-fill profile.) If this toolbar does not display, click the drop-down arrow next to the Webroot icon in your browser’s toolbar, then select Fill Forms > profile name > Fill Form.

The Password Manager transfers any information that applies to the fields in the form.

Note: For further instructions, see the Passwords User Guide at Webroot’s SecureAnywhere Help and Product Guides page.
Managing credentials in the Passwords page

You can manage and access all your login credentials in the Passwords page, which is part of your online Webroot account. This web page allows you to view and organize all sites, edit site information, and delete old sites you no longer use.

To manage credentials in the Passwords site:

1. Log in to my.webrootanywhere.com.
2. Click Go to Passwords.

The Passwords web page looks similar to the following example:

3. For further instructions on using the Passwords web page, see the Passwords User Guide at Webroot’s SecureAnywhere Help and Product Guides page.
If you have the *Essentials* or *Complete* editions of Webroot SecureAnywhere, you can use Backup & Sync to designate folders that automatically synchronize to Webroot’s online repository. This repository is a collection of secure servers where your data is safely encrypted and stored. The uploaded data is available from the Backups page of the SecureAnywhere website, on all your computers with Backup & Sync configured, and on your mobile devices with the SecureSync app installed.

After the initial upload, Backup & Sync monitors synchronized folders for updates made to the files (adding, editing, or deleting), then automatically uploads those changes to your SecureAnywhere account. Conversely, if you modify files from within your SecureAnywhere account, changes are synchronized back to your computer. The content between your computer and online account is always kept synchronized. You never need to manually synchronize files yourself.

**Note:** This chapter provides a quick overview of Backup & Sync. For further instructions, see the *Backups User Guide* at Webroot’s [SecureAnywhere Help and Product Guides](https://secureanycwhere.com) page.

To get started with Backup & Sync:

- About Backup & Sync ......................... page 70
- Downloading the Backup & Sync component .......... page 71
- Configuring synchronized folders .................... page 73
- Using the Magic Briefcase ........................ page 75
- Copying files to the Web Archive .................... page 76
- Managing files in the Webroot File Manager .......... page 77
- Managing files in the Backups page .................. page 78
About Backup & Sync

With Backup & Sync, you can rest assured that your important files and photos are automatically copied to the cloud (an online repository of secure servers where your data is encrypted and stored). If your computer or mobile device is lost or stolen, you can instantly retrieve your data from any device with an Internet connection. You can also start editing a file on one device, then continue editing it on another.

There are several methods of securing your data:

- **Synchronizing files and folders.** First, locate the folders on your computer where you store important files and designate them as sync folders. When you save files to those sync folders, Backup & Sync immediately uploads them to the cloud (the Webroot servers) and to any shared folders on other computers. You can access these synchronized files from your online SecureAnywhere account and from your mobile devices with the Webroot SecureSync app installed. (The SecureSync app is only available with the Complete edition.)

  Backup & Sync constantly monitors the sync folders. If it detects a change (an edited file, a new file, or a deleted file), it immediately makes the same change to your online account and to shared folders on other computers. If you are working offline, Backup & Sync automatically picks up changes the next time you connect to the Internet.

  If Backup & Sync detects an edited file, it does not overwrite the original version stored in the cloud. 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) from your online account. If you save changes a sixth time, your most recent version is saved and the oldest version is removed.

  For instructions, see “Downloading the Backup & Sync component” on page 71 and “Configuring synchronized folders” on page 73.

- **Storing files in the Magic Briefcase.** If you don’t want to configure your own sync folders, you can use the preconfigured folder called the Magic Briefcase. Any files you place in the Magic Briefcase are automatically synchronized in the cloud and to any other computers with SecureAnywhere installed.

  The Magic Briefcase is ideal for remotely accessing a small number of files. Do not place a large number of files there if you are concerned about conserving space on your computers.

  For instructions, see “Using the Magic Briefcase” on page 75.

- **Copying files to the Web Archive.** If you have important documents or photos that you want backed up, but not synchronized, you should upload them to the Web Archive. 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.

  The Web Archive folder does not reside on your home computer and you cannot view it from Windows Explorer. The contents of the Web Archive physically reside in the cloud (on the Webroot servers). You can only access them from your online SecureAnywhere account.

  For instructions, see “Copying files to the Web Archive” on page 76.
Downloading the Backup & Sync component

To begin using Backup & Sync, you must first download the Backup & Sync component.

To get started with Backup & Sync:

1. If you have not yet created a Webroot account and enabled Backups, see “Creating a Webroot account” on page 9. When you log in to my.webrootanywhere.com for the first time, be sure to click Set Up Account Now in the Backups panel.

2. From your computer, open the SecureAnywhere main interface (see “Using the main interface” on page 5). Click Backup & Sync, then click Download and Install.
3 If prompted, enter your Webroot account credentials (user name and password).
When the download completes, the Backup & Sync panel displays the following:

![Backup & Sync Panel](image)

4 You can now begin synchronizing or backing up files by following these instructions:
   - “Configuring synchronized folders” on page 73
   - “Using the Magic Briefcase” on page 75
   - “Copying files to the Web Archive” on page 76

Note: This chapter provides a quick overview of Backup & Sync. For further instructions, see the Backups User Guide at Webroot’s SecureAnywhere Help and Product Guides page.
Configuring synchronized folders

To use the synchronization feature, you must first designate folders that you want to use.

*Note:* Once folders are configured, be aware that any changes, deletions, or additions you make in the synchronized folders are also propagated to your online SecureAnywhere account and to other synchronized folders on other computers. For example, if you delete a file in one synchronized folder, it will be deleted across all synchronized folders.

To set up synchronized folders:

1. From the Backup & Sync panel, click Open File Manager.

If you have not yet created synchronized folders, the Setup dialog opens as shown below.
2 Click **Next**.

3 When the Select Sync Folders dialog box opens, select the checkbox next to the folders you want synchronized with the online servers, then click **Next**.

Any files residing in these folders are copied to your online SecureAnywhere account.

4 At the final dialog, click **Finish**.

Backup & Sync immediately begins an upload to the online repository. Depending on the number and size of the synchronized folders, the initial upload may take several minutes, but you can still work on your computer during this process.

5 If you want to see the upload progress, open the Webroot File Manager (from the Backup & Sync panel, click **Open File Manager**). Click the **View** menu, and select **File Transfer Status**.

A File Transfer Status panel opens and shows the name, size, priority, and location.

6 If you want to check that your folders and files were successfully synchronized, open Windows Explorer and access the folders you selected in the setup process. A green checkmark appears next to a file or folder to indicate that it is synchronized.
You can also check your online account in the Backups page. See “Managing files in the Backups page” on page 78.

Note: For further instructions about adding synchronized folders, synchronizing data between multiple computers, and managing backups, see the Backups User Guide at Webroot’s SecureAnywhere Help and Product Guides page.

Using the Magic Briefcase

The Magic Briefcase is a synchronized folder that Webroot has configured for your convenience under your personal Documents folder in Windows. Any files you put in the Magic Briefcase are automatically synchronized with your online account and with any other computers or mobile devices in your account.

We recommend that you use the Magic Briefcase to load files that you may want to access from other devices, as when you are traveling and want to access certain documents remotely. If you have multiple devices that share a SecureAnywhere account, you should not load a large amount of files in the Magic Briefcase. Backup & Sync copies all files placed in the Magic Briefcase to all your other devices with SecureAnywhere installed.

To use the Magic Briefcase:

1. Open Windows Explorer and select a folder or file you want to copy. Right-click to open the pop-up menu and select Copy.
2. Open the Magic Briefcase folder, located in your personal Documents folder in Windows Explorer. If you have trouble finding it, go to the Backup & Sync panel and click Open Magic Briefcase.
3. Paste the file into the Magic Briefcase folder.

When you copy the file to the Magic Briefcase, the file is instantly synchronized to your online SecureAnywhere account and to your other devices with SecureAnywhere installed. A green checkmark next to a file or folder indicates that it is synchronized.

If you want to verify that the file or folder was loaded into your online account, log in to my.webrootanywhere.com and click Go to Backups.
Copying files to the Web Archive

If you have important documents or photos that you want backed up, but not synchronized, you should upload them to the Web Archive. 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.

Although you can view the contents of the Web Archive folder from the Webroot File Manager, this folder does not reside on your home computer and you cannot view it from Windows Explorer. The contents of the Web Archive physically reside on the Webroot servers, accessible from your SecureAnywhere account.

To copy files to the Web Archive:

1. Open the main interface (see “Using the main interface” on page 5).
2. From the Backup & Sync panel, click Open File Manager.
3. In the Webroot File Manager, right-click Web Archive to display the pop-up menu, then select either Import Files or Import Folder.
4. From the dialog that opens, select the files or folders you want archived.
The files are instantly copied to the Web Archive in your online SecureAnywhere account. The Webroot File Manager shows the folders or files under the Web Archive folder. The Status column in the middle panel shows “Backed Up” next to each file that uploaded successfully.

**Note:** Your files remain in their original location. Backup & Sync does not move the files, only copies them.

If you want to verify that the files were copied into your online account, log in to [my.webrootanywhere.com](http://my.webrootanywhere.com) and click Go to Backups.

### Managing files in the Webroot File Manager

You can manage synchronized folders and files through the Webroot File Manager, which is an Explorer-type interface available on your computer. The Webroot File Manager enables you to open, copy, move, and delete files in your synchronized folders.

You do not need to connect to the Internet to view the Webroot File Manager. However, when you are connected, you can manage files online and across all your computers that have the Webroot software installed. For example, if you want to access a document that resides on your computer at home and edit the document on your laptop while you’re traveling, you can use the Webroot File Manager to open and edit the file.

**To open the Webroot File Manager:**

1. Open the main interface (see “Using the main interface” on page 5).
2. From the Backup & Sync panel, click **Open File Manager**.

The Webroot File Manager opens, similar to the following example. The left panel shows synchronized folders, the Magic Briefcase, the Web Archive, and Deleted Files. If you installed SecureAnywhere on multiple computers, the left panel lists each computer. The right panel shows more detail about whatever you select in the left panel.
Note: For more information about using the Webroot File Manager, see the Backups User Guide at Webroot’s SecureAnywhere Help and Product Guides page.

Managing files in the Backups page

You can manage and access all your synchronized and backed up files in the Backups page, which is part of your online Webroot account. This web page allows you to open, copy, move, delete, and share files in your synchronized folders. You can access these files from any computer or mobile device with an Internet connection and browser.

To manage files in the Backups page:

1. Log in to my.webrootanywhere.com.
2. Click Go to Backups.
The Backups web page looks similar to the following example:

![Image of the Backups web page]

For further instructions on using the Backups web page, see the *Backups User Guide* at Webroot’s [SecureAnywhere Help and Product Guides](https://www.webroot.com/support) page.
If you have the Essentials or Complete editions of Webroot SecureAnywhere, you can use the System Cleaner to remove all traces of your web browsing history, files that show your computer use, and other files that reveal your activity. By removing these items, you can protect your privacy. No one else who has access to your computer can see what websites you have visited or what search terms you have used.

The System Cleaner also removes unnecessary files that consume valuable disk space, such as files in the Recycle Bin or Windows temporary files.

To use the System Cleaner, see the following topics:

- About cleanups ........................................... page 82
- Running a cleanup ................................. page 83
- Changing Windows Desktop settings .......... page 85
- Changing Windows System settings .......... page 87
- Changing Application settings ................. page 89
- Changing Internet Explorer settings .......... page 91
- Using Secure File Removal ....................... page 93
- Viewing the Cleanup log ......................... page 95
About cleanups

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 Cleaner, 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 Cleaner 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: Cleanups remove unnecessary files and traces, not malware threats. Malware (spyware and viruses) are removed during scans (see “About scans” on page 14). You can think of the System Cleaner as the housekeeper for your computer, while the Scanner serves as the security guard.

The System Cleaner does not run automatically; you need to run it yourself. Before the first cleanup, select all the items you want removed. You can select these items in the Cleanup Settings panel (click System Tools, the System Cleaner tab, then the Cleanup Settings link). Then click the Clean Up Now button to remove the items.
Running a cleanup

The System Cleaner permanently removes all items selected in the Cleanup settings. These settings may include your web browsing history, files that show your computer use, and other files that reveal your activity.

To check your cleanup options:

1. Open the main interface (see “Using the main interface” on page 5).
2. Click System Tools, the System Cleaner tab, then the Cleanup Settings link.

The System Cleaner Settings panel opens.
3 Click each of the categories on the left side of the panel. On the right side, click in the checkboxes to select or deselect items to clean up. Items with a checkmark will be removed.

For more information about the settings, see:
• “Changing Windows Desktop settings” on page 85
• “Changing Windows System settings” on page 87
• “Changing Application settings” on page 89
• “Changing Internet Explorer settings” on page 91

4 In the System Cleaner Settings panel, select **Secure File Removal**. By default, file removal is set to “Normal,” which means items are deleted permanently (bypassing the Recycle Bin). However, data recovery utilities may be able to restore the files. If you want to make sure files can never be recovered, move the slider to **Medium** or **Maximum**. See “Using Secure File Removal” on page 93 for more information.

5 When you’re done selecting cleanup settings, click **Save All**, then click **Close**.

6 From the System Cleaner panel, click the **Clean Up Now** button.

The progress panel shows items as they are removed, along with the space recovered.
Changing Windows Desktop settings

The System Cleaner can remove files in the Recycle Bin and the traces of what files you recently opened or tried to locate in a search. While these history traces can be helpful, they also reveal your activity to other people using your computer. To maintain your privacy, you can remove all these traces. (The cleanup does not delete the files, just the places where Windows tracks your activity.)

To change Windows Desktop settings:

1. Open the main interface (see “Using the main interface” on page 5).
2. Click System Tools, the System Cleaner tab, then the Cleanup Settings link.

The System Cleaner Settings panel opens, with Windows Desktop highlighted on the left.
3 On the right side, click in the checkboxes to select or deselect items. Items with a checkmark will be cleaned. When you’re done, click the **Save All** button.

The settings are described in the table below.

<table>
<thead>
<tr>
<th>Windows Desktop Cleanup options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recycle Bin</td>
<td>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.</td>
</tr>
<tr>
<td>Recent document history</td>
<td>Clears the history of recently opened files, which is accessible from the Windows Start menu.</td>
</tr>
<tr>
<td>Start Menu click history</td>
<td>Clears the history of shortcuts to programs that you recently opened using the Start menu.</td>
</tr>
<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. <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. 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>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>
</tbody>
</table>
Changing Windows System settings

The System Cleaner can remove temporary files and traces left by the Windows operating system. These files and traces can sometimes be a threat to your privacy. They can also consume a lot of disk space if you don’t delete them once in awhile.

To change Windows System settings:

1. Open the main interface (see “Using the main interface” on page 5).
2. Click System Tools, the System Cleaner tab, then the Cleanup Settings link.
3. On the left side of the panel, click Windows System.
4 On the right side, click in the checkboxes to select or deselect items. Items with a checkmark will be cleaned. When you're done, click the **Save All** button.

The settings are described in the table below.

### Windows System cleanup options

<table>
<thead>
<tr>
<th>Option</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 use either the Copy or Cut function from any Windows program.</td>
</tr>
<tr>
<td>Windows temp folder</td>
<td>Deletes all files and folders in the Windows temporary folder, but not files that are in use by an open program. This folder is usually: C:\Windows\Temp. 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>System temp folder</td>
<td>Deletes all files and folders in the system temporary folder, but not files that are in use by an open program. This folder is usually in C:\Documents and Settings[username]\Local Settings\Temp. 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>Windows update temp folder</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. These files are normally in C:\Windows\Software\Distribution\Download. 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>Registry streams</td>
<td>Clears the history of recent changes you made to the Windows registry. (This option does not delete the registry changes themselves.)</td>
</tr>
<tr>
<td>Default logon user history</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 user name 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>Memory dump files</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>CD burning storage folder</td>
<td>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</td>
</tr>
<tr>
<td>Flash Cookies</td>
<td>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.)</td>
</tr>
</tbody>
</table>
Changing Application settings

The System Cleaner can remove the traces left behind by applications, such as a list of recently opened files. While these history traces can be helpful, they also reveal your activity to other people using your computer. To maintain your privacy, you can remove all these traces. (The cleanup does not delete the files, just the places where Windows tracks your activity.)

To change Application settings:

1. Open the main interface (see “Using the main interface” on page 5).
2. Click System Tools, the System Cleaner tab, then the Applications link.

The System Cleaner Settings panel opens, with Applications highlighted on the left. Applications currently installed on your computer will appear in this panel.
3 On the right side, click in the checkboxes to select or deselect applications you want cleaned.

   The System Cleaner will remove file history traces for applications with a checkmark.

4 When you’re done, click the **Save All** button.
Changing Internet Explorer settings

The System Cleaner can remove temporary files and traces left by the Windows operating system. While these history traces can be helpful, they also reveal your activity to other people and can consume lots of disk space. To maintain your privacy and system performance, you can remove all these files and traces. (The cleanup does not delete the files, just the places where IE tracks your activity.)

To change Internet Explorer settings:

1. Open the main interface (see “Using the main interface” on page 5).
2. Click System Tools, the System Cleaner tab, then the Cleanup Settings link.

   The System Cleaner Settings panel opens.

3. On the left side of the panel, click Internet Explorer.
4 On the right side, click in the checkboxes to select or deselect items. Items with a checkmark will be cleaned. When you’re done, click the Save All button.

The settings are described in the table below.

<table>
<thead>
<tr>
<th>Internet Explorer Cleanup Options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address bar history</strong></td>
</tr>
<tr>
<td>Removes the list of recently visited websites, which is stored as part of Internet Explorer’s AutoComplete feature. You see this list when you click the arrow on the right side of the Address drop-down list at the top of the Internet Explorer browser.</td>
</tr>
<tr>
<td><strong>Cookies</strong></td>
</tr>
<tr>
<td>Deletes all cookies from your computer. Cookies are small files that store information about your interaction with a website and may reveal what sites you visited. Be aware that if you remove all cookie files, some websites will not “remember” you. This means that you may need to re-enter passwords, shopping cart items, and other entries that these cookies stored.</td>
</tr>
<tr>
<td><strong>Temporary Internet files</strong></td>
</tr>
<tr>
<td>Deletes copies of stored web pages that you visited recently. 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>URL history</strong></td>
</tr>
<tr>
<td>Deletes the list of recently visited websites. You see this list when you click History on the Internet Explorer toolbar. While this history can be helpful, it also reveals your visited sites to other people using your computer.</td>
</tr>
<tr>
<td><strong>Setup log</strong></td>
</tr>
<tr>
<td>Deletes log files created when you update Internet Explorer. After you install the updates, you no longer need these files.</td>
</tr>
<tr>
<td><strong>MS download folder</strong></td>
</tr>
<tr>
<td>Deletes the contents in the folder that stores files you last downloaded using Internet Explorer. After downloading, you no longer need these files.</td>
</tr>
<tr>
<td><strong>MediaPlayer bar history</strong></td>
</tr>
<tr>
<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>
</tbody>
</table>
Using Secure File Removal

The System Cleaner can permanently remove files in a “shredding” process, which overwrites them with random characters. This shredding feature is a convenient way to make sure no one can ever access your files with a recovery tool. (Although you may think that you are permanently deleting files when you empty the Recycle Bin or when you use Shift-Delete, in actuality, you are only removing the operating system’s record of the file, not the physical file itself.)

To use Secure File Removal:

1. Open the main interface (see “Using the main interface” on page 5).
2. Click System Tools, the System Cleaner tab, then the Secure File Removal link.
The Secure File Removal panel opens. By default, file removal is set to “Normal,” which means items are deleted permanently (bypassing the Recycle Bin). Data recovery utilities may be able to restore the files.

3 If you want to make sure files can never be recovered, move the slider to **Medium** or **Maximum**.

“Medium” overwrites files with three passes, whereas “Maximum” overwrites files with seven passes and cleans the space around the files.

Be aware that cleanup operations take longer when moved to Medium or Maximum.

4 Click **Save All**.
Viewing the Cleanup log

You can view a log of what the System Cleaner removed.

To view the cleanup log:

1. From the main interface, click System Tools, the System Cleaner tab.
2. Click the View Cleanup Log link.

The log opens in Notepad and shows a list of files and traces removed.
System Control functions include tools for adjusting the threat-detection settings on computer processes and for isolating the actions of a malware program in a “sandbox” to observe its behavior.

See the following topics:

- Controlling active processes ................. page 98
- Using SafeStart Sandbox ...................... page 99
Controlling active processes

The Active Processes feature allows you to 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 adjust settings for active processes:

1. Open the main interface (see “Using the main interface” on page 5).
2. Click System Tools.
3. In the System Control tab, click the Start button under Control Active Processes.
   The Active Processes (Advanced) dialog opens.
4. For each process, you can select the radio button for:
   - **Trust**: The process is allowed to run on your system.
   - **Monitor**: Webroot SecureAnywhere will watch the process and open an alert on suspicious activity.
   - **Block**: The process is blocked from running on your system. Do NOT block a process unless you are absolutely certain it is non-essential.

If you want to terminate all untrusted processes, click **Kill Untrusted Processes**.
Using SafeStart Sandbox

If you are an advanced user and want to test a program you believe is malware, you can first execute 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 legitimate programs.

To execute a file in the SafeStart Sandbox:

1. Open the main interface (see “Using the main interface” on page 5).
2. Click **System Tools**.
3. In the System Control tab, click the **Start** button under SafeStart Sandbox.
   The SafeStart (Advanced) dialog opens.

4. You can select the file either by clicking the **Browse** button or by entering the filename and location in the **Command-line** field.

5. If you want to use some advanced features for controlling how the program is allowed to execute, select a checkbox to disable a function (uncheck the box) or activate it (check the box). When you’re done, click the **Start** button.
Webroot SecureAnywhere includes reports for scan activity, real-time protection statistics, and process executions. If you discover a particular file that is causing problems on your system, you can submit a file to Webroot for analysis.

See the following topics:

- Saving a scan log ............... page 102
- Viewing the protection statistics ........ page 103
- Viewing the execution history ........ page 104
- Submitting a file .................... page 105
Saving a scan log

If you want to investigate what Webroot 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. Open the main interface (see “Using the main interface” on page 5).
2. Click System Tools, then click the Reports tab.
3. Under Scan Log, click the Save as button.

4. Enter a filename and click Save.
Viewing the protection statistics

Protection Statistics are mainly used by Webroot Support to view the background processes that Webroot SecureAnywhere is monitoring.

To view the protection statistics:

1. Open the main interface (see “Using the main interface” on page 5).
2. Click System Tools, then click the Reports tab.
3. Under Protection Statistics, click the View button.

The Protection Statistics dialog opens.

4. Click on an event in the left column to view more detailed information.
Viewing the execution history

The Execution History is mainly used by Technical Support to see when and where a virus entered the system.

To view the execution history:

1. Open the main interface (see “Using the main interface” on page 5).
2. Click System Tools, then click the Reports tab.
3. Under Execution History (Advanced), click the View button.

The Execution History (Advanced) dialog opens.

4. Click on a process to view more detailed information, then click the More Info button.
Submitting a file

If a file on your system is causing problems or if you know a file is safe and want it reclassified, you can send the file to Webroot for analysis.

To submit a file:

1. From the main interface, click **System Tools**.
2. Click the **Submit a File** tab.
   
The following dialog opens.

3. Select the file by clicking the **Browse** button.
4. Select any of the checkboxes that apply to this file.
5. Enter any additional information in the bottom field.
6. Click **Send**.
Your Webroot account includes information about your software licenses and other details. Your account information is available from the My Account panel of the SecureAnywhere program or from my.webrootanywhere.com, which is the online interface.

To view or manage account settings from the SecureAnywhere program, see the following topics:

- About My Account .......................... page 108
- Activating a new keycode ..................... page 109
- Upgrading or renewing the software ............. page 110
- Checking for software updates ................. page 111
About My Account

The My Account panel shows your keycode, program version number, and the time remaining on your subscription. To view account details, open the main interface and click the My Account link at the bottom left.

Your account information appears in the My Account panel:
Activating a new keycode

If you have a new keycode, you can activate it as follows:

1. Open the main interface (see “Using the main interface” on page 5).
2. Click My Account.
3. In the Account panel, click **Activate a new keycode**.
4. In the dialog, enter the keycode and click the **Activate** button.
Upgrading or renewing the software

From the My Account panel, you can renew your subscription or upgrade to another Webroot SecureAnywhere version.

To upgrade or renew the software:

1. Open the main interface (see “Using the main interface” on page 5).
2. Click My Account.
3. In the Account panel, click Upgrade or renew.

The Webroot website opens. From here, you can purchase an upgrade to your software.
Checking for software updates

If you disabled automatic software updates from the Basic Configuration panel, you can manually check for software updates yourself in the My Account panel.

To check for updates:

1. Open the main interface (see “Using the main interface” on page 5).
2. Click My Account.
3. In the Account panel, click Check for software updates.

If a newer version exists, Webroot downloads the updates to your system.
To manage program settings, see the following topics:

- Setting basic configuration .............................. page 114
- Setting self protection ................................. page 116
- Setting access control ................................. page 117
- Defining proxy settings ............................... page 118
- Setting heuristics ....................................... page 120
- Importing or exporting settings ....................... page 123
Setting basic configuration

You can change the behavior of the program in the Basic Configuration settings.

To change Basic Configuration settings:

1. Open the main interface (see “Using the main interface” on page 5).
   At the bottom left, click Settings.

   ![Settings dialog]

   The Settings dialog opens to Basic Configuration.

2. To change a setting, select its checkbox to disable it (uncheck the box) or activate it (check the box). When you’re done, click Save All.

   The settings are described in the table below.

### Basic Configuration settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show a Webroot shortcut on the desktop</td>
<td>Provides quick, double-click access to the main interface by placing the shortcut icon on your desktop.</td>
</tr>
<tr>
<td>Show a system tray icon</td>
<td>Provides quick access to Webroot SecureAnywhere functions by placing the Webroot icon on your desktop:</td>
</tr>
<tr>
<td></td>
<td>![Webroot icon]</td>
</tr>
<tr>
<td></td>
<td>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 splash screen on bootup</td>
<td>Opens the Webroot splash screen on system startup, which lets you know that the program is running and protecting your computer.</td>
</tr>
<tr>
<td>Basic Configuration settings (continued)</td>
<td></td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Show Webroot in the Start Menu</strong></td>
<td>Lists Webroot SecureAnywhere in the Windows Startup menu items.</td>
</tr>
<tr>
<td><strong>Show Webroot in Add/Remove Programs</strong></td>
<td>Lists Webroot SecureAnywhere in the Windows Add/Remove Programs panel.</td>
</tr>
<tr>
<td><strong>Show Webroot in Windows Security Center</strong></td>
<td>Lists Webroot SecureAnywhere in the Windows Security Center, under Virus Protection information.</td>
</tr>
<tr>
<td><strong>Hide the Webroot license keycode on-screen</strong></td>
<td>Blocks your license keycode from displaying on the My Account panel.</td>
</tr>
<tr>
<td><strong>Automatically download and apply updates</strong></td>
<td>Downloads product updates automatically without alerting you.</td>
</tr>
<tr>
<td><strong>Operate background functions using fewer CPU resources</strong></td>
<td>Saves CPU resources by running non-scan related functions in the background.</td>
</tr>
<tr>
<td><strong>Favor low disk usage over verbose logging (fewer details stored in logs)</strong></td>
<td>Saves disk resources by saving only the last four log items.</td>
</tr>
<tr>
<td><strong>Lower resource usage when intensive applications or games are detected</strong></td>
<td>Suppresses Webroot SecureAnywhere functions while you are gaming, watching videos, or using other intensive applications.</td>
</tr>
<tr>
<td><strong>Allow Webroot to be shut down manually</strong></td>
<td>Displays a Shutdown command in the system tray menu. If you deselect this option, the Shutdown command is removed from the menu.</td>
</tr>
<tr>
<td><strong>Force non-critical notifications into the background</strong></td>
<td>Suppresses information-only messages from appearing in the system tray.</td>
</tr>
<tr>
<td><strong>Fade out warning messages automatically</strong></td>
<td>Closes warning dialogs in the system tray after a few seconds. If you disable this option, you must manually click on a message to close it.</td>
</tr>
<tr>
<td><strong>Store Execution History details</strong></td>
<td>Stores data for the Execution History logs, available under Reports.</td>
</tr>
</tbody>
</table>
Setting self protection

Self Protection prevents malicious software from modifying the Webroot SecureAnywhere program settings and processes. If Webroot SecureAnywhere detects that another product is attempting to interfere with its functions, it launches a protective scan to look for threats. It will also update the internal self protection status to prevent incompatibilities with other software.

We recommend that you keep Self Protection at the Maximum setting. However, if you use other security software along with Webroot SecureAnywhere, you should adjust Self Protection to the Medium or Minimum setting. The Maximum setting may interfere with other security software.

To change Self Protection settings:

1. Open the main interface (see “Using the main interface” on page 5).
   - At the bottom left, click Settings.

2. In the Settings panel, click Self Protection.

3. Click a radio button for Minimum, Medium, or Maximum security.
   - Note: If you want to turn off self protection, uncheck the Enable self protection response cloaking box.

4. Click Save All.
Setting access control

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 the Webroot SecureAnywhere software.

To change Access Control settings:

1. Open the main interface (see “Using the main interface” on page 5).
   
   At the bottom left, click Settings.

2. In the Settings panel, click Access Control.

3. If you want to change a setting, select its checkbox to disable it (uncheck the box) or activate it (check the box). When you’re done, click Save All.

Settings are described in the table below.

<table>
<thead>
<tr>
<th>Access Control settings</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>Allow users to scan without a password</td>
<td>Allows any user to scan the system, even if password protection is enabled.</td>
</tr>
<tr>
<td>Allow users to remove threats without a password</td>
<td>Allows any user to remove threats, even if password protection is enabled.</td>
</tr>
</tbody>
</table>
Defining proxy 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 further information about your proxy environment, contact your proxy server’s administrator.

To define proxy settings:

1. Open the main interface (see “Using the main interface” on page 5).
   At the bottom left, click Settings.

2. From the Settings panel, click Proxy.
3 Enter the proxy settings as described below, then click the **Save All** button.

<table>
<thead>
<tr>
<th><strong>Proxy settings</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Proxy Type</strong></td>
</tr>
<tr>
<td><strong>Authentication Method</strong></td>
</tr>
<tr>
<td><strong>Host</strong></td>
</tr>
<tr>
<td><strong>Port</strong></td>
</tr>
<tr>
<td><strong>Username</strong></td>
</tr>
<tr>
<td><strong>Password</strong></td>
</tr>
</tbody>
</table>
Setting heuristics

With Heuristics settings, you can adjust the level of threat analysis that Webroot SecureAnywhere performs when scanning your computer. Heuristics can be adjusted for separate areas of your computer, including the local drive, USB drives, the Internet, the network, CD/DVDs, and when your computer is offline. We recommend that you keep Heuristics at their default settings, unless you are an advanced user and understand how changing settings will impact threat detection.

Note: If you want to adjust Heuristics settings for all the computers managed in your SecureAnywhere account, go to the PC Security web page (see “Viewing the PC security status online” on page 11).

Webroot SecureAnywhere includes three types of heuristics:

- **Advanced Heuristics.** Analyzes new programs for suspicious actions that are typical of malware.

- **Age Heuristics.** Analyzes new programs based on the amount of time the program has been in the community. Legitimate programs are generally used in a community for a long time, but malware often has a short lifespan.

- **Popularity Heuristics.** Analyzes new programs based on statistics for how often the program is used in the community and how often it changes. Legitimate programs do not change quickly, but malware often mutates at a rapid pace. Malware may install as a unique copy on every computer, making it statistically “unpopular.”

To change Heuristics settings:

1. Open the main interface (see “Using the main interface” on page 5). At the bottom left, click **Settings**.

2. In the Settings panel, click **Heuristics**.
3 Select the tab for the area you want to change heuristics settings: Local, USB, Internet, Network, CD/DVD, or Offline.

4 Select the radio buttons and slide bars to adjust the settings, which are described in the following tables. When you’re done, click the Save All button.

### Radio buttons - additional heuristic options

<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>Apply advanced heuristics before Age/Popularity heuristics</td>
<td>Warns against new programs as well as old programs that exhibit suspicious behavior.</td>
</tr>
<tr>
<td>Apply advanced heuristics after Age/Popularity heuristics</td>
<td>Warns against suspicious programs detected with Advanced Heuristics, based on Age/Popularity settings.</td>
</tr>
<tr>
<td>Warn when new programs execute that are not trusted</td>
<td>Warns when malicious, suspicious, or unknown programs try to execute. (This setting may result in false detections.)</td>
</tr>
</tbody>
</table>

### Slider - Advanced Heuristics

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>Turns off Advanced Heuristics for the area selected in the tab, leaving it vulnerable to new threats. (However, it will still be protected against known threats.)</td>
</tr>
<tr>
<td>Low</td>
<td>Detects programs with a high level of malicious activity. This setting ignores some suspicious behavior and allows most programs to run.</td>
</tr>
<tr>
<td>Medium</td>
<td>Balances detection versus false alarms by using our tuned heuristics in the centralized community database.</td>
</tr>
<tr>
<td>High</td>
<td>Protects against a wide range of new threats. Use this setting if you think your system is infected or at very high risk. (This setting may result in false detections.)</td>
</tr>
</tbody>
</table>
Slider - Advanced Heuristics  *(continued)*

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum</td>
<td>Provides the highest level of protection against new threats. Use this setting if you think that your system is infected or at very high risk. (This setting may result in false detections.)</td>
</tr>
</tbody>
</table>

Slider - Age Heuristics

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>Turns off Age Heuristics for the area selected in the tab, leaving it vulnerable to new threats. (However, it will still be protected against known threats.)</td>
</tr>
<tr>
<td>Low</td>
<td>Detects programs that have been created or modified very recently.</td>
</tr>
<tr>
<td>Medium</td>
<td>Detects programs that are fairly new and not trusted, preventing zero-day or zero-hour attacks. We recommend using this setting if you do not install unpopular programs and want an extra degree of security to prevent mutating threats.</td>
</tr>
<tr>
<td>High</td>
<td>Detects programs that have been created or modified in a relatively short time and are not trusted. This setting is recommended only if you rarely install new programs and if you feel that your system is relatively constant. This setting may generate a higher level of false alarms on more obscure or unpopular programs.</td>
</tr>
<tr>
<td>Maximum</td>
<td>Detects all untrusted programs that have been created or modified fairly recently. You should only use this setting if your computer is in a high-risk situation or if you think that it is currently infected.</td>
</tr>
</tbody>
</table>

Slider - Popularity Heuristics

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>Turns off Popularity Heuristics for the area selected in the tab, leaving it vulnerable to new threats. (However, it will still be protected against known threats.)</td>
</tr>
<tr>
<td>Low</td>
<td>Detects programs that have been seen for the first time. This setting is recommended if you frequently install new programs, beta programs, or you are a software developer who frequently creates new programs.</td>
</tr>
<tr>
<td>Medium</td>
<td>Detects unpopular and mutating programs, preventing zero-day and zero-hour attacks. This setting is recommended if you do not frequently install new programs and want an extra level of protection over standard settings.</td>
</tr>
<tr>
<td>High</td>
<td>Detects programs that a significant percentage of the community has seen. This setting is recommended if you do not install new programs and suspect that your system is infected.</td>
</tr>
<tr>
<td>Maximum</td>
<td>Detects programs that a large percentage of the community has seen. This setting is recommended if you think your system is at a very high risk and are willing to accept that you may receive false alarms because of the strict heuristic rules.</td>
</tr>
</tbody>
</table>
Importing or exporting settings

If you changed the Webroot SecureAnywhere configuration, you can back up those new settings. A backup of your configuration is helpful if you ever need to reinstall the software or transfer your configuration to another computer.

To import or export settings:

1. Open the main interface (see “Using the main interface” on page 5).
   At the bottom left, click Settings.

2. From the left panel, click Import/Export.
   The following panel opens.

3. To transfer your settings to another computer, click Export Settings. Enter a name for the file and click Save. These settings can be from an external hard drive or USB drive. Depending on the file size, this may take a few seconds.

4. Access the other computer and click Import Settings. Select the file and click Save.
If you want to open a support ticket with Webroot Support, go to:
https://www.webrootanywhere.com/support
To uninstall the Webroot software:

1. From the Start menu (click Start in the system tray), point to All Programs, then Webroot, then Tools, then Uninstall Webroot.
2. At the prompt, click Yes to continue.
   
   Webroot removes the files from your computer.
The Webroot SecureAnywhere license agreement is available at:
http://detail.webrootanywhere.com/eula.asp
access control settings 117
account
   activating new keycode 109
   adding users and changing settings 10
   checking for software updates 111
   creating a Webroot account 9
   upgrading to new version 110
   viewing details in program 108
Active processes 98
Add/Remove programs, showing or hiding
   SecureAnywhere from 115
address bar history, removing 92
admin account 9
advanced heuristics 121
age heuristics 122
alerts 7
   fading out automatically 115
firewall 35
Identity shield 55
   remembering responses in 26
   setting auto-blocking and quarantine 26
suppressing from system tray 115
antimalware tools 45
applications
   adjusting threat-detection settings 98
   clearing activity traces 89
   providing additional security for 53
archived files, including in scans 22
autocomplete form data, clearing 93
CAPTCHA, enabling or disabling 118
CD burning storage folder, clearing 88
cleanup log 95
cleanup
   See System Cleaner
clipboard contents, clearing 88
clipboard data, shielding 57
compressed files, including in scans 22
cookies
   blocking third-party cookies from installing 52
   protecting against cookie-stealers 57
   removing for Internet Explorer browsers 92
Core System shield 29
CPU resources, using fewer 115
cross-site scripting attacks, shielding 32
custom scan 17
deep scan 17
Detection Configuration 43
disabling SecureAnywhere 6
disk space requirements 2
document history, clearing 86
execution history 104
Execution History logs, storing data for 115
file detection management 43
firewall 33
   changing alert settings 35
   enabling or disabling 34
   how the firewall works 34
   monitoring processes and applications 36
   used with Windows firewall 34
form-fill profiles 66
full scan 17
gaming
   suppressing SecureAnywhere functions 115
   turning off scans during games 20
heuristics 120
history, execution 104
Hosts file, shielding 30

I
Identity Protection 49
  changing shield settings 51
  enabling or disabling 50
  how it works 50
  protected applications 53
  protected websites 55
index.dat databases, clearing 93
installing the software 2
Internet Explorer, clearing activity traces 91
Internet requirements 2

K
kernal memory, shielding 30
keycode
  activating new code 109
  adding others to your Webroot account 10
  hiding from My Account screen 115
installation requirement 2
keyloggers, shielding 57

L
license agreement 129
lock icon 53
login credentials
  saving with Password Manager 63
  shielding 52
logon user history, clearing 88
logs
  cleanup 95
  saving resources in logging 115
  scan 6, 102
  storing data for Execution History 115
LSP chain, shielding 30

M
Magic Briefcase folder 75
main interface 5
man-in-the-browser attacks, shielding 57
man-in-the-middle attacks, shielding 52, 57
manual threat removal 46
master account 9
Master Boot Record (MBR) scanning 21
MediaPlayer bar history, clearing 92
memory dump files, clearing 88
MS download folder, clearing 92
My Account 107
  activating new keycode 109
  checking for software updates 111
  upgrading or renewing software 110
  viewing details 108

N
network applications, monitoring 36

O
offline threat protection 26
opening SecureAnywhere 5

P
padlock icon 53
Password Manager 59
  capturing login credentials 63
  creating form-fill profiles 66
  downloading components and getting started 61
  logging into websites 65
  overview on how to use 60
  setting up online access 62
  toolbar in browser 62
password protection, enabling for SecureAnywhere 117
Passwords page
  setting up account 62
  using 68
PC Security web page 11
phishing, protecting against 52, 57
popularity heuristics 122
processes
  adjusting threat-detection settings 98
  shielding 30
program settings 113
protected applications 53
protected websites 55
protection statistics 103
proxy server settings 118

Q
quarantine 39
  antimalware tools 45
  auto-quarantine during shielding 26
  enabling password for threat removal 117
  file detection configuration 43
  how it works 40
  restoring or deleting items 42
  saving threat log 47
  viewing items in 41
quick scan 17

R
RAM requirements 2
Realtime shield 25
Recycle Bin, clearing 86
registering SecureAnywhere 9
registry streams, clearing 88
removal script 46
removing SecureAnywhere 127
renewing subscription 110
Index
System Control 97
  active processes 98
  using SafeStart sandbox 99
system policies, resetting 46
system requirements 2
system temp folder, clearing 88
system tray
  menu 6
  showing or hiding the Webroot icon 114

T
Technical Support
  opening a support ticket 125
  submitting a file to 105
temporary Internet files, clearing 92
threat log 47
threat removal
  manual 46
  scanning 13
threats found during scan 16
toolbar, Webroot 62
tools
  antimalware 45
  enabling access to other users 118
  system control 97
tray menu 6
turning off SecureAnywhere 6

U
uninstallation
  enabling access to other users 118
  instructions for 127
  updating SecureAnywhere
    enabling or disabling automatic downloads 115
    from main interface 111
    from system tray 6
upgrading to new version 110
URL grabbing attacks, shielding 57
URL history, clearing for Internet Explorer 92
users, controlling access to SecureAnywhere 117

W
wallpaper, resetting 46
warnings
  See alerts
Web Archive 76
Web Threat shield 31
Webroot account 9
Webroot File Manager 77
Webroot support
  See Technical Support
Webroot website 9
websites
  analyzing for threats 32
  protecting from malicious content 55
  shielding from online identity threats 51
  whitelisting 32
Windows
  cleaning activity traces 85
  clearing operating system traces 87
  clearing temp folder 88
  system requirements for SecureAnywhere 2
Windows Security Center, showing or hiding SecureAnywhere from 115