8: Backup & Sync ................................................................. 85
   About the Backup & Sync Manager ........................................ 86
   Getting started with Backup & Sync ...................................... 87
   Downloading the Backup & Sync component .............................. 87
   Configuring synchronized folders (first-time setup) .................. 88
   Managing synchronized folders ........................................... 91
   Adding synchronized folders .............................................. 91
   Removing folders from synchronization .................................. 93
   Synchronizing data between multiple computers ...................... 95
   Using the Magic Briefcase .................................................. 98
   Using the Webroot File Manager .......................................... 99
   Menus ............................................................................ 100
   Toolbar .......................................................................... 100
   Left panel (folder tree) .......................................................... 100
   Middle panel ..................................................................... 101
   Status bar (bottom taskbar) ................................................... 101
   Commands ........................................................................ 101
   Copying files to the Web Archive ......................................... 104
   Managing files in the Backups site ....................................... 106
   My Folders and Files .......................................................... 106
   Recent Events ..................................................................... 108
   Photos ............................................................................. 108
   Accessing files remotely ....................................................... 110
   Downloading files ............................................................... 110
   Downloading photo albums .................................................... 111
   Editing files remotely .......................................................... 112
   Managing photo albums ....................................................... 114
   Sharing photo albums with others ........................................ 118
   Publishing photo albums to Facebook .................................... 120
   Sending files to others .......................................................... 120
   Restoring data ..................................................................... 123
   Restoring all data to a new computer ..................................... 123
   Retrieving an older version of a file ...................................... 124
   Retrieving a file or folder you accidentally deleted .................. 125
   Restoring files from the Web Archive .................................... 126
   Adding more storage space .................................................... 127

9: System Cleaner ................................................................. 129
   About cleansups ................................................................ 130
   Running a cleanup ............................................................. 131
   Changing Windows Desktop settings ..................................... 133
   Changing Windows System settings ...................................... 135
   Changing Application settings ............................................. 137
Changing Internet Explorer settings ................................................................. 138
Using Secure File Removal ........................................................................... 140
Viewing the Cleanup log ............................................................................. 142

10: System Control ....................................................................................... 143
Controlling active processes ...................................................................... 144
Using SafeStart Sandbox ............................................................................ 145

11: Reports ................................................................................................... 147
Saving a scan log .......................................................................................... 148
Viewing the protection statistics .................................................................. 149
Viewing the execution history ....................................................................... 150
Submitting a file ............................................................................................ 151

12: My Account ............................................................................................. 153
About My Account ........................................................................................ 154
Activating a new keycode ............................................................................... 155
Upgrading or renewing the software .............................................................. 156
Checking for software updates ..................................................................... 157

13: Settings .................................................................................................. 159
Setting basic configuration ........................................................................... 160
Setting self protection ................................................................................... 162
Setting access control ................................................................................... 163
Defining proxy settings ................................................................................. 164
Setting heuristics ........................................................................................... 165
Importing or exporting settings ..................................................................... 168

A: Webroot Support ...................................................................................... 169
B: Uninstalling the program ......................................................................... 171
C: License agreement ..................................................................................... 173
Index ............................................................................................................. 175
1: Getting Started

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

<table>
<thead>
<tr>
<th>Software</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Webroot SecureAnywhere AntiVirus</td>
<td>Standard version that provides protection against viruses, spyware, and other threats.</td>
</tr>
<tr>
<td>Webroot SecureAnywhere Essentials</td>
<td>All the protection of the AntiVirus version, 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 version and the Essentials version, plus:</td>
</tr>
<tr>
<td></td>
<td>• Password management.</td>
</tr>
</tbody>
</table>

To get started with Webroot SecureAnywhere, see the following:

- “Installing the software” on page 2
- “Using the main interface” on page 5
- “Creating a Webroot account” on page 8
- “Using the PC Security site” on page 10
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 or five computers.

To install the program:

1. Before you begin:
   • Read the license agreement at http://detail.webrootanywhere.com/eula.asp.
   • Make sure your system meets these minimum requirements:

<table>
<thead>
<tr>
<th>Minimum system requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows operating system:</td>
</tr>
<tr>
<td>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>RAM: 128 MB (minimum); 2 GB recommended on Windows Vista and Windows 7</td>
</tr>
<tr>
<td>Hard disk space: 10 MB</td>
</tr>
<tr>
<td>Internet/Browser: 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>Note: 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.
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.** Click the checkbox if you want 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 162 and “Setting access control” on page 163.

   Click **Close** when you’re done.

5. In the main installation dialog, click **Agree and Install.**
Webroot SecureAnywhere launches a scan.

![Webroot SecureAnywhere scan](image)

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

If it detects any threats, 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 it’s running, look for the Webroot icon in the system tray:

![Webroot 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.

![Webroot SecureAnywhere Overview Panel](image)

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.</td>
</tr>
<tr>
<td>PC Security</td>
<td>Change options for protecting your computer and for managing quarantined items.</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 versions. Password Management is only available in the Complete version.</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 versions.</td>
</tr>
<tr>
<td>System Tools</td>
<td>Use tools to manage processes and files, view reports, and submit a file to Webroot Support.</td>
</tr>
</tbody>
</table>
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, located in the bottom right of your computer desktop:

The system tray menu provides the following selections:

<table>
<thead>
<tr>
<th>System Tray Menu</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Status</td>
</tr>
<tr>
<td>Scans your computer for spyware, viruses, and other types of malware.</td>
</tr>
<tr>
<td>Check for updates</td>
</tr>
<tr>
<td>Checks for the latest software version and downloads it.</td>
</tr>
<tr>
<td>Save a Scan Log</td>
</tr>
<tr>
<td>Saves a log of scanning activity that you can send to Webroot Support for diagnostics.</td>
</tr>
<tr>
<td>Shut down Webroot</td>
</tr>
<tr>
<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:

![View Status](image1.png)

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 and provides a button for fixing it, as shown in the following example:

![SecureAnywhere Main Interface](image2.png)

For more information about detected threats, see “Managing quarantined items” on page 41.
Creating a Webroot account

Creating an 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.

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 for the account.

To create an account:

1. Open your browser and go to my.webrootanywhere.com.
2. Click Sign up now in the Create an Account panel of the SecureAnywhere website.
3. Complete the registration information:
   - **Webroot Product Keycode**: The license keycode you received when you purchased a product. Using the keycode, you can manage all products from the Webroot SecureAnywhere website.
   - **Email Address**: Your email address will be your login username. Your account activation confirmation will be sent to this address.
   - **Password**: Must be a minimum of 9 characters, and must contain at least 6 alphabetic characters and 3 numeric characters. Your password can be longer than the required 9 characters, and can include special characters.
     As you type, the Strength meter shows how secure your password is. For optimum security, it’s a good idea to make your password as strong as possible.
   - **Your Personal Security Code**: Enter a memorable word or number, using a minimum of 6 characters. Choose a code that is easy to remember, because you’ll be asked to enter two characters of it every time you log in. For example, Webroot SecureAnywhere might ask you to enter the third and sixth characters of this code.
4. Click **Register Now**.

Webroot SecureAnywhere notifies you that your registration was successful, and sends a confirmation message to the email address you specified.

5. Open your email application. Click the link in the confirmation email message to open the Confirm Registration page.

6. 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, showing the products you purchased. In this example, the user has access to PC Security, Backups, and Passwords. Mobile Security has not yet been activated.

<table>
<thead>
<tr>
<th>Security Question</th>
<th>Choose a question from the drop-down list. If you forget details of your login later, you’ll need to provide the answer to this question to retrieve the information.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Answer</td>
<td>Type an answer to your security question. The Security Answer is case-sensitive.</td>
</tr>
</tbody>
</table>

**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.
If desired, you can add keycodes for other Webroot products and other users to your account.

7. Open the drop-down menu by your user name to access account functions:

8. For further instructions on account setup, click Help in the menu.

**Using the PC Security site**

The PC Security site contains your license and status information for every computer in your SecureAnywhere account. This personalized website is available 24 hours a day, every day of the year.

**To log in to the PC Security site:**

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

The PC Security site 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. If you want to change the name displayed for your PC, click the Edit link at the top of the dialog. Enter a new name and click the ✓.

5. You can also change the security settings for each PC managed in your account. To change the security setting from the PC Security site, click the drop-down arrow in the Security Setting field, select a new setting from the drop-down menu, and click the ✓.
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 165.
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.

The System Scanner is preconfigured to scan your computer daily, without disrupting your work. If you want to change the automatic scanning behavior, see the following topics:

- “About scans” on page 14
- “Running an immediate scan” on page 15
- “Running a custom scan” on page 17
- “Changing the scan schedule” on page 19
- “Changing scan settings” on 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:

![Scan Information](image)

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 for all your Webroot-managed devices in the **PC Security** site. 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 con 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.

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 will launch 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 and removable 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. From the main interface, 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.

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.
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**.

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>
</tbody>
</table>
## Scan settings *(continued)*

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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. 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>
3: Shields

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 would like to change the shielding actions, see the following topics:

- “About shields” on page 24
- “Changing Realtime shield settings” on page 25
- “Changing Behavior shield settings” on page 27
- “Changing Core System shield settings” on page 29
- “Changing Web Threat shield settings” on 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 Windows system. Webroot has already 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 detects an item it 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 in our 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 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>Real Time shield settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Predictive Offline Protection from the central Webroot database</td>
</tr>
<tr>
<td>Downloads a small protection-definition file to your computer, so it will always be protected even when you’re offline. We recommend that you keep this option selected.</td>
</tr>
<tr>
<td>Remember actions on blocked files</td>
</tr>
<tr>
<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>
</tr>
<tr>
<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>
</tr>
<tr>
<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>
</tr>
<tr>
<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>
</tr>
<tr>
<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 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 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>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assess system modifications before they are allowed to take place</td>
<td>Intercepts any activity that attempts to make system changes, 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 Provider (LSP) chain or a virus-infected file, then restores the 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. The kernel is the central component of most computer operating systems. It acts as a bridge between applications and data processing done at the hardware level.</td>
</tr>
<tr>
<td>Prevent untrusted programs from modifying system processes</td>
<td>Stops unclassified programs from changing the system processes.</td>
</tr>
<tr>
<td>Verify the integrity of the LSP chain and other system structures</td>
<td>Monitors the Layered Service Provider (LSP) chain and other 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 for a website in the hosts file. It opens an alert where you can block or allow the changes. The hosts file is a Windows file that helps direct your computer to a website using Internet Protocol (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 suspicious file trying to download, 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. 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**.

![Website Filter](image)

6. When you’re done with Web Threat settings, click the **Save** button.
If you have the Essentials or Complete versions 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” on page 34
- “Changing firewall alert settings” on page 35
- “Managing network applications” on page 36
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 already 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 that it does not recognize and whether it should open an alert.

To change firewall alert settings:

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.

The Firewall settings in the application are shown below.

![Firewall settings image]

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 and 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.
5. Click on a radio button to allow or block a process or port address.
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” on page 40
• “Managing quarantined items” on page 41
• “Managing file detection” on page 43
• “Using antimalware tools” on page 45
• “Saving a threat log” on 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.
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>Antimalware tools</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset desktop wallpaper</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>Reset screensaver</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>Reset system policies</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>Reboot in Safe Mode</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>Perform an immediate system reboot</td>
<td>To reboot your system after threat removal, click the checkbox and click <strong>Run Tools</strong>.</td>
</tr>
<tr>
<td>Manual Threat Removal</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>Removal Script</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 versions of SecureAnywhere, you can use Identity Protection 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 Identity Protection” on page 50
- “Changing Identity shield settings” on page 51
- “Managing protected applications” on page 53
- “Managing protected websites” on page 55

Identity protection is available only in the Essentials and Complete versions. To upgrade, see “Upgrading or renewing the software” on page 156.
About Identity Protection

To guard against Internet fraud, the Identity shield protects sensitive data that may be exposed during your online transactions. It can protect you from many types of information-gathering methods, including phishing sites, cookie scrapers, clipboard grabbers, and browser hijackers.

If the Identity shield encounters 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, the Identity 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).

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 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>
<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>Identity shield settings (continued)</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Verify websites when visited to</strong></td>
<td>Analyzes the IP address of each website to determine if it has&lt;br&gt;<strong>determine legitimacy</strong></td>
</tr>
<tr>
<td><strong>Verify the DNS/IP resolution</strong></td>
<td>Looks for servers that could be redirecting you to a malicious&lt;br&gt;<strong>of websites to detect Man-in-website (man-in-the-middle attack). If the shield detects a&lt;br&gt;the-Middle attacks</strong></td>
</tr>
<tr>
<td><strong>Block websites from creating</strong></td>
<td>Blocks third-party cookies from installing on your computer if&lt;br&gt;<strong>high risk tracking information</strong></td>
</tr>
<tr>
<td><strong>Prevent programs from</strong></td>
<td>Blocks programs from accessing your login credentials (for&lt;br&gt;<strong>accessing protected credentials</strong></td>
</tr>
<tr>
<td><strong>Warn before blocking untrusted</strong></td>
<td>Opens an alert any time malware attempts to access data, instead&lt;br&gt;<strong>programs from accessing</strong></td>
</tr>
<tr>
<td><strong>Allow trusted screen capture</strong></td>
<td>Allows you to use legitimate screen capture programs, no matter&lt;br&gt;<strong>programs access to protected</strong></td>
</tr>
<tr>
<td><strong>screen contents</strong></td>
<td></td>
</tr>
</tbody>
</table>

---

Identity shield settings (continued)
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**.
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:\[padlock\].

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](image)

**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.
5. 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>Website protection options</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Block phishing and known malicious websites</td>
<td>Alerts you to phishing sites and other malicious sites listed in our Webroot database. 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>Protect cookies and saved website data</td>
<td>Alerts you if a malicious program attempts to gather personal data from cookies installed on your computer. 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>Detect and prevent man-in-the-middle attacks</td>
<td>Alerts you if a server is redirecting you to a malicious website (man-in-the-middle attack). This is a method of intercepting communications between two systems and stealing data.</td>
</tr>
<tr>
<td>Protect against keyloggers</td>
<td>Stops keyloggers from recording keystrokes on your computer. Keyloggers may monitor emails, chat room dialogue, instant message dialogue, websites visited, usernames, passwords, programs run, and any other typed entries. They have the ability to run in the background, hiding their presence.</td>
</tr>
<tr>
<td>Protect sensitive clipboard data</td>
<td>Stops malware programs from capturing clipboard data. The clipboard is a utility that allows you to cut and paste stored data between documents or applications.</td>
</tr>
<tr>
<td>Protect against URL grabbing attacks</td>
<td>Hides your web browsing activity from malware that attempts to log the websites you visit.</td>
</tr>
<tr>
<td>Protect browser components from external access</td>
<td>Hides your web browsing activity from malware that attempts to modify your browser with memory injection and other behind-the-scenes attacks.</td>
</tr>
<tr>
<td>Protect against Man-in-the-Browser attacks</td>
<td>Blocks a malicious toolbar from stealing data. A man-in-the-browser attack is a Trojan that infects a web browser. It can modify pages and the content of your transactions without being detected.</td>
</tr>
<tr>
<td>Isolate untrusted browser add-ons from data</td>
<td>Blocks a browser add-on (browser helper object) from stealing data. While most browser add-ons are legitimate, some can display ads, track your Internet activity, or hijack your home page.</td>
</tr>
<tr>
<td>Block browser process modification attempts</td>
<td>Analyzes browser memory to see if code injection is taking place.</td>
</tr>
<tr>
<td>Website protection options</td>
<td>(continued)</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Protect against screen grabbing attacks</td>
<td>Blocks a malicious program from viewing and capturing your screen content.</td>
</tr>
<tr>
<td>Block suspicious access to browser windows</td>
<td>Blocks a malicious program from viewing and capturing data in Windows components.</td>
</tr>
</tbody>
</table>
If you have SecureAnywhere Complete, you can use the Password Manager to automatically log you into 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.

To learn more about how to use the Password Manager, see the following topics:

- “About Password Management” on page 60
- “Storing user names and passwords” on page 61
- “Capturing other login fields” on page 64
- “Logging in to password-managed sites” on page 66
- “Populating fields in web forms” on page 67
- “Managing login credentials in the Passwords site” on page 69
- “Updating password-managed site information” on page 71
- “Generating a secure password” on page 74
- “Importing passwords from other applications” on page 76
- “Setting Password Manager preferences” on page 78
- “Exporting user names and passwords” on page 80
- “Creating Bookmarklets” on page 82
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.

The Password Manager works with both Internet Explorer and Firefox browsers. However, you can use some limited functions with other browsers by using Password Manager’s Bookmarklets.

To access Password Manager functions in your online SecureAnywhere account, log in to my.webrootanywhere.com and click the Passwords tab.

You can also access the Password Manager functions through the main interface. Click Identity & Privacy, the Password Management tab, then the Manage My Identity button.
Storing user names and passwords

The Password Manager can automatically fill in the user name and password fields for websites that require a login, such as banking, shopping, and networking sites. You can use the same login or a unique login for all the sites you want to manage. The Password Manager remembers all login data for you.

In addition, you can define separate credentials if you use different logins for the same website (for example, you and your spouse both use the same online bank, but have separate accounts). Whenever you access that web page again, the Password Manager will recognize that you have defined two different logins and will prompt you for the one you want.

To use the Password Manager, you must first capture your login credentials while you are accessing the website. You can also define login credentials for password-managed sites in your SecureAnywhere account, under the Passwords tab.

Defining logins while on the website

The easiest method of capturing login information is by loading the website in your browser and allowing the Password Manager to detect the user name and password you typed.

To define logins while on the website:

1. Open a web browser and sign in to your SecureAnywhere account. (Click the Webroot icon in your browser’s toolbar, then enter your SecureAnywhere user name and password.)

2. Open a website that requires a login, then sign in to that site using your user name and password. (If the site requires more than a user name and password to log in, see “Capturing other login fields” on page 64.)

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.

3. From the Webroot prompt, click Save Site.

Note: If the Password Manager cannot capture login credentials using this method, you can define credentials in the Passwords site. See the following section, “Defining logins from the Passwords site” on page 62.

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.)
4. 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><strong>Add Webroot Site dialog</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
</tr>
<tr>
<td><strong>Group</strong></td>
</tr>
<tr>
<td><strong>Make This a Favorite</strong></td>
</tr>
<tr>
<td><strong>Require Password Reprompt</strong></td>
</tr>
<tr>
<td><strong>AutoLogin</strong></td>
</tr>
</tbody>
</table>

5. Click the **Save Site** button.

The next time you access this website, 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. See “Logging in to password-managed sites” on page 66.

**Defining logins from the Passwords site**

You can also define logins in the Passwords site, which is available in your online SecureAnywhere account.

**To define logins from the Passwords site:**

1. Log into [my.webrootanywhere.com](http://my.webrootanywhere.com) and click **Passwords**.
The Passwords site looks similar to the following example:

2. On the far right of the panel, click **Add site** under “MyIdentity actions.”
3. At the prompt, click **Yes, let me manually add a site.**
   The Add Site dialog opens.

4. Fill in the Add Site dialog, as described in the following table.

<table>
<thead>
<tr>
<th>Add Site dialog</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the website; for example: My Bank. This name is displayed in the Passwords site and in Webroot prompts.</td>
</tr>
<tr>
<td>Group</td>
<td>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 site, such as Banking and Shopping. If you do not enter a group, the site is categorized in a Default group.</td>
</tr>
</tbody>
</table>
Click the Add site button.

The next time you access this website, make sure you are signed in to your SecureAnywhere account (click the Webroot icon in your browser’s toolbar, then enter your SecureAnywhere user name and password). When you’re signed in, the Password Manager can automatically fill in the user name and password for you. See “Logging in to password-managed sites” on page 66.

Capturing other login fields

Some websites require more than a user name and password for login, such as a social security number or medical plan number. If you frequently access a site with additional login credentials, you can use Save All Entered Data to capture the extra fields.

To create a site using Save All Entered Data:

1. Open a web browser and sign in to your SecureAnywhere account. (Click the Webroot icon in your browser’s toolbar, then enter your SecureAnywhere user name and password.)

2. Open a website that requires a login.
3. Fill in all the fields that you want.
4. From the Webroot drop-down menu, click Save All Entered Data.
The Edit Site Information dialog opens. This dialog shows data that it captured from the site. It captures all the fields it can, even if you did not enter data in those fields.

5. Make any changes that you want, then click OK.

The next time you access this website, make sure you are signed in to your SecureAnywhere account (click the Webroot icon in your browser's toolbar, then enter your SecureAnywhere user name and password). The Webroot icon appears at the end of the fields to indicate that the login credentials are stored in the Password Manager. (For drop-down fields, the icon is not shown.)
Logging in to password-managed sites

After you define login credentials for a site, the Password Manager can automatically log in for you. (You can add, edit, view, and delete login information as described in “Managing login credentials in the Passwords site” on page 69.)

To log in to a password-managed site:

1. Make sure you are logged in to your SecureAnywhere account. (Click the Webroot icon in your browser’s toolbar, then enter your SecureAnywhere user name and password.)

2. Open a password-managed site that you previously defined (see “Storing user names and passwords” on page 61).

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.

If you defined more than one login for a single website, the Password Manager prompts you to select the desired login credentials. Click the AutoFill button to display the different site names and select from one of them to fill in the fields.
Populating fields in web forms

You can use the Password Manager to automatically populate web forms with personal information that you commonly enter in fields, including your name, address, and credit card information. For example, you may want to create a personal profile with all your contact information, and also several different profiles for each credit card you use for Internet shopping. Then you can use a personal profile to automatically fill in your name and address in the fields, and another profile to automatically fill in your credit card information.

To create form-fill profiles:

1. Open a web browser and sign in to your SecureAnywhere account. (Click the Webroot icon in your browser’s toolbar, then enter 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. (If you selected Add Credit Card, only the Credit Card Information and Notes tabs appear in this dialog.)
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.

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**.

   ![Password Manager toolbar](image)

   The Password Manager transfers any information that applies to the fields into the web form.
Managing login credentials in the Passwords site

You can manage and access all your logins, passwords, and form fills in the Passwords site of your online SecureAnywhere account.

To access the Passwords site:

1. Log into my.webrootanywhere.com.
2. Click Passwords.

The Passwords site opens, similar to the example below.

Tabs

Under Passwords, you will see the following tabs:

- **Sites.** Edit, open, or delete previously defined sites and groups. Also view your passwords.
- **Favorites.** View, edit, and delete sites in your Favorites list.
- **Form Fill profiles.** View, edit, and delete Form Fill profiles.
- **Passwords.** View, edit, and delete secure passwords generated by the Password Manager.

The icons in these panels indicate if the site has an associated note ( ), is a Favorite ( ), requires a password reprompt ( ), or will auto-login ( ). Click **Edit** next to a site name to add a note and to designate a Favorite, password reprompt, or auto-login.
## MyIdentity actions panel

The website includes commands on the right side of the panel:

![MyIdentity actions panel](image)

See the following table for a description of each command.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add site</td>
<td>Define login information for a password-managed site. For instructions, see “Storing user names and passwords” on page 61.</td>
</tr>
<tr>
<td>Add group</td>
<td>Define a group for password-managed sites. Groups help you organize all sites into categories for easier viewing.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> To assign an existing site to this new group, select <strong>Edit</strong> in the row for the site and select the group from the drop-down field.</td>
</tr>
<tr>
<td>Add a Form Fill profile</td>
<td>Define a profile for automatic form-fill. A profile includes such personal information as your name, address, and credit card numbers for populating fields in website forms.</td>
</tr>
<tr>
<td></td>
<td>This feature saves you from manually typing your personal data into web forms every time you make an online purchase, complete a survey, and so on.</td>
</tr>
<tr>
<td></td>
<td>For instructions, see “Populating fields in web forms” on page 67.</td>
</tr>
<tr>
<td>Open all Favorites</td>
<td>Open sites that you specified as Favorites. All the sites open at once in separate tabs of your web browser, which can be convenient if you use the Passwords site as your browser’s home page.</td>
</tr>
<tr>
<td>View deleted items</td>
<td>View and recover any groups or sites you previously deleted.</td>
</tr>
<tr>
<td>View history</td>
<td>View a list of tasks you performed with the Password Manager.</td>
</tr>
<tr>
<td>View Never list</td>
<td>Suppress the toolbar prompts for specific websites. In the dialog, select the type of prompts to suppress and enter the websites where you do not want to see those prompts.</td>
</tr>
<tr>
<td>Install Bookmarklets</td>
<td>Create Bookmarklets, which help you access your data if you are traveling, have a mobile browser, or are not using Internet Explorer or Firefox. For instructions, see “Creating Bookmarklets” on page 82.</td>
</tr>
<tr>
<td>Import data</td>
<td>Import data from another password-management application. For instructions, see “Importing passwords from other applications” on page 76.</td>
</tr>
<tr>
<td>Export data</td>
<td>Copy your user names and passwords into an Excel spreadsheet. For instructions, see “Exporting user names and passwords” on page 80.</td>
</tr>
</tbody>
</table>
Updating password-managed site information

You can modify site information from a web browser or from the Passwords site.

To edit site information while that site is displayed in your browser:

1. Open a web browser and sign in to your SecureAnywhere account. (Click the Webroot icon in your browser’s toolbar, then enter your SecureAnywhere user name and password.)

2. Access the site you want to edit.

3. From the Webroot drop-down menu, select the site name at the bottom, then click **Edit**.

The Edit Site Information dialog opens. (Depending on what information you originally defined for the site, this dialog may display different fields.)

4. Make any desired changes.
The fields are described in the following table.

5. When you’re done, click **OK**.

<table>
<thead>
<tr>
<th><strong>Edit Site Information dialog</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>URL</strong></td>
<td>The URL of the website’s login page, which should not be modified unless the URL has changed.</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>The site name.</td>
</tr>
<tr>
<td><strong>Group</strong></td>
<td>A group you defined and assigned to this site (if any).</td>
</tr>
<tr>
<td><strong>User name</strong></td>
<td>Your login name for the site.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Your password for the site. Click <strong>Show</strong> if you want to see the actual password characters.</td>
</tr>
<tr>
<td><strong>Notes</strong></td>
<td>Any extra information about this site, such as a PIN number for your ATM machine at the bank.</td>
</tr>
<tr>
<td><strong>Options</strong></td>
<td>If desired, select any of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Favorite</strong>. Select this checkbox if you access this site frequently. You can then use the Open All Favorites feature from the Passwords site.</td>
</tr>
<tr>
<td></td>
<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></td>
<td>• <strong>Never AutoFill</strong>. Select this checkbox if you do not want the fields in the website automatically filled when you access the site.</td>
</tr>
<tr>
<td></td>
<td>• <strong>AutoLogin</strong>. Select this checkbox if you want to bypass a password prompt and go directly to the web page.</td>
</tr>
<tr>
<td><strong>Fields/Edit Form</strong></td>
<td>If this site includes fields that were captured with <strong>Save All Entered Data</strong>, the fields appear in this form. (There may also be a link to <strong>Edit Form Fields</strong>.)</td>
</tr>
</tbody>
</table>

**To edit site information from the Passwords site:**

1. Log into [my.webrootanywhere.com](http://my.webrootanywhere.com) and click **Passwords**.

[Image]

2. Locate the row for the site you want to change, then click **Edit**.

[Image]

The Edit Site dialog opens.
3. Edit this dialog as described in the following table, then click the **Save Site** button.

### Edit Site dialog

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The site name.</td>
</tr>
<tr>
<td>Group</td>
<td>A group you defined and assigned to this site (if any).</td>
</tr>
<tr>
<td>URL</td>
<td>The URL of the website’s login page, which should not be modified unless the URL has changed.</td>
</tr>
<tr>
<td>User name</td>
<td>Your login name for the site.</td>
</tr>
<tr>
<td>Password</td>
<td>Your password for the site.</td>
</tr>
<tr>
<td>Notes</td>
<td>Any extra information about this site, such as a PIN number for your ATM machine at the bank.</td>
</tr>
<tr>
<td>Options</td>
<td>If desired, select any of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Show in Favorites.</strong> Select this checkbox if you access this site frequently. You can then</td>
</tr>
<tr>
<td></td>
<td>use the Open all Favorites option from the Passwords site.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Reprompt for password.</strong> Click this checkbox if you don’t want your password automatically</td>
</tr>
<tr>
<td></td>
<td>filled in the field; and instead, want to manually enter the password yourself. This setting also</td>
</tr>
<tr>
<td></td>
<td>requires that you enter your SecureAnywhere master password before editing the site information.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Automatically fill.</strong> Keep this checkbox selected if you want your user name and password</td>
</tr>
<tr>
<td></td>
<td>automatically filled in when you access the site. Otherwise, de-select this checkbox.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Automatically log in.</strong> Select this checkbox if you want to bypass a password prompt and go</td>
</tr>
<tr>
<td></td>
<td>directly to the web page.</td>
</tr>
</tbody>
</table>
Generating a secure password

You can use the Password Manager to generate a strong, hack-resistant password for any website. A strong password is difficult to guess and helps protect you from identity theft.

You don’t need to remember these automatically generated passwords. When you access this web page again, the Password Manager automatically fills in the password field for you.

To use the password generator:

1. Open a web browser and sign in to your SecureAnywhere account. (Click the Webroot icon in your browser’s toolbar, then enter your SecureAnywhere user name and password.)

2. Access a password-protected web page and click inside the password field. The yellow Password Manager toolbar opens.

3. Click Generate from the toolbar. (If this toolbar doesn’t appear, click the drop-down arrow next to the Webroot icon, then select Tools > Generate Secure Password.) The Generate Secure Password dialog opens.
4. Click the **Accept** button to use the randomly generated password shown in the field. (If you are not logged in or you are not accessing a web page with a password field, a Copy button appears instead of the Accept button. Click **Copy** to copy the password to your clipboard. You can then paste the password into a password field.)

Once you click **Accept**, the new password is filled into the Password and Confirm Password fields in your web page.

If you want a different password than the one shown, you have several options:

- Click **Generate** to create another password, then click **Accept**. You can keep clicking **Generate** until you are satisfied with the password displayed in the field.

- Click in the **Show Advanced Options** checkbox to display more options for password generation, select the items you want, then click **Generate**. You can keep clicking **Generate** until you are satisfied with the password displayed in the field, then click the **Accept** button.
Importing passwords from other applications

If you are currently using another password-management application, you can import data from that application into the Webroot Password Manager.

To import passwords by using the Webroot drop-down menu:

1. Open a web browser and sign in to your SecureAnywhere account. (Click the Webroot icon in your browser’s toolbar, then enter your SecureAnywhere user name and password.)

2. From the Webroot drop-down menu, click Tools, then Import From.

   A list of applications appears in a submenu.

3. In the submenu, select from the list of password-management applications.

4. Follow the on-screen instructions for importing passwords from that application. (Since every password application is unique, the instructions for importing data from each one is also unique.)

To import passwords by using the Passwords site:

1. Log into my.webrootanywhere.com and click Passwords.

2. Under MyIdentity actions, click Import data.
3. From the dialog, click the arrow next to the **Import data from** field and select a password management application. Click **Continue**.

![Import data from dialog]

4. Follow the on-screen instructions for importing passwords from that application. (Since every password application is unique, the instructions for importing data from each one is also unique.)
Setting Password Manager preferences

You can set several preferences for your Password Manager tools, such as how notifications appear and what hotkeys you can use for shortcuts to tasks.

To set Password Management preferences:

1. Open a web browser and sign in to your SecureAnywhere account. (Click the Webroot icon in your browser’s toolbar, then enter your SecureAnywhere user name and password.)

2. From the Webroot drop-down menu, click Preferences.

The following dialog opens.
3. Change the preferences, as described in the following table. When you’re done, click **OK**.

<table>
<thead>
<tr>
<th><strong>Password Manager preferences</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td>Select whether you want to:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disable Insecure (IE or Firefox) Password Manager.</strong> When selected, the browser’s Password Manager does not prompt you to save passwords.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Open New Pages in...</strong> Select the current tab, Tabs, or new Windows.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Highlight Input boxes.</strong> When selected, the Password Manager displays fields in a different color.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Automatically Fill Login Information.</strong> When selected, the Password Manager fills in login fields with your user name and password.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Default Form Fill Profile.</strong> Select the Form Fill profile you want to use automatically and select the checkbox if you do not want to overwrite fields that are already filled.</td>
</tr>
<tr>
<td><strong>Notifications</strong></td>
<td>Select <strong>Notifications</strong> in the left panel, then click in the checkboxes for each type of notification you want the Password Manager to open.</td>
</tr>
<tr>
<td><strong>Hotkeys</strong></td>
<td>Select <strong>Hotkeys</strong> in the left panel, then enter key combinations you want to use for common Password Management tasks.</td>
</tr>
<tr>
<td><strong>Advanced</strong></td>
<td>Select <strong>Advanced</strong> in the left panel, then select any of these advanced functions:</td>
</tr>
<tr>
<td></td>
<td>• Enter the number of seconds to automatically log in to sites.</td>
</tr>
<tr>
<td></td>
<td>• Display a warning before filling insecure forms.</td>
</tr>
<tr>
<td></td>
<td>• Allow Web sites to disable AutoFill (keep the rule for AutoComplete=off).</td>
</tr>
<tr>
<td></td>
<td>• Select number of minutes until the Clipboard is cleared after use.</td>
</tr>
<tr>
<td></td>
<td>• Open a login dialog when you start the browser.</td>
</tr>
<tr>
<td></td>
<td>• Create new Form Fill Profiles automatically.</td>
</tr>
<tr>
<td></td>
<td>• Change the language displayed in all dialog boxes, menus, and prompts. (You must restart the browser.)</td>
</tr>
</tbody>
</table>
Exporting user names and passwords

You can use the Export feature to transfer all your Password Manager information into an HTML file, XML file, or a CSV file that can be imported into Microsoft Excel. The Export function is available from the Passwords site or from the Webroot drop-down menu.

To export data by using the Webroot drop-down menu:

1. Open a web browser and sign in to your SecureAnywhere account. (Click the Webroot icon in your browser’s toolbar, then enter your SecureAnywhere user name and password.)

2. From the Webroot drop-down menu, click Tools, then Export To.

3. Select one of the export options.
   A dialog opens that asks for your SecureAnywhere master password.

4. Enter your SecureAnywhere account password and click Sign In.
   If you selected Webroot CSV File or Webroot Encrypted File, you are prompted for a file name and a directory to store that file. If you selected a browser, our password data will be exported into the browser’s built-in password manager.

To export data by using the Passwords site:

1. Log into my.webrootanywhere.com and click Passwords.

2. Under MyIdentity actions, click Export data.

3. From the dialog, enter your SecureAnywhere master password and click OK.
   The Export Data dialog opens, similar to the example below. In this dialog, you can see all the information for your sites, passwords, and Form Fill profiles.
4. Click **Save to File** or **Send to Printer**.
   - If you are saving a file, another dialog opens that allows you to select a file format, then click **Export Data**.
   - If you are printing, your data is saved to an HTML page and another dialog opens where you can select a printer and click **OK**.
Creating Bookmarklets

If you are not using Internet Explorer or Firefox, you can still use some Password Manager features in other browsers by creating Bookmarklets. These are links that you drag and drop into another browser so you can use automatic logins and form filling. For example, to use Bookmarklets with Chrome, you would drag Bookmarklet links to Chrome’s Bookmarks Bar, then click on the bookmark to use automatic login.

Bookmarklets can be used with Safari, Chrome, Opera, Konqueror, and other browsers.

To create Bookmarklets:

1. Log into my.webrootanywhere.com and click Passwords.

2. From the MyIdentity actions panel, click Install Bookmarklets.

The Bookmarklets dialog opens.
3. Click on a tab for the browser you want to use.
   Instructions for that browser appear in the lower panel. Each browser requires a different set of steps.

4. Follow the instructions to create the Bookmarklets, then click **OK**.

5. To use the Bookmarklet, go to your browser and click on the bookmark for the Password Manager.
   The Password Manager either performs the function immediately or opens a dialog with more information.
If you have the Essentials or Complete versions of Webroot SecureAnywhere, you can use the Backup & Sync Manager to designate folders that automatically synchronize and upload files to your online account. The uploaded data is available from all the computers and mobile devices in your Webroot account.

To learn more about the Backup & Sync Manager:

- “About the Backup & Sync Manager” on page 86
- “Getting started with Backup & Sync” on page 87
- “Managing synchronized folders” on page 91
- “Synchronizing data between multiple computers” on page 95
- “Using the Magic Briefcase” on page 98
- “Using the Webroot File Manager” on page 99
- “Copying files to the Web Archive” on page 104
- “Managing files in the Backups site” on page 106
- “Accessing files remotely” on page 110
- “Managing photo albums” on page 114
- “Sharing photo albums with others” on page 118
- “Publishing photo albums to Facebook” on page 120
- “Sending files to others” on page 121
- “Restoring data” on page 123
- “Adding more storage space” on page 127
About the Backup & Sync Manager

The Backup & Sync Manager automatically uploads files from designated folders on your computer to Webroot’s online repository in a process called synchronization. This repository is a collection of secure servers where your data is safely encrypted and stored. You can access your synchronized data from any computer with Internet capabilities. Your data is stored in the Backups site, a personalized web interface that is available 24 hours a day, every day of the year. You can also use the Backup & Sync Manager to share files with friends and family.

For synchronization, you can designate folders yourself or you can use the preconfigured folder, called the Magic Briefcase. Any files you place in the Magic Briefcase are automatically synchronized with your SecureAnywhere account and any other computers with the SecureAnywhere software installed. If you only want to back up files, and not synchronize them, you can upload data to the Web Archive, which is a folder that resides only in your online account.

After the initial upload, the Backup & Sync Manager 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.

If you have another computer with the SecureAnywhere software installed, you can create shared folders between these computers or use the Magic Briefcase. When you make changes in a shared folder on one computer, the other computer automatically detects the changes and synchronizes the files, as long as that computer is connected to the Internet and logged in to your account. The changes are also propagated to your SecureAnywhere account. You can also access synchronized folders from a mobile device, such as an iPad or Android smartphone, when you install the SecureSync app (available when you purchase the SecureAnywhere Complete version.)

Backup & Sync functions are available from the main interface and from your online SecureAnywhere account. From the main interface, click **Backup & Sync**:
Getting started with Backup & Sync

To begin using the Backup & Sync Manager, you need to download the Backup & Sync component and create sync folders.

Downloading the Backup & Sync component

1. Open the main interface (see “Using the main interface” on page 5).
2. Click Backup & Sync, then click the Download and Install button.

When the download completes, the Backup & Sync panel displays the following:
Configuring synchronized folders (first-time setup)

To begin using the Backup & Sync Manager, you must first designate the folders on your computer that you want synchronized. Before you begin, make sure you have moved or copied your important files to those folders that you want synchronized.

Note: The Backup & Sync Manager provides one preconfigured folder called the Magic Briefcase. If desired, you can use that folder instead of configuring synchronized folders yourself. For more information about that folder, see “Using the Magic Briefcase” on page 98. If you only want to back up files, use the Web Archive. For more information, see “Copying files to the Web Archive” on page 104.

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**.

![Select Sync Folders dialog box](image)

Any files residing in these folders will be copied to your online SecureAnywhere account. If there are more folders that you would like to synchronize, but are not listed in the Setup dialog, see “Adding synchronized folders” on page 91.

You can manage these files in the Webroot File Manager (see “Using the Webroot File Manager” on page 99) or in the Backups site (see “Managing files in the Backups site” on page 106).

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

**Note:** If you installed Webroot SecureAnywhere on additional computers in your household and you want to include their folders in synchronization, see “Synchronizing data between multiple computers” on page 95.

The Backup & Sync Manager 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.

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 site (see “Managing files in the Backups site” on page 106).
Managing synchronized folders

After initial configuration, you can use the Webroot File Manager to add more folders or remove folders from synchronization.

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 computers. For example, if you delete a file in one synchronized folder, it will be deleted across all synchronized computers that share that folder and deleted in the online account.

Adding synchronized folders

If you want to add more synchronized folders after first-time configuration, you can open the Webroot File Manager and create as many synchronized folders as you like. If you want to configure multiple computers for synchronization, see “Synchronizing data between multiple computers” on page 95.

To add synchronized folders:

1. From the Backup & Sync panel, click Open File Manager.
2. Click Manage Sync Folders.
The Webroot Manage Folders dialog opens and shows your computer in the left column, under “This Computer.”

3. Click **Add Folders from this Computer**.

![Image of Webroot Manage Folders dialog]

4. When the Select New Folders dialog opens, click in the box next to the folders you want included in synchronization, then click **OK**.

The Manage Folders panel shows your selected folders under “This Computer.”

5. When you’re done selecting folders, click the **OK** button at the bottom of the Webroot Manage Folders dialog. You must click the **OK** button for the synchronization to begin.

The Backup & Sync Manager begins synchronizing and shows its status at the bottom of the Webroot File Manager.
Removing folders from synchronization
You can remove a folder from the automatic synchronization process, without actually deleting the folder from your computer.

To stop synchronizing folders:

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

2. Click Manage Sync Folders.

The Webroot Manage Folders dialog opens and shows your computer in the left column, under “This Computer.”

3. Click on the folder you want to remove, then click the X in the upper right.
4. At the prompt, click **OK**.

The Backup & Sync Manager no longer synchronizes this folder. It does not delete the folder from your computer, but it does remove the folder from your SecureAnywhere account.
Synchronizing data between multiple computers

If you installed Webroot SecureAnywhere on multiple computers, you can create shared, synchronized folders between them. Whenever you update data in one of these shared folders (adding, editing, moving, or deleting files), the Backup & Sync Manager automatically makes the same changes to the online servers and to shared folders on the other computers. This automatic synchronization can be beneficial when you frequently use multiple computers and need to access the most recent files.

To synchronize data between computers:

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

   ![Open File Manager](image)

   **Note**: The Webroot File Manager assigns a name to your computer, but you can assign a new name if you like. To do this, click on the Tools menu and click Rename this Computer. Do the same for each of your computers with Webroot SecureAnywhere installed. The new name and icon appear in the left panel.

2. For each computer, create at least one synchronized folder that you plan to use as a shared folder (see “Adding synchronized folders” on page 91).

3. From the Webroot File Manager on either computer, click Manage Sync Folders.
The Webroot Manage Folders dialog opens and shows the computer you are currently using in the left column, under “This Computer,” and your other computers in the right column.

4. Select a folder that you want to synchronize between the two computers. Click the Sync button under the folder name.

5. In the dialog that opens, select the destination computer and click OK.

6. Click OK at the bottom of Webroot Manage Sync Folders to send the sync request to the other computer.
7. From the other computer, look for the Pending Sync Folder message in the system tray. Click on the message to accept the sync request. In the next dialog that opens, click **OK** to accept the folder location or choose another location.

**Note:** If you select a folder with a name that is identical to a folder on the other computer, the dialog asks if you want to merge the two. During a merge, the Backup & Sync Manager copies the contents in each folder to the other, so they each contain the same files. If the folders contain files with identical names, the Backup & Sync Manager first determines if the contents of the files are identical or different. If the content is identical, it links the files and later synchronizes them if you make a change to one. If the content is different, it keeps both versions and suffixes filenames with *(from computer_name)*.

From now on, whenever you place a file in one of these synchronized folders, the Backup & Sync Manager uploads it to your online account and to the other computers. Be aware that any editing changes you make to these files (additions, modifications, or deletions) are also propagated to the other computers and your SecureAnywhere account.

If you have three or more computers with Webroot SecureAnywhere installed on each one, you can synchronize data between them by creating shared folders, as described above.
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. The Backup & Sync Manager 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, open the Backups site (see “Managing files in the Backups site” on page 106).
Using 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 SecureAnywhere 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. Click Backup & Sync.
3. Under Backup, click the Open File Manager button.

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.
See the following sections for details about the Webroot File Manager and available commands.

**Menus**

The File, Edit, View, and Tools menus provide access to Webroot File Manager commands. The Help menu provides access to complete online Help, some FAQs, and the ability to send an error report to Webroot.

**Toolbar**

The toolbar provides commands for reconfiguring synchronized folders, sending files, sharing folders, and synchronizing a folder to other computers.

**Left panel (folder tree)**

The left panel shows the following:

- **Your computers and folders.** This is a folder tree that shows your computer and its synchronized folders, as well as any other computers shared in your account.

- **Magic Briefcase.** This is a preconfigured, synchronized folder that resides under your personal Documents folder. It also resides in your online SecureAnywhere account. Any files you put in the Magic Briefcase are automatically synchronized with your account and with other devices where you installed SecureAnywhere. For more information, see “Using the Magic Briefcase” on page 98.

- **Web Archive.** This is a folder that only resides on the Webroot servers, not on your home computer. You should store files here that you need backed up, but not synchronized (for example: scanned copies of passports, old tax returns, and music files). For more
information, see “Copying files to the Web Archive” on page 104.

- **Deleted Files.** This is a recycle bin for files deleted from your account. You can retrieve files from here, if necessary.

### Middle panel

The middle panel shows more detail about an item selected in the folder tree on the left. You can click on a file to open it or right-click to open a pop-up menu of commands (see “Commands in the Webroot File Manager” on page 101).

<table>
<thead>
<tr>
<th>Pictures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>IMG_4767.JPG</td>
</tr>
<tr>
<td>IMG_4961.JPG</td>
</tr>
<tr>
<td>IMG_4980.JPG</td>
</tr>
<tr>
<td>IMG_4974.JPG</td>
</tr>
<tr>
<td>IMG_5016.JPG</td>
</tr>
<tr>
<td>NewWork.jpg</td>
</tr>
</tbody>
</table>

### Status bar (bottom taskbar)

The status bar at the bottom of the panel shows the amount of storage used and free, the status of synchronized files, a link to your personal account, and the connection status to the Internet.

### Commands

The Webroot File Manager includes many commands, which are available from either the menu bar at the top of the panel or from a pop-up menu that opens when you right-click on an item. (Some commands require that you connect to the Internet.) For a complete list of commands, see the following table.

<table>
<thead>
<tr>
<th>Commands in the Webroot File Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>New Folder</strong></td>
</tr>
<tr>
<td><strong>To create a subfolder:</strong></td>
</tr>
<tr>
<td>1. Select a “parent” folder from the left panel.</td>
</tr>
<tr>
<td>2. Select <strong>New Folder</strong> either from the File menu or from the pop-up menu when you right-click on the folder name.</td>
</tr>
<tr>
<td>3. When “New Folder” appears, enter your own name and press <strong>Enter</strong>.</td>
</tr>
<tr>
<td>You can then load files into this folder by using the <strong>Import Files</strong> command.</td>
</tr>
<tr>
<td><strong>Manage Sync Folders</strong></td>
</tr>
<tr>
<td>For further instructions, see “Managing synchronized folders” on page 91.</td>
</tr>
<tr>
<td><strong>Send File</strong></td>
</tr>
<tr>
<td><strong>Share</strong></td>
</tr>
</tbody>
</table>
### Import Files
Imports files into a synchronized folder.

**To import files:**
1. Select a folder from the left panel.
2. Click **Import Files** either from the File menu or from the pop-up menu when you right-click on the folder name.
3. When the Import dialog opens, select the files (use Ctrl or Shift to pick multiple files) and click Open.

The files appear in the Webroot File Manager and are immediately uploaded to the online servers.

### Import Folder
Imports subfolders into a synchronized folder.

**To import a folder:**
1. Select a “parent” folder from the left panel.
2. Click **Import Folder** either from the File menu or from the pop-up menu when you right-click on the folder name.
3. When the Browse dialog opens, select the folder and click OK.

The subfolder appears in the left panel.

### Export/Save As
Saves a synchronized file or folder to a different location on your computer.

**To export or save:**
1. Select a file or folder.
2. Click **Export/Save As** either from the File menu or from the pop-up menu when you right-click on the file or folder name.
3. When the Browse dialog opens, select the folder location and click OK.

The file or folder is saved to that other location.

### Restore
Restores a deleted file. For instructions, see “Restoring data” on page 123.

### Edit commands (Cut, Copy, Paste, Rename, Select All, and Delete)
Allows you to perform editing tasks, similar to the Edit menu in Windows Explorer and other Windows programs.

**Note:** Deleted files are moved to the Deleted Files recycle bin, where you can permanently delete them or restore them.

### Show in Windows Explorer
Open Windows Explorer and shows the location of the file on your computer.

**To show the file location in Explorer:**
1. Select a file in the middle panel.
2. Click **Show in Windows Explorer** either from the View menu or from the pop-up menu when you right-click on the file name.

Explorer opens to the file’s location.

### View in my Online Homepage
Opens the Backups site and shows the location of the file in your Webroot account.

**To show the file location in the Backups site:**
1. Select a file in the middle panel.
2. Click **View in My Online Homepage** from the pop-up menu when you right-click on the file name.

The Backups site opens in your Internet browser and shows the file’s location in your online account.
## Commands in the Webroot File Manager  (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Versions</strong></td>
<td>Allows you to see up to five previous versions of a file that have been uploaded to the online servers.</td>
</tr>
<tr>
<td></td>
<td><strong>To see file versions:</strong> 1. Select a file in the middle panel. 2. Click Versions either from the View menu or from the pop-up menu when you right-click on the file name. To access a previous version, see “Retrieving an older version of a file” on page 124.</td>
</tr>
<tr>
<td><strong>File transfer status</strong></td>
<td>Allows you to check the status of file uploads during synchronizations.</td>
</tr>
<tr>
<td></td>
<td><strong>To see the file transfer status:</strong> 1. Select the View menu. 2. Click File Transfer Status. Another panel opens where you can view the progress of uploads and downloads. If necessary, you can move files up in the priority list.</td>
</tr>
<tr>
<td><strong>Preferences</strong></td>
<td>Provides the following options:</td>
</tr>
<tr>
<td></td>
<td>• Show file status icons in Windows Explorer.</td>
</tr>
<tr>
<td></td>
<td>• Adjust the file upload speed from low to high. To access these preferences, select the Tools menu, then click Preferences.</td>
</tr>
<tr>
<td><strong>Rename this Computer</strong></td>
<td>Allows you to enter a more descriptive name and icon for the computers listed in the left panel.</td>
</tr>
<tr>
<td></td>
<td><strong>To rename a computer:</strong> 1. Select one of the computers in the left panel. 2. Select the Tools menu. 3. Click Rename this Computer. 4. In the Name Your Computer dialog, enter a new name and click on an icon. The new name and icon appear in the left panel.</td>
</tr>
<tr>
<td><strong>Remove a Computer</strong></td>
<td>Stops synchronizing folders on this computer. (It does not remove the actual folders on your computer.)</td>
</tr>
<tr>
<td></td>
<td><strong>To remove a computer from synchronization:</strong> 1. Select the computer in the left panel. 2. Select the Tools menu. 3. Click Remove a Computer. 4. In the next dialog, click the Remove button. Any files that were synchronized on this computer are moved from your online account to the Web Archive. If you don’t want the files stored there, go to the Web Archive and delete them.</td>
</tr>
<tr>
<td><strong>Reclaim Storage</strong></td>
<td>If you notice that the total size of the files in the Webroot File Manager does not match how much overall storage space you are using, go to the Tools menu and click Reclaim Storage to make sure all your files are properly accounted for.</td>
</tr>
</tbody>
</table>
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.

Note: To restore files from the Web Archive, see “Restoring files from the Web Archive” on page 126.

To copy files to the Web Archive:

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

2. In the Web File Manager, right-click Web Archive to display the pop-up menu, then select either Import Files or Import Folder.
3. 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. The Backup & Sync Manager does not move the files, only copies them.
Managing files in the Backups site

All your uploaded files are available from your online SecureAnywhere account, in the Backups site. This site is your personalized web interface that is available 24 hours a day, every day of the year. It allows you to open, copy, move, delete, and share files in your synchronized folders. You can access these files from any device with an Internet connection and browser.

To manage files in the Backups site:

1. Log into my.webrootanywhere.com.
2. Click Backups:

The Backups site opens, similar to the following example:

The Backups site includes three tabs across the top of the main panel: My Folders and Files, Recent Events, and Photos. These tabs are described in the following sections.

My Folders and Files

The My Folders and Files page lists all files that have been uploaded, as shown in the previous example. For a complete list of commands available from the My Folders and Files page, see the following table.

<table>
<thead>
<tr>
<th>My Folders and Files</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>New Folder</td>
<td>Create a subfolder within one of your synchronized folders.</td>
</tr>
<tr>
<td></td>
<td><strong>To create a new subfolder:</strong></td>
</tr>
<tr>
<td></td>
<td>1. Select a parent folder in the left panel.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>New Folder</strong>.</td>
</tr>
</tbody>
</table>

When the New Folder dialog opens, enter a name and a location, then click **OK**.
### My Folders and Files (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upload</td>
<td>Upload files from your computer to your synchronized folders.</td>
</tr>
<tr>
<td><strong>To upload files:</strong></td>
<td>1. Select a destination folder in the left panel.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Upload</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. When the Upload Files dialog opens, click <strong>Browse</strong> to select a file to</td>
</tr>
<tr>
<td></td>
<td>upload from your computer. You can use the additional fields to upload</td>
</tr>
<tr>
<td></td>
<td>multiple files.</td>
</tr>
<tr>
<td></td>
<td>4. When you’re done, click <strong>OK</strong>.</td>
</tr>
<tr>
<td>Send Files</td>
<td>Send an email to friends with a link to your files. For further instructions,</td>
</tr>
<tr>
<td></td>
<td>see “Sending files to others” on page 121.</td>
</tr>
<tr>
<td>Download</td>
<td>Access a file from another computer by opening it or by downloading it to</td>
</tr>
<tr>
<td></td>
<td>a Downloads folder. To download files, see “Accessing files remotely” on</td>
</tr>
<tr>
<td></td>
<td>page 110.</td>
</tr>
<tr>
<td>Copy, Move, Delete</td>
<td>Copy, move, or delete files.</td>
</tr>
<tr>
<td></td>
<td>1. Select one or more files in the middle panel by clicking in the checkbox</td>
</tr>
<tr>
<td></td>
<td>next to the file name.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Copy, Move, or Delete</strong>.</td>
</tr>
<tr>
<td></td>
<td>For Move and Copy, another dialog opens where you select the destination</td>
</tr>
<tr>
<td></td>
<td>folder. For Delete, files are moved to the Deleted folder, which serves as a</td>
</tr>
<tr>
<td></td>
<td>recycle bin.</td>
</tr>
<tr>
<td>Edit with WebSync</td>
<td>Edit files from any Internet-connected device and have the changes</td>
</tr>
<tr>
<td></td>
<td>immediately synchronized. For instructions, see “Accessing files remotely”</td>
</tr>
<tr>
<td></td>
<td>on page 110.</td>
</tr>
<tr>
<td>Versions</td>
<td>View previous versions of an uploaded file (five maximum) and restore</td>
</tr>
<tr>
<td></td>
<td>them if necessary.</td>
</tr>
<tr>
<td><strong>To see file versions:</strong></td>
<td>1. Click on a file name in the middle panel to display the pop-up menu.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Versions</strong>.</td>
</tr>
<tr>
<td></td>
<td>A dialog opens with more information about the file and previous versions</td>
</tr>
<tr>
<td></td>
<td>that were uploaded. For more information about restoring previous versions,</td>
</tr>
<tr>
<td></td>
<td>see “Retrieving an older version of a file” on page 124.</td>
</tr>
</tbody>
</table>
Recent Events

In the Recent Events page, you can view the ten most recent activities performed with the Backup & Sync Manager, which may include sharing an album, updating a file, or sending a file.

Photos

The Photos page shows all the synchronized folders that contain at least one JPG file, then displays those folders as “photo albums.”
For a complete list of commands available from the Photos page, see the following table.

<table>
<thead>
<tr>
<th>Photos</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>My Albums/Contact’s Albums</td>
<td>View your own albums or albums sent to you by friends. See “Managing photo albums” on page 114.</td>
</tr>
<tr>
<td>Share Album</td>
<td>Send an email to friends with a link to your photo albums. For instructions, see “Sharing photo albums with others” on page 118.</td>
</tr>
<tr>
<td>Publish to Facebook</td>
<td>Publish your photo albums on your Facebook page. For instructions, see “Publishing photo albums to Facebook” on page 120.</td>
</tr>
<tr>
<td>Properties</td>
<td>Specify who can see the album, rename an album, and view other properties.</td>
</tr>
<tr>
<td><strong>To set properties:</strong></td>
<td></td>
</tr>
<tr>
<td>1. Select the down arrow next to the Actions field beneath the album.</td>
<td></td>
</tr>
<tr>
<td>2. Click Properties.</td>
<td>From the Properties dialog, you can change the name of the album, view the folder location of the album, or specify whether this album can be viewed by only you, everyone on the Internet, or only selected contacts.</td>
</tr>
<tr>
<td>Download Album</td>
<td>Access an album from another computer by opening it or by downloading it to a Downloads folder. For instructions, see “Accessing files remotely” on page 110.</td>
</tr>
</tbody>
</table>
Accessing files remotely

You can access synchronized files or photo albums from any device with an Internet connection and browser. Simply access the Backups site, then download files or albums to your current computer. You can also edit files with WebSync, a program that provides access to some editing applications.

To access files remotely:

1. Log into my.webrootanywhere.com.
2. Click Backups:

   ![Backups Site Example]

The Backups site opens, similar to the following example:

![Backups Site Example]

The following sections describe:

- Downloading files
- Downloading photo albums
- Editing files remotely

Downloading files

You can download files residing in any of your synchronized folders from any location. For example, if you are traveling and need access to a file located on your home computer, you can download the file from any device with an Internet connection.

To download files:

1. Access the Backups site as described above.
2. Make sure the My Folders and Files tab is selected.
3. Do one of the following:
   - Click on a file to display the pop-up menu and select Download.
   - Select one or more files in the middle panel and click the Download button.
A dialog prompts you to open the file or save it to your current computer.

4. Select either:
   
   - **Open with and an application from the drop-down box.** If you chose to open the file, the Backup & Sync Manager opens the selected application and loads the file in it.
   
   - **Save File.** If you chose to save the file, it creates a Downloads folder (if not already created) and places your files there.

---

**Downloading photo albums**

The Backups site allows you to download photo albums residing in any of your synchronized folders from any location. For example, if you are traveling and want access to a photo album located on your home computer, you can download the album from any device with an Internet connection.

To download photo albums:

1. Access the Backups site as described above.
2. Click the Photos tab.
3. Beneath the album you want to download, click the down arrow next to the Actions field, then click Download Album from the menu.
A dialog prompts you to open the file or save it to your current computer.

4. Select either:
   • **Open with and an application for viewing photos from the Browse button.** If you chose to open the album, the Backup & Sync Manager opens the application you selected and loads the album.
   • **Save File.** If you chose to save the album, the Backup & Sync Manager creates a Downloads folder (if not already created) and places your album there.

**Editing files remotely**

You can open and edit files residing in any of your synchronized folders from any location. For example, if you are traveling and need access to a file located on your home computer, you can open the file from any device with an Internet connection. You can then edit the file and save it. The changes are immediately synchronized.

**To edit files remotely:**

1. Access the Backups site as described above.
2. Make sure the **My Folders and Files** tab is selected.
3. Click on a file to display the pop-up menu and select **Edit with WebSync.**
Note: If a dialog opens that instructs you to install Java, click on the install Java link and follow the on-screen instructions.

A dialog prompts you to open the file or save it to your current computer.

4. To edit your file, select **Java Web Start Launcher**.

Your document opens in Microsoft Word, along with a Webroot - WebSync dialog.

5. Edit your file, then click **Done With All** so your changes are immediately synchronized.
Managing photo albums

When you place photos in your synchronized folders, the Backup & Sync Manager uploads them to your online SecureAnywhere account and creates an album for every folder that contains at least one JPG file. You can access and manage all your uploaded photo albums from the Photos page.

To manage photo albums:

1. Log into my.webrootanywhere.com.
2. Click Backups:

3. Click the Photos tab on the far right.

The folders containing JPG files are organized into photo albums.

You can perform a number of tasks from the Photos page, as described in the following table.

<table>
<thead>
<tr>
<th>Photo Album commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>My Albums/Contact’s Albums</td>
</tr>
<tr>
<td>Sort by</td>
</tr>
</tbody>
</table>
### Photo Album commands (continued)

<table>
<thead>
<tr>
<th><strong>Show/Hide Albums</strong></th>
<th>If you want to hide some albums from this view, click the <strong>Show/Hide Albums</strong> link. In the next panel, click <strong>Hide</strong> if you do not want this album shown in the Photos tab or <strong>Show</strong> to display it again. When you hide an album, its files are still synchronized and accessible from your folders.</th>
</tr>
</thead>
</table>

| **Actions** | Click the drop-down arrow in the **Actions** field to access the drop-down menu. The menu items are described below.  
• **Share Album.** Sends an email to friends with a link to your photo albums. For further instructions, see “Sharing photo albums with others” on page 118.  
• **Publish to Facebook.** Publishes your photo albums on your Facebook page. For instructions, see “Publishing photo albums to Facebook” on page 120.  
• **Properties.** Opens the Properties dialog, where you can change the name of the album, view the folder location of the album, or specify whether this album can be viewed by only you, everyone on the Internet, or only selected contacts.  
• **Download Album.** Accesses an album from another computer by opening it or by downloading it to a Downloads folder. To download an album, see “Accessing files remotely” on page 110. |
|--------------|-------------------------------------------------------------------------------------------------------------------------------|

| **Settings** | If you do not want to receive notifications when someone opens the email with your album attached, click the **Settings** link below the album pictures. Under **Notifications**, click **Unsubscribe**. |
To view all photos within the album, click on the album picture. Another page opens with thumbnail views of your photos. From there, you can click on a thumbnail to view a larger image and access Photo Actions, similar to the example below.

From this panel, you can create contacts as follows:

- **Add Contact.** Click to manually enter a list of friends and family.
- **Add Group.** Click to create a group and assign contacts to the group. For example, you may want to create one group that includes only your family and another that includes all your friends.
- **Import Contacts.** Click to upload your address book from Gmail, Yahoo, Hotmail, or AOL.

To view all photos within the album, click on the album picture. Another page opens with thumbnail views of your photos. From there, you can click on a thumbnail to view a larger image and access Photo Actions, similar to the example below.
The right panel displays a list of commands for album actions (described in the previous table) and for individual photo actions, described in the following table.

<table>
<thead>
<tr>
<th>Photo Actions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View in My Folders and Files</td>
<td>Opens the My Folders and Files page and displays the location of the selected photo.</td>
</tr>
<tr>
<td>Download Photo</td>
<td>Downloads the selected photo (if it resides on another computer). To download a photo, see “Accessing files remotely” on page 110.</td>
</tr>
<tr>
<td>Rotate Left/</td>
<td>Rotates the picture’s orientation.</td>
</tr>
<tr>
<td>Rotate Right</td>
<td></td>
</tr>
<tr>
<td>Publish to Facebook</td>
<td>Publishes the selected photo on your Facebook page. For instructions, see “Publishing photo albums to Facebook” on page 120.</td>
</tr>
</tbody>
</table>

You can add descriptions of each photo by selecting **Click to add a caption** below the photo. The caption appears in the individual photo view and when you click **Slideshow** in the upper right of the picture.
Sharing photo albums with others

If you want to share photo albums with friends, you can use the Send Folders function to send them an email with a link to copies of your albums. Using the Send Folders function has several advantages: it preserves space because you are not attaching albums directly to an email and it protects your original files because you are not providing others with direct access to your albums.

Recipients are given access to a copy of your photos for 21 days. Be aware that since they do not have access to your original files, any future changes you make won’t be reflected in their copy. The recipients of your email do not need to have a SecureAnywhere account to access the albums. However, if they do have a SecureAnywhere account, they can view any albums you make public.

To share your photo albums with others:

1. Log into my.webrootanywhere.com.
2. Click Backups:
3. Select the Photos tab.
4. Select the drop-down arrow next to Actions, then click Share Album.

The Share Album dialog opens.
5. In the **To:** field, enter the email addresses of the recipients, separated by commas. You can also import email contacts you previously created by selecting **Import Contacts** in the upper right of the panel. (To create a Contacts list, see “Contacts” on page 116.)

6. In the **Message:** field, enter a short message for the invite. (If you select the **Make Public...** checkbox, your photo album is accessible to anyone on the Internet.)

7. When you’re done, click the **Share Album** button.

   A status message opens when your file is sent.

   Your recipients receive a message with a link to your photos. When they click on the link, a web page opens where they can download the files to their computers. (They do not need a SecureAnywhere account.) Recipients are given access to a copy of your photos for 21 days. Since they do not have access to your original files, any future changes you make won’t be reflected in their copy.

   When the recipients access the album, Webroot sends you a notification and logs an entry in the Recent Activity tab in the Backups site. If you do not want to receive notifications, click the **Photos** tab and click **Settings** below the album pictures. Under **Notifications**, click **Unsubscribe**.
Publishing photo albums to Facebook

Using the Backup & Sync Manager, you can easily publish your photo albums to Facebook.

To publish albums to Facebook:

1. Log into my.webrootanywhere.com.
2. Click Backups:

3. Select the Photos tab.
4. Click the Facebook icon below the album you want to publish.

5. When the next page opens, you can choose which photos you want published. Click Select All or click on each photo (use Ctrl and Shift), then click the Publish button.

6. In the Facebook dialog, enter your email address and password used for your Facebook account. If the Facebook Special Permissions dialog opens, select Allow Photo Uploads.

The following dialog opens:

7. Enter a name for the new album or click Existing Album and select one of your current Facebook albums to load the photos into an existing album. Click OK.

A message displays in the Backups site that your pictures are uploading to Facebook.

8. Open your Facebook account and check that your photos are posted on your profile.
Sending files to others

If you would like to share files with others, you can use the Send Folders function to send them an email that provides a link to copies of your files. Using the Send Files function has several advantages: it preserves space because you are not attaching files directly to an email and it protects your original files because you are not providing others with direct access to your files.

Recipients are given access to a copy of your files for 21 days. Be aware that since they do not have access to your original files, any future changes you make won’t be reflected in their copy. The recipients of your email do not need to have a SecureAnywhere account to access the files.

To send file links:

1. Log into my.webrootanywhere.com.
2. Click Backups:
   
   ![SecureAnywhere interface with Backups selected]

3. Click the My Folders and Files tab.
4. Select a file by clicking on its checkbox, then click Send Files from the toolbar or Send from the right-click pop-up menu.

   ![My Folders and Files interface with Send Files highlighted]

The Send Files dialog opens.
5. In the **To:** field, enter the email addresses of the recipients, separated by commas. In the **Message:** field, enter a short message for the invite. Then click **Send**.

A status message opens when your file is sent.

Your recipients receive a message that looks similar to the example below. When they click on the link, a web page opens where they can download the files to their computers. (They do not need a SecureAnywhere account.) Recipients are given access to a copy of your files for 21 days. Since they do not have access to your original files, any future changes you make won’t be reflected in their copy.

![Example email notification](image)

When the recipients access the files, Webroot sends you a notification and logs an entry in the Recent Activity page of the Backups site.
Restoring data

You may need to restore data in the following situations:

- You need to fully restore all data to a new computer. For example, your old computer crashed, your computer was stolen, or you purchased a new computer and want to quickly load all your old files. See “Restoring all data to a new computer,” below.

- You need to retrieve an older version of a file. For example, you accidentally overwrote an important file or you want to revert to an older version of it. See “Retrieving an older version of a file” on page 124.

- You need to retrieve a file or folder you deleted. For example, you accidentally deleted a synchronized folder from your computer (which also deleted it from your online account) and you want to restore it. See “Retrieving a file or folder you accidentally deleted” on page 125.

- You need to restore data from the Web Archive. For example, you accidentally deleted an important document from your computer, but it was copied to the Web Archive and you want to restore it. See “Restoring files from the Web Archive” on page 126.

Restoring all data to a new computer

The Backup & Sync Manager safely stores your old computer’s files in the synchronized folders, no matter if your computer is lost or damaged.

Note: Thieves cannot access your online files because they do not have your account name and password to launch your SecureAnywhere account.

To fully restore all data to a new computer:

1. On the new computer, install the SecureAnywhere software and activate your account on that computer.

2. Open the Webroot File Manager. See “Using the Webroot File Manager” on page 99.

3. Assign a new name and icon to the new computer by clicking on the Tools menu and selecting Rename this Computer. Assign a new icon and enter a unique name for your new computer, then click OK. The name must be different from your old computer.

4. Copy files from your old computer to your new computer by synchronizing each folder. Follow the instructions in “Synchronizing data between multiple computers” on page 95.

   Depending on the size and number of files, the synchronization may take awhile. When the process is complete, the status bar at the bottom of the Webroot File Manager shows “All files are backed up and in sync” and shows the synchronized folders under your new computer.
Retrieving an older version of a file

You can save up to five previous versions of a file and can restore any of those saved versions. (If you save changes a sixth time, your most recent versions are saved and the oldest version is removed.)

To retrieve an older version of a file:

1. Log into my.webrootanywhere.com.
2. Click Backups:

![Webroot SecureAnywhere interface]

3. Make sure the My Folders and Files tab is selected.
4. Select the file you want restored from the middle panel (click in its checkbox).
5. Click on the file name to display the pop-up menu, then click Versions.

![File versions dialog]

A dialog opens with more information about the file and previous versions that were uploaded.

6. Locate an older version and click Save As.

![Save As dialog]

The dialog prompts you to save a copy of the file and give it a new name.

7. Enter a new name or use the Webroot-generated name and click Save.

A copy of the file is added to your synchronized folder and is automatically synchronized (copied to both the online folder and your computer). You can access it locally or online.
Retrieving a file or folder you accidentally deleted

The Deleted Files folder acts like a recycle bin for files you deleted from your account. You can retrieve deleted files from this folder.

To retrieve a file or folder you accidentally deleted:

1. Log into my.webrootanywhere.com.
2. Click Backups:

3. Make sure the My Folders and Files tab is selected.
4. Click on the Deleted Files folder.
   All previously deleted files or folders reside in the Deleted Files folder.
5. Select the file you want restored from the middle panel (click in its checkbox) and click Restore.

6. In the dialog that opens, select a destination and click Restore.
   The file is moved to the selected folder and synchronized on your computer.
Restoring files from the Web Archive

If you copied files to the Web Archive folder, you can retrieve them from your online account.

To restore files from the Web Archive:

1. Open the Webroot File Manager. See “Using the Webroot File Manager” on page 99.
2. Click the Web Archive folder.
3. Select the folder or files you want to restore (use Ctrl or Alt to select multiple files).
4. From the middle panel, right-click to display the pop-up menu, then select Export/Save As.
5. In the dialog that opens, select the destination for the files and click OK.
Adding more storage space

If you need more synchronization space, you can purchase additional storage from Webroot.

To add more storage space to your account:

1. Open the main interface.
2. Click Backup & Sync.

A web page opens where you can use a credit card to purchase more data storage space.
If you have the Essentials or Complete versions 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” on page 130
- “Running a cleanup” on page 131
- “Changing Windows Desktop settings” on page 133
- “Changing Windows System settings” on page 135
- “Changing Application settings” on page 137
- “Changing Internet Explorer settings” on page 138
- “Using Secure File Removal” on page 140
- “Viewing the Cleanup log” on page 142
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. Most files are useful, and even required, for your computer to operate properly. However, other files are not necessary and consume valuable space on your hard drive. 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 **Cleanup 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 133
- “Changing Windows System settings” on page 135
- “Changing Application settings” on page 137
- “Changing Internet Explorer settings” on page 138

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 140 for more information.

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

6. From the System Cleaner panel, click the **Cleanup 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** button.

The settings are described in the table below.

<table>
<thead>
<tr>
<th>Windows Desktop Cleanup options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recycle Bin</td>
</tr>
<tr>
<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>
</tr>
<tr>
<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>
</tr>
<tr>
<td>Clears the history of shortcuts to programs that you recently opened using the Start menu.</td>
</tr>
<tr>
<td>Run history</td>
</tr>
<tr>
<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>
</tr>
<tr>
<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>
</tr>
<tr>
<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** button.

The settings are described in the table below.

<table>
<thead>
<tr>
<th>Windows System cleanup options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Clipboard contents</strong></td>
</tr>
<tr>
<td><strong>Windows temp folder</strong></td>
</tr>
<tr>
<td><strong>System temp folder</strong></td>
</tr>
<tr>
<td><strong>Windows update temp folder</strong></td>
</tr>
<tr>
<td><strong>Registry streams</strong></td>
</tr>
<tr>
<td><strong>Default logon user history</strong></td>
</tr>
<tr>
<td><strong>Memory dump files</strong></td>
</tr>
<tr>
<td><strong>CD burning storage folder</strong></td>
</tr>
<tr>
<td><strong>Flash Cookies</strong></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** 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.

   ![System Cleaner Settings panel](image)

   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** button.

The settings are described in the table below.

<table>
<thead>
<tr>
<th><strong>Internet Explorer Cleanup Options</strong></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address bar history</td>
<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>Cookies</td>
<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>Temporary Internet files</td>
<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>URL history</td>
<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>Setup log</td>
<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>MS download folder</td>
<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>IE MediaPlayer bar</td>
<td>Removes the list of audio and video files recently opened with the media player in Internet Explorer, which plays audio and video files that you access on websites.</td>
</tr>
</tbody>
</table>
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.
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.
10: System Control

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” on page 144
- “Using SafeStart Sandbox” on page 145
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, see the table below. Select a checkbox to disable a function (uncheck the box) or activate it (check the box). When you’re done, click the **Start** button.

<table>
<thead>
<tr>
<th>SafeStart settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Watch events originating from this process</td>
<td>Opens an event dialog to show a list of events as they take place. Deselect this option if you do not want to see these events.</td>
</tr>
<tr>
<td>Allow access to the Internet</td>
<td>Allows the program to access the Internet.</td>
</tr>
<tr>
<td>Allow the process to execute other processes</td>
<td>Allows the program to execute subprocesses.</td>
</tr>
<tr>
<td>Allow access to user resources</td>
<td>Allows the program to access folders in My Documents or active windows within a current session.</td>
</tr>
<tr>
<td>Allow access to administrative locations on the system</td>
<td>Allows the program to access system folders, registry entries, and other administrative locations.</td>
</tr>
</tbody>
</table>
## SafeStart settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow access to windows with a High integrity level</td>
<td>Allows the program to access Windows that have been elevated to High through user access control.</td>
</tr>
<tr>
<td>Allow access to windows with a Medium integrity level</td>
<td>Allows the program to access Windows that have been elevated to Medium through user access control.</td>
</tr>
<tr>
<td>Allow access to network shares</td>
<td>Allows the program to access files on a shared network directory.</td>
</tr>
</tbody>
</table>
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” on page 148
- “Viewing the protection statistics” on page 149
- “Viewing the execution history” on page 150
- “Submitting a file” on page 151
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.
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” on page 154
- “Activating a new keycode” on page 155
- “Upgrading or renewing the software” on page 156
- “Checking for software updates” on page 157
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” on page 160
- “Setting self protection” on page 162
- “Setting access control” on page 163
- “Defining proxy settings” on page 164
- “Setting heuristics” on page 165
- “Importing or exporting settings” on page 168
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](image)

   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.

   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><img src="image" alt="System tray 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>
</tbody>
</table>
### Basic Configuration settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show Webroot in the Start Menu</td>
<td>Lists Webroot SecureAnywhere in the Windows Startup menu items.</td>
</tr>
<tr>
<td>Show Webroot in Add/Remove Programs</td>
<td>Lists Webroot SecureAnywhere in the Windows Add/Remove Programs panel.</td>
</tr>
<tr>
<td>Hide the Webroot license keycode on-screen</td>
<td>Blocks your license keycode from displaying on the My Account panel.</td>
</tr>
<tr>
<td>Automatically download and apply updates</td>
<td>Downloads product updates automatically without alerting you.</td>
</tr>
<tr>
<td>Operate background functions using fewer CPU resources</td>
<td>Saves CPU resources by running non-scan related functions in the background.</td>
</tr>
<tr>
<td>Favor low disk usage over verbose logging (fewer details stored in logs)</td>
<td>Saves disk resources by saving only the last four log items.</td>
</tr>
<tr>
<td>Lower resource usage when intensive applications or games are detected</td>
<td>Suppresses Webroot SecureAnywhere functions while you are gaming, watching videos, or using other intensive applications.</td>
</tr>
<tr>
<td>Allow Webroot to be shut down manually</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>Force non-critical notifications into the background</td>
<td>Suppresses information-only messages from appearing in the system tray</td>
</tr>
<tr>
<td>Fade out warning messages automatically</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>Store Execution History details</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.
### 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**.

   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>
<tr>
<td>Require the completion of a CAPTCHA when changing critical features</td>
<td>Opens a CAPTCHA dialog that requires you to read distorted text on the screen and enter the text in a field before performing any critical actions. These actions include changing shields, importing configuration settings, uninstalling the program, and shutting down the agent.</td>
</tr>
<tr>
<td>Require the completion of a CAPTCHA when changing configuration</td>
<td>Opens a CAPTCHA dialog that requires you to read distorted text on the screen and enter the text in a field before performing any configuration changes.</td>
</tr>
<tr>
<td>Remember CAPTCHA completion until the window is closed</td>
<td>Allows you to complete configuration changes and critical functions without re-entering a CAPTCHA test again. Webroot SecureAnywhere will remember your last CAPTCHA until you close the main interface.</td>
</tr>
<tr>
<td>Allow non-administrative users to modify configuration options</td>
<td>Enables you to modify configuration options, whether you are logged in as an administrative user or not.</td>
</tr>
<tr>
<td>Allow uninstallation by non-administrative users</td>
<td>Enables you to uninstall the program, whether you are logged in as an administrative user or not.</td>
</tr>
<tr>
<td>Allow access to antimalware tools by non-administrative users</td>
<td>Enables you to access the Antimalware Tools (under Quarantine), whether you are logged in as an administrative user or not.</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.

   ![Settings icon]

2. From the Settings panel, click Proxy.

   ![Proxy settings panel]

3. Enter the proxy settings as described below, then click the Save 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>
</tbody>
</table>
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 site (see “Using the PC Security site” on page 10).

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** button.

### Radio buttons - additional heuristic options

<table>
<thead>
<tr>
<th>Radio button</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 Known Good</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>Slider position</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>
<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>Slider position</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>
</tbody>
</table>
### Slider - Age Heuristics (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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
A
access control settings 163
account
  activating new keycode 155
  adding users and changing settings 10
  checking for software updates 157
  creating a Webroot account 8
  upgrading to new version 156
  viewing details in program 154
Active processes 144
Add/Remove programs, showing or hiding
  SecureAnywhere from 161
address bar history, removing 139
admin account 8
advanced heuristics 166
age heuristics 166
alerts 7
  fading out automatically 161
  firewall 35
  Identity shield 55
  remembering responses in 26
  setting auto-blocking and quarantine 26
  suppressing from system tray 161
antimalware tools 45
applications
  adjusting threat-detection settings 144
  clearing activity traces 137
  providing additional security for 53
  archived files, including in scans 22
  autocomplete form data, clearing 140
AutoFill 66

B
backing up files 104
Backup & Sync 85
  accessing files remotely 110
  accessing previous versions of files 103
  adding more storage space 127
  adding sync folders 91
  configuring sync folders (initial setup) 88
  copying files to Web Archive 104
  creating Contacts 116
  downloading and installing Backup & Sync component 87
  downloading files 110
  downloading photo albums 111
  editing files remotely 112
  how it works 86
Backup & Sync (con’t)
  managing photo albums 114
  merging data in sync folders 97
  publishing photo albums to Facebook 120
  reclaiming storage space 103
  removing folders from sync 93
  renaming computers 103
  restoring data to a new computer 123
  restoring files from the Web Archive 126
  retrieving a deleted file or folder 125
  retrieving an older version of a file 124
  sending files to friends 121
  sharing photo albums 118
  stopping synchronization on a computer 103
  synchronizing data on multiple devices 95
  using the Backups site 106
  using the Magic Briefcase 98
  using the Web File Manager 99
  viewing file transfer status 103
Backups website 106
Basic Configuration 160
Behavior shield 27
BHOs, shielding 57
Bookmarklets in Password Manager 82
browser add-ons, shielding 57
browser requirements 2
browsing, shielding browsing activity 57
C
CAPTCHA, enabling or disabling 163
CD burning storage folder, clearing 136
cleanup log 142
cleanup
  See System Cleaner
clipboard contents, clearing 136
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 139
Core System shield 29
CPU resources, using fewer 161
cross-site scripting attacks, shielding 32
custom scan 17
D
deep scan 17
Detection Configuration 43
disabling SecureAnywhere 6
disk space requirements 2
document history, clearing 134

E
Edit with WebSync 112
execution history 150
Execution History logs, storing data for 161

F
Facebook, publishing photo albums to 120
file detection management 43
Fill Forms 67
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
full scan 17

G
gaming
    suppressing SecureAnywhere functions 161
    turning off scans during games 20
Generate Secure Password 74

H
heuristics 165
history, execution 150
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
IE MediaPlayer bar, clearing 139
index.dat databases, clearing 140
installing the software 2
Internet Explorer, clearing activity traces 138
Internet requirements 2

K
kernal memory, shielding 30
keycode
    activating new code 155
    adding others to your Webroot account 10
    hiding from My Account screen 161
    installation requirement 2
keyloggers, shielding 57

L
license agreement 173
lock icon 53
login credentials
    shielding 52
    storing in Password Manager 61
logon user history, clearing 136
logs
    cleanup 142
    saving resources in logging 161
    scan 6, 148
    storing data for Execution History 161
LSP chain, shielding 30

M
Magic Briefcase folder
    accessing online 100
    using 98
main interface 5
man-in-the-browser attacks, shielding 57
man-in-the-middle attacks, shielding 52, 57
manual threat removal 46
master account 8
Master Boot Record (MBR) scanning 21
memory dump files, clearing 136
MS download folder, clearing 139
My Account 153
    activating new keycode 155
    checking for software updates 157
    upgrading or renewing software 156
    viewing details 154

N
network applications, monitoring 36

O
offline threat protection 26
opening SecureAnywhere 5

P
padlock icon 53
Password Manager 59
    accessing 60
    AutoLogin 72
    capturing other types of login fields 64
    creating Bookmarklets (using other browsers) 82
    creating Favorites 70
    creating groups 70
    editing managed websites 71
    editing Save All Entered Data fields 74
    editing saved login credentials 69
    exporting to spreadsheet or other file 80
    generating a secure password 74
    hotkeys for 79
Password Manager (cont’d)
how it works 60
importing passwords from other applications 76
logging in to websites 66
modifying notifications for 79
Never AutoFill 72
populating fields in forms 67
require password reprompt 72
setting preferences 78
storing login credentials 61
suppress toolbar prompts 70
using the Passwords site 69
passwords
automatically filling 66
enabling for SecureAnywhere configuration
functions 163
generating secure passwords for website logins 74
saving in Password Manager 61
Passwords site 69
PC Security site 10
phishing, protecting against 51, 57
popularity heuristics 167
processes
adjusting threat-detection settings 144
shielding 30
program settings 159
protected applications 53
protected websites 55
protection statistics 149
proxy server settings 164

Q
quarantine 39
antimalware tools 45
auto-quarantine during shielding 26
enabling password for threat removal 163
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 134
registering SecureAnywhere 8
registry streams, clearing 136
removal script 46
removing SecureAnywhere 171
renewing subscription 156
reports 147
execution history 150
protection statistics 149
scan log 148
rootkit detection 21
Run dialog history, clearing 134

S
safe mode, rebooting in 46
SafeStart 145
sandbox testing area 145
Save All Entered Data 64
save threat log 47
scan log 6, 148
scanning 13
automatic scanning 14
changing scan settings 21
changing scheduled scan options and behavior 20
checking status from website 11
custom scans 17
enabling password for 163
how scans work 14
launching a scan 15
launching from system tray 6
launching from Windows Explorer 22
managing file detection 43
new or modified files 26
reducing memory and CPU usage 22
results in PC Security website 14
scanning single files or directories 18
threats found 16
screen capture programs, allowing 52
screen grabbers, shielding 58
screensaver, resetting 46
search history, clearing 134
search results, analyzing links for threats 32
Secure File Removal 140
SecureAnywhere website 9
self protection settings 162
settings 159
access control 163
basic configuration 160
defining proxy settings 164
heuristics 165
importing or exporting 168
self protection 162
setup log, clearing 139
shields 23
alerts 24
auto-blocking 26
Behavior shield 27
Core System shield 29
enabling and disabling 24
how shields work 24
shields (cont'd)
  Identity Protection 51
  managing file detection 43
  Realtime shield 25
  remembering responses in alerts 26
  scan new files 26
  setting auto-quarantine 26
  Web Threat shield 31
shortcut on desktop, adding 160
shredding files 140
shutdown command, hiding from system tray 161
shutting down SecureAnywhere 6
splash screen, showing or hiding on bootup 160
Start menu
  clearing history 134
  showing or hiding SecureAnywhere from 161
starting SecureAnywhere 5
statistics 149
status, viewing 7
submit a file 151
subscription renewal 156
support
  See Technical Support
sync folders
  adding 91
  setting up 88
  stopping sync 93
  synchronizing on all computers 95
synchronizing files 85
System Cleaner 129
  Address bar history 139
  Autocomplete form data 140
  CD burning storage folder 136
  changing application settings 137
  changing IE settings 138
  changing Windows Desktop settings 133
  changing Windows System settings 135
  Clipboard contents 136
  Default logon user history 136
  how it works 130
  IE MediaPlayer bar 139
  IE URL history 139
  index.dat databases 140
  Memory dump files 136
  MS download folder 139
  Recent document history 134
  Recycle Bin 134
  Registry streams 136
  removing IE cookies 139
  Run history 134
  running a cleanup 131
  Search history 134
  Secure File Removal 140
System Cleaner (cont'd)
  Setup log 139
  Start Menu history 134
  System temp folder 136
  Temporary Internet files 139
  viewing cleanup log 142
  Windows temp folder 136
System Control 143
  active processes 144
  using SafeStart sandbox 145
  system policies, resetting 46
  system requirements 2
  system temp folder, clearing 136
  system tray
    menu 6
    showing or hiding the Webroot icon 160
T
  Technical Support
    opening a support ticket 169
    submitting a file to 151
  temporary Internet files, clearing 139
threat log 47
threat removal
  manual 46
  scanning 13
threats found during scan 16
tools
  antimalware 45
  enabling access to other users 163
  system control 143
tray menu 6
turning off SecureAnywhere 6
U
  uninstallation
    enabling access to other users 163
    instructions for 171
  updating SecureAnywhere
    enabling or disabling automatic downloads 161
    from main interface 157
    from system tray 6
  upgrading to new version 156
  URL grabbing attacks, shielding 57
  URL history, clearing for Internet Explorer 139
users, controlling access to SecureAnywhere 163
W
  wallpaper, resetting 46
warnings
  See alerts
Web Archive
  accessing online 100
  copying files to 104
Web Archive (con’t)
  restoring files from  126
Web File Manager  99
Web Threat shield  31
Webroot account  8
Webroot support
  See Technical Support
Webroot website  8
websites
  analyzing for threats  32
  automatically filling in forms with Password Manager  67
websites (con’t)
  automatically storing passwords  61
  protecting from malicious content  55
  shielding from online identity threats  51
  whitelisting  32
WebSync  112
Windows
  cleaning activity traces  133
  clearing operating system traces  135
  clearing temp folder  136
  system requirements for SecureAnywhere  2
Windows Security Center, showing or hiding SecureAnywhere from  161