WEBROOT®

SecureAnywhere™

User Guide

for the

Complete Edition

Webroot Software, Inc.
385 Interlocken Crescent
Suite 800
Broomfield, CO 80021

www.webroot.com

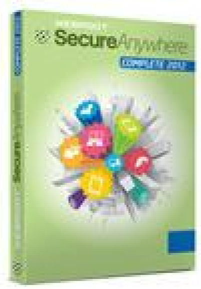
Version 8.0.1

Webroot SecureAnywhere User Guide for the Complete Edition

Version 8.0.1; May, 2012

Contents

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 guide describes how to use all features and functions of the Webroot SecureAnywhere Complete edition. The Complete edition uses a radically new cloud-based approach to online security that protects you against the latest threats, scanning your entire PC in about two minutes. It also updates itself so your protection is always current. With the Complete edition, you can back up photos online, wipe away traces of all your browser activity, block dangerous web links, and manage login information. Plus, with Webroot's first-of-its-kind security portal, you can access all your passwords and manage the protection settings for your PCs and mobile devices, no matter where you are.

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

- Installing the software . . . . page 2
- Using the main interface . . . . page 5
- Using the system tray menu . . . . page 6
- Viewing the protection status . . . . page 7
- Creating a Webroot account . . . . page 8
- Viewing the PC security status online . . . . page 11

Installing the software

SecureAnywhere can be installed on a Windows® 8, Windows 7, Vista®, or XP computer with an Internet connection. If you purchased a multi-user license, you can use the same keycode to install the software on up to three computers or five computers.

To install the program:

1. Before you begin:

   - Read the license agreement.
   - Make sure your system meets these minimum requirements:

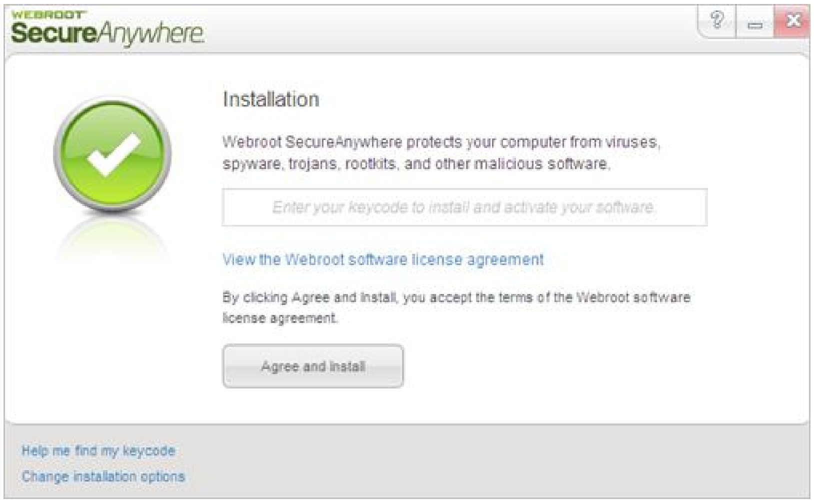
Minimum system requirements	
Windows operating system:	Webroot SecureAnywhere can be installed on a computer with one of the following operating systems: • Windows XP 32-bit and 64-bit SP2, SP3 • Windows Vista 32-bit (all Editions), Windows Vista SP1, SP2 32-bit and 64-bit (all Editions) • Windows 7 32-bit and 64-bit (all Editions), Windows 7 SP1 32-bit and 64-bit (all Editions) • Windows 8 32-bit and 64-bit (all Editions)
RAM:	128 MB (minimum); 2 GB recommended
Hard disk space:	10 MB
Internet/Browser:	Internet access is required. Browser: • Internet Explorer 7.0 and higher (32-bit only) • Mozilla Firefox 3.6 and higher (32-bit only) **Note:** The Identity shield also supports Google Chrome 11 and higher, and Opera 9 and higher (32-bit only).

   - Make sure your computer is connected to the Internet.
   - Close all programs that may be open on your computer.
   - Make sure you have the keycode. Your keycode comes in an email message or is listed on the instructions inside the retail box. The keycode is associated only with the Webroot SecureAnywhere software and does not include any information related to your computer or its configuration. Webroot does not use the keycode in any way to track individual use of its products.

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.



Installation

Webroot SecureAnywhere protects your computer from viruses, spyware, trojans, rootkits, and other malicious software.

Enter your keycode to install and activate your software.

View the Webroot software license agreement

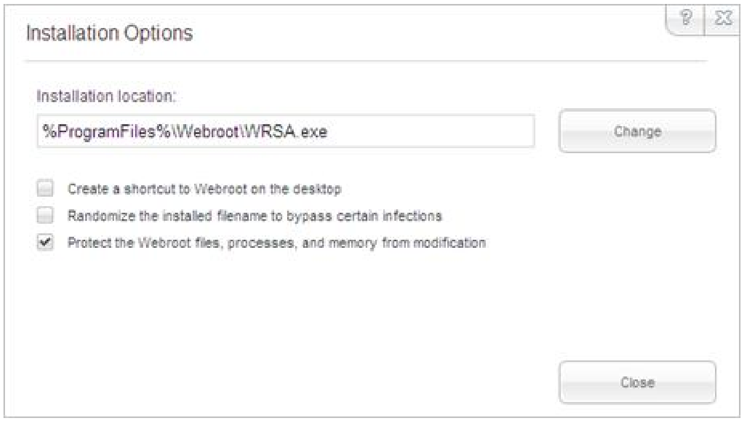
By clicking Agree and Install, you accept the terms of the Webroot software license agreement.

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

4 If desired, you can click **Change installation options** at the bottom of the dialog to modify these settings:

- **Create a shortcut to Webroot on the desktop**. This option places a shortcut icon on your Windows Desktop for Webroot SecureAnywhere.
- **Randomize the installed filename to bypass certain infections**. This option changes the Webroot installation filename to a random name (for example, “QrXC251G.exe”), which prevents malware from detecting and blocking Webroot’s installation file.
- **Protect the Webroot files, processes, and memory from modification**. This option enables self protection and the CAPTCHA prompts. (CAPTCHA requires you to read distorted text on the screen and enter the text in a field before performing any critical actions.) For more information, see “Setting self protection” on page 122 and “Setting access control” on page 123.

  Click **Close** when you’re done.



Installation Options

Installation location:

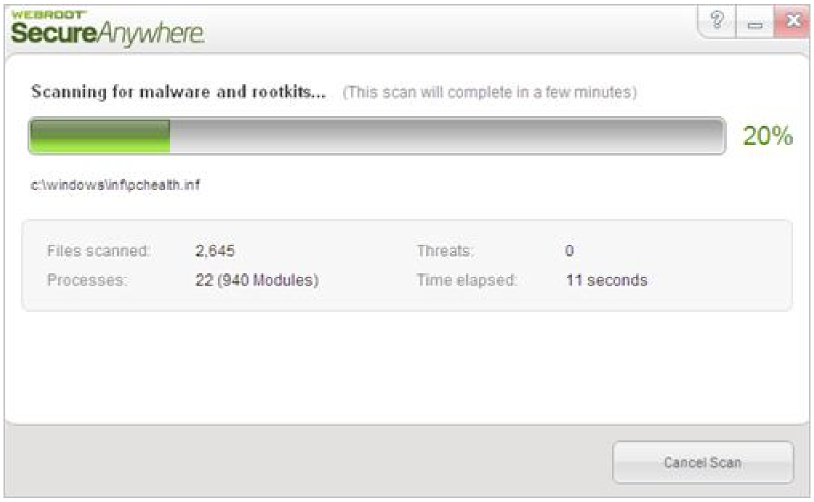
%ProgramFiles%\Webroot\WRSA.exe

☐ Create a shortcut to Webroot on the desktop
☐ Randomize the installed filename to bypass certain infections
☑ Protect the Webroot files, processes, and memory from modification

5 In the main installation dialog, click **Agree and Install**.

6 If you are prompted to enter an email address, enter your address and click **Continue**.

Webroot SecureAnywhere launches a scan.



Scanning for malware and rootkits... (This scan will complete in a few minutes)

20%

c:\windows\inf\pchealth.inf

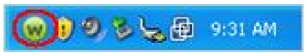
Files scanned:	2,645	Threats:	0
Processes:	22 (940 Modules)	Time elapsed:	11 seconds

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

If Webroot SecureAnywhere detects threats during the scan, it moves the items to quarantine where they are rendered inoperable and can no longer harm your system or steal data. For more information, see "About scans" on page 16 and "About quarantine" on page 42.

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

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



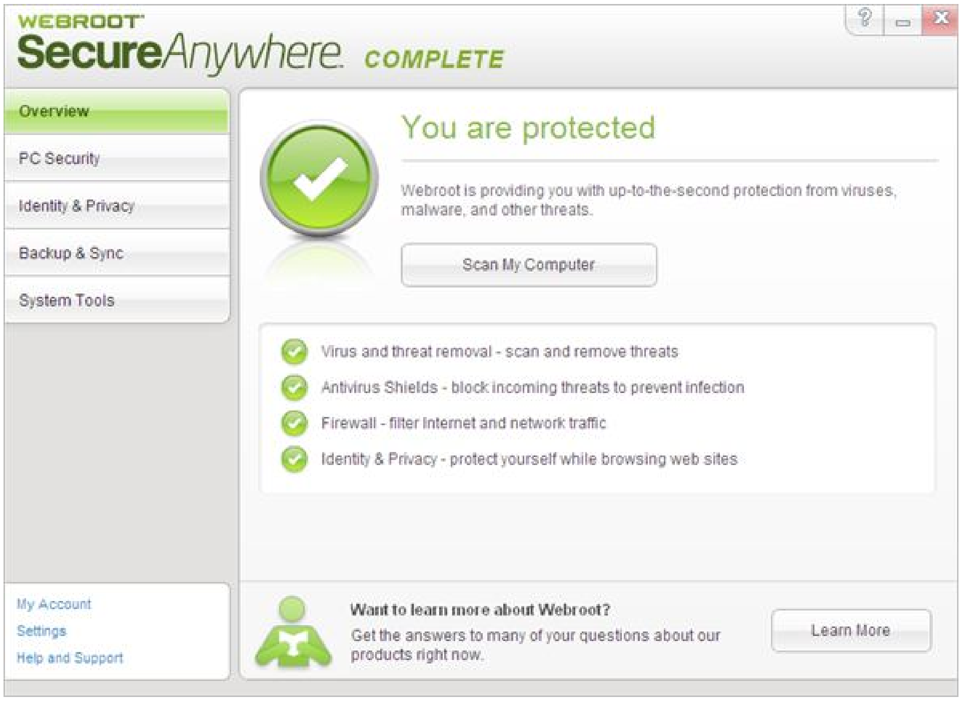
If an important message requires your attention, the icon turns yellow or red, and a dialog opens with further details.

7 If you purchased a multi-user license, follow the previous steps to install SecureAnywhere on other PCs.

Using the main interface

The main interface provides access to all Webroot SecureAnywhere functions and settings. To open the main interface, right-click on the Webroot icon from the system tray menu, then click **View Status**. If you cannot locate the system tray icon, open the Windows **Start** menu, click **All Programs** (or **Programs**), **Webroot SecureAnywhere**, then **Webroot SecureAnywhere** again.

When you open the main interface, it displays the Overview panel.



You are protected

Webroot is providing you with up-to-the-second protection from viruses, malware, and other threats.

- ✓ Virus and threat removal - scan and remove threats
- ✓ Antivirus Shields - block incoming threats to prevent infection
- ✓ Firewall - filter Internet and network traffic
- ✓ Identity & Privacy - protect yourself while browsing web sites

Want to learn more about Webroot?

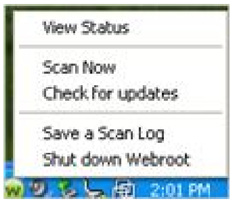
Get the answers to many of your questions about our products right now.

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

Navigation buttons and links	
Overview	View your system status and manually scan your computer.
PC Security	Run custom scans, change shield settings, set firewall protection, and manage the quarantine.
Identity & Privacy	Protect sensitive data that may be exposed during your online transactions and automatically fill in user names and passwords.
Backup & Sync	Protect your files by uploading them to Webroot's online repository.
System Tools	Use tools to manage processes and files, clean up files, view reports, and submit a file to Webroot Support.
My Account	View your SecureAnywhere account information, check for updates, and renew or upgrade your subscription.
Settings	Set advanced configuration options, proxy server settings, scan and shield settings, heuristics, and access control.
Help and Support	Connect to Webroot SecureAnywhere support options, Help files, FAQs, and user guides.

Using the system tray menu

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



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

The system tray menu provides the following selections:

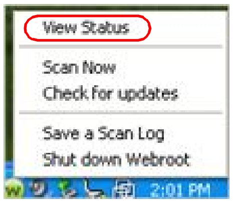
System Tray Menu	
View Status	Opens the main interface and displays your computer's security status. (This selection is only available when the main interface is closed.)
Scan Now	Scans your computer for spyware, viruses, and other types of malware.
Check for updates	Checks for the latest software version and downloads it. Typically, you do not need to check for updates. Your device checks into the cloud at regular intervals and automatically updates the software. Only use this option if you want to force changes immediately.
Save a Scan Log	Saves a log of scanning activity that you can send to Webroot Support for diagnostics.
Shut down Webroot	Closes the main interface and stops all protection operations. Be aware that if you shut down Webroot SecureAnywhere, your computer is not protected.

Viewing the protection status

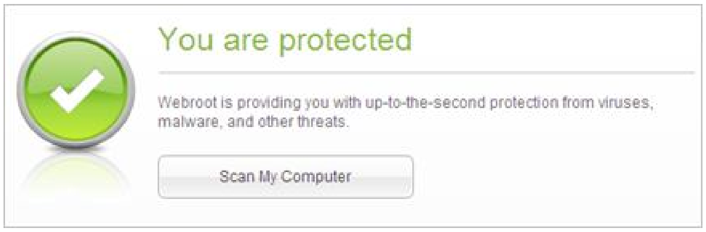
To show your computer's overall protection status, the system tray icon and the main interface change colors, as follows:

- **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 by right-clicking on the Webroot icon from the system tray menu, then **View Status**.



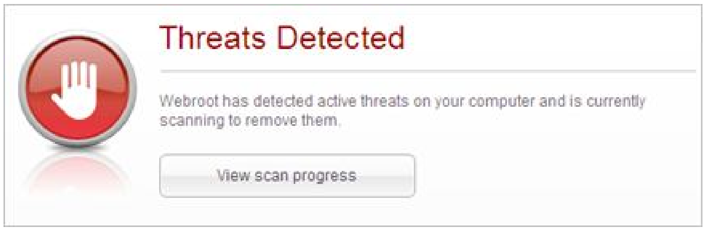
If your system is secure, the main interface is green and displays a message that you are protected.



You are protected

Webroot is providing you with up-to-the-second protection from viruses, malware, and other threats.

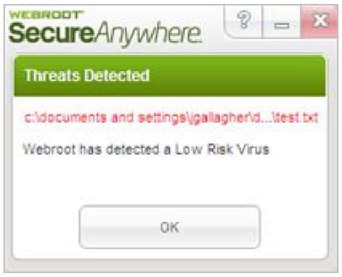
If an issue requires your attention, the main interface describes the problem.



Threats Detected

Webroot has detected active threats on your computer and is currently scanning to remove them.

SecureAnywhere also opens an alert in the system tray.



Threats Detected

c:\documents and settings\gallagher\d...\test.txt

Webroot has detected a Low Risk Virus

SecureAnywhere takes the appropriate action to quarantine the items. It may also prompt you to take action yourself (see "Running an immediate scan" on page 17 and "Managing quarantined items" on page 43).

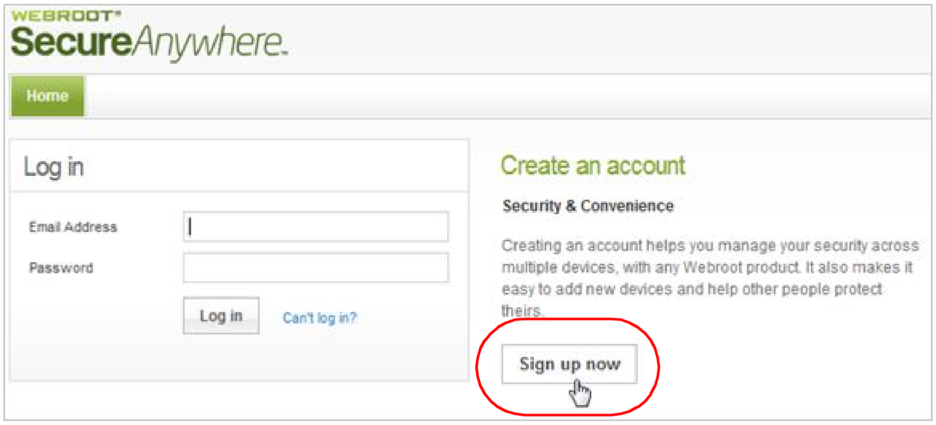
Creating a Webroot account

By creating a Webroot account, you can view the security status of your device remotely. The SecureAnywhere website shows if your device is secure, or if it's infected with a virus, spyware, or other online threat.

> **Note**: If you have a multi-licensed version, you can view the status of *all* devices in your account and set access levels for additional users associated with the account. For more information about administrator functions, see the SecureAnywhere Website User Guide.

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.



WEBROOT
SecureAnywhere.
Home
Log in
Email Address
Password
Log in
Can't log in?
Create an account
Security & Convenience
Creating an account helps you manage your security across multiple devices, with any Webroot product. It also makes it easy to add new devices and help other people protect theirs.
Sign up now

3. Complete the registration information and click **Register Now**. (For more information, see the SecureAnywhere Website User Guide.)

   Webroot SecureAnywhere sends a confirmation message to the email address you specified.

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

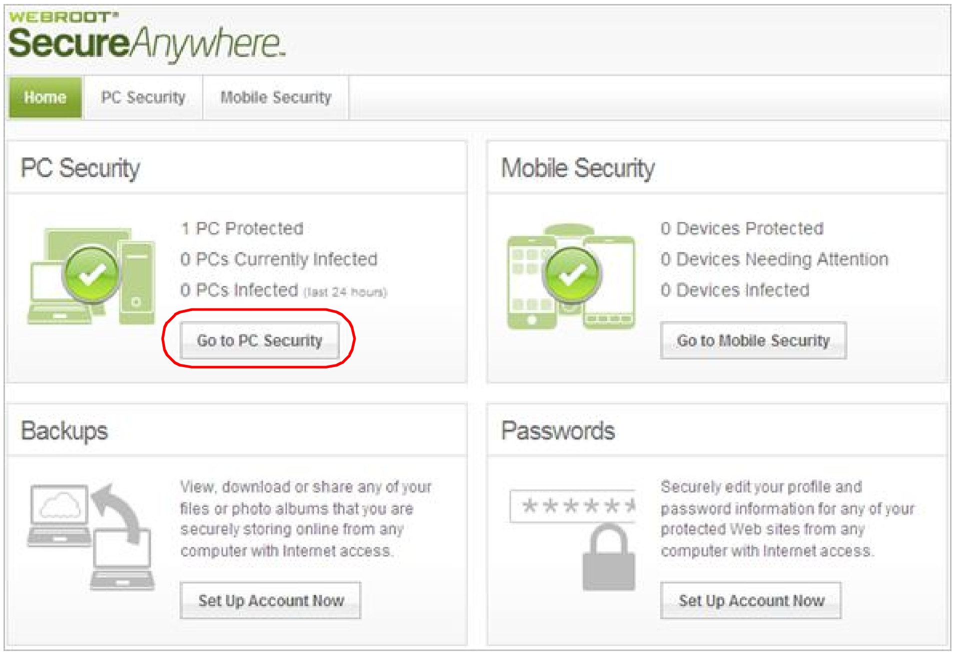
   Note: Until you click the link in the confirmation email and validate your account, you won't be able to log in to the Webroot SecureAnywhere website.

5. SecureAnywhere requests two randomly selected characters of the security code you specified when you created the account. Type the requested characters and click **Confirm Registration Now**.

   The SecureAnywhere website opens.

6 Click on **Go to PC Security** to access status information for your computer. For more information, see "Viewing the PC security status online" on page 11.

Note: When you install SecureAnywhere on additional PCs using the same multi-license keycode, their status information automatically displays in this website. For example, if you installed SecureAnywhere on five computers, the PC Security panel displays "5 PCs Protected." If you installed SecureAnywhere on an additional PC using a different keycode, you need to manually add its keycode to the website, as described in "Adding PCs to your account" on page 9.



PC Security

1 PC Protected
0 PCs Currently Infected
0 PCs Infected (last 24 hours)

Mobile Security

0 Devices Protected
0 Devices Needing Attention
0 Devices Infected

Backups

View, download or share any of your files or photo albums that you are securely storing online from any computer with Internet access.

Passwords

Securely edit your profile and password information for any of your protected Web sites from any computer with Internet access.

7 To begin using the Backups feature and the Passwords feature, click **Set Up Account Now** in both the Backups and Passwords panels. Your *Complete* subscription also includes SecureAnywhere apps for your mobile phones and tablets. For download instructions, see Downloading SecureAnywhere Mobile Complete.

Adding PCs to your account

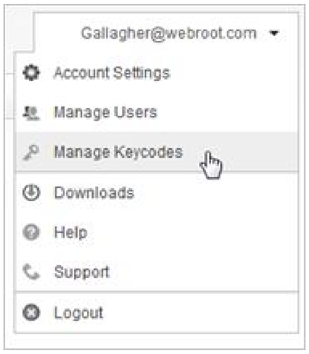
If you have a multi-licensed SecureAnywhere edition, you can install the software on additional PCs using the same keycode. After installation is complete, the PCs automatically report their status to the SecureAnywhere website and appear in the PC Security panel.

If you purchased another SecureAnywhere product with a new keycode, you must add that keycode to your account before you can view it on the SecureAnywhere website. Follow the instructions below to add a PC with a different keycode.

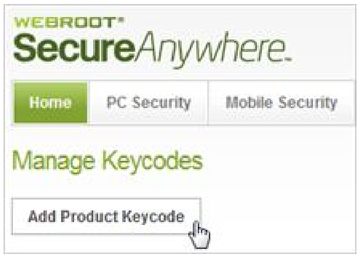
To add a managed PC to your account:

1 Look for the arrow next to your login ID in the upper right of the panel. Click on the arrow to open the drop-down menu.

2 Click **Manage Keycodes** from the drop-down menu.



3 Click **Add Product Keycode**.



4 In the displayed field, enter your keycode and click **Add**.

The new device will appear in the website the next time SecureAnywhere reports its status. You can force a status update by running a scan on the PC (see "Running an immediate scan" on page 17).

Adding mobile devices to your account

Webroot security apps are available for Android and Apple devices at Webroot Mobile & Tablet Security. For Android smartphones and tablets, you can view status information in the SecureAnywhere website. Simply install Webroot's Android app using your Webroot account login credentials and the product keycode. The information for the mobile device then appears in the Mobile Security panel.

If for some reason the device information does not appear, you can manually add the app's keycode in the Manage Keycodes panel. To do this, follow the previous instructions for "Adding PCs to your account."**Note**: Your *Complete* subscription includes SecureAnywhere apps for your mobile phones and tablets. For download instructions, see Downloading SecureAnywhere Mobile Complete. When installation is complete, your devices automatically appear in your SecureAnywhere account.

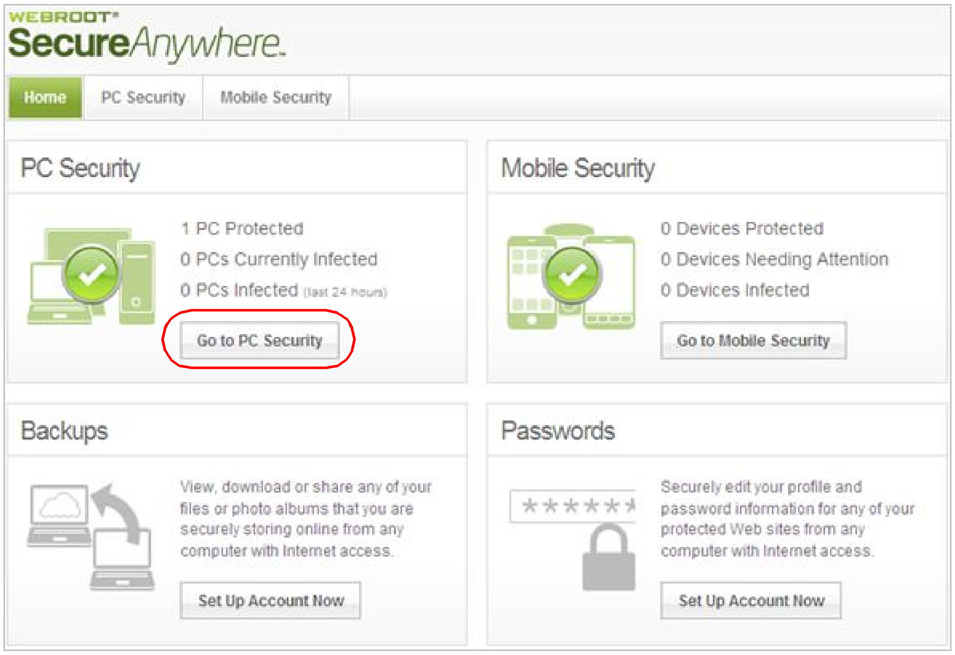
Viewing the PC security status online

The SecureAnywhere website contains your license and status information. If you have not yet created an account, see “Creating a Webroot account” on page 8.

To view PC status online:

1 Log in at my.webrootanywhere.com.

2 Click **Go to PC Security**.



PC Security

1 PC Protected
0 PCs Currently Infected
0 PCs Infected (last 24 hours)

Mobile Security

0 Devices Protected
0 Devices Needing Attention
0 Devices Infected

Backups

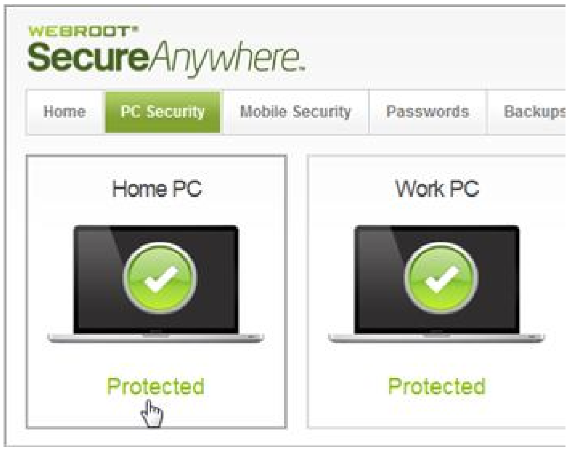
View, download or share any of your files or photo albums that you are securely storing online from any computer with Internet access.

Passwords

Securely edit your profile and password information for any of your protected Web sites from any computer with Internet access.

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

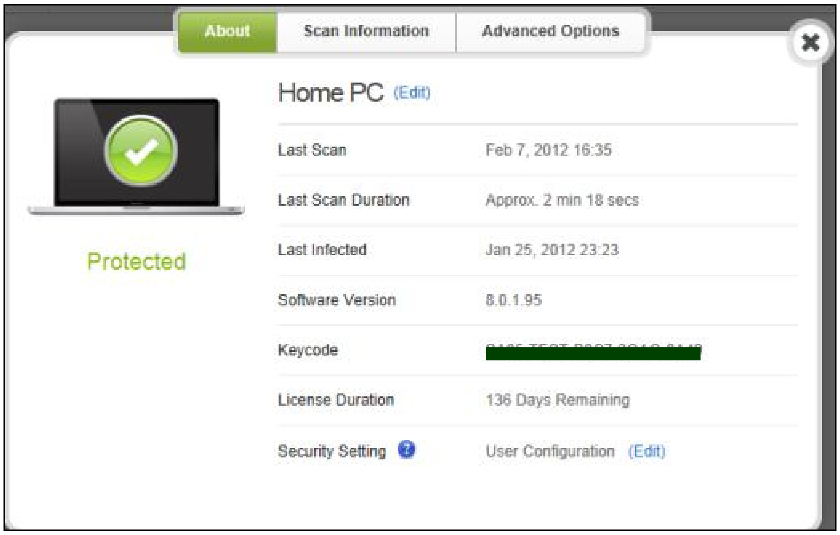
3 Click on the desired PC.



Home PC
Protected

Work PC
Protected

A dialog opens that provides license information and status of previous scans on this device. If SecureAnywhere has not detected any threats, the About panel displays “Protected” in green, as shown in the following example.

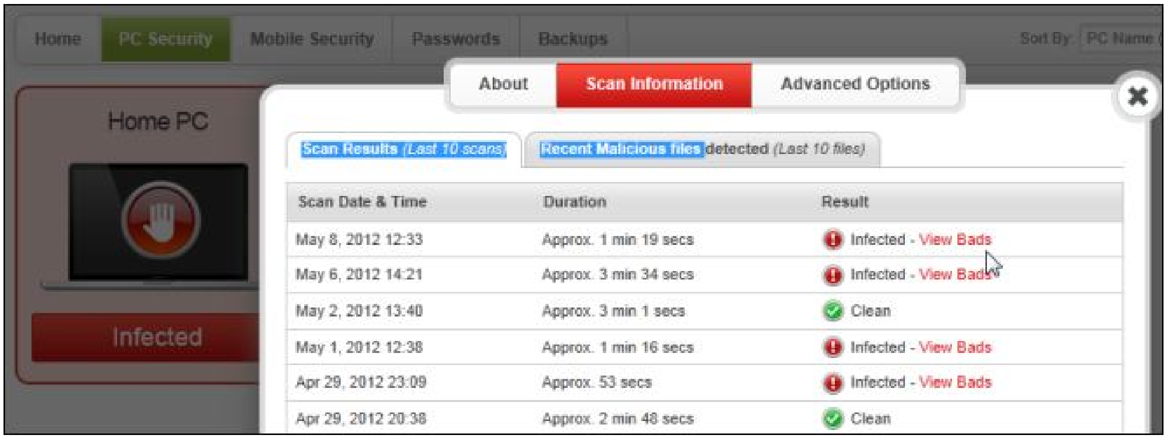


Home PC (Edit)

Last Scan	Feb 7, 2012 16:35
Last Scan Duration	Approx. 2 min 18 secs
Last Infected	Jan 25, 2012 23:23
Software Version	8.0.1.95
Keycode	[redacted]
License Duration	136 Days Remaining
Security Setting	User Configuration (Edit)

Note: For easier viewing, you can change the display name for your PC. To do this, click the **Edit** link at the top of the dialog. Enter a new name and click the checkmark ✓.

If SecureAnywhere detected a threat during a recent scan, this panel displays “Infected” in red, as shown in the following example. Click on the **Scan Information** tab to view the scan results. In the **Result** column on the far right, you can click the **View Bads** link for more information about the threat. To remove the threat, open SecureAnywhere from your PC and run a scan (see “Running an immediate scan” on page 17). Check quarantine to make sure the threat has been removed (see “Managing quarantined items” on page 43).

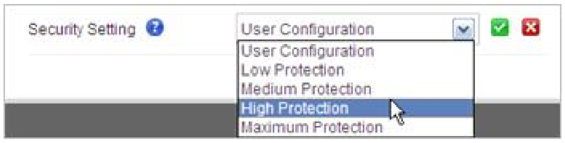


Scan Date & Time	Duration	Result
May 8, 2012 12:33	Approx. 1 min 19 secs	Infected - View Bads
May 6, 2012 14:21	Approx. 3 min 34 secs	Infected - View Bads
May 2, 2012 13:40	Approx. 3 min 1 secs	Clean
May 1, 2012 12:38	Approx. 1 min 16 secs	Infected - View Bads
Apr 29, 2012 23:09	Approx. 53 secs	Infected - View Bads
Apr 29, 2012 20:38	Approx. 2 min 48 secs	Clean

Note: If you want to remove an old computer from the PC Security panel (one that no longer includes the SecureAnywhere software), click the **Advanced Options** tab, then the **Deactivate Computer** button.

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

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



Security Setting ?

User Configuration

By default, Webroot SecureAnywhere uses the settings that you configured in the desktop application (“User Configuration”). To learn more about the settings, click the blue question mark ? 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 126.

2: Scans

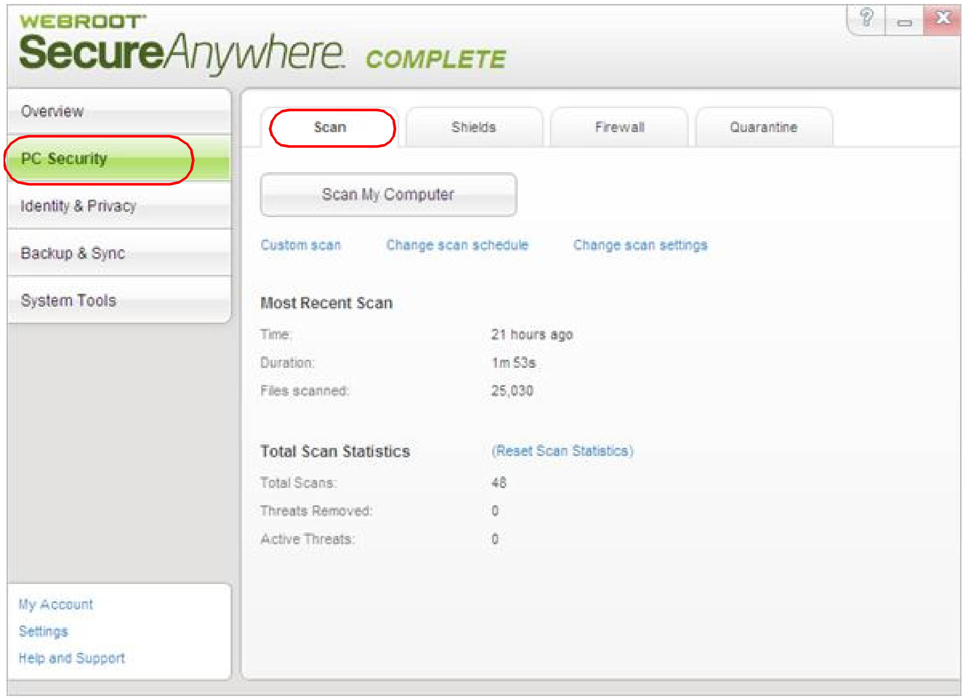
When Webroot SecureAnywhere scans your computer, it searches for spyware, viruses, and any other threats that may infect your computer or compromise your privacy. If it detects a known threat, it moves the item to quarantine, where it is rendered inoperable and can no longer run on your computer.

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

About scans

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**. The Scan tab shows the most recent scan results, total scans, threats removed, and active threats detected.



Most Recent Scan

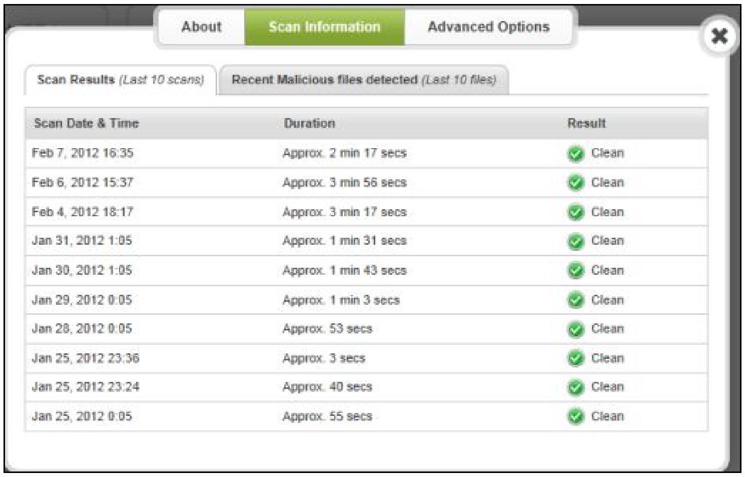
Time: 21 hours ago
Duration: 1m 53s
Files scanned: 25,030

Total Scan Statistics (Reset Scan Statistics)

Total Scans: 48
Threats Removed: 0
Active Threats: 0

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.

You can also view scan results online, as shown in the website example below (see "Viewing the PC security status online" on page 11).


About
Scan Information
Advanced Options
Scan Results (Last 10 scans)
Recent Malicious files detected (Last 10 files)

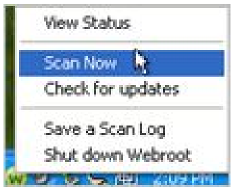
Scan Date & Time	Duration	Result
Feb 7, 2012 16:35	Approx. 2 min 17 secs	✓ Clean
Feb 6, 2012 15:37	Approx. 3 min 56 secs	✓ Clean
Feb 4, 2012 18:17	Approx. 3 min 17 secs	✓ Clean
Jan 31, 2012 1:05	Approx. 1 min 31 secs	✓ Clean
Jan 30, 2012 1:05	Approx. 1 min 43 secs	✓ Clean
Jan 29, 2012 0:05	Approx. 1 min 3 secs	✓ Clean
Jan 28, 2012 0:05	Approx. 53 secs	✓ Clean
Jan 25, 2012 23:36	Approx. 3 secs	✓ Clean
Jan 25, 2012 23:24	Approx. 40 secs	✓ Clean
Jan 25, 2012 0:05	Approx. 55 secs	✓ Clean

Running an immediate scan

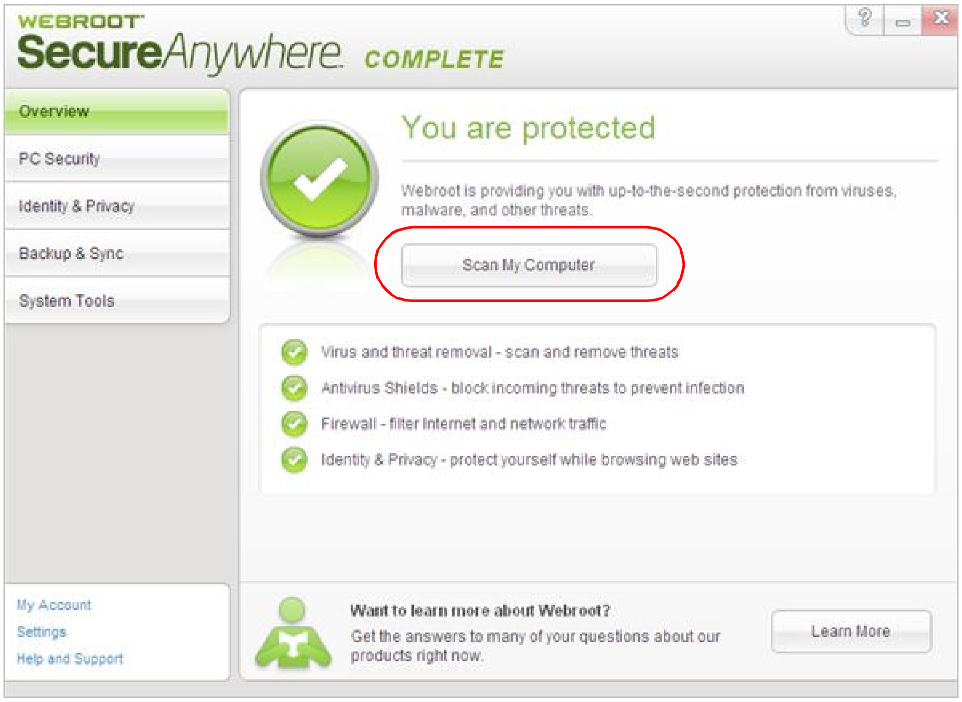
Although scans run automatically, you can launch a scan at any time. An immediate scan might be necessary if you surfed a high-risk website (networking, music, or adult entertainment), downloaded high-risk items (screen savers, music, or games), or accidentally clicked on a suspicious pop-up advertisement.

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

- If the main interface is closed, right-click the System Tray icon and select **Scan Now**. This runs a Deep scan, which looks for all types of malware in every area.



- If the main interface is open, click **Scan My Computer** from the Overview panel. This runs a Deep scan, which looks for all types of malware in every area.



You are protected

Webroot is providing you with up-to-the-second protection from viruses, malware, and other threats.

Virus and threat removal - scan and remove threats

Antivirus Shields - block incoming threats to prevent infection

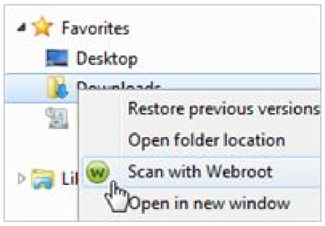
Firewall - filter Internet and network traffic

Identity & Privacy - protect yourself while browsing web sites

Want to learn more about Webroot?

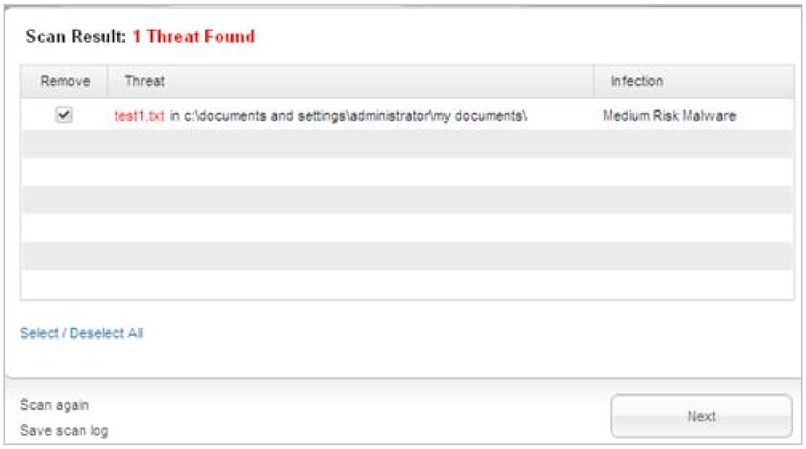
Get the answers to many of your questions about our products right now.

- To target an area for scanning, open Windows Explorer and right-click on the file, folder, or drive. From the pop-up menu, select **Scan with Webroot**.



You can also run a quick memory scan or a customized scan. For instructions, see "Running a custom scan" on page 19.

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.



Scan Result: 1 Threat Found

Remove	Threat	Infection
☑	test1.txt in c:\documents and settings\administrator\my documents\	Medium Risk Malware

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 43.

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

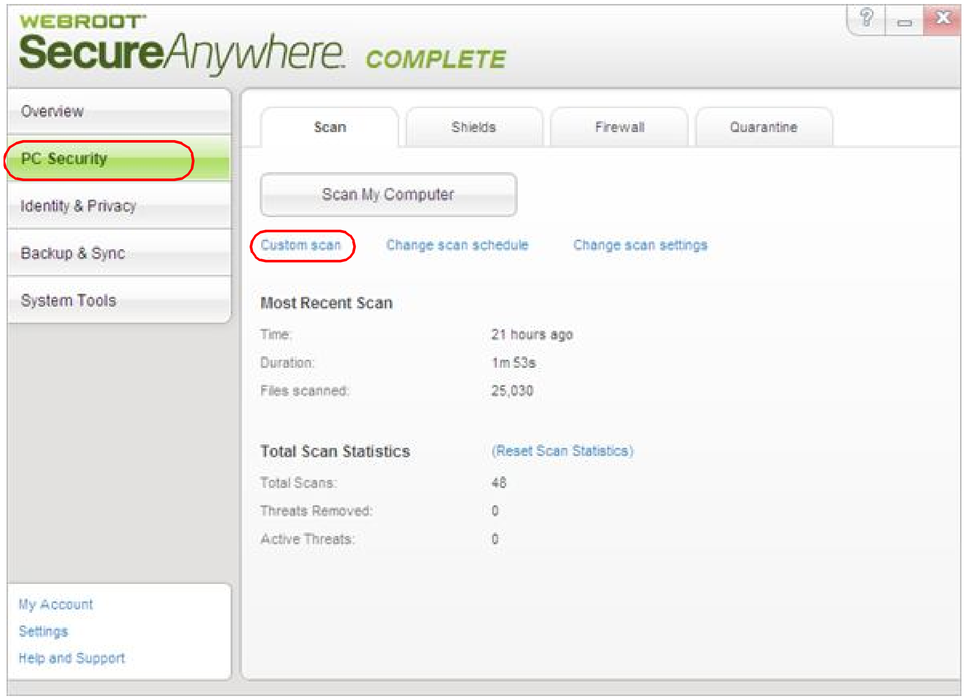
Running a custom scan

Webroot SecureAnywhere allows you to select several types of scans:

- **Quick**. A surface scan of files loaded in memory. This scan runs quickly, but may miss some types of inactive malware that launch after a system reboot. **Note**: If the Quick scan misses an infection, the main interface remains red until you run a Full or Deep scan.
- **Full**. A scan of all hard drives. This type of scan is helpful if you frequently switch between system partitions or you have several programs that have never been scanned before.
- **Deep**. An analytical scan that searches for all types of threats, including rootkits and inactive malware. This is the default scan that runs from the main panel or system tray.
- **Custom**. A customized scan of files and folders (see the instructions below).

To run a custom scan:

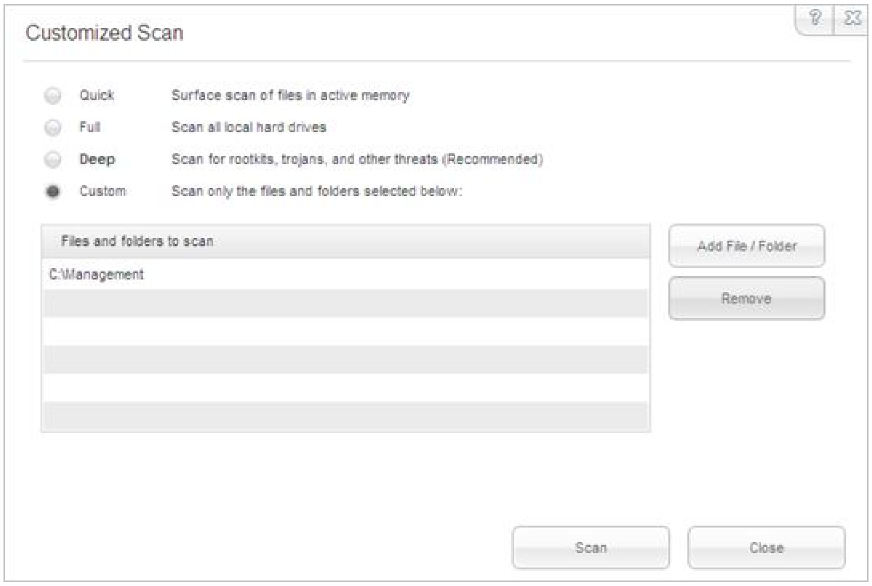
1. Open the main interface (see "Using the main interface" on page 5).
2. Click **PC Security**.
3. From the Scan tab, click **Custom scan**.



Most Recent Scan	
Time:	21 hours ago
Duration:	1m 53s
Files scanned:	25,030

Total Scan Statistics	
Total Scans:	48
Threats Removed:	0
Active Threats:	0

4 In the Customized Scan dialog, select the radio button for the type of scan you want to perform. If you want to select specific files or drives, choose **Custom**. Then you can either drag/drop files into this dialog or click the **Add File/Folder** button to select the directories and files you want.



Customized Scan

○ Quick Surface scan of files in active memory

○ Full Scan all local hard drives

○ **Deep** Scan for rootkits, trojans, and other threats (Recommended)

● Custom Scan only the files and folders selected below:

Files and folders to scan
C:\Management

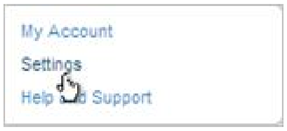
5 Click the **Scan** button to launch the scan.

Changing the scan schedule

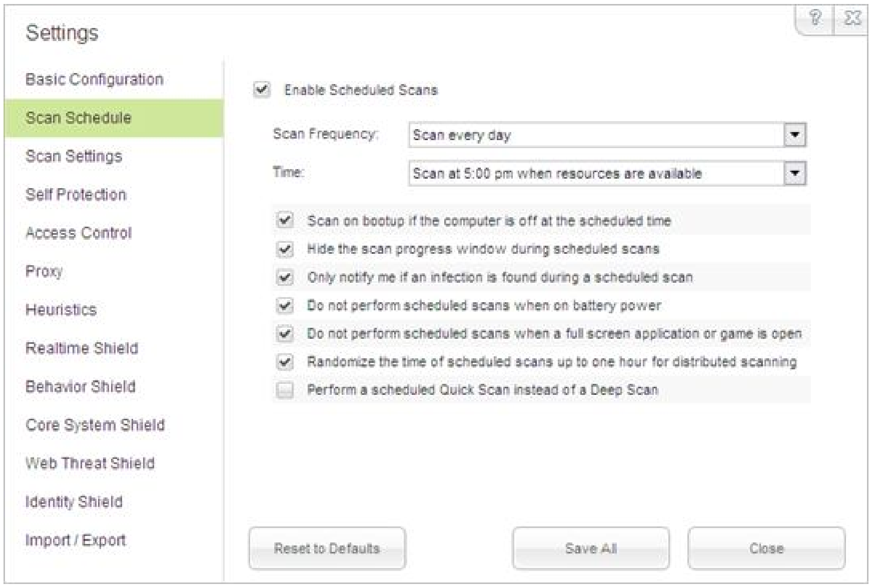
Webroot SecureAnywhere launches scans automatically every day, at about the same time you installed the software. If desired, you can change the scan schedule to run at different times.

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**.



☑ Enable Scheduled Scans

Scan Frequency: Scan every day

Time: Scan at 5:00 pm when resources are available

☑ Scan on bootup if the computer is off at the scheduled time
☑ Hide the scan progress window during scheduled scans
☑ Only notify me if an infection is found during a scheduled scan
☑ Do not perform scheduled scans when on battery power
☑ Do not perform scheduled scans when a full screen application or game is open
☑ Randomize the time of scheduled scans up to one hour for distributed scanning
☐ Perform a scheduled Quick Scan instead of a Deep Scan

4. Make sure the **Enable Scheduled Scans** checkbox is selected.
5. In the **Scan Frequency** field, select one of the following options: every day, a day of the week, or when you boot up (turn on your computer).
6. In the **Time** field, select an approximate time for the scan to launch.

   Note: The scan will launch when computer resources are available, generally within an hour of the time you select.

7. If you want to change one of the schedule settings, select its checkbox to disable it (uncheck the box) or activate it (check the box). When you’re done, click **Save All**.

The settings are described in the table below.

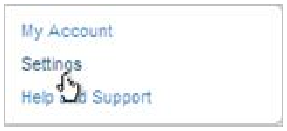
Scan schedule options	
Scan on bootup if the computer is off at the scheduled time	Launches a scheduled scan within an hour after you turn on your computer. If this option is disabled, Webroot SecureAnywhere ignores missed scans.
Hide the scan progress window during scheduled scans	Runs scans silently in the background. If this option is disabled, a window opens and shows the scan progress.
Only notify me if an infection is found during a scheduled scan	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.
Do not perform scheduled scans when on battery power	Helps conserve battery power. If you want Webroot SecureAnywhere to launch scheduled scans when you are on battery power, deselect this option.
Do not perform scheduled scans when a full screen application or game is open	Ignores scheduled scans when you are viewing a full-screen application (such as a movie) or a game. Deselect this option if you want scheduled scans to run anyway.
Randomize the time of scheduled scans up to one hour for distributed scanning	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.
Perform a scheduled Quick Scan instead of a Deep Scan	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.

Changing scan settings

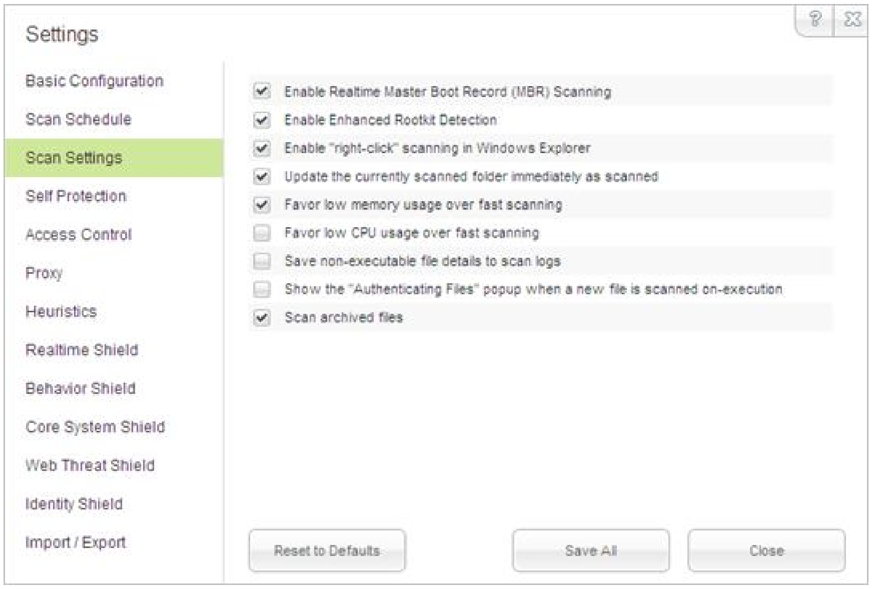
Scan settings provide advanced users with a little more control over scanning performance.

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**.

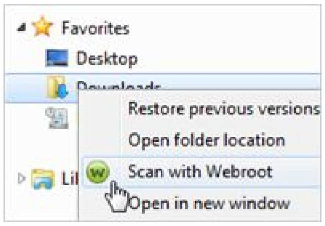


☑ Enable Realtime Master Boot Record (MBR) Scanning
☑ Enable Enhanced Rootkit Detection
☑ Enable "right-click" scanning in Windows Explorer
☑ Update the currently scanned folder immediately as scanned
☑ Favor low memory usage over fast scanning
☐ Favor low CPU usage over fast scanning
☐ Save non-executable file details to scan logs
☐ Show the "Authenticating Files" popup when a new file is scanned on-execution
☑ Scan archived files

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

   The settings are described in the table below.

Scan settings	
Enable Realtime Master Boot Record (MBR) Scanning	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.
Enable Enhanced Rootkit Detection	Checks for rootkits and other malicious software hidden on your disk or in protected areas. Spyware developers often use rootkits to avoid detection and removal. We recommend that you keep this option selected. It adds only a small amount of time to the scan.

Scan settings ***(continued)***	
Enable "right-click" scanning in Windows Explorer	Enables an option for scanning the currently selected file or folder in the Windows Explorer right-click menu.  Favorites Desktop Downloads Restore previous versions Open folder location Scan with Webroot Lil Open in new window This option is helpful if you downloaded a file and want to quickly scan it.
Update the currently scanned folder immediately as scanned	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.
Favor low memory usage over fast scanning	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.
Favor low CPU usage over fast scanning	Reduces CPU usage during scans, but scans will also run a bit slower. Deselect this option to run faster scans.
Save non-executable file details to scan logs	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.
Show the "Authenticating Files" pop-up when a new file is scanned on-execution	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.
Scan archived files	Scans compressed files in zip, rar, cab, and 7-zip archives.

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.

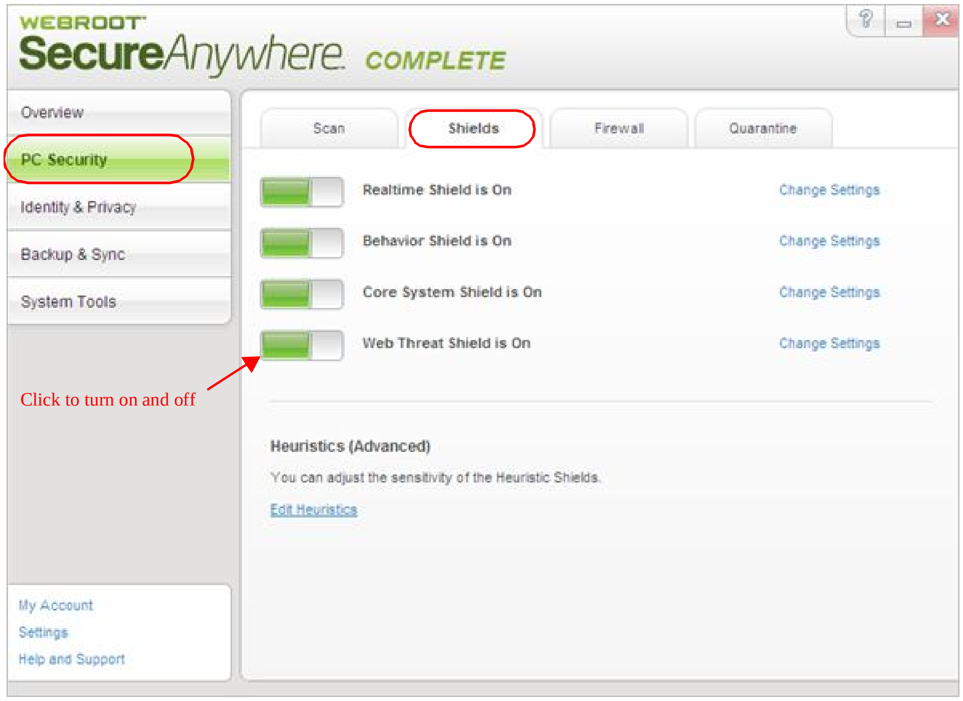
> **Note:** If an alert opens and you aren't certain whether to allow or block the detected item, your safest action is to block it. The file name is displayed in the alert box. Write down the file name and do an Internet search on that file or contact Webroot support at https://www.webrootanywhere.com/support.

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

About shields

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

To view the shield status, click **PC Security** and the **Shields** tab. Each shield setting is displayed in this panel. A green button next to the shield name indicates the shield is **on**. We recommend that you keep all shields enabled; however, you can disable a shield by clicking the green button.



Realtime Shield is On

Behavior Shield is On

Core System Shield is On

Web Threat Shield is On

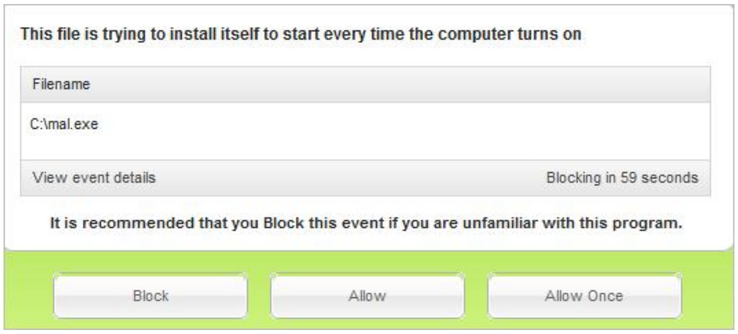
Click to turn on and off

Heuristics (Advanced)

You can adjust the sensitivity of the Heuristic Shields.

Edit Heuristics

Shields run in the background without disrupting your work. If a shield detects an item that it classifies as a potential threat or does not recognize, it opens an alert. The alert asks if you want to allow the item to run or you want to block it.



This file is trying to install itself to start every time the computer turns on

Filename

C:\mal.exe

View event details   Blocking in 59 seconds

It is recommended that you Block this event if you are unfamiliar with this program.

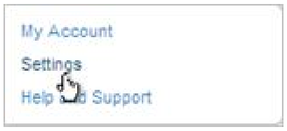
If you recognize the file name and you are purposely downloading it (for example, you were in the process of downloading a new toolbar for your browser), click **Allow** to continue. If you were *not* trying to download anything, you should click **Block**. As you surf Internet sites, you could be targeted for a drive-by download, where an unwanted program launches and silently installs on your computer as you view pages.

Changing Realtime shield settings

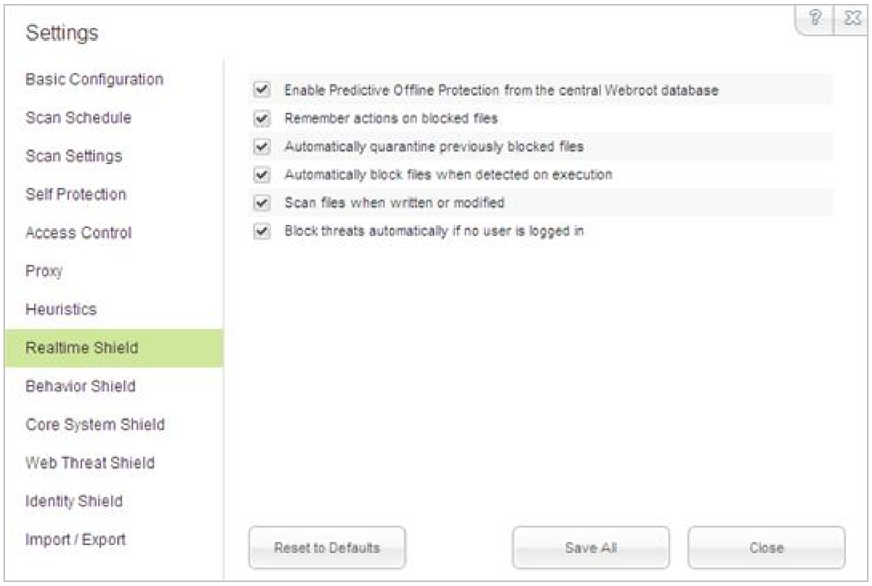
The Realtime shield blocks known threats that are listed in Webroot's threat definitions and community database. If the shield detects a suspicious file, it opens an alert and prompts you to block or allow the item. If it detects a known threat, it immediately blocks and quarantines the item before it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

To change shield settings:

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



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



- ☑ Enable Predictive Offline Protection from the central Webroot database
- ☑ Remember actions on blocked files
- ☑ Automatically quarantine previously blocked files
- ☑ Automatically block files when detected on execution
- ☑ Scan files when written or modified
- ☑ Block threats automatically if no user is logged in

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

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

The settings are described in the table below.

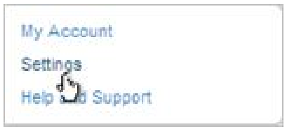
Realtime shield settings	
Enable Predictive Offline Protection from the central Webroot database	Downloads a small threat definition file to your computer, which protects your computer even when it’s offline. We recommend that you keep this option selected.
Remember actions on blocked files	Remembers 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.)
Automatically quarantine previously blocked files	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.
Automatically block files when detected on execution	Automatically blocks threats and sends them to quarantine. If this option is deselected, you must respond to alerts about detected threats.
Scan files when written or modified	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).
Block threats automatically if no user is logged in	Stops threats from executing even when you are logged off. Threats are sent to quarantine without notification.

Changing Behavior shield settings

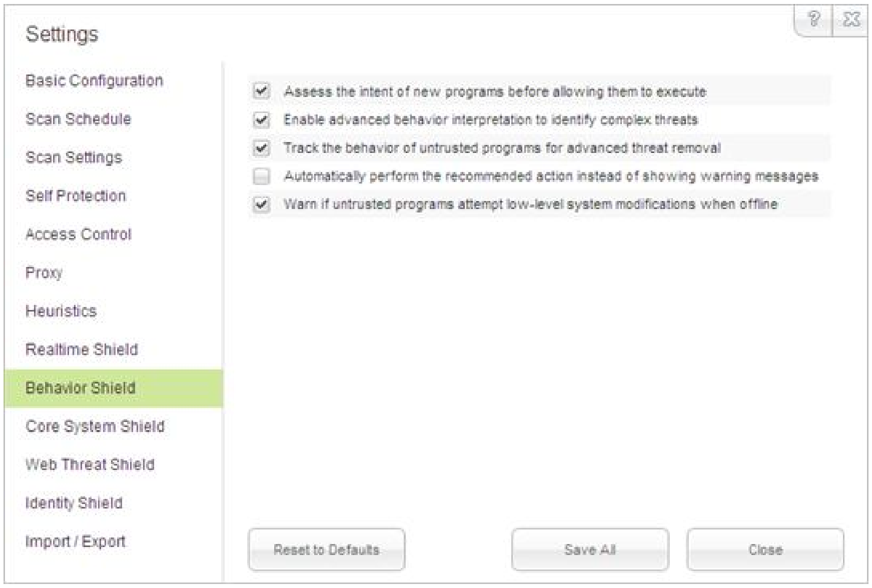
The Behavior shield analyzes the applications and processes running on your computer. If it detects a suspicious file, it opens an alert and prompts you to block or allow the item. If it detects a known threat, it immediately blocks and quarantines the item before it causes damage to your computer or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



☑ Assess the intent of new programs before allowing them to execute
☑ Enable advanced behavior interpretation to identify complex threats
☑ Track the behavior of untrusted programs for advanced threat removal
☐ Automatically perform the recommended action instead of showing warning messages
☑ Warn if untrusted programs attempt low-level system modifications when offline

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

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

The settings are described in the table below.

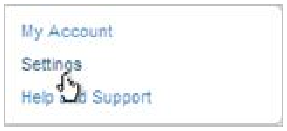
Behavior shield settings	
Assess the intent of new programs before allowing them to execute	Watches the program’s activity before allowing it to execute. If it appears okay, Webroot SecureAnywhere allows it to launch and continues to monitor its activity.
Enable advanced behavior interpretation to identify complex threats	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.)
Track the behavior of untrusted programs for advanced threat removal	Watches programs that have not yet been classified as legitimate or as malware.
Automatically perform the recommended action instead of showing warning messages	Does not prompt you to allow or block a potential threat. Webroot SecureAnywhere will determine how to manage the item.
Warn if untrusted programs attempt low-level system modifications when offline	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.)

Changing Core System shield settings

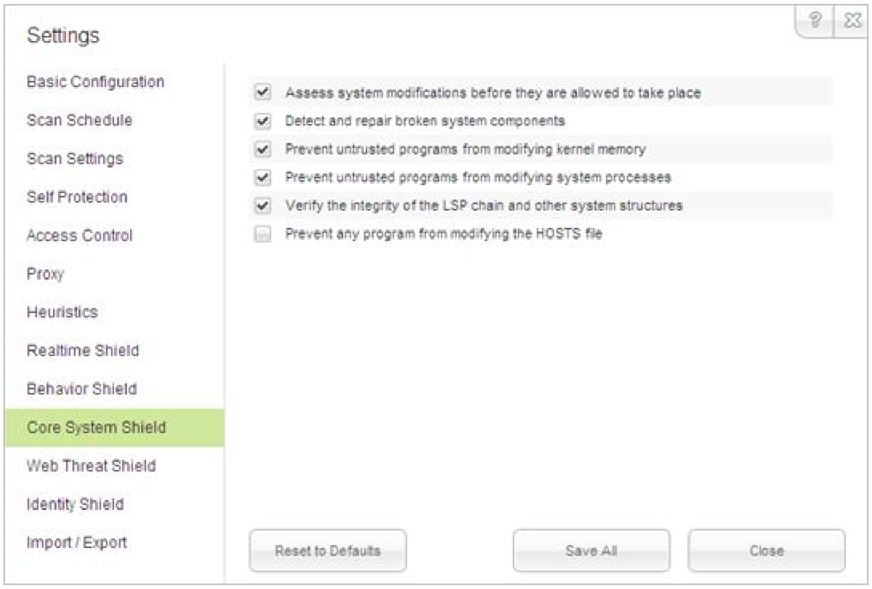
The Core System shield monitors the computer system structures and makes sure malware has not tampered with them. If it detects a suspicious file trying to make changes, it opens an alert and prompts you to block or allow the item. If it detects a known threat, it immediately blocks and quarantines the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



☑ Assess system modifications before they are allowed to take place
☑ Detect and repair broken system components
☑ Prevent untrusted programs from modifying kernel memory
☑ Prevent untrusted programs from modifying system processes
☑ Verify the integrity of the LSP chain and other system structures
□ Prevent any program from modifying the HOSTS file

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

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

The settings are described in the table below.

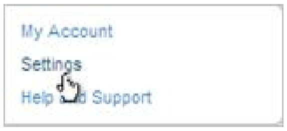
Core System shield settings	
Assess system modifications before they are allowed to take place	Intercepts any activity that attempts to make system changes, such as a new service installation.
Detect and repair broken system components	Locates corrupted components, such as a broken Layered Service Provider (LSP) chain or a virus-infected file, then restores the component or file to its original state.
Prevent untrusted programs from modifying kernel memory	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.
Prevent untrusted programs from modifying system processes	Stops unclassified programs from changing the system processes.
Verify the integrity of the LSP chain and other system structures	Monitors the Layered Service Provider (LSP) chain and other system structures to make sure malware does not corrupt them.
Prevent any program from modifying the HOSTS file	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.

Changing Web Threat shield settings

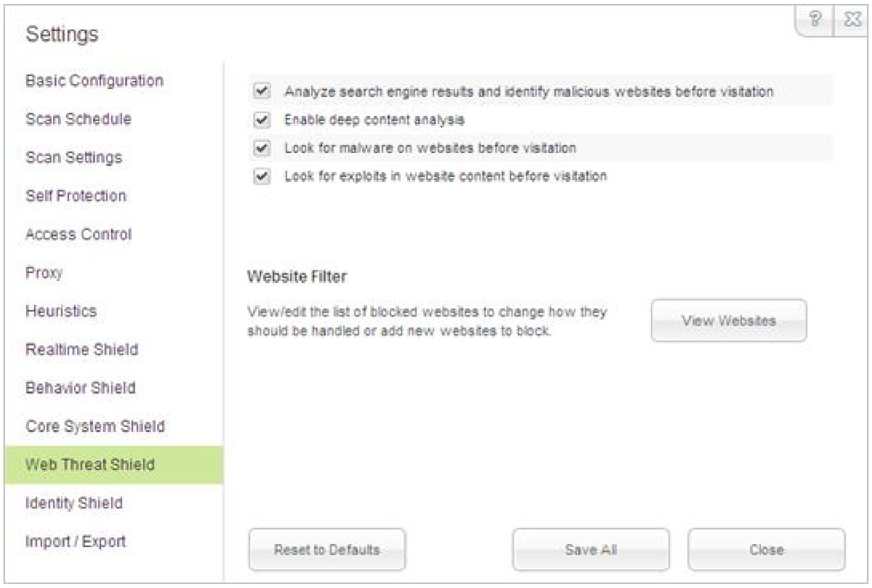
The Web Threat shield protects your system as you surf the Internet. If it detects a website that may be a threat, it opens an alert that allows you to decide whether you want to block the site or continue despite the warning. When you use a search engine, this shield analyzes all the links on the search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

To change shield settings:

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



3. In the Settings dialog, click **Web Threat Shield**.



☑ Analyze search engine results and identify malicious websites before visitation
☑ Enable deep content analysis
☑ Look for malware on websites before visitation
☑ Look for exploits in website content before visitation

Website Filter

View/edit the list of blocked websites to change how they should be handled or add new websites to block.

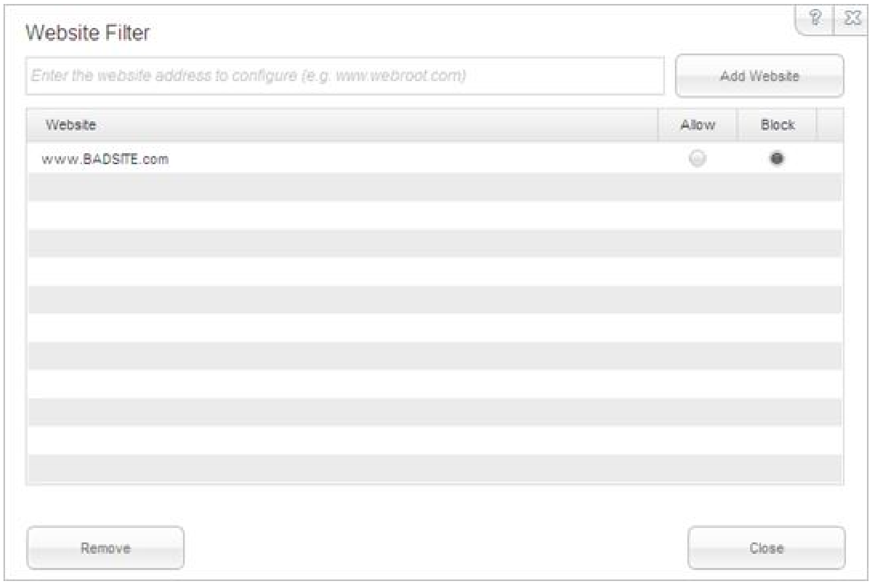
4. If you want to change a setting, select its checkbox to disable it (uncheck the box) or activate it (check the box).

   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.

Web Threat shield settings	
Analyze search engine results and identify malicious websites before visitation	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.
Enable deep content analysis	Analyzes all data traffic on your computer as you visit websites. If threats try to install, it blocks their activity.
Look for malware on websites before visitation	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.
Look for exploits in website content before visitation	Looks for cross-site scripting attacks that may try to redirect you to a different website.

5 If you want to create a list of websites to always block or always allow, click **View Websites**. In the dialog, 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
?
Enter the website address to configure (e.g. www.webroot.com)
Add Website
Remove
Close

Website	Allow	Block
www.BADSITE.com	○	●

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

4: Firewall

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:

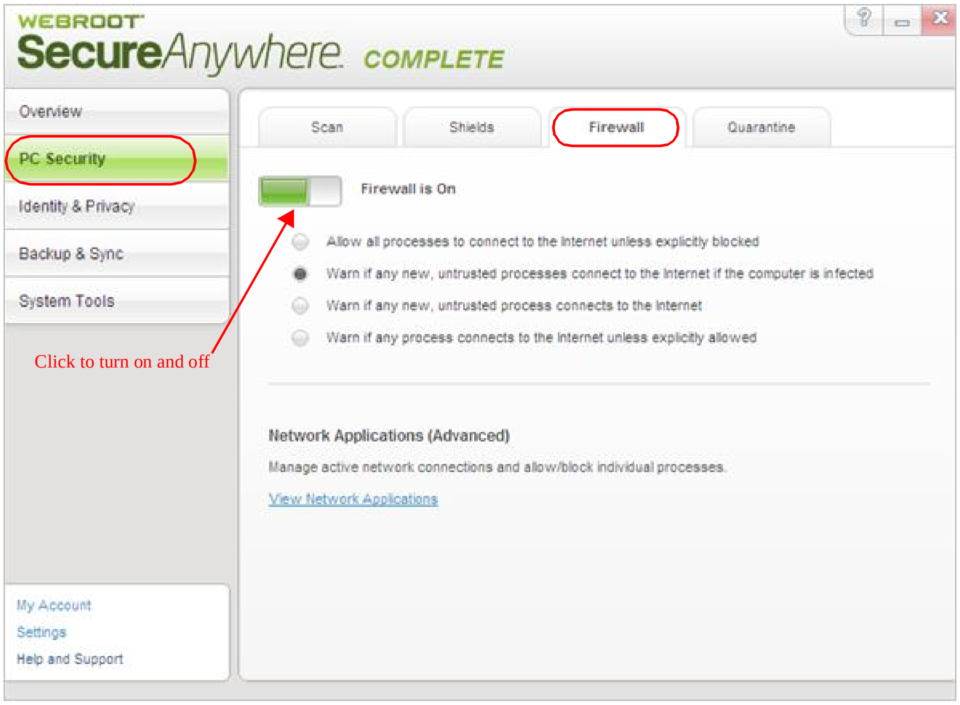
About the firewall

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

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

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

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



Firewall is On

○ Allow all processes to connect to the Internet unless explicitly blocked
● Warn if any new, untrusted processes connect to the Internet if the computer is infected
○ Warn if any new, untrusted process connects to the Internet
○ Warn if any process connects to the Internet unless explicitly allowed

Network Applications (Advanced)

Manage active network connections and allow/block individual processes.

View Network Applications

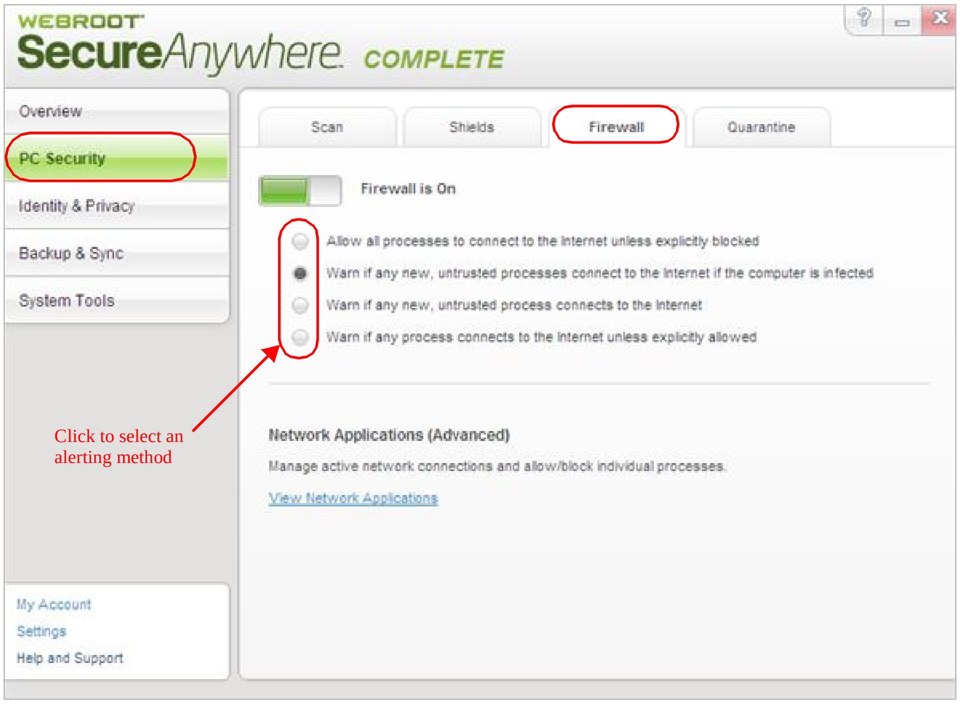
Click to turn on and off

Changing firewall alert settings

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

To change firewall alert settings:

1. Open the main interface (see “Using the main interface” on page 5).
2. Click **PC Security**.
3. Click the **Firewall** tab.
4. Click a radio button to select an alerting method.



Firewall is On

○ Allow all processes to connect to the Internet unless explicitly blocked
● Warn if any new, untrusted processes connect to the Internet if the computer is infected
○ Warn if any new, untrusted process connects to the Internet
○ Warn if any process connects to the Internet unless explicitly allowed

Network Applications (Advanced)

Manage active network connections and allow/block individual processes.

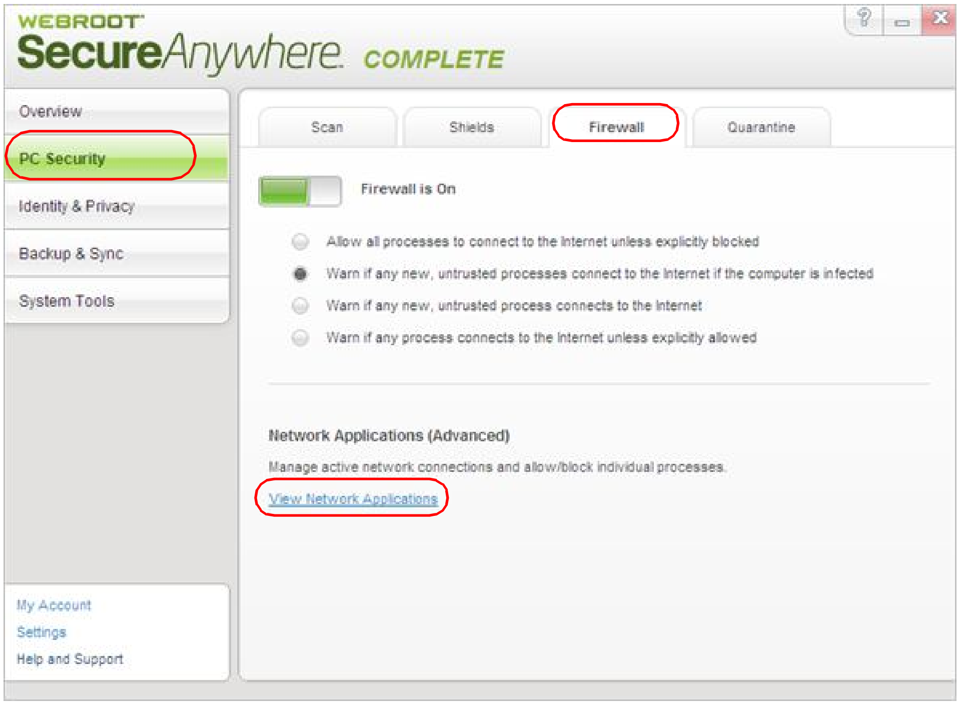
Click to select an alerting method

Managing network applications

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

To change settings for active connections:

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



Firewall is On

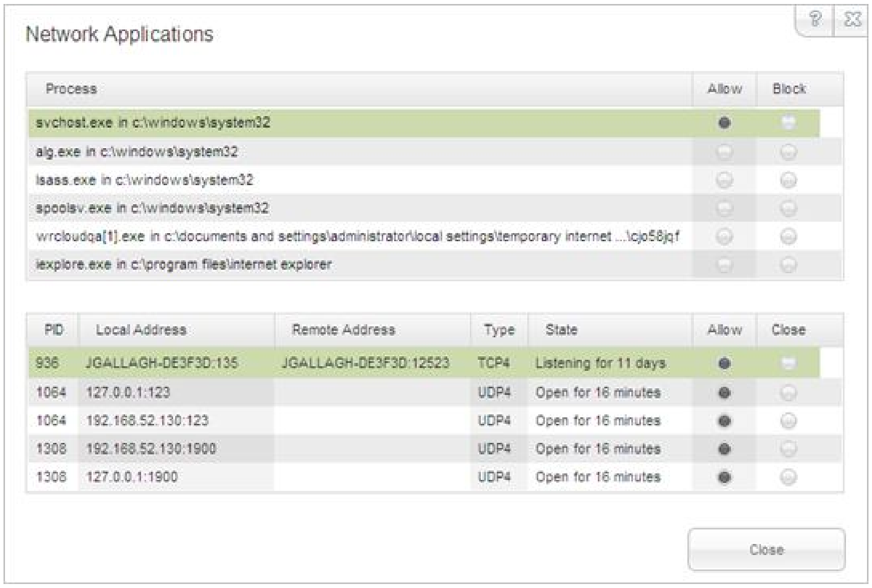
○ Allow all processes to connect to the Internet unless explicitly blocked
● Warn if any new, untrusted processes connect to the Internet if the computer is infected
○ Warn if any new, untrusted process connects to the Internet
○ Warn if any process connects to the Internet unless explicitly allowed

Network Applications (Advanced)

Manage active network connections and allow/block individual processes.

The Network Applications dialog opens.

5 Click on a radio button to allow or block a process, or to allow or close a port.



Network Applications

Process	Allow	Block
svchost.exe in c:\windows\system32	●	○
alg.exe in c:\windows\system32	○	○
lsass.exe in c:\windows\system32	○	○
spoolsv.exe in c:\windows\system32	○	○
wrcloudqa[1].exe in c:\documents and settings\administrator\local settings\temporary internet ...\cjo58jqf	○	○
iexplore.exe in c:\program files\internet explorer	○	○

PID	Local Address	Remote Address	Type	State	Allow	Close
936	JGALLAGH-DE3F3D:135	JGALLAGH-DE3F3D:12523	TCP4	Listening for 11 days	●	○
1064	127.0.0.1:123		UDP4	Open for 16 minutes	●	○
1064	192.168.52.130:123		UDP4	Open for 16 minutes	●	○
1308	192.168.52.130:1900		UDP4	Open for 16 minutes	●	○
1308	127.0.0.1:1900		UDP4	Open for 16 minutes	●	○

5: Quarantine

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.

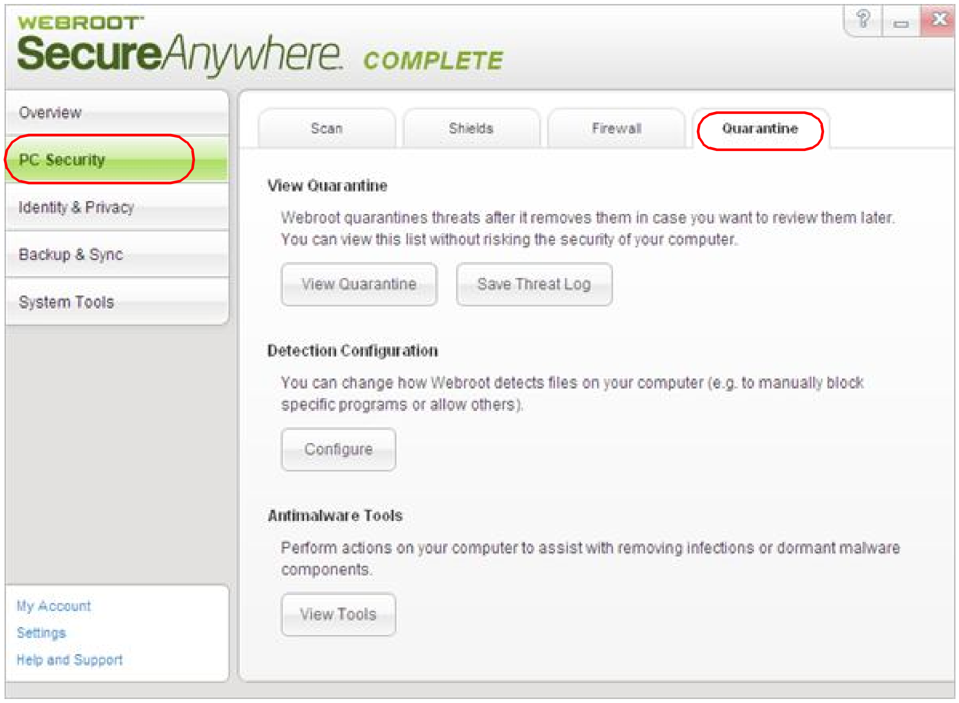
To manage file detection and perform some advanced quarantining functions, see the following topics:

About quarantine

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.



View Quarantine

Webroot quarantines threats after it removes them in case you want to review them later. You can view this list without risking the security of your computer.

Detection Configuration

You can change how Webroot detects files on your computer (e.g. to manually block specific programs or allow others).

Antimalware Tools

Perform actions on your computer to assist with removing infections or dormant malware components.

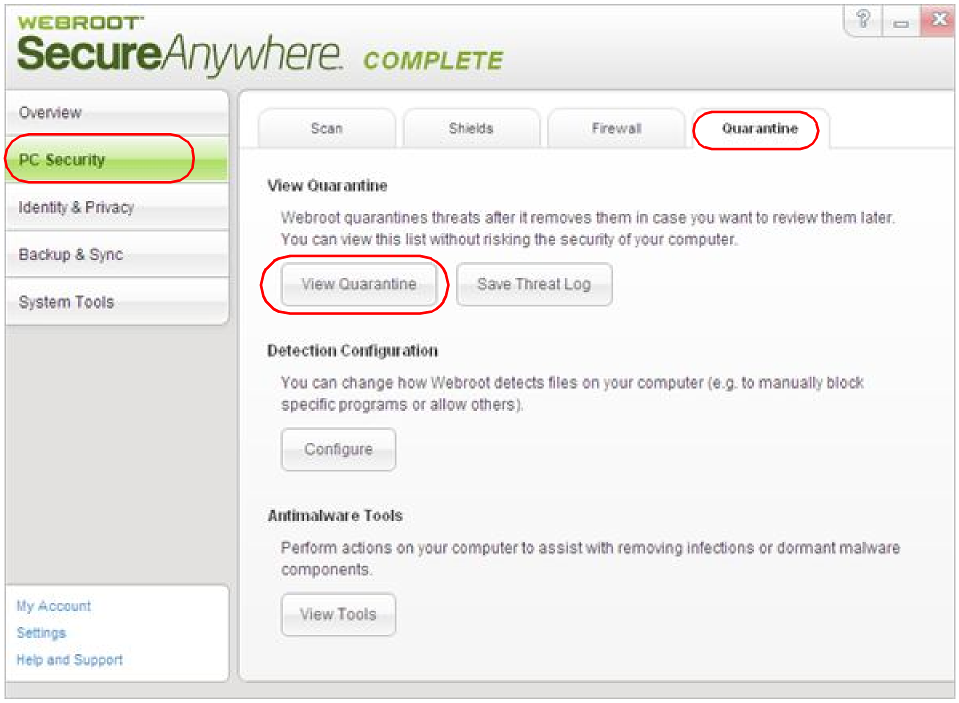
Managing quarantined items

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.



View Quarantine

Webroot quarantines threats after it removes them in case you want to review them later. You can view this list without risking the security of your computer.

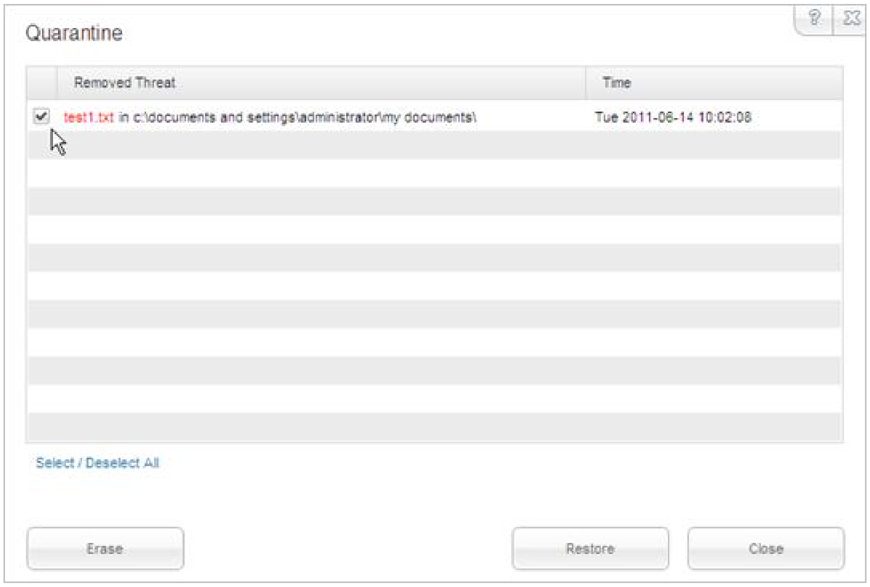
Detection Configuration

You can change how Webroot detects files on your computer (e.g. to manually block specific programs or allow others).

Antimalware Tools

Perform actions on your computer to assist with removing infections or dormant malware components.

The Quarantine panel shows the name of the item, its original location, and the date and time it was quarantined.



Quarantine

	Removed Threat	Time
☑	test1.txt in c:\documents and settings\administrator\my documents\	Tue 2011-06-14 10:02:08

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 45).

Managing file detection

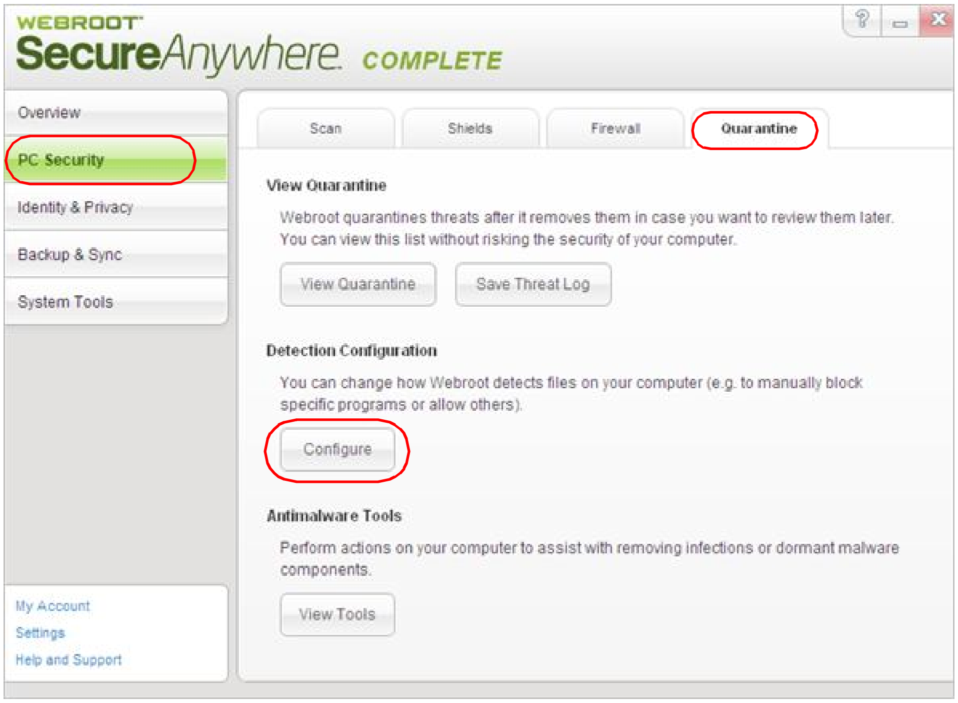
If you want more control over scans and shielding when Webroot SecureAnywhere encounters a specific executable file, you can use Detection Configuration to specify one of the following actions:

- **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.



View Quarantine

Webroot quarantines threats after it removes them in case you want to review them later. You can view this list without risking the security of your computer.

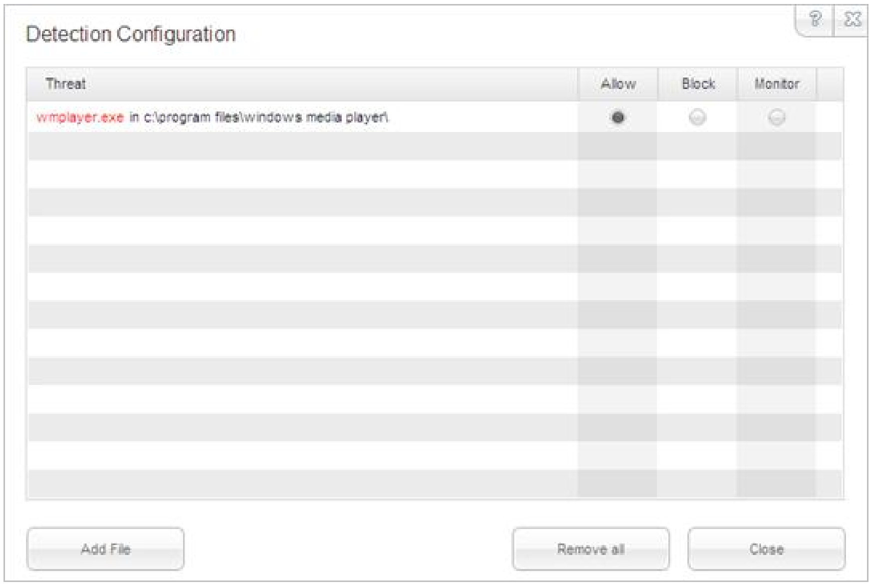
Detection Configuration

You can change how Webroot detects files on your computer (e.g. to manually block specific programs or allow others).

Antimalware Tools

Perform actions on your computer to assist with removing infections or dormant malware components.

The Detection Configuration panel opens.



Threat	Allow	Block	Monitor
wmplayer.exe in c:\program files\windows media player\	●	○	○

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.

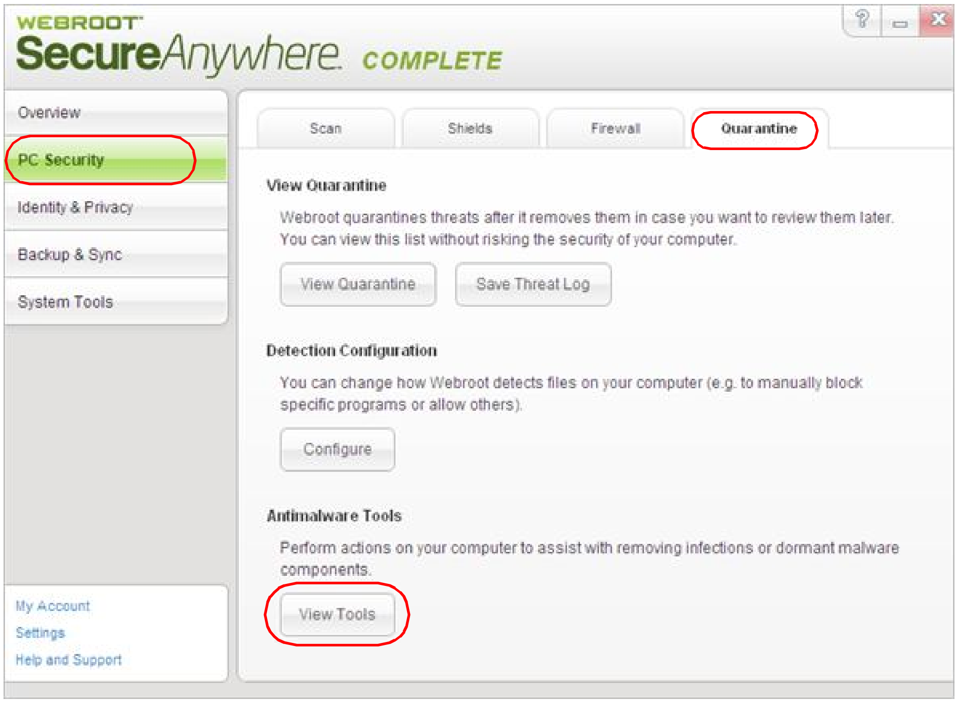
Using antimalware tools

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.



View Quarantine

Webroot quarantines threats after it removes them in case you want to review them later. You can view this list without risking the security of your computer.

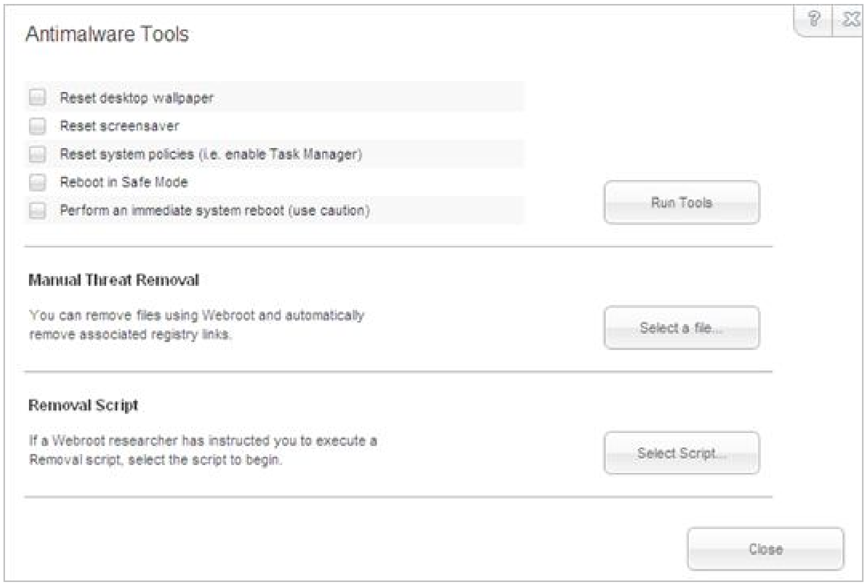
Detection Configuration

You can change how Webroot detects files on your computer (e.g. to manually block specific programs or allow others).

Antimalware Tools

Perform actions on your computer to assist with removing infections or dormant malware components.

The Antimalware Tools panel opens.



□ Reset desktop wallpaper
□ Reset screensaver
□ Reset system policies (i.e. enable Task Manager)
□ Reboot in Safe Mode
□ Perform an immediate system reboot (use caution)

Manual Threat Removal

You can remove files using Webroot and automatically remove associated registry links.

Removal Script

If a Webroot researcher has instructed you to execute a Removal script, select the script to begin.

See the table below for descriptions and instructions.

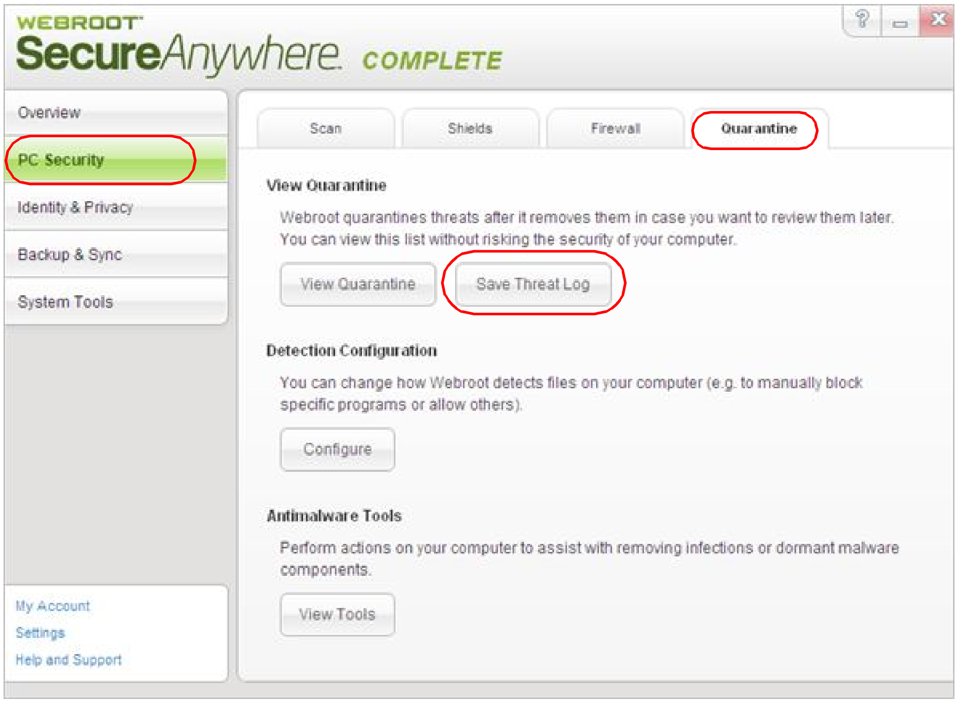
Antimalware tools	
Reset desktop wallpaper	If your computer was recently infected with malware that changed your wallpaper, click the checkbox and click **Run Tools**.
Reset screensaver	If your computer was recently infected with malware that changed your screensaver, click the checkbox and click **Run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

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.



View Quarantine

Webroot quarantines threats after it removes them in case you want to review them later. You can view this list without risking the security of your computer.

Detection Configuration

You can change how Webroot detects files on your computer (e.g. to manually block specific programs or allow others).

Antimalware Tools

Perform actions on your computer to assist with removing infections or dormant malware components.

4. In the dialog, select a folder location for the log and click **Save**.

6: Identity Protection

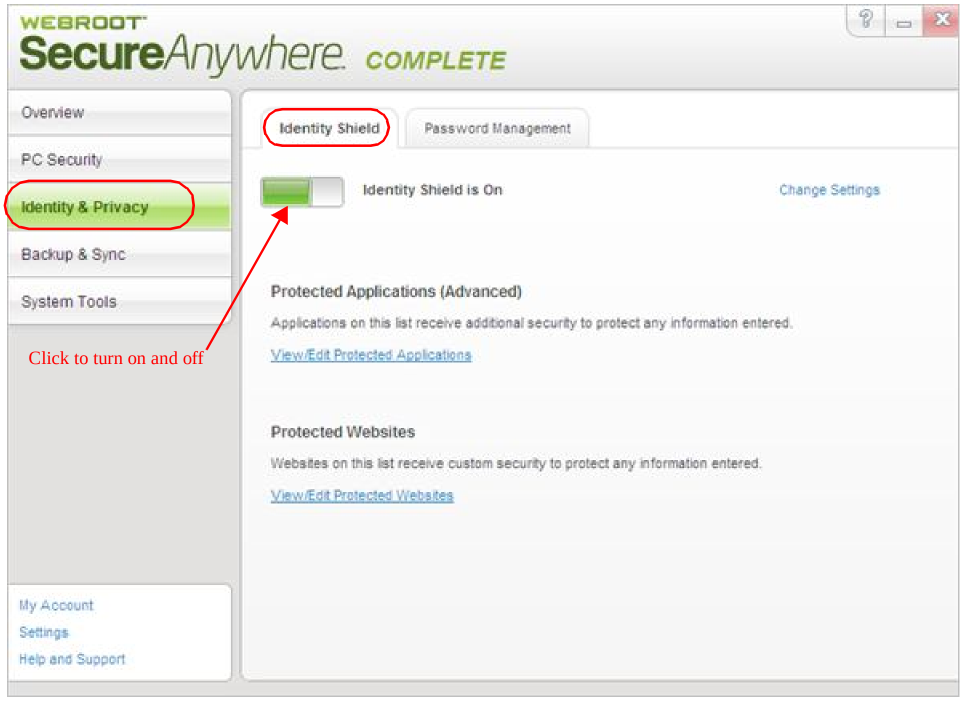
You can use the Identity shield to safely surf the Internet and enter sensitive data in applications. The Identity shield watches for any suspicious activity that may indicate an outside program is attempting to steal information from your computer.

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

About the Identity shield

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

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



Click to turn on and off

Identity Shield is On

Protected Applications (Advanced)

Applications on this list receive additional security to protect any information entered.

Protected Websites

Websites on this list receive custom security to protect any information entered.

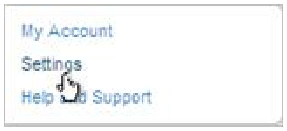
Changing Identity shield settings

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.

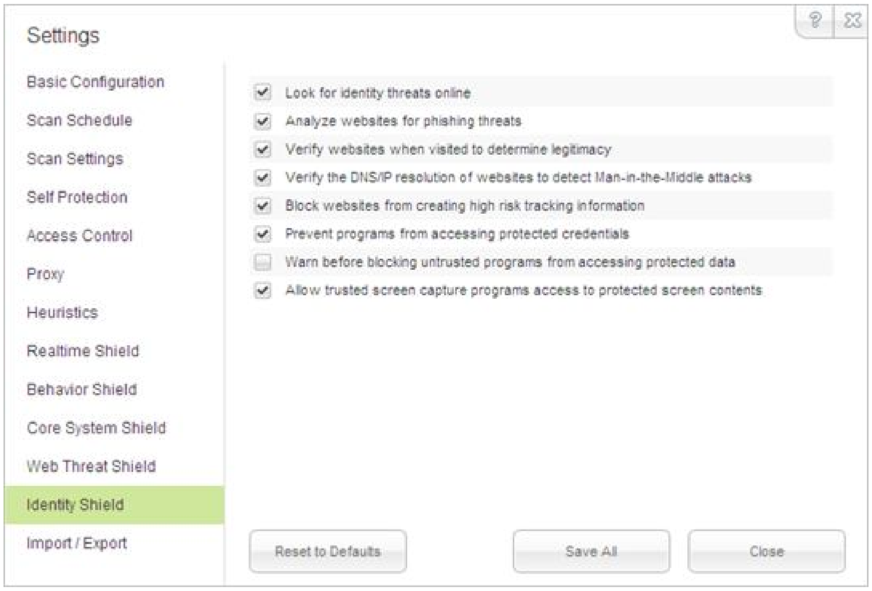
To change Identity shield settings:

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**.



☑ Look for identity threats online
☑ Analyze websites for phishing threats
☑ Verify websites when visited to determine legitimacy
☑ Verify the DNS/IP resolution of websites to detect Man-in-the-Middle attacks
☑ Block websites from creating high risk tracking information
☑ Prevent programs from accessing protected credentials
☐ Warn before blocking untrusted programs from accessing protected data
☑ Allow trusted screen capture programs access to protected screen contents

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

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

The settings are described in the table below.

Identity shield settings	
Look for identity threats online	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.
Analyze websites for phishing threats	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.
Verify websites when visited to determine legitimacy	Analyzes the IP address of each website to determine if it has been redirected or is on our blacklist. If the shield detects an illegitimate website, it blocks the site and opens an alert.
Verify the DNS/IP resolution of websites to detect Man-in-the-Middle attacks	Looks for servers that could be redirecting you to a malicious website (man-in-the-middle attack). If the shield detects a man-in-the-middle attack, it blocks the threat and opens an alert.
Block websites from creating high risk tracking information	Blocks third-party cookies from installing on your computer if the cookies originate from malicious tracking websites. Cookies are small bits of text generated by a web server and then stored on your computer for future use. Cookies can contain everything from tracking information to your personal preferences.
Prevent programs from accessing protected credentials	Blocks programs from accessing your login credentials (for example, when you type your name and password or when you request a website to remember them).
Warn before blocking untrusted programs from accessing protected data	Opens an alert any time malware attempts to access data, instead of blocking known malware automatically. (This option is for technical users only; we recommend that you keep this option disabled so the program does not open numerous alerts.)
Allow trusted screen capture programs access to protected screen contents	Allows you to use legitimate screen capture programs, no matter what content is displayed on your screen.

Managing protected applications

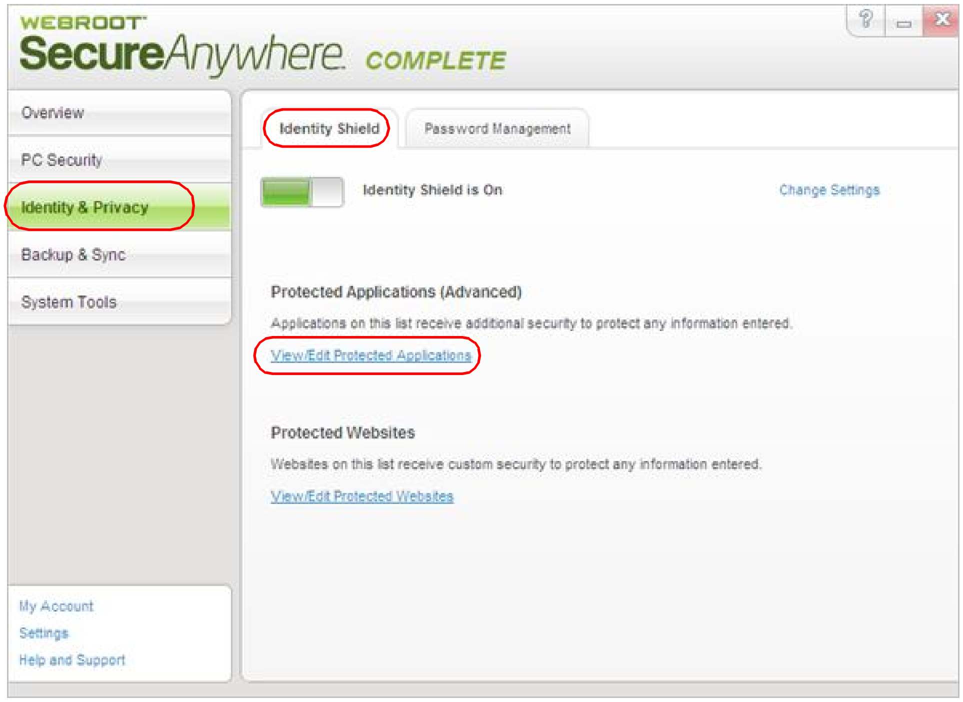
You can provide additional security for software applications that may contain confidential information, such as Instant Messaging clients or tax preparation software. By protecting these applications, you secure them against information-stealing Trojans like keyloggers, man-in-the-middle attacks, and 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**.



Identity Shield is On

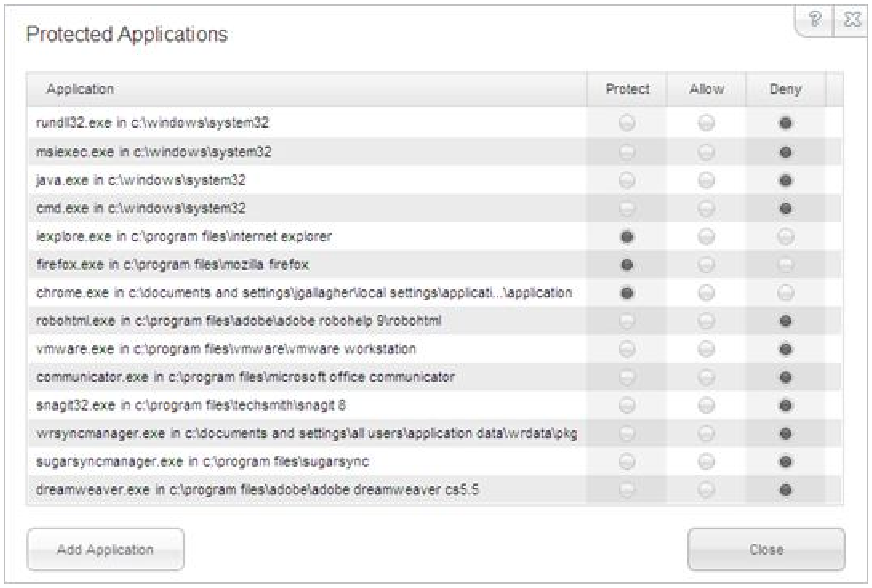
Protected Applications (Advanced)

Applications on this list receive additional security to protect any information entered.

Protected Websites

Websites on this list receive custom security to protect any information entered.

The Protected Applications panel opens. This panel shows the web browsers on your system and any other applications that you run on the computer.



Protected Applications

Application	Protect	Allow	Deny
rundll32.exe in c:\windows\system32	○	○	●
msiexec.exe in c:\windows\system32	○	○	●
java.exe in c:\windows\system32	○	○	●
cmd.exe in c:\windows\system32	○	○	●
iexplore.exe in c:\program files\internet explorer	●	○	○
firefox.exe in c:\program files\mozilla firefox	●	○	○
chrome.exe in c:\documents and settings\jgallagher\local settings\applicati...\application	●	○	○
robohtml.exe in c:\program files\adobe\adobe robohelp 9\robohtml	○	○	●
vmware.exe in c:\program files\vmware\vmware workstation	○	○	●
communicator.exe in c:\program files\microsoft office communicator	○	○	●
snagit32.exe in c:\program files\techsmith\snagit 8	○	○	●
wrsyncmanager.exe in c:\documents and settings\all users\application data\wrdata\pkg	○	○	●
sugarsyncmanager.exe in c:\program files\sugarsync	○	○	●
dreamweaver.exe in c:\program files\adobe\adobe dreamweaver cs5.5	○	○	●

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

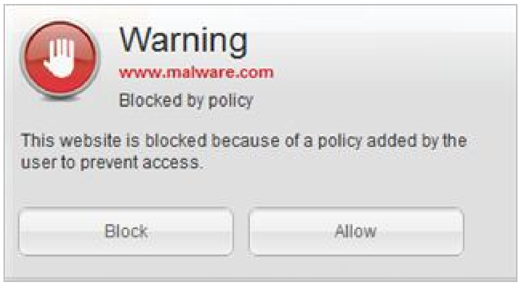
The Identity shield already includes the recommended security settings for specific types of websites. If desired, you can adjust security for a website to one of the following levels:

- **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 secured website, the Webroot icon in the system tray displays a padlock: 🔒.

> **Note: The Identity shield only protects a secured website when the browser window is active in the foreground window** (the padlock is shown in the tray icon). For full protection from screen grabbers, information-stealing Trojans, and other threats, make sure the browser window is in the foreground and you see the padlock in the tray icon.

If the Identity shield encounters a website that may be a threat, it opens an alert. You can decide whether you want to stay secure (click **Block**) or continue despite the warning (click **Allow**).



Warning

www.malware.com

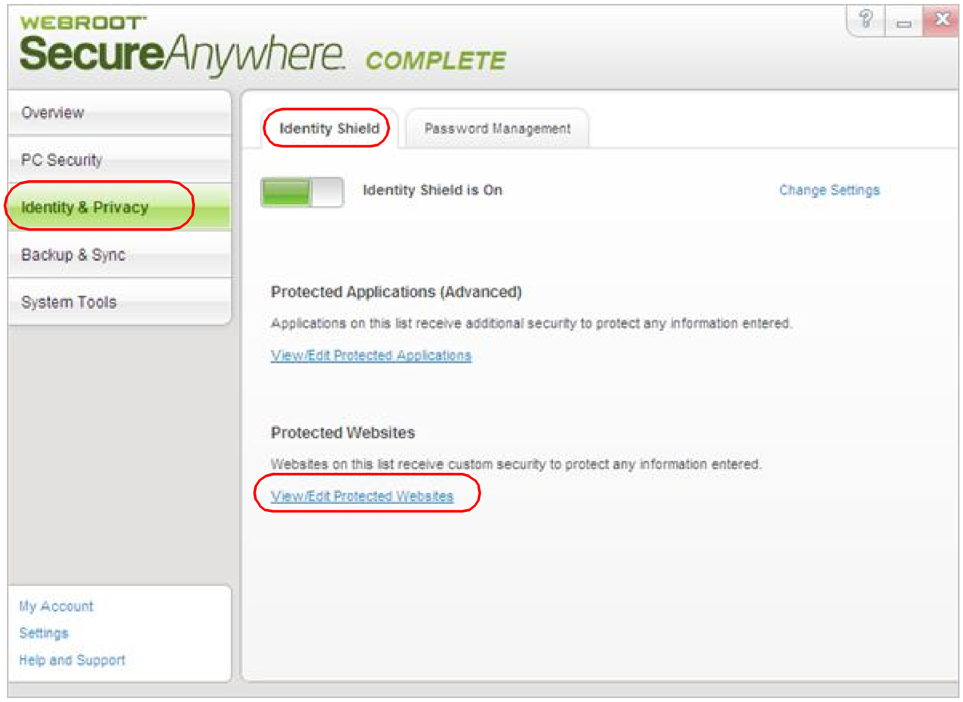
Blocked by policy

This website is blocked because of a policy added by the user to prevent access.

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**.



Identity Shield is On

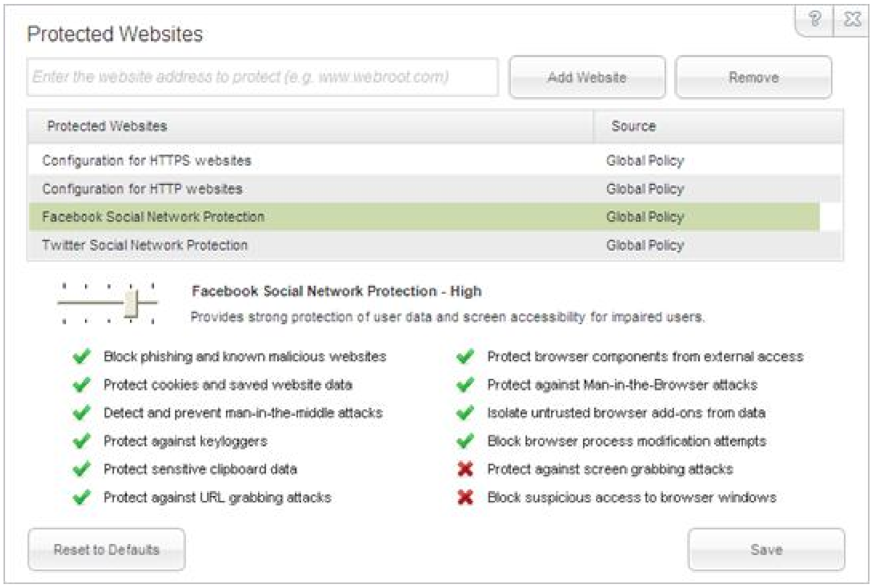
Protected Applications (Advanced)

Applications on this list receive additional security to protect any information entered.

Protected Websites

Websites on this list receive custom security to protect any information entered.

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.



Protected Websites	Source
Configuration for HTTPS websites	Global Policy
Configuration for HTTP websites	Global Policy
Facebook Social Network Protection	Global Policy
Twitter Social Network Protection	Global Policy

Facebook Social Network Protection - High

Provides strong protection of user data and screen accessibility for impaired users.

- ✓ Block phishing and known malicious websites
- ✓ Protect cookies and saved website data
- ✓ Detect and prevent man-in-the-middle attacks
- ✓ Protect against keyloggers
- ✓ Protect sensitive clipboard data
- ✓ Protect against URL grabbing attacks
- ✓ Protect browser components from external access
- ✓ Protect against Man-in-the-Browser attacks
- ✓ Isolate untrusted browser add-ons from data
- ✓ Block browser process modification attempts
- ✗ Protect against screen grabbing attacks
- ✗ Block suspicious access to browser windows

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:

Website protection options	
Block phishing and known malicious websites	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.
Protect cookies and saved website data	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.
Detect and prevent man-in-the middle attacks	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.
Protect against keyloggers	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.
Protect sensitive clipboard data	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.
Protect against URL grabbing attacks	Hides your web browsing activity from malware that attempts to log the websites you visit.
Protect browser components from external access	Hides your web browsing activity from malware that attempts to modify your browser with memory injection and other behind-the-scenes attacks.
Protect against Man-in-the-Browser attacks	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.
Isolate untrusted browser add-ons from data	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.
Block browser process modification attempts	Analyzes browser memory to see if code injection is taking place.
Protect against screen grabbing attacks	Blocks a malicious program from viewing and capturing your screen content.
Block suspicious access to browser windows	Blocks a malicious program from viewing and capturing data in Windows components.

7: Password Management

You can use the Password Manager to automatically log in to websites that require a user name and password. The Password Manager works from your computer or mobile devices. You can also use the Password Manager to populate fields in web forms, saving you the hassle of manually entering your personal data and credit card number in fields.

> **Note**: This section provides a quick overview of the Password Manager. For further instructions, see the *Passwords User Guide* at Webroot's SecureAnywhere Help and Product Guides page.

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

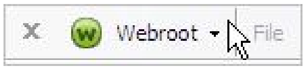
About Password Management

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

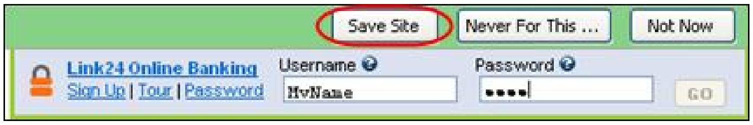
To keep your data safe from hackers, the Password Manager encrypts all your login and password data on your local computer. Webroot uses the same encryption method employed by the US Government for Top Secret data. The encrypted data is meaningless to Webroot and to anyone else without the decryption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

You can use the Password Manager, as follows:

1 **Log in to your Webroot account from the browser toolbar**. After the Passwords component downloads (see "Downloading the Passwords component" on page 63), you can log in to your Webroot account from a browser toolbar. When logged in, the Password Manager detects any information you enter in web forms and prompts you to save the data for future use.



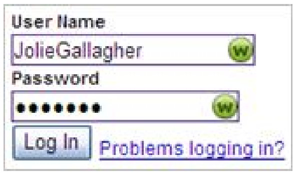
2 **Define or capture login credentials and personal information**. You can either allow the Password Manager to capture data as you enter it in a website or you can manually define the data in the SecureAnywhere website. (See "Capturing login credentials in a website" on page 66 and "Populating fields in web forms" on page 69.)



Username MyName

Password ••••

3 **Access a website that requires a login or personal data in web forms**. After defining login credentials and personal information, you can log in to your Webroot account from the toolbar each time you open a browser. When you are logged in, the Password Manager automatically detects fields in a form and can log in to the website automatically. The Webroot icon appears at the end of the fields to indicate that the login information is stored in the Password Manager. (See "Logging in to websites" on page 68.)



User Name JolieGallagher

Password •••••••

4 **Manage your website information in the SecureAnywhere website.** If you want to change your login credentials for any website, you can open your SecureAnywhere account (my.webrootanywhere.com), click **Go to Passwords**, and edit the information. (See "Managing credentials in the Passwords page" on page 71.)

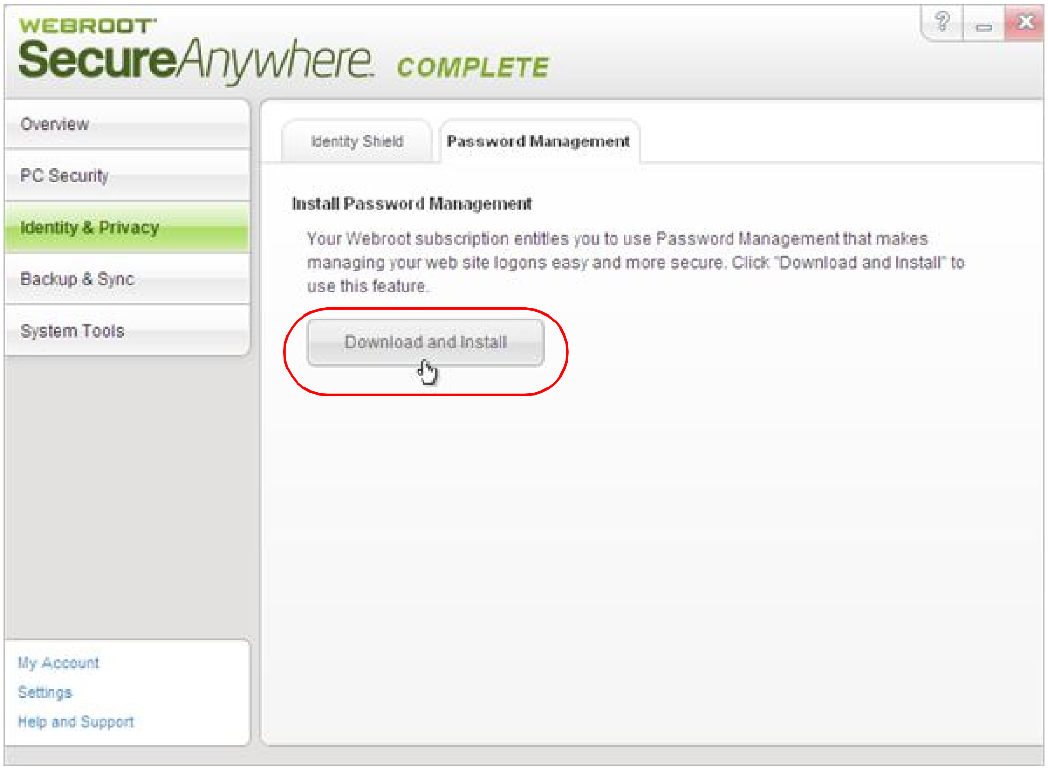
Downloading the Passwords component

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

To get started with the Password Manager:

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

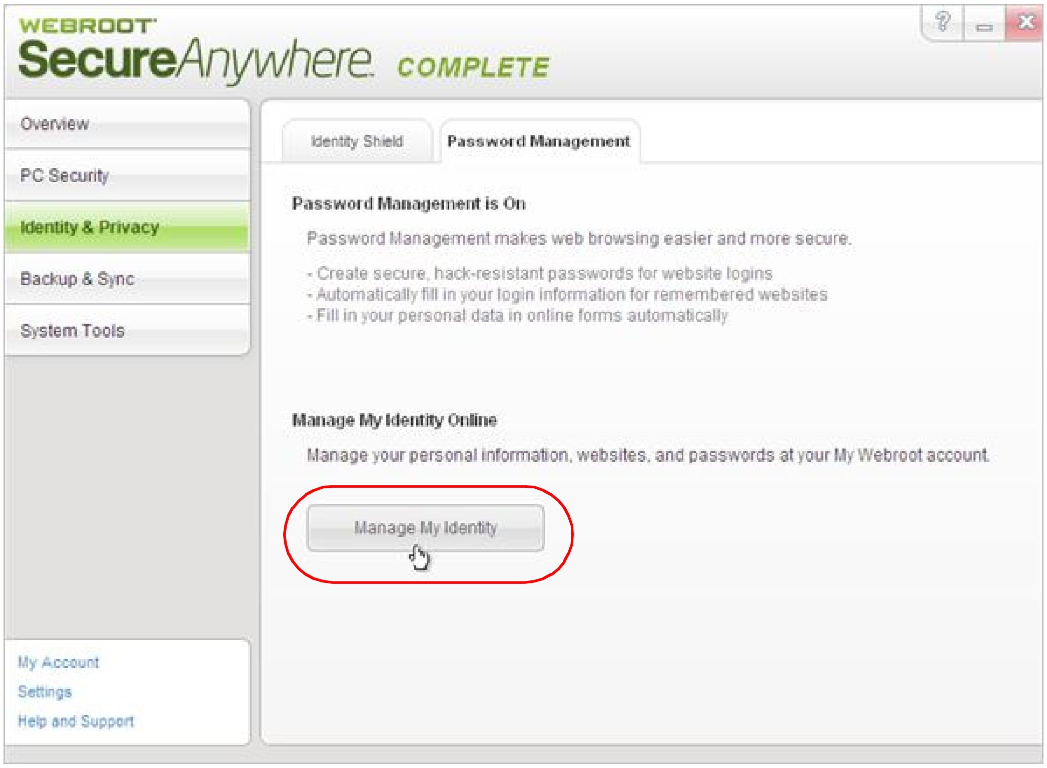
   Note: This button may not appear if the Passwords component installed along with the SecureAnywhere installation.



Install Password Management

Your Webroot subscription entitles you to use Password Management that makes managing your web site logons easy and more secure. Click "Download and Install" to use this feature.

2 When the download completes, you can click **Manage My Identity** to open my.webrootanywhere.com and begin managing your passwords online.



Password Management is On

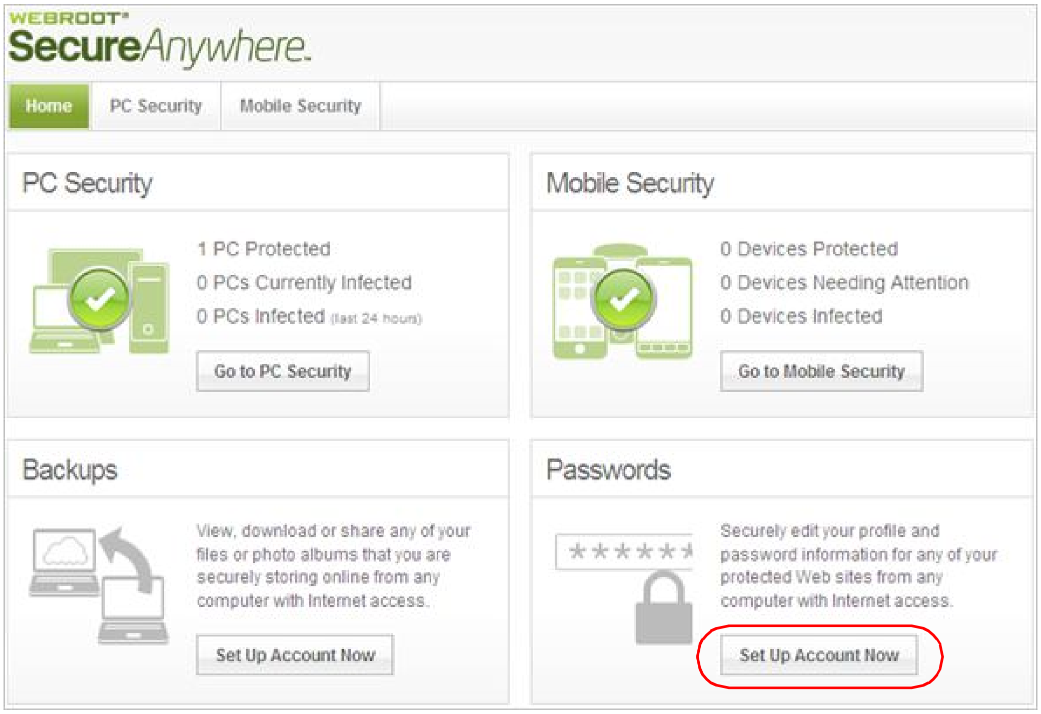
Password Management makes web browsing easier and more secure.

- Create secure, hack-resistant passwords for website logins
- Automatically fill in your login information for remembered websites
- Fill in your personal data in online forms automatically

Manage My Identity Online

Manage your personal information, websites, and passwords at your My Webroot account.

If you have not yet created a Webroot account and enabled Passwords, see "Creating a Webroot account" on page 8. When you log in to my.webrootanywhere.com for the first time, be sure to click **Set Up Account Now** in the Passwords panel.



PC Security

1 PC Protected
0 PCs Currently Infected
0 PCs Infected (last 24 hours)

Mobile Security

0 Devices Protected
0 Devices Needing Attention
0 Devices Infected

Backups

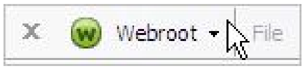
View, download or share any of your files or photo albums that you are securely storing online from any computer with Internet access.

Passwords

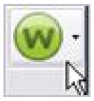
Securely edit your profile and password information for any of your protected Web sites from any computer with Internet access.

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

Internet Explorer:



Firefox:



For further instructions, see the *Passwords User Guide* at Webroot’s SecureAnywhere Help and Product Guides page.

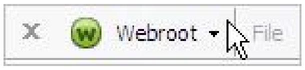
Capturing login credentials in a website

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

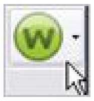
To capture login credentials from a website:

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

Internet Explorer:

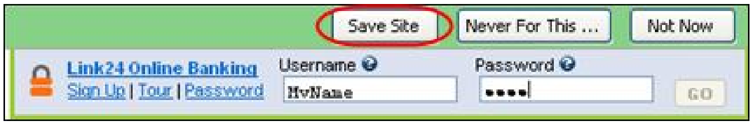


Firefox:



2. Open a website that requires you to log in, such as a banking site or social media site.
3. Enter your user name and password for the site and log in.

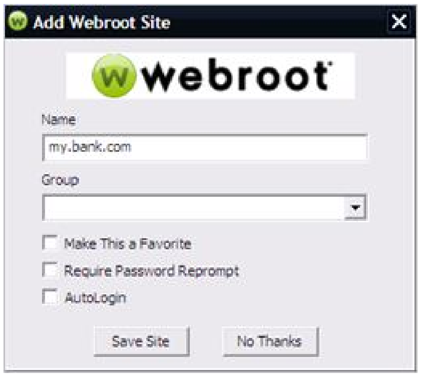
   The Password Manager detects the user name, password, and URL, then prompts you to save the login information from a green toolbar near the top of your browser.
4. From the Webroot prompt, click **Save Site**.



Username: MvName

Password: ••••

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.)



Name: my.bank.com

Group:

□ Make This a Favorite

□ Require Password Reprompt

□ AutoLogin

5 You can specify more information about the site and how you want to access it in the future, as described in the following table:

Add Webroot Site dialog	
Name	The web address will be used for the site name, unless you want to change it to something simple, such as “My Credit Union.”
Group	You can define a name for a group or select one from the list (if you already defined groups). By defining a group, you can organize sites by categories in the Passwords page of the SecureAnywhere website, such as Banking and Shopping. If you do not enter a group, the site is categorized in a Default group.
Make This a Favorite	If you access this site frequently, select the checkbox. You can then use the Open all Favorites option from the Passwords page.
Require Password Reprompt	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.
AutoLogin	If you want to bypass the password prompt and log in automatically, select the checkbox.

6 Click the **Save Site** button.

Your password-managed sites are displayed in your online SecureAnywhere account. See “Managing credentials in the Passwords page” on page 71.

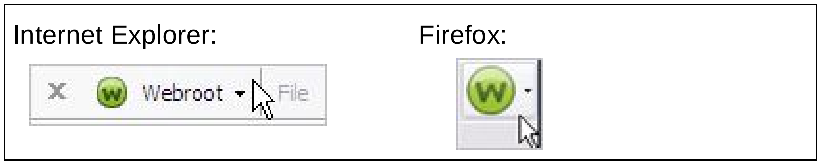
Note: For further instructions, see the *Passwords User Guide* at Webroot’s SecureAnywhere Help and Product Guides page.

Logging in to websites

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

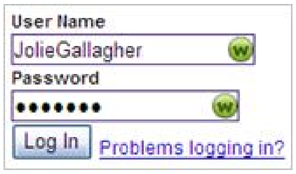
To log in to a website using Password Manager:

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



2 Open a website where you previously saved login credentials with the Password Manager.

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



User Name
JolieGallagher
Password
•••••••
Log In
Problems logging in?

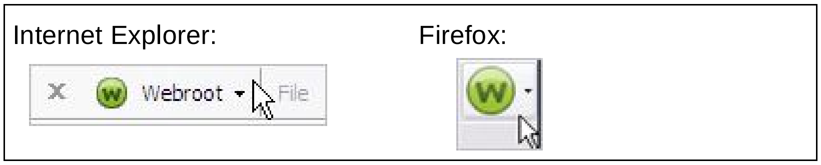
Note: For further instructions, see the *Passwords User Guide* at Webroot's SecureAnywhere Help and Product Guides page.

Populating fields in web forms

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

To create form-fill profiles:

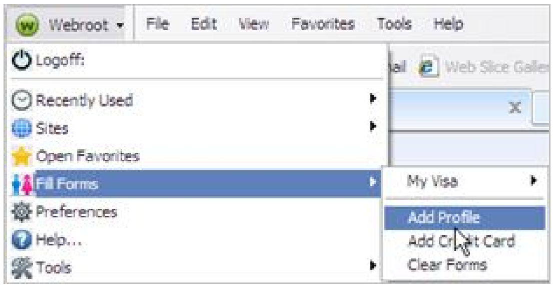
1 Open Internet Explorer or Firefox. Log in to your SecureAnywhere account by clicking the Webroot icon in your browser's toolbar, then entering your SecureAnywhere user name and password.



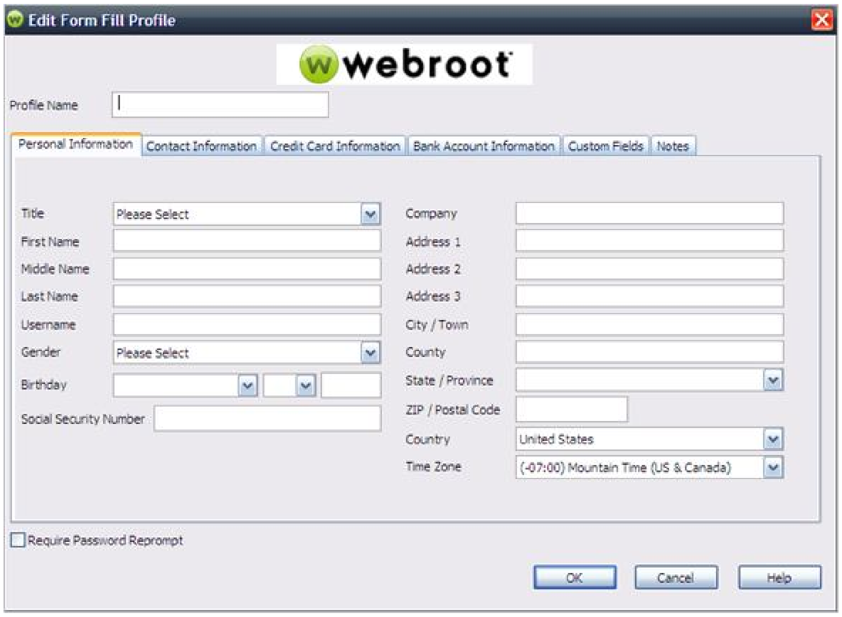
Internet Explorer:

Firefox:

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



The Edit Form Fill Profile dialog opens.



Profile Name

Title: Please Select

First Name

Middle Name

Last Name

Username

Gender: Please Select

Birthday

Social Security Number

Company

Address 1

Address 2

Address 3

City / Town

County

State / Province

ZIP / Postal Code

Country: United States

Time Zone: (-07:00) Mountain Time (US & Canada)

☐ Require Password Reprompt

3 In the **Profile Name** field, enter a name that defines this profile, such as Personal Info or My Visa.

4 Enter as much information as you want in each field. (Click on the tabs for **Personal Information**, **Contact Information**, **Credit Card Information**, **Bank Account Information**, **Custom Fields**, and **Notes** to move between panels.)

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

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

5 When you're done, click **OK**.

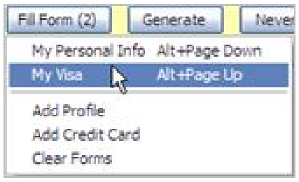
You can now use the profile to automatically fill your personal data in web fields.

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

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

The yellow Password Manager toolbar opens.

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



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

Note: For further instructions, see the *Passwords User Guide* at Webroot's SecureAnywhere Help and Product Guides page.

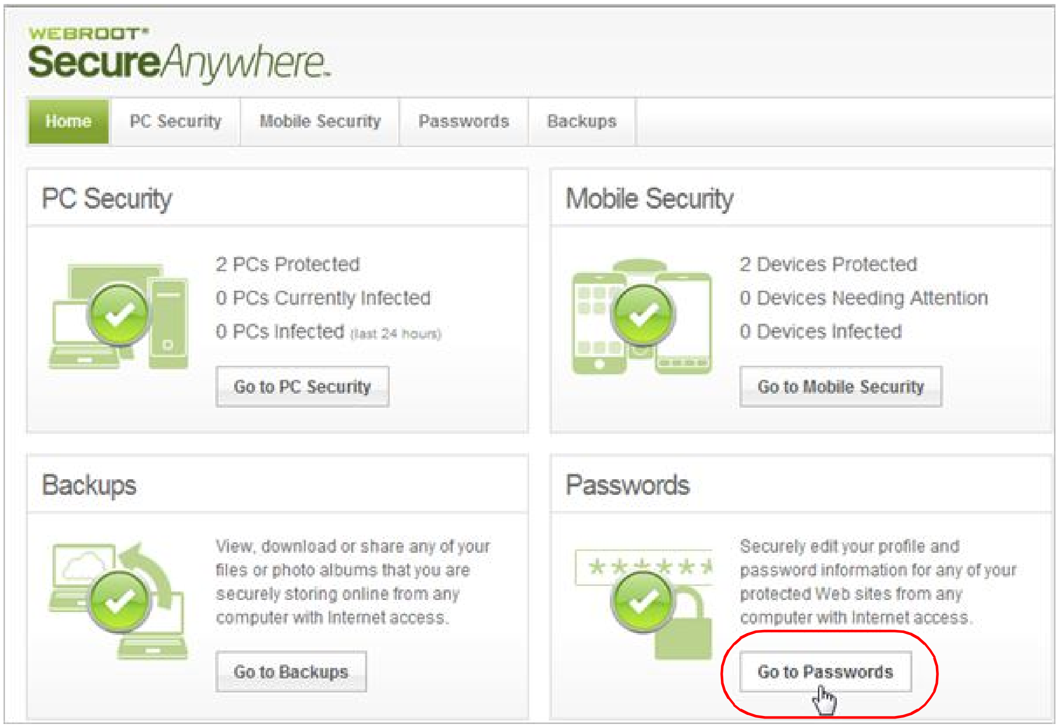
Managing credentials in the Passwords page

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

To manage credentials in the Passwords site:

1 Log in to my.webrootanywhere.com.

2 Click **Go to Passwords**.



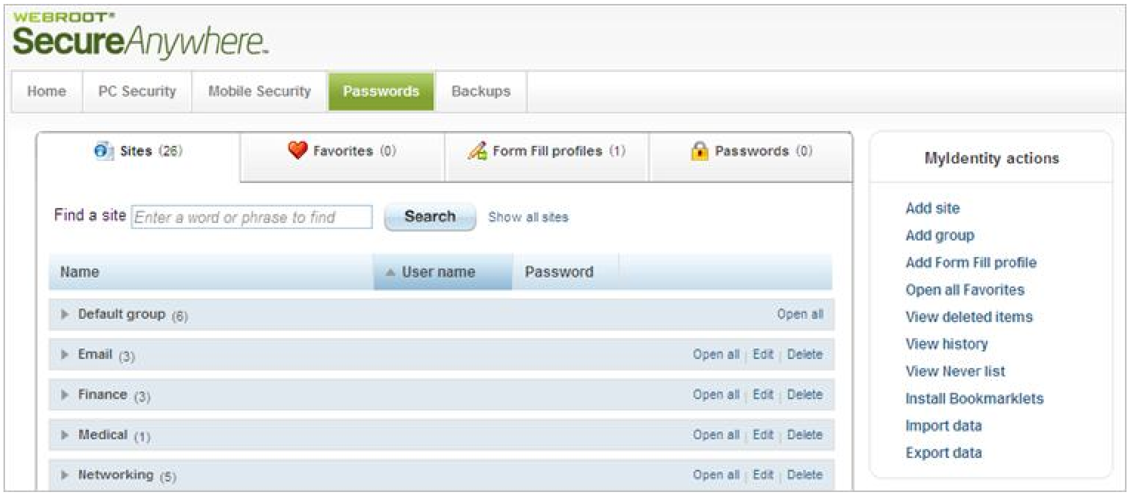
2 PCs Protected
0 PCs Currently Infected
0 PCs Infected (last 24 hours)

2 Devices Protected
0 Devices Needing Attention
0 Devices Infected

View, download or share any of your files or photo albums that you are securely storing online from any computer with Internet access.

Securely edit your profile and password information for any of your protected Web sites from any computer with Internet access.

The Passwords web page opens in your browser.



Name	User name	Password	
Default group (6)			Open all
Email (3)			Open all | Edit | Delete
Finance (3)			Open all | Edit | Delete
Medical (1)			Open all | Edit | Delete
Networking (5)			Open all | Edit | Delete

3 For further instructions on using the Passwords web page, see the *Passwords User Guide* at Webroot's SecureAnywhere Help and Product Guides page.

8: Backup & Sync

You can use Backup & Sync to designate folders that automatically synchronize to Webroot's online repository. This repository is a collection of secure servers where your data is safely encrypted and stored. The uploaded data is available from the Backups page of the SecureAnywhere website, on all your computers with Backup & Sync configured, and on your mobile devices with the SecureSync app installed. After the initial upload, Backup & Sync monitors synchronized folders for updates made to the files (adding, editing, or deleting), then automatically uploads those changes to your SecureAnywhere account. Conversely, if you modify files from within your SecureAnywhere account, changes are synchronized back to your computer. The content between your computer and online account is always kept synchronized. You never need to manually synchronize files yourself.

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

To get started with Backup & Sync:

About Backup & Sync

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

There are several methods of securing your data:

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

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

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

  For instructions, see "Downloading the Backup & Sync component" on page 75 and "Configuring synchronized folders" on page 77.

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

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

  For instructions, see "Using the Magic Briefcase" on page 79.

- **Copying files to the Web Archive**. If you have important documents or photos that you want backed up, but not synchronized, you should upload them to the Web Archive. For example, you may want to back up tax returns, old photos, and a scanned copy of your passport. These types of documents won't change and don't need to be kept in synchronization with other computers.

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

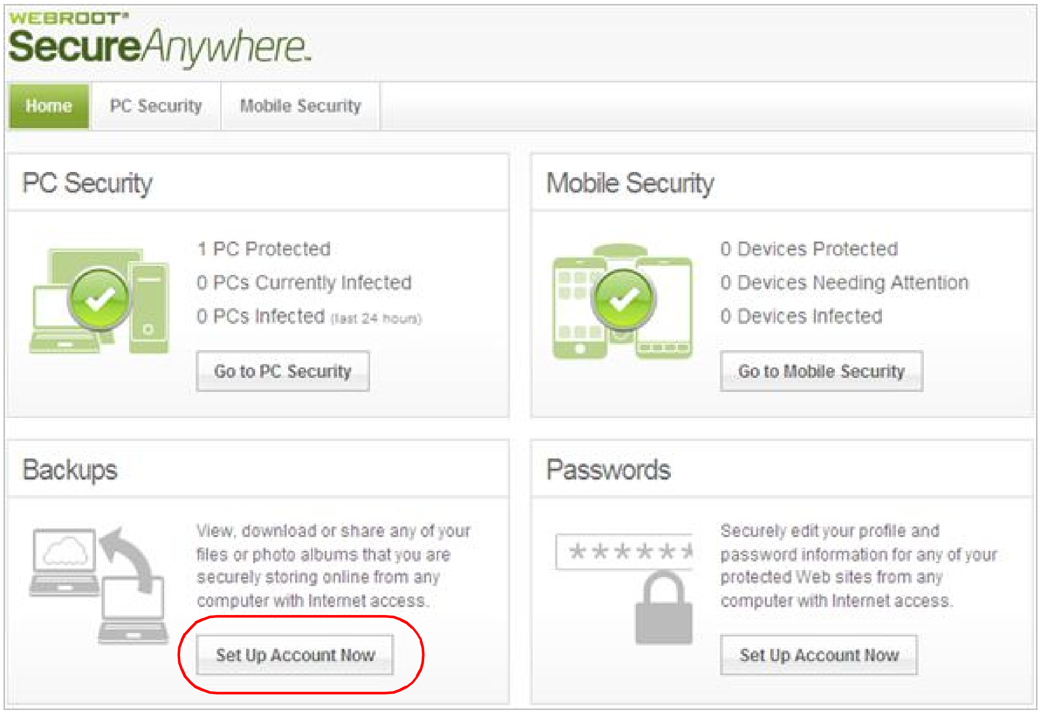
  For instructions, see "Copying files to the Web Archive" on page 80.

Downloading the Backup & Sync component

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

To get started with Backup & Sync:

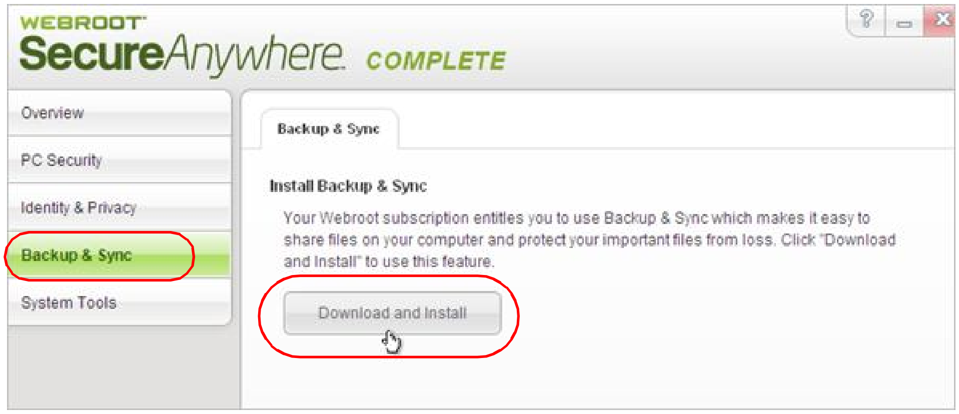
1 If you have not yet created a Webroot account and enabled Backups, see "Creating a Webroot account" on page 8. When you log in to my.webrootanywhere.com for the first time, be sure to click **Set Up Account Now** in the Backups panel.



View, download or share any of your files or photo albums that you are securely storing online from any computer with Internet access.

Securely edit your profile and password information for any of your protected Web sites from any computer with Internet access.

2 From your computer, open the SecureAnywhere main interface (see "Using the main interface" on page 5). Click **Backup & Sync**, then click **Download and Install**.

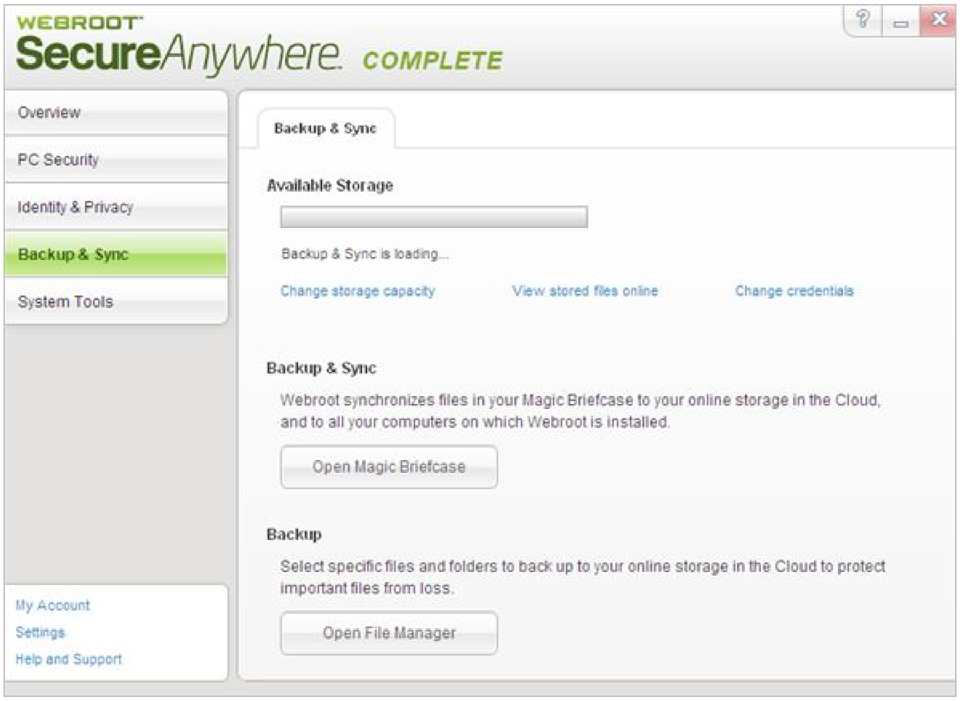


Install Backup & Sync

Your Webroot subscription entitles you to use Backup & Sync which makes it easy to share files on your computer and protect your important files from loss. Click "Download and Install" to use this feature.

3 If prompted, enter your Webroot account credentials (user name and password).

When the download completes, the Backup & Sync panel opens.



Backup & Sync is loading...

Webroot synchronizes files in your Magic Briefcase to your online storage in the Cloud, and to all your computers on which Webroot is installed.

Select specific files and folders to back up to your online storage in the Cloud to protect important files from loss.

4 You can now begin synchronizing or backing up files by following these instructions:

- "Configuring synchronized folders" on page 77
- "Using the Magic Briefcase" on page 79
- "Copying files to the Web Archive" on page 80

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

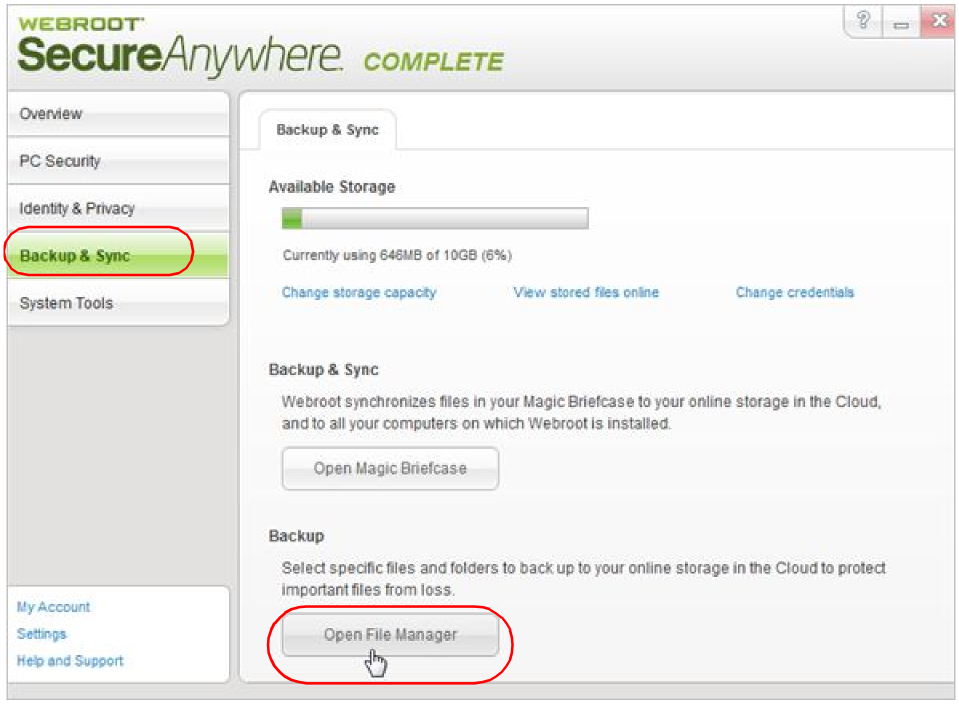
Configuring synchronized folders

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

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

To set up synchronized folders:

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



Available Storage

Currently using 646MB of 10GB (6%)

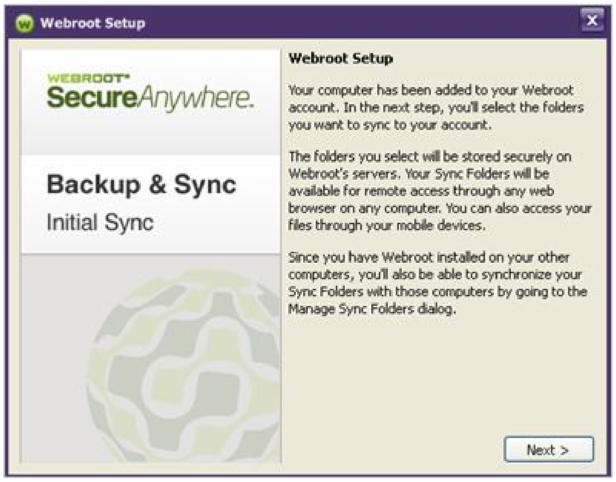
Backup & Sync

Webroot synchronizes files in your Magic Briefcase to your online storage in the Cloud, and to all your computers on which Webroot is installed.

Backup

Select specific files and folders to back up to your online storage in the Cloud to protect important files from loss.

If you have not yet created synchronized folders, the Setup dialog opens.



Webroot Setup

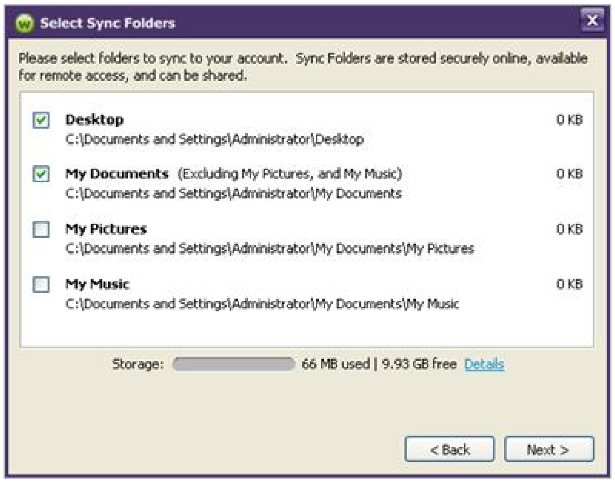
Your computer has been added to your Webroot account. In the next step, you'll select the folders you want to sync to your account.

The folders you select will be stored securely on Webroot's servers. Your Sync Folders will be available for remote access through any web browser on any computer. You can also access your files through your mobile devices.

Since you have Webroot installed on your other computers, you'll also be able to synchronize your Sync Folders with those computers by going to the Manage Sync Folders dialog.

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**.



Please select folders to sync to your account. Sync Folders are stored securely online, available for remote access, and can be shared.

☑ **Desktop** 0 KB
C:\Documents and Settings\Administrator\Desktop

☑ **My Documents** (Excluding My Pictures, and My Music) 0 KB
C:\Documents and Settings\Administrator\My Documents

□ **My Pictures** 0 KB
C:\Documents and Settings\Administrator\My Documents\My Pictures

□ **My Music** 0 KB
C:\Documents and Settings\Administrator\My Documents\My Music

Storage: 66 MB used | 9.93 GB free Details

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

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

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

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

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

6. You can also check your online account in the Backups page. See "Managing files in the Backups page" on page 84.

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

Using the Magic Briefcase

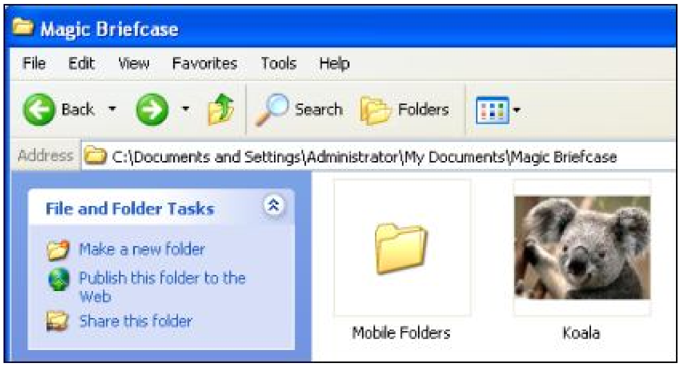
The Magic Briefcase is a synchronized folder that Webroot has configured for your convenience. It resides under your personal Documents folder in Windows. Any files you put in the Magic Briefcase are automatically synchronized with your online account and with any other computers or mobile devices in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

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

To use the Magic Briefcase:

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

   When you copy the file to the Magic Briefcase, the file is instantly synchronized to your online SecureAnywhere account and to your other devices with SecureAnywhere installed.



Address C:\Documents and Settings\Administrator\My Documents\Magic Briefcase

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

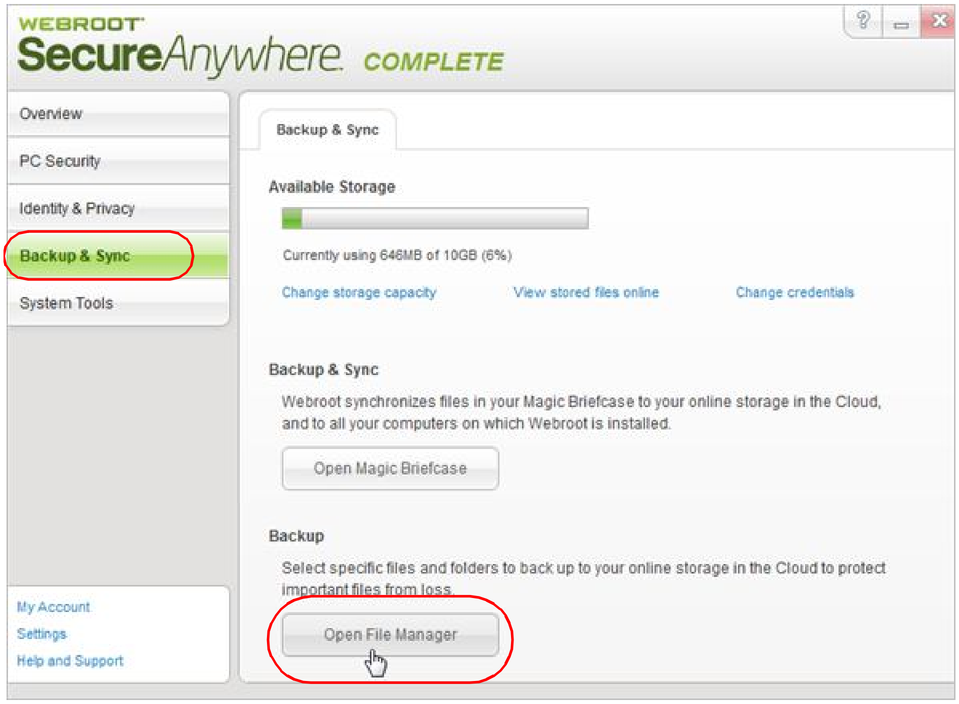
Copying files to the Web Archive

If you have important documents or photos that you want backed up, but not synchronized, you should upload them to the Web Archive. For example, you may want to back up tax returns, old photos, and a scanned copy of your passport. These types of documents won’t change and don’t need to be kept in synchronization with other computers.

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

To copy files to the Web Archive:

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

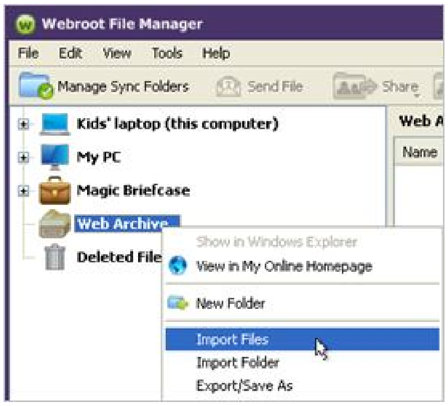


Currently using 646MB of 10GB (6%)

Webroot synchronizes files in your Magic Briefcase to your online storage in the Cloud, and to all your computers on which Webroot is installed.

Select specific files and folders to back up to your online storage in the Cloud to protect important files from loss.

3 In the Webroot File Manager, right-click **Web Archive** to display the pop-up menu, then select either **Import Files** or **Import Folder**.



4 From the dialog that opens, select the files or folders you want archived.

The files are instantly copied to the Web Archive in your online SecureAnywhere account. The Webroot File Manager shows the folders or files under the Web Archive folder. The Status column in the middle panel shows “Backed Up” next to each file that uploaded successfully.

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

If you want to verify that the files were copied into your online account, log in to my.webrootanywhere.com and click **Go to Backups**.

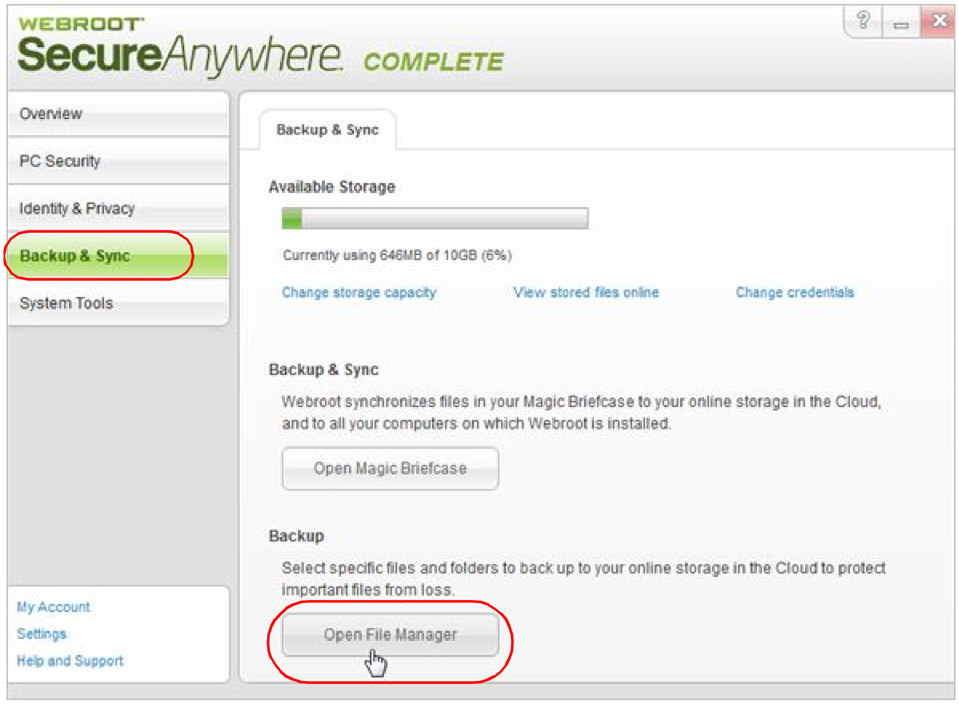
Managing files in the Webroot File Manager

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

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

To open the Webroot File Manager:

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

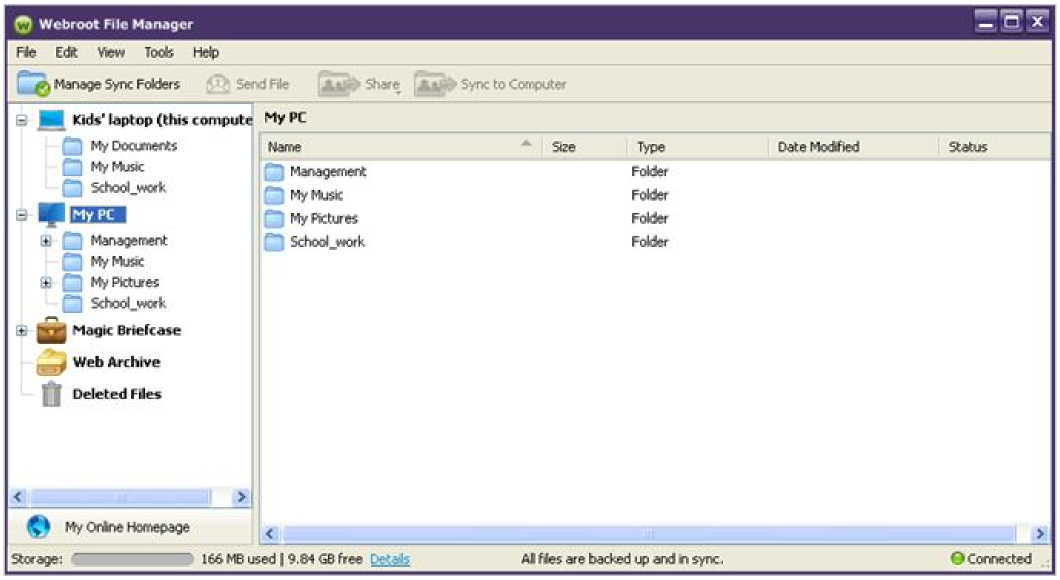


Currently using 646MB of 10GB (6%)

Webroot synchronizes files in your Magic Briefcase to your online storage in the Cloud, and to all your computers on which Webroot is installed.

Select specific files and folders to back up to your online storage in the Cloud to protect important files from loss.

The Webroot File Manager opens. 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.



Name	Size	Type	Date Modified	Status
Management		Folder		
My Music		Folder		
My Pictures		Folder		
School_work		Folder		

Storage: 166 MB used | 9.84 GB free Details All files are backed up and in sync. Connected

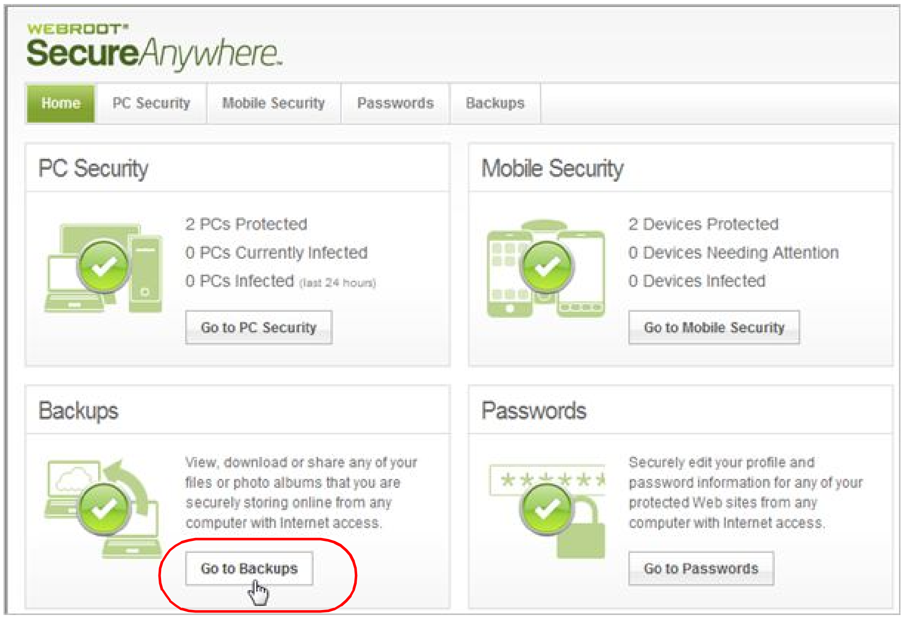
Note: For more information about using the Webroot File Manager, see the *Backups User Guide* at Webroot’s SecureAnywhere Help and Product Guides page.

Managing files in the Backups page

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

To manage files in the Backups page:

1. Log in to my.webrootanywhere.com.
2. Click **Go to Backups**.



PC Security

2 PCs Protected
0 PCs Currently Infected
0 PCs Infected (last 24 hours)

Mobile Security

2 Devices Protected
0 Devices Needing Attention
0 Devices Infected

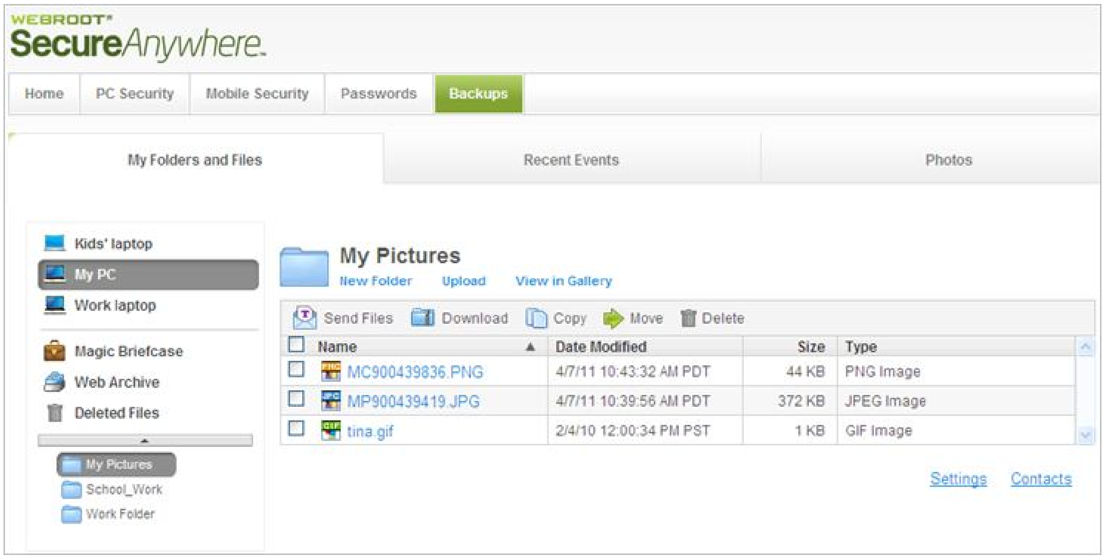
Backups

View, download or share any of your files or photo albums that you are securely storing online from any computer with Internet access.

Passwords

Securely edit your profile and password information for any of your protected Web sites from any computer with Internet access.

The Backups web page opens in your browser.



My Pictures

	Name ▲	Date Modified	Size	Type
□	MC900439836.PNG	4/7/11 10:43:32 AM PDT	44 KB	PNG Image
□	MP900439419.JPG	4/7/11 10:39:56 AM PDT	372 KB	JPEG Image
□	tina.gif	2/4/10 12:00:34 PM PST	1 KB	GIF Image

3. For further instructions on using the Backups web page, see the *Backups User Guide* at Webroot's SecureAnywhere Help and Product Guides page.

9: System Cleaner

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:

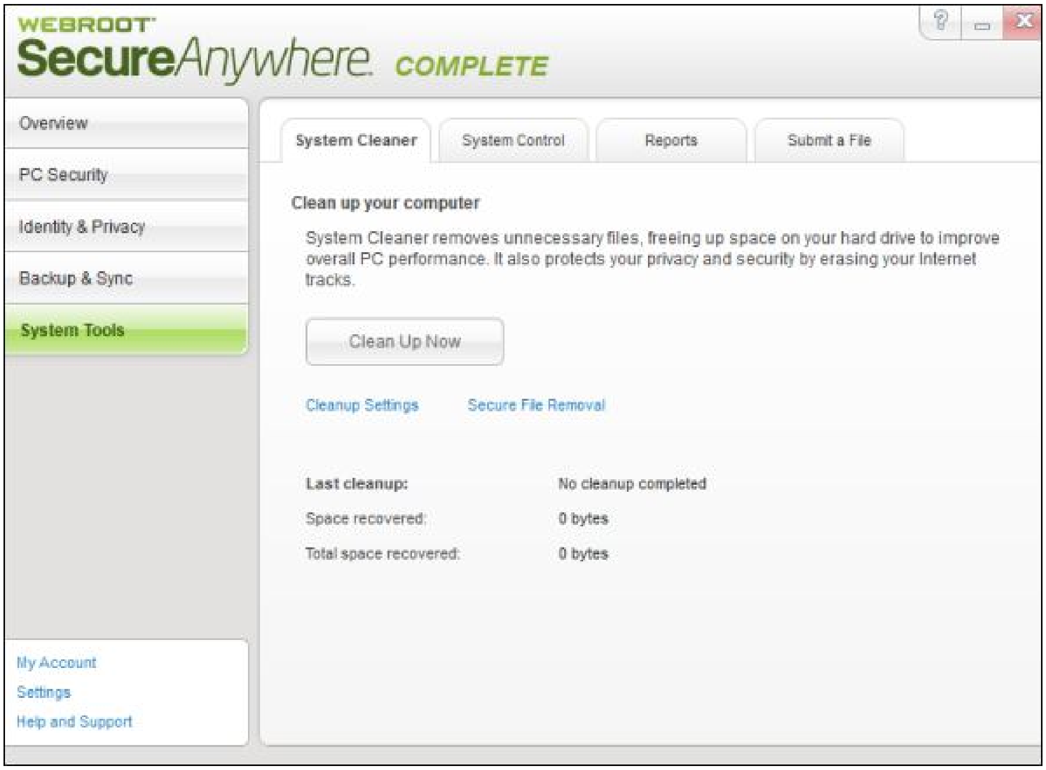
About cleanups

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

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

> **Note**: Cleanups remove unnecessary files and traces, not malware threats. Malware (spyware and viruses) are removed during scans (see “About scans” on page 16). You can think of the System Cleaner as the housekeeper for your computer, while the Scanner serves as the security guard.

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



Clean up your computer

System Cleaner removes unnecessary files, freeing up space on your hard drive to improve overall PC performance. It also protects your privacy and security by erasing your Internet tracks.

Last cleanup:	No cleanup completed
Space recovered:	0 bytes
Total space recovered:	0 bytes

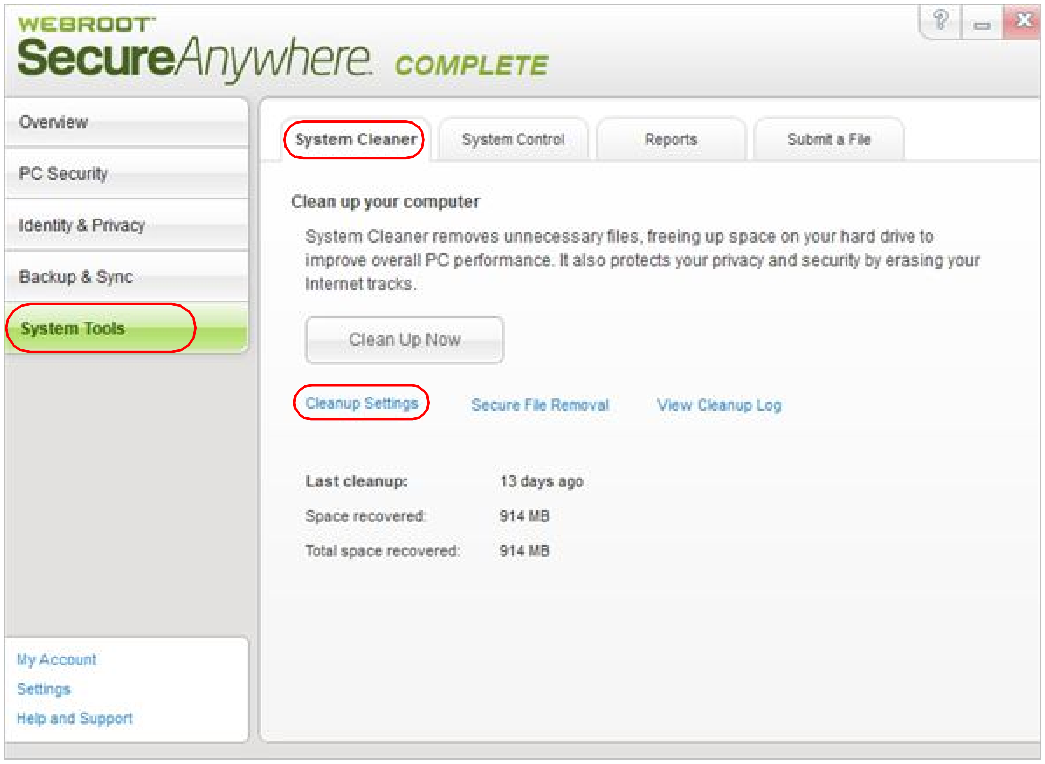
Running a cleanup

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.

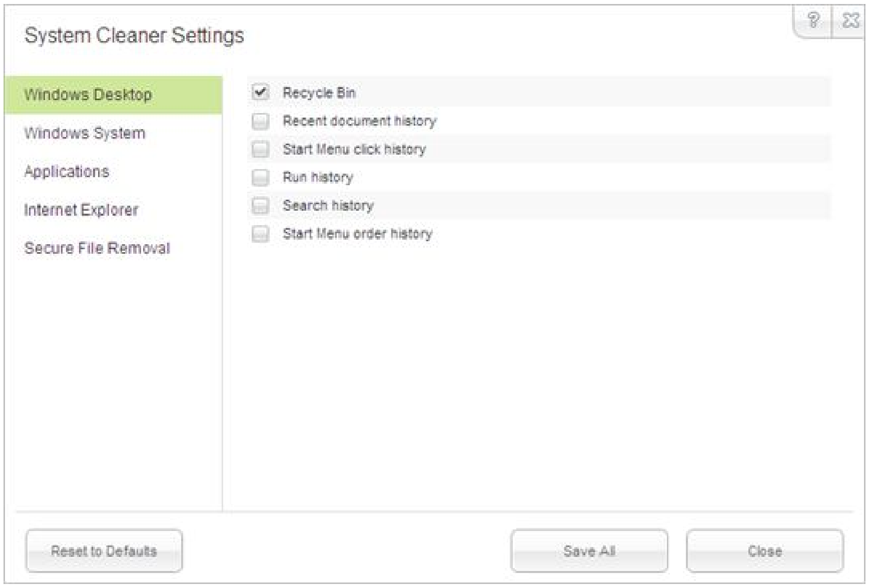


Clean up your computer

System Cleaner removes unnecessary files, freeing up space on your hard drive to improve overall PC performance. It also protects your privacy and security by erasing your Internet tracks.

Last cleanup:	13 days ago
Space recovered:	914 MB
Total space recovered:	914 MB

The System Cleaner Settings panel opens.



System Cleaner Settings

- ☑ Recycle Bin
- □ Recent document history
- □ Start Menu click history
- □ Run history
- □ Search history
- □ Start Menu order history

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 cleaned.

For more information about the settings, see:

- "Changing Windows Desktop settings" on page 89
- "Changing Windows System settings" on page 91
- "Changing Application settings" on page 94
- "Changing Internet Explorer settings" on page 96

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 99 for more information.

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

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

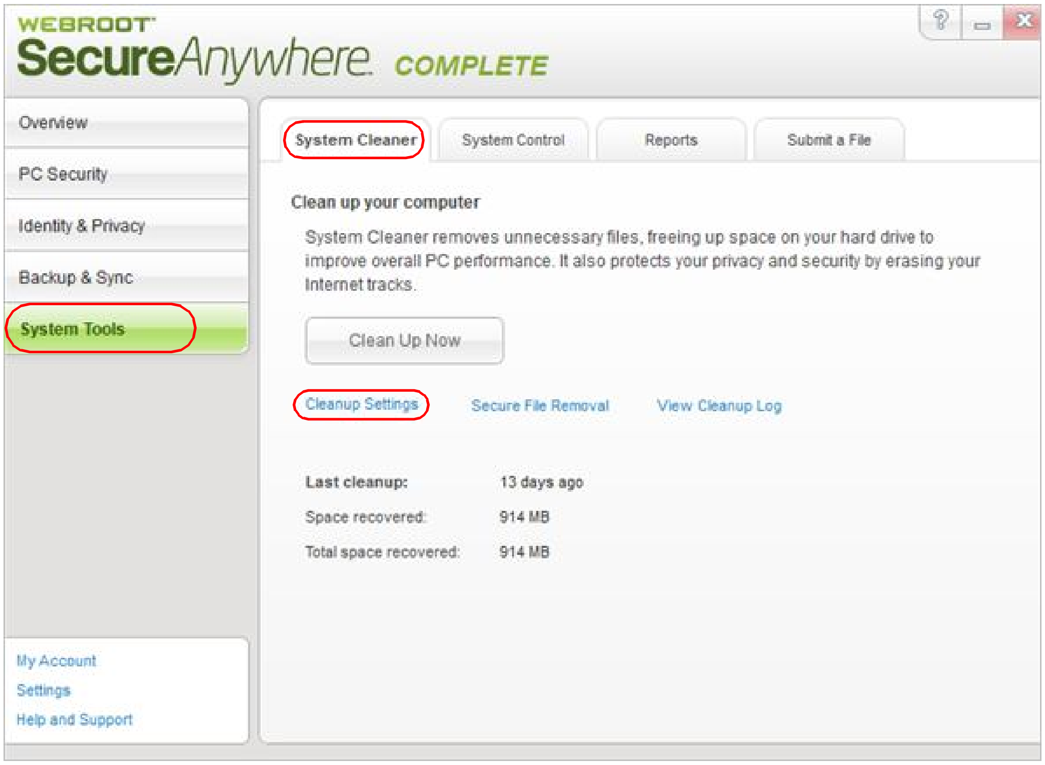
The progress panel shows items as they are removed, along with the space recovered.

Changing Windows Desktop settings

The System Cleaner can remove files in the Recycle Bin and the traces of what files you recently opened or tried to locate in a search. While these history traces can be helpful, they also reveal your activity to other people using your computer. To maintain your privacy, you can remove all these traces.

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.

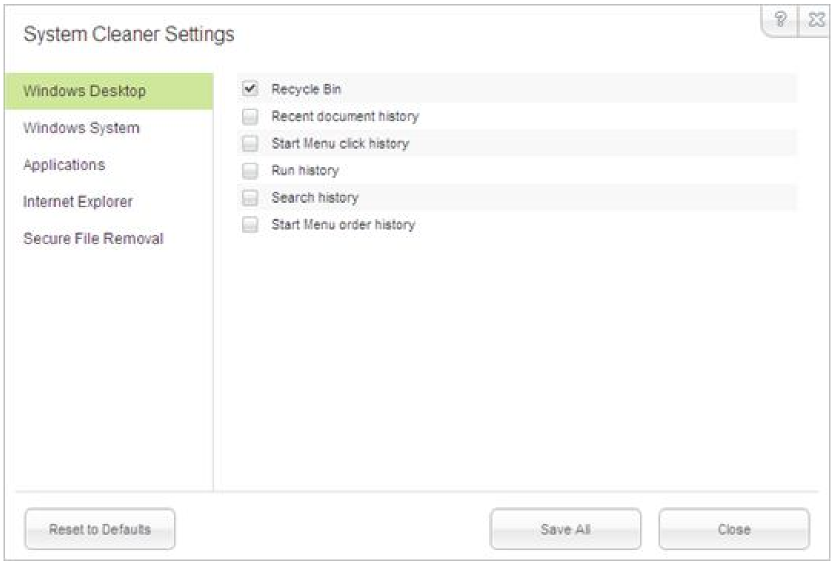


Clean up your computer

System Cleaner removes unnecessary files, freeing up space on your hard drive to improve overall PC performance. It also protects your privacy and security by erasing your Internet tracks.

Last cleanup:	13 days ago
Space recovered:	914 MB
Total space recovered:	914 MB

The System Cleaner Settings panel opens, with Windows Desktop highlighted on the left.



☑ Recycle Bin
□ Recent document history
□ Start Menu click history
□ Run history
□ Search history
□ Start Menu order history

3 On the right side, click in the checkboxes to select or deselect items. Items with a checkmark will be cleaned. When you're done, click the **Save All** button.

The settings are described in the table below.

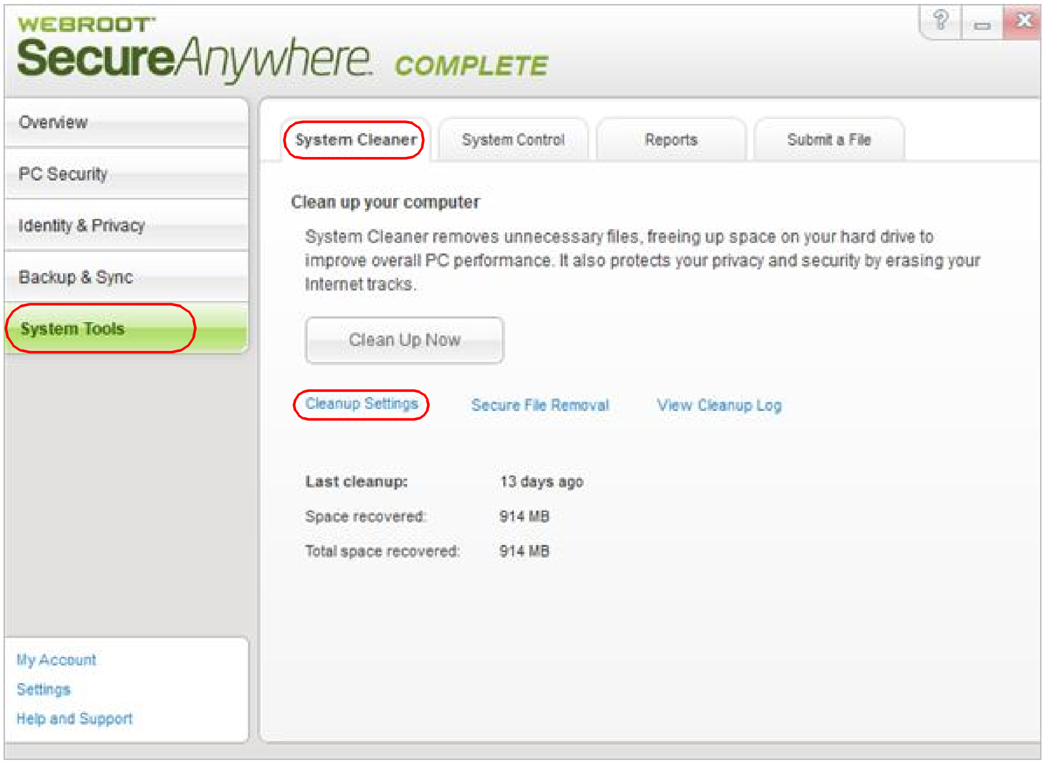
Windows Desktop Cleanup options	
Recycle Bin	Removes all files from your Recycle Bin, which contains files you have deleted using Windows Explorer. When you delete a file, it is stored in the Recycle Bin until you empty it. You should periodically empty the Recycle Bin to preserve valuable disk space on your computer.
Recent document history	Clears the history of recently opened files, which is accessible from the Windows Start menu. (The cleanup does not delete the actual files.)
Start Menu click history	Clears the history of shortcuts to programs that you recently opened using the Start menu.
Run history	Clears the history of commands that you recently entered into the Run dialog, which is accessible from the Start menu. **Note**: After the cleanup, you may need to restart your computer to completely remove items from the Run dialog.
Search history	Clears the history of files or other information that you searched for on your computer. Your computer stores recent searches and displays them when you start entering a new search that starts with the same characters. You access the search (also called "find") from Windows Explorer or from your Start button. (The cleanup does not delete the actual files.)
Start Menu order history	Reverts the list of programs and documents in the Start menu back to alphabetical order, which is the default setting. After you run the cleanup, you must reboot your system for the list to revert back to alphabetical order.

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.

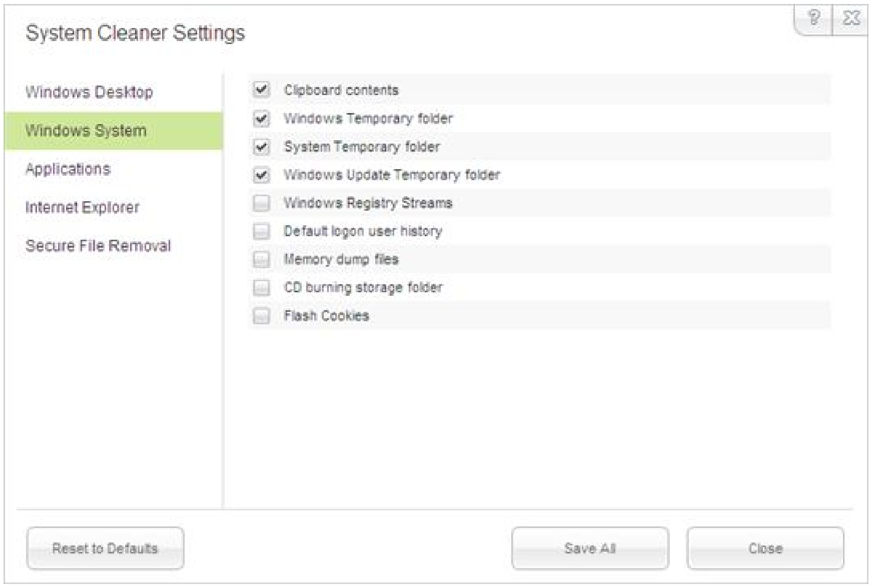


Clean up your computer

System Cleaner removes unnecessary files, freeing up space on your hard drive to improve overall PC performance. It also protects your privacy and security by erasing your Internet tracks.

Last cleanup:	13 days ago
Space recovered:	914 MB
Total space recovered:	914 MB

3 On the left side of the panel, click **Windows System**.



System Cleaner Settings

- ☑ Clipboard contents
- ☑ Windows Temporary folder
- ☑ System Temporary folder
- ☑ Windows Update Temporary folder
- □ Windows Registry Streams
- □ Default logon user history
- □ Memory dump files
- □ CD burning storage folder
- □ Flash Cookies

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

The settings are described in the table below.

Windows System cleanup options	
Clipboard contents	Clears the contents from the Clipboard, where Windows stores data when you use either the Copy or Cut function from any Windows program.
Windows temp folder	Deletes all files and folders in the Windows temporary folder, but not files that are in use by an open program. This folder is usually: C:\Windows\Temp. You should not put any files here that you need to keep. The files in this folder can consume a lot of space on your hard drive.
System temp folder	Deletes all files and folders in the system temporary folder, but not files that are in use by an open program. This folder is usually in C:\Documents and Settings\[username]\Local Settings\Temp. You should not put any files here that you need to keep. The files in this folder can consume a lot of space on your hard drive.
Windows update temp folder	Deletes all files and subfolders in this folder, but not files that are in use by an open program. Windows uses these files when you run Windows Update. After you install the updates, you no longer need these files. These files are normally in C:\Windows\Software\Distribution\Download. You should not put any files here that you need to keep. The files in this folder can consume a lot of space on your hard drive.
Registry streams	Clears the history of recent changes you made to the Windows registry. (This option does not delete the registry changes themselves.)

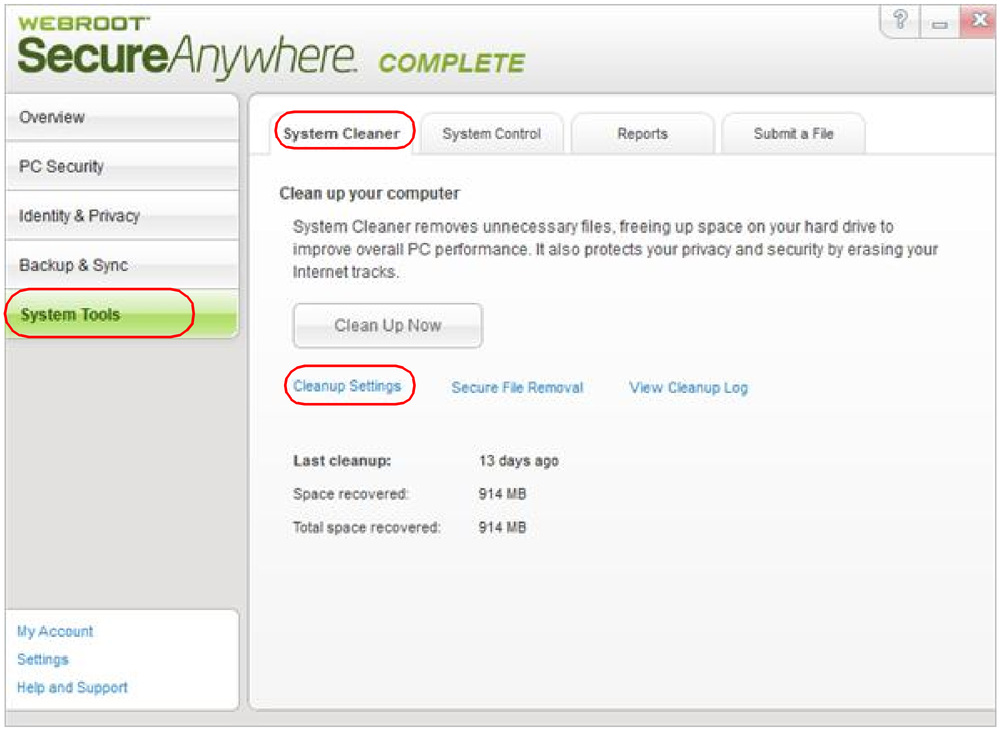
Windows System cleanup options ***(continued)***	
Default logon user history	Deletes the Windows registry entry that stores the last name used to log on to your computer. When the registry entry is deleted, you must enter your user name each time you turn on or restart your computer. This cleanup option does not affect computers that use the default Welcome screen.
Memory dump files	Deletes the memory dump file (memory.dmp) that Windows creates when you receive certain Windows errors. The file contains information about what happened when the error occurred.
CD burning storage folder	Deletes the Windows project files, created when you use the Windows built-in function to copy files to a CD. These project files are typically stored in one of the following directories: C:\Documents and Settings\[username]\Local Settings\Application Data\Microsoft\CDBurning C:\Users\[username]\AppData\Local\Microsoft\Windows\Burn\Burn
Flash Cookies	Deletes bits of data created by Adobe Flash, which can be a privacy concern because they track user preferences. (Flash cookies are not actually “cookies,” and are not controlled through the cookie privacy controls in a browser.)

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 **Cleanup Settings** link.



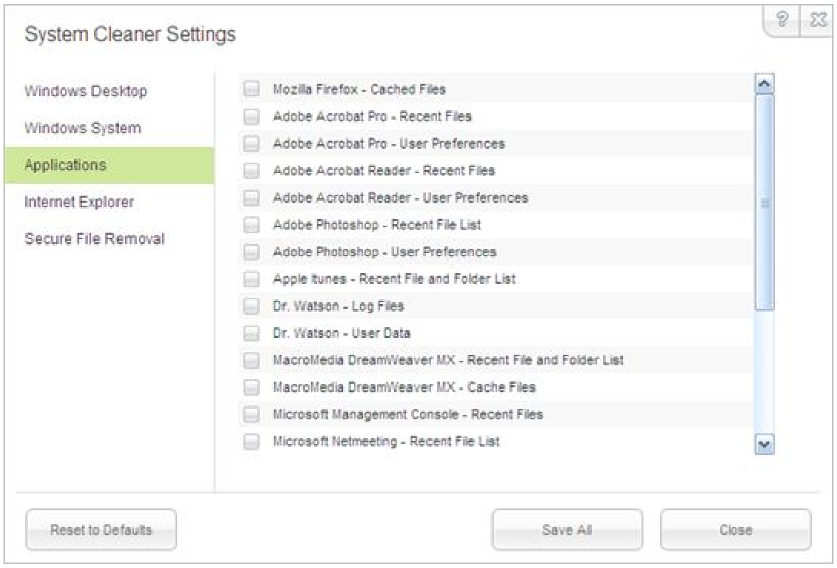
Clean up your computer

System Cleaner removes unnecessary files, freeing up space on your hard drive to improve overall PC performance. It also protects your privacy and security by erasing your Internet tracks.

Last cleanup:	13 days ago
Space recovered:	914 MB
Total space recovered:	914 MB

The System Cleaner Settings panel opens.

3 Click **Applications** on the left. Applications currently installed on your computer will appear in this panel.



☐ Mozilla Firefox - Cached Files
☐ Adobe Acrobat Pro - Recent Files
☐ Adobe Acrobat Pro - User Preferences
☐ Adobe Acrobat Reader - Recent Files
☐ Adobe Acrobat Reader - User Preferences
☐ Adobe Photoshop - Recent File List
☐ Adobe Photoshop - User Preferences
☐ Apple itunes - Recent File and Folder List
☐ Dr. Watson - Log Files
☐ Dr. Watson - User Data
☐ MacroMedia DreamWeaver MX - Recent File and Folder List
☐ MacroMedia DreamWeaver MX - Cache Files
☐ Microsoft Management Console - Recent Files
☐ Microsoft Netmeeting - Recent File List

4 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.

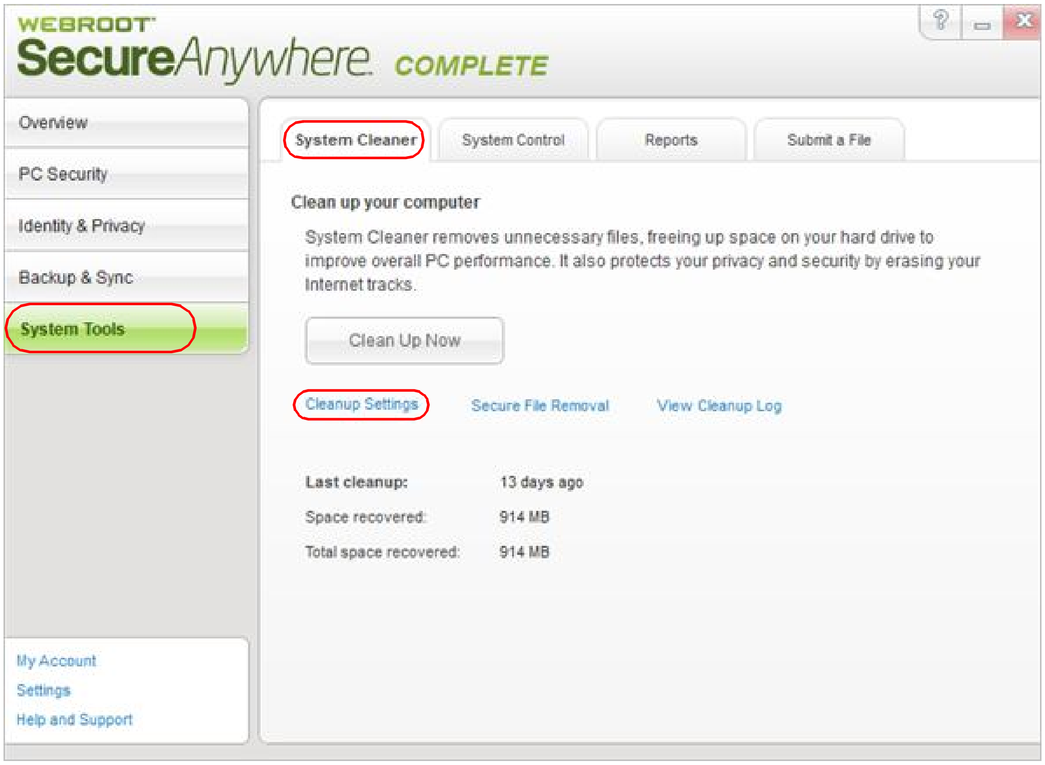
5 When you’re done, click the **Save All** button.

Changing Internet Explorer settings

The System Cleaner can remove temporary files and traces left by the Windows operating system. While these history traces can be helpful, they also reveal your activity to other people and can consume lots of disk space. To maintain your privacy and system performance, you can remove all these files and traces.

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.



Clean up your computer

System Cleaner removes unnecessary files, freeing up space on your hard drive to improve overall PC performance. It also protects your privacy and security by erasing your Internet tracks.

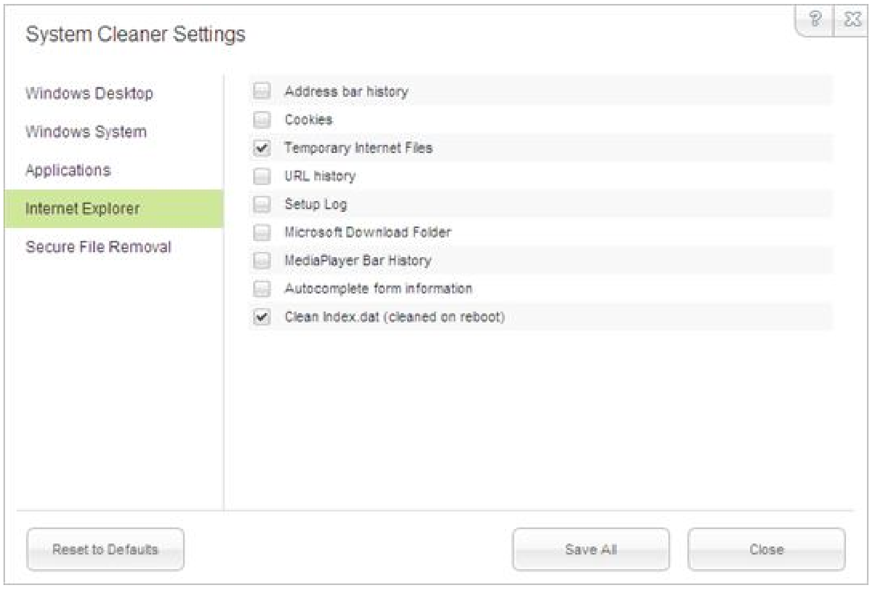
Last cleanup: 13 days ago

Space recovered: 914 MB

Total space recovered: 914 MB

The System Cleaner Settings panel opens.

3 On the left side of the panel, click **Internet Explorer**.



☐ Address bar history
☐ Cookies
☑ Temporary Internet Files
☐ URL history
☐ Setup Log
☐ Microsoft Download Folder
☐ MediaPlayer Bar History
☐ Autocomplete form information
☑ Clean Index.dat (cleaned on reboot)

4 On the right side, click in the checkboxes to select or deselect items. Items with a checkmark will be cleaned. When you're done, click the **Save All** button.

The settings are described in the table below.

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

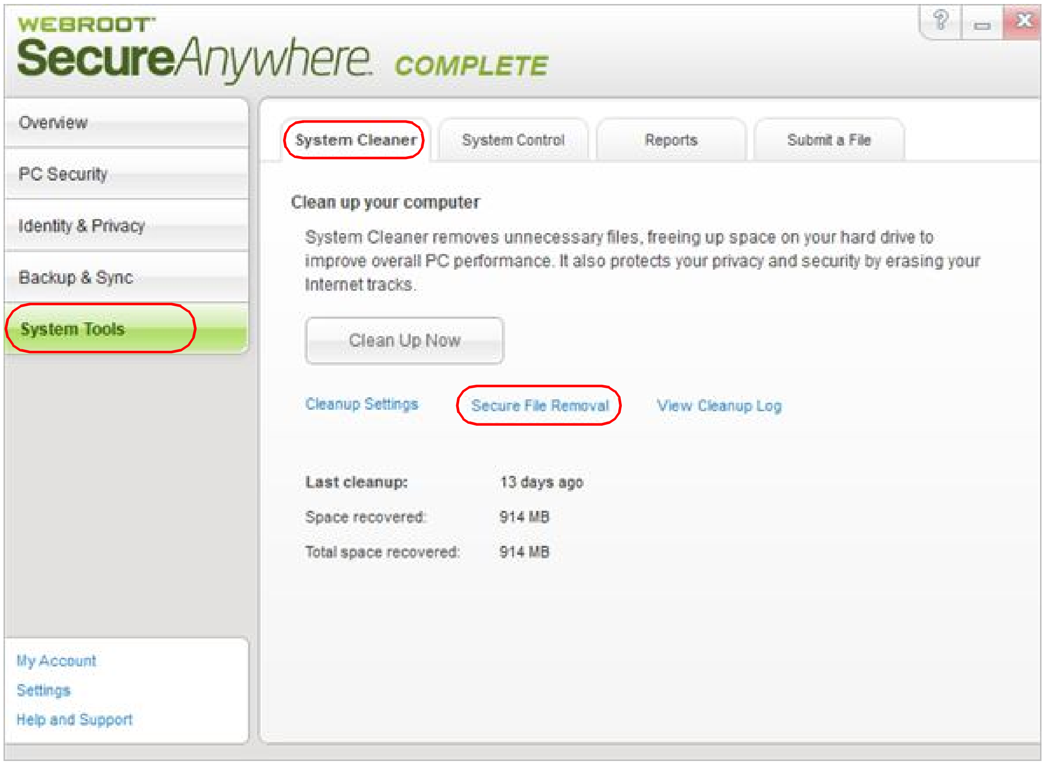
Internet Explorer Cleanup Options ***(continued)***	
MediaPlayer bar history	Removes the list of audio and video files recently opened with the media player in Internet Explorer, which plays audio and video files that you access on websites. (The cleanup does not delete the files, just the Windows "memory" that you opened them or searched for them.)
Autocomplete form data	Deletes data that Internet Explorer stores when you enter information into fields on websites. This is part of Internet Explorer’s AutoComplete feature, which predicts a word or phrase based on the characters you begin to type (for example, your email address or password).
Cleanup index.dat databases on Windows startup	Marks files in the index.dat file for deletion, then clears those files after you reboot the system. The index.dat file is a growing Windows repository of web addresses, search queries, and recently opened files. This option works when you also select one or more of the following options: Cookies, Temporary Internet Files, or URL History. **Note:** Index.dat functions like an active database. It is only cleaned after you reboot Windows.

Using Secure File Removal

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

To use Secure File Removal:

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

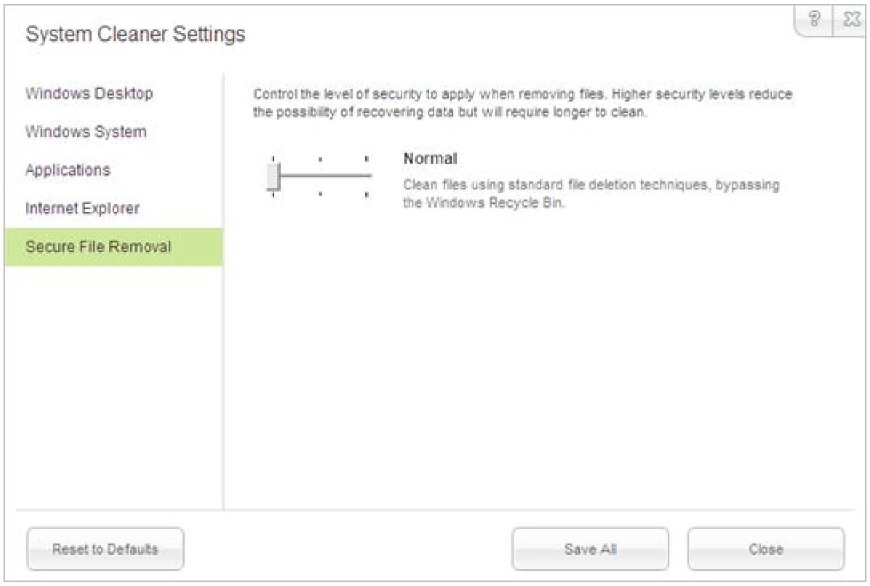


Clean up your computer

System Cleaner removes unnecessary files, freeing up space on your hard drive to improve overall PC performance. It also protects your privacy and security by erasing your Internet tracks.

Last cleanup:	13 days ago
Space recovered:	914 MB
Total space recovered:	914 MB

The Secure File Removal panel opens. 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.



Control the level of security to apply when removing files. Higher security levels reduce the possibility of recovering data but will require longer to clean.

Normal

Clean files using standard file deletion techniques, bypassing the Windows Recycle Bin.

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. Also be aware that cleanup operations take longer when you move the slider to Medium or Maximum.

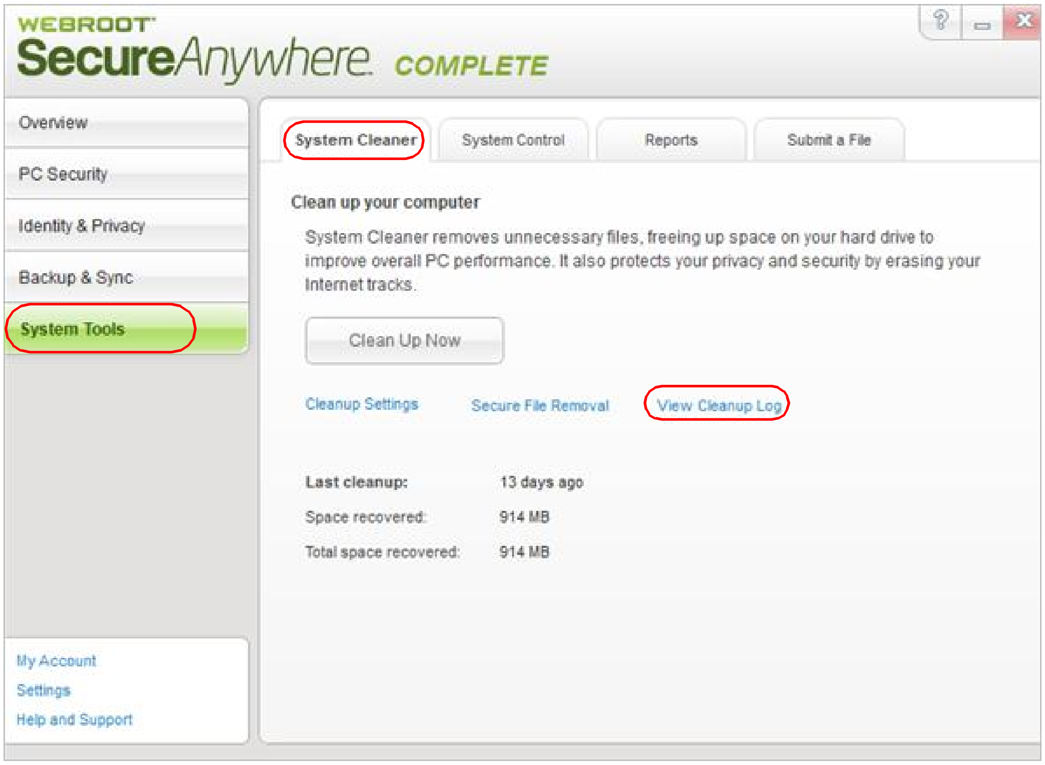
4 Click **Save All**.

Viewing the Cleanup log

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

To view the cleanup log:

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



Clean up your computer

System Cleaner removes unnecessary files, freeing up space on your hard drive to improve overall PC performance. It also protects your privacy and security by erasing your Internet tracks.

Last cleanup:	13 days ago
Space recovered:	914 MB
Total space recovered:	914 MB

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:

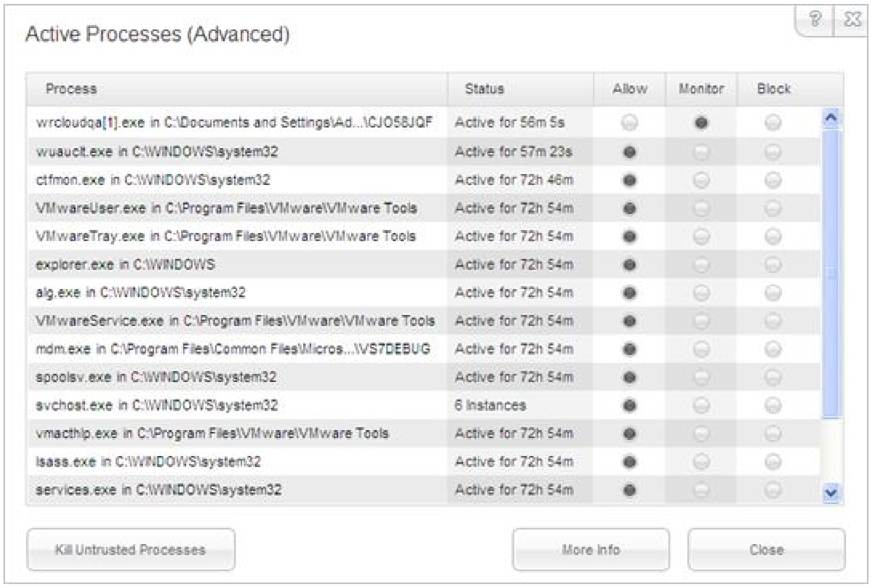
Controlling active processes

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.



Active Processes (Advanced)

Process	Status	Allow	Monitor	Block
wrcloudqa[1].exe in C:\Documents and Settings\Ad...\CJO58JQF	Active for 56m 5s	○	●	○
wuauclt.exe in C:\WINDOWS\system32	Active for 57m 23s	●	○	○
ctfmon.exe in C:\WINDOWS\system32	Active for 72h 46m	●	○	○
VMwareUser.exe in C:\Program Files\VMware\VMware Tools	Active for 72h 54m	●	○	○
VMwareTray.exe in C:\Program Files\VMware\VMware Tools	Active for 72h 54m	●	○	○
explorer.exe in C:\WINDOWS	Active for 72h 54m	●	○	○
alg.exe in C:\WINDOWS\system32	Active for 72h 54m	●	○	○
VMwareService.exe in C:\Program Files\VMware\VMware Tools	Active for 72h 54m	●	○	○
mdm.exe in C:\Program Files\Common Files\Micros...\VS7DEBUG	Active for 72h 54m	●	○	○
spoolsv.exe in C:\WINDOWS\system32	Active for 72h 54m	●	○	○
svchost.exe in C:\WINDOWS\system32	6 Instances	●	○	○
vmacthlp.exe in C:\Program Files\VMware\VMware Tools	Active for 72h 54m	●	○	○
lsass.exe in C:\WINDOWS\system32	Active for 72h 54m	●	○	○
services.exe in C:\WINDOWS\system32	Active for 72h 54m	●	○	○

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

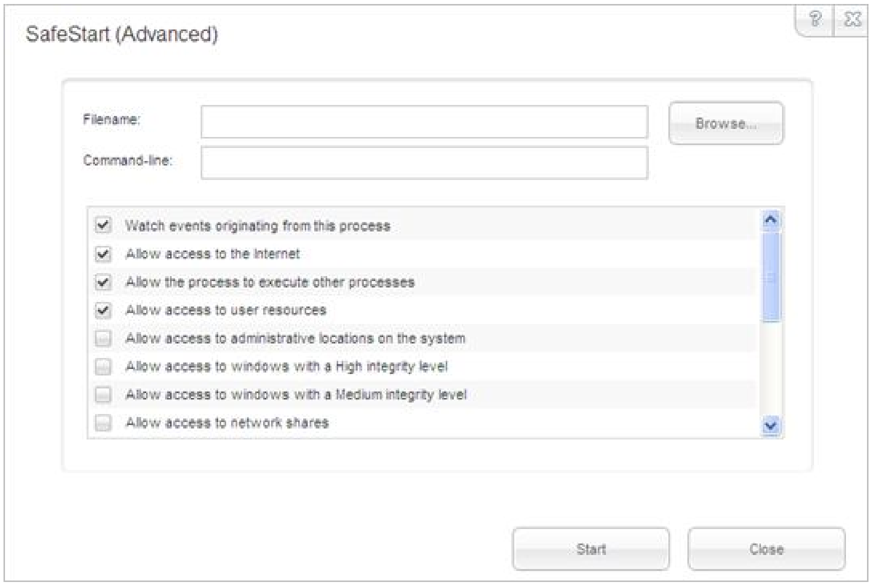
If you are an advanced user and want to test a program you believe is malware, you can first execute the program in a protected area called the SafeStart Sandbox. This sandbox allows you to isolate the actions of the malware program and observe its behavior.

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.



☑ Watch events originating from this process
☑ Allow access to the Internet
☑ Allow the process to execute other processes
☑ Allow access to user resources
☐ Allow access to administrative locations on the system
☐ Allow access to windows with a High integrity level
☐ Allow access to windows with a Medium integrity level
☐ Allow access to network shares

4. You can select the file either by clicking the **Browse** button or by entering the filename and location in the **Command-line** field.
5. If you want to use some advanced features for controlling how the program is allowed to execute, select a checkbox to disable a function (uncheck the box) or activate it (check the box). When you’re done, click the **Start** button.

11: Reports

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.

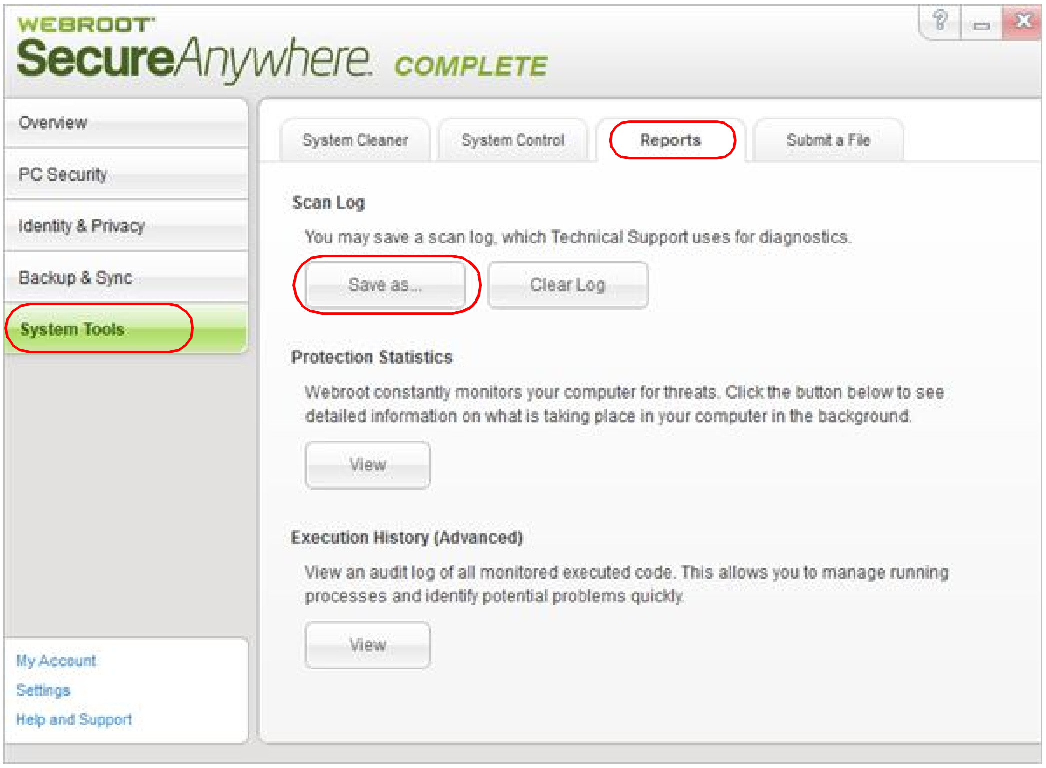
See the following topics:

Saving a scan log

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.



Scan Log

You may save a scan log, which Technical Support uses for diagnostics.

Protection Statistics

Webroot constantly monitors your computer for threats. Click the button below to see detailed information on what is taking place in your computer in the background.

Execution History (Advanced)

View an audit log of all monitored executed code. This allows you to manage running processes and identify potential problems quickly.

4. Enter a filename and click **Save**.

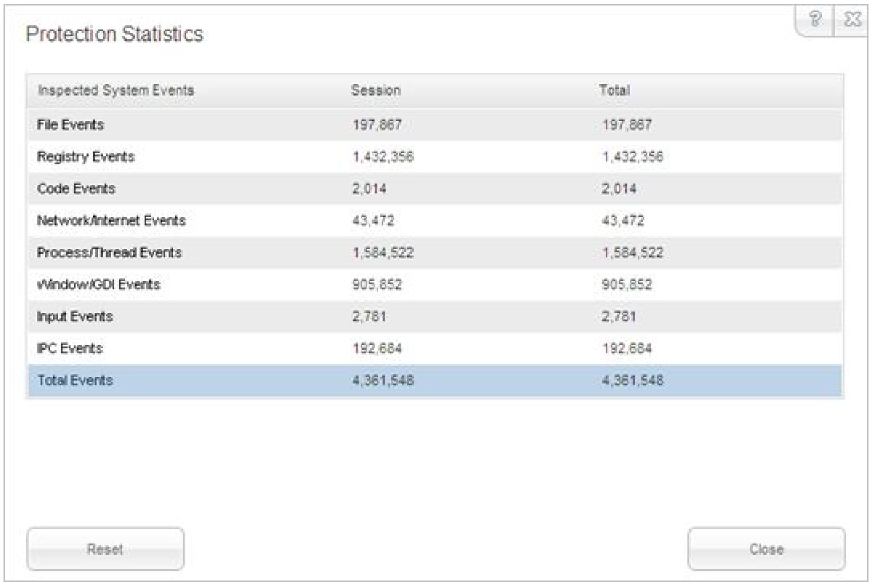
Viewing the protection statistics

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.



Protection Statistics

Inspected System Events	Session	Total
File Events	197,867	197,867
Registry Events	1,432,356	1,432,356
Code Events	2,014	2,014
Network/Internet Events	43,472	43,472
Process/Thread Events	1,584,522	1,584,522
Window/GDI Events	905,852	905,852
Input Events	2,781	2,781
IPC Events	192,684	192,684
Total Events	4,361,548	4,361,548

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

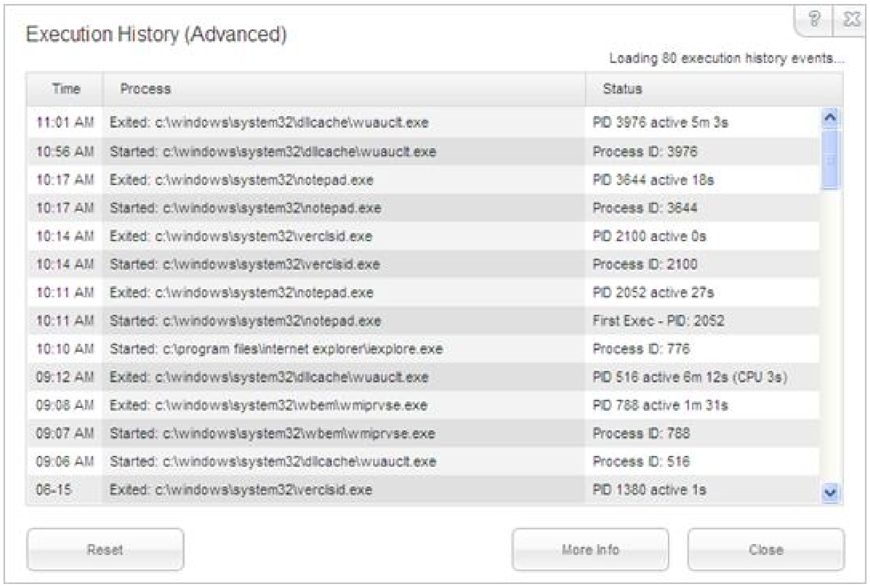
Viewing the execution history

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.



Execution History (Advanced)

Loading 80 execution history events...

Time	Process	Status
11:01 AM	Exited: c:\windows\system32\dllcache\wuauclt.exe	PID 3976 active 5m 3s
10:56 AM	Started: c:\windows\system32\dllcache\wuauclt.exe	Process ID: 3976
10:17 AM	Exited: c:\windows\system32\notepad.exe	PID 3644 active 18s
10:17 AM	Started: c:\windows\system32\notepad.exe	Process ID: 3644
10:14 AM	Exited: c:\windows\system32\verclsid.exe	PID 2100 active 0s
10:14 AM	Started: c:\windows\system32\verclsid.exe	Process ID: 2100
10:11 AM	Exited: c:\windows\system32\notepad.exe	PID 2052 active 27s
10:11 AM	Started: c:\windows\system32\notepad.exe	First Exec - PID: 2052
10:10 AM	Started: c:\program files\internet explorer\iexplore.exe	Process ID: 776
09:12 AM	Exited: c:\windows\system32\dllcache\wuauclt.exe	PID 516 active 6m 12s (CPU 3s)
09:08 AM	Exited: c:\windows\system32\wbem\wmiprvse.exe	PID 788 active 1m 31s
09:07 AM	Started: c:\windows\system32\wbem\wmiprvse.exe	Process ID: 788
09:06 AM	Started: c:\windows\system32\dllcache\wuauclt.exe	Process ID: 516
06-15	Exited: c:\windows\system32\verclsid.exe	PID 1380 active 1s

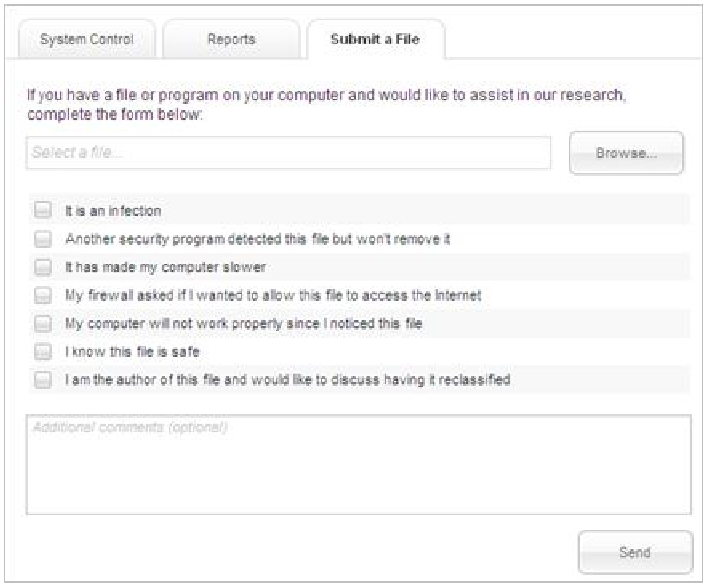
4. Click on a process to view more detailed information, then click the **More Info** button.

Submitting a file

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

To submit a file:

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



If you have a file or program on your computer and would like to assist in our research, complete the form below:

- □ It is an infection
- □ Another security program detected this file but won't remove it
- □ It has made my computer slower
- □ My firewall asked if I wanted to allow this file to access the Internet
- □ My computer will not work properly since I noticed this file
- □ I know this file is safe
- □ I am the author of this file and would like to discuss having it reclassified

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**.

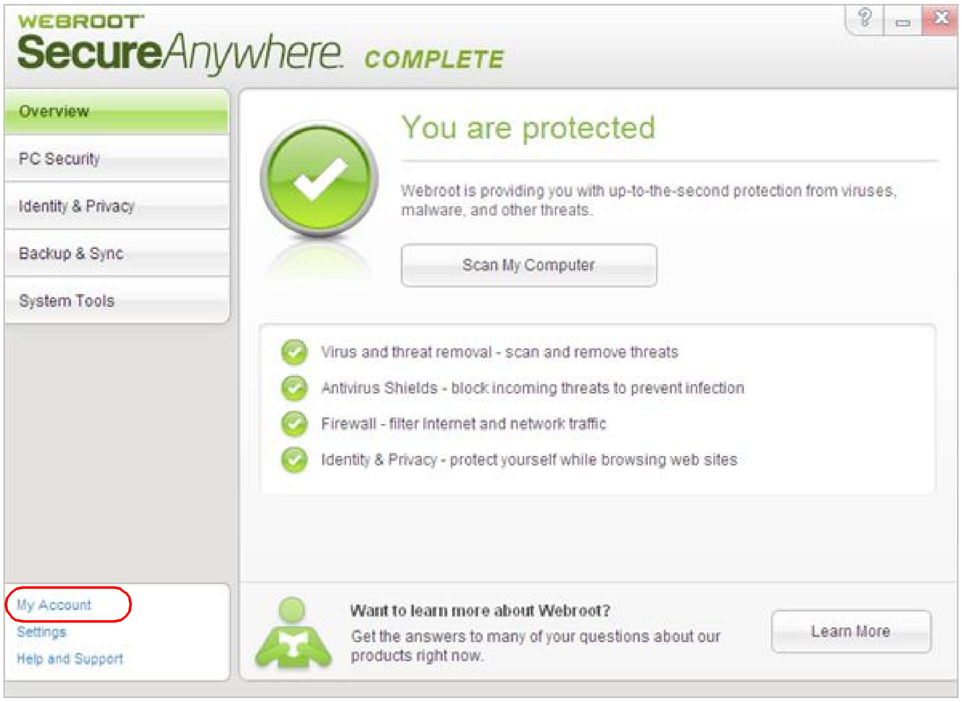
12: My Account

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

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.



You are protected

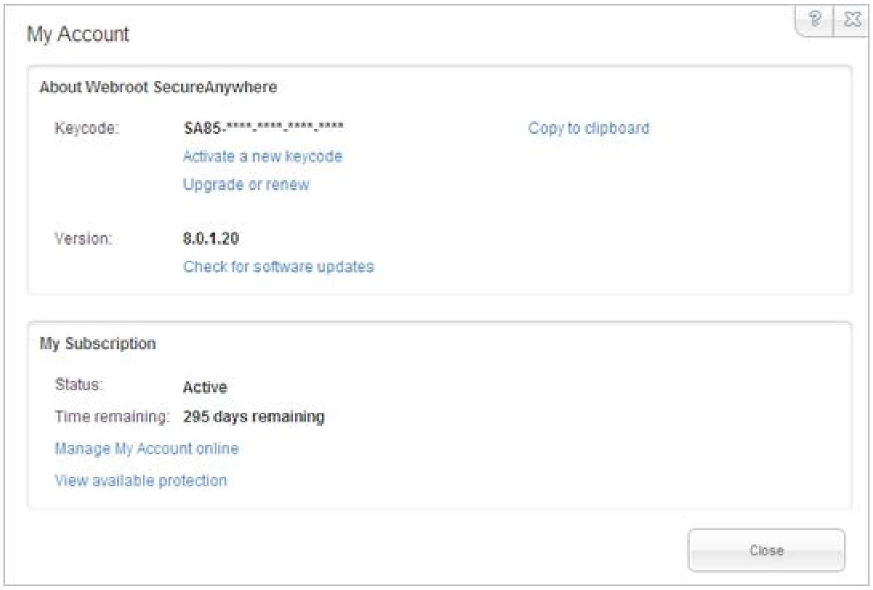
Webroot is providing you with up-to-the-second protection from viruses, malware, and other threats.

- ✓ Virus and threat removal - scan and remove threats
- ✓ Antivirus Shields - block incoming threats to prevent infection
- ✓ Firewall - filter Internet and network traffic
- ✓ Identity & Privacy - protect yourself while browsing web sites

Want to learn more about Webroot?

Get the answers to many of your questions about our products right now.

Your account information appears in the My Account panel.



My Account

About Webroot SecureAnywhere

Keycode: SA85-****-****-****-****

Version: 8.0.1.20

My Subscription

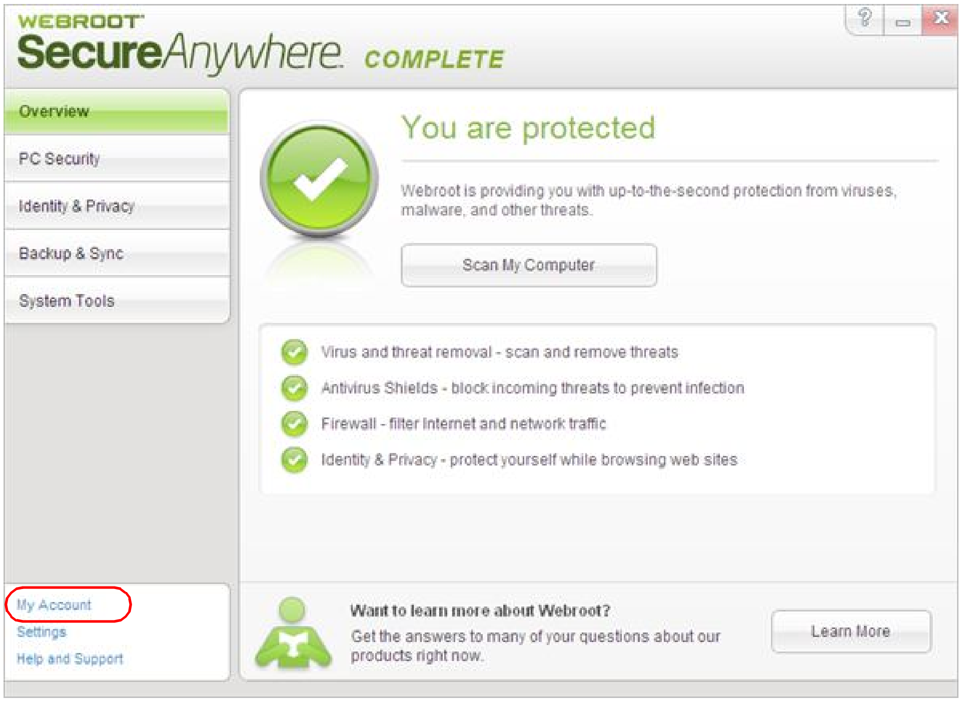
Status: Active

Time remaining: 295 days remaining

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**.



You are protected

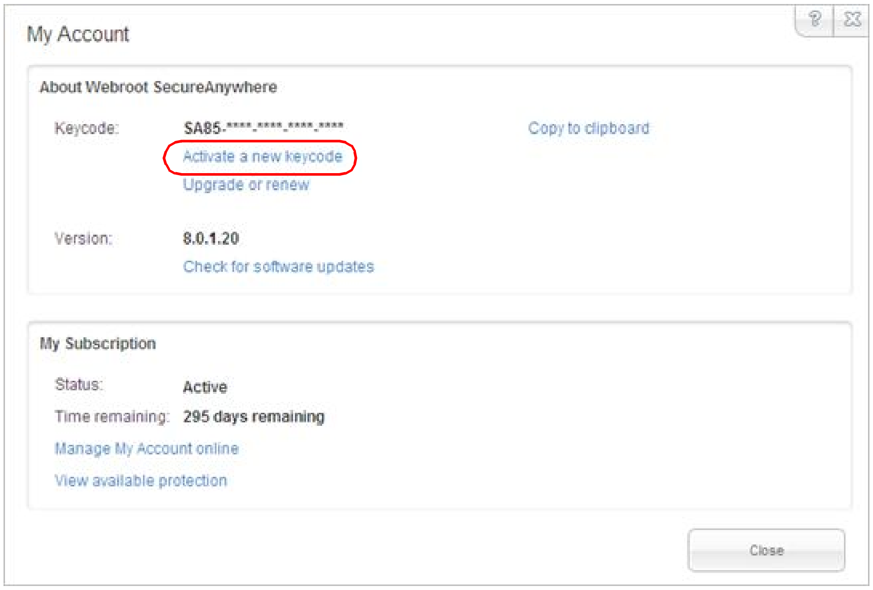
Webroot is providing you with up-to-the-second protection from viruses, malware, and other threats.

- Virus and threat removal - scan and remove threats
- Antivirus Shields - block incoming threats to prevent infection
- Firewall - filter Internet and network traffic
- Identity & Privacy - protect yourself while browsing web sites

Want to learn more about Webroot?

Get the answers to many of your questions about our products right now.

3. In the Account panel, click **Activate a new keycode**.



My Account

About Webroot SecureAnywhere

Keycode: SA85-****-****-****-****

Version: 8.0.1.20

My Subscription

Status: Active

Time remaining: 295 days remaining

4. In the dialog, enter the keycode and click the **Activate** button.

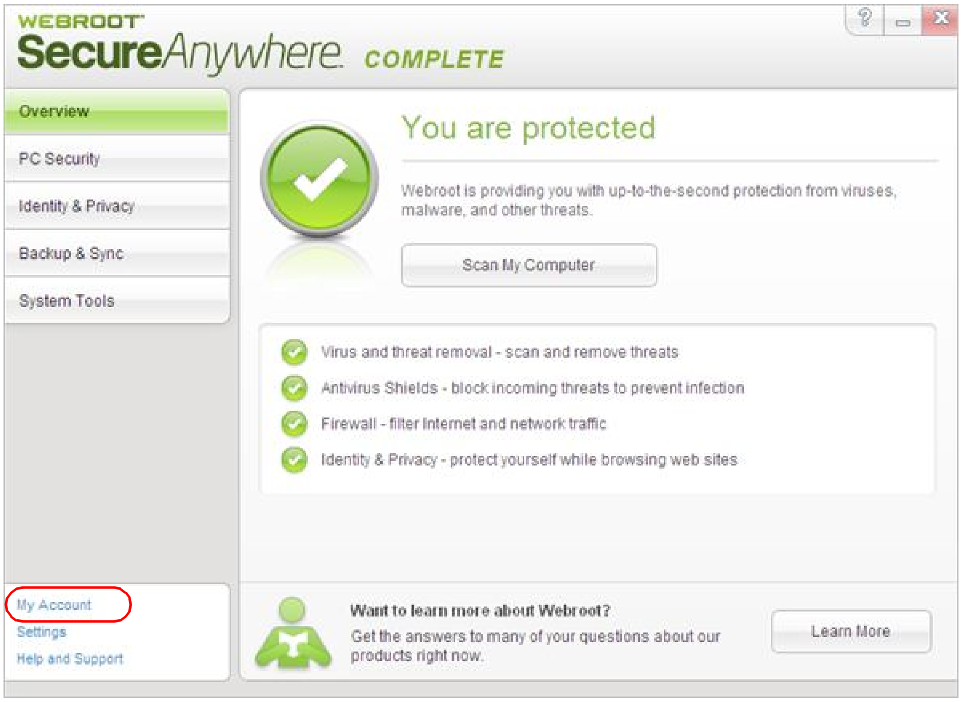
Upgrading or renewing the software

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**.



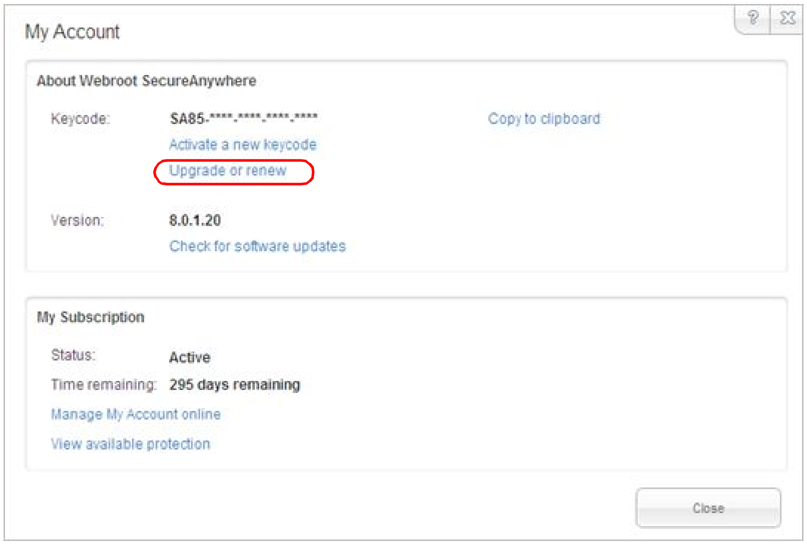
You are protected

Webroot is providing you with up-to-the-second protection from viruses, malware, and other threats.

Virus and threat removal - scan and remove threats
Antivirus Shields - block incoming threats to prevent infection
Firewall - filter Internet and network traffic
Identity & Privacy - protect yourself while browsing web sites

Want to learn more about Webroot?
Get the answers to many of your questions about our products right now.

3 In the Account panel, click **Upgrade or renew**.



My Account

About Webroot SecureAnywhere

Keycode: SA85-****-****-****-****

Version: 8.0.1.20

My Subscription

Status: Active

Time remaining: 295 days remaining

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

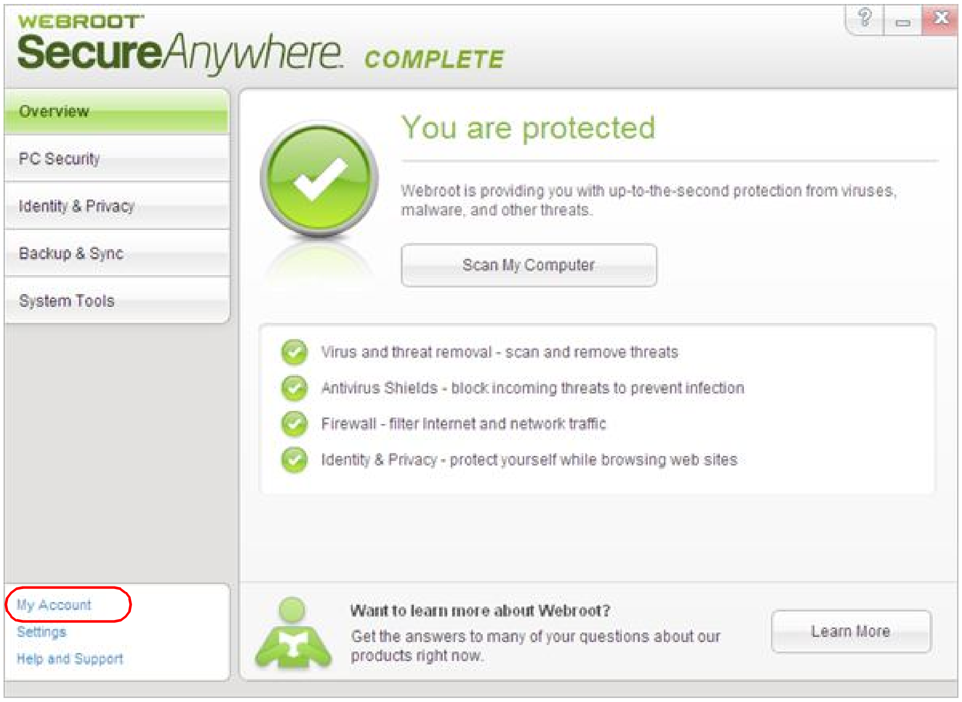
Checking for software updates

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**.



You are protected

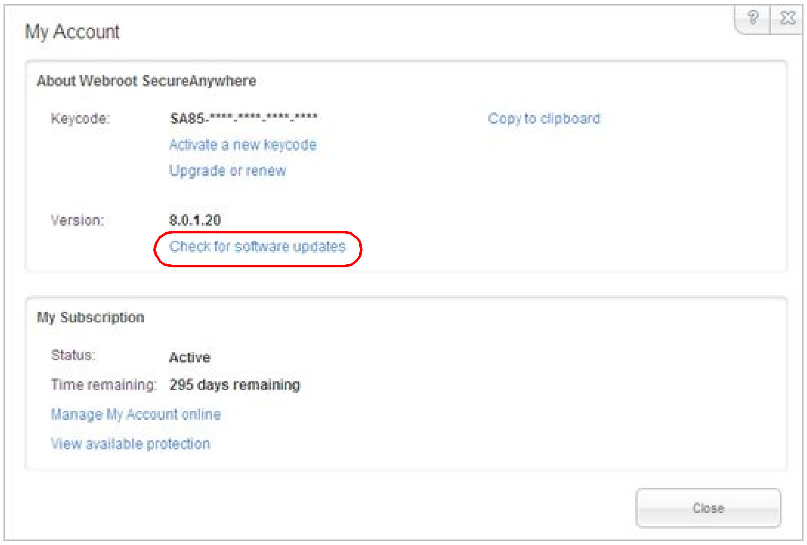
Webroot is providing you with up-to-the-second protection from viruses, malware, and other threats.

- Virus and threat removal - scan and remove threats
- Antivirus Shields - block incoming threats to prevent infection
- Firewall - filter Internet and network traffic
- Identity & Privacy - protect yourself while browsing web sites

Want to learn more about Webroot?

Get the answers to many of your questions about our products right now.

3 In the Account panel, click **Check for software updates**.



About Webroot SecureAnywhere

Keycode: SA85-****-****-****-****

Version: 8.0.1.20

My Subscription

Status: Active

Time remaining: 295 days remaining

If a newer version exists, Webroot downloads the updates to your system.

13: Settings

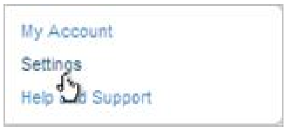
To manage program settings, see the following topics:

Setting basic configuration

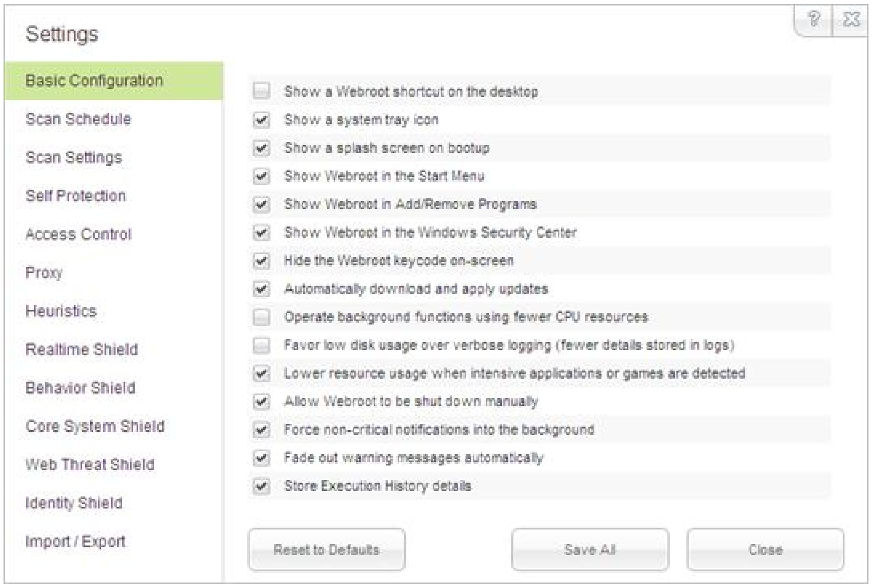
You can change the behavior of the program in the Basic Configuration settings.

To change Basic Configuration settings:

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



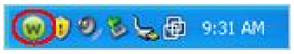
The Settings dialog opens to Basic Configuration.



☐ Show a Webroot shortcut on the desktop
☑ Show a system tray icon
☑ Show a splash screen on bootup
☑ Show Webroot in the Start Menu
☑ Show Webroot in Add/Remove Programs
☑ Show Webroot in the Windows Security Center
☑ Hide the Webroot keycode on-screen
☑ Automatically download and apply updates
☐ Operate background functions using fewer CPU resources
☐ Favor low disk usage over verbose logging (fewer details stored in logs)
☑ Lower resource usage when intensive applications or games are detected
☑ Allow Webroot to be shut down manually
☑ Force non-critical notifications into the background
☑ Fade out warning messages automatically
☑ Store Execution History details

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

The settings are described in the table below.

Basic Configuration settings	
Show a Webroot shortcut on the desktop	Provides quick, double-click access to the main interface by placing the shortcut icon on your desktop.
Show a system tray icon	Provides quick access to Webroot SecureAnywhere functions by placing the Webroot icon on your desktop:  You can double-click the icon to open the main interface or right-click to open a menu of common functions, like scanning.
Show a splash screen on bootup	Opens the Webroot splash screen on system startup, which lets you know that the program is running and protecting your computer.

Basic Configuration settings ***(continued)***	
Show Webroot in the Start Menu	Lists Webroot SecureAnywhere in the Windows Startup menu items.
Show Webroot in Add/Remove Programs	Lists Webroot SecureAnywhere in the Windows Add/Remove Programs panel.
Show Webroot in Windows Security Center	Lists Webroot SecureAnywhere in the Windows Security Center, under Virus Protection information.
Hide the Webroot license keycode on-screen	Blocks your license keycode from displaying on the My Account panel.
Automatically download and apply updates	Downloads product updates automatically without alerting you.
Operate background functions using fewer CPU resources	Saves CPU resources by running non-scan related functions in the background.
Favor low disk usage over verbose logging (fewer details stored in logs)	Saves disk resources by saving only the last four log items.
Lower resource usage when intensive applications or games are detected	Suppresses Webroot SecureAnywhere functions while you are gaming, watching videos, or using other intensive applications.
Allow Webroot to be shut down manually	Displays a Shutdown command in the system tray menu. If you deselect this option, the Shutdown command is removed from the menu.
Force non-critical notifications into the background	Suppresses information-only messages from appearing in the system tray.
Fade out warning messages automatically	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.
Store Execution History details	Stores data for the Execution History logs, available under Reports.

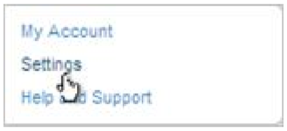
Setting self protection

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.

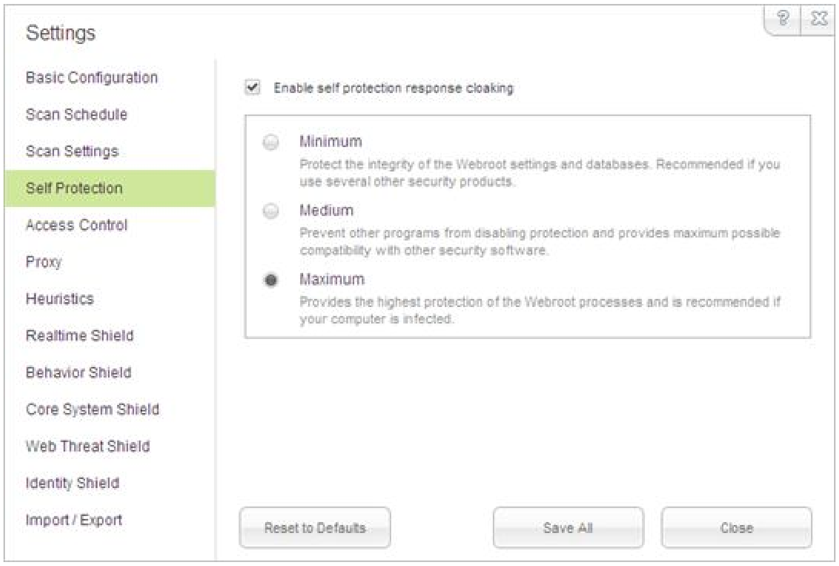
We recommend that you keep Self Protection at the Maximum setting. However, if you use other security software along with Webroot SecureAnywhere, you should adjust Self Protection to the Medium or Minimum setting. The Maximum setting may interfere with other security software.

To change Self Protection settings:

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



3. In the Settings panel, click **Self Protection**.



☑ Enable self protection response cloaking

○ Minimum
Protect the integrity of the Webroot settings and databases. Recommended if you use several other security products.

○ Medium
Prevent other programs from disabling protection and provides maximum possible compatibility with other security software.

● Maximum
Provides the highest protection of the Webroot processes and is recommended if your computer is infected.

4. 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.

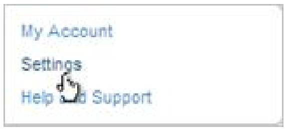
5. Click **Save All**.

Setting access control

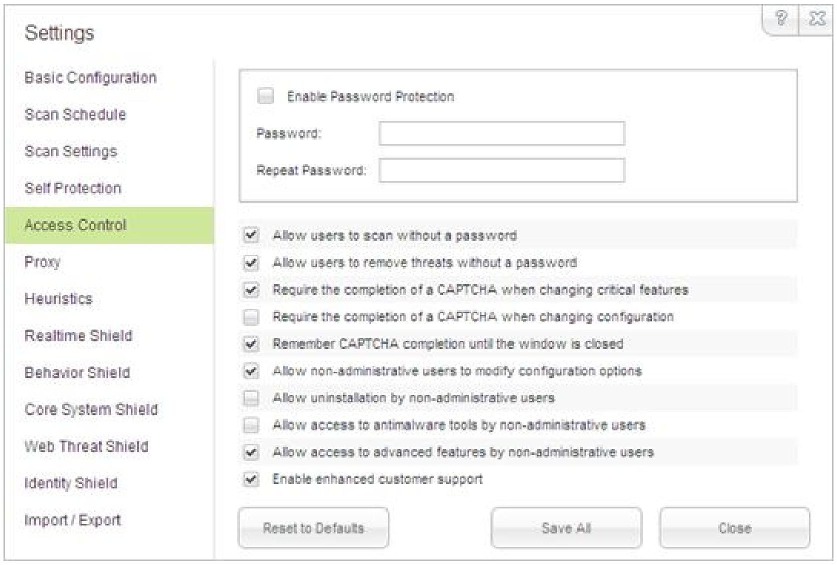
If multiple people use your computer, you can set some permissions that provide or deny access to certain functions. These access controls also protect your computer from malware that tries to change settings in the Webroot SecureAnywhere software.

To change Access Control settings:

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



3. In the Settings panel, click **Access Control**.



□ Enable Password Protection

Password:

Repeat Password:

☑ Allow users to scan without a password

☑ Allow users to remove threats without a password

☑ Require the completion of a CAPTCHA when changing critical features

□ Require the completion of a CAPTCHA when changing configuration

☑ Remember CAPTCHA completion until the window is closed

☑ Allow non-administrative users to modify configuration options

□ Allow uninstallation by non-administrative users

□ Allow access to antimalware tools by non-administrative users

☑ Allow access to advanced features by non-administrative users

☑ Enable enhanced customer support

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

   Settings are described in the table below.

Access Control settings	
Enable Password Protection	Requires that users enter a password for any configuration changes or critical actions.
Allow users to scan without a password	Allows any user to scan the system, even if password protection is enabled.
Allow users to remove threats without a password	Allows any user to remove threats, even if password protection is enabled.

Access Control settings ***(continued)***	
Require the completion of a CAPTCHA when changing critical features	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.
Require the completion of a CAPTCHA when changing configuration	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.
Remember CAPTCHA completion until the window is closed	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.
Allow non-administrative users to modify configuration options	Enables you to modify configuration options, whether you are logged in as an administrative user or not.
Allow uninstallation by non-administrative users	Enables you to uninstall the program, whether you are logged in as an administrative user or not.
Allow access to antimalware tools by non-administrative users	Enables you to access the Antimalware Tools (under Quarantine), whether you are logged in as an administrative user or not.
Allow access to advanced features by non-administrative users	Enables you to access the advanced features, whether you are logged in as an administrative user or not. Advanced features include all options in the Settings panels and the Antimalware tools under Quarantine.
Enable enhanced customer support	Provides configuration and debug data to Webroot Support when you initiate a support request. This feature allows Support to quickly diagnose and repair the issue.

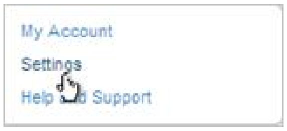
Defining proxy settings

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.

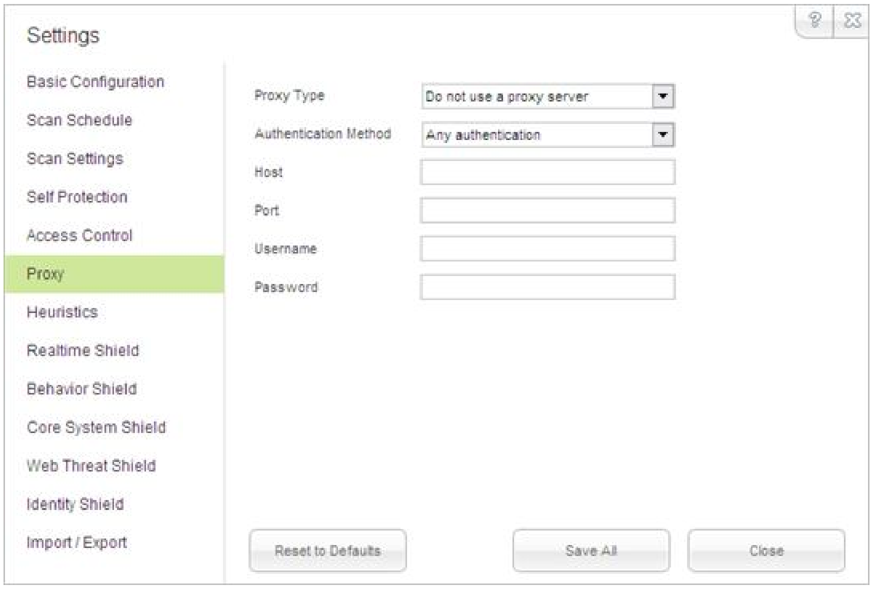
To define proxy settings:

1 Open the main interface (see "Using the main interface" on page 5).

2 At the bottom left, click **Settings**.



3 From the Settings panel, click **Proxy**.



Proxy Type: Do not use a proxy server
Authentication Method: Any authentication
Host
Port
Username
Password

4 Enter the proxy settings as described below, then click the **Save All** button.

Proxy settings	
Proxy Type	Select HTTP Proxy from the drop-down box.
Authentication Method	Select an authentication method from the drop-down box, either Basic, Digest, Negotiate, or NTLM.
Host	Enter the fully qualified domain name of the server (for example, proxy.company.com).
Port	Enter the port number the server uses.
Username	Enter the username for the server, if used.
Password	Enter the password for the server, if used.

Setting heuristics

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

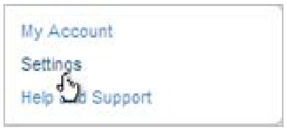
> **Note**: If you want to adjust Heuristics settings for all the computers managed in your SecureAnywhere account, go to the PC Security web page (see "Viewing the PC security status online" on page 11).

Webroot SecureAnywhere includes three types of heuristics:

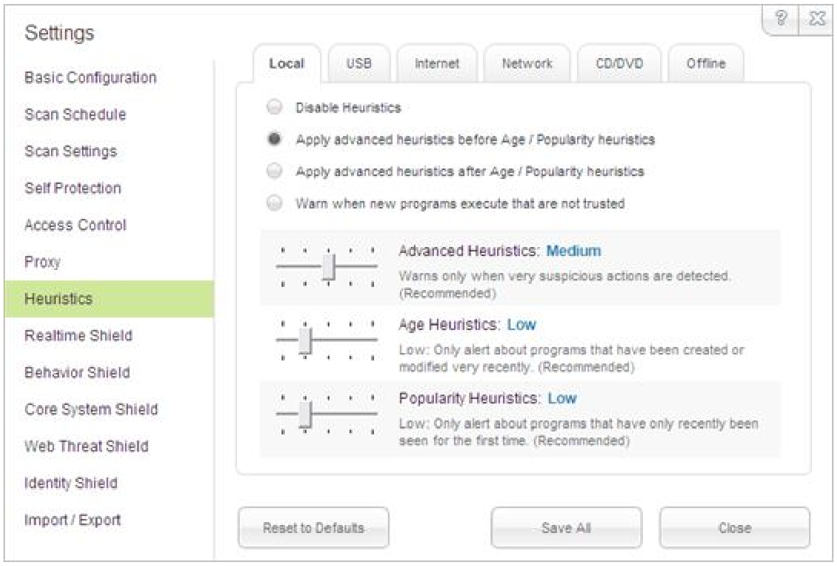
- **Advanced Heuristics**. Analyzes new programs for suspicious actions that are typical of malware.
- **Age Heuristics**. Analyzes new programs based on the amount of time the program has been in the community. Legitimate programs are generally used in a community for a long time, but malware often has a short lifespan.
- **Popularity Heuristics**. Analyzes new programs based on statistics for how often the program is used in the community and how often it changes. Legitimate programs do not change quickly, but malware often mutates at a rapid pace. Malware may install as a unique copy on every computer, making it statistically "unpopular."

To change Heuristics settings:

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



In the Settings panel, click **Heuristics**.



○ Disable Heuristics

● Apply advanced heuristics before Age / Popularity heuristics

○ Apply advanced heuristics after Age / Popularity heuristics

○ Warn when new programs execute that are not trusted

Advanced Heuristics: Medium
Warns only when very suspicious actions are detected. (Recommended)

Age Heuristics: Low
Low: Only alert about programs that have been created or modified very recently. (Recommended)

Popularity Heuristics: Low
Low: Only alert about programs that have only recently been seen for the first time. (Recommended)

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

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

Radio buttons - additional heuristic options	
Disable Heuristics	Turns off heuristic analysis. Not recommended.
Apply advanced heuristics before Age/Popularity heuristics	Warns against new programs as well as old programs that exhibit suspicious behavior.
Apply advanced heuristics after Age/Popularity heuristics	Warns against suspicious programs detected with Advanced Heuristics, based on Age/Popularity settings.
Warn when new programs execute that are not trusted	Warns when malicious, suspicious, or unknown programs try to execute. (This setting may result in false detections.)

Slider - Advanced Heuristics	
Disabled	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.)
Low	Detects programs with a high level of malicious activity. This setting ignores some suspicious behavior and allows most programs to run.
Medium	Balances detection versus false alarms by using our tuned heuristics in the centralized community database.
High	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.)

Slider - Advanced Heuristics ***(continued)***	
Maximum	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.)

Slider - Age Heuristics	
Disabled	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.)
Low	Detects programs that have been created or modified very recently.
Medium	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.
High	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.
Maximum	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.

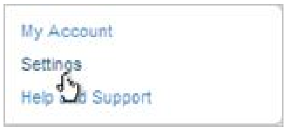
Slider - Popularity Heuristics	
Disabled	Turns off Popularity Heuristics for the area selected in the tab, leaving it vulnerable to new threats. (However, it will still be protected against known threats.)
Low	Detects programs that have been seen for the first time. This setting is recommended if you frequently install new programs, beta programs, or you are a software developer who frequently creates new programs.
Medium	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.
High	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.
Maximum	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.

Importing or exporting settings

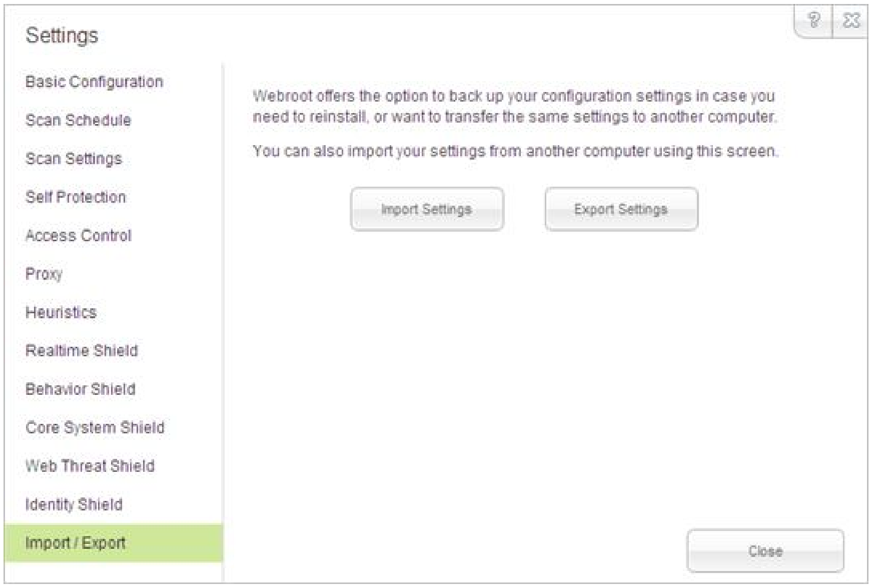
If you changed the Webroot SecureAnywhere configuration, you can back up those new settings. A backup of your configuration is helpful if you ever need to reinstall the software or transfer your configuration to another computer.

To import or export settings:

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



3. From the left panel, click **Import/Export**.



Webroot offers the option to back up your configuration settings in case you need to reinstall, or want to transfer the same settings to another computer.

You can also import your settings from another computer using this screen.

4. 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.

5. Access the other computer and click **Import Settings**. Select the file and click **Save**.

A: Webroot Support

If you want to open a support ticket with Webroot Support, go to:

https://www.webrootanywhere.com/support

B: Uninstalling the program

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.

C: License agreement

The Webroot SecureAnywhere license agreement is available at:

http://detail.webrootanywhere.com/eula.asp

Index