

Webroot[®] Software

User Guide

*for
Webroot AntiVirus with AntiSpyware*



Webroot Software, Inc.
PO Box 19816
Boulder, CO 80308

www.webroot.com

Version 6.1

Webroot Software User Guide

Version 6.1

© 2003 – 2009 Webroot Software, Inc. All rights reserved. Webroot, Spy Sweeper, Webroot AntiVirus with AntiSpyware, and the Webroot and Spy Sweeper icons are trademarks or registered trademarks of Webroot Software, Inc.

Included antivirus software © 2000 – 2009 Sophos Group. All rights reserved. Sophos and Sophos Anti-Virus are registered trademarks of Sophos Plc and Sophos Group.

All other product and company names mentioned may be trademarks or registered trademarks of their respective owners.

Contents

1: Getting Started	1
Determining your product version	2
Protecting your system	3
How online threats can damage your computer	3
How Webroot software protects your computer	3
Sweeps and quarantine	4
Shields	4
Subscription updates	4
Backup protection	5
Running the program	6
Opening the Main window	6
Main window	6
Tabs	9
Closing the Main window	9
Using the System Tray menu	10
Shutting down program operations	10
Using multiple accounts	11
Renewing your subscription	11
Checking for updates	12
Setting Gamer (silent) mode	13
Responding to alerts	14
Alerts related to potential threats	14
Alerts related to system status	14
2: Sweeping your System	15
Determining what to sweep	16
Running a sweep	17
Starting an on-demand sweep	17
Monitoring the sweep process	18
Reviewing and quarantining items	19
Viewing the sweep summary	22
Managing quarantined items	23
Keeping quarantined items	23
Deleting quarantined items permanently	24
Restoring quarantined items	24
3: Shielding your System	27
Viewing the shield summary	28
Setting Web Browser shields	29
Editing BHOs used by Internet Explorer	30
Editing the IE Hijack shield settings	30
Setting Network shields	32
Editing the Hosts file	33
Setting Windows System shields	34
Setting the Startup Programs shield	38
Setting the E-mail Attachments shield	39
Communication errors with the E-mail Attachments shield	40

4: Managing Backups	41
Managing backup accounts	42
Activating a backup account	42
Logging into a backup account	44
Switching the active account	44
Using online backup and restore	45
Creating an online backup set	45
Backing up data to the online repository	47
Restoring data from the online repository	47
Accessing your account online	49
Adding more online storage	50
5: Setting Options	51
Viewing and setting sweep options	52
Reviewing options for Full and Quick sweeps	52
Configuring Custom sweep options	54
Setting shield options	57
Setting antivirus protection	57
Setting behavioral detection	58
Changing the shield alert method	58
Setting Gamer mode options	59
Managing detected items automatically	60
Managing automatic updates	62
Setting program options	62
Viewing the session log	64
6: Creating Scheduled Events	65
Scheduling sweeps	66
Scheduling backups	68
Managing scheduled events	69
A: Webroot Support	71
Requesting Technical Support	72
Accessing the Knowledge Base	72
Reporting potential threats	72
Joining the WARN program	73
Glossary	75
Index	83

1: Getting Started

For an introduction to Webroot® Spy Sweeper and Webroot AntiVirus with AntiSpyware, see the following topics:

- **Determining your product version.**
Make sure you know which version you have.
- **Protecting your system.**
Learn how the Webroot software protects your computer from spyware and other unwanted items.
- **Running the program.**
Open the Main window, learn its functions, and shut down the program.
- **Renewing your subscription.**
Make sure your subscription is current, so you receive the latest threat protection.
- **Checking for updates.**
Keep updated on the latest product releases.
- **Setting Gamer (silent) mode.**
Set the Webroot software to a silent mode for uninterrupted gaming.
- **Responding to alerts.**
Learn about Webroot software alerts and how to respond to an alert.






Note

This guide assumes you have a basic understanding of the Windows operating system. If you need assistance with the Webroot software, see [Appendix A, “Webroot Support”](#) for contact information.

Determining your product version

This guide describes how to use the features available for the following product versions:

Webroot software versions	
Spy Sweeper	Provides protection from spyware and other potentially unwanted programs. This version includes a subscription to the evolving database of security definitions from Webroot.
Webroot AntiVirus with AntiSpyware	Provides the same protection from spyware and other potentially unwanted programs as the regular version of Spy Sweeper, along with sophisticated Sophos [®] Anti-Virus protection. This version includes a subscription to the evolving database of security definitions from Webroot. Also provides a feature for backing up your computer files.  This symbol indicates notes that apply only to the antivirus function.
Trial Version	Lets you use the Webroot software on a trial basis. When the trial expires, the Webroot software notifies you and lets you purchase a full version with a subscription from the Webroot Web site.  This symbol indicates notes that apply only to trial versions.
Scan-Only Trial Version	Performs a complimentary scan (sweep) of your computer and locates any spyware or other potentially unwanted programs. This is a limited version that demonstrates where you might have potential risks. This version does not quarantine or remove potential risks. After performing a scan, the Webroot software notifies you and lets you purchase a full version with a subscription from the Webroot Web site.  This symbol indicates notes that apply only to trial versions.

Protecting your system

The Webroot software provides a comprehensive solution for protecting your privacy and your computer from online security risks, including spyware, adware, and other potentially unwanted programs. To learn more, read the following topics:

- [How online threats can damage your computer](#)
- [How Webroot software protects your computer](#)

How online threats can damage your computer

Online security threats come in many forms — the most common types come from [spyware](#) and [viruses](#), which could install themselves without your knowledge as you visit Web sites or download software. Spyware programs are specifically designed to infiltrate your computer for commercial gain (stealing personal information or displaying annoying advertisements), while viruses are typically designed to damage your computer.

Types of spyware programs include [system monitors](#) that capture your e-mails and keystrokes, [Trojan horses](#) that can steal or destroy data, [adware](#) that pops up advertising, and [cookies](#) that store information about your online preferences and habits. While some of these programs may be harmless, others can steal your personal information and send it to a third party for malicious purposes. In some cases, these programs can damage your computer enough to slow down processing times or cause system crashes. Spyware and other unwanted programs may be part of a program that you installed or they may install themselves as you visit Web sites. They could also arrive bundled with freeware or shareware, through e-mail, or by someone with access to your computer. These programs are difficult to detect, and difficult (if not impossible) to remove. Spyware can hide in multiple locations and can reinstall if you don't remove it properly with specialized antispyware software.

A virus is computer code that often duplicates itself and causes a specific event to occur. The event may be harmless, such as displaying a message on a specific date, or may be malicious, such as deleting data or duplicating data to fill a hard drive. Viruses can arrive as file attachments to e-mail, as embedded files on a CD, and as clickable graphics in an e-mail. Once on your hard drive, viruses are difficult to detect and remove, unless you have specialized antivirus software.



Virus protection

To protect against virus attacks, you must have the Webroot AntiVirus with AntiSpyware version.

How Webroot software protects your computer

The Webroot software offers continuous protection from potential threats and helps secure your valuable data, by offering the following features:

- [Sweeps and quarantine](#)
- [Shields](#)
- [Subscription updates](#)
- [Backup protection](#)

Sweeps and quarantine

You can schedule sweeps to run at convenient times, typically while you are away from your computer (the computer must be turned on) or you can run sweeps on demand. During a sweep, the Webroot software performs the following process:

1. **Search.** The Webroot software searches for potential threats, looking for any items that match security **definitions** in the Webroot database. You can specify where the program searches (for example, search specific folders or file types) and the types of items to include or ignore (for example, bypass tracking cookies).
2. **Quarantine.** After a search, the Webroot software removes items that match security definitions from their current locations and sends them to a holding area, called the **Quarantine**, where they are rendered inoperable and cannot harm the computer. After items are quarantined, you can delete them permanently or restore them to their original locations. You can also control whether certain items are always quarantined or whether certain items like tracking cookies are always ignored.



Virus protection

If Webroot AntiVirus with AntiSpyware detects a virus, it removes the infected portions of a file during a **virus cleaning** process.

3. **Summarize.** Once you have taken action on each detected item (deleted, ignored, or restored), the Webroot software summarizes your actions.

Shields

For added protection, the Webroot software includes a shielding function that continuously monitors activity as you work (for example, when you connect to the Internet or when you open an e-mail attachment). Shields can monitor functions related to your Web browser settings, network communications between your computer and Web sites, Windows system settings, Windows Startup programs, and e-mail attachments.

If the Webroot software detects spyware or any other potential threat attempting to download, it displays an alert message. For most types of detected items, the alert message asks if you want to proceed anyway or stop the download. You can also specify that certain types of items are always managed in the same way (allowed or blocked).

Subscription updates

The Webroot Threat Research team is constantly updating security **definitions** to protect your computer from ever-changing spyware and other potential threats. The Webroot software can automatically download these definitions to your computer so you are always protected against the most current online threats.

With your purchase of the Webroot software, you receive a one-year subscription to all security definition updates and also to newly released program versions. When your subscription is within 30 days of expiration, the Webroot software will notify you in the alert panel. You can extend your subscription (or upgrade the program) at any time from the Webroot Web site. For more information, see “**Managing automatic updates**” on page 62.

Backup protection

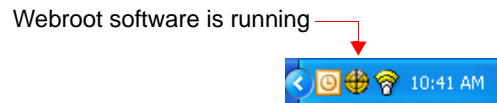
If your system crashes and you lose access to the hard drive, all your important files could be lost — family photos, financial records, school projects. Everything. If you do not perform regular backups, your files are vulnerable to system failures, theft, fire, and common human error like accidentally erasing files. Most people understand these risks, but don't take the time to back up their files.

With the Webroot software's automatic scheduling feature, you never need to think about the chore of backing up files. You can set a schedule to perform backups automatically to our online [data center](#). The backup conveniently runs in the background without interrupting your computer activity.

Whenever you need to recover files, you can access them any time from your account on our Web site. You can also set up the account to share files with friends and family.

Running the program

The Webroot software runs automatically when Windows starts. Look for the Webroot icon in the Windows system tray in the lower-right corner of your screen. This icon indicates that the Webroot software is running and actively protecting your computer.



Note


If you turned off the [Load the program at Windows startup](#) option in the Options/Program tab, you must manually start the Webroot software by double-clicking the Webroot icon on your computer desktop or selecting it through the Windows Start Menu. This action also opens the [Main window](#).

For information about running or stopping the program, see the following topics:

- [Opening the Main window](#)
- [Closing the Main window](#)
- [Using the System Tray menu](#)
- [Shutting down program operations](#)
- [Using multiple accounts](#)

Opening the Main window

Open the Main window by doing one of the following:


- Double-click the Webroot icon on your Windows desktop or select the program from the Windows **Start** menu.
- Double-click the Webroot icon  in the system tray (lower-right corner of your screen). You can also right-click the icon to open the task bar menu, then click **Home**.

Main window


The Main window is divided into two areas: the Icon panel at the left allows you to select options, while the Main panel on the right displays the corresponding settings available for the selected icon.



The following table describes the Icon functions.

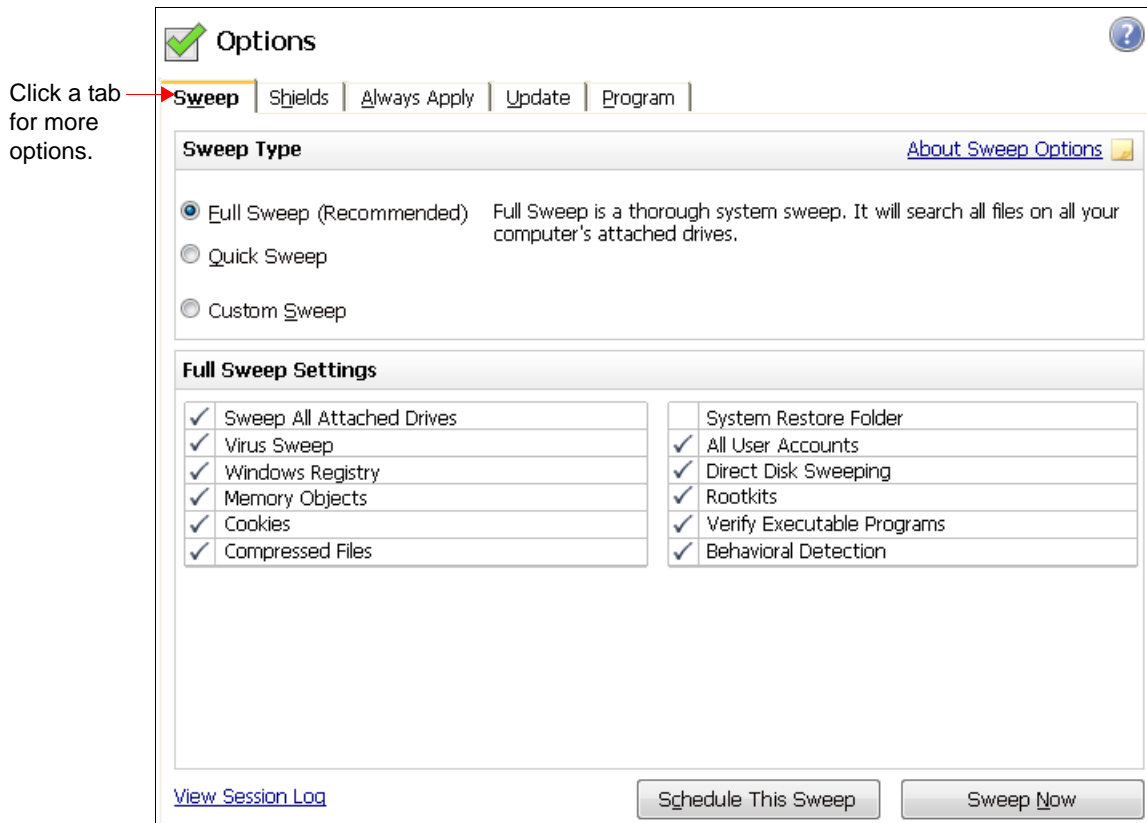
Icon functions	
Home	View overall status, as shown in the example above and described in the next table.
Sweep	Start a Full, Quick, or Custom sweep.
Shields	Set shields to continuously monitor and block activity.
Backup	Create a backup account, back up files, or restore files.
Options	Set options for sweeps, shields, quarantines, updates, and the program.
Schedule	Create schedules for automatic events, such as sweeps.
Help	Open the online instructions (you can also click the  icon).

When the Home icon is selected, the Main panel shows overall program status and provides functions, as described in the following table.


Home panel functions	
Sweep, Shields, Updates	<p>Last full sweep: Shows how long ago the Webroot software swept for viruses, spyware, and other unwanted items.</p> <p> Antivirus functions are only available with the following versions: Webroot AntiVirus with AntiSpyware or Webroot Internet Security Essentials. You can upgrade to one of these versions by clicking the Upgrade Now link in the Improve Your Protection panel.</p> <p>Shields: Shows the status of shield settings and warns you if recommended shields are turned off.</p> <p>Manage Quarantine: Click to delete or restore items after a sweep. (Only appears if there are quarantined items.)</p> <p>Sweep Now: Click to begin sweeping for spyware and other unwanted items.</p>
Backup	<p>Last backup: Shows the date and time of the last backup.</p> <p>Online storage used: Shows the amount and percentage of your account's online storage space used.</p> <p>Backup Now: Click to back up files online.</p> <p>Restore Now: Click to restore files from the online repository.</p>
Improve Your Protection	<p>Displays features you could receive by upgrading the Webroot software to another version.</p> <p>Upgrade Now: Click this link to purchase an upgrade.</p>
Subscription	<p>Active Through: Shows the date your subscription ends.</p> <p>About My Subscription: Click for program version information and definitions status.</p>
Updates	<p>Last check: Shows how long ago the Webroot software checked the update site for program and definition updates.</p> <p>Check for Updates: Click to view Webroot's update site.</p>
Gamer Mode	<p>Click Turn Gamer Mode On to set the program to "silent" operation, which suppresses functionality that could interfere with gaming.</p> <p>Click Turn Gamer Mode Off to return to normal operation.</p>
Alerts	<p>Shows if any alerts were triggered. Click an alert link to view more information.</p>

Tabs

Some panels display tabs that give you access to additional options. The following example shows the settings available when you click the Options icon.



Closing the Main window

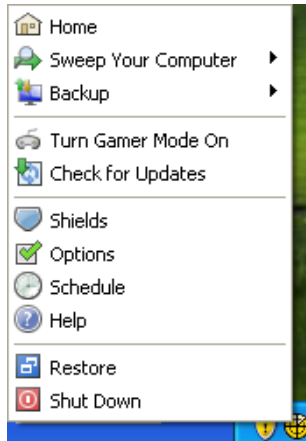
When you are finished using the Main window, click **Close**  in the upper-right corner of the screen. This action closes the window, but keeps the program running. Look for the Webroot icon in the Windows system tray at the lower-right corner of your screen; this icon means that the Webroot software is actively protecting your computer with shields. We recommend that you always keep the Webroot software running.

The program is still running



Using the System Tray menu


You can access many of the Webroot software's main features from the System Tray menu. To access this menu, right-click on the system tray icon (lower right corner of the desktop).



Shutting down program operations

To completely stop Webroot software operations, you can shut down the program. A shut-down action is only necessary if you plan to upgrade to a new version. Otherwise, you should keep the program running so that shields can actively block potential threats.

To shut down the Webroot software:

1. Right-click the Webroot icon  in your system tray.
A System Tray menu opens.
2. Click **Shut Down**.

Using multiple accounts

If your computer is configured for multiple user accounts (each person logs in with a unique name and password), the Webroot program is available to all those accounts. Users with administrative privileges have full access to all areas of the Webroot software, while other users have limited access.

The following table describes program functions not available to limited users (those without administrative privileges).

Functions unavailable to limited users	
Shields	Limited users cannot change shield settings, with the exception of the IE Hijack shield options: <ul style="list-style-type: none">• User—Limited users can use this drop-down list to change these settings. Only the current user account is affected. These settings effectively override the system settings below.• System—Only the computer administrator can use this drop-down list to change these settings. Changes here affect all user accounts, unless a limited user has customized the setting. See “ Editing the IE Hijack shield settings ” on page 30.
Program Options	Limited users cannot change settings for these options: <ul style="list-style-type: none">• Add “Sweep” option to Windows Explorer context menu• Load the program at Windows startup See “ Setting program options ” on page 62.
Quarantine panel	Limited users can view the Quarantine panel, but cannot restore or delete items that have been quarantined. See “ Managing quarantined items ” on page 23.
Scheduled Sweeps	All users can run sweeps. However, for scheduled sweeps to run, you must be logged in to the account where you created the schedule. In addition, you can only see the scheduled sweeps configured from your own account. See “ Scheduling sweeps ” on page 66.

Renewing your subscription

Your subscription includes updated security **definitions**, which protect your computer from ever-changing spyware and other potential threats. When your subscription is within 30 days of expiration, you will see a red banner and a **Renew** button at the top of the Main window. Click **Renew** to renew your subscription. You can also renew your subscription any time from the Webroot Web site (www.webroot.com) by clicking the [Renew your subscription](#) link. The renewal adds time to your existing subscription, so you never lose any subscription time that you have paid for.

If you are not sure when your subscription ends, check the Subscription section of the Home panel. If you see a [Check Status](#) link, click that link to see up-to-date subscription information.

Checking for updates

While your subscription is valid, you can install updates to the program and to security **definitions** when they are available. You should always make sure to keep updated definitions, which identify spyware and other potentially unwanted programs that the Webroot software uses as a basis for detecting potential threats during sweeps. Webroot frequently updates these definitions and makes them available for you to download (manually or automatically) from the Webroot Web site.

The Webroot software is preconfigured to check for program updates and new security definitions on a daily basis. (You must be connected to the Internet for update checks to be successful.) In addition, the Webroot software is also set to automatically download definitions, if available. We recommend that you keep these settings, as described in “**Managing automatic updates**” on page 62. You can also manually check for updates at any time; for example, you might want to check if you have the latest security definitions before running a sweep.



Trial Versions

If you have a trial version, you can download updates within your trial period.

To check for updates to the program version or security definitions:

1. Make sure you are connected to the Internet.
2. From the **Home** panel, click the [Check for Updates](#) link below **Updates**. (You can also click the **Options** icon, click the **Update** tab, and click **Check for Updates** from there.)

Your browser opens and displays the Webroot Web site. The Web site indicates if your version of the program is current and if an update is available.



Note

If you are updating the program, do *not* uninstall your previous version of the Webroot software. Installing the new version over the old one retains Quarantine information from previous sweeps and lets you keep program settings.

If new definitions are available, the Webroot software downloads and installs them. A progress bar shows the status of the download.



Virus protection

Updates include both spyware and virus definitions, for the Webroot AntiVirus with AntiSpyware version.

Setting Gamer (silent) mode

If the Webroot software interferes with your gaming, you can set the program to a silent Gamer mode. While in this mode, the program will not perform the following activities:

- **Scheduled sweeps.** The program does not run scheduled sweeps. When the program returns to regular operations (Gamer mode is switched off), an alert indicates that an event was missed. The missed event will not run automatically.
- **Shield functions.** All shields will be turned off, except for the Execution shield, which stops executable programs from launching a process on your computer. If the Execution shield detects a potential threat, it will move the item to Quarantine without alerting you. If desired, you can specify that the Execution shield is turned off along with all other shields (for instructions, see [“Setting Gamer mode options”](#) on page 59).
- **Alert pop-ups.** The program will not open alerts in the system tray.
- **Communications with the Webroot server.** The program will not contact the Webroot server to check for definition updates or program updates.

To run the program in Gamer mode, you can do either of the following:

- From the Main window in the lower-right corner, click **Turn Gamer Mode On**.
- Right-click the Webroot system tray icon in the lower-right corner of your computer screen. In the task bar menu, click **Turn Gamer Mode On**.

Gamer mode will automatically turn off after 4 hours. To change that setting, see [“Setting Gamer mode options”](#) on page 59.

To manually turn off Gamer mode, you can do either of the following:

- From the Main window in the lower-right corner, click **Turn Gamer Mode Off**.
- Right-click the Webroot system tray icon in the lower-right corner of your computer screen. In the task bar menu, click **Turn Gamer Mode Off**.

All program activities will be re-enabled, including the previously set shields. The Webroot software will also contact the Webroot server and check for any updates to security definitions and to the program.

Note

If you shut down and restart the Webroot software, it disables Gamer mode on start-up.

Responding to alerts

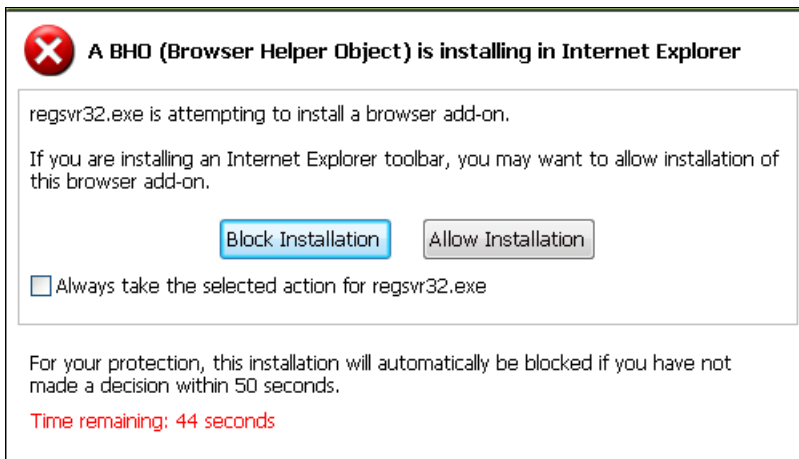
During normal program operation and shielding functions, the Webroot software may open the following types of alerts:

- Alerts related to potential threats
- Alerts related to system status

Alerts related to potential threats

When a potential threat is detected, such as spyware trying to download, Webroot's shields block the activity and open an alert window. You can respond to the alert by blocking the item or allowing it. If you do not respond within the allotted time shown in the counter at the bottom, the Webroot software blocks the activity.

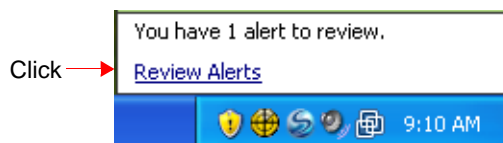
Some alerts allow you to select **Always take the selected action...**, so that if the Webroot software frequently detects this item, it will always handle it based on your selection here.



Alerts related to system status

For alerts that do not require immediate action, such as a missed scheduled sweep, the Webroot software displays an alert in either a pop-up near the system tray (lower-right corner of your screen) or in the Alerts section of the Main window. For more information about changing how status alerts are displayed, see [“Changing the shield alert method”](#) on page 58.

The following example shows an alert in the system tray. To read more information about an alert, click the [Review Alerts](#) link.



2: Sweeping your System

The sweep function scans your computer's drives, the Windows [registry](#), memory, and other places where spyware and potential threats can hide. You decide what you want to sweep: all areas (Full), only areas where spyware is commonly found (Quick), or selected areas based on your needs (Custom). For Custom sweeps, you decide what types of potential threats you want the sweep to locate and what areas of the computer to scan.

When the sweep locates potential threats that match items in the security [definitions](#), it moves the items to [Quarantine](#), a holding area where they cannot harm your computer. From there, you decide to keep, restore, or delete the items. To help you decide on an action, the Webroot software shows risk ratings for threats (from low to critical) and provides a link to the Webroot Threat Research site, where you can read more about them.

To sweep your computer and manage quarantined items, see the following topics:

- [Determining what to sweep.](#)
Decide whether to run a Full, Quick, or Custom sweep.
- [Running a sweep.](#)
Start scanning for potential spyware and other unwanted items.
- [Managing quarantined items.](#)
Keep, restore, or delete items moved to Quarantine.

You can also perform these tasks related to sweeps:

- [Reviewing options for Full and Quick sweeps.](#)
Check the preconfigured options for Full and Quick sweeps.
- [Configuring Custom sweep options.](#)
Customize where the Webroot software looks for suspicious items and what types of items it scans.
- [Managing detected items automatically.](#)
Determine if certain items are always ignored or always quarantined during the sweep.
- [Scheduling sweeps.](#)
Create schedules for running Full, Quick, or Custom sweeps.

Determining what to sweep

The Webroot software offers several types of preconfigured and customizable sweeps. See the following table to help determine what type of sweep you should perform.

Sweep recommendations	
To thoroughly sweep all areas of the computer:	<p>Perform a Full sweep, which checks all internal drives and any drives directly attached to your computer. This sweep takes longer than a Quick sweep, but is more thorough. The areas swept during a Full sweep are preconfigured and cannot be changed (see “Reviewing options for Full and Quick sweeps” on page 52).</p> <p>We recommend that you set a schedule for performing a Full sweep weekly, as described in “Scheduling sweeps” on page 66. We also recommend that you run a Full sweep immediately if you suspect that spyware or a virus has downloaded to your computer. Your system might be compromised if you notice slow or erratic performance, numerous pop-up ads, unexplained changes to your browser, or other suspicious activity. See “Running a sweep” on page 17.</p>
To quickly sweep only potential problem areas of the computer:	<p>Perform a Quick sweep, which checks only the locations where spyware and other unwanted programs are commonly found. This type of sweep is less thorough than a Full sweep, but maximizes use of your computer’s processing power to make the sweep as fast as possible. The areas swept during a Quick sweep are preconfigured and cannot be changed (see “Reviewing options for Full and Quick sweeps” on page 52).</p> <p>We recommend that you run a Quick sweep (or a Full sweep) after you perform potentially unsafe Internet activity, such as downloading free software or accidentally clicking on a pop-up advertisement. Spyware commonly piggybacks on free downloads and can install on your computer without your knowledge. Spyware can even get installed in a “drive-by download” as you surf an infected Web site. See “Running a sweep” on page 17.</p>
To sweep selected areas of the computer:	<p>Perform a Custom sweep, which lets you focus on specific drives, areas of the computer, or file types. The Webroot software saves these settings for future Custom sweeps.</p> <p>You might want to perform a Custom sweep in a variety of situations; for example, you could use the Custom sweep options to limit the sweep only to your C: drive and to skip certain file types that you know are safe. See “Configuring Custom sweep options” on page 54 and then follow the instructions in “Running a sweep” on page 17.</p>
To sweep a single file or folder:	<p>From Windows Explorer, you can right-click on a specific file or folder to start a sweep from the pop-up menu. This method of sweeping is useful if you downloaded a file and want to quickly scan it for threats. To run a sweep from Windows Explorer, see “Running a sweep” on page 17.</p>

Running a sweep

During a sweep, the Webroot software performs a three-step process:

1. **Search.** Scans your computer for known threats, looking for any items that match **definitions** and that meet the criteria specified in the Options tab's Sweep settings.
2. **Quarantine.** Lists all items that matched security definitions and lets you determine whether to send the items to Quarantine or keep them in their current locations. Items in Quarantine are rendered inoperable and cannot harm your computer.
3. **Summarize.** Describes actions taken for each found item.

To run an immediate sweep, see the following topics:

- [Starting an on-demand sweep](#)
- [Monitoring the sweep process](#)
- [Reviewing and quarantining items](#)
- [Viewing the sweep summary](#)

If you want to set an automatic sweep schedule, see [“Scheduling sweeps”](#) on page 66.

Starting an on-demand sweep

You can start an on-demand sweep from the program's Main window or from Windows Explorer. Before you begin the sweep, do the following:

- Close all programs that are listed in the taskbar at the bottom of your screen. The Webroot software may not be able to remove spyware associated with a particular program if that program is open. You do not need to close programs shown in the system tray in the lower-right corner of your screen; these programs are only running in the background.
- Make sure the security definitions are up-to-date, as described in [“Checking for updates”](#) on page 12.
- Optionally, you can check what criteria the Webroot software uses for sweeping your system, as described in [“Viewing and setting sweep options”](#) on page 52.

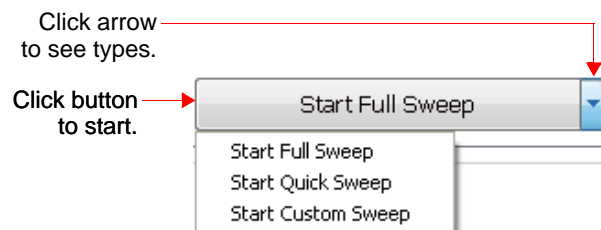
To start a sweep from the Home panel:

From the Home panel, click **Sweep Now**. The Webroot software performs either a Full, Quick, or Custom sweep, depending on which one is selected in the Sweep panel, as described below.

To start a sweep from the Sweep panel:

1. If you want to select from a Full, Quick, or Custom Sweep, click **Sweep** from the Icon panel.

The Sweep Your Computer panel displays a Start button:



2. Click the down arrow on the button to select one of these sweep types:
 - **Start Full Sweep.** Sweeps all areas of the computer thoroughly.
 - **Start Quick Sweep.** Sweeps only areas where threats are commonly found.
 - **Start Custom Sweep.** Sweeps only selected areas (see “[Configuring Custom sweep options](#)” on page 54).
3. Click the button to start the sweep.

To start a sweep from Explorer:

1. Make sure you have enabled the [Add “Sweep” option to Windows Explorer context menu](#) as described on [page 63](#).

You do not need to open the Main window; the program just needs to be running (the Webroot icon appears in the system tray).

2. Open Windows Explorer.
3. Right-click the file, folder, or drive you want to sweep.
4. From the pop-up menu, select **Perform Security Sweep**.

Monitoring the sweep process

When you start a sweep, the Sweeping panel opens and the Webroot software shows its progress, including the number of items found, progress bar, current sweep location, and a list of detected items.



Note

If you want to pause the sweep, click **Pause Sweep**. When you want to resume the sweep, click **Resume**.

If you want to stop the sweep entirely, click **Stop Sweep**.

On the right side of the Sweeping panel, the fields show more details about what the Webroot software is inspecting and what it has found.

Sweep Details	
Search for	
Total Definitions	Current security definitions being used to locate potentially unwanted programs. You should update your definitions regularly to ensure that you are using the most current version (see “ Checking for updates ” on page 12).
Items Inspected	
Memory	Program pieces that were swept in your computer’s memory. Some of these pieces may be part of a potentially unwanted program.
Registry	Items in the Windows registry that were searched. Some registry entries may be associated with potentially unwanted programs.
Cookies	The cookies that were searched. Some cookies contain personal information (including surfing habits, user names and passwords, and areas of interest).

Sweep Details	
Files/Folders	Files and folders on the selected drives that were searched.
Detected	
Items	The security definitions matched during the sweep. A security definition is a set of fingerprints that characterize a potentially unwanted program, such as spyware or adware.
Traces	The traces found during the sweep.

If the Webroot software did *not* detect any potential threats, it opens the Summary panel and shows details about the sweep. You can click **Back to Home** to return to the Home panel.

If the Webroot software did detect potential threats, it opens the Quarantine panel and shows details about the items it found. See the next section, “**Reviewing and quarantining items.**”

Reviewing and quarantining items

After the Webroot software runs a sweep, it opens the Quarantine panel, similar to the following example.

Sweep Your Computer

Sweeping → **Quarantine** → Summary

Found: 4 Items
Auto-quarantined: 0 Items
Auto-ignored: 0 Items

Select items to quarantine (quarantined items cannot harm your computer). Items not selected will be kept and will remain active.

✓	Name	Risk
<input checked="" type="checkbox"/>	2o7.net cookie	High
<input checked="" type="checkbox"/>	c:\document...\dana@2o7[1].txt	
<input checked="" type="checkbox"/>	c:\document...\evan@2o7[1].txt	
<input checked="" type="checkbox"/>	mediaplex cookie	Medium
<input checked="" type="checkbox"/>	dealtime cookie	Medium
<input checked="" type="checkbox"/>	specificclick.com cookie	Medium

Select All Deselect All View Sweep Details

Item Details

Name: 2o7.net cookie
Category: Spy Cookie
Risk Rating: High
Traces Found: 2
Description: 2o7.net Cookie is a cookie that may track the unique visitors to a Web site, as well as their personal preferences.








View More Details Online

Quarantine Selected

Click to view folder location. (points to folder icon)

Select to move. Deselect to keep. (points to checkbox)

The Quarantine panel provides details about detected items, as described in the following table.

Quarantine Details	
Summary panel (left):	
Found	List of potential threats that were found. All items are automatically selected and ready to be moved to Quarantine.  If you have Webroot AntiVirus with AntiSpyware and you turned on the Automatically quarantine viruses detected during sweep option (see page 55), the Webroot software does not list files with detected viruses in this panel. Instead, it automatically places them in Quarantine.
Auto-quarantined: Auto-ignored:	If you performed sweeps previously and already set some items to Always Ignore or Always Quarantine, those items are counted in these fields, but not listed in the panel below. For more information, see “Managing detected items automatically” on page 60.
Item Details panel:	
Name	Name of the item currently selected in the list. The Webroot software automatically pre-selects all items in preparation for moving them to Quarantine, except those listed as a rootkit . Items with a green check mark <input checked="" type="checkbox"/> next to them will be moved to Quarantine once you click Quarantine Selected .
Category	Type of item currently selected in the list, such as “Spy Cookie.” The Glossary includes definitions for many of the categories.
Risk Rating	Red bars show the risk level of the selected item. The more bars shown, the higher the risk, as follows: <ul style="list-style-type: none"> •  —Low •  —Moderate •  —High •  —Very high •  —Critical
Traces Found	Number of traces found related to this item. Traces are the individual elements that make up the definition database.
Description	Description of the item. For more information, click View More Details Online .  You must be connected to the Internet to see the additional information.

You can select items to move to Quarantine, which is a holding area where potential threats cannot harm your computer. Moving items to Quarantine does not permanently delete them; you must manually delete items from Quarantine. You can also specify that certain items stay in their current locations and remain active.



Trial Versions

If you have the Scan-Only trial version, you cannot quarantine and remove detected items. Click **Subscribe** to buy a subscription so you can remove these items.

To select items and move them to Quarantine:

1. Review all items listed in the Quarantine panel:
 - To see more details about an item, click on the item name in the list. Details appear on the right. If you need more information, click [View More Details Online](#) to connect to the Webroot Threat Research Center (you must be connected to the Internet).
 - To see the location (full path) to the traces found, click the arrow ▶ next to an item.
2. Determine which items you want to remove or keep. Items with a green check mark will be moved to Quarantine. If there are any items that you want to keep, click on the box to remove the green check mark. You can also use the [Deselect All](#) or the [Select All](#) links at the bottom of the panel.

If you aren't sure what to do with an item, the safest action is to move it to Quarantine, where it cannot harm your computer, but can also be restored if necessary.



Note

If you know you will always want to ignore or quarantine an item for future sweeps, you can right-click an item and select **Always Ignore** or **Always Quarantine**. For more information, see [“Managing detected items automatically”](#) on page 60.

If you want to quarantine a **rootkit**, make sure you click on the box to add a green check mark. If you are uncertain whether the items listed as rootkits should be quarantined, contact technical support for assistance (see [“Requesting Technical Support”](#) on page 72).

3. Click **Quarantine Selected** to move all selected items (with a green check mark) to Quarantine.

The Webroot software first encrypts each trace, removes it from its original location (so it will no longer run), then copies it to Quarantine. Items are not permanently deleted during this process.



Virus protection

If Webroot AntiVirus with AntiSpyware is able to clean the file (remove the virus safely), it keeps the cleaned file in its original location and sends a copy of the corrupted file to Quarantine. The cleaned file is safe to use; the file in Quarantine is *not* safe to use.

The quarantine process can take several minutes or longer depending on the number of traces and the speed of your computer. When finished, the Webroot software opens a summary panel (see [“Viewing the sweep summary”](#) on page 22). Once items are quarantined, you can leave them in Quarantine, restore them (if necessary), or delete them. See [“Managing quarantined items”](#) on page 23.

Some detected items require that you download and use an additional tool to completely remove them from their original locations. If this is the case, the Additional Tools Required panel opens during the quarantine process. (You must be connected to the Internet to download additional tools.)

To download and use an additional tool:

1. From the Additional Tools Required panel, click the **Download** link to download the tool to your computer.

The Webroot Web site opens in your Web browser.

2. Follow the instructions on the Web site to download the file that contains the tool.

Make a note of where you downloaded the file on your computer.

3. Follow the instructions on the Web page to install and use the tool.

4. From the Additional Tools Required panel, click **Finish**.

The Home panel opens.

Viewing the sweep summary

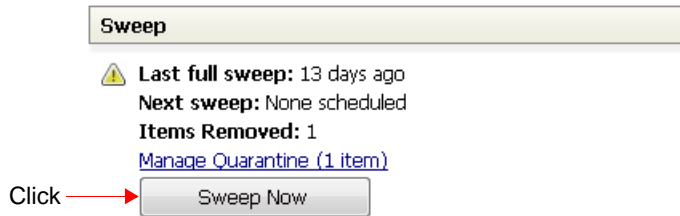
When the Webroot software is finished managing items, the Summary panel opens and provides a status of the sweep and quarantine process. The Action Taken column shows how the item was managed (for example, moved to Quarantine).

Sweep summary actions	
Quarantined	All traces of the item were moved to Quarantine. For more information, see “Managing quarantined items” on page 23.
Ignored	The item was skipped, because you deselected it in the previous panel.
Always Quarantine	The item was automatically quarantined, because you have it set to Always Quarantine. For more information, see “Managing detected items automatically” on page 60.
Always Ignore	The item was automatically bypassed, because you have it set to Always Ignore. For more information, see “Managing detected items automatically” on page 60.
Partially Quarantined	Some traces of the item were quarantined, but not all, because you deselected some traces in the previous panel.

If desired, you can view the detailed sweep session log by clicking the [View Session Log](#) link. To view the detailed log later, click the **Options** icon, then the **Sweep** tab, then click the [View Session Log](#) link.

Managing quarantined items

Once items are quarantined, you can view and manage them by selecting the [Manage Quarantine](#) link from the Home panel. (If the Quarantine is empty, this link does not appear.)



You have the following options for managing items detected during a sweep:

- **Keeping quarantined items** (recommended). This is the safest action for found items, since it allows you to test your computer without the item in its original location and determine if all your programs still work properly after it's moved. However, if the Quarantine area gets too full, the Webroot software alerts you and you must remove some items.
- **Deleting quarantined items permanently**. You can permanently delete an item if you're sure it's unwanted spyware or another type of threat.
- **Restoring quarantined items**. If you discover that some of your legitimate programs won't work properly when an item was placed in Quarantine, you can restore that item from Quarantine to its original location on the computer.



Trial Versions

If you have the Scan-Only trial version, you cannot quarantine and remove detected items. Click **Subscribe** to buy a subscription so you can remove found items.

Keeping quarantined items

You can keep items in Quarantine, where they are rendered inoperable and cannot harm your computer. This is the safest action to take. It allows you to test your computer to make sure that all legitimate programs still function properly without an item. If necessary, you can restore an item from Quarantine.

If the Quarantine area reaches certain size limits or when your computer's hard drive is low on space, the Webroot software opens a pop-up alert from the system tray (lower-right corner of your screen), in the Alerts panel, or in a Webroot message window. If you see the Webroot message window, the alert is critical and space on your hard drive is very low. You should take action to make more space available. The alert message gives you three options:

- **Delete Old Items**. Click to delete all items in Quarantine that are more than seven days old. If deleting these items does not make enough space available, the Webroot software opens another message recommending that you go to Quarantine and delete more items (see "[Deleting quarantined items permanently](#)" on page 24).
- **Manage Quarantine**. Click to open the program with the Quarantine panel displayed, where you can selectively delete items from Quarantine (see "[Deleting quarantined items permanently](#)" on page 24).

- **Remind Me Later.** Click to have the Webroot software remind you tomorrow. If you take this action, you may want to delete other files to make more hard drive space available.

Deleting quarantined items permanently

If your legitimate programs run properly after quarantining a potential threat, you can permanently delete the item. You will *not* be able to restore the item after deleting it from Quarantine.

To permanently delete quarantined items:

1. From the Home panel, click the [Manage Quarantine](#) link.

The Quarantine panel opens with information about items that you have quarantined, but have not permanently deleted. For more information, see the [Quarantine Details](#) table on [page 20](#).

2. Select each item that you want to permanently delete.

A check mark next to the item shows that it is selected and will be deleted.

3. Click **Delete Selected Items**.



Note

If the **Delete Selected Items** button is unavailable (dimmed), you may not have access to this function. For more information, see [“Using multiple accounts”](#) on [page 11](#).

The Webroot software deletes the selected items and displays information about the deletion at the bottom of the panel.

Restoring quarantined items

You may need to restore a quarantined item if you discover that a program on your computer is not working correctly without it. Sometimes, a piece of spyware is an integral part of a legitimate program and is required to run that program.

In some cases, components with copy protection may not restore from Quarantine properly. You must reinstall these programs from the original media or installation file.



Virus protection

Do not restore a file with a detected virus. If Webroot AntiVirus with AntiSpyware was able to clean the file (remove the virus safely), it keeps the cleaned file in its original location and places a copy of the corrupted file in Quarantine. The cleaned file is safe to use; the file in Quarantine is not safe to use.

To restore quarantined items:

1. From the Home panel, click the [Manage Quarantine](#) link.

The Quarantine panel opens with a list of the items that you have quarantined, but have not permanently deleted. For more information, see the [Quarantine Details](#) table on [page 20](#).

2. Select each item that you want to restore.

A check mark next to the item shows that it is selected and will be restored.

3. Click **Restore Selected Items**.



Note

If the **Restore Selected Items** button is unavailable (dimmed), you may not have access to this function (see [“Using multiple accounts”](#) on page 11).

The Webroot software restores the selected items to their original locations and shows the restore status at the bottom of the panel. If a selected item is part of an e-mail attachment, the Webroot software saves it to the location specified in the **Always save to:** option of the [Setting the E-mail Attachments shield](#) (see [page 39](#)) or prompts you to select the location to restore the attachment (if you selected the **Ask me where to save every file** option).



3: Shielding your System

While the Webroot software is running, the shields actively monitor for potential threats that try to download onto your computer. If the shields detect a suspicious item, an alert opens and asks if you want to continue downloading the item or if you want to block it.



Virus protection

Shields also protect against viruses attempting to download to your computer, if you have Webroot AntiVirus with AntiSpyware. See “[Setting antivirus protection](#)” on page 57.

The Webroot software has preconfigured shields. To change shield settings for your own needs, see the following topics:

- [Setting Web Browser shields.](#)
Protect your **default** home page, list of favorites, and other settings related to your Web browser.
- [Setting Network shields.](#)
Monitor network communication between your computer and other Web sites.
- [Setting Windows System shields.](#)
Protect your Windows system settings.
- [Setting the Startup Programs shield.](#)
Stop unwanted programs from displaying in the Windows Start menu.
- [Setting the E-mail Attachments shield.](#)
Monitor e-mail file attachments for potential threats.







You can also perform these tasks related to shields:

- [Setting antivirus protection.](#)
Block viruses in some of the shield types.
- [Setting behavioral detection.](#)
Block potential threats based on the item’s behavior.
- [Changing the shield alert method.](#)
Determine how status alerts open.
- [Setting Gamer mode options.](#)
Determine if the Execution shield turns off when Gamer mode is enabled.

Viewing the shield summary

To see a summary of all shields and their status, click **Shields** in the Icon panel to display the Shields Summary tab.

The icons in the Shields Summary panel indicate the following:



Status icons	
 —Full Protection	In the Shield Status, a green check mark indicates that all critical and recommended shields are turned on.
 —Partial Protection	In the Shield Status, a yellow exclamation mark indicates that all critical shields are on, but some recommended shields are off. In the panels below, an exclamation mark appears next to the shield that is turned off. You can click the shield name to go to the tab where you can turn the shield back on.
 —Vulnerable	In the Shield Status, a red X indicates that one or more critical shields are not turned on. In the panels below, a red X appears next to the shield that is turned off. You can click the shield name to go to the tab where you can turn the shield on. We strongly recommend keeping all critical shields turned on.
 —Spyware shield	This icon appears next to shields that block spyware and potentially unwanted programs. If it is grayed out, the shield is off.
 —Virus shield	 <i>Webroot AntiVirus with AntiSpyware only.</i> This icon appears next to shields that block viruses. If it is grayed out, the shield is off.

Setting Web Browser shields

You can modify the shields that protect your **default** home page, list of favorites, and other settings related to your Web browser.

To set Web Browser shields:

1. In the Icon panel, click **Shields**.
The Shields Summary tab opens, showing a summary of the available shields and their status. (If any shields are dimmed, you do not have access to them; see “Using multiple accounts” on page 11.)
2. Click the **Web Browser** tab.
3. Select the options you want to use. Items with a green check mark are enabled.

Web Browser shields	
Tracking Cookies	Watches for known cookies (matching those in the security definitions) and removes them. Tracking cookies are cookies that can track your Web activities. These <i>may</i> include cookies that contain user names, passwords, or similar information that you enter on some Web sites.
IE Favorites	Protects your Internet Explorer favorites. Whenever a Web site tries to change your favorites, the Webroot software alerts you and lets you accept or reject the change. Some Web sites add entries to your favorites without informing you; this shield ensures that you are aware of attempted changes. Even if the Webroot software is not open when your favorites change, it detects the changes and alerts you the next time you start the program.
IE Security	Protects your Internet Explorer security settings (select Tools > Internet Options and click the Security tab). Whenever a program tries to change these settings, the Webroot software alerts you and lets you accept or reject the change. Some programs change these options without informing you; this shield ensures that you are aware of attempted changes.
Browser Helper Object (BHO)	Watches for the installation of Browser Helper Objects (BHOs) . Whenever a BHO tries to install itself, the Webroot software alerts you and lets you accept or reject the change. BHOs are add-on programs that work with your browser. Some spyware programs add BHOs without your knowledge; this shield ensures that programs do not add a BHO without your consent.  This option also blocks viruses that try to install along with a BHO, if you have Webroot AntiVirus with AntiSpyware. BHO Shield Options button: Click to change the BHOs that start with Internet Explorer. See the next section, “Editing BHOs used by Internet Explorer.”  Editing BHOs is for advanced users. Deselecting BHOs could cause your browser to not work properly or cause your computer to be unstable.

Web Browser shields *(continued)*

IE Hijack	<p>Protects various Internet Explorer functions, such as the search page, error pages, and other default pages that Internet Explorer opens. Whenever a program tries to change these pages, the Webroot software alerts you and lets you accept or reject the change. Some programs change (“hijack”) these pages without informing you; this option ensures that you are aware of attempted changes.</p> <p>Even if the Webroot software is not open when these pages change, it detects the changes and alerts you the next time you start the program.</p> <p>IE Hijack Shield Options button:</p> <p>Click to edit the list of Hijack shields. See “Editing the IE Hijack shield settings” on page 30.</p>
-----------	---

Editing BHOs used by Internet Explorer

You can edit the BHOs that run when you start Internet Explorer. BHOs are add-on programs that work with your browser. Some spyware and other potentially unwanted programs add BHOs without your knowledge.



Caution

Editing browser add-on items is for advanced users. Editing items in the list could cause your browser to not work properly or cause your computer to be unstable. Edit with extreme caution.

To edit BHOs used by Internet Explorer:

1. From the **Shields/Web Browser** tab, click **BHO Shield Options**.

The Edit Browser Helper Objects window opens, with a list of the installed BHOs. Items with a check mark start whenever Internet Explorer starts. To see more information about an item, select it and click **More Details**. Not all programs provide additional details.

2. Deselect any BHOs you do not want to start whenever Internet Explorer starts.
3. Click **OK**.

Editing the IE Hijack shield settings

You can edit the individual IE Hijack shield settings, including the **default** home and search pages for Internet Explorer.

To edit the IE Hijack shield settings:

1. From the **Shields/Web Browser** tab, click **IE Hijack Shield Options**.

A window opens for editing the settings.

2. Select the options you want to use. Items with a green check mark are enabled.

IE Hijack Shield Settings	
IE Home Page Shield	Protects the Web site set as your home page (the site that opens automatically when you start Internet Explorer or when you click the Home button). Some spyware programs change your home page.
Use This Page	Enter the desired Web site address. The address must be in the following format: http://www.webroot.com.
Alert me before restoring this setting	Select to display an informational alert when the Webroot software automatically changes the home page back to the site listed above. To avoid seeing alerts about changes to your home page, do not select this option.
IE Search Page Shield	Protects the page that automatically opens when you enter a non-existent Web site. Some spyware programs change this page.
Use This Page	Enter the desired Web site address for performing Web searches. The address must be in the following format: http://www.webroot.com.
Alert me before restoring this setting	Select to display an informational alert when the Webroot software automatically changes the search page back to the site listed above. To avoid seeing alerts about changes to your search page, do not select this option.
Advanced Settings	Provides advanced configuration options used only in error conditions and/or when a system is severely infected. Use these options to repair your Internet Explorer settings when a browser hijacker embeds itself deeply in your browser. Webroot customer support is available to assist.
User	Use this drop-down list to change settings to the current user account. These settings effectively override the system settings below. Enter the Web site addresses in the following format: http://www.webroot.com. You can also enter the path to a file.
System	Use this drop-down list to change settings for all user accounts, unless a limited user has customized the setting. (Only the computer administrator can change this setting; see “Using multiple accounts” on page 11.) Enter the Web site addresses in the following format: http://www.webroot.com. You can also enter the path to a file.
Alert me before restoring this setting	Select to display an informational alert when the Webroot software automatically changes the pages listed in the Advanced Settings drop-down list back to the site or path listed in the text field. To avoid seeing these alerts, do not select this option.

3. If you want to reset all of the Internet Explorer page settings back to the defaults (automatic options) used when Internet Explorer was first installed, click **Reset IE Page Settings to Defaults**.
4. Click **OK**.

Setting Network shields

You can modify the shields that monitor network communication between your computer and other Web sites. These communication settings are vulnerable to the effects of spyware and viruses and can be changed without your permission. Network shields block some ads that may open in your browser. They also stop Web sites from sending you to other, unexpected Web sites.

To set Network shields:

1. In the Icon panel, click **Shields**.

The Shields panel opens, showing a summary of the available shields and their status. (If any shields are dimmed, you do not have access to them; see [“Using multiple accounts”](#) on page 11.)

2. Click the **Network** tab.
3. Select the options you want to use. Items with a green check mark are enabled.

Network shields	
Common Ad Sites	Blocks banner and other advertising from common advertising sites. When you go to a Web site that has advertising from one of the blocked sites, you may see a small graphic that indicates a broken link to a graphic (typically a red X in a box). This X just shows where the blocked ad would display. The Webroot software updates these sites when you update your definitions.
Hosts File	Monitors the Hosts file for any changes. Some programs will add or change the IP address for a Web site in the Hosts file. When you try to go to the added or changed Web site, you will really go to a different Web site, such as an advertising site. This shield ensures that programs do not change an IP address without your knowledge. Hosts File Shield Options button: Click to edit the Hosts file. For more information, see “Editing the Hosts file” on page 33.
Internet Communication	Monitors communication from your computer to known Web sites that are related to potentially unwanted programs. The Webroot software includes a list of known sites with its definitions . If the Webroot software detects an attempt to communicate with a site on the list, it displays a pop-up alert in the system tray (lower-right corner of your screen) telling you that access to the site was blocked.

Editing the Hosts file



Caution

This section describes highly technical features associated with how your computer locates the actual address of a Web site. The features described here will not damage your computer or remove anything you need if you enable them, but the underlying technology is complex if you are not aware of how IP addressing works.

You can configure the Webroot software to continuously monitor several functions related to the Hosts file. The Hosts file is a Windows file that helps direct your computer to a Web site using Internet Protocol (IP) addresses. Your Web browser uses the IP address to actually connect to a site.

When you go to a Web site, your computer first looks in the Hosts file to see if it already knows where to go. If the domain (for example, webroot.com) is listed, your computer goes directly to the IP address listed in the Hosts file. If the domain is not in the Hosts file, your computer looks up the information from the Internet (a slightly slower process).


You can use the Hosts file to your advantage by routing certain domains, such as advertising sites, to a dead end. This will block tracking cookies and other monitoring programs. However, some spyware and adware will route (or “hijack”) certain domains to false addresses (for example, by making a commonly used search site open to a porn site).

Using the Webroot software to manage the Hosts file, you can block a lot of unwanted adware activity, while preventing your Web browsing from being hijacked. When the Webroot software detects activity related to the Hosts File shield, it displays an alert.

To edit the Hosts file:

1. From the **Shields/Network** tab, click **Hosts File Shield Options**.

The Edit Hosts File window opens, showing entries that you, your IT department, or potentially unwanted programs have added to your Hosts file. If you have the Common Ad Sites Shield turned on, it does not display the blocked ad sites.

The Webroot software compares the IP address of each entry in the Hosts file to the correct address on a domain name system (DNS) server. Any address that does not match and is not set to the local machine address (127.0.0.1) is flagged as possibly hijacked .

2. Select the entries you want to remove.
3. Click **Delete Selected**.

The Webroot software deletes the selected entries from your Hosts file.

4. Click **Close**.

Setting Windows System shields



You can modify the shields that monitor Windows system settings, which some malware can change if not protected.

To set Windows System shields:


1. In the Icon panel, click **Shields**.

The Shields panel opens, showing a summary of the available shields and their status. (If any shields are dimmed, you do not have access to them; see “Using multiple accounts” on page 11.)

2. Click the **Windows System** tab.
3. Select the options you want to use. Items with a green check mark are enabled.

Windows System shields	
ActiveX	<p>Watches for programs that install ActiveX technology on your computer. Whenever a program tries to install ActiveX technology, the Webroot software alerts you and lets you continue the installation or stop it.</p> <p> This option also blocks any viruses that try to install ActiveX technology, if you have Webroot AntiVirus with AntiSpyware.</p> <p>ActiveX Shield Options button: Click to edit the ActiveX shield option.</p> <p>Prompt me only for known spyware items: This option watches for only known items from the security definitions that try to install ActiveX technology. Leaving this option turned on will reduce alert notifications, but could permit a new threat to install that is not yet included in the definitions.</p>
Alternate Data Stream Execution	<p>Watches for programs that try to start from an Alternate Data Stream (ADS). Turning on this shield lets the Webroot software alert you if a program tries to start from an ADS.</p> <p> This option also actively watches for viruses that try to start from an alternate data stream, if you have Webroot AntiVirus with AntiSpyware.</p>
Windows Messenger Service	<p><i>Applies only to Windows XP. Not available for Vista.</i></p> <p>Turns off and actively watches the Microsoft Messenger Service. This service is <i>not</i> an instant messaging program and does <i>not</i> affect your use of instant messaging. This service is often used for sending spam (unwanted e-mail) and creating pop-up ads. Turning off the service stops these types of spam and pop-ups.</p> <p>If your computer is in your home, you can turn off this service without any problem. If you work in a corporate environment, contact your system administrator to determine if your company uses the service to communicate with company employees. If you are not sure, leave the service turned on until you know.</p>

Windows System shields *(continued)*


System Services	<p>Monitors the system registry and protects against unwanted services and drivers from installing.</p> <p> This option also blocks viruses that try to install in the system registry, if you have Webroot AntiVirus with AntiSpyware.</p> <p>System Services Shield Options button: Click to edit System Services shield options.</p> <p>Highest Security: Select this option to display an alert related to any item detected by the System Services shield.</p> <p>High Security: Select this option to allow a signed service, but display an alert when an unsigned service or a potential malware application is detected.</p> <p>Moderate Security: Select this option to prompt only when potential malware is detected.</p>
-----------------	---

Windows System shields (continued)

Execution

Watches for known items from the security definitions that try to install themselves. Whenever a potentially unwanted program tries to install itself, the Webroot software alerts you and allows you to block or allow the installation.

This option also actively watches for potentially unwanted programs that try to start when you start a program and when you save to the disk drive. Whenever the Webroot software detects a potentially unwanted program in either of these situations, it alerts you and allows you to block or allow the action. If you block the action, the Webroot software places the file that tried to install, start, or save itself in Quarantine. You can then remove or restore the file. See [“Managing quarantined items”](#) on page 23.


 This option also watches for viruses that try to install themselves, if you have Webroot AntiVirus with AntiSpyware.


Execution Shield Options button:

Click to edit Execution shield options.

Automatically quarantine programs detected by this shield:

Automatically stops the installation, startup, or saving of known items from the security definitions and places the file that tried to install, start, or save itself in Quarantine, without alerting you.

 **Automatically quarantine viruses detected by these shields:** This option automatically stops the installation, startup, or saving of known viruses that are in the security definitions and places the file that tried to install, start, or save itself in Quarantine, without alerting you. You must have Webroot AntiVirus with AntiSpyware.


 **Scan for viruses when starting applications:** This option watches for viruses that try to start when you start a program on your computer, alerts you, and allows you to block or allow the startup. Select this option if you want stronger protection against viruses. If programs take longer to start than you want, deselect this option. You must have Webroot AntiVirus with AntiSpyware.

Analyze executable programs in protected memory space before starting: Isolates and examines suspect processes when you start a program and looks for potentially unwanted programs. The process isolation gives the Webroot software a better chance to see what the process does. If the process matches a security definition, the Webroot software alerts you and allows you to block or allow the startup. Select this option if you want stronger protection against potentially unwanted programs. If programs take a long time to start, deselect this option.

Windows System shields (continued)

File System

Watches for programs during write and read operations.

 This option also blocks any viruses that try to install during write and read operations, if you have Webroot AntiVirus with AntiSpyware.

File System Shield Options button:


Click to edit File System shield options.

Scan on Write: Monitors files or programs that attempt to install (write) to your computer.

Scan on Read: Monitors programs as your computer attempts to read them. You can specify that all files types (extensions) are included by clicking “Conduct full on-read scanning,” or specify that only certain file types are included by clicking “Scan only selected file types on read.” To include only specific file types, select the extension types and click **Add to Extensions to Scan**. You can also delete items from the list by clicking on the file extension and clicking **Delete Selected**. To return the list to its original contents, select **Reset List to Default**.

Automatically quarantine programs detected by this shield:

Automatically stops the installation, startup, or saving of known items from the security definitions and places those items in Quarantine, without alerting you.

 **Automatically quarantine viruses detected by this shield:** This option automatically stops the installation, startup, or saving of known viruses that are in the security definitions and places those viruses in Quarantine, without alerting you. You must have Webroot AntiVirus with AntiSpyware.

Setting the Startup Programs shield

You can set a shield to monitor the list of programs that start every time you start Windows. Some spyware add themselves to this startup list if you are not protected, which causes the spyware program to start every time you start Windows. The Webroot software also lets you edit the startup items.



Caution

Editing startup items is for advanced users. Some items listed may be required by Windows or other programs. Deselecting items from the list could cause your computer to not start properly or cause some programs not to work. Edit with extreme caution.

To set up the Startup Programs shield:

1. In the Icon panel, click **Shields**.
The Shields panel opens, showing a summary of the available shields and their status.
2. Click the **Startup Programs** tab.
3. Select the options you want to use. Items with a green check mark are enabled.

Startup Programs shield

Startup Items Watches for attempts to add any item to your startup list. Select an option below to set when you want the Webroot software to alert you.


 This option also actively watches for attempts to add viruses to your startup list, if you have Webroot AntiVirus with AntiSpyware.

Startup Programs Shield Options... button:

Click to edit Startup Items shield options.


Alert me only for suspected spyware and virus changes to startup items:

Watches for attempts to add potentially unwanted programs, such as spyware, adware, and suspect programs, to your startup list. Some spyware will install to your startup list, so the programs will always run on your computer. This shield ensures that spyware programs do not add themselves to your startup list without you being aware of it.

 This option also watches for viruses, if you have Webroot AntiVirus with AntiSpyware.

Alert me for all startup item changes: Watches your startup list for all changes. Some spyware will install to your startup list, so the programs will always run on your computer. This shield ensures that you are always alerted when a program tries to add an item to your startup list.

Checked items automatically start when Windows starts: The items in this list start on your computer when Windows starts. To see more information about an item, select it and click **More Details** (however, not all programs provide additional details). If you do not want an item to start with Windows, deselect its checkbox.

 Some items listed may be required by Windows or other programs and may cause your computer to not start properly if removed. Edit with caution.

Setting the E-mail Attachments shield

You can set a shield to monitor file attachments for both incoming and outgoing e-mails. If the Webroot software detects that an attachment or its contents match a threat definition, it replaces the content of the attachment with an alert message that describes what it found. The Webroot software will move the original attachment to Quarantine, where you can decide whether to save it to your computer or delete it. You can also direct the Webroot software to always restore quarantined e-mail attachments to a specific directory.



Note

The E-mail Attachments shield does not support e-mail clients that use Secure Sockets Layer (SSL).


To set up the E-mail Attachments shield:

1. In the Icon panel, click **Shields**.
The Shields panel opens, showing a summary of the available shields and their status.
2. Click the **E-mail Attachments** tab.
3. Select the options you want to use. Items with a green check mark are enabled.

E-mail Attachments shield

E-mail Attachments Monitors e-mail attachments for incoming e-mail (through POP3 protocol) and outgoing e-mail (through SMTP protocol). If it detects a suspicious attachment, it replaces the content of the original file with an alert message describing the potential threat, and then places the original file in Quarantine.

Note: Some firewall configurations might prevent the E-mail Attachments shield from monitoring e-mail. For more information, see [“Communication errors with the E-mail Attachments shield”](#) on page 40.

 This option also blocks any e-mail attachments where a virus has been detected, if you have Webroot AntiVirus with AntiSpyware.

E-mail Attachments Shield Options... button:
Click to edit E-mail Attachments shield options.

Restoring Attachments:

Select **Ask me where to save every file** if you want to be prompted for every quarantined attachment that you want restored or select **Always save to:** to create a **default** location for restored e-mail attachments. You can enter a file location in the field or click **Select Location** to browse directories from Windows Explorer.

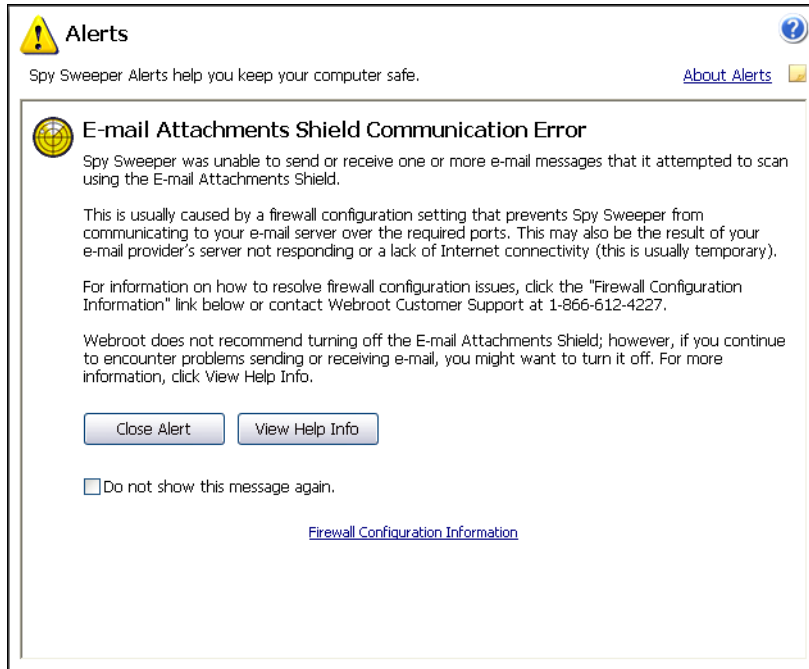
E-mail Port Settings:

Enter the POP3 port number for incoming mail and the SMTP port number for outgoing mail. The Webroot software automatically displays port numbers that most computers use for e-mail communications. If necessary, change the port numbers or contact your ISP (Internet Service Provider) for the port numbers.

Communication errors with the E-mail Attachments shield

When the E-Mail Attachments shield is turned on, the Webroot software intercepts all traffic on the POP3 and SMTP ports used for e-mail communications so it can scan attachments for spyware and viruses. By **default**, the Webroot software monitors port 110 (POP3) for incoming mail and port 25 (SMTP) for outgoing mail, but you can change the port numbers in the **E-mail Attachments** settings, if necessary.

Some firewall configurations might prevent the Webroot software from intercepting e-mail traffic. If this is the case, the following alert appears every time an e-mail is sent or received:



If this alert appears because a firewall application is blocking the Webroot software, you need to configure your firewall application to allow the program to monitor the port traffic. For more information about resolving communication issues between your firewall application and the Webroot software, you can contact Webroot Technical Support or click the following link (you must be connected to the Internet):

[Firewall Configuration Information](#)

If the alert appears only once or just periodically, the problem may be due to an inactive network configuration or a non-responsive SMTP or POP server at the ISP (Internet Service Provider). This is a temporary situation; the E-Mail Attachments shield should be able to function normally once communication is restored. If the message appears frequently when these types of communication errors occur, you can select “Do not show this message again,” so the alert only appears in the session log (see “[Viewing the session log](#)” on page 64).



4: Managing Backups

Webroot's backup function preserves your files from hard drive crashes, fire, theft, or accidental deletion. You can run backups at any time to Webroot's online [data center](#). You can also schedule automatic backups so you never need to remember to run them yourself. The backup runs in the system's background, without interrupting your computer activity. The Webroot software even backs up files that are open and in use.

To ensure the highest level of data protection during backups, the Webroot software first encrypts data with the Advanced Encryption Standard (AES). Next, it transmits the data to Webroot's high-security data centers, located in two different locations within the United States, and then encrypts the data a second time. Finally, it replicates data at both data centers. With these multiple layers of security, you can rest assured that your data can always be retrieved.

To manage backup and restore functions, you must create a backup account. This account is available from the Webroot software's Main screen or from Webroot's Web site. From this Web site, you can restore files (convenient if you are traveling) or share files with others. Your backup account is available 24 hours a day, every day of the year, and provides one gigabyte of backup storage space. If necessary, you can purchase additional storage capacity.

To manage backups and restore data, see the following topics:

- [Managing backup accounts](#).
Create a backup account with your user name and password.
- [Using online backup and restore](#).
Copy files to Webroot's data centers for safe storage. Later, you can easily recover files or share them with friends online.



Note

If you previously installed the standalone version of Webroot Secure Backup, you do not need to uninstall it from your computer. You can access your backup account from Webroot Secure Backup, as well as from Webroot AntiVirus with AntiSpyware.

Managing backup accounts

A backup account defines your user name, password, and e-mail address. To access backup and restore functions, you must log into the account using this name and password.

To manage backup accounts, see the following topics:

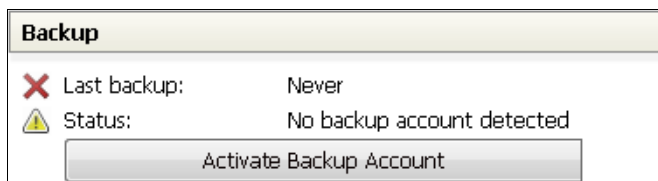
- [Activating a backup account](#)
- [Logging into a backup account](#)
- [Switching the active account](#)

Activating a backup account

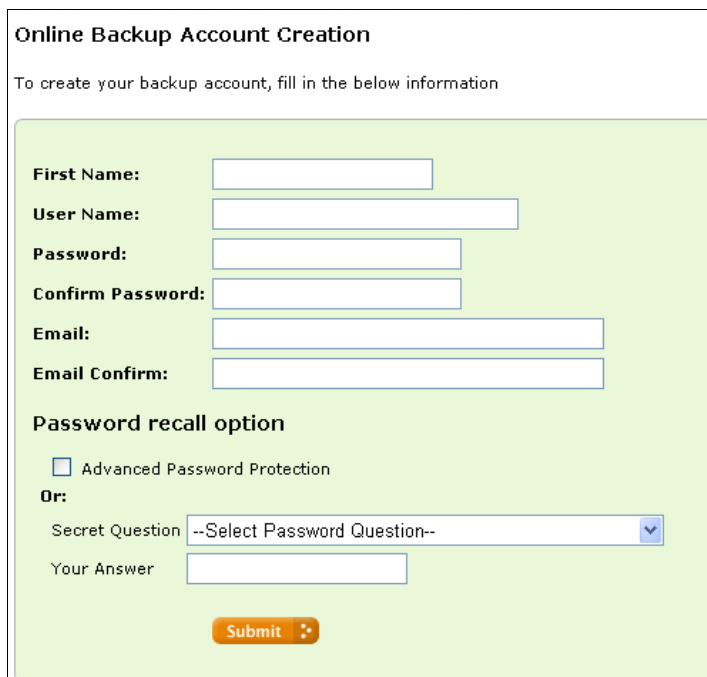
If you have not already created a backup account, you can use the Webroot software's Main screen to access Webroot's account activation. If you already created a backup account, see "[Logging into a backup account](#)" on page 44.

To create a new account:

1. Make sure you are connected to the Internet.
2. From the Main screen, click **Activate Backup Account**.



The Webroot Web site opens in your browser and displays a dialog for creating an account.

A screenshot of a web form titled "Online Backup Account Creation". The form instructs the user to "fill in the below information". It includes input fields for "First Name", "User Name", "Password", "Confirm Password", "Email", and "Email Confirm". Below these is a "Password recall option" section with a checkbox for "Advanced Password Protection" and an "Or:" section containing a "Secret Question" dropdown menu (set to "--Select Password Question--") and a "Your Answer" input field. A "Submit" button is at the bottom.

3. Enter information in the fields, as described in the following table.

Creating an online backup account	
First Name/User Name	Enter your first name and a name you will use to log into the account. The user name can be a single word from 3 to 50 characters. You may include letters from the English alphabet, numbers, a period, an underscore, an @ sign, or a dash.
Password/Confirm Password	Enter a password you will use to log into the account. The password can be a single word from 5 to 20 characters. You may include letters from the English alphabet, numbers, or these special characters: ! @ # \$ % ^ & * (). The password cannot contain a space.
Email/Email Confirm	Enter your e-mail address. Webroot will use this address for sending a password reminder (if you request it) and for allowing you to share files online with friends.
Password recall option	To allow Webroot to send you a password reminder (if necessary), select a security question and enter an answer from 2 to 100 characters. The answer must begin with an English alphabet letter, then either a letter or a number for the second character. Remaining characters can be letters, numbers, or an underscore. If you do not want Webroot to have access to your password, select the Advanced Password Protection checkbox. Keep in mind that if you select this option, Webroot does not know your password and will not be able to send you a password reminder. Be sure to write down your password and store it in a safe location.

4. Click **Submit**.

The Webroot software opens a confirmation screen and creates your account in a few minutes. If desired, you can click [Check for Updates](#) on the right of the Home panel to retrieve account information immediately.

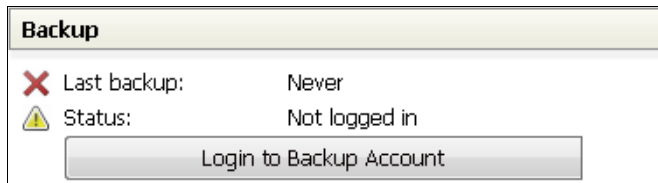
When account creation completes, the Backup panel and Backup icon are activated on the Main screen.

Logging into a backup account

Before you can use the backup and restore functions, you must log into your backup account. The backup account remains active until you shut down the computer.

To log into an account:

1. Make sure you are connected to the Internet.
2. From the Main screen, click **Login to Backup Account**.



A Backup Account dialog opens with your user name already displayed.

3. Enter your password, then click **OK**.

The Backup panel and Backup icon are then activated on the Main screen.

Switching the active account

If you previously installed the standalone version of Webroot Secure Backup, you can switch to that account from the Backup tab. Only one backup account can be active at one time.

To switch backup accounts:

1. In the Icon panel, click **Backup**.
2. Under Active User Account, click **Switch User Account**.

A Switch User Account dialog opens with your current user name already displayed.

3. Enter the new user name and password, then click **OK**.

Using online backup and restore

Online backup ensures that your important files are always kept safe and available in Webroot's storage repository, which consists of redundant data centers in different geographic areas. The backup feature also maintains your privacy. Because of the sophisticated encryption system, your archived files cannot be accessed without your user name and password.

To use online backup and restore functions, see the following topics:

- [Creating an online backup set](#)
- [Backing up data to the online repository](#)
- [Restoring data from the online repository](#)
- [Accessing your account online](#)
- [Adding more online storage](#)

Creating an online backup set

A backup set contains details of what you want copied and when you want the backup to occur. You must create a backup set before running a backup.

To create an online backup set:

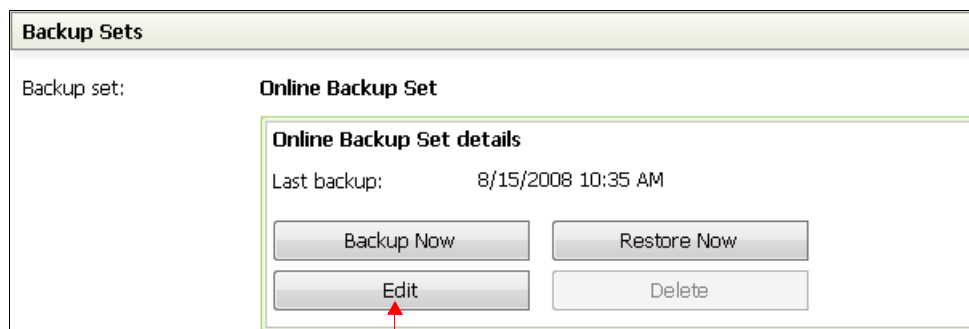
1. Make sure you are connected to the Internet and logged into your backup account.
2. In the Icon panel, click **Backup**.

The Backup panel opens.

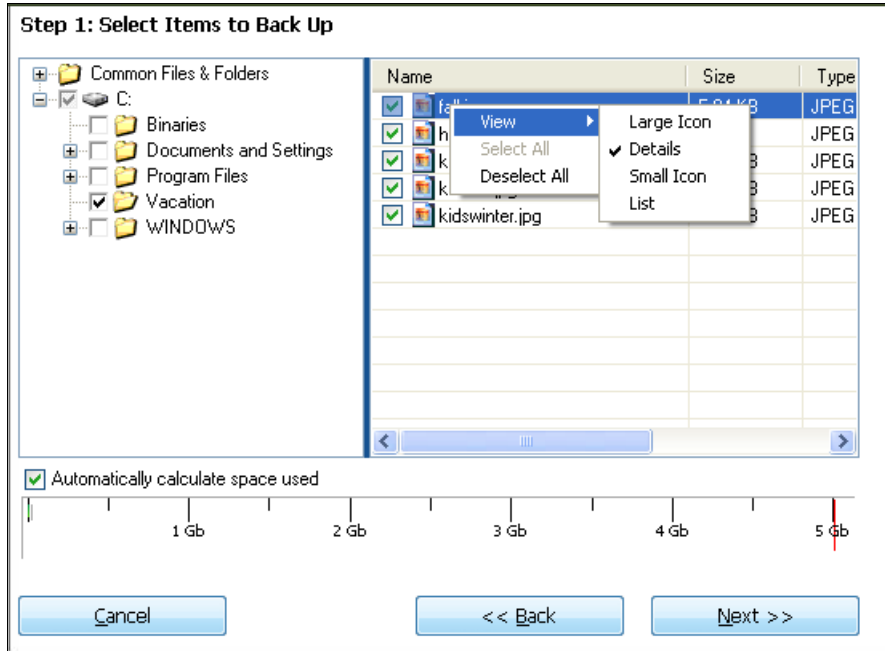
Note

If the Backup icon is grayed out, you must create a backup account and log in (see [“Managing backup accounts”](#) on page 42).

3. From the Backup Sets panel, click **Edit**.



The Online Backup setup wizard opens.



4. Enter your backup settings in each screen, as described in the following table. Click **Next** or **Back** to move between the screens.

Editing an online backup set	
Step 1: Select Items to Back Up	<p>Select the individual drives, folders, and files you want to include in the data set. We recommend that you back up any files that you consider irreplaceable (digital photos, financial records, and so on). Items with unchecked boxes will not be backed up.</p> <p>You can see the contents of folders by clicking the plus sign to the left of the folder name. You can also right-click in the list of files (as shown above) to see the files in different views.</p> <p>Once you select items, the Webroot software calculates the capacity (if Automatically calculate space used is checked). If you exceed the account's storage allotment, you must choose a lesser amount or purchase more storage (see "Adding more online storage" on page 50).</p>
Step 2: Schedule Automatic Backups	<p>If you want to create an automatic backup schedule, select a frequency, time, and interval.</p> <p>To ensure that this backup runs even if you are logged out, select the Run backups even when Windows user is not logged on checkbox at the bottom (however, the computer must still be turned on for backups to run). If you do <i>not</i> want to schedule automatic backups, de-select the Schedule this backup to run automatically checkbox at the top.</p>
Step 3: Other Backup Options	<p>If you want reports sent to your e-mail address when a scheduled backup is finished, select the Send email reports... checkbox and enter your e-mail address. Also make sure that the Internet connection speed (Dial-up, DSL/Cable, or Corporate LAN) reflects your current connection type.</p>
Step 4: Summary	<p>Review your backup set selections. If necessary, return to previous screens by clicking Back.</p>

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

The wizard closes. You can run the backup by clicking **Backup Now**.



Note

You can also add a file or folder to the online backup set at any time from Windows Explorer or from your Windows Desktop. To do this, right-click on the file or folder, then select **Protect with Webroot Backup** from the pop-up menu. The file or folder is then included in the next scheduled online backup.

Backing up data to the online repository

After you create a backup set, you can copy data to the online repository. This process runs in the background and does not slow down your system.

To back up data:

1. Make sure you are connected to the Internet and logged into your backup account.
2. If you have not already done so, create a backup set (see [“Creating an online backup set”](#) on page 45).
3. Click **Backup Now** either from the Main screen or from the **Backup** tab.

A dialog window opens and shows the progress of the backup. The files are compressed first, then copied to the online repositories. The time required for the backup depends on how many files you selected, the capacity of the files, and the speed of your Internet connection.

Restoring data from the online repository

You can restore an entire data set, a specific folder, or just an individual file from the online repository. This repository is available 24 hours a day, every day of the year.

To restore data:

1. Make sure you are connected to the Internet and logged into your backup account.
2. Click **Restore Now** either from the Main screen or from the **Backup** tab.

The Restore setup wizard opens.

Step 1: Search Backup Points

To browse all files backed up, simply click Next. You can also search your online backup by date, or other filters provided below.

Search by Date

< September, 2008 >

Sun	Mon	Tue	Wed	Thu	Fri	Sat
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	1	2	3	4
5	6	7	8	9	10	11

Today: 9/4/2008

Refresh recovery data

Other Search Filters

File size:

File type:

File name (all or part):

- Enter your restore criteria in each screen, as described in the following table. Click **Next** or **Back** to move between the screens.

Restoring data from an online backup	
Step 1: Search Backup Points	<p>Locate a backup set that contains files or folders you want restored. Dates shown in bold are when backups were performed. If you search by date, the Webroot software locates backups performed on or before the date you selected.</p> <p>To limit the results, you can also search by file size, file type, or a specific file name.</p>
Step 2: Select Items to Restore	<p>Select what folders or files you want recovered. (Items with unchecked boxes are not included in the recovery.)</p>
Step 3: Select Location for Recovered Files	<p>Determine where you want files recovered. You can accept Webroot's default folder or enter a new one. Specify recovery options, as follows:</p> <ul style="list-style-type: none"> To restore files to the default location, leave the Default location checkbox selected. If you want files restored to a folder other than the default location shown, select New location. Enter a new directory or click the browse button <input type="button" value="..."/> to select a new directory. If you want to save this new location as the default, be sure to select the Save this new location as my Default location checkbox. If you want to append the directory structure of the original backup to this new location, select the Include original path checkbox. For example, if the directory of the original backup was C:\mystuff\ and you specify C:\backups\ as the new location, the restore process saves data to C:\backups\mystuff\.

- When you're done, click **Finish**.

A dialog window opens and shows the progress of the recovery.

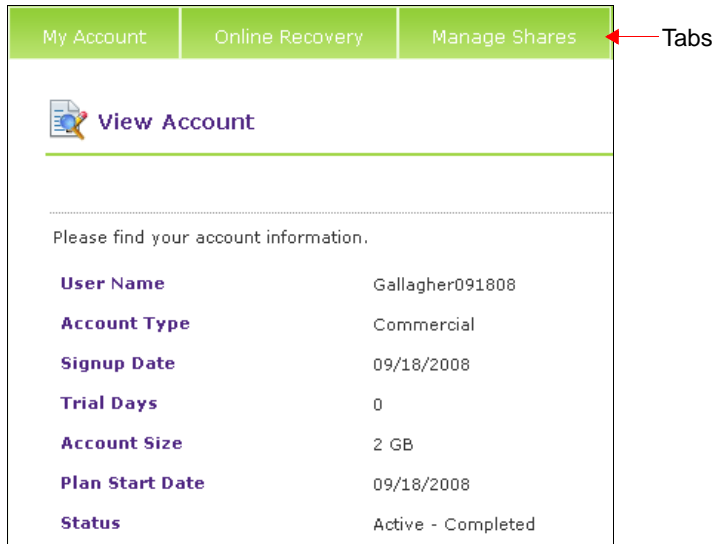
Accessing your account online


You can access your backup account from any computer with an Internet connection, so you can change account settings, retrieve files remotely, or share files with others.

To access your account remotely:

1. Open your browser and go to myaccount.webrootbackup.com, or click **Backup** in the Icon panel and then click the [Online Backup Web Access](#) link.
2. In the Login dialog, enter your user name and password. Click **Login**.

An account summary page opens, similar to the following example:



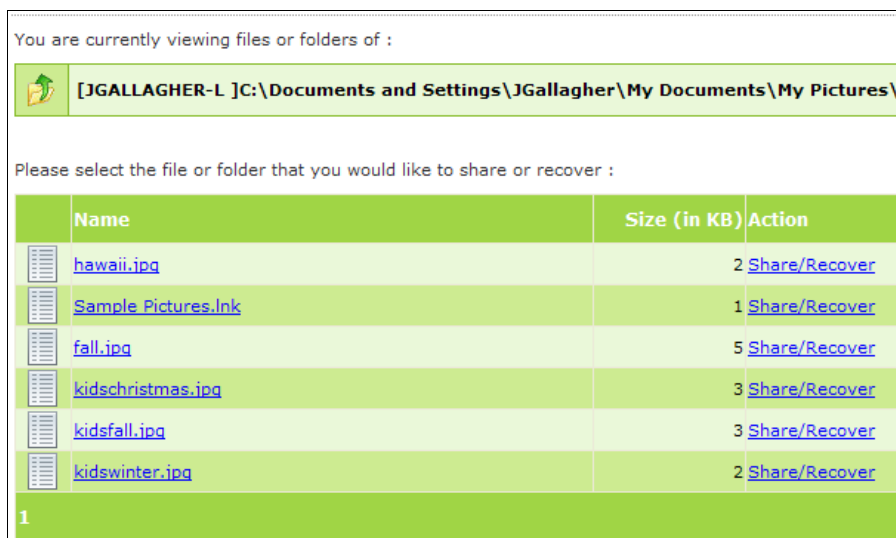
My Account	Online Recovery	Manage Shares
 View Account		
Please find your account information.		
User Name	Gallagher091808	
Account Type	Commercial	
Signup Date	09/18/2008	
Trial Days	0	
Account Size	2 GB	
Plan Start Date	09/18/2008	
Status	Active - Completed	

The tabs at the top of this page allow you to manage your account, recover files, and share files.

To recover or share files remotely:

1. From the top panel, select **Online Recovery > Recover**.
2. Follow the on-screen instructions to select the computer, drive, and the desired files.







Recovery screens look similar to the example below.



You are currently viewing files or folders of :

[JGALLAGHER-L] C:\Documents and Settings\JGallagher\My Documents\My Pictures\

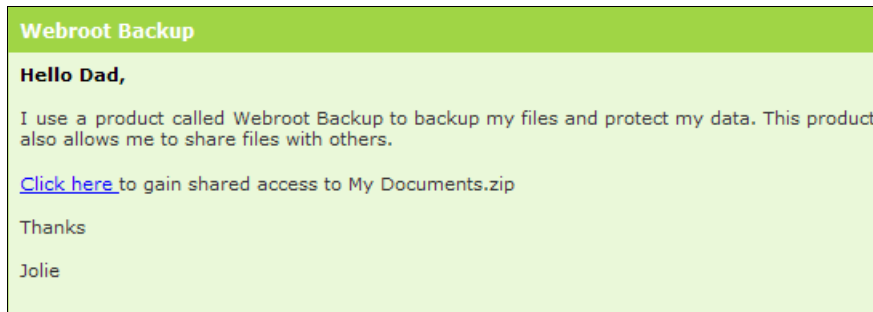
Please select the file or folder that you would like to share or recover :

Name	Size (in KB)	Action
 hawaii.jpg	2	Share/Recover
 Sample Pictures.lnk	1	Share/Recover
 fall.jpg	5	Share/Recover
 kidschristmas.jpg	3	Share/Recover
 kidsfall.jpg	3	Share/Recover
 kidswinter.jpg	2	Share/Recover

1

3. If you want to share files with friends, click the [Share](#) link in the Action column. Another screen opens where you can enter your friend's name, e-mail address, and a message. To send the e-mail with a link to your share, click the **Share** button.

The e-mail your friend receives looks similar to the example below.



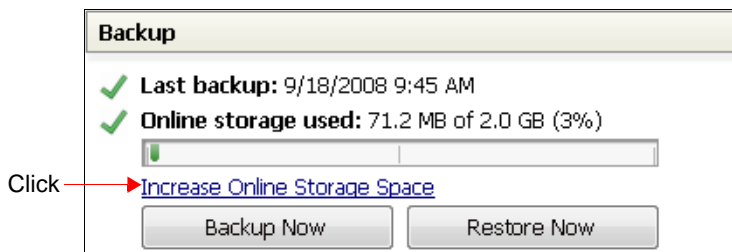
4. To remove a shared file or directory, select **Manage Shares > View Shares**, and click the [Unshare](#) link.

Adding more online storage

Your account includes one gigabyte of backup storage space. If desired, you can use a credit card to purchase additional storage capacity in the following levels: 2, 5, 10, 25, and 50 gigabytes.

To add more storage space:

1. Make sure you are connected to the Internet and logged into your backup account.
2. From the Main screen, click [Increase Online Storage Space](#).



The Webroot upgrade site opens in your browser.

3. Follow the on-screen instructions for purchasing more storage.
4. Click **Submit**.



5: Setting Options

The Webroot software includes options that allow you to control sweep settings, shield settings, and other items related to program activity.

To set Webroot software options, see the following topics:

- [Viewing and setting sweep options.](#)
Review preconfigured sweep settings (the areas it searches and the types of threats it detects) and change settings for a Custom sweep.
- [Setting shield options.](#)
Change options that affect how shields block threats.
- [Managing detected items automatically.](#)
Determine how you want the sweeps and shields to manage items that are frequently detected (block or ignore).
- [Managing automatic updates.](#)
Change the interval at which the Webroot software checks for program updates and new security definitions.
- [Setting program options.](#)
Change some options that affect the Webroot software's operation, such as whether it loads when you start your computer.
- [Viewing the session log.](#)
View activity for sweeps, shields, updates, and any errors that may have occurred.

Viewing and setting sweep options

Before running a sweep, you should review what options are currently set for each sweep type: [Full Sweep](#), [Quick Sweep](#), and [Custom Sweep](#).

See the following topics:

- [Reviewing options for Full and Quick sweeps](#)
- [Configuring Custom sweep options](#)

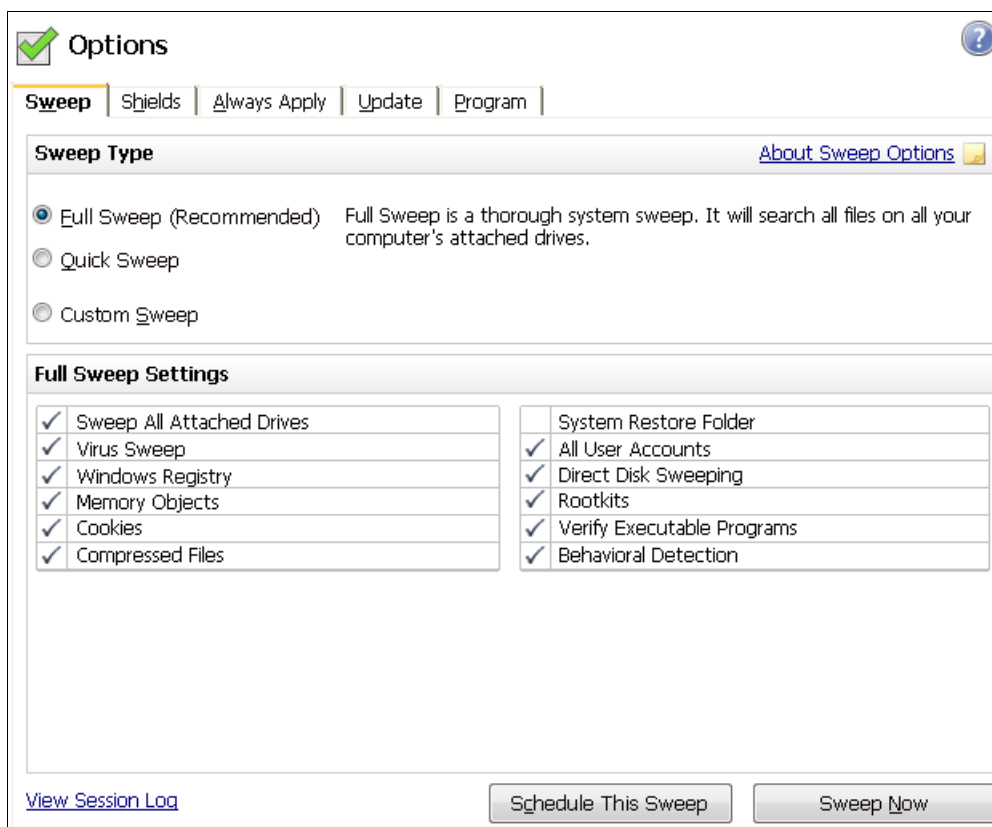
Reviewing options for Full and Quick sweeps

The Webroot software includes pre-set options for a [Full Sweep](#) and a [Quick Sweep](#). You cannot change these options. To run a sweep with modified settings, you must run a [Custom Sweep](#) (see “[Configuring Custom sweep options](#)” on page 54).



To review option settings for Full and Quick Sweeps:

1. In the Icon panel, click **Options**.
2. Make sure the **Sweep** tab is selected.
3. Under **Sweep Type**, select either **Full Sweep** or **Quick Sweep**.

In the lower panel, a check mark appears next to each option that is currently enabled for the selected sweep type.



The following table describes each option.

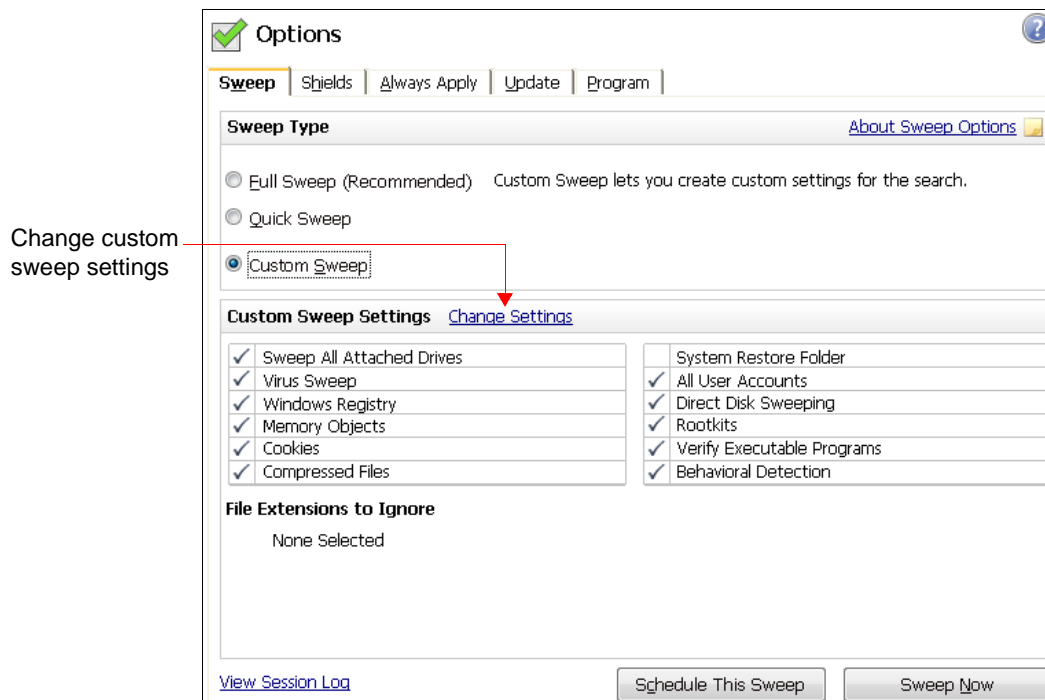
Sweep Options	
Sweep All Attached Drives	Sweeps all drives attached to your computer (such as a CD-RW drive), as well as the internal drives.
Virus Sweep	 <i>Applies only to Webroot AntiVirus with AntiSpyware.</i> Performs virus-sweeping in the following areas: Memory Objects, Compressed Files, System Restore Folder, All User Accounts, and Direct Disk Sweeping (providing those options are also turned on).
Windows Registry	Sweeps the computer's registry , where spyware and other potentially unwanted programs commonly create entries.
Memory Objects	Sweeps the computer's random access memory (RAM) , where spyware and other potentially unwanted programs commonly load into memory.
Cookies	Sweeps for known cookies that are included in the security definitions. You can determine which ones you want to keep from Quarantine.
Compressed Files	Sweeps compressed files such as .zip, .rar, .lzh, and .cab files, where potentially unwanted programs can hide. The first time the Webroot software scans compressed files, the sweep time takes considerably longer than it would without sweeping compressed files. But after the first sweep with this option, it will skip compressed files that have not changed, thereby saving time.
System Restore Folder	<i>Applies only to Windows XP.</i> Sweeps the folder where Windows saves system restore files. If a restore point contains a potentially unwanted program, the Webroot software finds it and lets you remove it. After removing the unwanted program, you can still use that restore point in the future.
All User Accounts	Sweeps registry entries for all user accounts or login IDs on your computer.
Direct Disk Sweeping	Searches for strains of spyware that hide themselves from the Windows operating system.
Rootkits	Sweeps for rootkits. A rootkit is a software tool that an attacker can use to maintain access to your computer for malicious purposes.
Verify Executable Programs	Performs a thorough analysis of executable programs by running them in a protected memory area. This is an advanced detection technique that may lead to longer scan times.
Behavioral Detection	 <i>Applies only to Webroot AntiVirus with AntiSpyware.</i> Initiates Behavioral Detection , which analyzes programs for behavior typical of malware before its code can execute.

Configuring Custom sweep options

You can change **Custom Sweep** settings to customize where the program looks for suspicious items and what types of items the program scans.

To configure options for a Custom Sweep:

1. In the Icon panel, click **Options**.
2. Make sure the **Sweep** tab is selected.
3. Under **Sweep Type**, select **Custom Sweep**.
4. Click the [Change Settings](#) link.



The Custom Sweep window opens, with a panel in the middle that provides four buttons for selecting custom options: Where to Sweep, What to Sweep, Skip File Types, and Advanced Options. You can select any button, in any order.



5. In the Where to Sweep panel, you can exclude certain drives, directories, or folders from the sweep by deselecting them (click the checkbox to remove the green check mark next to each folder or file). Typically, most spyware and other threats install on the C: drive, but you should sweep all drives periodically.



Virus protection

If you have Webroot AntiVirus with AntiSpyware, you should sweep all drives regularly. Webroot AntiVirus with AntiSpyware can sweep all internal drives for viruses. Viruses can be found in all types of files and in any location.

6. In the What to Sweep panel, you can select options as described in the following table. (Items with a check mark are enabled. Click in the box to deselect or select options.)

What to Sweep (Custom options)	
Sweep for Viruses	 <i>Applies only to Webroot AntiVirus with AntiSpyware.</i> Enables virus sweeping in the following areas: Memory Objects, Sweep All User Accounts, Compressed Files, System Restore Folder, and Direct Disk Sweeping (providing those options are also turned on).
Automatically quarantine viruses detected during sweep	 <i>Applies only to Webroot AntiVirus with AntiSpyware.</i> After performing virus cleaning , it places files in Quarantine that contain a virus and lists them on the Quarantine panel during the sweep process.
Windows registry	Sweeps the computer's registry , where spyware and other potentially unwanted programs commonly create entries.
Memory objects	Sweeps the computer's random access memory (RAM) , where spyware and other potentially unwanted programs commonly load into memory.
Cookies	Sweeps for known cookies that are included in the security definitions.
Sweep all user accounts	Sweeps registry entries for all user accounts or login IDs on your computer. If this option is turned off, the Webroot software only sweeps the registry entries for the current user account.
Compressed files	<p>Sweeps compressed files such as .zip, .rar, .lzh, and .cab files, where potentially unwanted programs can hide. You may want to use this option after you have found spyware programs and you want to be sure that you have removed them.</p> <p>Enabling this option increases sweep time significantly. (After the first sweep with this option, the Webroot software will skip compressed files that have not changed, thereby saving time.)</p> <p>If you download a compressed file in the future, you can run a sweep on just that file from Windows Explorer to save time. For more information, see the instructions for setting the Add "Sweep" option to Windows Explorer context menu on page 63.</p>
System Restore folder	<i>Applies only to Windows XP.</i> Sweeps the folder where Windows saves system restore files. If a restore point contains a potentially unwanted program, the Webroot software finds it and lets you remove it. After removing the unwanted program, you can still use that restore point in the future.




- In the Skip File Types panel, you can specify the file types for the Webroot software to ignore during a sweep. Enter the file extension and click **Add to Skip List**. For multiple entries, use a comma or semicolon to separate entries (for example: .mp3,.wma).



Note

Do not skip .dll, .exe, or .com file types, because spyware and other potentially unwanted programs typically hide in them. Be very careful when determining file types to skip. Threats can hide in any type of file.

- In the Advanced Options panel, you can select additional sweep options, as described in the following table.

Advanced Options (Custom Options)	
Enable Direct Disk Sweeping including Rootkit detection	Searches for strains of malware that hide themselves from the Windows operating system, including rootkit files. Keep this option selected, unless sweeps do not complete. Some computers need to turn off this option for sweeps to run completely.
Sweep for masked files	Sweeps for items hidden from the operating system.  When this option is selected, the time required for the sweep will double. Use this option only if you are particularly concerned about your computer's security or continue to see unwanted advertising after running a full system sweep. Otherwise, turn off this option for quicker sweeps.
Analyze executable programs in a protected memory space	Performs a thorough analysis of executable programs by running them in a protected memory area. This is an advanced detection technique that may lead to longer scan times.
Enable behavioral detection	 <i>Applies only to Webroot AntiVirus with AntiSpyware.</i> Enables Behavioral Detection , which analyzes programs for behavior typical of malware before its code can execute.
Automatically quarantine behavioral detections	 <i>Applies only to Webroot AntiVirus with AntiSpyware.</i> Places any items found with the Behavioral Detection feature in Quarantine.
Sweep Speed vs. Processor Usage	Allows you to provide more processing power to other programs as sweeps are running. To do this, move the slider (click with your mouse and drag) toward "Conserve processing power" at the left. This setting slows the sweep process, but provides more processing power for other programs. For the fastest sweeps, leave the slider all the way to the right.

- When you are finished selecting options, click **OK**.

Your Custom Sweep settings are automatically saved and are used any time you select Custom Sweep as your sweep type.

Setting shield options

To configure shield options, see the following topics:

- [Setting antivirus protection](#). Blocks viruses in some of the shield types.
- [Setting behavioral detection](#). Blocks potential threats based on the item's behavior.
- [Changing the shield alert method](#). Determines how shield alerts open.
- [Setting Gamer mode options](#). Determines if the Execution shield turns off when Gamer mode is enabled.

Setting antivirus protection

When Antivirus Protection is turned on, the following shields also block viruses:

- Browser Helper Object shield (see [page 29](#))
- ActiveX shield (see [page 34](#))
- Alternate Data Stream shield (see [page 34](#))
- System Services shield (see [page 35](#))
- Execution shield (see [page 36](#))
- File System shield (see [page 37](#))
- Startup Items shield (see [page 38](#))
- E-mail Attachments shield (see [page 39](#))



Virus protection

Antivirus Protection is available only in the Webroot AntiVirus with AntiSpyware version.

To set Antivirus Protection:

1. In the Icon panel, click **Options**.
2. Click the **Shields** tab.
3. Select the **Protect against viruses** option to enable virus-blocking in the shields listed above.

Setting behavioral detection

Behavior detection is a method of identifying emerging threats, based on suspicious behavior that is typical of malware programs. When this option is turned on, shields will block new threats that may not yet be listed in the security **definitions**. However, be aware that on very rare occasions, this detection method could classify a legitimate program as malicious because it shows malware-like behavior.



Virus protection

The Behavioral Detection option is available only in the Webroot AntiVirus with AntiSpyware version.

To set Behavioral Protection:

1. In the Icon panel, click **Options**.
2. Click the **Shields** tab.
3. Select **Enable behavioral detection**.
4. Select **Automatically quarantine behavioral detection** to move any found items into Quarantine.

Changing the shield alert method

When the Webroot software detects activity related to any of the shield settings, it displays an alert. Alerts that require immediate attention always open in a separate window and cannot be changed. Alerts that do not require immediate attention open in a pop-up window from the system tray; if desired, you can change the alert method so that the program opens and shows alert details in the Alerts panel on the Home page.

To select the alert method:

1. From the Icon panel, click **Options**.
2. Click the **Shields** tab.
3. From Shield Alerts Method, select either:
 - **Show notification above system tray**: Shows a small, pop-up window above the system tray (lower-right corner of your screen) whenever the Webroot software needs to alert you to an activity that does not require immediate action. If the pop-up has a link, you can click it for more details.
 - **Open the program to show alert details**: Opens the program's Main window for most types of alerts that require additional information. (Some alerts are informational pop-ups, which still display only as a pop-up above the system tray.)

Setting Gamer mode options

For Gamer mode (silent program operation), you can control several options:

- **Turn off the Execution Shield.** When you set the program to Gamer mode, all shields will be turned off except for the Execution shield, so it can stop potentially harmful executable files from launching on your computer. If desired, you can specify that the Execution shield is turned off along with all other shields.
- **Automatically turn off Gamer Mode.** You can specify how long you want to run the program in silent mode before it automatically switches back to regular operations.

To turn off the Execution shield:

1. From the Icon panel, click **Options**.
2. Click the **Shields** tab.
3. From Gamer Mode Options, de-select the checkbox next to **Turn Execution Shield OFF when entering Gaming Mode**.

To specify how long Gamer mode runs:

1. From the Icon panel, click **Options**.
2. Click the **Shields** tab.
3. From Gamer Mode Options, make sure the checkbox next to **Automatically turn Gamer Mode OFF...** is selected. Enter the number of hours you want to use Gamer mode before it turns off and switches to regular program operations.
4. If you do not want Gamer mode to automatically switch off, deselect the checkbox.

Managing detected items automatically

You can specify how certain items are automatically handled when detected by sweeps or shields. By **default**, the Webroot software sets all items to Always Ask, which means that the program always lists the items it detects and requires you to take action on each one (or just leave them in Quarantine).



Trial Versions

If you have the Scan-Only trial version, you cannot quarantine and remove detected items. Click **Subscribe** to buy a subscription so you can remove found items.

If you repeatedly see the same items during sweeps and shielding, you can specify that these items are always ignored or always quarantined:

- **Always Quarantine.** If the same unwanted items appear during sweeps, you can specify that they are always quarantined and not listed in the Quarantine panel during a sweep. For example, you might want to quarantine certain tracking cookies that get downloaded whenever you visit a particular Web site so you don't need to always quarantine the cookies manually after every sweep. For shields, the Always Quarantine setting blocks activities related to the particular item and does not open an alert.
- **Always Ignore.** If you know some items are required for legitimate programs, you can specify that they are always ignored and not listed in the Quarantine panel during a sweep. For example, a legitimate program might need a piece of spyware that should not be removed. In this case, you can instruct the Webroot software to always bypass that spyware program during sweeps so it does not get moved. For shields, the Always Ignore setting allows activities related to the particular item and does not open an alert.

After you specify how Webroot software manages items in the Always Apply tab, the sweep function still detects them and includes them in its count of found items and traces, but it will not include the items in the Quarantine list, which reduces the number of items you must evaluate after sweeps.



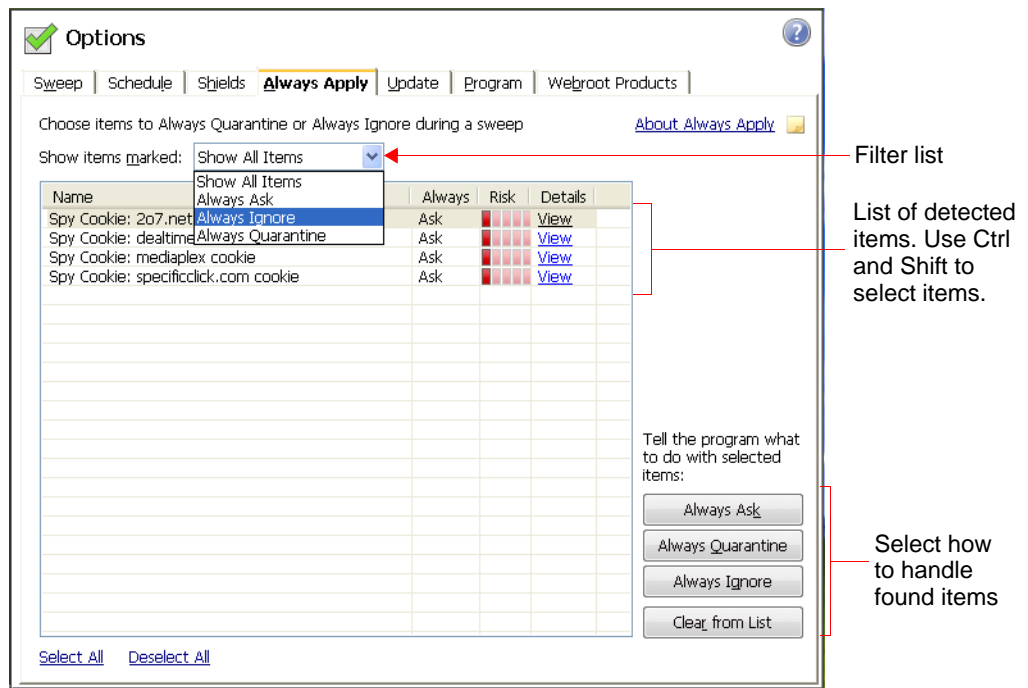
Virus protection

Detected viruses are not displayed on the Always Apply tab (applies only to Webroot AntiVirus with AntiSpyware).

To manage detected items automatically:

1. In the Icon panel, click **Options**.
2. Click the **Always Apply** tab.

The Always Apply tab opens with a list of all items found on your computer during past sweeps.



If desired, you can filter which items appear in the list by choosing one of the following options from the drop-down list:

- **Show All Items.** Displays all items found in any sweep, unless you have cleared the item from the list.
- **Always Ask.** Displays only found items that are set to Always Ask, which is the default setting.
- **Always Ignore.** Displays only found items that you have set to Always Ignore.
- **Always Quarantine.** Displays only found items that you have set to Always Quarantine.

To sort the list based on the heading, click a column head.

If you want to further reduce the number of items shown in the list, select ones that you don't plan to handle with Always Quarantine or Always Ignore and click **Clear from List**. Clearing items does not delete them; it just makes the list on the Always Apply tab shorter for you to manage. If the program finds the same item again, it will be added to the list.

3. To learn more about any item listed, click the [View](#) link. (You must be connected to the Internet to see the additional information.)

The Webroot Web site opens in your browser and displays information about the selected item to help you decide whether to ignore or quarantine the item.

4. Select each item that you want to either quarantine or ignore every time. To select more than one item, hold down the **Ctrl** key and click each item you want to include.
5. Click either **Always Quarantine** or **Always Ignore**.

Later, if you want the Webroot software to always ask about an item, you can return to the Always Ask panel, select the item again, and click **Always Ask**.

Managing automatic updates

For the highest level of protection, the Webroot software is already configured to check for program updates and new security **definitions** on a daily basis. (You must be connected to the Internet for update checks to be successful.) In addition, the Webroot software is also set to automatically download definitions, if available. If desired, you can change the interval for checking updates to hourly or you can turn off automatic checks and automatic downloads for definitions. If you decide to turn off automatic checks, make sure you remember to manually check for definition updates at least once a week. To see when you last updated them, open the Main window (Home panel) and read the Updates panel.

To check or change settings for automatic updates:

1. In the Icon panel, click **Options**.
2. Click the **Update** tab.
3. Under **Auto-Update**, you can change the following settings:
 - **Automatically check for program updates.** We recommend that you keep this option selected. If desired, you can change the interval from daily to hourly. If you deselect this option, Webroot cannot notify you of either security definition updates or program updates, nor can it automatically send updates to you (the next options are automatically disabled). You will need to check for updates manually by clicking **Check for Updates** below Update Now.
 - **Automatically download security definitions if available.** We recommend that you keep this option selected. Updates will automatically download as long as you are connected to the Internet. If you deselect this option, you must download updates manually by clicking **Check for Updates** below Update Now.



Setting program options

You can set program options that allow you to control the behavior of the Webroot software, such as whether you can run sweeps from Explorer.

To set program options:

1. In the Icon panel, click **Options**.
2. Click the **Program** tab.
3. Select the options you want to use. (Items with a green check mark are enabled. Click in the box to deselect or select options.)

Program options	
Display	
Display splash screen on program startup	Displays the splash screen whenever the Webroot software first starts.
Perform "Check Status" on startup	Automatically performs a license check when the Webroot software starts to provide up-to-date subscription information.

Program options (continued)	
Add “Sweep” option to Windows Explorer context menu	<p>Adds the Perform Security Sweep menu option to Windows Explorer. When you right-click a file or folder from Explorer, you can select this option to run a sweep at the selected location. For more information, see “Starting an on-demand sweep” on page 17.</p> <p> If this option is unavailable (dimmed), you may not have access to it (see “Using multiple accounts” on page 11).</p>
Proxy Settings	
Proxy Settings ...	<p>Allows you to enter a domain and port number for a proxy server, if you use one to connect to the Internet. Click the Proxy Settings button. Another window opens that allows you to select:</p> <ul style="list-style-type: none"> • Use Internet Explorer proxy settings • Use custom proxy settings <p>If you select Use custom proxy settings, enter the fully qualified domain name of the server (for example, <i>proxy.company.com</i>), the port number, user name, and password.</p> <p>Click OK when you have changed the setting.</p>
Other Options	
Load the program at Windows startup	<p>Starts the Webroot software whenever you start Windows, so it is always protecting your computer. We recommend keeping this option enabled. If you deselect this option, but have a scheduled sweep set to When I Log On, the Webroot software still loads with Windows.</p> <p> If this option is unavailable (dimmed), you may not have access to it (see “Using multiple accounts” on page 11).</p>
Enable password protection	<p>Lets you create a password to protect access to the following areas: Options, Shields, Alerts, and Quarantine panels, and shut down. The Webroot software remembers your password as long as you are actively using the program. After five minutes of inactivity or after you minimize the program, it will ask for the password again.</p> <p>To enable a password, click this option. A window appears where you can enter the password and confirm it. Be sure to remember your password when using the program.</p>
Report Potential Threat	
Report Potential Threat	<p>Lets you help the Webroot Threat Research team identify new spyware and viruses. If you encounter something that you suspect is a potential threat, click Report Potential Threat. See “Reporting potential threats” on page 72 for more information.</p>
Run Setup Wizard	
Run Setup Wizard	<p>Opens the Setup wizard, which allows you to configure some key tasks in the Webroot software.</p>

Viewing the session log

The session log shows all Webroot software activity for sweeps, shields, updates, and any errors that may have occurred.

To view the session log:

1. In the Icon panel, click **Options**.
2. Click the **Sweep** tab.
3. Click the [View Session Log](#) link at the bottom of the panel.

A Session Log panel opens and shows all activity related to Webroot software operations. By **default**, the Webroot software shows the last 20 log sessions, but you can modify that amount by changing the value at the top, right of the panel.

If you want to save log activity to a file, click **Save to File** and enter a log name.

You can clear old log activity by clicking **Clear Session Log**.



6: Creating Scheduled Events

The Webroot software allows you to create scheduled events, such as automatic sweeps, so you don't need to run them manually. Scheduled events can run at intervals, such as monthly or weekly, or at any time and day you specify.

To create scheduled events, see the following topics:

- [Scheduling sweeps.](#)
Run sweeps automatically to scan your computer for spyware and other unwanted items.
- [Scheduling backups.](#)
Run backups automatically to preserve your files in a safe location.
- [Managing scheduled events.](#)
Edit or delete schedules for automatic events, such as sweeps.

Scheduling sweeps

You can schedule sweeps to run automatically. The sweep function scans your computer's drives, the Windows [registry](#), memory, and other places where spyware and potential threats can hide. We recommend that you run a Full sweep once a week. For more details, see [Chapter 2, "Sweeping your System"](#) on page 15.

The Webroot software does not need to be open in the system tray for a scheduled sweep to run; however, the computer must be turned on.

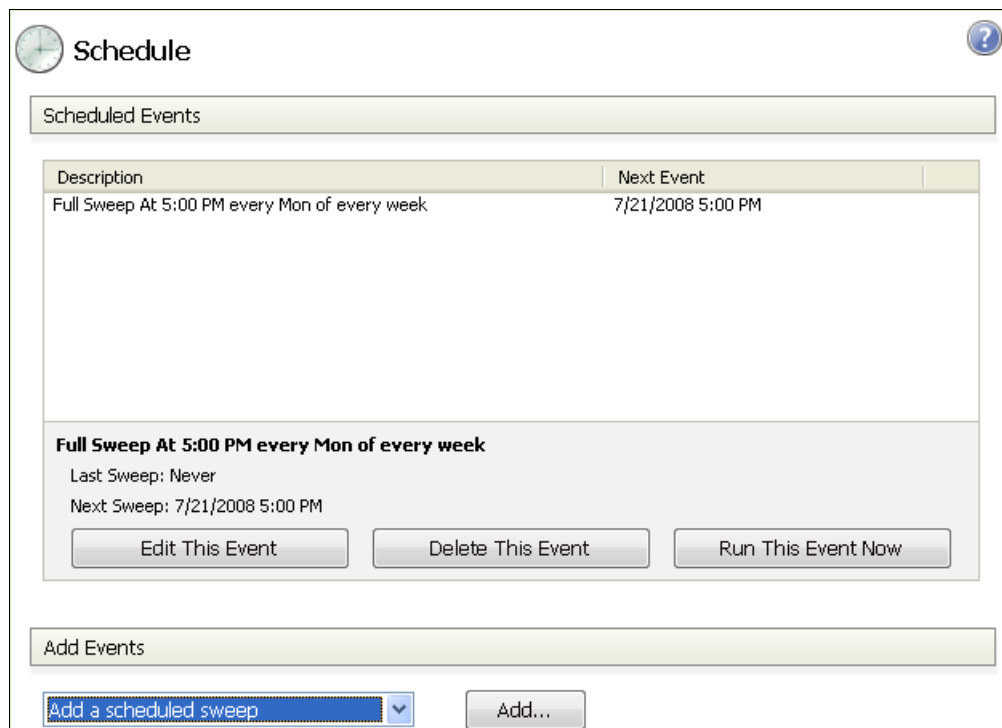
Note

If your computer is configured for multiple user accounts (each person logs in with a unique name and password, as described in ["Using multiple accounts"](#) on page 11), users can schedule their own sweeps. To run your own scheduled sweep and to view the results, you must be logged into the user account where you created the schedule.

To schedule sweeps:

1. From the Icon panel, click **Schedule**.

The Schedule window opens.



2. Under **Add Events**, select "Add a scheduled sweep" from the drop-down box and click **Add**.

The Schedule Wizard window opens.

3. Select the type of sweep you want to schedule and click **Next**:
 - **Full Sweep**. If you select this type of sweep, a Schedule Wizard panel opens for entering the desired frequency and times (continue with **step 4** below).
 - **Quick Sweep**. If you select this type of sweep, a Schedule Wizard panel opens for entering the desired frequency and times (continue with **step 4** below).
 - **Custom Sweep**. If you select this type of sweep, there are several panels for entering custom options. Click **Next** after entering information for each panel; click **Back** if you want to return to a previous panel and change the options. (You can create multiple custom sweep schedules, each with different sweep settings.)

Custom sweep panels	
Where to Sweep	If desired, you can exclude certain drives, directories, or folders from the sweep by deselecting them (click the checkbox to remove the green check mark next to each folder or file). Typically, spyware and other threats install on the C: drive, but you should sweep all drives periodically.
What to Sweep	Select the areas where you want to sweep for threats. For more information, see the What to Sweep (Custom options) table on page 55 .
Skip File Types	If there are any file types that you would like to skip during the sweep, enter the file extension and click Add to Skip List . For multiple entries, use a comma or semicolon to separate entries. Do not skip .dll, .exe, or .com file types; spyware typically hides in these types of files.
Advanced Options	Select the advanced options that you want to set. For more information, see the Advanced Options (Custom Options) table on page 56 .

4. Select an interval for the sweep (based on time or when you log onto the computer), then click **Finish**.

The Schedule panel opens and shows your scheduled sweep. If desired, you can repeat the previous steps to add another scheduled sweep.

To change a scheduled sweep, select it and click **Edit This Event**. To delete a scheduled sweep, select it and click **Delete This Event**.

If desired, you can run one of the scheduled sweeps now by selecting it and clicking **Run This Event Now**. If a potential threat is detected, see [“Reviewing and quarantining items”](#) on page 19.

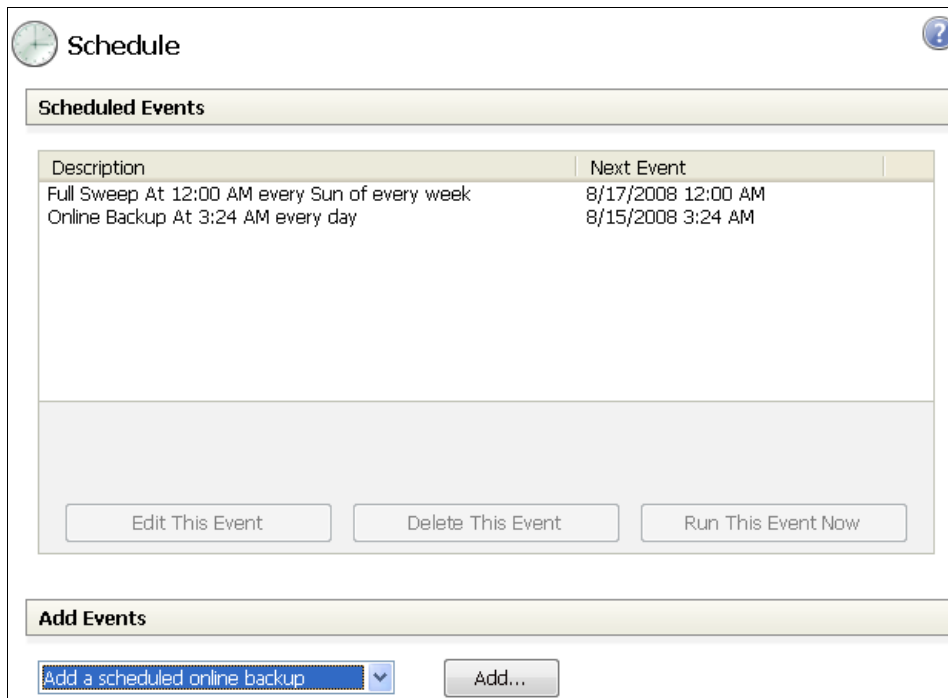
Scheduling backups

You can schedule backups to run automatically. The backup function preserves your files from hard drive crashes, fire, theft, or accidental deletion. For more details, see [Chapter 4, “Managing Backups”](#) on page 41.

To schedule backups:

1. From the Icon panel, click **Schedule**.

The Schedule window opens.



2. Under **Add Events**, select to add a scheduled backup from the drop-down box and click **Add**.

The Backup wizard opens.

3. For Backup wizard instructions, see [Chapter 4, “Managing Backups”](#) on page 41.
4. In the final wizard screen, review your backup set selections and click **Finish**.

The Schedule panel opens and shows your scheduled backup. If desired, you can repeat the previous steps to add another scheduled backup.

To change a scheduled backup, select it and click **Edit This Event**. To delete a scheduled backup, select it and click **Delete This Event**.

If desired, you can run one of the scheduled backups now by selecting it and clicking **Run This Event Now**.

Managing scheduled events

You can edit, delete, or run a schedule event at any time.

To manage scheduled events:

1. From the Icon panel, click **Schedule**.
The Schedule panel opens.
2. Click on a scheduled event.
3. Select one of the following:
 - **Edit This Event:** Opens the schedule wizard, where you can make changes.
 - **Delete This Event:** Removes the event from the schedule.
 - **Run This Event Now:** Initiates the event immediately.



A: Webroot Support

You can contact Webroot through our Web site for:

- **Requesting Technical Support.**
Submit an online trouble ticket.
- **Accessing the Knowledge Base.**
Read articles that describe common issues and resolutions.
- **Reporting potential threats.**
Report suspicious items to the Webroot Threat Research Center.
- **Joining the WARN program.**
Help fight emerging threats by participating in Webroot Automated Research Network (WARN).

Requesting Technical Support

Technical support is available from the Webroot Web site. Submit a trouble ticket to our service representatives at:

www.webroot.com/support



Note

If clicking the link above does not open your browser and take you to the Webroot Support page, copy the text of the link and paste it into your browser.

We make every effort to respond to your request on the same day you send it in, but please allow up to 48 hours.

Accessing the Knowledge Base

The Webroot Knowledge Base contains many articles that describe common issues and resolutions for Webroot software operations. These articles are constantly updated, expanded, and refined by Webroot support professionals to ensure that you have access to the very latest information.

To access this database, visit the Support Center at:

support.webroot.com



Note

If clicking the link above does not open your browser and take you to the Support Center, copy the text of the link and paste it into your browser.

Reporting potential threats

If you believe that the Webroot software is not finding something you suspect is spyware, adware, a virus, or a potentially unwanted program that you have on your computer, you can report it to the Webroot Threat Research Center. Webroot follows up on all reports to determine if it should add to its definitions.



Trial Versions

If you have a trial version, you cannot report potential threats.

To report spyware or viruses:

1. Make sure you are connected to the Internet.
2. In the Icon panel, click **Options**.
3. Click the **Program** tab.
4. Click **Report Potential Threat**.

The Report Potential Threat window opens. You can use this window to enter information about any problems you believe are related to spyware, adware, or viruses. In addition to your comments, the program will send a log that contains information about the items found on your computer.

5. Enter your e-mail address in the first field. If you do not want Webroot to contact you about the problem, de-select the checkbox under the e-mail field.
6. Enter a description of the problem in the Comments field.
7. Click **Send Report**.

When the data has been transmitted successfully, a confirmation screen appears.

Joining the WARN program

The Webroot Automated Research Network (WARN) is a global community of individuals and businesses who provide Webroot with sample items detected on their computers to help us identify and fight emerging threats. When you join WARN, the software gathers information during sweeps and shielding activities, including spyware, viruses, and potential threats that are not yet classified, then sends the data to Webroot.



Note

The Webroot software does not gather personal information. Your participation is completely anonymous.

After you installed the software, the Webroot Setup wizard prompted you to join the WARN program. You can return to that Setup wizard and change your selection.

To join or opt-out of the WARN program:

1. In the Icon panel, click **Options**.
2. Click the **Program** tab.
3. Click **Run Setup Wizard**.
4. Follow the on-screen instructions to join the WARN program.
5. Click **Next** until you see the final Setup Complete screen, then click **Finish**.



Glossary

ActiveX

Developed by Microsoft, ActiveX technology is a group of functions allowing programs to share information. Many legitimate programs use ActiveX, but some spyware programs also use ActiveX to install themselves.

adware

Adware is a type of software that may display advertisements on your system. Some adware may also hijack Web searches, meaning it may reroute your Web searches through its own Web page. It may change your default home page to a specific Web site. Adware generally propagates itself using dialog boxes, various social engineering methods, or through scripting errors. Adware and BHOs are often bundled with various free software programs, such as clocks, messengers, alerts, and software such as screensavers, cartoon cursors, backgrounds, sounds, etc. Removing adware bundled with free software programs may cause the software to stop operating. These adware programs may also cause slowing of your Web browser and system performance issues.

Alternate Data Stream (ADS)

An Alternate Data Stream is a highly technical way to hide images, data, or code in a file and can be used to hide malicious code. The hidden content is impossible to detect using regularly available tools, such as Windows Explorer.

API

Application Program Interface. API is a language and message format used by an application program to communicate with the operating system, a program, or a communications protocol. The Windows API, also called WinAPI, is the core set of APIs available in the Microsoft Windows operating systems.

applications

An application is a set of files that work together to make a software program. Some applications, like Internet Explorer, access the Internet and allow traffic to flow in and out of your computer.

Behavioral Detection

Additional protection against programs that may not match a threat definition, but exhibit behavior typical of malware. The Webroot software stops the program from executing before it can cause damage. This option can locate many emerging threats, but on very rare occasions, a legitimate program could be classified as malicious because it shows malware-like behavior.

Browser Helper Objects (BHOs)

Browser Helper Objects are add-on programs that work with your browser. Some spyware programs add BHOs without your knowledge.

cache

A temporary storage area where data that you access frequently can be stored for rapid retrieval.

certificate

A digital certificate identifies an entity and verifies its credentials so that information it sends can be trusted. Certificates are issued by a Certificate Authority (CA), who attest that the public key contained in the certificate belongs to the person, organization, server, or other entity noted in the certificate.

child process

A computer process that is linked to a parent process and inherits most of the parent's attributes. Malware writers can sometimes create a child process and attach it to a legitimate parent application. For example, Internet Explorer is used quite often by malicious processes to circumvent security. Since Internet Explorer is usually "allowed" in security products, a malicious process can spawn a child process and instruct it to perform some malicious task.

cookies

Cookies are small files that are generated by a Web server and stored on your computer for future access. When you visit some Web sites, a cookie may be placed on your system to track your personal preferences and Web surfing habits through uniquely identifiable information (browsing habits, usernames and passwords, areas of interest, etc.). Some cookies may just track which ads the site displayed while you were there to make sure the site does not display the same ads. Other cookies may store preferences that you set, passwords you create for the site, and information about the pages you visited. Some cookies can be helpful, because they contain user names and passwords that let you log in to a Web site automatically or contain preferences you set for a Web site.

CPU

Central Processing Unit. The CPU performs the computer processing and is usually contained on a single chip. A complete computer system is comprised of the CPU, clock, main memory, operating system, storage devices, and other controls.

Custom Sweep

A Custom Sweep lets you select options to meet your needs. The Webroot software saves your custom sweep settings and uses them as the basis for any scheduled custom sweep that you configure.

data center

A group of computer systems and associated components used to store a repository of data.

default

An option that automatically appears or is pre-selected.

definitions

A security definition is a set of fingerprints that characterize a potentially unwanted program, such as spyware or adware, or that identifies types of viruses. Webroot regularly updates these definitions to provide better protection against the latest versions of spyware and other unwanted items.

dialer

Dialers may disconnect your computer from your Internet Service Provider (ISP) and reconnect you to the Internet using an expensive toll or international phone number. Dialers can accrue significant phone charges and can run in the background, hiding their presence. They generally propagate themselves using dialog boxes, various social engineering methods, through scripting errors, or may be delivered with a Trojan horse. The Federal Trade Commission recommends that you dispute the charges with your telephone company and report the incident.

domain name

A name that identifies a Web site (for example, “webroot.com”). You can use either the domain name or an IP address to access a Web site; in most cases, the domain name and the IP address are interchangeable. Other times, a server can host several different Web sites (each with unique domain names).

executable files

An executable file contains a program that can be launched when you double-click the file name in Windows Explorer. Typically, executable files have an **.exe** file extension, but they can also have other extensions, such as **.bat** or **.com**.

filters

A filter is a set of firewall rules for what packets to allow or deny. To monitor packets, filters use a variety of screening methods, such as looking at the IP addresses, protocols, and ports that the packets are using.

Full Sweep

A thorough sweep of all internal drives and drives directly attached to your computer.

host name

The name assigned to a computer so it can be identified on the Internet or a network. Computers on the Internet are often named WWW. Computers on a network are usually single names that describe the computer, such as “accounting1.” Host names can be part of a fully qualified domain name (FQDN). For example, in “www.webroot.com,” the “www” is the host name and “webroot.com” is the domain name.

HTML

HyperText Markup Language. The method used to display content in Web pages.

IP address

An **Internet Protocol** address identifies a machine (computer or server) on the Internet. The address is a series of four numbers separated by periods (for example, 64.78.182.210). Your own computer’s IP address may be the same address during every Internet connection (called a *static IP*, used in most T1/DSL connections) or it may change for each Internet connection (called a *dynamic IP*, used in most cable/dial-up connections).

keylogger

A keylogger is a type of system monitor that has the ability to record all keystrokes on your computer. Therefore, a keylogger may monitor keystrokes, e-mails, chat room dialogue, instant message dialogue, Web sites visited, usernames, passwords, programs run, and any other typed material. They may have the ability to run in the background, hiding their

presence. Keyloggers and system monitors may be used for legitimate purposes but can also be installed by a user to record sensitive information for malicious purposes.

Someone with administrative access to your computer, such as a system administrator or someone who shares your computer, typically installs commercial system monitors. This program may be installed on the machine without your knowledge or consent, and may allow an unauthorized, third party to view potentially sensitive information.

Worst case scenario: A third party may be able to view your personal conversations and may gain access to private information such as your usernames, passwords, credit card numbers, or your Social Security number.

local drive

A drive on your computer system, such as a CD, DVD, or disk drive (hard drive), that is connected directly to the computer.

malware

Malicious software that is designed to destroy or harm your computer system, such as a virus.

netmask

The part of an IP address that identifies the host by filtering out (masking) the network address. (An IP address has two components: the host address and the network address.) Also called a *subnetmask*.

packets

Chunks of data that travel between machines on the Internet. When you send or receive data over the Internet, the Transmission Control Protocol (TCP) divides the message into manageable packets, which are efficient for routing. When the packets arrive on the receiving end, TCP reassembles the message into its original form.

parent process

A computer process that has subprocesses (or “children”) associated with it.

ports

Ports are numbers that identify the entry and exit points of your computer. Computers divide one physical port connection into thousands of virtual port connections, most of which are never used. All communications protocols have designated entrance ports to your computer. For example, traffic sent using HTTP for Web pages generally travels through port 80. Your computer’s ports are either open or closed. An open port allows any information to flow through it and can make your computer vulnerable to hackers. A closed port blocks incoming traffic.

potentially unwanted program

A potentially unwanted program is a program that may change the security or privacy state of your computer and online activities. These programs can (but do not necessarily) collect information about your online activities and send it to a third party without your knowledge or consent. A potentially unwanted program may arrive bundled with freeware or shareware, various social engineering methods, or by someone with access to your computer.

processes

A process refers to the actual running of a program module. When a computer is booted, numerous processes are started. Some are parts of the operating system, while others are applications that have been designated to run at startup. Several processes may be associated

with the same application. In Windows, you can view a list of running processes in the Task Manager (press **Ctrl-Alt-Delete**, then click **Task Manager**).

protocols

Rules that govern the way information is transmitted from one device to another. For example, the standard communications protocol for the Internet is TCP/IP and the standard protocol for local networks is Ethernet.

proxy server

A computer system or router that acts as a relay between a client and server. Proxy servers are used to help prevent an attacker from invading the private network and are often used in building a firewall.

Quarantine

A holding area for spyware, viruses, and other potentially unwanted programs found during a sweep. The quarantine process does not delete items from your computer. Rather, it keeps the items in a safe place until you decide whether to delete them permanently or restore them.

Quick Sweep

A fast sweep of only locations where potentially unwanted programs are commonly found. This type of sweep maximizes use of your computer's processing power, to make the sweep as fast as possible.

random access memory (RAM)

The main memory that acts as the computer's workspace for running programs. Spyware and other unwanted programs can steal the computer's memory resources, which can lead to system crashes, slower performance, or instability.

registry

A database of hardware and software settings about your computer's configuration, such as the types of programs that are installed. Spyware can create entries in the Windows registry, which can ultimately slow down your computer and cause problems in your system.

restore point

A copy of the computer's contents that allows you to restore your computer to a previous state.

rootkit

Rootkits use file obfuscation techniques to allow spyware and other malicious software to avoid detection and removal. Rootkits typically hide logins, processes, files and logs, and may include software to capture information from desktops or a network. A rootkit's abilities to hide the presence of an intruder and the intruder's actions explain the increase in use of this method.

signed service

A certificate from an authorized certificate verification service (such as from VeriSign), which ensures that an application, service, or driver is from a trusted source and has not been tampered with.

spyware

Spyware is a program that may either monitor your online activities or possibly install programs without your consent. Information about online activities may be subsequently sent to a third party for malicious purposes without your knowledge. Spyware may arrive bundled

with freeware or shareware, through e-mail or instant messenger, may propagate itself using dialog boxes, various social engineering methods, scripting errors, or by someone with access to your computer. Spyware is difficult to detect, and difficult (if not impossible) for the average user to remove without the use of a top-quality antispymware program.

system monitors

System monitors, typically non-commercial, may monitor and capture your computer activity, including recording all keystrokes, e-mails, chat room dialogue, instant message dialogue, Web sites visited, usernames, passwords, and programs run. This type of program may be capable of taking screen shots of your desktop at scheduled intervals and storing the information on your computer in an encrypted log file for later retrieval. These log files may be sent to a pre-defined e-mail address. A system monitor can run in the background, hiding its presence. These programs typically install via other threats, such as music downloads and Trojan downloaders. These system monitors may allow an unauthorized, third party to view potentially sensitive information, such as passwords, e-mail, and chat room conversation.

threads

A thread represents a single process in a multitasking application, allowing that application to split itself into two or more tasks running simultaneously.

traces

Individual elements that make up the security definition database. The more traces found and put into the definitions, the more complete the removal of the potential threats.

training mode

A firewall function that analyzes the normal activities of your computer's applications and processes. The firewall uses this training period as a baseline, so that later, it can more easily determine what activities deviate from normal. (If you do *not* enable a training period, numerous alerts may display for all Internet applications and WinAPI processes as they launch, which may require you to take action by selecting "allow" or "block" each time one of these events first occurs.)

Trojan horses

A Trojan horse may take control of your computer files by using a program manager that allows a hacker to install, execute, open, or close programs. The hacker can gain remote control of your cursor and keyboard and can even send mass e-mails from your infected computer. It can run in the background, hiding its presence. A Trojan is usually disguised as a harmless software program and may also be distributed as an e-mail attachment. Opening the program or attachment may cause an auto-installation process that loads the downloader onto your computer and download third-party programs on your computer, resulting in the installation of unwanted programs without your knowledge or consent, and jeopardizing your privacy. Trojans can also open a port on your computer that enable a hacker to gain remote control of your computer.

virus cleaning

A procedure that removes infected portions of a file, when a virus is detected during a sweep. If the Webroot software can remove the virus successfully, it restores the cleaned file to your computer in its original location and places a copy of the corrupted file in Quarantine. The cleaned file is safe to use; the file in Quarantine is not safe to use.

URL

Uniform Resource Locator. The URL is the unique address for a file that is accessible on the Internet. To access the home page of a Web site, you can enter the URL of the home page (for example: `http://www.webroot.com`) in the browser's address line. You can also access specific files using URLs (for example: `ftp://www.webroot.com/sample.txt`). The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname for a specific file.

viruses

A virus is a self-replicating program that can infest computer code, documents, or applications. While some viruses are purposefully malignant, others are more of a nuisance, replicating uncontrollably and inhibiting system performance.



Index

A

- accounts 42
 - activating a backup account 42
 - switching the account 44
- ActiveX shield 34
- Additional Tools download 21
- administrative privileges 11
- advertising, blocking 32
- alerts 14
 - changing display method 58
 - disabling for gaming 13
 - viewing in session log 64
- Alternate Data Stream Execution shield 34
- Always Apply tab 60
- Always Ignore option 60
- Always Quarantine option 60
- Antivirus Protection shield 57
- attachments, E-mail Attachments shield 39
- automatic quarantine or ignore 20
- automatic updates 62
- Auto-Update option 62

B

- backup 41
 - access to account 41
 - accessing and changing account 49
 - creating an account 42
 - creating online backup set 45
 - immediate online backup 47
 - including files from Explorer 47
 - increasing online storage 50
 - logging into an account 44
 - online backup and restore 45
 - scheduling 68
 - sharing files online 49
 - switching account 44
- behavioral detection 53
 - custom sweep setting 56
 - enabling 58
- BHOs, editing shield options 30
- Browser Helper Object shield 29

C

- categories of threats 20
- Change Settings link for sweep 54
- Check for Updates link 12
- Check Status link 11
- closing the Main window 9

- Common Ad Sites shield 32
- compressed files sweep setting 53
- cookies 3
 - found during sweep 18
 - shielding from 29
 - sweep setting 53
- Custom Sweep 16
 - changing options 54
 - running 17
- customer support 72

D

- definitions 4
 - updating 12
 - used during sweep 18
- direct disk sweep setting 56
- direct disk sweeping 53
- drives, sweeping 53

E

- E-mail Attachments shield 39
- e-mail, communications error alert 40
- errors, viewing 64
- events 65
 - backups 68
 - changing or deleting 69
 - sweeps 66
- executable programs, analyzing in protected space 56
- Execution shield 36
- Explorer, running sweeps from 18
- extensions, file system scanning 37

F

- favorites for IE, protecting 29
- File System shield 37
- firewall issues with E-mail Attachments shield 40
- Full Sweep 16
 - options for 52
 - running 17

G

- Gamer mode 13
 - turning off automatically 59
 - turning off Execution shield 59

H

- home page for IE, protecting 31
- Home panel 8

Hosts File shield 32
Hosts file, editing 33

I

Icon panel 6
IE Hijack shield 30
IE Hijack shield, editing 30
Increasing Online Storage Space link 50
Internet Communication shield 32
IP address changes, blocking 32
items detected during sweep 19

K

Knowledge Base, at Webroot Web site 72

L

Load the program at Windows startup 63
logging into a backup account 44
logs, sweeps and shield activity 64

M

Main window and panel 6
 closing 9
 Home functions 8
 icon functions 7
 opening 6
masked files, sweeping for 56
memory objects sweep setting 53
memory, program pieces swept 18
Messenger Service shield 34

N

Network shields, setting 32

O

online backup and restore 45
opening the main window 6
operating system, sweeping 53
options, program 62

P

password, setting for backup account 42
password, setting for program 63
processing power, conserving 56
program options 62
Protect with Webroot... function from Explorer 47
proxy settings 63

Q

Quarantine 23
 accessing and managing detected items 23
 automatically place items in 60
 deleting items from 24
 items displayed in panel 19
 keeping items in 23

Quarantine 23 (continued)
 moving items after sweep 20
 restoring items from 24

Quick Sweep 16
 options for 52
 running 17

R

RAM sweep setting 53
Read shield 37
registry entries 53
registry items swept 18
registry sweep setting 53
registry, protecting 35
renewing subscription 11
Report Potential Threat option 63
reporting potential threats 72
restore 41
 access files remotely 49
 immediate restore from online 47
restore point, sweeping 53
risk ratings of threats 20
rootkits, sweeping 53
Run Setup Wizard 63
running sweeps immediately 17
running the program 6

S

Scan on Read shield 37
Scan on Write shield 37
scheduling 65
 backups 68
 deleting or editing schedules 69
 sweeps 66
search page for IE, protecting 31
security settings for IE, protecting 29
server, proxy 63
session log, viewing 64
Setup Wizard 63
sharing files from online backup 49
Shield Alerts method 58
shields 27
 alerts for 14
 Antivirus Protection 57
 disabling for gaming 13
 E-mail Attachments 39
 Network 32
 Startup Programs 38
 summary 28
 Web Browser 29
 Windows System 34
shutting down the program 10
silent mode 13
Skip File Types panel 55

- splash screen, disabling 62
- spyware 3
 - managing in quarantine 23
 - reporting 72
 - shielding from downloading 27
 - sweeping for 17
 - viewing more details online 20
- starting the program 6
- starting the program from Explorer 63
- Startup Programs shield 38
- stopping program operation 10
- subscriptions 4
 - renewing 11
 - viewing status 8
- Summary panel 22
- support 72
- Sweep Speed vs. Processor Usage 56
- sweeps 15
 - adding option to Explorer 63
 - automatic ignore or quarantine 60
 - changing what to sweep 54
 - disabling for gaming 13
 - results of 18
 - running from Explorer 18
 - running immediately 17
 - scheduling 66
 - setting options 52
 - summary of 22
 - types of 16
- system restore folder sweep setting 53
- System Services shield 35
- system tray icon 6
- system tray menu 10
- system tray, changing alert method 58

T

- tabs, using 9

- technical support 72
- traces found during sweep 19
- Trial version 2

U

- updates to program 12
 - automatic 62
 - perform Check Status on startup 62
- user accounts sweep setting 53
- user accounts, using multiple 11

V

- verify executable programs 53
- version, viewing current version number 8
- viruses 3
 - automatic quarantine setting 55
 - changing automatic quarantine setting 56
 - managing in quarantine 23
 - reporting 72
 - setting sweep option 55
 - shielding from downloading 57
 - sweep option setting 53
 - sweeping for 17
 - updating program for protection 12
 - viewing more details online 20

W

- WARN program 73
- Web Browser shields, setting 29
- Webroot products 2
- Webroot Support 71
- What to Sweep panel 54
- Windows Messenger Service shield 34
- Windows Startup shield 38
- Windows System shields, setting 34
- Write shield 37

