



**User Guide
for the Identity Shield**

Copyright

Webroot SecureAnywhere User Guide for the Identity Shield

January, 2013

© 2013 Webroot Software, Inc. All rights reserved. Webroot is a registered trademark and SecureAnywhere is a trademark of Webroot Software, Inc. All other product and company names mentioned may be trademarks or registered trademarks of their respective owners.

Table of Contents

Getting Started	1
Installing the Identity Shield	2
Using the Identity Shield	5
Opening the main interface	6
Responding to alerts	8
Setting program configuration options	9
Managing Identity Protection	13
Changing shield settings	14
Managing protected applications	17
Managing protected websites	20
Disabling the shield	25
Managing Your Account	27
Viewing your account details	28
Upgrading to a threat-removal version	29
Accessing Support and Resources	33
Accessing Technical Support options	34
Accessing additional publications	35
Shutting down or uninstalling the Identity Shield	36
Glossary	37
Index	41

Getting Started

The Webroot® Identity Shield provides safe Internet browsing and data protection. As you perform online transactions, it watches for Trojans or phishing sites that try to steal personal data -- including user names, passwords, security codes, account numbers, and credit card numbers. The Identity Shield blocks any attempts to gain personal information, so you can rest assured that the details you provide on a website are always secure.

Two versions of the Identity Shield are available:

- Identity protection only. Blocks threats that try to steal information during your online activity.
- Identity protection, plus threat detection. In addition to protecting your online activity, this version scans for threats on your computer. If you want to remove the threat, you must upgrade to a full version of Webroot SecureAnywhere. See "[Upgrading to a threat-removal version](#)" on page 29.

To get started with the Identity Shield, see the following topics:

Installing the Identity Shield	2
Using the Identity Shield	5
Opening the main interface	6
Responding to alerts	8
Setting program configuration options	9

Installing the Identity Shield

You can install the Identity Shield on a PC with one of the following operating systems and browsers:

Operating systems:

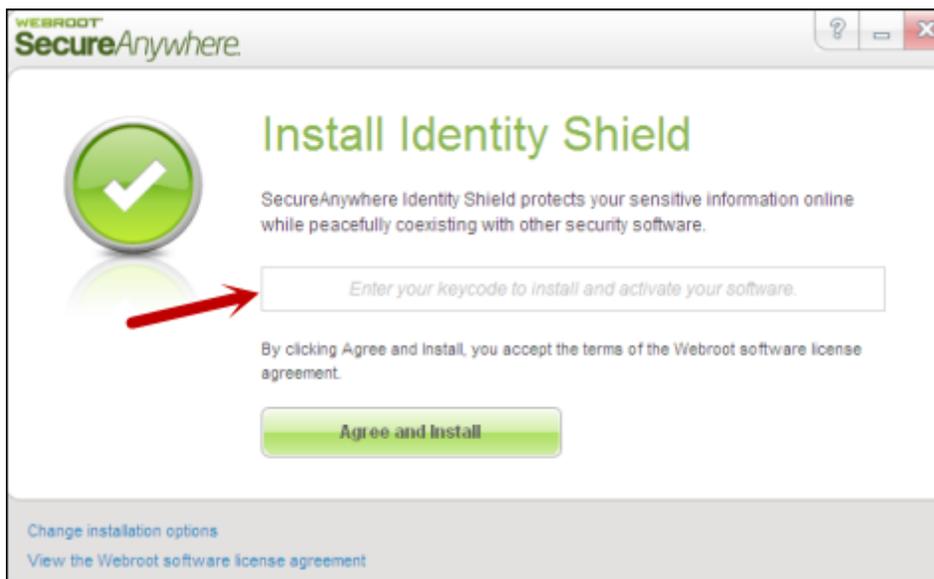
- Windows® 8 32-bit and 64-bit
- Windows 7 32-bit and 64-bit (all Editions), Windows 7 SP1 32-bit and 64-bit (all Editions)
- Windows XP 32-bit and 64-bit SP2, SP3
- Windows Vista® 32-bit (all Editions), Windows Vista SP1, SP2 32-bit and 64-bit (all Editions)

Browsers:

- Microsoft® Internet Explorer® 7.0 and higher
- Mozilla® Firefox® 3.6 and higher (32-bit only)
- Google Chrome™ 10.0 or higher
- Opera 9 and higher (32-bit only)

To install the software:

1. Your banking institution will provide a login link to the Webroot Identity Shield. Click on the Webroot download link, available when you log into your banking account.
2. When the installation dialog opens, click **Run**.
The following dialog opens.



3. In the middle field, enter the keycode provided by your banking institution. (If you don't see a field in the middle of the dialog, your version does not require a keycode.)
4. If desired, you can click "Change installation options" at the bottom of the dialog to modify the following settings:
 - **Create a shortcut to SecureAnywhere on the desktop.** This option places a shortcut icon on your Windows Desktop for the Identity Shield.
 - **Randomize the installed filename to bypass certain infections.** This option changes the Webroot installation filename to a random name (for example, "QrXC251G.exe"), which prevents malware from detecting and blocking Webroot's installation file.
 - **Protect the SecureAnywhere files, processes, and memory from modification.** This option enables self protection and the CAPTCHA prompts. (CAPTCHA requires you to read distorted text on the screen and enter the text in a field before performing any critical actions.)
 - **Change Language.** To change the language displayed in the Identity Shield, click the **Change Language** button and select from the supported languages. (You can only change the displayed language during installation, not after.)
5. Click **Agree and Install**.
The Identity Shield installs in a few seconds.

6. To verify that the Identity Shield is running, look for the Webroot icon in your system tray.



The Identity Shield runs in the background to automatically protect your online activities. You do not need to manually start Identity Shield protection, nor do you need to shut it down.

Using the Identity Shield

After you install the Identity Shield, it works silently in the background to protect your browsing activity. The Identity Shield will not slow down your computer or interrupt normal operations.

If the Identity Shield detects suspicious activity, it performs one of the following actions:

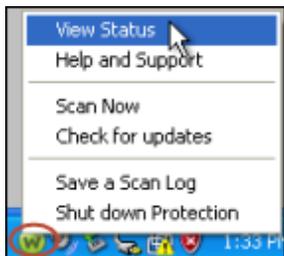
- Blocks malicious programs on websites, which try to steal your login credentials and other personal data.
- Opens an alert if you try to access a phishing website or if malware tries to re-direct you to a malicious website. See "Responding to alerts" on page 8.
- Prevents malware from reading or copying your information on a website.

Webroot has configured the Identity Shield for you. You do not need to change its settings or perform any tasks yourself. However, if you are an advanced user, you can open the main interface and adjust protection levels (see "Opening the main interface" on page 6).

Note: The Identity Shield cannot remove malware already installed on your computer. To fully protect your computer, you should upgrade to one of the following Webroot SecureAnywhere versions: AntiVirus, Internet Security Plus, or Complete. See "Upgrading to a threat-removal version" on page 29.

Opening the main interface

The main interface for the Identity Shield provides access to all functions and settings. To open the main interface, double-click on the Webroot icon  from the system tray menu. You can also right-click on the icon, and then click **View Status**.



The main interface opens, similar to the example below.

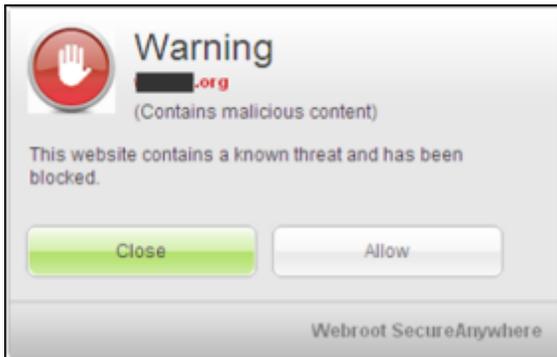


Along the top of the panel, the main interface includes navigation tabs.

Navigation tab	Description
Overview	View your system status.
PC Security	Run support tools. If you have the threat-detection version, additional options are available to scan for threats. For instructions on scanning, see "Scanning for Malware" in the Webroot SecureAnywhere User Guide for PCs . To remove threats, you must upgrade to a full version of Webroot SecureAnywhere. See "Upgrading to a threat-removal version" on page 29.
Identity & Privacy	Adjust the Identity Protection settings. See "Managing Identity Protection" on page 13.
System Tools	Use tools to manage processes and files, view reports, and submit a file to Webroot Support. For more information about system tools, see the Webroot SecureAnywhere User Guide for PCs .
My Account	View your account information and upgrade your subscription to include threat removal.

Responding to alerts

The Identity Shield blocks known phishing sites. If it detects a suspicious site, it opens an alert similar to the following example.



If this alert opens, you must decide whether to continue or not. If you aren't sure what to do, we recommend that you click **Close**. Only click **Allow** if you are *absolutely sure* the website is legitimate, and not a phishing site.

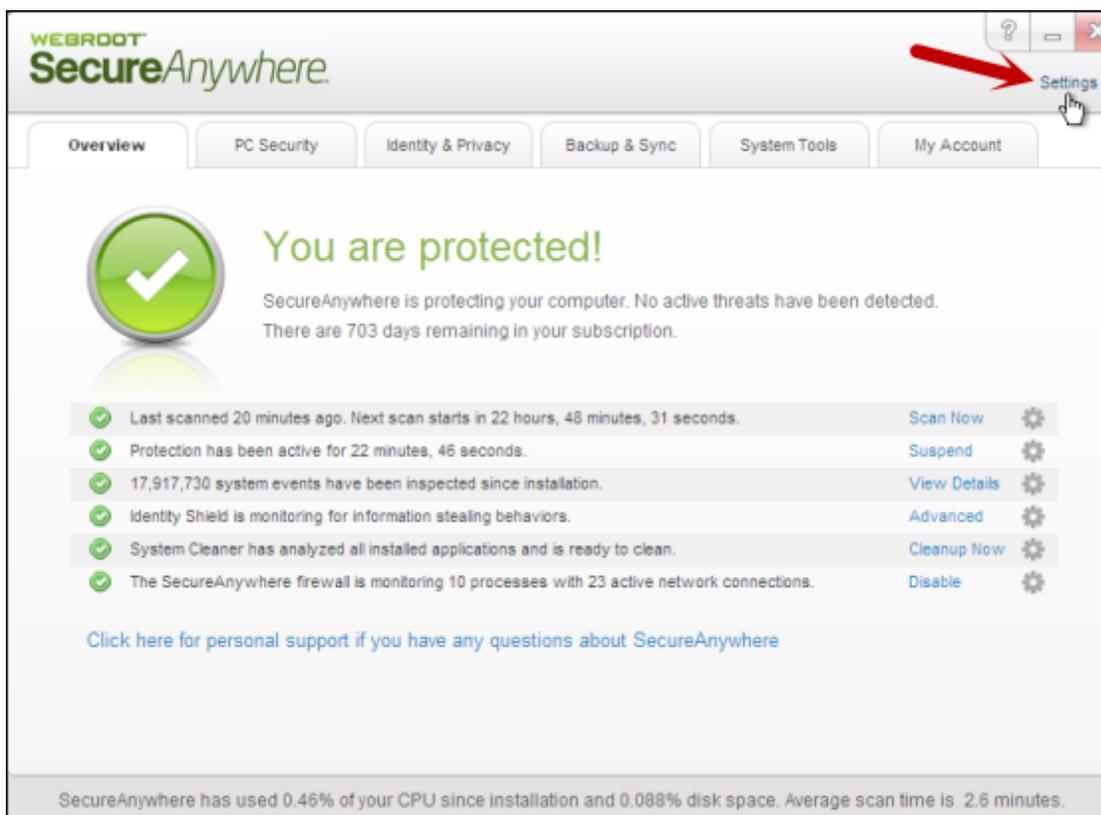
Setting program configuration options

Webroot has preconfigured the Identity Shield with our recommended settings. If desired, you can modify these settings to change the behavior of the program.

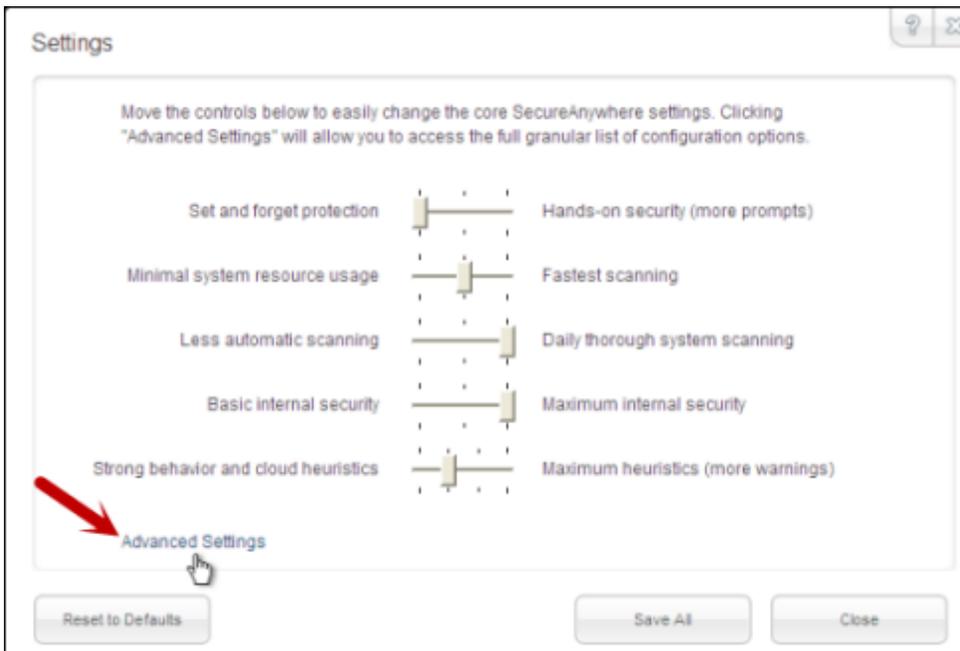
Note: This section describes basic configuration. For information about other program settings, see the [Webroot SecureAnywhere User Guide for PCs](#).

To change basic configuration:

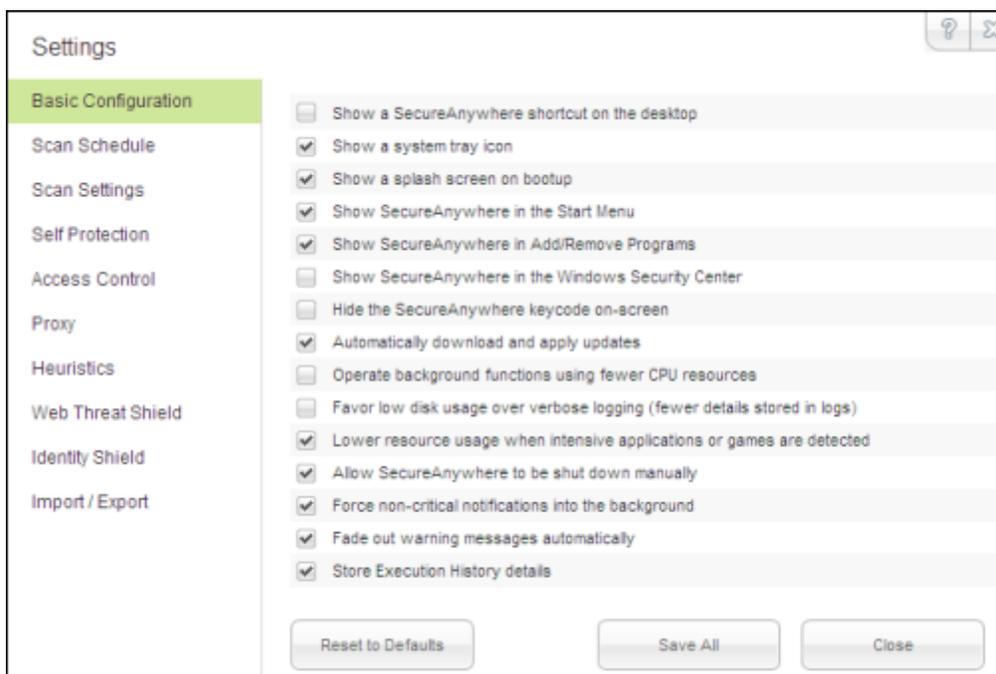
1. Open the main interface (see "Opening the main interface" on page 6).
2. In the upper right corner, click **Settings**.



3. In the Settings panel, click **Advanced Settings**.



4. Make sure **Basic Configuration** is selected at the left.



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

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

The following table describes the options.

Basic Configuration setting	Description
Show a SecureAnywhere shortcut on the desktop	Provides quick, double-click access to the main interface by placing the shortcut icon on your desktop.
Show a system tray icon	Provides quick access to Identity Shield functions by placing the Webroot icon on your desktop. You can double-click the icon to open the main interface or right-click to open a menu of common functions, like scanning.

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

Managing Identity Protection

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

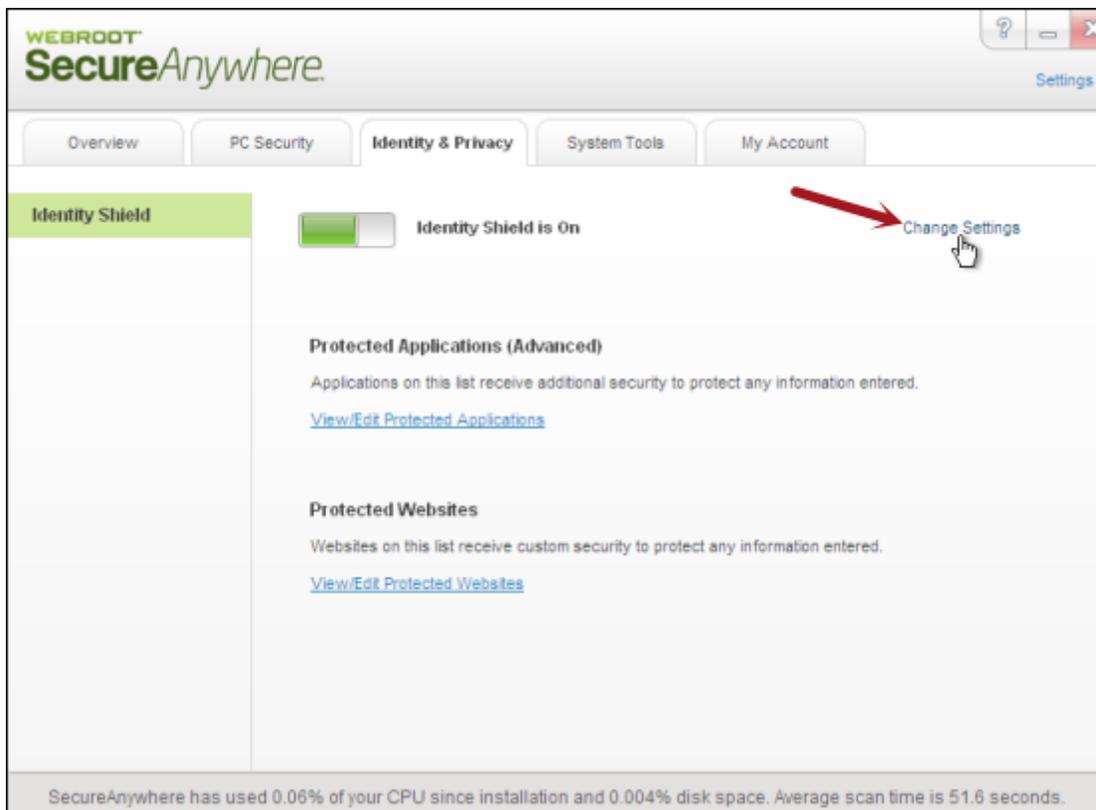
Changing shield settings	14
Managing protected applications	17
Managing protected websites	20
Disabling the shield	25

Changing shield settings

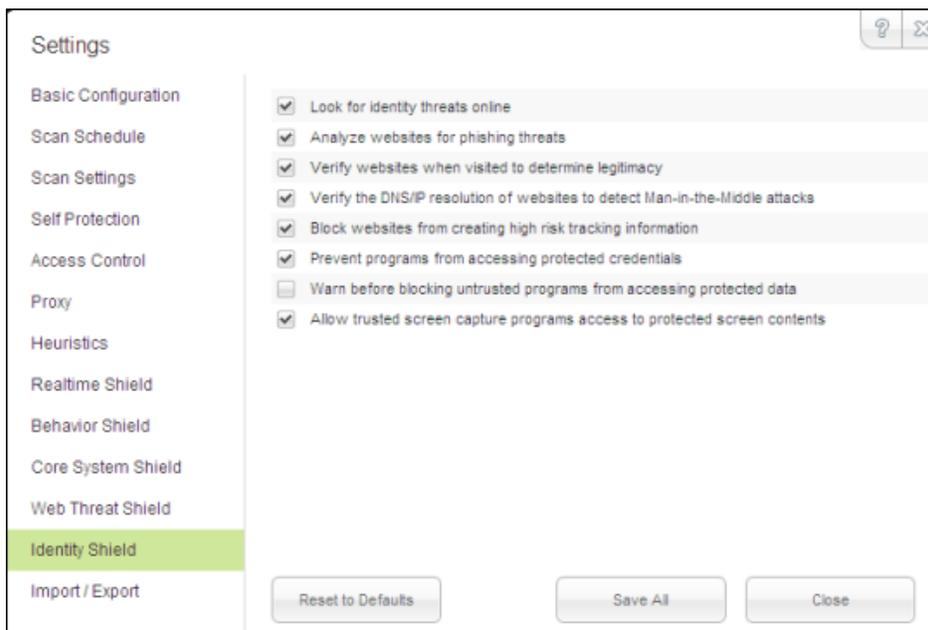
You can change the behavior of the Identity Shield and control what it blocks, as described in this section.

To change Identity Shield settings:

1. Open the main interface (see "Opening the main interface" on page 6).
2. Click the **Identity & Privacy** tab.
3. Click the **Change Settings** link on the upper right.



The Identity Shield settings panel opens.



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

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

The following table describes the shield options.

Identity Shield settings	Description
Look for identity threats online	Analyzes websites as you browse the Internet or open links. If the shield detects any malicious content, it blocks the site and opens an alert.

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

Managing protected applications

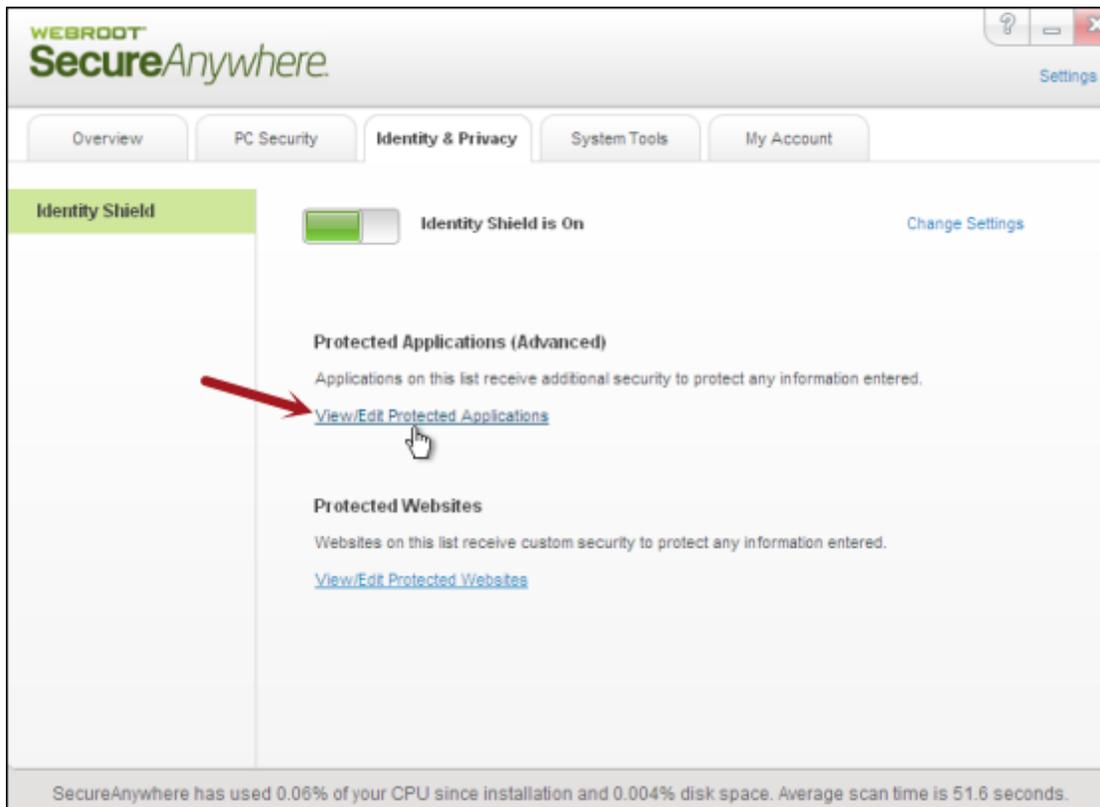
You can provide additional security for software applications that may contain confidential information, such as Instant Messaging clients or tax preparation software. By protecting these applications, you secure them against information-stealing Trojans like keyloggers, man-in-the-middle attacks, and clipboard stealers. As you work on your computer, the Identity Shield automatically adds web browsers and applications to the Protected Applications list. It assigns applications to one of these levels of protection:

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

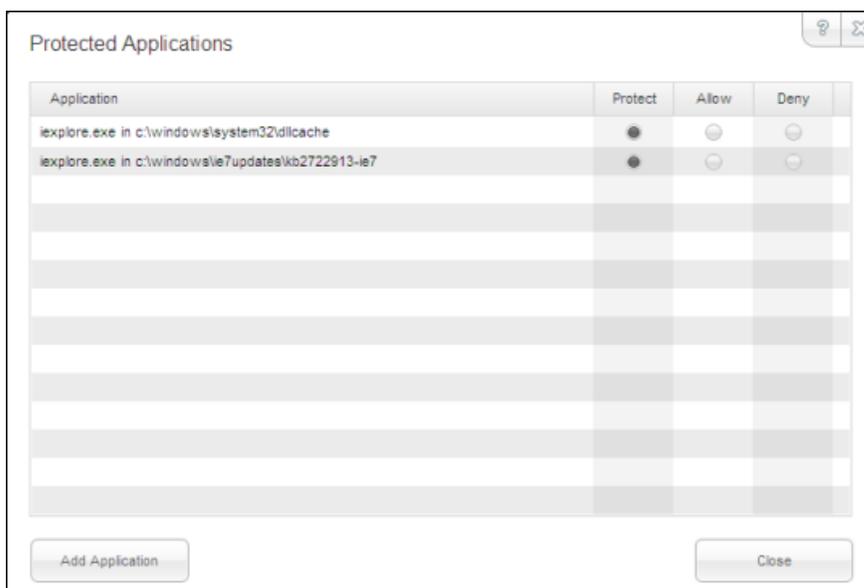
- **Allow.** “Allowed applications” are not secured against information-stealing malware, and also have full access to protected data on the system. Many applications unintentionally access protected screen contents or keyboard data without malicious intent when running in the background. If you trust an application that is currently marked as “Deny,” you can change it to “Allow.”
- **Deny.** “Denied applications” cannot view or capture protected data on the system, but can otherwise run normally.

To manage the application list and specify levels of protection:

1. Open the main interface (see “Opening the main interface” on page 6).
2. Click the **Identity & Privacy** tab.
3. Click **View/Edit Protected Applications**.



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



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

Managing protected websites

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

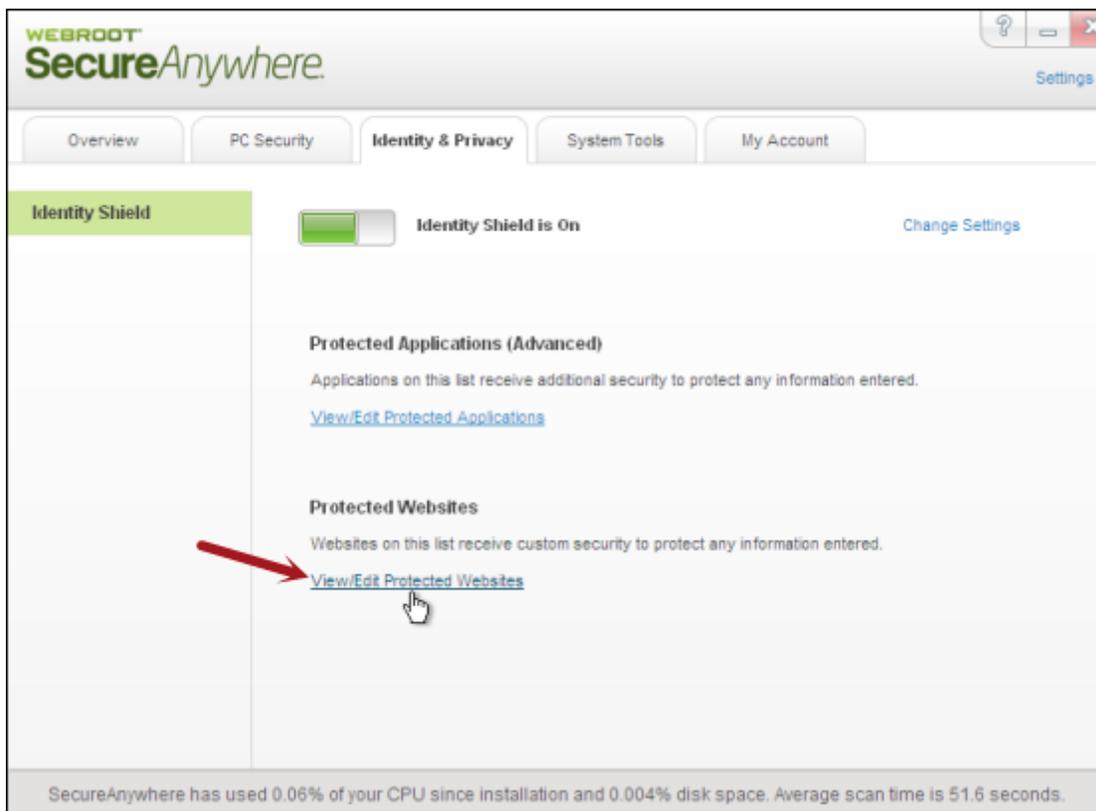
- **None.** Provides unfiltered access to all potentially malicious content. (Not recommended.)
- **Low.** Protects stored data and identifies malware in real time. You may want to use this setting if you have an application that does not work properly when the security level is set to Medium or higher.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



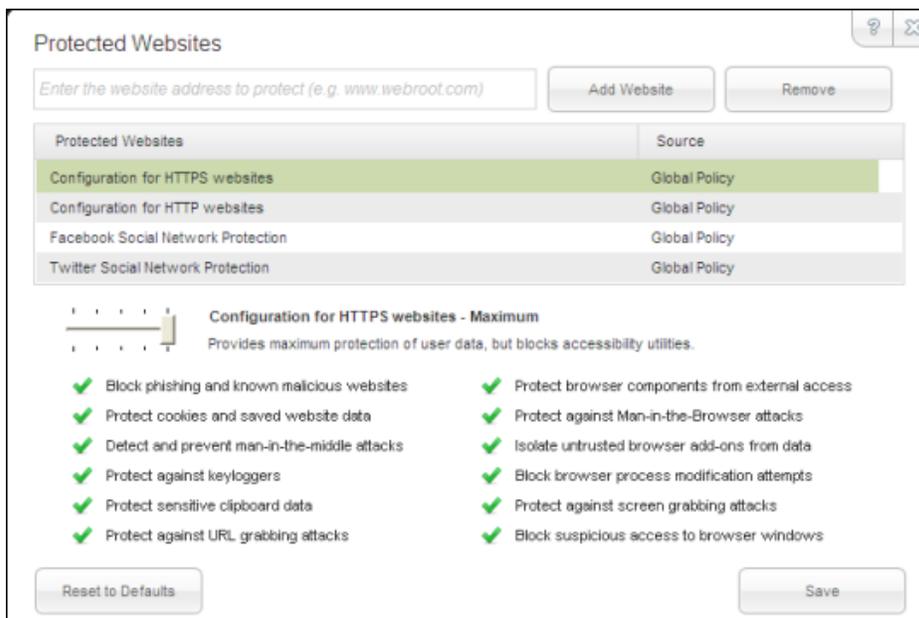
Note: The Identity Shield only protects a secured website when the browser window is active in the foreground window (the padlock is shown in the tray icon). For full protection from screen grabbers, information-stealing Trojans, and other threats, make sure the browser window is in the foreground and the padlock is displayed in the tray icon. If the Identity Shield encounters a website that may be a threat, it opens an alert. You can decide whether you want to stay secure (click **Block**) or continue despite the warning (click **Allow**).

To manage settings for protected websites:

1. Open the main interface (see "Opening the main interface" on page 6).
2. Click the **Identity & Privacy** tab.
3. Click **View/Edit Protected Websites**.



The Protected Websites panel opens.



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

The following table describes the protection options.

Website protection options	Description
Block phishing and known malicious websites	Alerts you to phishing sites and other malicious sites listed in our Webroot database. Phishing is a fraudulent method used by criminals to steal personal information. Typical scams might include websites designed to resemble legitimate sites, such as PayPal or a banking organization, which trick you into entering your credit card number.

Website protection options	Description
Protect cookies and saved website data	Alerts you if a malicious program attempts to gather personal data from cookies installed on your computer. Cookies are small bits of text generated by a web server and then stored on your computer for future use. Cookies can contain everything from tracking information to your personal preferences.
Detect and prevent man-in-the-middle attacks	Alerts you if a server is redirecting you to a malicious website (man-in-the-middle attack). This is a method of intercepting communications between two systems and stealing data.
Protect against keyloggers	Stops keyloggers from recording keystrokes on your computer. Keyloggers may monitor emails, chat room dialogue, instant message dialogue, websites visited, usernames, passwords, programs run, and any other typed entries. They have the ability to run in the background, hiding their presence.
Protect sensitive clipboard data	Stops malware programs from capturing clipboard data. The clipboard is a utility that allows you to cut and paste stored data between documents or applications.
Protect against URL grabbing attacks	Hides your web browsing activity from malware that attempts to log the websites you visit.
Protect browser components from external access	Hides your web browsing activity from malware that attempts to modify your browser with memory injection and other behind-the-scenes attacks.
Protect against Man-in-the-Browser attacks	Blocks a malicious toolbar from stealing data. A man-in-the-browser attack is a Trojan that infects a web browser. It can modify pages and the content of your transactions without being detected.
Isolate untrusted browser add-ons from data	Blocks a browser add-on (browser helper object) from stealing data. While most browser add-ons are legitimate, some can display ads, track your Internet activity, or hijack your home page.
Block browser process modification attempts	Analyzes browser memory to see if code injection is taking place.

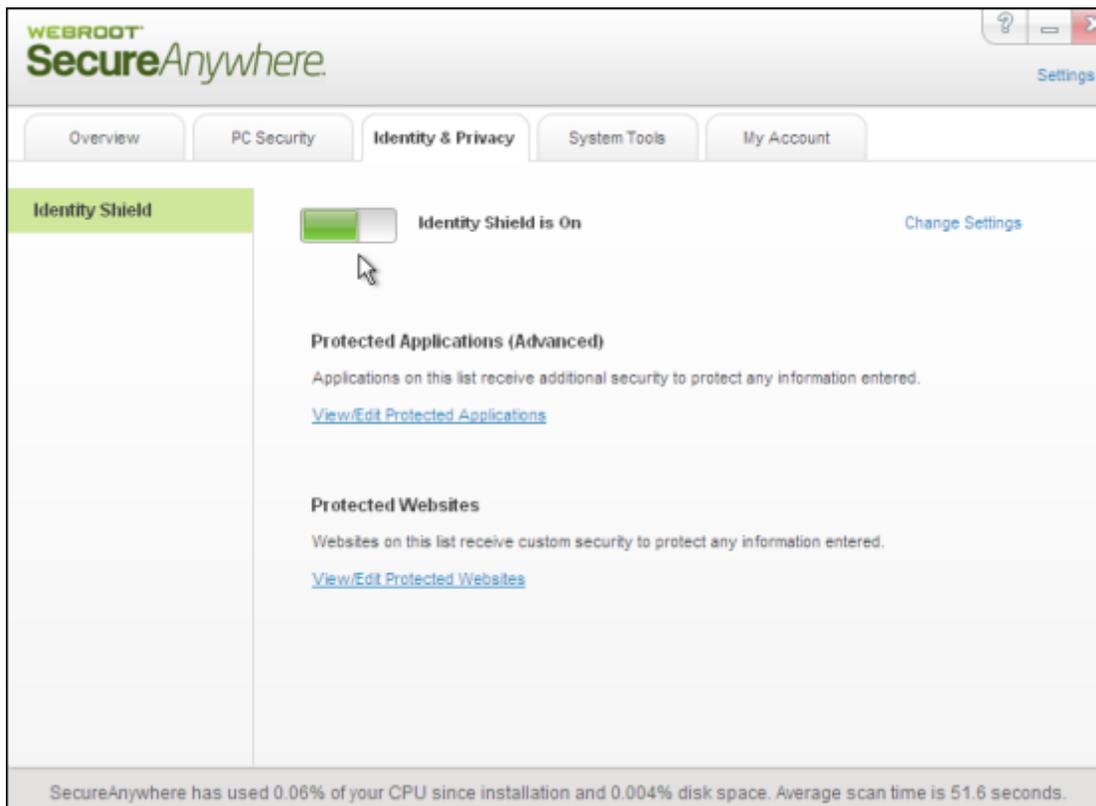
Website protection options	Description
Protect against screen grabbing attacks	Blocks a malicious program from viewing and capturing your screen content.
Block suspicious access to browser windows	Blocks a malicious program from viewing and capturing data in Windows components.

Disabling the shield

We recommend that you keep the Identity Shield enabled; however, you can disable it if you want.

To disable the Identity Shield:

1. Open the main interface (see "Opening the main interface" on page 6).
2. Click the **Identity & Privacy** tab.
The Identity Shield panel opens. The green button indicates the shield is on.
3. Click the green button to turn it off.
The button turns gray when the shield is off.



Managing Your Account

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

Viewing your account details	28
Upgrading to a threat-removal version	29

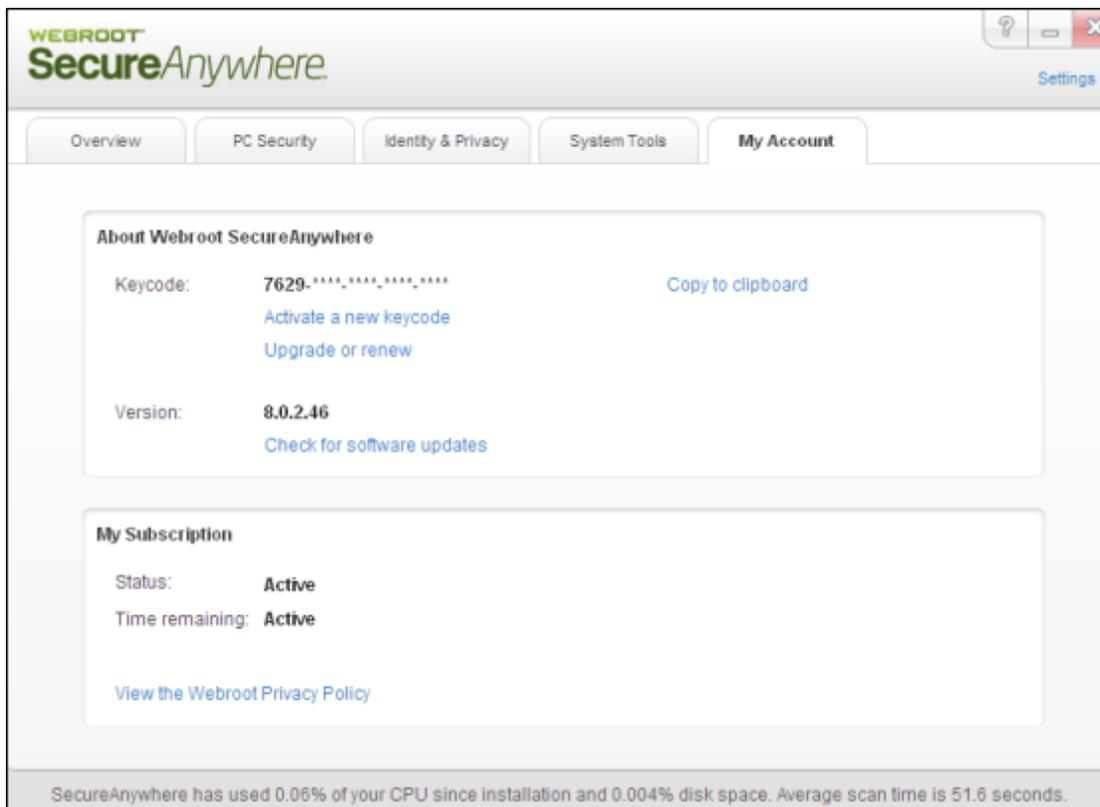
Viewing your account details

You can view your keycode and the time remaining on your subscription from the My Account window.

To view account details:

1. Open the main interface (see "Opening the main interface" on page 6).
2. Click the **My Account** tab.

Your account information appears in the panel.



From here, you can activate a new keycode, upgrade or renew your license, or check for software updates.

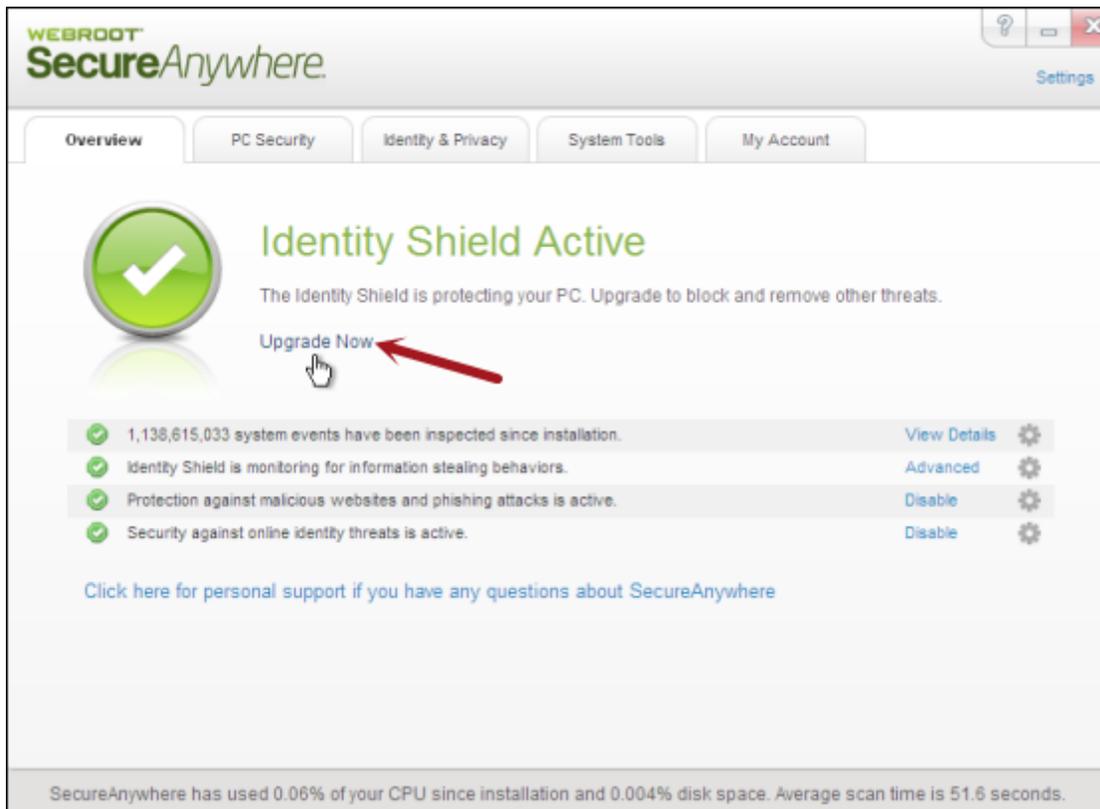
Upgrading to a threat-removal version

If you want to block and remove malware from your computer, you can upgrade to one of the following SecureAnywhere editions:

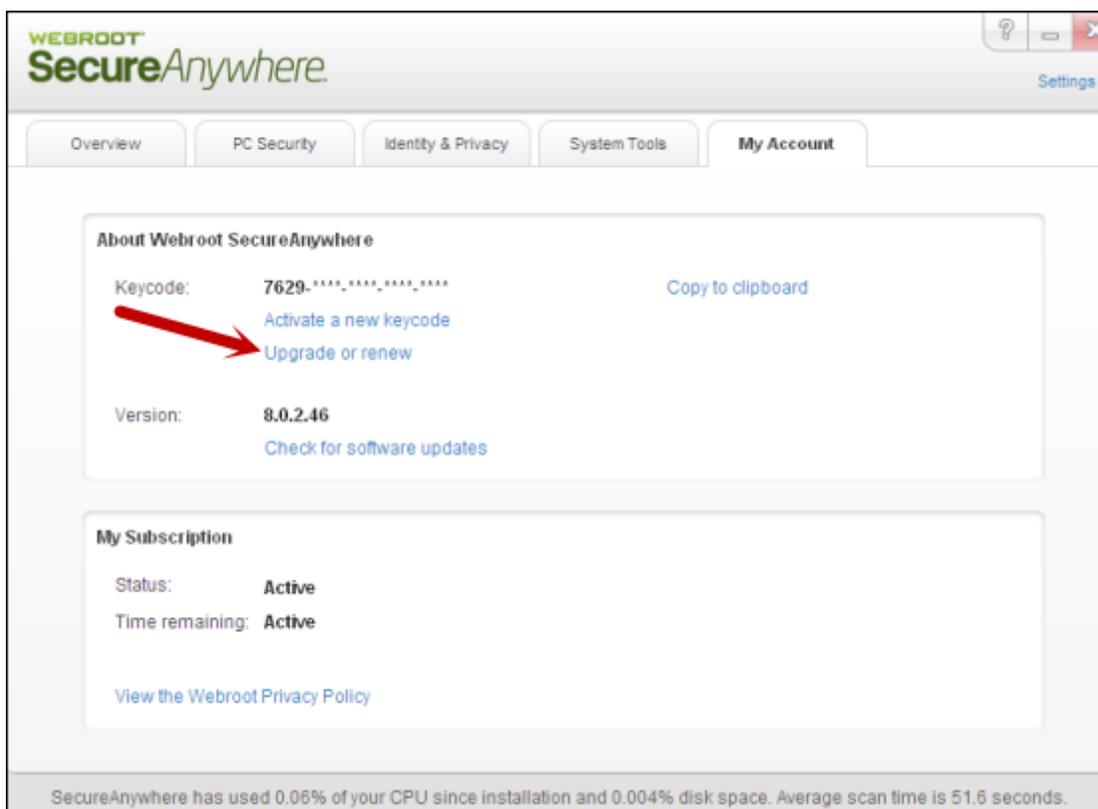
- **AntiVirus.** Provides protection from viruses and spyware, and also includes the Identity Shield and firewall protection.
- **Internet Security Plus.** Provides all the features of the AntiVirus edition, plus password management and protection for mobile devices.
- **Complete.** Provides all the features of the Internet Security Plus edition, as well as backup management and a system cleaner that removes temporary files and your browsing history.

To upgrade your version:

1. Open the main interface (see "Opening the main interface" on page 6).
2. Click on the **Upgrade Now** link.



If you don't see this link on the Overview panel, click the **My Account** tab and then the **Upgrade or renew** link.



3. When the Webroot website opens, you can purchase an upgrade to your software.

Accessing Support and Resources

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

Accessing Technical Support options	34
Accessing additional publications	35
Shutting down or uninstalling the Identity Shield	36

Accessing Technical Support options

Webroot offers a variety of Technical Support options, including:

- Ticket and phone support.
- Interactive knowledgebase.

To access these support options, go to our online Support site: [SecureAnywhere Product Support](#).

Accessing additional publications

To access additional user guides and other resources, go to our [Help and Product Guides page](#).

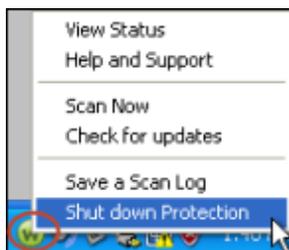
Shutting down or uninstalling the Identity Shield

If desired, you can temporarily shut down Identity Shield protection or uninstall the program entirely, as described below.

Note: We recommend that you keep the Identity Shield running in the background at all times. Normally, you do not need to shut it down.

To shut down the Identity Shield:

1. Right-click on the Webroot icon  from the system tray menu.
2. Click **Shut down Protection**, then click **Yes** at the prompt.



3. If a CAPTCHA dialog opens, enter the displayed characters and click **Enter**.
The Identity Shield stops its protection activities and the Webroot icon is removed from the system tray.
4. To turn on protection again, go to the Windows **Start** menu and select **All Programs, Webroot SecureAnywhere**, and **Webroot SecureAnywhere** again.

To uninstall the Identity Shield:

1. Go to the Windows **Start** menu and select **All Programs, Webroot SecureAnywhere**, and **Tools**.
2. Click **Uninstall Webroot**.
3. At the prompt, click **Yes** to continue.

Glossary

A

adware

Software designed to display advertisements on your system or hijack web searches (rerouting searches through its own web page). It may also change your default home page to a specific website. Adware generally propagates itself using dialog boxes and social engineering methods.

C

CAPTCHA

Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA). These prompts require you to read distorted text on the screen and enter the text in a field before performing any critical actions.

cookies

Small strings of text designed to help websites remember your browser and preferences. Cookies cannot steal information off your machine, but some do store personal information that you may not want outside parties to gather. You can manage cookie settings in your browser's security or privacy preferences.

H

hosts file

A file that helps direct your computer to a website using Internet Protocol (IP) addresses. When you enter a web address in a browser, your computer first looks in the hosts file to see if the domain is already listed. If so, it goes directly to the IP address. Some types of malware can hijack the entries in the hosts file.

K

keycode

Your keycode is the 20-character license that identifies your Webroot account. After installation, the My Account panel lists your keycode.

keylogger

A system monitor that records keyboard activity. Keyloggers can be used for legitimate purposes, but can also record sensitive information for malicious purposes.

M

malware

Malicious software that is designed to destroy or harm your computer system. Malware includes viruses, spyware, adware, and all types of threats.

P

phishing

A fraudulent method criminals use to steal personal information. These criminals design websites or email messages that appear to originate from trustworthy sources, such as eBay, PayPal, or even your own bank. Typical scams can trick you into entering your user names, passwords, and credit card information.

R

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.

rootkit

A collection of tools that enable administrator-level access to a computer or network. By using file-obfuscation techniques, rootkits can hide logins, processes, files and logs, and may include software to capture information from desktops or a network. Spyware developers often use rootkits to avoid detection and removal.

S**scan**

Webroot's process of searching for potential threats on your computer, such as spyware and viruses. It then moves items to quarantine, where they are rendered inoperable.

spyware

A program that may either monitor your online activities or install programs without your knowledge. Spyware may get bundled with freeware, shareware, or email attachments. You can also accidentally install spyware by clicking on dialog boxes in websites. Once installed, spyware can send information about your online activities to a third party for malicious purposes.

T**Trojan Horse**

A program that takes control of your computer files, allowing a hacker to install, execute, open, or close programs. A Trojan is usually disguised as a harmless software program. It may also be distributed as an email attachment. When you open the program or attachment, the Trojan can launch an auto-installation process that downloads third-party programs onto your computer.

V**virus**

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

- account
 - changing keycode 28
 - viewing details 28
- Add/Remove programs, removing
 - SecureAnywhere from 12
- alerts
 - disabling fade-out 12
 - forcing in the background 12
 - reducing number of 16
 - responding to 8
- applications, managing protection for 17

B

- basic configuration settings 9
- browser add-ons, blocking 23
- browsers supported 2
- browsing activity, hiding 23

C

- Chrome support 2
- clipboard data, protecting 23
- configuration settings 9
- cookies
 - blocking 23
 - blocking third-party 16
- CPU resources, preserving 12

D

- disk usage, lowering 12

E

- Execution History details, storing 12

-
- Explorer support 2

F

- Firefox support 2

I

- Identity & Privacy tab 7
- installation 2

K

- keycode
 - changing 28
 - entering at installation 3
 - hiding on screen 12
- keyloggers, protection from 23
- knowledgebase 34

L

- language, changing 3
- license, renewing 28
- lock icon in system tray
 - with applications 17
 - with browsers 20
- login credentials, protecting 16

M

- main interface 6
- man-in-the-browser attacks, protection from 23
- man-in-the-middle attacks
 - in website protection 23
 - protection in general settings 16
- My Account tab 7

O

- opening the main interface 6
- Opera support 2

operating systems supported 2
Overview panel 6

P

padlock icon in system tray
 with applications 17
 with browsers 20
PC Security 7
phishing
 protection in general settings 16
 protection in website settings 22
publications, Webroot 35

R

renewing subscription 28
reports 7
resource usage 12

S

scanning for threats 7
screen capture programs, allowing 16
screen grabbers, protecting from 24
Security Center, listing Webroot in 12
settings
 changing for basic configuration 9
 changing for Identity Shield 14
shortcut, desktop 3, 11
shutdown command, removing from tray
 menu 12
shutting down 36
splash screen, disabling on bootup 12
Start Menu, removing SecureAnywhere from 12
subscription, extending 28
support options 34
system requirements 2
System Tools 7
system tray icon, showing 11

T

Technical Support 34
turning off 36

U

uninstalling SecureAnywhere 36
updates, automatically downloading 12
URL grabbing attacks, protection from 23

W

warnings, responding to 8
web browsers supported 2
Webroot publications 35
Webroot Support 34
Windows systems supported 2