WEBROOT®

an opentext™ company

Identity Shield User Guide

Copyright

Copyright 2019 Webroot. All rights reserved.

WSA Identity Shield User Guide

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Webroot.

Table of Contents

Chapter 1: Identity Shield User Guide *1*

Identity Shield User Guide Overview *2*

Chapter 2: Getting Started With Identity Shield *3*

Installing Identity Shield *4*

System Requirements for Windows *8*

Operating Systems *8*

RAM *8*

Hard Disk Space *8*

Internet/Browser *8*

Using Identity Shield *9*

Changing Protection Levels *10*

Responding to Alerts *13*

Changing Basic Configuration Settings *14*

Chapter 3: Managing Identity Protection *24*

Changing Identity Shield Settings *25*

Managing Protected Applications *29*

Managing Protected Websites *42*

Disabling Identity Shield *50*

Chapter 4: Managing Your Account *58*

Viewing Your Account Details *59*

Shutting Down Identity Shield *66*

Uninstalling Identity Shield *69*

Upgrading to a Threat Removal Version *70*

Chapter 5: Identity Shield Support *72*

Accessing Technical Support *73*

Index ..... *i*

Chapter 1: Identity Shield User Guide

To get started using the Identity Shield User Guide, see the following topic:

Identity Shield User Guide Overview **2**

Identity Shield User Guide Overview

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.

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 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 be able to remove threats, you must upgrade to a full version of Webroot SecureAnywhere. For more information, see *Upgrading to a Threat Removal Version on page 70*.

Chapter 2: Getting Started With Identity Shield

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

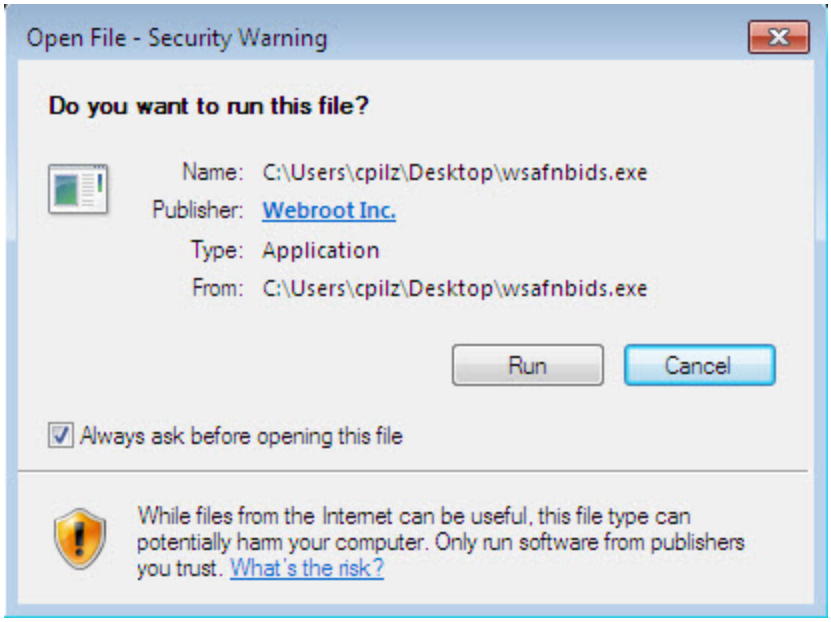
Installing Identity Shield *4*
System Requirements for Windows *8*
Operating Systems *8*
RAM *8*
Hard Disk Space *8*
Internet/Browser *8*
Using Identity Shield *9*
Changing Protection Levels *10*
Responding to Alerts *13*
Changing Basic Configuration Settings *14*

Installing Identity Shield

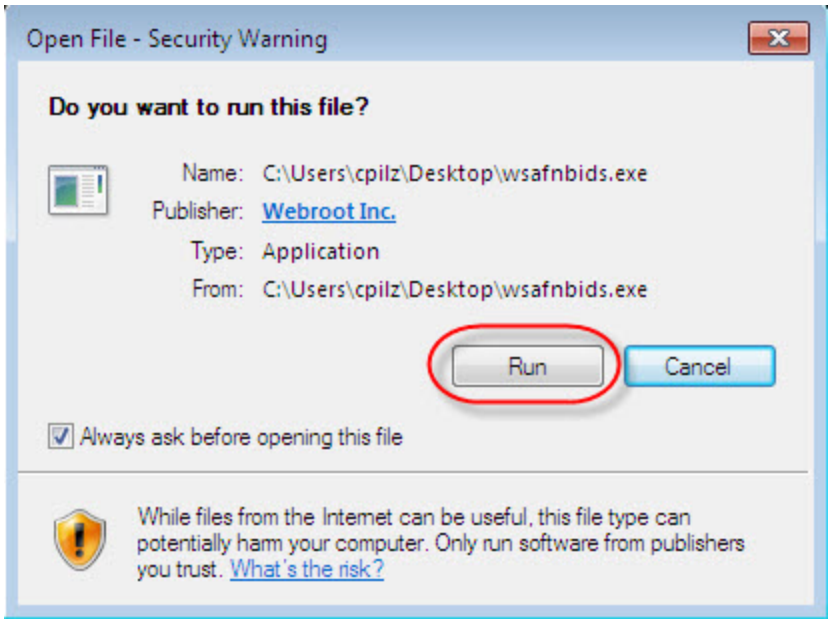
You can install Identity Shield on a PC with one of the following operating systems and browsers:

To install Identity Shield:

1. Your banking institution provides a login link to the Webroot Identity Shield. Click the **Webroot** download link, available when you log into your banking account. The installation window displays.



2. Click the **Run** button.



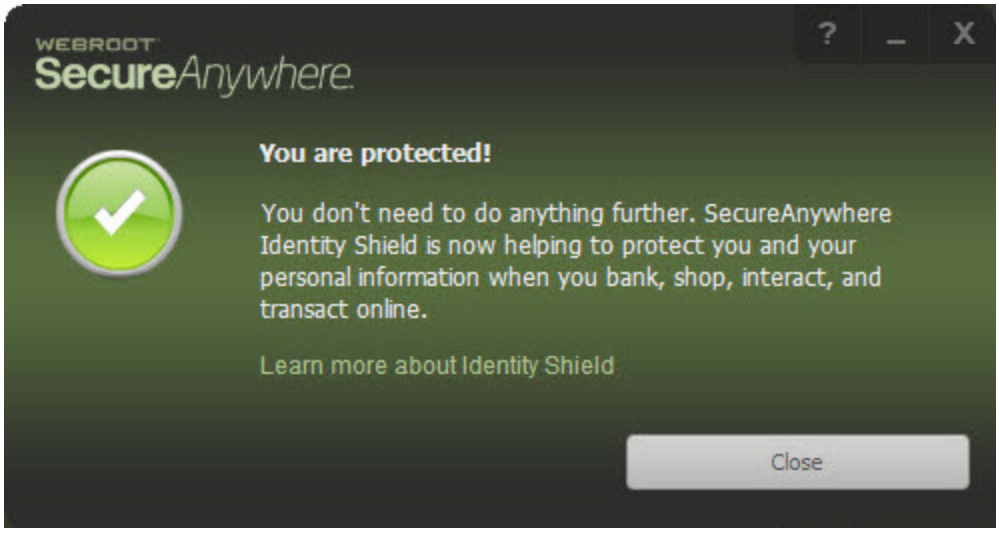
The following dialog displays.

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.

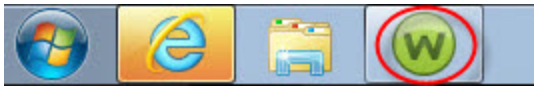
4. In the upper right corner, click the **Advanced Settings** link to modify any of the following settings.

OPTION	DESCRIPTION
Create a shortcut to SecureAnywhere on the desktop	Places an Identity Shield shortcut icon on your Windows Desktop.
Randomize the installed filename to bypass certain infections	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	Enables self-protection and 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	Changes the default display language. To change the language displayed in Identity Shied, click the **Change Language** button and select from the supported languages. You can only change the displayed language during installation, not after.

5. Click the **Agree and Install** button. Identity Shield installs in a few seconds.



6. When you're done, to verify that Identity Shield is running, look for the Webroot icon in your system tray.



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.

System Requirements for Windows

The following describes the system requirements for using Identity Shield functionality on Windows.

Operating Systems

- Windows 10 (32-bit and 64-bit).
- Windows 8 and 8.1 (32-bit and 64-bit).
- Windows 7 (32-bit and 64-bit), Windows 7 SP1 (32-bit and 64-bit).

RAM

- Intel Pentium®/Celeron® family, or AMD® K6™/Athlon®/AMD Duron™ family, or other compatible processor.
- 128 MB RAM (minimum).
- 2 GB RAM recommended (minimum).

Hard Disk Space

- 15 MB

Internet/Browser

Internet access is required:

- Internet Explorer® 11.0 and higher (32-bit and 64-bit).
- Mozilla Firefox® (32-bit and 64-bit); current and most recent versions.
- Google Chrome® (32-bit and 64-bit); current and most recent versions.

Using Identity Shield

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

If 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.
- Displays an alert if you try to access a phishing website or if malware tries to re-direct you to a malicious website. For more information, see *Responding to Alerts on page 13*.
- Prevents malware from reading or copying your information on a website.

Webroot has configured 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 display the main interface and adjust protection levels. For more information, see *Changing Protection Levels on page 10*.

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:

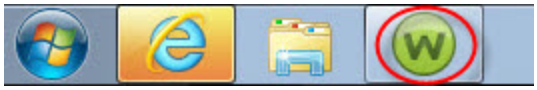
- AntiVirus
- Internet Security Plus
- Complete
- For more information, see *Upgrading to a Threat Removal Version on page 70*.

Changing Protection Levels

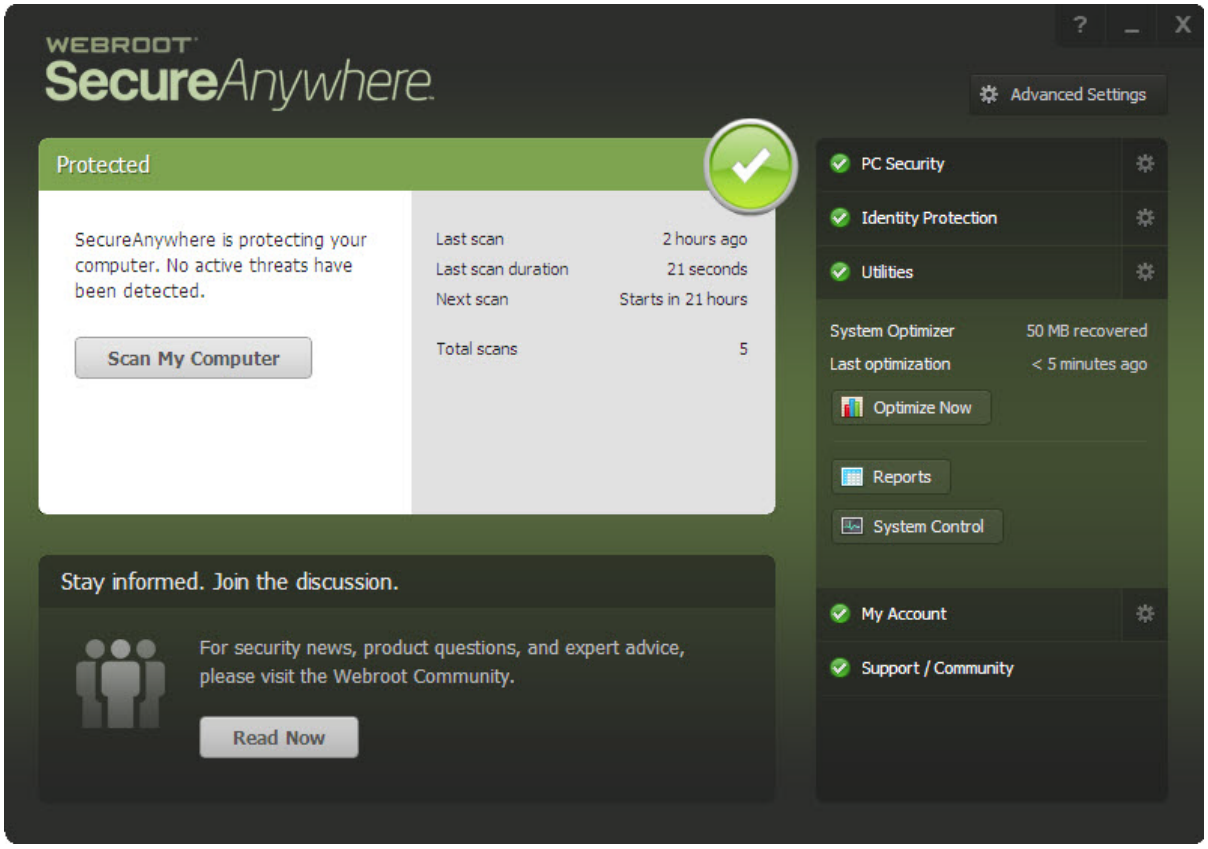
The main interface for Identity Shield provides access to all functions and settings.

To change protection levels:

1. From the system tray, double-click the **Webroot** icon.



The main interface displays.



The following are the areas and links can take you to different parts of the system.

AREA	DESCRIPTION
Main Interface	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 Running Scans in the WSA PC User Guide. To remove threats, you must upgrade to a full version of Webroot SecureAnywhere. For more information, see *Upgrading to a Threat Removal Version on page 70*.
Identity Protection	Adjust Identity Protection settings. For more information, see Managing Identity Protection in the WSA PC User Guide.
Utilities	Use tools to: • Manage processes and files • Generate and view reports • Submit files to Webroot Support For more information about system tools, see *Webroot SecureAnywhere PC User Guide*.

AREA	DESCRIPTION
My Account	View your account information and upgrade your subscription to include threat removal. For more information, see *Viewing Your Account Details on page 59*.
Support Community	Provides access to the online Webroot community. For more information, see *Accessing Technical Support on page 73*.

Responding to Alerts

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

If this alert displays, you must decide whether or not to continue. Do either of the following:

- If you aren't sure what to do, we recommend that you click the **Close** button.
- If you are absolutely sure the website is legitimate and not a phishing site, click the **Allow** button.

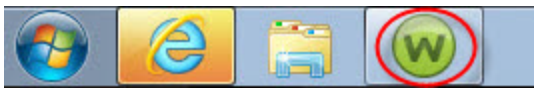
Changing Basic Configuration Settings

Webroot has preconfigured the Identity Shield with our recommended settings. We recommend that you keep Webroot's default settings, however, you can modify these settings to change the behavior of the program.

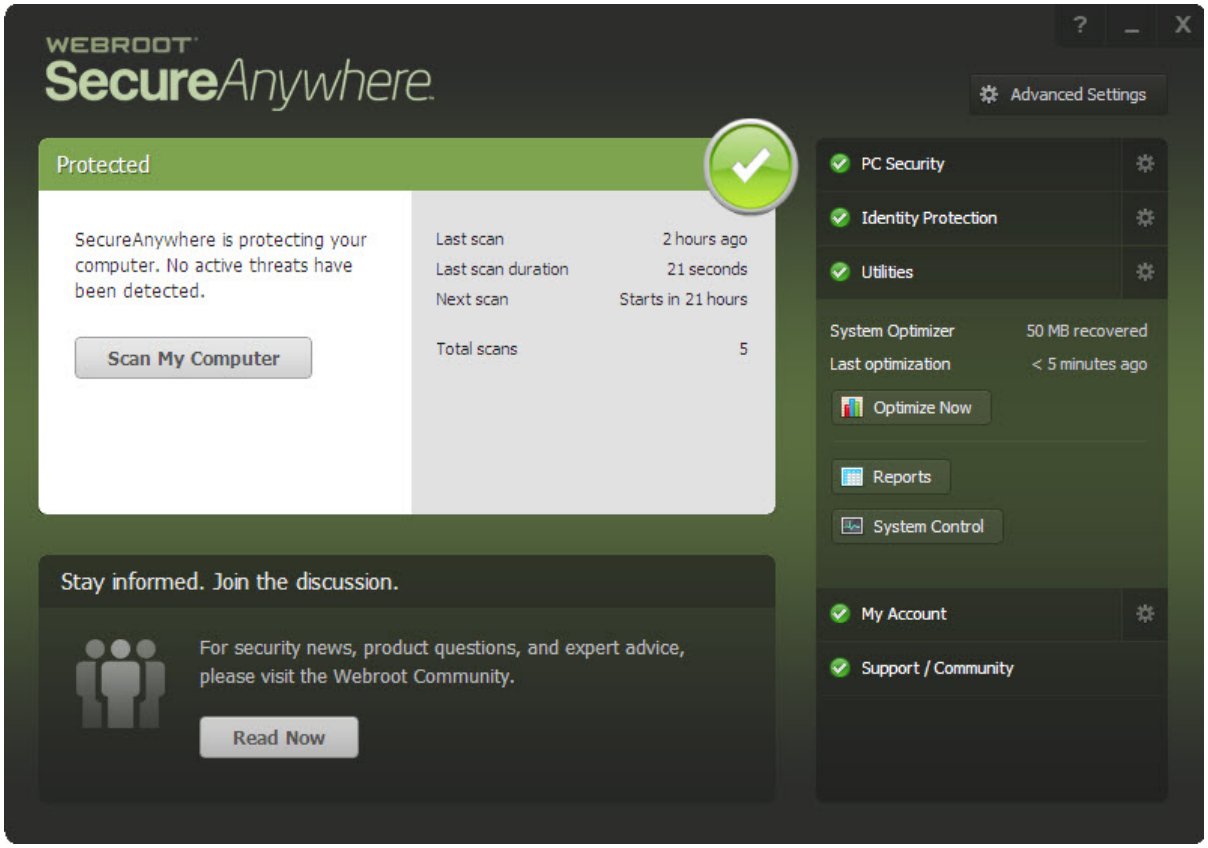
This page describes basic configuration. For information about other program settings, see Changing Shield Settings in the WSA PC User Guide.

To change basic configuration settings:

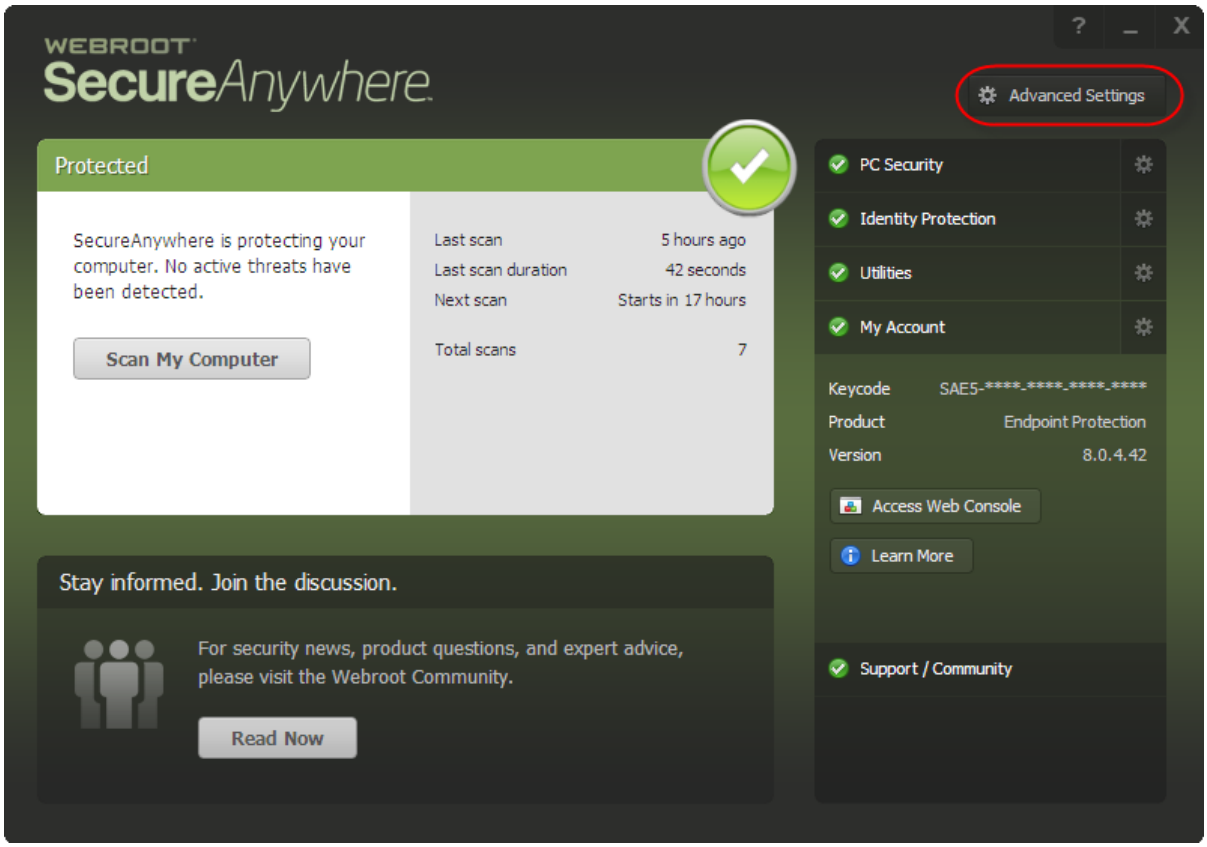
1. In the system tray, double-click the **Webroot** icon to display the main interface.



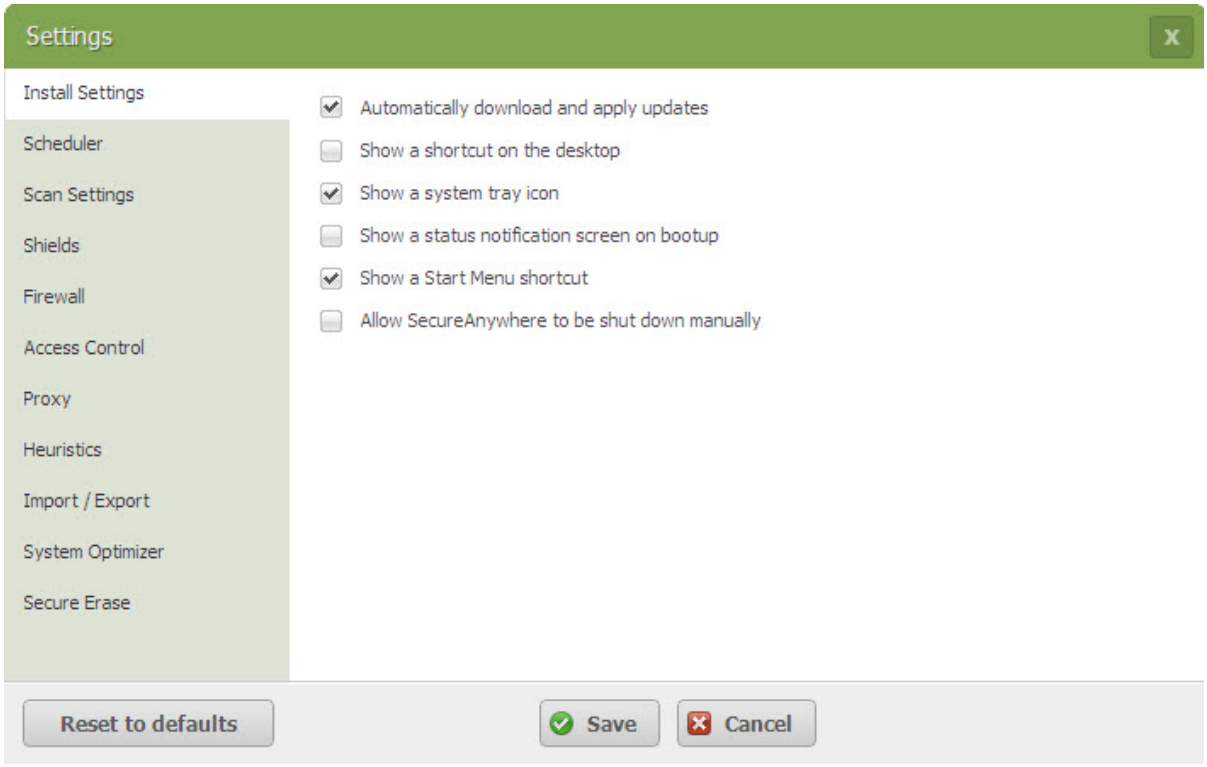
The main interface displays.



2. In the upper right corner, click the **Advanced Settings** link.



The Settings window displays.

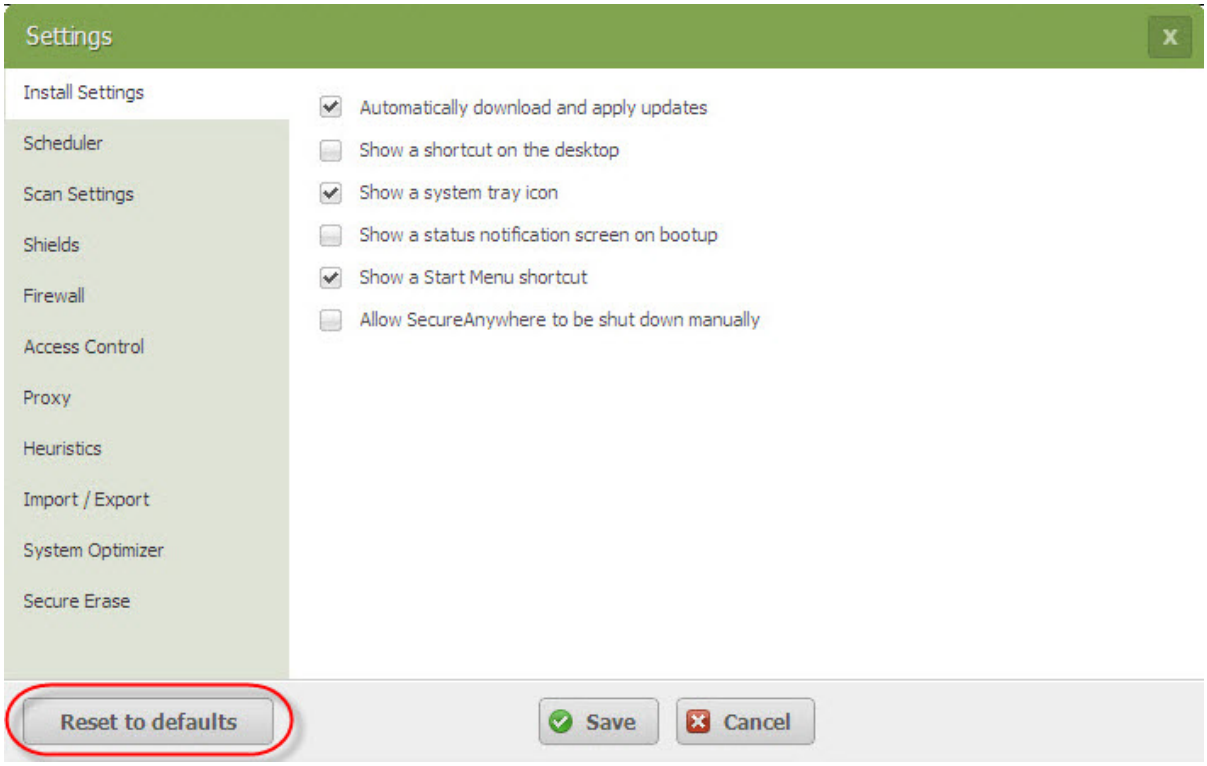


3. To change a setting, do one of the following:
   - To activate a setting, select the checkbox.
   - To deactivate a setting, deselect the checkbox.

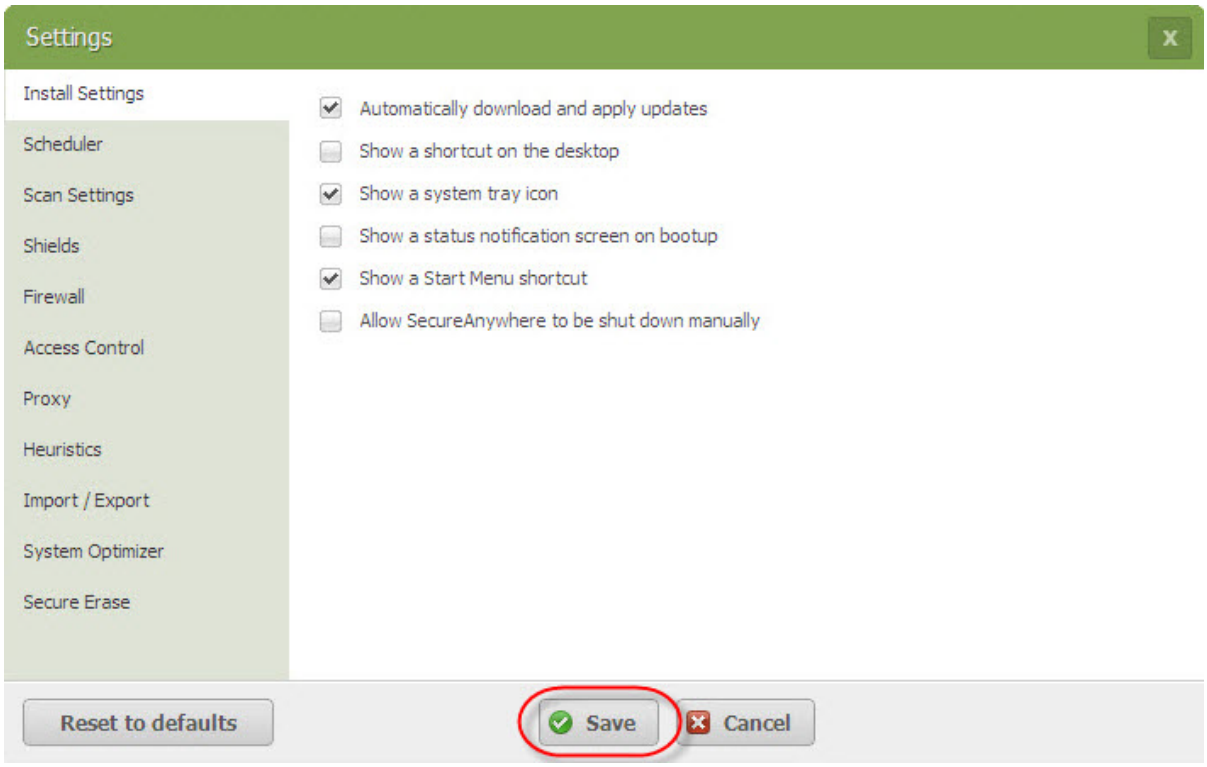
   The following table describes the settings.

SETTING	DESCRIPTION
Automatically download and apply updates	Downloads product updates automatically without alerting you.
Show a SecureAnywhere shortcut on the desktop	Provides quick, double-click access to the main interface by placing the Webroot 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 display the main interface or right-click the icon to display a menu of common functions, like scanning.
Show a status notification on bootup	Displays the Webroot splash screen on system startup, which lets you know that the program is running and protecting your computer.
Show Start Menu shortcut	Lists Webroot SecureAnywhere in the Windows Startup menu.
Allow SecureAnywhere to be shut down manually	Displays a Shutdown command in the system tray. If you deselect this option, the Shutdown command is removed from the menu.

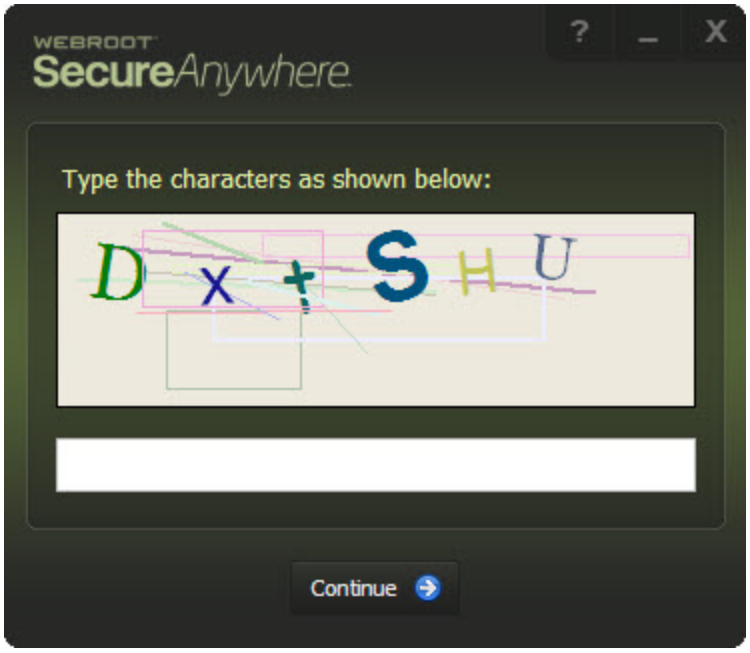
4. If you make changes and decide you want to return to the recommended settings, click the **Reset to Defaults** button.


Settings
Install Settings
Scheduler
Scan Settings
Shields
Firewall
Access Control
Proxy
Heuristics
Import / Export
System Optimizer
Secure Erase
Automatically download and apply updates
Show a shortcut on the desktop
Show a system tray icon
Show a status notification screen on bootup
Show a Start Menu shortcut
Allow SecureAnywhere to be shut down manually
Reset to defaults
Save
Cancel

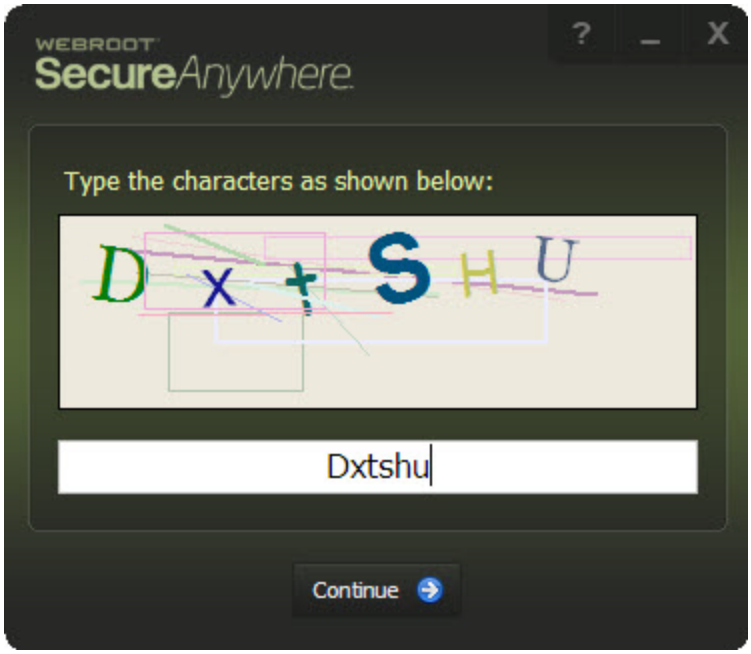
5. When you're done, click the **Save** button.



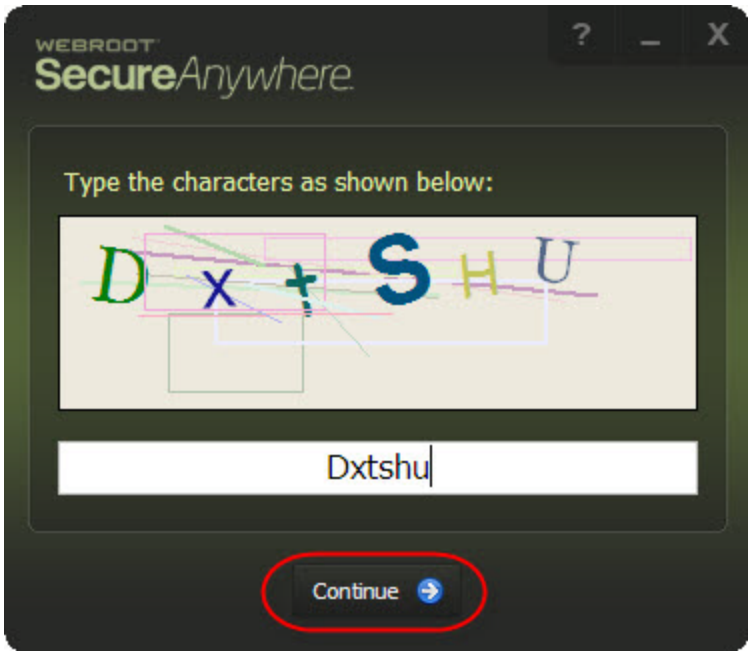
The system displays a CAPTCHA window.



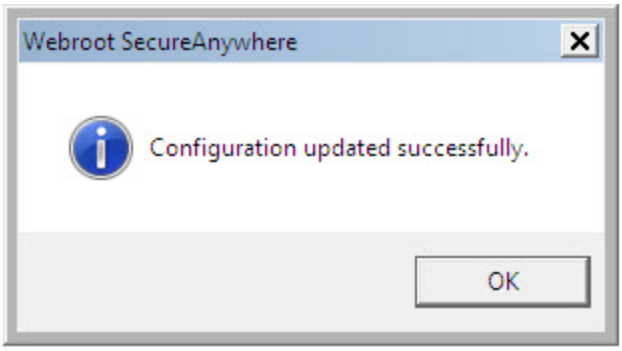
6. In the blank field, enter the characters as shown; letters are not case sensitive.



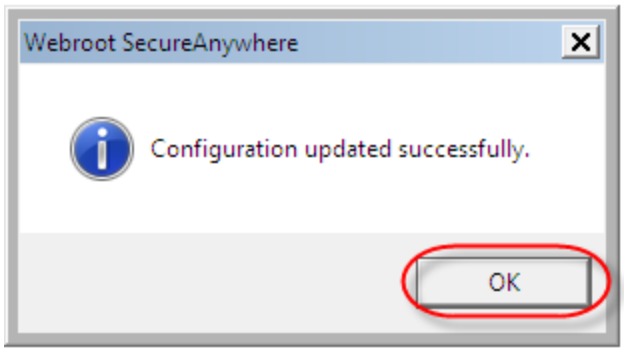
7. Click the **Continue** button.



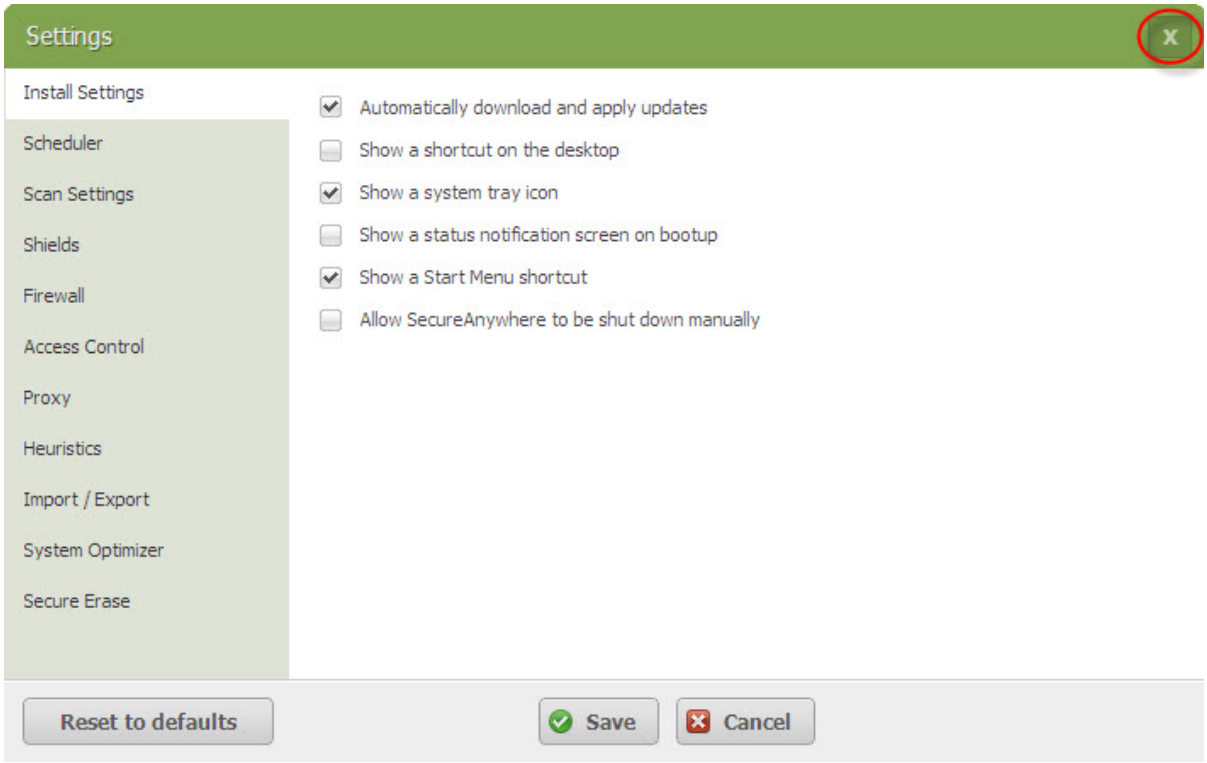
The system displays a success message.



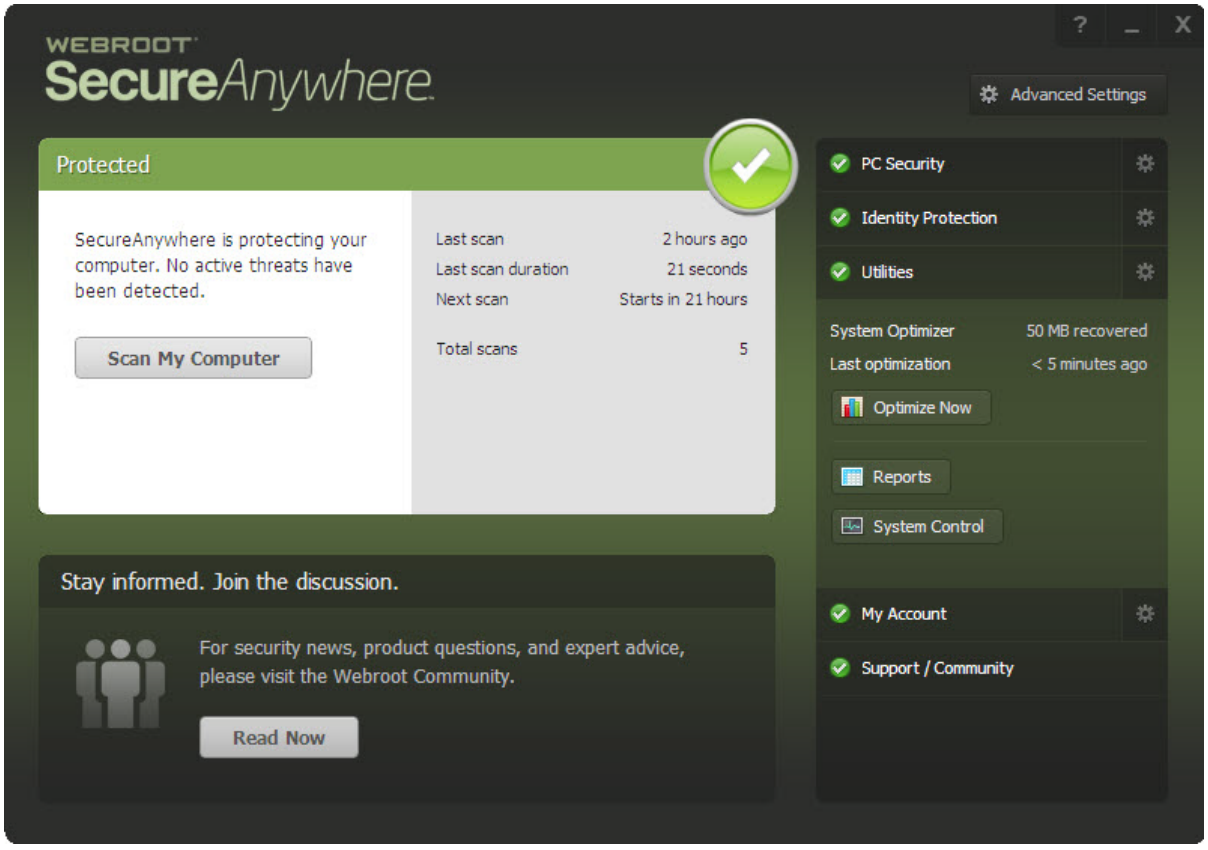
8. Click the **OK** button.



9. To return to the main interface, in the upper right corner, click the **X**.



The main interface displays.


WEBROOT
SecureAnywhere
Advanced Settings
Protected
SecureAnywhere is protecting your computer. No active threats have been detected.
Scan My Computer
Last scan 2 hours ago
Last scan duration 21 seconds
Next scan Starts in 21 hours
Total scans 5
PC Security
Identity Protection
Utilities
System Optimizer 50 MB recovered
Last optimization < 5 minutes ago
Optimize Now
Reports
System Control
Stay informed. Join the discussion.
For security news, product questions, and expert advice, please visit the Webroot Community.
Read Now
My Account
Support / Community

Chapter 3: Managing Identity Protection

To manage Identity Protection, see the following topics:

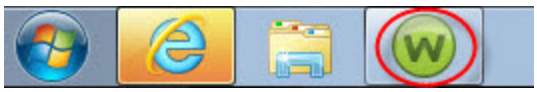
Changing Identity Shield Settings ***25***
Managing Protected Applications ***29***
Managing Protected Websites ***42***
Disabling Identity Shield ***50***

Changing Identity Shield Settings

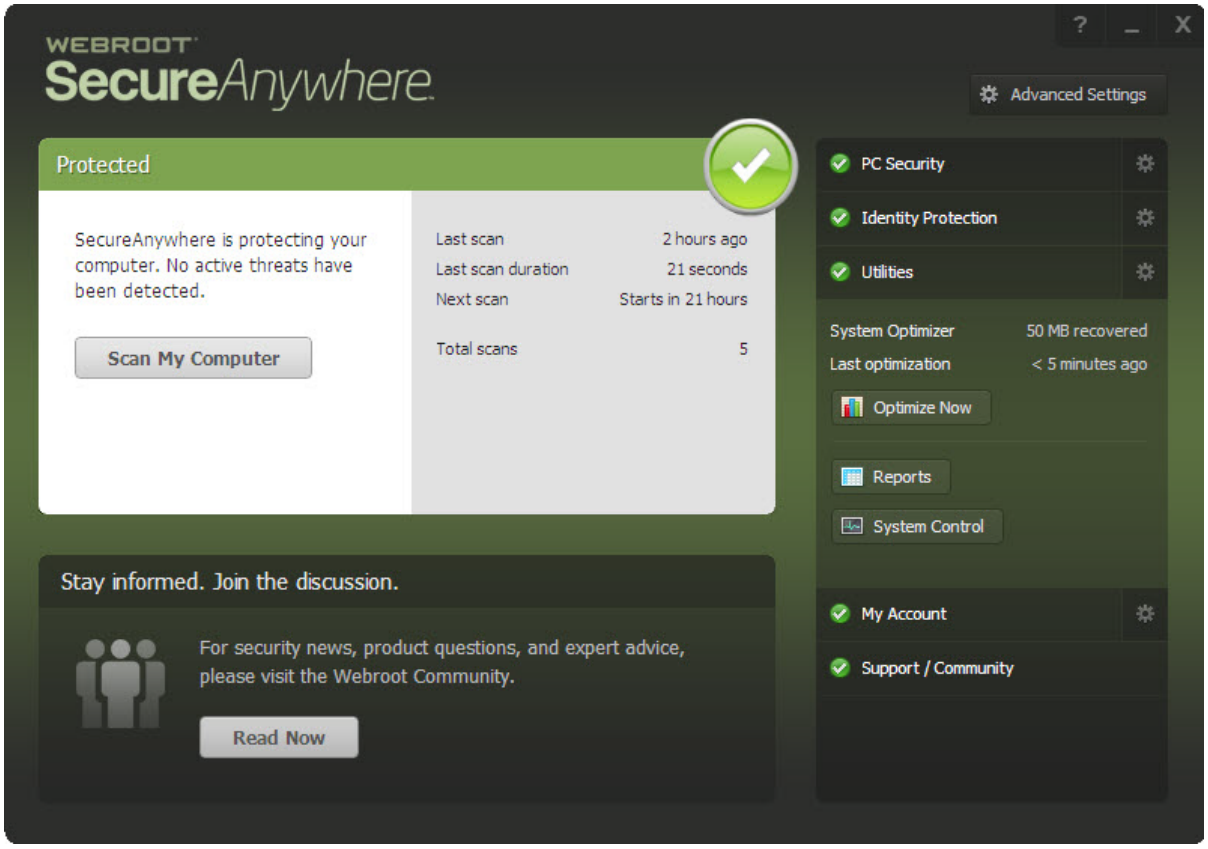
You can change the behavior of Identity Shield and control what it blocks, as described in this section. We recommend that you keep Webroot's default settings.

To change Identity Shield settings:

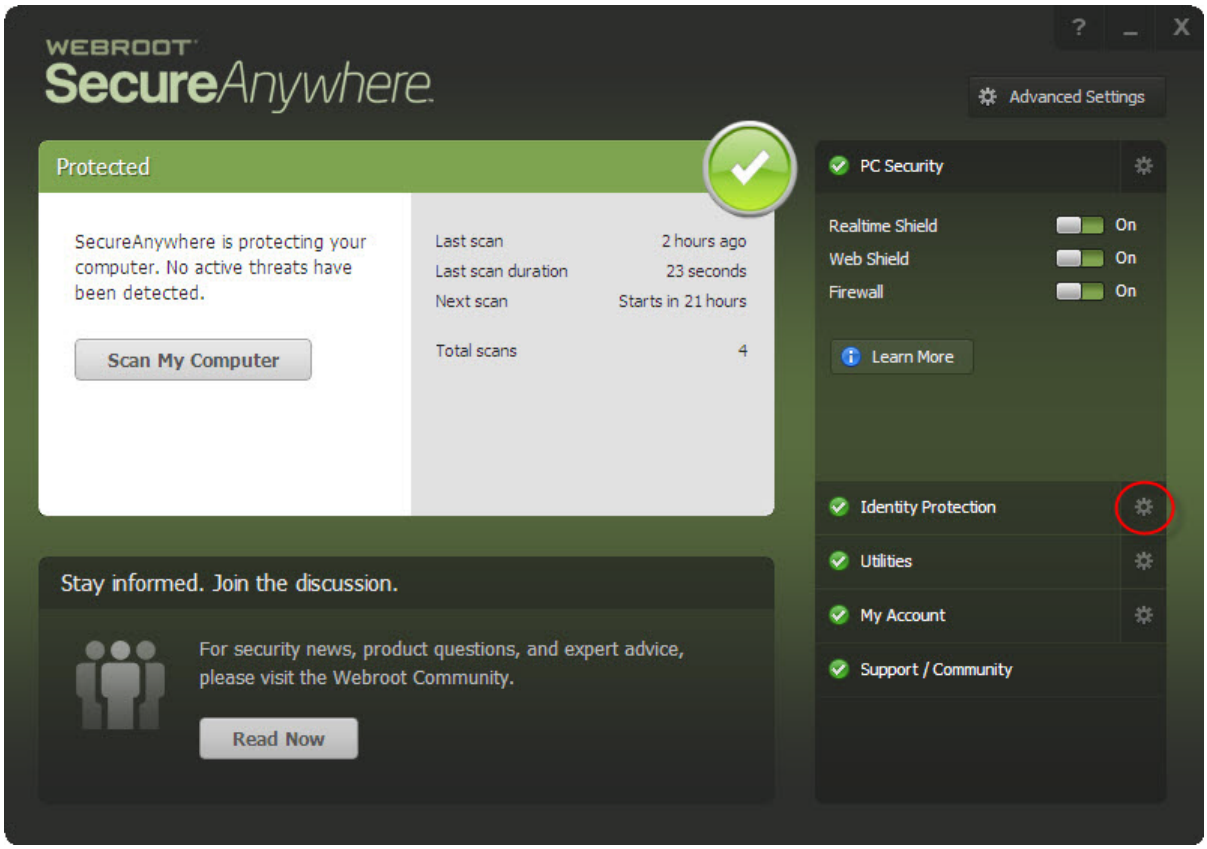
1. From the system tray, double-click the **Webroot** icon to display the main interface.



The main interface displays.



2. Click the **Identity Protection** tab.



The Identity Protection tab displays.

3. In the upper right corner, click the **Change Settings** link.

The Identity Shield settings window displays.

4. To change a setting, do either of the following:
   - To activate a setting, select the checkbox.
   - To deactivate a setting, deselect the checkbox.

The following table describes the checkbox settings:

CHECKBOX	DESCRIPTION
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 displays 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, a man-in-the-middle attack. If the shield detects a man-in-the-middle attack, it blocks the threat and displays 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.

CHECKBOX	DESCRIPTION
Warn before blocking untrusted programs from accessing protected data	Displays 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 display 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.

5. If you make changes and decide you want to return to the recommended settings, click the **Reset to Defaults** button.
6. When you're done, click the **Save All** button.

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 such as:

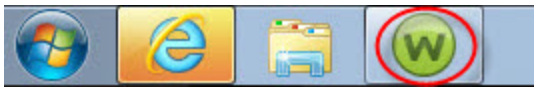
- Keyloggers
- Man-in-the-middle attacks
- Clipboard stealers

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

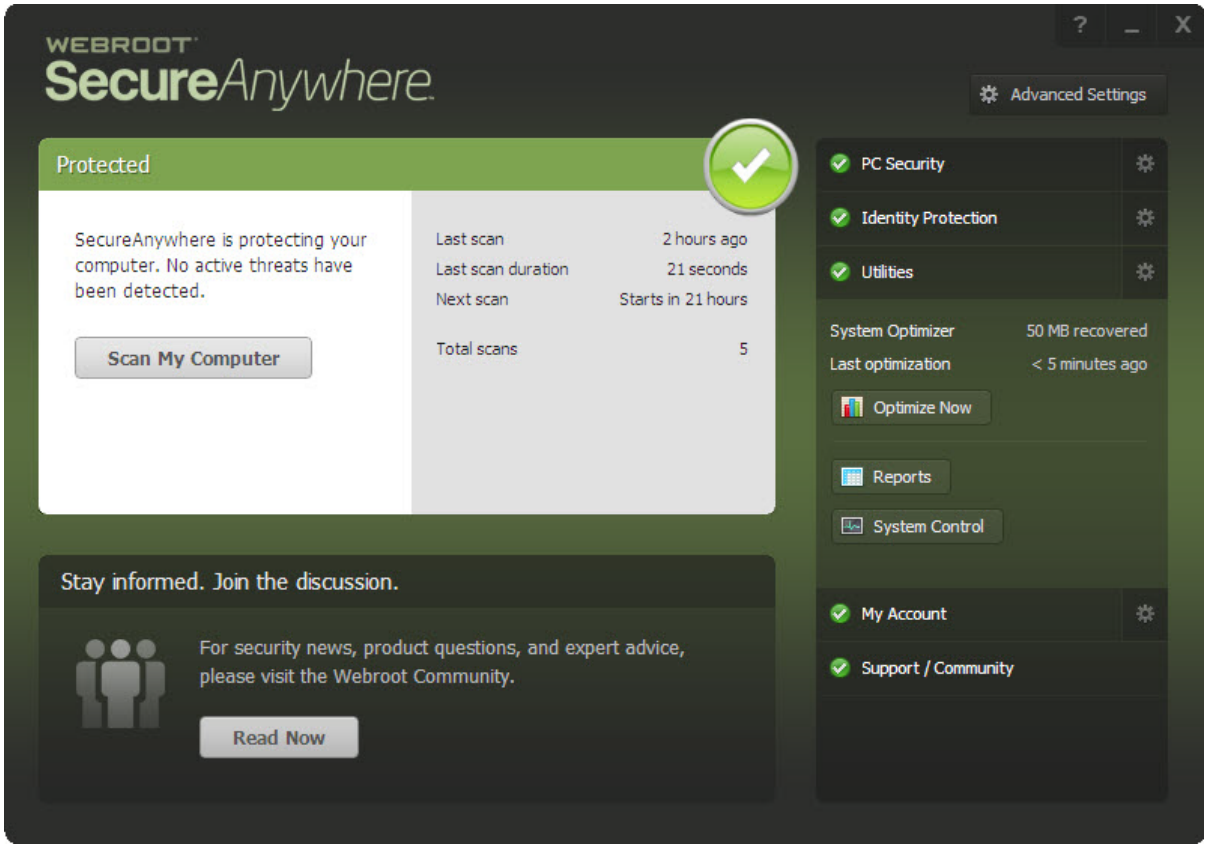
- Protect
- Allow
- Deny

To manage protected applications:

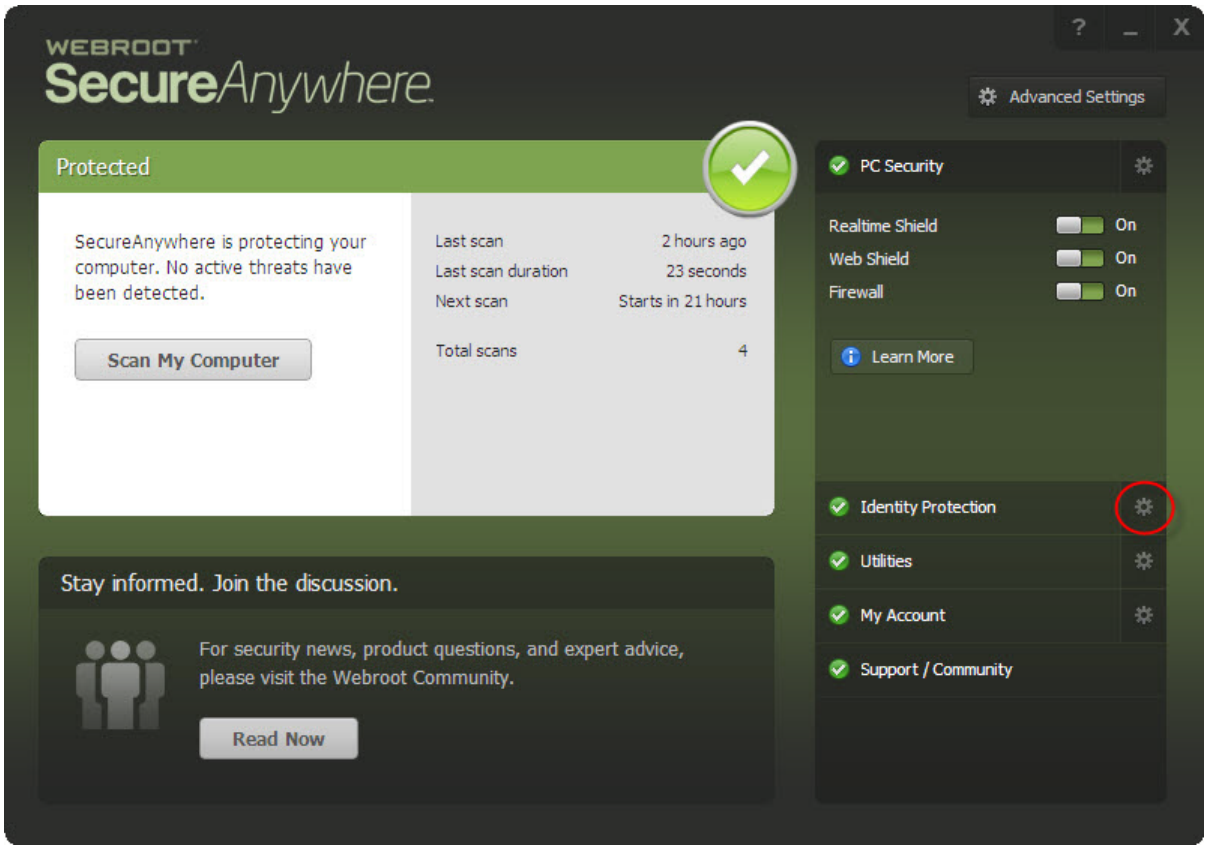
1. From the system tray, double-click the **Webroot** icon to display the main interface.

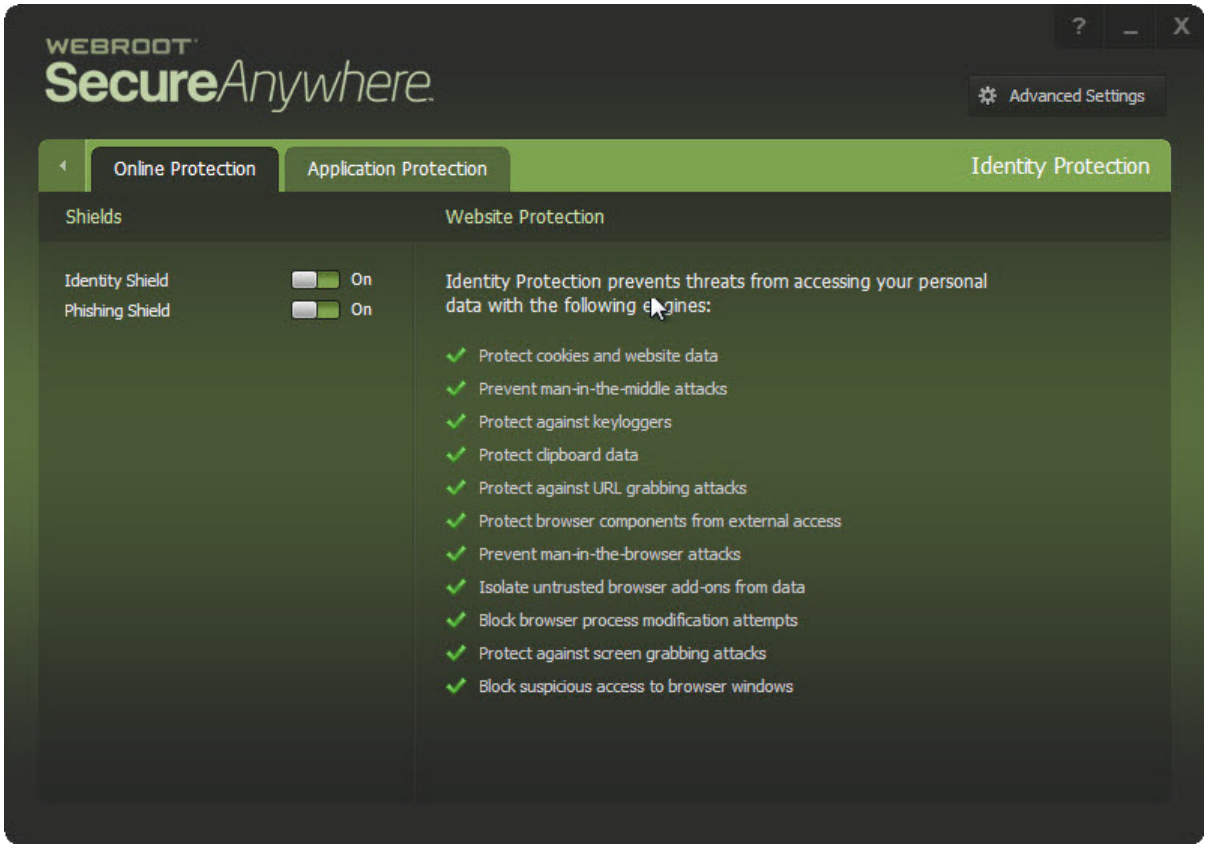
   The main interface displays.


WEBROOT
SecureAnywhere
Advanced Settings
Protected
SecureAnywhere is protecting your computer. No active threats have been detected.
Scan My Computer
Last scan 2 hours ago
Last scan duration 21 seconds
Next scan Starts in 21 hours
Total scans 5
PC Security
Identity Protection
Utilities
System Optimizer 50 MB recovered
Last optimization < 5 minutes ago
Optimize Now
Reports
System Control
Stay informed. Join the discussion.
For security news, product questions, and expert advice, please visit the Webroot Community.
Read Now
My Account
Support / Community

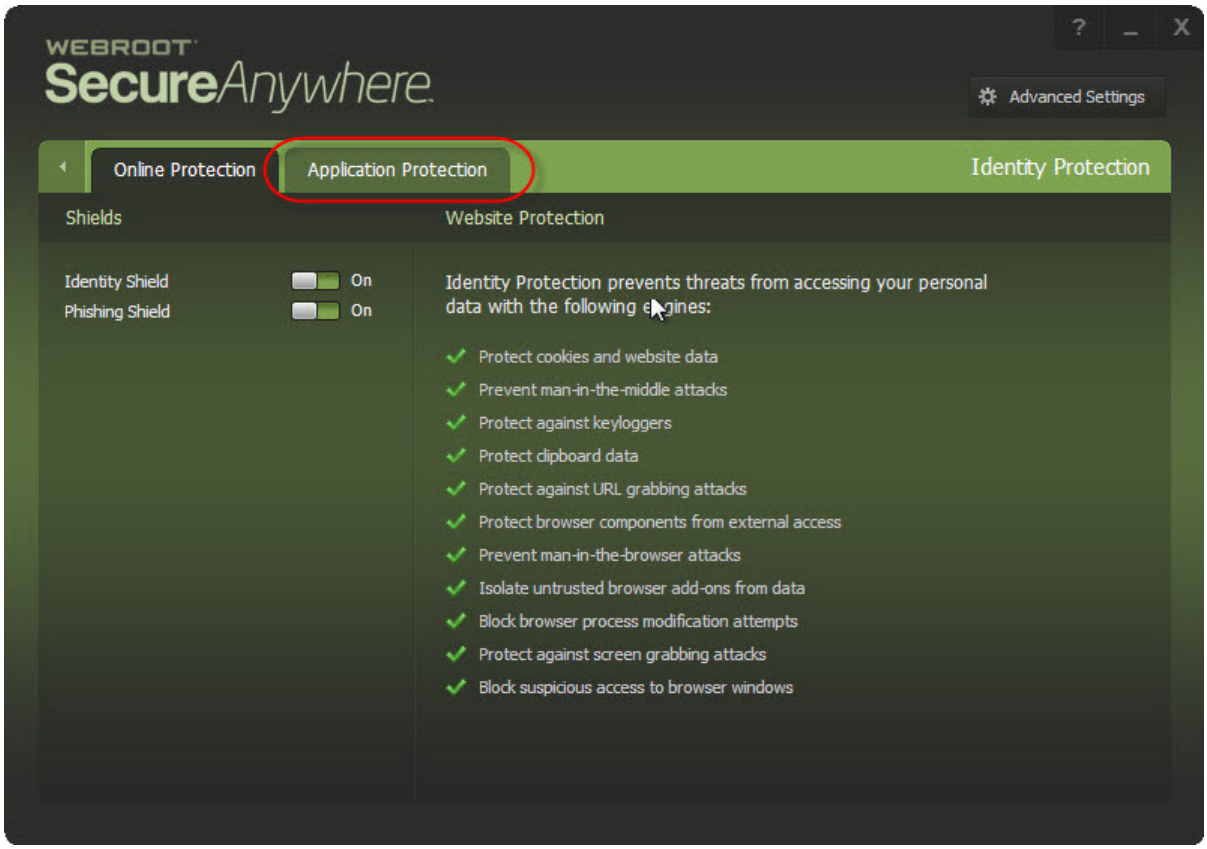
2. Click the **Identity Protection** gear icon.



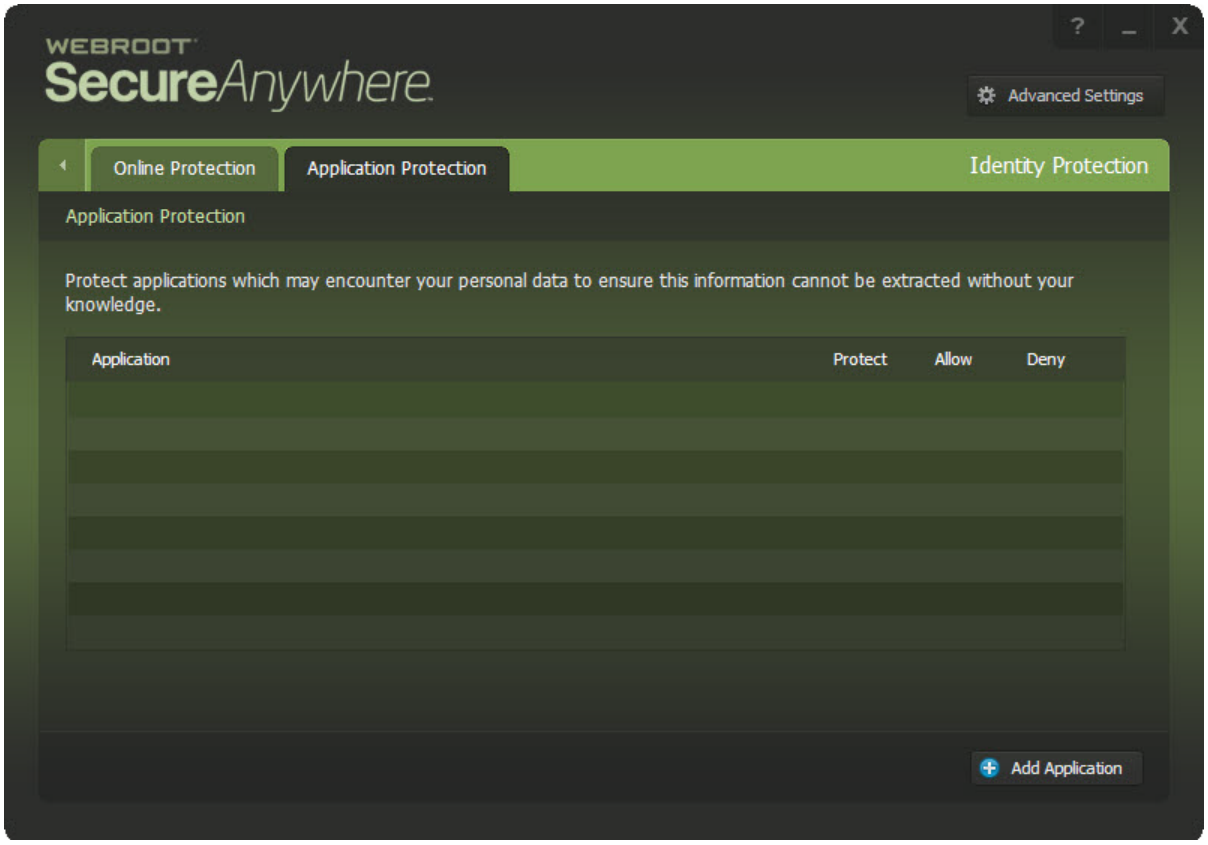
The Identity Protection interface displays.


WEBROOT
SecureAnywhere
Advanced Settings
Online Protection
Application Protection
Identity Protection
Shields
Website Protection
Identity Shield
On
Phishing Shield
On
Identity Protection prevents threats from accessing your personal data with the following engines:
Protect cookies and website data
Prevent man-in-the-middle attacks
Protect against keyloggers
Protect clipboard data
Protect against URL grabbing attacks
Protect browser components from external access
Prevent man-in-the-browser attacks
Isolate untrusted browser add-ons from data
Block browser process modification attempts
Protect against screen grabbing attacks
Block suspicious access to browser windows

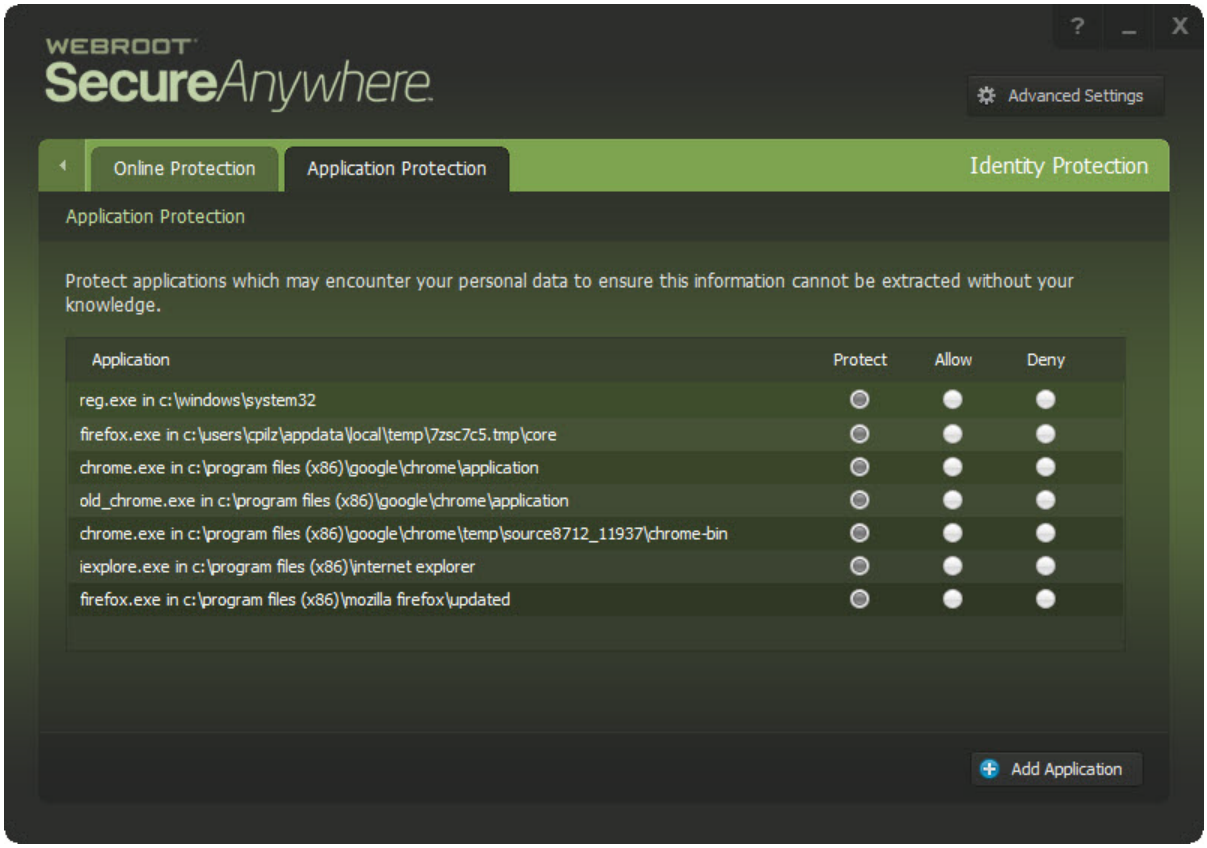
3. Click the **Application Protection** tab.



The Application Protection interface displays.



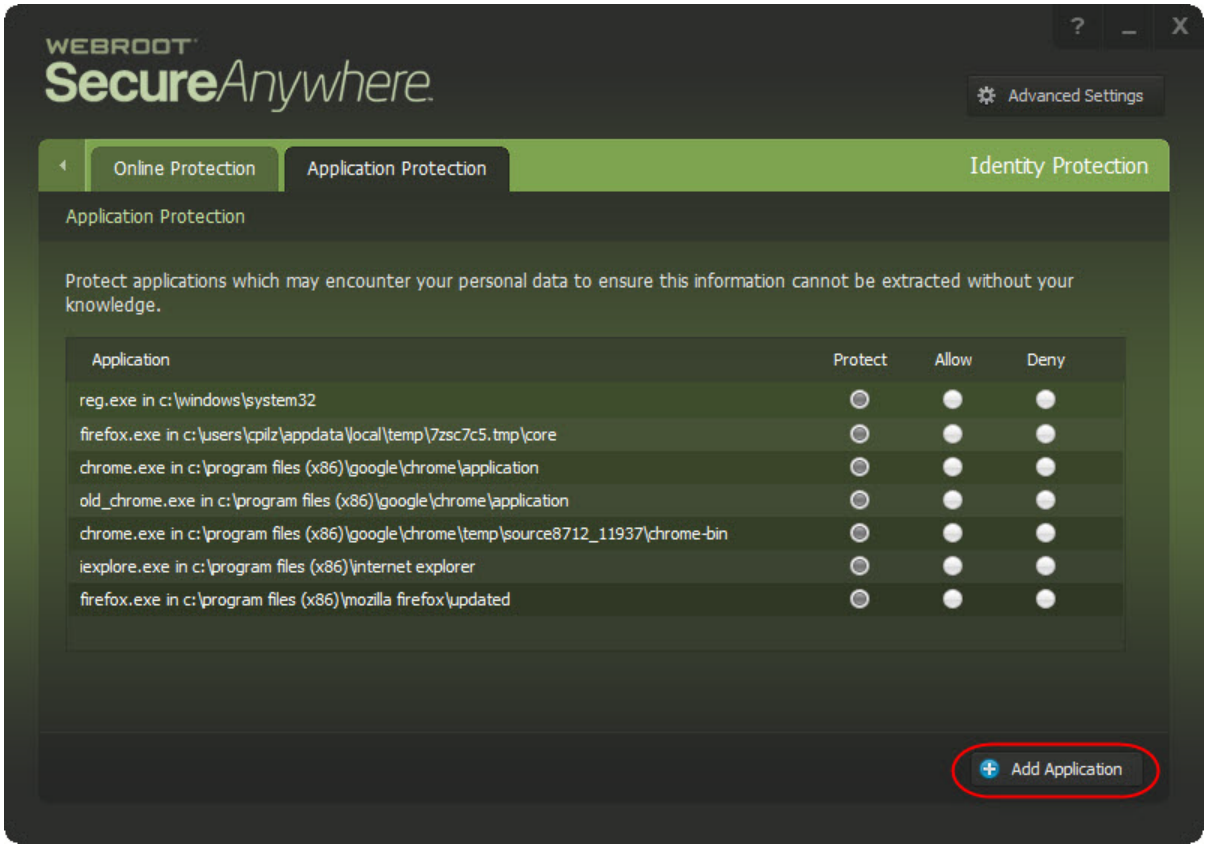
This interface lists the web browsers on your system and any other applications that you run on the computer.


WEBROOT
SecureAnywhere
Advanced Settings
Online Protection
Application Protection
Identity Protection
Application Protection
Protect applications which may encounter your personal data to ensure this information cannot be extracted without your knowledge.
Application
Protect
Allow
Deny
reg.exe in c:\windows\system32
firefox.exe in c:\users\cpilz\appdata\local\temp\7zsc7c5.tmp\core
chrome.exe in c:\program files (x86)\google\chrome\application
old_chrome.exe in c:\program files (x86)\google\chrome\application
chrome.exe in c:\program files (x86)\google\chrome\temp\source8712_11937\chrome-bin
iexplore.exe in c:\program files (x86)\internet explorer
firefox.exe in c:\program files (x86)\mozilla firefox\updated
Add Application

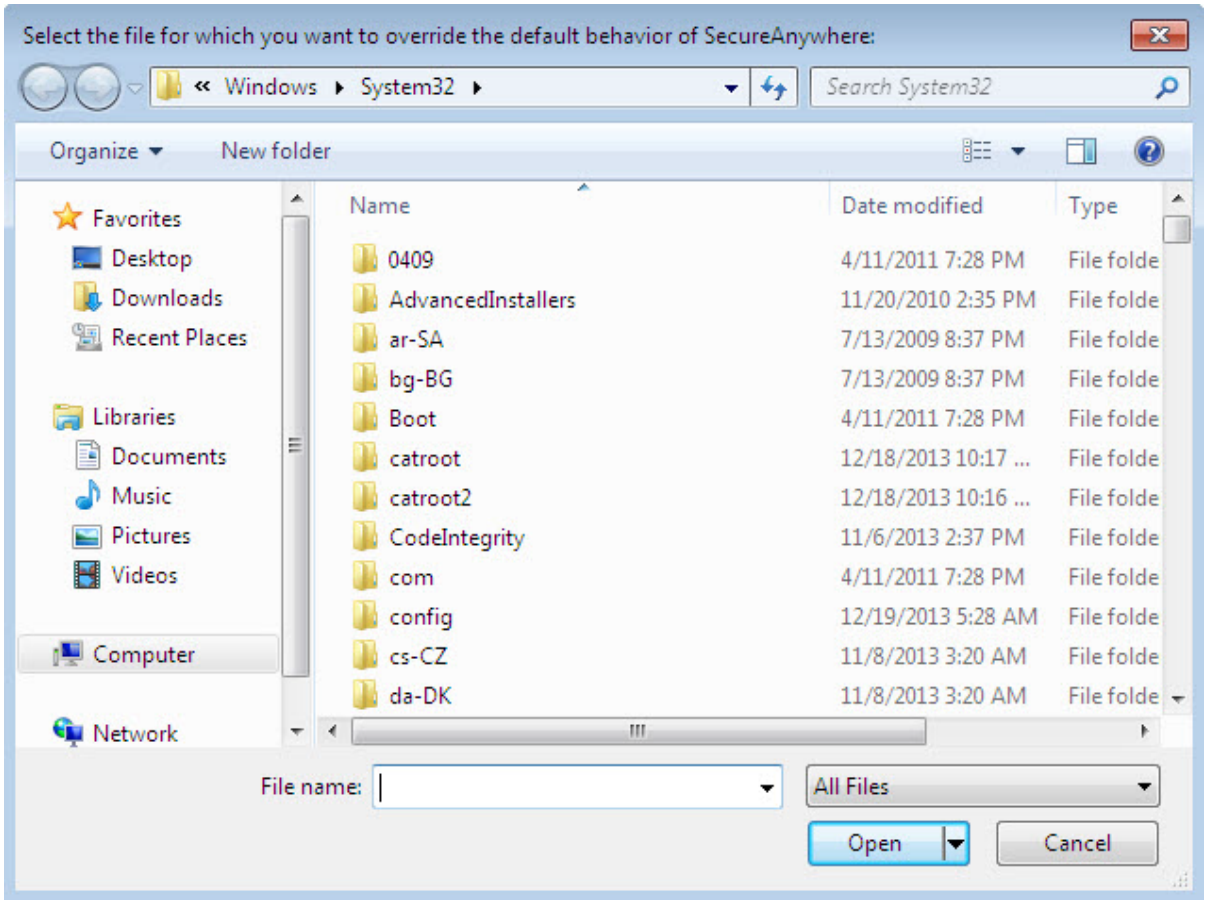
4. In the row for the application you want to modify, select the radio button for one of the following:

RADIO BUTTON	DESCRIPTION
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 the protect status. You can to add other software applications to protect level, 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.

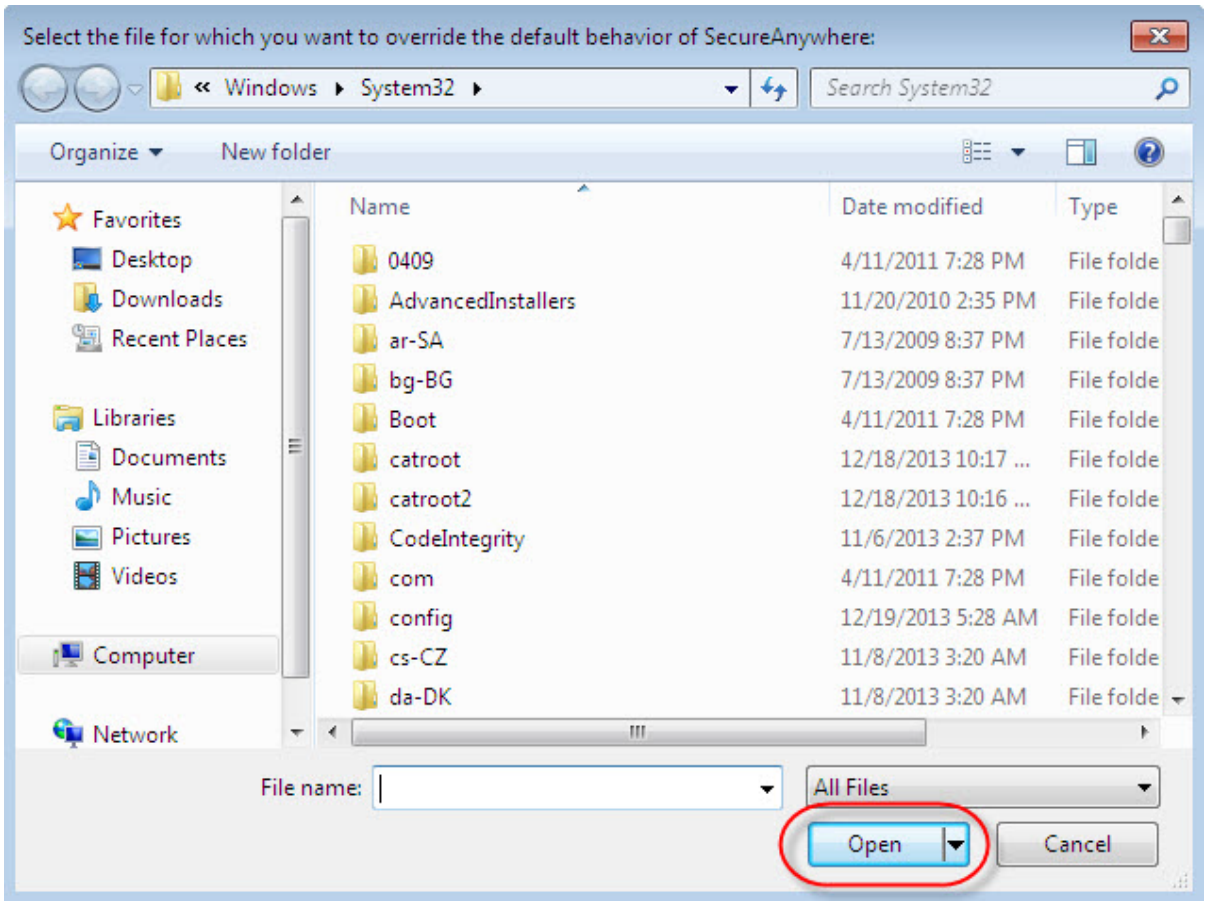
5. To include another application in this list, click the **Add Application** button.



The system displays a browser window. Browse to the executable file you want to add to the Application Protection list.

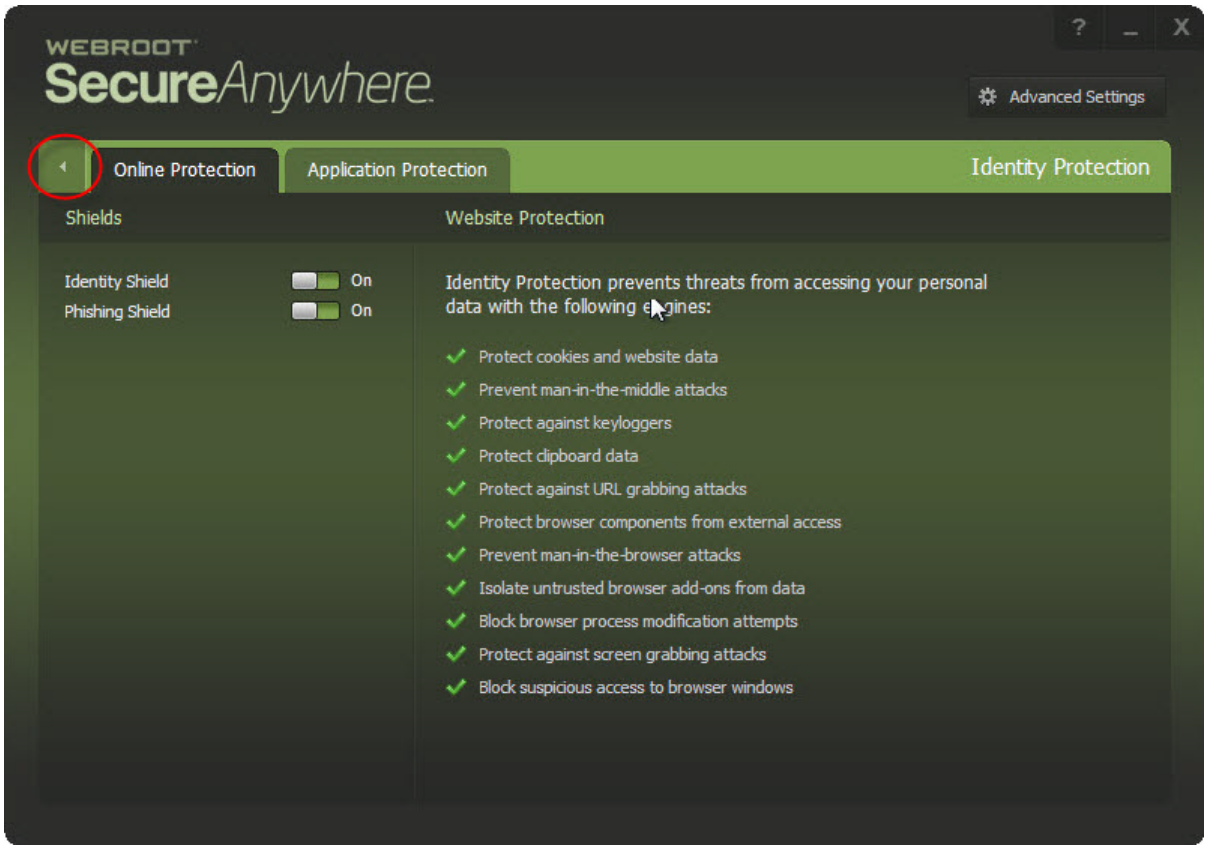

Select the file for which you want to override the default behavior of SecureAnywhere:
« Windows ▸ System32 ▸
Search System32
Organize
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Name
Date modified
Type
0409 4/11/2011 7:28 PM File folde
AdvancedInstallers 11/20/2010 2:35 PM File folde
ar-SA 7/13/2009 8:37 PM File folde
bg-BG 7/13/2009 8:37 PM File folde
Boot 4/11/2011 7:28 PM File folde
catroot 12/18/2013 10:17 ... File folde
catroot2 12/18/2013 10:16 ... File folde
CodeIntegrity 11/6/2013 2:37 PM File folde
com 4/11/2011 7:28 PM File folde
config 12/19/2013 5:28 AM File folde
cs-CZ 11/8/2013 3:20 AM File folde
da-DK 11/8/2013 3:20 AM File folde
File name:
All Files
Open
Cancel

6. When you have found the executable file, click the **Open** button.

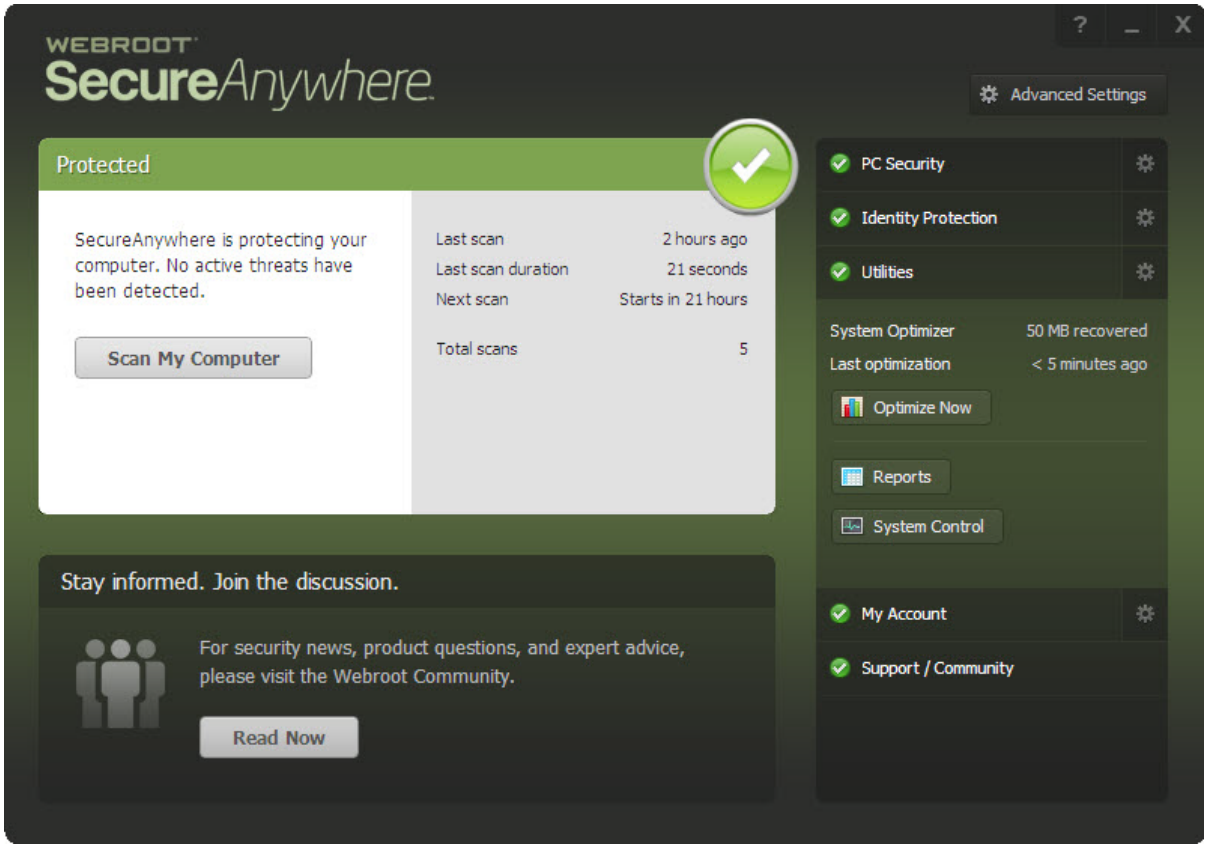


The system adds the file to the Application Protection list.

7. When you're done, click the **Back** arrow to return to the main interface.



The main interface displays.


WEBROOT
SecureAnywhere
Advanced Settings
Protected
SecureAnywhere is protecting your computer. No active threats have been detected.
Scan My Computer
Last scan 2 hours ago
Last scan duration 21 seconds
Next scan Starts in 21 hours
Total scans 5
PC Security
Identity Protection
Utilities
System Optimizer 50 MB recovered
Last optimization < 5 minutes ago
Optimize Now
Reports
System Control
Stay informed. Join the discussion.
For security news, product questions, and expert advice, please visit the Webroot Community.
Read Now
My Account
Support / Community

Managing Protected Websites

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

- None
- Low
- Medium
- High
- Maximum

Identity Shield only protects a secured website when the browser window is active in the foreground window; the padlock displays in the tray icon.

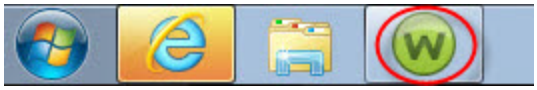
For full protection from screen grabbers, information-stealing Trojans, and other threats, make sure the browser window is in the foreground and the padlock is displayed in the tray icon. If Identity Shield encounters a website that may be a threat, it displays an alert.

If an alert displays, do one of the following:

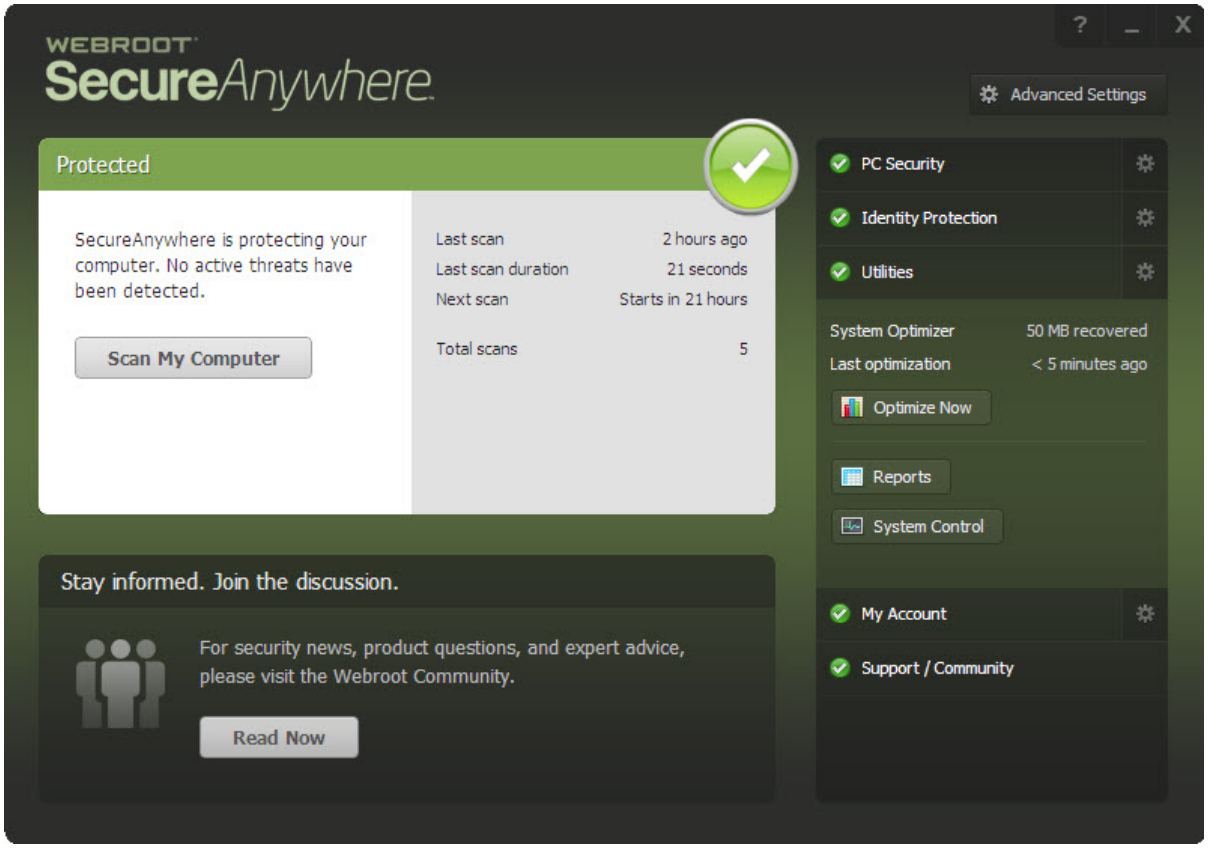
- **To stay secure** — Click the **Block** button.
- **To continue despite the warning** — Click the **Allow** button.

To manage protected websites:

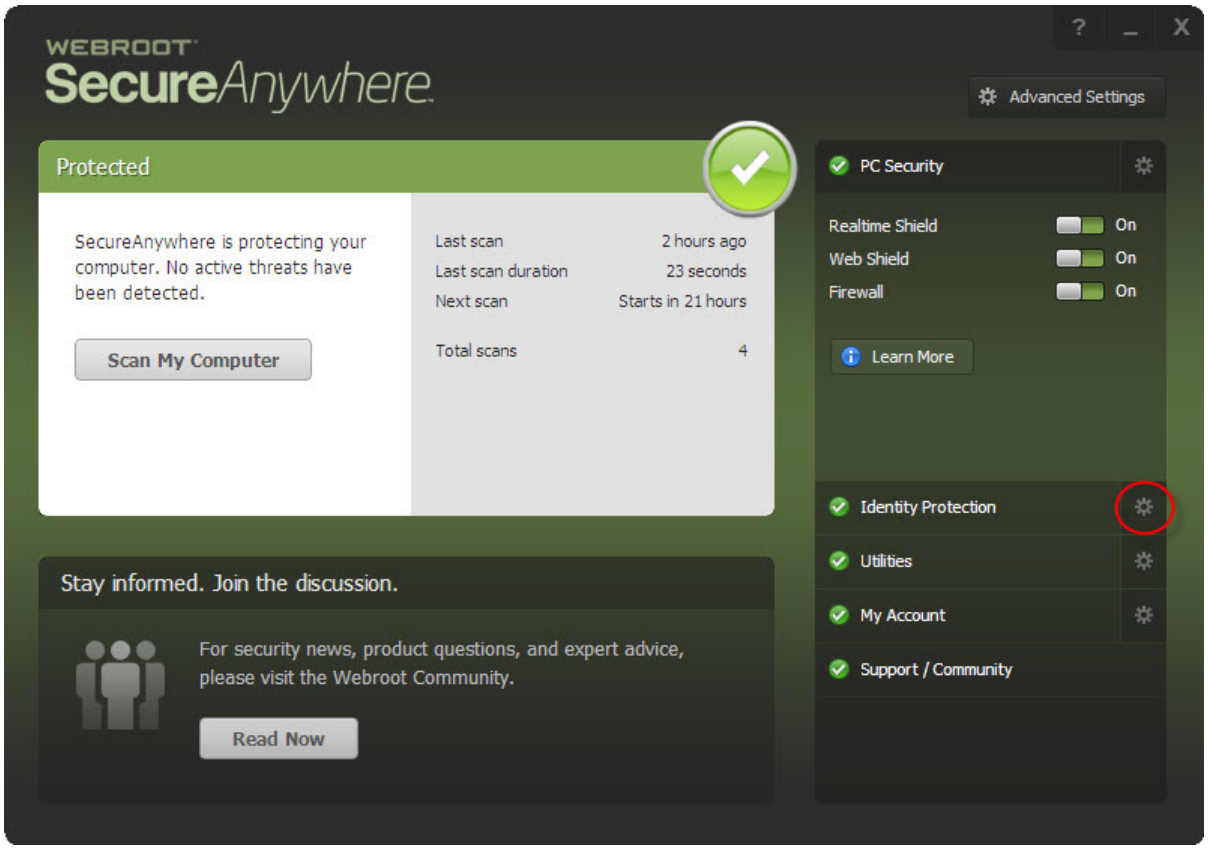
1. From the system tray, double-click the **Webroot** icon to display the main interface.



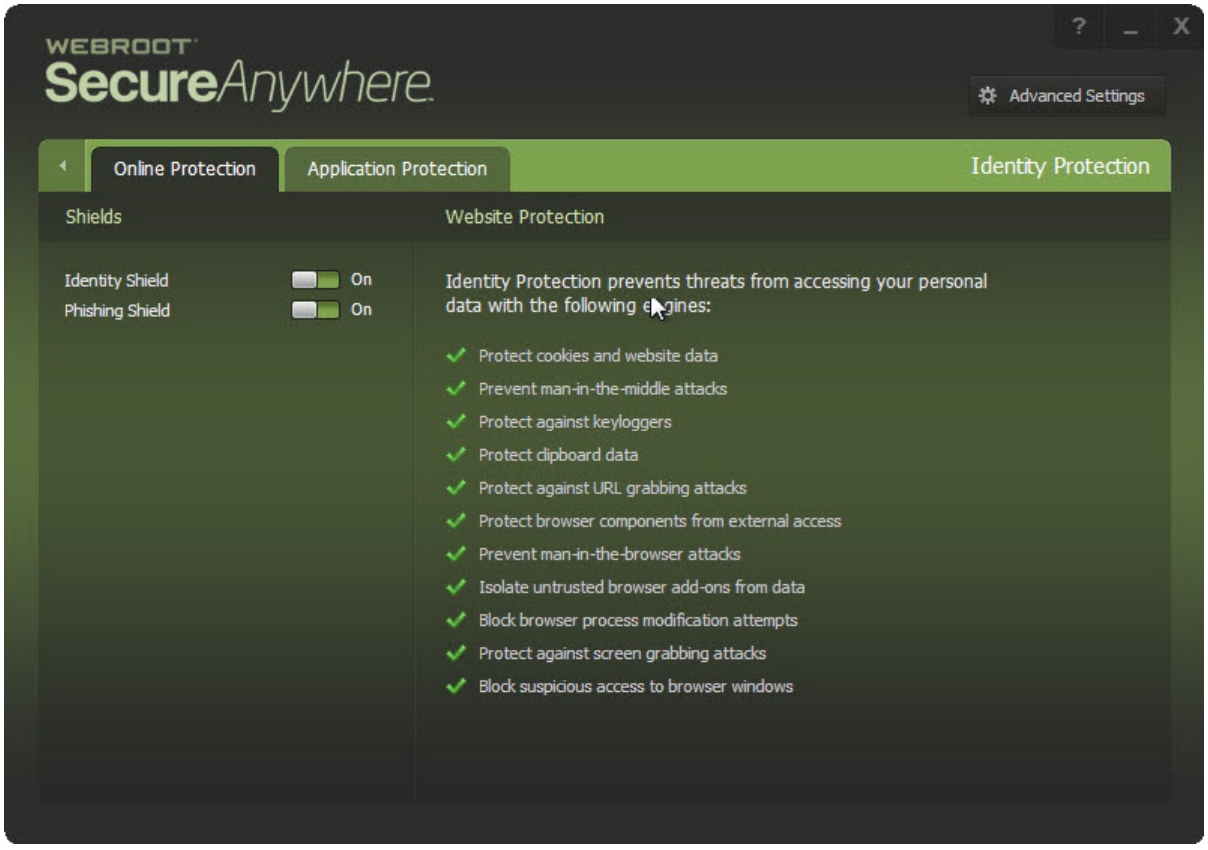
The main interface displays.


WEBROOT
SecureAnywhere
Advanced Settings
Protected
SecureAnywhere is protecting your computer. No active threats have been detected.
Scan My Computer
Last scan 2 hours ago
Last scan duration 21 seconds
Next scan Starts in 21 hours
Total scans 5
PC Security
Identity Protection
Utilities
System Optimizer 50 MB recovered
Last optimization < 5 minutes ago
Optimize Now
Reports
System Control
Stay informed. Join the discussion.
For security news, product questions, and expert advice, please visit the Webroot Community.
Read Now
My Account
Support / Community

2. Click the **Identity Protection** gear icon.



The Identity Protection interface displays.



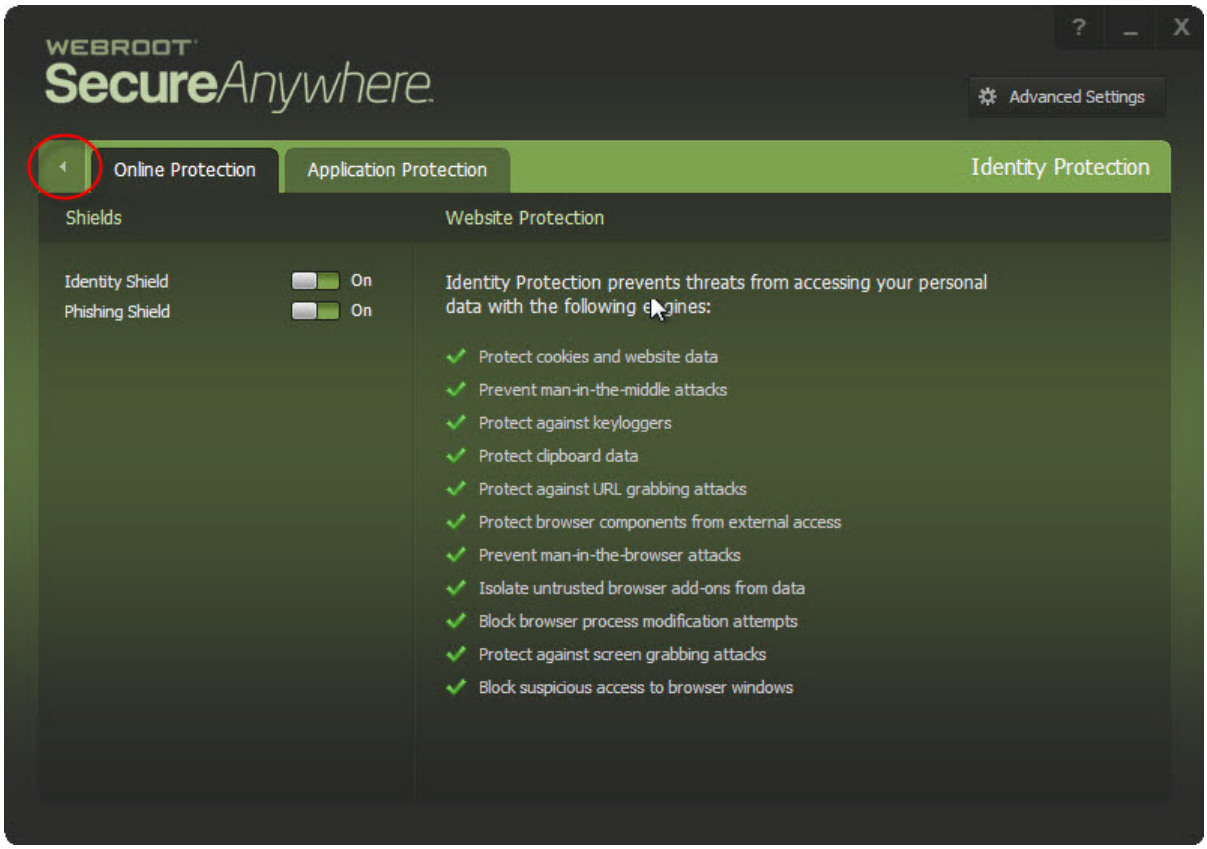
The following table describes the protection options.

OPTION	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.
Prevent man-in-the middle attacks	Intercepts main-in-the-middle attacks. A main-in-the-middle attack is when a server attempts to redirect you to a malicious website.
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.

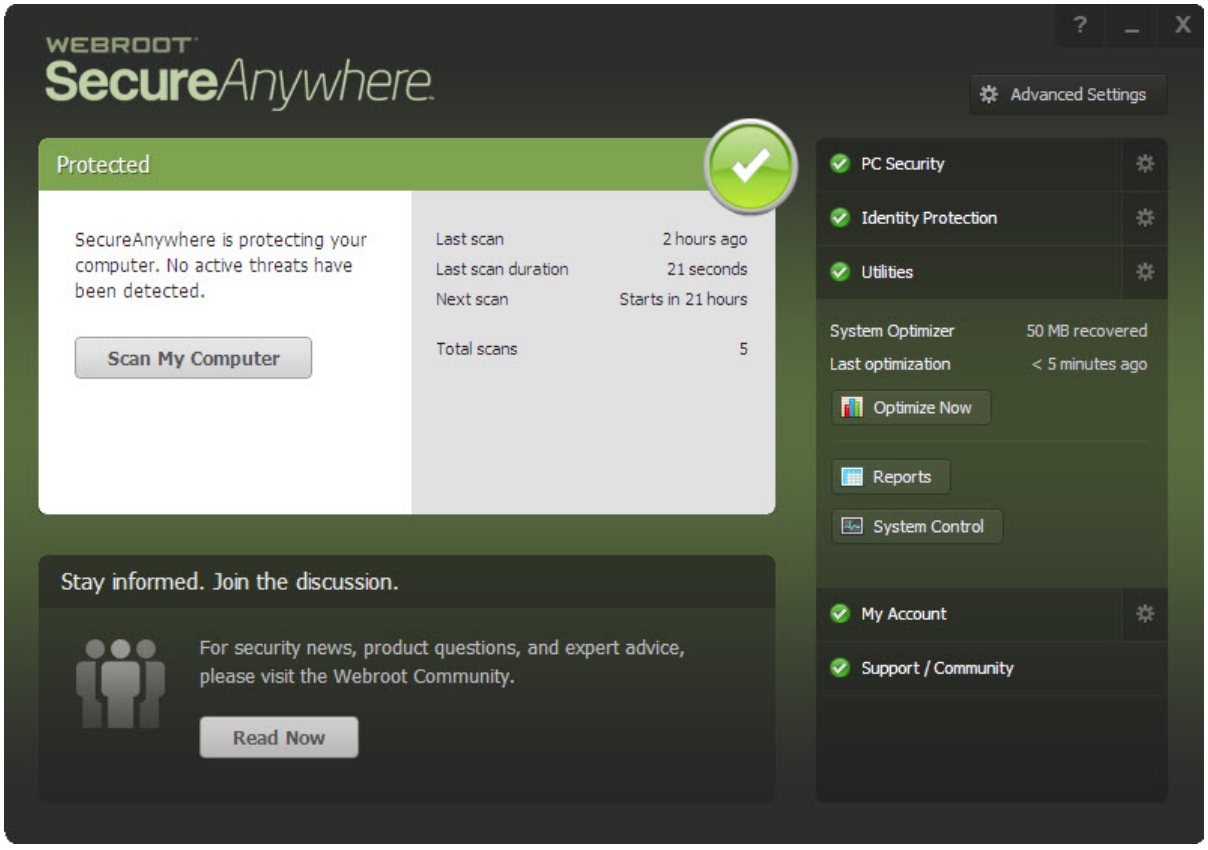
OPTION	DESCRIPTION
Protect against man-in-the-browser attack	Blocks a malicious toolbar from stealing data. A man-in-the-browser attack is a Trojan that infects a web browser. It can modify pages and the content of your transactions without being detected.
Isolate untrusted browser add-ons from data	Blocks a browser add-on, a browser helper object, from stealing data. While most browser add-ons are legitimate, some can display ads, track your Internet activity, or hijack your home page.
Block browser process modification attempts	Analyzes browser memory to see if code injection is taking place.
Protect against screen grabbing attacks	Blocks a malicious program from viewing and capturing your screen content.
Block suspicious access to browser windows	Blocks a malicious program from viewing and capturing data in Windows components.

For information about turning Identity Shield off, see *Disabling Identity Shield on page 50*.

3. When you're done, click the **Back** arrow.



The main interface displays.

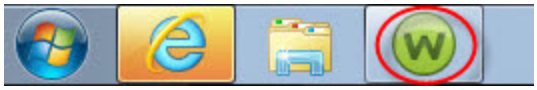

WEBROOT
SecureAnywhere
Advanced Settings
Protected
SecureAnywhere is protecting your computer. No active threats have been detected.
Scan My Computer
Last scan 2 hours ago
Last scan duration 21 seconds
Next scan Starts in 21 hours
Total scans 5
PC Security
Identity Protection
Utilities
System Optimizer 50 MB recovered
Last optimization < 5 minutes ago
Optimize Now
Reports
System Control
Stay informed. Join the discussion.
For security news, product questions, and expert advice, please visit the Webroot Community.
Read Now
My Account
Support / Community

Disabling Identity Shield

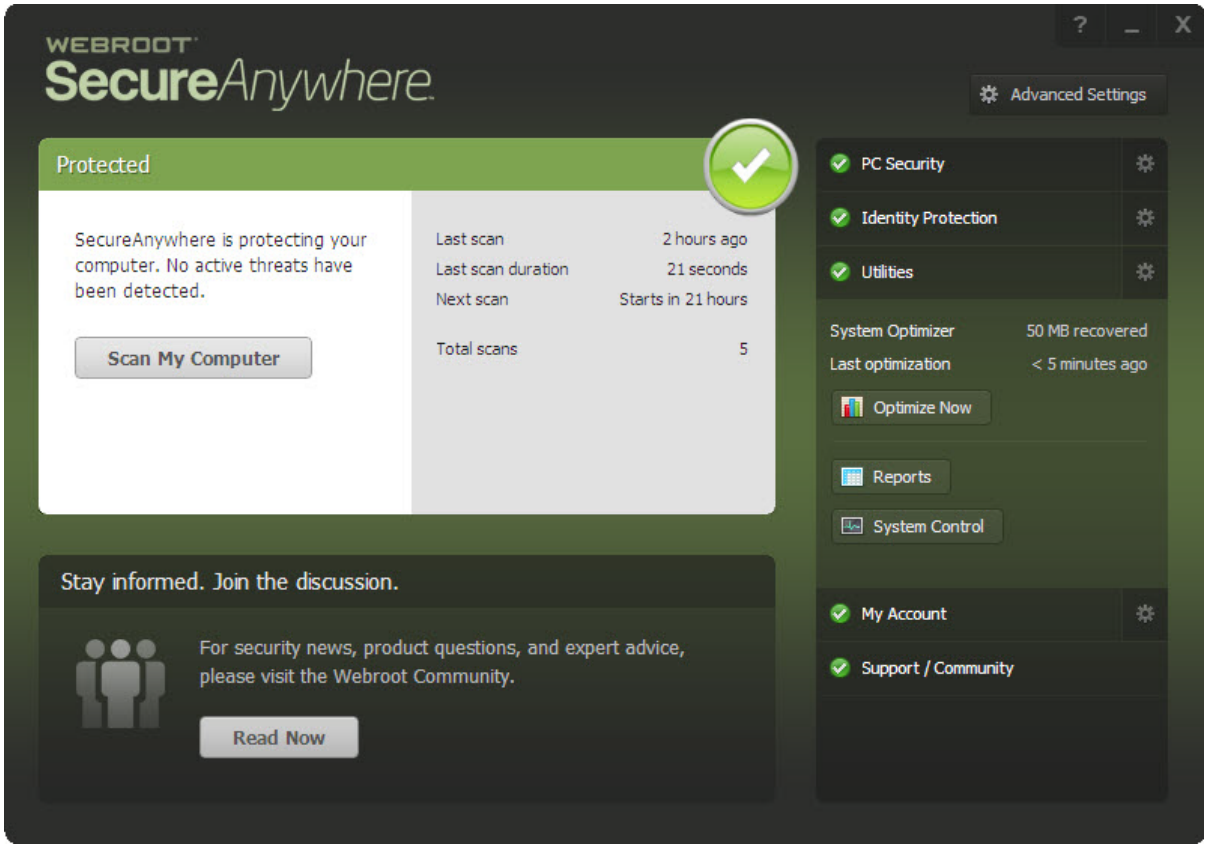
We recommend that you keep Identity Shield enabled; however, you can disable it if you want.

To disable Identity Shield:

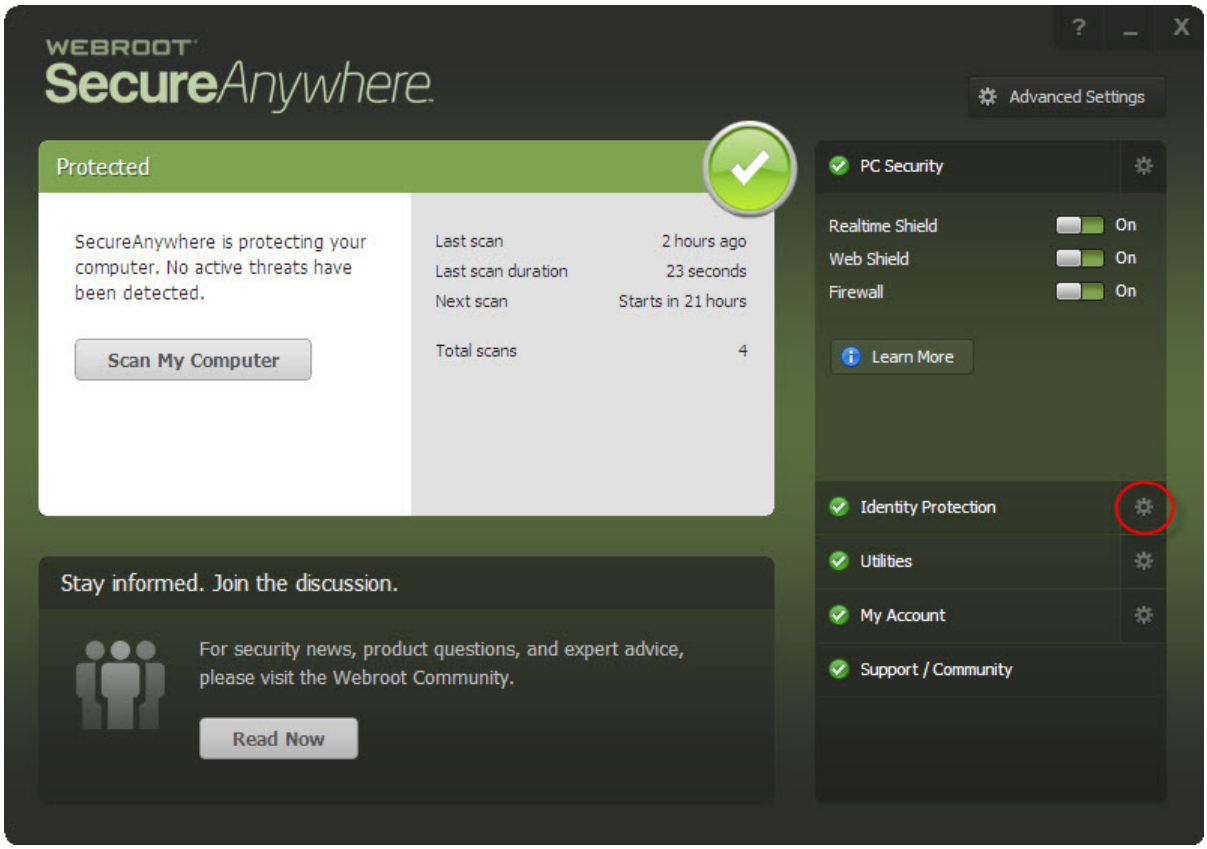
1. From the system tray, double-click the **Webroot** icon to display the main interface.



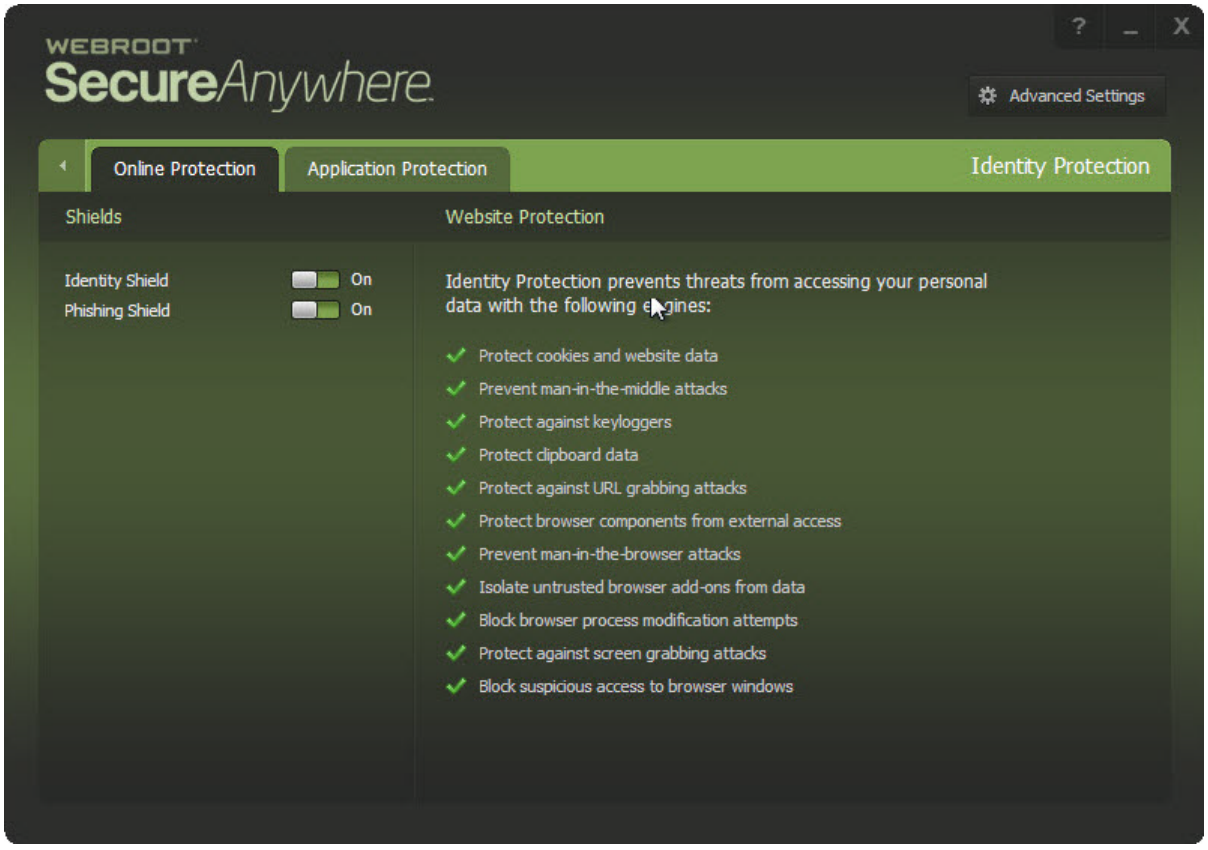
The main interface displays.



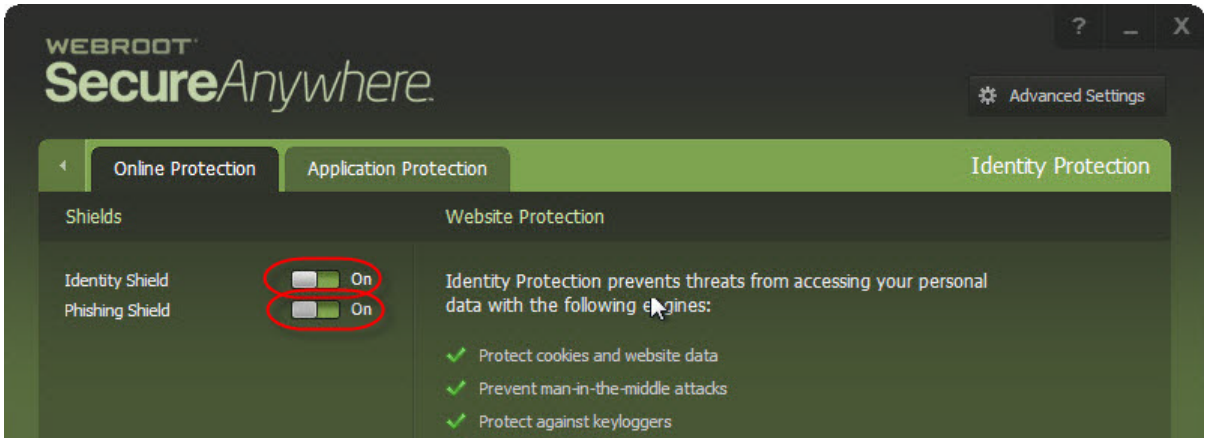
2. Click the **Identity Protection** gear icon.



The Identity Protection interface displays.

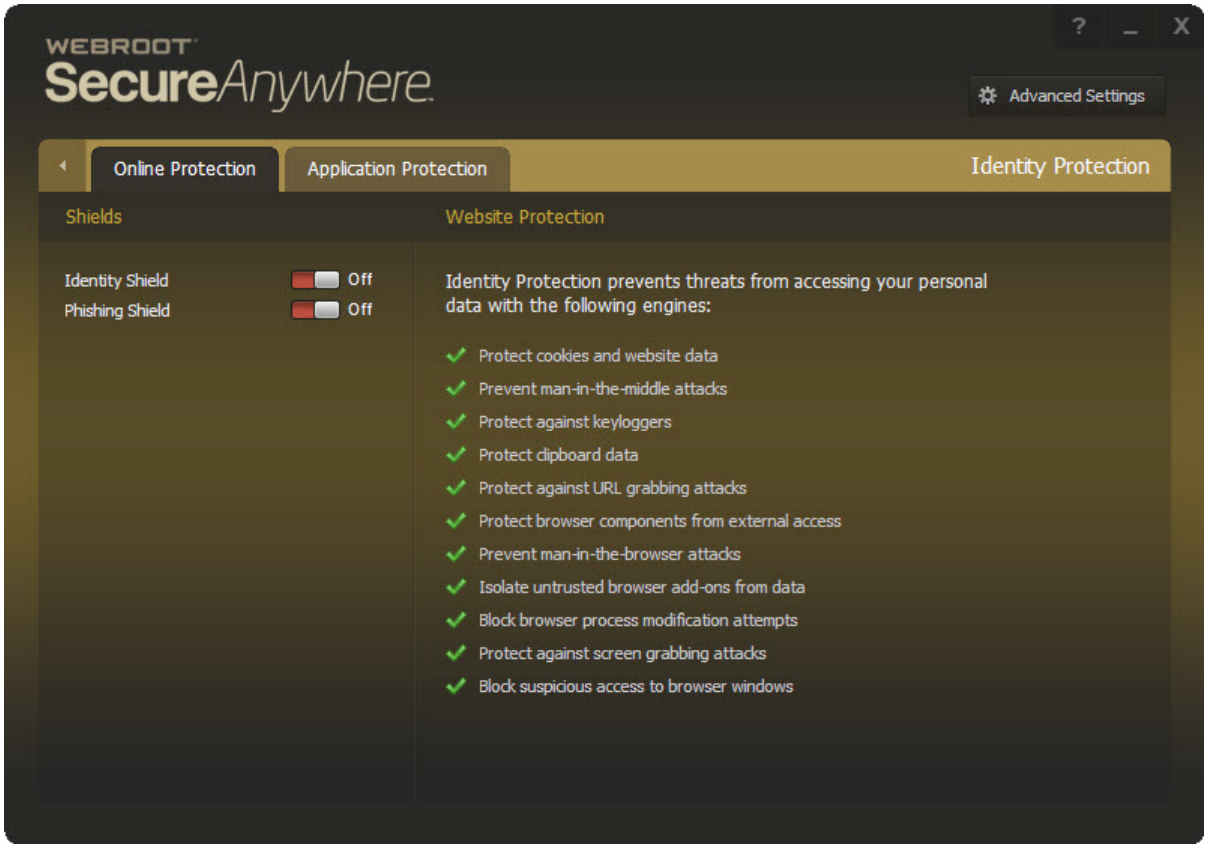


The Green button indicates that both shields are on.

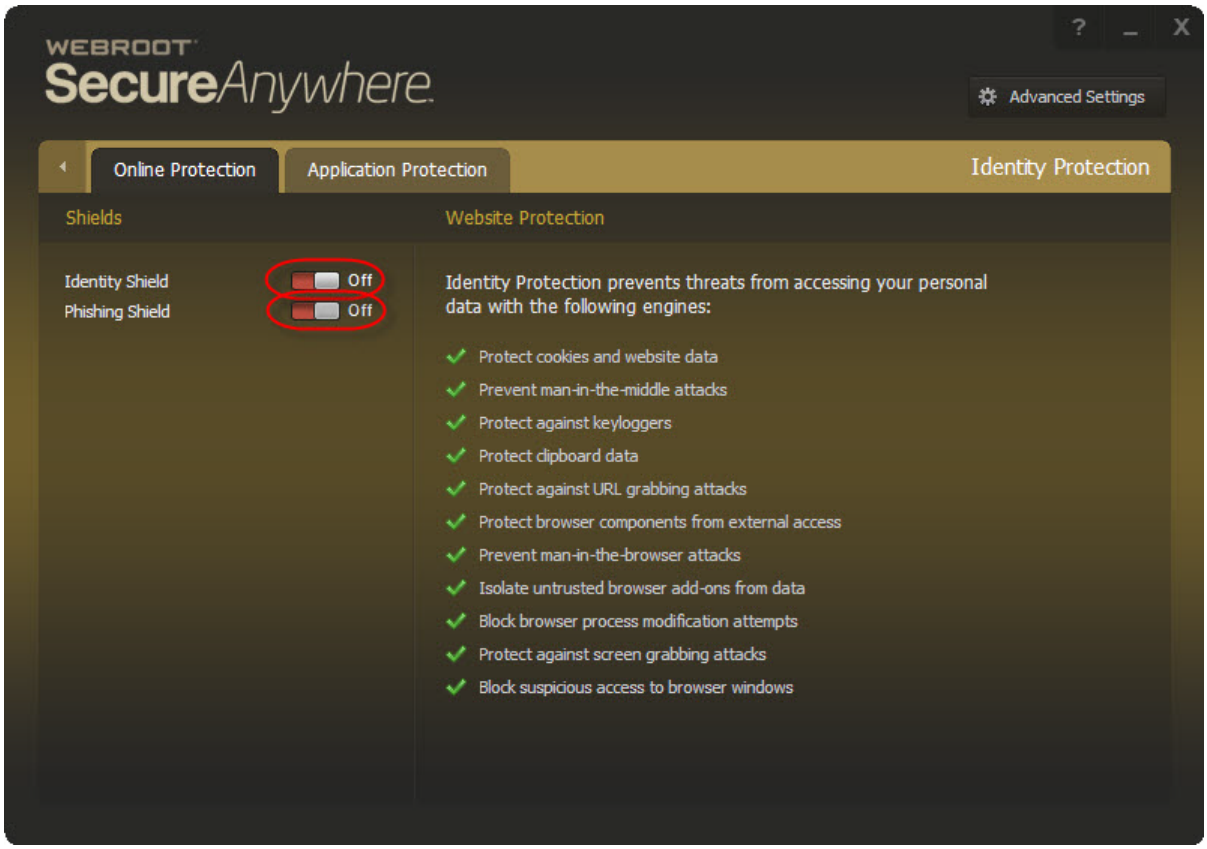


3. You can do either of the following:
   - To turn Identity Shield off, click **Green** button.
   - To turn Phishing Shield off, click the **Green** button.

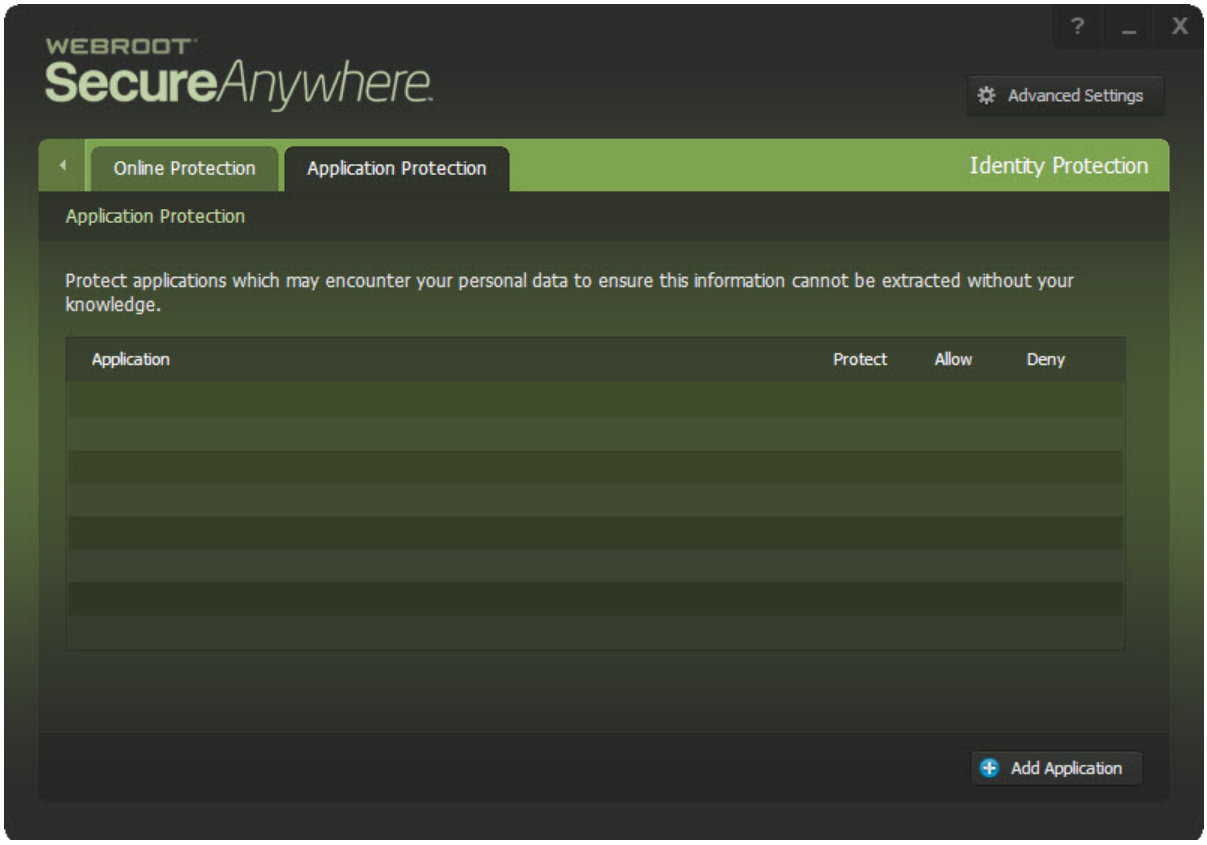
   When you turn a shield off, the button turns red and the interface turns brown, indicating that one or both shields is off.



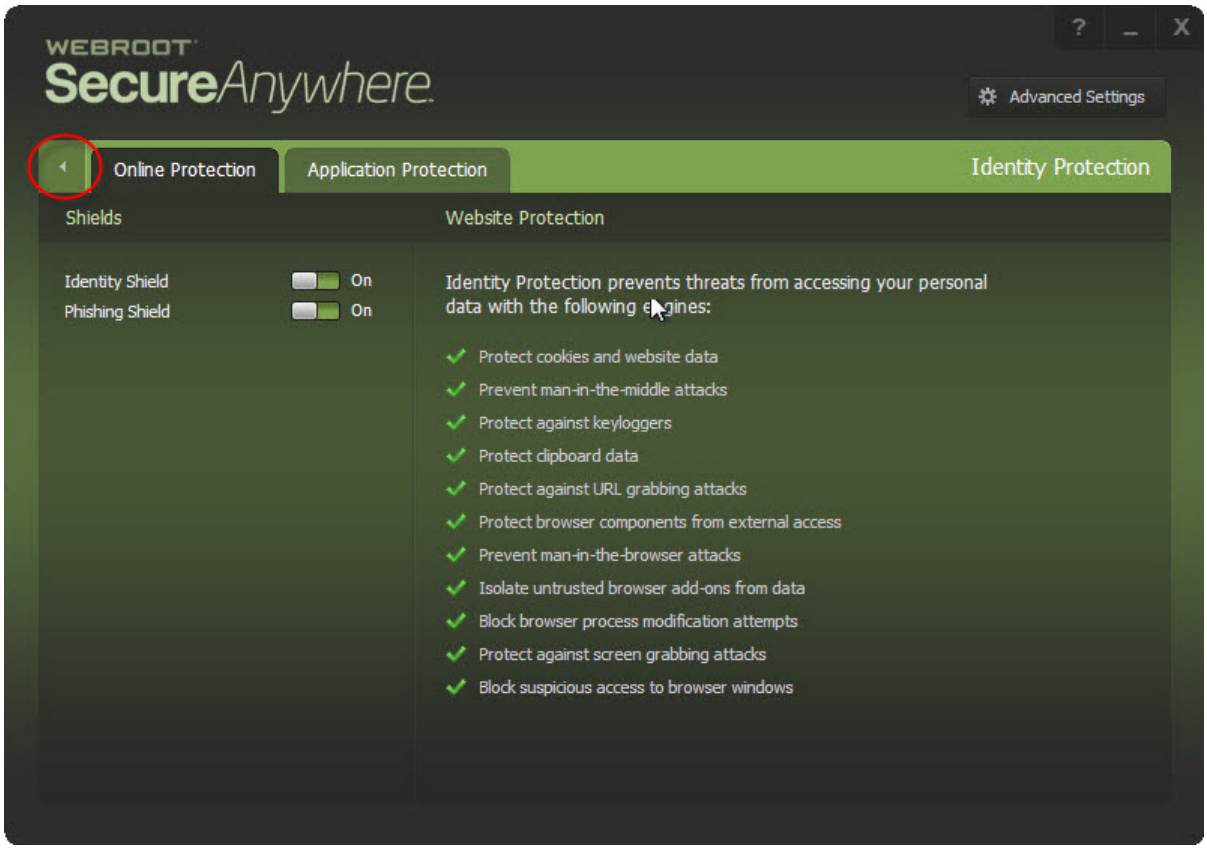
4. To turn either shield on again, click the **Red** button.



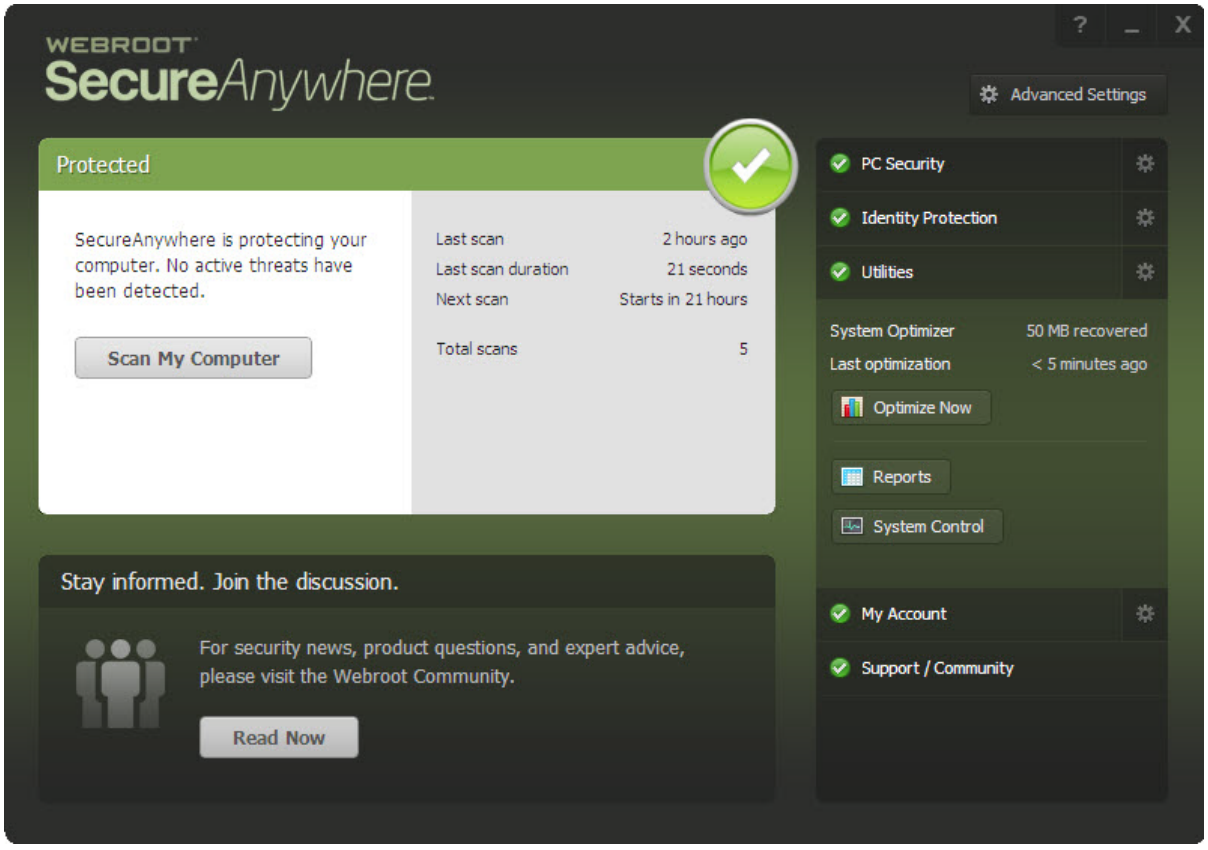
The buttons turn green and the interface turns green and black, indicating that the shields are on.


WEBROOT
SecureAnywhere
Advanced Settings
Online Protection
Application Protection
Identity Protection
Application Protection
Protect applications which may encounter your personal data to ensure this information cannot be extracted without your knowledge.
Application
Protect
Allow
Deny
Add Application

5. When you're done, click the **Back** arrow to return to the main interface.



The main interface displays.


WEBROOT
SecureAnywhere
Advanced Settings
Protected
SecureAnywhere is protecting your computer. No active threats have been detected.
Scan My Computer
Last scan 2 hours ago
Last scan duration 21 seconds
Next scan Starts in 21 hours
Total scans 5
PC Security
Identity Protection
Utilities
System Optimizer 50 MB recovered
Last optimization < 5 minutes ago
Optimize Now
Reports
System Control
Stay informed. Join the discussion.
For security news, product questions, and expert advice, please visit the Webroot Community.
Read Now
My Account
Support / Community

Chapter 4: Managing Your Account

To manage your account, see the following topics:

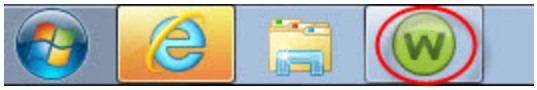
Viewing Your Account Details ***59***
Shutting Down Identity Shield ***66***
Uninstalling Identity Shield ***69***
Upgrading to a Threat Removal Version ***70***

Viewing Your Account Details

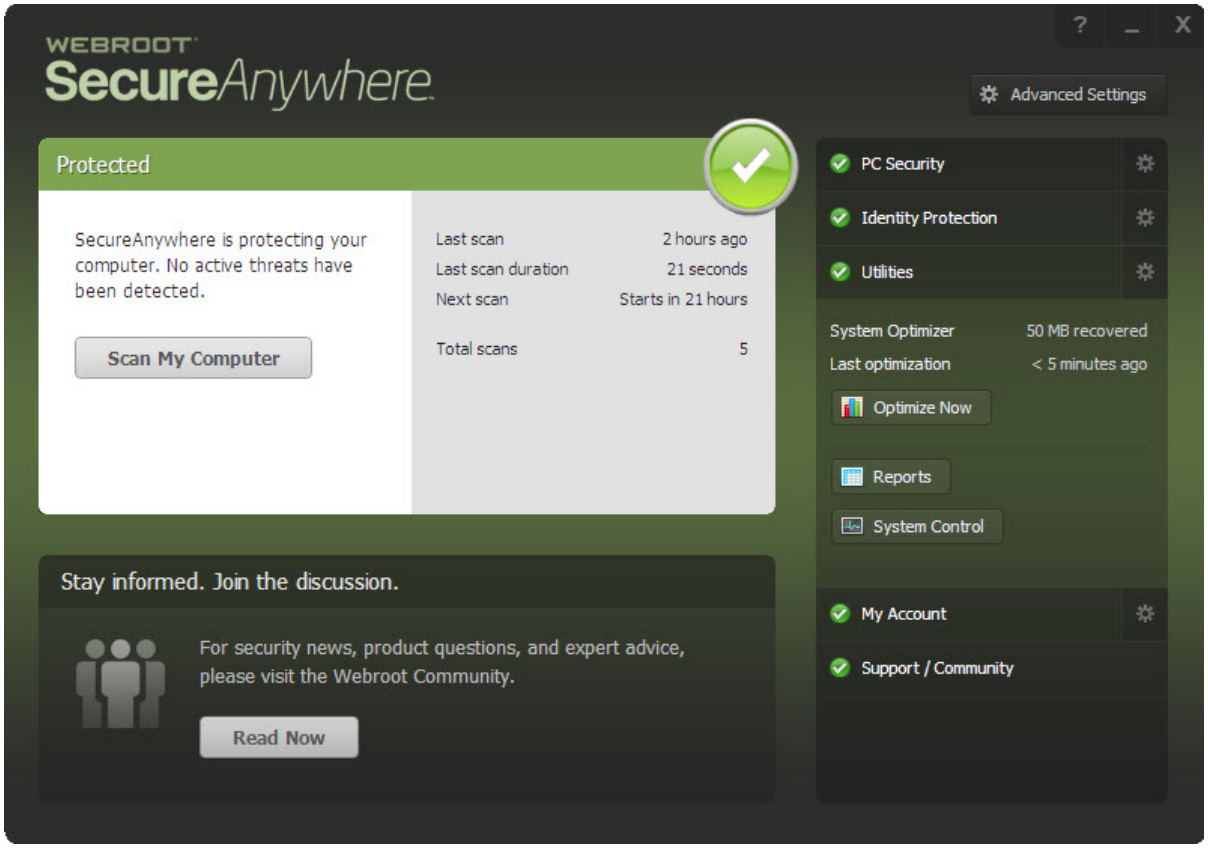
You can view your keycode and the time remaining on your subscription from the My Account window.

To view account details:

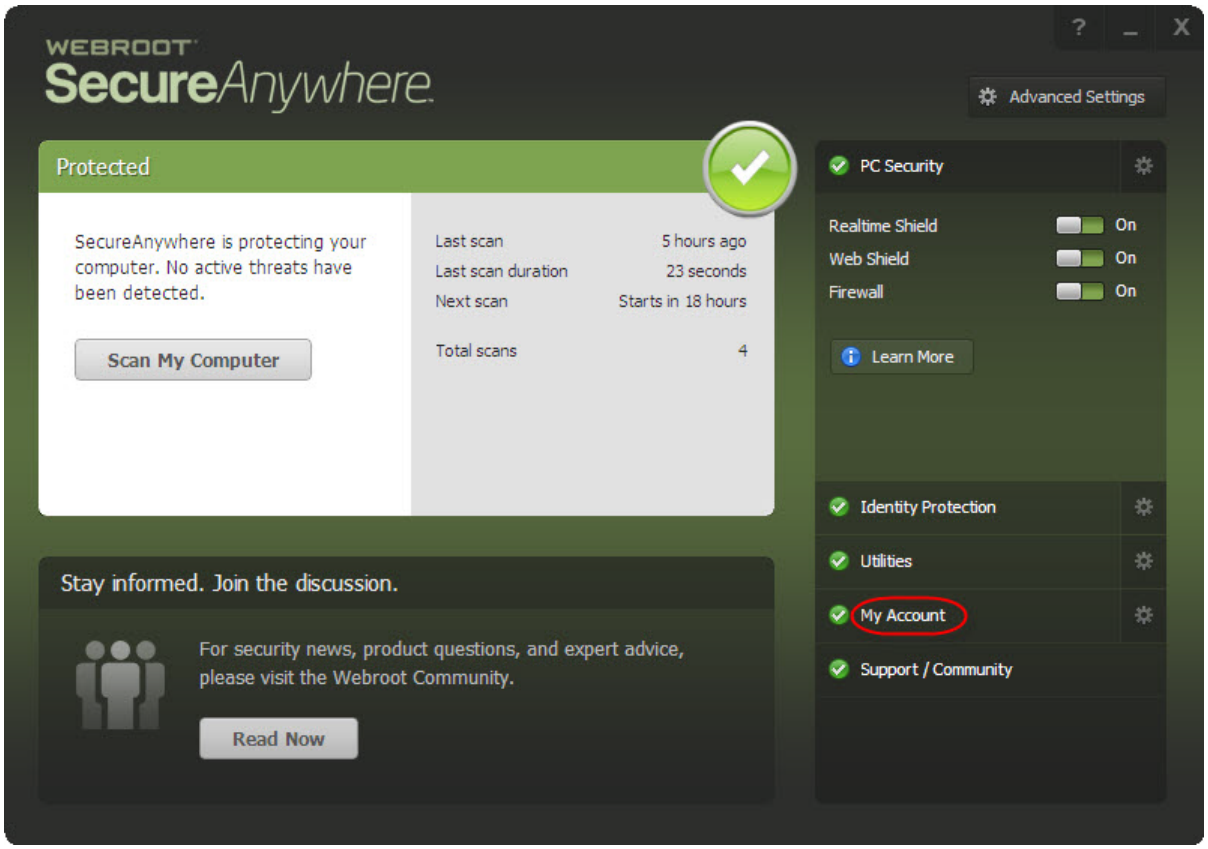
1. From the system tray, double-click the **Webroot** icon to display the main interface.



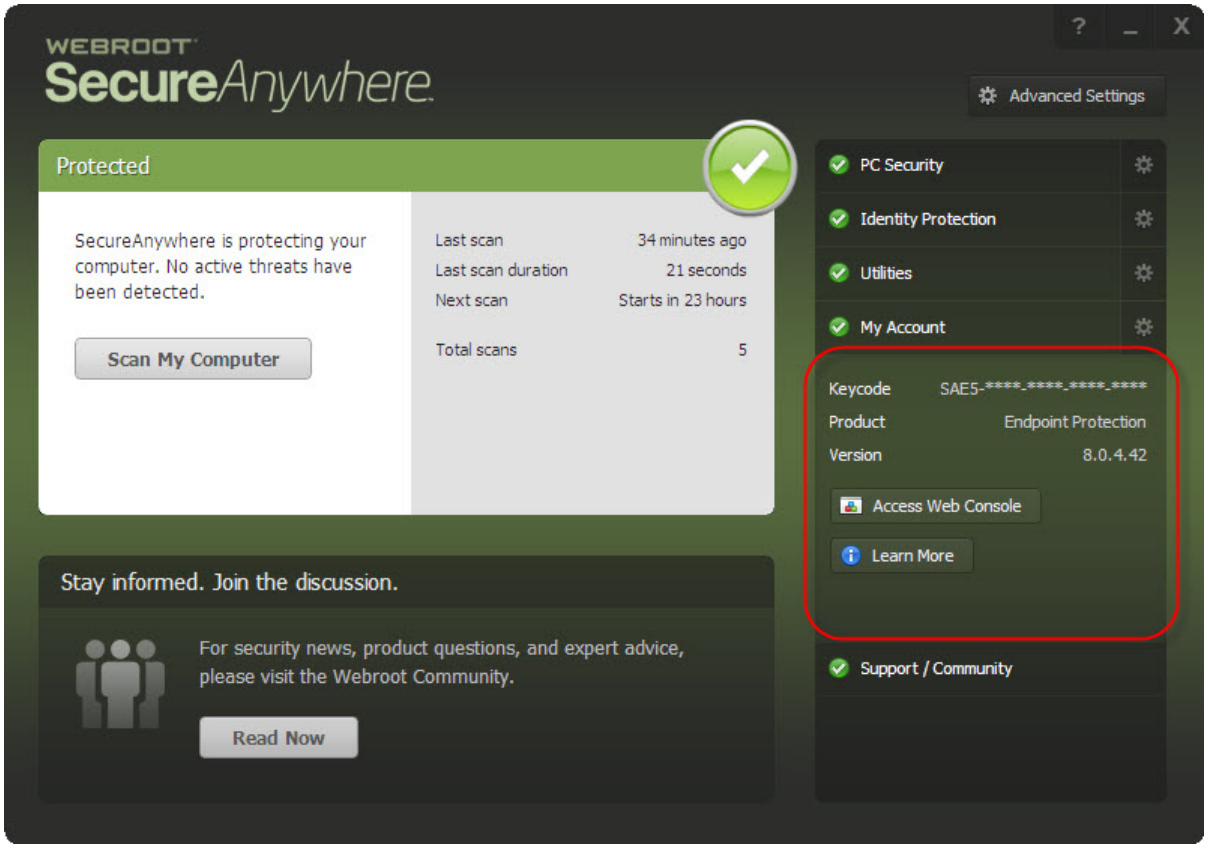
The main interface displays.



2. Click the **My Account** link.



The My Account area displays, with your account information.

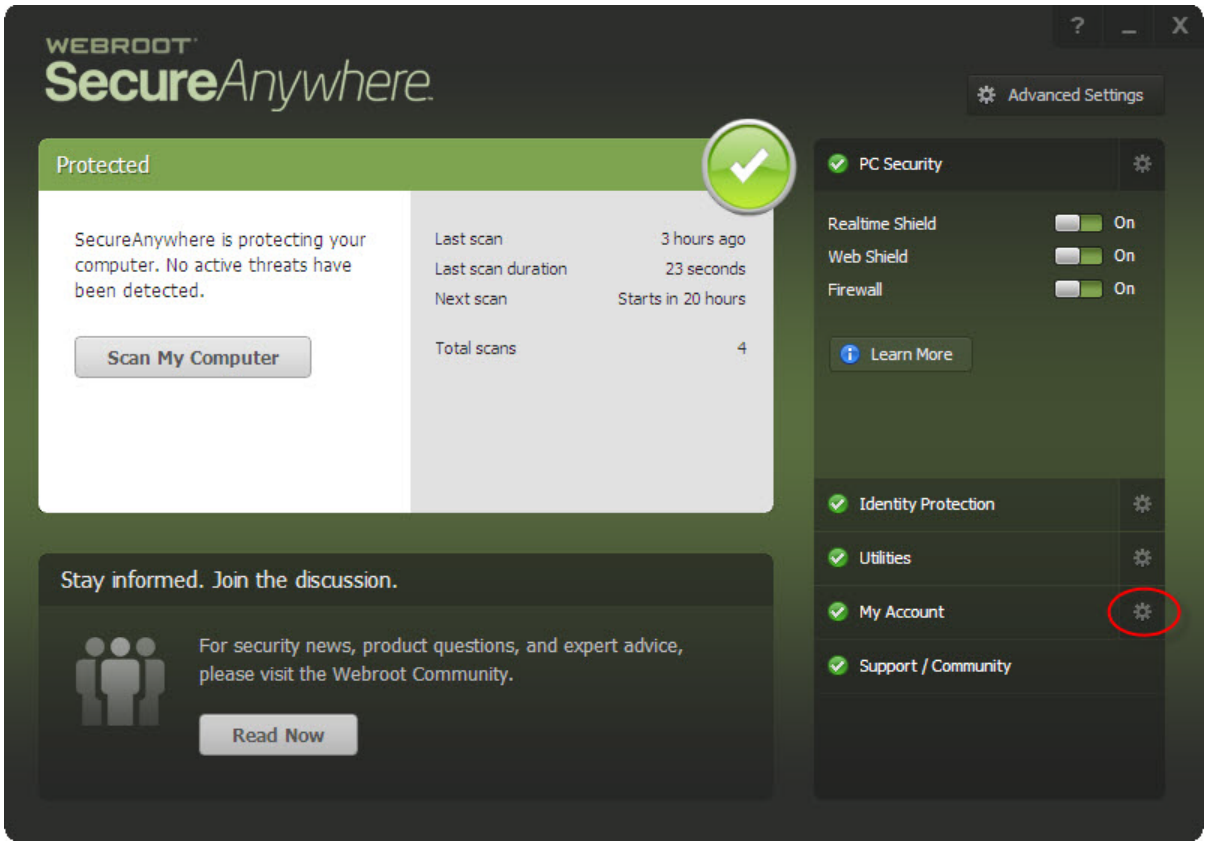


The My Account area has the following information:

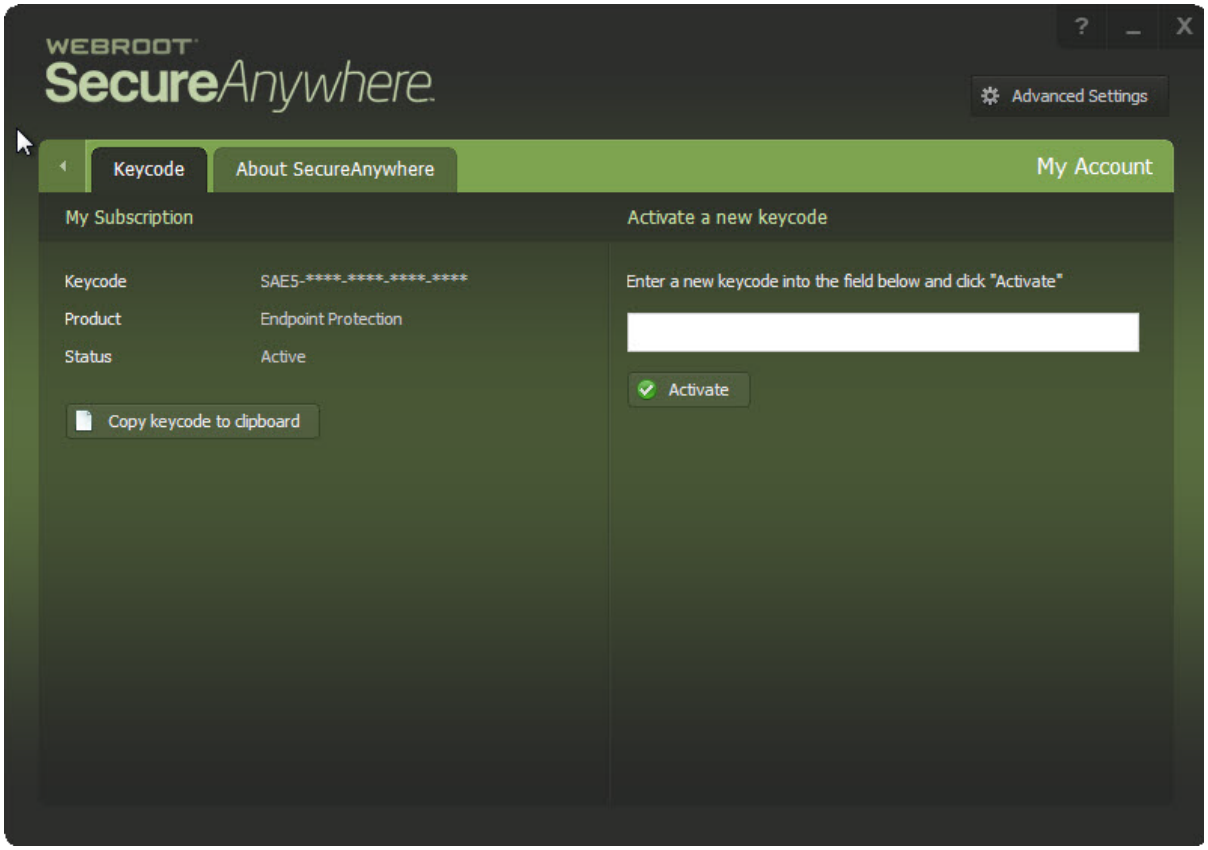
- **Keycode** – This is your keycode; the numbers are blocked out based on your security settings.
- **Product Name** – This is the name of the product you purchased.
- **Product Version Number** – This is the version number of the product you purchased.

3. In the My Account area, click either of the following buttons, as needed:
   - **Activate a New Keycode** – Displays the Webroot SecureAnywhere online console, where you can create an account that allows you to manage your security across multiple devices.
   - **Learn More** – Displays the Webroot SecureAnywhere Customer webpage where you can read about security features of Webroot SecureAnywhere functionality.

4. To view additional account information, click the **My Account** gear icon.



The My Account interface displays.

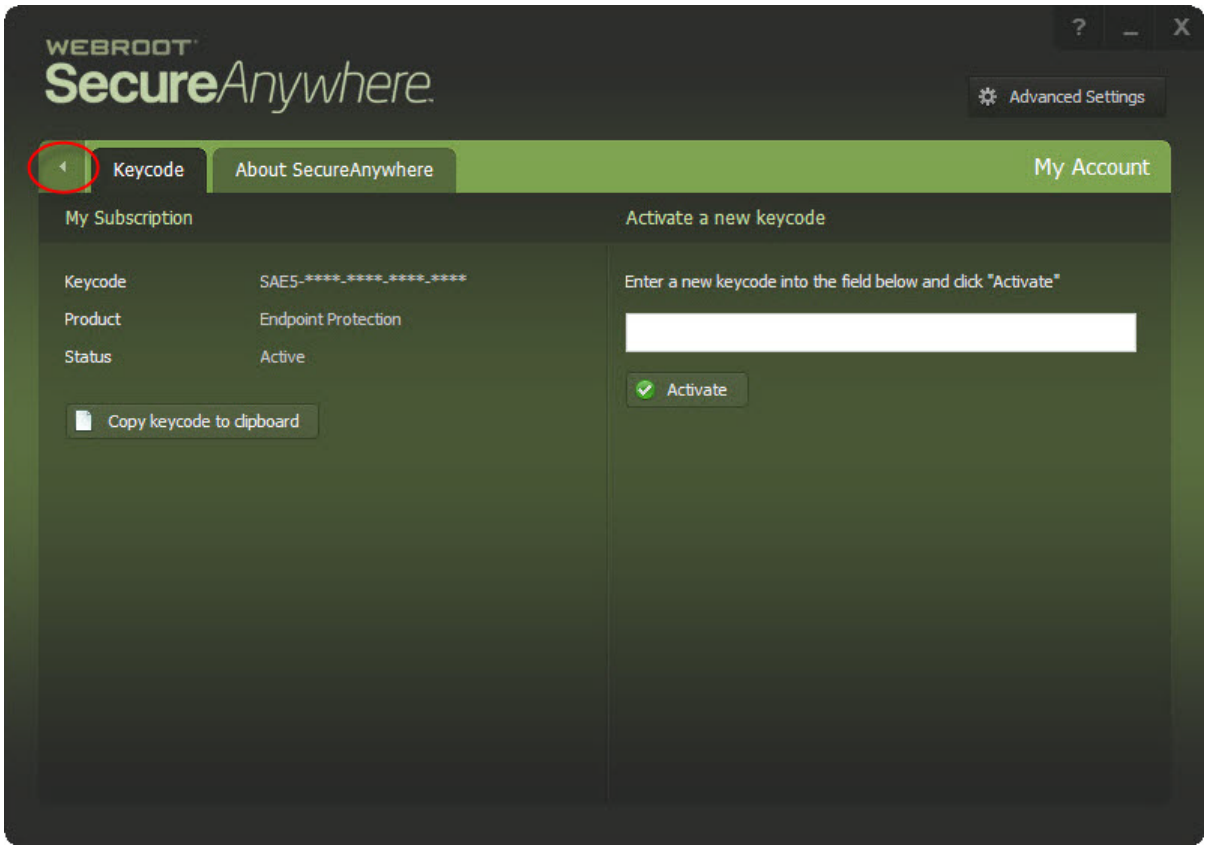


The My Account interface has the following information:

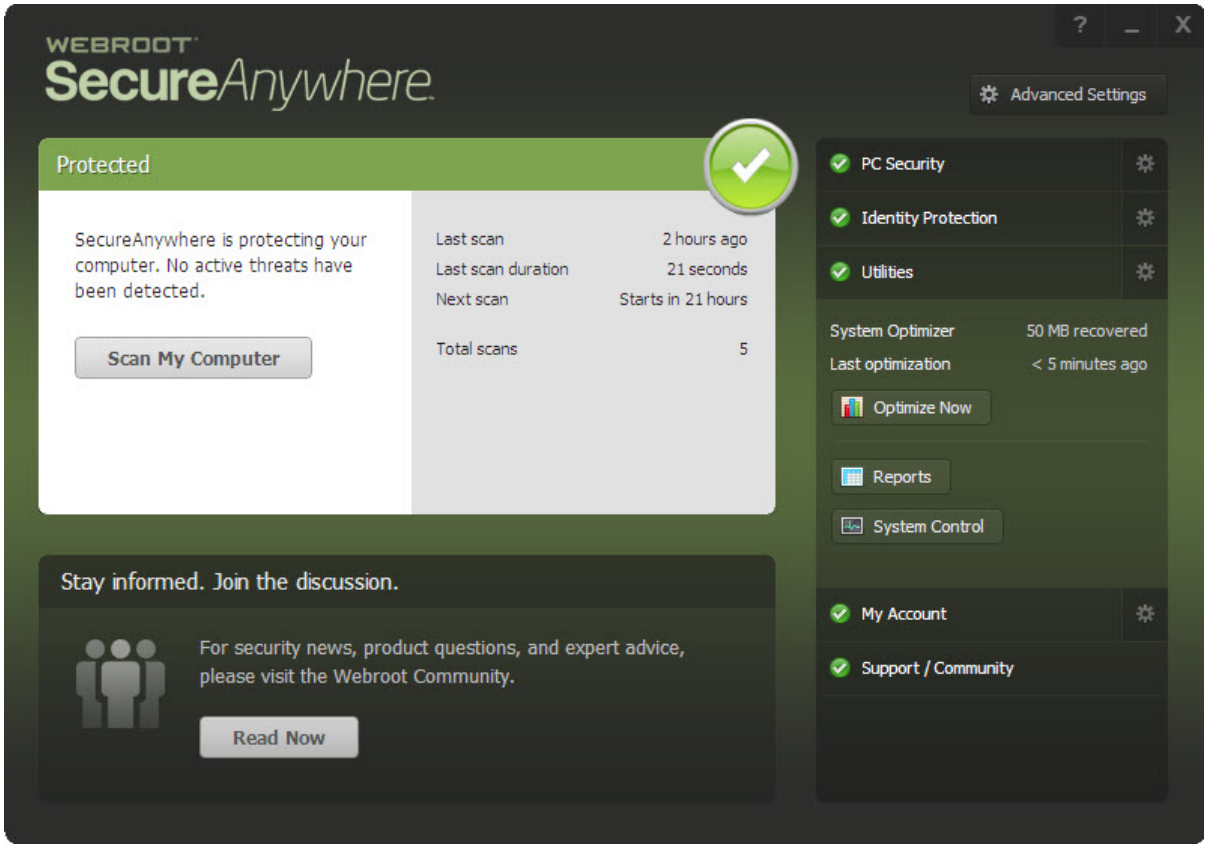
- **Keycode** — This is your keycode; the numbers are blocked out based on your security settings.
- **Product Name** – This is the name of the product you purchased.
- **Status** – This is the status of the product you purchased.

5. From here, you can do any of the following:
   - Activate a New Keycode. For more information, see Creating Webroot Accounts in the WSA PC User Guide
   - Check for Software Updates. For more information, see Checking For Updates in the WSA PC User Guide.

6. When you're done viewing your account details, click the **Back** arrow to return to the main interface.



The main interface displays.

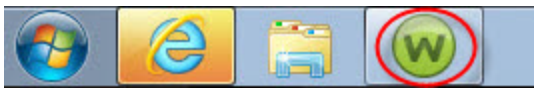

WEBROOT
SecureAnywhere
Advanced Settings
Protected
SecureAnywhere is protecting your computer. No active threats have been detected.
Scan My Computer
Last scan 2 hours ago
Last scan duration 21 seconds
Next scan Starts in 21 hours
Total scans 5
PC Security
Identity Protection
Utilities
System Optimizer 50 MB recovered
Last optimization < 5 minutes ago
Optimize Now
Reports
System Control
Stay informed. Join the discussion.
For security news, product questions, and expert advice, please visit the Webroot Community.
Read Now
My Account
Support / Community

Shutting Down Identity Shield

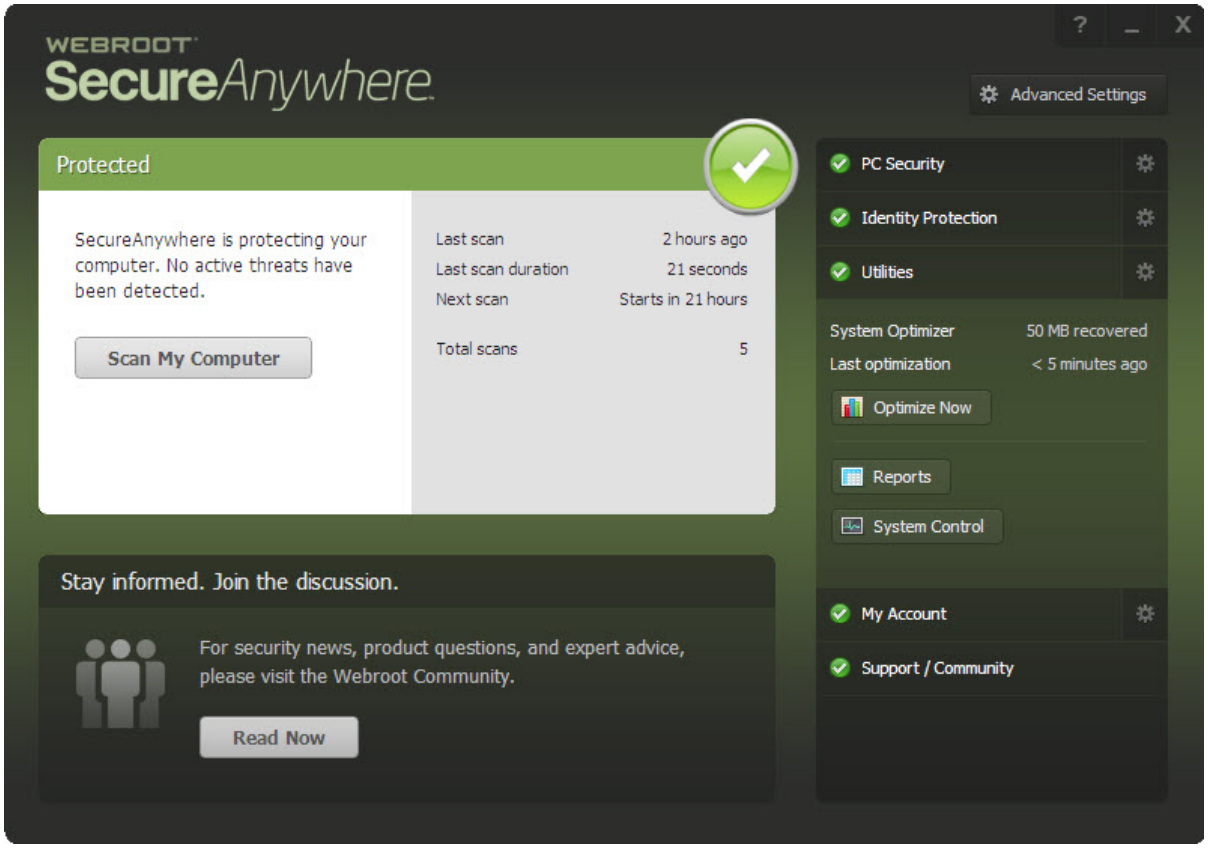
You can temporarily shut down Identity Shield protection or uninstall the program entirely, as described below. We recommend that you keep Identity Shield running in the background at all times; normally, you do not need to shut it down.

To shut down Identity Shield:

1. From the system tray, double-click the **Webroot** icon to display the main interface.



The main interface displays.

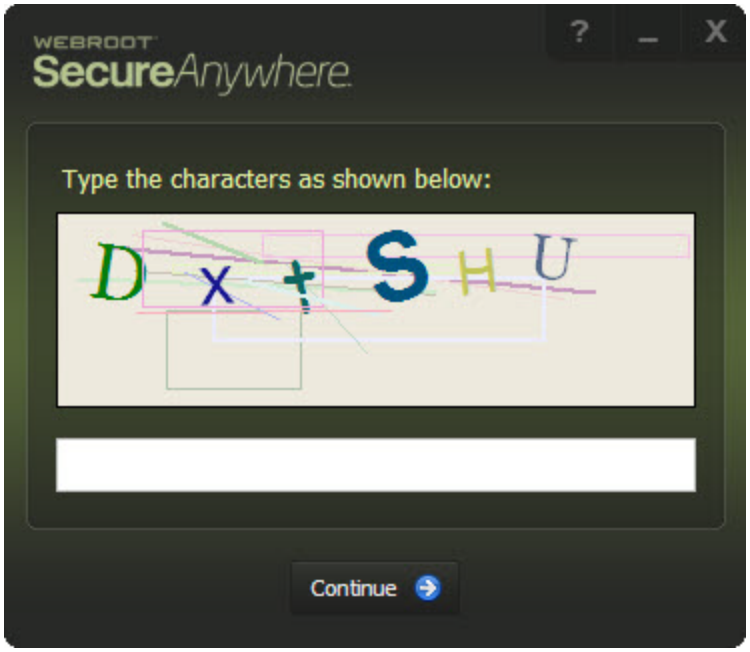


2. Click the **Shut down Protection** button.

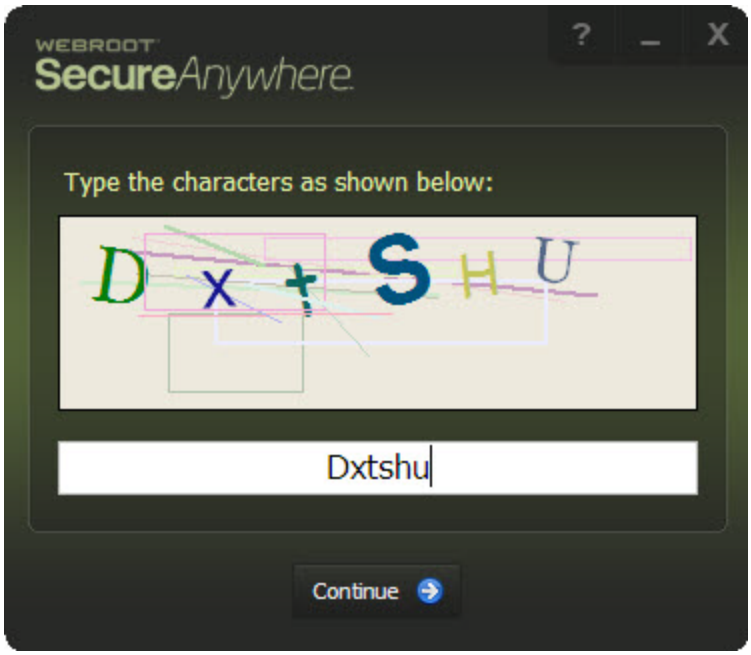
   A prompt displays.

3. At the prompt, click the **Yes** button.

   A CAPTCHA dialog window displays.



4. Enter the displayed characters and click the **Enter** button.



   The Identity Shield stops its protection activities and the Webroot icon is removed from the system tray.

5. To turn Identity Shield back on, from the Windows Start menu, select **All Programs > Webroot SecureAnywhere > Webroot SecureAnywhere**.

Uninstalling Identity Shield

If needed, you can uninstall Identity Shield completely.

To uninstall Identity Shield:

1. From the Windows start menu, select **All Programs > Webroot SecureAnywhere**.

   The Webroot SecureAnywhere interface displays.

2. Select **Tools**.
3. Click **Uninstall Webroot**.
4. At the prompt, click **Yes** to continue.

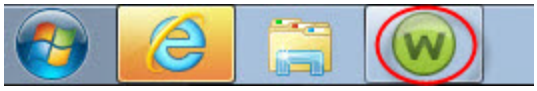
Upgrading to a Threat Removal Version

To block and remove malware from your computer, you can upgrade to one of the following SecureAnywhere version:

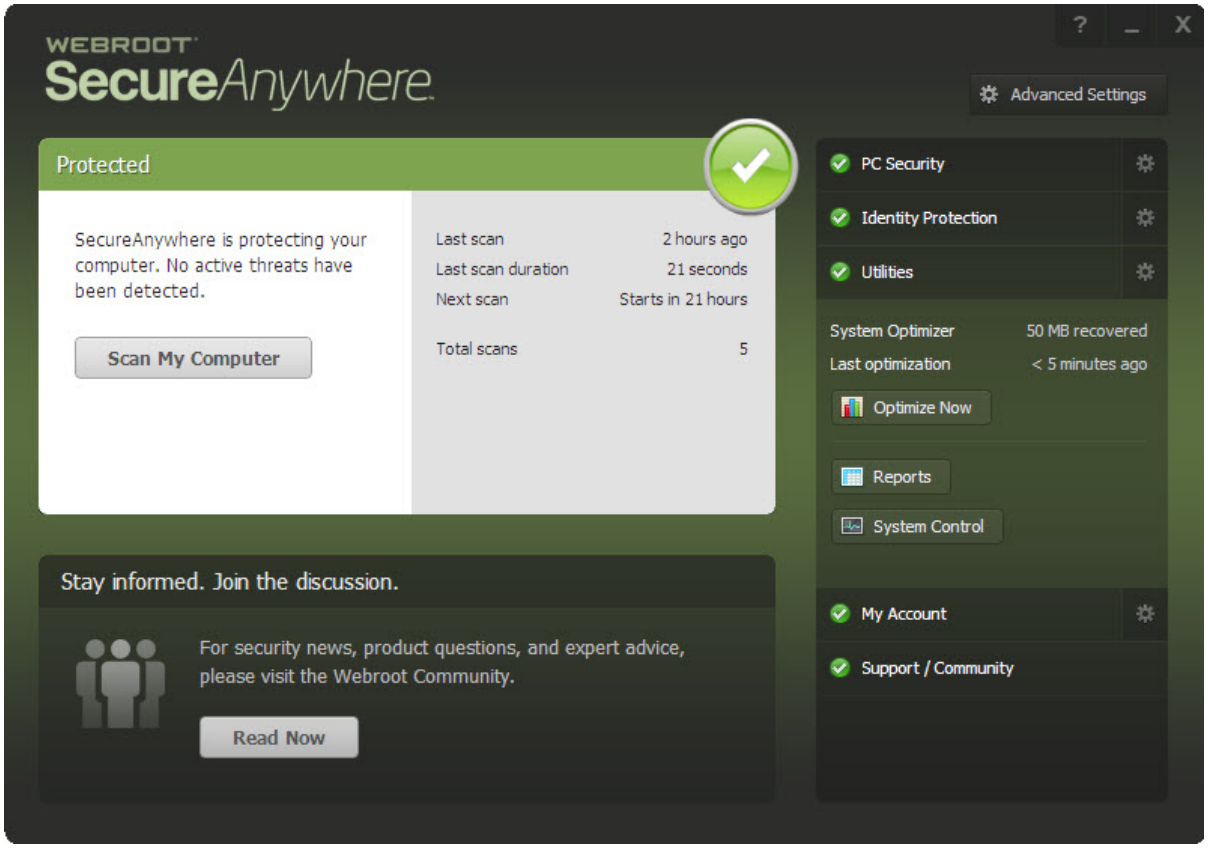
- **AntiVirus** — Provides protection from viruses and spyware, and also includes Identity Shield and firewall protection.
- **Internet Security Plus** — Provides all the features of the AntiVirus edition, plus password management and protection for mobile devices.
- **Complete** — Provides all the features of 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. From the system tray, double-click the **Webroot** icon to display the main interface.

   The main interface displays.



2. Click on the **Upgrade Now** link.
3. If you don't see this link on the Overview window, click the **My Account** tab and then the **Upgrade** or **Renew** link.
4. When the Webroot website opens, you can purchase an upgrade to your software.

Chapter 5: Identity Shield Support

To access support, see the following topic:

Accessing Technical Support *73*

Accessing Technical Support

Webroot offers a variety of support options. You can do any of the following:

- Is your Webroot subscription through Best Buy? Click here for additional support options.
- Look for the answer in our knowledge base and FAQs.
- Look for the answer in our online documentation.
- Enter a help ticket.
- Connect to the Webroot Security for Android forum.

Index

A

account details, viewing *59*
activating keycodes *61*
alerts
  malware *28*
  responding to *13*
allowing
  applications *36*
  trusted screen capture programs *28*
applications
  allowing *36*
  denying *36*
  protecting *36*
applying
  updates *17*

B

basic configuration settings *14*
blocking
  browser modifications *47*
  suspicious access *47*
  third party cookies *27*
browser
  components, protecting *46*
  modifications, blocking *47*

C

changing
  Identity Shield settings *25*
  language settings *6*
  protection levels *10*
clipboard data, protecting *46*
configuration settings *14*
cookies
  protecting *46*
creating
  shortcut *6*

D

denying
applications *36*
description
identity shield *11*
main interface *11*
my account *12*
Support Community *12*
utilities *11*
disabling Identity Shield *50*
DNS IP resolution, verifying *27*
download
updates *17*

I

identity protection description *11*
Identity Shield
disabling *50*
overview *2*
settings, changing *25*
shutting down *66*
uninstalling *69*
upgrading *70*
installation *4*
isolating untrusted browser add-ons *47*

K

keycode *61*
keycodes, activating *61*
keyloggers, protecting against *46*

L

language settings
changing *6*

M

main interface, description *11*
malware
alerts *28*
man-in-the-browser attacks
protecting against *47*

man-in-the-middle attacks
    preventing *46*
managing
    protected applications *29*
    protected websites *42*
my account description *12*

O

overview, Identity Shield *2*

P

PC security description *11*
preventing
    access *27*
    man-in-the-middle attacks *46*
product
    keycode *61*
    name *61*
    version number *61*
protect
    cookies *46*
    saved data *46*
protected
    applications, managing *29*
    websites, managing *42*
protecting
    against keyloggers *46*
    against man-in-the-browser attacks *47*
    against screen-grabbing attacks *47*
    against URL grabbing attacks *46*
    browser components *46*
    clipboard data *46*
protection
    levels, changing *10*
    options *45*

S

saved data, protecting *46*
screen-grabbing attacks, protecting against *47*
security levels *45*
settings
    changing basic *14*
shortcut, creating *17*

show
    start menu shortcut *17*
    status notificaton *17*
    system tray icon *17*
shut down SecureAnywhere manually *17*
shutting down Identity Shield *66*
start menu shortcut, show *17*
status *63*
    notification, show *17*
Support Community description *12*
suspicious access, blocking *47*
system requirements *4*
system tray icon, show *17*

T

third party cookies, blocking *27*
trusted screen capture programs, allowing *28*

U

uninstalling Identity Shield *69*
untrusted browser add-ons, isolating *47*
updates
    applying *17*
    downloading *17*
upgrading Identity Shield *70*
URL grabbing attacks, protecting against *46*
utilities, description *11*

V

verifying
    DNS IP resolutions *27*
    websites *27*
viewing account details *59*

W

warnings, responding to *13*
websites, veryifying *27*