

WEBROOT®

an **opentext™** company

Webroot SecureAnywhere Mac User Guide

Copyright

Copyright 2019 Webroot. All rights reserved.

WSA Mac 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: Mac User Guide	1
WSA Mac User Guide Overview	2
Getting Started	2
Scanning for Malware	2
Shielding Your Mac	2
Managing Quarantine	2
Managing Your Account	3
Identity and Privacy	3
Using Advanced Tools	3
Setting Preferences	3
Chapter 2: Getting Started With Mac	5
Installing SecureAnywhere	6
System Requirements for Mac	15
Operating System	15
Memory	15
Storage	15
Internet/Browser	15
About the SecureAnywhere Interface	16
Creating Webroot Accounts	20
Responding to Alerts	21
Chapter 3: Scanning For Malware	23
Running Scans	24
Managing Detected Threats	27
Changing Scan and Optimization Schedules	29
Changing Scan Settings	33
Scanning Specific Files and Folders	36
Chapter 4: Shielding Your Mac	37
Mac Shields Overview	38
Types of Shields	38
Indicators Displayed With Query Results	39
Infrared Shielding and Warning Messages	40
Low-Risk Warning	41
Medium-Risk Warning	41
High-Risk Warning	42

Managing Shields	43
Accessing and Updating Web Threat Shield Settings	46
Changing Realtime Shield Settings	52
Managing Web Threats	56
Chapter 5: Managing Quarantine	59
Managing Quarantined Items	60
Managing File Detection	65
Saving Threat Logs	67
Chapter 6: Managing Your Account	71
Viewing Your Account Details	72
Activating Keycodes	73
Renewing Subscriptions	75
Checking for Updates	77
Chapter 7: Managing Backup And Sync	81
Backup & Sync Overview	82
Storing Files in the Anywhere Folder or in Your Own Sync Folders	82
Backing Up Files	82
Downloading Backup & Sync	83
Adding Sync Folders	85
Backing Up Files	88
Changing Backup & Sync Settings	92
Changing Backup Filters	95
Changing Backup Schedules	98
Checking File Backup & Sync Statuses	100
Synchronizing Files	104
Synchronizing Folders Between Computers	107
Removing Folders From Synchronization	110
Chapter 8: Managing Passwords	113
About Managing Passwords	114
Chapter 9: Using Advanced Tools	115
Changing System Control Settings	116
Saving Scan Logs	120
Submitting Scan Logs	126
Running System Analyzer	133
Chapter 10: Using System Optimizer	139

Running System Optimizer	140
Changing System Optimizer Settings	148
Creating Secure Erase Settings	156
Chapter 11: Managing Preferences	163
Setting General Preferences	164
Defining Proxy Server Settings	170
Chapter 12: WSA Mac Support	177
Accessing Technical Support	178
Index	i

Chapter 1: Mac User Guide

To use the Mac User Guide, see the following topic:

WSA Mac User Guide Overview	2
Getting Started	2
Scanning for Malware	2
Shielding Your Mac	2
Managing Quarantine	2
Managing Your Account	3
Identity and Privacy	3
Using Advanced Tools	3
Setting Preferences	3

WSA Mac User Guide Overview

Webroot SecureAnywhere™ delivers complete protection against viruses, spyware, and other online threats without slowing down Mac performance or disrupting your normal activities. With its fast scans and threat removal, you can rest assured that malware is eliminated quickly and easily. SecureAnywhere gives you the freedom to surf, share, shop, and bank online all with the confidence that your Mac and your identity will be kept safe.

To learn more about using SecureAnywhere, see the following topics.

Note: This user guide describes the features of all SecureAnywhere editions. Your edition may not include some of the features described here.

Getting Started

- [Installing SecureAnywhere on page 6](#)
- [About the SecureAnywhere Interface on page 16](#)

Scanning for Malware

- [Running Scans on page 24](#)
- [Managing Detected Threats on page 27](#)
- [Changing Scan and Optimization Schedules on page 29](#)
- [Changing Scan Settings on page 33](#)

Shielding Your Mac

- [Changing Realtime Shield Settings on page 52](#)
- [Accessing and Updating Web Threat Shield Settings on page 46](#)
- [Managing Web Threats on page 56](#)

Managing Quarantine

- [Managing Quarantined Items on page 60](#)
- [Managing File Detection on page 65](#)
- [Saving Threat Logs on page 67](#)

Managing Your Account

- [*Activating Keycodes on page 73*](#)
- [*Renewing Subscriptions on page 75*](#)

Identity and Privacy

-

Note: This option is available only if you have purchased [Internet Security Plus](#) or [Internet Security Complete](#) editions.

Using Advanced Tools

- [*Changing System Control Settings on page 116*](#)
- [*Saving Scan Logs on page 120*](#)
- [*Submitting Scan Logs on page 126*](#)

Setting Preferences

- [*Setting General Preferences on page 164*](#)
 - [*Defining Proxy Server Settings on page 170*](#)
-

Chapter 2: Getting Started With Mac

To get started with Mac, see the following topics:

Installing SecureAnywhere	6
System Requirements for Mac	15
Operating System	15
Memory	15
Storage	15
Internet/Browser	15
About the SecureAnywhere Interface	16
Creating Webroot Accounts	20
Responding to Alerts	21

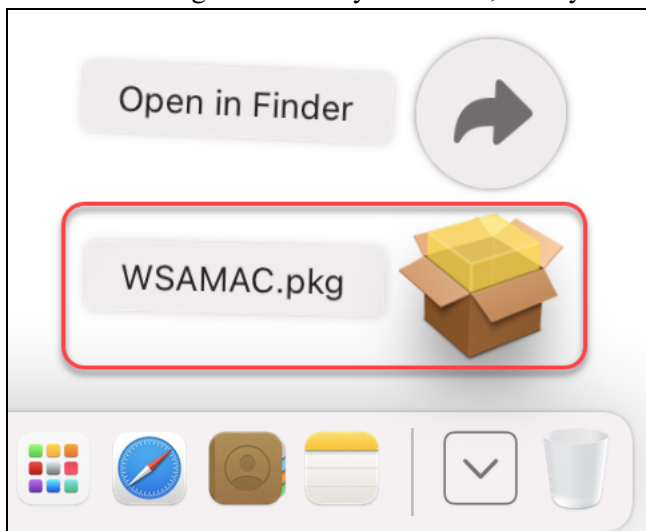
Installing SecureAnywhere

To install SecureAnywhere:

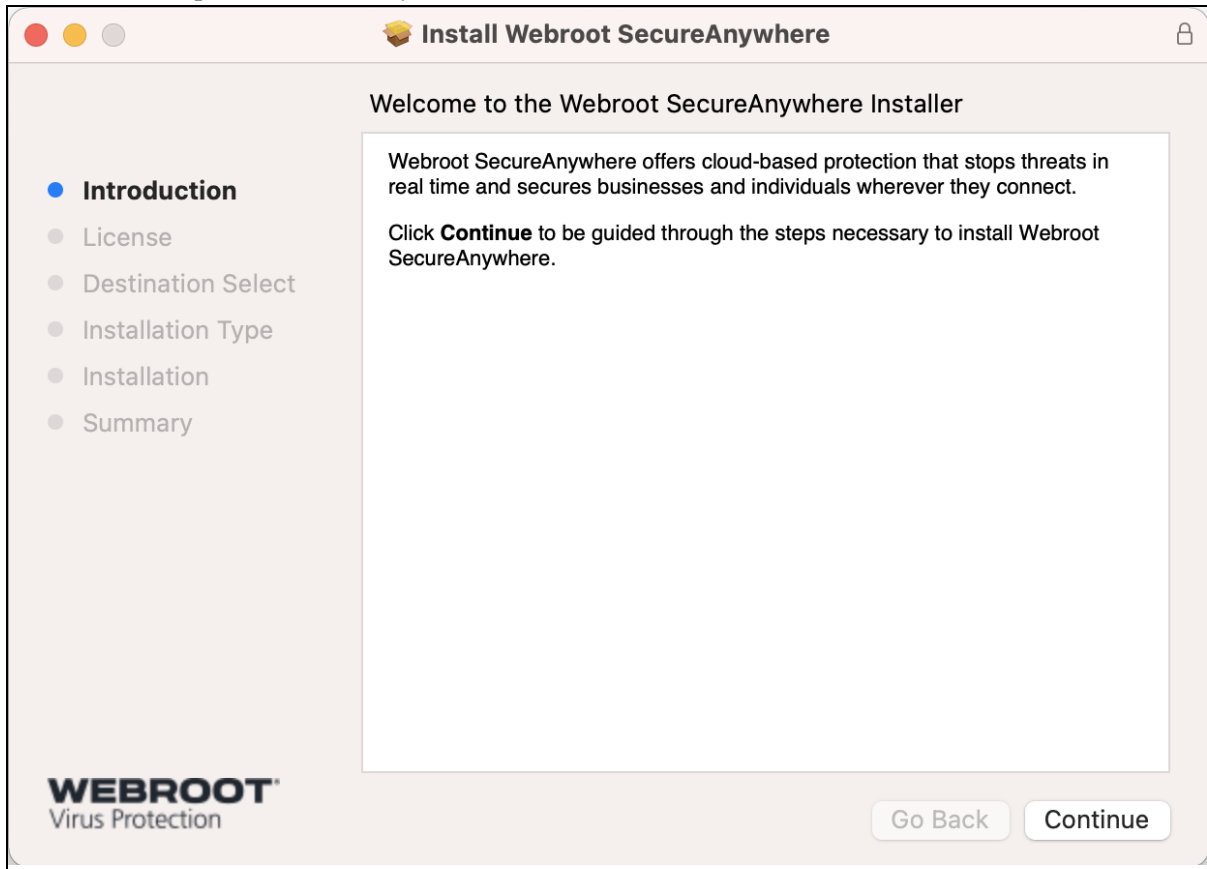
1. [Click here](#) to reach the Webroot SecureAnywhere installer for your Mac, then click **Download Now** to begin the installation process.



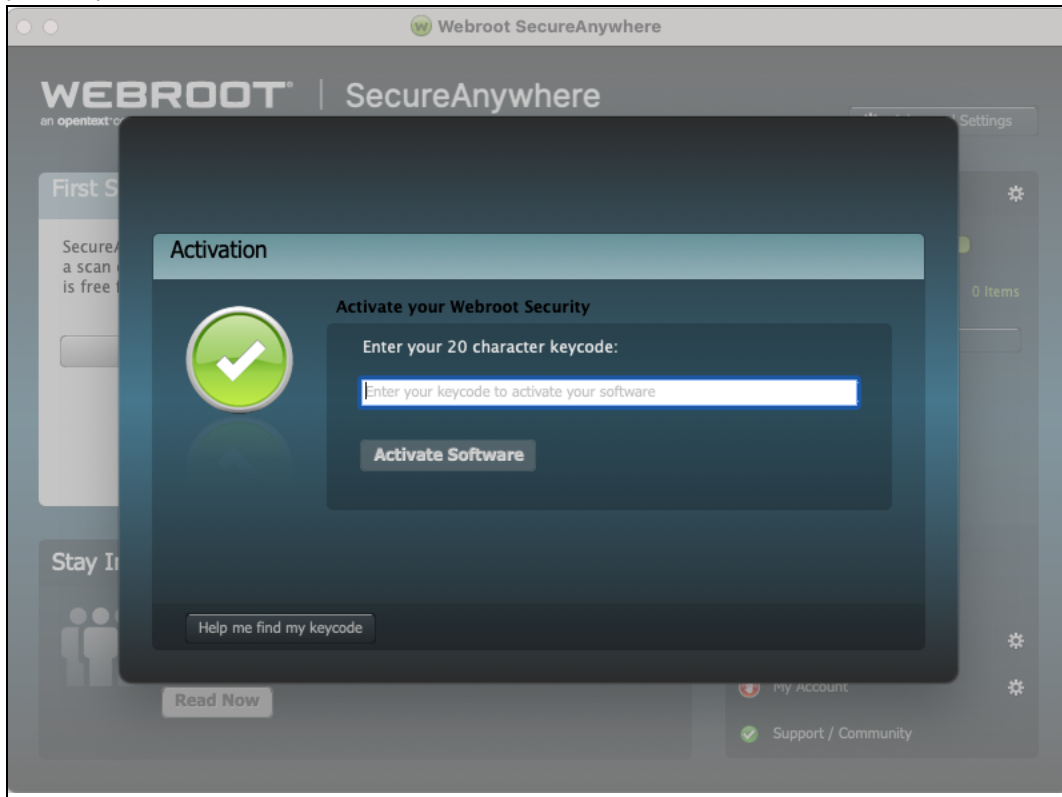
2. In the bottom right corner of your screen, or in your downloads folder, open the file WSAMAC .pkg.



3. In the **Install Webroot SecureAnywhere** installer that launches, follow the instructions until the installation completes successfully, then click **Close**.



4. After a short delay, Webroot SecureAnywhere launches and shows the **Activation** dialog box. Enter your keycode and click **Activate Software**.



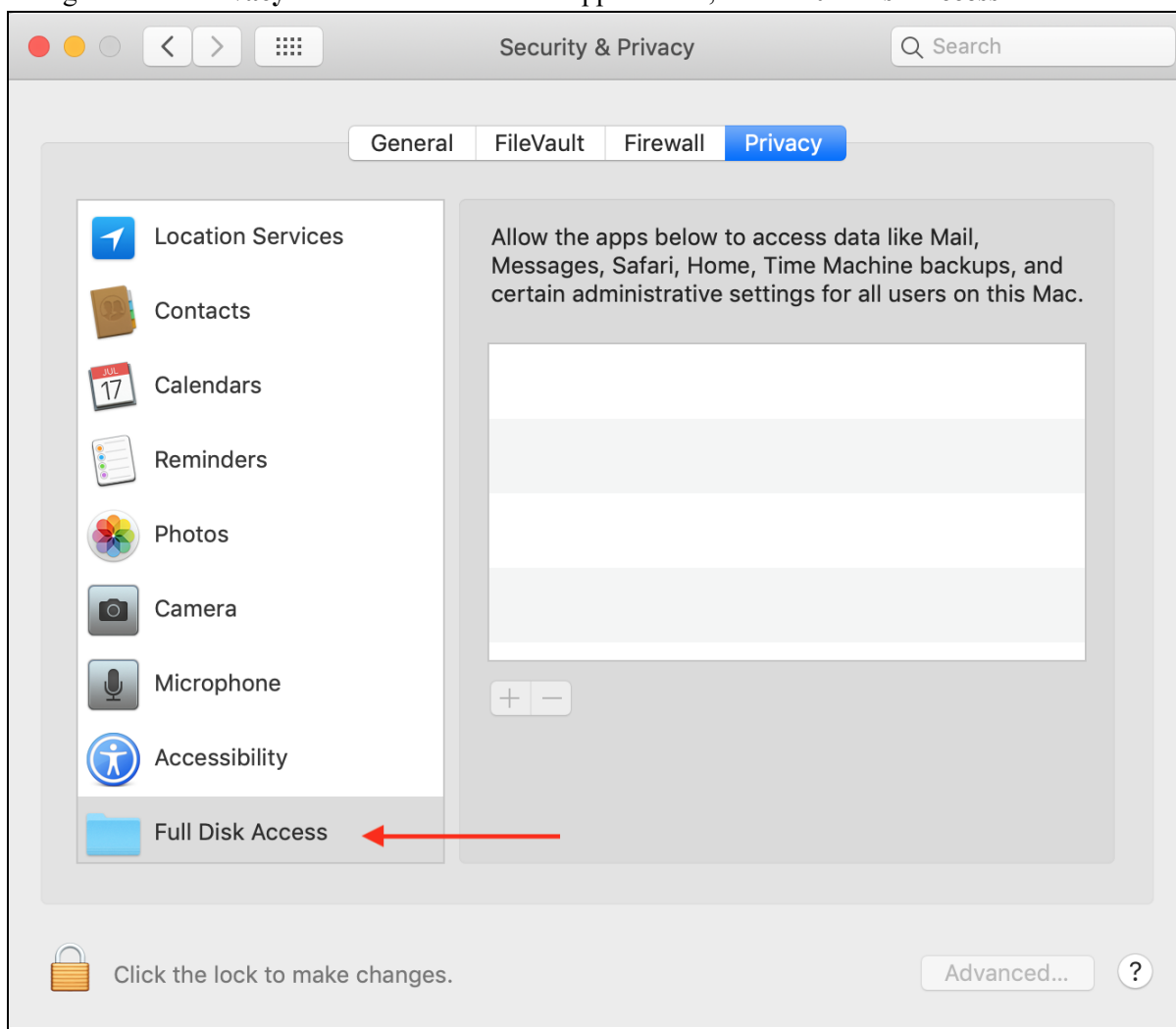
Note: Your keycode is the 20-character license that identifies your Webroot account. This keycode also identifies whether you purchased a multi-user license, which allows you to install SecureAnywhere on the total number of devices you purchased on your subscription.


5. Webroot SecureAnywhere may ask you to grant full disk access. In the **Full Disk Access** dialog box, click **Open System Preferences** to grant permission.

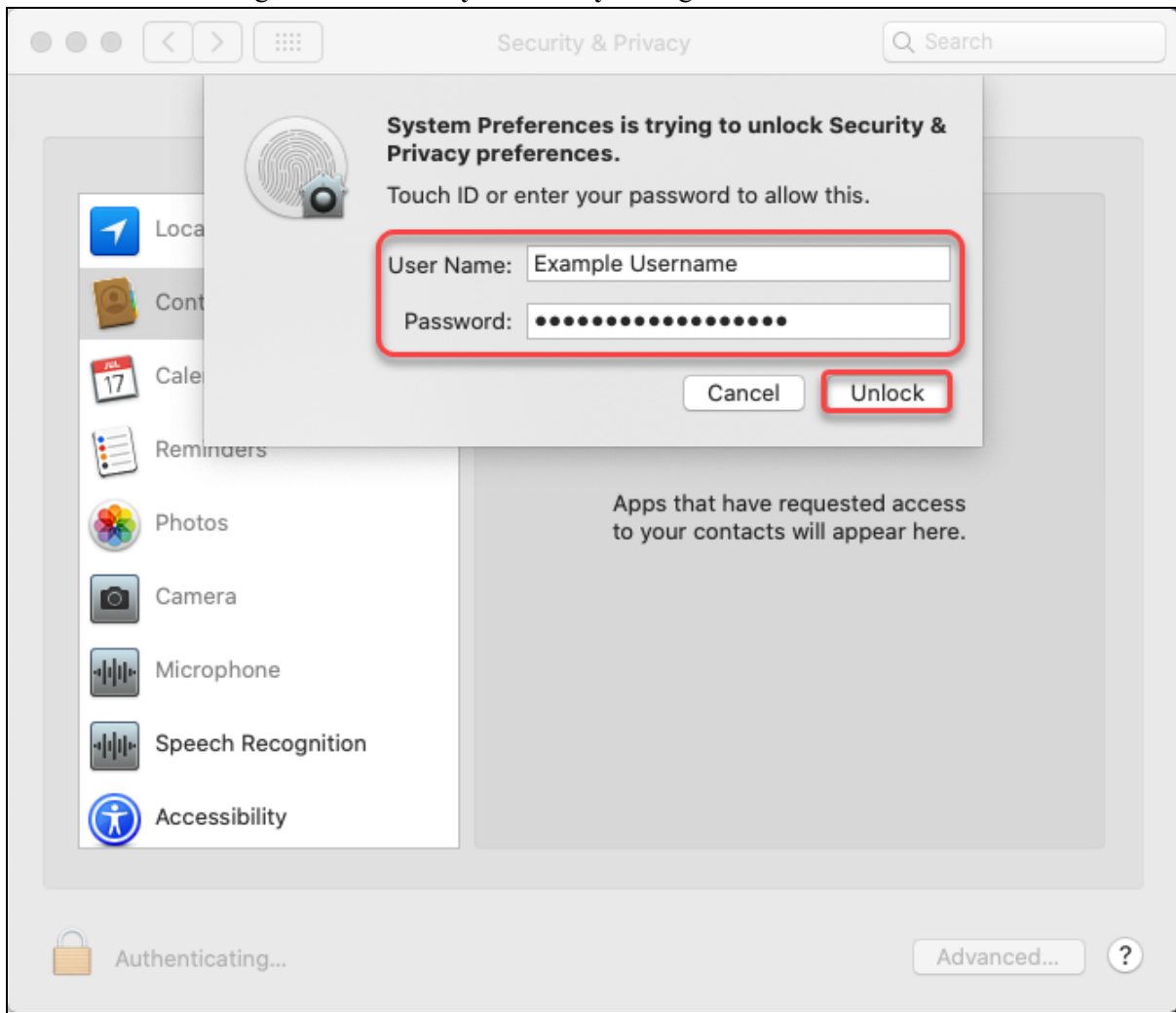



6. You should be taken directly to the Full Disk Access settings window. If you are not taken directly to Full Disk Access settings:

- Open your Mac's **System Preferences**, then click **Security & Privacy**.
- Navigate to the **Privacy** tab and from the list of applications, select **Full Disk Access**.



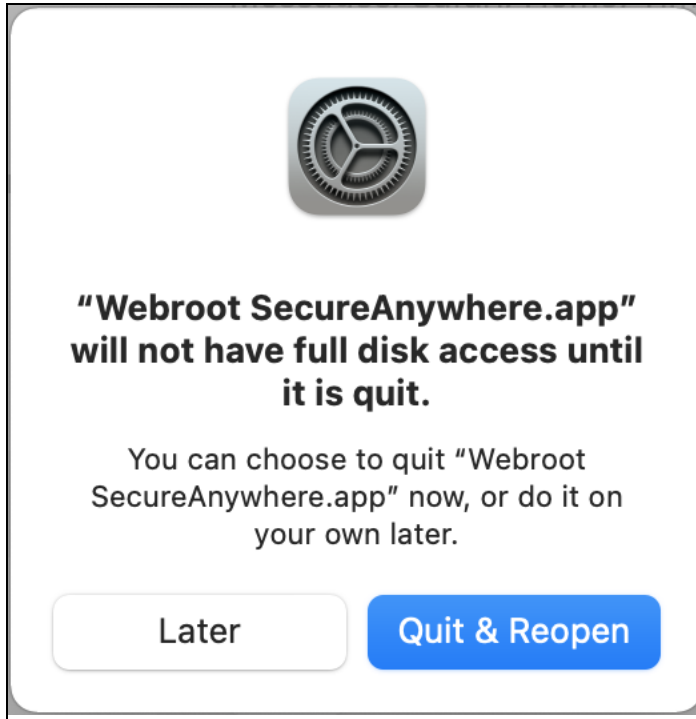
7. If the **Lock** button  is locked, you will need to click it and enter your Mac's password. Then, click **Unlock** to make changes to the **Security & Privacy** settings.



8. In the **Security & Privacy** window, click the **Add an application** button . Navigate to your Mac's **Applications** tab, then select **Webroot SecureAnywhere** and click **Open**.



9. In the dialog box that opens, click **Quit & Reopen**.



10. When complete, Webroot SecureAnywhere appears in the **Full Disk Access** list of allowed applications with a selected check box next to it.
11. Return to the **Webroot SecureAnywhere** window and click **Done** to close the **Full Disk Access** dialog box. See Step 5.
12. The **Webroot SecureAnywhere** window turns blue as it begins scanning your Mac for viruses, spyware, and other potential threats. If it detects threats during the scan, the window changes to a red color and it prompts you to move the infected items to quarantine. In quarantine, these items are rendered inoperable and can no longer harm your system or steal data. If the scan does not find any threats, the window turns green when the scan completes. For more information, see [Managing Detected Threats on page 27](#).



System Requirements for Mac

The following describes the system requirements for using SecureAnywhere functionality on Mac devices.

Operating System

- macOS 10.14 (Mojave®)
- macOS 10.15 (Catalina®)
- macOS 11 (Big Sur®) with Apple M1 ARM or Intel® processors
- macOS 12 (Monterey®) with Apple M1 ARM or Intel® processors

Memory

- 128 MB RAM (minimum)

Storage

- 15 MB

Internet/Browser

Internet access is required:

- Apple Safari® 7.0 or higher.
 - Mozilla Firefox®; current and most recent versions.
 - Google Chrome®; current and most recent versions.
-

About the SecureAnywhere Interface

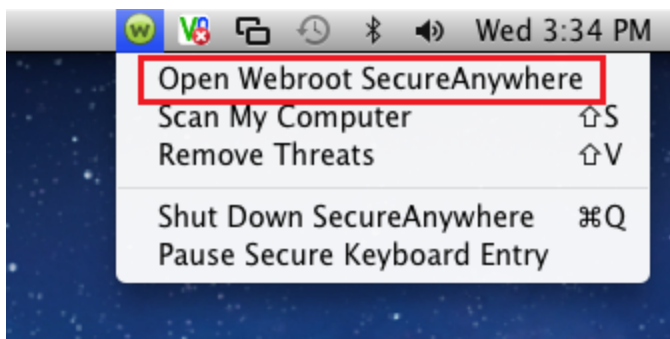
The SecureAnywhere interface provides access to all functions and settings.

The interface includes the following access methods:

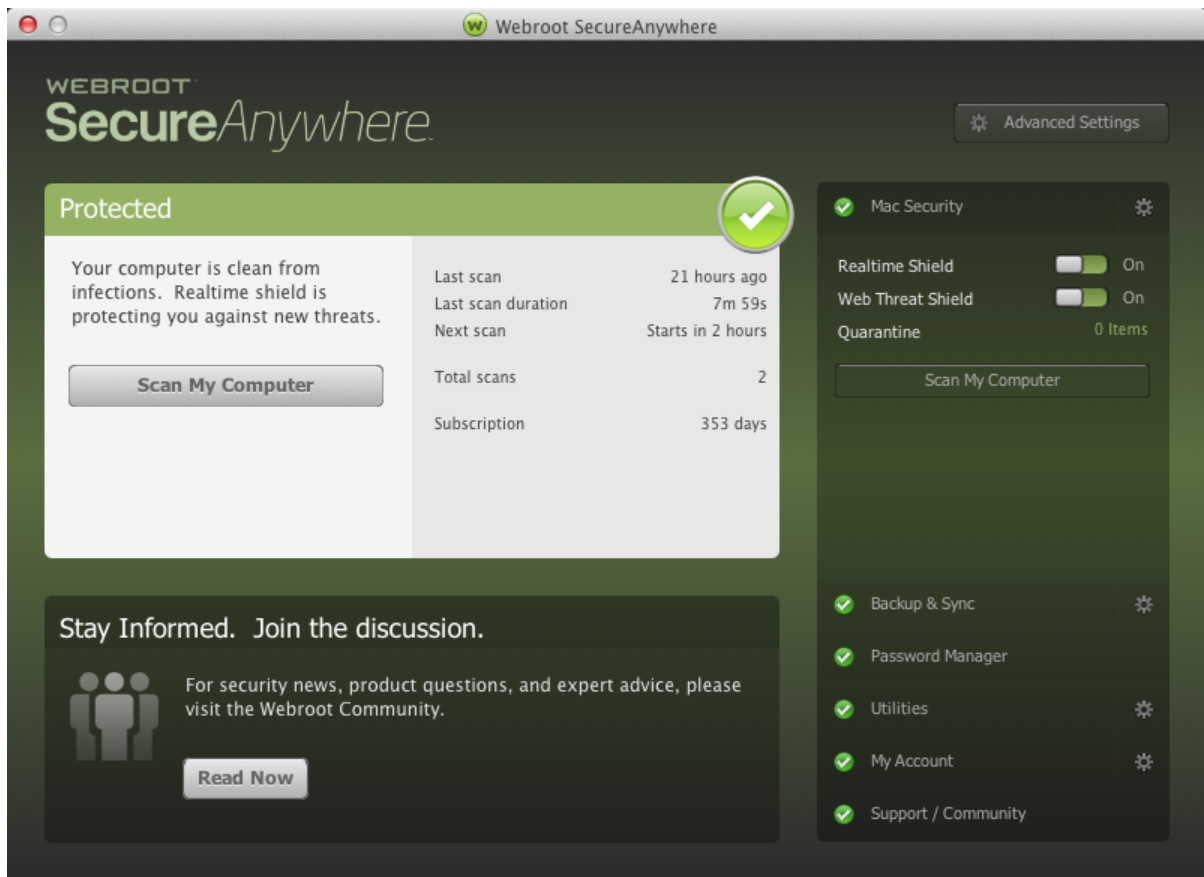
- [Main window](#)
- [Menu bar](#)

To use the main window:

1. To display the main window, from the menu bar, click the **Webroot** icon.
2. From the drop-down menu, select **Open Webroot SecureAnywhere**.



When your system is secure, the main window looks similar to the following example.



To indicate your Mac's overall protection status, the interface changes colors as follows:

- **Green** — Your Mac is secure.
- **Blue** — One or more potential risks require your attention.
- **Red** — One or more critical items require your intervention.

To use the menu bar:

1. To display the menu bar options, click the **Webroot SecureAnywhere** menu.

The following options display.



The following table describes the menu items under Webroot SecureAnywhere.

OPTION	DESCRIPTION
About SecureAnywhere	Displays the SecureAnywhere version number.
Preferences	Allows you to change system preferences, scan schedules, and other settings.
My SecureAnywhere Account	Displays your keycode and other account details.
Check for Updates	Downloads and applies the latest program updates.
Hide Webroot SecureAnywhere	Hides the main window, but does not shut down SecureAnywhere protection. To shut down protection, click the Webroot icon in the menu bar and select Shut Down SecureAnywhere .

The following table describes the drop-down menu items under Utilities.

OPTION	DESCRIPTION
System Control	Allows you to adjust the threat-detection settings for all programs and processes running on your Mac.
Reports	Allows you to save a scan log, which might be helpful if you are working with Webroot Support to determine the cause of a problem.
Submit a File	Allows you to send the file to Webroot for analysis. You might want to submit a file if you think it's causing problems or if you know it's safe and want it reclassified.
System Analyzer	Provides a simple utility for locating threats, security vulnerabilities, and other computer problems. The completed report recommends how to increase system performance, privacy, and protection.

Creating Webroot Accounts

By creating a Webroot account, you can view and manage the security status of your Mac from any device with an Internet connection. This status information is available on the SecureAnywhere website, at my.webrootanywhere.com. From here, you can manage security across multiple devices from a single location, making it easier to determine if all your devices are protected or if any need attention.

- For more information, see [Creating Accounts](#) in the [WSA Management Website User Guide](#).
 - For more information about using the website to manage your devices, see [Managing Your Account](#) in the [WSA Management Website User Guide](#).
-

Responding to Alerts

If SecureAnywhere detects a potential threat on your Mac, it may display an alert.

To respond to an alert:

1. When an alert displays, it prompts you to make a decision:
 - If you aren't sure how to manage this item, we recommend that you click **OK** to block it.



- If you are absolutely certain that the detected activity is legitimate, click **Ignore** to proceed.

The system moves blocked items to quarantine. For more information, see [Managing Quarantined Items on page 60](#).

Chapter 3: Scanning For Malware

To scan for malware, see the following topics:

Running Scans	24
Managing Detected Threats	27
Changing Scan and Optimization Schedules	29
Changing Scan Settings	33
Scanning Specific Files and Folders	36

Running Scans

Scans run automatically every day, at about the same time you installed SecureAnywhere. For example, if you installed SecureAnywhere at 8 p.m., the system always launches a scan around 8 p.m. It will not disrupt your work, nor will it launch while you play games or watch a movie. During scans, SecureAnywhere searches all areas where potential threats can hide, including drives, files, and system memory. It looks for items that match our threat definitions, match descriptions in our community database, or exhibit suspicious behavior.

Although scans run automatically, you can launch a scan at any time. An immediate scan might be necessary if you surfed a high-risk website, such as networking, music, or adult entertainment, downloaded high-risk items such as screen savers, music, or games, or accidentally clicked on a suspicious pop-up advertisement. You can run a scan from the menu bar or from the main window.

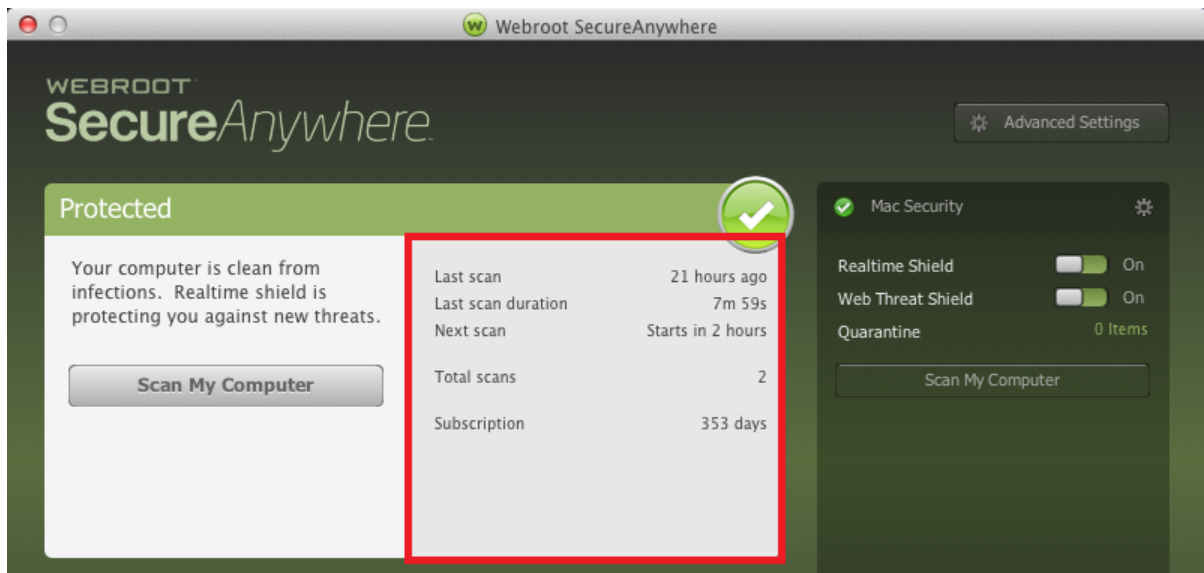
This topic contains the following procedures:

- [Viewing Scan Results](#)
- [Running Scan From Menu Bar](#)
- [Running Scan From Window](#)

To view scan results:

1. Open the SecureAnywhere interface by clicking the **Webroot** icon in the menu bar, then, from the drop-down menu, select **Open Webroot SecureAnywhere**.

The scan statistics display in the middle of the Protected window.



To run a scan from the menu bar:

1. From the menu bar, click the **Webroot** icon.
2. From the drop-down menu, click **Scan My Computer**.

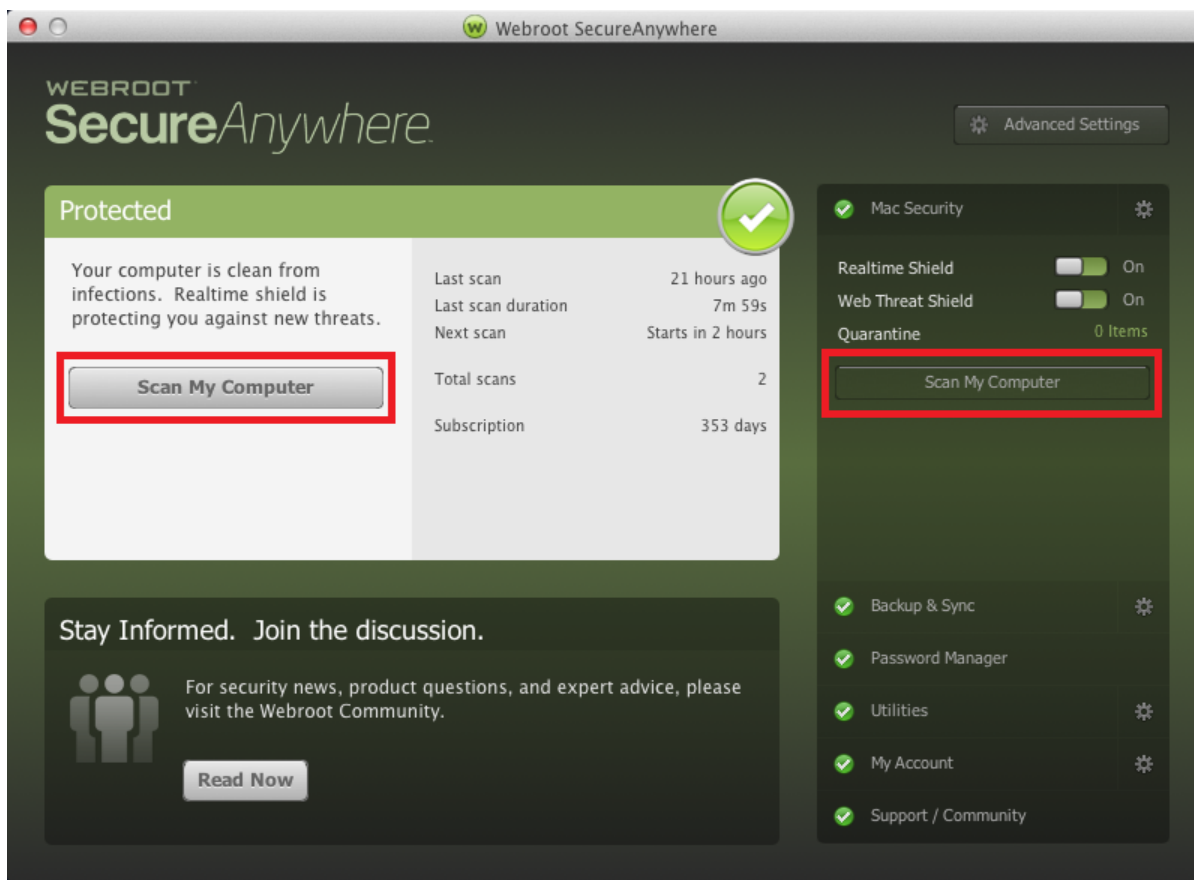


If SecureAnywhere locates threats, it opens a window that guides you through the quarantine process. For more information, see [Managing Detected Threats on page 27](#).

To run a scan from the main window:

1. Open the SecureAnywhere interface by clicking the **Webroot** icon in the menu bar, then, from the drop-down menu, select **Open Webroot SecureAnywhere**.

2. Click the **Scan My Computer** button.



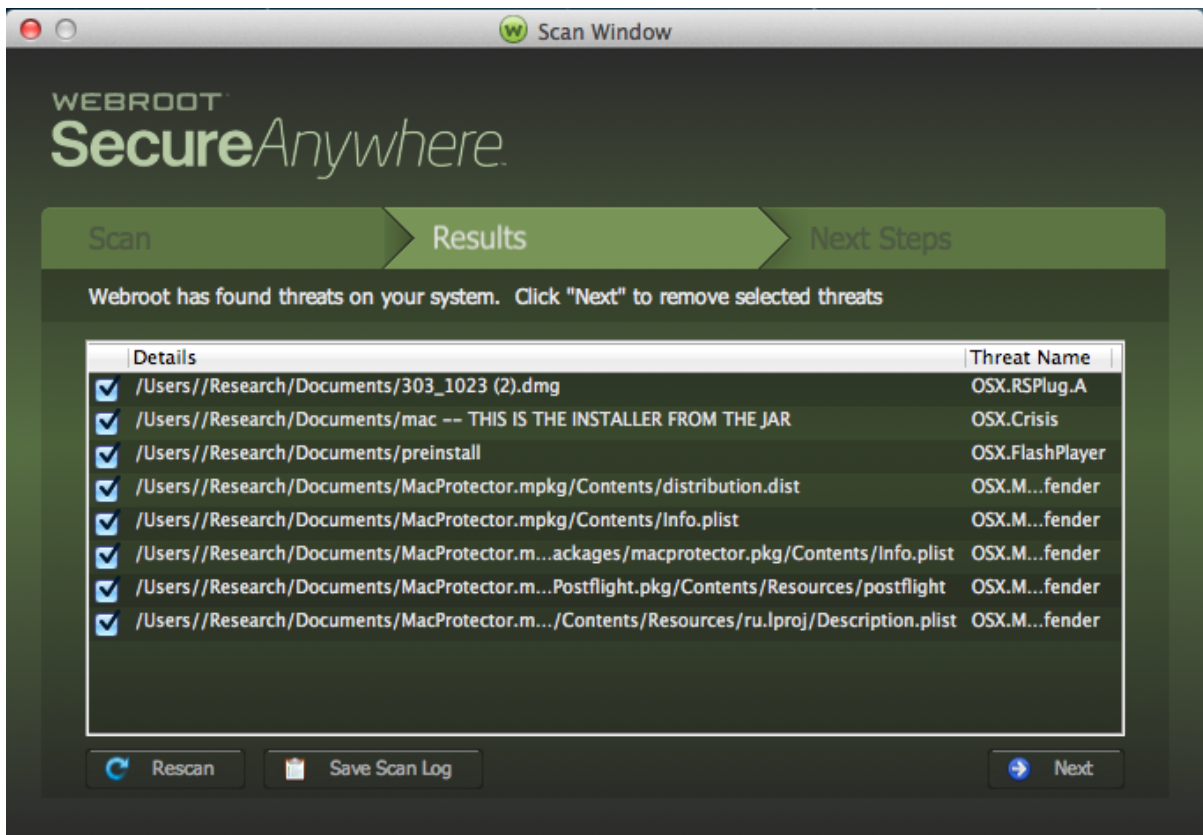
If SecureAnywhere locates threats, it opens a window that guides you through the quarantine process. For more information, see [Managing Detected Threats on page 27](#).

Managing Detected Threats

If SecureAnywhere detects a threat or suspicious file, it prompts you to manage the item. Follow this procedure on how to manage any threats to your system.

To manage detected threats:

1. In the Results panel, review the list of file names.

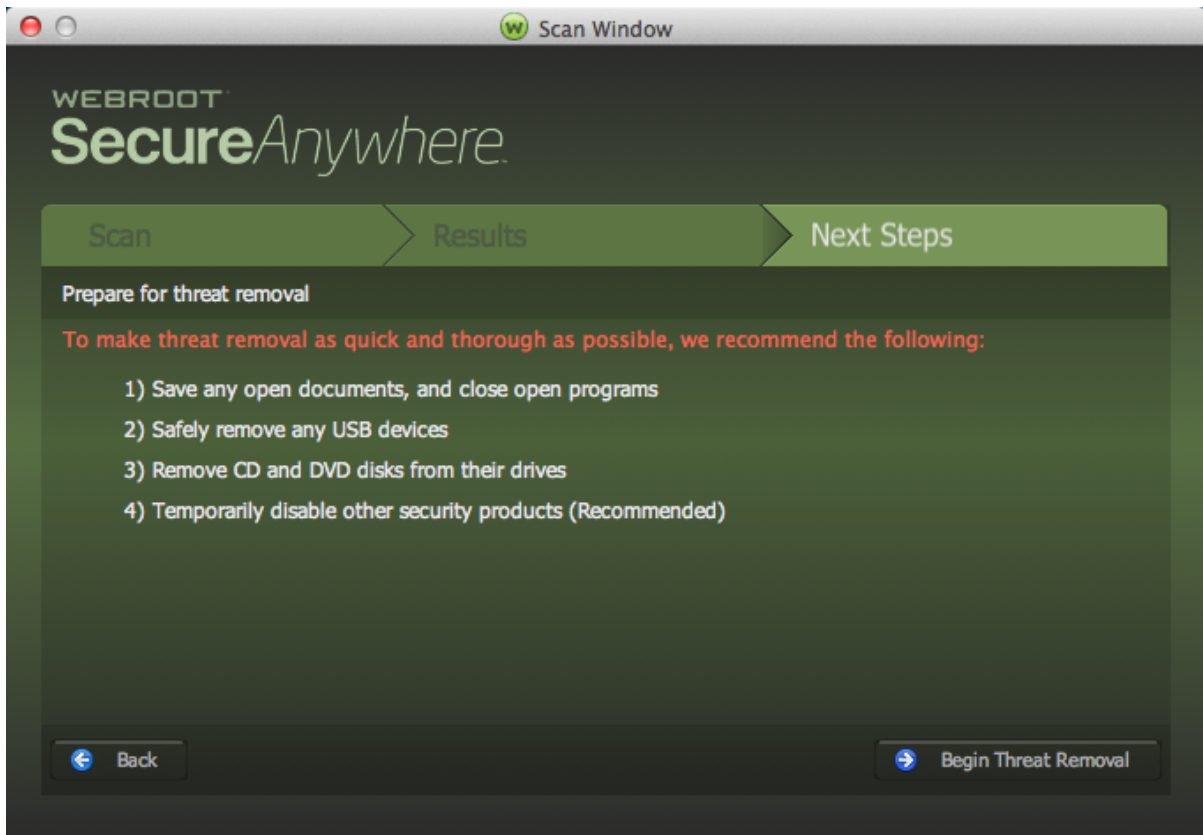


2. Do either of the following:
 - Keep the checkboxes selected, so items will be moved to quarantine.
 - Deselect any checkbox for which you recognize a filename and know that you need it to run an application.

For any items you deselect, SecureAnywhere restores them to their original locations.

Note: Do not restore a file unless you are absolutely sure it is legitimate.

3. On the bottom right of the window, click the **Next** button.



Note: We recommend that you click the **Next** button to move all items to quarantine, where they are rendered inoperable. If you determine later that you need a file, you can restore it to its original location.

4. On the Next Steps panel, click the **Begin Threat Removal** button. SecureAnywhere runs a follow-up scan again to make sure all threat traces are removed. If you cancel the scan, the main panel remains in a Threats Detected state and prompts you to run a scan.

Changing Scan and Optimization Schedules

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

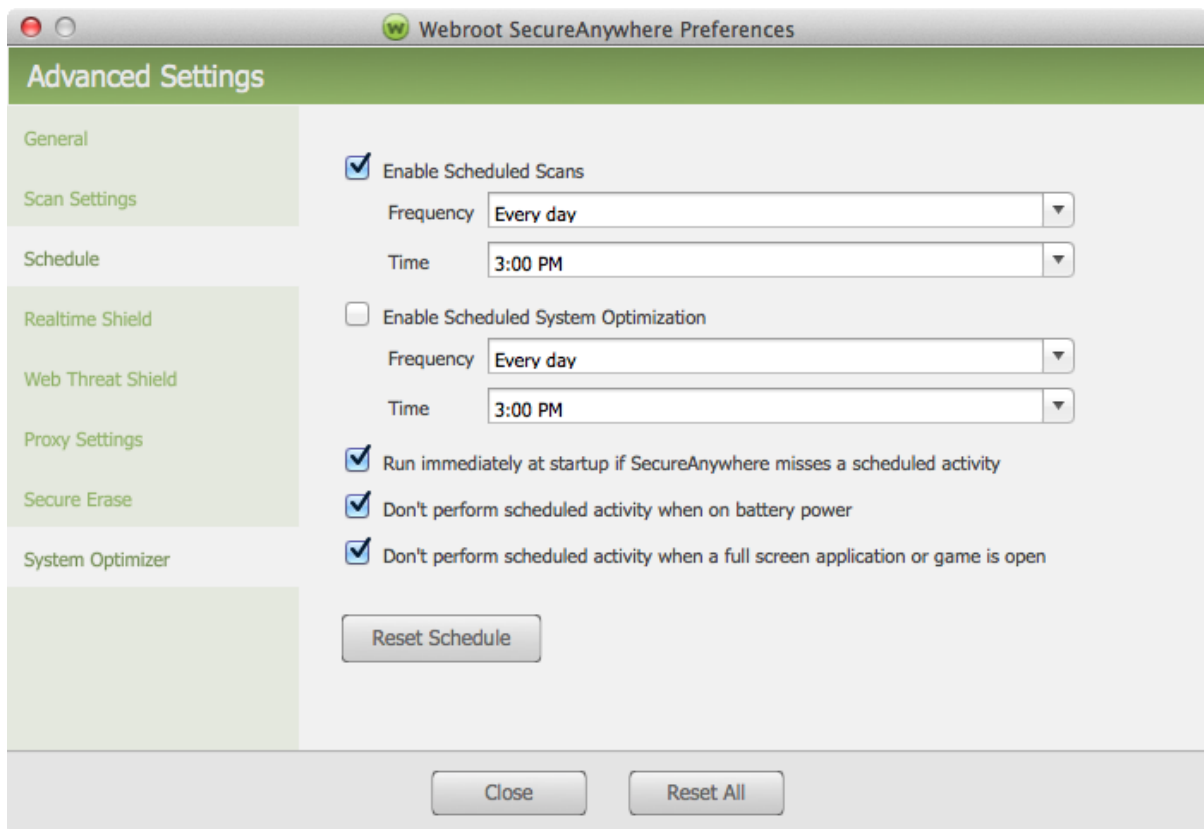
To change the scan schedule:

1. Open the SecureAnywhere interface by clicking the **Webroot** icon in the menu bar, then, from the drop-down menu, select **Open Webroot SecureAnywhere**.
2. From the menu bar, select **Webroot SecureAnywhere > Preferences**.

You can also access the scan schedule by clicking the **Advanced Settings** button from the main interface.



3. In the Preferences window, in the left of the pane, select **Scan Schedule**.



4. Select the checkbox to enable it, or deselect the checkbox to disable it.

SETTING	DESCRIPTION
Enable Scheduled Scans	If needed, select the checkbox, then enter scan frequency and time in the fields.
Enable Scheduled System Optimization	<p>If needed, select the checkbox, then enter scan frequency and time in the fields.</p> <p>Note: System Optimizer for Mac is only available on the consumer edition of Webroot SecureAnywhere.</p>
Scan immediately at startup if SecureAnywhere misses a scheduled scan	Launches a scheduled scan within an hour after you turn on your Mac. If you deselect this checkbox, SecureAnywhere ignores missed scans.
Don't perform scheduled scans when on battery power	Helps conserve battery power. If you deselect this checkbox, scans will run while your Mac is disconnected from a power source.
Don't perform scheduled scans when a full screen application or game is open	Ignores scheduled scans when you are viewing a full-screen application, such as a movie or a game. Deselect this checkbox to scheduled scans to run anyway.

5. As needed, do either of the following:
- To return to the recommended settings, click the **Reset Scan Schedule** button.
 - To return to the recommended settings for all preferences, click the **Reset All** button.

6. Click the **Close** button to save the new settings.
-

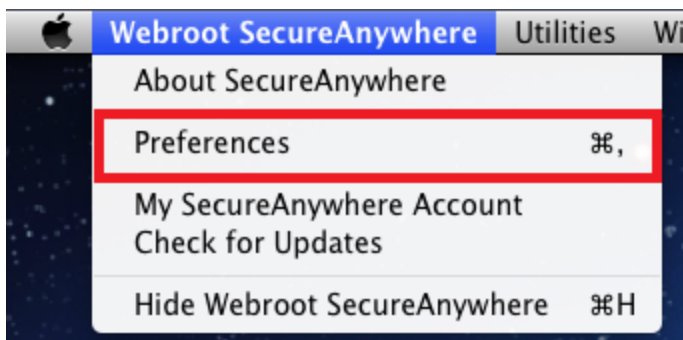
Changing Scan Settings

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

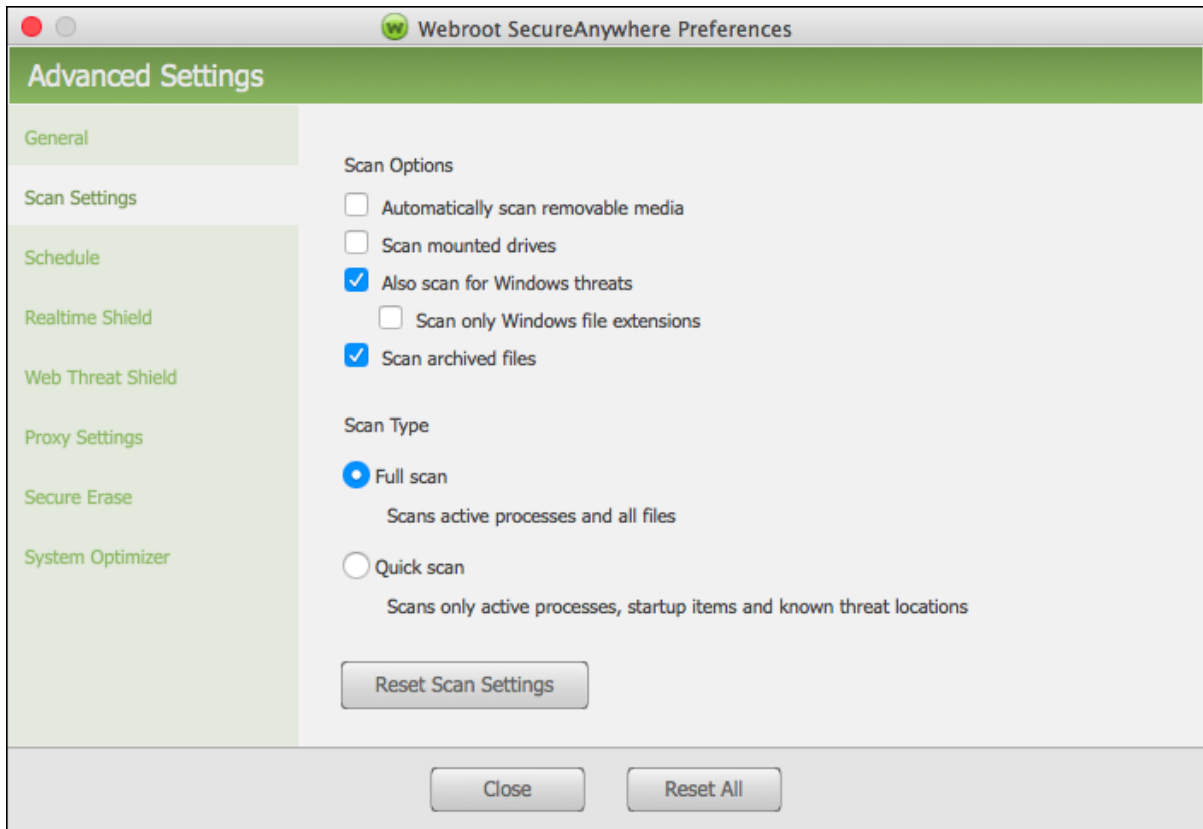
To change the scan settings:

1. Open the SecureAnywhere interface by clicking the **Webroot** icon in the menu bar, then, from the drop-down menu, select **Open Webroot SecureAnywhere**.
2. From the menu bar, select **Webroot SecureAnywhere > Preferences**.

You can also access the scan schedule by clicking the **Advanced Settings** button from the main interface.



3. In the Preferences window, in the left column, select **Scan Settings**.



4. Do any of the following:
 - **Automatically scan removable media** — Select this checkbox to scan any removable media upon insertion.
 - **Scan mounted drives** — Select this checkbox to include USB flash drives, external hard drives, disk image files, and other types of mounted drives in the scan.
 - **Also scan for Windows threats** — This checkbox is automatically selected, and pertains to threats that may be carried on the Mac, but that are designed to attack Windows machines.
 - **Scan only Windows file extensions** — Select this checkbox to only scan files with Windows file extension types such as .exe, .dll, etc.
 - **Scan archived files** — This checkbox is automatically selected, and determines that archived files such as .ZIP are included in the scan.

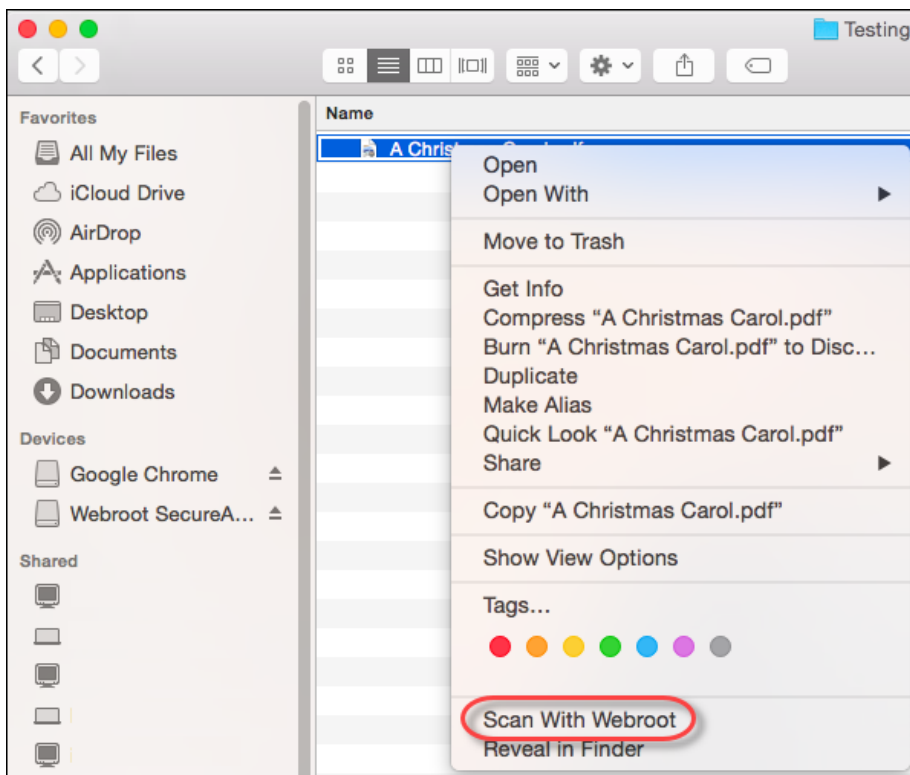
5. In the Scan Type area, select one of the following radio buttons:
 - **Full scan** — Thoroughly searches for all types of threats in all areas. This radio button is automatically selected, and the scan runs automatically.
 - **Quick scan** — Performs a surface scan of locations where threats are commonly found. This scan runs quickly, but may miss some types of inactive malware that launch after a system reboot.
 6. As needed, do either of the following:
 - To return to the recommended Scan settings, click the **Reset Scan Settings** button.
 - To return to the recommended settings for all preferences, click the **Reset All** button.
 7. When you're done, click the **Close** button.
-

Scanning Specific Files and Folders

Webroot scans your computer based on your [scan settings](#), however, you can scan specific files and folders, as needed.

To scan a specific file or folder:

1. Go to the file or folder you want to scan, and select it.
2. Press the **Control** button and right click on the file or folder.
3. From the menu that displays, select **Scan With Webroot**.



4. Webroot scans the individual file or all of the files in the folder you selected. Scan results display.
 5. As needed, follow the [Managing Detected Threats on page 27](#) procedure.
-

Chapter 4: Shielding Your Mac

To shield your Mac, see the following topics:

Mac Shields Overview	38
Types of Shields	38
Indicators Displayed With Query Results	39
Infrared Shielding and Warning Messages	40
Low-Risk Warning	41
Medium-Risk Warning	41
High-Risk Warning	42
Managing Shields	43
Accessing and Updating Web Threat Shield Settings	46
Changing Realtime Shield Settings	52
Managing Web Threats	56

Mac Shields Overview

Shields constantly monitor activity while you surf the Internet and work on your computer, protecting your computer from malware and viruses. As you surf Internet sites, you could be targeted for a drive-by download, where an unwanted program launches and silently installs on your computer as you view pages. We recommend you keep all shields enabled. For more information, see [Changing Realtime Shield Settings on page 52](#) or [Accessing and Updating Web Threat Shield Settings on page 46](#).

Shields run in the background without disrupting your work.

- If a shield detects an item that it classifies as a potential threat or does not recognize, it displays an alert. The alert asks if you want to continue or block the site. Do one of the following:
 - If you recognize the file name and you are purposely downloading it, for example, you were in the process of downloading a new toolbar for your browser, click **Unblock page and continue**.
 - If you were not trying to download anything, you should click **Go back to safety**
 - If you feel that the shield is alerting you to a page that is not high risk, then you can click the **Request Review** button.

For more information on all of these options, see [Managing Web Threats on page 56](#).

Types of Shields







SecureAnywhere includes the following types of shields:

- **Realtime shield** — Monitors unknown programs to determine whether or not they contain threats. Blocks known threats from running on your computer that are listed in Webroot's threat definitions and in our community database. You should never disable this shield.
- **Rootkit shield** — Blocks rootkits from being installed on your computer and removes any that are present.
- **Web shield** — Blocks known threats encountered on the Internet and displays a warning. The Web shield maintains information on more than 200 million URLs and IP addresses to comprise the most accurate and comprehensive data available for classifying content and detecting malicious sites.
- **USB shield** — Monitors an installed USB flash drive for threats, blocks and removes any threats that it finds.
- **Offline shield** — Protects your system from threats while your computer is not connected to the Internet.

The shields are pre-configured, based on our recommended settings. You do not need to configure any settings yourself unless you are an advanced user and would like to change the settings. For more information, see [Changing Shield Settings](#).

Indicators Displayed With Query Results

When you run an Internet query such as a Google search, SecureAnywhere shields modify the results display with icons that give you safety information about each website returned as a result of the search. The icon displays to the left of each website name in the list of query results. The table below describes the meaning of each icon.

ICON	Description
	These are well known sites with strong security practices, and rarely exhibit characteristics that expose you to security risks. There is a very low probability that you will be exposed to malicious links or payloads.
	These are benign sites, and rarely exhibit characteristics that expose you to security risks. There is a low probability that you will be exposed to malicious links or payloads.
	These are generally benign sites, but have exhibited some characteristics that suggest security risk. There is some probability that you will be exposed to malicious links or payloads.
	These are suspicious sites. There is a higher than average probability that you will be exposed to malicious links or payloads.
	These are high risk sites. There is a high probability that you will be exposed to malicious links or payloads.
	Ratings are temporarily unavailable or the Webroot agent is shut down. Wait for service to be restored or check to be sure the Webroot agent is running.

Infrared Shielding and Warning Messages

SecureAnywhere might display warnings to you even if you are not currently running a scan. There could be an unauthorized access to your computer even if you are working elsewhere on your computer and not currently surfing the Internet.

In some cases, SecureAnywhere takes care of the problem automatically; for less severe cases, you are prompted to make a decision about whether or not you want to continue.

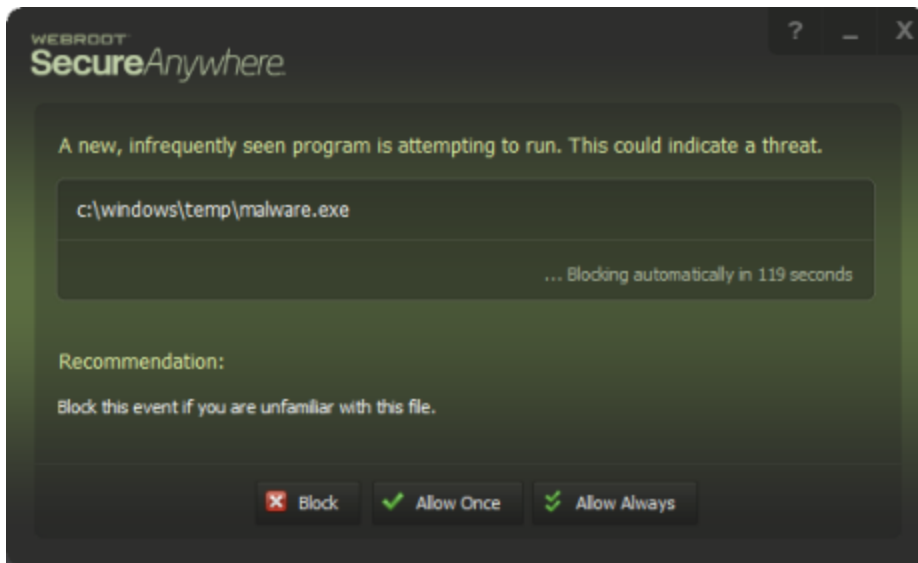
To make a determination about what level of warning to display, SecureAnywhere uses a technology called Infrared. Infrared is a multi-layer defense that blocks threats very early in their lifecycle. This is accomplished through a number of engines that work together, considering several factors:

- The safety level of websites.
- The reputation and behavior of newly introduced applications.
- By interpreting user behavior with an overall assessment of the safety level of the system. If a user is classified as a higher risk, based on a combined view of the security of their operating system, applications, and prior threats which have been observed, Infrared dynamically tunes its heuristics and background processing, flexing within the configuration options the user has set, but increasing their effectiveness while preventing false positives for the vast majority users.

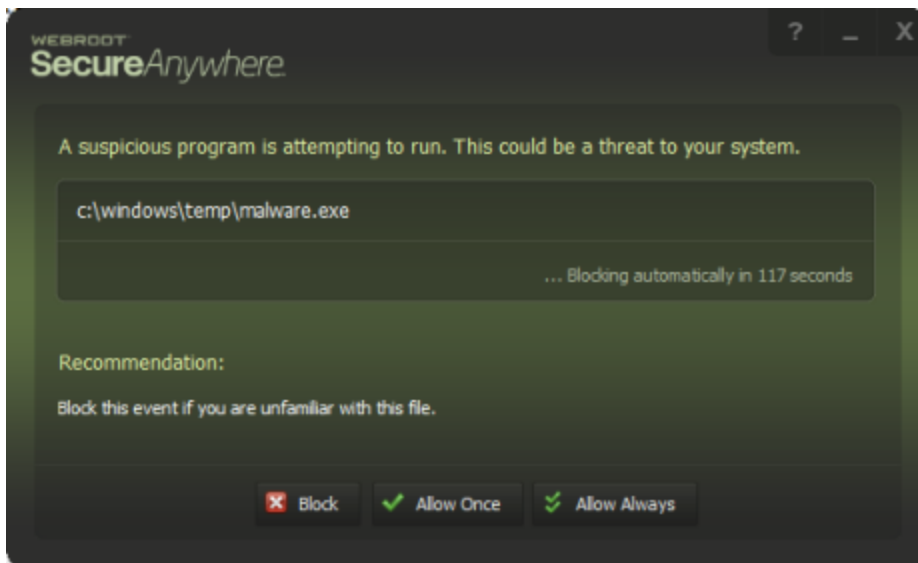
This risk assessment affects every protection module, from the firewall to behavior monitoring to realtime protection, and eventually to website blocking as well. The end result is a set of protections that is custom-tailored to the user's specific circumstances.

The following are samples of warnings that may display on your screen.

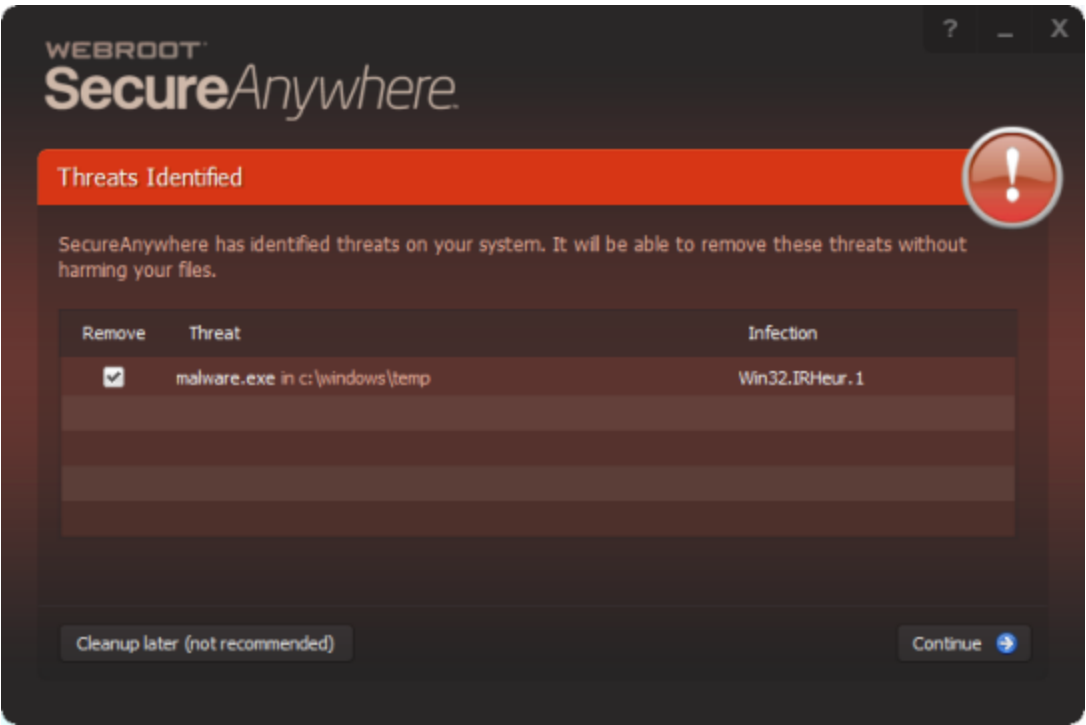
Low-Risk Warning



Medium-Risk Warning



High-Risk Warning



Managing Shields

As you surf the Internet, the shields automatically block and quarantine any threats that attempt to download and run on your Mac.

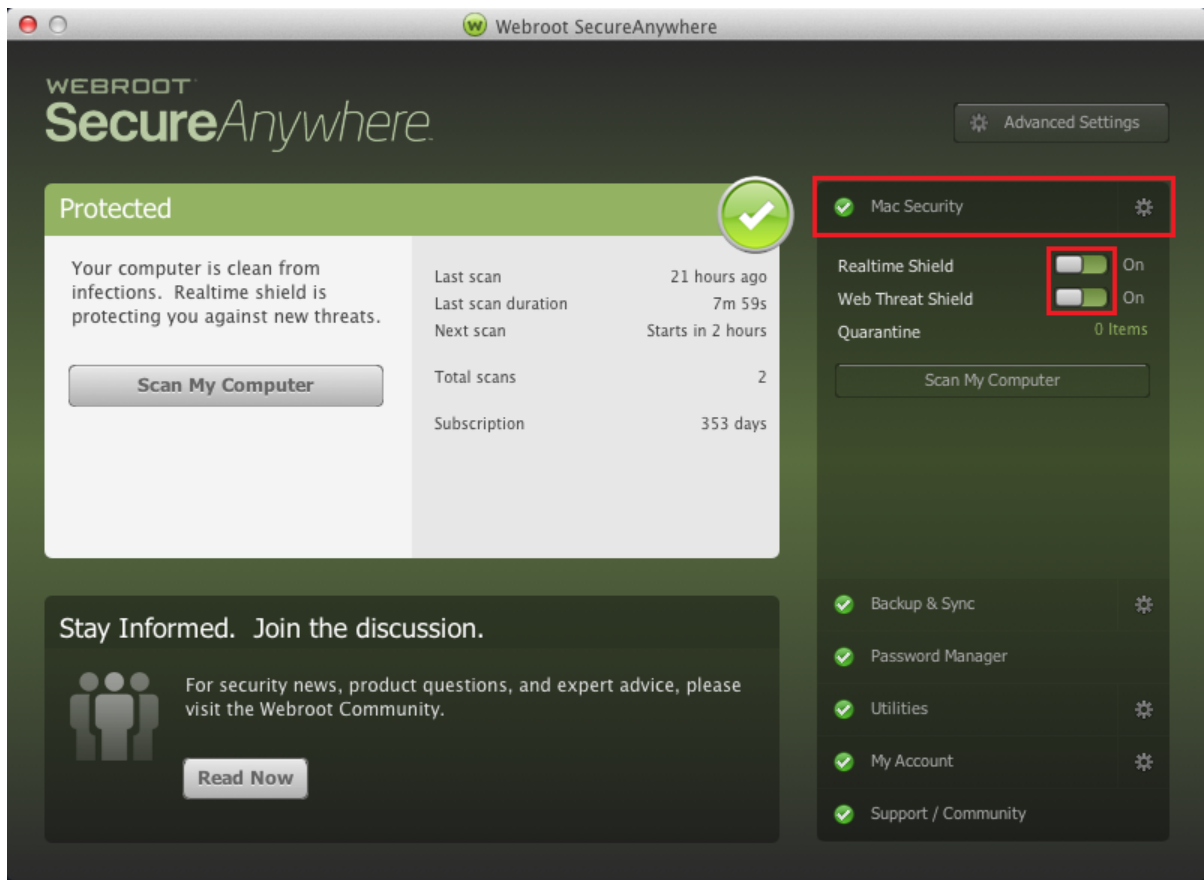
If a shield detects an item that it classifies as a potential threat or an item it does not recognize, it opens an alert. The alert asks if you want to allow the item to run or if you want to block it. If you aren't sure what to do, we recommend blocking the file.

The shields are preconfigured, based on our recommended settings. You do not need to configure any settings yourself unless you are an advanced user and would like to modify shield behavior.

To view shield status or to disable shields:

1. In the menu bar, click the **Webroot** icon to open the SecureAnywhere interface.
2. From the drop-down menu, select **Open Webroot SecureAnywhere**.

3. From the main window, click **Mac Security**.



SecureAnywhere includes two types of shields:

- **Realtime shield** — Controls how threats are blocked and quarantined on your Mac.
- **Web Threat shield** — Protects your system as you surf the Internet.

4. Click the button next to the shield name to turn it off.
 - If the orange indicator is to the left, the shield is off.
 - If the green indicator is to the right, the shield is on.

If you disable a shield, your Mac is vulnerable. The SecureAnywhere interface turns orange, which is a warning state.



5. You must restart your browser for website filter changes to take effect.
-

Accessing and Updating Web Threat Shield Settings

The Web Threat shield protects your Mac as you surf the Internet. If it detects a website that may be a threat, it blocks the page and asks if you want to continue despite the warning. In addition, this shield analyzes all the links on a search results page. It displays an image next to each link that signifies whether it's a trusted site or a potential risk. For more information about using Web Threat protection while surfing or using search engines, see [Managing Web Threats on page 56](#).

This topic contains the following procedures:

- [Accessing Web Threat Shield Settings](#)
- [Changing Web Threat Shield Settings](#)
- [Overriding Website Filters](#)
- [Shielding Mac Host Files](#)
- [Disabling Website Filters](#)

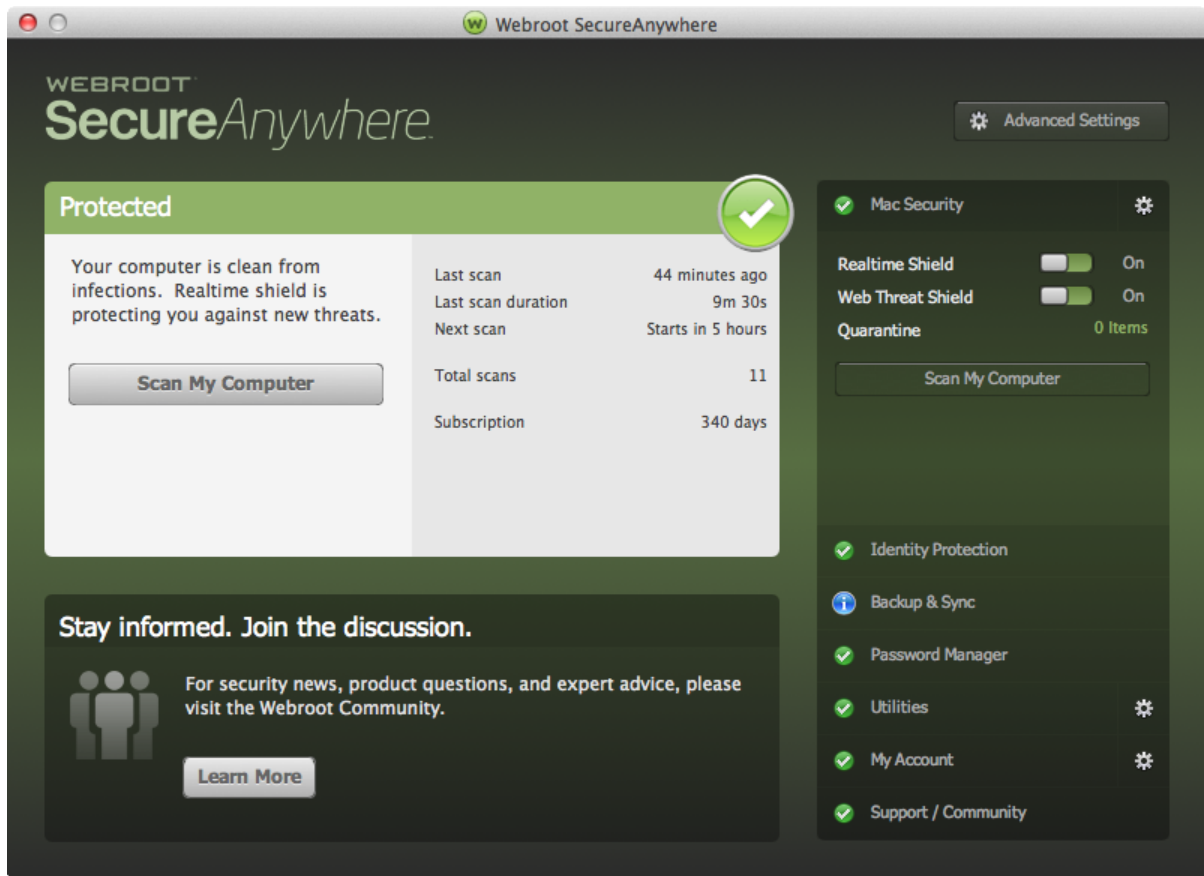
Note: During installation, SecureAnywhere prompted you to install the Safari extension, and also extensions for Chrome and Firefox, if they are installed. If you declined to install these, you cannot use Web Threat protection. If you decide later to turn on Web Threat protection, SecureAnywhere will then prompt you to install the extensions. For more information on enabling shield, see [Managing Shields on page 43](#).

To access Web Threat shield settings:

1. From the dock, click the **Webroot** icon.



2. The main interface displays.

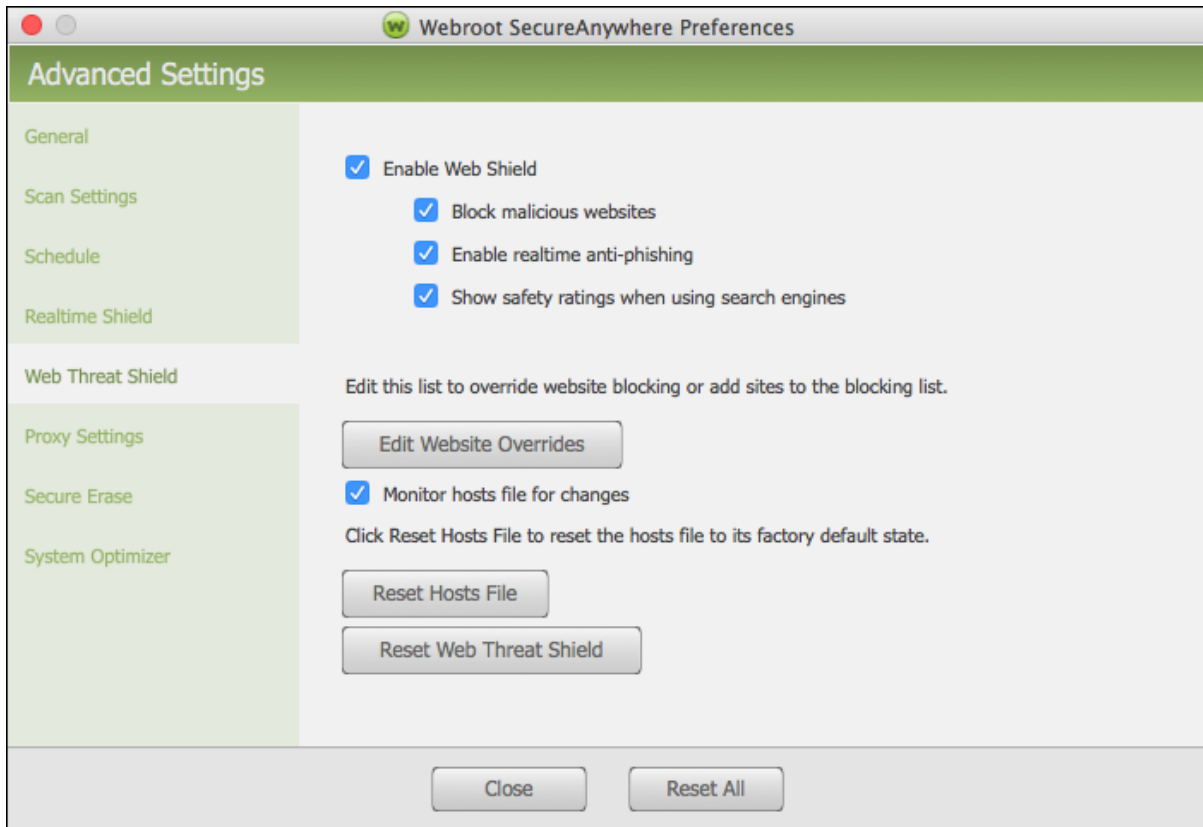


3. From the menu bar, select **Webroot SecureAnywhere > Preferences**.



The Advanced Settings Window displays.

4. In the left column, select **Web Threat Shield**.



Continue with any of the following procedures, as needed:

- [Changing Web Threat Shield Settings](#)
- [Overriding Website Filters](#)
- [Shielding Mac Host Files](#)
- [Disabling Website Filtering](#)

To change Web threat Shield settings:

1. Do either of the following:
 - To enable a setting, select the checkbox.
 - To disable a setting, deselect the checkbox.

SETTING	DESCRIPTION
Enable Web Shield	Enable or disable the Web Shield. This checkbox is selected by default, which is the setting we recommend.
Block malicious websites	Any URLs and IPs you enter in a browser are checked and a block page is presented for known malicious sites. This checkbox is selected by default, which is the setting we recommend.
Enable realtime anti-phishing	Protects against zero day phishing sites. Zero day phishing sites are sites that have never been seen before, and their related viruses do not yet have a definition. This checkbox is selected by default, which is the setting we recommend.
Show safety ratings when using search engines	Search result are annotated with an icon and tooltip, indicating the likelihood that a site is malicious. This checkbox is selected by default, which is the setting we recommend.
Suppress the user's ability to bypass blocked websites (Business versions only)	Prevents users from bypassing blocked websites when a malicious website is detected. This checkbox is selected by default, which is the setting we recommend.
Suppress the user's ability to request website reviews (Business versions only)	Prevents users from submitting website reviews from the block page when a malicious website is detected. This checkbox is selected by default, which is the setting we recommend.

To override website filters:

1. Click the **Edit Website Overrides** button.
2. In the dialog, enter a website name in the field, using the form *www.sitename.com*, and click the **Add Website** button.
3. In the table, click one of the following radio buttons:
 - **Allow** — Allows the website.
 - **Block** — Blocks the website.
4. Click the **Close** button.
5. If Safari is open, quit the browser and reopen it.

You must restart your browser for website filter changes to take effect.

To shield the Mac's Hosts file:

1. Select the **Monitor hosts file for changes** checkbox.
2. To return the Hosts file to its factory state and remove changes malware may have made to the file, click the **Reset Hosts File** button.
3. Click the **Close** button.

To disable website filtering:

1. Click the **Webroot** icon in the menu bar to open Webroot.
2. From the drop-down menu, select **Open Webroot SecureAnywhere**.
3. From the main window, click **Mac Security**.
4. Click the button next to the shield name to turn it off.
 - If the orange indicator is to the left, the shield is off.
 - If the green indicator is to the right, the shield is on.

If you disable a shield, your Mac is vulnerable. The SecureAnywhere interface turns orange, which is a warning state.



5. You must restart your browser for website filter changes to take effect.
-

Changing Realtime Shield Settings

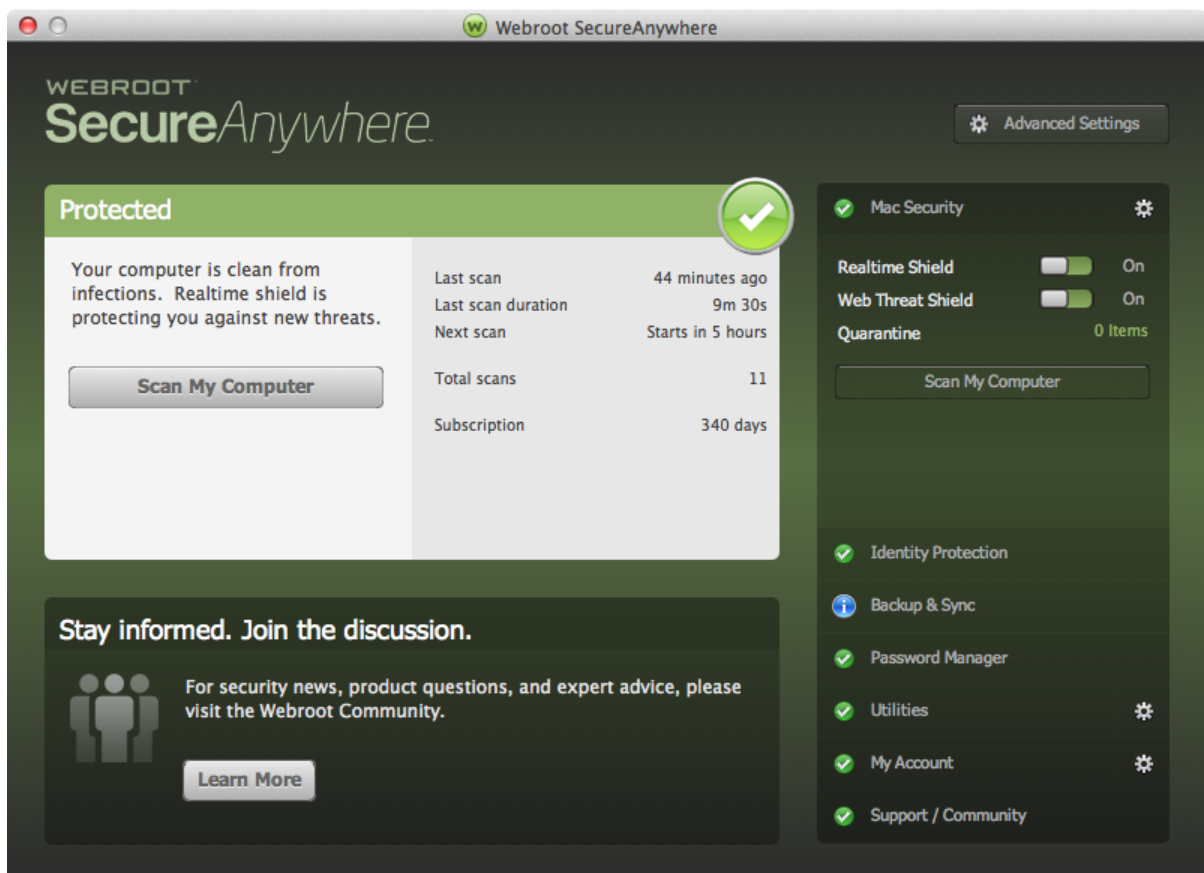
The Realtime shield controls how threats are blocked and quarantined on your Mac. Webroot already configured this shield with our recommended settings, but you can adjust them as needed.

To change Realtime shield settings:

1. From the dock, click the **Webroot** icon.



The main interface displays.

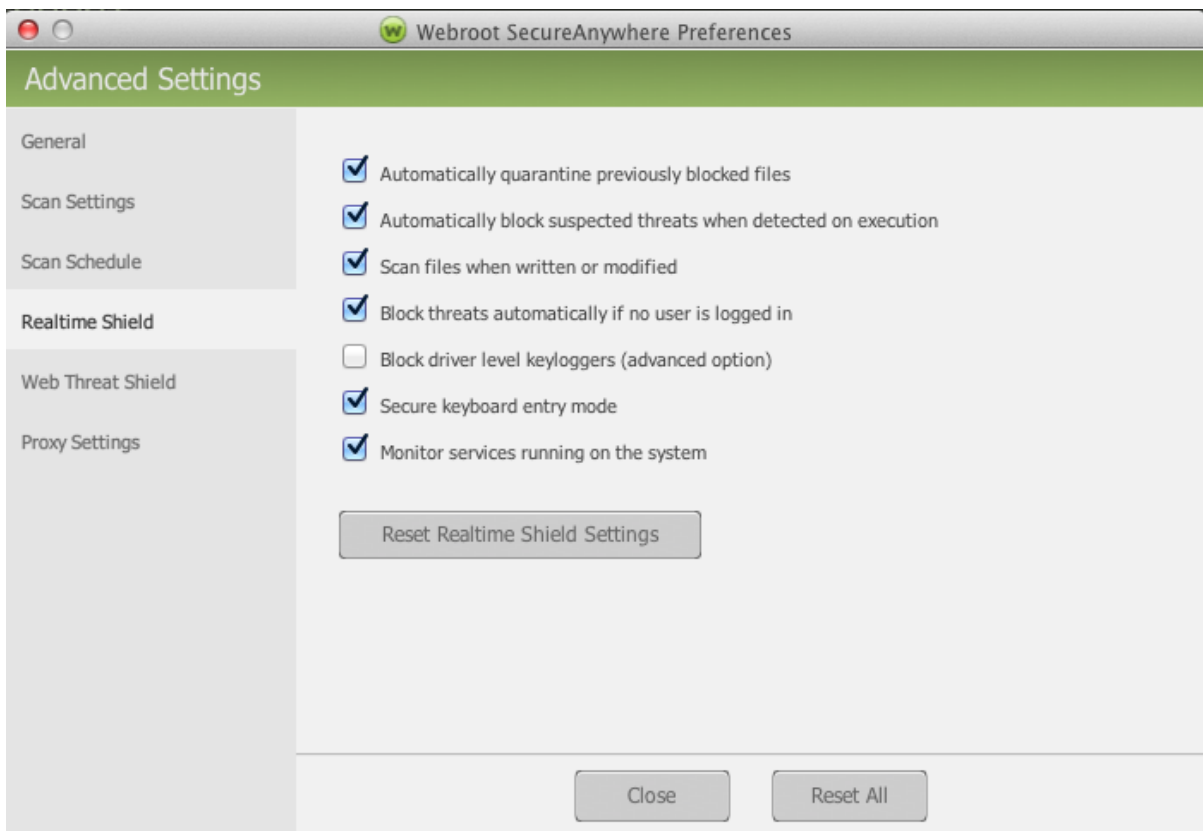


- From the menu bar, select **Webroot SecureAnywhere > Preferences**.



The Advanced Settings window displays.

- In the left column, select **Realtime Shield**.



4. Do either of the following, using the information in the following table:

- To enable a setting, select the checkbox.
- To disable the setting, deselect the checkbox.

SETTING	DESCRIPTION
Automatically quarantine previously blocked files	Sends an application file to quarantine if you had blocked and quarantined that file before. If you deselect this option, SecureAnywhere launches a scan if it detects the file again.
Automatically block suspected threats when detected on execution	Opens a notification if you attempt to launch an application that might be a threat. SecureAnywhere then scans the directory where the application resides. When the scan completes, it gives you the option of quarantining the items or allowing them to remain in their current locations.
Scan files when written or modified	Scans any new or modified files that you save to disk. If this option is deselected, it ignores new file installations.
Block threats automatically if no user is logged in	Stops threats from executing, even when you are logged off. Threats are sent to quarantine without notification.
Secure keyboard entry mode	Prevents keyloggers on websites from capturing keystrokes. A keylogger is a type of system monitor that can record all keystrokes in your browser. Keyloggers may be used for legitimate purposes, but can also be installed without your knowledge and used to record sensitive information.

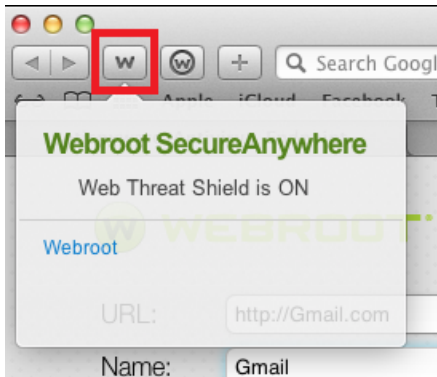
SETTING	DESCRIPTION
Block driver level keyloggers (advanced option)	Prevents keyloggers on your Mac from capturing keystrokes. A keylogger is a type of system monitor that can record all keystrokes in your browser. Keyloggers may be used for legitimate purposes, but can also be installed without your knowledge and used to record sensitive information. This setting is recommended for advanced users only.
Monitor services running on the system	Monitors the folders of system services running on your Mac, and protects against unwanted activity. If SecureAnywhere detects changes in the folders, it opens an alert. System services are programs that load automatically either as part of an application's startup process or the operating system startup process. Services are often a target for malware developers.

5. Do one of the following:

- To save the new settings, click the **Close** button.
- To return to the recommended settings, click the **Reset Realtime Threat Shield** button.
- To return to the recommended settings for all preferences, click the **Reset All** button.

Managing Web Threats

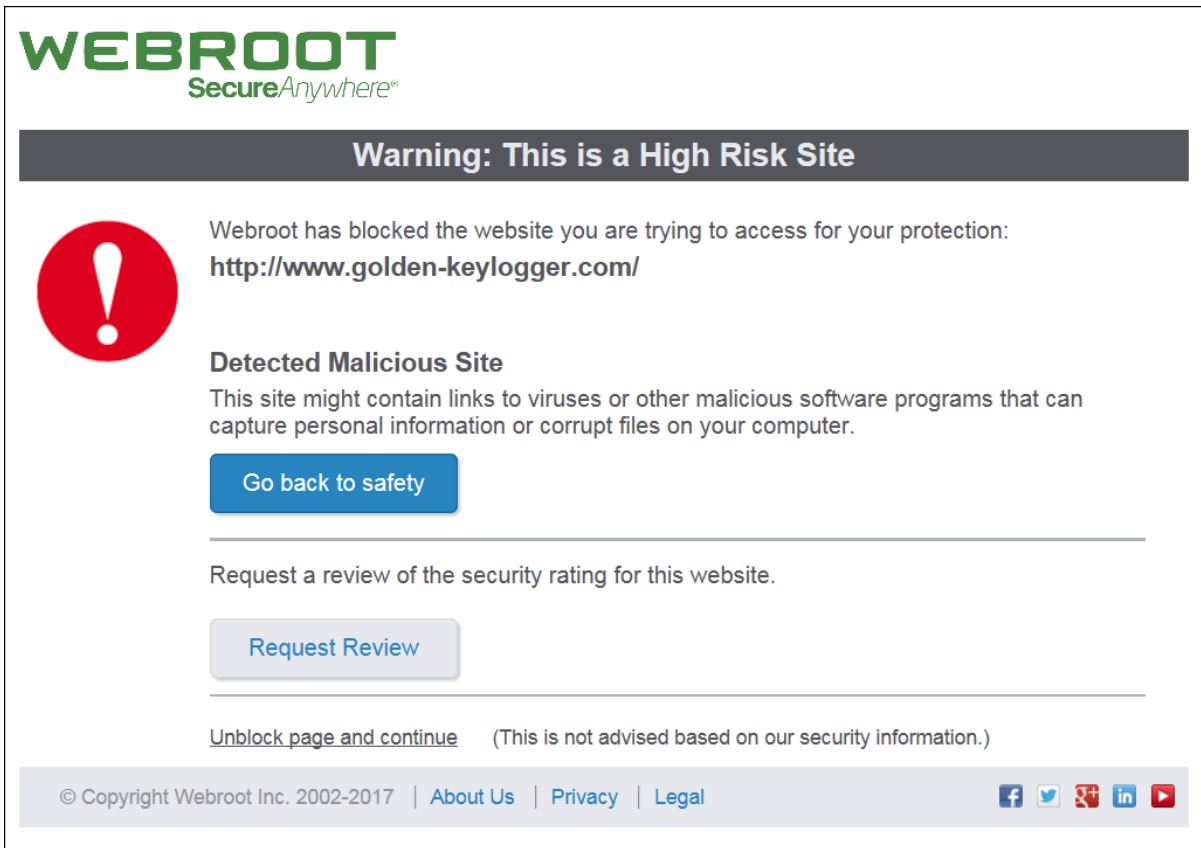
For Web Threat protection to work, make sure that the Web Threat shield is enabled, as described in [Accessing and Updating Web Threat Shield Settings on page 46](#). You can also determine if it's enabled by looking for the W button in the Safari taskbar:



When you are surfing the web and Webroot alerts you to the suspicious nature of a website, for example a [phishing attack](#), a [key logger attack](#), or a [malicious attack](#), follow this procedure to manage the threat.

To manage a web threat:

1. If when you are surfing the web, and Webroot displays a message similar to the following, stop and review the threat.



2. After you review information on the page, such as the URL or the type of threat that has been detected, click one of the following buttons:
 - **Go back to safety** — Click this button when you don't know the website, and do not want to expose your computer to malicious links or payloads. When you click this button, you are navigated away from the currently blocked content to a blank page to keep you safe.
 - **Request Review** — Click this button when you know the website, are comfortable with the contents, but believe the classification provided by Webroot of this URL needs to be changed to make sure the warning message does not display in future.

When you click this button, the page expands to display a field where you can enter information about the site. Enter any comments, your email, and enter your email address, if you would like to receive follow-up regarding your request. For more information about the categorization of the website you would like to have changed, see [URL Categorization Change Request](#).

When you're done, click the **Submit** button. Change requests are usually processed in 48-72 hours. If, after this period, you do not see the change you requested, you can [open a ticket with Webroot Support](#).

Request a review of the security rating for this website.

[Request Review](#)

Thank you for taking the time to help improve Webroot security.

By pressing the Submit button below, you will send us all the information we need to take a second look at the reputation of **http://www.golden-keylogger.com/**

Additional comments on the site are appreciated:

You may provide your email address so that our analysts can get back to you with questions and the status of your request. Your email will only be used for communicating regarding this request.

example@email.com

Submit

Note: To close the Request Review area, click the **Request Review** button again.

- **Unblock page and continue** — Click this button when you know the website, are comfortable with the contents, and want to visit the site. When you select this option, Webroot bypasses this URL, and will not block it again.

Chapter 5: Managing Quarantine

To manage quarantine, see the following topics:

Managing Quarantined Items	60
Managing File Detection	65
Saving Threat Logs	67

Managing Quarantined Items

As SecureAnywhere scans and shields your Mac, it removes all items associated with threats. It then disables their operation and moves them to a holding area, called quarantine. While in quarantine, threats can no longer harm your Mac or steal your information. You do not need to delete them, unless you want to conserve disk space.

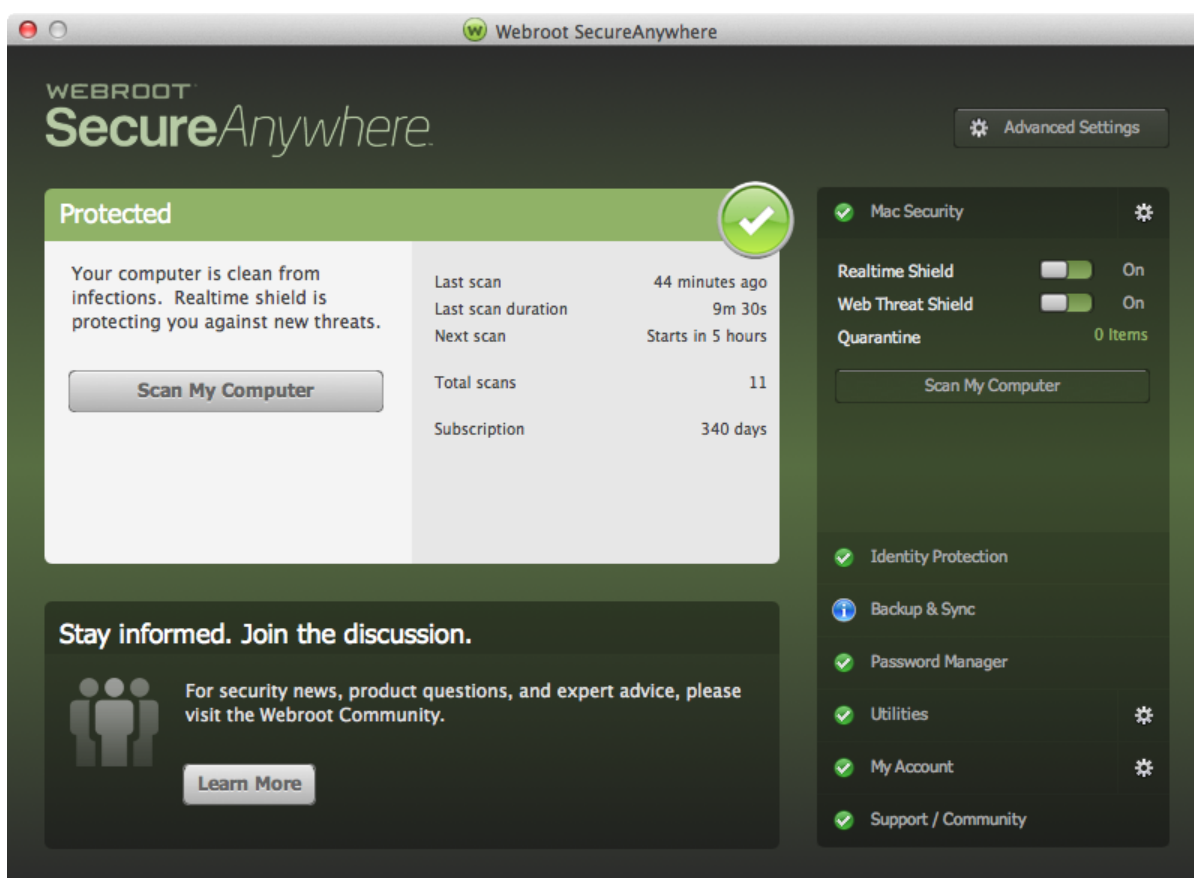
Note: Your safest action is to keep items in quarantine until you determine that all programs still work properly after the scan. If you discover that some legitimate programs cannot function after an item was moved to quarantine, you can restore the item to its original location.

To manage quarantined items:

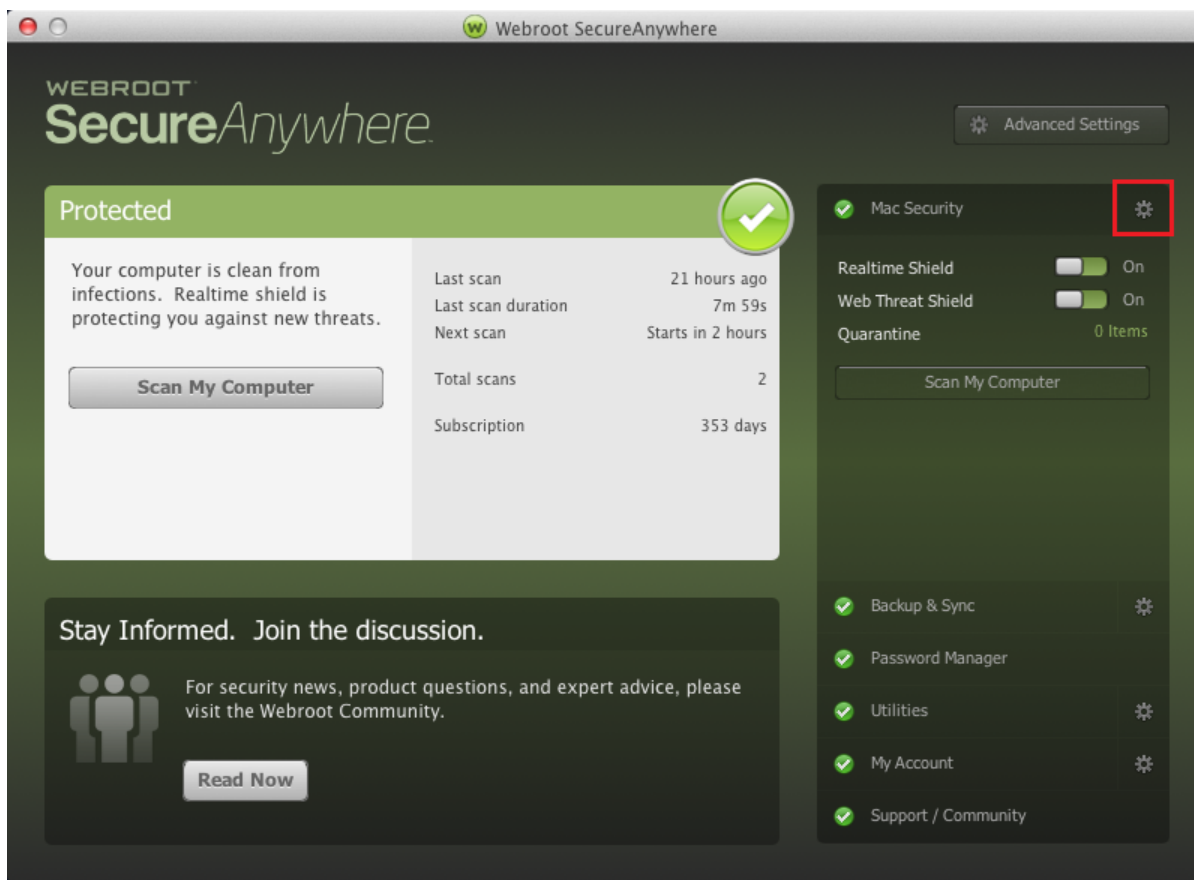
1. From the dock, click the **Webroot** icon.



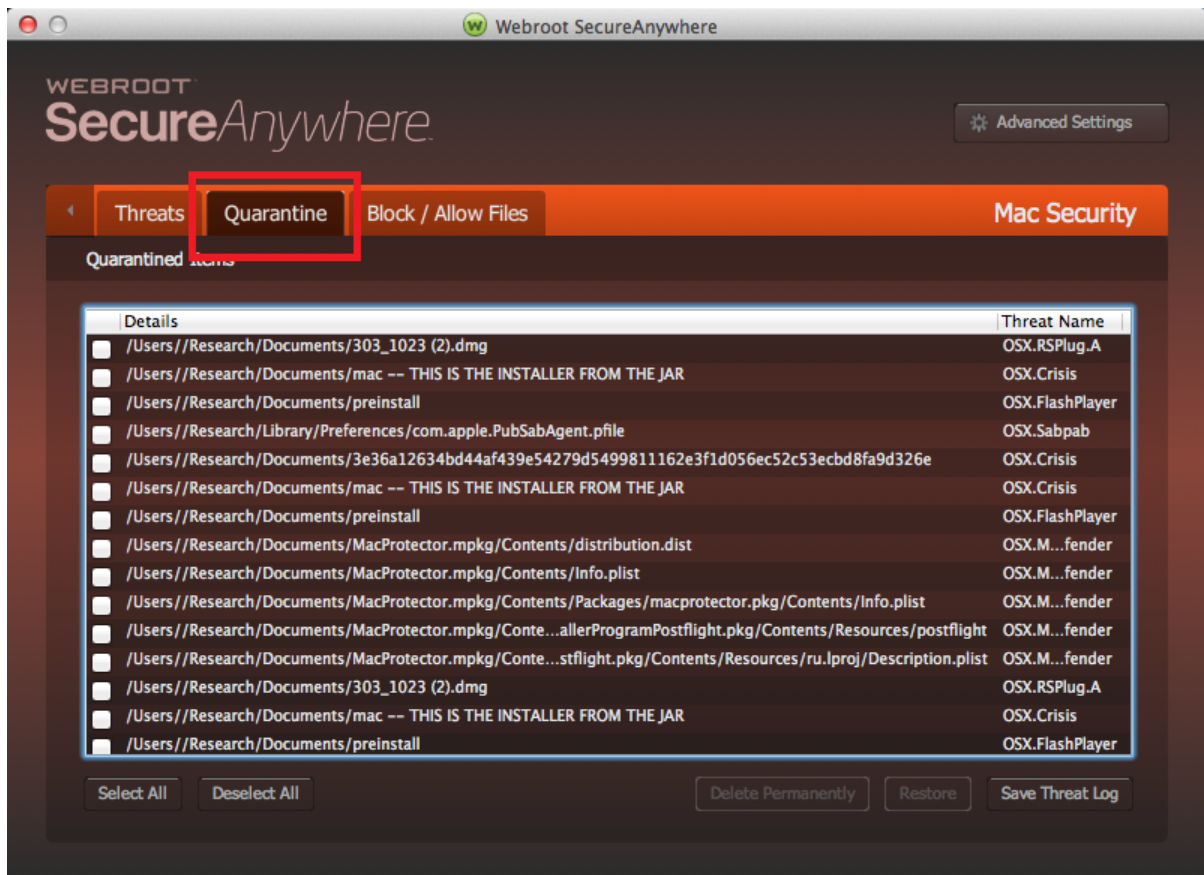
The main interface displays.



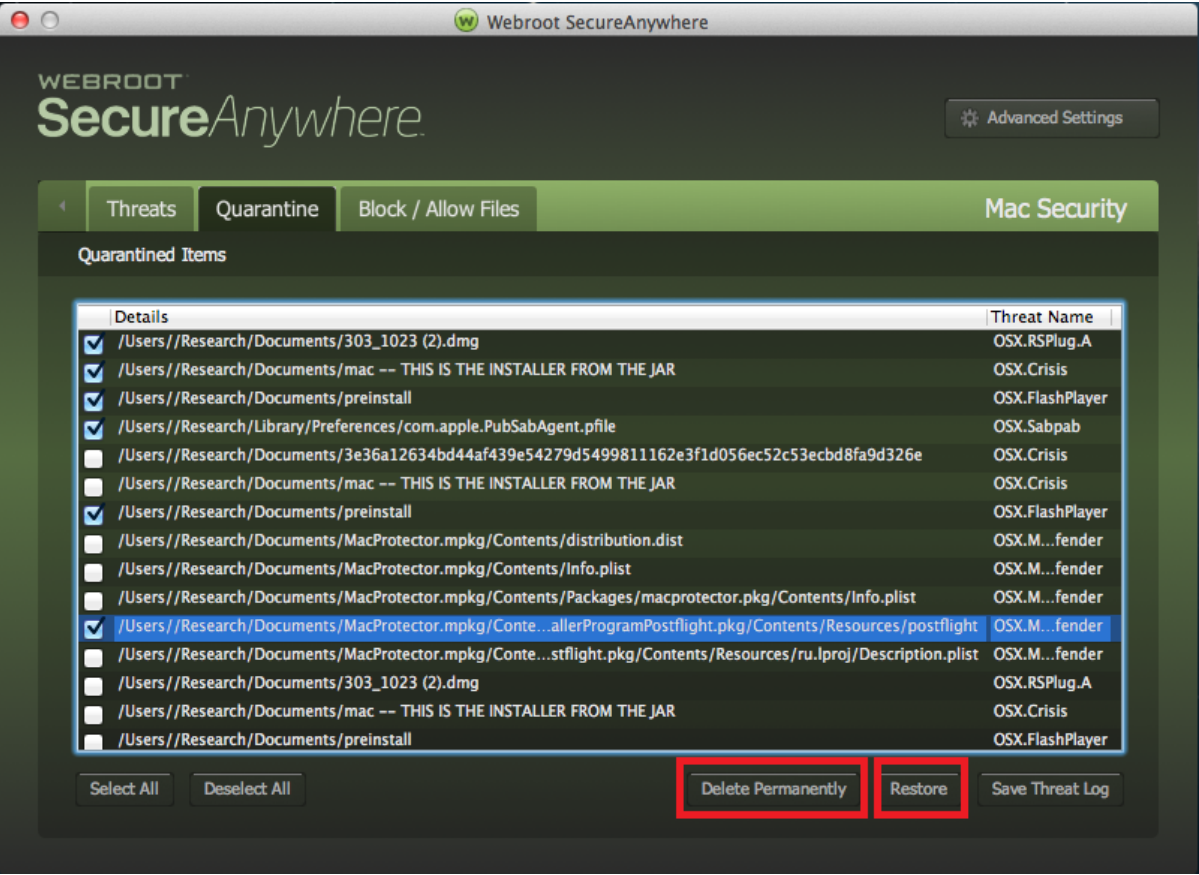
2. Click the **Mac Security** gear icon.



3. In the Mac Security window, click the **Quarantine** tab.



4. To delete or restore files:
 - To remove an item permanently, select the checkbox next to its pathname and click the **Delete Permanently** button. Keep in mind that permanently deleted files can never be restored.
 - To move the item back to its original location, select the checkbox next to its pathname and click the **Restore** button. When an item is restored, SecureAnywhere will no longer detect it during scans. If you want the item to be detected again in the future, you can change its detection rules. For more information, see [Managing File Detection on page 65](#).



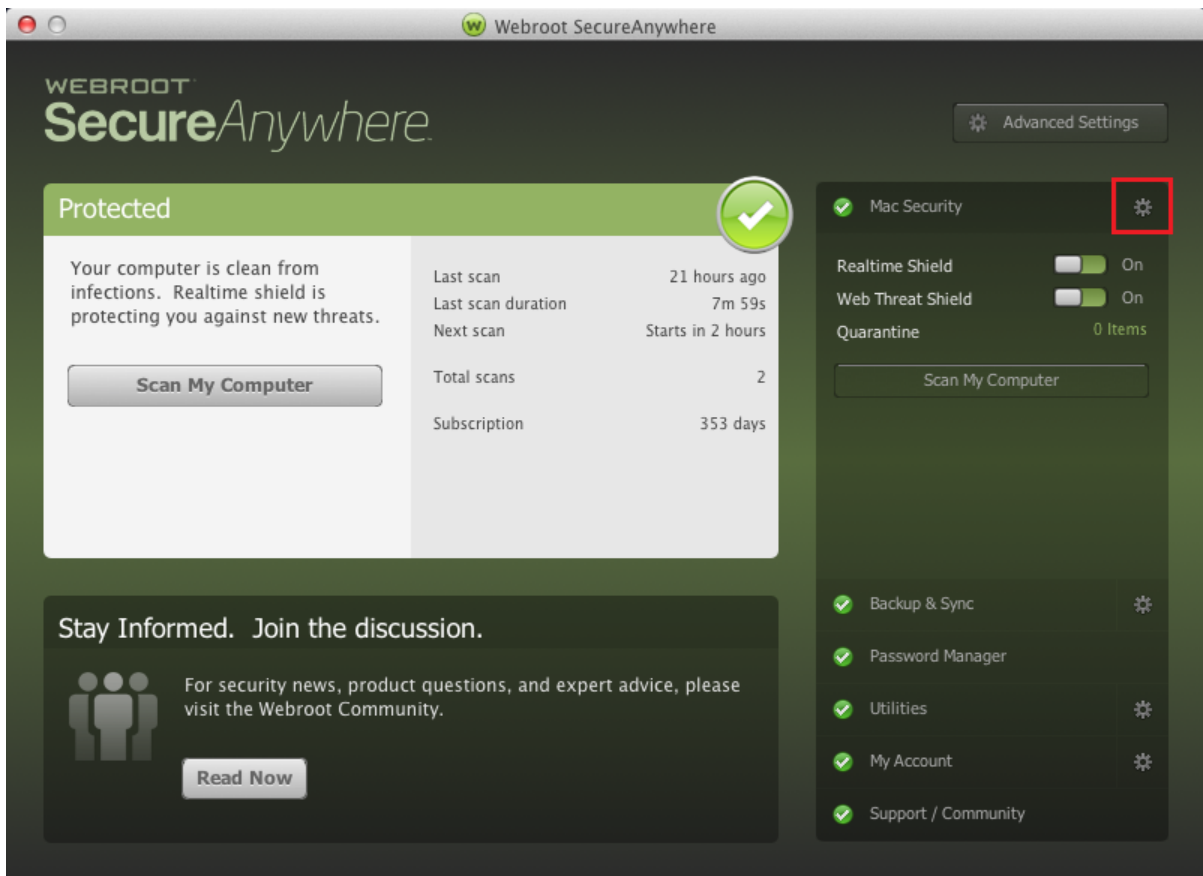
Managing File Detection

If you want more control over scans and shielding behavior, you can use Detection Configuration to specify one of the following actions:

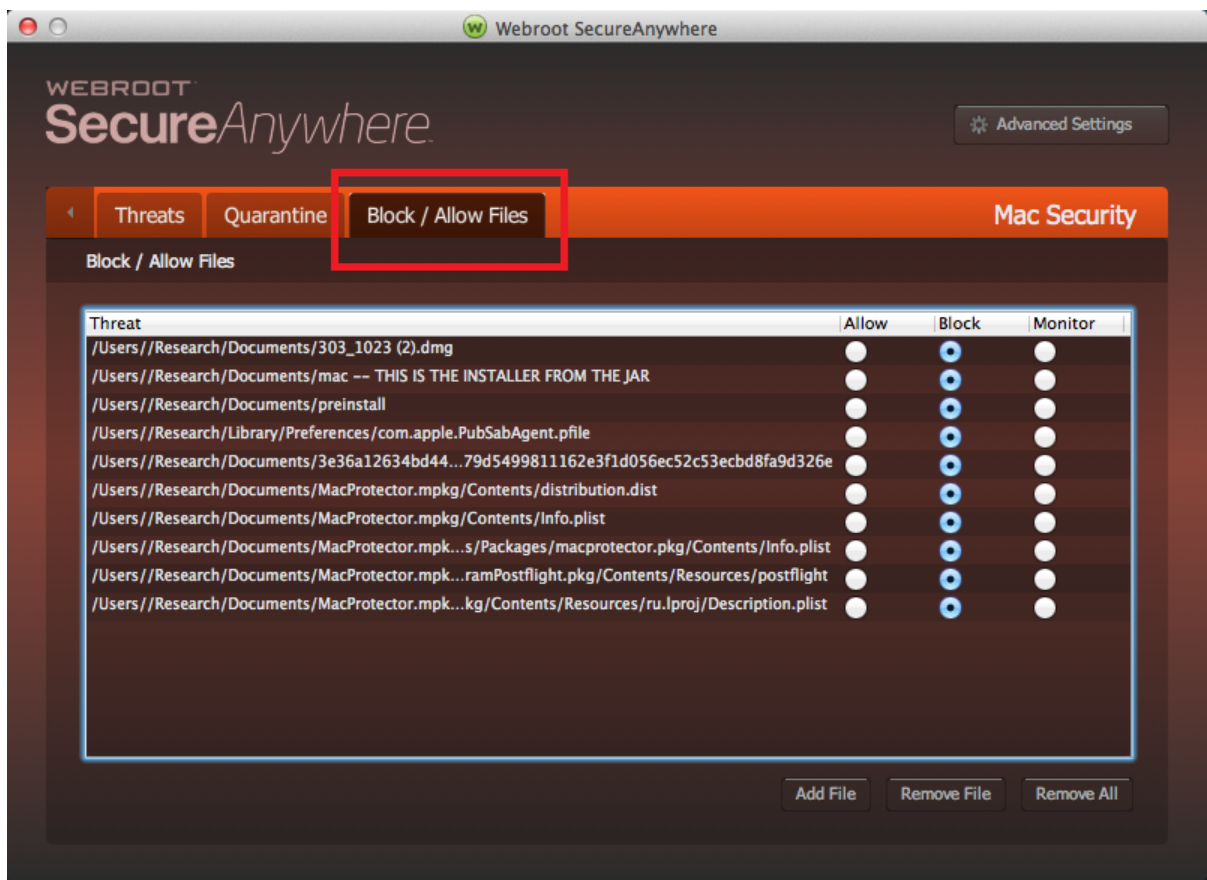
- **Allow** — Ignore a file during scans and shielding.
- **Block** — Stop a file from executing or being written to your Mac.
- **Monitor** — Watch the program to determine if it is legitimate or related to malware.

To manage file detection:

1. Open the SecureAnywhere interface by clicking the **Webroot** icon.
2. From the drop-down menu, select **Open Webroot SecureAnywhere**.
3. From the main window, click **Mac Security** gear icon.



4. From the Mac Security window, click the **Block/Allow Files** tab.



This list includes files you may have allowed. You can also add files to this list. You can change the configuration for files already listed in this panel, or you can include other files by clicking the **Add File** button.

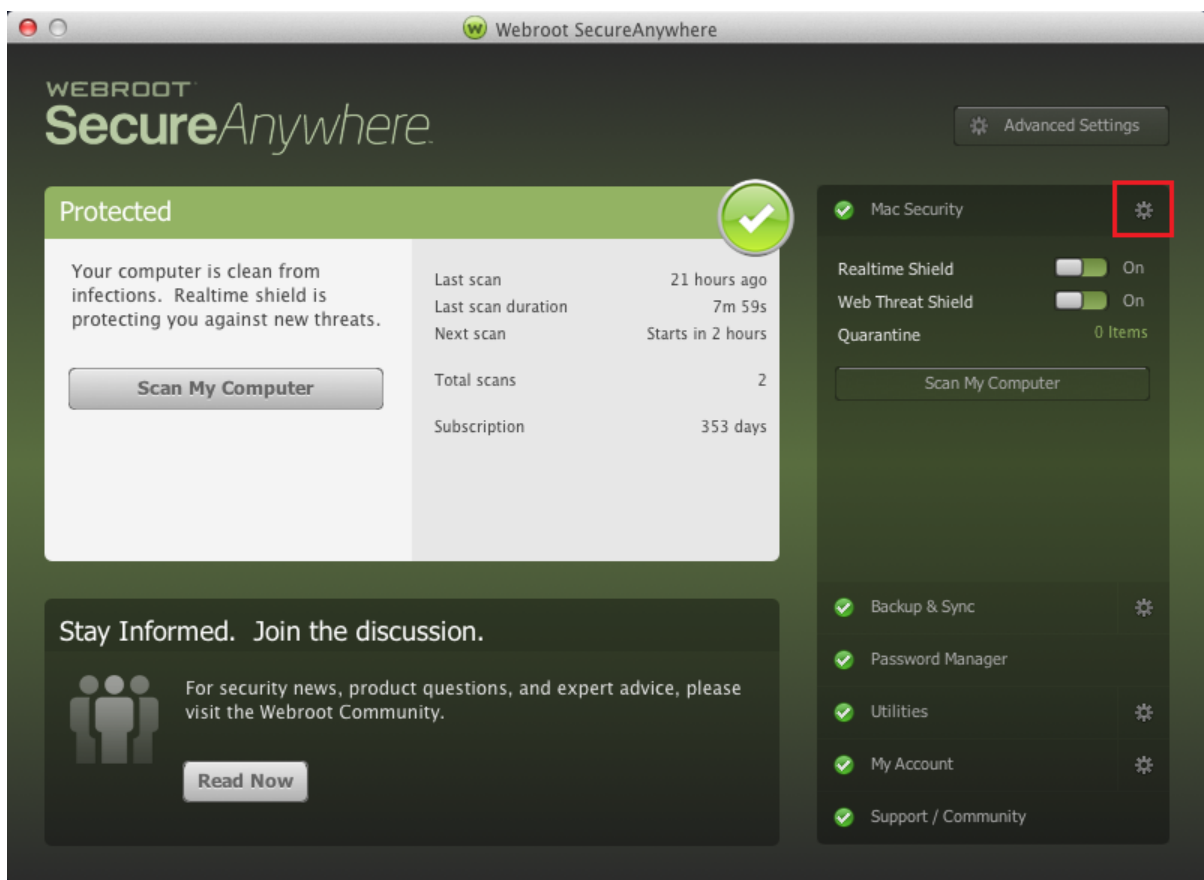
5. In the right column, select the radio button for either **Allow**, **Block**, or **Monitor**.
6. To clear an item from the list, click either the **Remove File** or **Remove All** button.

Saving Threat Logs

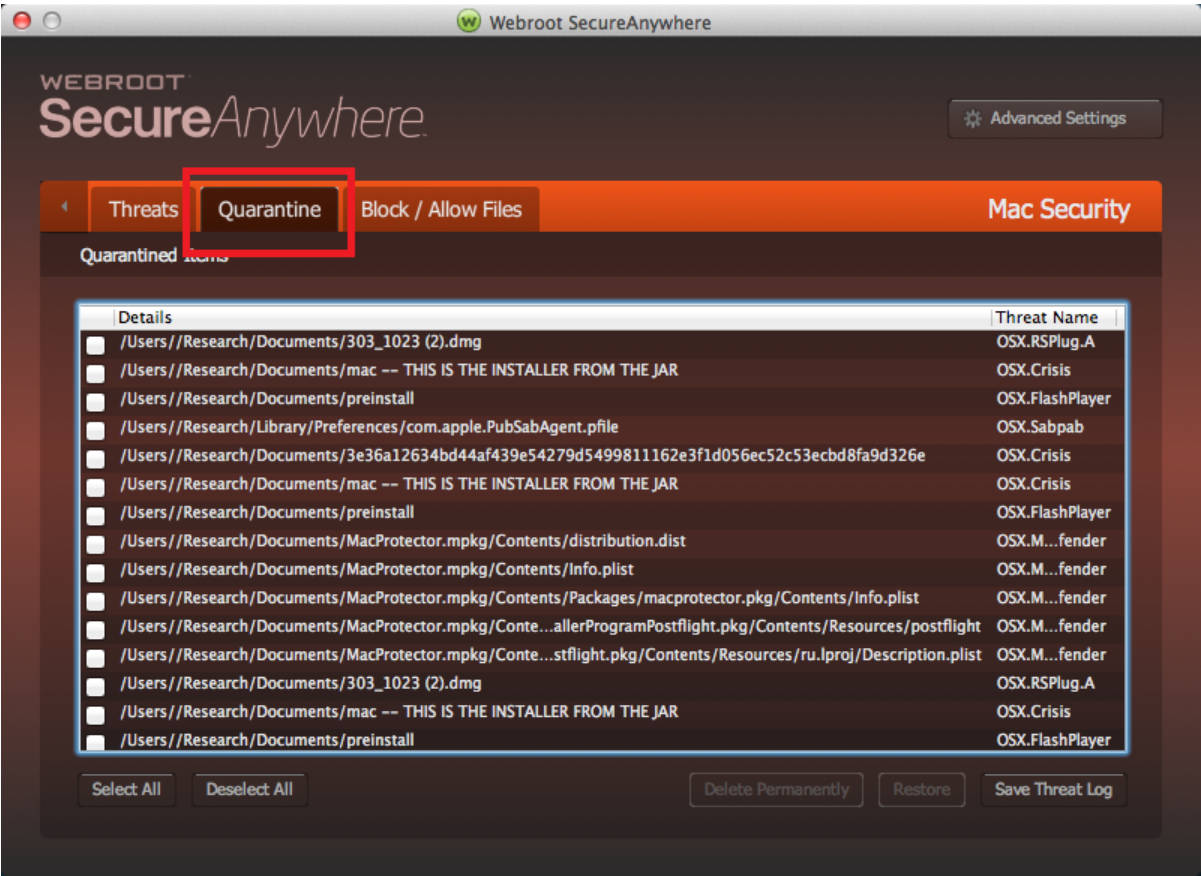
If you want to investigate an infection with Webroot Support, you can save a threat log and send it to Webroot. The threat log lists details about threats removed from your Mac.

To save a threat log:

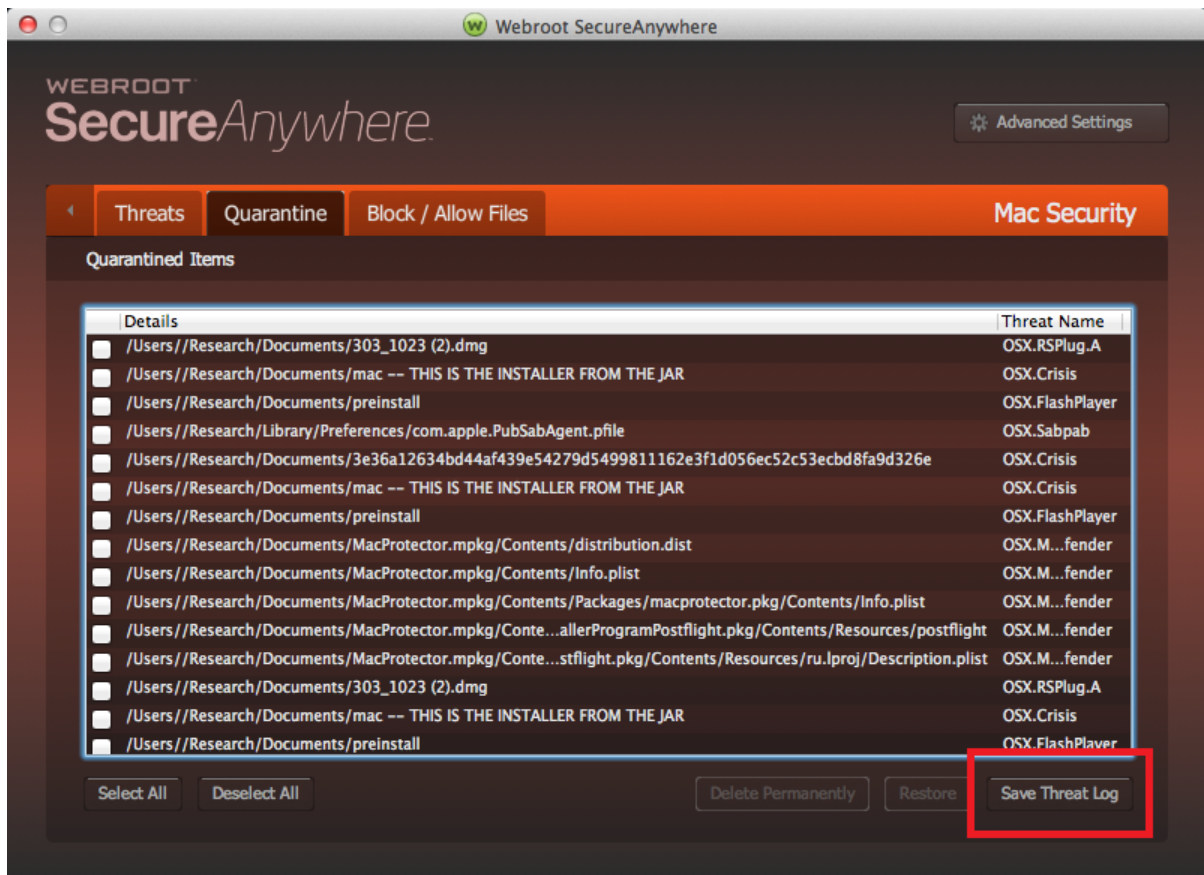
1. Open the SecureAnywhere interface by clicking the **Webroot** icon.
2. From the drop-down menu, select **Open Webroot SecureAnywhere**.
3. From the main window, click the **Mac Security** gear icon.



4. From the Mac Security panel, click the **Quarantine** tab.



5. In the bottom left, click **Save Threat Log**.



6. Select a folder location for the threat log and click **Save**.

Chapter 6: Managing Your Account

To manage your account, see the following topics:

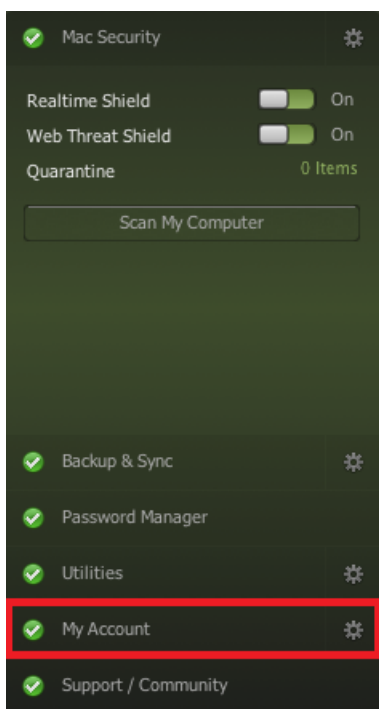
Viewing Your Account Details	72
Activating Keycodes	73
Renewing Subscriptions	75
Checking for Updates	77

Viewing Your Account Details

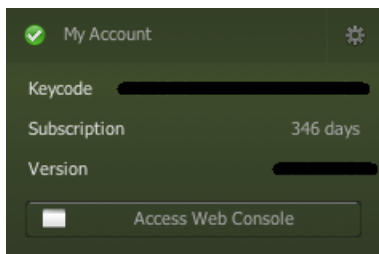
You can view your keycode and the time remaining on your subscription from the My Account window.

To view account details:

1. Open the SecureAnywhere interface.
2. From the drop-down menu, select **Open Webroot SecureAnywhere**.
3. From the main window, click **My Account**.



Your account details display.

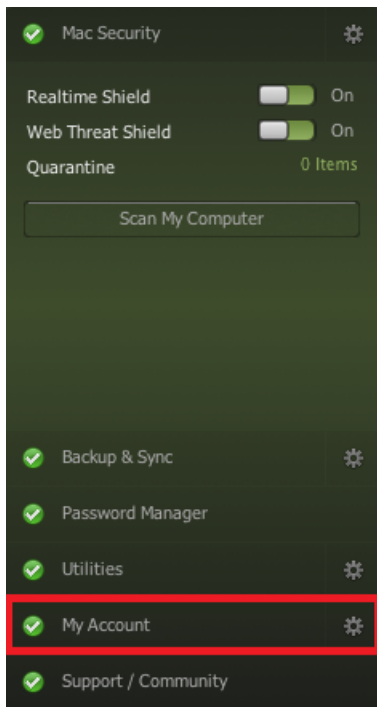


Activating Keycodes

If you receive a new keycode from Webroot, you can activate it from the My Account window.

To activate a new keycode:

1. Open the SecureAnywhere interface.
2. From the drop-down menu, select **Open Webroot SecureAnywhere**.
3. From the main window, click **My Account**.



4. In the My Account window, click the **My Account** gear icon.



5. Enter your new keycode in the Enter your keycode to activate your software field and click **Activate**.

Keycode

About SecureAnywhere

My Account

My Subscription

Keycode

Product

Status

Subscription

SecureAnywhere Complete

Active

351 days

Upgrade / renew

Copy keycode to clipboard

Activate a New Keycode

Enter a new keycode in the field below and click "Activate"

Enter your keycode to activate your software

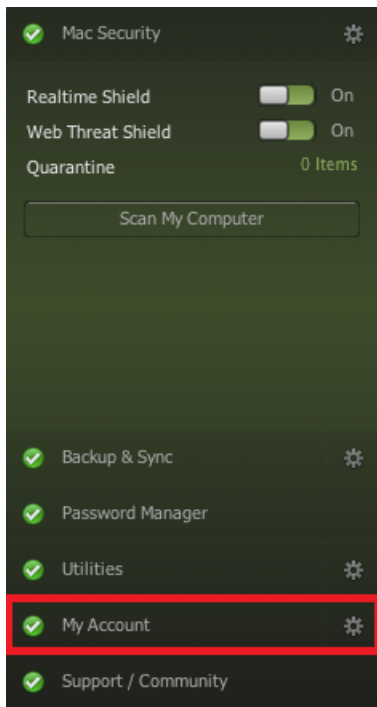
Activate

Renewing Subscriptions

You can renew your subscription from the My Account window.

To renew SecureAnywhere:

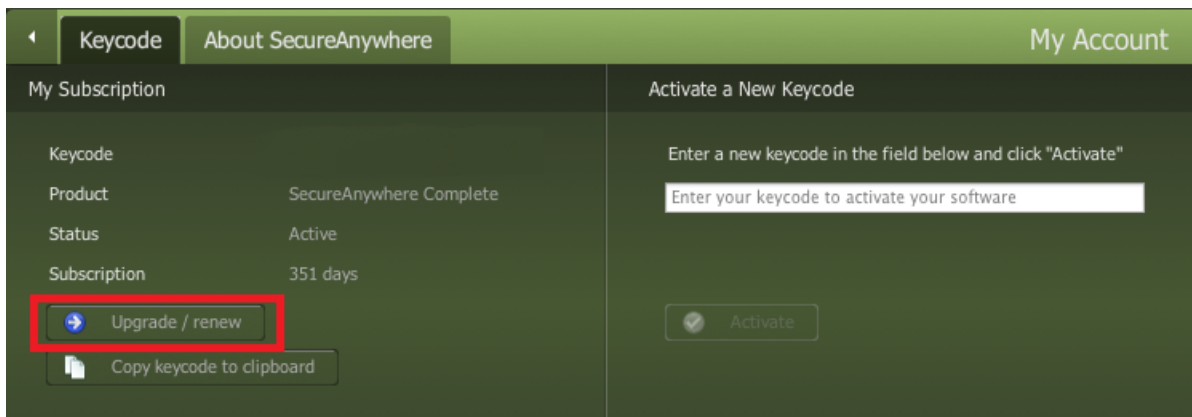
1. Open the SecureAnywhere interface
2. From the drop-down menu, select **Open Webroot SecureAnywhere**.
3. From the main window, click **My Account**.



4. Click the **My Account** gear icon.



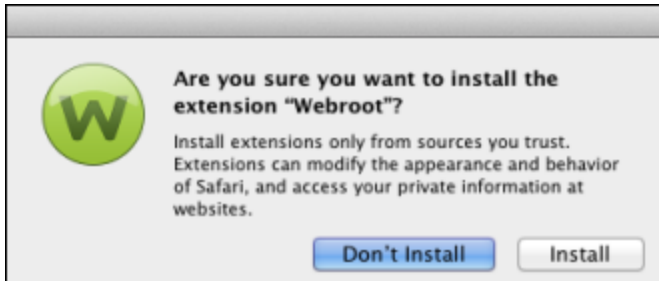
5. Click **Upgrade/Renew**.



[The Webroot website opens](#). From here, you can purchase an upgrade to your software.

Checking for Updates

SecureAnywhere automatically sends program updates to your Mac, provided it is connected to the Internet and you did not deactivate the Automatically download and apply updates setting in General Preferences. When an update occurs, a message opens briefly in a dialog box at the top right of the screen. You may also see a message from Safari asking you to allow these updates for the toolbar extensions. If you see this message, click **Install** to continue.

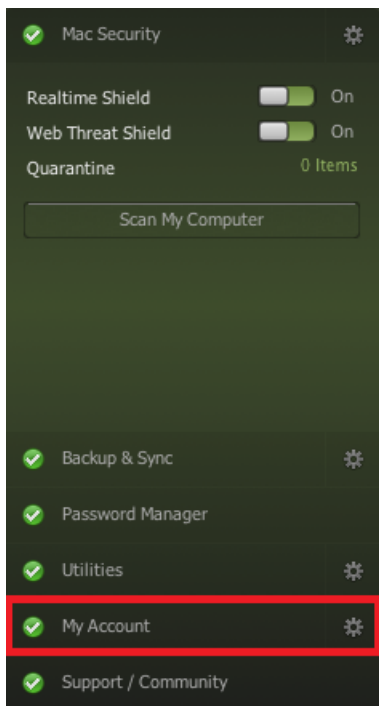


To disable automatic updates, you can manually check for updates whenever it is convenient. For more information, see [Setting General Preferences on page 164](#).

To check for SecureAnywhere updates:

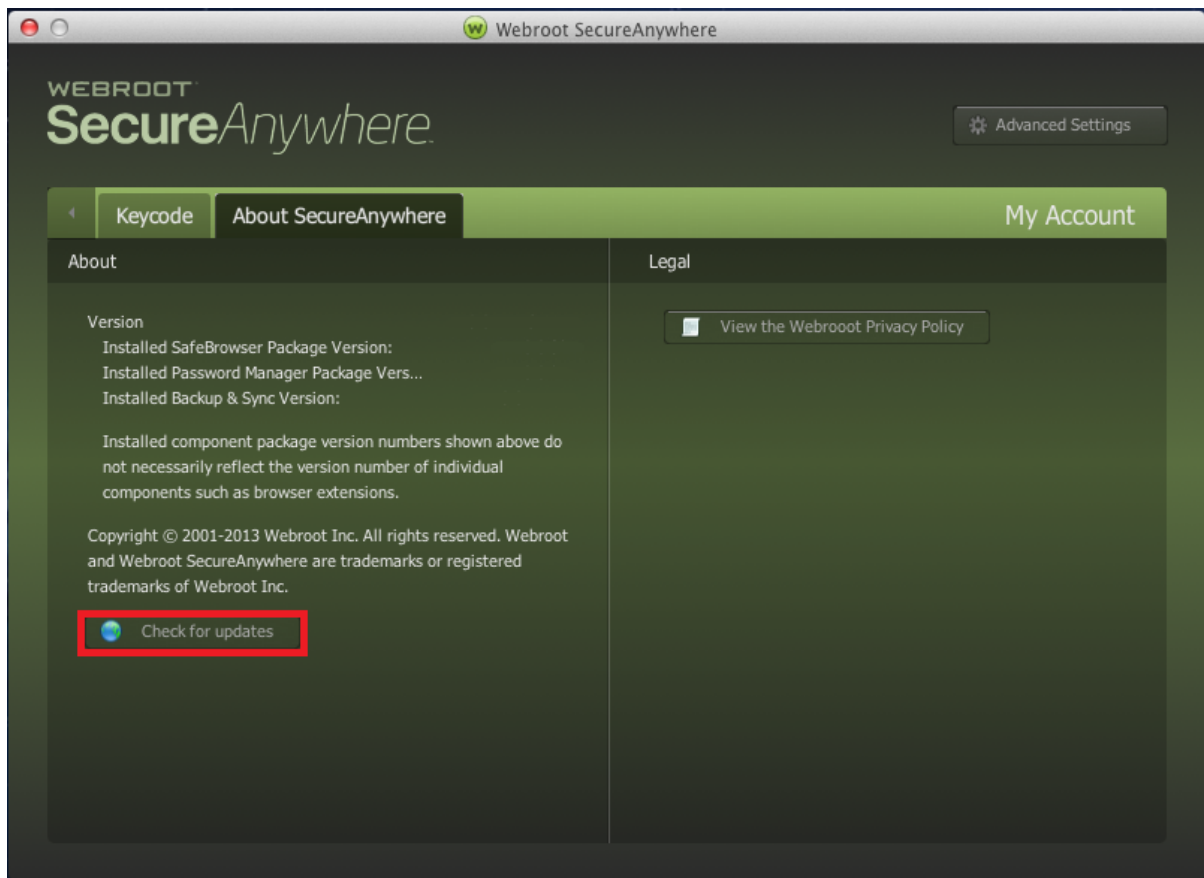
1. Open the SecureAnywhere interface.
2. From the drop-down menu, select **Open Webroot SecureAnywhere**.

3. From the main window, click **My Account**.



4. Click the **My Account** gear icon.
5. Click the **About SecureAnywhere** tab.

6. Click **Check for updates**.



If a newer version of SecureAnywhere is available, Webroot downloads and applies the update.

Chapter 7: Managing Backup And Sync

To manage Backup & Sync, see the following topics:

Backup & Sync Overview	82
Storing Files in the Anywhere Folder or in Your Own Sync Folders	82
Backing Up Files	82
Downloading Backup & Sync	83
Adding Sync Folders	85
Backing Up Files	88
Changing Backup & Sync Settings	92
Changing Backup Filters	95
Changing Backup Schedules	98
Checking File Backup & Sync Statuses	100
Synchronizing Files	104
Synchronizing Folders Between Computers	107
Removing Folders From Synchronization	110

Backup & Sync Overview

If your SecureAnywhere edition includes Backup & Sync, you can protect your important files and photos.

Storing Files in the Anywhere Folder or in Your Own Sync Folders

You can use Webroot's preconfigured folder called the Anywhere folder or you can create your own sync folders. Any files you place in these folders are automatically synchronized in your account, to any other computers with shared folders, and to mobile devices with the Backup & Sync app installed.

SecureAnywhere constantly monitors the Anywhere folder and other sync folders. If it detects a change, such as an edited file, a new file, or a deleted file, it immediately makes the same change to your online account, to shared folders on other computers, and to mobile devices with the Backup & Sync app installed. If you are working offline, SecureAnywhere automatically picks up changes the next time you connect to the Internet.

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

To learn more about the preconfigured Anywhere folder, see [Synchronizing Files on page 104](#).

To create sync folders of your own, see [Adding Sync Folders on page 85](#).

Backing Up Files

Instead of synchronizing files with multiple devices, you can simply back them up. For example, you may want to back up tax returns, old photos, and a scanned copy of your passport. These types of documents won't change and don't need to be kept in synchronization with other computers.

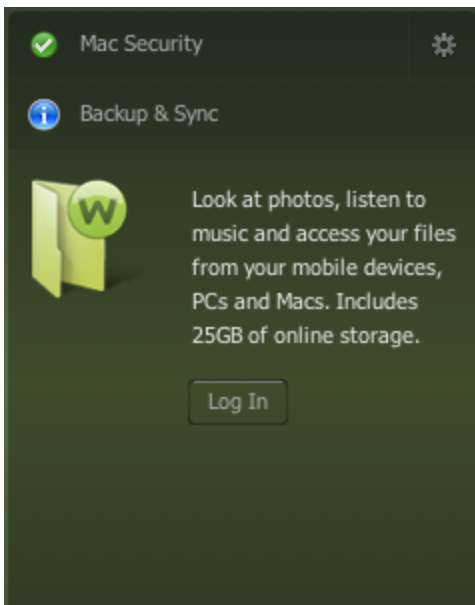
To learn more about backups, see [Backing Up Files on page 88](#).

Downloading Backup & Sync

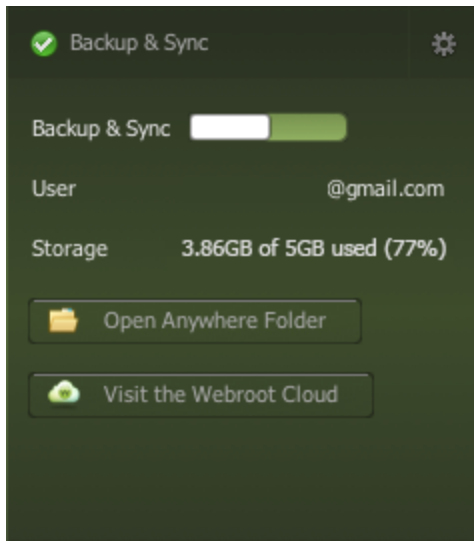
To begin using Backup & Sync, you must download its component to your computer.

To download the component:

1. If you have not yet created a Webroot account, see [Creating Webroot Accounts on page 20](#).
2. Open SecureAnywhere; for more information, see [About the SecureAnywhere Interface on page 16](#).
3. Click the **Backup & Sync** tab, then click the **Log in** button.



4. If prompted, enter your Webroot account credentials, that is, your user name and password. When the download completes, the Backup & Sync panel looks like the example below.



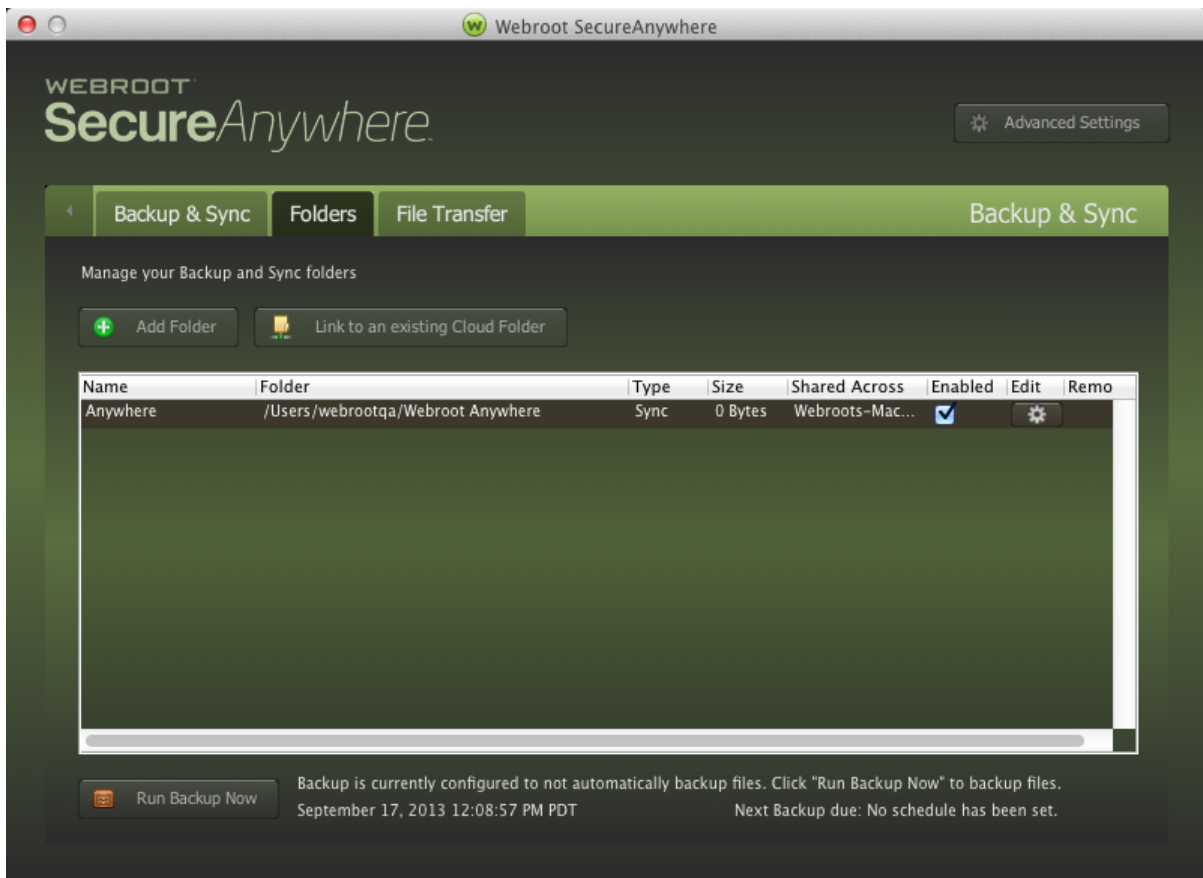
- By default, once logged in the Backup and Sync setting is turned on.
 - For more information on synchronizing folders across devices, see [Synchronizing Files on page 104](#). Only the Anywhere folder, which is created on install of the Backup and Sync component, is set to Sync by default.
 - To configure which files you would like to backup, see [Backing Up Files on page 88](#). No files are selected to be backed up by default.
-

Adding Sync Folders

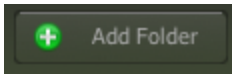
Webroot already configured one synchronization folder called the Anywhere folder. However, you can designate more folders for synchronization, as needed. For more information, see [Synchronizing Files on page 104](#).

To add a sync folder:

1. Open SecureAnywhere. For more information, see [About the SecureAnywhere Interface on page 16](#).
2. Click the **Backup & Sync** tab.
3. Click the **Backup & Sync** gear icon.
4. Click the **Folders** tab.

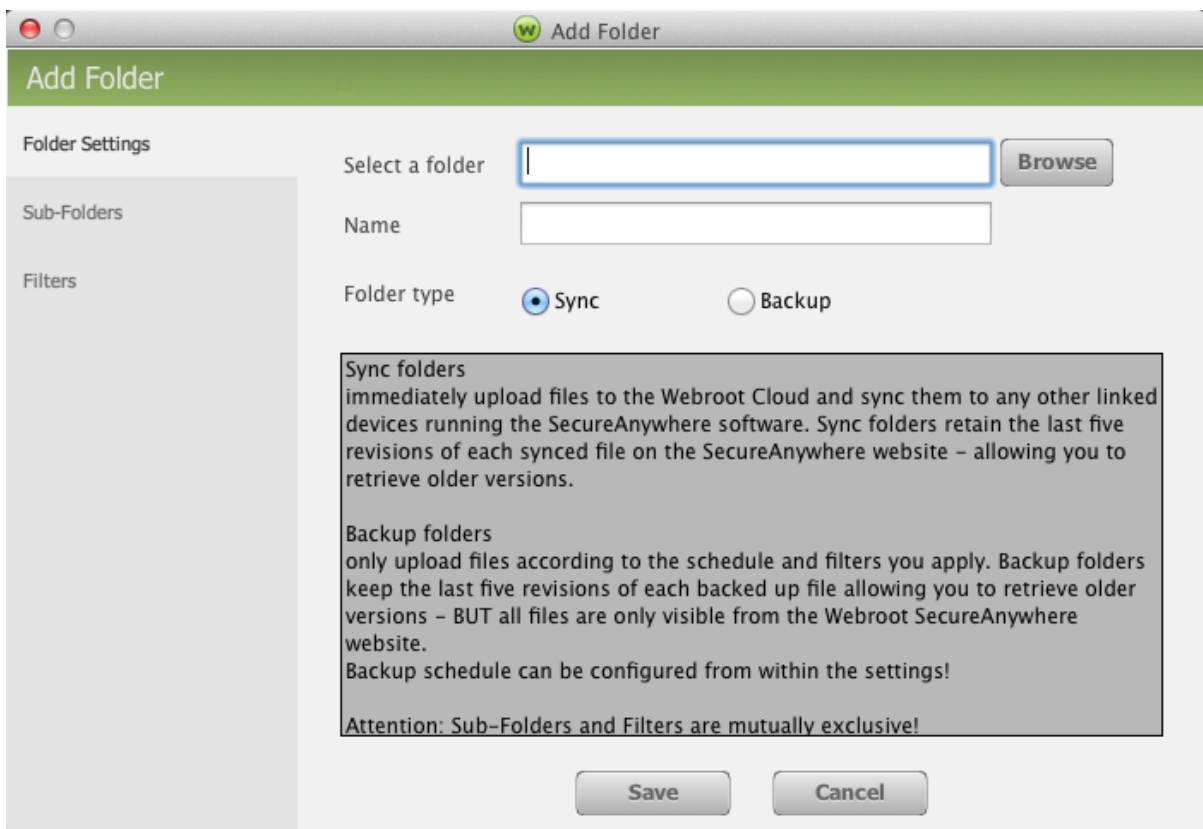


5. Click the **Add Folder** button.

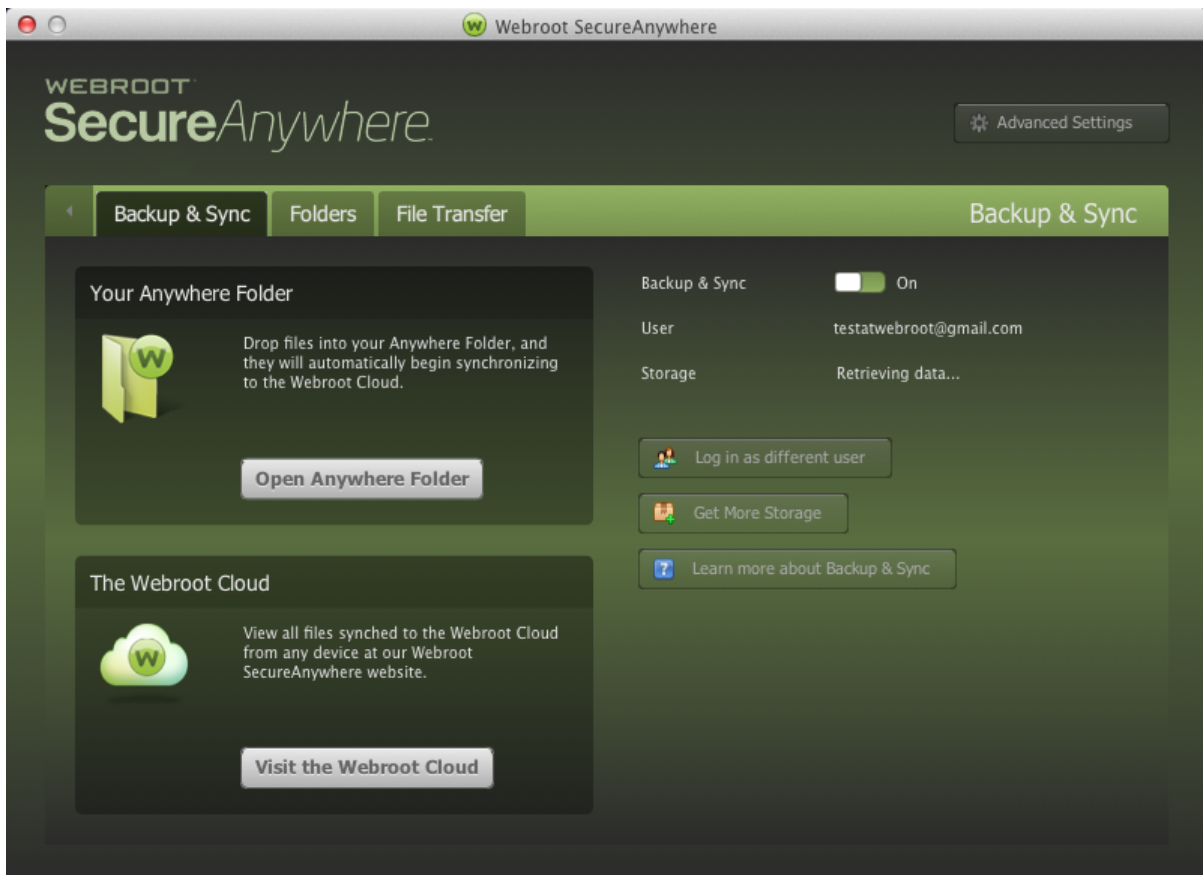


6. In the next panel, click the **Browse** button to open the folder you want synchronized.
7. If needed, you can specify a different name for this folder that will display in SecureAnywhere. For syncing a folder, for each folder type, you must select the **Sync** radio button.
8. Click **Sub-Folders** to sync sub-folders within the synced folder.
9. When you're done, click **Add**.

Note: To share a folder across multiple computers, see [Synchronizing Folders Between Computers on page 107](#).



10. To check that your files successfully uploaded to your account, click the **Backup & Sync** tab, then click **Visit the Webroot Cloud**.



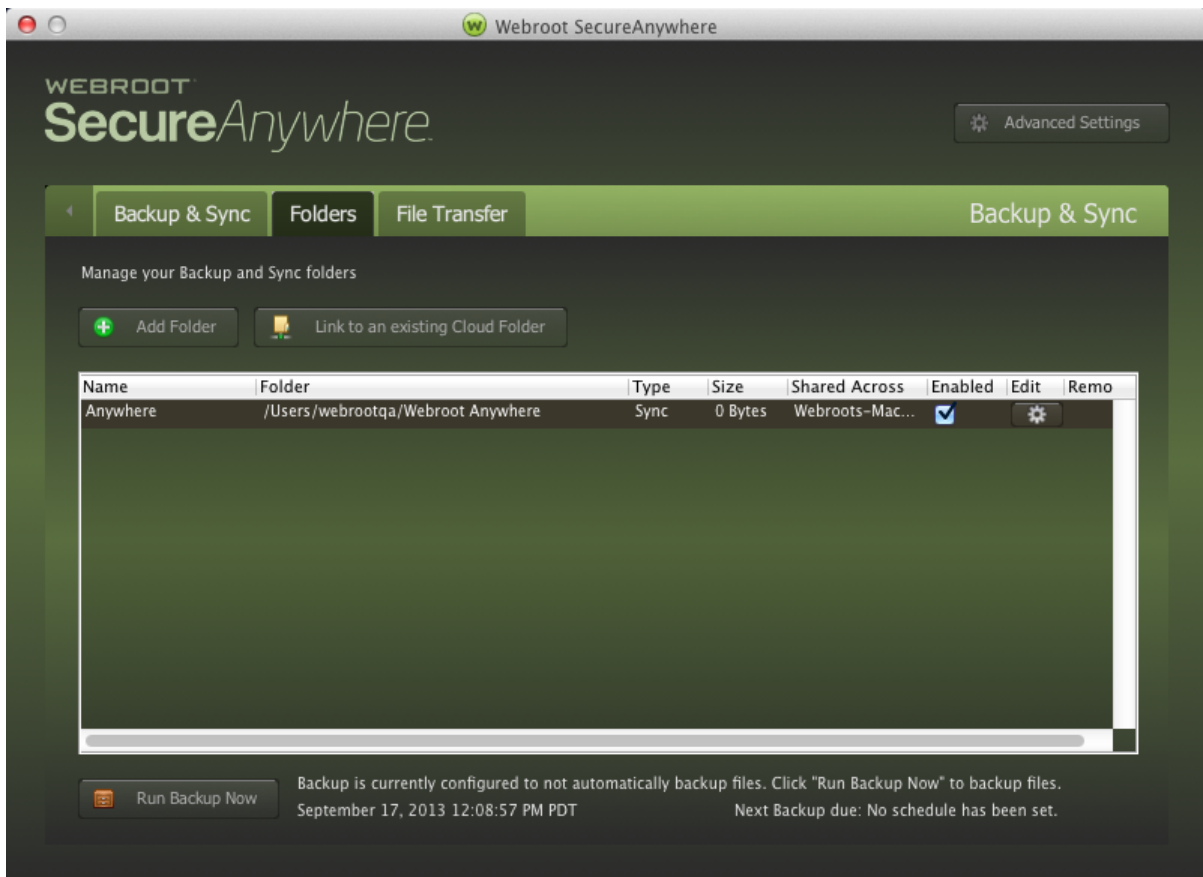
11. When your browser opens to my.webrootanywhere.com, log in to your account, click **Go to Backup & Sync**, then click on the folder name from the left panel.

Backing Up Files

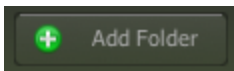
Instead of synchronizing files, you can archive them instead. For example, you may want to back up tax returns, old photos, and a scanned copy of your passport. These types of documents won't change and don't need to be kept in synchronization with other computers. Your backed-up files are uploaded to the Webroot servers, which are accessible from your SecureAnywhere account.

To configure backup:

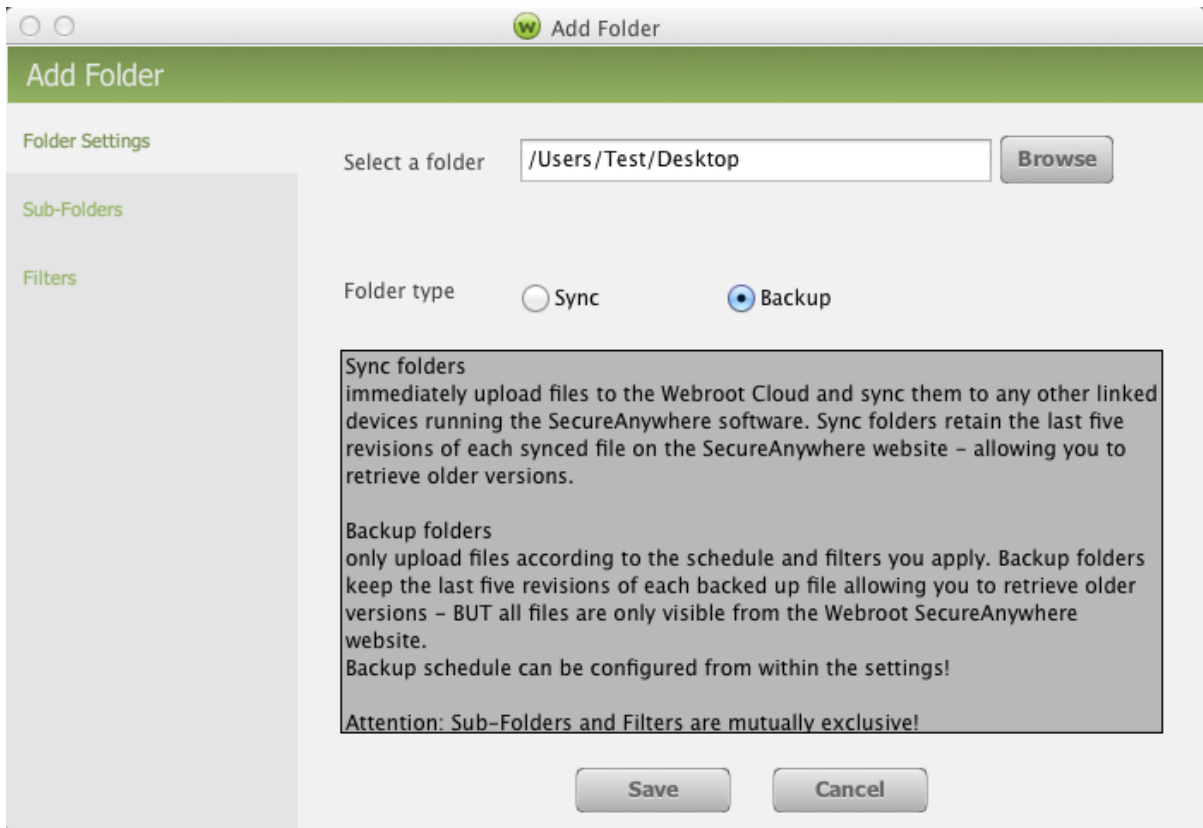
1. Open **SecureAnywhere**. For more information, see [About the SecureAnywhere Interface on page 16](#).
2. Click the **Backup & Sync** tab.
3. Click the **Backup & Sync** gear icon, then click the **Folders** tab.



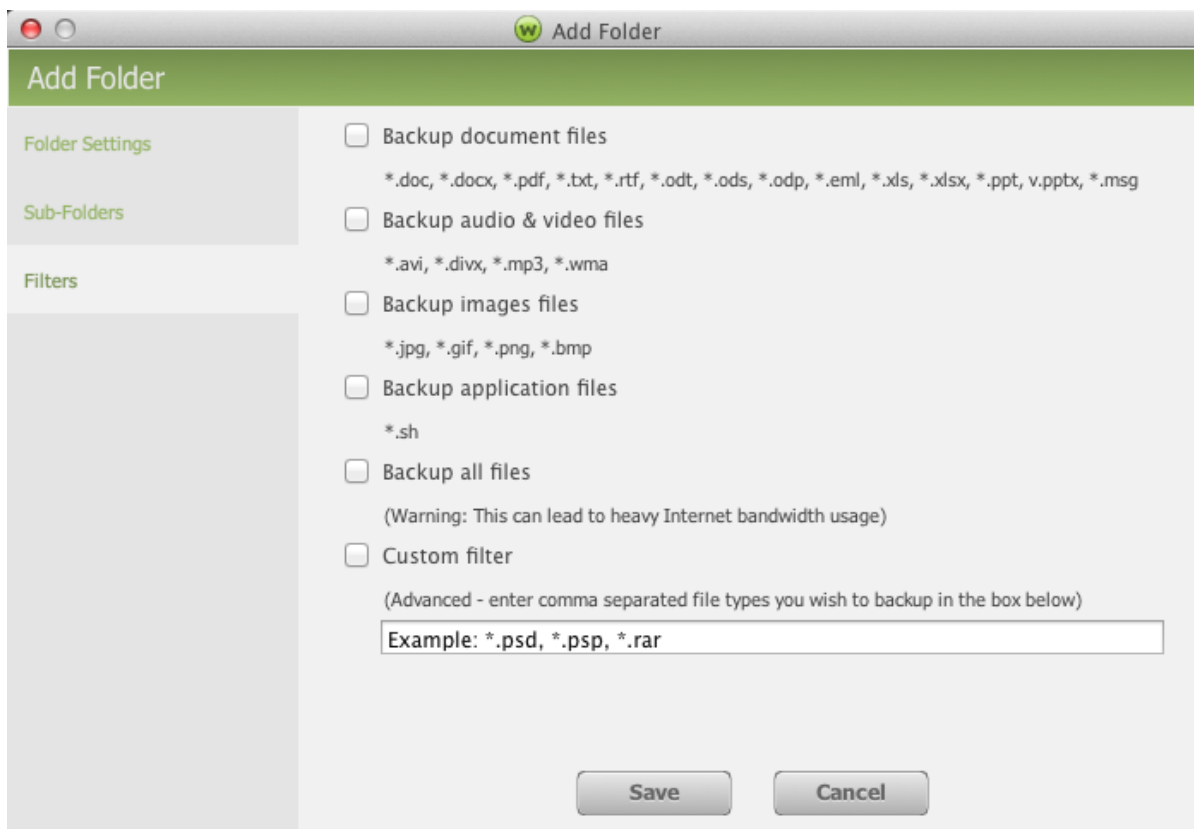
4. Click the **Add Folder** button.



5. In the next panel, click the **Browse** button to open the folder which contains the files you want to backup. You cannot create a name for backup folders. For backing up a folder, select the **Backup** radio button for that folder.

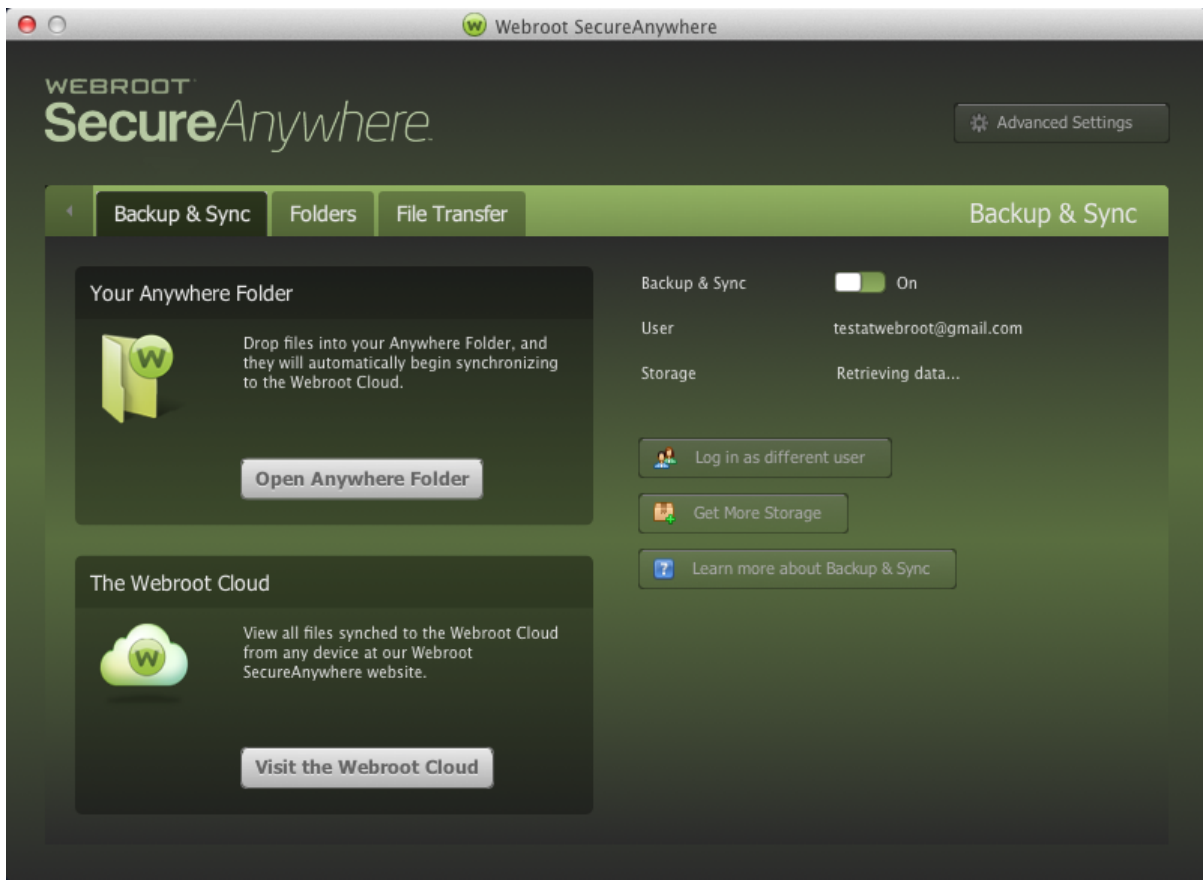


6. Click **Filters** to select specific file types to be backed up.



7. When you're done, click **Save**.
8. To check that your files successfully uploaded to your account, click the **Backup & Sync** tab, then click

Visit the Webroot Cloud.



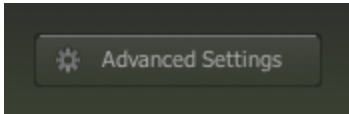
9. When your browser opens to my.webrootanywhere.com, log in to your account, click **Go to Backup & Sync**, then click on the folder name from the left panel.

Changing Backup & Sync Settings

Webroot already configured backup and synchronization with our recommended settings, but you can adjust the settings if you want. For example, you can adjust the size limit of files to upload, or allow a backup or synchronization to run while your computer is on battery power.

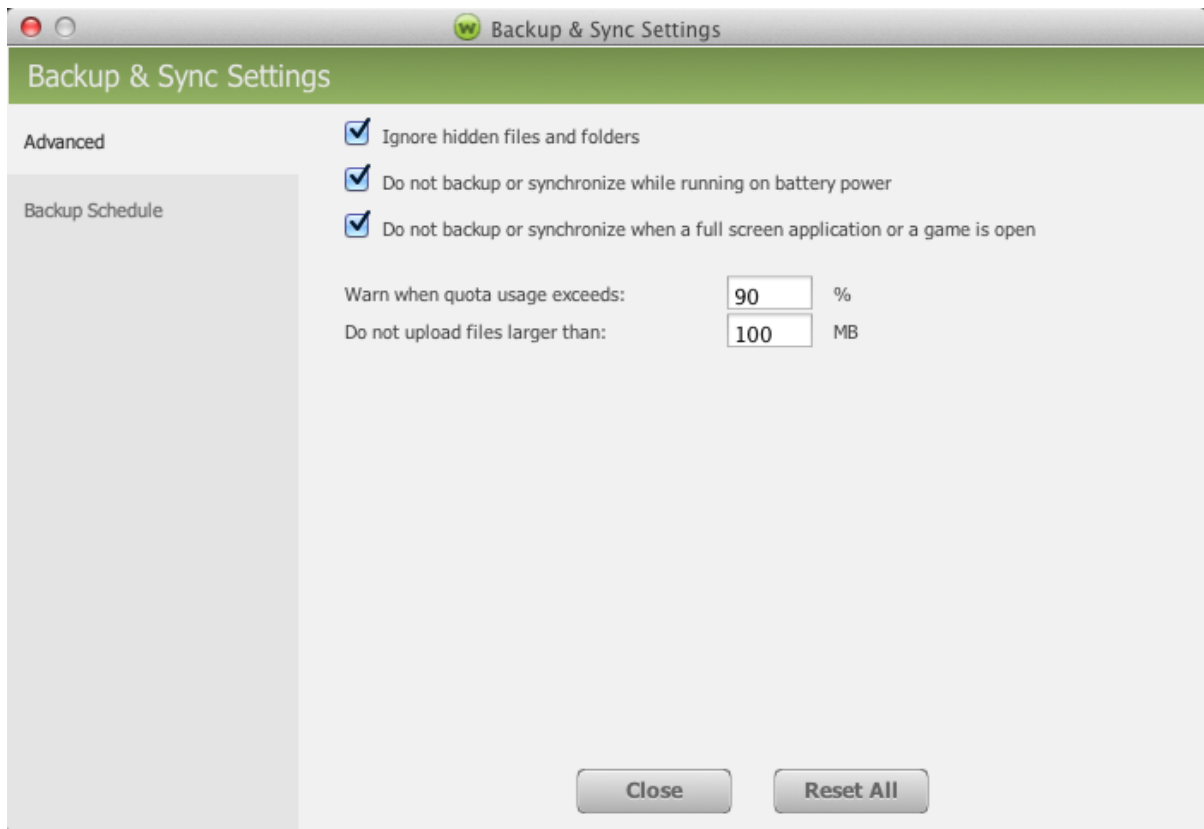
To change backup and sync settings:

1. Open **SecureAnywhere**.
2. Click the **Backup & Sync** tab.
3. Click the **Backup & Sync** gear icon.
4. Click the **Advanced Settings** button.



The Backup & Sync panel displays.

5. To change a setting, do either of the following:
 - To enable the setting, select the checkbox.
 - To disable the setting, deselect the checkbox.



Note: This can only be accessed if you click the Backup & Sync gear icon first. If you click the Advanced Settings button on the home screen, it will only take you to the advanced settings for the antivirus.

FIELD	DESCRIPTION
Ignore hidden files and directories	When selected, files and directories that Windows has hidden in Explorer are not included in the sync. "Hidden" files are typically system files that do not need to be synchronized. They can also consume a lot of storage space.
Do not backup or synchronize files while running on battery power	When selected, SecureAnywhere does not run a synchronization when your computer is unplugged and running on the battery.
Do not back or synchronize files when a full-screen application or game is running	When selected, SecureAnywhere does not run a synchronization when you are watching a movie in full-screen mode or running a gaming application.
Warn when quota usage exceeds	The number in the field determines when SecureAnywhere displays a warning when your storage limit is exceeded. You can adjust the percentage by entering a new number.
Do not upload files larger than	The number in the field determines the size of files to include in synchronization. If the file size exceeds the displayed limit, it will not be uploaded. You can adjust the size limit by entering a new number in megabytes.

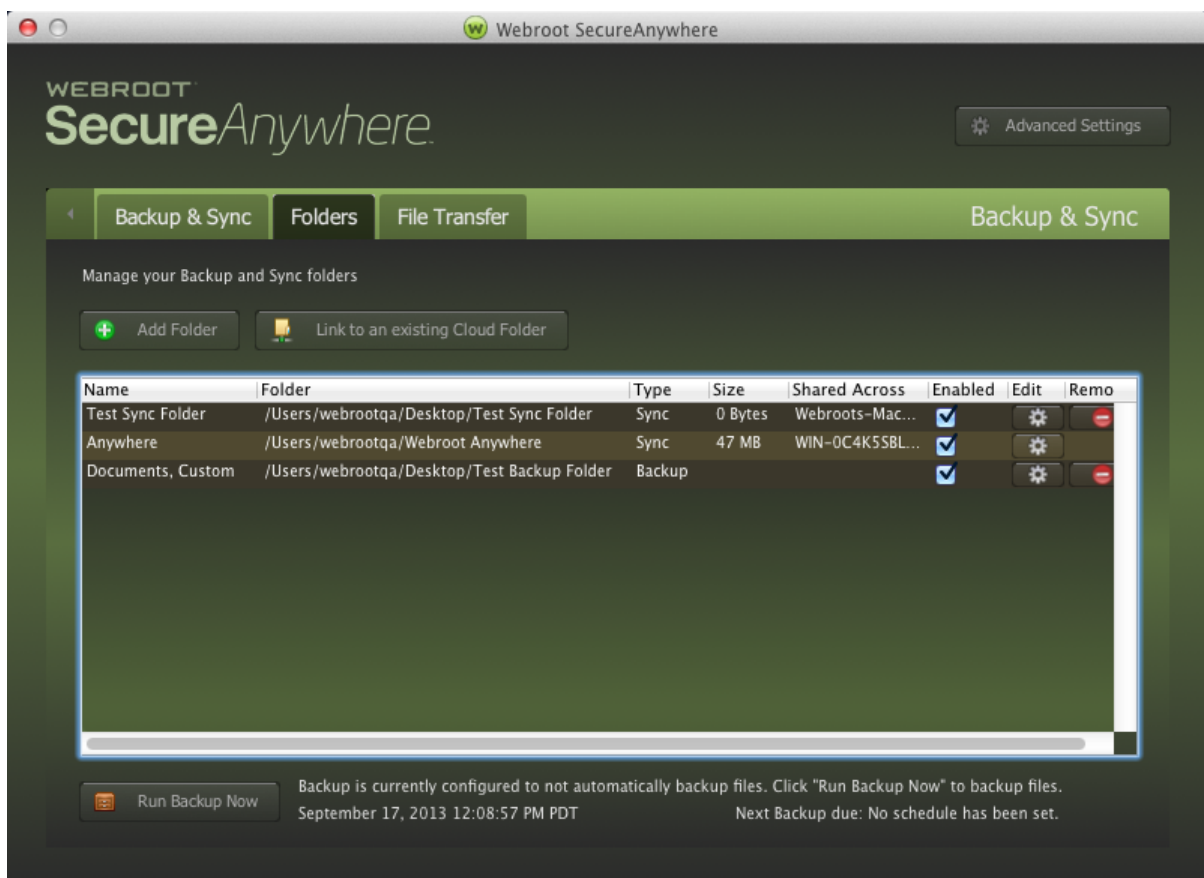
Note: We recommend that you keep Webroot's default settings. If you make changes and decide you want to return to the recommended settings, click the **Reset to Defaults** button.

Changing Backup Filters

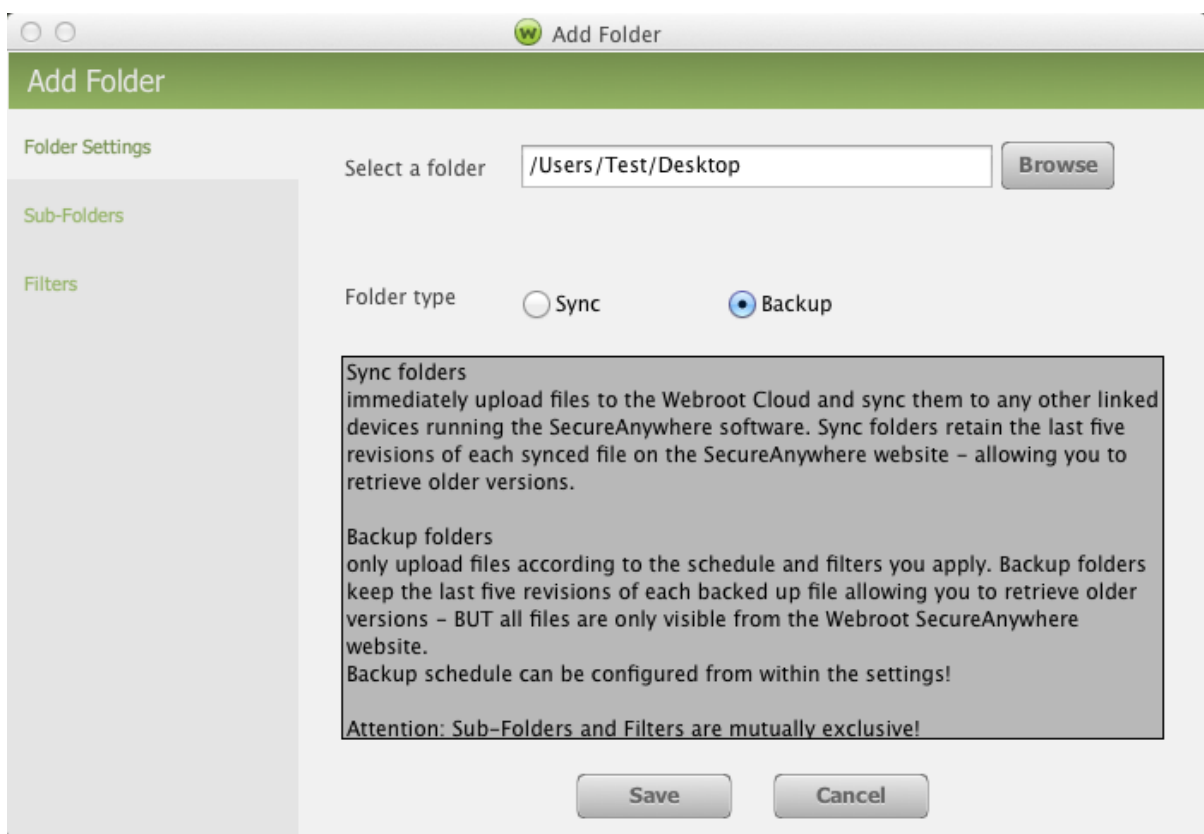
Using backup filters, you can include or exclude certain file types or subfolders for the backup.

To add or change the backup filters:

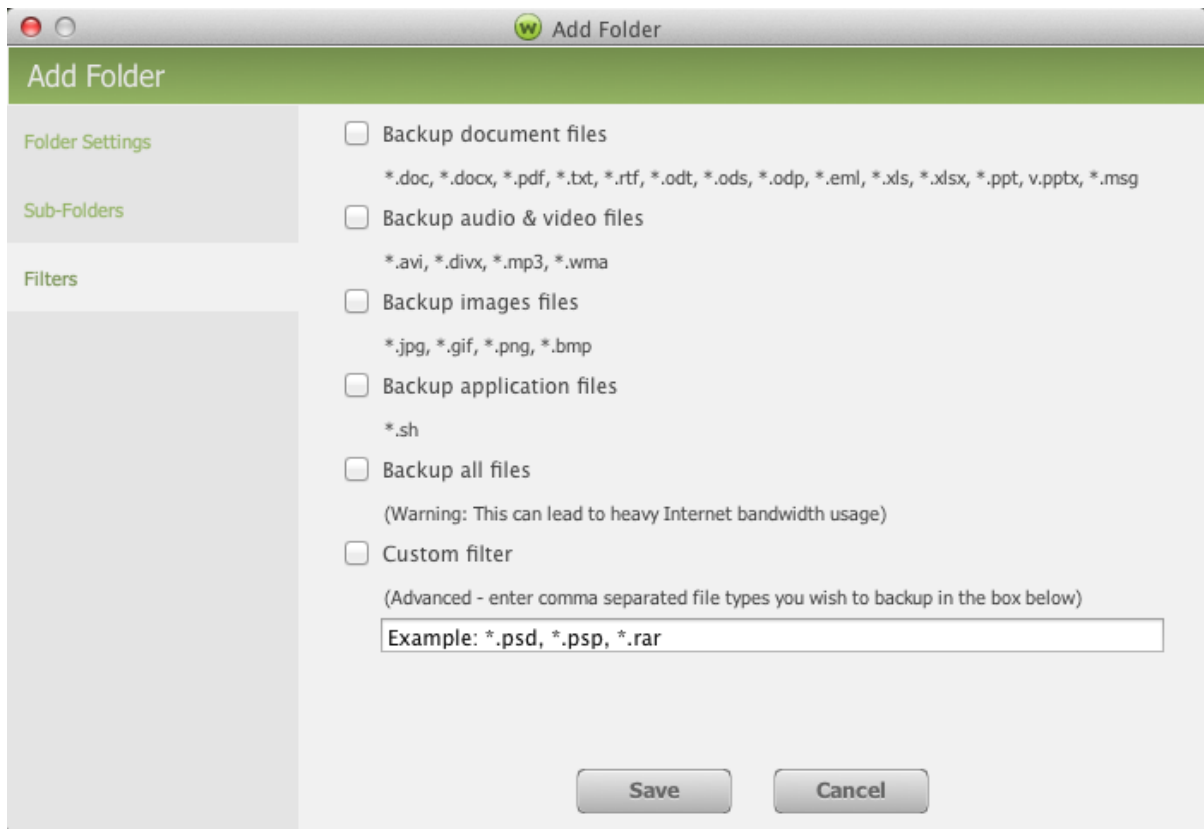
1. Open SecureAnywhere. For more information, see [About the SecureAnywhere Interface on page 16](#).
2. Click the **Backup & Sync** tab.
3. Click **Backup & Sync** gear icon. Then click the **Folders** tab.



4. Click the gear icon for the Backup folder you want to update. The Add Folder window displays. From here you can change the folder being backed up by clicking **Browse**.



5. In the left column, select **Filters** to change which file types are being backed up for this folder.



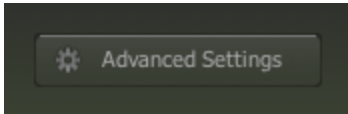
6. When you're done, click the **Save** button.

Changing Backup Schedules

Webroot already configured backup and synchronization with our recommended settings, but you can adjust the settings if you want. For example, you can adjust the size limit of files to upload, or allow a backup or synchronization to run while your computer is on battery power.

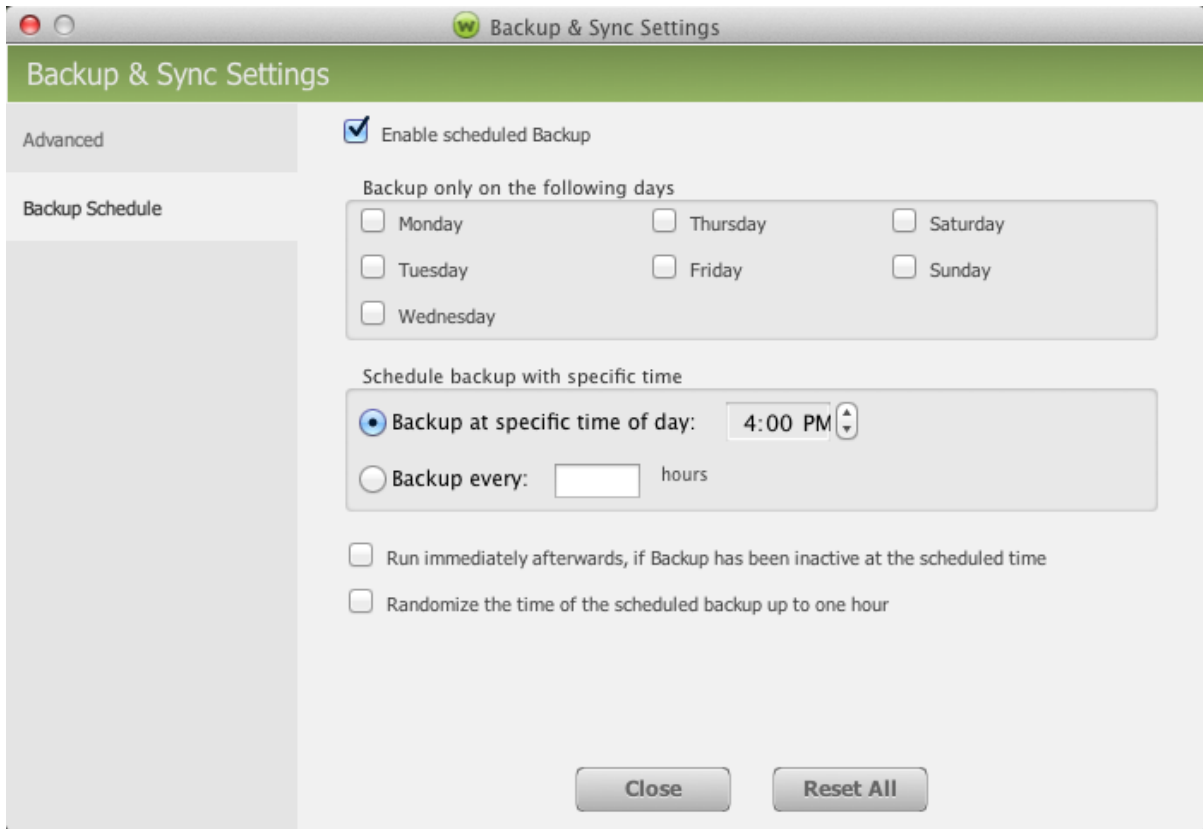
To change backup schedule:

1. Open SecureAnywhere.
2. Click the **Backup & Sync** tab.
3. Click the **Backup & Sync** gear icon.
4. Click the **Advanced Settings** button.



Note: This can only be accessed if you click the Backup & Sync gear icon first. If you click the Advanced Settings button on the home screen, it will only take you to the advanced settings for the antivirus.

5. In the left column, select **Backup Schedule**.



6. To turn off automatic backups, deselect the **Enable scheduled archiving** checkbox. Otherwise, keep it selected.
7. If needed, select the **Back up only on the following days** checkbox and select a day of the week to run the backups.
8. Select the time of day to run the backup or an hourly interval.
9. At the bottom of the panel, you have two additional checkboxes:
- **Run immediately if Backup was inactive at the scheduled time** — Keep this checkbox selected if you want to run a backup immediately after a missed schedule. A backup might be skipped if you disabled backups, if you shut down SecureAnywhere, or if your logged off your computer.
 - **Randomize the time of a scheduled archive up to one hour** — Keep this checkbox selected if you want a scheduled backup to run within an hour of the scheduled time. This selection makes better use of network resources.

Checking File Backup & Sync Statuses

You can check the status of synchronization and backup from the main interface or from your account on the SecureAnywhere website.

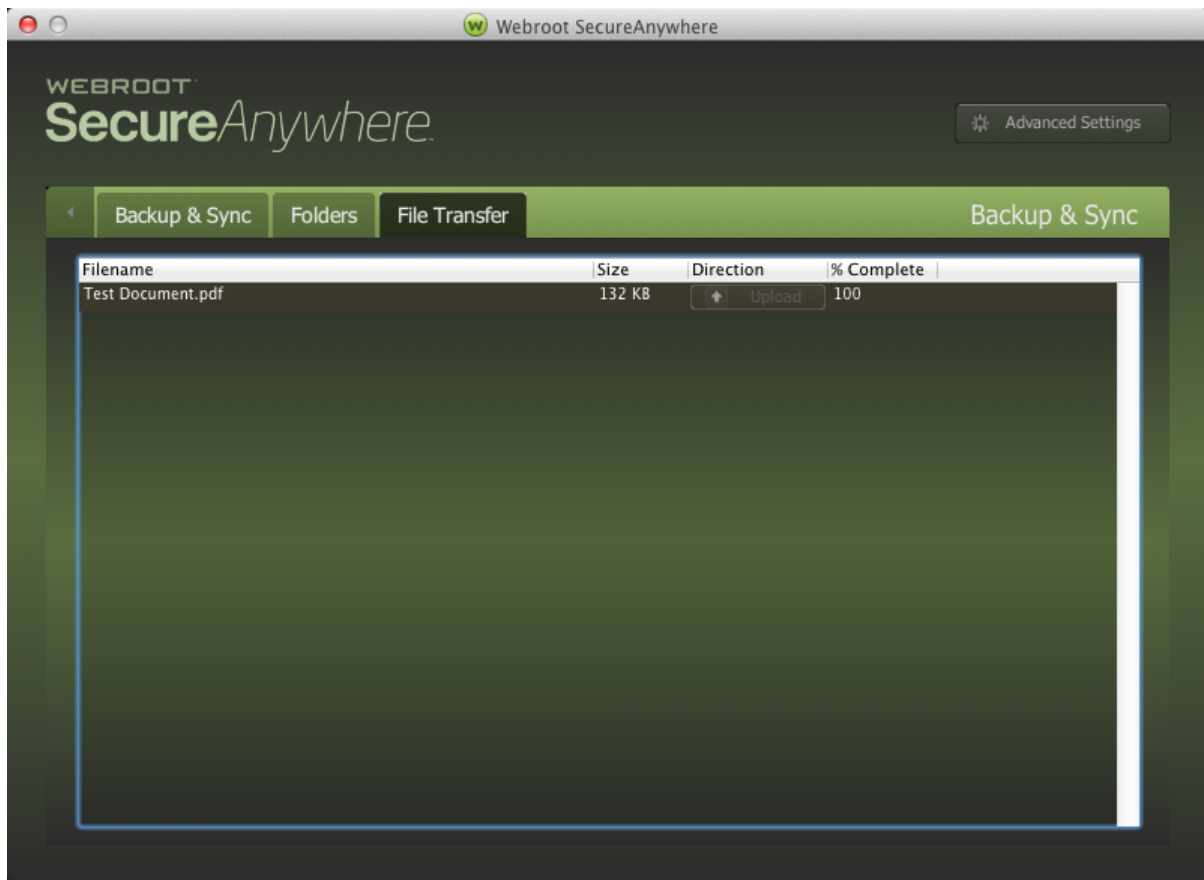
This topic contains the following procedures:

- [Checking File Transfer Status From Main Interface](#)
- [Checking File Transfer Status From Website](#)

To check file transfer status from the main interface:

1. Open SecureAnywhere. For more information, see [About the SecureAnywhere Interface on page 16](#).
2. Click the **Backup & Sync** tab.
3. Click the gear icon to the right.

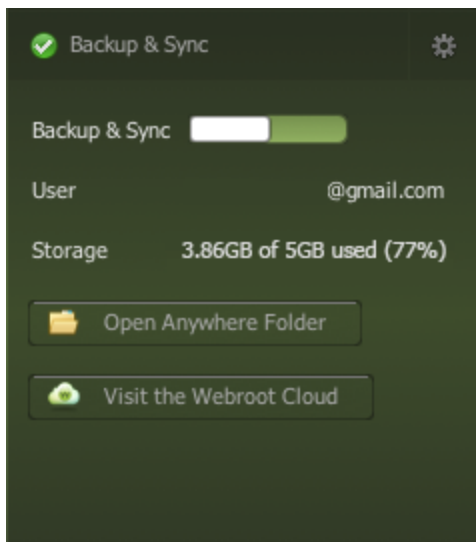
4. Click the **File Transfers** tab.



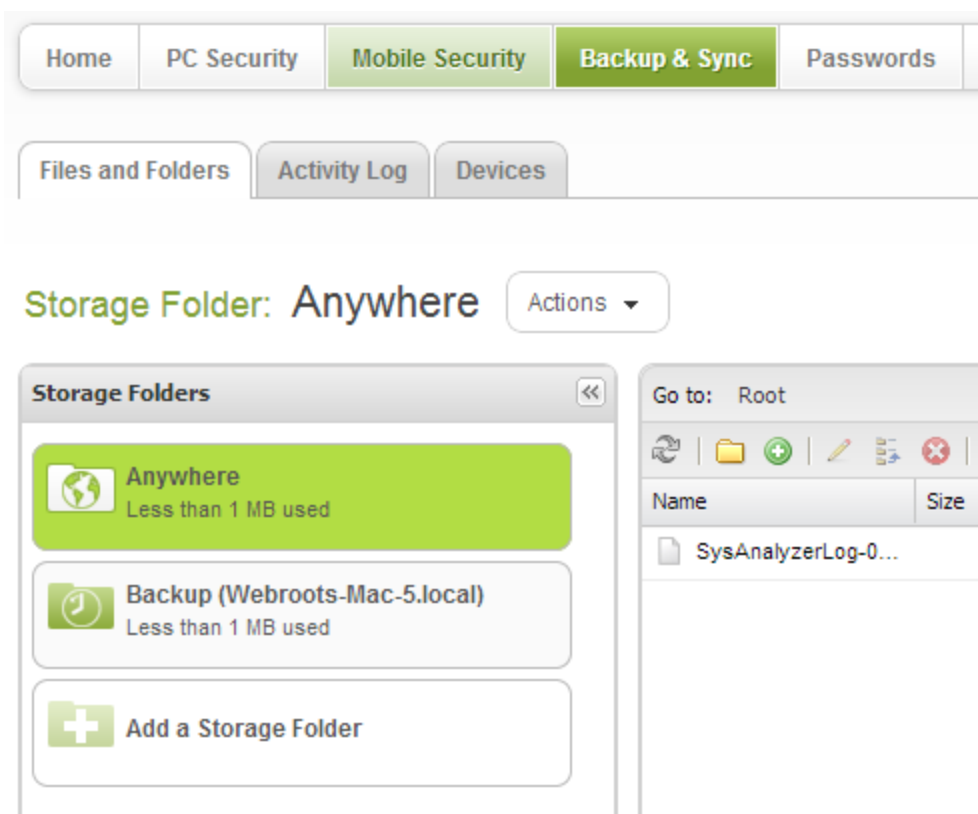
To check your file status from the SecureAnywhere website:

1. Open SecureAnywhere. For more information, see [About the SecureAnywhere Interface on page 16](#).
2. Click the **Backup & Sync** tab. The amount of disk space used is displayed under Storage.

3. To view your online account, click **Visit the Webroot Cloud**.



4. When your browser opens to my.webrootanywhere.com, log in to your account, click **Go to Backup & Sync**, then click the folders in the left panel.



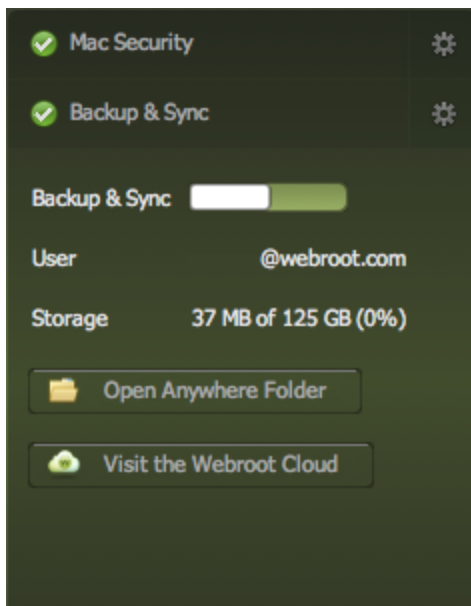
For more information about Backup & Sync in your account, see the [SecureAnywhere Website User Guide](#).

Synchronizing Files

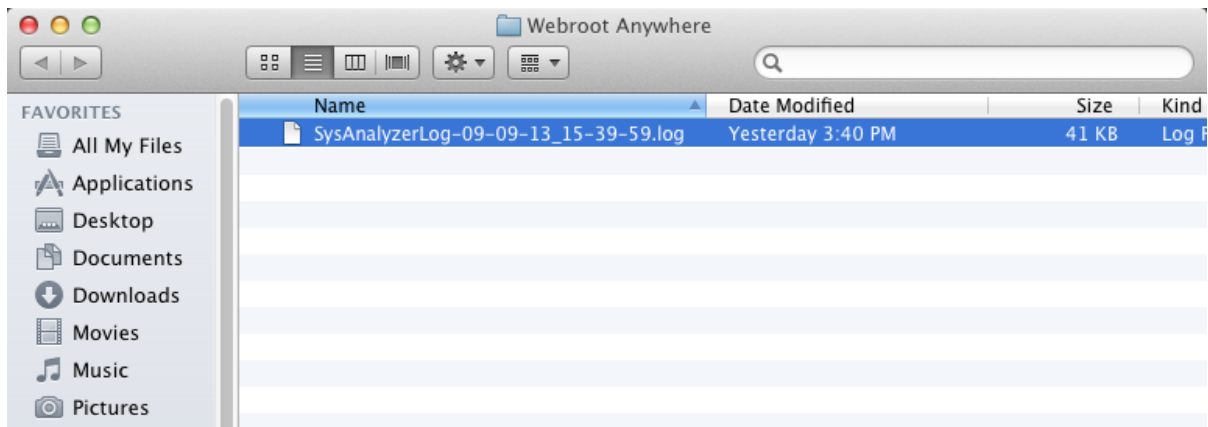
Webroot includes one preconfigured folder for synchronization, called the Anywhere folder. It resides under your personal folder on your Mac (\Users\[Username]\Webroot Anywhere). Any files you put in the Anywhere folder are automatically synchronized with your online account and with shared folders on other computers or mobile devices in your account.

To synchronize files using the Anywhere folder:

1. Open SecureAnywhere; for more information, see [About the SecureAnywhere Interface on page 16](#).
2. Click the **Backup & Sync** tab.
3. Click the Open Anywhere Folder **button**.



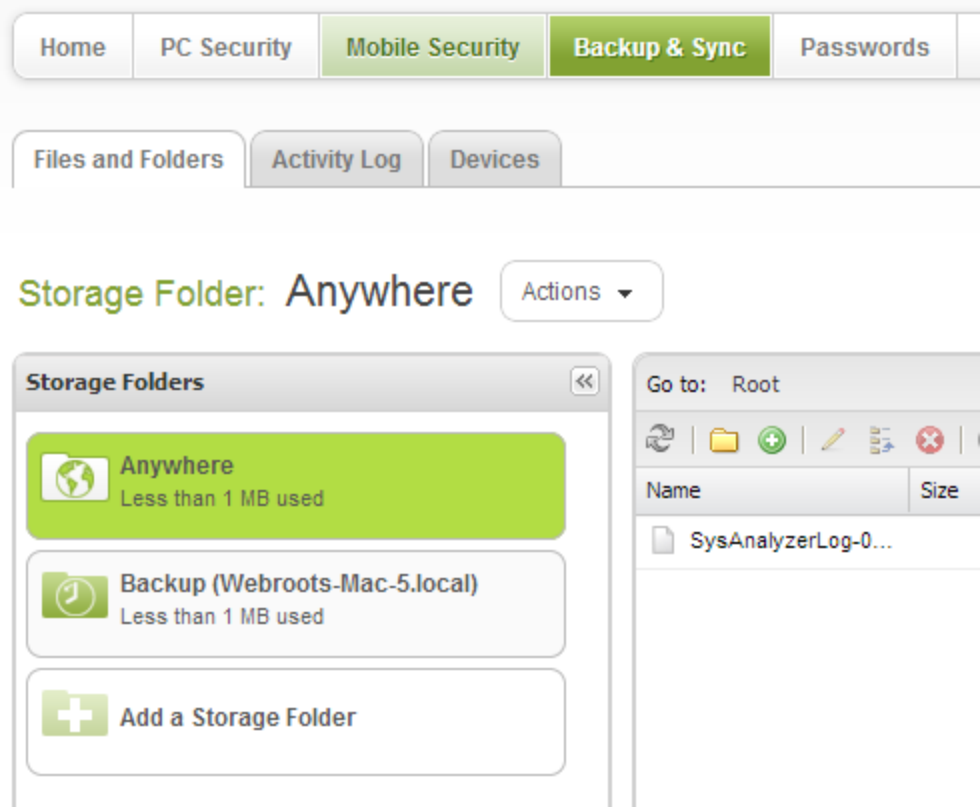
Mac Finder displays your Webroot Anywhere folder.



4. Copy files or folders into the Webroot Anywhere folder. The files are instantly synchronized to your online SecureAnywhere account and to other shared folders on other computers, if you configured them.

Note: Some files may fail to synchronize because their storage size is larger than the upload limit. You can adjust the limit in the Do not upload files larger than field in the Sync Settings panel. See [Changing Backup & Sync Settings on page 92](#).

5. To see the amount of used storage in your account, look at the Storage listed on the Backup & Sync panel. To check that your files were successfully copied, access your online account by clicking the **Visit the Webroot Cloud** button.
6. When your browser opens to my.webrootanywhere.com, log in to your account, click **Go to Backup & Sync**, then click **Anywhere**.



For more information about using Backups in your online account, see the [SecureAnywhere Management Website User's Guide](#).

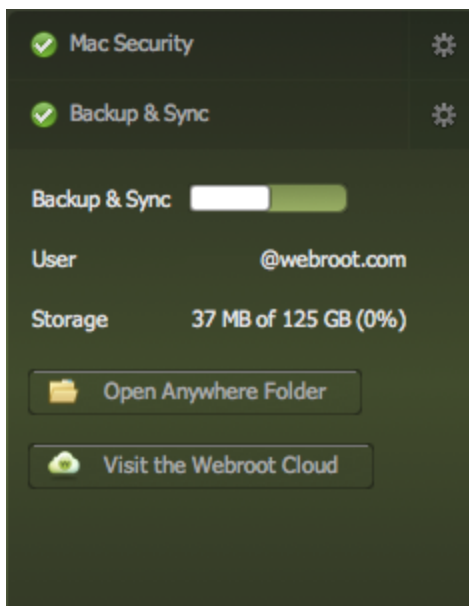
Synchronizing Folders Between Computers

If you installed SecureAnywhere on multiple computers, you can create shared, synchronized folders between them. Whenever you update data in one of these shared folders such as adding, editing, moving, or deleting files, SecureAnywhere automatically makes the same changes in your online account and to all shared folders. This automatic synchronization can be beneficial when you frequently use multiple computers and need access to the most recent files.

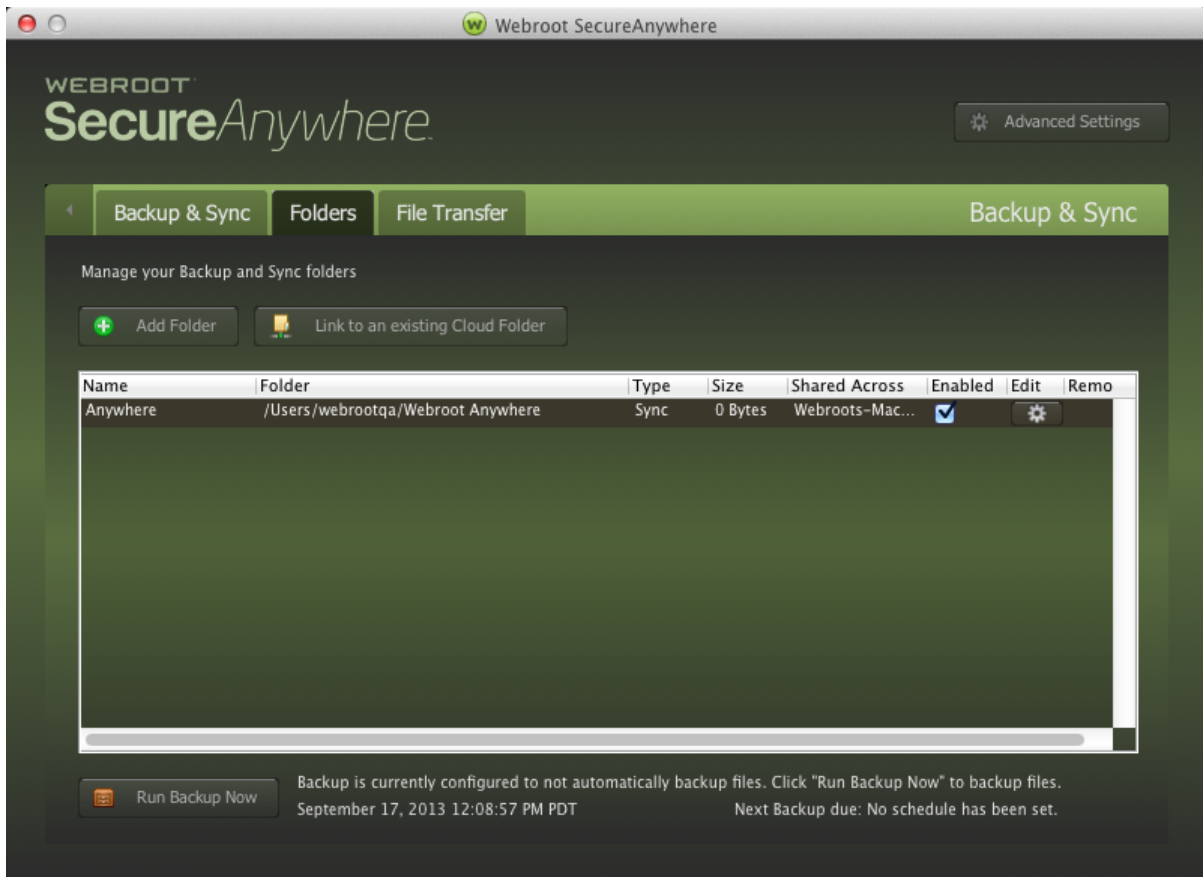
Note: Be aware that when you make changes to a folder on one computer, the changes are propagated across the shared folders on all computers. For example, if you delete a shared folder, it is removed from all the devices. However, you can still access a deleted folder or file from the Recycle Bin in your SecureAnywhere account.

To sync folders on two different computers:

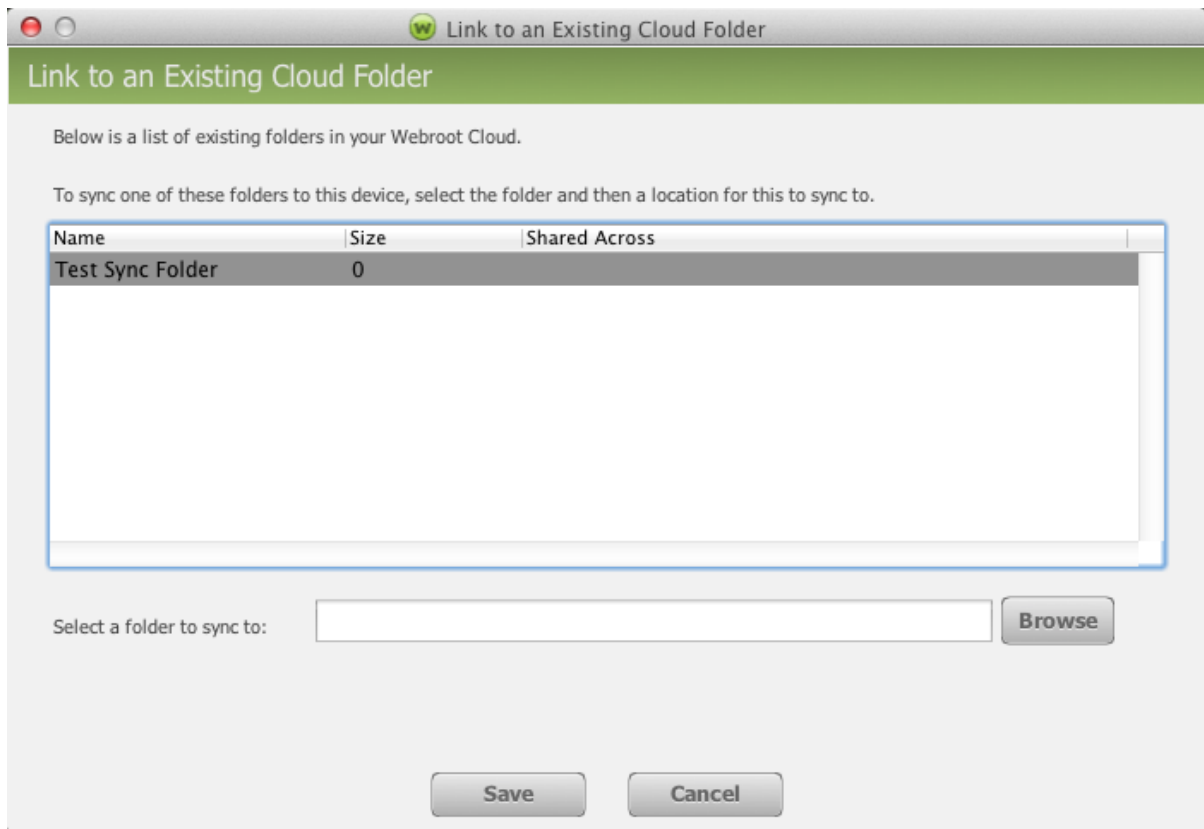
1. Configure a sync folder on the first computer. For more information, see [Adding Sync Folders on page 85](#).
2. On the second computer, open the Backup & Sync Settings panel. Click the **Backup & Sync** tab, make sure Backup & Sync is enabled, then click the **Backup & Sync** gear icon.



3. Click **Folders** on the top.
4. Click the **Link to an existing Cloud Folder** button.



5. In the next panel, select the folder to sync with from the list provided. Then click **Browse** at the bottom to select where to have the sync folder saved on this computer. Click **Save**.



SecureAnywhere synchronizes all files in that folder with your other computer. In the Backup & Sync Settings panel, the Shared Across column lists the computers sharing that folder.

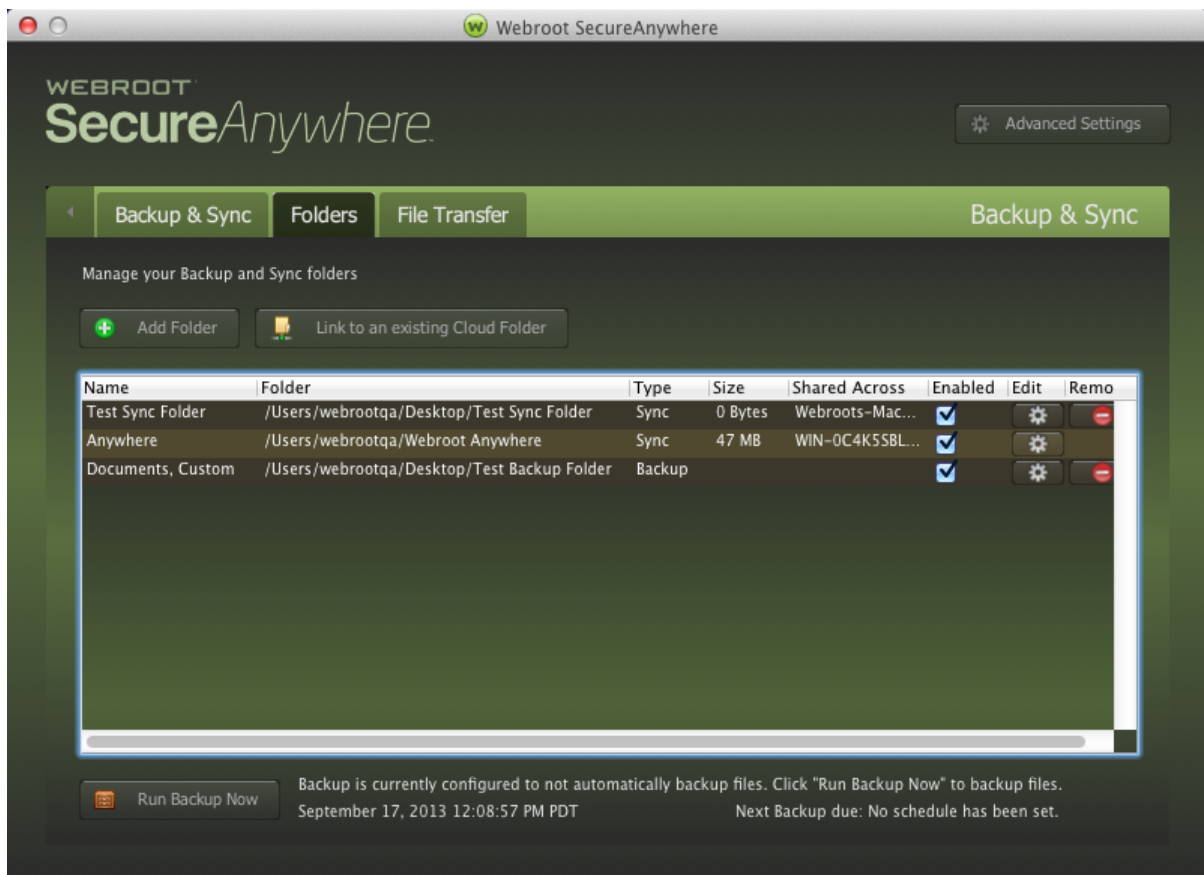
Removing Folders From Synchronization

You can stop synchronizing the contents in a folder by detaching it from the automatic synchronization process.

Note: Detaching the folder does not delete it from your computer.

To remove a folder from synchronization:

1. Open SecureAnywhere. For more information, see [About the SecureAnywhere Interface on page 16](#).
2. Click the **Backup & Sync** tab.
3. Click the **Backup & Sync** gear icon.
4. Click the **Folders** tab.



5. To the far right of the folder you want to stop syncing, click the **Remove** icon. The folder will no longer display in the panel and will no longer synchronize to your SecureAnywhere account.
 6. When you're done, click the **Close** button.
-

Chapter 8: Managing Passwords

To manage passwords, see the following topic:

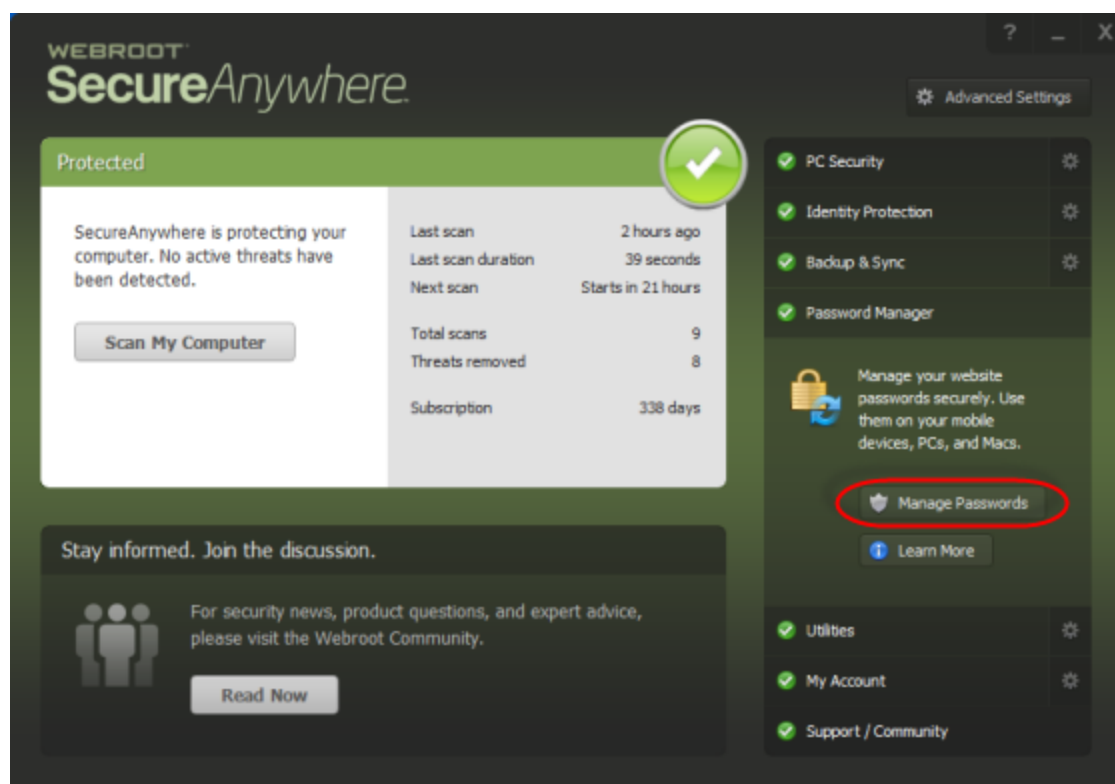
About Managing Passwords	114
---------------------------------------	------------

About Managing Passwords

If you purchased a SecureAnywhere edition that includes password management, you can use an additional component for managing passwords and profiles online.

Once you define your personal information and passwords in SecureAnywhere, you can automatically log in to websites or populate fields in web forms, saving you the hassle of manually entering your personal data and credit card numbers.

All Password Management features are managed from your account's web interface. You can access that page by clicking the Manage Passwords button under Password Manager. For step-by-step instructions covering all features, see [Working With Passwords](#) in the [Management Website User Guide](#).



Note: For more information about LastPass, see the [LastPass Reference Guide](#).

Chapter 9: Using Advanced Tools

To use advanced tools, see the following topics:

Changing System Control Settings	116
Saving Scan Logs	120
Submitting Scan Logs	126
Running System Analyzer	133

Changing System Control Settings

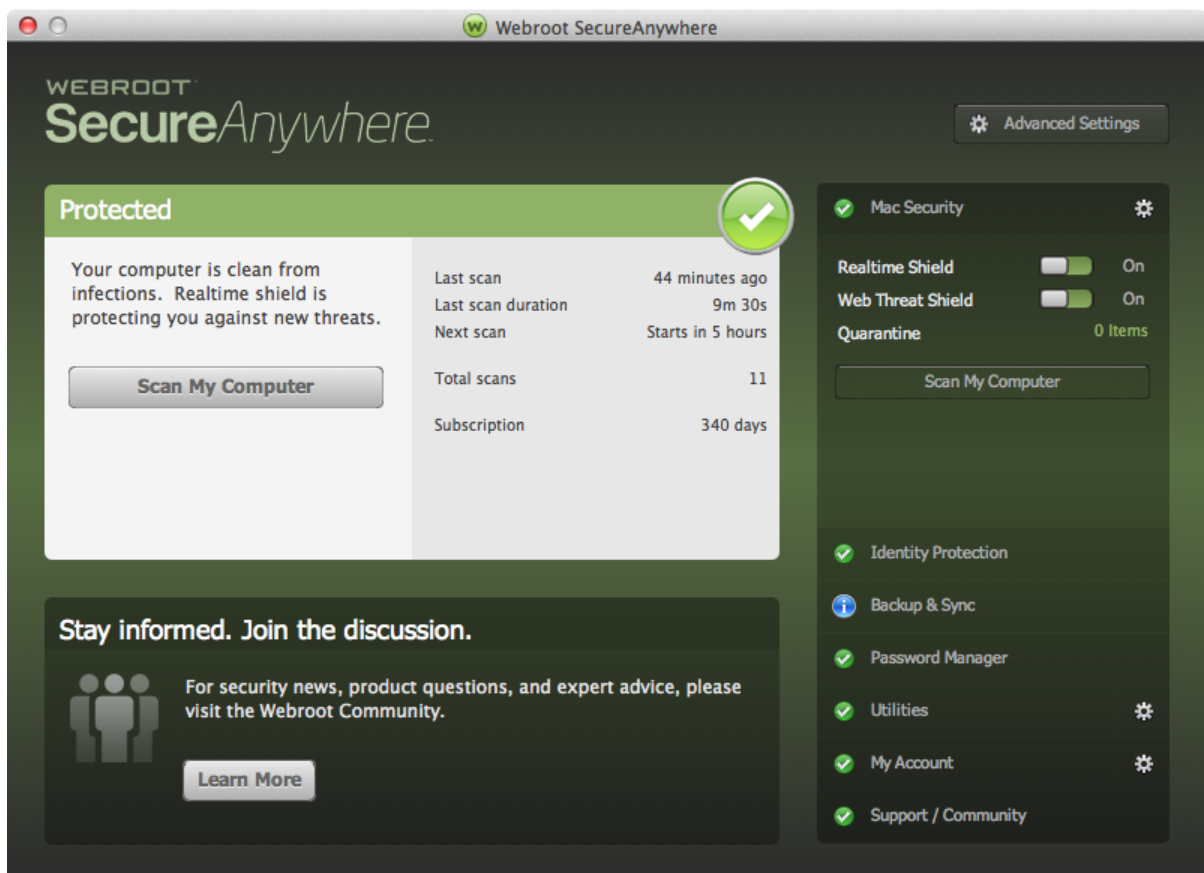
The Active Processes feature allows you to adjust the threat-detection settings for all programs and processes running on your Mac.

To change system control settings:

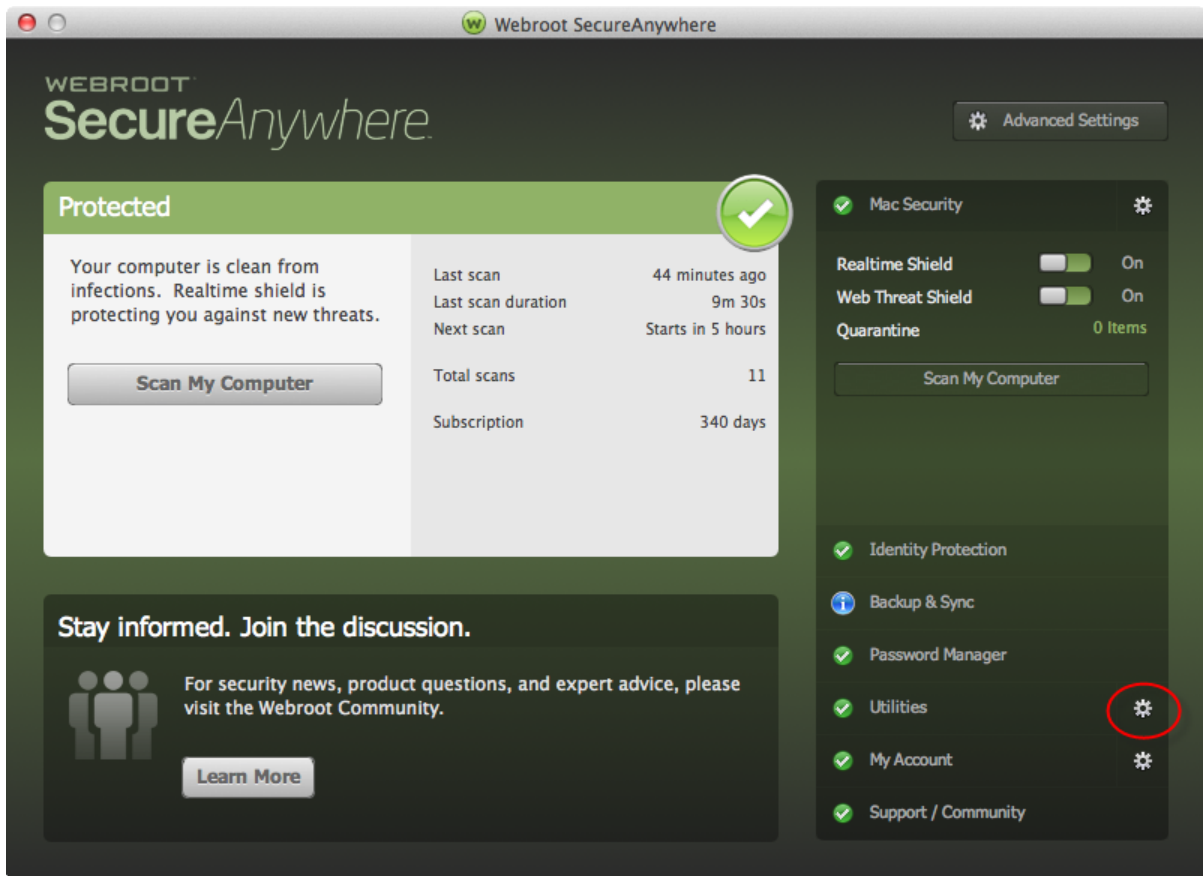
1. From the dock, click the **Webroot** icon.



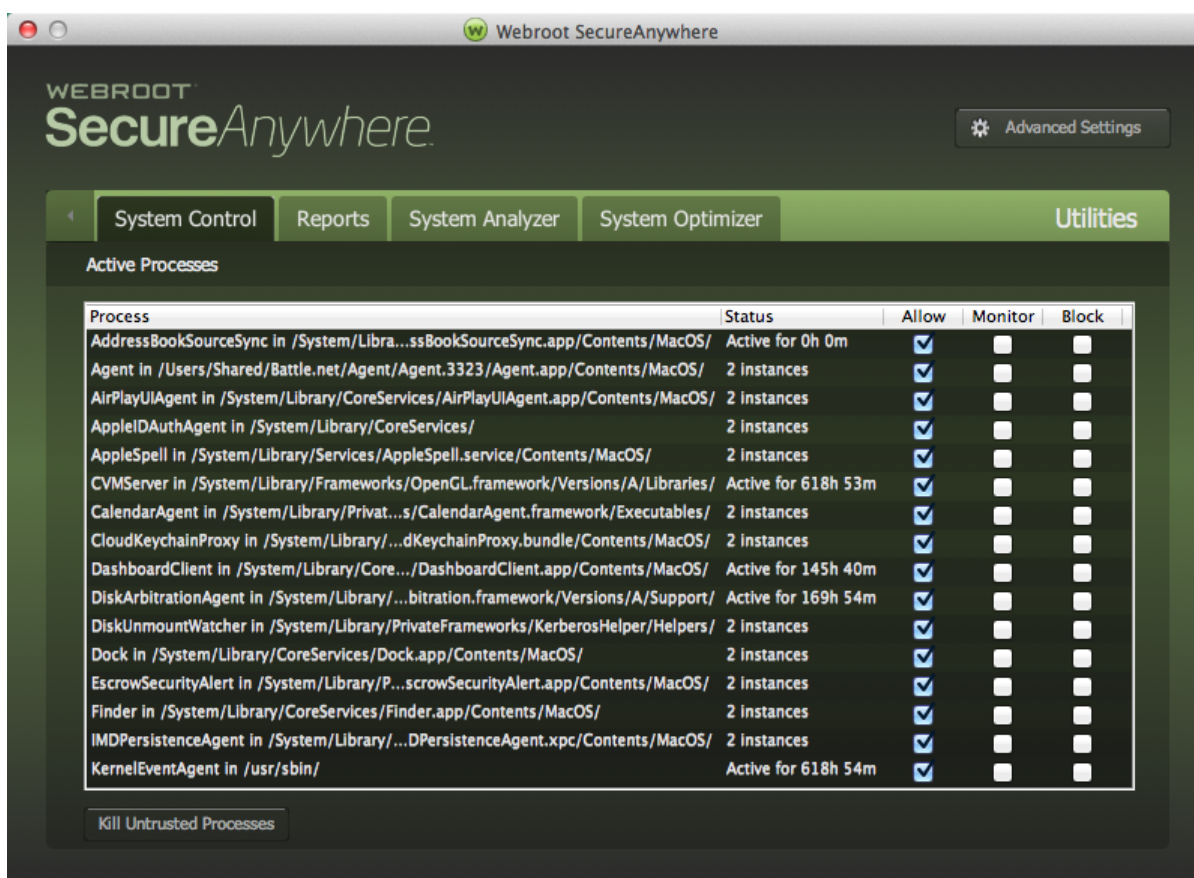
The main interface displays.



2. Click the **Utilities** gear icon.



The Utilities panel displays with the System Control tab active.



Note: You can also access the Active Processes menu by clicking Utilities on the Menu bar and selecting System Control from the drop-down menu.

- For each process, you can select or deselect the checkbox for any of the following:
 - Allow** — Allows the process to run on your system.
 - Monitor** — Watches the process and opens an alert on suspicious activity.
 - Block** — Stops the process from running on your system.

Note: Do not block a process unless you have been advised to do so by Webroot Support.

- Optionally, you can click the **Kill Untrusted Processes** button.

5. When you're done, click the **Back Arrow** to return to the main panel, or click the **Close** button.
-

Saving Scan Logs

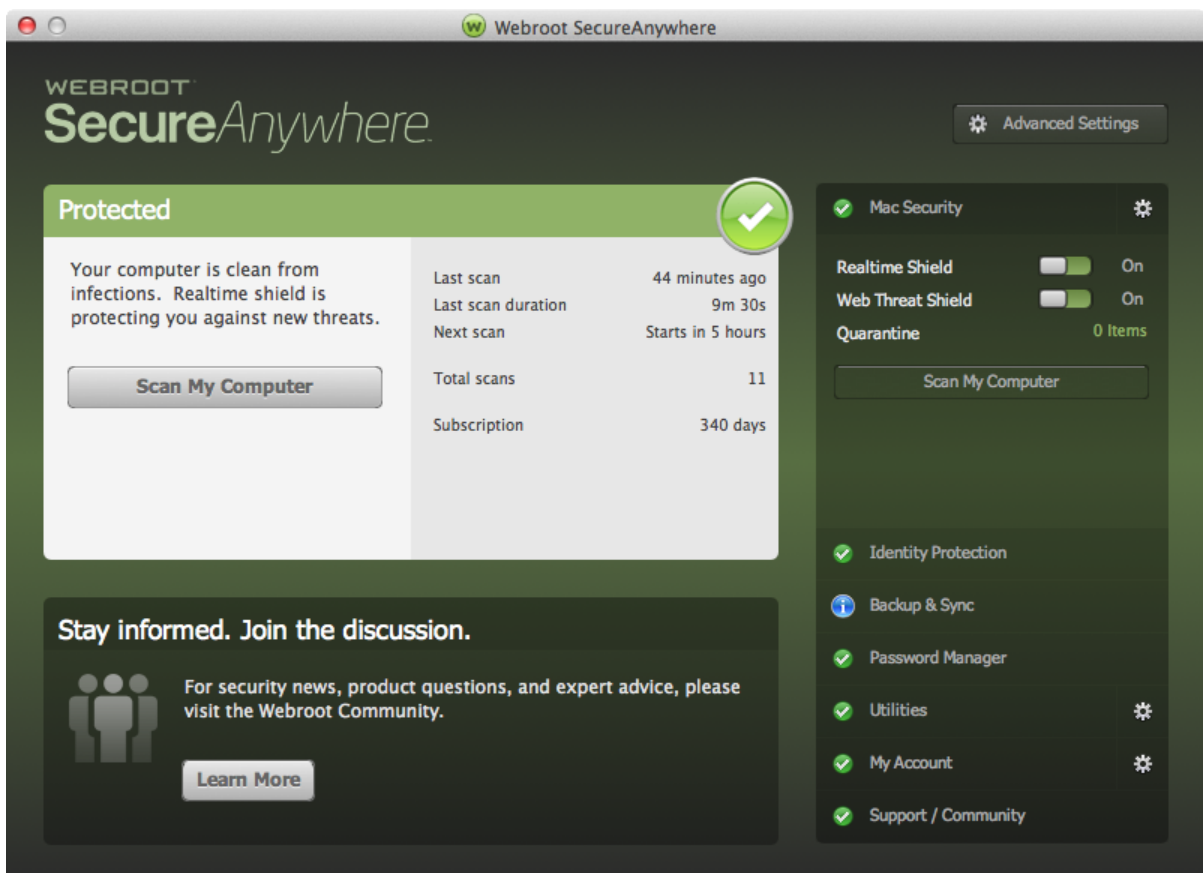
If you want to investigate what SecureAnywhere scanned and what it found, you can save a scan log. This log might be helpful if you are working with [Webroot Support](#) to determine the cause of a problem.

To save a scan log:

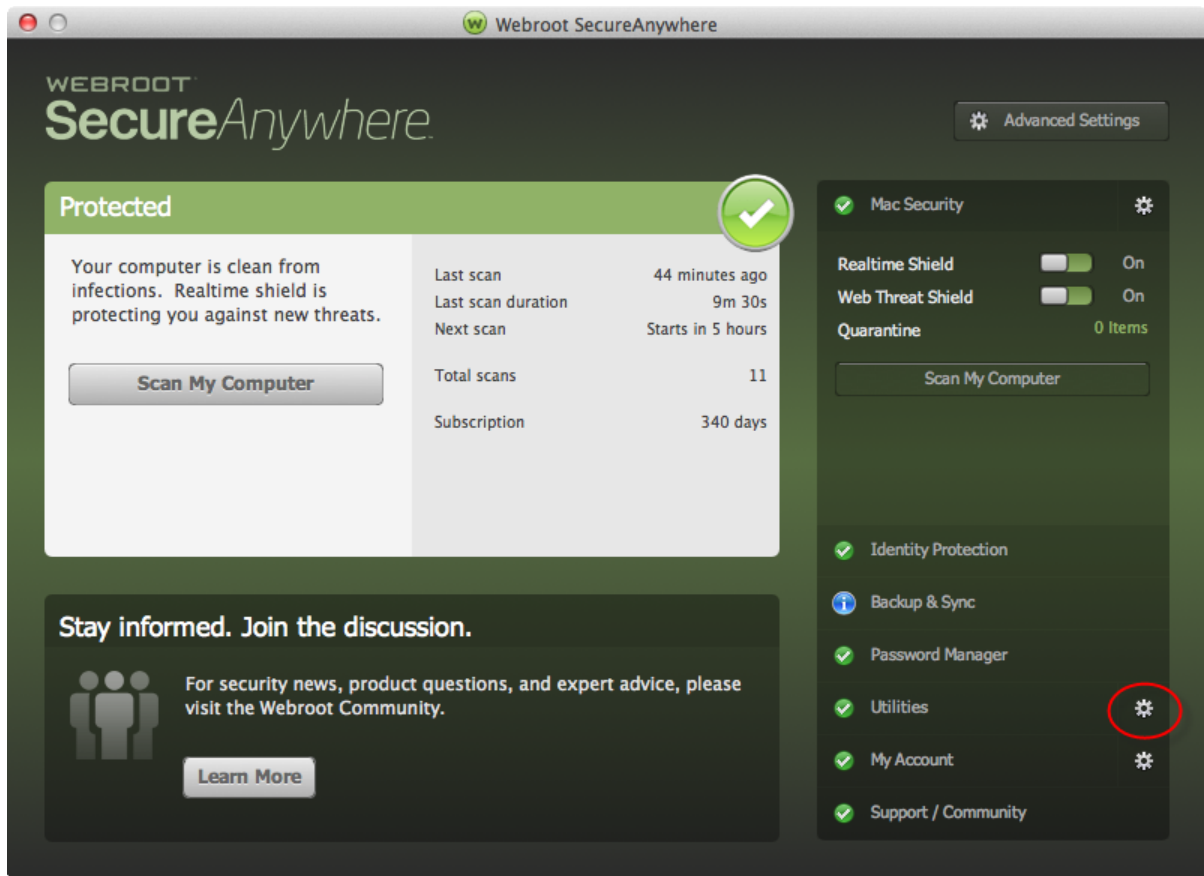
1. From the dock, click the **Webroot** icon.



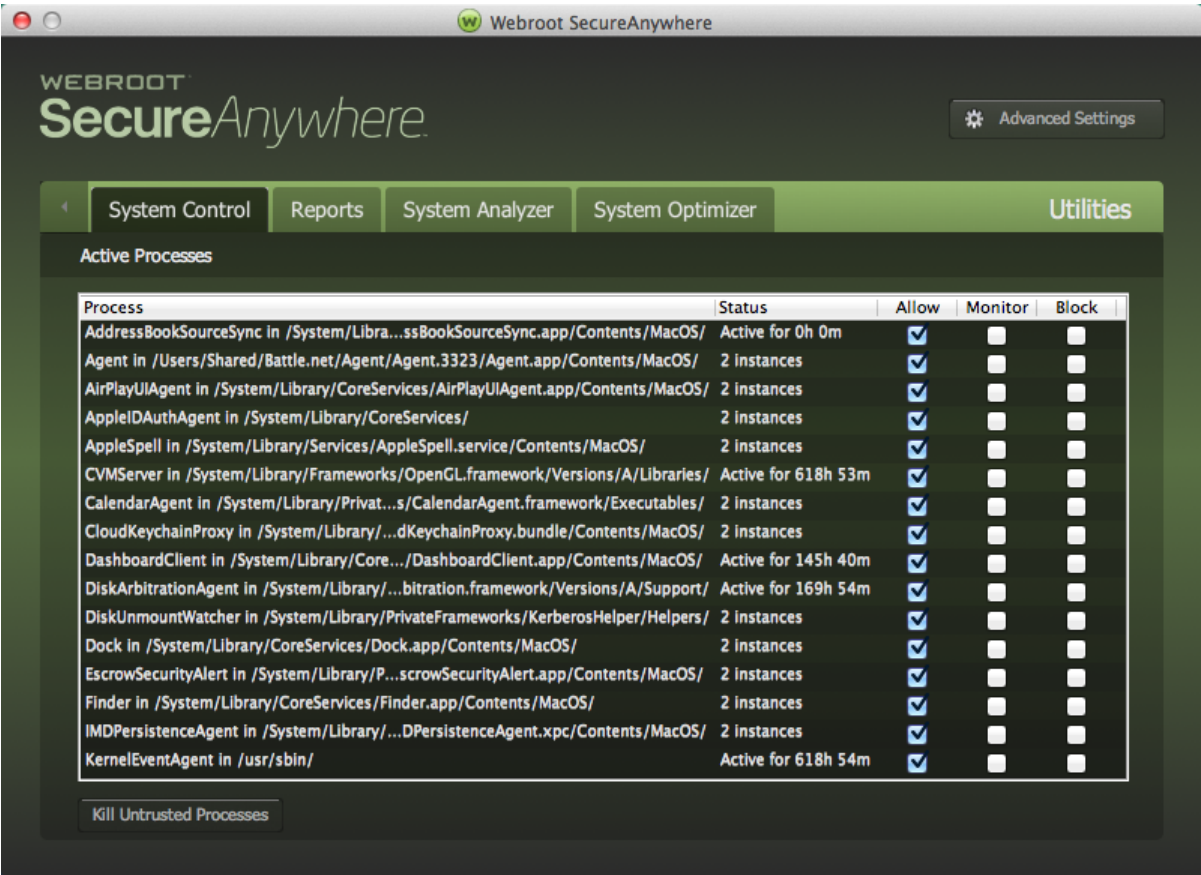
The main interface displays.



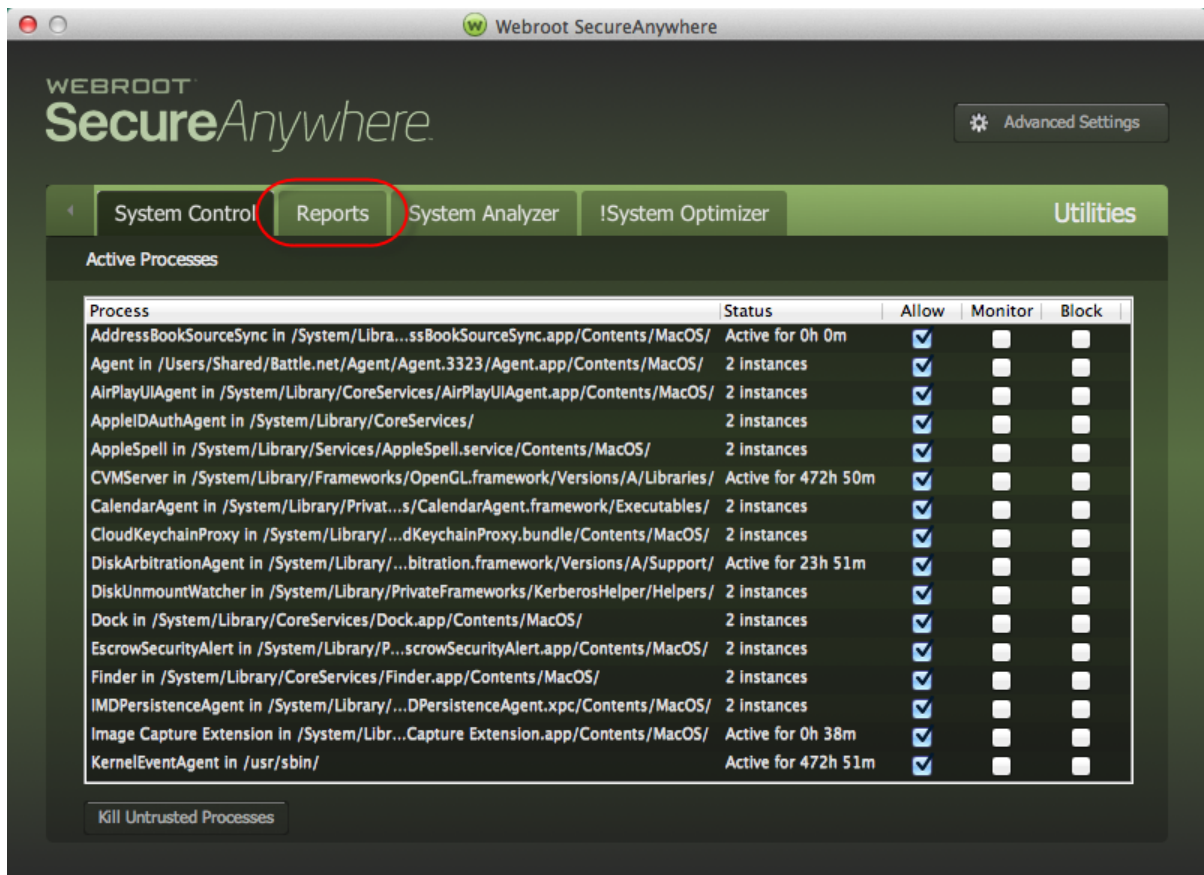
2. Click the **Utilities** gear icon.



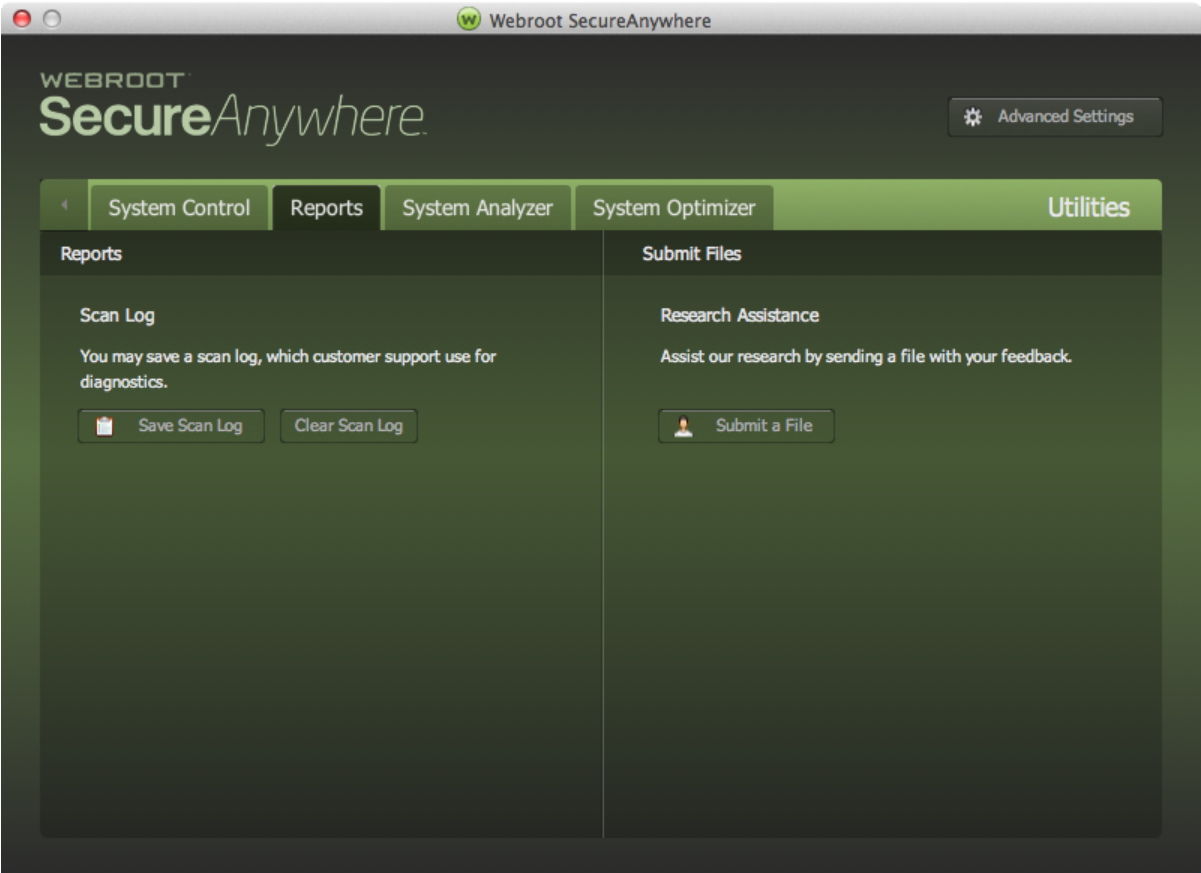
The Utilities panel displays with the System Control tab active.



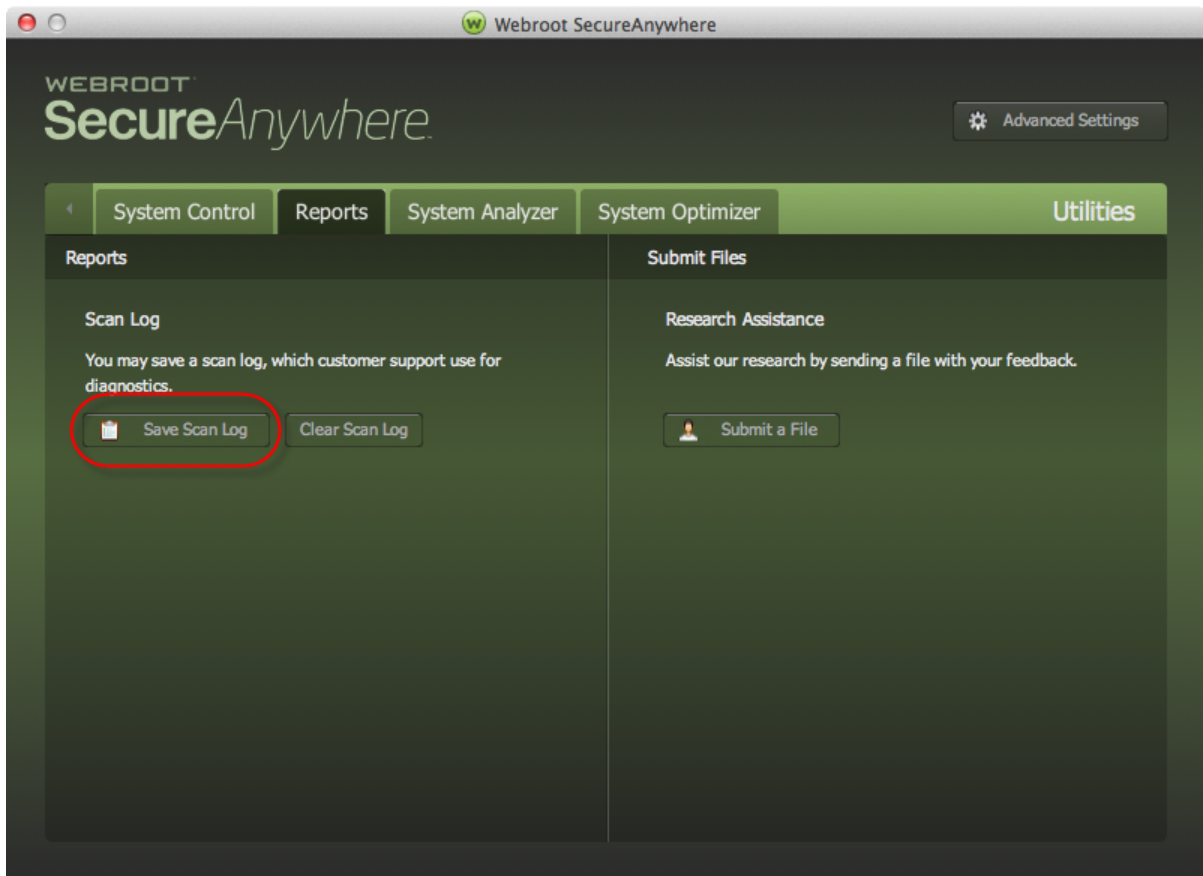
3. Click the **Reports** tab.



The system displays the Reports panel.



4. Click the **Save Log** button.



Note: You can also access the Save Scan Log option by clicking **Utilities** on the Menu bar and selecting **Reports** from the drop-down menu.

5. Enter a filename and location, then click the **Save** button.
-

Submitting Scan Logs

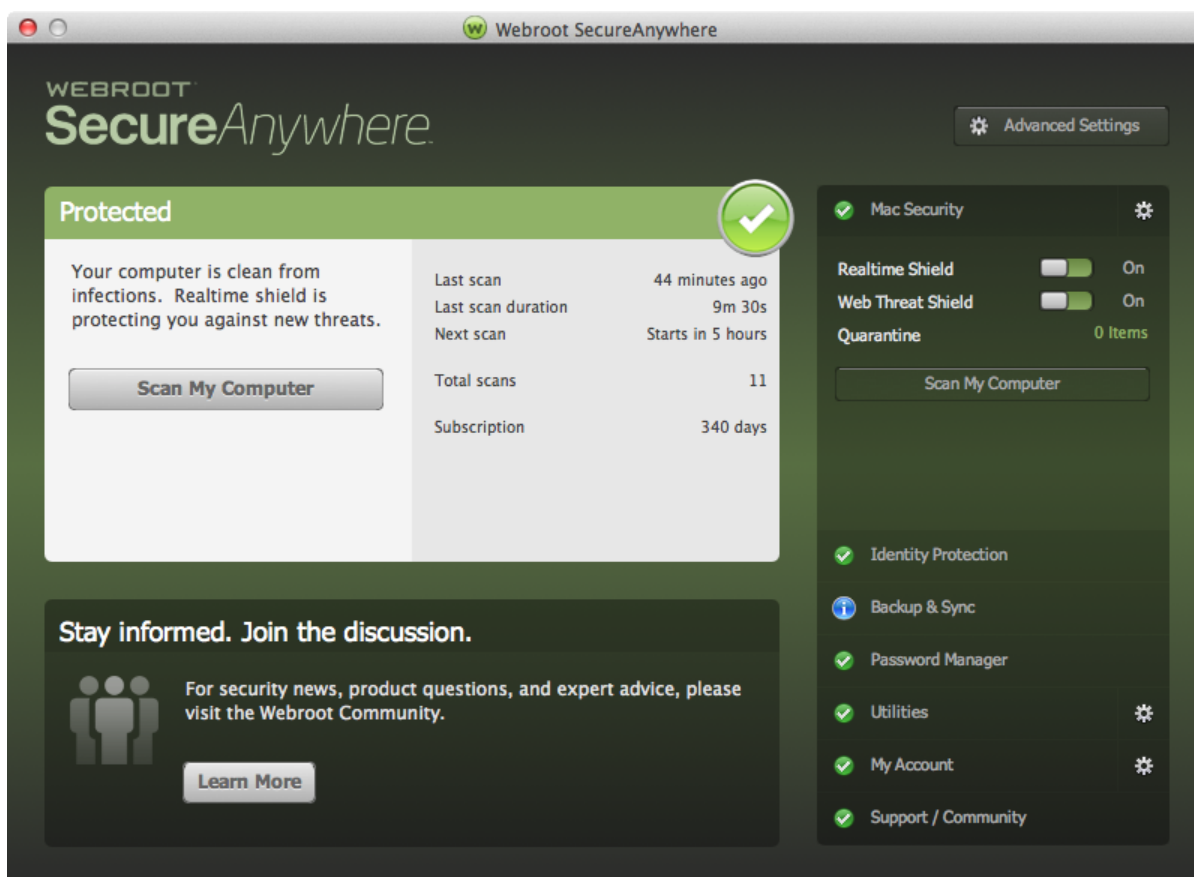
If a file on your system is causing problems or if you know a file is safe and want it reclassified, you can send the file to [Webroot](#) for analysis.

To submit a scan log:

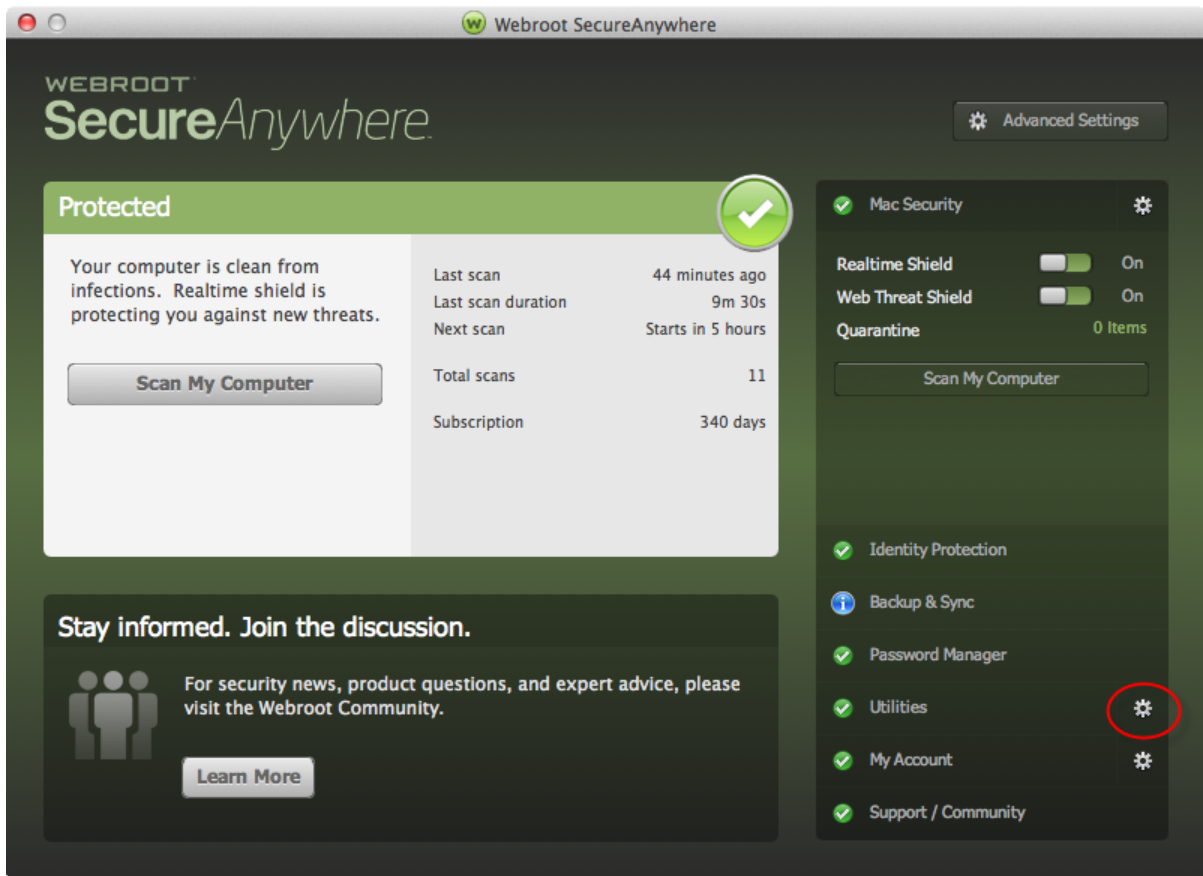
1. From the dock, click the **Webroot** icon.



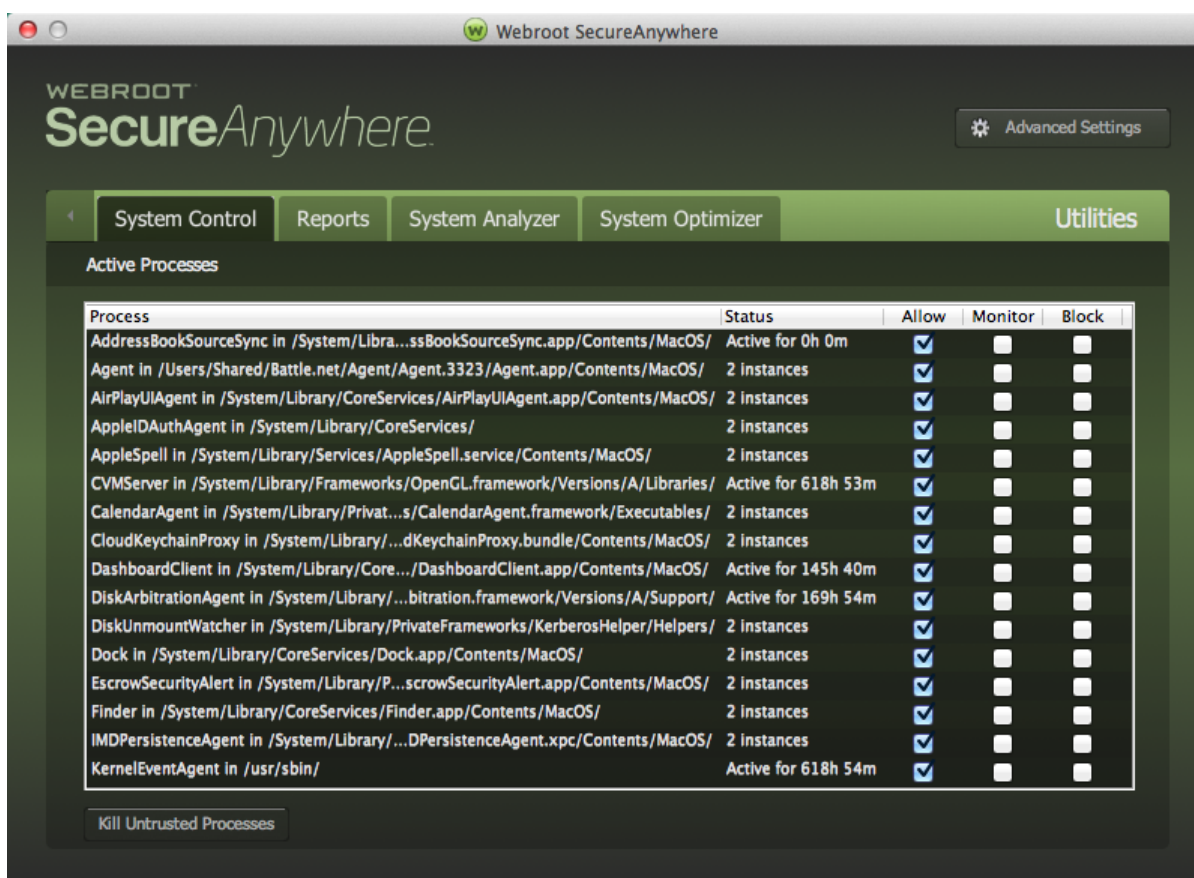
The main interface displays.



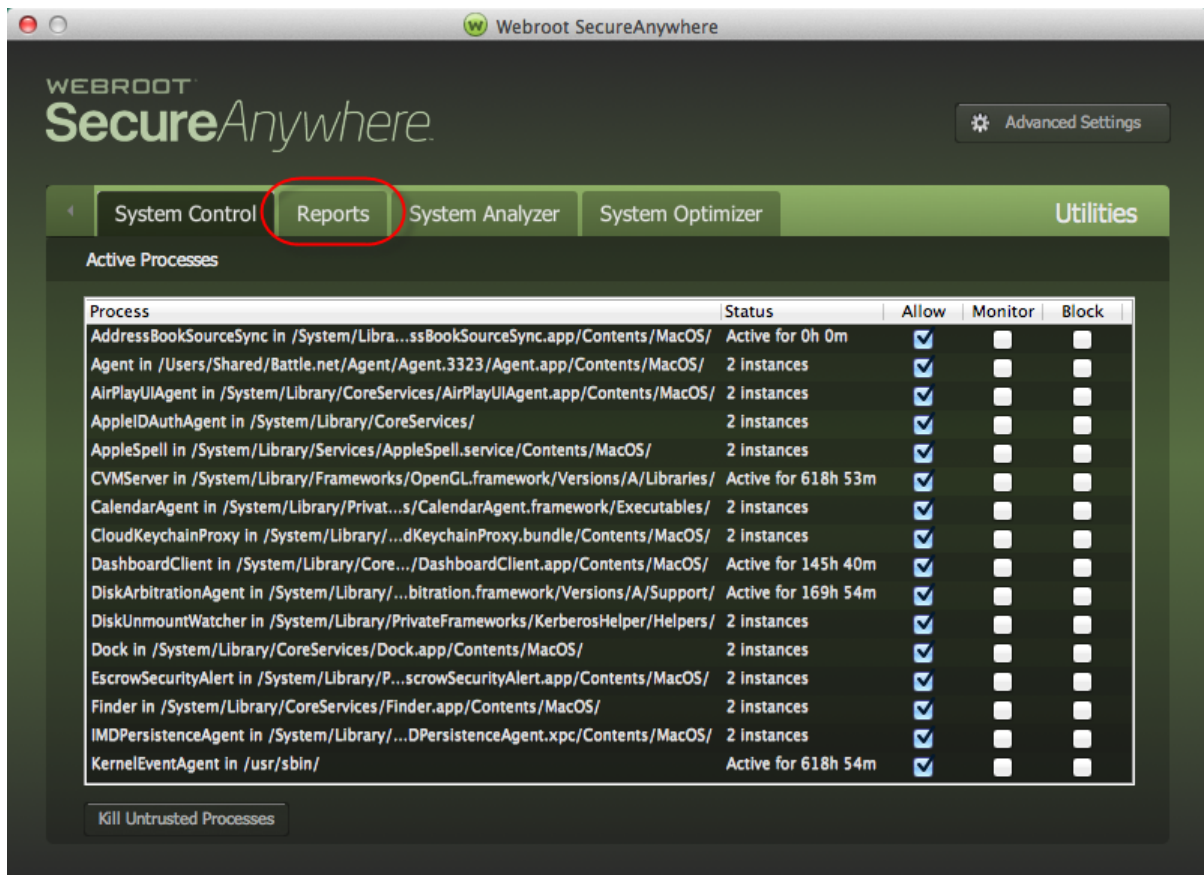
2. Click the **Utilities** gear icon.



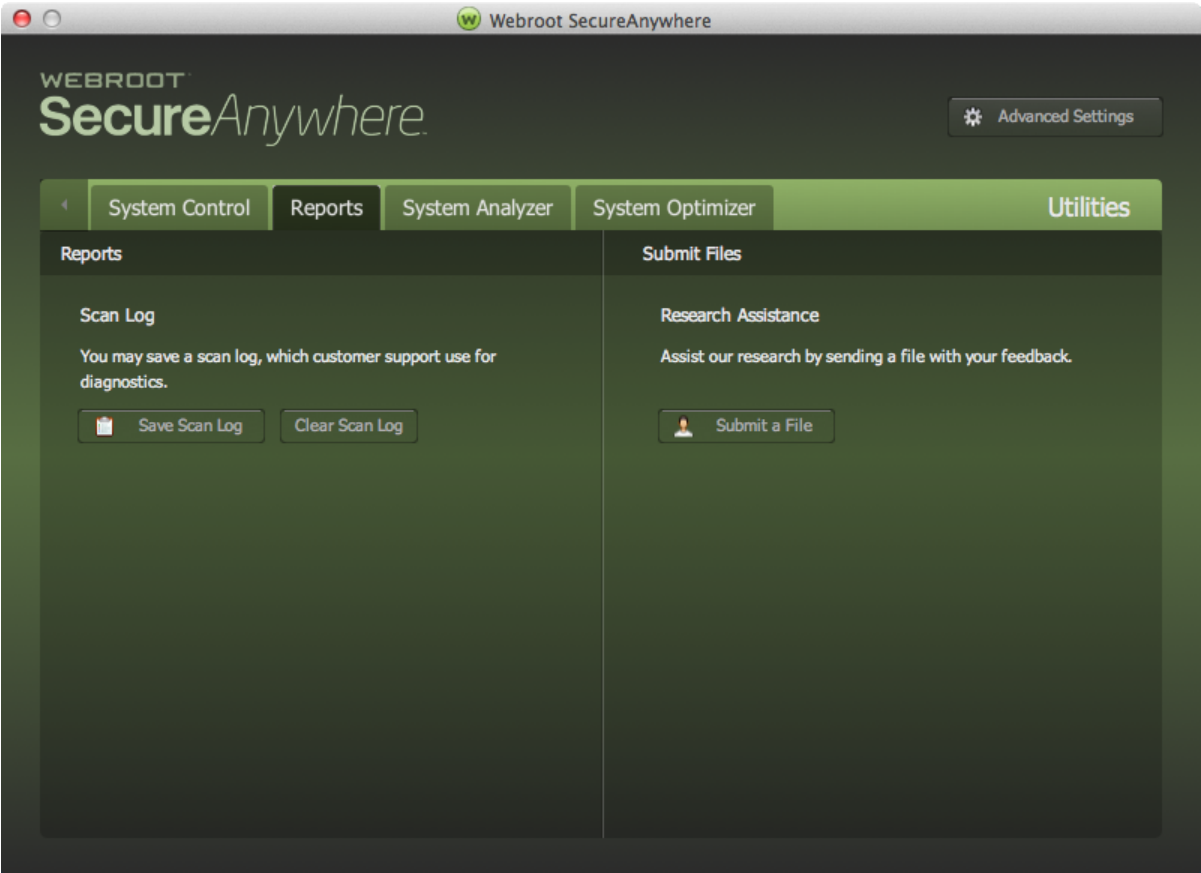
The Utilities panel displays with the System Control tab active.



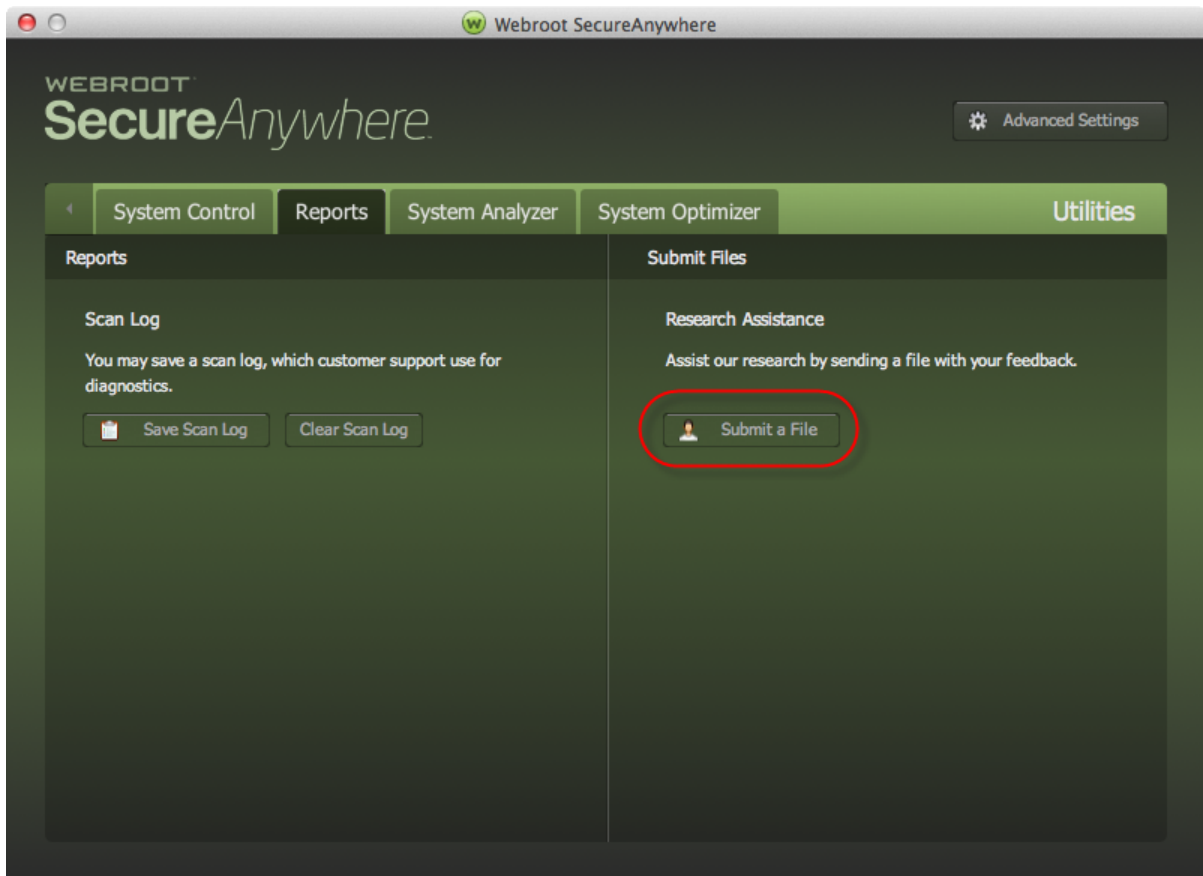
- Click the **Reports** tab.



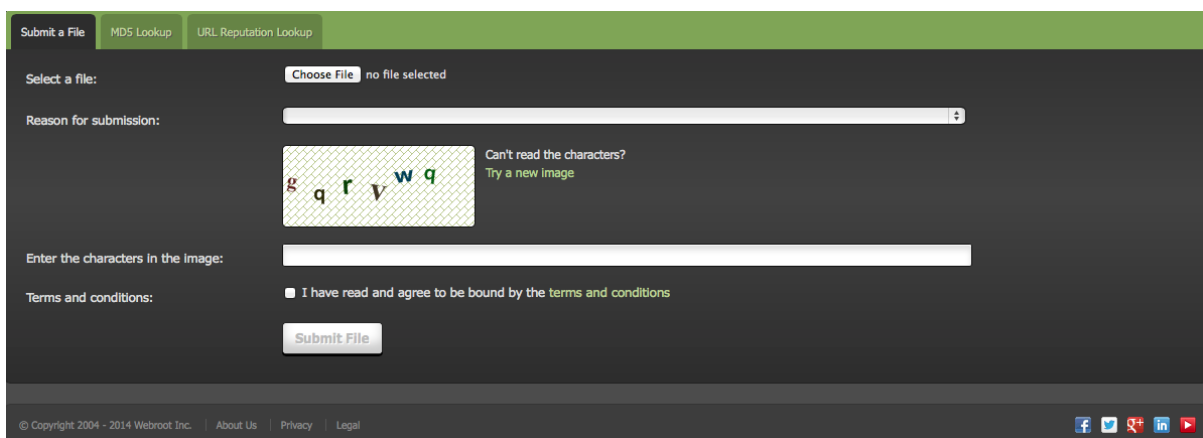
The system displays the Reports panel.



4. Click the **Submit a File** button.



A web page displays where you can send a file to [Webroot](https://www.webroot.com) for analysis.



5. Use the **Browse** button to select the file that you want Webroot to analyze.
 6. Enter in a reason for sending this file to Webroot.
 7. Enter the CAPTCHA characters in the next line.
 8. When you're done, click the **Submit File** button.
-

Running System Analyzer

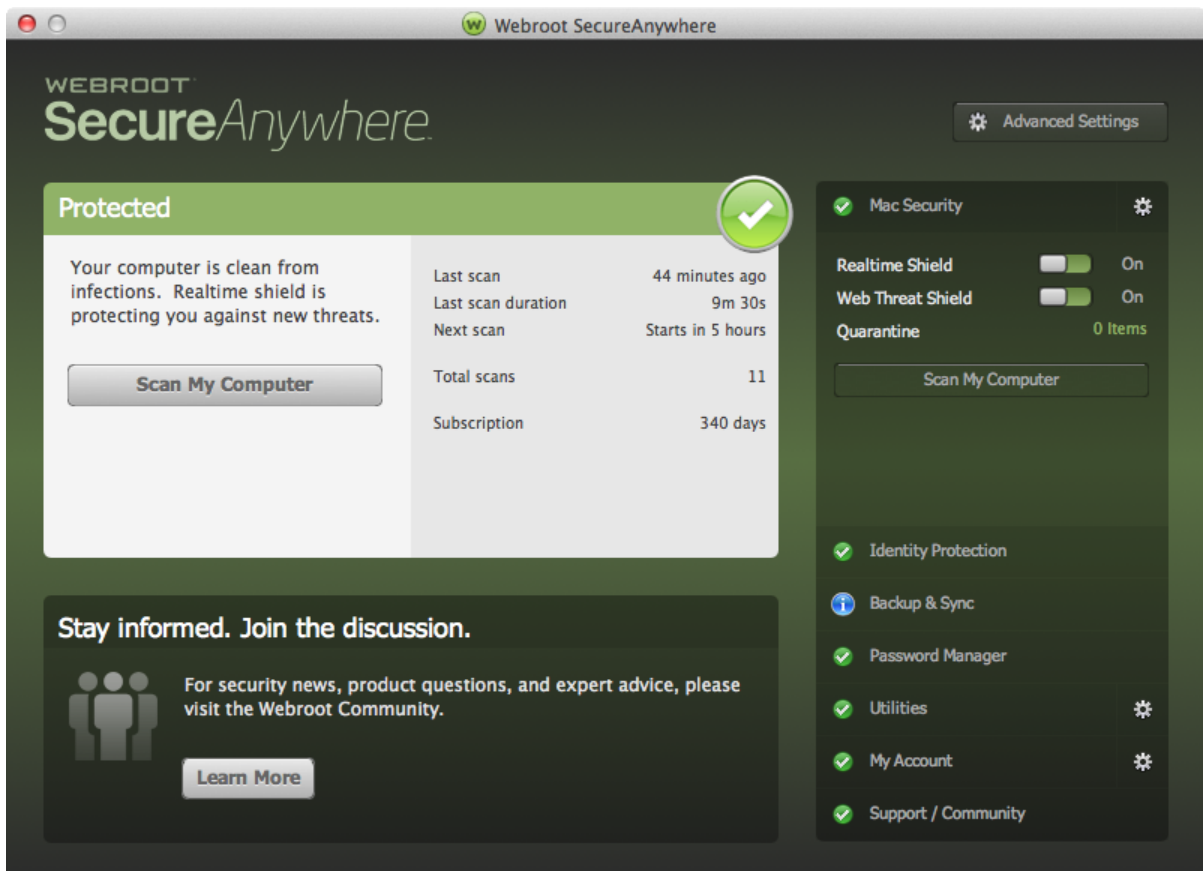
System Analyzer is a simple utility that quickly scans for threats, security vulnerabilities, and other computer problems. After the scan, it displays a report that describes any vulnerabilities it found. It also provides recommendations about enhancements that can increase system performance, privacy, and protection.

To run System Analyzer:

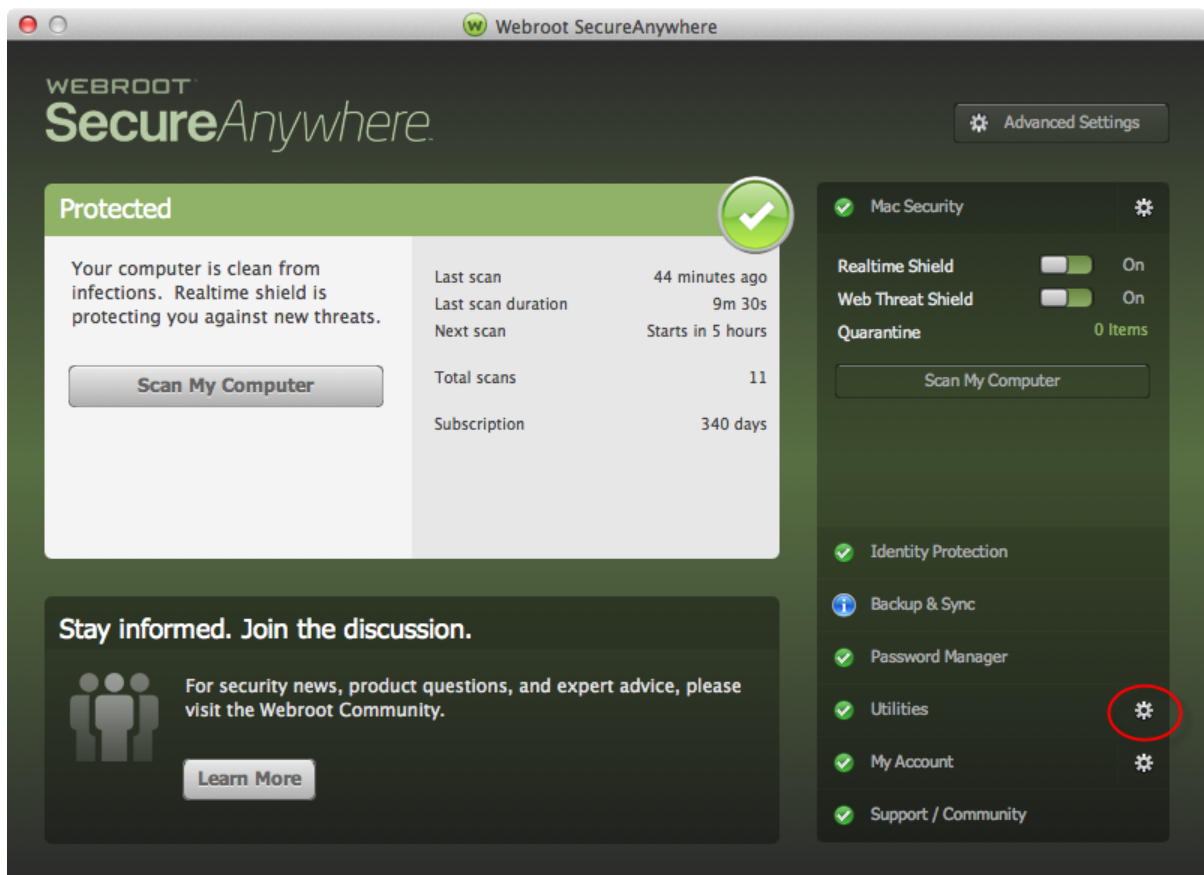
1. From the dock, click the **Webroot** icon.



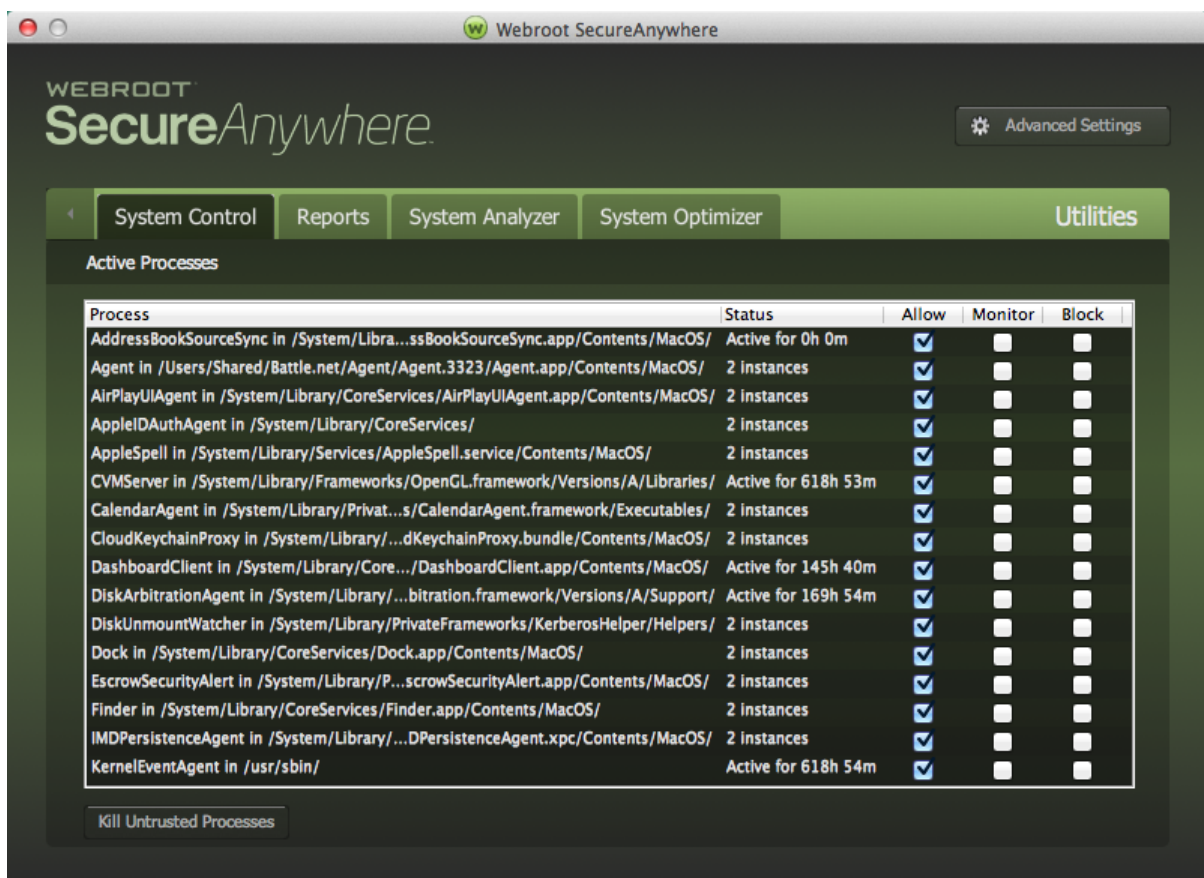
The main interface displays.



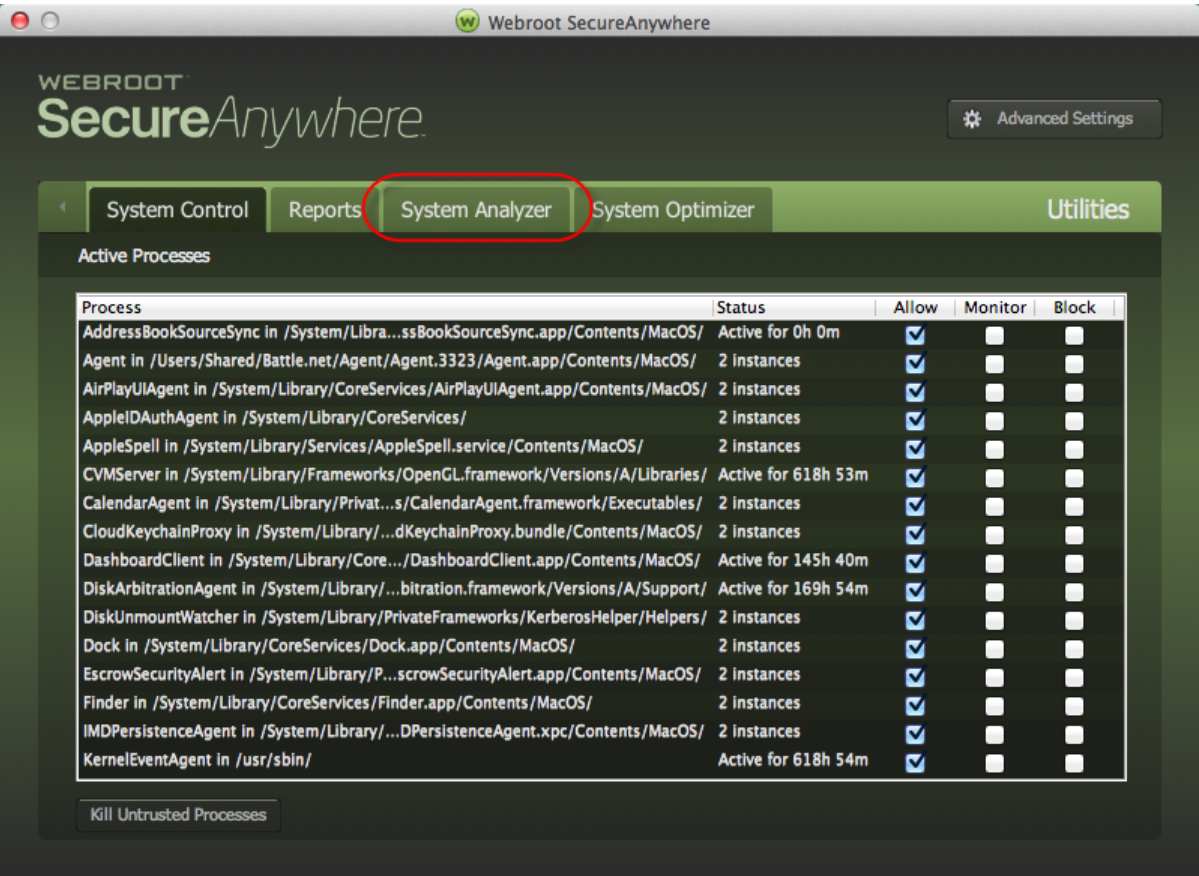
2. Click the **Utilities** gear icon.



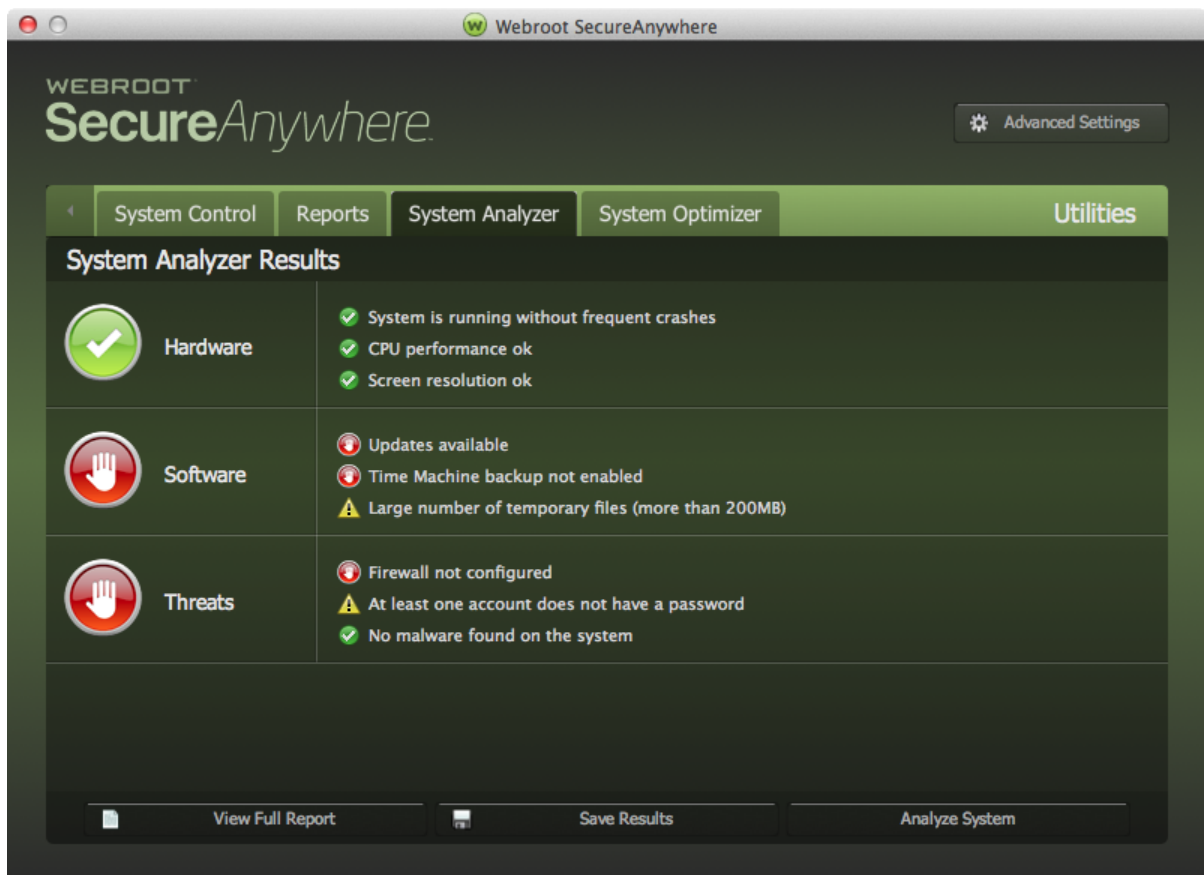
The Utilities panel displays with the System Control tab active.



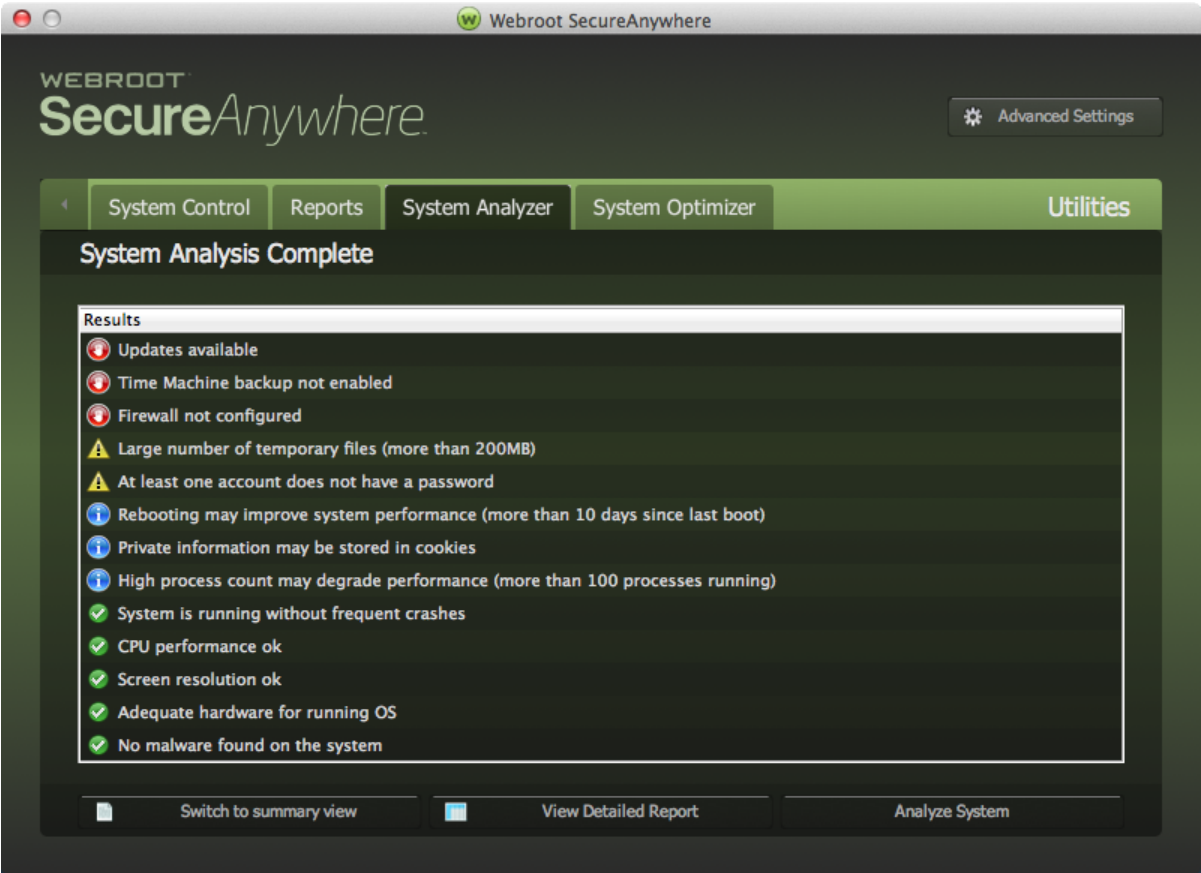
3. Click the **System Analyzer** tab.



SecureAnywhere launches its system analysis. When finished, it displays a summary view.



4. Do either of the following:
 - To view more items, click the **View Full Report** button.
 - To save it in HTML format, click the **Save Results** button.



Chapter 10: Using System Optimizer

To use System Optimizer, see the following topics:

Running System Optimizer	140
Changing System Optimizer Settings	148
Creating Secure Erase Settings	156

Running System Optimizer

If you purchased a SecureAnywhere edition that includes System Optimizer, you can remove all traces of your web browsing history, files that indicate your computer use, and other files that reveal your activity.

Note: System Optimizer for Mac is only available on the [consumer edition of Webroot SecureAnywhere](#).

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

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

Optimizations remove unnecessary files and traces, not malware threats. Malware such as spyware and viruses are removed during scans. Think of the System Optimizer as the housekeeper for your computer, while the Scanner serves as the security guard. For more information about scans, see [Running Scans on page 24](#).

Before running the optimizer, you can customize it using any of the following procedures:

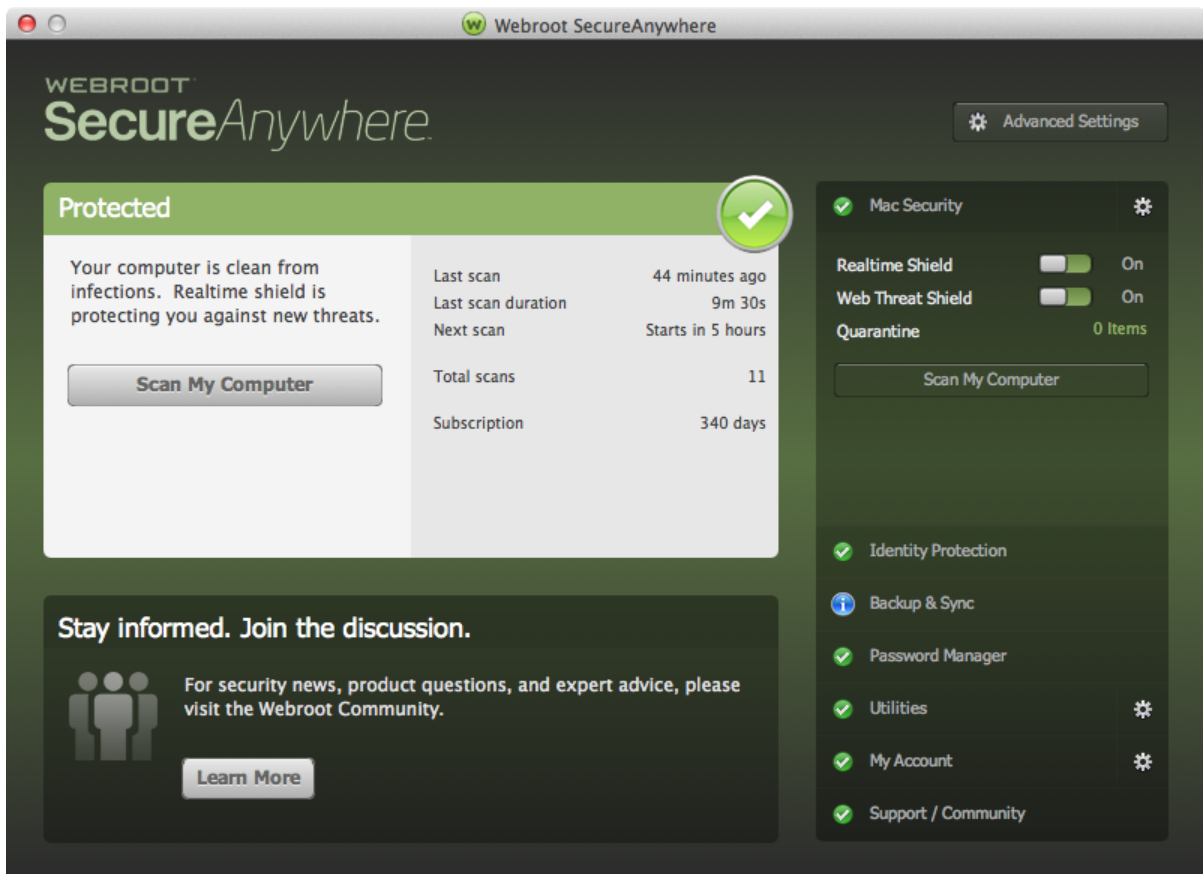
- **To select what files you want erased** — [Changing System Optimizer Settings on page 148](#).
- **To specify how recoverable you want the erased files to be** — [Creating Secure Erase Settings on page 156](#)
- **To schedule system optimizer** — [Changing Scan and Optimization Schedules on page 29](#).

To run System Optimizer:

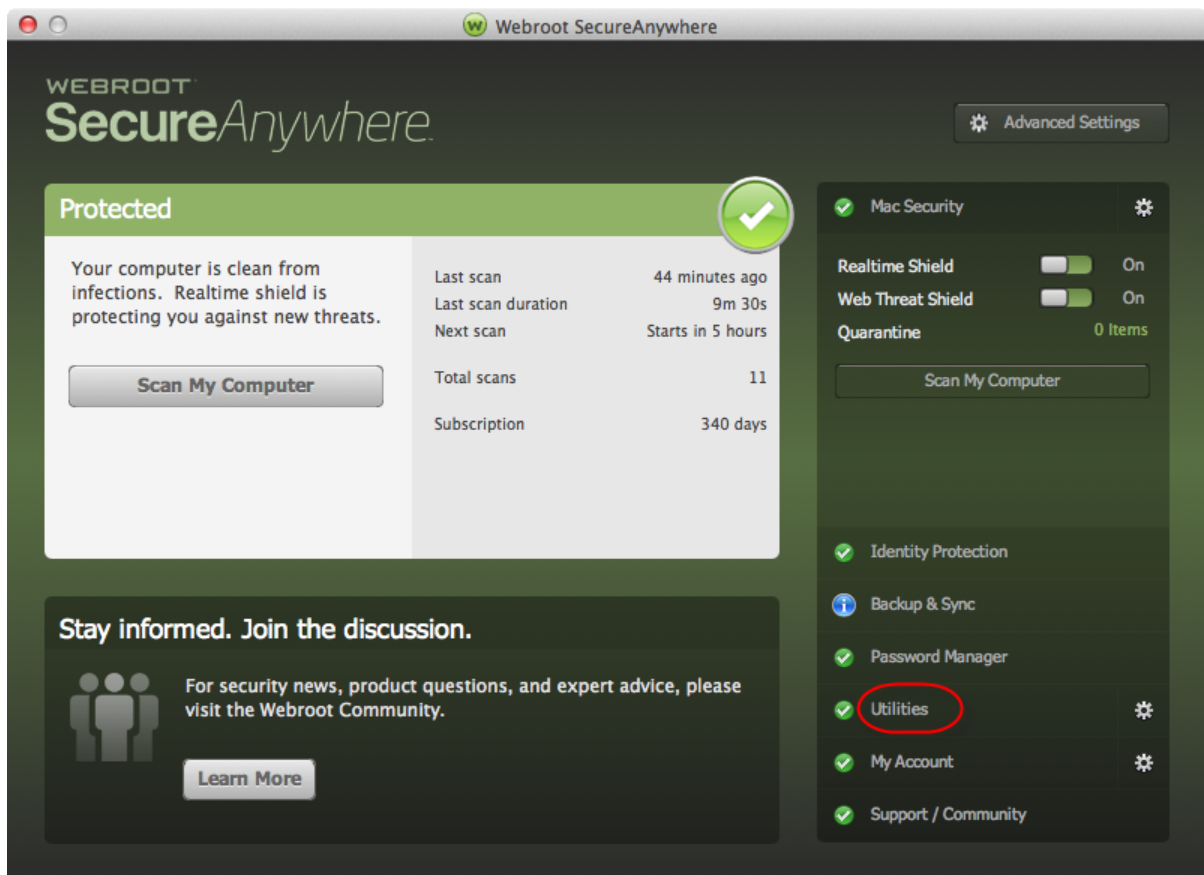
1. From the dock, click the **Webroot** icon.



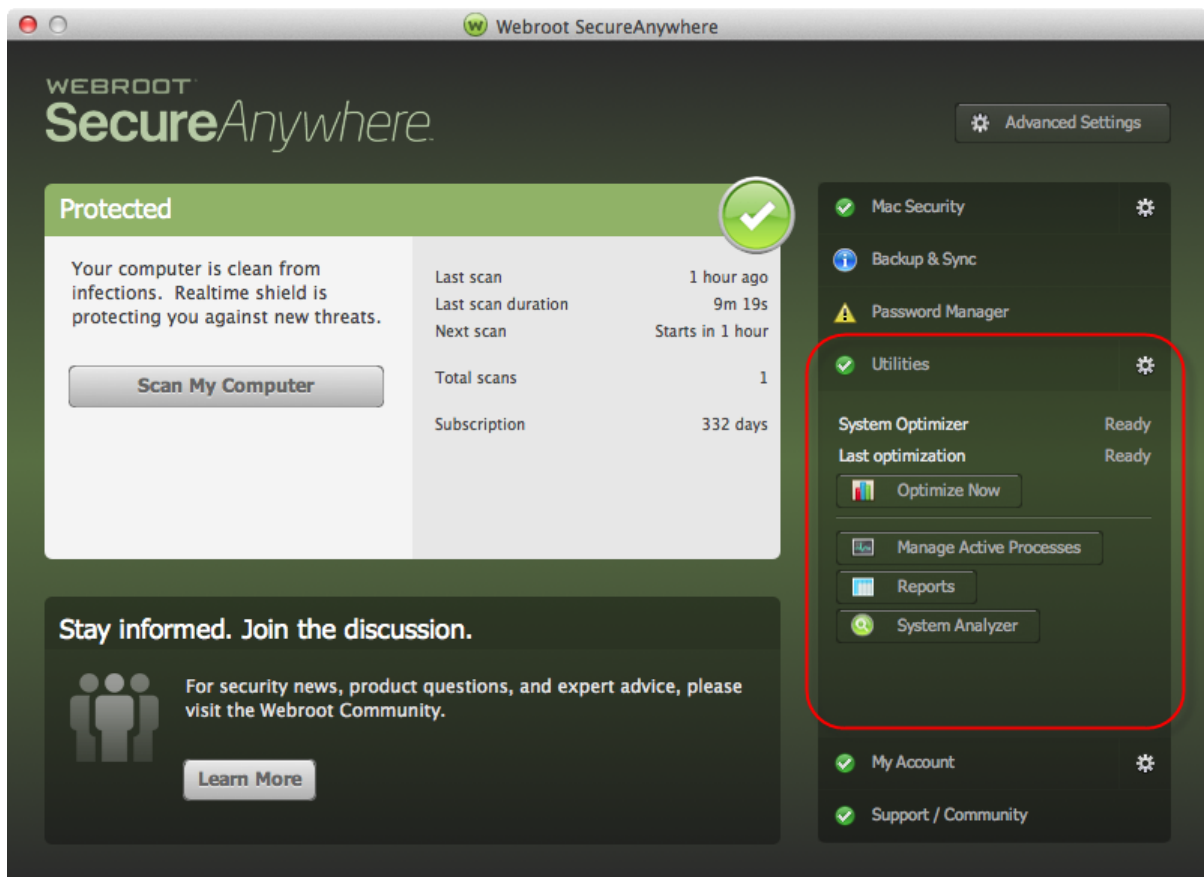
The main interface displays.



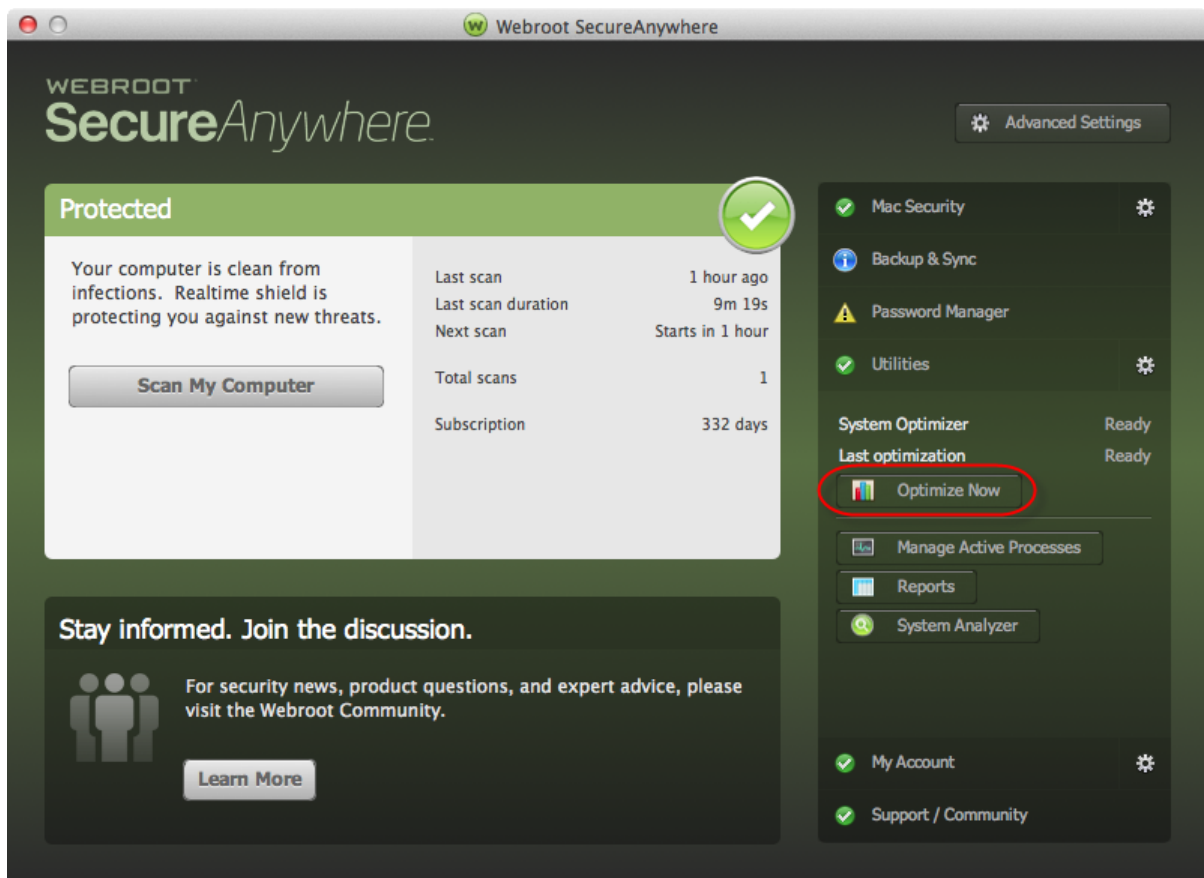
2. Click **Utilities** to expand the Utilities drop-down menu.



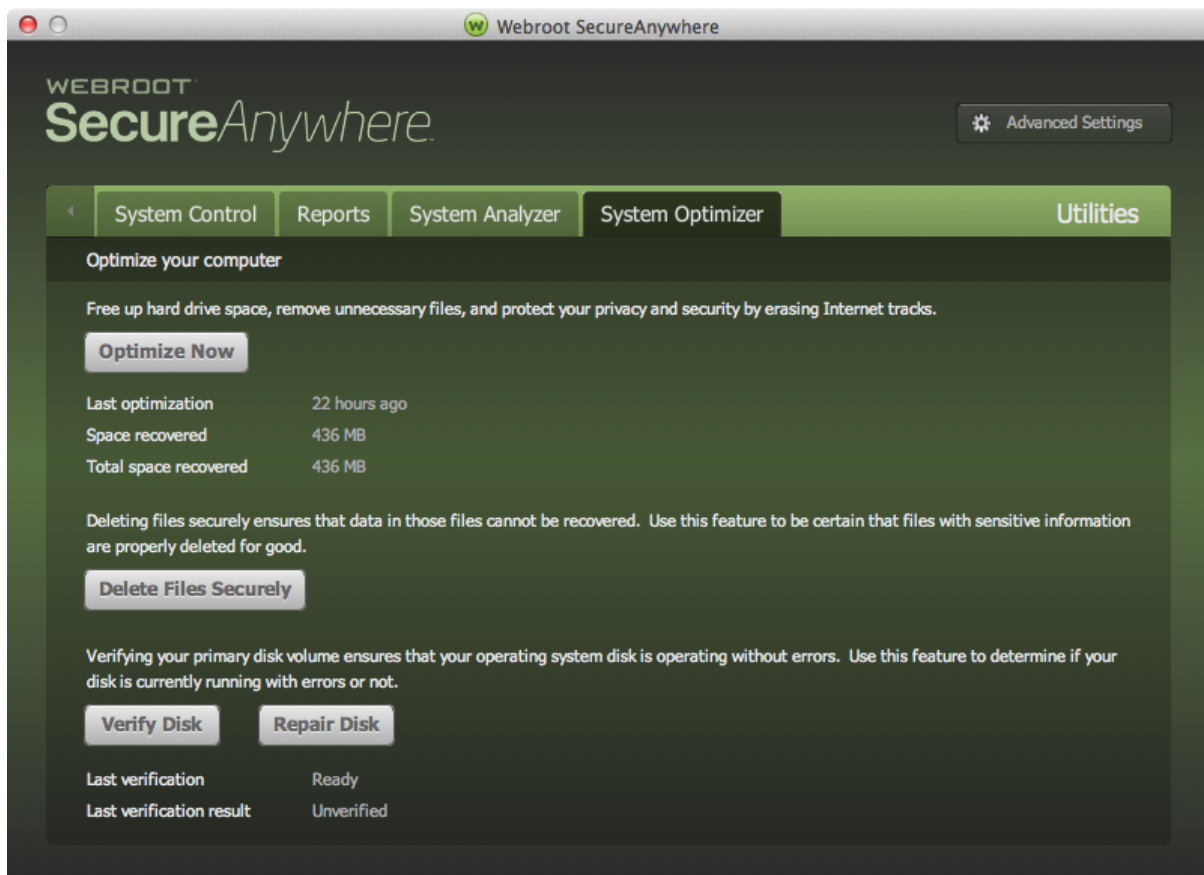
The Utilities menu expands.



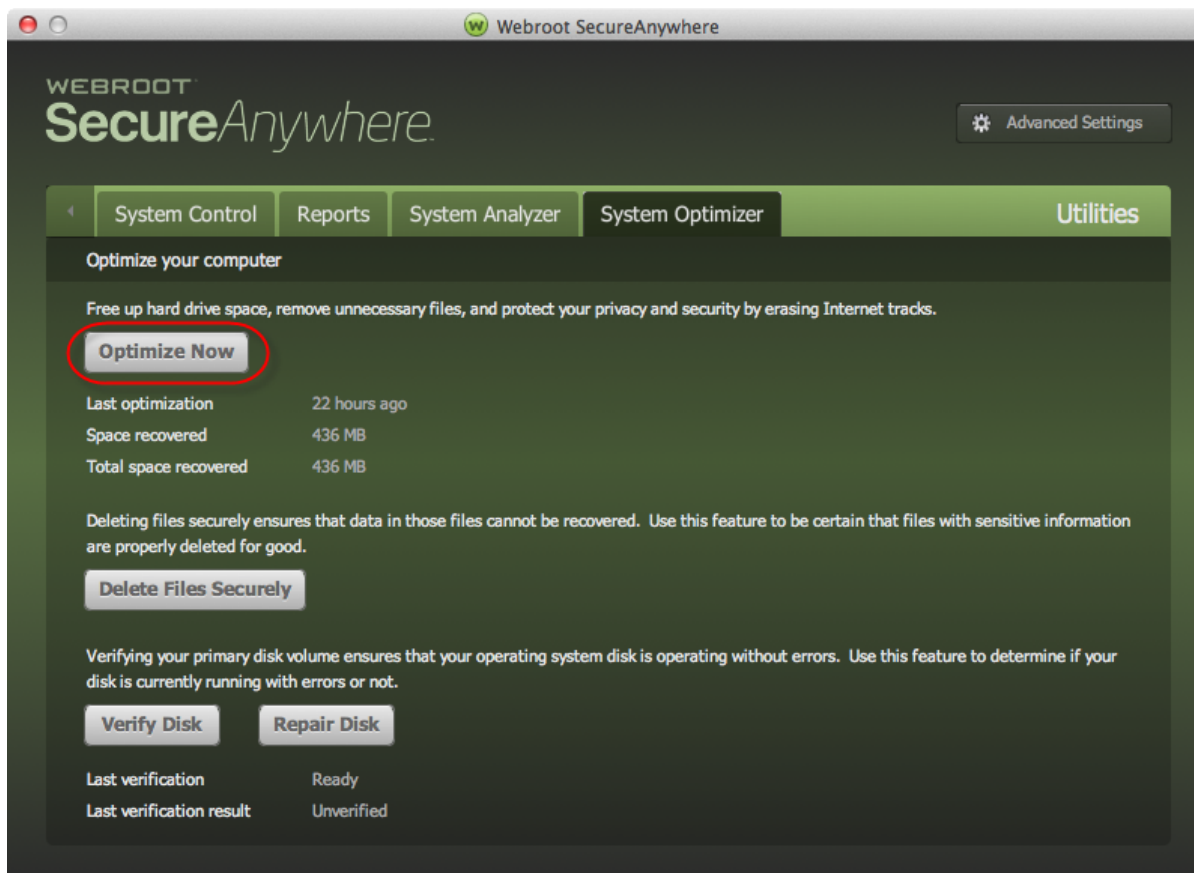
3. From the Utilities drop-down menu, click the **Optimize Now** button.



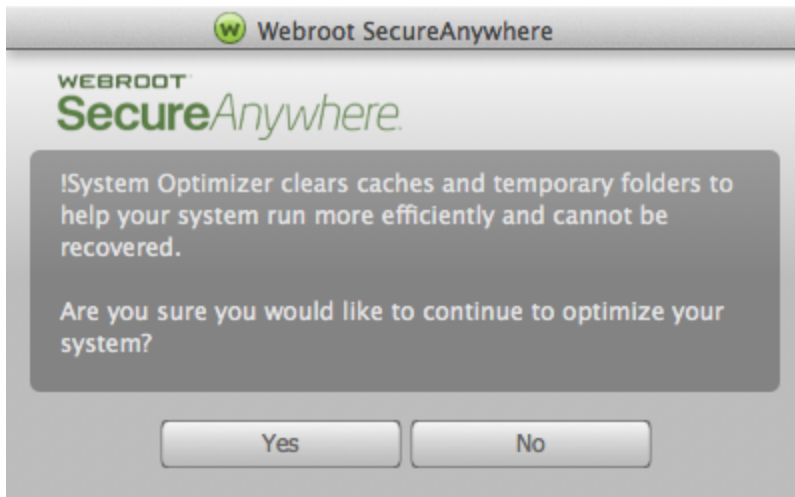
The System Optimizer tab displays.



4. Click the **Optimize Now** button.



The system displays a confirmation message.



5. To proceed, click the **Yes** button, otherwise, click the **No** button.
 6. When the optimizer completes, the system displays the following information:
 - How long ago the last optimization ran.
 - How much disk space was recovered in the last optimization.
 - How much total disk space has been recovered by system optimization.
 7. Optionally, you can do any of the following:
 - To confirm deletion of specific files — Click the **Delete Files Securely** button.
 - To verify that your operating system disk is operating without errors — Click the **Verify Disk** button.
 - To repair any broken files — Click the **Repair Disk** button.
 8. When you're done, click the **Back Arrow** to return to the main panel or click the **Close** button.
-

Changing System Optimizer Settings

You can customize what the System Optimizer cleans up from your system by enabling or disabling the settings. The options on the settings list may change depending on what browsers and other applications you currently have installed.

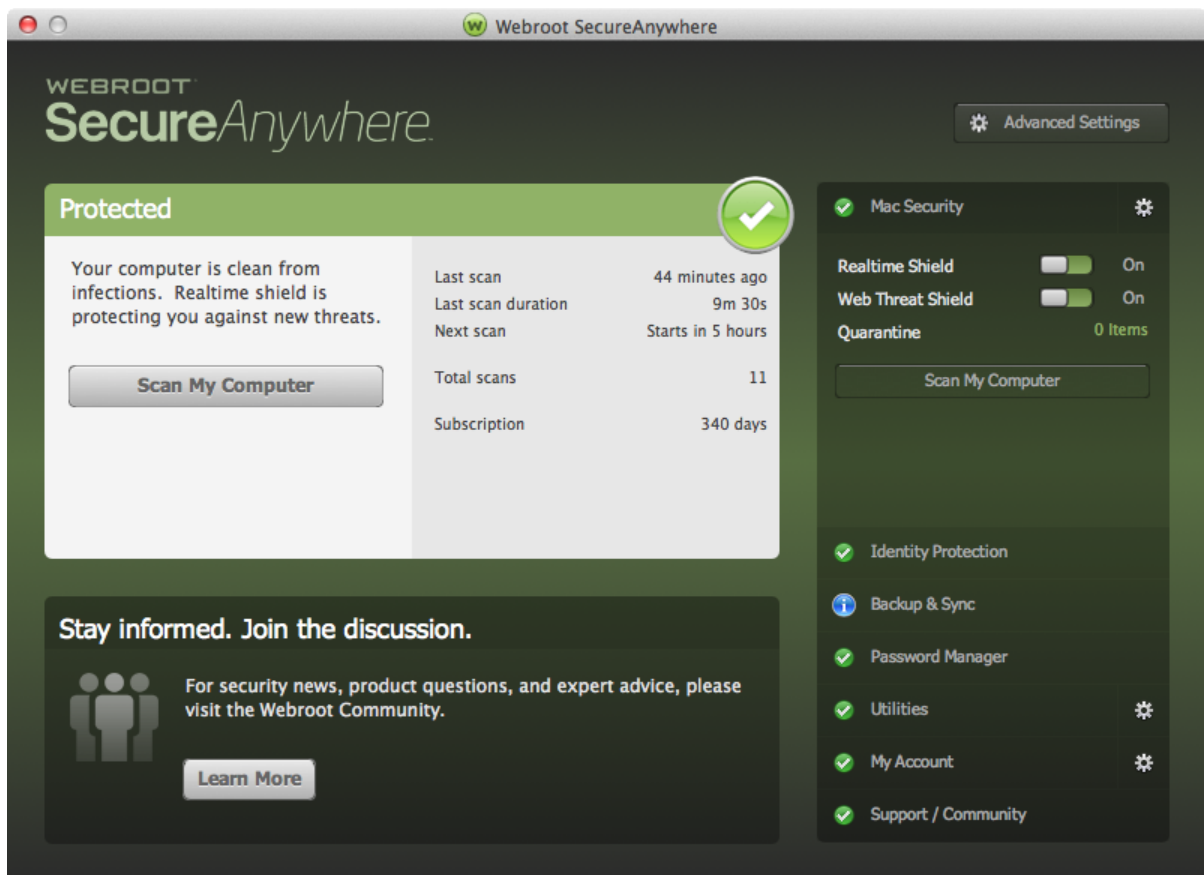
Note: System Optimizer for Mac is only available on the [consumer edition of Webroot SecureAnywhere](#).

To change System Optimizer settings:

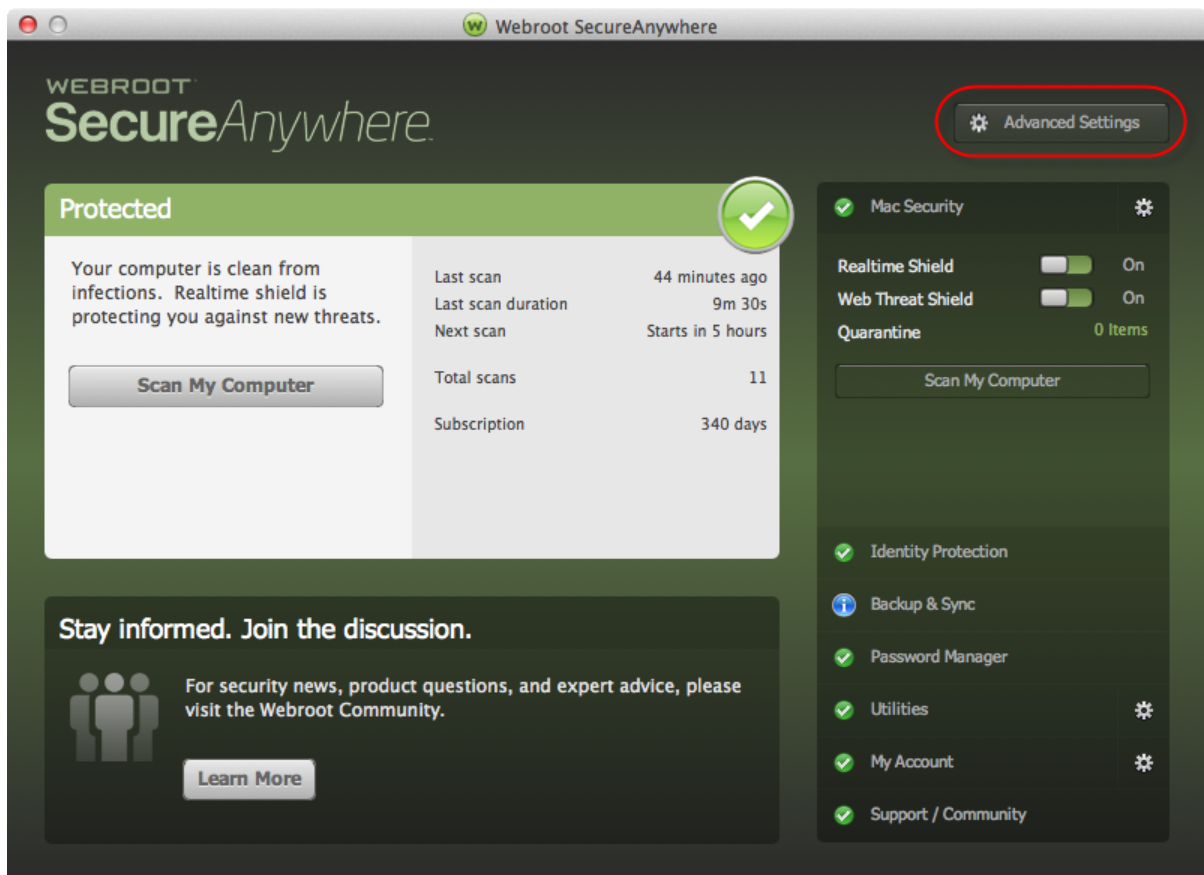
1. From the dock, click the **Webroot** icon.



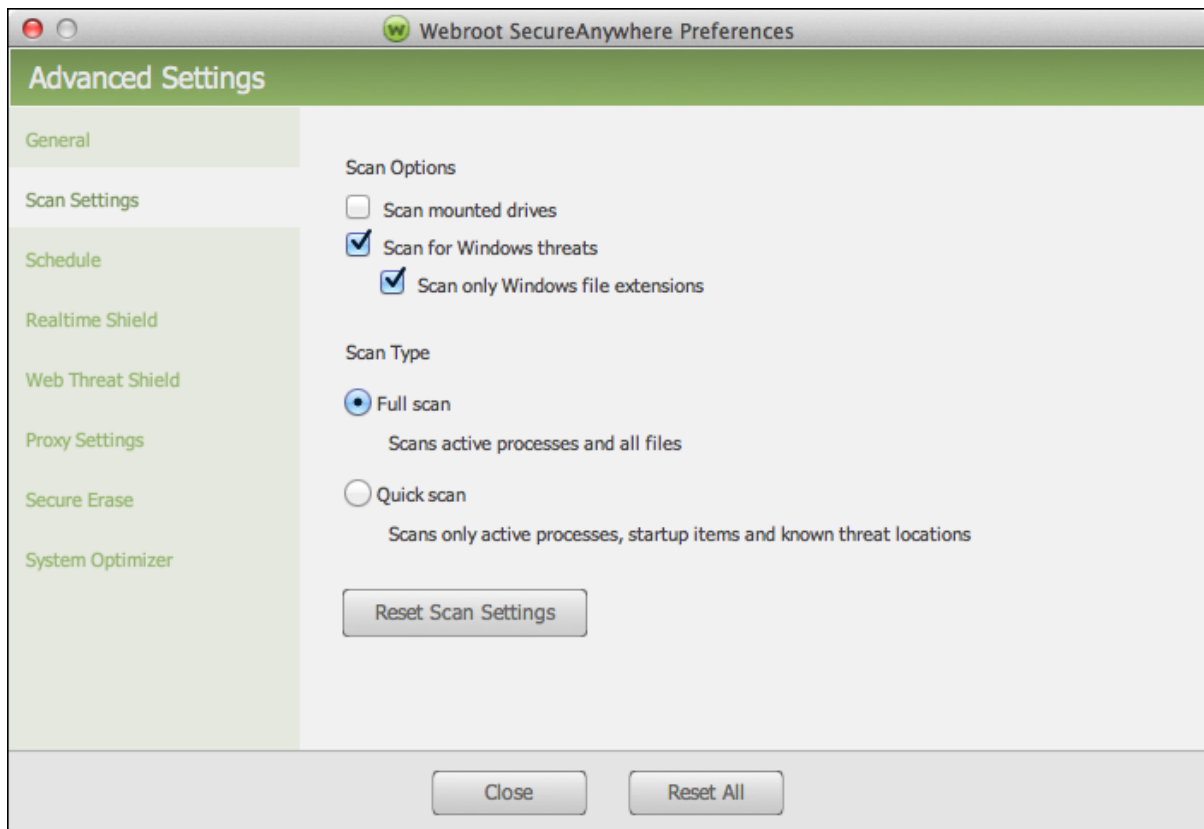
The main interface displays.



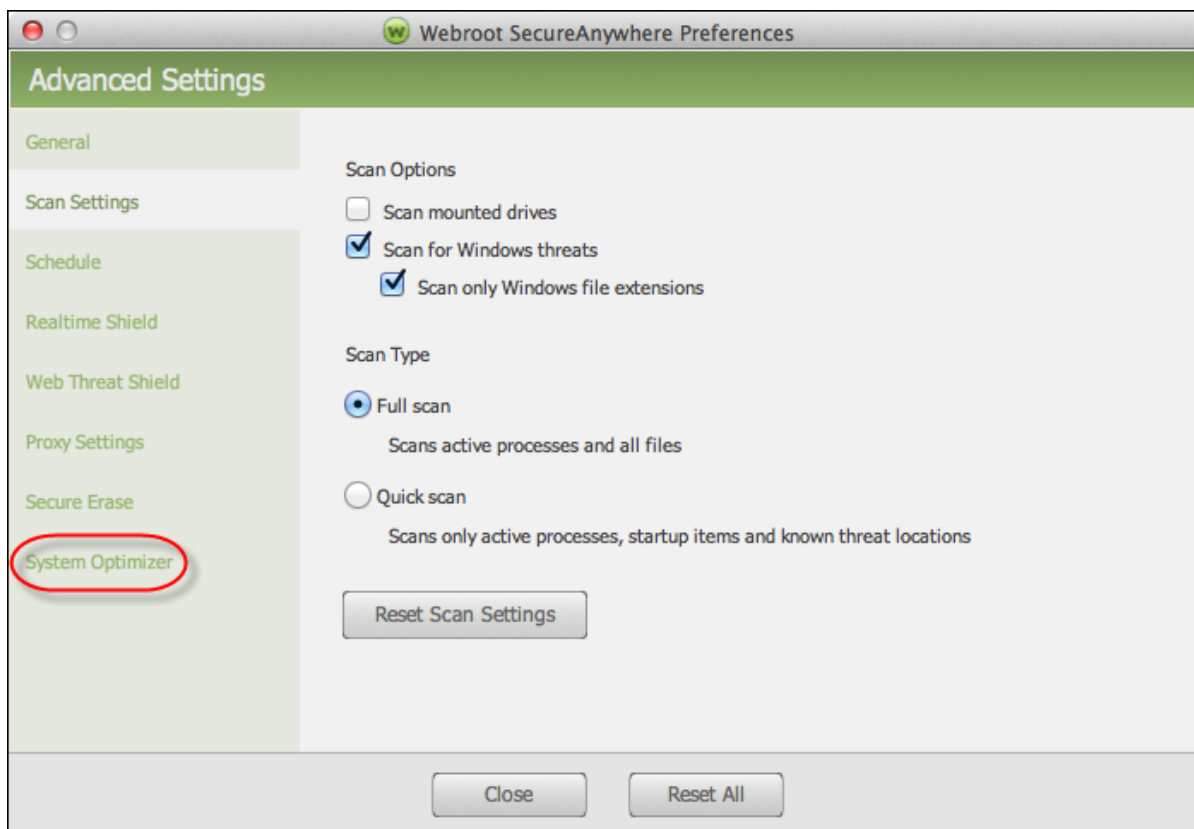
2. Click the **Advanced Settings** button.



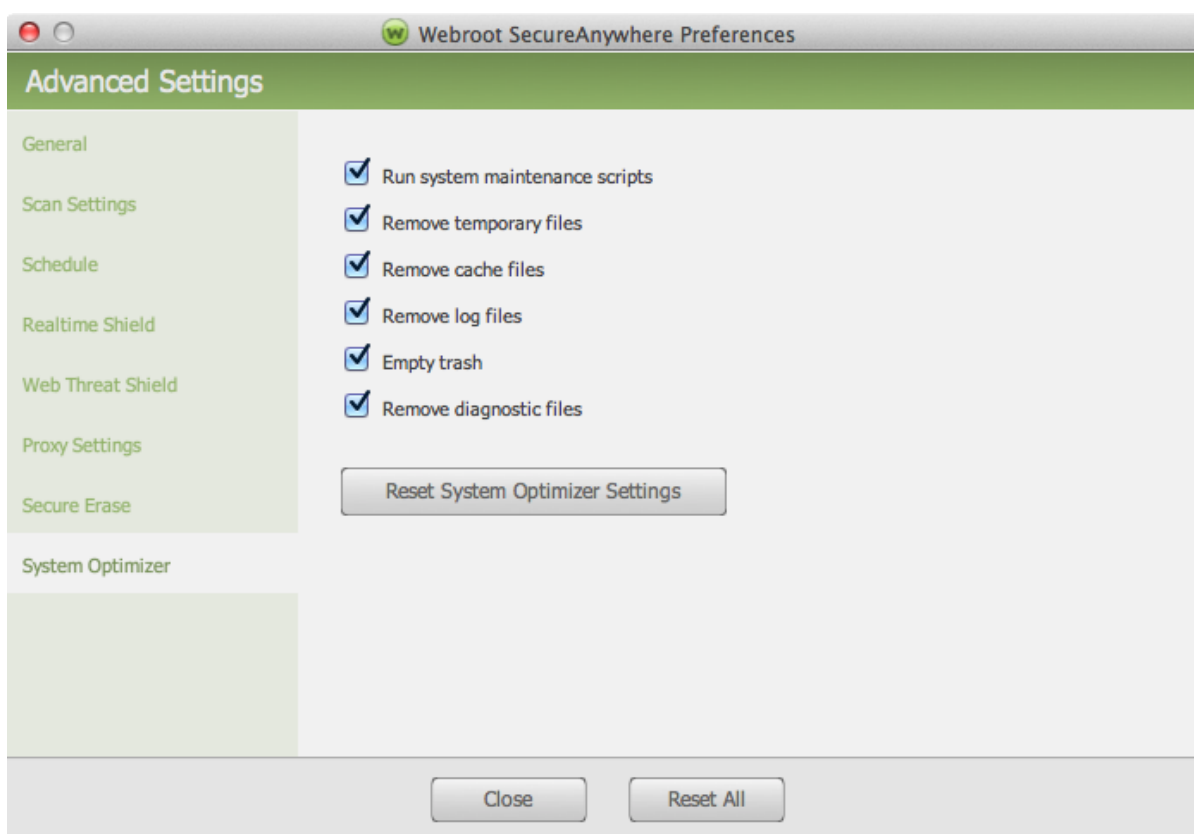
The Advanced Settings window displays.



3. In the left pane, select **System Optimizer**.



The System Optimizer panel displays.



4. Select or deselect any of the options, described in the following table:

SETTING	DESCRIPTION
Run system maintenance scripts	<p>Runs system maintenance scripts to clean up a variety of System logs and temporary files. By default, these are executed between 03:15 and 05:30 hours local time, depending on the script.</p> <p>For more information, see Running the Mac OS X Maintenance Scripts.</p>
Remove temporary files	<p>Deletes all files and folders in the system temporary folder, but not files that are in use by an open program. This folder is usually located at:</p> <p><code>/tmp</code></p> <p>You should not put any files here that you need to keep. The files in this folder can consume a lot of space on your hard drive.</p>
Remove cache files	<p>Removes any files that have been cached.</p> <p>The Cache is located at:</p> <p><code>/Users//Library/Cache</code></p>
Remove log files	<p>Removes any logs on your system.</p> <p>The logs are located at:</p> <p><code>/private/var/log/asl</code></p>

SETTING	DESCRIPTION
Empty trash	<p>Removes all files from your Trash, which contains files you have deleted using Windows Explorer.</p> <p>When you delete a file, it is stored in the Trash until you empty it. You should periodically empty the Trash to preserve valuable disk space on your computer.</p> <p>The Trash is located at:</p> <p><code>/Users//Trash</code></p>
Remove diagnostic files	<p>Removes any files that have been created when diagnostic reports have been run.</p> <p>Theses files are located at:</p> <p><code>/Users//Library/Logs/DiagnosticReports</code></p>

5. Do any of the following:
 - If you selected or deselected any of the checkboxes, click the **Reset System Optimizer Settings** button.
 - To leave the Settings pane without making changes, click the **Close** button.
 - To reset to default settings, click the **Reset All** button.
-

Creating Secure Erase Settings

The Secure Erase feature allows you to specify how thoroughly the System Optimizer deletes files when it runs.

Normally, when you delete a file, you are moving it to the Trash, where anyone can access it. Even when you empty the Trash, you are not actually deleting the files; you are only deleting the operating system's pointers to the files. The actual data still exists on your hard drive and, unless it is overwritten by other data, it could be resurrected using special recovery tools.

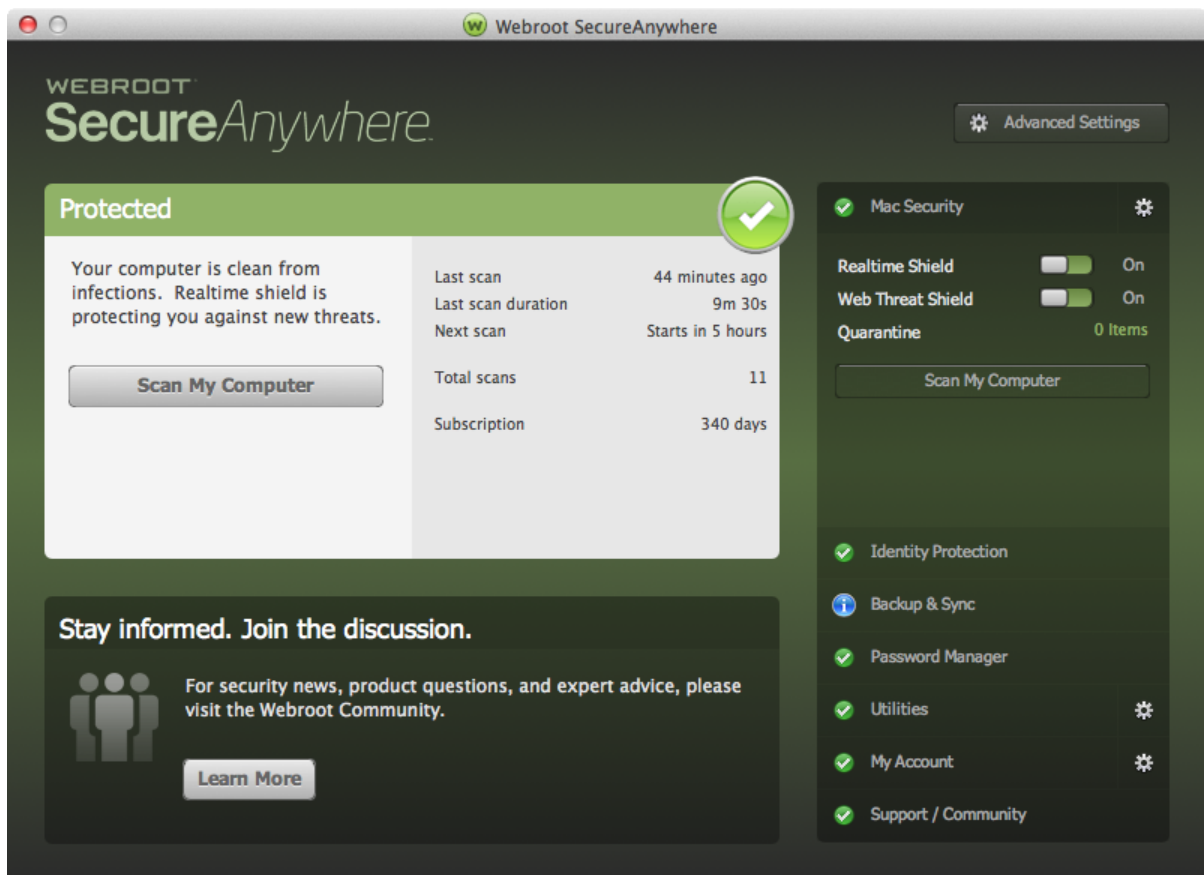
Note: System Optimizer for Mac is only available on the [consumer edition of Webroot SecureAnywhere](#).

To create Secure Erase settings:

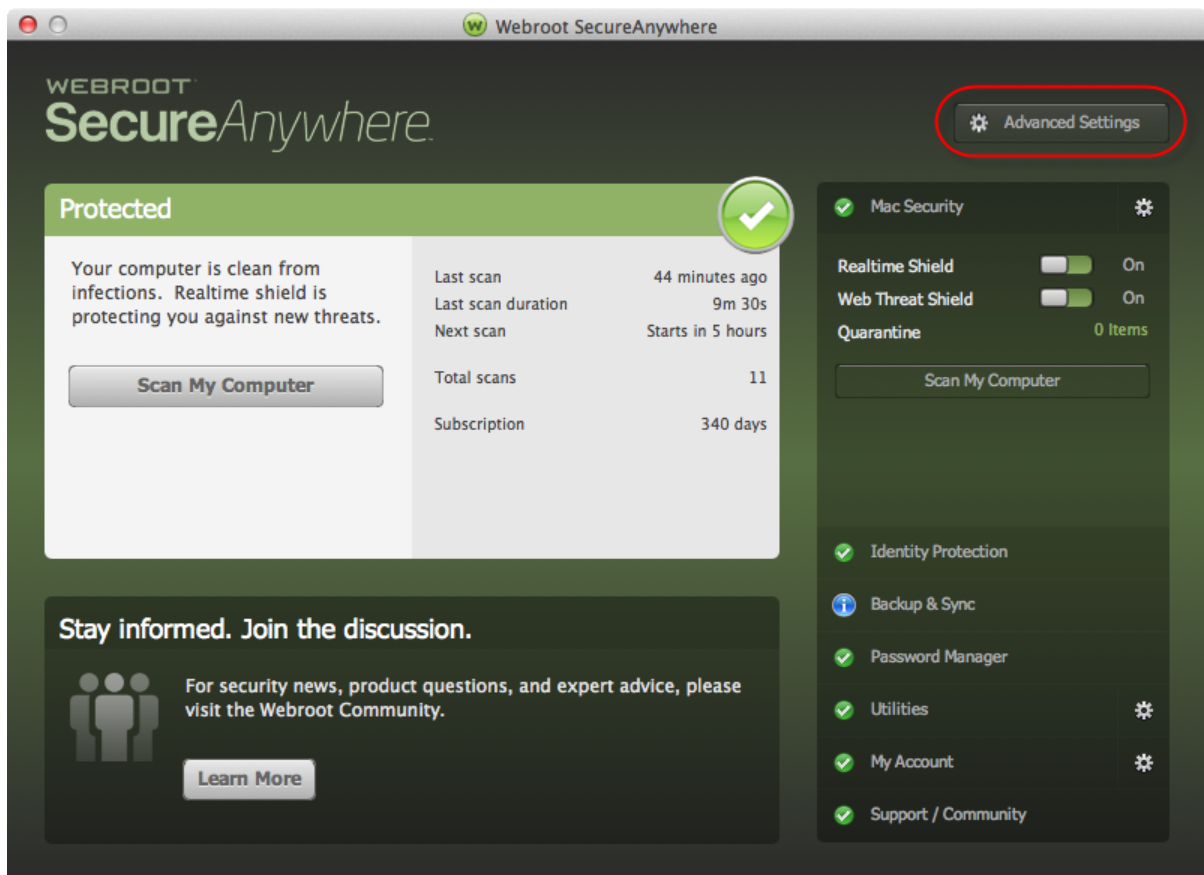
1. From the dock, click the **Webroot** icon.



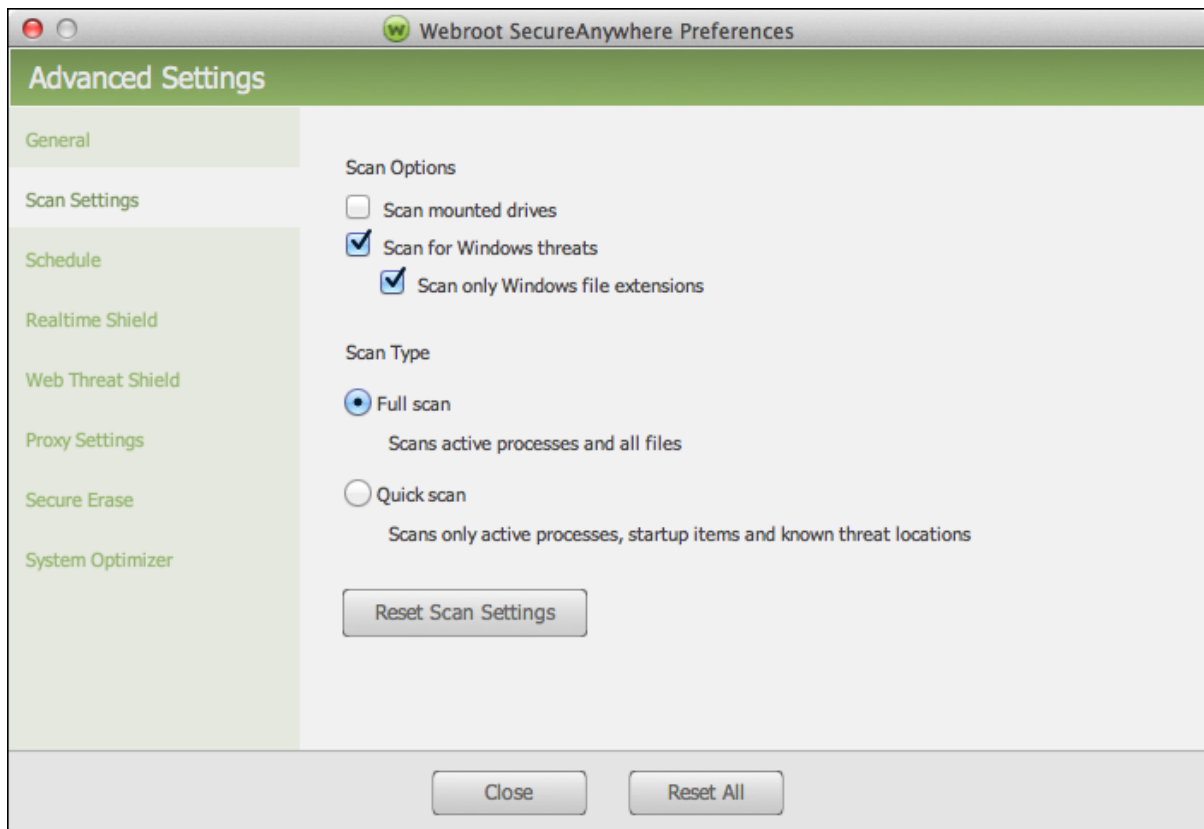
The main interface displays.



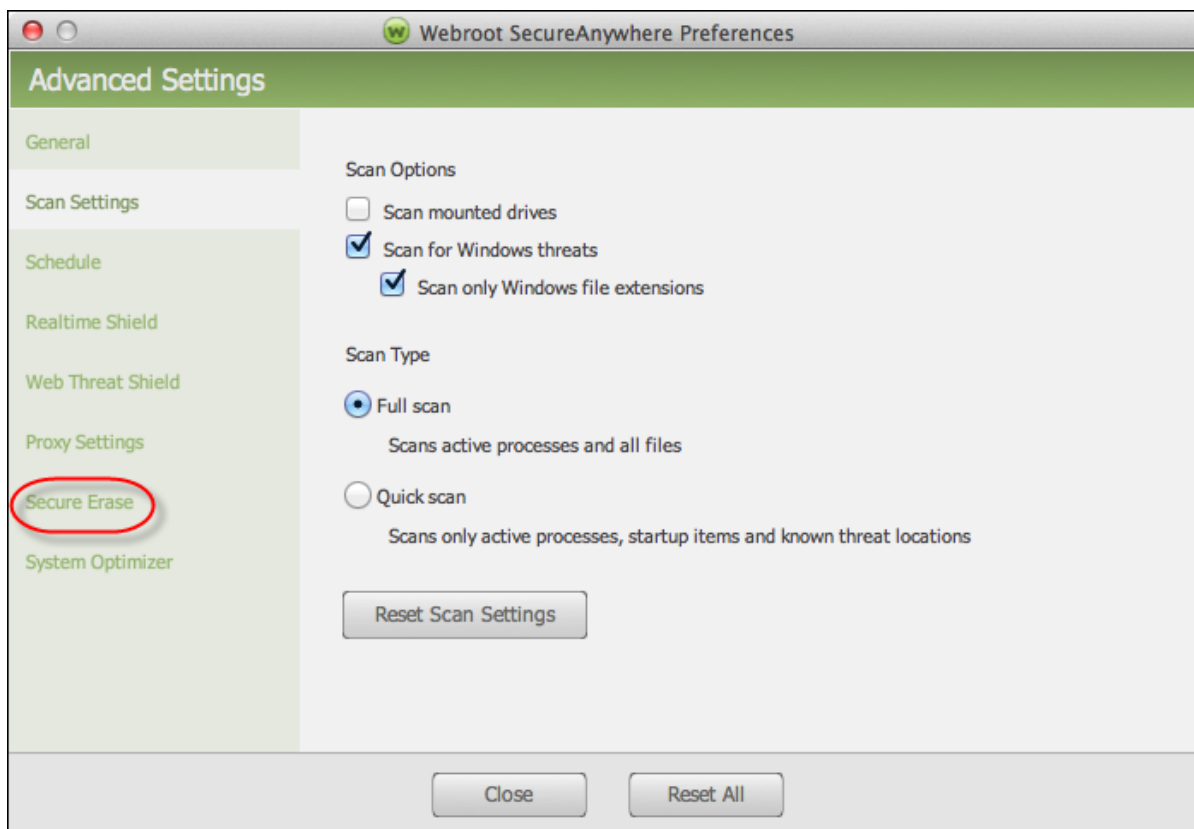
2. In the upper right corner, click the **Advanced Settings** button.



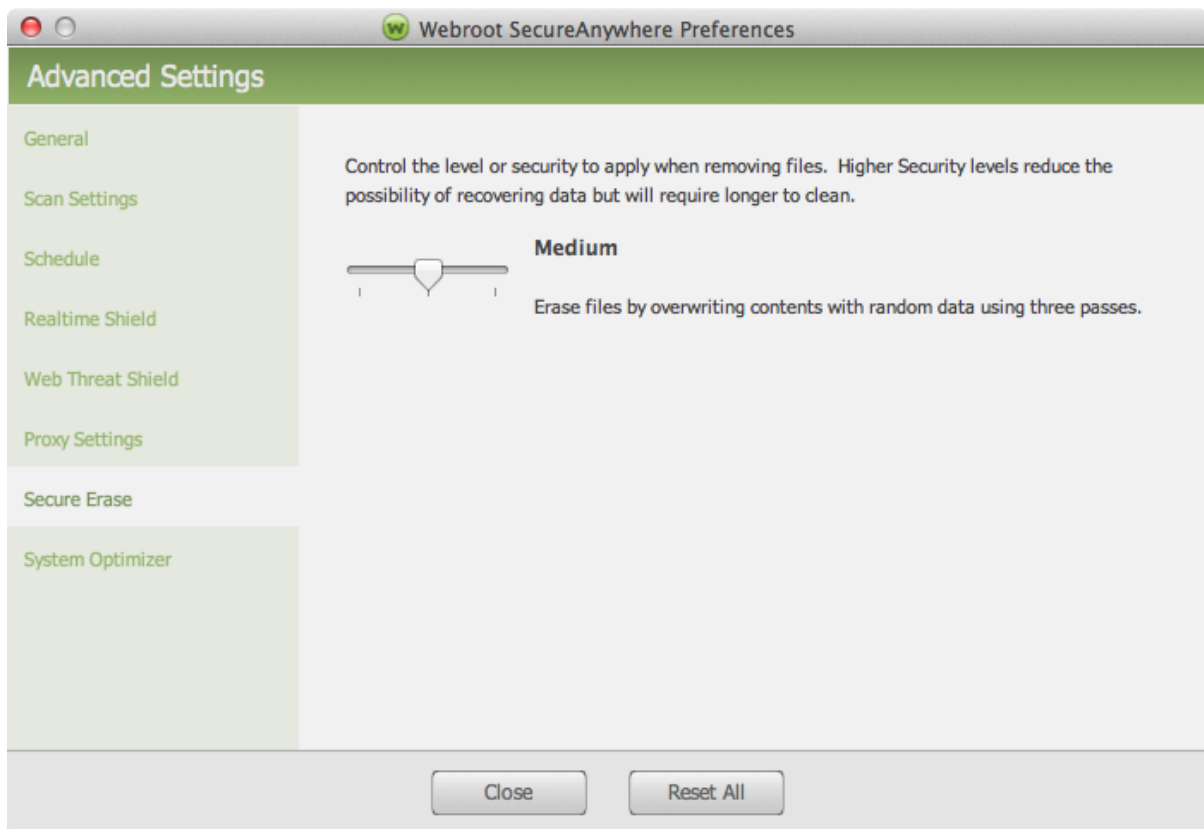
The Advanced Settings window displays.



3. In the left pane, select **Secure Erase**.



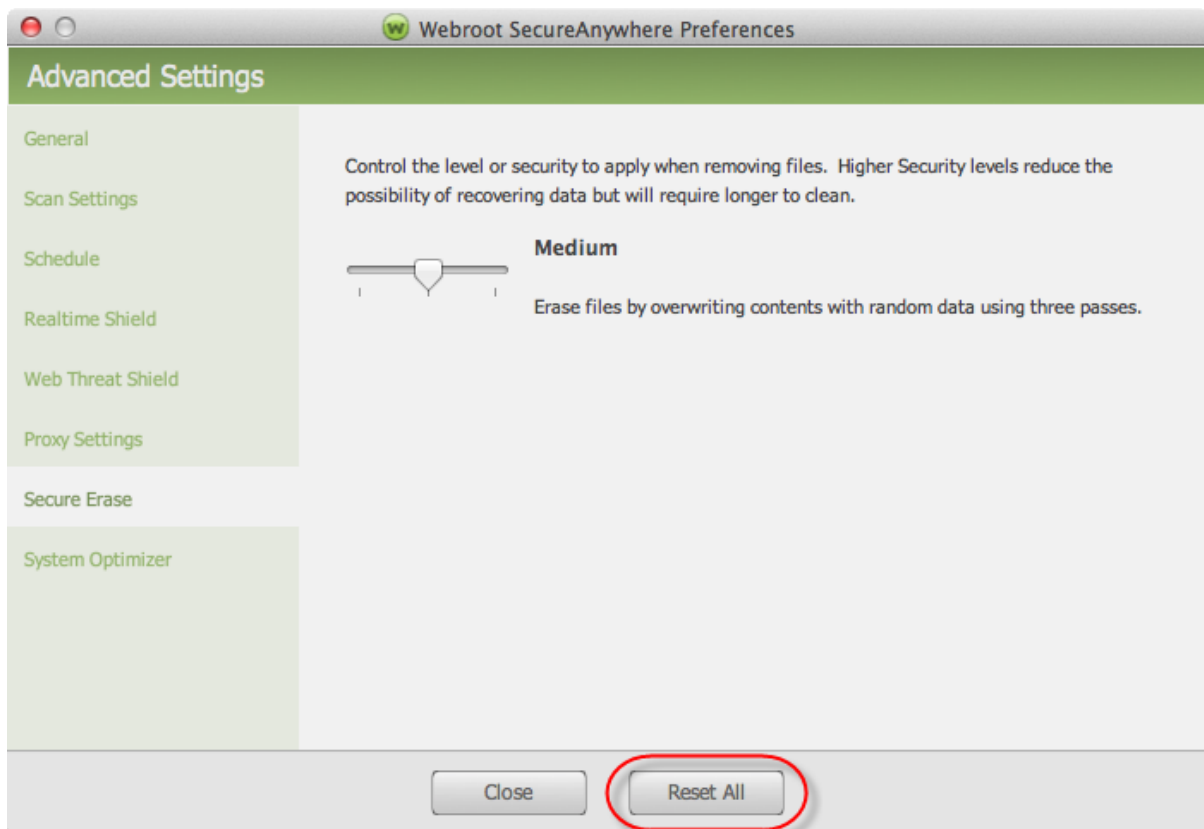
The Secure Erase pane displays.



4. Move the slider to select any of the following options:
- **Normal** — Deletes the files without overwriting them.
 - **Medium** — Overwrites the data with three passes.
 - **Maximum** — Overwrites the data with seven passes.

Note: These settings may have a significant impact on the amount of time it takes to run a system optimization.

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



Chapter 11: Managing Preferences

To manage preferences, see the following topics:

Setting General Preferences	164
Defining Proxy Server Settings	170

Setting General Preferences

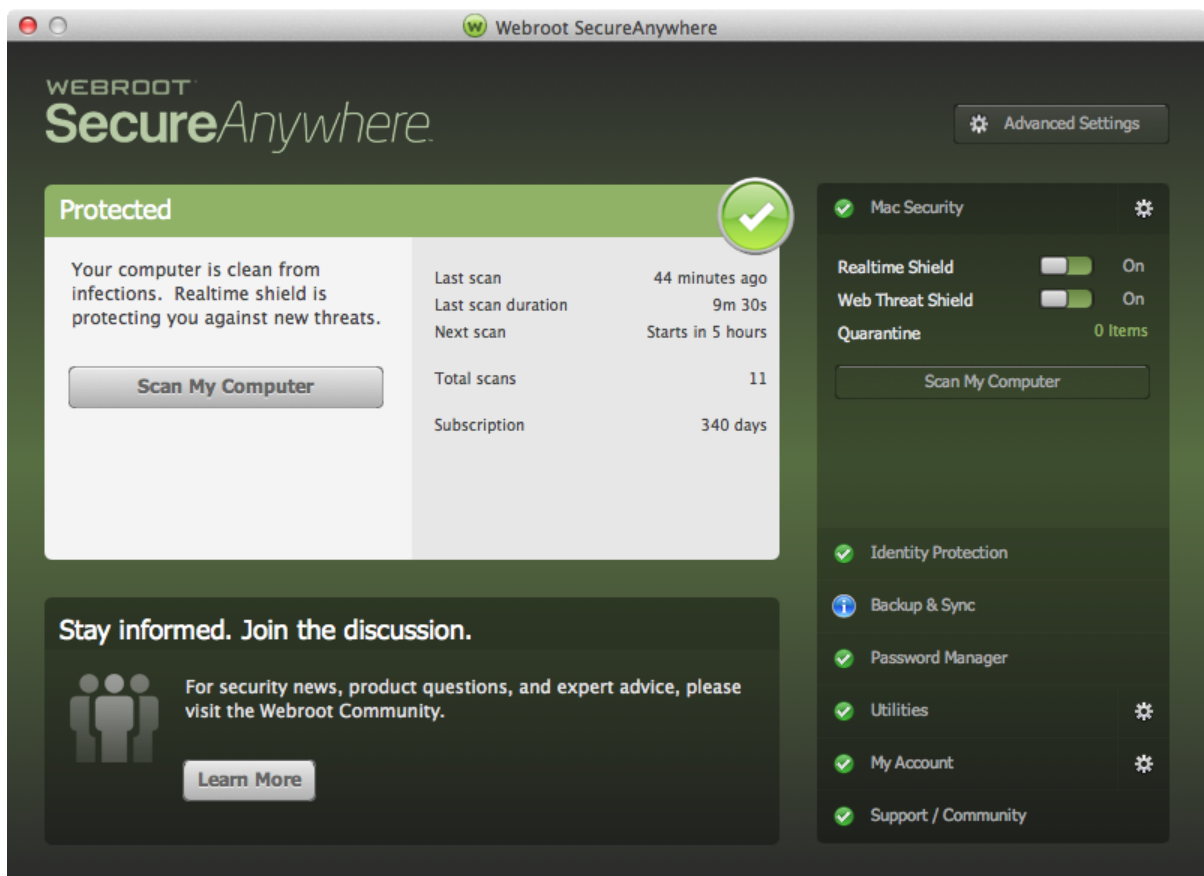
You can change the behavior of the program in General Preferences, using this procedure.

To change general preferences:

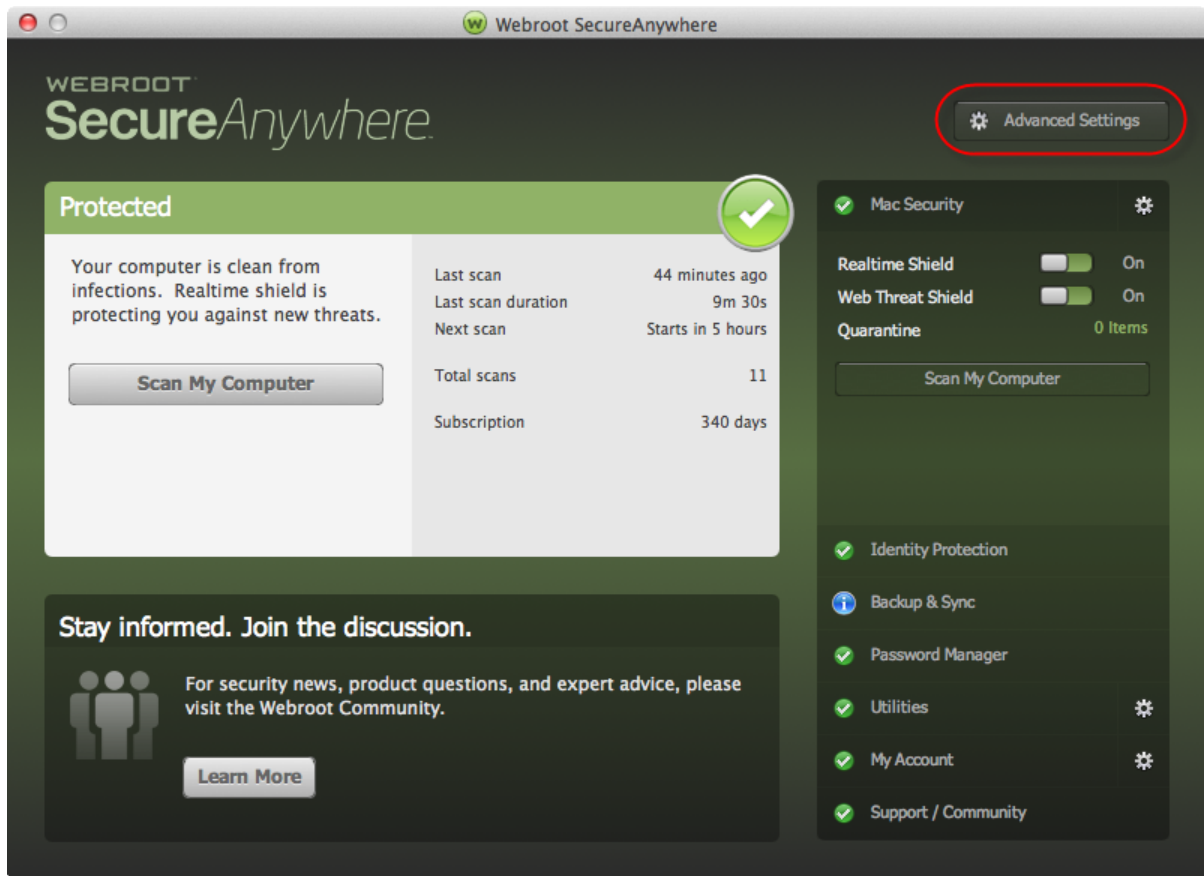
1. From the dock, click the **Webroot** icon.



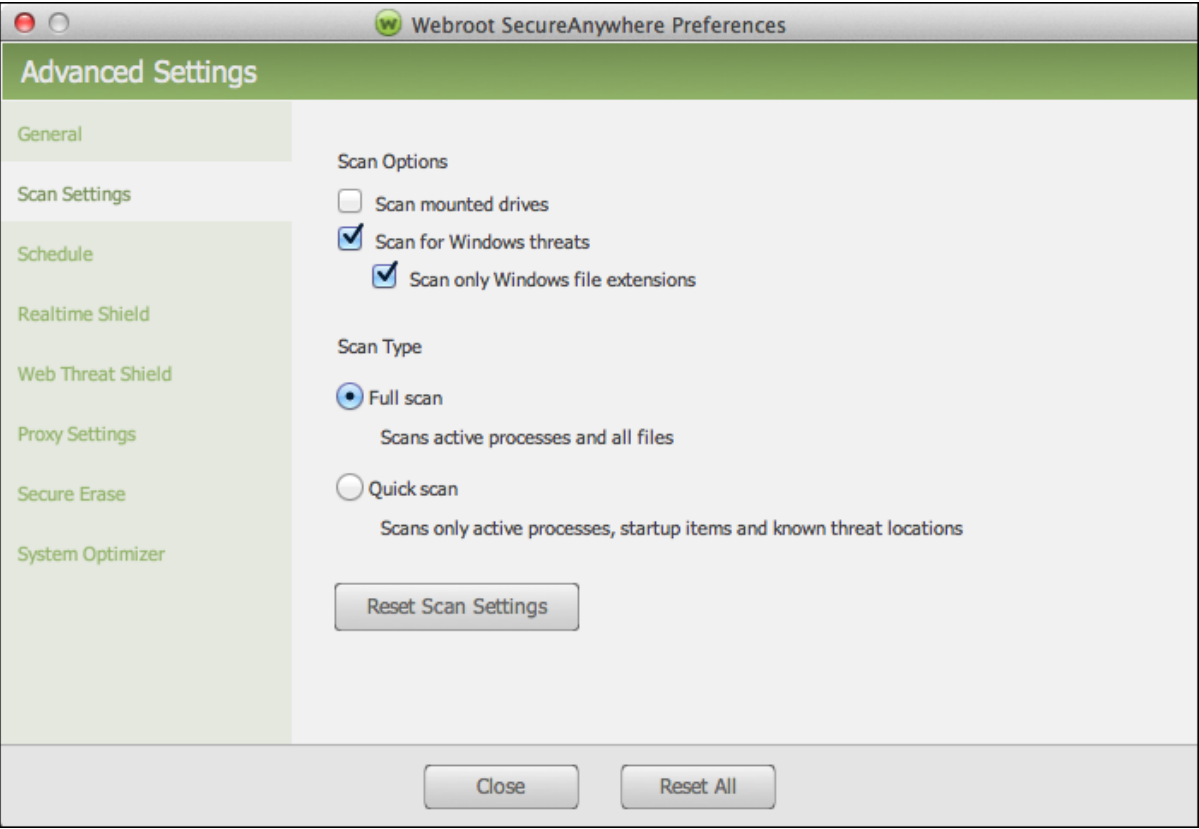
The main interface displays.



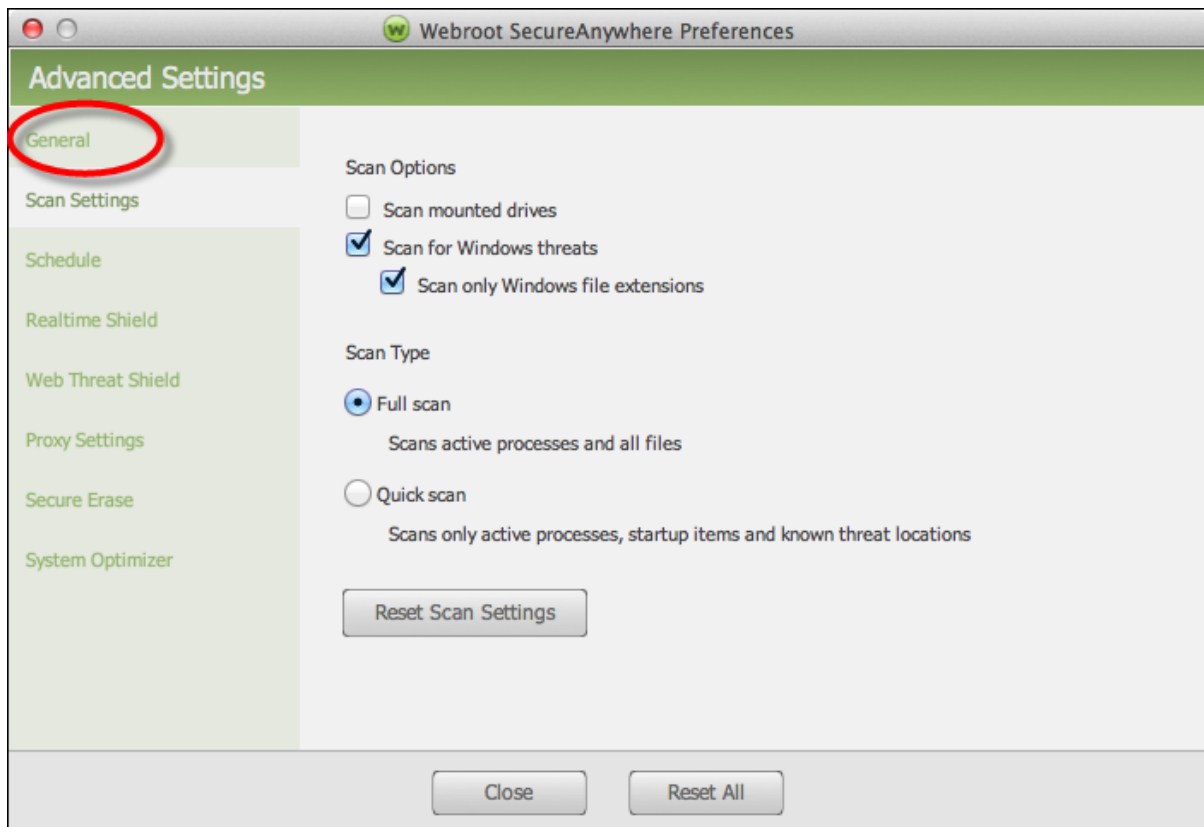
2. Click the **Advanced Settings** button.



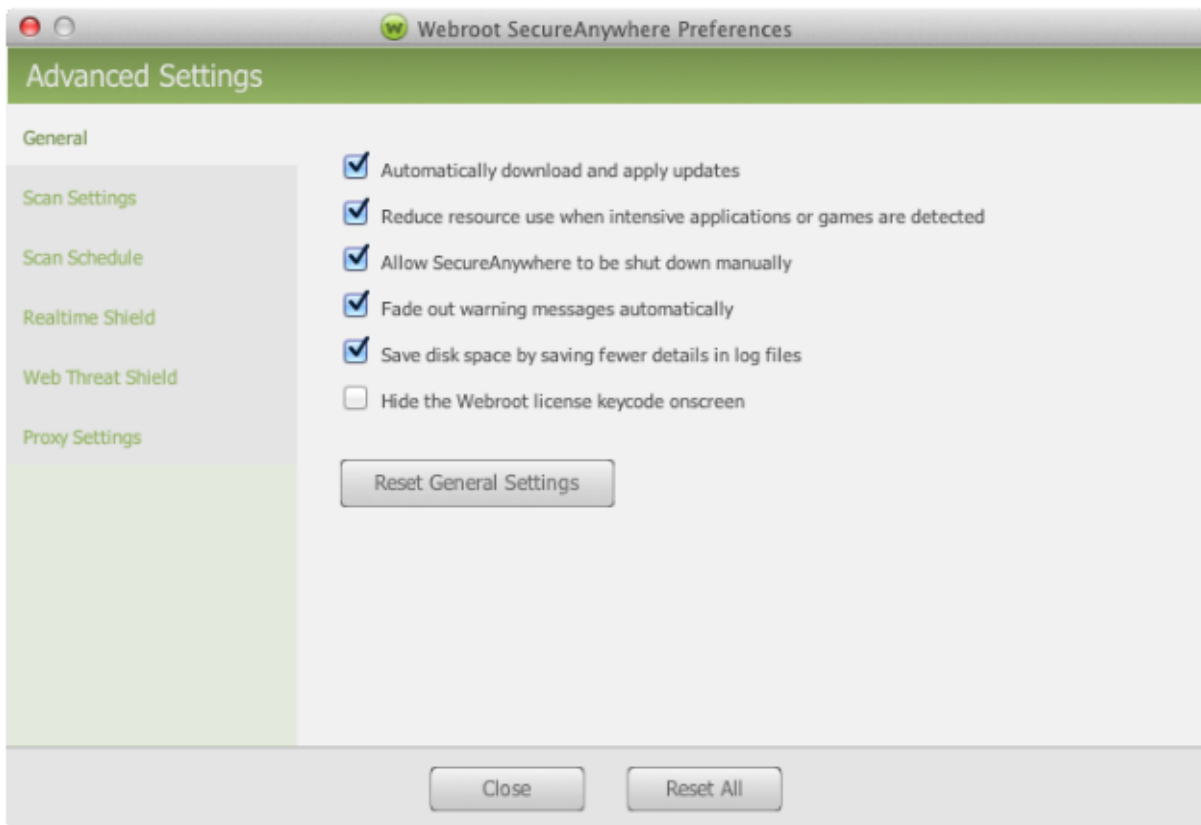
The Advanced Settings window displays.



3. In the left column, select **General**.



4. The General settings display.



5. Do one of the following:
 - To activate a setting, select the checkbox.
 - To deactivate a setting, deselect the checkbox.

FIELD	DESCRIPTION
Automatically download and apply updates	Downloads product updates automatically without alerting you.
Reduce resource use when intensive applications or games are detected	Suppresses SecureAnywhere functions while you are gaming, watching videos, or using other intensive applications.
Allow Webroot 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.
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.
Save disk space by saving fewer details in log files	Saves disk resources by saving only the last four log items.
Hide the Webroot license keycode on screen	Blocks your license keycode from displaying on the My Account panel

6. When you're done, click **Close**.

- To return to the recommended settings, click **Reset General Settings**.
- To return to the recommended settings for all settings, click **Reset All**.

Defining Proxy Server Settings

If you use a proxy server to connect to the Internet, you must define the proxy connection data; otherwise, Webroot cannot send updates to your computer.

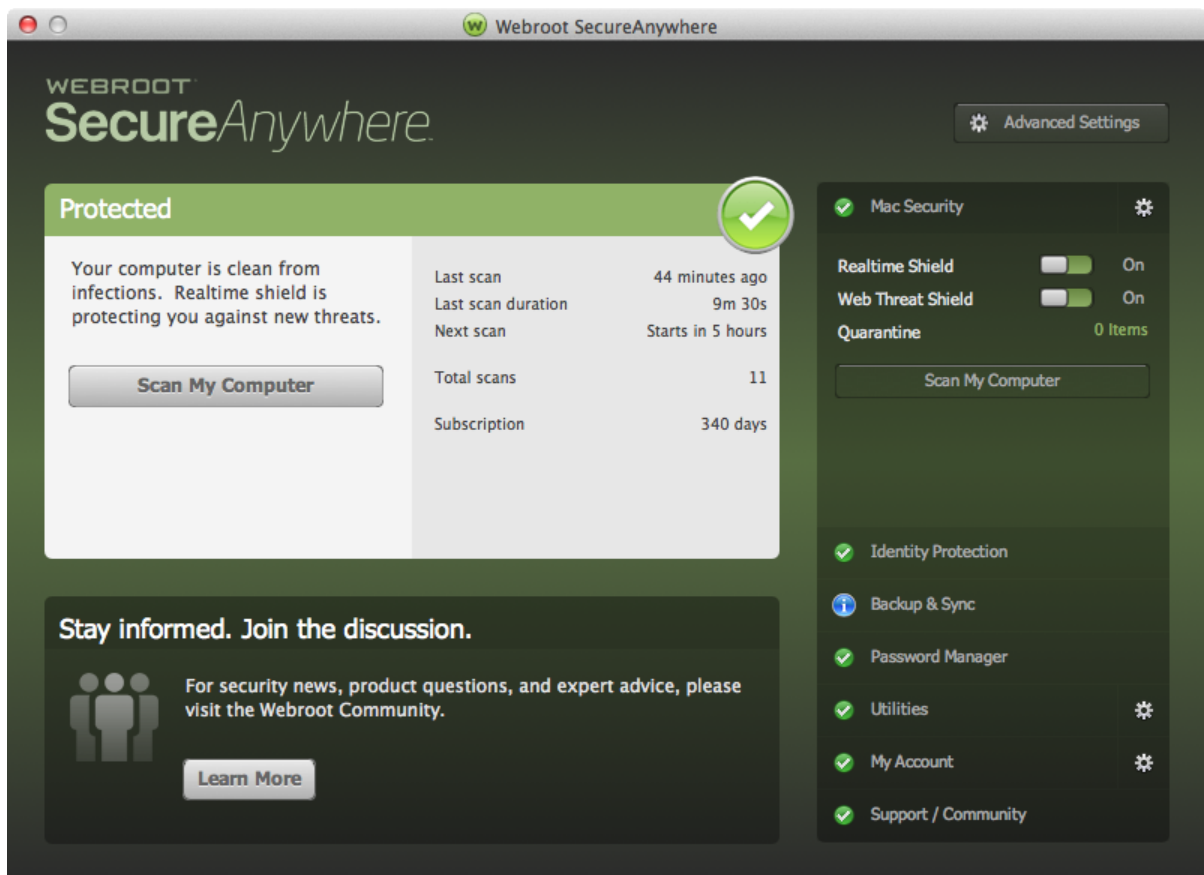
A proxy server is a computer system or router that acts as a relay between your computer and another server. For more information about your proxy environment, contact your proxy server's administrator.

To define proxy server settings:

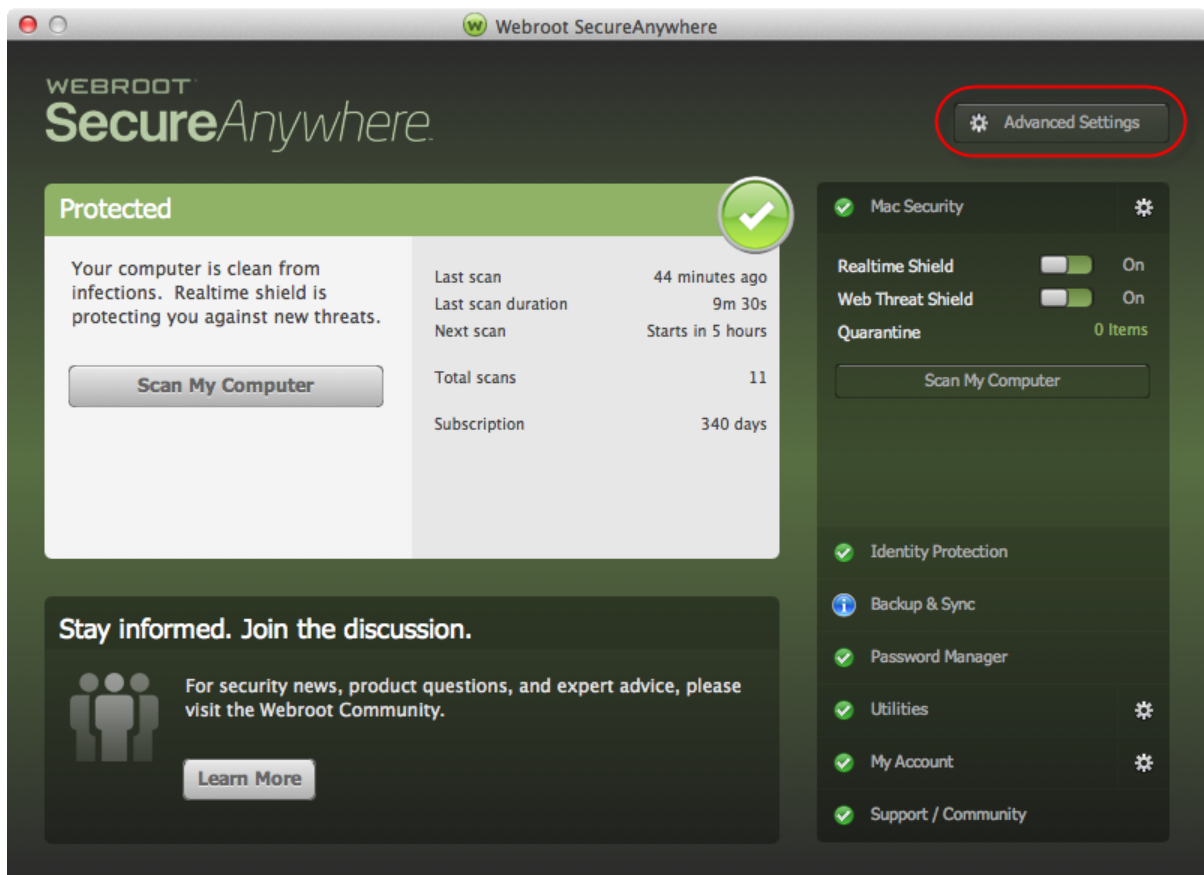
1. From the dock, click the **Webroot** icon.



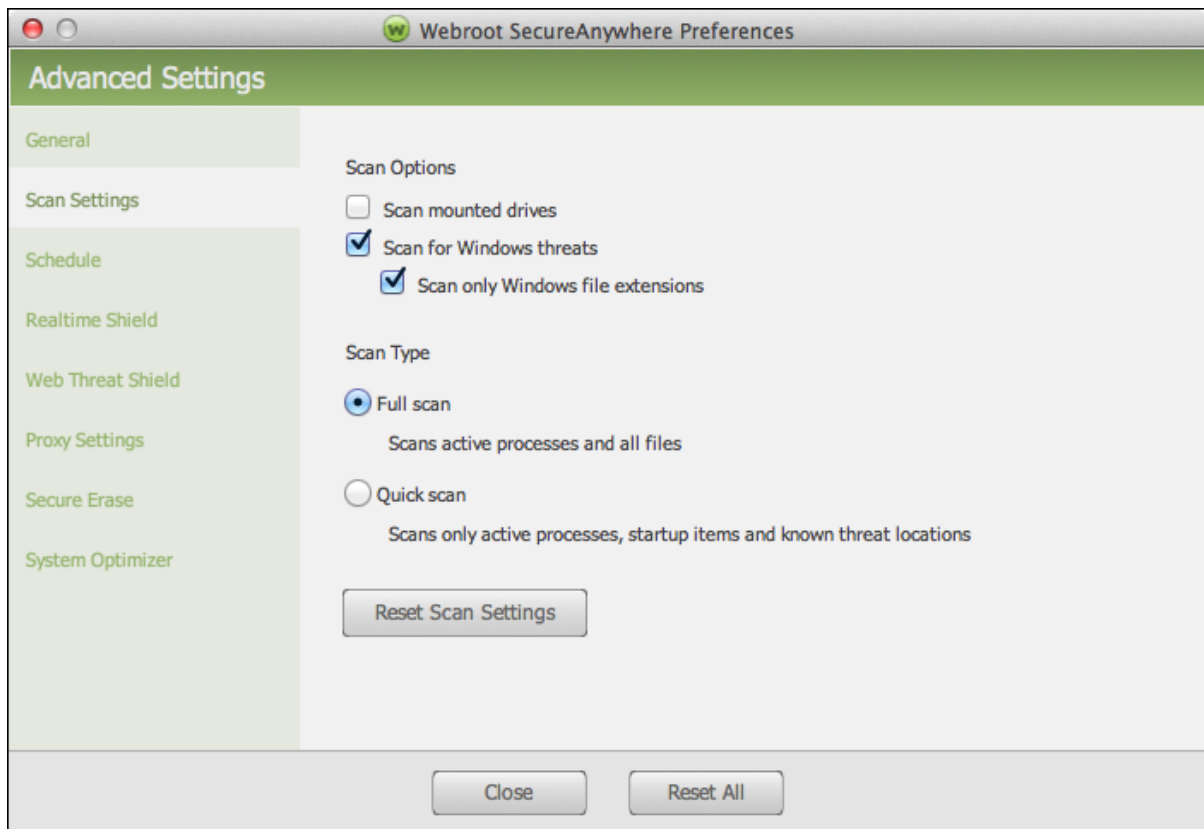
The main interface displays.



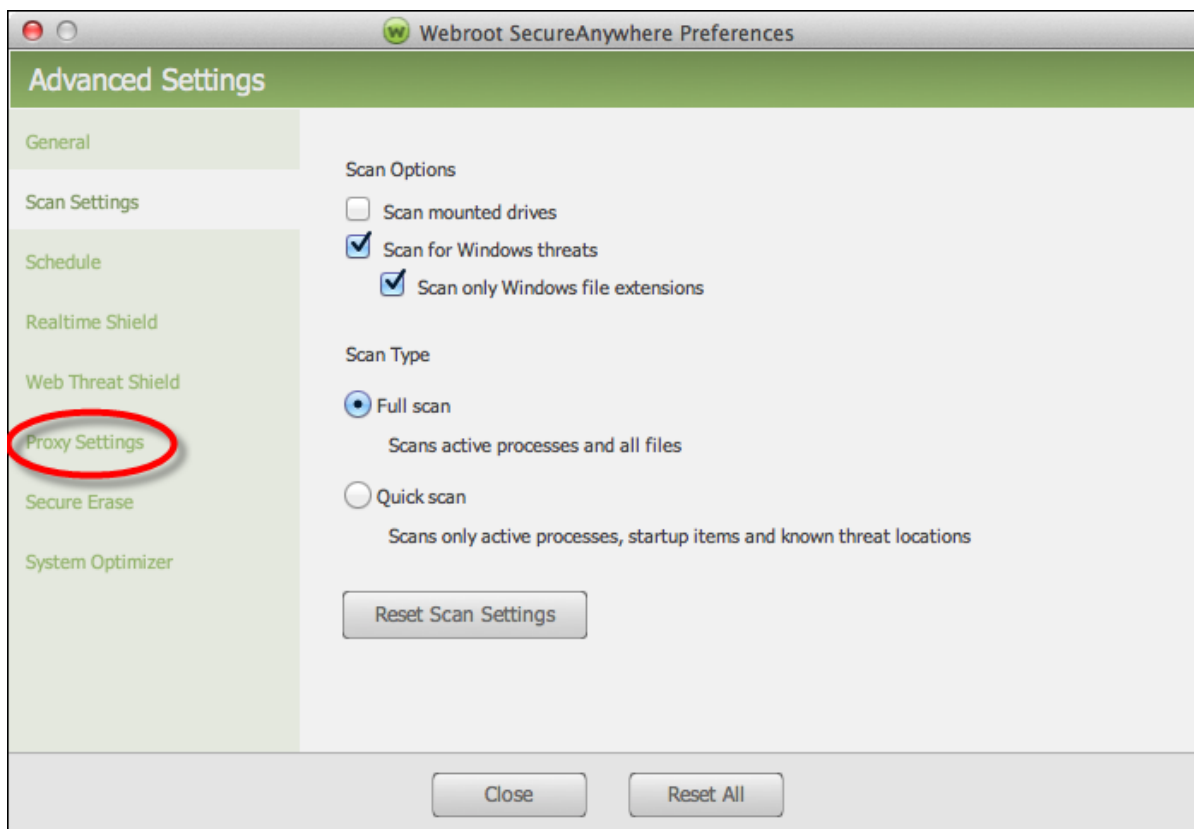
2. Click the **Advanced Settings** button.



The Advanced Settings window displays.



3. In the left column, select **Proxy Settings**.



Note: You can also access the settings window by clicking on Webroot SecureAnywhere from the menu bar and then selecting **Preferences** from the drop-down menu.

4. Enter the proxy settings, which are described in the following table.

FIELD	DESCRIPTION
Proxy Type	Select HTTP Proxy from the drop-down menu.
Authentication Method	Select an authentication method from the drop-down menu.
Host	Enter the IP address or the fully qualified domain name of the server, for example, proxy.company.com.
Port	Enter the port number the server uses.
Username	Enter the user name of the server, if used.
Password	Enter the password of the server, if used.

Chapter 12: WSA Mac Support

For information about support, see the following topic:

Accessing Technical Support	178
--	------------

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 Mac forum.](#)
-

Index

A

- about
 - SecureAnywhere 16
- accessing
 - technical support 178
- account details, viewing 72
- activating keycodes 73
- adding sync folders 85
- alerts, responding to 21

B

- backing up files 88
- backup
 - filters, changing 95
 - schedules, changing 98
- Backup & Sync
 - downloading 83
 - overview 82
 - settings, changing 92
 - statuses, checking 100

C

- changing
 - Backup & Sync settings 92
 - backup filters 95
 - backup schedules 98
 - optimization schedules 29
 - realtime shield settings 52
 - scan schedules 29
 - scan settings 33
 - system control settings 116
 - System Optimizer settings 148
 - web threat shield settings 46
- checking
 - Backup & Sync statuses 100
 - for updates 77
- creating
 - Secure Erase settings 156
 - Webroot accounts 20

D

- defining proxy server settings 170
- description, shields 38
- detected threats, managing 27
- downloading Backup & Sync 83

F

- file detection, managing 65
- files
 - backing up 88
 - synchronizing 104
- folders
 - removing from synchronization 110
 - synchronizing 107

G

- general preferences, setting 164

I

- indicators, query results 39
- installing SecureAnywhere 6

K

- keycodes, activating 73

M

- Mac, overview 2
- managing
 - detected threats 27
 - file detection 65
 - quarantined items 60
 - shields 43
- messages, warning 40

O

- optimization schedules, changing 29
- overview
 - Backup & Sync 82
 - Mac 2

P

proxy server settings, defining 170

Q

quarantined items, managing 60

query result indicators 39

R

realtime shield settings, changing 52

removing folders from synchronization 110

renewing subscriptions 75

responding to alerts 21

running

scans 24

System Analyzer 133

System Optimizer 140

S

saving

scan logs 120

threat logs 67

scan

schedules, changing 29

settings, changing 33

scan logs

saving 120

submitting 126

scans, running 24

Secure Erase settings, creating 156

SecureAnywhere

about 16

installing 6

setting

general preferences 164

shield types 38

shields, managing 43

submitting scan logs 126

subscriptions, renewing 75

sync folders, adding 85

synchronizing

files 104

folders 107

- System Analyzer, running 133
- system control settings, changing 116
- System Optimizer
 - running 140
 - settings, changing 148

T

- technical support, accessing 178
- threat logs, saving 67

U

- updates, checking for 77
- using
 - web threat protection 56

V

- viewing account details 72

W

- warning messages 40
- web threat
 - protection, using 56
 - shield settings, changing 46
- Webroot accounts, creating 20