



Verizon Internet Security Suite Powered by
McAfee 1.0
User Guide

COPYRIGHT

Copyright © 2010 McAfee, Inc. All Rights Reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc., or its suppliers or affiliate companies.

TRADEMARK ATTRIBUTIONS

AVERT, EPO, EPOLICY ORCHESTRATOR, FOUNDSTONE, GROUPSHIELD, INTRUSHIELD, LINUXSHIELD, MAX (MCAFFEE SECURITYALLIANCE EXCHANGE), MCAFFEE, NETSHIELD, PORTALSHIELD, PREVENTSYS, SECURITYALLIANCE, SITEADVISOR, TOTAL PROTECTION, VIRUSSCAN, WEBSHIELD are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners.

LICENSE INFORMATION

License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Contents

- Introduction..... 4**
 - About this Guide..... 5
 - Features..... 5
 - System Requirements..... 6
- Using the Verizon Internet Security Suite application..... 7**
 - Opening Verizon Internet Security Suite..... 7
 - Home Page..... 7
 - History of product events..... 8
 - Quarantine..... 9
 - Accessing your Account..... 10
 - Family Protection..... 11
 - Online Backup and Sharing..... 11
 - Full Scan..... 11
 - Scheduled Scan..... 11
 - Custom Scan..... 11
 - Update..... 12
 - Opening the Verizon Internet Security Suite Preferences..... 12
 - Configuring General Preferences..... 12
 - Configuring Anti-malware Preferences..... 13
 - Configuring Application Protection Preferences..... 18
 - Configuring Desktop Firewall Preferences..... 22
- Uninstallation..... 26**
- Appendix A — Help options..... 27**
- Appendix B — Default Preferences..... 28**
- Appendix C — Network Interface..... 29**
- Glossary..... 30**

Introduction





Verizon Internet Security Suite Powered by McAfee is a proactive, always-updating security bundle that helps protect your Mac from viruses, spyware, spam, phishing or emails with infected attachments, hackers, and online predators. With this security software, you can surf the web, shop, bank, email, instant message, and download files with confidence.

This software scans files, folders, and all other items on your Mac in real-time for viruses, spyware, and other potential threats. You can manually scan your entire Mac or schedule scans to run at a particular time or at regular intervals. You can also manually scan specific items or volumes to reduce overall scan time.

You can create rules to prevent the execution of unknown applications on your Mac and to prevent specific applications from accessing the network. You can also create rules to allow or block access to unsolicited networks, subnets, hosts, or IP addresses.

Using Verizon Internet Security Suite, you can open the Family Protection application that helps protect your children from social networking risks, strangers, exposure to inappropriate content, and other threats.

Verizon SiteAdvisor Powered by McAfee continuously tests the safety of the web and provides one of the following site-rating icons in your search results, browser buttons, and optional search boxes. When you place your cursor on these icons, you can see a visual cue that determines whether the websites are safe or risky, before you visit them.

Icons	Description
	The website is safe and can be visited.
	The website contains potential security risks in it and must not be visited.
	The website contains potential suspicious behavior that might pose a security risk.
	The website is not tested for safety yet. In this case, you can place your cursor on the icon, click Submit for testing and wait till it is tested. You also see this icon if testing is already started but the results are not known yet.

Contents

- ▶ [About this Guide](#)
- ▶ [Features](#)
- ▶ [System Requirements](#)

About this Guide


Start with this User Guide to find detailed information on using Verizon Internet Security Suite Powered by McAfee; whether you simply want to discover the best way to use your features or if you need to learn how to troubleshoot a problem.

McAfee Virtual Technician

If you can't solve your problems by using this guide, try running McAfee Virtual Technician from [Verizon Support](#). Like a personal technical support representative, McAfee Virtual Technician collects information about Verizon Internet Security Suite Powered by McAfee so that it can help you fix protection issues on your Mac.

Features

Verizon Internet Security Suite Powered by McAfee 1.0 offers the following features:

Features	Description
Easy access to the application	You are just one click away from accessing Verizon Internet Security Suite Powered by McAfee. Click the menulet  on your menu bar to access the application.
Anti-malware	Safeguards your Mac from viruses, spyware, Trojan horses, and other potential threats.
Application Protection	Prevents the execution of unknown applications and/or restricts network access to them based on the rules you define.
Desktop Firewall	Allows or denies access to specific networks, subnets, hosts, or IP addresses based on the rules you define.
Verizon SiteAdvisor Powered by McAfee	The Verizon SiteAdvisor Powered by McAfee add-on continuously tests the safety of the web and provides color-coded icons in your search results, browser buttons, and optional search boxes. These icons let you know which sites are safe and which are risky — before you visit them.
History of product events	Logs and displays all events of scan, product update, and application protection in the History & Log screen.
Quarantine	Items containing viruses, spyware, and other potential threats are isolated to a location, so that they cannot be opened or infect other items on your Mac.
Easy access to your Verizon account	On the left pane of your application, click the My Account link to visit the Verizon Central webpage. Here you can log in to your Verizon account and view information about your product subscription.
Family Protection	On the left pane of your application, click the Family Protection to open the application. If it's not installed on your Mac, you will be directed to a website where you can download and install the application.
Verizon Online Backup and Sharing	You can purchase Verizon's Online Backup and Sharing service from Verizon website by clicking Verizon Online Backup and Sharing on the left pane of your application.
Alerts and Notifications	Alerts appear if an unknown or modified application tries to start, and also after your product subscription has expired. Notifications appear when your software detects viruses, spyware, and other potential threats. They also inform you when an unknown application tries to start, or when an application cannot access the network.

Features	Description
Full Scan	Full scan allows you to thoroughly scan all items on your Mac for malware.
Scheduled Scan	Scheduled scan enables you to schedule a scan to run at any convenient time.
Custom Scan	Custom scan enables you to scan specific items or volumes manually.
Update	When your Mac is connected to the Internet, the latest product updates will be downloaded regularly so that your Mac is protected against the latest threats. You can also download the product updates manually.

System Requirements

You need these minimum system requirements to install Verizon Internet Security Suite Powered by McAfee:

- Mac computer with an Intel processor.
- Mac OS X Snow Leopard 10.6 (or later) or Mac OS X Leopard 10.5 (or later) operating system.
- 1024 x 768 or higher resolution.
- 1 GB RAM or more.
- 300 MB free hard disk space.
- Internet connection.
- Mozilla Firefox version 3.0.5 or later (for Verizon SiteAdvisor Powered by McAfee browser add-on).

NOTE: For installation instructions, refer to the *Verizon Internet Security Suite Powered by McAfee Installation Guide*.

Using the Verizon Internet Security Suite application

You can access the Verizon Internet Security Suite application to:


- Use the dashboard items, and the scan and update event items.
- Set up the product preferences.

Contents

- ▶ [Opening Verizon Internet Security Suite](#)
- ▶ [Opening the Verizon Internet Security Suite Preferences](#)

Opening Verizon Internet Security Suite

You can open Verizon Internet Security Suite in one of two ways:

- On your menu bar, click the menulet , and then select **Internet Security Suite Console**.
- In **Finder**, click **Applications**, and then double-click **Internet Security Suite**.

Use the left pane of the application to navigate through the dashboard items, scan your Mac, and manually download the latest product updates.

Contents

- ▶ [Home Page](#)
- ▶ [History of product events](#)
- ▶ [Quarantine](#)
- ▶ [Accessing your Account](#)
- ▶ [Family Protection](#)
- ▶ [Online Backup and Sharing](#)
- ▶ [Full Scan](#)
- ▶ [Scheduled Scan](#)
- ▶ [Custom Scan](#)
- ▶ [Update](#)

Home Page

This page appears when you open Verizon Internet Security Suite. Here, you can:

- Check the security status of your Mac.
- View the subscription status.

- Activate or renew the software.
- View the details of the last scan and update.



History of product events

After opening the application, click **History & Log** on the left pane to see all events related to scan, product updates, and application protection that occurred since the software was installed on your Mac.

TIP: Use the arrows at the bottom of the application to navigate through multiple **History & Log** pages.

Viewing event details

- 1 Click **History & Log** on the left pane of the application. A list of events appear that occurred since you installed the software on your Mac.



2 Double-click on an event to see its details.

TIP: Alternatively, you can click an event, click **History & Log** on the Verizon Internet Security Suite menu bar, and then select **View Details**.

Arranging events

To arrange the events alphabetically, click the column headers **Event** and **Type** on the screen. Click the column header of **Date & Time** to arrange the events based on when they occurred.

TIP: Alternatively, you can click **History & Log** on the Verizon Internet Security Suite menu bar, select **Arrange By**, and then select **Event**, **Type**, or **Date & Time** as required.

Removing events

NOTE: You must have administrator rights to remove events or clear the history of events.

- 1 After opening the application, click **History & Log** on the left pane.
- 2 Click the lock, type your administrator password, and then click **OK**.
- 3 Select an event that you want to remove.
- 4 Click **Delete** and then click **OK**.

TIP: To delete multiple events, select them using the **shift** key, click **Delete**, and then click **OK**.

To delete all events from the **History & Log** screen, click **History & Log** on the Verizon Internet Security Suite menu bar, select **Clear History & Log**, and then click **OK**.

Quarantine

After opening the application, click **Quarantine** on the left pane to see the original location of items that were quarantined and when they were quarantined.

TIP: Use the arrows at the bottom of the console to navigate through multiple **Quarantine** pages.

Family Protection

After opening the application, click the **Family Protection** link on the left pane to launch the Family Protection product on your Mac. If the product is not installed on your Mac, you will be directed to a website from where you can download the Family Protection package and install it.

Online Backup and Sharing

Click the **Verizon Online Backup and Sharing** link on the left pane of the console to purchase Verizon's Online Backup and Sharing service.

Full Scan

Click **Full Scan** on the left pane of the console, then click **Start** to thoroughly scan your Mac for malware.

Scheduled Scan

NOTE: You must have administrator rights to schedule a scan.

You can schedule a scan to check items on your Mac for threats at any convenient time, probably when you do not want the scans to interfere with your work or when your work on the Mac is comparatively low.

- 1 Launch the Verizon Internet Security Suite Console. For instructions on launching the console, see [Opening Verizon Internet Security Suite](#).
- 2 Click **Scheduled Scan** on the left pane of the console.
- 3 Click the lock, type your administrator password, then click **OK**.
- 4 In the **When to scan** pane, select the schedule as required.
After scanning completes, a summary of the scheduled scan is displayed, which includes the number of items scanned and threats detected.

TIP: You can view the details of the scheduled scan on the **History & Log** screen.

Custom Scan

You can use Custom Scan to manually scan items/volumes of your choice.

- 1 Launch the Verizon Internet Security Suite Console. For instructions on launching the console, see [Opening Verizon Internet Security Suite](#).
- 2 Click **Custom Scan** on the left pane of the console.
- 3 In the **What to scan** pane, select items from the drop-down menu or drag-and-drop the items you want to scan.

TIP: You can use the  and  buttons to add and delete items respectively.

- 4 Click **Start**.

After scanning completes, a summary of the custom scan is displayed, which includes the number of items scanned and threats detected.

TIP: You can view the details of the custom scan on the **History & Log** screen.

Update


NOTE: Your Mac must be connected to the Internet to receive automatic updates regularly.

Run an Update to download all product updates to ensure you are running the most current security to combat the ever-evolving threats on the Internet for the duration of your subscription.

To run a manual update, click **Update** on the left pane of the console, then click **Start**. You can enable or disable automatic updates in **General Preferences**.

Opening the Verizon Internet Security Suite Preferences

You can launch the Verizon Internet Security Suite Preferences in one of two ways:

- Click the menulet  on your menu bar, then select **Internet Security Suite Preferences**.
- Launch the Verizon Internet Security Suite console (see [Opening Verizon Internet Security Suite](#)), click **Internet Security Suite** on the menu bar, then select **Preferences**.

Contents

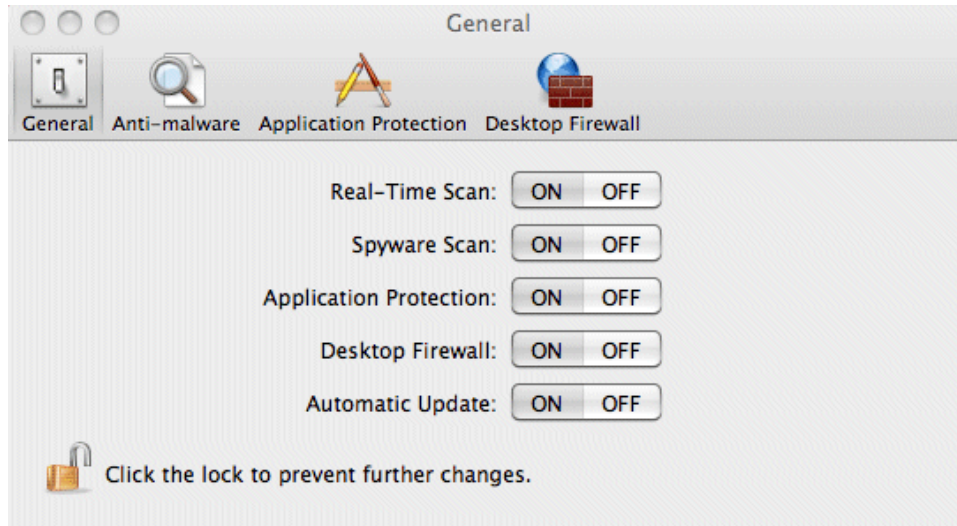
- ▶ [Configuring General Preferences](#)
- ▶ [Configuring Anti-malware Preferences](#)
- ▶ [Configuring Application Protection Preferences](#)
- ▶ [Configuring Desktop Firewall Preferences](#)

Configuring General Preferences

NOTE: You must have administrator rights to configure General Preferences.

You can use General preferences to enable or disable the Real-Time Scan, Spyware Scan, Application Protection, Desktop Firewall, and the Update features.

- 1 Open the Verizon Internet Security Suite Preferences. See [Opening the Verizon Internet Security Suite Preferences](#) for instructions.
- 2 Click the lock to make changes. Type your administrator password when prompted, and then click **OK**. The following screen appears.



3 Click **ON** or **OFF** to enable or disable the following features:

- Real-Time Scan
- Spyware Scan
- Application Protection
- Desktop Firewall
- Automatic Update

NOTE: By default, all features are enabled.

Configuring Anti-malware Preferences

NOTE: You must have administrator rights to configure Anti-malware Preferences.

You can use Anti-malware Preferences to:

- Configure the Real-Time Scan and Scheduled & Manual Scan preferences.
- Specify items to be excluded from Real-Time and Scheduled & Manual scanning separately.

TIP: You can specify regular expression based exclusions.

NOTE: Click **Reset**, then **OK** to reset the Anti-malware preferences to their default values.

Tasks

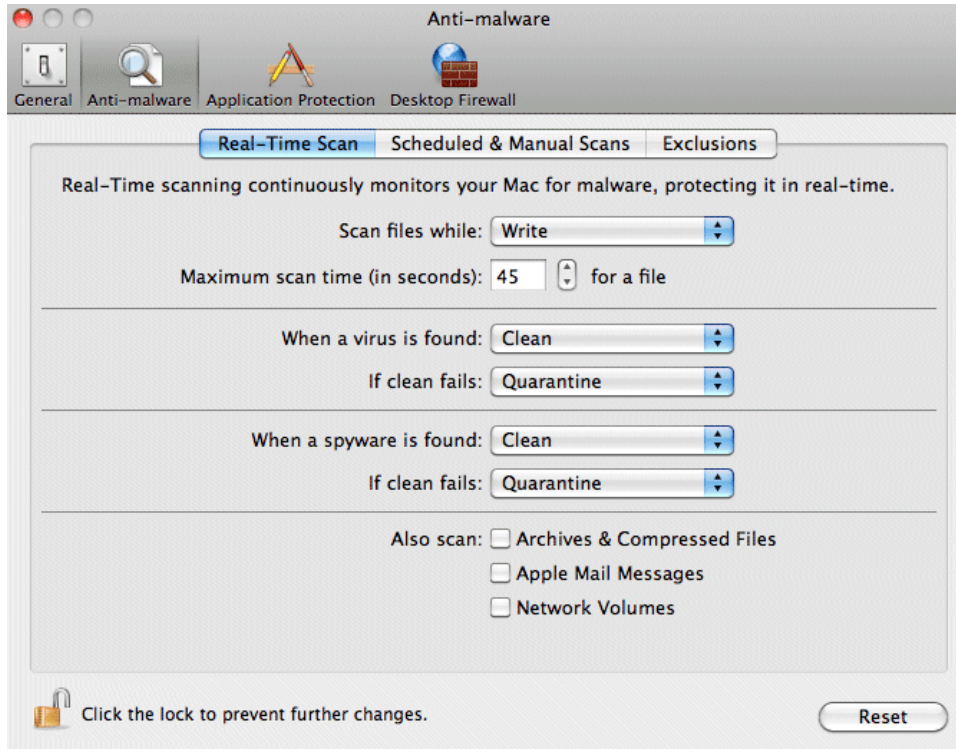
- ▶ [Configuring Real-Time Scan Preferences](#)
- ▶ [Configuring Scheduled & Manual Scan Preferences](#)
- ▶ [Specifying Exclusions](#)

Configuring Real-Time Scan Preferences

NOTE: You must have administrator rights to configure Real-Time Scan Preferences.

Real-Time Scan consistently monitors all items on your Mac for malware. Scanning takes place whenever an item is read from the disk, written to the disk (or both) based on the preferences you configure.

- 1 Open the Verizon Internet Security Suite Preferences. See [Opening the Verizon Internet Security Suite Preferences](#) for instructions.
- 2 Click **Anti-malware**.
By default, the **Real-Time Scan** Preferences screen is displayed.
- 3 To configure the Real-Time Scan Preferences, click the lock, type your administrator password, then click **OK**. The following screen appears.



TIP: The Real-Time scan Preferences will have default settings. For more information about the Real-Time scan default settings, see [Appendix B — Default Preferences](#).

- 4 Use the following options to configure the Real-Time Scan Preferences:
 - From the Scan files while drop-down menu, select one of the following options:

Option	Description
Read	To scan items that are only being read from the hard disk.
Write	To scan items when they are written to the hard disk.
Read & Write	To scan items that are being read from or written to the hard disk.

- In **Maximum scan time (in seconds)**, specify a time after which the scanning of each file terminates. The minimum and maximum values you can specify are 10 and 999 seconds respectively. Default value is 45 seconds.
- From the **When a virus is found** and **When a spyware is found** drop-down menus, select one of the following primary actions:

Action	Description
Clean	To clean (repair) the item on your Mac containing virus and spyware respectively. Selecting this option enables you to select a secondary action in the If clean fails drop-down menu (that allows you to quarantine, delete, or notify the virus/spyware detection) if the cleaning process fails.

Action	Description
Quarantine	To isolate the item containing virus and spyware respectively. Selecting this option enables you to define a secondary action in the If quarantine fails drop-down menu (that allows you to delete or notify the virus/spyware detection) if the quarantining process fails.
Delete	To delete the item containing virus/spyware.
Notify	To notify you in case of a virus/spyware detection (no other actions being taken).

- You can also enable scanning for:
 - Archives & Compressed Files
 - Apple Mail Messages
 - Network Volumes

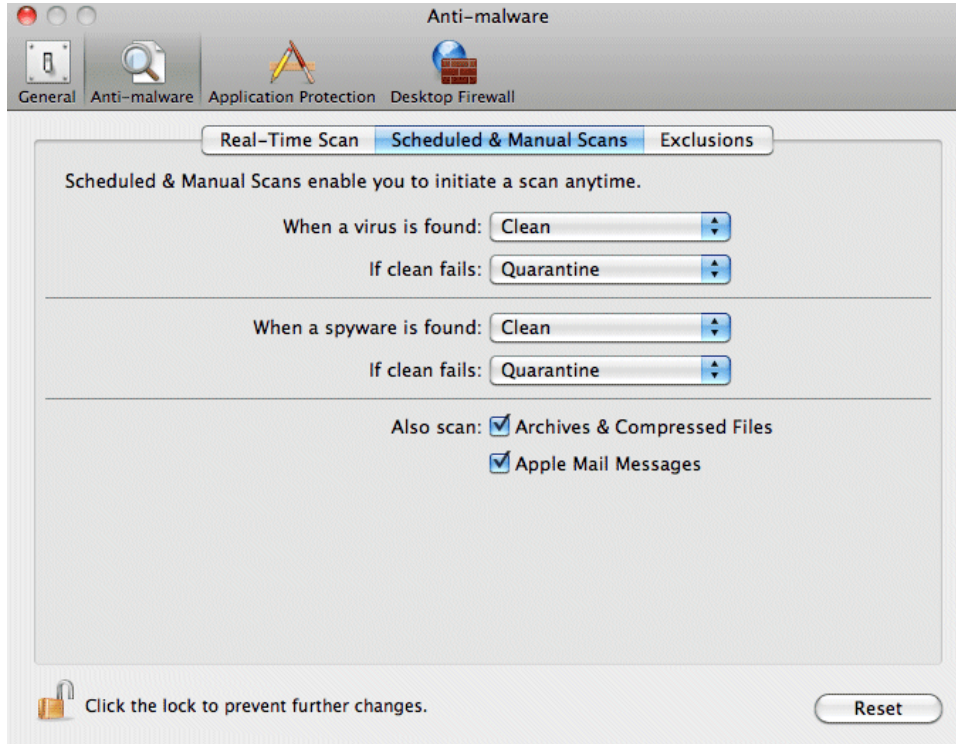
NOTE: By default, scanning is disabled for these items.

Configuring Scheduled & Manual Scan Preferences

NOTE: You must have administrator rights to configure Scheduled & Manual Scan Preferences.

Scheduled scan enables you to schedule a scan at any convenient time. You can also perform a manual scan (Custom Scan) for specific items/volumes of your choice.

- 1** Open the Verizon Internet Security Suite Preferences. See [Opening the Verizon Internet Security Suite Preferences](#) for instructions.
- 2** Click **Anti-malware**.
- 3** Click **Scheduled & Manual Scans**.
- 4** To configure the Scheduled & Manual Scan Preferences, click the lock, type your administrator password, then click **OK**. The following screen appears.



TIP: The Scheduled & Manual Scan Preferences will have default settings. For more information about the Scheduled & Manual Scan default settings, see [Appendix B — Default Preferences](#).

- 5 Use the following options to configure the Scheduled & Manual Scan Preferences:
- From the **When a virus is found** and **When a spyware is found** drop-down menus, select one of the following primary actions:

Action	Description
Clean	To clean (repair) the item on your Mac containing virus and spyware respectively. Selecting this option enables you to select a secondary action in the If clean fails drop-down menu (that allows you to quarantine, delete, or notify the virus/spyware detection) if the cleaning process fails.
Quarantine	To isolate the item containing virus and spyware respectively. Selecting this option enables you to define a secondary action in the If quarantine fails drop-down menu (that allows you to delete or notify the virus/spyware detection) if the quarantining process fails.
Delete	To delete the item containing virus/spyware.
Notify	To notify you in case of a virus/spyware detection (no other actions being taken).

- You can also enable or disable scanning for:
 - Archives & Compressed Files
 - Apple Mail Messages

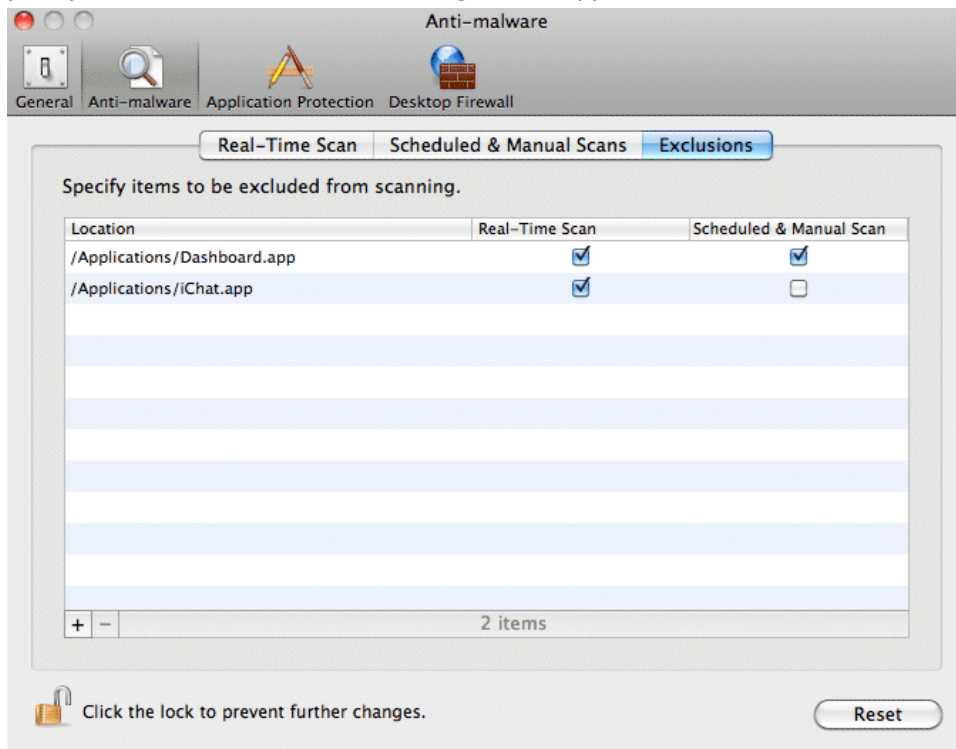
NOTE: By default, scanning is enabled for these items.

Specifying Exclusions

NOTE: You must have administrator rights to specify exclusions.

You can exclude specific items from your scans if you do not want to check them for threats. Excluding items shortens the amount of time it takes to scan your Mac.

- 1 Open the Verizon Internet Security Suite Preferences. See [Opening the Verizon Internet Security Suite Preferences](#) for instructions.
- 2 Click **Anti-malware**.
- 3 Click **Exclusions**.
- 4 To specify exclusions, click the lock to make changes. Type your system password when prompted, then click **OK**. The following screen appears.



- 5 Click **+** at the bottom left corner of the screen. A screen appears allowing you to select and add items to the exclusion list.
- 6 Select the items you want to exclude from the scans, then click **Open** to return to the **Exclusions** screen.
- 7 Select or deselect the **Real-Time Scan** and/or **Scheduled & Manual Scan** options as required. By default, both options are enabled so that the selected items are excluded from both scans.

NOTE: To modify the location/item of an existing exclusion, double-click it in the corresponding cell. The location/item becomes editable. Specify the new location/item.

TIP: You can also specify regular expression based exclusions.

For example: `/Users/<username>/Desktop/images[1-4]`

In the above example, all files on the desktop with filenames images1, images2, images3, and images4 will be excluded from being scanned.

NOTE: To delete an exclusion, select it, then click **-** at the bottom left corner of the screen.

Configuring Application Protection Preferences

NOTE: You must have administrator rights to configure Application Protection Preferences.

You can use Application Protection preferences to create rules to prevent the execution of unknown applications and/or deny network access to specific applications. You can exclude specific applications from these rules.

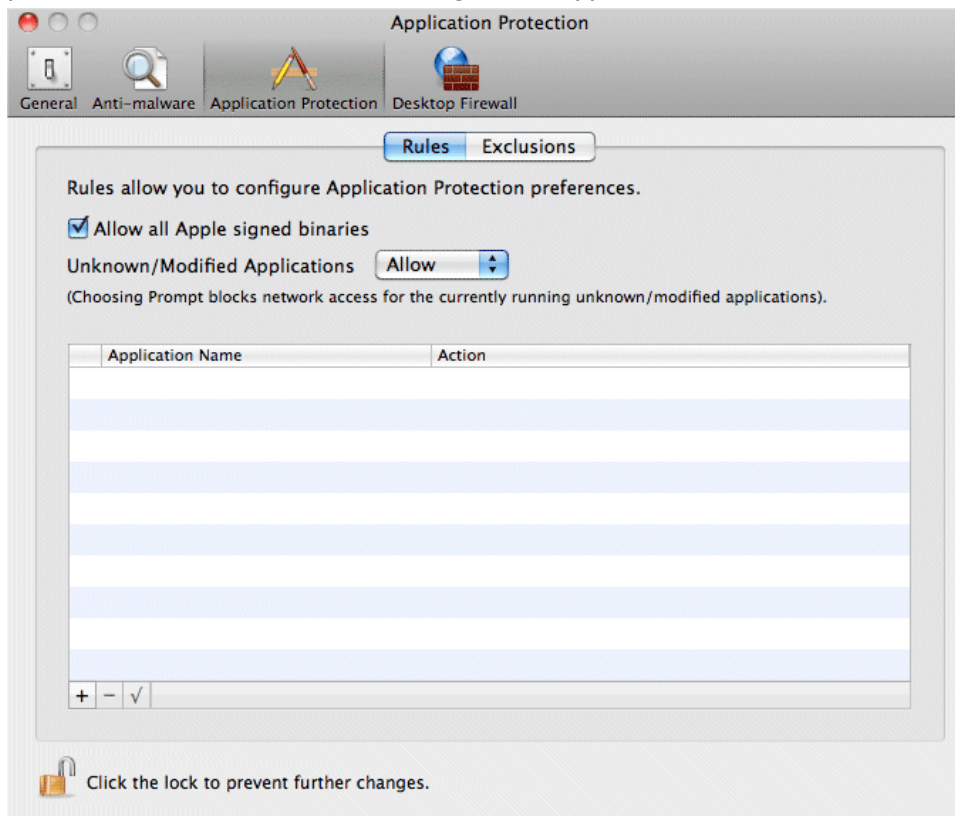
Tasks

- ▶ [Creating Application Protection Rules](#)
- ▶ [Re-applying Application Protection Rules for Modified Applications](#)
- ▶ [Excluding Applications from the Application Protection Rules](#)

Creating Application Protection Rules

NOTE: You must have administrator rights to create Application Protection Rules.

- 1 Open the Verizon Internet Security Suite Preferences. See [Opening the Verizon Internet Security Suite Preferences](#) for instructions.
- 2 Click **Application Protection**.
- 3 To configure the Application Protection preferences, click the lock, type your administrator password, then click **OK**. The following screen appears.



TIP: The application protection preferences will have default settings. For more information about the Application Protection default settings, see [Appendix B — Default Preferences](#).

- 4 In **Rules**, use the following options to configure the Application Protection Preferences:

- Select or deselect the **Allow all Apple signed binaries** as required. This option is selected by default.
- Select **Allow**, **Block**, or **Prompt** from the **Unknown/Modified Applications** drop-down menu for configuring the application execution and network access settings for all unknown and modified applications.

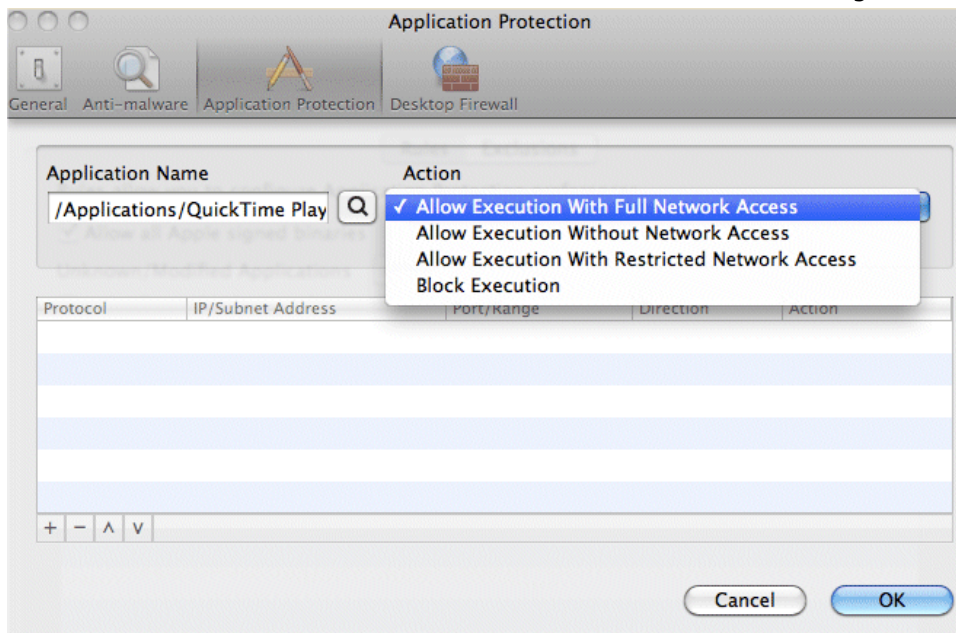
NOTE: If you select **Prompt** for <n> seconds ($n \leq 300$ seconds), try launching an unknown or modified application, the Alert screen appears for <n> seconds prompting you to select an appropriate action for the application execution that must be applicable **Always** or **Once**.



The available actions are:

Actions	Description
Allow execution with full network access	To allow the application to execute and access the network.
Allow execution with no network access	To allow the application only to execute and deny network access to it.
Block execution	To block the application from executing.

NOTE: If you do not specify one of the above actions within <n> seconds, execution and network access will be denied for that application.

- 5 Click  at the bottom left corner of the Preferences screen. The following screen appears.



- 6 In **Application Name**, browse and add an application/binary using the  button.
- 7 In **Action**, select one of the options from the drop-down menu, then click **OK**.
- 8 If you select **Allow Execution With Restricted Network Access**, you can click  on the bottom left corner of the **Application Protection** screen and specify a **Protocol**,

IP/Subnet Address, Port/Range, and the Direction of network that can be allowed or denied (in **Action**).

NOTE: If you do not click to add these options, network access for the selected application/binary is denied.

- 9 Click **OK** to return to the **Rules** screen.

NOTE: To edit the **Action** (selected in Step 3 of this procedure) in **Rules** screen, click the appropriate cell of the required application below **Action**, then select another option, then click **OK**.

To disable an existing Application Protection rule, click the corresponding application's checkbox

Modifying an existing Application Protection Rule (To restrict network access)

- 1 For an existing rule, click on the cell below **Action**, select **Allow Execution With Restricted Network Access**.

NOTE: In **Application Protection** screen, you can again select the required **Action**. However, you cannot re-select another application.

- 2 Click on the bottom left corner of the **Application Protection** screen and specify a **Protocol, IP Address/Subnet, Port/Range, and the Direction** of network that can be allowed or denied (in **Action**).
- 3 Click **OK** to return to the **Rules** screen.

NOTE: To delete a rule, select it then click at the bottom left corner of the Preferences screen.

Re-applying Application Protection Rules for Modified Applications

NOTE: You must have administrator rights to re-apply Application Protection Rules for modified applications.

When there is a change in a binary/application (due to a software update, OS upgrade, and so on), the rule configured for that binary/application becomes invalid. To re-apply rules for such binaries/applications, select the modified application rules (prefixed with a symbol), then click at the bottom left corner of the Preferences screen.

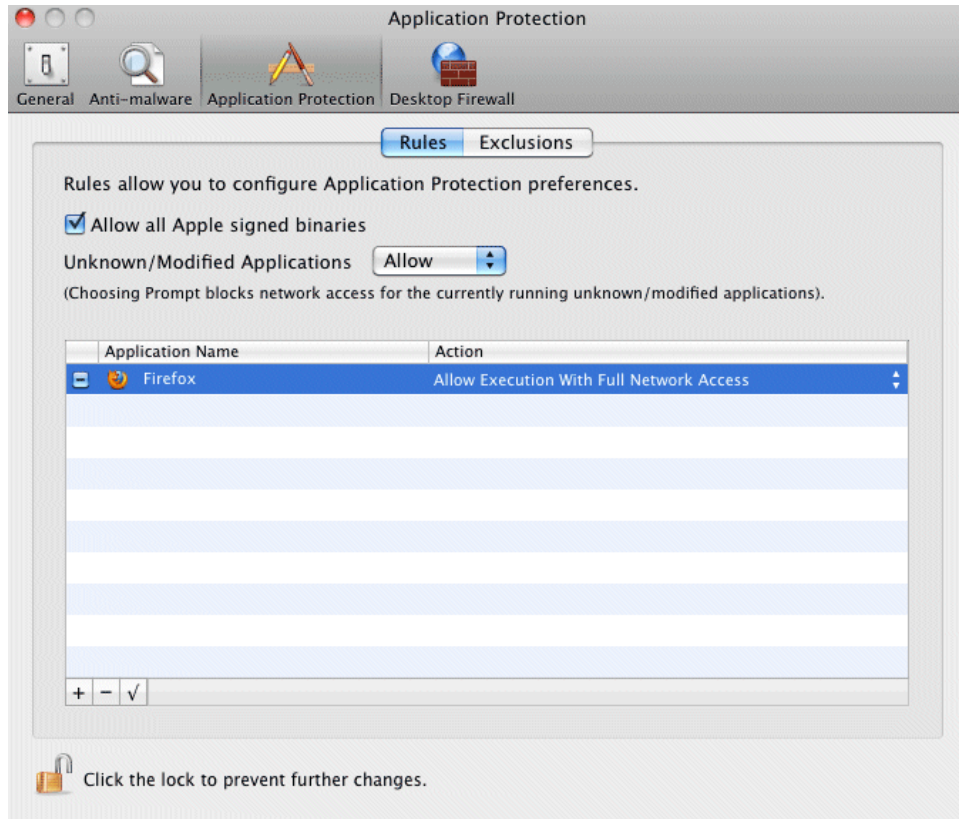
By default, the option is disabled.

To enable and use this option, select the required modified application rule(s), then click .

To select all rules, press **command + A**, then click . The rules for modified binaries/applications will be applicable again.

TIP: The option has a tooltip text associated with it stating **Re-apply rules for modified applications**.

The following figure shows a typical application that was modified for which you can re-apply Application Protection Rule.



Excluding Applications from the Application Protection Rules

NOTE: You must have administrator rights to exclude applications from the Application Protection rules.

You can exclude applications from the application protection rules. The Exclusions option overrides the Application Protection rules you create.

- 1 Open the Verizon Internet Security Suite Preferences. See [Opening the Verizon Internet Security Suite Preferences](#) for instructions.
- 2 Click **Application Protection**.
- 3 To specify Application Protection exclusions, click the lock, type your administrator password, then click **OK**.
By default, the **Rules** screen opens.
- 4 Click **Exclusions**.
- 5 Click **+** at the bottom left corner of the screen to add an exclusion.
- 6 From the list, add the application(s) you want to exclude from the Application Protection rule(s), then click **Open**.

NOTE: To delete an exclusion, select it, then click **-** at the bottom left corner of the console.

Configuring Desktop Firewall Preferences

NOTE: You must have administrator rights to configure Desktop Firewall Preferences.

You can use Desktop Firewall preferences to create rules to prevent access to unsolicited networks/hosts/subnets/IP addresses. You can exclude Trusted Networks from these rules by specifying them in Groups.

IMPORTANT

Desktop Firewall Rules take precedence over Application Protection Rules.

Tasks

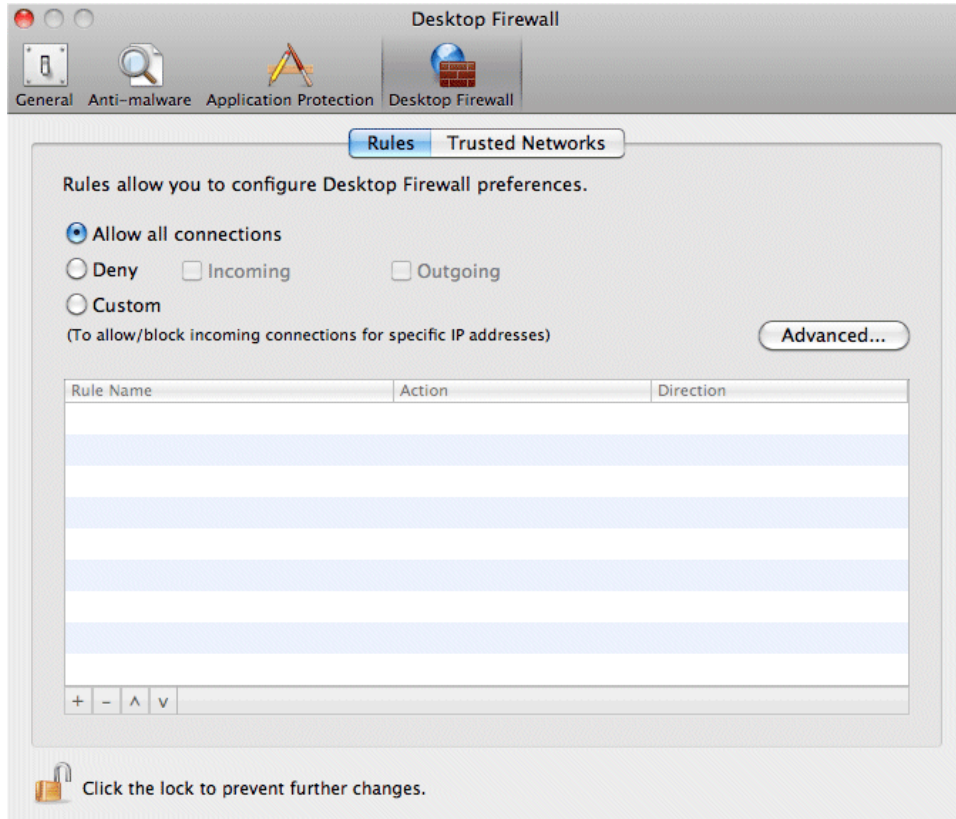
- ▶ [Creating Desktop Firewall Rules](#)
- ▶ [Specifying Trusted Networks](#)

Creating Desktop Firewall Rules

NOTE: You must have administrator rights to create Desktop Firewall Rules.

You can create Desktop Firewall Rules to allow or block access to specific networks or IP addresses.

- 1** Open the Verizon Internet Security Suite Preferences. See [Opening the Verizon Internet Security Suite Preferences](#) for instructions.
- 2** Click **Desktop Firewall**.
- 3** To configure the Desktop Firewall Preferences, click the lock, type your administrator password, then click **OK**. The following screen appears.



TIP: The Desktop Firewall Preferences will have default settings. For more information about the Desktop Firewall default settings, see [Appendix B — Default Preferences](#).


- 4 Select one of the following options:

Actions	Description
Allow all connections	To allow all network connections.
Deny	To deny incoming and/or outgoing network connection.
Custom	To customize the firewall rule.

- 5 If you select **Custom** in step 4, click at the bottom left corner of the Preferences screen to add a rule.
- 6 Type a unique rule name.
- 7 In **General**, select an **Action**, **Protocol**, **Direction** of the network connection, and a network interface for the rule from the drop-down lists.
For information on network interface, see [Appendix C — Network Interface](#).
- 8 In **IP/Subnet Address/Network**, select the source and destination IP address/subnet/network and the port/port range for which the access must be provided or denied.
- 9 Click **OK**.

NOTE: To edit a rule, double-click the corresponding cell under **Rule Name**, then perform step 6 to 9. You can also click on the cell below **Action** or **Direction** to change the settings directly on the **Rules** screen.

TIP: You can also use:

- 5 Click  in the **IP/Subnet Address/Host Name** pane to add the trusted IP/subnet addresses, host names or URLs of that Group to be excluded from the Desktop Firewall Rules.

NOTE: To edit a Group name, IP/Subnet Address/Host Name you created, double-click the corresponding cell under **Groups**, then re-type the new Group name.

Uninstallation

NOTE: You must have administrator rights to uninstall Verizon Internet Security Suite from your Mac.

1 Click **Finder**, go to **Applications**, and then double-click **Internet Security Suite Uninstaller**. The **Welcome to Internet Security Suite Uninstaller** screen appears.

2 Click **Continue**.

NOTE: Selecting the **Uninstall SiteAdvisor** option uninstalls Verizon SiteAdvisor Powered by McAfee while uninstalling Verizon Internet Security Suite.

3 Type the administrator password when prompted, and then click **OK**. A progress bar appears displaying the uninstallation status. After the uninstallation is complete, the **Summary** screen appears.

4 Click **Finish**.

Appendix A — Help options

After opening Verizon Internet Security Suite Powered by McAfee, you can use the following options by clicking **Help** on the menu bar:

Search

This option enables you to type keywords and find Help related topics for your Mac OS X operating system.

Internet Security Suite Help

This option helps you access the Verizon Internet Security Suite Help, which provides detailed instructions on how to use the software.

Support

This option opens the Verizon Support webpage, which provides:

- Answers to your product support questions.
- Contact information for Verizon Technical Support.

Appendix B — Default Preferences

NOTE: You must have administrator rights to change your Verizon Internet Security Suite preferences.

Feature	Preferences	Default preferences
Anti-malware • Real-Time Scan	Scan on write	Enabled
	Scan time for a file	45 seconds
	When a virus/spyware is found, Primary action	Clean
	If primary action fails, Secondary action	Quarantine
	Scan Archives & Compressed Files	Disabled
	Scan Apple Mail Messages	Disabled
	Scan Network Volumes	Disabled
• Scheduled & Manual Scans	When a virus/spyware is found, Primary action	Clean
	If primary action fails, Secondary action	Quarantine
	Scan Archives & Compressed Files	Enabled
	Scan Apple Mail Messages	Enabled
Application Protection	Allow all Apple signed binaries	Allow
	Execution and network access of Unknown/Modified applications	Allow
Desktop Firewall	Allow All Connections	Enabled

Appendix C — Network Interface

Network interface is the point of interconnection between a computer and a private or public network. While creating a Desktop Firewall rule, you are prompted to select a network interface from the drop-down menu. The network interface options displayed in the drop-down menu depends on the services or applications that use physical or virtual interfaces.

Some of the commonly available interfaces are:

Interface	Description
en0	Standard Ethernet interface
en1	Standard AirPort interface
fw0	Standard Firewire interface
gif0	Tunnel Interface (Tunnels IPv[46] traffic over IPv[46])
lo0	Loopback Interface (Used for network troubleshooting)
stf0	Tunnel Interface (Tunnels IPv6 traffic over IPv4)

NOTE: If other interface options are shown in the **Interface** drop-down menu, then it means your Mac might be using applications like Parallels, VMWare, Virtual Box and so on.

Glossary

This section defines the terminology used in this guide.

Administrator

A user account with read, write, and delete permissions and rights to all operations.

Anti-malware

This feature helps in setting up the Real-Time scan and Scheduled and Manual scan preferences and in specifying items to be excluded from these scans.

Application Protection

This feature prevents unknown application execution and/or blocks network access to them.

Custom Scan

Custom scan enables you to scan specific files, folders, or volumes manually.

Desktop Firewall

Desktop Firewall helps you configure rules to prevent unauthorized access to networks/subnet/IP addresses.

DMG file

Self-mounting disk image.

Family Protection

Family Protection application helps protect your children from any social networking risks, strangers, exposure to inappropriate content, and other threats.

Firewall

A program that acts as a filter between your computer and the network or Internet, based on the rules you define.

Full Scan

Full Scan enables you to scan your Mac thoroughly for malware.

Log

A record of the activities of a component of the Verizon software. Logs record the actions taken during installation, scanning, or updating tasks.

Real-Time Scan

Real-Time Scan continuously monitors all items on your Mac for viruses, spyware, and other potential threats. Scanning takes place whenever an item is read from the disk, written to the disk (or both) based on the preferences you configure.

Scheduled Scan

Scheduled scan enables you to schedule a scan task to run at any convenient time.

Spyware

A software that might transmit your personal information to a third party without your knowledge or consent.

Trojan

A non-replicating program that pretends to have a set of useful or desirable features, but actually facilitates unauthorized access to your Mac. Once a Trojan horse is installed on your Mac, it is possible for a hacker to access your Mac remotely and perform various operations. Trojans are not technically viruses because they do not replicate.

Update

Update allows you to download the latest product updates so that your Mac is protected against the latest threats. An Internet connection is required for this.

Verizon Internet Security Suite Powered by McAfee Console

The common user interface for Verizon Internet Security Suite Powered by McAfee.

Virus

A computer program that can copy itself and infect a computer without a user's knowledge or permission.

Index

A

- about this guide 5
- access your account 10
- application protection
 - preferences 18
 - rules 18

C

- configure
 - anti-malware preferences 13
 - application protection preferences 18
 - desktop firewall preferences 22
 - general preferences 12
 - real-time preferences 13, 15
- console
 - access your account 10
 - custom scan 11
 - Family Protection 11
 - full scan 11
 - history and log 8
 - home page 7
 - online backup and sharing 11
 - quarantine 9
 - scheduled scan 11
 - Update 12
- custom scan 11

D

- default preferences 28
- desktop firewall
 - preferences 22
 - rules 22
 - specify trusted networks 24

E

- exclusions 17

F

- Family Protection 11
- full scan 11

G

- glossary 30

H

- Help option
 - menu bar 27
- home page 7

I

- introduction
 - Verizon Internet Security Suite 4

M

- menu bar
 - help option 27

N

- network interface 29
- network interface options 29

O

- online backup and sharing 11
- open product 7

P

- preferences
 - anti-malware 13
 - application protection 18
 - application protection exclusions 21
 - desktop firewall 22
 - general 12
 - real-time scan 13, 15
 - specify exclusions 17
- Preferences 12
- prerequisites 6
- product
 - features 5
- product console 7
- product events
 - history 8
- product updates 12

Q

- quarantine malware 9

R

- re-apply rules
 - modified applications 20
- rules
 - application protection 18
 - desktop firewall 22

S

- scan
 - custom 11
 - full 11
 - scheduled 11
- scheduled scan 11

system requirements [6](#)

T

trusted networks [24](#)

U

uninstallation [26](#)

V

Verizon Internet Security Suite

application usage [7](#)

features [5](#)

introduction [4](#)

prerequisites for installing [6](#)

