

# User's Guide

---

## VirusScan for Macintosh



*Network Security & Management*

2805 Bowers Avenue  
Santa Clara, CA 95051-0963

Phone: (408) 988-3832  
Monday - Friday  
6:00 A.M. - 6:00 P.M.

## **COPYRIGHT**

Copyright © 1997 by McAfee Associates, 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 Associates, Inc.

## **TRADEMARK NOTICES**

McAfee, McAfee Associates, VirusScan, NetShield, and Site Meter are registered trademarks of McAfee Associates, Inc. WebScan, WebScanX, SiteExpress, BootShield, ServerStor, ScreenScan, WebCrypto, PCCrypto, PCFirewall, NetCrypto, GroupShield, GroupScan, Remote Desktop 32, WebShield, NetRemote, eMail-It, Hunter, ScanPM, and SecureCast are trademarks of McAfee Associates, Inc. All other products or services mentioned in this document are identified by the trademarks or service marks of their respective companies or organizations.

“SABRE” is a trademark of American Airlines, Inc. and is licensed for use to McAfee. Saber Software is not affiliated with American Airlines, Inc. or SABRE Travel Information Network. All trademarks are the property of their respective owners.

## **FEEDBACK**

McAfee appreciates your comments and reserves the right to use any information you supply in any way it believes appropriate without incurring any obligations whatsoever. Please address your feedback to: McAfee Associates, Inc., Documentation, 2805 Bowers Avenue, Santa Clara, CA 95051-0963, send e-mail to [documentation@cc.mcafee.com](mailto:documentation@cc.mcafee.com), or send a fax to McAfee Documentation at (408) 970-9727.

*Issued December 1997/VirusScan v3.0.0*

---

# Table of Contents

<b>Chapter 1. Introducing VirusScan .....</b>	<b>6</b>
What is VirusScan?.....	6
Why use VirusScan?.....	6
VirusScan features.....	7
How VirusScan works .....	8
When to scan for viruses .....	8
How To Contact McAfee .....	9
Customer service .....	9
Technical support.....	9
McAfee training .....	10
International contact information .....	11
Reporting new items for VirusScan updates.....	12
<b>Chapter 2. Installing VirusScan .....</b>	<b>13</b>
Before You Begin .....	13
System requirements .....	13
Preparing to Install from Archived Files .....	14
Preparing to Install from CD-ROM .....	15
Preparing to Install from Floppy Disks .....	16
Using Prescan .....	17
Installation Steps.....	19
Uninstalling VirusScan .....	20
Creating a Custom Installer .....	21

---

<b>Chapter 3. Using Config Wizard .....</b>	<b>24</b>
Setting Basic Scanning Properties .....	24
Starting Config Wizard .....	24
Closing and reopening Config Wizard .....	28
A note about Config Wizard .....	28
<b>Chapter 4. Using the VirusScan Application.....</b>	<b>29</b>
Getting Started .....	29
Performing Immediate Scans .....	30
Cleaning Infected Files .....	31
Scheduling Scan Tasks.....	32
Adding or editing tasks.....	33
Deleting tasks .....	36
Exporting tasks .....	37
Excluding items from scans .....	38
Viewing and Printing the VirusScan Activity Log .....	39
Saving Admin Information.....	40
<b>Chapter 5. Tips and Troubleshooting .....</b>	<b>41</b>
Getting Help .....	41
About the VirusScanner Extension .....	41
Renaming the VirusScanner extension.....	42
What if another extension needs to be loaded first?.....	42
Disabling the extension.....	42
Tips for Faster Scanning.....	43
Other Sources of System Problems .....	44
<b>Appendix A. Preventing Virus Infection .....</b>	<b>46</b>
Creating a Secure Environment.....	46
Updating your VirusScan database files .....	47
Recommendations for system administrators.....	48

---

<b>Appendix B. VirusScan Messages .....</b>	<b>50</b>
Error Messages .....	50
Alert Messages .....	60
<b>Appendix C. McAfee Support Services .....</b>	<b>67</b>
Customer Service Programs.....	68
Free VirusScan support program.....	68
Free subscription maintenance and support program .....	69
Optional support plans .....	70
Enterprise support.....	71
Optional 7 x 24 enterprise support.....	71
<b>Index .....</b>	<b>72</b>

# 1

## Introducing VirusScan

---

### What is VirusScan?

VirusScan is McAfee's comprehensive anti-virus software solution for detecting and removing virus infections from Macintosh and Mac OS computer systems. Use VirusScan to scan your hard disk, removable disks, floppy disks and other virus entry points. Scan according to a schedule, in response to specific events, or whenever you believe you have virus-infected files. VirusScan includes flexible response options, custom alert messages, activity logging and easy configuration, all of which help you to prevent or remove virus infections that can disable your system and destroy your data.

### Why use VirusScan?

Not so long ago, computer users could avoid virus infections without much thought or planning, simply because they rarely came into contact with likely virus sources. Today, however, most computer users send electronic messages to each other, share data, and transfer files constantly—whether through a modem, via diskettes, or over a network or the Internet. In this same span of time, viruses that affect the Macintosh platform—though not nearly so numerous as those that affect other platforms—have continued to increase in number, complexity, and sophistication. That same virus you removed from your hard disk yesterday could reappear today with the next e-mail message you receive.

In this environment, taking precautions to protect yourself from a computer virus infection is no longer a luxury, but a necessity. Consider the extent to which you rely on the data on your computer and the time, trouble and money it would take to replace that data if it became corrupted or unusable because of a virus infection. Balance that possibility against the time and effort it takes to put a few common sense security measures in place, and you can quickly see the utility in protecting yourself against infection.

Even if your own data is relatively unimportant to you, neglecting to guard against viruses might mean that your computer could play unwitting host to a virus that could spread to computers that your co-workers and colleagues use. Checking your hard disk periodically with VirusScan significantly reduces your vulnerability to infection and keeps you from losing time, money and data unnecessarily.

## VirusScan features

VirusScan incorporates McAfee's industry-leading Hunter scanning technology and features:

- Full support for Mac OS 8 and System 7.x
- The VirusScanner extension, which conducts real-time, continuous background scans in response to configuration options you set
- Task scheduling—tell VirusScan to examine your hard disks, mounted servers, or floppy disks at certain times or in response to certain events
- Pre-programmed scanning tasks for common VirusScan operations—use these as they are or modify them to suit your needs
- Flexible response options—remove virus infections from files, move infected files to the Trash, or have VirusScan ask you what to do when it finds a virus
- Config Wizard, an easy-to-use utility you can use to customize VirusScan operations
- A Fat Binary installer for native-code operation on PowerPC or Motorola 680x0-series processors
- An activity log that records all VirusScan detection results, responses, and other actions
- Free monthly Virus Definition file updates—combat new virus strains by downloading data files with the latest in McAfee virus detection technology. See “McAfee Support Services” on page 67 for details.

## How VirusScan works

VirusScan consists of three related components: the VirusScanner extension, which performs all scanning operations; the VirusScan application, which controls how the VirusScanner extension runs and which tasks it performs; and the VirusScan support files, which include virus definitions and other preferences.


Once you use the VirusScan application to configure a set of scanning tasks for it to perform, the VirusScanner extension takes care of running the scan tasks at the appointed time, notifying you when it detects viruses, responding to those viruses, and logging the results. The VirusScanner extension uses its support files to identify known viruses and recognize new and unknown strains.

## When to scan for viruses

Maintaining a secure computing environment means scanning for viruses regularly. Depending on the degree to which you swap floppy disks with other users, share files over your local area network, or interact with other computers via the Internet, scanning “regularly” could mean scanning as often as once a month—even once a day. Other good habits to cultivate include scanning right before you back up your data, scanning before you install new or upgraded software—particularly software you download from other computers—and scanning when you start or shut down your computer each day. Under most circumstances this should protect your system integrity.

If you connect to the Internet frequently or download files often, you might want to supplement regular scans with scans based on certain events. VirusScan includes a default set of scanning tasks to help you monitor your system at the likely points of virus entry, such as

- Whenever you insert a floppy disk into your floppy drive
- Whenever you start an application or open a file
- Whenever a file’s size or other identifying characteristics change

 *Although this type of scanning provides a high level of protection against virus infections, it can increase the time it takes your system to start an application, open a file, or mount a floppy disk.*



## How To Contact McAfee

### Customer service

To order products or obtain product information, we invite you to contact our Customer Care department by calling (408) 988-3832 or by writing to the following address:

McAfee Associates, Inc.  
2805 Bowers Avenue  
Santa Clara, CA 95051-0963  
U.S.A.

### Technical support

McAfee is famous for its dedication to customer satisfaction. We have continued this tradition by making our site on the World Wide Web a valuable resource for answers to technical support issues. We encourage you to make this your first stop for answers to frequently asked questions, for updates to McAfee software, and for access to McAfee news and virus information.

World Wide Web                      <http://www.mcafee.com>

If you do not find what you need or do not have web access, try one of our automated services.

Automated Voice and Fax              (408) 988-3034  
Response Systems

Internet                                      [support@mcafee.com](mailto:support@mcafee.com)

McAfee BBS                                (408) 988-4004

1200 bps to 28,800 bps

8 bits, no parity, 1 stop bit

Available 24 hours, 365 days a year

CompuServe                                GO MCAFEE

America Online                            keyword MCAFEE

# 1

## Introducing VirusScan How To Contact McAfee

---

If the automated services do not have the answers you need, contact McAfee at one of the following numbers Monday through Friday between 6:00 A.M. and 6:00 P.M. Pacific time.

For corporate-licensed customers:

Phone (408) 988-3832

Fax (408) 970-9727

For retail-licensed customers:

Phone (972) 278-6100

Fax (408) 970-9727

To provide the answers you need quickly and efficiently, the McAfee technical support staff needs some information about your computer and your software. Please have this information ready before you call:

- Product name and version number
- Computer brand and model
- Any additional hardware or peripherals connected to your computer
- Operating system type and version numbers
- Network type, if applicable
- Specific steps to reproduce the problem

### **McAfee training**

For information about scheduling on-site training for any McAfee product, call (800) 338-8754.

## International contact information

To contact McAfee outside the United States, use the addresses and numbers below.

**McAfee Canada**

139 Main Street, Suite 201  
Unionville, Ontario  
Canada L3R 2G6  
Phone: (905) 479-4189  
Fax: (905) 479-4540

**McAfee France S.A.**

50 rue de Londres  
75008 Paris  
France  
Phone: 33 1 44 908 737  
Fax: 33 1 45 227 554

**McAfee (UK) Ltd.**

Hayley House, London Road  
Bracknell, Berkshire  
RG12 2TH  
United Kingdom  
Phone: 44 1344 304 730  
Fax: 44 1344 306 902

**McAfee Korea**

135-090, 18th Fl., Kyoung Am Bldg.  
157-27 Samsung-Dong, Kangnam-Ku  
Seoul, Korea  
Tel: 82 2 555-6818  
Fax: 82 2 555-5779

**McAfee Europe B.V.**

Gatwickstraat 25  
1043 GL Amsterdam  
The Netherlands  
Phone: 31 20 586 6100  
Fax: 31 20 586 6101

**McAfee Deutschland GmbH**

Industriestrasse 1  
D-82110 Germering  
Germany  
Phone: 49 8989 43 5600  
Fax: 49 8989 43 5699

**McAfee Japan Co, Ltd.**

Toranomon 33 Mori Bldg.  
3-8-21 Toranomon  
Minato-Ku, Tokyo 105  
Japan  
Phone: 81 3 5408 0700  
Fax: 81 3 5408 0780

**McAfee South East Asia**

7 Temasek Boulevard  
The Penthouse  
#44-01, Suntec Tower One  
Singapore 038987  
Tel: 65 430-6670  
Fax: 65 430-6671

## Reporting new items for VirusScan updates

McAfee is committed to providing you with effective and up-to-date tools you can use to protect your system. To that end, we invite you to report any new viruses that your software does not now detect. Please note that McAfee reserves the right to use any information you supply as it deems appropriate, without incurring any obligations whatsoever. Send your suggestions to:

AVResearch@mcafee.com      Use this address to report new virus strains.

To report items to our European research office, use this e-mail address:

virus\_research\_europe@cc.mcafee.com

To report items to our Asia-Pacific research office, or our office in Japan, use one of these e-mail addresses:

avert-jp@ccj.mcafee.com      Use this address to report harmful items to our office in Japan.

avert\_apac@ccj.mcafee.com      Use this address to report harmful items to our Asia-Pacific office.

# 2

## Installing VirusScan

---

### Before You Begin

McAfee distributes VirusScan in three ways: as a downloadable, archived file available from the McAfee website or other electronic services; on floppy disk; and on CD-ROM. The actions you take to prepare for installation depend on which distribution format you have, but the installation steps you follow after you prepare are the same. Review the system requirements shown below to verify that VirusScan will run on your system, then follow the steps that correspond to the type of distribution you have to prepare for installation.

### System requirements

VirusScan installs and runs on any Macintosh or Power Macintosh equipped with

- At least 2MB of random-access memory (2.5MB recommended)
- At least 2MB of free hard disk space for the VirusScan application, the VirusScanner extension and associated support files (3MB recommended)
- Mac OS 7.x or later (System 7.5 or later recommended)

## Preparing to Install from Archived Files


McAfee makes VirusScan for Macintosh available for downloading as archived .hqx files on the McAfee website. If you suspect that your computer has a virus infection, download these files onto a computer that is **not** infected.

To prepare to install downloaded files, follow these steps:

- | Step | Action  |
|------|---|
| 1.   | Use DeHqx, BinHex, Aladdin Systems' StuffIt, or a similar utility to convert files with an .hqx extension to a binary format that your computer can recognize. You can download applications that perform this conversion from most online services.<br><br>The conversion utility saves a copy of the file on your hard disk as a self-extracting archive with the extension .sea. |
| 2.   | Double-click VirusScan 3.0 Installer.sea to extract the file from its archived format. An extracted copy of the Installer application appears on your hard disk.  |
| 3.   | Before you continue, disable your system extensions and any other anti-virus software you might have running in order to prevent memory conflicts that could interfere with your installation.  |

To disable your system extensions, restart your computer, then press and hold SHIFT on your keyboard until you see the message "Welcome to Macintosh. Extensions Disabled." Consult the documentation for your other anti-virus software to learn how to disable it.

4. Skip to "Installation Steps" on page 19 to continue.

 **Important:** If you suspect that your computer already has a virus infection and you have downloaded VirusScan Prescan, go first to "Using Prescan" on page 17 before you proceed with installation. If you do not have Prescan available, install VirusScan according to the procedure outlined in "Installation Steps" on page 19, then immediately scan your hard disk. Waiting to scan your hard disk could subject your files, including VirusScan itself, to infection.

## Preparing to Install from CD-ROM

McAfee recommends that you remove other anti-virus software from your system and disable all system extensions that you don't need for access to your CD-ROM drive before you install VirusScan. See the user's guide for your other anti-virus software to learn how to remove it. To disable extensions, follow these steps:

- | Step | Action   |
|------|--|
| 1.   | Double-click the Extensions Manager control panel to open it. You'll find the Extensions Manager in the Control Panels folder inside your System folder. |




Extensions Manager

A list of all extensions and control panels installed on your system appears in the Extensions Manager dialog box.

- |    |  |
|----|--|
| 2. | Choose Save Set... from the Sets menu at the top of the dialog box, then type a name for the collection of extensions you now have enabled. Click OK to save this set and return to the Extensions Manager dialog box. |
| 3. | Choose All Off from the Sets menu.   |
| 4. | Select each of the extensions that must remain active in the list below the menu. Enable these extensions if you see them listed: Apple CD-ROM, High Sierra File Access, and ISO 9660 File Access.                     |
| 5. | Close the Extensions Manager window, then restart your computer.   |


*✎ After you finish installing VirusScan, enable your system extensions again by opening the Extensions Manager and choosing the name of the extensions set you saved in step 2 from the Sets menu. Enable VirusScanner68K or VirusScannerPPC, depending on the version you installed, then save your extensions set again. Restart your computer to have your changes take effect.*

6. Insert the VirusScan CD-ROM into your drive, then locate the VirusScan 3.0 Installer program icon. To continue, follow the procedure outlined in "Installation Steps" on page 19.

 *If you suspect that your computer already has a virus infection, you should perform a pre-installation scan of your hard disk before continuing. See "Using Prescan" on page 17 to learn how to perform this type of scan.*

## Preparing to Install from Floppy Disks



To prepare to install VirusScan from floppy disks, follow these steps:

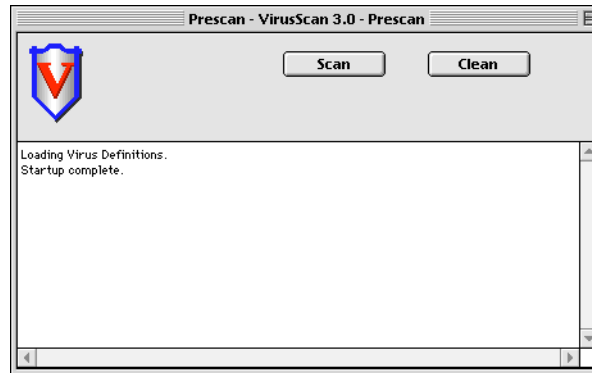
Step	Action
1.	<p>Disable your system extensions and any other anti-virus software you might have running in order to prevent memory conflicts that could interfere with your installation.</p> <p>To disable your system extensions, restart your computer, then press and hold SHIFT on your keyboard until you see the message "Welcome to Macintosh. Extensions Disabled." Consult the documentation for your other anti-virus software to learn how to disable it.</p>
2.	<p>Insert the first VirusScan floppy disk into your drive, then locate the VirusScan 3.0 Installer program icon.</p> <p> <i>If you suspect that your computer already has a virus infection, you should perform a pre-installation scan of your hard disk before continuing. See "Using Prescan" on page 17 to learn how to perform this type of scan.</i></p>
3.	<p>To continue, follow the procedure outlined in "Installation Steps" on page 19.</p>



## Using Prescan

The CD-ROM and floppy disk versions of VirusScan come with a Prescan, a utility you can use to check your system before you install VirusScan. You can also download this file from the McAfee website. If you suspect that your computer system already has a virus infection, you should run Prescan before you continue with installation. Follow these steps:

- | Step | Action   |
|------|--|
| 1.   | Shut down your computer, then wait for five seconds before turning it on again. Do not restart or reset your computer, as viruses can remain active in memory through a brief power loss.  |
| 2.   | When you turn your computer on again, disable your system extensions by pressing SHIFT on your keyboard until you see the message "Welcome to Macintosh. Extensions Disabled."   |
| 3.   | <p>If your copy of VirusScan comes on CD-ROM, insert the disc into your drive. If VirusScan comes on floppy disks, verify that the disk that contains Prescan is locked, then insert it into your floppy drive. If you downloaded the Prescan files from the McAfee website, convert the files from .hqx to binary format, then extract them to a clean, newly formatted floppy disk. Next, lock the disk, then insert it into your floppy drive.</p> <p> <i>A locked floppy disk shows two holes near the edge of the disk opposite the metal shutter. If you don't see two holes, look for a plastic sliding tab at one of the disk corners, then slide the tab until it locks in an open position. Because no software can save to a locked disk, viruses cannot infect files stored on one.</i></p> |
| 4.   | <p>Locate the VirusScan Prescan program icon on your CD-ROM or floppy disk, then double-click it to start. Prescan loads the virus definition files included on the disk and readies itself to begin scanning (see Figure 2-1 on page 18).</p> <p> <i>Do not copy the contents of the Prescan folder from your CD-ROM or floppy disk onto your hard disk—doing so exposes the Prescan application to potential virus infection.</i></p>   |



**Figure 2-1. The Prescan main window**

5. Click Scan to examine your hard disk for viruses. Click Clean to remove any virus infections present on your hard disk.
6. Choose the network or local hard disk volume, the folder, or the file that you want to scan from the directory dialog box that appears.

Next, click the Scan button or the Clean button at the bottom of the dialog box.

7. VirusScan immediately examines the volume you have chosen and reports its progress in Prescan's main window. You can start consecutive scan or clean operations by repeating Steps 5 and 6 as Prescan examines your disk.

When Prescan finishes its scan, it reports its results in the main window.

8. Quit the application, then drag the Prescan floppy disk icon to the Trash to eject it.

To continue, follow the steps listed in "Installation Steps" on page 19.

*✎ If your computer continues to display the same symptoms it did before you scanned your hard disk, your problem might not be the result of a virus. See "Other Sources of System Problems" on page 44 for details.*

## Installation Steps

Step	Action
1.	Double-click the VirusScan 3.0 Installer icon. A VirusScan introduction screen appears. Click Continue.
2.	The installer displays the VirusScan product license agreement. Review the agreement, then click Agree to continue.  To print the license text for your reference, click Print. To save the license as a text file, click Save.
3.	The next dialog box tells you the disk space requirements for VirusScan. You may install this version on top of previous VirusScan versions, but you should remove other anti-virus software. Click Install to continue.  The installer copies the VirusScan application to your desktop, along with three text files: McAfee Read Me First; McAfee What's New; and McAfee Contact Information. It also places the VirusScanner extension in the Extensions folder and the VirusScan support files in the Preferences folder inside your System folder.
4.	The installer tells you that you must restart your computer to use VirusScan. Click Restart.  VirusScan loads the VirusScanner extension as your computer restarts. Be sure to read the text files located on your desktop—they contain important additions and updates to this manual, along with licensing and McAfee contact information.

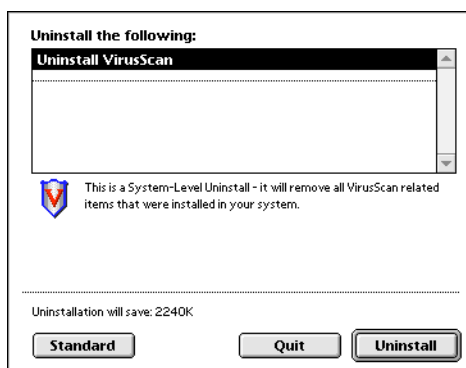
Once started, the VirusScanner extension provides immediate protection, automatically checking for viruses according to its default configuration options. You can change these options and set specific tasks for the VirusScanner extension to perform either with the Config Wizard or with the VirusScan application. Double-click the VirusScan icon on your desktop to get started.

If you have never used it before, the VirusScan application starts you out in the Config Wizard. To learn more about how to use the Config Wizard, see the following chapter in this guide. If you already have experience with VirusScan, or want to set scanning tasks beyond the scope allowed by the Config Wizard, click Configure VirusScan Manually in the VirusScan Wizard window. See “Using the VirusScan Application” on page 29 to learn how to set configuration options that suit your needs.

## Uninstalling VirusScan

To remove VirusScan for Macintosh from your computer, follow these steps:

- | Step | Action  |
|------|---|
| 1.   | Double-click the VirusScan 3.0 Installer icon. A VirusScan introduction screen appears. Click Continue.                         |
| 2.   | The installer displays the VirusScan product license agreement. Click Agree to continue.  |
| 3.   | The next dialog box tells you the disk space requirements for VirusScan. Click Custom to display the Custom Install dialog box. |
| 4.   | Press and hold OPTION on your keyboard to change the Install VirusScan option to Uninstall VirusScan (Figure 2-2).              |



**Figure 2-2. The Custom Install dialog box (Uninstall option)**

5. Verify that you have the Uninstall VirusScan option selected, then click Uninstall.
6. The installer tells you that you must restart your computer to use VirusScan. Click Restart.

## Creating a Custom Installer


If you administer a Macintosh network and want to standardize your anti-virus security measures easily and reliably, you can create a custom version of the VirusScan installer to distribute those scan tasks that you want each of your users to run from their own computers. You can then place the custom installer on a network volume available to all users or distribute the installer on floppy disk.

To create a custom installer, follow these steps:

1. Install VirusScan according to the installation instructions outlined earlier in this chapter.
2. Create the scan tasks you want each of your users to run from their own computers and enter the administration information you want them to see.

To learn how to create custom scan tasks, see “Scheduling Scan Tasks” on page 32. To learn about entering administration information, see “Saving Admin Information” on page 40.

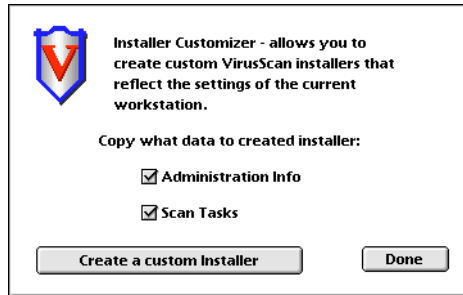
3. Locate the McAfee Customizer program icon on the VirusScan CD-ROM, then double-click it to start the application.

 *The Customizer application comes only with licensed corporate CD-ROM distributions of McAfee's VirusScan Security Suite and the multi-platform VirusScan CD-ROM. Licensed McAfee corporate customers can also download Customizer from the McAfee website. Customizer does **not** come with retail or evaluation versions of VirusScan for Macintosh.*

## 2 Installing VirusScan Creating a Custom Installer

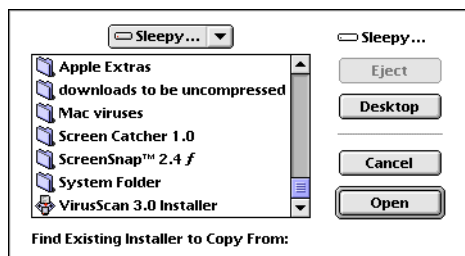
---

After a brief introduction screen, Customizer displays its main window (see Figure 2-3).



**Figure 2-3. The Customizer main window**

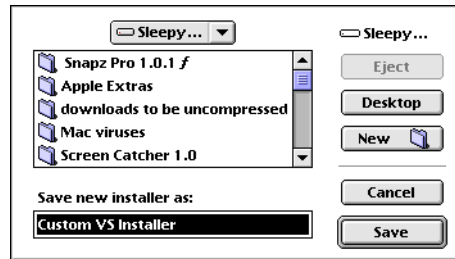
4. Select the elements you want to include in your custom installer:
  - **Administration Info.** Select this to include the information you entered in VirusScan's Admin Info dialog box. This includes contact information your users need to reach you, whether users can scan other volumes on the network from their machines, and other options.
  - **Scan Tasks.** Select this to include the scan tasks you want each user to run. Customizer takes this information from the VirusScan application on your local computer.
5. Click Create a Custom Installer.
6. In the directory dialog box that appears, locate a copy of the VirusScan installer on your CD-ROM, on your hard disk, or on floppy disk (Figure 2-4)



**Figure 2-4. The Customizer directory dialog box**

7. Click Open.

Customizer displays a Save As dialog box (Figure 2-5).



**Figure 2-5. The Customizer Save As dialog box**

8. Enter a name and choose a location to save your custom installer, then click Save.

Customizer copies the administration information and scan tasks stored in the VirusScan copy on your hard disk and creates a new VirusScan installer.

9. Distribute the custom installer over your network. Each copy your users install will contain the scan tasks and administration information you specified.

*McAfee provides you with the Customizer application to help you administer your network security policies. You may use it to install only as many VirusScan copies as your license agreement permits. For questions about the terms of your license agreement, please contact McAfee Customer Care.*

# 3

## Using Config Wizard

### Setting Basic Scanning Properties

VirusScan comes with a default set of configuration options that enables it to begin scanning for viruses as soon as you install it. With VirusScan's extensive configuration options, however, you can tailor the application to your own particular needs. To take advantage of some of those options, use the Config Wizard utility to determine which disks to examine, when to examine them, and what to do when you find a virus. To get started, double-click the VirusScan icon on your desktop.

#### Starting Config Wizard

When you start it for the first time, the VirusScan application launches the Config Wizard for you. To open the Wizard yourself, choose Config Wizard from the File menu. The window shown in Figure 3-1 appears.

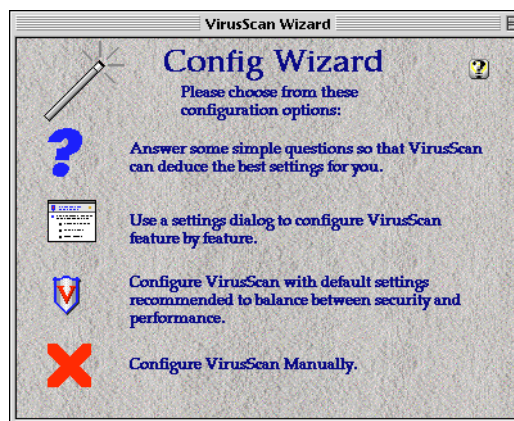






Figure 3-1. The Config Wizard window



### 3 Using Config Wizard Setting Basic Scanning Properties

---

The Config Wizard offers you four ways to set your configuration options. You may:

- Answer questions about how you work with your computer and how often you download or receive software from colleagues, the Internet and other sources. Click  to start the VirusScan Interview.
- Specify the options you want the VirusScanner extension to use in a settings dialog box. Click  to open the VirusScan Settings dialog box.
- Configure VirusScan with a default set of options designed to provide you with security without degrading your computer's performance. Click  to use this default set of configuration options.
- Specify tasks for the VirusScanner extension to perform. This is the most flexible option of those available through the Config Wizard. Click  to open the Scan Tasks dialog box.

#### The VirusScan Interview

This dialog box (Figure 3-2) consists of a series of questions that focus on how often you receive software and data files from outside sources—colleagues, a network, the Internet, and others—and how that software and data arrives, whether via floppy disk, e-mail, or over a network. The Config Wizard uses your responses to these questions to determine how often to scan your hard disk, whether to scan floppy disks, and which events should trigger a scan. First-time VirusScan users should use this option.

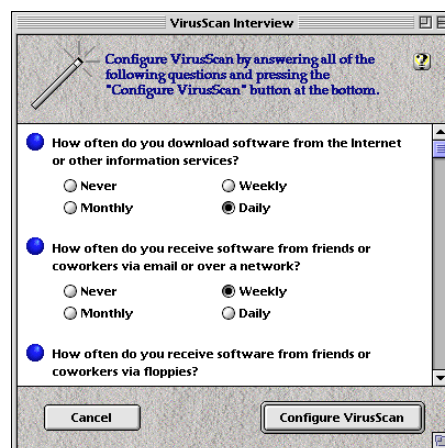


Figure 3-2. The VirusScan Interview

### 3 Using Config Wizard Setting Basic Scanning Properties

---

Choose the answers that most closely resemble your own situation, scrolling down the dialog box and clicking the buttons that correspond to your choices. When you have answered all questions, click Configure VirusScan to use the options you set and close the dialog box. Click Cancel to close the dialog box without choosing any options.

#### The VirusScan Settings dialog box

This dialog box (Figure 3-3) lets you take a more active role in deciding how and when you want the VirusScanner extension to look for viruses than does the VirusScan Interview. Options that you have direct control over include which events trigger a scan, which actions VirusScan takes when it finds a virus, whether it should examine compressed files, and whether it should use changes in a file's characteristic "fingerprint" as a basis for beginning a scan.

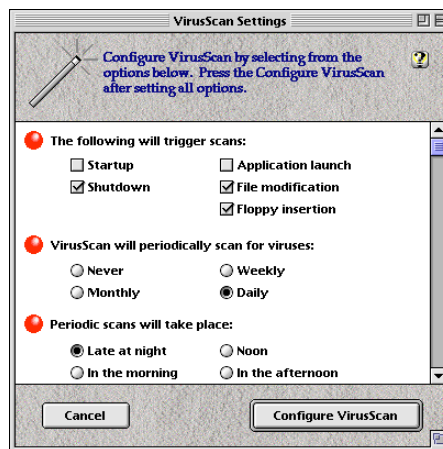


Figure 3-3. The VirusScan Settings dialog box

Other options in this dialog box give you indirect or approximate control over how the VirusScanner extension behaves. To control these options more precisely, choose Configure VirusScan Manually in the VirusScan Wizard dialog box.

Choose the VirusScan settings you want to use, scrolling down the dialog box and clicking the buttons that correspond to your choices. When you have finished, click Configure VirusScan to use these options and close the dialog box. Click Cancel to close the dialog box without choosing any options.

## VirusScan default options

Use this set of options to guard against virus infection without significantly slowing down most of your computer's operations. The protection afforded by this set of options is limited and represents McAfee's best judgment about what constitutes a good balance between protection and performance. The assumptions built into these settings might not describe your work habits and needs correctly. If you want more control, therefore, choose a different configuration method.

## Manual configuration

This method offers you precise control over what the VirusScanner extension does. VirusScan collects the options you choose here into lists of tasks for the extension to perform. Each task consists of:

- An event that triggers a scanning operation—starting an application, reading a floppy disk, or reaching a scheduled time, for instance.
- A scanning target—local and remote hard disks or floppy disks, for example.
- The action that VirusScan should take when it finds a virus.
- Any sounds or messages you want the program to use to alert you when it finds a virus.
- Any applications, including AppleScript applets, that VirusScan should start when it finds a virus. VirusScan comes with applets that let you notify other people via e-mail when the VirusScanner extension detects a virus.

Choosing Configure VirusScan Manually in the Config Wizard window is the same as launching the VirusScan application and clicking the Scan Tasks button—both actions open the Scan Tasks dialog box. See “Using the VirusScan Application” on page 29 for more information.

## Closing and reopening Config Wizard

Choosing any configuration method except the Default Settings method closes the Config Wizard window and opens the dialog box for the method you chose. To close the Config Wizard window after choosing the Default Settings method, choose Quit from the File menu.

To change any of the options you set with the Config Wizard, double-click the VirusScan program icon to start the application, then choose Config Wizard from the File menu. Once you have opened the Config Wizard, choose the same method you used to specify your configuration options earlier, then edit them to suit your needs.

## A note about Config Wizard

Scan tasks govern all VirusScan operations, whether you start a scan yourself or schedule a scan to run later. When you specify configuration options in Config Wizard, VirusScan generates a task or set of tasks for the VirusScanner extension to perform. VirusScan also includes a default set of scan tasks that ensure its effectiveness as soon as you install it. These default tasks also control how VirusScan operates when you choose Scan Now or Clean Now from the Scan menu in the VirusScan application.

For the most part, you can use either Config Wizard or the Scan Tasks dialog box to specify the options you want. The Config Wizard, however, is easier to use and includes some options not available in the Scan Tasks dialog box, such as the ability to set some options for all scheduled tasks at once. The Scan Tasks dialog box, on the other hand, offers you more precise control over each option, but is more complex to administer. See “Using the VirusScan Application” on page 29 to learn more about the Scan Tasks dialog box.

# 4

## Using the VirusScan Application

### Getting Started

The VirusScan application controls how the VirusScanner extension behaves—when it performs a scan, which parts of your computer system it examines, and what it does when it finds infected files. You can use the application to tell the VirusScanner extension to scan a hard disk, floppy disk, or other volume immediately, or you can use it to schedule tasks for the extension to perform automatically.

*✍ The VirusScan application does not need to be running for the VirusScanner extension to work. After you schedule the tasks you want the extension to perform, quit the VirusScan application—the extension remains in your computer's memory, waiting for the triggering events you specify to begin scanning operations.*

To start the application, double-click the VirusScan icon, which by default appears on your desktop. The VirusScan main window (Figure 4-1) appears.

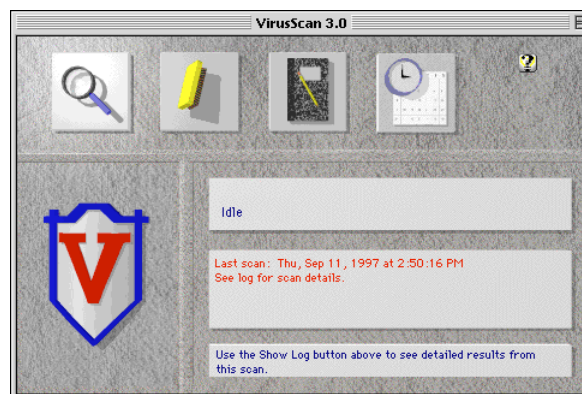



Figure 4-1. The VirusScan main window

## Performing Immediate Scans



To have VirusScan immediately search for viruses on a floppy disk, on a local or remote hard disk volume, or in a file or folder, follow these steps:


- | Step | Action   |
|------|--|
| 1.   | Click  in the VirusScan application main window, or choose Scan Now from the Scan menu. You can also drag the icon for the volume you want to scan onto the VirusScan application icon. |
| 2.   | In the directory dialog box that appears (Figure 4-2), choose the file, folder, disk, or disk volume that you want to scan.  |



**Figure 4-2.** The Scan directory dialog box


3. Click the Scan button at the bottom of the dialog box.

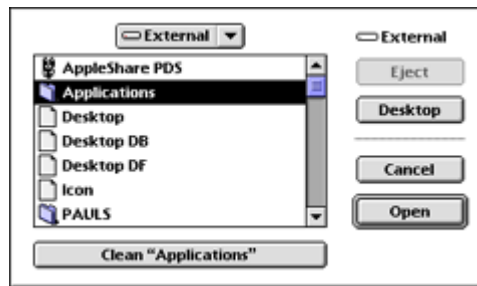
VirusScan immediately examines the volume you have chosen and reports its progress in the main window. To pause a scan operation, click  at the bottom left of the main window. To stop a scan operation altogether, click  or press **⌘ + .** (COMMAND+PERIOD).

If the VirusScanner extension finds an infected file, it plays a warning sound and displays an alert message in the main window. The message identifies the virus it found and the infected file that contains it, along with the file's last modification date. The program records the same information in its activity log. Click  in the main window, or choose Show Log from the Scan menu, to display the VirusScan Activity dialog box. See "Viewing and Printing the VirusScan Activity Log" on page 39 for more details.

## Cleaning Infected Files



To have VirusScan immediately clean virus-infected files on a floppy disk, a folder, or a local or remote hard disk volume, follow these steps:

- | Step | Action  |
|------|---|
| 1.   | Click  in the VirusScan application main window, or choose Clean Now from the Scan menu. |
| 2.   | In the directory dialog box that appears (Figure 4-3), choose the file, folder, disk, or disk volume that you want to scan.   |



**Figure 4-3. The Clean directory dialog box**


3. Click the Clean button at the bottom of the dialog box.

VirusScan immediately begins removing virus code from files stored on the volume you have chosen. To pause a cleaning operation, click  at the bottom left of the main window. To stop a cleaning operation altogether, click  or press **⌘ + .** (COMMAND+PERIOD).

As the VirusScanner extension finds and cleans infected files, VirusScan plays a warning sound and displays an alert message in the main window. The message identifies the virus it found and the infected file, and reports whether VirusScan successfully cleaned the file.

*Some infections corrupt a file thoroughly and cannot be removed. McAfee recommends that you delete infected files that VirusScan cannot clean or files that it identifies as “damaged,” and replace them with uninfected backup copies.*

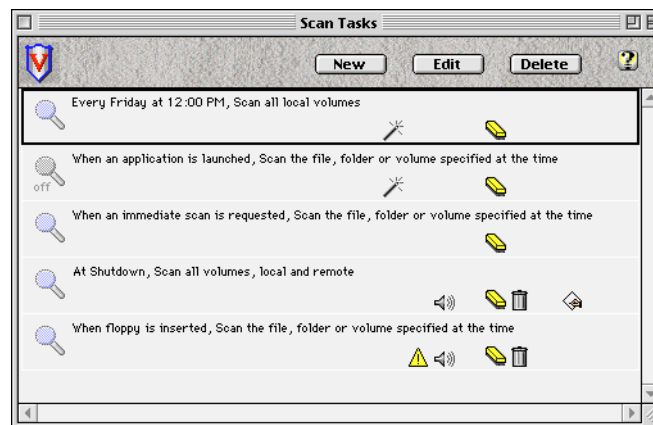
## 4 Using the VirusScan Application Scheduling Scan Tasks

VirusScan records the same information you see in the main window in its activity log. Click  in the main window, or choose Show Log from the Scan menu, to display the VirusScan Activity dialog box. See “Viewing and Printing the VirusScan Activity Log” on page 39 for more details.



## Scheduling Scan Tasks

Once you have dealt with any immediate virus infections on your system, you can have the VirusScanner extension keep your system free of viruses automatically by scheduling scanning tasks for it to perform. You might already have used the Config Wizard (see “Using Config Wizard” on page 24 for details) to configure a basic set of scanning tasks that protect your system. After you have some experience with VirusScan, however, and a better idea of what and when you want it to scan, you can use the VirusScan application to create a detailed scanning regimen, change options you chose in the Config Wizard, or delete tasks you no longer need performed.

To add, schedule, or delete a task, click  in the VirusScan main window or choose Schedule Task from the Scan menu. The Scan Tasks dialog box (Figure 4-4) appears.



**Figure 4-4. The Scan Tasks dialog box**

This dialog box lists all of the tasks that you have asked the VirusScanner extension to perform. The task list indicates which part of your computer system VirusScanner examines, when it conducts its scan, what it does when it finds a virus, and any other actions you have asked it to take. The magnifying glass beside each summary indicates active tasks  and inactive tasks .



## Adding or editing tasks

To add a task to the list, click New at the top of the Scan Tasks dialog box. To edit an existing task, select one of those listed, then click Edit. The Task Description dialog box appears, with the Trigger property page selected (Figure 4-5).



**Figure 4-5. The Task Description dialog box**

Each task consists of a set of configuration options, much like those you set initially with the Config Wizard. The Task Description dialog box divides the components of each task into five property pages, each of which offers you several options for scheduling a VirusScan task. Click each tab in turn to specify all of the options for your task—see the following sections for descriptions of the options available.


When you have finished choosing your options, verify that the Task Enabled checkbox is selected. To protect the task definitions you create from unauthorized changes, click the Task Password Protected checkbox, then enter a password in the dialog box that appears. Enter the password again for verification, then click OK to close the dialog box.

*✍ The password protection option is especially useful for system administrators who want to ensure data security for machines in their care. To change any task options, you must click Edit in the Scan Tasks dialog box, then enter the password you supplied earlier. Clear the Task Password Protected checkbox to disable protection.*


Finally, click OK to activate the task and close the Task Description dialog box.

## Trigger

Use this property page to tell VirusScan when it should begin the task. You can specify a particular time, either immediately or in the future; a recurring time, such as daily, weekly, or monthly; or an event. Possible events include starting or shutting down your computer; launching an application; or inserting a floppy disk. You can also have VirusScan look for viruses whenever the identifying characteristics of your files change.


 *Setting a File Modification trigger is ideal for protection against infection from Internet downloads and e-mail attachments. Because it tells the VirusScanner to scan files as they are created, this trigger eliminates the need to store downloaded files and attachments in a separate folder for later scanning. Using this trigger can, however, increase the time your computer takes to download files or e-mail.*

Choose a trigger from the pop-up menu at the top of the dialog box. If you chose a recurring time other than daily, you also must specify a particular day of the week or of the month, along with a particular time. If you chose a one-time scan, you must specify the month, day, year, and time. You do not need to specify a time for tasks keyed to events.

 *If you have specified an event trigger for another task, you may not choose the same event trigger for the current task. You may, however, choose as many time-based triggers as you want.*

## Target

Use this property page to tell VirusScan what it should scan. You can specify all hard disk volumes, local volumes (disks connected directly to your computer), remote volumes (disks or servers available over a network), or a specific file, folder or disk volume. A separate option targets the System folder specifically.

 *Choosing On Launch, Floppies, or File Modification as your event trigger disables the options shown in the Target property page because these event triggers also specify their targets.*


The Fingerprint option improves VirusScan's performance by telling it to scan only those files whose identifying characteristics have changed since your last scan. McAfee recommends that you choose Optimal, the default option, from the pop-up menu. This restricts each scan to newly created files or files that have changed, which improves VirusScan's performance considerably.

Choose None to scan all files, whether they have changed or not. Choose Maximum to perform a full integrity check on all files and restrict subsequent scanning to new or modified files.

To scan files compressed with the shareware or commercial versions of Aladdin Systems' StuffIt, click the Scan Compressed Files checkbox.


### Action

Use this property page to tell VirusScan what to do when it finds an infected file. You can have it clean the file, move the file to the Trash, or ask you what it should do. Click the checkboxes beside your choices.

 *The Trash can serve as a quarantine area for infected files. Files stored there cannot be opened and therefore cannot infect other files.*

*Choosing Shutdown, File Modification, or On Launch as your event triggers in the Trigger property page disables the Prompt User for Action checkbox in the Action property page. Asking for a prompt would interfere with your computer's shutdown and file launching procedure.*

VirusScan normally records its actions in its default activity log. To have it copy log information to another file, click the Extra Log File checkbox, then choose the file you want to use from the dialog box that appears. Use this option when you want to share your activity log with others, or open it with a text editor.

 *Before you can choose a file to serve as your extra log, you must first create one with a text editor—SimpleText, for example. Save your file as ASCII or text-only.*

### Alert


Use this property page to specify how VirusScan should tell you when it finds a virus. You can have it play a warning sound, or you can have it play a custom voice message. VirusScan uses Apple's text-to-speech technology to speak the message you enter in the Notify property page. Click the checkboxes beside your choices.

If you told VirusScan to play a sound, choose which sound it should play from the pop-up menu. Available sounds include the default warning, system alert beeps and any other sound you have installed in your System file. Consult your Mac OS documentation to learn how to add new sounds to the System file.

## Notify

Use this property page to specify how VirusScan should tell you and others when it finds a virus. You can have it launch a particular application or display a custom alert message.


VirusScan includes two complete AppleScript applets that send alert messages either via the Eudora e-mail client or via Claris E-mailer. If you have either of these e-mail clients, choose the appropriate applet from the pop-up menu. When it finds an infected file, VirusScan sends an e-mail message to the address specified in the Admin Information dialog box—usually your network administrator. If you want VirusScan to start another application, choose Other from the pop-up menu.

 *VirusScan includes an example AppleScript applet you can use as a model to enable this type of notification for other e-mail clients. You'll find the example script in System Folder:Preferences:VirusScan:Launch Scripts. Use the AppleScript Script Editor to modify the example to suit your needs. For more information, consult the documentation for AppleScript.*

To have VirusScan display a custom message when it finds a virus, select the Custom Alert Message checkbox, then enter the message you want to see in the text box provided. VirusScan will also speak this message if you have Apple's text-to-speech extensions enabled and if you have selected the Voice Messages checkbox in the Alert property page.

## Deleting tasks


To delete a task from the task list, select one of those listed in the Scan Tasks dialog box, then click Delete. If you have protected the task with a password, you must first select the task, click Edit, enter the password you chose to open the Task Description dialog box, then clear the Task Password Protected checkbox.

 *VirusScan does not ask you to confirm that you want to delete a task, so be sure that you want to delete it before you do.*

You may delete any of the tasks listed except the Immediate Scan task. VirusScan uses the configuration options set in this task to guide its Scan Now and Clean Now operations. You can change the configuration options assigned to this task, but you may not remove it from the Scan Tasks list.


## Exporting tasks

VirusScan's Export feature enables you to share any of the tasks you create with other VirusScan users. This feature is particularly useful for network administrators who want to standardize their anti-virus security measures across all Macintosh computers on the network.

 *McAfee distributes a utility that corporate network administrators can use to install custom versions of VirusScan preconfigured with scanning tasks that they choose to include. See "Creating a Custom Installer" on page 21 for more information.*

To export a task or a set of tasks for others to use, follow these steps:

Step	Action
1.	Configure the tasks you want to export by choosing options from the Task Description dialog box. Refer to the sections on pages 26–29 for descriptions of each of the options available.

 *To prevent those who use the exported task from changing the configuration options you set, assign a password to your task when you create it. Select the Task Password Protected option, then enter a password—the task retains that password when exported.*

- |    |   |
|----|---|
| 2. | Select the task you want to export from the list shown in the Scan Tasks dialog box. You may select only one task at a time for export. |
| 3. | Choose Export Task from the Scan menu.  |

VirusScan saves the exported task as an application tailored specifically to update other VirusScan copies with the task list you create. You can distribute the update application via the network, or using floppy disks, e-mail, or other methods. Users who receive the application simply double-click it to add the exported tasks to their task list.

- |    |  |
|----|--|
| 4. | In the dialog box that appears, click New if this is the first task you are exporting. Click Append if you are adding this task to an existing update application. |
|----|--|

## 4 Using the VirusScan Application Scheduling Scan Tasks

---

5. Choose a name and a location for a new update application in the Save As dialog box, then click Save. The default filename for the application is VirusScan Updater.

To append a task to an existing application, select the application you want to use in the directory dialog box that appears, then click Open.

VirusScan saves the update application with the name you give it, in the location you specify.

### Excluding items from scans

Excluding items that are not susceptible to virus infection from regular scanning operations can significantly improve VirusScan's performance. Data files, locked files, or files in locked folders, for example, rarely pick up viruses. Use this feature with care, however, since VirusScan ignores excluded files. If they do get infected, they can continuously reinfect other files without detection.

To create an exclusion list, follow these steps:

- | Step | Action   |
|------|--|
| 1.   | Choose Exclusion List from the Scan menu to open the Exclusion List dialog box (Figure 4-6). |

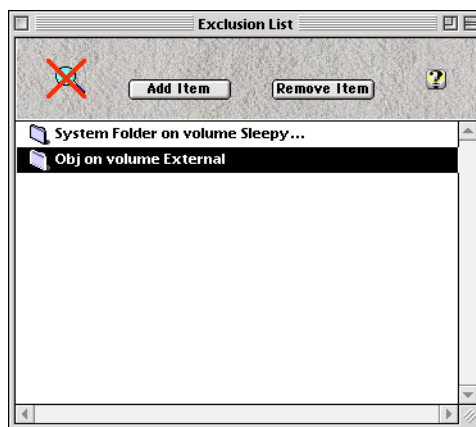


Figure 4-6. The Exclusion List dialog box

2. Click Add Item.
3. In the directory dialog box that appears, choose the file, folder, or hard disk volume you want VirusScan to ignore when it conducts a scan, then click Exclude.


To remove an item from the list, select it, then click Remove Item. This tells VirusScan to examine the item when it conducts a scan.

4. When you have finished editing the list, click the close box to close the Exclusion List dialog box.


## Viewing and Printing the VirusScan Activity Log

VirusScan summarizes all of the actions it takes during its scanning operations in a file called VirusScan Activity. You can open, view and print this file from within VirusScan or using any word processing program that can read plain text files. To locate the VirusScan Activity file, look in the VirusScan folder in the Preferences folder. You'll find the Preferences folder in your System folder.


### Viewing the activity log

To view the activity log from within VirusScan, click  in the VirusScan main window. Scroll through the file to review the actions VirusScan took during scheduled scan operations.

### Printing the activity log

To print the activity log from within VirusScan, click  in the VirusScan main window to open the file, then choose Print from the File menu. VirusScan uses your default printer and print settings.


### Copying the activity log to another file

You can extract any portion of the activity log and copy it to another document or file—to include it as part of a report or memo to other users, for instance. Click  in the VirusScan main window to open the file, then choose Select All from the Edit menu to copy the entire log. To copy portions of the log, highlight the text you want to copy. Use standard Macintosh copy and paste commands, or keyboard shortcuts, to copy the text to the Clipboard or to another open file.


## Saving Admin Information

VirusScan gives system administrators tools they can use to standardize security for all Macintosh computers on the network. If you administer a Macintosh network, you can store your name, your pager number, and your e-mail address where your users can find it easily. You can also enable or disable scan tasks for each computer on the network.

To save contact information for your users, choose Admin Information from the File menu. Enter your name, pager number and e-mail address in the text boxes provided. VirusScan users can choose this same command to see the information you entered.

 *If you have set VirusScan to notify you when it finds a virus via Eudora, Claris E-mailer, or another e-mail client, alert messages go to the e-mail address you enter here. To learn how to use the Notification property page to set up e-mail notification, see "Notify" on page 36.*

To allow VirusScan to scan hard disk volumes on other network computers, select the Allow Remote Volume Scans option. To disable all scanning functions for your computer, select the Disable All Functions option.

 *Disabling all scanning functions deactivates all of the triggers set in all scheduled tasks until one of three events occurs:*

- *The user drags and drops a file, folder or other item onto the VirusScan program icon;*
- *The user starts the VirusScan application again; or*
- *The user restarts his or her computer.*

*McAfee does not recommend deactivating all scanning tasks because it leaves your system vulnerable to virus infection if you forget to reactivate scanning.*

Enter a password to keep users from changing the options you set here without authorization. Click OK to close the Admin Information dialog box when you have finished setting these configuration options.






# 5



## Tips and Troubleshooting

---

### Getting Help

VirusScan includes a full implementation of Apple's Balloon Help utility, which you can use to see descriptions of buttons, dialog box elements, and other VirusScan components as you work with the application. To activate Balloon Help for VirusScan, click  in the VirusScan main window, the Scan Tasks dialog box, or the Task Description dialog box. You may also choose Show Balloons from the  menu.

* Enabling Balloon Help for VirusScan also enables Balloon Help for all other applications that support it, including the Finder.*


Once enabled, help balloons appear whenever you position your cursor over a screen element that has an associated help topic. To deactivate Balloon Help, click  again in one of VirusScan's dialog boxes or choose Hide Balloons from the  menu.

### About the VirusScanner Extension

Technically, the VirusScanner extension is not a system extension. Rather, it is a “background application,” or a program that executes in the “background” on your Macintosh. You cannot interact directly with applications of this type. Instead, you must use a “foreground application,” like the VirusScan application, to control their behavior. Background applications communicate with foreground applications via Apple events.

The VirusScanner extension starts running when you start your computer. It continues to run as long as it has scanning tasks to complete; if it has no tasks scheduled, it remains idle.

Some scanning tasks—scanning all applications as they start, for example—can keep the VirusScanner extension busy almost constantly. If you value system performance over system security, consider setting VirusScan up with *no* tasks beyond the required Immediate Scan task. With no tasks to complete, the VirusScanner extension simply waits until you tell it to perform an immediate scan or a cleaning operation. This allows your system to continue normal operations without the delays associated with scanning.

 *McAfee does not recommend this configuration because it leaves your system vulnerable to virus infection if you forget to perform regular scans.*

## Renaming the VirusScanner extension

McAfee recommends that you do not rename the VirusScanner extension, because an extension's name governs the order in which it loads into your computer's memory. VirusScanner needs to load early in the extension chain, so that it can protect against INIT viruses. The INIT 1984 virus, for example, spreads from extension to extension at system start-up. If the VirusScanner Extension has already loaded, it can detect and block the INIT 1984 virus before it attacks.

If you absolutely must rename the extension, keep it as near to the top of the extension list, alphabetically, as you can. Scan any extensions you place ahead of VirusScanner in the extension chain to ensure they are not infected, as VirusScan might not be able to detect or block them.


## What if another extension needs to be loaded first?

A number of other popular extensions also require that they load first. Before installing such an extension, scan it with VirusScan to make sure it is not infected by INIT 1984 or any other virus. Depending on its name, the extension might load before or after VirusScanner, but if the extension is virus-free it should not cause any problems.

## Disabling the extension


You should never remove the VirusScanner Extension or disable it from the Extensions Manager control panel. If you do, you cannot start the VirusScan application, and your system is vulnerable to virus infection.


Some software manuals might instruct you to remove VirusScanner before installing software. If you are concerned about VirusScanner conflicting with an installer, you might want to disable the File Modification trigger and any floppy scanning task you have scheduled, or select the Disable All Functions checkbox in the Admin Information dialog box. See “Adding or editing tasks” on page 33 or “Saving Admin Information” on page 40 for details. Disabling scanning tasks temporarily allows you to continue to protect your system from viruses without worrying about problems with installers.

 *No known cases exist where VirusScanner has interfered in any way with an installer.*

## Tips for Faster Scanning

- Use VirusScan’s Fingerprint feature to speed scanning time. Fingerprinting establishes a baseline identity for the files on your computer, then scans them only if they have changed since your last scan. To activate fingerprinting for a specific task, choose the task you want to change in the Scan Tasks dialog box, then click Edit. Next, click the Target tab, then choose the level of fingerprinting you want from the pop-up menu. Choose Optimal fingerprinting for the fastest scans. See “Adding or editing tasks” on page 33 for more details.

To activate the Fingerprint feature at once for all of the tasks you have scheduled, start the Config Wizard, then click  to open the VirusScan Settings dialog box. Click the Will Be On button beneath the VirusScan “fingerprint” option. See “Setting Basic Scanning Properties” on page 24 for more details.

 *Use this feature with caution—choosing options in the VirusScan Settings dialog box can overwrite the configuration options for other existing tasks that do not have password protection.*

- If your Macintosh can shut down unattended, create one task that scans only the System folder at start-up and a second task that performs a full scan on system shutdown. To learn how to schedule scanning tasks, see “Scheduling Scan Tasks” on page 32.
- Exclude data files, files in locked folders, and other files not susceptible to virus infection from scanning operations with the Exclusion List feature. See “Excluding items from scans” on page 38 for more information.

## Other Sources of System Problems

If your computer is behaving strangely, but VirusScan reports that your system is clean, you might not have a virus at all. Instead, you might have an extension conflict, a software error, incorrect software installations, or a hardware error. This section lists common sources of problems and recommended solutions.

- **Extension conflicts.** System crashes and unpredictable behavior often result from a memory or other type of conflict between two extensions, or between an extension and an application. To test for an extension conflict, restart your Macintosh and press SHIFT on your keyboard until you see the message “Welcome to Macintosh. Extensions disabled.” Try to replicate the actions you took when you had the problem. If your system behaves normally, an extension conflict, not a virus, is probably the source of the problem. Correct the extension conflict (see your Mac OS user’s guide for more information), then restart with extensions on.
- **Damaged desktop file.** Some users believe that their systems have a virus when they see altered icons in Finder windows. Usually a damaged desktop file, not a virus, causes this anomaly. To correct this problem, rebuild your desktop file. Press  $\text{⌘}+\text{OPT}$  (COMMAND+OPTION) on your keyboard during system start-up until you see a dialog box that asks you whether you want to rebuild your desktop file. Click OK to continue.

*✎ Depending on the Mac OS version you use, you might have to reenter comments you saved in the Get Info windows associated with your files. See your Mac OS documentation for details.*

- **Incorrect parameter RAM (PRAM).** Incorrect settings in your computer’s PRAM—the hardware component that keeps track of the time and date and provides other information for the System’s use—can cause odd behavior, especially in applications that rely on your computer’s clock to perform some operations. To reset, or “zap” the PRAM, restart your computer, then immediately press  $\text{⌘}+\text{OPT}+\text{P}+\text{R}$  (COMMAND, OPTION, P, and R) on your keyboard during the start-up cycle until your computer beeps and starts again. Release the keys and allow it to start normally.

*✎ You might need to reset certain parameter settings, including the current date and time, your sound level, and other settings.*

- Other software errors. Incorrectly installed software, corrupted software components, damaged hard disk file directories and other software-related problems can cause odd behavior. Common solutions for these problems include:
  - **Remove recently installed software.** Remove any software you installed recently to see if it might be the source of your problem. The software might contain an error, might have been installed or configured improperly, or might be damaged or corrupted. If, after removing the software, your computer returns to normal, try re-installing the software from your locked original master copy.
  - **Reinstall system software.** Damaged system files can cause a number of seemingly unrelated problems, including random crashes and freezes. If none of the other remedies you have tried works, try reinstalling your system software from the original floppies or the CD-ROM that came with your computer. For very serious cases, you might have to perform a “clean” system install, which means that you allow the system installer to overwrite all system files, not just to update those that have changed. See your Mac OS user’s guide for more information.
  - **Repair your hard disk directory.** Corrupted hard disk file directories or other software problems related to how your hard disk stores information can render needed files, folders or entire hard disks inaccessible. Use a hard disk repair utility, such as Apple’s Disk First Aid, to scan and repair your hard disk.
- **Hardware problems.** Some problems that appear as though they are software problems actually result from damaged or incorrectly configured hardware components. If your computer does not start from its hard disk, for example, check the cables and termination for any SCSI (Small Computer System Interface) devices—usually external hard disks, scanners, or similar peripherals—attached to your computer.

You may have up to seven devices (including your computer) on one SCSI “daisy chain,” and you must terminate the last device in the chain with a special resistor pack or with the device’s built-in terminator. Your computer, the first device in the chain, has built-in termination. Check to see that you have connected your cables properly, and that you do not have more than one terminated device—with the exception of your computer—on your SCSI chain.

# A

## Preventing Virus Infection

---

### Creating a Secure Environment

VirusScan is an effective tool for preventing, detecting, and recovering from virus infection. It is most effective, however, when used in conjunction with a comprehensive computing security program that includes a variety of safety measures, such as regular backups, meaningful password protection, user training, and awareness. This appendix provides additional recommendations to prevent virus infection.

To create a secure system environment and minimize your chance of infection, McAfee recommends that you:

- Update VirusScan regularly for the latest protection against new viruses and new virus strains. For more information about updating VirusScan, see “Updating your VirusScan database files” on page 47 for details.
- If you installed VirusScan from floppy disks, lock your disks by sliding the plastic write-protection tab on the back of the floppy to an open position. Keep these disks or your VirusScan CD-ROMs in a safe place. If your system is infected or damaged you can re-install your applications from the original, uninfected CD-ROMs or diskettes.
- Make backups of your hard drive at least once a week. Scan the backups to make sure they do not become infected.
- Scan every diskette before you install software from it, copy its files to your hard drive, launch an application from it, or start your computer with it. To scan a diskette quickly, drag its icon onto the VirusScan icon. To scan diskettes automatically as you insert them, create a Scan Task using floppy insertion as a trigger. See “Scheduling Scan Tasks” on page 32 for details.

- Scan all CD-ROMs, files copied from network resources, files downloaded from the Internet, and e-mail attachments before you open them. Although you may not save files on CD-ROMs, the CD-ROM disc manufacturer might have inadvertently stored a virus on the disc. Scanning for viruses before you copy files from the disc can prevent infection.
- If you are a network administrator, create password-protected tasks on your computer, then export them to other Macintosh systems on your network with VirusScan's Export Task feature. See "Exporting tasks" on page 37 for more details.

## Updating your VirusScan database files

New viruses (and variants of old ones) appear frequently and circulate throughout the Macintosh community. McAfee responds to these new viruses by regularly updating VirusScan's virus definition files and upgrading the application and extension. Each new update detects and removes new viruses, while upgrades may add new features to the VirusScan product.

### Updating virus definition files


To update your Virus Definition files, download the most recent update package from the McAfee website or from other electronic services (see "How To Contact McAfee" on page 9 for website and other addresses). Next, follow these steps:

Step	Action
1.	Use DeHqx, BinHex, Stuffit, or a similar utility to convert files with an .hqx extension to a binary format that your computer can recognize. You can download applications that perform this conversion from most online services.

The conversion utility saves a copy of the file on your hard disk as a self-extracting archive with the extension .sea. Be sure to save this copy in a folder separate from your current VirusScan files.

2. Double-click VirusDef 30xx 3.x.sea to extract the file from its archived format. The actual filename varies with each version.

An extracted copy of the Installer application appears on your hard disk.

 *At this point, as with all software you download from another source, you should perform a VirusScan check of the files you extract.*

3. Double-click the VirusDef 30xx 3.x program icon. The installer places the new definition files on your hard disk. To use these files, restart your computer.

### Downloading new VirusScan versions

You can download evaluation copies of new versions of McAfee products from the McAfee Web Site, the McAfee Bulletin Board System, or the McAfee forum available through various online services. For details, see “How To Contact McAfee” on page 9.

Always download and decompress the files in a folder separate from your current files.

### Recommendations for system administrators

If you manage Macintosh networks, laboratories, bulletin boards, or collections of public domain and shareware software, use the following recommendations to protect your environment against viruses. As you know, whenever many people share computers, viruses find many opportunities to spread. If you sell software, moreover, you also have a special responsibility to make sure that your software is free from infection. Implementing the following measures can reduce your risk:

- Install the VirusScanner extension on all of your startup disks.
- Verify that the floppy disks you use have no viruses by scanning frequently with VirusScan. Also, check to make sure that the VirusScanner extension is still installed and active on all of your startup disks. Open the Extensions Manager to see if VirusScanner appears in the active file list.



- Educate people in your organization about viruses and how to protect against them. Give them licensed copies of VirusScan and teach them how to use the application.
- Store software to which others need frequent access in write-protected folders on AppleShare server disks. Viruses cannot infect applications you have stored in folders that do not have the Make Changes privilege. Any computer that has a virus, on the other hand, can infect applications stored in unlocked server folders. Each computer that uses one of the stored applications can then spread the virus to other computers on your network that do not have the VirusScanner extension installed. Because some applications insist on writing to their own file or folder, you may not always be able to store applications in write-protected folders, but you should do so when possible.
- Check server disks frequently with VirusScan to make sure that they are uninfected. For best results, you should take the server offline and restart it with a locked copy of your Disk Tools disk or the Mac OS CD-ROM that came with your system. This way, you can be sure that VirusScan can examine all of the files on the server disk.
- Check all new software with VirusScan before you install it on a server.
- Back up your servers frequently. Run VirusScan just before each backup.
- The WDEF virus can cause serious performance problems if it infects an AppleShare server. To avoid these problems, never grant the Make Changes privilege on server root directories.
- Bulletin board system operators and others who maintain and distribute public domain software and shareware have a special responsibility to the Macintosh community. Please carefully test all new software before distributing it. Of course, you should also run VirusScan on all new software you receive.
- If you sell software, please check your master disks for virus infections before you send them out for duplication and distribution.


# B

## VirusScan Messages

---

### Error Messages

This section lists error messages that might appear in the VirusScan activity log and suggests actions to take if you encounter these messages. The messages in this table appear in alphabetical order.

Message	Error	Action
An error or inconsistency was detected while trying to repair this file.	<p>Your file was infected, and while attempting to repair it, VirusScan discovered something wrong with the file. The file may still be infected.</p> <p> <i>This error sometimes occurs when you attempt to use another anti-virus tool to repair the file before running VirusScan. Some anti-virus tools leave the application damaged in such a way that VirusScan cannot repair it properly.</i></p>	Scan the file again with VirusScan to find out if it is still infected. If it is still infected, you should delete it. If VirusScan reports that it is no longer infected, you can try running it to see if it works. It may be usable or it may be damaged in such a way that it cannot be used.


**B**Error Messages

---

Message	Error	Action
An I/O error occurred while trying to check this file.	A hardware error occurred while VirusScan was trying to read or write a file. This error usually means that the disk itself or the disk drive is not operating properly.	Try running VirusScan again on the same file. If the hardware problem is intermittent, it might work the second time.
An I/O error occurred while trying to repair this file. WARNING: This file may still be infected!	A hardware error occurred while VirusScan was trying to read or write a file. This error usually means that the disk itself or the disk drive is not operating properly.	Try running VirusScan again on the same file. If the hardware problem is intermittent, it might work the second time.
CRC Database Corrupted!	VirusScan could not update its Fingerprints database properly. This might be the result of low memory, low disk space, another program having crashed, or an improper or incomplete system shutdown.	Delete the VirusScan Fingerprints database and restart your Macintosh.
Data and resource fork errors encountered while CRCing this file.	The operating system returned an I/O error while VirusScan was Fingerprinting a file. A possible cause is damaged storage media.	Find and repair the cause of the I/O error.

**B**Error Messages

---

Message	Error	Action
Data fork error encountered while CRCing this file.	The operating system returned an I/O error while VirusScan was Fingerprinting a file. A possible cause is damaged storage media.	Find and repair the cause of the I/O error.
File infected by <virus name>.	Your file is infected by the virus named in the message.	Use VirusScan to clean the file.
File infected by an unknown strain of <virus name>.	Your file is infected by a strain of the WDEF or the CDEF virus that has not yet been reported.	Use VirusScan to clean the file.
File partially infected by <virus name>, but not contagious.	<p>Your file is partially infected by the virus named in the message, but the infection is not contagious. Such infections are not dangerous and they cannot spread to other files.</p> <p> <i>Files sometimes retain part of the infecting virus code when another anti-virus tool has an error or cannot complete an operation. In such cases, the other virus tool may remove part, but not all, of the infection.</i></p>	You may leave the infection in the file or you may use VirusScan to remove the infection.

**B**Error Messages

---

Message	Error	Action
File partially infected by nVIR A or nVIR B, but not contagious.	nVIR A and nVIR B are different viruses, but some of their parts are identical. It is possible for only those common parts to be present in an infected file. In this case, VirusScan has no way of knowing which virus originally attacked the file, so it issues this message.	You can use VirusScan to remove the infection. This is not necessary, however, since the files are not contagious.
Ran out of disk space accessing CRC database.	There was not enough disk space to open and use the VirusScan Fingerprints database.	Make more room on your hard disk by moving files elsewhere.
Ran out of memory accessing CRC database.	VirusScan could not allocate enough memory to open and use the VirusScan Fingerprints database.	Give VirusScan more memory. To do this, quit VirusScan, then select the VirusScan program icon in the Finder. Choose Get Info from the Finder's File menu, then enter the increased amount of memory that VirusScan can use in the text box provided. Next, start VirusScan again.
Resource fork error encountered while CRCing this file.	The operating system returned an error while VirusScan was Fingerprinting a file.	Find and repair the cause of the error. A possible cause is a damaged hard disk.
Scan canceled.	You canceled a scan or clean operation.	To complete the scan, start it over.



**B**Error Messages

---

Message	Error	Action
The disk is too full to repair this file. WARNING: This file may still be infected!	This error may occur if a disk is full and you attempt to repair an infected file on the disk. VirusScan requires a small amount of free space on the disk before it can repair a file.	Move some of the files off the disk to increase disk space, then run VirusScan again.
The inserted disk is uninitialized, damaged, or not a Mac disk. It cannot be scanned.	This error occurs if you insert a floppy disk that is not correctly formatted or that is damaged into a computer with no mouse or keyboard. The disk is ejected and not scanned.	Make sure the disk you are attempting to scan is formatted correctly and not damaged.

**B**Error Messages

---

Message	Error	Action
The resource fork of this file is damaged or in an unknown format. It cannot be checked.	<p>Macintosh files have two parts or <i>forks</i>: the resource fork and the data fork. When VirusScan checks a file, it tries to open the resource fork. This message means that the information stored in the resource fork is not valid. The data fork may still be intact and usable.</p> <p> <b>WARNING:</b> <i>A damaged application might still be infected and contagious. You should not attempt to use applications that have damaged resource forks.</i></p> <p> <i>You may see this error when an application makes non-standard use of the resource fork in its database files. These files are not really damaged and are still usable.</i></p>	For document files, this is usually not a problem. For applications and system files, this usually indicates that something is seriously wrong with the file and you should replace it with a copy of the file that you know is good.

**B**Error Messages

---

Message	Error	Action
There is not enough memory to check this file.	VirusScan did not have enough memory to check the file. This error is usually caused by applications that contain very large Code Resources. VirusScan must load these resources into memory to check them for viruses—if it does not have enough memory to do this, VirusScan returns this error message. A damaged file is another possible cause of this error.	Give VirusScan more memory. To do this, quit VirusScan, then select the VirusScan program icon in the Finder. Choose Get Info from the Finder's File menu, then enter the increased amount of memory that VirusScan can use in the text box provided. Next, start VirusScan again.
There is not enough memory to repair this file. WARNING: This file is probably still infected!	VirusScan did not have enough memory to check the file. This error is usually caused by applications that contain very large Code Resources. VirusScan must load these resources into memory to check them for viruses—if it does not have enough memory to do this, VirusScan returns this error message. A damaged file is another possible cause of this error.	Give VirusScan more memory. To do this, quit VirusScan, then select the VirusScan program icon in the Finder. Choose Get Info from the Finder's File menu, then enter the increased amount of memory that VirusScan can use in the text box provided. Next, start VirusScan again.



**B**Error Messages

---

Message	Error	Action
This file is busy and cannot be checked.	VirusScan could not open a file to check it because the file was already open with exclusive access by another application. This message should occur only on server disks.	For server disks, take the server offline and restart using a start-up floppy disk. This should avoid file busy errors.
This file is busy and cannot be repaired. Restart using a locked Apple "Disk Tools" disk and try running VirusScan again. WARNING: This file is still infected!	VirusScan could not open a file to check it because the file was already open with exclusive access by another application. This error is common when using System 7, or when scanning server disks.	For server disks, take the server offline and restart using a start-up floppy disk. This should avoid file busy errors. For other files, close the file and scan the disk again.
This file is busy and cannot be repaired. Restart using your locked "Virus Tools" disk and try running VirusScan again. WARNING: This file is still infected!	VirusScan could not open a file to check it because the file was already open with exclusive access by another application. This error is common when scanning server disks.	For server disks, take the server offline and restart using a start-up floppy disk. This should avoid file busy errors. For other files, close the file and scan the disk again.
This file is busy and cannot be repaired. To repair this file, rebuild the desktop. WARNING: This file is still infected!	The Finder's desktop file is infected, but it cannot be opened for repair because it is already being used.	The easiest way to remove the infection is to rebuild the desktop. Press COMMAND+OPTION as you restart your computer.

**B**Error Messages

---

Message	Error	Action
This file was damaged by the virus, and it cannot be repaired properly. You should delete the file and replace it with a known good copy.	<p>Viruses sometimes damage files in such a way that they cannot be repaired properly. In this case, VirusScan removes the virus from the file, but leaves the file damaged.</p> <p>For example, the T4 virus damages files when it infects them. Files infected by T4 cannot be repaired. If you attempt to repair a file infected by T4, you will get this error message.</p>	Do not attempt to use such a file. Delete it and replace it with a copy of the file that you know is not damaged or infected.
Unexpected error <error name>.	VirusScan could not determine the cause for an error that occurred.	Contact McAfee technical support.
Unexpected error <error name> occurred while trying to open this file for repair. WARNING: This file is still infected.	VirusScan could not determine the cause for an error that occurred.	Contact McAfee technical support.
WARNING: You do not have the proper privileges to access files in some of the folders. Some files in those folders may be infected!	VirusScan found an infection in a server folder for which you do not have the necessary access privileges.	To avoid this error, McAfee recommends taking the server offline and restarting it using a locked start-up diskette.

**B**Error Messages

---

Message	Error	Action
You do not have Make Changes privilege to the folder containing this file. It cannot be repaired. WARNING: This file is still infected!	VirusScan found an infected file in a server folder for which you do not have the necessary access privileges.	To avoid this error, McAfee recommends taking the server offline and restarting it using a locked start-up diskette.
You do not have See Files privilege to this folder. Files within this folder cannot be checked.	VirusScan encountered a server folder for which you do not have the necessary access privileges.	To avoid this error, McAfee recommends taking the server offline and restarting it using a locked start-up diskette.
You do not have See Folders privilege to this folder. Folders within this folder cannot be checked.	VirusScan encountered a server folder for which you do not have the necessary access privileges.	To avoid this error, McAfee recommends taking the server offline and restarting it using a locked start-up diskette.
You have neither See Files nor See Folders privileges to this folder. This folder cannot be checked.	VirusScan encountered a server folder for which you do not have the necessary access privileges.	To avoid this error, McAfee recommends taking the server offline and restarting it using a locked start-up diskette.

## Alert Messages

This section lists and explains alert messages you may see when using VirusScan. The table also lists actions you can take to respond to each message. The messages appear in alphabetical order.

Alert	Reason	Action
A virus may still be active in memory. Some of your files may have or could become reinfected. You should immediately restart your Macintosh using a locked start-up floppy and run VirusScan again.	When you quit after a clean operation, VirusScan checks to see if it can find any infected files in the currently active system folder. If it finds any, it displays this alert message.	Click Restart to restart your Macintosh. Click Cancel to return to VirusScan. Click Quit to quit VirusScan.
An unexpected error <error name> occurred while trying to save a file.	VirusScan displays this alert message if it encounters an unexpected error while trying to save a copy of a report or the VirusScanner extension.	Contact McAfee technical support.
Data fork CRC changed on this file.	VirusScan displays this alert message when you have set its Fingerprint feature to maximum sensitivity and it detects a change in a file's data fork. Suspicious or unexpected changes may mean the file is infected.	Use VirusScan to scan the file.

**B**Alert Messages

---

Alert	Reason	Action
File type has changed.	VirusScan displays this alert if it sees that the file type designated in a file's resource fork has changed. The value for a file's type can change for many reasons, but if it changes unexpectedly, the file might be infected.	Use VirusScan to scan the file.
Out of memory.	VirusScan displays this alert if it runs out of memory.	Click OK to quit VirusScan. Then free more memory before running VirusScan again.
Please wait.	Your computer displays this message if you eject the disk that contains VirusScan and/or the active System file. VirusScan loads all the information from the disk that it might need later before it allows the disk to eject.	This can take quite some time. Wait until VirusScan has finished reading, then remove the disk from your floppy drive.
Printing error: could not locate printer driver in System folder.	VirusScan displays this alert message if you try to print the Activity log and your printer driver is not properly installed.	Make sure your printer driver is properly installed. See your Mac OS documentation to learn how to install printer drivers and use the Chooser.
Printing error: the start-up disk is full.	VirusScan displays this alert message if it doesn't have enough room on your start-up disk to print.	Increase the space available on your start-up disk, then print again.

**B**Alert Messages

---

Alert	Reason	Action
Printing error: the start-up disk is locked.	VirusScan displays this alert message if it could not print because the start-up disk is locked.	Unlock the start-up disk or create an unlocked copy of your start-up disk, then print again.
Printing error: you must use the Chooser to select a printer.	VirusScan displays this alert message if you try to print without having selected a printer.	Use the Chooser desk accessory to select a printer.
Printing error: (error code = nnnn).	An unexpected error occurred during printing.	Click OK to return to VirusScan, then print again. If the problem persists, call McAfee technical support.
Resource fork CRC changed on this file.	VirusScan displays this alert message when you have set its Fingerprint feature to maximum sensitivity and it detects a change in a file's data fork. Suspicious or unexpected changes may mean the file is infected.	Use VirusScan to scan the file.
The application <application name> is infected by the <virus name> virus. Use VirusScan to remove the virus.	VirusScan displays this alert message when it detects an infected file.	Use the VirusScan clean feature to remove the virus code from the file.

**B**Alert Messages

---

<b>Alert</b>	<b>Reason</b>	<b>Action</b>
The disk cannot be repaired because it is locked. Please unlock and reinsert the disk.	If you try to clean a locked floppy disk, VirusScan ejects the disk and displays this alert.	Unlock and reinsert the disk. VirusScan automatically begins to scan and repair the disk as soon as you reinsert it. Click Cancel to stop the operation and return to VirusScan.
The disk <disk name> is infected by the <virus name> virus. Rebuild the Desktop file on the disk or use VirusScan to remove the virus.	VirusScan displays this alert when it detects a disk infected with the WDEF or CDEF viruses.	Rebuild the desktop file on the disk or use VirusScan to remove the virus.
The document cannot be printed because some pages would be truncated on the bottom. To correct this problem, use the Page Setup command. Make the margins smaller or make the font size smaller.	This alert may appear if you try to print with a large font size and/or large margins.	Choose Page Setup from the File menu to display the Page Setup dialog. Make your font size or your margins smaller.

**B**Alert Messages

---

Alert	Reason	Action
The document cannot be printed because some pages would be truncated on the right. To correct this problem, use the Page Setup command. Make the left and right margins smaller or make the font size smaller. You might also try printing with landscape orientation instead of portrait orientation.	This alert may appear if you try to print with a large font size and/or large margins.	If you are trying to print a scan activity log in a large font size (more than 18 points) and you get this alert, use the Page Setup command to select landscape orientation instead of portrait orientation.
The file could not be saved because the disk is full.	You tried to save an activity log and there is not enough room on the disk to save the file.	Click OK. Then try to save to a different disk or make more room on the disk.
The file could not be saved because the old version of the file is locked.	VirusScan displays this alert if you try to save a scan activity log or if you try to install or save the VirusScanner extension and a locked version of the file already exists.	Unlock the old version of the file and try again.
The extension file <file name> is infected by the INIT 1984 virus. Use VirusScan to remove the virus.	This alert is presented by the VirusScanner extension when it detects an extension file infected by the INIT 1984 virus.	Use VirusScan to clean the file.



**B**Alert Messages

---

Alert	Reason	Action
The margins you specified are too large. Please make them smaller or click the Cancel button.	The margins you specified are too large to allow the document to print correctly. VirusScan requires at least a five-inch square print area, after taking into account the margins and page size.	Enter smaller margins in the Page Setup dialog.
The protection extension could not be installed because the start-up disk is locked.	You tried to install the VirusScanner extension on a locked start-up disk.	Unlock the disk and try again.
The report is too big. It must be saved or cleared before the scan can continue. Save the report?	VirusScan has an upper limit for the size of the scan activity log. Most people will never be affected by this limit. If you produce a very long activity log that approaches the size limit, you will get this alert, with three buttons: Save, Cancel and Clear.	Select the option you want. Save is the default button. It saves the partial report as a text file, clears the report field, and continues the scan. The Cancel button cancels the scan without clearing or saving the report. The Clear button clears the report field without saving and continues the scan.
The stack <stack name> is infected by the MacMag virus. Use VirusScan to remove the virus.	VirusScan displays this alert message when it detects a HyperCard stack infected with the MacMag virus.	Use VirusScan to clean the stack.

**B**Alert Messages

---

<b>Alert</b>	<b>Reason</b>	<b>Action</b>
This copy of VirusScan has been damaged, infected by a virus, or otherwise modified. Please delete this copy and use an original unmodified copy.	VirusScan checks itself when it starts up and notifies you if it has been modified. This may mean that it has been infected by a virus.	Remove this particular copy of VirusScan from your disk and replace it with an uninfected or undamaged copy of VirusScan.
You selected the page range xxx through yyy. There are no pages in this range.	The Activity log has no pages in the range you asked your computer to print.	Select a valid page range and try to print again.




# McAfee Support Services

---

McAfee offers several flexible support programs to meet your needs. By offering support solutions that range from a complimentary 90-day introductory technical support program to an optional one-year personal support plan, McAfee helps to ensure that you receive the level of technical assistance you require.

McAfee also offers a variety of technical assistance plans designed to meet the needs of business customers, including training, consulting, enterprise support, and a Jump Start program. Please review each of the different support service plans and benefits listed in this appendix and pick the one best suited for you or your business.

 *The term “update” refers only to the virus definition files; the term “upgrade” refers to both product version revisions and definition files. McAfee offers free virus definition file updates for the life of your product. McAfee cannot, however, guarantee backward compatibility of the virus definition files with previous VirusScan versions. By regularly upgrading your software to the latest product version and updating to the latest virus definition files, you ensure complete virus protection for the term of your software subscription or maintenance plan.*

## Customer Service Programs

### Free VirusScan support program

All registered owners of single-node (one computer) VirusScan products purchased at local retail stores or downloaded from the McAfee Web Site are entitled to:


- Unlimited free online virus definition file updates for the life of your product
- One year of unlimited free online product upgrades (product version revisions) with the newest features
- Free support services listed below

### Support services

- Electronic and online support, available 24 hours a day, seven days a week on each of the forums listed below:
  - Automated voice and fax system: (408) 988-3034
  - McAfee BBS (electronic bulletin board system): (408) 988-4004
  - World Wide Web site: <http://www.McAfee.com>
  - CompuServe: GO MCAFEE
  - America Online: keyword MCAFEE
- 90 days of free technical support phone assistance, available during regular business hours, 6:00 A.M.– 6:00 P.M. Pacific time, Monday through Friday, from our professionally trained support representatives at (408) 988-3832.

## Free subscription maintenance and support program


McAfee offers all registered owners of licensed multiple-node (ten computers or more) subscription products the following free support services and maintenance during the two-year term of the software subscription.

 *You must be a registered owner to receive these services.*

### Support services

- Electronic and online support, available 24 hours a day, seven days a week on each of the forums listed below:
  - Automated voice and fax system: (408) 988-3034
  - McAfee BBS (electronic bulletin board system): (408) 988-4004
  - World Wide Web site: <http://www.McAfee.com>
  - CompuServe: GO MCAFEE
  - America Online: keyword MCAFEE
- Technical support phone assistance during regular business hours, 6:00 A.M.–6:00 P.M. Pacific time, Monday through Friday, from our professionally trained support representatives at (408) 988-3832.
- Two years of free online product upgrades with the newest features and virus definition data. If you upgrade your operating system, you can also upgrade your product version to one that runs on your new platform.

## Optional support plans

 *Contact McAfee for current pricing structures.*


### **Option 1: One-year personal support plan**

For registered owners of single-node products who want to extend their support coverage, this plan allows you to call in for unlimited technical telephone support, download the latest virus protection updates each month, and periodically download upgrades from any of McAfee's registered online services—all for a full year. If you upgrade your operating system, you can also upgrade your product version to one that runs on your new platform.

### **Option 2: One-year quarterly disk/CD-ROM maintenance and support programs**

This plan is for registered owners of either single- or multiple-node subscription products. It offers all the features of Option 1, while adding a quarterly mailing of software upgrade diskettes or CD-ROMs (depending on the product) and a quarterly update newsletter. With this option, you can update your product to include the latest features and virus data files without having to download from an online service.

Each optional support plan begins as soon as you purchase the product and is good for one year, at which time you can renew your support program through McAfee's Customer Care department at (408) 988-3832.

 *McAfee reserves the right to change part or all of its Customer Service Programs at any time without notice.*

## Enterprise support

McAfee's Enterprise Support Program provides customers with the highest level of support possible. This fee-based program is designed for those customers who need a higher level of personal service.

The Enterprise Support Program offers the following features:

- Direct pager number to your assigned senior Enterprise Support Program analyst
- Extended support hours: 7:00 A.M. to 7:00 P.M. central time, Monday through Friday
- Five designated McAfee contacts
- Proactive support, providing updated company and product information as it becomes available
- On-site services at a 25% discount
- VIP issues review list
- Beta site (if desired)

Every Enterprise Support Representative calls clients each week. This phone call is used to forward any information such as technical notes and application anomalies of which you should be aware. This call also ensures that you have no unresolved problems or complications with the product. Enterprise Support representatives will return your page on the day it is received.

## Optional 7 x 24 enterprise support

Frequently, customers are responsible for their own LANs, which run 24 hours a day, seven days a week. This feature offers round-the-clock support for clients requiring support outside normal business hours.

*✍ McAfee reserves the right to change part or all of its Professional Services Programs at any time without notice.*

## A

- Action tab 35
- activity logs
  - opening, copying and saving 35, 39
  - printing 39
- adding or editing scan tasks 33
- admin information
  - including in custom installations 21
  - saving 40
- alert messages
  - explanations for 60
  - to other users
    - via e-mail 36
  - to you
    - sounds 30, 31, 35
- Alert tab 35
- Apple events 41
- AppleScript
  - using to send e-mail notifications 36
- application
  - starting 29
- archived files
  - installing from 14
- ASCII text, saving activity logs in 35

## B

- Balloon Help, using 41
- BinHex 14, 47
- Bulletin Board System (BBS) 9

## C

- CD-ROM, installing from 15
- Claris E-mailer, using to alert others to virus infections 36
- cleaning infected files
  - immediately 31
  - pausing or stopping 31
- components of VirusScan 8
  - Config Wizard 24
  - VirusScan application 29
  - VirusScanner 29, 41
- Config Wizard
  - closing and reopening 27
  - starting 24

- configuration options
  - changing 27
  - methods for setting
    - manual
      - configuration 27
      - scheduling tasks 32
    - use default options 26
    - VirusScan
      - interview 25
      - VirusScan Settings dialog box 26
- Custom Alert Message checkbox 36
- custom installations 21
- Customer Care
  - contacting 9
  - programs 69

## D

- default options 26
- DeHGX 14, 47
- Delete button 36
- deleting tasks 36
- desktop file
  - rebuilding 44
- disabling VirusScanner 42
- downloading virus definition files 47





## E

Edit button 33  
e-mail  
    using to alert others to  
    virus infections 36  
enterprise support 71  
error messages,  
    explanations for 50  
Eudora, using to alert others  
    to virus infections 36  
events  
    as scan triggers 34  
excluding items from scan  
    tasks 38  
Exclusion List 38  
    using to improve scan  
    performance 43  
exporting scan tasks 37  
extensions  
    conflicts 44  
    disabling 14, 15  
Extensions Manager control  
    panel 15  
Extra Log File checkbox 35

## F

faster scanning, tips for 43  
features of VirusScan 7  
file modification  
    as scan trigger 34  
files installed 19  
Fingerprint option 34  
    activating for all tasks  
    43  
floppy disk  
    as scan trigger 34  
    locking 17

## H

hardware errors  
    as cause for system  
    problems 45  
hardware requirements 13  
Help menu 41

## I

immediate scans,  
    performing 30  
installing VirusScan  
    custom installations 21  
    from archived files 14  
    files installed 19  
    from CD-ROM 15  
    over previous versions  
    19  
    scanning before 17  
    steps 19  
interview  
    as method for setting  
    configuration options  
    25

## M

Mac OS 8  
    supported in VirusScan  
    3.0 7  
main window 29  
    progress report 30, 31

## McAfee

contacting  
    BBS 9  
    Customer Care 9  
    outside the United  
    States 11  
    via America Online  
    9  
    via CompuServe 9  
    within the United  
    States 10  
enterprise support 71  
support services 67  
training 10

## N

network installations 21  
New button 33  
Notify tab 36

## O

online help, using 41  
Optimal fingerprint option  
    34  
Option key, use of for  
    uninstalling VirusScan 20

## P

Parameter RAM  
    "zapping" 44  
parts of VirusScan 8  
password protection 33, 37  
pausing or stopping  
    cleaning operations 31  
    scans 30  
performance, balancing  
    against protection 27, 43

personal support plan 70  
PreScan, using 17  
preventing virus infections 46  
printing activity logs 39  
professional services  
    enterprise support 71

## R

removing VirusScan 20  
renaming VirusScanner 42  
reporting items not detected 12  
responses to infected files 35

## S

saving admin information 40  
    in custom installations 21  
Scan Compressed Files checkbox 34  
Scan menu 30  
    Clean Now 31  
    Exclusion List 38  
    Export Task 37  
    Scan Now 30  
    Schedule Task 32  
    Show Log 30, 32

scan tasks  
    active and inactive 32  
    adding or editing 33  
    deleting 36  
    excluding items 38  
    exporting 37  
    including in custom installations 21  
    setting start times 34

Scan Tasks dialog box 32

scanning  
    before installation 17  
    how often 8  
    immediately 30  
    pausing or stopping 30  
    scheduling tasks for 32  
    setting basic properties for 24  
    using drag and drop 30

security, tips 46

Settings dialog box 26

settings, *see* configuration options

Show Balloons 41

SimpleText  
    using to create and open activity logs 35

software errors  
    as cause for system problems 45

starting Config Wizard 24

StuffIt 14, 34, 47

subscription maintenance program 69

support  
    programs 69

system administrators  
    recommendations for 48

system extensions  
    conflicts 44  
    disabling 14, 15  
system problems  
    other sources 44  
system requirements 13

## T

Target tab 34

task components 27, 33

Task Description dialog box

    Action tab 35

    Alert tab 35

    Notify tab 36

    Target tab 34

    Trigger tab 33, 34

Task Enabled checkbox 33

Task Password Protected checkbox 33, 36, 37

technical support

    McAfee Bulletin Board System (BBS) 9

    automated voice and fax response systems 9

    e-mail address 9

    free support policies 69

    information needed from user 10

    online 9, 69

    programs 67

tips for faster scanning 43

training for McAfee products 10

Trash

    as quarantine area 35

Trigger tab 33, 34



Troubleshooting 46

## U

uninstalling VirusScan 20  
update, definition of 68  
updating virus definition files 47  
upgrade, definition of 68  
using Balloon Help 41  
using custom installers 37

## V

virus definition files  
    updating 47  
viruses  
    when to scan for 8

## VirusScan

Interview 25  
Settings dialog box 26  
activity log 39  
application  
    starting 29  
components of  
    Config Wizard 24  
    VirusScan application 29  
    VirusScanner 41  
default options 26  
downloading new versions 48  
error messages 50  
features of 7  
files included in 8  
installing  
    files installed 19  
    from CD-ROM 15  
    from archived files 14  
    over previous versions 19  
    scanning before 17  
    steps 19  
introducing 6  
main window in application 29  
manual configuration 27  
messages 50  
system requirements 13  
uninstalling 20  
what it is 6  
why use it? 6  
VirusScan Updater 38

## VirusScanner

as background application 41  
background operation 29  
controlling 27, 29, 32  
disabling 42  
loading first 42  
renaming 42

## W

what is VirusScan? 6  
why use VirusScan? 6  
wizard, *see* Config Wizard 25

## Z

zapping the Parameter RAM 44