



Symantec AntiVirus™ for Macintosh®

User Guide
Version 10

Symantec AntiVirus™ for Macintosh® User Guide

Copyright© 2005 Symantec Corporation. All rights reserved.
Documentation version 10

Symantec, and the Symantec logo are U.S. registered trademarks of Symantec Corporation. LiveUpdate, Symantec AntiVirus, Symantec Enterprise Security Architecture, and Symantec Security Response are trademarks of Symantec Corporation.

Mac, Macintosh, Mac OS, eMac, Safari, and the Mac logo are trademarks of Apple Computer, Inc. PowerMac, iMac, and Xserve are trademarks of Apple Computer, Inc., registered in the U.S. and other countries. MySQL is a registered trademark of MySQL AB in Sweden and other countries. MySQL is a trademark in the United States and other countries. Red Hat and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc. in the United States and other countries. Linux is a registered trademark of Linus Torvalds. RSA is a registered trademark or trademark of RSA Security Inc. in the United States and/or other countries. Netscape is a registered trademark of Netscape Communications Corporation in the United States and other countries. Windows and Internet Explorer are either registered trademarks or trademarks of Microsoft Corporation. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THIS DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
<http://www.symantec.com>

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product feature and function, installation, and configuration. The Technical Support group also authors content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's maintenance offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web-based support that provides rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week worldwide. Support is provided in a variety of languages for those customers that are enrolled in the Platinum Support program
- Advanced features, including Technical Account Management

For information about Symantec's Maintenance Programs, you can visit our Web site at the following URL:

www.symantec.com/techsupp/ent/enterprise.html

Select your country or language under Global Support. The specific features that are available may vary based on the level of maintenance that was purchased and the specific product that you use.

Contacting Technical Support

Customers with a current maintenance agreement may access Technical Support information at the following URL:

www.symantec.com/techsupp/ent/enterprise.html

Select your region or language under Global Support.

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to recreate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
 - Error messages and log files
 - Troubleshooting that was performed before contacting Symantec
 - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/techsupp/ent/enterprise.html.

Select your region or language under Global Support, and then select the Licensing and Registration page.

Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp/ent/enterprise.html

Select your country or language under Global Support.

Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade insurance and maintenance contracts
- Information about Symantec Value License Program
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Maintenance agreement resources

If you want to contact Symantec regarding an existing maintenance agreement, please contact the maintenance agreement administration team for your region as follows:

- Asia-Pacific and Japan:
contractsadmin@symantec.com
- Europe, Middle-East, and Africa:
semea@symantec.com
- North America and Latin America:
supportolutions@symantec.com

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively. Additional services that are available include the following:

Symantec Early Warning Solutions

These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.

Managed Security Services

These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.

Consulting services Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring and management capabilities, each focused on establishing and maintaining the integrity and availability of your IT resources.

Educational Services These services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about Enterprise Services, please visit our Web site at the following URL:

www.symantec.com

Select your country or language from the site index.

Symantec License and Warranty

Symantec AntiVirus™ for Macintosh®

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK THE "I DO NOT AGREE" OR "NO" BUTTON OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE SOFTWARE.

1. License:

The software and documentation that accompanies this license (collectively the "Software") is the proprietary property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, You will have certain rights to use the Software after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that the Licensor may furnish to You. Except as may be modified by an applicable Symantec license certificate, license coupon, or license key (each a "License Module") that accompanies, precedes, or follows this license, and as may be further defined in the user documentation accompanying the Software, Your rights and obligations with respect to the use of this Software are as follows.

You may:

A. use the number of copies of the Software as have been licensed to You by Symantec under a License Module. If the Software is part of a suite containing multiple Software titles, the total number of copies You may use, in any combination of Software titles, may not exceed the total number of copies indicated in the License Module. Your License Module shall constitute proof of Your right to make such copies. If no License Module accompanies, precedes, or follows this license, You may make one copy of the Software You are authorized to use on a single computer;

B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of Your computer and retain the original for archival purposes;

C. use the Software on a network, provided that You have a licensed copy of the Software for each computer that can access the Software over that network;

D. use the Software in accordance with any written agreement between You and Symantec; and

E. after written consent from Symantec, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software and the transferee agrees in writing to the terms of this license.

You may not:

A. copy the printed documentation that accompanies the Software;

B. sublicense, rent, or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;

C. use the Software as part of a facility management, timesharing, service provider, or service bureau arrangement;

D. use a previous version or copy of the Software after You have received and installed a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;

E. use a later version of the Software than is provided herewith unless You have purchased corresponding maintenance and/or upgrade insurance or have otherwise separately acquired the right to use such later version;

F. use, if You received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which You have not received permission in a License Module; nor

G. use the Software in any manner not authorized by this license.

2. Content Updates:

Certain Software utilize content that is updated from time to time (including but not limited to the following Software: antispy software utilize updated antispy rules; antivirus software utilize updated virus definitions; content filtering software utilize updated URL lists; some firewall software utilize updated firewall rules; policy compliance software utilize updated policy compliance updates; and vulnerability assessment products utilize updated vulnerability signatures; these updates are collectively referred to as "Content Updates"). You shall have the right to obtain Content Updates for any period for which You have purchased maintenance, except for those Content Updates that Symantec elects to make available by separate paid subscription, or for any period for which You have otherwise separately acquired the right to obtain Content

Updates. Symantec reserves the right to designate specified Content Updates as requiring purchase of a separate subscription at any time and without notice to You; provided, however, that if You purchase maintenance hereunder that includes particular Content Updates on the date of purchase, You will not have to pay an additional fee to continue receiving such Content Updates through the term of such maintenance even if Symantec designates such Content Updates as requiring separate purchase. This License does not otherwise permit the licensee to obtain and use Content Updates.

3. Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of thirty (30) days from the date of delivery of the Software to You. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money You paid for the Software. Symantec does not warrant that the Software will meet Your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

4. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT, OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether or not You accept the Software.

5. U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items," as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014, United States of America.

6. Export Regulation:

Certain Symantec products are subject to export controls by the U.S. Department of Commerce (DOC), under the Export Administration Regulations (EAR) (see www.bxa.doc.gov). Violation of U.S. law is strictly prohibited. Licensee agrees to comply with the requirements of the EAR and all applicable international, national, state, regional and local laws, and regulations, including any applicable import and use restrictions. Symantec products are currently prohibited for export or re-export to Cuba, North Korea, Iran, Iraq, Libya, Syria and Sudan or to any country subject to applicable trade sanctions. Licensee agrees not to export, or re-export, directly or indirectly, any product to any country outlined in the EAR, nor to any person or entity on the DOC Denied Persons, Entities and Unverified Lists, the U.S. Department of State's Debarred List, or on the U.S. Department of Treasury's lists of Specially Designated Nationals, Specially Designated Narcotics Traffickers, or Specially Designated Terrorists. Furthermore, Licensee agrees not to export, or re-export, Symantec products to any military entity not approved under the EAR, or to any other entity for any military purpose, nor will it sell any Symantec product for use in connection with chemical, biological, or nuclear weapons or missiles capable of delivering such weapons.

7. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England and Wales. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i)

supersedes all prior or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment, or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Software and documentation is delivered Ex Works California, U.S.A. or Dublin, Ireland respectively (ICC INCOTERMS 2000). This Agreement may only be modified by a License Module that accompanies this license or by a written document that has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A., (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland, or (iii) Symantec Customer Service, 1 Julius Ave, North Ryde, NSW 2113, Australia.

8. Additional Uses and Restrictions:

A. If the Software You have licensed is a specified Symantec AntiVirus for a corresponding third party product or platform, You may only use that specified Software with the corresponding product or platform. You may not allow any computer to access the Software other than a computer using the specified product or platform. In the event that You wish to use the Software with a certain product or platform for which there is no specified Software, You may use Symantec Scan Engine.

B. If the Software you have licensed is Symantec AntiVirus or Symantec Scan Engine utilizing Web Server optional licensing as set forth in the License Module, the following additional use(s) and restriction(s) apply:

- i) You may use the Software only with files that are received from third parties through a web server;
- ii) You may use the Software only with files received from less than 10,000 unique third parties per month; and
- iii) You may not charge or assess a fee for use of the Software for Your internal business.

C. If the Software You have licensed is Symantec Client Security, this Software utilizes the Standard Template Library, a C++ library of container classes, algorithms, and iterators. Copyright (c) 1996-1999. Silicon Graphics Computer Systems, Inc. Copyright (c) 1994. Hewlett-Packard Company.

Contents

Technical Support

Chapter 1	Feature summary	
	Virus and threat protection features	13
	Quick access features	15
Chapter 2	Getting started	
	Starting and quitting Symantec AntiVirus	17
	Disabling and enabling Auto-Protect	18
Chapter 3	Responding to emergencies	
	What to do if a virus is found by	
	Auto-Protect	20
	If a virus is found during a manual scan	21
	Repairing infected files	21
	If Symantec AntiVirus can't repair a file	22
	About Symantec AntiVirus Quarantine	22
	Repairing, deleting, and restoring files in	
	Quarantine	23
	Looking up virus names and definitions	24
	Looking up virus definitions on the Symantec	
	Web site	24
Chapter 4	Frequently asked questions	
	Exploring the Symantec support Web site	27
	What if I have problems installing?	28
	Why does Auto-Protect fail to start?	29
	Why does Symantec AntiVirus report that a	
	file is invalid or can't be found?	29
	Why aren't all files scanned?	30

Why can't I update virus definitions using LiveUpdate?	30
---	----

Index

Feature summary

1

Symantec AntiVirus™ 10 for Macintosh® provides a variety of threat protection and quick access features that help you maintain the security of your computer.

Virus and threat protection features

Symantec AntiVirus monitors your computer for known and unknown viruses. A known virus is one that Symantec AntiVirus can detect, define, and identify by name. An unknown virus is one that Symantec AntiVirus can detect, but does not yet have a definition for.

Symantec AntiVirus protects your computer from both types of viruses, using virus definitions to detect known viruses, and Bloodhound technology to detect unknown viruses. Symantec AntiVirus uses virus definitions and Bloodhound technology during scheduled scans and manual scans, and Auto-Protect uses them to monitor your computer constantly.

Virus and threat protection features

Symantec AntiVirus 10 for Macintosh includes these antivirus features:

Bloodhound technology	Bloodhound is the Symantec AntiVirus scanning technology for detecting new and unknown viruses. It detects viruses by analyzing an executable file's structure, behavior, and other attributes, such as programming logic, computer instructions, and any data contained in the file.
Auto-Protect	Auto-Protect provides virus and threat protection as soon as you start your computer, and provides constant protection while you work. It eliminates viruses, including macro viruses, and quarantines and repairs damaged files. It also checks for viruses every time you use software programs on your computer, insert CDs or other removable media, use the Internet, receive email, or copy or save files to your computer.
Mount Scan	<p>Mount Scan will scan removable disks, including CDs, Zip disks, and flash drives, to ensure that they don't contain viruses.</p> <p>Mount Scan allows you to select the kinds of media that Auto-Protect scans for viruses when you use them with your computer. You can prevent the scanning of specific types of CDs, DVDs, or an iPod, that you know are virus-free.</p>
SafeZones	<p>SafeZones are locations you designate on your computer that Auto-Protect protects automatically. Whenever a file is copied, changed, or added within a SafeZone, Auto-Protect scans the file for viruses.</p> <p>You can select specific folders on the computer as SafeZones, or select the entire hard disk as a SafeZone. If you select the entire hard disk as a SafeZone, Auto-Protect scans every file that is created, copied, or modified on your hard disk. By default, your entire computer is considered a SafeZone.</p>
LiveUpdate	LiveUpdate downloads and installs the latest program updates and virus definition files automatically to protect your computer against new threats. Symantec AntiVirus uses virus definition files to recognize viruses and intercept their activity.

Windows virus repair	Windows virus repair automatically attempts to remove Windows and DOS viruses so hidden PC viruses cannot be planted in your computer and spread to Windows computers.
Archived file scanning	Archived file scanning automatically scans and repairs files inside archives, such as .sit files.



Access to some Symantec AntiVirus 10 for Macintosh features, such as the ability to configure Mount Scan and SafeZones, may be restricted by your system administrator. Consult with your system administrator for more information about these features.

Quick access features

You can quickly access certain Symantec AntiVirus 10 for Macintosh features.

Symantec QuickMenu	Symantec QuickMenu provides access to Auto-Protect settings. Use of QuickMenu and access to the Auto-Protect settings may be restricted by your system administrator. Consult with your system administrator for more information about QuickMenu and the Auto-Protect settings.
Contextual Finder menu	Control-click or right-click a file in the Finder to scan it for viruses.



These topics include general information about how to start and quit Symantec AntiVirus, and how to access more information.

Starting and quitting Symantec AntiVirus

You don't have to open the Symantec AntiVirus program to be protected from viruses if you have Auto-Protect running. You do have to open Symantec AntiVirus when you want to:

- Start a manual virus scan of your computer.
- Start a manual LiveUpdate session.
- Schedule Symantec AntiVirus to run unattended virus scans or LiveUpdate downloads.
- Customize virus protection options.



Your system administrator may restrict access to some Symantec AntiVirus features, such as the ability to disable Auto-Protect, schedule scans, or customize protection options. Consult with your system administrator for more information about these features.

To start Symantec AntiVirus

- 1 In the Finder, open the **Applications** folder.
- 2 Double-click **Symantec AntiVirus**.

Quitting Symantec AntiVirus closes the Symantec AntiVirus window, but leaves Auto-Protect and scheduled LiveUpdate events running.

To quit Symantec AntiVirus

Do one of the following:

- On the Symantec AntiVirus menu, click **Quit Symantec AntiVirus**.
- On the keyboard, press **Command-Q**.

Disabling and enabling Auto-Protect

By default, Auto-Protect guards against viruses as soon as your computer starts. It checks programs for viruses as they run, and monitors your computer for any activity that might indicate the presence of a virus. Running a Symantec AntiVirus manual scan is not necessary as long as Auto-Protect is enabled. Auto-Protect interception prevents viruses from infecting your computer, and you should keep Auto-Protect turned on.



Your system administrator may restrict access to some Symantec AntiVirus 10 for Macintosh features, such as the ability to disable Auto-Protect, schedule scans, or customize protection options. Consult with your system administrator for more information about these features.

To disable Auto-Protect temporarily

- ❖ On the menu bar, on the Symantec QuickMenu, click **Symantec AntiVirus > Disable Auto-Protect**.
When you disable Auto-Protect, the Symantec QuickMenu changes the icon for Symantec AntiVirus to remind you that you have disabled your protection.

If you have turned off Auto-Protect, you should enable it as soon as possible.

To enable Auto-Protect

- ❖ On the menu bar, on the Symantec QuickMenu, click **Symantec AntiVirus > Enable Auto-Protect**.

Responding to emergencies

3

Symantec AntiVirus notifies you that it has detected a virus or other security risk when one of the following has occurred:

- Auto-Protect has found a virus while monitoring your computer.
- A virus scan that you scheduled or started manually has found a virus.

With default settings, Symantec AntiVirus automatically attempts to repair any virus it finds. If it can't repair the file, Symantec AntiVirus safely quarantines the file, so that it cannot harm your computer. Usually, Symantec AntiVirus performs these repairs without any action by you.

In certain circumstances, Symantec AntiVirus prompts you to choose whether you want to repair, delete, or restore an infected file that it has found. Your responses determine what Symantec AntiVirus does with the infected file.



For more information about a particular virus, refer to the Symantec Security Response Web site located at the following URL:

<http://securityresponse.symantec.com>

What to do if a virus is found by Auto-Protect

When a virus is found while Auto-Protect is running, an alert displays what happened, and what your options are. Read the alert message carefully to determine whether you need to do anything.



Access to some Symantec AntiVirus 10 for Macintosh features, such as Auto-Protect preferences, may be restricted by your system administrator. Consult with your system administrator for more information about these features.

Resolution	Your action
Repaired infected file	None needed.
Asks for your approval before repairing infected file	Approve the repair. If you don't repair the file, it is left as it is on your computer. If you have set the Auto-Protect Repair preference to Manually repair infected files, Auto-Protect informs you of infected files, and asks for your approval before repairing them.
Unable to repair infected file	Open Quarantine. In a few cases, Auto-Protect may not be able to repair an infected file, whether or not you have preferences set to Automatic Repair. With default preferences on, if Auto-Protect cannot repair a file, it puts it in Quarantine. See "Repairing, deleting, and restoring files in Quarantine" on page 23.



Do not click **No** in the Symantec AntiVirus Alert unless you are sure the file is safe. If you do not repair a detected file, it is left as it is on your computer.

If a virus is found during a manual scan

To manually repair an infected file that has been detected but not repaired

- In the Symantec AntiVirus Alert, click **Yes** to repair the file.
If the file cannot be repaired, Auto-Protect automatically quarantines it.

If a virus is found during a manual scan

If you are performing a manual scan and Symantec AntiVirus finds a virus, the scan window shows you the name of the infected file. Usually, infected files are repaired or quarantined automatically and you don't have to do anything else. To determine if the file was repaired or if you need to take further action, check the status of the file in the scan window. If the file was not quarantined, you can attempt to repair or delete the file.

To check the status of infected files in the scan window

- ❖ In the Virus Scan window, under Scan Results, select the infected file.
The Virus Scan window displays the name and status of any infected files found by the scan. Selecting the name of a file in the Virus Scan window enables you to repair, delete, or learn more about a file.

Repairing infected files

If an infected file in the scan window was not repaired or placed in Quarantine, you can initiate the repair yourself.

To repair infected files

- 1 In the scan results list, select the file to repair.
- 2 Click **Repair**.
- 3 After repairing all infected files, scan your disks again to verify that there are no other infected files.
- 4 Check the repaired files to make sure that they function properly.

If you have set Auto-Protect to ignore removable media, you can use Symantec AntiVirus to scan and repair removable media manually.



Access to some Symantec AntiVirus 10 for Macintosh features, such as Auto-Protect preferences, may be restricted by your system administrator. Consult with your system administrator for more information about these features.

To repair infected removable media

- 1 Open Symantec AntiVirus.
- 2 Click **Scan**.
- 3 In the Select Scan Target window, select the media to scan.
The Virus Scan window displays the name and status of any infected files found by the scan. Selecting the name of a file in the Virus Scan window enables you to repair, delete, or learn more about a file.

If Symantec AntiVirus can't repair a file

If Symantec AntiVirus cannot repair the infected file, first make sure you have scanned with the latest virus definitions. If you are not sure that you have the latest definitions, run LiveUpdate, and then scan your hard disk again.

About Symantec AntiVirus Quarantine

Sometimes Symantec AntiVirus detects an unknown virus that cannot be eliminated with the current set of virus definitions. Symantec AntiVirus prompts you to put the file in Quarantine, or it quarantines it automatically. Files that are in Quarantine have been removed from their original location on your computer and are isolated, so that they cannot spread or reinfect your computer. You can't view the file in the Finder or use the file while it is in Quarantine. This prevents you from accidentally opening the file and spreading the virus.

Repairing, deleting, and restoring files in Quarantine

The Quarantine window displays the items that Symantec AntiVirus has detected as potentially harmful, and has put in Quarantine to prevent the file from infecting your computer.

You can leave a file in Quarantine without doing any harm to your computer, but you can't view the file in the Finder or use the file while it is in Quarantine. Depending on whether you want to keep the file, you can repair, delete, or restore quarantined files from the Quarantine window.



An administrator password is required to perform actions on files in Quarantine.

To repair, delete, or restore a file in Quarantine

- 1 Open Symantec AntiVirus.
- 2 On the Tools menu, click **Quarantine**.
 If the buttons in the Quarantine window are dimmed, click the lock icon, and then type an administrator name and password.
- 3 In the Quarantine window, select the file you want to take action on, and then choose an option. Your options are:

Repair	<p>Use Repair if you want to try to repair a quarantined file that contains information you want to keep.</p> <p>Use this action if you have received new virus definitions since the file was added to Quarantine. New virus definitions may be able to repair a file that couldn't previously be repaired.</p>
Delete	<p>If you don't need the contents of the file in Quarantine, you can permanently remove it from your computer by clicking the Delete button.</p>
Restore	<p>If you're sure the file in Quarantine does not contain a virus, you can move the file back to its original location on your computer by clicking the Restore button. Restoring a file does not repair it.</p>

Looking up virus names and definitions

You can look up a virus name from within Symantec AntiVirus. The Virus Definitions Info window lists the viruses in the current virus definitions file. You can export the list to a text file. You can also search the list for a specific virus.



To make sure you have the latest virus definitions, run LiveUpdate.

To look up virus names

- 1 In Symantec AntiVirus, on the Tools menu, click **Virus Info**.
- 2 Type the name or part of the name of the virus.

You can look up detailed information about a virus if you have an active Internet connection. Symantec AntiVirus obtains the detailed virus information from the Symantec Security Response Web site and displays it in separate window.

To look up detailed information about a virus

- 1 In Symantec AntiVirus, on the Tools menu, click **Virus Info**.
- 2 In the Virus Definitions Info window, click the name of a virus.
- 3 Click **Learn More**.

Looking up virus definitions on the Symantec Web site

Because of the large number of viruses, the Virus Definitions Info file does not include descriptions of each virus. The Symantec Security Response Web site contains a complete list of all known viruses and related malicious code, along with descriptions.

To look up virus definitions

- 1 Using your Web browser, go to the Symantec Security Response Web site at the following URL:
<http://securityresponse.symantec.com>
- 2 Click **View all virus threats**.

Looking up virus names and definitions

- 3 Do one of the following:
 - Type the name of a virus for which to search.
 - Scroll through the alphabetical list to locate a virus.
- 4 Click a virus's name to read its description.



Frequently asked questions

4

This section addresses some frequently encountered problems and troubleshooting steps. If you cannot resolve your problem using this information, read the Read Me file on the Symantec AntiVirus 10 for Macintosh CD, or in the Symantec Solutions folder.

For a comprehensive list of the latest troubleshooting tips, see the Symantec Service and Support Web site from the following URL:

<http://service.symantec.com>

Exploring the Symantec support Web site

The Symantec support Web site provides extensive information about Symantec AntiVirus. You can access free online support to find information about product subscriptions, product registration, and common support issues. Fee-based phone support is also available to help solve your problem.

To explore the Symantec support Web site

- 1 On the Internet, go to the following URL:
<http://service.symantec.com>
- 2 On the support Web page, under home & home office/small business, click **Continue**.
- 3 On the home & home office/small business Web page, click **access free online support**.
- 4 Follow the instructions on the Web site to get the information you need.

If you cannot find what you are looking for using the free online support pages, you can call Symantec to use fee-based technical support services, or you can search the Web site.

To search the Symantec support Web site

- 1 On the left side of any Web page in the Symantec support Web site, click **search**.
- 2 Type a word or phrase that best represents the information for which you are looking.
For tips on entering your search text, click **help** at the bottom of the page.
- 3 Check the area of the Web site that you want to search.
- 4 Click **search**.

What if I have problems installing?

If you encounter any problems installing Symantec AntiVirus, try any of the following:

- Restart Symantec AntiVirus
- Reinstall Symantec AntiVirus
- Copy the Symantec AntiVirus installer from the Symantec AntiVirus for Macintosh CD to your Macintosh and install from there.



You must know your Macintosh OS X administrator password to install Symantec AntiVirus.

See the *Symantec AntiVirus 10 for Macintosh Installation Guide* for information on installing Symantec AntiVirus.

Why does Auto-Protect fail to start?

If Auto-Protect fails to load, some program files and virus definitions may not have installed properly. To make sure that Auto-Protect is properly installed, reinstall Symantec AntiVirus.

Also, make sure that Auto-Protect is enabled.



Access to some Symantec AntiVirus 10 for Macintosh features, such as the ability to configure Auto-Protect preferences, may be restricted by your system administrator. Consult with your system administrator for more information about these features.

To enable Symantec Auto-Protect

- 1 Open System Preferences.
- 2 In System Preferences, click **Symantec Auto-Protect**.
- 3 Check **Enable Symantec Auto-Protect**.
You may need to click the padlock icon at the bottom of the Preference window and enter a Mac OS X Administrator name and password before you can enable Auto-Protect.

Why does Symantec AntiVirus report that a file is invalid or can't be found?

This is an indication that one of the files making up the virus definitions is damaged or otherwise invalid.

To repair a damaged or missing virus definitions file

- 1 Uninstall Symantec AntiVirus.
- 2 Reinstall Symantec AntiVirus.
- 3 Run LiveUpdate and update your virus definitions.
This restores the current versions of the items in the Symantec AntiVirus Additions folder.

See the *Symantec AntiVirus 10 for Macintosh Installation Guide* for more information.

Why aren't all files scanned?

Symantec AntiVirus scans only those files for which your account has access privileges. For example, if you are logged on with a Macintosh OS X Administrator account, Symantec AntiVirus scans all the files to which you have access as an administrator. If you are logged on with a standard user account, Symantec AntiVirus scans only those files to which you have access as a standard user.

Why can't I update virus definitions using LiveUpdate?

In some rare cases, such as immediately after the emergence of a new virus, the LiveUpdate servers may be very busy and it may be difficult to get a connection. In such cases, keep making connection attempts and you should eventually be successful.

When using LiveUpdate, make sure that your Internet connection is working by testing the connection with an Internet application, such as your Web browser.



In some Symantec AntiVirus installations, LiveUpdate may contact a locally maintained LiveUpdate server. Consult with your system administrator for more information about LiveUpdate.

Index

A

- alerts, virus 19-20
- archive, scanning for viruses 15
- Auto-Protect
 - description 14, 18
 - disabling 18
 - enabling 18
 - finds a virus 20
 - troubleshooting 29

B

- Bloodhound technology 14

D

- delete quarantined file 23
- DOS virus repair 15

F

- features, virus and threat protection 13
- files
 - quarantined 22
 - repair infected 21
- finder contextual menu 15

H

- Help, knowledge base articles 27

I

- infected files, repairing 21
- installing, problems 28

K

- knowledge base articles 27

L

- LiveUpdate
 - description 14
 - trouble updating 30

M

- messages, Auto-Protect 20
- Mount Scan 14

P

- Panther Mac OS X antivirus protection 13
- protect. See Auto-Protect
- protection features 13

Q

- quarantine
 - about 22
 - repair, delete, and restore files 23

quit Symantec AntiVirus 17

R

repair

- infected files 21

- quarantined file 23

restore quarantined file 23

S

SafeZones 14

scan archives 15

Security Response Web site,
Symantec 24

Service and Support Web site,
Symantec 27, 28

start Symantec AntiVirus 17

Symantec Service and Support Web
site 27

T

threats, protecting against 13

Tiger Mac OS X antivirus
protection 13

troubleshooting 27

V

viruses

- alerts 19-21

- information 24

- repairing infected files 21

- Symantec Security Response Web
site 24

- viewing descriptions 24

W

Web site

- Symantec Security Response 24

- Symantec Service and Support 27

Windows virus repair 15