Norton AntiVirus™ for Macintosh Reference Guide

NAVm50REF

Norton AntiVirus™ for Macintosh Reference Guide

Copyright Notice

Trademarks

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

SYMANTEC LICENSE AND WARRANTY

NOTICE: SYMANTEC LICENSES THE ENCLOSED SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE OPENING THIS PACKAGE, AS OPENING THE PACKAGE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN SYMANTEC IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE FULL PRODUCT WITH PROOF OF PURCHASE TO THE DEALER FROM WHOM IT WAS ACQUIRED WITHIN SIXTY DAYS OF PURCHASE, AND YOUR MONEY WILL BE REFUNDED.

LICENSE AND WARRANTY:

The software which accompanies this license (the "Software") is the 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. Except as may be modified by a license addendum which accompanies this license, your rights and obligations with respect to the use of this Software are as follows:

• You may:
(i) use only one copy of one version of the various versions of the Software contained on the enclosed CD-ROM on a single computer;

(ii) 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;

(iii) 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;

(iv) after written notice to 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 to the terms of this agreement; and

(v) if a single person uses the computer on which the Software is installed at least 80% of the time, then after returning the completed product registration card which accompanies the Software, that person may also use the Software on a single home computer.

• You may not:
(i) copy the documentation which accompanies the Software;
(ii) sublicense, rent or lease any portion of the Software;
(iii) reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software; or
(iv) use a previous version or copy of the Software after you have received a disk replacement set or an upgraded version as a replacement of the prior version, unless you donate a previous version of an upgraded version to a charity of your choice, and such charity agrees in writing that it will be the sole end user of the product, and that it will abide by the terms of this agreement. Unless you so donate a previous version of an upgraded version, upon upgrading the Software, all copies of the prior version must be destroyed.

• Sixty Day Money Back Guarantee:
If you are the original licensee of this copy of the Software and are dissatisfied with it for any reason, you may return the complete product, together with your receipt, to Symantec or an authorized dealer, postage prepaid, for a full refund at any time during the sixty day period following the delivery to you of the Software.

• Limited Warranty:
Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) 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.
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 NONINFRINGEMENT. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE.

• Disclaimer of Damages:
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.
SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.
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 you accept the Software.

• U.S. Government Restricted Rights:
RESTRICTED RIGHTS LEGEND. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c) (1) and (2) of the Commercial Computer Software-Restricted Rights clause at 48 CFR 52.227-19, as applicable, Symantec Corporation, 10201 Torre Avenue, Cupertino, CA 95014.

• General:
This Agreement will be governed by the laws of the State of California. This Agreement may only be modified by a license addendum which accompanies this license or by a written document which 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: Symantec Customer Sales and Service, 10201 Torre Avenue, Cupertino, CA 95014.

SYMANTEC SOFTWARE LICENSE ADDENDUM

Notwithstanding any of the terms and conditions contained in the Symantec Software License, you may make and use up to that number of copies of the Software that is indicated on the License Authorization Coupon contained in your box. The coupon will constitute proof of your right to make and use such additional copies.

C O N T E N T S

Appendix A Troubleshooting

Appendix B System messages

Appendix C Using Norton AntiVirus on a network

Glossary

Symantec Service and Support Solutions

Disk Exchange and/or Replacement Form

Index

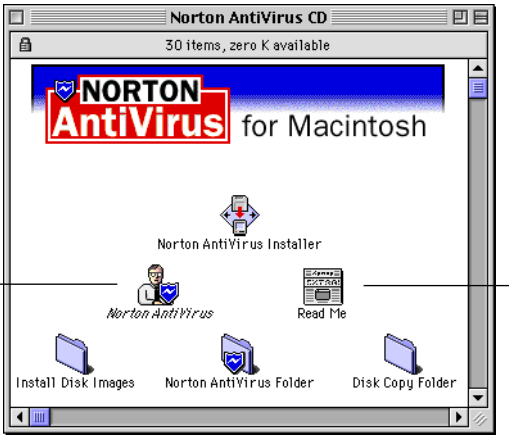
About this guide

This Adobe Acrobat Portable Document Format (PDF) file contains everything you might need to know about Norton AntiVirus for Macintosh.

- Click on any table of contents or index entry to go to that section.
- Click any cross-reference to go to the reference.
- If you can't find the information you want, try the Search features in Adobe Acrobat.

Note: The Read Me file on the Norton AntiVirus for Macintosh CD contains information that was unavailable at the time this guide was published. Read this information before you go any further.

About this CD



As well as the Norton AntiVirus for Macintosh installer and application software, there are several other items on the CD:

- **Install Disk Images folder**

  Contains compressed disk images that let you create a set of installation floppy disks.

- **Documentation folder**

  Contains this Reference Guide, a PDF file of the User's Guide, and installation files for Adobe Acrobat.

- **Symantec Trialware folder**

  Lets you test drive other Symantec products.

- **Disk Copy folder**

  Lets you create a set of installation floppy disks with the disk images in the Install Disk Images folder.

- **SimpleText application**

  Lets you read the Read Me file.

Restarting and scanning from the CD

Use the following procedure to scan for viruses before you install Norton AntiVirus. Restarting from the CD ensures that no viruses are in memory and that no system extensions cause conflicts during installation.

To scan for viruses:

1. Insert your Norton AntiVirus CD into the CD-ROM drive.
2. Restart from your Norton AntiVirus CD:
   - On a Power Macintosh, restart while holding down the letter “c” key on your keyboard.
   - On a third-party Macintosh, or on a Macintosh with a third-party CD-ROM drive, go to Control Panels, open Startup Disk, and select the Norton AntiVirus CD as your Startup Disk, then restart.

   When your computer restarts from the CD, the Norton AntiVirus pattern should appear in the background.
3. In the CD window, double-click the Norton AntiVirus icon.

Note: If you have already downloaded Norton AntiVirus virus definitions that are newer than those on the CD, you can use the newer file to scan. Hold down the Option key when you open Norton AntiVirus, then select the newer file.

---

4. In the Norton AntiVirus main window, select the disk to scan.
5. Click Scan or Scan/Repair.

   Norton AntiVirus scans your entire hard disk. If a virus is found during the scan, you can repair or delete it. See “To delete an infected file:” on page 55.
6. Click Done.

Warning: If you changed the Startup Disk Control Panel setting to start up from the Norton AntiVirus CD, don’t forget to restore the setting to your normal startup disk.

Getting more information

Extensive context-sensitive help is built into the Norton AntiVirus application. The CD jewel case also contains a *Norton AntiVirus for Macintosh User's Guide*. Together with this *Reference Guide*, these documents provide a wealth of valuable information about Norton AntiVirus:

- See Norton AntiVirus Help for information about Norton AntiVirus features. To access Help, click the Help button on any screen in Norton AntiVirus.
- See Norton AntiVirus Balloon Help for explanations of items on the screen. To turn on Balloon Help, choose Show Balloons from the Help Menu; point to any item to see a description.
- Refer to *Norton AntiVirus for Macintosh User's Guide* for information about installing, using LiveUpdate, and responding to Norton AntiVirus Auto-Protect alerts.
- To view descriptions of individual Macintosh system viruses, search for "known viruses" in the Norton AntiVirus Help.

  For the latest information on macro and other viruses, see the Virus Encyclopedia on Symantec's AntiVirus Research Center website:

  http://www.symantec.com/avcenter/

CHAPTER 1

About Norton AntiVirus for Macintosh

Norton AntiVirus for Macintosh is the most comprehensive virus prevention, detection, and elimination software available for your Macintosh computer.

About automatic protection

Norton AntiVirus automatically:

- Eliminates viruses, including macro viruses, and repairs files.
- Covers strategic areas of your computer with customizable SafeZones, protected by Norton AntiVirus Auto-Protect, to provide comprehensive virus protection to the areas you designate.
- Checks for viruses every time you use software programs on your computer, insert floppy disks, or use document files that you receive or create. (Many viruses are spread through Microsoft Word and Excel macros.)
- Monitors your computer for any unusual symptoms that may indicate an active virus.
- Protects your computer from Internet-borne viruses.

When to use Norton AntiVirus

New viruses are being created and distributed all the time. Hundreds of viruses are discovered every month. If you don't maintain your virus protection regularly, you are not protected against viruses that have been released into the computer world since you bought the product.

To keep your protection up to date, do the following:

- Once a month, obtain from Symantec updated virus definition files that Norton AntiVirus needs to keep your virus protection up-to-date. You can do this from a bulletin board service or over the Internet, using LiveUpdate or another method. To update virus protection, see "How to update virus protection" on page 36.
- Scan disks, folders, and files for viruses.
- Schedule virus scans to occur at specified times.
- Customize Norton AntiVirus to fit your virus-prevention needs.
- Repair infected files automatically, using Auto-Repair.
- Designate a wider area of your computer to be monitored as a SafeZone. You can also designate your entire computer as a Universal SafeZone.

About computer viruses

A computer virus is a parasitic program written intentionally to alter the way your computer operates without your permission or knowledge. A virus attaches copies of itself to other files, and when activated, may damage files, cause erratic system behavior, or merely display annoying messages.

What are known and unknown viruses?

A *known virus* is one that can be detected and identified by name. An *unknown virus* is one for which Norton AntiVirus does not yet have a definition. Norton AntiVirus can protect your computer from both types of viruses.

The virus definition files installed with Norton AntiVirus protect you from known viruses. Symantec's Bloodhound Macro technology detects unknown macro viruses, ensuring that you are protected against today's known viruses as well as tomorrow's new ones.

Is my computer virus-free?

Use Norton AntiVirus to scan your computer for viruses. If a virus is found, Norton AntiVirus steps you through the process of eliminating the virus.

For more information, see "Scanning disks, folders, and files" on page 43.

Is my computer protected against viruses?

If you installed Norton AntiVirus with all of the default options, your computer is automatically protected from viruses as soon as you restart it. The Norton AntiVirus Auto-Protect extension loads into memory when your computer starts up, providing constant protection while you work. You should update virus definitions to keep protection current.

For added protection, you should run Norton AntiVirus regularly to scan your entire hard disk, in case dormant viruses are present.

Tips for avoiding viruses

Here's a list of important steps you can take to combat computer viruses:

- Scan disks before you use them.

  For instructions, see "Scanning disks, folders, and files" on page 43.
- Make sure Auto-Protect is on at all times to prevent your computer from becoming infected. Auto-Protect is already turned on unless you specifically turn it off.

  For more information, see "About Norton Auto-Protect" on page 30.
- Update virus definitions regularly so you get maximum protection against new viruses.

  For more information, see "Keeping virus protection current" on page 35.

What viruses do and don't do

Computer viruses infect *system files* and *documents* created by applications with macro capabilities. Macintosh system files include system extensions (such as Apple menu items and control panels), and applications such as word processing and spreadsheet programs.

Some system viruses are programmed specifically to corrupt programs, delete files, or even erase your hard disk. Many of the currently known Macintosh viruses, however, are not designed to do any damage. They simply replicate themselves and may display messages. Nevertheless, bugs within the viruses may cause your system to behave erratically or crash unexpectedly.

What viruses don't do

Computer viruses don't infect files on write-protected disks, and they usually don't infect documents. They don't infect compressed files either. However, applications *within* a compressed file can become infected before they are compressed. Viruses also don't infect computer hardware, such as monitors or computer chips; they only infect software.

Except for macro viruses, Macintosh viruses don't infect DOS-based computer software and vice versa. For example, the infamous Michelangelo virus does not infect Macintosh applications. Macro viruses, however, are attached to documents and templates that can be shared between Macintosh and DOS-based computers, and can therefore jump platforms. Your Microsoft Word for Macintosh files can be infected by files created in Microsoft Word for Windows.

Finally, viruses don't necessarily let you know they are there—even after they do something destructive.

How viruses spread

A virus is inactive until you launch an infected application, start your computer from a disk that has infected system files, or open an infected document. For example, if a word processing program contains a virus, the virus activates when you run the program. Once a virus is in memory, it usually infects any application you run, including network applications (if you have write access to network folders or disks).

Viruses behave in different ways. Some viruses stay active in memory until you turn off your computer. Other viruses stay active only as long as the infected application is running. Turning off your computer or exiting the application removes the virus from memory, but *does not* remove the virus from the infected file or disk. That is, if the virus resides in a system file, the virus activates the next time you start your computer from the infected disk. If the virus resides in an application, the virus activates again the next time you run the application.

To prevent virus-infected applications from getting onto your computer, scan files with Norton AntiVirus before you copy or run them. This includes applications you download from bulletin board services and any demo disks you receive.

About macro viruses

Macro viruses attack document files. Document files include data document and template files, created in Microsoft Word or Excel. When you open an infected document in Microsoft Word or Excel, the macro virus is activated and copied to your Normal.dot template. When you open an infected document, such as a Microsoft Word document, other documents you create with Microsoft Word are also infected.

About Trojan horses

Trojan horses are not viruses, but they are often thought of as viruses. A Trojan horse is a program that appears to serve some useful purpose or provide entertainment, which encourages you to run it. But, like the Trojan horse of old, the program also serves a covert purpose, which may be to damage files or perhaps plant a virus on your computer.

A Trojan horse is not a virus because it does not replicate and spread like a virus. To ensure the safety of your computer, Norton AntiVirus detects Trojan horses so you can delete them from your computer.

About worms

Worms are not viruses either. Worms are programs that replicate without infecting other programs. Some worms spread by copying themselves from disk to disk, while others replicate only in memory, creating myriad copies of themselves, all running simultaneously, which slows down the computer.

Although worms exist in the realm of IBM-compatible personal computers, no occurrences of Macintosh worms have been reported—yet.

CHAPTER 2

Installing Norton AntiVirus for Macintosh

This section tells you how to install Norton AntiVirus from the CD, using either the standard or the customized installation. We strongly recommend that you scan your computer to check for viruses before installing.

If your Macintosh does not have a CD-ROM drive, see "If you don't have a CD-ROM drive" on page 26.

Note: If you have a more recent virus definitions file than the Norton AntiVirus Virus Defs file on the Norton AntiVirus for Macintosh CD, you can use it to scan. Hold down the Option key when you open Norton AntiVirus, and then select the newer virus definitions file.

Old Symantec AntiVirus for Macintosh (SAM) files are deleted when you install Norton AntiVirus to the same (default) location.

Checking for viruses and installing

Restarting from the CD ensures that no viruses are in memory and that no system extensions cause conflicts during installation.

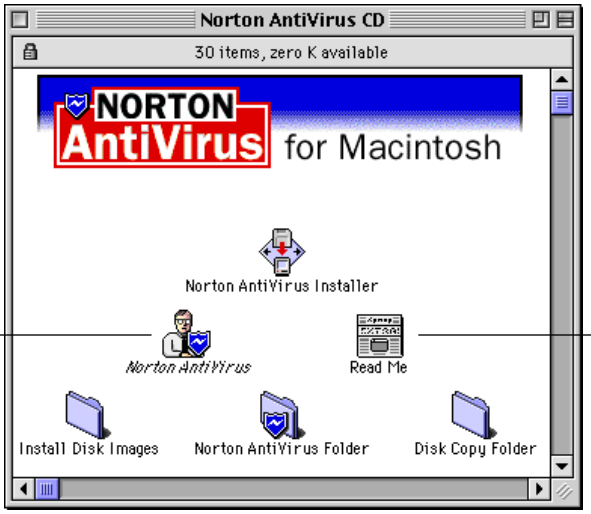
To scan for viruses and install:

1. Restart from your Norton AntiVirus CD:
   - On a Power Macintosh, restart while holding down the letter "c" key on your keyboard.

- On a third-party Macintosh, or on a Macintosh with a third-party CD-ROM drive, go to Control Panels, open Startup Disk, and select the Norton AntiVirus CD as your Startup Disk, then restart.

When your Macintosh restarts from the CD, the Norton AntiVirus pattern should appear in the background.When your Macintosh restarts, the CD window appears with the Norton AntiVirus pattern in the background.

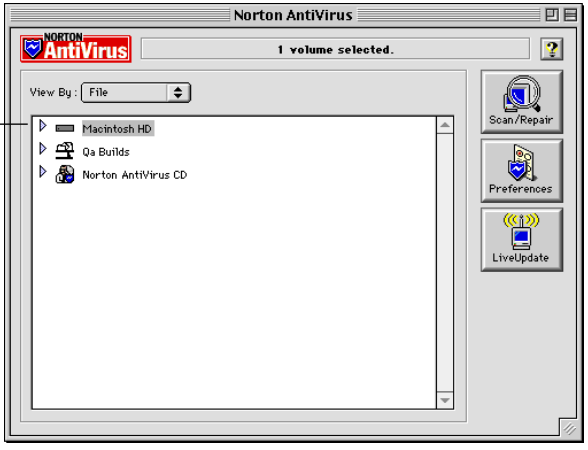
2 In the CD window, double-click the Norton AntiVirus icon.



Double-click to run Norton AntiVirus

Double-click the Read Me to see late-breaking information before you install

The Norton AntiVirus main window appears.

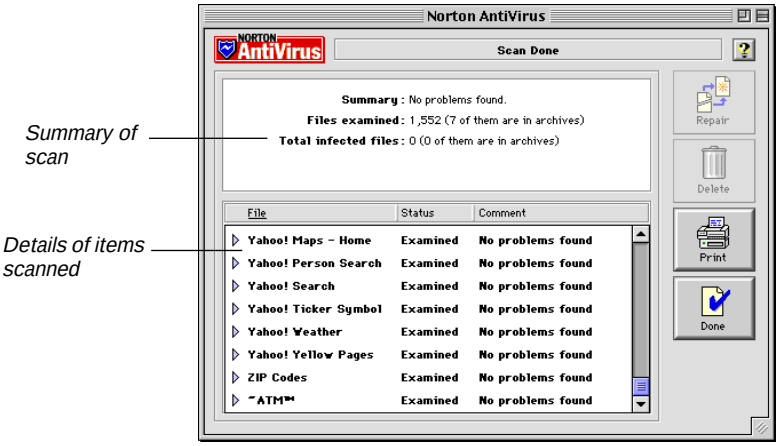


Select the disk to scan

3 In the Norton AntiVirus main window, select the disk to scan.

4 Click Scan or Scan/Repair.

Norton AntiVirus scans your entire hard disk. When the scan is complete, the results appear in the scan window.



If a virus is found during the scan, you can repair or delete it See "To delete an infected file:" on page 55

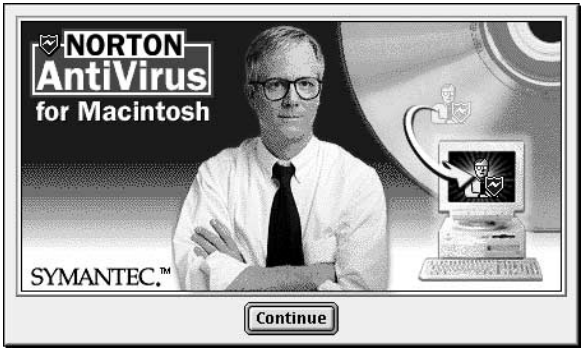
5 Click Done.

6 Choose Quit from the File menu.

Now that you know that your computer is virus-free, you are ready to install.

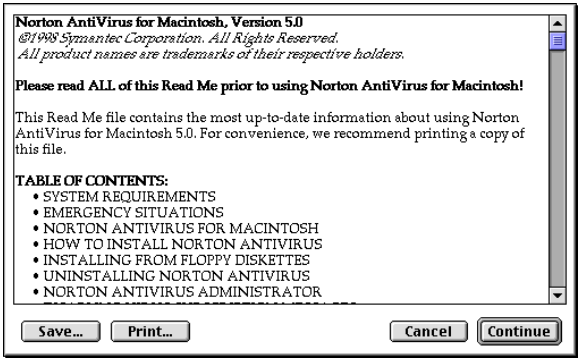
7 In the CD window, double-click the Norton AntiVirus Installer icon.

The Norton AntiVirus welcome screen appears.



8 Click Continue.

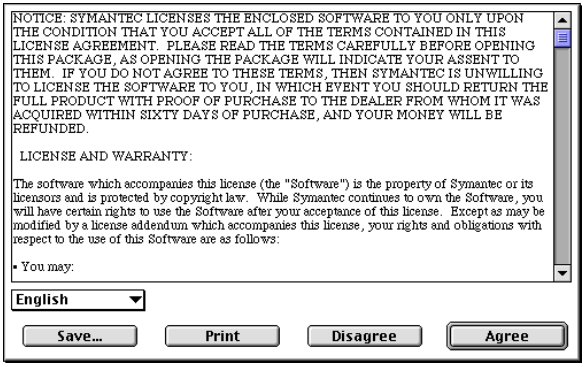
The Read Me window appears.



9 Scroll through the Read Me text file for any late-breaking information.

You can also print the Read Me text by clicking the Print button. Otherwise, click Continue.

The License Agreement window appears.



10 Click Agree to accept the License and Warranty Agreement.

If you click Disagree, the installation is cancelled.

11 Click Install.

The disk selection dialog box appears.

12 Select the disk on which to install.

If necessary, click Switch Disk to select the disk.

13 Follow the on-screen instructions to complete the installation.

A dialog box informs you when installation is complete.

14 Click Restart to restart your Macintosh from your hard disk.

Norton AntiVirus Auto-Protect loads when you restart and actively protects your computer unless you turn it off.

Note: If you used the Startup Disk Control Panel setting to start up from the Norton AntiVirus CD, you must restore the old setting at this time. Go to Control Panels, open Startup Disk, and select your hard disk as the Startup Disk, then choose Restart from the Special menu.

---

15 Update your virus definitions as soon as you can. See "Keeping virus protection current" on page 35.

16 Scan with the latest virus definitions after you have obtained them. See "Starting and exiting Norton AntiVirus" on page 30.

When you perform the standard install and restart your computer, Norton AntiVirus Auto-Protect loads on startup and provides protection to your entire computer, including hard disk, memory, and downloads from the Internet or email.

You do not have to run the Norton AntiVirus application to be alerted about a virus or virus-like activity as long as Auto-Protect is active.

Installing selected components

Use the custom installation procedure to install Norton AntiVirus with selected features.

Note: If you have a more recent virus definitions file than the Norton AntiVirus Virus Defs file on the Norton AntiVirus CD, you can use it to scan. Hold down the Option key while launching Norton AntiVirus, then select the alternate virus definitions file.

To install selected components:

1. Restart from your Norton AntiVirus CD:
   - On a Power Macintosh, restart while holding down the letter “c” key on your keyboard.
   - On a third-party Macintosh, or on a Macintosh with a third-party CD-ROM drive, go to Control Panels, open Startup Disk, and select the Norton AntiVirus CD as your Startup Disk, then restart.
2. When your Macintosh restarts, the CD window appears with the Norton AntiVirus pattern in the background.

   In the CD window, double-click the Norton AntiVirus Installer icon.

   The Norton AntiVirus welcome screen appears.

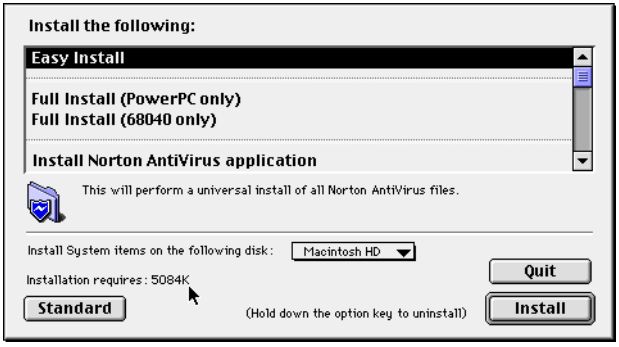
3. Click Continue to progress through the information screens.
4. Click Agree to accept the License and Warranty Agreement. (If you click Disagree, the installation is cancelled.)

The installation window appears.

5 Click Custom.

6 Scroll down the list and Shift-Click the parts of Norton AntiVirus to install.

Click any item to see its description and icon.



7 Select the disk on which to install.

If necessary, click Switch Disk to select the disk.

8 When you have selected all the features, click Install.

9 Follow the instructions on the screen to complete the installation.

If you changed the Startup Disk Control Panel setting to start up from the Norton AntiVirus CD, don't forget to restore the setting to your normal startup disk.

If you don't have a CD-ROM drive

If you don't have a CD-ROM drive, you can either use another Macintosh computer with a CD-ROM drive to create a set of installation disks using the disk images on the CD, or you can exchange the CD for floppy disks. To use the disk images, see "Creating installation diskettes" on page 26.

To exchange your CD, send in the Disk Exchange Form included in your package and send it to Symantec. See the Symantec Service and Support information in the *Norton AntiVirus 5.0 for Macintosh User's Guide* on the CD if you need to contact Symantec for further assistance.

Creating installation diskettes

Follow these steps to create installation diskettes from the disk images on the Norton AntiVirus CD.

To create installation diskettes:

1. On the Norton AntiVirus CD, open the Install Disk Images folder.

   The Install Disk Image window appears.

2. Double-click the first install disk image icon.

   Disk Copy prompts you to insert a floppy disk.

3. Insert an empty floppy disk in your disk drive, and click OK.

   The disk image contents are copied to the floppy disk.

4. Repeat this process with all the Norton AntiVirus disk images.

Installing Norton AntiVirus from floppy disks

If you created a set of installation diskettes from the Norton AntiVirus CD, use the following procedure to install Norton AntiVirus.

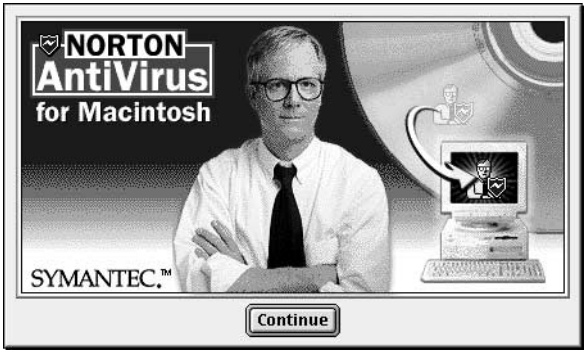
To install from floppy disks

1 Insert Install Disk 1 in your floppy disk drive.

The disk window appears.

2 Double-click the Norton AntiVirus Installer icon.

The Norton AntiVirus welcome screen appears.



3 Click Continue to progress through the information screens.

4 Click Agree to accept the License and Warranty Agreement. (If you click Disagree, the installation is cancelled.)

The installation window appears.

5 Click Install or Custom:

- Install installs all of Norton AntiVirus.
- Custom lets you select specific components to install.

A progress bar displays the progress of the install. A message prompts you to insert another installation disk.

6 Insert the installation disks when prompted.

7 Follow the onscreen messages until installation is complete.

Uninstalling Norton AntiVirus

If you need to remove Norton AntiVirus from your system, use the Norton AntiVirus Installer.

To uninstall Norton AntiVirus:

1 Insert the Norton AntiVirus CD in your CD-ROM drive.

2 In the CD ROM window, double-click the Norton AntiVirus Installer icon.

3 Click Continue to progress through the information screens.

4 Click Agree to accept the License and Warranty Agreement.

If you click Disagree, the installation is cancelled.

5 Click Custom.

6 Hold down the Option key on your keyboard.

The Uninstall Norton AntiVirus option appears in the Custom Install dialog box.

7 Click Uninstall.

Norton AntiVirus removes its files from your system.

Where to go after installation

When you install Norton AntiVirus with its preset options, Norton AntiVirus is set to protect your computer against viruses from any source. You don't have to do anything else to have protection.

Now that you've installed Norton AntiVirus:

- Make sure you have the latest virus protection by using LiveUpdate, or by downloading new virus definitions from our websites at:

  http://www.symantec.com

  http://service.symantec.com

  http://www.symantec.com/avcenter

Check our websites for the latest antivirus news, too.

- Scan all of your disks (including floppy disks) to make sure they are virus-free. See "Scanning disks, folders, and files" on page 43 for more information.
- Learn more about virus prevention by reading "About the virus definitions file" on page 35.
- Customize the installed settings for Norton AntiVirus. See "Setting preferences" on page 61.
- Find out how to protect your system and avoid viruses by reading "How to update virus protection" on page 36.
- Find out about scanning for viruses by reading "Checking for viruses" on page 43.

About Norton Auto-Protect

Norton AntiVirus Auto-Protect is the Norton AntiVirus system extension that guards against viruses as soon as your computer starts up. It checks programs for viruses as they are run and monitors your computer for any activity that might indicate the presence of a virus. When a virus or "virus-like" activity (an event that could be the work of a virus) is detected, Auto-Protect alerts you.

When you install Norton AntiVirus using the preset options, Auto-Protect is already turned on. It loads into your computer's memory each time you start up your Macintosh and provides constant protection while you work.

Turning Auto-Protect off temporarily

Auto Protect asks you if you want to suspend alerts when you're installing software, so that it doesn't interfere with installation. However, if you need to disable it for any other purpose, start Norton AntiVirus and choose Turn Auto-Protect Off from the Preferences menu.

Warning: Turning Auto-Protect off drastically reduces protection against viruses. Make sure you turn it back on as soon as possible!

Starting and exiting Norton AntiVirus

You don't have to start the Norton AntiVirus application to be protected from viruses if you have Auto-Protect running. You do have to start Norton AntiVirus application when you want to:

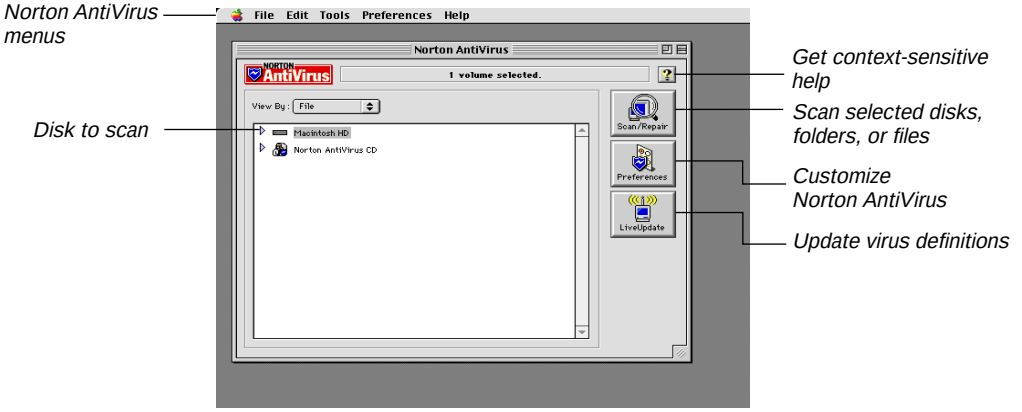
- Scan specific disks, folders or files on demand.
- Run LiveUpdate to update your virus protection.
- Schedule Norton AntiVirus to run unattended scans.
- Customize virus protection options.
- Repair infections found by Auto-Protect when files are opened or applications are launched.

To start Norton AntiVirus and scan for viruses:

1 Open the Norton AntiVirus folder and double-click the Norton AntiVirus icon.

The Norton AntiVirus main window appears.

The following picture shows the Norton AntiVirus main window on the desktop.



2 Select a disk, folder or file to scan. To select a folder or file, choose File from the View By list.

3 Click Scan.

Tip: To have Norton AntiVirus scan a specific file, folder, or disk, drag the file, folder, or disk icon to the Norton AntiVirus program icon.

To exit Norton AntiVirus:

- Choose Quit from the File menu, or press Command-Q.

Getting Help

Norton AntiVirus has an extensive, context-sensitive help system that you can access from open dialog boxes or windows.

To get context-sensitive help:

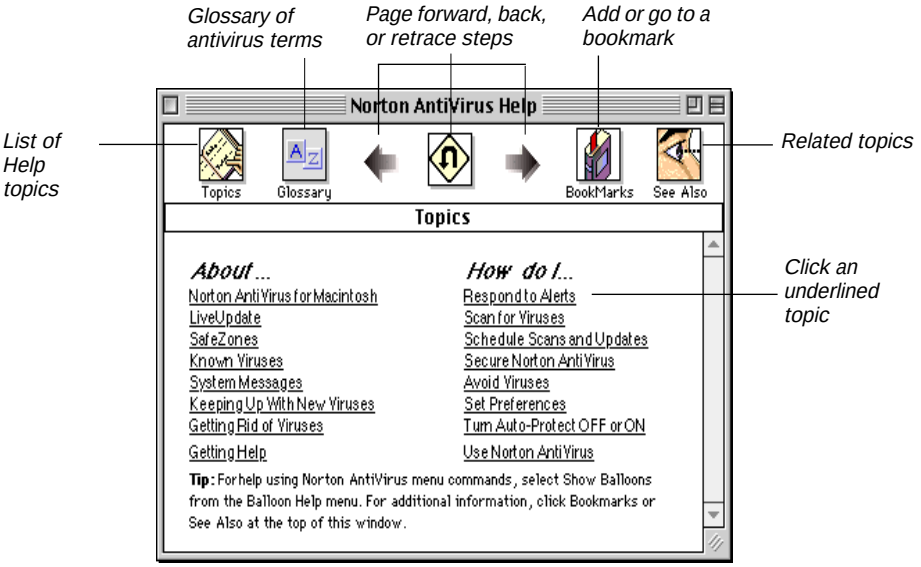
- Click the Help button in the upper right-hand corner of a dialog box or window.

Click the Help button to get help about a particular window or dialog box

To use Norton AntiVirus help:

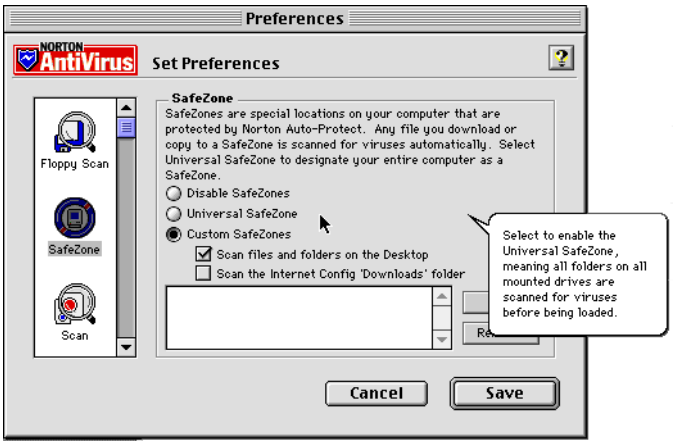
- Choose Norton AntiVirus Help from the Help menu.

  The Norton AntiVirus Help window appears.



Using Balloon Help

You can also use Balloon Help to familiarize yourself with the menu commands and dialog box options in Norton AntiVirus. With Balloon Help turned on, a descriptive text balloon appears when you move the cursor over a dialog box option, menu, or window item.



To turn Balloon Help on:

- Choose SHOW BALLOONS from the Help menu.

  A text balloon appears when you move the cursor over an item for which Balloon Help is available.

To turn Balloon Help off:

- Choose HIDE BALLOONS from the Help menu.

Using the Read Me file

The Read Me file on the CD contains late-breaking information, compatibility issues, and other helpful information.

To open the Read Me file:

- In the Norton AntiVirus CD window, double-click the Read Me icon.

CHAPTER 3

Keeping virus protection current

This chapter explains the various ways you can update virus definitions and view the list of viruses that Norton AntiVirus detects.

WHY? New viruses are found every day. You have to regularly obtain files for Norton AntiVirus that contain the latest virus protection. If you don't, you are not protected against viruses that have been released into the computer world since you bought the product. One of the most common reasons your computer is infected with viruses is that you have not updated your protection files since you bought the product.

Symantec provides online access to updated protection files, called *virus definitions* files with your subscription. Virus definitions files, produced regularly, contain the very latest in antivirus protection.

About the virus definitions file

The virus definitions files contain the latest virus information and technology from the Symantec AntiVirus Research Center (SARC). SARC engineers work around the clock to provide up-to-date virus definition files and keep your Macintosh safe. The information in the updated virus definition files lets Norton Auto-Protect and Norton AntiVirus detect and repair the newest viruses.

Note: In addition to virus definitions files, updates to files in the Norton AntiVirus Additions folder in the System Extensions folder are included whenever an update is created.

How to update virus protection

Use LiveUpdate's modem or Internet connection to automatically download and install updated virus protection files with your subscription.

As well as using LiveUpdate, you can access the latest virus definitions files and other update files on our World Wide Web server, at the Symantec FTP (File Transfer Protocol) site, on Symantec's bulletin board service (BBS), and through America Online or CompuServe. For information about these and other methods, see "Symantec Service and Support Solutions" on page 111.

When to update virus protection

You need to update virus definitions files regularly. New virus definitions files are made available monthly with your subscription.

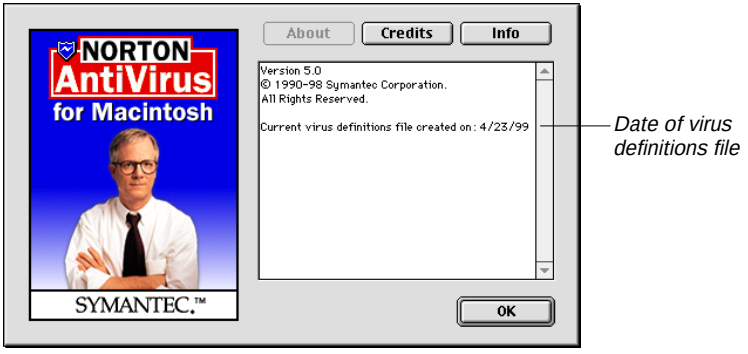
Checking the date of your virus definitions file

The Norton AntiVirus About box, accessible from the Apple menu, shows you the last date the files were updated.

To view your virus definitions file date:

1. Start Norton AntiVirus.
2. From the Apple menu, choose About Norton AntiVirus.

   The About box displays the revision number of the Norton AntiVirus application, and the date of your virus definitions.



3. Click OK.

Updating virus protection with LiveUpdate

WHY? LiveUpdate is the easiest way to keep virus protection current because it downloads the files for you and puts them in the correct location automatically. You can update virus protection anytime by clicking the LiveUpdate button.

To ensure that your computer is protected from the latest viruses, you should update virus protection as soon as you have installed Norton AntiVirus. You can update virus definitions using LiveUpdate (if you have a modem or Internet connection, this is the easiest method).

Using LiveUpdate

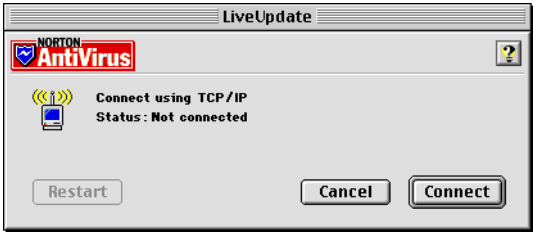
You can start Norton AntiVirus and use LiveUpdate at any time. You can also set LiveUpdate to run at a scheduled time. For details on scheduling, see "Scheduling virus protection updates" on page 40.

LiveUpdate is preset to use your modem to direct-dial the Symantec LiveUpdate server. If you have an existing Internet connection, you can change LiveUpdate's settings to connect to the LiveUpdate server through your Internet connection. For more information, see "LiveUpdate preferences" on page 78.

To update virus definitions with LiveUpdate:

1. Start Norton AntiVirus.
2. Click LiveUpdate.

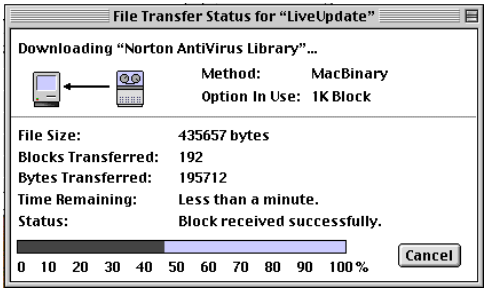
   The LiveUpdate dialog box appears.



3. Click Connect

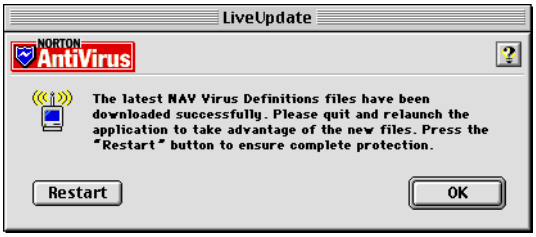
   If you have configured the LiveUpdate settings to match your system, the virus definitions are transferred automatically.

A status dialog box in the background keeps you informed of the file transfer process.



The file transfer takes a few minutes.

If your virus definitions files are up to date, a messages tells you that those files were not transferred.



4 Click Restart to restart your computer.

The new virus definitions are not in effect until you restart your computer.

Tip: You can schedule virus definitions updates to occur at regular intervals. For more information, see "Scheduling virus protection updates" on page 40.

Unsuccessful file transfer

If the transfer through TCP didn't work, check that your other Internet software, such as your browser, is working correctly.

If the file transfer through direct-dial modem didn't work, make sure you have the correct modem settings selected. See "Customizing modem settings" on page 80 for more information.

If your modem settings are correct and the file transfer still doesn't work, make sure the modem is properly connected and turned on. Then refer to ""System messages" on page 95." If you cannot find an answer in these sections, refer to your modem's manual for help.

Note: If the file transfer was unsuccessful or otherwise aborted, the original virus definitions file is restored.

If the file transfer aborted because of a power outage, Norton AntiVirus starts with an error message. You must restore the virus definitions file before Norton AntiVirus can load. Look up the error message in ""System messages" on page 95 for more information on how to resolve this problem.

Updating virus protection through Symantec's website

The current virus definitions files are located on Symantec's website and FTP site.

To use the website:

1. With your Internet browser, go to the following site:

   `http://www.symantec.com/avcenter/download.html`
2. Choose Norton AntiVirus for Macintosh from the product list, along with the language you wish to use.
3. Click the Next button.
4. Select the file you wish to download.

   Information about the update, such as the names of new viruses detected by Norton AntiVirus, is included with the download. A text file describes how to install the update.

To use the FTP site:

1. With your Internet browser, or FTP client software, go to the following FTP location:

   `ftp://ftp.symantec.com`

   The virus definitions files are located under the following directory:

   `public/english_us_canada/antivirusdefinitions/`
2. Download the most recent files in the directory.

Note: Make sure to decode or decompress the file if necessary. If the file you have downloaded ends in an extension such as .SIT, .SEA, .BIN, or .HQX, it must be expanded before Norton AntiVirus can use it. In most cases, double-clicking the file will expand it. See the instructions accompanying the virus definitions for more information.

Updating virus definitions from other sources

When a new virus definitions file becomes available, Symantec posts messages on several different online and bulletin board services (BBSs). You can use any of these services to download a new virus definitions file.

For information on updating virus protection from the Symantec BBS, CompuServe, or America Online, see the Service and Support Guide in the Norton AntiVirus 5.0 for Macintosh User's Guide in the CD jewel box.

Scheduling virus protection updates

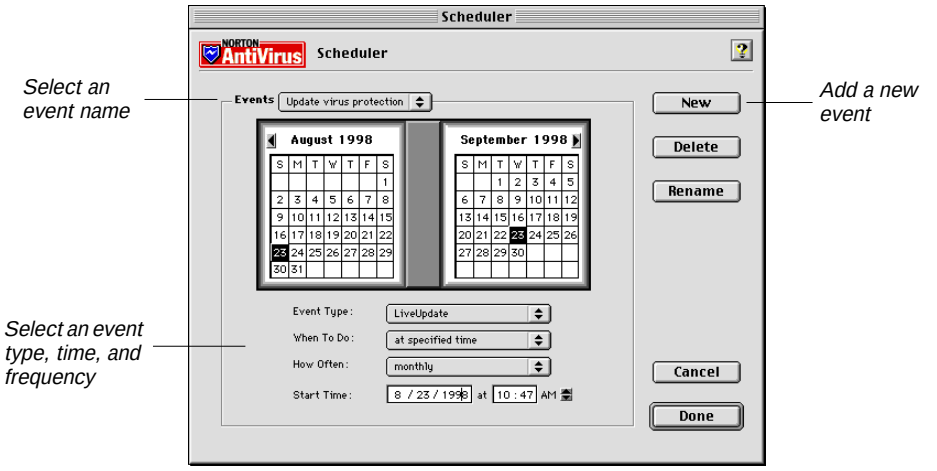
If you have a modem or Internet access, you can schedule automatic LiveUpdate sessions to update virus protection. Using the Scheduler, you can set up events to run automatically.

Tip: Before scheduling automatic virus protection updates, make sure the update process works correctly by stepping through the process manually. See "Updating virus protection with LiveUpdate" on page 37, for instructions.

To schedule virus definitions updates:

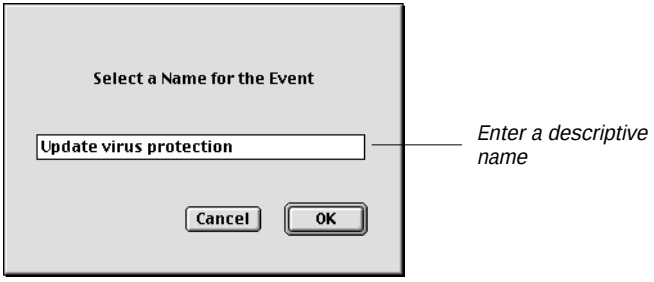
1 Choose Scheduler from the Tools menu.

The Scheduler dialog box appears.



2 Click New.

A dialog box appears prompting you to type a name for the scheduled event.



3 Type the event name (for example, “Update Virus Protection”) in the text box, then click OK.

The event name appears on the Scheduler dialog box.

4 Choose LiveUpdate from the Event Type list.

5 Choose At Specified Time from the When To Do list.

LiveUpdate updates virus definitions files at the time you specify on the scheduled days.

6 Choose the frequency of updates in the How Often list.

We recommend choosing Monthly. Virus definitions files are posted monthly, or more frequently when necessary.

The days on which updates occur are highlighted in the calendar. Dates for other scheduled events are underlined.

7 Finish scheduling the update by typing the schedule time and date.

- Click the Hour text box and use the arrow keys to set the start hour.
- Click the Minute text box to set the start minute.

8 Click Done.

CHAPTER 4

Checking for viruses

Viruses activate when you launch an infected application, start your computer from a disk that has infected system files, access a floppy disk with infected desktop files, or access a document containing a Macro virus. With Norton AntiVirus you can scan any file, folder, or disk for viruses.

You can customize the way Norton AntiVirus performs scans. For more information, see “Customizing Norton AntiVirus” on page 61.

Note: Norton AntiVirus can check compressed files for viruses, but not encrypted files. Encrypted files, which normally require a password to open, must be decrypted before you scan them. For information on which compressed file types Norton AntiVirus scans, see “Compression preferences” on page 77.

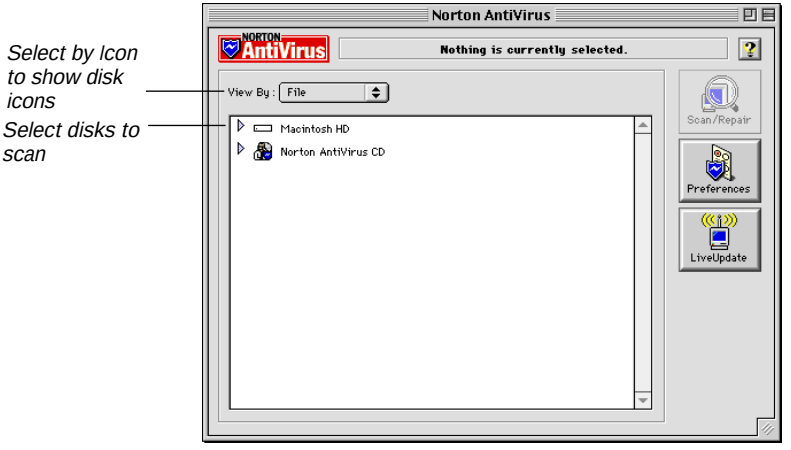
Scanning disks, folders, and files

Although Norton Auto-Protect monitors your computer for viruses, we recommend that you scan all disks before you use them.

To scan disks, folders, and files for viruses:

1 Start Norton AntiVirus.

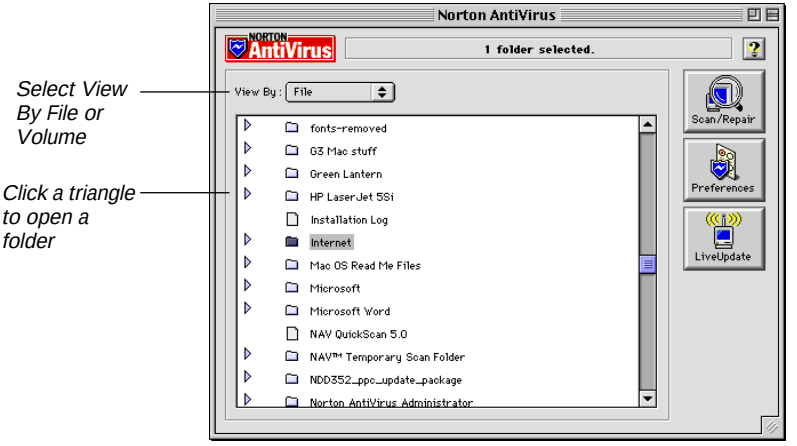
The Norton AntiVirus main window appears.



2 In the Norton AntiVirus main window, select the disks you want to scan:

- To select folders or files, choose File from the View By list.
- To view the contents of the disk, click the triangle next to the disk name.

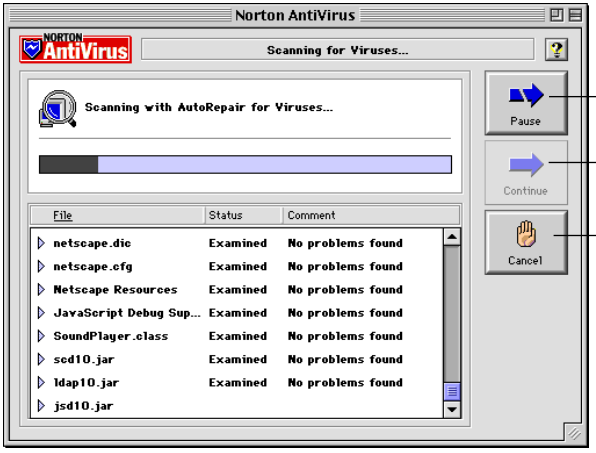
A list of folders and files appears.



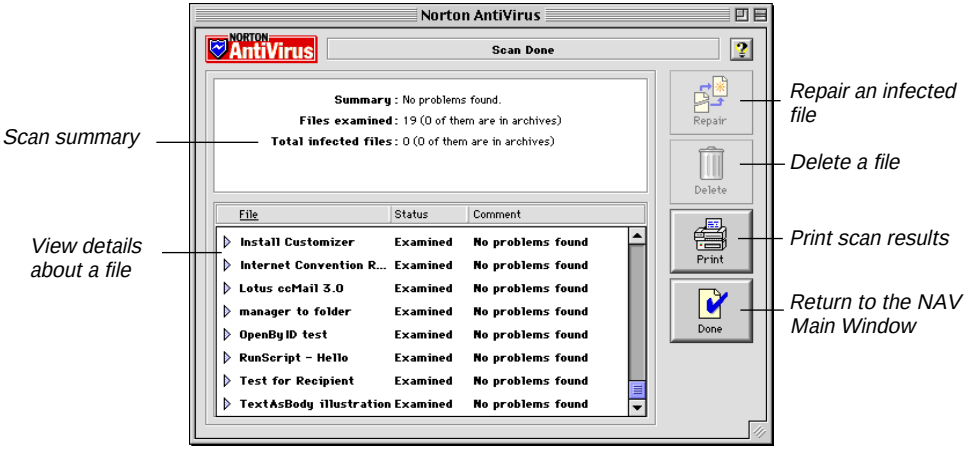
Tip: To select more than one adjacent icon, hold down the Shift and click the icons. To select non-adjacent icons, hold down the Command key and click the icons. To select all of the disk icons, choose Select All from the Edit menu.

3 Click Scan.

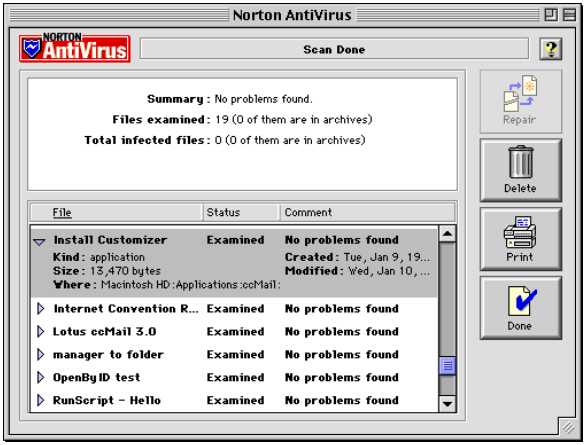
The scan window shows the progress of the scan.



When the scan is complete, the results of the scan are shown in the window. The top portion of the screen shows a summary of the scan. The bottom portion of the screen lists any files that were found to have problems.



4 To see details of a selected file, click the triangle beside the file.



What to do if a virus is found

Problems found

If a virus was found, and Auto-Repair is enabled, the file is automatically repaired.

If the virus was not repaired, don't panic—it can be removed. See "If Norton AntiVirus can't repair a file" on page 55, for instructions on how to proceed.

No problems found

If no problems were found during the scan, the scan results window shows summary information. See "Saving and printing a scan report" on page 46, for more information.

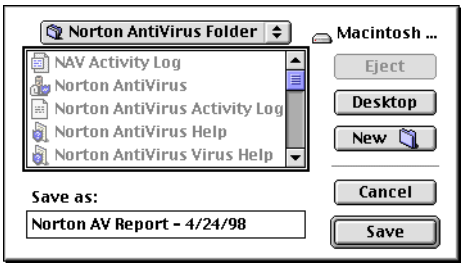
Saving and printing a scan report

You can save a report of the scan results to a file and view it later. You can also print a report.

To save the scan report to a file:

- Choose Save Report As from the File menu.

A standard file dialog box appears where you can specify a name and location for the file. The default filename is "Norton AV Report *date*," where *date* is the date of the scan.



Note: For information on the report's file format and other report options, see "Customizing scan reports" on page 74.

To print the scan report:

- Do one of the following:
  - Click Print in the scan results window.
  - Choose Print Report from the File menu.

  A standard Print dialog box appears, letting you change the printing options before printing the scan results.

Scheduling automatic virus scans

To make virus prevention as easy as possible, Norton AntiVirus lets you schedule different types of activities, such as the following:

- Virus scans to occur at specified times. *See* "Scheduling virus scans" on page 48.
- Automatic updates of virus definitions with LiveUpdate. *See* "Scheduling virus protection updates" on page 40.

NOTE: If your Macintosh is turned off during the time an event should take place, the event occurs the next time you start your Macintosh.

When Norton AntiVirus completes an unattended scheduled scan, it creates a report and saves it on the desktop before quitting. The report name is "NAV Scheduled Scan *mm/dd/yy*".

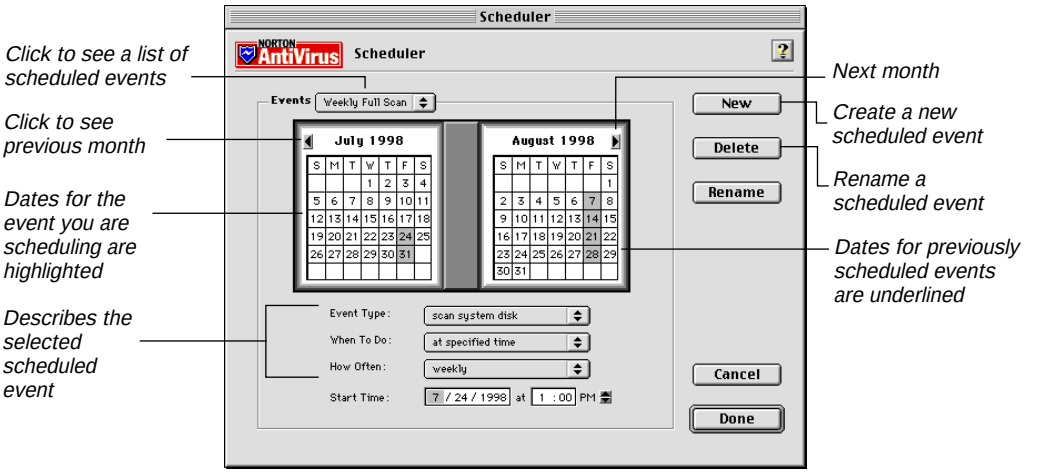
Scheduling virus scans

Follow the procedure below to schedule automatic virus scans.

To schedule virus scans:

1 Choose Scheduler from the Tools menu.

The Scheduler dialog box appears.



2 Click New.

A dialog box appears prompting you to type a name for the scheduled event.

3 Type the event name in the text box, then click OK.

4 Choose the item you want to scan from the Event Type list:

- **Scan System Folder**

  Scans the System folder on the startup disk.

- **Scan System Disk**

  Scans the entire startup disk.

- **Scan All Local Disks**

  Scans all disks physically connected to your computer.

- **Scan All Network Disks**

  Scans all network drives mounted at the time the scan runs.

- **Scan All Mounted Disks**

  Scans all local and network drives mounted at the time the scan runs.

- **LiveUpdate**

  Run LiveUpdate.

5 Choose when the scan should occur from the When list:

- **At Specified Time**

  Lets you decide the time for the scan to occur.

- **At Startup**

  Scans for viruses each time your computer starts up.

- **At Shutdown**

  Scans for viruses each time your computer shuts down.

6 Choose the frequency of the scan from the How Often list:

- **Never**

  Never run the event.

- **Once**

  Run the event one time only at the indicated time.

- **Hourly**

  Run the event hourly at the indicated time.

- **Daily**

  Run the event daily at the indicated time.

- **Weekdays**

  Run the event every weekday, Mondays through Fridays, at the indicated time.

- **Monthly**

  Run the event monthly at the indicated time.

- **Always**

  Always run the event.

The days on which the scans will occur appear highlighted in the calendar.

7 Finish scheduling the scan by entering the correct time and date information:

- Click the Hour text box and use the arrow keys to set the start hour.
- Click the Minute text box to set the start minute.

  This option is dimmed if the scan occurs at startup or shutdown.

8 Click Done.

Note: You can store the scan results in a file called "Norton AV Report *mm//dd/yy*" where *mm/dd/yy* represents the date the scan occurred. You can view the file by double-clicking it.

For information on selecting an application for viewing these reports, see "Customizing scan reports" on page 74.

Editing scheduled events

You can easily make changes to the events you schedule.

To edit a scheduled event:

1 Choose Scheduler from the Tools menu.

The Scheduler appears.

2 Choose the scheduled event you want to change from the Event list.

3 Make your changes.

For information on the options, see "Scheduling virus scans" on page 48, or "Scheduling virus protection updates" on page 40.

4 Click Done.

Deleting scheduled events

You should delete events you no longer want.

To delete a scheduled event:

1 Choose Scheduler from the Tools menu.

The Scheduler dialog box appears.

2 Choose the scheduled event you want to delete from the Event list.

3 Click Delete.

CHAPTER 5

What to do if a virus is found

This chapter helps you resolve problems detected by Norton AntiVirus, such as a virus or virus-like activity on your computer.

If Norton AntiVirus reported a problem, skim this chapter to find the section that best describes the problem reported on your screen, then follow the instructions provided.

If the message on your screen is not discussed in this chapter, see "System messages" on page 95, for more information.

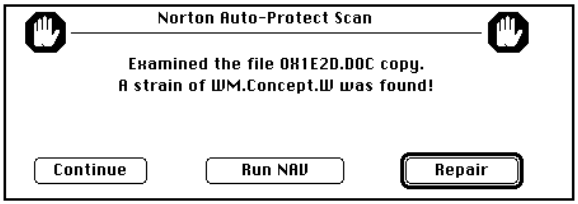
Responding to virus alerts

When a virus is found while Norton AntiVirus Auto-Protect is running, an alert message displays what happened, and what your options are.

Auto-Protect alerts you to any virus activity, whether the file is repaired automatically or not. Read the message carefully to determine whether you need to do anything.

If a virus is found but not repaired by Auto-Protect

Look for words that identify the type of problem. Read the whole message.



- Press Return to choose the action that is preselected for you, or click the button of the action you want to take (for example, click Repair).

  When Repair is highlighted, it is always the best choice. Repair eliminates the virus and repairs the infected item automatically.

If a virus is found and repaired by Auto-Protect

1. When Norton AntiVirus Auto-Protect reports that it repaired an infected file automatically, *you don't have to do anything else.*

   A message informs you when an infected file is repaired.

2. Even if the file was repaired, it is still a good idea to click Run NAV and scan with Norton AntiVirus to ensure no other viruses exist on your computer.

If a virus can't be repaired

- If the file can't be repaired automatically, click Run NAV and scan the folder or file containing the virus.

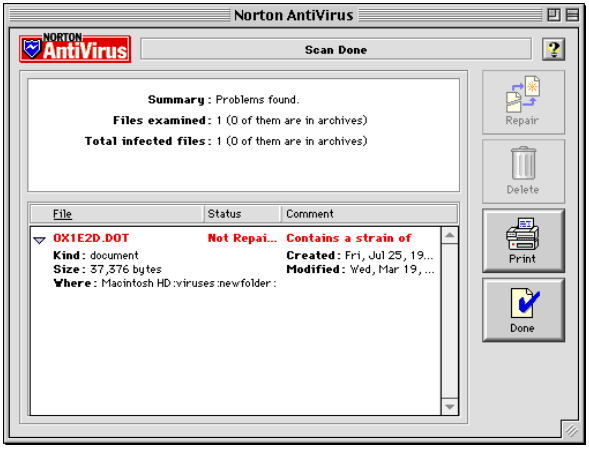
  In the scan window, you can view more details about the infected file and take further action. See "If Norton AntiVirus can't repair a file" on page 55 for what to do when a file can't be repaired.

If a virus is found while scanning

If you are scanning with Norton AntiVirus and a virus is found, a “Problem found” alert appears in the scan window. Usually, infected files are repaired automatically and you don’t have to do anything else.

If “Problem found” appears in the scan window:

1. Highlight an entry in the scan results window. You can view more details about the infected files and take further action.
2. Click the triangle to view more information about the file.



3. If the infected file was not repaired automatically, click Repair.
4. If a file can’t be repaired, click Delete. See “If Norton AntiVirus can’t repair a file” on page 55 for more information.

Repairing infected files

When a virus is found, you can repair the infected file:

- If Auto-Repair is enabled, an infected file is repaired automatically and you are informed of the results.
- If Auto-Repair is not enabled, you must click Repair in the Auto-Protect alert, or start the Norton AntiVirus applications and scan the infected file.

To repair infected files:

1. Select the file or files to repair in the scan results list.
2. Do one of the following:
   - Click Repair.
   - Double-click the selected file or files.

   The Repair dialog box appears.

3. In the Repair dialog box, do one of the following:
   - Click Repair.
   - Click Copy/Repair if you want a backup copy of the file created before it is repaired.

   The Status column in the scan window shows “Repaired” for the file.
4. After repairing all infected files, scan your hard disks and floppy disks again to verify that there are no other infected files.
5. Check the repaired files to make sure they function properly.

   For example, if you repaired a word processing program, start it, edit a file, save a file, and so forth to make sure it has been repaired correctly.

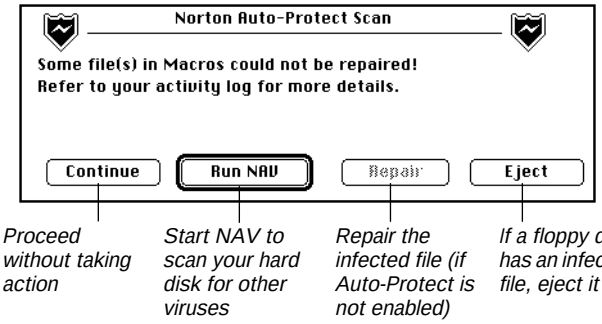
Note: If you chose to have Norton AntiVirus make a backup copy of the infected file before you repaired it, be sure to delete the backup file (because it too is infected) once you are certain the repair worked correctly. The infected backup copy of the file is stored in the same directory as the original file. (The backup copy is named “infected filename” where *filename* is the name of the original file.)

If Norton AntiVirus can't repair a file

If Norton 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, use LiveUpdate. See "Updating virus protection with LiveUpdate" on page 37 for details.)

Deleting infected files

Sometimes viruses damage a file beyond repair. If Norton AntiVirus finds an irreparable file, we recommend that you delete the infected file and replace it with an uninfected backup copy.



You cannot delete an infected file from an Auto-Protect alert. You must delete it from the Norton AntiVirus scan window.

To delete an infected file:

1. In the Norton AntiVirus scan results window, if a file is infected and can't be repaired, select it and click Delete.
2. Click OK to confirm the deletion.

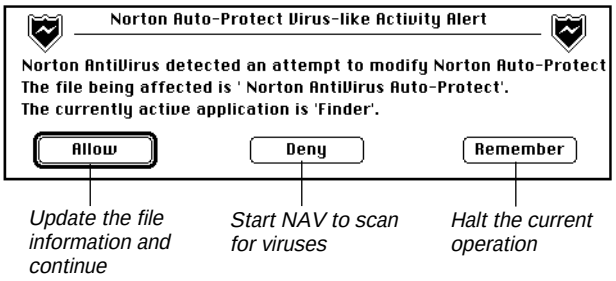
   The Status column in the scan window shows "Deleted" for the file.

Responding to virus-like activity alerts

A *virus-like activity* is an activity that viruses often perform when spreading or damaging your files. This alert does *not* necessarily mean a virus is present. The virus-like activity reported is often legitimate. However, because it is an action that viruses also perform, you should investigate it. When a virus-like activity is detected, an alert box appears.

Tip: Make sure you have the most recent virus definitions file. If the application does contain an unknown virus, the newest virus definitions file may have a definition for it. See "Keeping virus protection current" on page 35, for more information on updating the virus definitions file.

For a description of each virus-like activity detected by Norton AntiVirus, see "Prevention preferences" on page 68.



To resolve a virus-like activity alert:

Do one of the following

- Press Return to choose the action that is preselected for you.
- Click the button of the action you want to take:
  - **Allow**

    Click Allow if the message describes a valid activity for the application you are running. For example, if you are changing a system setting.
  - **Deny**

    Click Deny if the detected activity isn't related to what you are trying to do. If the Deny button is dimmed, the virus-like activity has proceeded too far for Norton AntiVirus to stop without causing damage or "crashing" the system. If this happens, note the file involved and the currently active application before continuing. Then scan both files to check for known viruses.
  - **Remember**

    Click Remember if you don't want the alert to appear again. If the activity is valid for the application you are running and you don't want Norton AntiVirus to alert you

when the same application performs the same activity in the future, click Remember.

This activity is added to the Exceptions List. Future attempts to perform the same action by the same application will not trigger the activity alert. See "Managing virus-like activities" on page 86, for more information on viewing and editing the exceptions list.

Responding to file changed alerts

A Norton AntiVirus Auto-Protect alert appears when an application file has changed since the last time it was scanned. If you selected Protect Against Unknown Viruses in the Scan Preferences, Auto-Protect looks out for changes to application files. These changes could indicate the presence of an unknown virus. However, they do *not* necessarily mean the file is infected. Although it's unusual, sometimes applications modify themselves

---

TIP: If you have been using the application for some time without an alert of this kind appearing, the file is more likely to have a problem.

To resolve a file changed alert:

1 Click one of the following buttons:

- **Proceed**

  If you are certain the application file has changed for legitimate reasons (for example, you recently installed a new version of the application), click Proceed.

  If the Proceed button is dimmed, Norton AntiVirus is configured not to allow the application to run. This is the default setting. To view or change the setting, see "Scan preferences" on page 67.

- **Stop**

  If you are uncertain about the file, click Stop to prevent the application from running. Then delete the file and reinstall the application from the original *locked* diskette or CD.

- **Run NAV**

  Click Run Norton AntiVirus to launch the Norton AntiVirus application and automatically rescan the file.

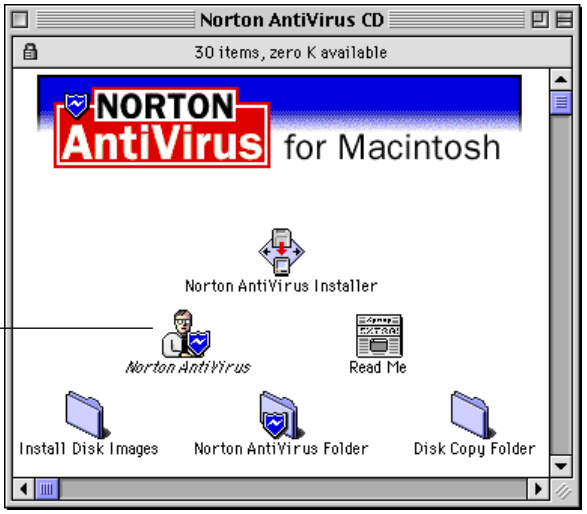
Decontamination procedures

If you think a virus has infected your Macintosh, and you are afraid there might be a virus in memory, you can use the Norton AntiVirus CD to restart your Macintosh and remove the virus.

To scan for viruses:

1. Insert your Norton AntiVirus CD into the CD-ROM drive.
2. To restart from your Norton AntiVirus CD, do one of the following:
   - On Apple Power Macintosh computers, restart while holding down the letter “c” key on your keyboard.
   - On third-party Macintosh computers, or on Macintosh computers with third-party CD-ROM drives, go to Control Panels, open Startup Disk, and select the Norton AntiVirus CD as your Startup Disk, then restart.

   When your Macintosh restarts, the CD window appears with the Norton AntiVirus pattern in the background.



3. In the CD window, double-click the Norton AntiVirus icon.

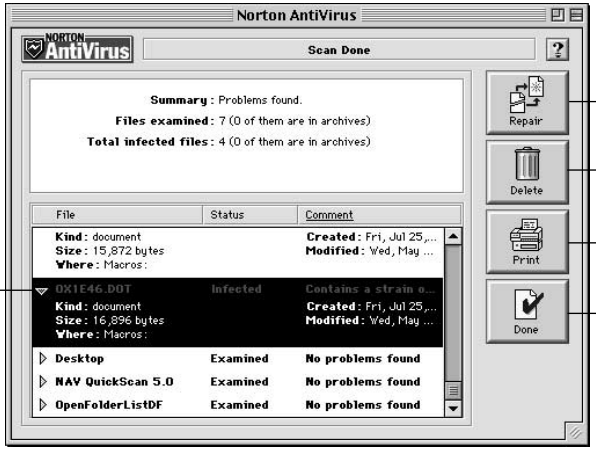
Note: If you have a more recent Norton AntiVirus Virus Defs file than the file on the Norton AntiVirus CD, you can use it to scan. Hold down the Option key when you open Norton AntiVirus, and then select the alternate virus definitions file.

4 In the Norton AntiVirus main window, select the disk to scan.

5 Click Scan.

Norton AntiVirus scans your entire hard disk.

When the scan is complete, the results of the scan are shown in the scan window. The top portion of the screen shows a summary of the scan. The bottom portion of the window lists any infected files.



6 If a virus was found, select the infected file or files in the scan window, then click Repair.

To select more than one file, press the Apple or Command key when you click the filename.

The Status column in the results list shows “Repaired” for the file.

Note: If Norton AntiVirus was not able to repair an infected file, see “If Norton AntiVirus can’t repair a file” on page 55 for more information.

---

7 Click Done in the scan window.

8 Choose Quit from the File menu.

9 Restart your Macintosh.

Note: If you changed the Startup Disk Control Panel setting to start up from the Norton AntiVirus CD, don’t forget to restore the setting to your normal startup disk.

Now that your hard disk is virus-free, scan any other disks that might be infected. See “Scanning disks, folders, and files” on page 43.

CHAPTER 6

Customizing Norton AntiVirus

This chapter explains how to change Norton AntiVirus settings to fit your work environment. For settings that govern the behavior of scanning, Auto-Protect, LiveUpdate, and related activities, use the Preferences dialog box, accessible by clicking the Preferences button in the main window. The Tools menu has additional settings for the Scheduler and the Exceptions List. The Preferences menu has additional settings for Menu Security and Turn Auto-Protect Off.

Setting preferences

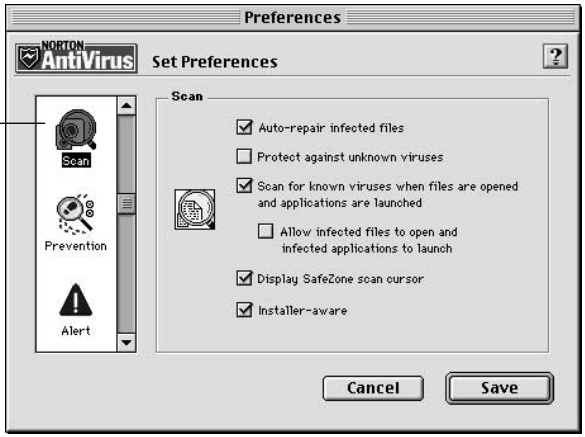
You can change a wide range of settings for the way Auto-Protect and the Norton AntiVirus application perform.

Accessing preferences

To open the Preferences dialog box:

1 Click the Preferences button on the Norton AntiVirus main window.

The Preferences dialog box appears.



Click an icon to display its preferences

The left side of the Preferences dialog box contains icons that, when you click them, open set of options you can customize.

2 Click an icon in the list:

- **Floppy Scan**

  Covers how Norton Auto-Protect handles floppy disks and other removable media.

- **SafeZone**

  Determines what areas of your computer are protected by Auto-Protect.

- **Scan**

  Determines how Auto-Protect and the Norton AntiVirus application performs scans, and whether Auto-Protect alerts you to changes in application files.

- **Prevention**

  Customizes how Auto-Protect and the Norton AntiVirus application monitor virus-like activities.

- **Alert**

  Customizes the type and duration of Auto-Protect alert messages.

- **Report**

  Identifies a file format for Activity Logs, and chooses which activities to record in the log.

- **Compression**

  Chooses which types of compressed files you want to scan.

- **LiveUpdate**

  Indicates whether LiveUpdate updates virus protection through an existing connection or by dialing the Symantec LiveUpdate server directly.

Use the scroll bar to view and select all the icons.

Note: You can also select each preference from the Preferences menu.

---

3 Make the changes to the preference settings.

For details about each setting, see the individual preferences settings.

4 When you have changed the preference settings, click Save.

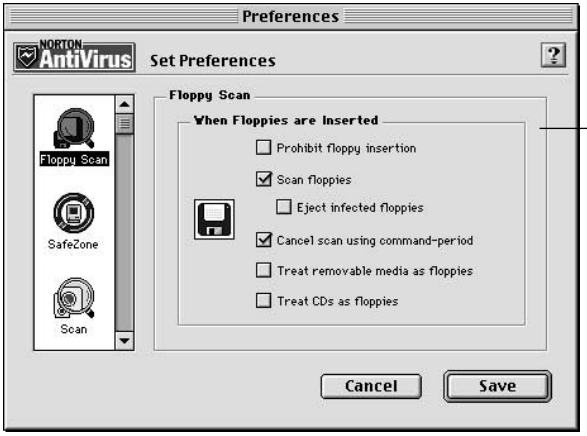
Floppy Scan preferences

The most common way for a virus to enter your computer is through floppy disks or other removable media. To prevent this from happening, Norton AntiVirus Auto-Protect scans these items each time they are inserted into your computer. Change this Floppy Scan default setting if you do *not* want Auto-Protect to scan floppy disks when they are inserted.

To customize floppy disk scanning:

1 Click the Floppy Scan icon in the Preferences dialog box.

The Floppy Scan options appear.



2 Specify what Norton AntiVirus should do when a floppy disk is inserted.

3 Click Save.

The following options are available for Floppy Scan preferences:

- **Prohibit Floppy Insertion**

  Ejects all floppy disks. Norton AntiVirus does not allow access to floppy disks. This option must be cleared before you can repair an infected floppy disk.

- **Scan Floppies**

  Scans floppy disks each time they are inserted

- **Eject Infected Floppies**

  Norton AntiVirus Auto-Protect ejects floppy disks with infected files.

- **Cancel Scan Using Command-Period**

  Lets you stop an in-progress floppy disk scan. Pressing Command-period (⌘-.) stops the scan.

- **Treat Removable Media As Floppies**

  Causes all removable media, such as Jaz and Zip cartridges, to be treated like floppy disks.

- **Treat CDs As Floppies**

  Causes all CDs to be treated like floppy disks.

SafeZone preferences

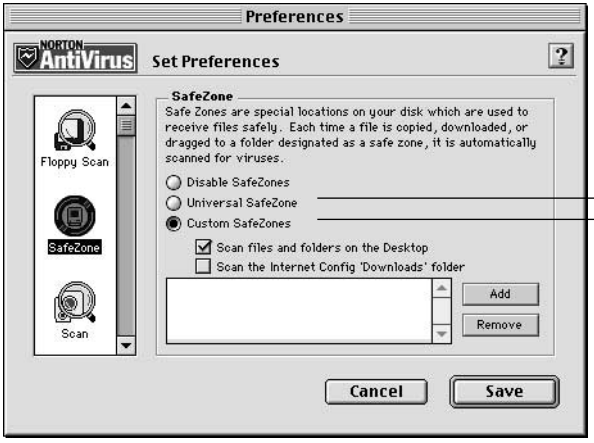
You run the risk of infecting your Macintosh every time you download or receive a file from the Internet and bulletin board services (BBS), or copy files from any other source. SafeZones are special locations on your computer that are protected by Norton AntiVirus Auto-Protect. To prevent virus infection, Auto-Protect immediately scans any file for viruses that are copied or downloaded to an area designated as a SafeZone. The cursor changes to a special SafeZone cursor while files are scanned.

When you perform a standard installation, part of your computer is set up as a Custom SafeZone. You can, however, designate any folder as a SafeZone. If you would like to configure your SafeZone settings to protect your entire computer, including email folders, Internet folders, or network volumes, you can use the Preferences settings to establish a Universal SafeZone.

To specify a different SafeZone:

1 Click the SafeZone icon in the Preferences dialog box.

The SafeZone options appear.



2 Specify the SafeZone settings.

3 Click Save.

The following options are available for SafeZone preferences:

- **Disable SafeZones**

  Select if you don't want Auto-Protect to automatically scan downloaded files for viruses.

- **Universal SafeZone**

  Select to have Auto-Protect scan every file that is downloaded in addition to files that are launched or created.

- **Custom SafeZones**

  Select to specify additional folders as SafeZones.

- **Scan Files And Folders On The Desktop**

  Select to have Auto-Protect scan all files and folders on your desktop.

- **Scan The Internet Config 'Downloads' Folder**

  If you use the Internet Config utility program. Internet Config is a popular Macintosh utility program to configure Internet browsers. With Internet Config, you designate a particular folder for all Internet downloads. If selected, Auto-Protect scans files arriving in this folder automatically.

Adding and removing SafeZones

Use the following procedure to add and remove SafeZones.

To configure a Custom SafeZone:

1. Click Custom SafeZones.

   By default, Scan Files And Folders On The Desktop is selected.

2. If you use the Internet Config utility program, select Scan Internet Config 'Downloads' folder.

   Internet Config is a popular Macintosh utility program to configure Internet browsers. With Internet Config, you designate a particular folder for all Internet downloads. If selected, Norton AntiVirus scans files arriving in this folder automatically.

3. Click Add.

   Select the folder or volume to be a SafeZone. The location appears in the list.

   You can designate as many SafeZones as are appropriate for your work habits.

4. Click Save.

To create a Universal SafeZone:

1. Click Universal SafeZones.
2. Click Save.

To remove a Custom SafeZone:

1. Click Custom SafeZones.
2. Click the SafeZone to be removed.
3. Click Remove.
4. Click Save.

Note: If a Custom SafeZone volume is unavailable, it is listed as "Not found."

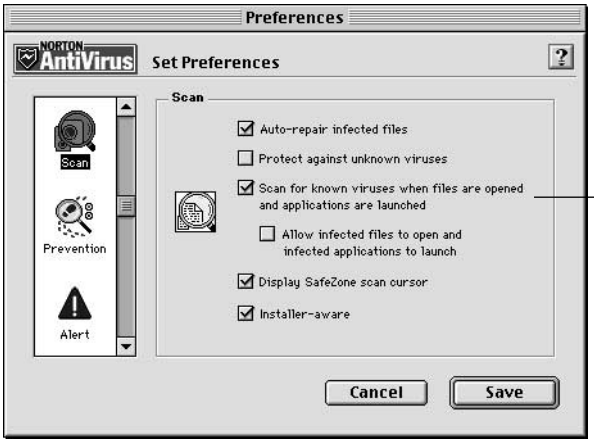
Scan preferences

The Scan options apply to all scans performed by the Norton AntiVirus application and by Auto-Protect. This includes scans you initiate, scheduled scans, automatic floppy disk scans, and scans that Norton AntiVirus initiates automatically (when you launch an application, for example).

To modify scanning options:

1 Click the Scan icon in the Preferences dialog box.

The Set Preferences dialog box appears with the Scan options displayed.



2 Select the scan options you want.

See the description of settings below.

3 Click Save.

The following options are available for Scan preferences:

- **Auto-Repair Infected Files**

  Norton AntiVirus and Auto-Protect automatically detect and repair infected files and inform you of the result.

- **Protect Against Unknown Viruses**

  Norton AntiVirus Auto-Protect monitors application files for changes that could indicate the presence of an unknown virus.

  The Norton AntiVirus QuickScan technology records critical information about all the files on your hard disk. On subsequent scans, Auto-Protect checks the file against the QuickScan information

and notifies you if there are any changes that could indicate an unknown virus.

- **Scan For Known Viruses When Files Are Opened And Applications Are Launched**

  Norton AntiVirus Auto-Protect scans applications when they are launched and scans documents when they are opened.

- **Allow Infected Files To Open And Infected Applications To Launch**

  Selecting this option enables a "Proceed" button Auto-Protect alerts, allowing you to run an application even though it might contain a virus. An alert box lets you choose whether to run the application or not.

  Warning: Use caution when selecting this option. If you choose to run an infected application, the virus activates and spreads.

- **Display SafeZone Scan Cursor**

  The SafeZone cursor appears in place of the Macintosh pointer when Norton AntiVirus or Norton AntiVirus Auto-Protect are scanning files.

- **Installer-Aware**

  Suppress Norton AntiVirus virus-like activity alerts during installation of applications such as Norton Utilities for Macintosh, and other programs that use common installation programs.

Prevention preferences

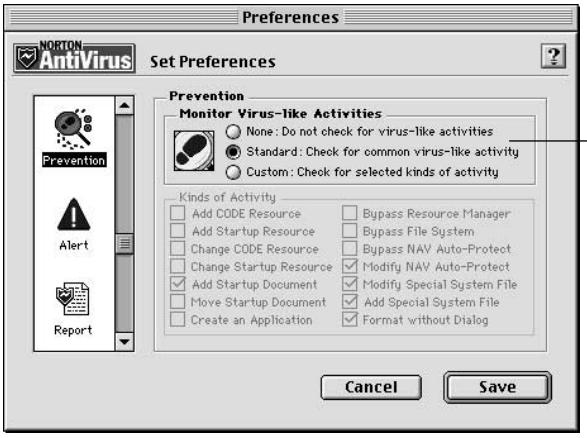
The Prevention options let you set the level of virus-like activities monitored by Auto-Protect. A *virus-like activity* is an action that a virus might perform when damaging your files or spreading through your system. Although some applications perform these actions for valid reasons, Norton AntiVirus can monitor for these activities on the chance that an unknown virus is performing one of them. In most environments, the default Standard setting is sufficient.

If a virus-like activity is detected, it does not necessarily mean that a virus is performing the activity—you must decide whether to continue or not. For more information, see "Responding to virus-like activity alerts" on page 55.

To customize virus-like activity monitoring:

1 Click the Prevention icon in the Preferences dialog box.

The Prevention options appear.

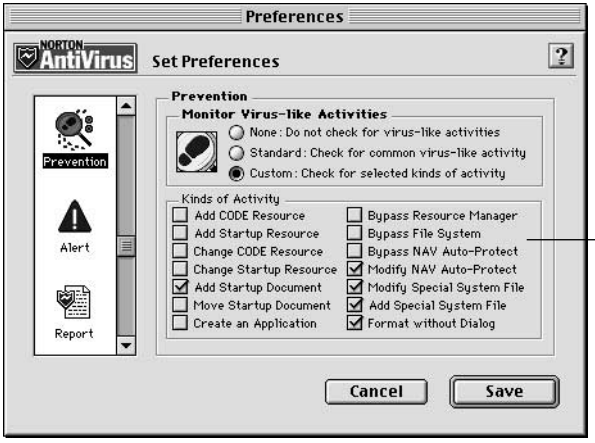


Select a prevention level for monitoring virus-like behavior

2 Select a prevention level for monitoring virus-like activities.

Tip: If you're not sure which option to choose, select Standard.

3 If you select Custom, an additional group of check boxes appears.



Select the virus-like behaviors to monitor

4 Select the custom options you want.

5 Click Save.

The following options are available for Prevention preferences:

- **None**

  No virus-like activity monitoring

- **Standard**

  Monitors applications for the most common virus behavior, such as adding code instructions to an application file.

- **Custom**

  Lets you choose which virus-like activities Norton AntiVirus monitors.

- **Add Code Resource**

  A program tries to add code instructions to another file. This is the most common way viruses infect files. If this activity is detected, it is a good indication of an unknown virus at work.

- **Add Startup Resource**

  A program tries to add startup resource code to any file in the System folder. This is also a common way viruses infect. If this activity is detected, it is a good indication of an unknown virus at work.

- **Change Code Resource**

  A program tries to change a file's existing instructions. Programs rarely modify themselves. If this activity is detected, it is a good indication of an unknown virus at work.

- **Change Startup Resource**

  A program tries to change code resources in a startup document. If this activity is detected, it is a good indication of an unknown virus at work.

- **Add Startup Document** (default Standard option)

  A program attempts to create a new startup document. Although this activity often happens legitimately (during the installation of new software, for instance), it could indicate an unknown virus at work.

- **Move Startup Document**

  A program tries to move a startup document into or out of the System folder. Although this activity often happens legitimately (when you move startup documents using the Finder, for example), it could indicate an unknown virus at work.

- **Create An Application**

  A program tries to create an application file that can be started. Although this activity often happens legitimately (when you copy files using the Finder, for example), it could indicate an unknown virus at work.

- **Bypass Resource Manager**

  A program attempts to modify a resource file without going through the Macintosh Resource Manager. Modifications to a resource file are common; however, they normally take place using the facilities of the Resource Manager. Although this activity often happens legitimately (when you use a backup program, for instance), it could indicate an unknown virus at work.

- **Bypass File System**

  A program attempts to modify a disk without going through the Macintosh file system. Although this activity could indicate an unknown virus at work, some applications (such as ResEdit, THINK C, and Macintosh Programmer's Workshop) bypass the file system as part of their normal processing.

- **Bypass NAV Auto-Protect**

  A program attempts to modify a resource file without passing through checkpoints that Norton AntiVirus Auto-Protect sets up for monitoring modification attempts.

  This alert is fairly rare. If it appears, you should be suspicious because only a few programs (for example, THINK C, Pascal, ResEdit, and some FAX programs) bypass Auto-Protect legitimately. Check the Read Me file for the names of any other software programs that bypass Auto-Protect.

- **Modify NAV Auto-Protect** (default Standard option)

  A program attempts to make changes to Norton AntiVirus Auto-Protect. If this activity is detected, it is a good indication of an unknown virus at work.

- **Modify Special System File** (default Standard option)

  A program attempts to write to the debugger, disassembler, or System file in a System folder. If this activity is detected, it is a good indication of an unknown virus at work.

- **Add Special System File** (default Standard option)

  A program attempts to move, rename, or create a debugger or disassembler file in a System folder. Attempts like this are infrequent and should be viewed suspiciously.

- **Format Without Dialog** (default Standard option)

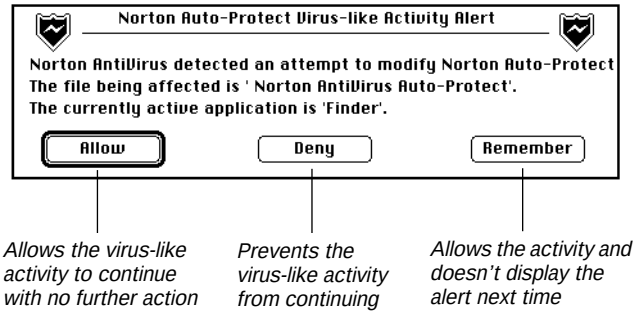
  A program attempts to format a disk without the standard format dialog box. This may be caused maliciously by a Trojan horse or legitimately by an application, such as a utility program attempting to create a disk partition. Attempts like this are infrequent and should be viewed suspiciously.

Alert preferences

The Alert settings specify how Norton AntiVirus Auto-Protect informs you that it has detected a virus or *virus-like activity*.

You can customize the message that appears in the alert dialog box, and change other characteristics of the alert. You can set how long the alert stays on the screen, enter a special message, alert others on a network, or tell Auto-Protect not to alert you to this type of activity again.

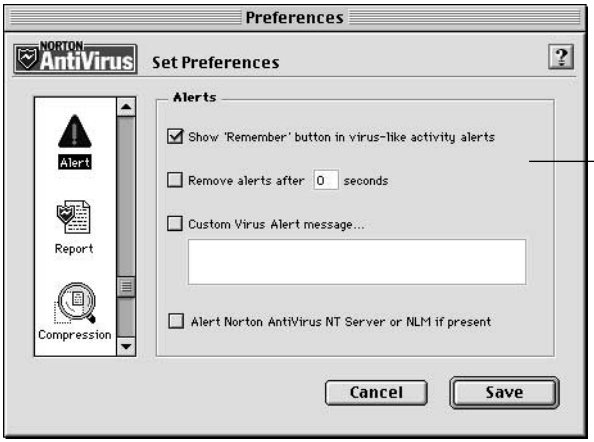
The following picture shows a typical virus-like activity alert.



To customize alerts:

1 Click the Alert icon in the Preferences dialog box.

The Alerts options appear.



2 Select the options you want.

3 Click Save.

The following options are available for Alert preferences:

- **Show 'Remember' Button In Virus-Like Activity Alerts**

  Causes Norton AntiVirus Auto-Protect to ignore specific actions while a particular program is running. (This setting affects the Prevention preferences.)

  Sometimes Norton AntiVirus alerts you of actions that could be the work of a virus, but in fact are not. In these cases, you can select the Remember button to add the file to the exceptions list, preventing the alert from appearing in the future. See "Managing virus-like activities" on page 86 for more information.

- **Remove Alerts After ___ Seconds**

  Select to specify how long alert boxes stay on your screen before the default button is selected automatically. Then type the number of seconds (0 to 99) in the seconds text box.

  For virus alerts the default button is always Stop. For virus-like activity alerts the default button is always Allow.

  Clear this option if you want alerts to stay on the screen until you respond to them.

- **Custom Virus Alert Message**

  Select if you want a custom message to appear in virus alerts and virus-like activity alerts. Enter the message (such as “Call Help Desk - 55555”) in the text box.

- **Alert Norton AntiVirus NLM If Present**
  Select to have alerts from Norton AntiVirus sent to the Norton AntiVirus NetWare Loadable Module (NAVNLM) or Norton AntiVirus for Windows NT (NAV NT) if it is present on your local network.

Report preferences

Norton AntiVirus generates two types of reports:

- Scan results that appear in the Norton AntiVirus main window from scans that you initiate or schedule.
- Scan results from Norton AntiVirus Auto-Protect activity, such as automatic floppy disk scans, automatic scans when documents are opened and when you launch an application, and virus-like activity alerts. These results are stored in the *Activity Log* file.
- Scan results from a scheduled scan.

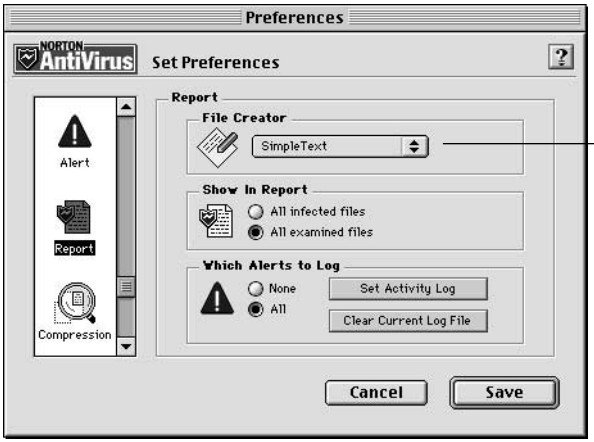
Customizing scan reports

You can specify whether to report on all files scanned or only those with problems. You can also specify which application you use to view the saved scan report files.

To customize reports:

1 Click the Report icon in the Preferences dialog box.

The Set Preferences dialog box appears with the Report options displayed.



2 Select an application from the File Creator list.

3 Select an option in the Show in Report group box.

The following options are available for Report preferences:

- **File Creator**

  Select an application from this list. This lets you view saved reports and the Activity Log in the application of your choice.

  Choose Other ( ) to select an application other than those listed. A dialog box appears that lets you locate the application.

- **Show In Report**

  Select an option in this group box to specify the scope of reported information when scans are performed:

  - **All Examined Files**

    Lists every scanned file and reports whether a problem was found or not.

  - **All Infected Files**

    Lists infected files only.

You can specify the name and location for the Activity Log and the types of alerts to record. You can also clear the Activity Log when it gets too big.

The following options are available for Activity Log preferences:

- **Which Alerts To Log**

  Select an option in the group box to specify the type of alerts to save to the Activity Log:

  - **None**

    Does not log any information in the Activity Log file.

  - **All**

    Logs virus warnings and virus-like activity alerts in the Activity Log file.

- **Set Activity Log File**

  Click to specify a location for the Activity Log file.

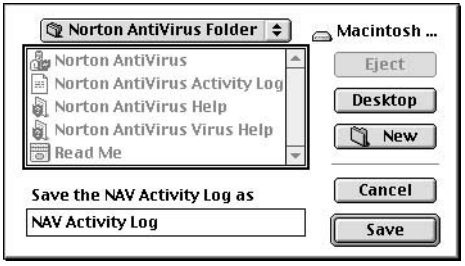
- **Clear Current Log File**

  Click to clear the contents of the Activity Log file.

To customize the Activity Log

1. Select an option in the Which Alerts to Log group box to specify the type of alerts to save to the Activity Log.
2. Click Save.

   The Finder directory dialog box appears.



3. Navigate to the location where you want to save the file.
4. Type a name for the report.
5. Click Save.

Note: To view the Activity Log, double-click the file.

Compression preferences

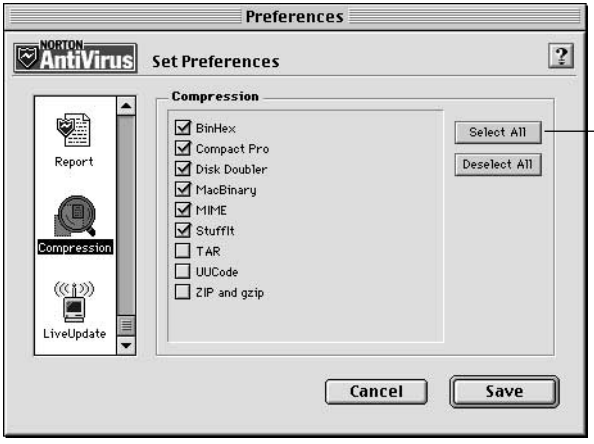
Norton AntiVirus can scan several different types of compressed files. Norton AntiVirus automatically scans all files compressed using StuffIt or DiskDoubler. In addition, Norton AntiVirus scans other types of compressed files using Alladin Systems' StuffIt technology. You can specify which other compressed file types Norton AntiVirus should scan.

Note: Auto-Protect does not scan compressed files.

To select which compressed file types to scan:

1 Click the Compression icon in the Preferences dialog box.

The Set Preferences dialog box appears with the Compression options displayed.



Norton AntiVirus supports the following compression file types:

- BinHex
- Compact Pro
- DiskDoubler
- MacBinary
- MIME
- StuffIt
- TAR (UNIX Tape ARchive file)
- UUCode
- ZIP and gzip

2 Select the file compression types for Norton AntiVirus to scan:

- **Select All**

  All file types are scanned.

- **Deselect All**

  No compressed files are scanned.

Note: Scanning time may increase if you have many compressed files.

---

3 Click Save.

LiveUpdate preferences

If you have a modem or an Internet connection, using LiveUpdates is the best way to update virus protection. For complete details on using Live Update, see "Updating virus protection with LiveUpdate" on page 37.

Before you first use LiveUpdate, you may need to select an Internet or direct-dial modem connection. If you have an existing Internet connection and you select Internet, you don't need to change any other LiveUpdate settings. If you select Modem, LiveUpdate uses your modem to direct-dial the Symantec LiveUpdate server. You can change your modem type, speed, port, and redial frequency.

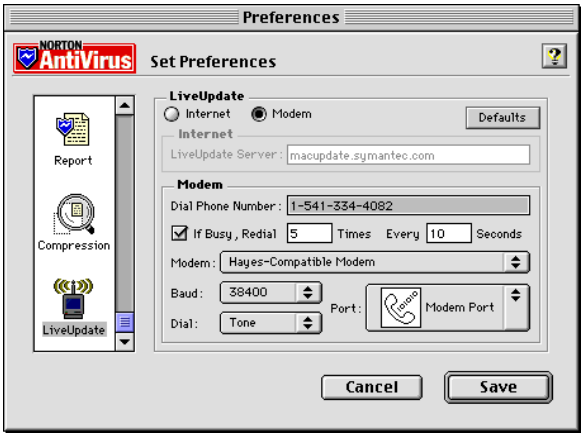
To configure LiveUpdate:

1 Start Norton AntiVirus.

2 In the Norton AntiVirus main window, click Preferences.

3 In the Preferences dialog box, select the LiveUpdate icon.

The LiveUpdate preferences appear.



4 Specify how you want to obtain updates:

- **Internet**

  Select this option if you have a functioning Internet connection. The LiveUpdate server URL becomes active.

- **Modem**

  Select this option if you do not have an Internet Service Provider (ISP) or other connection to the Internet. The modem settings become active. You can change the modem type, baud rate, modem port, and dial tone. For details, see "Customizing modem settings" on page 80.

5 Click Save.

Configuring LiveUpdate

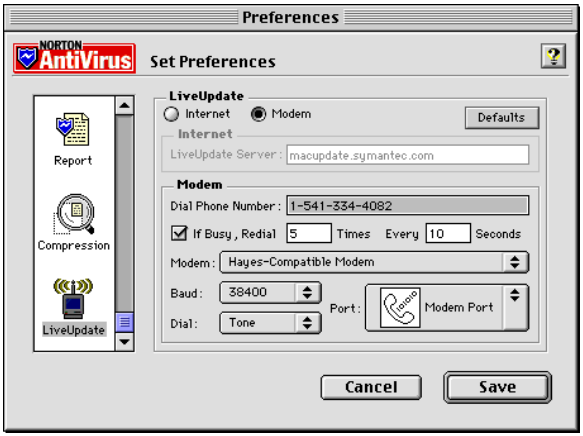
If you need to select modem settings to access the Norton AntiVirus LiveUpdate server, you can use Norton AntiVirus Preferences to change LiveUpdate settings.

To configure LiveUpdate:

1 In the Norton AntiVirus main window, click Preferences.

2 In the Preferences dialog box, select the LiveUpdate icon.

The LiveUpdate preferences appear.



3 Specify how you want to obtain updates by clicking Internet or Modem:

- If you select Internet, the LiveUpdate server URL is displayed.
- If you select Modem, you can select the modem name, baud rate, modem port, and dial tone preference that match your system.

The phone number is provided automatically during Norton AntiVirus installation. If the text box is blank or contains an incorrect phone number, click Defaults to restore the correct phone number.

4 Select your modem type from the Modem list.

If you do not know what kind of modem you have, the default selection works in most cases. However, you may be able to speed up the file transfer by selecting the proper modem type.

5 Click Save.

Customizing modem settings

Although it is usually not necessary, there may be times when you need to change the modem settings for the file transfer to work.

Tip: If you already have Internet access that you know is working properly, you don't need to customize modem settings.

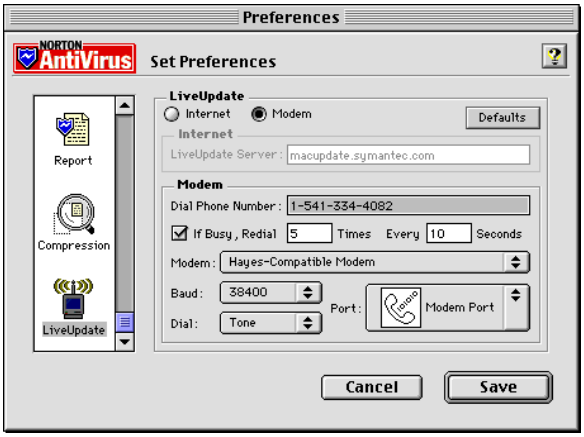
To customize modem options:

1 Click Preferences.

The Preferences dialog box appears.

2 Select the LiveUpdate icon in the icon list.

The LiveUpdate preferences appear.



3 Click Modem.

4 Select If Busy, then specify in the Redial *N* Times and Every *N* Seconds text boxes how often Norton AntiVirus should redial if the phone line is busy.

The default settings are appropriate in most cases.

5 Select your modem type in the Modem list.

If your modem is not in the list, select the generic option that most closely matches your modem:

- Hayes-compatible
- Generic V.32
- Generic MNP

Hayes-compatible works in most situations.

Tip: You can speed up the file transfer by selecting the proper modem type.

---

6 Select the baud rate from the Baud list.

The fastest baud rate for your modem is selected automatically. You don't need to lower the baud rate unless the phone-line quality is impaired.

7 Select the dial type from the Dial list:

- Tone is used for a touch-tone phone.
- Pulse is used for a rotary dial phone.
- Mixed dial type is used, for example, to dial out by pulse and then send a calling card number by tone.

8 Select the port to which your modem is connected.

If you are not sure which port icon to select, look at the back of your Macintosh. The port to which your modem is connected has an icon next to it that matches one of the icons in this dialog box.

Password-protecting Norton AntiVirus menus

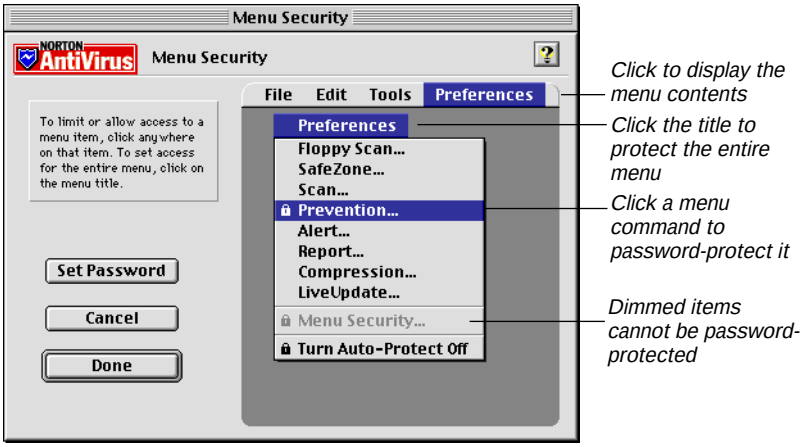
You can restrict access to most settings by setting a password. Use the Menu Security command to define what features you want password-protected, and to set or change the password.

Note: Once you enter a password to access a password-protected feature, you can access all password-protected features without entering the password again.

To password-protect Norton AntiVirus features:

1 Choose MENU SECURITY from the Preferences menu.

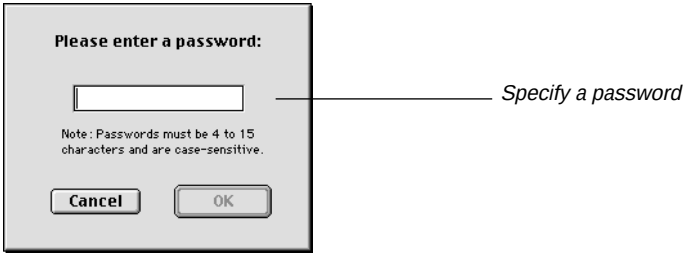
The Menu Security dialog box appears.



2 To password-protect a specific menu command, click the menu command.

3 Click Set Password.

The set password dialog box appears.



4 Type a password between 4 and 15 characters long (passwords are case-sensitive—for example, “a” is not the same as “A”), then click OK.

A dialog box appears prompting you to re-type your password to validate it.

Tip: Write down your password and store it in a safe place.

---

5 Type the password again, then click OK.

6 Click Done.

The protected features have a padlock icon next to them.

Changing your password

Once you've established a password, you can easily change it.

To change your password:

1. Choose MENU SECURITY from the Preferences menu, then type your password when prompted.

   The Menu Security dialog box appears.
2. Click Set Password.

   The set password dialog box appears.
3. Type the new password, then click OK.

   A dialog box appears prompting you to re-enter your password.
4. Type the new password again, then click OK.
5. Click Done.

Removing password protection

If you decide you no longer want password-protection for some or all of the features you previously protected, you can easily remove the protection.

To remove password protection:

1. Choose MENU SECURITY from the Preferences menu, then type your password when prompted.

   The Menu Security dialog box appears.
2. Click the items that have a padlock icon next to them.

   To unlock an entire menu, click the menu title.

   The padlock icon disappears.
3. Click Done.

Protecting against unknown viruses

An *unknown virus* is one for which Norton AntiVirus does not yet have a definition. You can protect files against unknown viruses by:

- Turning the Protect against unknown viruses feature on in Scan Preferences.

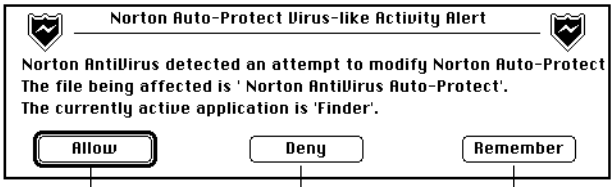
When Norton AntiVirus protects an application file, it records critical information about it (similar to taking a “fingerprint”). On subsequent scans, Norton AntiVirus checks the file against the “fingerprint” and notifies you if there are any changes that could indicate the presence of an unknown virus.

For information on enabling this feature, see “Scan preferences” on page 67.

- Monitoring for virus-like activities.

About virus-like activities

A *virus-like activity* is an activity that viruses sometimes perform when damaging your files or spreading through your system. Although some applications perform these actions for valid reasons, Norton AntiVirus can monitor for the activities on the chance that an unknown virus is performing one of them. The following is an example of a virus-like activity alert.



Allows the action to continue

Prevents the action from taking place

Allows the action to continue and prevents this alert from appearing in the future

If a virus-like activity is detected, it does *not* necessarily mean that a virus is performing the activity—you decide whether the activity can continue or not. For example, if you are changing an application’s preferences and receive an alert, you can allow the action to continue because you know it is valid in the context of the application you are running. On the other hand, if you are entering numbers in a spreadsheet and receive the same alert, you should not let the activity continue because it is not valid in the context of using your spreadsheet application.

If you installed Norton AntiVirus using the preset options, the most common virus-like behaviors are monitored. To customize virus-like activity monitoring, see “Prevention preferences” on page 68.

Warning: If a virus-like activity alert appears on your screen right now, see "Responding to virus-like activity alerts" on page 55 for instructions on how to proceed.

Managing virus-like activities

You can edit the list of virus-like activities that you want Norton AntiVirus Auto-Protect to ignore. This list is called the *Exceptions List*. The Exceptions List contains conditions or activities that would normally be flagged as virus-like, which you have told Auto-Protect to remember.

An Exception is saved when you click the Remember button in a virus-like activity alert. See "Customizing scan reports" on page 74, for information on turning this feature on or off.

Note: If you rename an application, you must reestablish exceptions for the application by clicking the Remember button when Auto-Protect displays a virus-like activity alert.

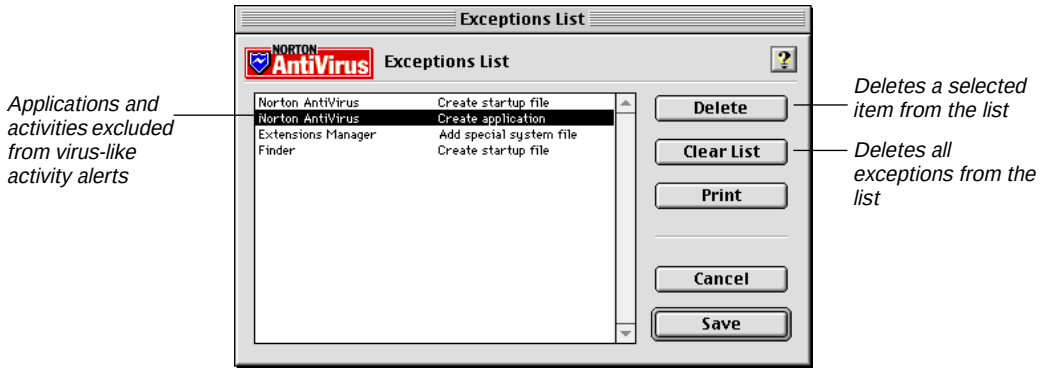
Removing entries from the Exceptions List

You can remove exceptions you no longer need or want. For example, if you remove an application from your hard disk for which you an exception, you can remove the exception saved for that application.

To remove entries from the list:

1 Choose Edit Exceptions List from the Tools menu.

The Exceptions List dialog box appears.



2 Select the exception to delete.

If you want to select more than one exception, Shift-Click or Command-Click the exceptions.

3 Click Delete.

4 Click Save to save your changes.

Clearing all entries from the Exceptions List

You can remove all entries from the Exceptions List, if you ever need to. Be aware, however, that Auto-Protect resumes alerting you of virus-like activities when they occur.

To clear all entries from the list:

1 Choose Edit Exceptions List from the Tools menu.

The Exceptions List dialog box appears.

2 Click Clear List.

3 Click Save.

APPENDIX A

Troubleshooting

This appendix suggests solutions to common problems that arise while you are using Norton AntiVirus for Macintosh.

These problems are not directly related to virus activity. If the problem you are trying to resolve is not discussed in this appendix, consult the Read Me file on the Norton AntiVirus CD. For scanning problems, also see "System messages" on page 95, and "Decontamination procedures" on page 58, for more information.

Installation of Norton AntiVirus fails

1. Restart your Macintosh from the CD:
   - On Apple Power Macintosh computers, restart while holding down the letter "c" key on your keyboard.
   - On third-party Macintosh computers, or on Macintosh computers with third-party CD-ROM drives, go to Control Panels, open Startup Disk, and select the Norton AntiVirus CD as your Startup Disk, then restart.

   When your Macintosh restarts, the CD window appears with the Norton AntiVirus pattern in the background.
2. Install Norton AntiVirus again.

NOTE: If you continue to have difficulty installing Norton AntiVirus, see "General Macintosh troubleshooting" on page 92.

Norton AntiVirus Auto-Protect fails to load when I start my Macintosh

- Norton AntiVirus Auto-Protect may have a conflict with one or more of your other system extensions.

  Check the Norton AntiVirus Read Me file for the most up-to-date information on compatibility with other system extensions. If the Norton Read Me file does not provide the answer, see "General Macintosh troubleshooting" on page 92.

- If you are using an extension manager program, the program may have turned Norton AntiVirus Auto-Protect off.

  Launch the extension manager program and make sure Norton AntiVirus Auto-Protect is turned on.

- Your copy of Norton AntiVirus Auto-Protect could be damaged in some way.

  Reinstall Norton AntiVirus Auto-Protect using the Custom install option. See "Installing selected components" on page 24.

- Make sure all engine files and virus definitions are installed. Norton AntiVirus will not run without them. For a list of all the installed files, see "Norton AntiVirus installed files" on page 93.

Norton AntiVirus cannot find the Norton AntiVirus Virus Defs file

- The Norton AntiVirus Virus Defs file must be located in the Norton AntiVirus Additions folder.

  Use the Find command on the Finder's File menu to locate the Norton AntiVirus Virus Defs file, then move the file into the Norton AntiVirus Additions folder.

Norton AntiVirus is password-protected and I forgot my password

- If you forget your password, you must remove Norton AntiVirus from the Norton AntiVirus Folder and Norton AntiVirus Preferences from the Preferences folder. Then reinstall Norton AntiVirus to gain access to password-protected features.

How do I prevent Norton AntiVirus from loading first?

- Use an extension manager program to change the load order. Items in the Extensions folder load earlier than items in other locations in the System Folder.
- You can change the location of Norton AntiVirus Auto-Protect by moving it to the Control Panels folder or the System folder. Extensions load alphabetically, so changing the first character of the name will change the load order.
- Change the name of Norton AntiVirus Auto-Protect.

During an automatic floppy scan, Norton AntiVirus did not scan every file on my disk

- A file on the disk may be damaged, or Norton AntiVirus ran out of memory, or some other error occurred during scanning.

  Scan your disk again from the Norton AntiVirus main window. You may also want to examine the disk using a program such as Norton Disk Doctor (part of Norton Utilities for Macintosh).

  If you have large files, or a large number of files, you may need to raise the memory allocation for Norton AntiVirus. Close Norton AntiVirus, select its icon, and choose Get Info from the File menu. Increase the memory allocation in the Preferred Size field.

Updating virus definitions via LiveUpdate

- Make sure the modem is connected properly.
- Make sure you are using the correct modem cables.
- Make sure the modem is turned on.
- Verify that the modem settings are correct. See “Customizing modem settings” on page 80, for more information.
- For an Internet connection to LiveUpdate, make sure you can already connect to the Internet with other applications, such as your web browser.

See “System messages” on page 95, for information on specific error messages reported.

General Macintosh troubleshooting

If you experience a problem starting your Macintosh after installing Norton AntiVirus, there may be a conflict with other extensions on your computer. Follow the procedures below to troubleshoot the problem.

Extensions may conflict for one or more of the following reasons:

- There may be more than one copy of the System file.
- A file may be damaged.
- The files may need to be loaded in a different order.
- One of the files may need to be updated.

To identify multiple copies of system files:

1. Use Find to search for additional copies of the System file and the System folder.

   If there is more than one copy of the System file or the System folder, delete the additional copies.
2. Restart your Macintosh.

   If the restart is successful, the problem is resolved.

Other troubleshooting steps

Here are some other steps you can take to resolve problems with your Macintosh.

- Reinstall or upgrade the System software.

  See your Macintosh System documentation for more information.
- Use Norton Utilities for Macintosh to find and fix disk problems.
- Rebuild the Desktop file.

  See your Macintosh System documentation for more information.
- Reinstall Norton AntiVirus. See "Installing selected components" on page 24.
- Update the disk driver.

  See your Macintosh System documentation for more information.
- Reset the PRAM (Parameter RAM).

  See your Macintosh System documentation, or the Norton Utilities for Macintosh documentation, for more information.

Norton AntiVirus installed files

The following files are installed in Norton AntiVirus for Macintosh.

Norton AntiVirus folder

- Norton AntiVirus
- Norton AntiVirus Help
- Norton AntiVirus Virus Help
- Read Me

Control Panels folder

- Norton AntiVirus (alias)

Extensions folder

- CFM-68K Runtime Enabler (invisible character and 68K only)
- Norton AntiVirus Auto-Protect
- Apple Modem Tool
- Norton AntiVirus Additions
  - Norton AntiVirus Library
  - Norton AntiVirus Macro Scan Lib
  - Norton AntiVirus Virus Defs
  - Norton AntiVirus Activity Data
  - virscan1.dat
  - virscan6.dat
- ObjectSupportLib
- TCPack
- XModem Tool

Preferences folder

- Norton AntiVirus Preferences Folder
  - Norton AntiVirus Preferences
  - Virus Definitions Subscription

APPENDIX B

System messages

The following messages might be encountered when you are running Norton AntiVirus or Norton Auto-Protect.

Note: Angle brackets (<>) identify variables or filenames.

Norton AntiVirus messages

The entered subscription code is not valid. Please retype in the 9 character subscription code again.

You entered a virus definitions subscription code incorrectly. Try typing the number again.

The passwords did not match. Please try again.

The second password you typed does not match the first one.

That password is incorrect. Please try again.

You typed an incorrect password. If you forgot your password, see "Troubleshooting" on page 89.

There is not enough memory to view any more items. Collapse some of the expanded items and try again.
No more items can be viewed: <error string>. Collapse some of the expanded items and try again.

There is not enough available memory for Norton AntiVirus to display or store information for the number or the size of files on the disks to be scanned. Try collapsing folders, scanning a more limited area, or changing the memory allocated to Norton AntiVirus in the Finder. For more information, see "General Macintosh troubleshooting" on page 92.

Please enter a LiveUpdate server address before proceeding.

The URL (Internet address) for the LiveUpdate server in the LiveUpdate Preferences dialog box is incorrect. Click Defaults in the LiveUpdate Preferences dialog box to restore the correct address.

Please enter a phone number before proceeding.

There must be a phone number for the LiveUpdate modem to dial in to the LiveUpdate server. Click Defaults in the LiveUpdate Preferences dialog box to restore the correct phone number.

Please enter a number greater than zero for "Redial Times" before proceeding.

Enter the number of times you would like LiveUpdate to redial, or clear the Redial checkbox.

Please enter a number greater than zero for "Seconds" before proceeding.

Enter the time between redials for LiveUpdate to redial, or clear the Redial checkbox.

The startup disk is read-only. Preferences can be changed, but will not be saved when you quit.

If you restarted from the CD-ROM and changed Norton AntiVirus preferences, they will not be saved to the active System Folder on the CD. To change and save preferences to your System Folder, you must install Norton AntiVirus on your hard disk.

The items(s) you have selected to scan contain too many files to scan with report all examined items on. There is not enough memory to display all examined items. You can continue scanning with report all examined items turned off.

The setting in Report Preferences should be changed to Report. You could also try scanning a more limited area, or changing the memory allocated to Norton AntiVirus in the Finder. For more information, see "General Macintosh troubleshooting" on page 92.

The "Event Type" option has been changed to "Scan System disk" because only the System disk or folder can be scanned at startup.

The startup scan you scheduled can only scan the System Folder or the entire system disk.

The “How often” option has been changed to “weekly” because “always” can only be used with startup or shutdown scans.

When you change the type of scan from startup or shutdown to some other type, the frequency must also change if it was set to “always.” The “always” setting only applies to startup and shutdown scans.

The “When” option has been changed to “at specified time” because virus definition updates cannot be scheduled at startup or shutdown.

Virus definitions updates cannot occur at startup or shutdown. You must specify a different time for the update to occur.

The “Start Time” for the displayed event can’t be saved until a valid number is entered in the <“minute”>, <“hour”>, or <“day”>, <“month”>, or <“year”> field.

In the Scheduler, make sure you enter a valid date and time for the event you are scheduling.

The scheduled events could not be saved because an error occurred: <error string>

Check your Scheduler settings and try saving to a different location.

Norton AntiVirus cannot be used unless ObjectSupportLib is in the Extensions Folder. Re-installing either the Mac OS software or the Norton AntiVirus will place a copy of ObjectSupportLib in the Extensions Folder.

The Macintosh OS system file, ObjectSupportLib, is required for Norton AntiVirus to run. Either reinstall Norton AntiVirus or your Macintosh OS to install a copy of ObjectSupportLib in the Extensions folder.

Norton AntiVirus could not locate “Norton AntiVirus Library” in the “Norton AntiVirus Additions” folder. It is required to scan for viruses. You can continue, but you will not be able to scan for viruses.

The Norton AntiVirus Additions folder may not be in the default location. It must be in the Extensions folder in the active System folder. For more information on file locations, see “Norton AntiVirus installed files” on page 93.

Norton AntiVirus could not locate “virscan1.dat” in the “Norton AntiVirus Additions” folder. It is required to scan for viruses. You can continue, but you will not be able to scan for viruses.

The Norton AntiVirus Additions folder may not be in the default location. It must be in the Extensions folder in the active System Folder. For more information on file locations, see “Norton AntiVirus installed files” on page 93.

Norton AntiVirus could not locate “virscan6.dat” in the “Norton AntiVirus Additions” folder. It is required to scan for viruses. You can continue, but you will not be able to scan for viruses.

The Norton AntiVirus Additions folder may not be in the default location. It must be in the Extensions folder in the active System Folder. For more information on file locations, see “Norton AntiVirus installed files” on page 93.

Norton AntiVirus requires a Macintosh OS system with the Thread Manager installed. It is required to scan for viruses and to do LiveUpdates. You can continue, but you will not be able to scan for viruses or do LiveUpdates.

Norton AntiVirus requires System 7.5 or higher.

Norton AntiVirus could not locate the “Norton AntiVirus Virus Defs” in the “Norton AntiVirus Additions” folder. It is required to scan for viruses. You can try to find it or you can continue with virus scanning disabled.

The Norton AntiVirus Additions folder may not be in the default location. It must be in the Extensions folder in the active System Folder. For more information on file locations, see “Norton AntiVirus installed files” on page 93.

An error occurred loading the “Norton AntiVirus Library.” It is required to scan for viruses. You can continue, but you will not be able to scan for viruses.

The Norton AntiVirus Additions folder may not be in the default location. It must be in the Extensions folder in the active System Folder. For more information on file locations, see “Norton AntiVirus installed files” on page 93.

Norton AntiVirus could not locate the "Norton AntiVirus Macro Scan Lib" in the "Norton AntiVirus Additions" folder. It is required to scan for macro viruses. You can continue, but you will not be able to scan for macro viruses.

The Norton AntiVirus Additions folder may not be in the default location. It must be in the Extensions folder in the active System Folder. For more information on file locations, see "Norton AntiVirus installed files" on page 93.

A network error occurred that will prevent Norton AntiVirus from alerting the Norton AntiVirus NT or NLM Server when a virus is found. You can continue, but any viruses identified will not be reported to a network server.

If you want to alert others on the network, save the scan report and then send it separately.

There is no printer selected in the Chooser, or the selected printer could not be found.

You can't print the Activity Log or scan report because your printer could not be found. Reselect the printer in the Chooser and try again.

There is not enough memory to add any more items to the scan report. You can continue scanning but non-infected items will be removed from the scan report and will not be added as the scan continues.

Norton AntiVirus uses available memory to store items for the scan report. If you have many files, you will not be able to record all items to scan. You can change the Report Preferences to only record infected files.

Auto-Protect messages

Norton AntiVirus Auto-Protect is damaged. It may be infected with a virus!

Please scan all volumes with Norton AntiVirus on a CD-ROM or locked floppy, then re-install Auto-Protect.

The Norton AntiVirus Virus Defs file could not be loaded. Either the file is not in the Norton AntiVirus Additions folder, or it is invalid.

The Norton AntiVirus Additions folder may not be in the default location. It must be in the Extensions folder in the active System Folder. For more

information on file locations, see “Norton AntiVirus installed files” on page 93.

The Norton AntiVirus Activity Data file was not found in Norton AntiVirus Additions or it is damaged.

The Norton AntiVirus Additions folder may not be in the default location. It must be in the Extensions folder in the active System Folder. For more information on file locations, see “Norton AntiVirus installed files” on page 93.

The Macro Scan Library could not be found, but Auto-Protect will still perform its other functions.

Norton AntiVirus Auto-Protect is searching for a required file. For more information on file locations, see “Norton AntiVirus installed files” on page 93.

Norton AntiVirus Auto-Protect requires the shared library <xxxx>.

Norton AntiVirus Auto-Protect is searching for a required file. For more information on file locations, see “Norton AntiVirus installed files” on page 93.

Norton AntiVirus Auto-Protect was not loaded because <one of the following will be concatenated:>

- Norton Auto-Protect did not have enough memory.
- CFM-68K Runtime Enabler was not properly installed.
- Norton AntiVirus Intercept or Norton AntiVirus Auto-Protect is already loaded.
- System 7.5 or higher is required.

The Norton AntiVirus Library could not be found in Norton AntiVirus Additions or it is damaged.

Norton AntiVirus Auto-Protect is searching for a required file. For more information on file locations, see “Norton AntiVirus installed files” on page 93.

There was a problem with the Norton AntiVirus Preferences file.

Norton AntiVirus Auto-Protect is searching for the Preferences file, or the file may be damaged. Try deleting the file.

A68040 or PowerPC processor is required.

Norton AntiVirus must have a 68040 or PowerPC processor to run.

APPENDIX C

Using Norton AntiVirus on a network

You can run Norton AntiVirus on any AppleTalk Transaction Protocol server, such as AppleShare or TOPS. You can configure Norton AntiVirus to alert you or others on the network if a virus is found on a client machine running Norton AntiVirus NetWare Loadable Module (NAV NLM) or Norton AntiVirus for Windows NT (NAV NT). This appendix offers tips and suggestions for using Norton AntiVirus efficiently on a network.

Note: You can install Norton AntiVirus on workstations over an AppleTalk network using the Norton AntiVirus Administrator to distribute packages. This program is included with multi-user packs and site licenses of Norton AntiVirus software. If you are a network administrator, see the *Norton AntiVirus for Macintosh Administrator's Guide*, included with Norton AntiVirus Administrator.

Notes to the administrator

We recommend setting up Norton AntiVirus the following way in a networking environment:

- Run Norton AntiVirus Auto-Protect and the Norton AntiVirus main window on the system administrator's computer.
- At the very least, make sure Norton AntiVirus Auto-Protect is run on all workstation Macintosh computers.
- Use the Scheduler command from the Norton AntiVirus Tools menu to schedule periodic scans of all network drives.

Scanning network drives

When you are scanning network drives from a workstation, the server slows down for other users. If others are creating, deleting, or moving files on a network drive while Norton AntiVirus is scanning, all files may not get scanned.

To prevent this, you can do the following:

- Make sure you are the only one logged on to the server when scanning network drives.
- Shut down the server and restart it as a workstation. Then perform the scan.

Note: The Norton AntiVirus main window cannot run on an AppleShare volume at the same time as AppleShare (version 2.*x* or higher).

Using Norton AntiVirus Auto-Protect on a server

To protect against viruses, we strongly recommend using Norton AntiVirus Auto-Protect on your server or servers. Norton AntiVirus Auto-Protect monitors file activity and alerts you if a virus tries to infect any applications on the server.

If you are using the Prevention feature to monitor virus-like activities, you may experience delays because Norton AntiVirus Auto-Protect constantly monitors the Macintosh on which it is installed.

To prevent a network slowdown when Prevention features are active:

1. In the Norton AntiVirus main window, click Preferences.

   The Preferences dialog box appears.

2. Do the following:

   - In the Prevention preferences, select the Standard prevention level.

     The Standard option monitors applications for the most common virus behavior, such as adding code instructions to an application file. For more information, see “Prevention preferences” on page 68.

   - In the Alert preferences, select Remove alerts after, and type 0 in the seconds text box.

This causes Norton AntiVirus Auto-Protect to accept the default button in the alert box, and prevents virus-like activity alerts from halting access to files on the server. For more information see “Alert preferences” on page 72.

3 Select All in the Which Alerts To Log Report options.

This ensures that virus-like alerts are logged in the Activity Log file so you can view the alerts at a later time. For more information, see “Customizing scan reports” on page 74.

Preparing an emergency response plan

To be fully prepared in case of a virus attack on a workstation, be sure to have a detailed emergency response plan written and distributed within your networking group before a problem arises. This will maintain order and prevent panic in case of an infection.

The following sections include a partial listing of the items that should be included in your plan. You will, of course, want to complete your plan based on the dynamics and needs of your organization.

Before a virus is detected

Conduct an informational meeting with your network users to discuss the basic nature and behavior of computer viruses. Stress that while having a computer virus on your system is reason to take immediate action, there is no need to panic. Emphasize that many viruses spread from illegal or “bootlegged” software copies, and prohibit the use of such software in your organization. Finally, explain how you’ve configured Norton AntiVirus to respond to a virus.

Tip: You can add a customized message to all virus alerts and virus-like activity alerts to indicate who the user should call for help (for example, “Call Help Desk for help at ext. 5555”). For more information, see “Alert preferences” on page 72.

Instruct your users to:

- Scan all software before using it. This includes programs downloaded from bulletin board services as well as new software right out of the shrink-wrapped box.
- Watch for warning signs such as frequent system crashes, lost data, screen interference, or suddenly unreliable programs.
- Keep a current store of virus-free program backups.
- Avoid running programs from floppy disks they haven't scanned.
- Write-protect their floppy disks before using them in someone else's computer.

To protect the workstations:

- Scan each workstation to make sure it is virus-free.
- Train your users to use a file backup utility on a regular basis.
- Train your users to update the virus definitions file when it becomes available. If you are using Norton AntiVirus Administrator, the virus definitions files on workstations can be updated automatically.

To protect the network:

- Password-protect all network executable directories so that only you (the administrator) have write access to them.
- Scan for viruses on new and rental computers before using them.
- Schedule periodic scans of all network servers.
- If you are using a Novell NetWare server, use Norton AntiVirus for NetWare to protect the server from virus infections.

If a virus is detected

- Physically disconnect the workstation from the network. Then eradicate the virus on the workstation before reconnecting to the network.
- Notify other users on the network to scan for viruses immediately.
- Scan your network servers for viruses.
- You can set Norton AntiVirus preferences to alert you over a network running under Norton AntiVirus NetWare Loadable Module (NAV NLM) or Norton AntiVirus for Windows NT (NAV NT). For details, see "Alert preferences" on page 72.

G L O S S A R Y

alert	Dialog box that appears on your screen to notify you that a virus or virus-like activity has been detected. You must respond by clicking a button or pressing Return.
alias	Shortcut icon that points to an original object (file, folder, or disk). *See* your Macintosh system documentation for details.
AppleShare	Extension that lets you access shared files on other networked Macintosh computers or AppleShare file servers.
AppleTalk	Network communications environment developed by Apple Computer.
application	Computer program written for a specific purpose, such as word processing or creating a spreadsheet. Also called program or application program.
archive file	Single file or group of files that have been compressed into one file for storage purposes. *See also* “compressed file” on page 105.
ASCII	American Standard Code for Information Interchange. Standard that assigns a unique binary number (a byte) to each text character and control character.
baud rate	The speed at which a modem can transmit data. Baud rate measures the number of signal changes that occur in one second. *See also* “bps.”
boot (v.)	To start a computer.
bps	bits per second. Measure of speed in serial transmission. Also used to describe hardware capabilities (i.e., a 56000 bps modem). *See also* “baud rate.”
BBS	Bulletin board service. Online service that allows messaging, electronic mail, and file transfer between computer users via modem.
compressed file	File that has been compressed using a special data storage format to save space on your disk. *See also* “archive file” on page 105.

creator code	Four-character sequence associated with a file that specifies which application created the file.
data fork	Part of a Macintosh file that contains data. For example, text entered using a word processor is stored in the data fork of the document file. *See also* "resource fork" on page 108.
document file	File that is created by or associated with an application and contains no executable code. Examples include word processing documents, databases, and spreadsheets.
download	To transfer a file from one computer system to another, usually through a modem. Usually refers to the act of transferring a file from the Internet, a bulletin board service, or a service such as America Online.
encryption	Method of imposing data security on selected files, folders, or disks. Encryption disguises data. Often the encrypted item is protected with a password so that only those knowing the password can access (decrypt and use) the data.
Exceptions List	Group of normally virus-like conditions that you have told Norton AntiVirus not to look for in a particular file. Exceptions are saved when you click the Remember button in a virus-like activity alert.
executable file	File containing program code that can be launched. Generally includes any file that is an application, extension, or a system file.
extension	*See* "system extension" on page 108.
file server	Central disk storage device connected to a network that provides network users access to shared applications and data files.
file type	Four-character code, stored along with a creator code in each file, that identifies its type. Applications use this code to determine if a file is in a format that can be read by the application.
Hayes-compatible	Modem that responds to the same commands as a modem manufactured by Hayes Microcomputer Products, originators of the standard for microcomputer modems.

icon	Graphic symbol used to represent a file, folder, disk or other entity.
INIT	*See* “system extension” on page 108.
infected file	File that contains a virus.
known virus	Any virus that Norton AntiVirus can detect and identify by name.
LAN	Local Area Network. Group of computers connected for the purpose of sharing resources. The computers on a local area network are typically located within a small “local” area such as a single building or section of a building.
launch	To start or run an application.
locked disk	*See* “write-protected disk” on page 109.
locked file	File that can be viewed, but cannot be written to or deleted. Also referred to as read-only.
mount	To make a Macintosh disk available for use on the desktop. When a disk is mounted, its icon appears on the desktop and you can access its files.
network	Set of computers and associated hardware (printers and so forth) connected together in a work group for the purpose of sharing information and hardware among users.
Norton AntiVirus Auto-Protect	Automatic protection feature that loads into memory at startup to guard your computer against viruses.
operating system	Program that ties the capabilities of computer hardware and software to input/output devices such as disks, keyboards, and mice.
partition	Portion of a disk (prepared and set aside by a special disk utility) that functions as a separate disk. When partitions are mounted to the desktop, a separate icon appears for each partition.
program	*See* “application” on page 105.
read-only	Disk, folder, or file containing data that can be read, but cannot be written to or deleted. Also referred to as “locked” or “write-protected.”

removable media	Disks that can be removed, as opposed to hard disks that are stationary. Some examples of removable media are floppy disks, disk cartridges (SyQuest and Bernoulli, for example), compact discs, and zip drives.
repair	To remove a virus from a file and return the file to its original, uninfected state.
resource fork	Part of a file that contains information used by an application, such as menus, fonts, icons, and the executable code. Most viruses attach themselves to the resource fork of application files.
scan	Systematic search for viruses by Norton AntiVirus.
startup	Process by which your computer starts working. During this process, system extensions such as Norton Auto-Protect are loaded into memory.
startup disk	Disk (hard disk or floppy disk) with all the necessary program files—such as the Finder and System files contained in the System folder—to set a Macintosh into operation. Sometimes called a boot disk or system disk.
system extension	Program that loads into memory when a Macintosh is started. Also known as a startup document. In System 6, a system extension is called an INIT file.
System file	File stored in the System folder that the Macintosh uses to start up.
System folder	Folder on the startup disk that contains the files your Macintosh requires to run, such as the System file, Finder, system extensions, desk accessories, and control panels.
Trojan horse	Program that promises to be something useful or interesting (like a game), but may covertly damage or erase files on your computer while you are running it. Trojan horses are not actually viruses because they do not replicate or spread to other files.
unknown virus	Virus for which NAV does not contain a virus definition. *See also* “virus definitions file” on page 109.

virus	Self-replicating program written intentionally to alter the way your computer operates without your permission or knowledge. A virus attaches copies of itself to other files, and when activated, may damage files, cause erratic system behavior, or merely display annoying messages.
virus definitions file	File that comes with the NAV software package and provides information for finding and repairing viruses. Also called built-in definitions. You can download a new virus definitions file from Symantec BBS, CompuServe, Applelink, and America Online bulletin board services.
virus-like activity	Activity or action caused by other software that NAV perceives as the work of a possible unknown virus. Virus-like activity alerts do not necessarily indicate the presence of a virus, but should be investigated.
worm	Program that replicates without infecting other programs. Some worms spread by copying themselves from disk to disk, while others replicate only in memory to slow down a computer. So far, worms do not exist in the Macintosh world.
write-protected disk	Disk that cannot be written to or erased. Write-protecting disks prevents viruses from infecting them. To write-protect a 3.5-inch disk, slide the tab on the back of the disk to uncover the hole through the disk. Also referred to as a “locked disk” or “read-only disk.”

Symantec Service and Support Solutions

Symantec is committed to excellent service worldwide. Our goal is to provide you with professional assistance in the use of our software and services, wherever you are located.

Technical Support and Customer Service solutions vary by country. If you have questions about the services described below, please refer to the section “Worldwide Service and Support” at the end of this chapter.

Registering your Symantec product

To register your Symantec product, please complete the registration card included with your package and drop the card in the mail. You can also register via modem during the installation process (if your software offers this feature) or via fax to (800) 800-1438 or (541) 984-8020.

Virus definitions update disk

If you don’t have a modem to obtain virus definitions files using the Internet, Compuserve, America Online, or the Symantec BBS, you can order regular updates from Symantec to arrive by mail. This service requires a fee.

To order, do one of the following:

- In the United States, call (800) 441-7234.
- Outside the United States, contact your local Symantec office or representative.

Technical support

Symantec offers an array of technical support options designed for your individual needs to help you get the most out of your software investment.

World Wide Web

The Symantec World Wide Web site (http://service.symantec.com) is the doorway to a set of online technical support solutions where you will find the following services:

Interactive problem solver

Symantec’s online interactive problem solver (known as the Support Genie) helps you solve problems and answer questions about many Symantec products.

Product knowledgebases

Product knowledgebases enable you to search thousands of documents used by Symantec Support Technicians to answer customer questions.

FAQs

Frequently Asked Questions documents, also known as FAQs, list commonly asked questions and clear answers for specific products.

Discussion groups

Discussion groups provide a forum where you can ask questions and receive answers from Symantec online support technicians.

FTP

Point your Web browser to http://service.symantec.com to search for and download technical notes and software updates. You can also click the LiveUpdate button in programs enabled with this feature to automatically download and install software updates and virus definitions.

Other Symantec support options include the following:

America Online	Type Keyword: SYMANTEC to access the Symantec forum.
CompuServe	Type GO SYMANTEC to access the Symantec forum.
Symantec BBS	Set your modem to 8 data bits, 1 stop bit, no parity and dial (541) 484-6669.
Automated fax retrieval system	To receive general product information, fact sheets and product upgrade order forms directly to your fax machine, please call our Customer Service fax retrieval system at (800) 554-4403 or (541) 984-2490. For technical application notes, please call our Technical Support fax retrieval system at (541) 984-2490 and select option 2.
StandardCare Support	If you can't access the Internet, take advantage of your 90 days of free telephone technical support (from the date of your first call) at no charge to all registered users of Symantec software. Please see the back of this manual for the support telephone number for your product.

PriorityCare and PlatinumCare Support

Expanded telephone support services available to all registered customers. For complete information, please call our automated fax retrieval service, located in the United States, at (800) 554-4403 or (541) 984-2490, and request document 070, or visit www.symantec.com/techsupp/telesupp.html

Support for old and discontinued versions

When a new version of this software is released, registered users will receive upgrade information in the mail. Telephone support will be provided for the previous version for 6 months after the release of the new version. Technical information may still be available through online support.

When Symantec announces that a product will no longer be marketed or sold, telephone support will be discontinued 60 days later. Support will only be available for discontinued products through online services. See the section “Technical support” for online service options.

Customer Service

Symantec's Customer Service department can assist you with non-technical questions. Call Customer Service to:

- Order an upgrade.
- Subscribe to the Symantec Support Solution of your choice.
- Fulfill your request for product literature or demonstration disks.
- Find out about dealers and consultants in your area.
- Replace missing or defective CDs, disks, manuals, etc.
- Update your product registration with address or name changes.

You can also visit Customer Service online at www.symantec.com/custserv for the latest Customer Service FAQs, to find out the status of your order or return, or to post a query to a Customer Service discussion group.

Worldwide Service and Support

Symantec provides Technical Support and Customer Service worldwide. Services vary by country and include International Partners who represent Symantec in regions without a Symantec office. For general information, please contact the Symantec Service and Support Office for your region.

Service and Support offices

NORTH AMERICA

Symantec Corporation 175 W. Broadway Eugene, OR, 97401	(800) 441-7234 (USA & Canada) (541) 334-6054 (all other locations) Fax: (541) 984-8020
Automated Fax Retrieval	(800) 554-4403 (541) 984-2490

BRAZIL

Symantec Brazil Av. Juruce, 302 - cj 11 São Paulo - SP 04080 011 Brazil	+55 (11) 5561 0284 Fax: +55 (11) 5530 8869

EUROPE

Symantec Europe Ltd. Kanaalpark 145 2321 JV Leiden The Netherlands	+31 (71) 535 3111 Fax: +31 (71) 535 3150
Automated Fax Retrieval	+31 (71) 535 3255

ASIA/PACIFIC RIM

Symantec Australia Pty. Ltd. 408 Victoria Road Gladesville, NSW 2111 Australia	+61 (2) 9850 1000 Fax: +61 (2) 9850 1001
Automated Fax Retrieval	+61 (2) 9817 4550

Most International Partners provide Customer Service and Technical Support for Symantec products in your local language. For more information on other Symantec and International Partner locations, please call our Technical Support automated fax retrieval service, in the United States at +1 (541) 984-2490, choose Option 2, and request document 1400.

Every effort has been made to ensure the accuracy of this information. However, the information contained herein is subject to change without notice. Symantec Corporation reserves the right for such change without prior notice.

8/97

Norton AntiVirus for Macintosh®

Disk Exchange and/or Replacement Form

DISK EXCHANGE: Norton AntiVirus for Macintosh is available on 3.5" high-density disks. If you purchased a product that does not contain the correct disk size for your computer, you may exchange the disk. Fill out Section A and return 1) this form, 2) a shipping and handling payment of $4.95, to the address below.

CD REPLACEMENT: After your 60-Day Limited Warranty, if your disk or CD-ROM becomes unusable, fill out Sections A & B and return 1) this form, 2) your payment (see pricing below, add sales tax if applicable), to the address below to receive replacement disks. *DURING THE 60-DAY LIMITED WARRANTY PERIOD, THIS SERVICE IS FREE.* You must be a registered customer in order to receive disk replacements.

SECTION A - FOR DISK EXCHANGE *AND* REPLACEMENT

Please send me: ___ 3.5" high-density disk (exchange/replacement) ___ CD-ROM (replacement)

Name_____

Company Name _____

Street Address (No P.O. Boxes, Please)_____

City _____State _____ Zip/Postal Code _____

Country* _____Daytime Phone _____

Software Purchase Date_____

*This offer limited to U.S., Canada, and Mexico. Outside North America, contact your local Symantec office or distributer.

SECTION B - FOR CD REPLACEMENT *ONLY*

Briefly describe the problem:_____

_____

Disk Replacement Price	$ 10.00
Sales Tax (See Table)	_____
Shipping & Handling	$ 4.95
TOTAL DUE	_____

SALES TAX TABLE: AZ (5%), **CA** (7.25%), **CO** (3%), **CT** (6%), **DC** (5.75%), **FL** (6%), **GA** (4%), **IA** (5%), **IL** (6.25%), **IN** (5%), **KS** (4.9%), **LA** (4%), **MA** (5%), **MD** (5%), **ME** (6%), **MI** (6%), **MN** (6.5%), **MO** (4.225%), **NC** (6%), **NJ** (6%), **NY** (4%), **OH** (5%), **OK** (4.5%), **PA** (6%), **SC** (5%), **TN** (6%), **TX** (6.25%), **VA** (4.5%), **WA** (6.5%), **WI** (5%). Please add local sales tax (as well as state sales tax) in AZ, CA, FL, GA, MO, NY, OH, OK, SC, TN, TX, WA, WI.

FORM OF PAYMENT ** (Check One):

___ Check (Payable to Symantec) Amount Enclosed $_____ __Visa __Mastercard __ American Express

Credit Card Number _____ Expires _____

Name on Card (please print) _____Signature _____

****U.S. Dollars. Payment must be made in U.S. dollars drawn on a U.S. bank.**

MAIL YOUR DISK EXCHANGE AND/OR DISK REPLACEMENT ORDER TO:

Symantec Corporation
Attention: Order Processing
175 West Broadway
Eugene, OR 97401-3003

Please allow 2-3 weeks for delivery within the U.S.

SYMANTEC.™

06-70-00289

I N D E X

H

I

K

L

M

N

P

R

S

T

U

V

W