Norton AntiVirus™ Professional Edition User's Guide

Norton AntiVirus™ 2002 Professional Edition

Norton AntiVirus™ Professional Edition User's Guide

Documentation version 8.07

Copyright Notice

Trademarks

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

SYMANTEC SOFTWARE LICENSE AGREEMENT

IMPORTANT: PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE", "NO" BUTTON, OR OTHERWISE INDICATE REFUSAL, MAKE NO FURTHER USE OF THE SOFTWARE, AND RETURN THE FULL PRODUCT WITH PROOF OF PURCHASE TO THE DEALER FROM WHOM IT WAS ACQUIRED WITHIN SIXTY (60) DAYS OF PURCHASE, AND YOUR MONEY WILL BE REFUNDED.

1. License:

The software which accompanies this license (collectively 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. This license governs any releases, revisions, or enhancements to the Software that Symantec may furnish to you. Except as may be modified by a Symantec license certificate, license coupon, or license key (each a "License Module") which accompanies, precedes, or follows this license, your rights and obligations with respect to the use of this Software are as follows:

You may:

A. use one copy of the Software on a single computer. If a License Module accompanies, precedes, or follows this license, you may make that number of copies of the Software licensed to you by Symantec as provided in your License Module. Your License Module shall constitute proof of your right to make such copies.

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

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

D. 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 license.

You may not:

A. copy the printed documentation which accompanies the Software;

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

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

D. use a later version of the Software than is provided herewith unless you have purchased upgrade insurance or have otherwise separately acquired the right to use such later version;

E. use, if you received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which you have not received a permission in a License Module; or

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

2. Content Updates:

Certain Symantec software products utilize content that is updated from time to time (antivirus products utilize updated virus definitions; content filtering products utilize updated URL lists; firewall products utilize updated firewall rules; vulnerability assessment products utilize updated vulnerability data, etc.; collectively, these are referred to as "Content Updates"). You may obtain Content Updates for any period for which you have purchased a subscription for Content Updates for the Software (including any subscription included with your original purchase of the Software), purchased upgrade insurance for the Software, entered into a maintenance agreement that includes Content Updates, or otherwise separately acquired the right to obtain Content Updates. This license does not otherwise permit you to obtain and use Content Updates.

3. 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 (60) day period following the delivery to you of the Software.

4. 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 OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

5. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR

INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

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

IN NO CASE SHALL SYMANTEC'S OR ITS LICENSORS' LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether you accept the Software.

6. U.S. Government Restricted Rights:

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

7. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment or similar communications between the parties. This Agreement may only be modified by a License Module or by a written document which has been signed by both You and Symantec. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Should you have any questions concerning this Agreement, or if you desire to contact Symantec for any reason, please write: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, USA, or (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland.

C O N T E N T S

Chapter 3 Norton AntiVirus Professional Edition basics

Section 2 Antivirus tools

Chapter 4 Protecting your computer from viruses

Chapter 5 Protecting your handheld device from threats

Section 3 Advanced tools

Chapter 6 Recovering missing or erased files

Chapter 7 Eliminating data permanently

Section 4 What to do if a virus is found

Chapter 8 What to do if a virus is found on your computer

Chapter 9 What to do if a threat is found on your handheld device

Section 5 Appendix

Appendix A Troubleshooting

Service and support solutions

Glossary

Index

CD Replacement Form

1

Getting started

CHAPTER 1

About Norton AntiVirus Professional Edition

Welcome to Norton AntiVirus Professional Edition, essential computer and *handheld device* (such as Palm Pilot, Visor, or a cell phone using Palm OS) protection for small businesses and professionals. This powerful combination of Norton and Symantec antivirus products safeguards your computer and Palm OS device from viruses, helps you recover lost or deleted files, and lets you completely erase confidential files.

Norton AntiVirus provides comprehensive virus prevention, detection, and elimination software for your computer. It finds and repairs infected files to keep your data safe and secure. Easy updating of the virus definition service over the Internet keeps Norton AntiVirus prepared for the latest threats.

Symantec AntiVirus for Palm OS protects you when harmful code tries to infiltrate your Palm OS device. You are safe from infection whether you are running applications, or exchanging files via *IR* (infrared) or desktop synchronization.

Advanced tools in Norton AntiVirus Professional Edition help you securely recover lost, deleted, or overwritten files and permanently remove unwanted files that result from a virus or threat to your computer or Palm OS device.

What's new in Norton AntiVirus Professional Edition

Norton AntiVirus Professional Edition introduces access to Norton AntiVirus tools through Windows Explorer, increased automation of virus repair with improved nonobtrusive feedback, totally integrated install, uninstall, and subscription services for Norton AntiVirus and Symantec AntiVirus for Palm OS, Norton AntiVirus advanced tools, and Windows XP support.

- Norton AntiVirus tools in Windows Explorer: For users with Internet Explorer 5.0 or later and for Windows NT users with the Windows Desktop Update, Norton AntiVirus Professional Edition adds a button to the Windows Explorer toolbar that allows you to view protection status, manage the Quarantine area of your computer, view the Activity Log, view the virus encyclopedia, and scan for viruses.
- Expanded email protection and options: You can scan both incoming and outgoing email messages. You can choose options to automatically quarantine or delete an infected email message, with or without your intervention.
- Automated virus repair: Norton AntiVirus can scan and repair your files entirely in the background, requiring no intervention from you. You receive a report containing the results of the scan.
- Integrated install: Norton AntiVirus, Symantec AntiVirus for Palm OS, and Norton AntiVirus advanced tools install together as one single application. You can choose whether to install Symantec AntiVirus for Palm OS initially or at a later time.
- Integrated uninstall: Norton AntiVirus, Symantec AntiVirus for Palm OS, and Norton AntiVirus advanced tools uninstall as one single application.
- Integrated subscription alerting and renewal: Subscription alerts and renewals for all products merge into one single subscription.
- Windows XP compatibility: Norton AntiVirus provides complete antivirus protection for your Windows XP operating system.

How viruses work

A software *virus* is a parasitic program written intentionally to alter the way your computer or handheld device 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 display messages.

Viruses infect system files and documents created by programs with macro capabilities. Some viruses are programmed specifically to corrupt programs, delete files, or erase your disk.

Macro viruses spread quickly

Macros are simple programs that are used to do things such as automate repetitive tasks in a document or make calculations in a spreadsheet. Macros are written in files created by such programs as Microsoft Word and Microsoft Excel.

Macro viruses are malicious macro programs that are designed to replicate themselves from file to file and can often destroy or change data. Macro viruses can be transferred across platforms and spread whenever you open an *infected file*. An infected file has been contaminated with a virus.

Trojan horses hide their true purposes

Trojan horses are programs that appear to serve some useful purpose or provide entertainment, which encourages you to run them. But the programs also serve a covert purpose, which may be to damage files or place a virus on your computer or handheld device.

A Trojan horse is not a virus because it does not replicate and spread like a virus. Because Trojan horses are not viruses, files that contain them cannot be repaired. To ensure the safety of your computer and handheld device, Norton AntiVirus detects Trojan horses so you can delete them immediately.

Worms take up space

Worms are programs that replicate without infecting other programs. Some worms spread by copying themselves from disk to disk. They search for specific types of files on a hard disk or server volume, and try to damage or destroy those files. Other worms replicate only in memory, creating myriad copies of themselves, all running simultaneously, which slows down the computer or handheld device. Like Trojan horses, worms are not viruses and therefore cannot be repaired. They must be deleted from your handheld or computer completely.

How viruses spread

A virus is inactive until you launch an infected program on your computer or handheld device, 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 program you run, including programs on a handheld device or network (if you can make changes to network folders or disks).

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

Like computers, other handheld devices that share data with each other or *download* (transfer) files via the *Internet* (global network of computers) are susceptible to malicious attacks. As the use of these mobile devices increases for conducting personal and corporate business, so does the potential risk for security threats.

While you are connected to the Internet, or *synchronizing* (comparing and updating information for the purpose of ensuring that the information matches) a handheld device to a desktop computer, attackers can download your data, including your private phone numbers, passwords, and other personal information, if they know the name of the Palm OS device and the IP (Internet Protocol) number of the computer where Palm Desktop is running.

To prevent virus-infected programs from getting onto your computer or Palm OS device, scan files with Norton AntiVirus or Symantec AntiVirus for Palm OS before you copy, run, or exchange them. This includes programs you download from *newsgroups* (online discussion forums) or Internet *Web sites* (group of Web pages managed by a single company, organization, or individual) and any email attachments that you receive.

How Norton AntiVirus Professional Edition works

Norton AntiVirus Professional Edition monitors your computer and handheld devices for 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 Professional Edition protects your computer and handheld devices from both types of viruses, using virus definitions to detect known viruses, and Bloodhound technology and Script Blocking to detect unknown viruses. Symantec AntiVirus for Palm OS uses a micro-engine specifically optimized for Palm OS software to detect known and potential threats to handheld devices. Virus definitions, Bloodhound technology, and Script Blocking are all used during scheduled scans and manual scans, and are used by Auto-Protect to constantly monitor your computer. Auto-Protect for your Palm OS device provides constant background protection against threats to Palm OS devices.

The virus definition service stops known viruses

The *virus definition* service consists of files that Norton AntiVirus Professional Edition uses to recognize viruses and intercept their activity. New definitions are transferred to your Palm OS device every time you synchronize it with your computer.

You can look up virus names in Norton AntiVirus and Symantec AntiVirus for Palm OS, and access an encyclopedia of virus descriptions on the Symantec Web site. For more information, see "Norton AntiVirus Professional Edition on the Web" on page 59.

Bloodhound technology stops unknown viruses

Bloodhound is the Norton AntiVirus scanning technology for detecting new and unknown viruses. It detects viruses by analyzing an executable file's structure, behavior, and other attributes such as programming logic, computer instructions, and any data contained in the file. It also sets up simulated environments in which to load documents and test for macro viruses.

Script Blocking stops script-based viruses

A *script* is a list of instructions that can be executed without user interaction. Scripts can be opened with text editors or word processing programs, so they are very easy to change.

Script Blocking detects Visual Basic and Java script-based viruses without the need for specific virus definitions. It monitors the scripts for virus-like behavior and alerts you if it is found.

Micro-engine safeguards Palm OS data

Symantec AntiVirus for Palm OS uses a micro-engine specifically optimized for Palm OS to detect known and potential threats to Palm OS devices. The scanning engine examines all of the applications in the handheld device and checks for the presence of a virus. Upon detection, it prompts you to remove the virus. It safeguards critical data against potential attacks by Palm OS viruses, worms, or Trojan horses.

Auto-Protect keeps you safe

Norton AntiVirus Professional Edition Auto-Protect loads into memory when you start your computer or handheld device providing constant protection while you work.

Using Auto-Protect, Norton AntiVirus Professional Edition automatically:

- Eliminates viruses and Trojan horses, including macro viruses, and repairs damaged files
- Checks for viruses every time you use software programs on your computer, insert floppy disks or other removable media, or use document files that you receive or create
- Checks for viruses every time you start or synchronize your handheld device, or exchange files via infrared transmission
- Protects your computer and your Palm OS device from Internet-borne viruses

How to maintain protection

When Norton AntiVirus Professional Edition is installed and you have synchronized your Palm OS device, you have complete virus protection. However, new viruses are created constantly. Viruses can spread when you start your computer or handheld device from an infected file, or run an infected program.

There are several things you can do to avoid viruses and to recover quickly should a virus strike.

Avoid viruses

It is important that you practice regular file maintenance, keep Norton AntiVirus Professional Edition and Symantec AntiVirus for Palm OS up-to-date, and synchronize your Palm OS devices on a regular basis.

To avoid viruses:

- Write-protect removable media.
- Stay informed about viruses by logging on to the Symantec Security Response Web site (securityresponse.symantec.com) where there is extensive, frequently updated information on viruses and virus protection.
- Use LiveUpdate regularly to update your computer and Palm OS programs and virus definition service files. Remember to synchronize your handheld device after running LiveUpdate. For more information, see "Keep current with LiveUpdate" on page 47.
- Keep Norton AntiVirus Professional Edition Auto-Protect turned on at all times to prevent viruses from infecting your computer or handheld devices. For more information, see "Ensure that Auto-Protect is enabled" on page 63.
- If Norton AntiVirus Professional Edition Auto-Protect is not turned on, scan removable media before you use them. For more information, see "Scan disks, folders, and files" on page 64.
- Watch for *email* (electronic mail) from unknown senders. Do not open anonymous attachments.
- Schedule scans to occur automatically on your computer. For more information, see "Schedule automatic virus scans" on page 70.

- Set the preference to manually scan your handheld device following a synchronization. For more information, see "Set a preference to scan after a synchronization" on page 74.
- Manually scan your handheld device after *beaming* (transferring by IR transmission) data to or receiving data from another device.
- Don't synchronize via an Internet connection unless you know that the source is secure.
- Be extremely careful about the sources you use when you beam any kind of file, whether it contains names and addresses, email, games, programs, or any other type of data. Make sure the source uses antivirus and security software.

Prepare for emergencies

It is also important that you are prepared in case your computer or handheld device is infected by a virus.

To prepare for emergencies:

- Back up files regularly and keep more than just the most recent backup.
- If you are using Windows NT/2000/ XP and your computer cannot start from a CD, create a set of Emergency Disks, from which you can start your computer and scan for viruses. For more information, see "Create Emergency Disks" on page 22.
- If you are using Windows 98/Me, create a set of Rescue Disks, with which you can start your computer in DOS mode and use Norton AntiVirus to fix virus-related problems and recover from a system crash. For more information, see "About Rescue Disks" on page 45.
- Synchronize your handheld device regularly.
- Know the difference between a soft reset and a hard reset on your handheld device. Be extremely careful when performing a reset. A hard reset erases all data including your user name.
- Prevent unexpected beaming to your handheld device by turning off the Beam Receive option from the Preferences program.

CHAPTER 2

Installing Norton AntiVirus Professional Edition

Before installing Norton AntiVirus Professional Edition, take a moment to review the system requirements listed in this chapter. Windows 98/Me users should have some blank 1.44-MB disks available to make Rescue Disks.

System requirements

Note: Installation of Norton AntiVirus Professional Edition is not supported on Macintosh, Linux, or server versions of Windows NT 4.0/2000/XP computers.

Palm OS device

To use Symantec AntiVirus for Palm OS, your handheld device must meet the following minimum requirements:

- Palm OS version 3 or 4 (3.5 recommended)
- HotSync Manager version 3 or 4
- 2 MB of RAM
- 50 KB of available hard disk space

Windows computers

To use Norton AntiVirus Professional Edition, your computer must have one of the following Windows operating systems:

- Windows 98/98SE
- Windows Me
- Windows NT 4.0 Workstation with Service Pack 6.0 or later
- Windows 2000 Professional with Service Pack 1.0 or later
- Windows XP Professional/Home Edition

Note: If you are planning to upgrade your Windows operating system from Windows 98/Me to Windows 2000/XP, you must uninstall Norton AntiVirus Professional Edition first and then reinstall after the upgrade is complete.

Your computer must also meet the following minimum requirements.

If you are installing on Windows NT/2000/XP, you must install with administrator privileges.

Windows 98/Me

- Intel Pentium processor at 150 MHz or higher for Windows Me
- Intel Pentium processor at 133 MHz or higher for Windows 98
- 32 MB of RAM
- 50 MB of available hard disk space
- Internet Explorer 4.01 Service Pack 1 or later
- CD-ROM or DVD-ROM drive

Windows NT 4.0 Workstation

- Service Pack 6 or later
- Intel Pentium processor at 133 MHz or higher
- 32 MB of RAM
- 50 MB of available hard disk space
- Internet Explorer 4.01 Service Pack 1 or later
- CD-ROM or DVD-ROM drive

Windows 2000 Professional

- Intel Pentium processor at 133 MHz or higher
- 64 MB of RAM
- 50 MB of hard disk space
- Internet Explorer 4.01 Service Pack 1 or later
- CD-ROM or DVD-ROM drive

Windows XP Home Edition/Professional

- Intel Pentium processor at 233 MHz or higher
- 64 MB of RAM
- 50 MB of hard disk space
- Internet Explorer 4.01 Service Pack 1 or later
- CD-ROM or DVD-ROM drive

Note: For Windows XP, you must use Palm Desktop 4.01. To be sure that you have the most recent version of HotSync Manager, contact the vendor of your handheld device for available updates.

Email clients

Email scanning is supported for any POP3 compatible email client including:

- Microsoft Outlook Express version 4 or 5
- Microsoft Outlook 97/98/2000/XP
- Netscape Messenger version 4, Netscape Mail version 6
- Eudora Light version 3, Eudora Pro version 4, Eudora version 5

Before installation

Before you install Norton AntiVirus Professional Edition, prepare your computer and handheld device. If your computer cannot start from a CD, create Emergency Disks.

If you suspect that you have a virus

If your computer has a virus, Norton AntiVirus Professional Edition immediately shuts down your computer. Restart from the Norton AntiVirus Professional Edition CD and scan your computer's hard disk for viruses. The Norton AntiVirus emergency program uses the virus definitions from the Norton AntiVirus Professional Edition CD, and is not as up-to-date as virus definitions downloaded using LiveUpdate. For more information, see "If you are using the CD as an Emergency Disk" on page 99.

Once the virus has been repaired, delete the Norton AntiVirus Professional Edition install files in the temporary folder that are left behind after the forced shutdown.

Prepare your computer

If you have any other antivirus programs on your computer, you must uninstall them before installing Norton AntiVirus Professional Edition. For more information, see "If you need to uninstall Norton AntiVirus Professional Edition" on page 31.

To uninstall any other antivirus program, see the user documentation that came with the program.

You must close all other Windows programs before installing Norton AntiVirus Professional Edition.

Prepare your handheld device

If you have any other antivirus programs on your handheld, you must uninstall them before installing Norton AntiVirus Professional Edition with Symantec AntiVirus for Palm OS.

To uninstall any other antivirus program, see the user documentation that came with the program.

Create Emergency Disks

Emergency Disks are used to start your computer and scan for viruses in case of a problem. If your computer can start from a CD, you can use the Norton AntiVirus Professional Edition CD in place of Emergency Disks and do not need to create them. If you cannot start your computer, you can use

these instructions to create Emergency Disks on another computer. For more information, see "If you need to use Emergency Disks" on page 98.

Use the Norton AntiVirus Professional Edition CD to create Emergency Disks. You will need several formatted 1.44-MB disks.

To create Emergency Disks

1. Insert the Norton AntiVirus Professional Edition CD into the CD-ROM drive.
2. Click **Browse CD**.
3. Double-click the **Support** folder.
4. Double-click the **Edisk** folder.
5. Double-click **Ned.exe**.
6. In the welcome window, click **OK**.
7. Label the first disk as instructed and insert it into drive A.
8. Click **Yes**.
9. Repeat steps 7 and 8 for the subsequent disks.
10. When the procedure is complete, click **OK**.
11. Remove the final disk from drive A and store the Emergency Disk set in a safe place.

Install Norton AntiVirus Professional Edition

Installing Norton AntiVirus Professional Edition is a two phase process:

- Install Norton AntiVirus Professional Edition files to the desktop computer on which HotSync Manager or other synchronization software is installed. This provides the base from which the files can be transferred to your Palm OS device.
- Synchronize your Palm OS device to your computer in the usual way. For more information, see "Synchronize to your Palm OS device" on page 27.

Install the Windows component

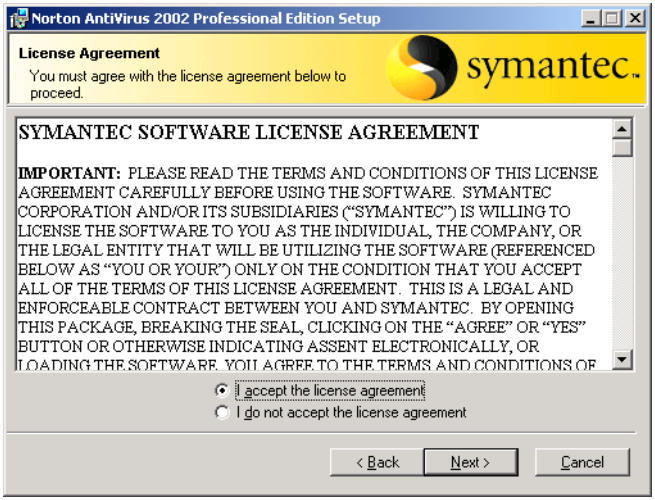
Install Norton AntiVirus Professional Edition from the Norton AntiVirus Professional Edition CD.

To install Norton AntiVirus Professional Edition

1. Insert the Norton AntiVirus Professional Edition CD into the CD-ROM drive.
2. In the Norton AntiVirus Professional Edition window, click **Install Norton AntiVirus Professional Edition**.

   If your computer is not set to automatically open a CD, you will have to open it yourself. For more information, see "If the opening screen does not appear" on page 27.
3. If you are installing in Windows 98/98SE/Me, Norton AntiVirus scans your computer's memory for viruses before installing. If a virus is found, you are prompted to use your Emergency Disks to remove the virus before continuing. For more information, see "Test your Rescue Disks" on page 46.

   The opening installation window reminds you to close all other Windows programs.
4. Click **Next**.



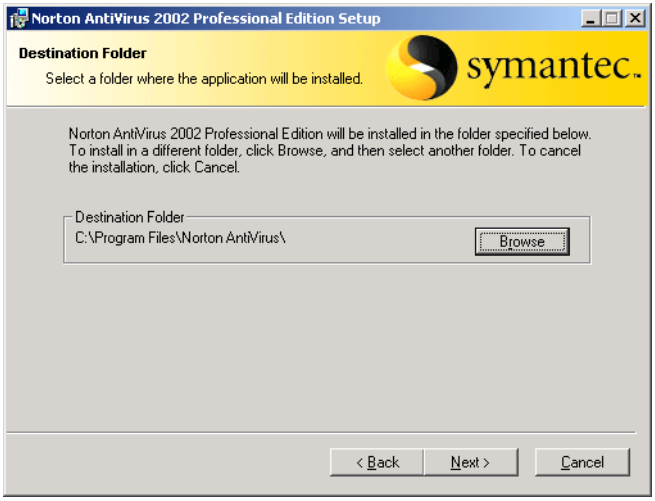
5. In the License Agreement window, click **I accept the license agreement**.

   If you decline, you cannot continue with the installation.

6 Click **Next**.

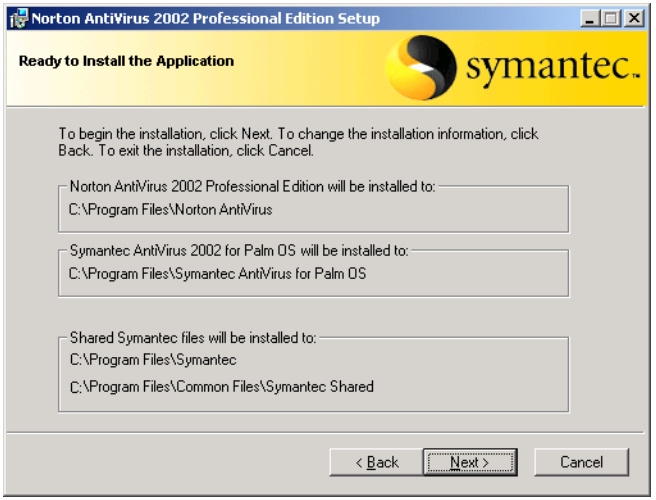
7 Check **Install Symantec AntiVirus for Palm OS**.

8 Click **Next**.

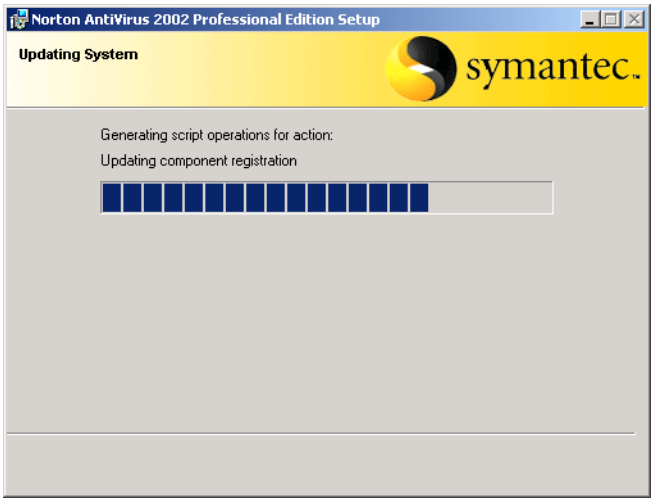


9 Click **Browse** to select a folder into which you want to install Norton AntiVirus Professional Edition.

10 Click **Next**.

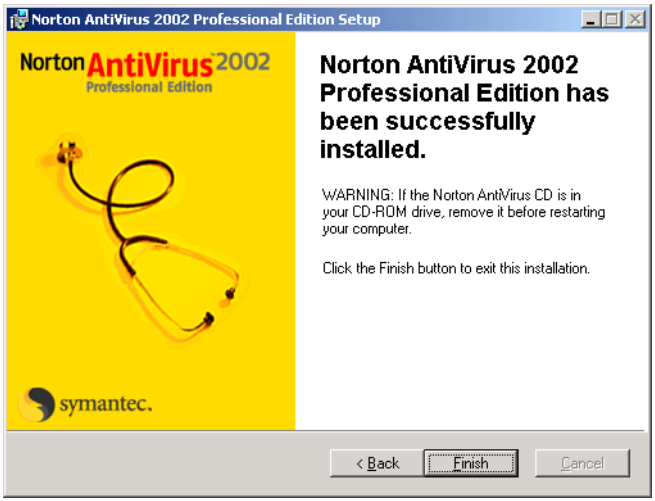


11 Confirm the installation location, then click **Next**.



12 After Norton AntiVirus is installed, scroll through the Readme text, then click **Next**.

For more information see "Read the Readme file" on page 31.



13 Click **Finish** to exit the installation.

If the opening screen does not appear

Sometimes, a computer's CD-ROM drive does not automatically start a CD.

To start the installation from the Norton AntiVirus Professional Edition CD

1 On your desktop, double-click **My Computer**.

2 In the My Computer dialog box, double-click the icon for your CD-ROM drive.

3 From the list of files, double-click **CDSTART.EXE**.

Synchronize to your Palm OS device

Once you have installed Norton AntiVirus Professional Edition on your Windows computer, you must synchronize. During synchronization, Symantec AntiVirus for Palm OS installs on your Palm OS device.

After synchronizing, the AntiVirus *icon* or graphical symbol appears on the Applications and Utilities screens, with the label AntiVirus.

Note: You cannot beam Symantec AntiVirus for Palm OS between Palm OS devices via IR transmission. You must use your device's synchronization software.

To install Symantec AntiVirus for Palm OS to your Palm OS device

1. Install Symantec AntiVirus for Palm OS on your Windows computer, as described in "Install Norton AntiVirus Professional Edition" on page 23.
2. Synchronize your Palm OS device to your Windows computer as described in your device's owner's manual.
3. Perform a soft reset on your Palm OS device after you synchronize.

After installation

If your computer needs to be restarted after Norton AntiVirus Professional Edition is installed, a prompt appears giving you the option to do so immediately. After restart or, if your computer does not need to be restarted, after installation is complete, the Information Wizard appears.

For Windows 98/Me/NT 4.0, you must restart your computer after installing Norton AntiVirus Professional Edition.

Restart your computer

After installation, you may receive a prompt telling you that your computer needs to be restarted in order for the updates to take effect.

To restart your computer

- In the dialog box, click **Yes**.

  If you click No, configuration of Norton AntiVirus Professional Edition is not complete until you restart your computer.

Use the Information Wizard

The Information Wizard lets you register your copy of Norton AntiVirus Professional Edition, get information about the virus definition subscription service, select post-install tasks to be done automatically, and review your Norton AntiVirus Professional Edition settings.

Note: If you choose not to register the software using the Information Wizard or if registration fails for some reason, you can register on the Symantec Web site at www.symantec.com or by using the Product Registration option on the Help menu. On the Web site, go to the Products page for the registration link.

To use the Information Wizard

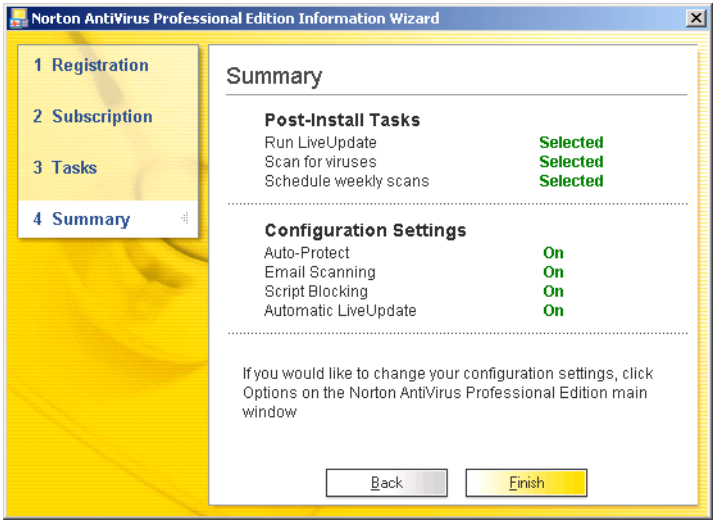
1. In the welcome window, click **Next**.
2. In the first Registration window, select the country from which you are registering and the country in which you live (if different), then click **Next**.
3. If you would like information from Symantec about Norton AntiVirus Professional Edition, select the method by which you want to receive that information, then click **Next**.
4. Enter your name and whether you want Norton AntiVirus Professional Edition registered to you or your company, then click **Next**.
5. Enter your address, then click **Next**.
6. Answer the survey questions to help Symantec improve its products and services, then click **Next** when you are done or to skip the survey.
7. Select whether you want to register Norton AntiVirus Professional Edition through the Internet or by mail, then click **Next**.

   If you submitted your registration through the Internet, a dialog box displays the serial number for your product.
8. Write down the number or click **Print** to get a copy of your registration information for future reference.
9. Click **Next**.
10. Select whether you want to use your existing profile the next time you register a Symantec product, or type the information as part of registration.
11. Click **Finish**.
12. Review the subscription service information, then click **Next**.

13 Select the post-install tasks that you want Norton AntiVirus Professional Edition to perform automatically. Your options are:

- Run LiveUpdate to ensure that you have the latest virus definitions. For more information, see "Keep current with LiveUpdate" on page 47.
- Perform a full system scan. For more information, see "Scan disks, folders, and files" on page 64.
- Schedule a weekly scan of your local hard drives. You must have Microsoft Scheduler installed to use this option. If you select this option, you can change the schedule for this scan as desired. For more information, see "Customize Norton AntiVirus Professional Edition" on page 51.
- If you are installing in Windows 98/Me, you also have the option to create a Rescue Disk set. For more information, see "About Rescue Disks" on page 45.

14 Click **Next**.



15 Review the configuration settings for Norton AntiVirus Professional Edition. If you want to change any of the settings, do so using Norton AntiVirus Professional Edition options. For more information, see "Customize Norton AntiVirus Professional Edition" on page 51.

16 Click **Finish**.

If you selected any post-install tasks, they start automatically.

Read the Readme file

The Readme file contains technical tips and information about product changes that occurred after this guide went to press. It is installed on your hard disk in the same location as the Norton AntiVirus Professional Edition product files.

To read the Readme file

1. Using Windows Explorer, navigate to the location where your Norton AntiVirus Professional Edition files are installed.

   If you installed Norton AntiVirus Professional Edition in the default location, the files are in C:\Program Files\Norton AntiVirus.
2. Double-click **Readme.txt** to open the file in Notepad or WordPad.

   The Readme file includes instructions for printing it if you want to do so.
3. Close the word processing program when you are done reading the file.

If you need to uninstall Norton AntiVirus Professional Edition

If you need to remove Norton AntiVirus Professional Edition from your computer, use the Add/Remove Programs option from the Windows Control Panel.

Note: During uninstall, Windows may indicate that it is installing software. This is a standard Microsoft installation message and can be disregarded.

To uninstall Norton AntiVirus Professional Edition

1. Do one of the following:
   - On the Windows taskbar, click **Start > Settings > Control Panel**.
   - On the Windows XP taskbar, click **Start > Control Panel**.
2. In the Control Panel, double-click **Add/Remove Programs**.

3 In the list of currently installed programs, click **Norton AntiVirus Professional Edition**.

4 Do one of the following:

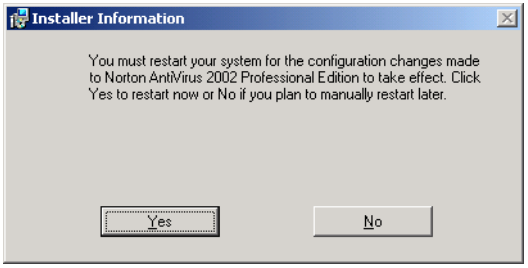
- In Windows 2000/Me, click **Change/Remove**.
- In Windows 98/NT, click **Add/Remove**.
- In Windows XP, click **Remove**.

5 Click **Yes** to confirm that you want to uninstall the product.

6 If you have files in Quarantine, you are asked if you want to delete them. Select one of the following:

- Yes: Deletes the quarantined files from your computer.
- No: Leaves the quarantined files on your computer, but makes them inaccessible. To repair or submit the files to Symantec for analysis, reinstall Norton AntiVirus Professional Edition.

7 Click **Finish**.



8 Click **Yes** to restart your computer.

If you have no other Symantec products on your computer, you should also uninstall LiveReg and LiveUpdate.

To uninstall LiveReg and LiveUpdate

1 Do one of the following:

- On the Windows taskbar, click **Start > Settings > Control Panel**.
- On the Windows XP taskbar, click **Start > Control Panel**.

2 In the Control Panel, double-click **Add/Remove Programs**.

3 In the list of currently installed programs, click **LiveReg**.

4 Do one of the following:
   - In Windows 2000/Me, click **Change/Remove**.
   - In Windows 98/NT, click **Add/Remove**.
   - In Windows XP, click **Remove**.
5 Click **Yes** to confirm that you want to uninstall the product.
6 Repeat steps 1 through 5, selecting LiveUpdate in step 3, to uninstall LiveUpdate.

Remove application from your Palm OS device

If you need to remove Symantec AntiVirus for Palm OS from your handheld device, use the Application menu on the Applications screen.

To remove Symantec AntiVirus for Palm OS from your Palm OS device

1 Tap **Applications**.
2 Tap **Menu**.
3 Tap **Delete**.
4 Tap **Symantec AntiVirus for Palm OS**.
5 Tap **Delete**.
6 Tap **Done** to close the delete screen.

CHAPTER 3

Norton AntiVirus Professional Edition basics

Norton AntiVirus Professional Edition basics include general information about how to work with Norton AntiVirus Professional Edition, keep your computer and Palm OS device protected, customize Norton AntiVirus Professional Edition, and access more information about Norton AntiVirus.

Work with Norton AntiVirus Professional Edition

You can perform a variety of tasks with Norton AntiVirus Professional Edition to protect your computer and your handheld device.

Access Norton AntiVirus Professional Edition tools on your computer

Norton AntiVirus Professional Edition tools include status reporting, scanning options, scheduling options, activity reporting, file recovery and removal, and configuration options for your computer and your handheld device. Access these tools from the Norton AntiVirus Professional Edition main window, the Windows Explorer toolbar, and the Norton AntiVirus Windows tray icon.

Use the Norton AntiVirus Professional Edition main window

A variety of tools are available from the Norton AntiVirus Professional Edition main window.

To start Norton AntiVirus Professional Edition on your computer

- Do one of the following:
  - On the Windows taskbar, click **Start > Programs > Norton AntiVirus > Norton AntiVirus 2002 Professional Edition**.
  - On the Windows XP taskbar, click **Start > More Programs > Norton AntiVirus > Norton AntiVirus 2002 Professional Edition**.

Use the Windows Explorer toolbar

Norton AntiVirus Professional Edition adds a button and menu to Windows Explorer. The button launches a scan of whatever you have selected in the Explorer pane. When you click the arrow to the right of the button, you have the following options on the Norton AntiVirus Professional Edition menu.

Option	Action
View Status	Launches Norton AntiVirus, displaying the Status pane with system status.
View Quarantine	Displays the Quarantine area and the files currently stored there. For more information, see "If you have files in Quarantine" on page 95.
View Activity Log	Displays the Activity Log, showing you various Norton AntiVirus activities, such as scans performed and problems found. For more information, see "Keep current with LiveUpdate" on page 47.
View Virus Encyclopedia	Connects you to the Symantec Security Response Web page, from which you can search for information on all types of viruses.
Scan for Viruses	Opens Norton AntiVirus in the Scan for Viruses pane, on which you can specify a scan to run.

When you first open Windows Explorer after installing Norton AntiVirus, you may not see the Norton AntiVirus button and menu.

To display the Norton AntiVirus button and menu

1 On the View menu, click **Toolbars**.

2 Click **Norton AntiVirus**.

Note: You may not be able to access the Norton AntiVirus Windows Explorer menu, depending on your computer's configuration. For more information, see "What's new in Norton AntiVirus Professional Edition" on page 12.

Use the Norton AntiVirus Windows tray icon

You can use the Norton AntiVirus Windows tray icon to start Norton AntiVirus Professional Edition.

To use the Norton AntiVirus Windows tray icon

- Right-click the Norton AntiVirus Windows tray icon.

Access Symantec AntiVirus for Palm OS on your handheld device

When Symantec AntiVirus for Palm OS is synchronized to your Palm OS device, the AntiVirus icon appears on the Applications and Utilities screens. You can place the icon wherever you want using your device's system software.

To start Symantec AntiVirus for Palm OS

- On your Palm OS device, tap the **AntiVirus** icon.

Check the version number

You can check the version number of Norton AntiVirus Professional Edition and Symantec AntiVirus for Palm OS on your computer and Symantec AntiVirus for Palm OS on your handheld device.

To check the version number on your computer

1. Start Norton AntiVirus Professional Edition on your computer.
2. Click **Help**.
3. Click **About Norton AntiVirus Professional**.
4. Do one of the following options:
   - Click **Norton AntiVirus**.
   - Click **AntiVirus for Palm OS**.

   The version number appears.
5. Click **OK** to return to the main window.

To check the version number on your handheld device

1. Start Symantec AntiVirus for Palm OS on your handheld.
2. Tap **Menu**.
3. Tap **Help**.
4. Tap **About Symantec AntiVirus**.

   The version number and copyright information appear.
5. Tap **OK** to return to the main window.

Temporarily disable Auto-Protect

If you have not changed the default option settings, Auto-Protect loads when you start your computer or your handheld device to guard against viruses. On your computer, it checks programs for viruses as they are run and monitors your computer for any activity that might indicate the presence of a virus. On your handheld device, it checks for threats when you synchronize to your computer or exchange data via infrared transmission. When a virus or *virus-like activity* (an event that could be the work of a virus) is detected, Auto-Protect alerts you.

In some cases, Auto-Protect may warn you about a virus-like activity that you know is not the work of a virus. If you will be performing such an activity and want to avoid the warning, you can temporarily disable Auto-Protect on either your computer or handheld or both.

To temporarily disable Auto-Protect on your computer

1. Start Norton AntiVirus Professional Edition. For more information, see "Access Norton AntiVirus Professional Edition tools on your computer" on page 35.
2. At the top of the Norton AntiVirus Professional Edition main window, click **Options**.
3. Click **Norton AntiVirus**.
4. In the Options dialog box, under System, click **Auto-Protect**.
5. In the Auto-Protect pane, uncheck **Enable Auto-Protect**.

Be sure to enable Auto-Protect when you have completed your task to ensure that your computer remains protected.

To enable Auto-Protect on your computer

1. Start Norton AntiVirus Professional Edition. For more information, see "Access Norton AntiVirus Professional Edition tools on your computer" on page 35.
2. At the top of the Norton AntiVirus Professional Edition main window, click **Options > Norton AntiVirus**.
3. In the Options dialog box, under System, click **Auto-Protect**.
4. In the Auto-Protect pane, check **Enable Auto-Protect**.

If the Norton AntiVirus icon appears in the Windows tray, you can use it to enable and disable Auto-Protect.

To enable or disable Auto-Protect on your computer using the tray icon

1. Right-click the Norton AntiVirus Windows tray icon.
2. Do one of the following:
   - If Auto-Protect is enabled, click **Disable Auto-Protect**.
   - If Auto-Protect is disabled, click **Enable Auto-Protect**.

You can enable or disable Auto-Protect for your handheld device.

To temporarily disable Auto-Protect on your handheld device

1. Start Symantec AntiVirus for Palm OS on your handheld. For more information, see "Access Symantec AntiVirus for Palm OS on your handheld device" on page 37.
2. Tap to clear the **Auto-Protect On** check box.

Be sure to enable Auto-Protect when you have completed your task to ensure that your handheld remains protected.

To enable Auto-Protect on your handheld device

1. Start Symantec AntiVirus for Palm OS on your handheld. For more information, see "Access Symantec AntiVirus for Palm OS on your handheld device" on page 37.
2. Tap the **Auto-Protect On** check box.

Check antivirus status

If Norton AntiVirus Professional Edition is behaving in an unexpected way, or if you're not sure that your computer or handheld device are being scanned for viruses, check the status of your configuration.

The status of your computer or handheld device appears in the Norton AntiVirus Professional Edition main window, as a green check mark if system status is OK, or a yellow triangle if your system needs attention. If your system needs attention, review the features and services to see which area needs attention.

If you need to make any changes to the settings for your computer, do so using Options. For more information, see "Customize Norton AntiVirus Professional Edition" on page 51.

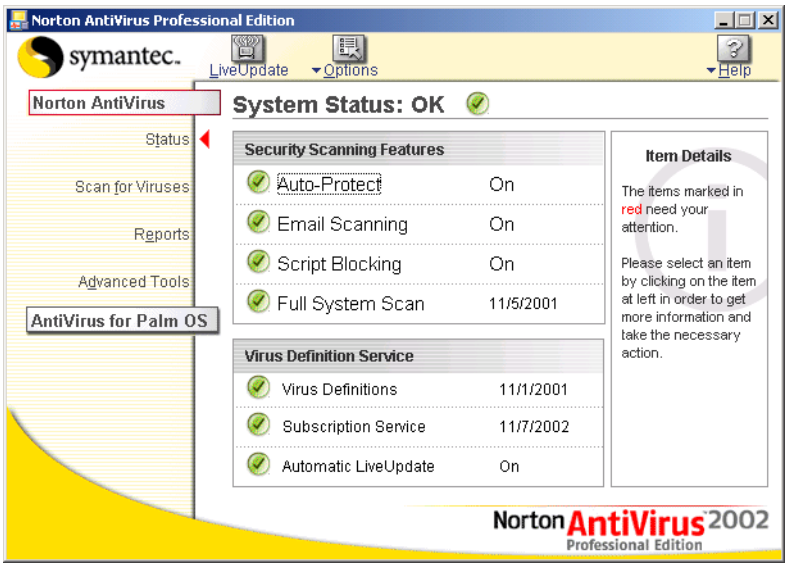
You can also view status and make adjustments on the Symantec AntiVirus for Palm OS main screen on your handheld device.

Check system status on your computer

You can check the status of most Norton AntiVirus and Symantec AntiVirus for Palm OS settings in the Norton AntiVirus Professional Edition main window.

To check system status on your computer

1 Start Norton AntiVirus Professional Edition on your computer. For more information, see "Access Norton AntiVirus Professional Edition tools on your computer" on page 35.



2 Do one of the following:

- Click **Norton AntiVirus**.
- Click **AntiVirus for Palm OS**.

3 Review the status displayed in the main window.

Check Office Plug-in status on your computer

Office Plug-in protects Microsoft Office documents. It scans those documents whenever you open them in an Office program. Office Plug-in is enabled in Options.

To check Office Plug-in status

1 Start Norton AntiVirus Professional Edition. For more information, see "Access Norton AntiVirus Professional Edition tools on your computer" on page 35.

2 Click **Options**.

3 Click **Norton AntiVirus**.

4 On the left side of the Options window, under Other, click **Miscellaneous**.

5 Verify that Office Plug-in is enabled.

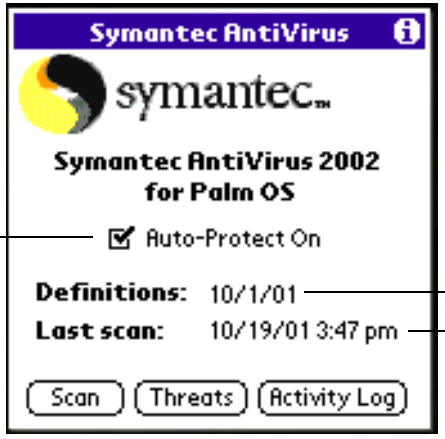
Check system status on your handheld device

The Symantec AntiVirus for Palm OS main window on your handheld shows you current status at a glance:

- Auto-Protect turned on or off
- Date of the latest virus definitions
- Date of the most recent scan

To check system status

- Start Symantec AntiVirus for Palm OS on your handheld.



Maintain Norton AntiVirus protection

New threats are discovered all the time, so it is important to update your virus definitions regularly. Norton AntiVirus Professional Edition uses LiveUpdate to provide you with the latest virus definitions to keep your device safe.

On your Windows computer, check your antivirus status, and run LiveUpdate to obtain new virus definitions and program updates from Symantec. Synchronize your handheld device after you run LiveUpdate, so it is protected from the latest known threats.

On your Palm OS device, periodically check your antivirus status and review scanning or Auto-Protect activities on the Activity Log.

Depending upon which operating system you are using, you may want to keep a set of Rescue Disks available and keep them up-to-date. For more information, see "About Rescue Disks" on page 45. You should also keep your virus protection current.

Check recent antivirus activity

Norton AntiVirus Professional Edition keeps a record of its scanning and virus detection events on your computer in the Activity Log. You can print and sort the events to get a more focused view of your activity.

The log is set by default to record all events. You can change this setting in Options. For more information, see "Customize Norton AntiVirus Professional Edition" on page 51.

Scanning and virus detection events for your handheld are recorded in the Activity Log on your handheld. It stores the date and time of each event. You can delete events one at a time or all of them at once.

Check activity on your computer

Check the Activity Log on your computer occasionally to see what tasks Norton AntiVirus Professional Edition has performed and the results of those tasks to make sure your Options settings are adequate.

Use the Reports option to view the Activity log.

To view and manage the Activity Log on your computer

1. Start Norton AntiVirus Professional Edition on your computer. For more information, see "Access Norton AntiVirus Professional Edition tools on your computer" on page 35.
2. In the Norton AntiVirus Professional Edition main window, click **Reports**.
3. In the Reports window, on the Activity Log line, click **View Report**.
4. Scroll through the Activity Log to see the recorded events.

   The most recent events appear at the end of the log.

5 To see only certain types of events, in the Activity Log window, click **Filter**.

6 When you are done, click **Close**.

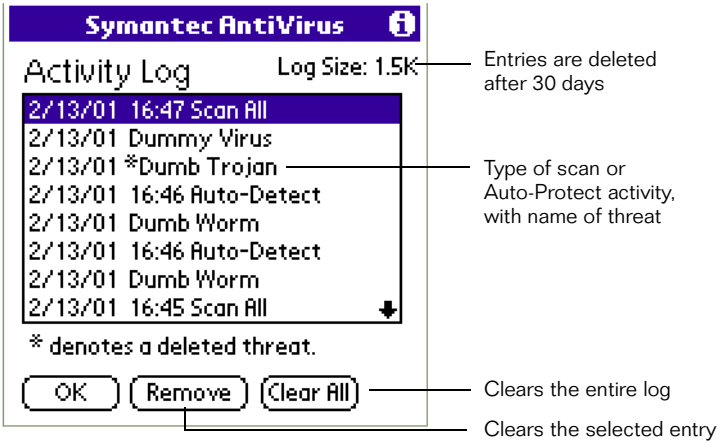
Check activity on your handheld device

The Activity Log on your handheld device shows the date and type of scans and other activities performed, the size of the *log* (record of events and activities), and the names of threats that were found. You can remove individual entries from the log, or clear the entire log. Symantec AntiVirus for Palm OS clears entries when they are over 30 days old.

To view and manage the Activity Log on your handheld device

1 Start Symantec AntiVirus for Palm OS on your handheld device.

2 Tap **Activity Log**.



3 On the Activity Log screen, do one of the following:

- To delete a specific entry, tap it, tap **Remove**, then tap **Yes** to confirm the deletion.
- To clear the Activity Log of all entries, tap **Clear All**.

4 When you are done, tap **OK**.

About Rescue Disks

Rescue Disks record a duplicate set of system startup files and disk partition information, and store rescue items and a virus scanner across multiple floppy disks or on a network drive. Rescue Disks can be made for Windows 98/Me operating systems; they are not needed for Windows NT/2000/XP.

A Rescue Disk set consists of one bootable floppy disk, one Norton AntiVirus Program floppy disk, and three Virus Definition floppy disks. If you have Norton Utilities installed, you will also have two Norton Utilities floppy disks in your Rescue Disk set. With a Rescue Disk set, you can start your computer in DOS mode and use Norton AntiVirus to fix virus-related problems.

Note: Rescue Disks contain information specific to the computer on which they were made. If you are using Rescue Disks for recovery, you must use the disks made for your computer. If you are using Rescue Disks to scan for viruses, you can use disks made for a different computer.

Rescue Disks can and should be updated whenever you update your virus protection, install new software, or make changes to your hardware.

Create a Rescue Disk set

Rescue Disks can be created at any time. If you have chosen to create Rescue Disks as a post-install task in the Information Wizard, the Rescue Disk Wizard appears automatically. Otherwise, you can start the Rescue Disk Wizard from the Norton AntiVirus Professional Edition main window.

If you start the Rescue Disk Wizard from the Norton AntiVirus Professional Edition main window, temporarily disable Auto-Protect while you are creating the Rescue Disk set. If you do not restart your computer after creating Rescue Disks, remember to enable Auto-Protect again. For more information, see "Temporarily disable Auto-Protect" on page 38.

You will need several formatted 1.44-MB disks.

To create Rescue Disks

1. Start Norton AntiVirus Professional Edition on your computer.
2. At the top of the Norton AntiVirus Professional Edition main window, click **Rescue**.

   If you chose to make Rescue Disks as a post-install task, the Rescue Disk Wizard opens automatically.
3. Select drive A to create the Rescue Disk set.
4. Click **Create**.
5. Label the disks as specified in the Basic Rescue Disk List window, then click **OK**.
6. Insert the disks as requested.

Test your Rescue Disks

At the end of the Create Rescue Disks process, you are prompted to test your disks. This requires that you restart your computer using the Rescue Disks.

To test your Rescue Disks

1. Close all open Windows programs.
2. Insert the disk labeled Basic Rescue Boot Floppy Disk into drive A, then click **Restart**.

   If the Rescue Disk screen appears on your monitor, the Rescue Disk works properly. If the Rescue Disk screen does not appear, you have several options for correcting the problem. For more information, see "My Rescue Disk does not work" on page 109.
3. Press **Escape** to exit to DOS.
4. Remove the disk from drive A, then slide open the plastic tab on the back of the disk to write-protect it.
5. Restart your computer.

Update your Rescue Disks

You can update your Rescue Disks as often as you like. Rescue Disk lets you update your basic Rescue Disks without having to recreate them.

If you are updating a floppy disk set, make sure your disks are not write-protected before you begin.

To update your Rescue Disks

1. Start Norton AntiVirus Professional Edition on your computer.
2. At the top of the Norton AntiVirus Professional Edition main window, click **Rescue**.
3. Under Select Destination Drive, select drive A.
4. Click **Update**.
5. Insert the disk labeled Basic Rescue Boot Floppy Disk into drive A.
6. Click **OK**.
7. Insert the remaining disks in your set as requested.

Make sure to test your newly updated Rescue Disk set when prompted. For more information, see "Test your Rescue Disks" on page 46.

Keep current with LiveUpdate

Symantec products depend on current information to protect your computer from newly discovered threats. Symantec makes this information available to you through LiveUpdate. Using your Internet connection, LiveUpdate downloads program updates and protection updates to your computer.

Your normal Internet access fees apply when you use LiveUpdate.

Note: If you are using Norton AntiVirus Professional Edition on Windows NT/2000/XP, you must have Administrator access rights to run LiveUpdate.

About program updates

Program updates are minor improvements to your installed product. These differ from product upgrades, which are newer versions of entire products. Program updates that have self-installers to replace existing software code are also called patches. Patches are usually created to extend operating system or hardware compatibility, adjust a performance issue, or fix bugs.

LiveUpdate automates the process of downloading and installing program updates. It saves you the trouble of locating and downloading files from an Internet site, then installing them, and deleting the leftover files from your disk.

About protection updates

One of the most common reasons for computer virus infections is that you have not updated your protection files regularly. Symantec provides online access to protection updates by subscription.

The virus definition service provides access to the latest virus signatures and other technology from Symantec. Norton AntiVirus, Norton SystemWorks, Norton Internet Security, and Symantec AntiVirus for Palm OS use the updates available from the virus definition service to detect the newest virus threats.

About your subscription

Your Symantec product includes a complimentary, limited time subscription to protection updates for the subscription services used by your product. When that subscription is due to expire, you are prompted to renew your subscription about one month prior to expiration. For more information, see "Subscription policy" on page 120.

If you do not renew your subscription, you can still use LiveUpdate to retrieve program updates. However, you cannot retrieve protection updates and will not be protected against newly discovered threats.

Obtain program and protection updates

Use LiveUpdate regularly to obtain updates. For example, to keep your virus protection current, you should use LiveUpdate once a week or whenever new viruses are discovered. Program updates are released on an as-needed basis.

Note: If you connect to the Internet through America Online (AOL), CompuServe, or Prodigy, connect to the Internet first, then run LiveUpdate.

To obtain updates using LiveUpdate

1. Open your Symantec product.
2. At the top of the window, click **LiveUpdate**.

   You might receive a warning that your subscription has expired. Follow the on-screen instructions to complete the subscription renewal.
3. Click **Next** to locate updates.

4 If updates are available, click **Next** to download and install them.

5 When the installation is complete, click **Finish**.

Run LiveUpdate automatically

You can choose to have LiveUpdate check for program and protection updates automatically, on a set schedule, by enabling automatic LiveUpdate. Once it's enabled, you can let it run according to the default schedule, or you can set when you want it to run using the Microsoft Scheduler.

Note: Automatic LiveUpdate periodically checks for an Internet connection: every five minutes until a connection is found, then every four hours. For users with ISDN routers set to automatically connect to your Internet Service Provider (ISP), this setting results in many connections being made, with connection and phone charges possibly being incurred for each connection. If this is a problem, you can set your ISDN router to not automatically connect to the ISP or disable Automatic LiveUpdate in the Norton AntiVirus options.

To enable automatic LiveUpdate

1 Start Norton AntiVirus Professional Edition.

2 At the top of the Norton AntiVirus Professional Edition main window, click **Options > Norton AntiVirus**.

3 In the Options dialog box, under Internet, click **LiveUpdate**.

4 In the LiveUpdate pane, check **Enable automatic LiveUpdate**.

5 Set how you want updates to be applied by selecting one of the following:

- Apply updates without interrupting me: LiveUpdate checks for and installs protection updates without prompting you. LiveUpdate notifies you when a protection update has been downloaded. You should still run LiveUpdate occasionally to check for program updates.
- Notify me when updates are available: LiveUpdate checks for protection updates and asks if you want to install them.

6 Click **OK**.

Automatic LiveUpdate is set by default to check for updates every four hours. To change that schedule, use the Microsoft Scheduler.

Note: Automatic LiveUpdate requires Internet Explorer version 4.0 or later with Microsoft Scheduler. For Windows NT 4.0, you must use Internet Explorer 5.0 with a full installation. The Scheduler tasks are located in C:\WINNT\TASKS or in My Computer.

To change the automatic LiveUpdate schedule

1. On the Windows taskbar, click **Start > Programs > Accessories > System Tools > Scheduled Tasks**.
2. In the Scheduled Tasks window, double-click **Symantec NetDetect**.
3. In the scheduler dialog box, on the Schedule tab, change the default schedule as desired.

   Do not change any entries on the Task and Settings tabs.
4. Click **OK**.

You can set multiple schedules for automatic LiveUpdate.

To set multiple schedules for LiveUpdate

1. On the Windows taskbar, click **Start > Programs > Accessories > System Tools > Scheduled Tasks**.
2. In the Scheduled Tasks window, double-click **Symantec NetDetect**.
3. In the scheduler dialog box, on the Schedule tab, at the bottom of the Schedule pane, click **Show multiple schedules**.
4. At the top of the Schedule pane, click **New**.
5. Set another schedule as desired.
6. Click **OK**.

To delete the schedule for automatic LiveUpdate, disable automatic LiveUpdate.

To disable automatic LiveUpdate

1. Start Norton AntiVirus.
2. At the top of the Norton AntiVirus main window, click **Options**.
3. In the Options dialog box, under Internet, click **LiveUpdate**.
4. In the LiveUpdate pane, uncheck **Enable automatic LiveUpdate**.
5. Click **OK**.

Customize Norton AntiVirus Professional Edition

The default settings for Norton AntiVirus Professional Edition provide complete virus protection for your computer and handheld device. However, you may want to adjust them to optimize system performance or disable options that do not apply.

This section does not discuss the individual options you can change, but gives a general description of what they do and how you can find them. For specific information about an option, check the online Help.

Note: If you are using Norton AntiVirus Professional Edition on Windows NT, Windows 2000, or Windows XP and you do not have Local Administrator access, you cannot change Norton AntiVirus Professional Edition options. If you are an Administrator and share your computer with others, keep in mind that the changes you make apply to everyone using the computer.

About Norton AntiVirus Professional Edition Options

All the settings in Options are organized into four main categories. The options contained under each category are as follows.

Category for Norton AntiVirus	Options
Norton AntiVirus	
System	Auto-Protect Script Blocking Manual Scan Exclusions
Internet	Email LiveUpdate
Other	Activity Log Inoculation Miscellaneous Advanced tools
AntiVirus for Palm OS	
Automatic LiveUpdate	Enable LiveUpdate

System options

The System options are those options that control scanning and monitoring of your computer. You use System options to determine what gets scanned, what the scan is looking for, and what happens when a virus or virus-like activity is encountered.

With higher levels of protection, there can be a slight tradeoff in computer performance. If you notice a difference in your computer's performance after you install Norton AntiVirus Professional Edition, you may want to set protection to a lower level or disable those options that you do not need.

Auto-Protect options

Auto-Protect options determine if Auto-Protect starts when you start your computer, what it looks for while monitoring your computer, and what it does if it finds something.

Auto-Protect also has two subcategories of options, Bloodhound and Advanced:

- Bloodhound is the scanning technology that protects against unknown viruses. Use these options to enable Bloodhound technology in Auto-Protect and set its level of sensitivity in detecting viruses. For more information, see "Bloodhound technology stops unknown viruses" on page 15.
- Advanced options determine the activities to be monitored when scanning for virus-like activities and when scanning floppy disks.

Script Blocking options

Use Script Blocking options to enable Script Blocking and set what Norton AntiVirus should do if it finds a malicious script. For more information, see "Auto-Protect keeps you safe" on page 16.

Note: If you are developing or debugging scripts, disable Script Blocking. Otherwise this feature might block the script you are developing.

Manual Scan options

Manual Scan options determine what gets scanned and what happens if a virus is found during a scan that you request. Manual Scan options also include a Bloodhound subcategory that lets you enable Bloodhound technology during manual scans and set its level of sensitivity in detecting viruses.

Exclusions list

The Exclusions list defines the files that should not be scanned. You can define groups of files by file extension and you can list specific files. Be careful not to exclude the types of files that are more likely to be infected by viruses, such as files with macros or executable files.

Internet options

Internet options define what happens when your computer is connected to the Internet.

Email options

Use Email options to enable email scanning and define how Norton AntiVirus should behave while scanning email. Scanning incoming email protects your computer against viruses sent by others. Scanning outgoing email prevents you from inadvertently transmitting viruses to others. You can choose to scan incoming or outgoing email, or both, and to display an icon or progress indicator while scanning. You can set options to automatically repair, quarantine or delete infected email with or without your intervention.

LiveUpdate options

Use LiveUpdate options to enable Automatic LiveUpdate and define how updates should be applied for your computer. Automatic LiveUpdate checks for updated virus definitions automatically when you are connected to the Internet.

Other options

Other options include Activity Log settings, Inoculation settings, and Miscellaneous settings.

Activity Log options

The Activity Log records all Norton AntiVirus Professional Edition activities. You can choose to limit the activities recorded using the Activity Log options. You can also limit the size of the Activity Log. When the specified file size is reached, each new entry in the log causes the deletion of the oldest logged entry.

Inoculation options

Inoculation options are available only on Windows 98, Windows 98SE, and Windows Me.

Inoculation takes a snapshot of your critical system files. If Norton AntiVirus detects changes in these system files when comparing them to the original snapshot during a scan, it warns you about the changes.

Use Inoculation options to enable inoculation and, if a system file changes, to give you the choice to update the inoculation snapshot or repair the file by restoring it to its original values.

Miscellaneous options

There are four miscellaneous options:

- Backup file in Quarantine before attempting a repair
- Enable Office Plug-in
- Alert me on startup if my virus protection is out of date
- Scan system files at startup (this option is available only for Windows 98/98SE operating systems)

Advanced Tools

Options for advanced tools include properties for the Norton and Windows Recycle Bins for the Unerase tool.

Automatic LiveUpdate options for your handheld device

Live Update options for your handheld device include enabling and disabling LiveUpdate.

Enable Automatic LiveUpdate

Use Automatic LiveUpdate options to enable Automatic LiveUpdate for your handheld and define how updates should be applied for your handheld device. Automatic LiveUpdate checks for updated virus definitions automatically when your computer connects to the Internet. Then synchronize your Palm OS device to your computer to complete the updates.

Open the Options dialog box for your computer

You change Norton AntiVirus Professional Edition settings in the Options dialog box.

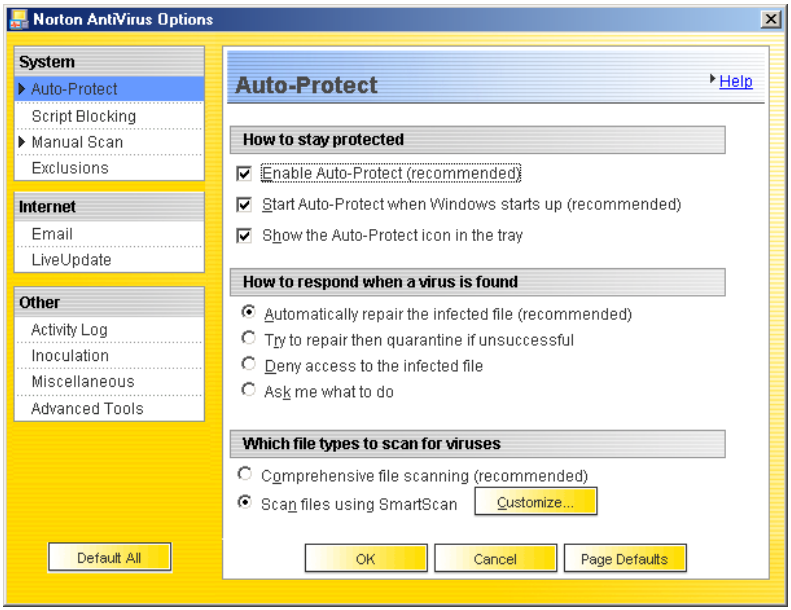
To open the Options dialog box

1 Start Norton AntiVirus Professional Edition.

For more information, see "Access Norton AntiVirus Professional Edition tools on your computer" on page 35.

2 Click **Options**.

3 Click **Norton AntiVirus**.



If you need to restore default settings in Options

You can change any or all of the options listed. If you have made a number of changes that have unwanted results, you can restore all options to the default settings.

To restore default settings on a page

- On the page for which you want to restore default settings, click **Page Defaults**.

To restore default settings for all Options

- On any page in the Options dialog box, click **Default All**.

For more information

Norton AntiVirus Professional Edition provides online Help, this User's Guide in PDF format, and links to the Symantec Web site.

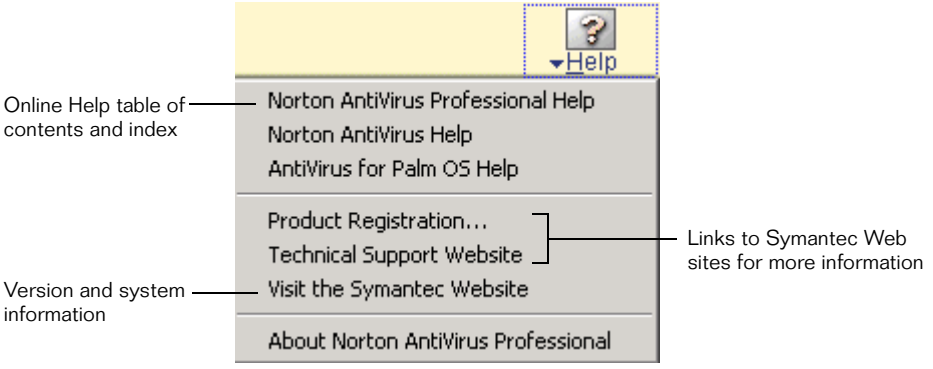
Symantec AntiVirus for Palm OS provides online Help on your handheld and your computer, this User's Guide in PDF format, and links to the Symantec Web site.

Use online Help on your computer

Help is always available from the Norton AntiVirus Professional Edition main window.

To access the Help menu on your computer

- At the top of the Norton AntiVirus Professional Edition main window, click **Help**.



In addition, Norton AntiVirus Professional Edition includes two kinds of more specific Help:

- Context-sensitive Help for dialog boxes
- How-to Help

Help for dialog boxes on your computer

When you request Help while working in a Norton AntiVirus Professional Edition dialog box, the Help that appears is specific to that dialog box.

To get Help for a dialog box

- In the dialog box, click **Help**.

How-to Help on your computer

How-to Help explains procedures that you are likely to perform using Norton AntiVirus Professional Edition on your computer. You can access these topics on the Contents and Index tabs.

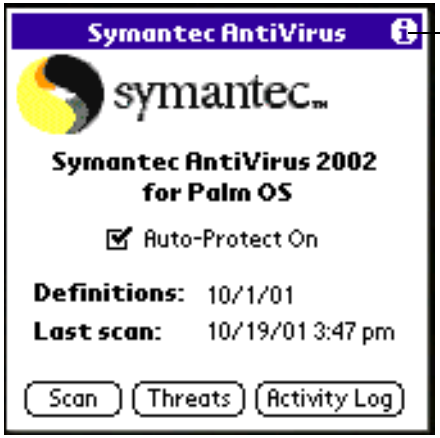
To get How-to Help

1. In the Norton AntiVirus Professional Edition main window, click **Help**.
2. On the Help menu, click **Norton AntiVirus Professional Help**.
3. In the Help window, select one of the following:
   - Contents: Search for Help by topic.
   - Index: Search for Help by key word.

   Contents and Index tabs are also available on many other Help windows and can always be used to search for Help.

Use online Help on your handheld device

Context-sensitive Help is available from within Symantec AntiVirus for Palm OS through the Tip icons.



To access context-sensitive Help

1. In any window, tap the **Tip** icon.
2. Tap **Done** to close the Tip window.

Access the User's Guide PDF

This User's Guide is provided on the Norton AntiVirus Professional Edition CD in PDF format. You must have Adobe Acrobat Reader installed on your computer to read the PDF.

To install Adobe Acrobat Reader

1. Insert the Norton AntiVirus Professional Edition CD into the CD-ROM drive.
2. Click **Browse CD**.
3. Double-click the **Manual** folder.
4. Double-click the **Acrobat** folder.
5. Double-click **AR500ENU**.
6. Follow the on-screen instructions to select a folder for Adobe Acrobat Reader and complete the installation.

Once you have installed Adobe Acrobat Reader, you can read the PDF from the CD.

To read the User's Guide PDF from the CD

1. Insert the Norton AntiVirus Professional Edition CD into the CD-ROM drive.
2. Click **Browse CD**.
3. Double-click the **Manual** folder.
4. Double-click **NAP2002**.

You can also copy the User's Guide to your hard disk and read it from there. It needs approximately 1 MB of disk space.

To read the User's Guide from your hard disk

1. Open the location into which you copied the PDF.
2. Double-click **NAP2002**.

Norton AntiVirus Professional Edition on the Web

The Symantec Web site provides extensive information about Norton AntiVirus Professional Edition virus protection, antivirus technology, and other Symantec products. There are several ways to access the Symantec Web site.

To access the Symantec Web site from the Norton AntiVirus main window

1. Click **Help**.
2. Select one of the following:
   - Technical Support Web site: Takes you to the Technical Support page of the Symantec Web site, from which you can search for solutions to specific problems, update your virus protection, and read the latest information about antivirus technology.
   - Visit the Symantec Web site: Takes you to the home page of the Symantec Web site, from which you can get product information on every Symantec product.

The Reports page of Norton AntiVirus Professional Edition contains a link to the Symantec online virus encyclopedia.

To access the Symantec Web site from the Reports page

1. In the Norton AntiVirus main window, click **Reports**.
2. On the Reports page, next to the Online Virus Encyclopedia heading, click **View Report**.

There is a link to the Symantec Web site on the Windows Explorer toolbar.

To access the Symantec Web site from Windows Explorer

1. Open Windows Explorer.
2. On the toolbar, on the Norton AntiVirus menu, click **View Virus Encyclopedia**.

   This option connects you to the Symantec Security Response Web page, from which you can search for information on all types of viruses.

You can always access the Symantec Web site through your Internet browser.

To access the Symantec Web site in your browser

- Type the Symantec Web site address:

  www.symantec.com

2

Antivirus tools

CHAPTER 4

Protecting your computer from viruses

Keeping your computer protected requires regular monitoring by Auto-Protect, scanning of your email, and frequent system scans. All of these tasks can be set to occur automatically.

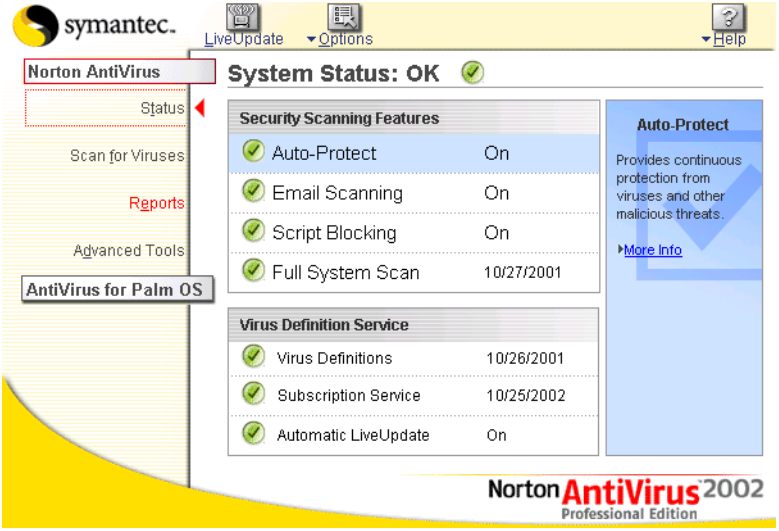
Ensure that Auto-Protect is enabled

Norton AntiVirus Professional Edition is configured to provide you with complete protection against viruses. It is unlikely that you need to change any settings. However, you should ensure that Auto-Protect is enabled.

To ensure that Auto-Protect is enabled

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus Professional Edition main window, click **Norton AntiVirus**.
3. In the Status pane of the Norton AntiVirus Professional Edition main window, ensure that Auto-Protect is set to On.

4 If Auto-Protect is not enabled, in the Status pane, select the Auto-Protect status line.



5 In the lower right-hand corner of the window, click **Enable**.

Scan disks, folders, and files

You can request scans of your entire computer, or of individual elements such as floppy disks, drives, folders, or files.

Perform a full system scan

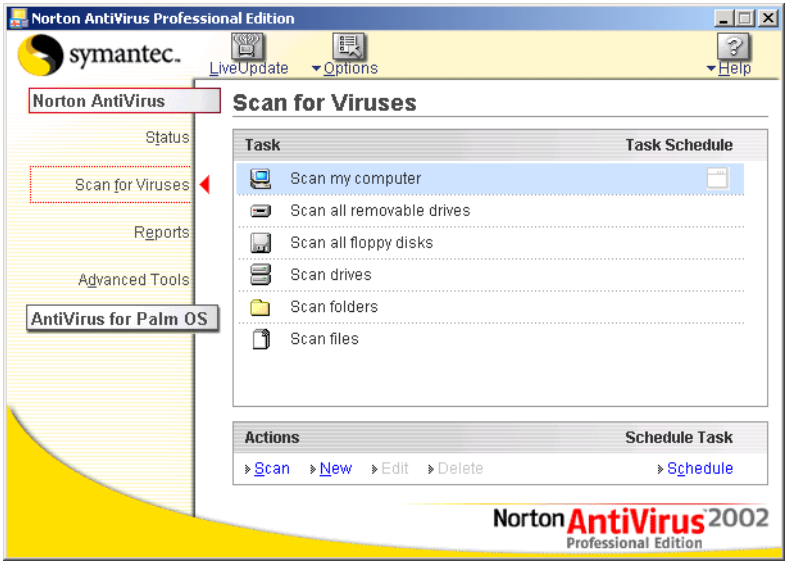
A full system scan scans all boot records and files on your computer.

To perform a full system scan

1 Start Norton AntiVirus Professional Edition.

2 In the Norton AntiVirus Professional Edition main window, click **Norton AntiVirus > Scan for Viruses**.

3 In the Scan for Viruses pane, click **Scan my computer**.



4 Under Actions, click **Scan**.

When the scan is complete, a scan summary appears.

5 When you are done reviewing the summary, click **Finished**.

Scan individual elements

You can choose to scan all removable drives, a floppy disk, any of your computer's drives, or any folders or files on your computer.

To scan individual elements

1 Start Norton AntiVirus Professional Edition.

2 In the Norton AntiVirus Professional Edition main window, click **Norton AntiVirus > Scan for Viruses**.

3 In the Scan for Viruses pane, select the scan that you want to run.

4 Under Actions, click **Scan**.

If you choose to scan all removable drives or a floppy disk, the scan starts automatically.

If you choose to scan drives, folders, or files, a dialog box appears in which you choose which drives, folders, or files to scan.

5 Click **Scan** after making your selection.

When the scan is complete, a scan summary appears.

6 When you are done reviewing the summary, click **Finished**.

About custom scans

You can create a custom scan if you regularly scan a particular segment of your computer and don't want to have to specify the segment to be scanned every time. You can delete the scan when it is no longer necessary. For example, if you are working on a project for which you need to frequently swap files with others, you might want to create a folder into which you copy and scan those files before using them. When the project is done, you can delete the custom scan for that folder.

You can also schedule the custom scan to run automatically. For more information, see "Schedule a custom scan" on page 70.

Create a custom scan

You can create a custom scan that includes specific locations on your computer.

To create a custom scan

1 Start Norton AntiVirus Professional Edition.

2 In the Norton AntiVirus Professional Edition main window, click **Norton AntiVirus > Scan for Viruses**.

3 In the Scan for Viruses pane, under Actions, click **New**.

4 In the opening window of the Norton AntiVirus Scan Wizard, click **Next**.

5 Do one or both of the following:

- To select individual files to be scanned, click **Add files**.
- To select folders and drives to be scanned, click **Add folders**.

You can use both options to select the combination of items that you want.

6 In the resulting dialog box, select the items that you want to scan.

If you select a folder, all files in that folder are included. If you select a drive, all folders and files on that drive are included.

7 Add the selected items to the list of items to scan by doing one of the following:

- In the Scan Files dialog box, click **Open**.
- In the Scan Folders dialog box, click **Add**.

8 To remove an item from the list, select it, then click **Remove**.

9 When you are done creating the list of items to be scanned, click **Next**.

10 Type a name for the scan by which you can identify it in the list of scans.

11 Click **Finish**.

Run a custom scan

When you run a custom scan, you do not have to redefine what you want to scan.

To run a custom scan

1 Start Norton AntiVirus Professional Edition.

2 In the Norton AntiVirus Professional Edition main window, click **Norton AntiVirus > Scan for Viruses**.

3 In the Scan for Viruses pane, select the custom scan.

4 Under Actions, click **Scan**.

When the scan is complete, a scan summary appears.

5 When you are done reviewing the summary, click **Finished**.

Delete a custom scan

You can delete custom scans if they are no longer needed.

To delete a custom scan

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus Professional Edition main window, click **Norton AntiVirus > Scan for Viruses**.
3. Select the scan that you want to delete by clicking the scan name.

   If you click the button next to the scan name, the scan runs.
4. Under Actions, click **Delete**.
5. Click **Yes** to verify that you want to delete the scan.

Scan email messages

If email protection is enabled, your email messages are scanned automatically. Norton AntiVirus Professional Edition supports all email programs that use either POP3 or SMTP communications protocol. To prevent connection time-outs while receiving large attachments, enable time-out protection.

Ensure that email protection is enabled

You can choose to scan incoming or outgoing email, or both. If your email program uses one of the supported communications protocols, both options are selected by default.

To ensure that email protection is enabled

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus Professional Edition main window, click **Norton AntiVirus** > **Options**.
3. In the Options window, under Internet, click **Email**.
4. For complete email protection, ensure that both Scan incoming Email and Scan outgoing Email are checked.

   To disable one of the options, uncheck it.
5. Click **OK**.

Enable time-out protection

Norton AntiVirus Professional Edition scans email by monitoring the communications port used for email and intercepting email transmissions. After incoming email has been scanned it is passed along to the email program. If you are downloading email with a large attachment, your email program may not receive a transmission for a few minutes and may time out as a result. If you enable time-out protection, Norton AntiVirus Professional Edition regularly confirms the connection with your email program and prevents a time-out.

Note: Time-out protection places hidden text at the top of your email messages. Your email program should remove this text. If you see NAV Time-out Protection in your email messages, you can ignore it.

To enable time-out protection

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus Professional Edition main window, click **Norton AntiVirus**.
3. In the Norton AntiVirus Professional Edition main window, click **Options**.
4. In the Options window, under Internet, click **Email**.
5. Ensure that Protect against time-outs when scanning Email is checked.
6. Click **OK**.

If problems are found during a scan

At the end of a scan, a summary report appears to tell you what Norton AntiVirus Professional Edition found during the scan. If a virus was found and you have requested that Norton AntiVirus Professional Edition repair the file automatically, it is listed as repaired.

If the file cannot be repaired, it can be quarantined or deleted. For more information, see "If a virus is found during a scan" on page 91.

Schedule automatic virus scans

When you install Norton AntiVirus Professional Edition and complete the Information Wizard, you can choose to schedule a weekly full system scan as part of post-install tasks. If you make that choice, the scan is scheduled automatically.

Note: You cannot schedule the predefined scans in the scan list, but you can schedule any custom scans that you have created.

Schedule a custom scan

You have complete flexibility in scheduling custom scans. When you select how frequently you want a scan to run (such as daily, weekly, or monthly), you are presented with additional fields with which you can refine your request. For example, you can request a daily scan, then schedule it to occur every two days or every three days instead.

To schedule a custom scan

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus Professional Edition main window, click **Norton AntiVirus > Scan for Viruses**.
3. Select the scan that you want to schedule by clicking the scan name.

   If you click the button next to the scan name, the scan runs.
4. Click **Schedule**.
5. In the Schedule dialog box, if Show multiple schedules is checked, click **New** to enable the scheduling fields.

   If it is not checked, the fields are already enabled.
6. Set the frequency and time at which you want the scan to run.

   Most of the frequency options include additional options that let you further refine the schedule. Set the additional options as necessary.
7. When you are done, click **OK**.

You can also create multiple schedules for a scan. For example, you could run the same scan at the beginning of your work day and at the end.

To create multiple schedules for a single scan

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus Professional Edition main window, click **Norton AntiVirus > Scan for Viruses**.
3. Select the scan that you want to schedule by clicking the scan name.

   If you click the button next to the scan name, the scan runs.
4. Click **Schedule**.
5. In the Schedule dialog box, check **Show multiple schedules**.
6. To set an additional schedule, click **New**.
7. Set the frequency and time at which you want the scan to run.

   Most of the frequency options include additional options that let you further refine the schedule. Set the additional options as necessary.
8. When you are done, click **OK**.

Edit scheduled scans

You can change the schedule of any scheduled scan, including the weekly full system scan.

To edit a scheduled scan

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus Professional Edition main window, click **Norton AntiVirus > Scan for Viruses**.
3. Select the scan that you want to schedule by clicking the scan name.

   If you click the button next to the scan name, the scan runs.
4. Click **Schedule**.
5. Change the schedule as desired.
6. Click **OK**.

Delete a scan schedule

You can delete any scan schedule. Deleting the schedule does not delete the scan.

To delete a scan schedule

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus Professional Edition main window, click **Norton AntiVirus > Scan for Viruses**.
3. Select the scan you want to schedule by clicking the scan name.

   If you click the button next to the scan name, the scan runs.
4. Click **Schedule**.
5. In the Schedule dialog box, check **Show multiple schedules**.
6. Select the schedule that you want to delete (if more than one).
7. Click **Delete**.
8. Click **OK**.

CHAPTER 5

Protecting your handheld device from threats

Keeping your handheld device protected requires regular monitoring by Auto-Protect and frequent system scans. Both of these tasks can be set to occur automatically.

About Auto-Protect

Auto-Protect, the automatic protection feature, monitors for threats while you are using your Palm OS device. Threats are received during HotSync or IR transmission with other devices.

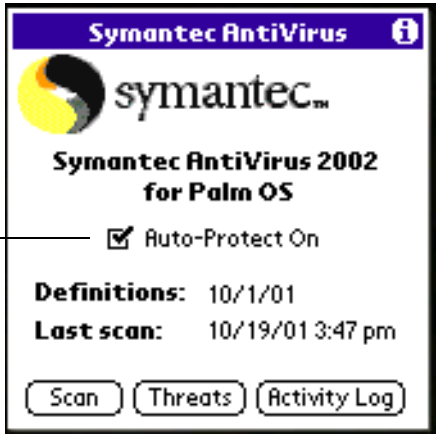
Keep Auto-Protect turned on

For maximum protection from known threats, keep Auto-Protect turned on. If you disable Auto-Protect, you will not be alerted if you attempt to open an infected application. However, you will still be able to scan for threats manually.

As you open and use programs on your Palm OS device, Auto-Protect checks to make sure no viruses or other threats exist in the files being accessed. If any threats exist, Auto-Protect intercepts them and alerts you.

To ensure that Auto-Protect is turned on

1 Start Symantec AntiVirus for Palm OS on your handheld.



The check mark indicates that Auto-Protect is turned on, monitoring activity, and alerting you to any known threats

2 Verify that the Auto-Protect On check box is checked.

Set a preference to scan after a synchronization

As extra protection, Symantec AntiVirus for Palm OS can automatically scan your entire device after a synchronization, when Auto-Protect is turned on. Use the Preferences menu in Symantec AntiVirus for Palm OS to turn this option on or off.

This option is active only if Auto-Protect is turned on. If Auto-Protect is turned off, Symantec AntiVirus for Palm OS does not scan after a synchronization.

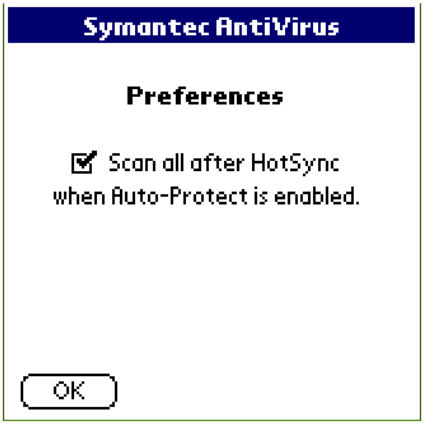
To specify scan preference after a synchronization

1 Start Symantec AntiVirus for Palm OS on your handheld.

2 Tap **Menu**.

3 Tap **Preferences**.

4 Check **Scan all after HotSync when Auto-Protect is enabled**.



5 Tap **OK**.

Scan for threats

Perform regular scans of your Palm OS device even if you have Auto-Protect turned on. Scanning can detect a threat that exists on your device, but is not active.

To scan for threats

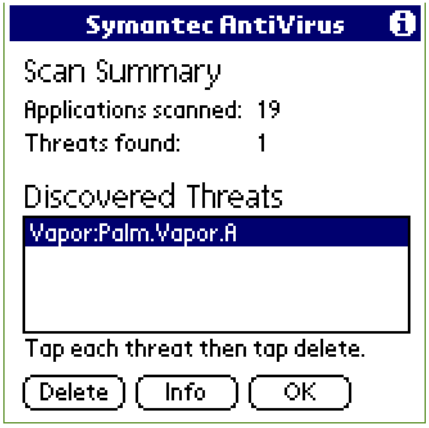
1 Start Symantec AntiVirus for Palm OS on your handheld device.

2 In the main window, tap **Scan**.

The Scan window shows the progress of the scan, how many threats were found, and the name of any threats found in previous scans.

View the Scan Summary

The Scan Summary window summarizes activity in the scan just performed. It shows how many viruses were found and deleted.



For information about what to do if you find a threat during a scan, see "If a threat is found by a scan" on page 103.

3

Advanced tools

CHAPTER 6

Recovering missing or erased files

Warning: If you purchased Norton AntiVirus Professional Edition to recover files, do not install Norton AntiVirus Professional Edition and do not start Windows. Any new files copied to your hard drive might overwrite existing data. Starting Windows writes to your hard drive. The Windows swap file could overwrite data you would like to recover. For more information, see "About Rescue Disks" on page 45.

About Norton Protection

When you erase a file using Windows Explorer, Windows keeps a temporary copy of the file in the Recycle Bin. The standard Windows Recycle Bin only protects files or folders deleted while you are using Windows.

Norton Protection transforms the standard Windows Recycle Bin into the Norton Protected Recycle Bin. It guards against losing the files the Recycle Bin does not protect. The Norton Protected Recycle Bin protects files that are deleted while you are using the command line, files created and deleted by Windows applications, and older versions of files that you modify and overwrite. If the Recycle Bin is not enabled, Norton Protection also protects files that would otherwise be under Recycle Bin protection.

Files shared on a network or stored on a network server, and files deleted while using your computer in DOS mode rather than Windows are not protected.

To configure Norton Protection

1. On the Windows desktop, right-click the **Norton Protected Recycle Bin**, then click **Properties**.
2. On the Norton Protection tab, make sure that Enable Protection is checked.
3. On the Recycle Bin tab, select the item to open when the Recycle Bin icon is double-clicked.
4. Use the context-sensitive Help to view more options on the Norton Protected Recycle Bin.

If you start your computer in DOS mode, you may find that DOS reports less free disk space than expected. This discrepancy is because DOS does not deduct the space used by deleted files protected by Norton Protection.

About UnErase Wizard

UnErase Wizard helps you recover deleted files that are protected by Norton Protection. Norton Protection, which appears on your desktop as the Norton Protected Recycle Bin, enhances the standard Windows Recycle Bin by protecting files from permanent deletion. UnErase Wizard lets you recover these protected files.

UnErase Wizard also helps you recover files that are deleted from the standard Windows Recycle Bin. In Windows 98/Me, UnErase Wizard frequently recovers unprotected files as well, even those deleted from the Recycle Bin.

Although UnErase Wizard can recover files that were not first protected with Norton Protection, enable Norton Protection to ensure the successful recovery of all deleted files. You can search for a deleted file by its file name and by words that you think the file may contain. This is especially useful if you can't remember the file name, but you do remember its contents.

Note: For Windows NT systems, Norton Protection must be running to be able to recover any files.

When you erase a file using Windows Explorer, Windows keeps a temporary copy of the file in the Recycle Bin. However, Windows does not detect files that were erased or overwritten by applications running in Windows, erased from a command prompt, or deleted via a permanent method such as using Shift-Delete.

Norton AntiVirus Professional Edition can help you recover these files. Norton Protection guards against losing files the Windows Recycle Bin does not protect. In Windows 98/Me, UnErase Wizard can help you restore files unprotected by Norton Protect. Windows NT/2000/XP can only recover files if Norton Protect is turned on.

If you have files that you want to be excluded from Norton Protect, you can set aside a portion of your disk or designate a particular type of file to be excluded. If these excluded files are deleted, they are not intercepted by the Windows Recycle Bin or Norton Protection and therefore are not recoverable in Windows NT/2000/XP systems.

If you have a dual boot system

If you have a dual boot system and the volume is not NTFS, you can start in Windows 98/Me, and use that version of UnErase to recover the file.

Recover a file with UnErase Wizard

UnErase Wizard helps you recover files that have been deleted but are not in the Windows Recycle Bin.

UnErase Wizard displays a list of deleted files or the files that conform to file name criteria that you provide. Each file is described by its name, original location, the date it was deleted, file type, file size, and the program that was used to delete it.

Note: For Windows NT/2000/XP systems, Norton Protect must be installed to recover files.

To recover a file that you recently erased

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus Professional Edition main window, click **Advanced Tools**.
3. On the UnErase Wizard line, click **Start Tool**.
4. In the UnErase Wizard dialog box, select one of the following:
   - Find recently deleted files: Searches for the names of the most recently deleted files and displays up to a maximum of 25 deleted files. (This option is available in Windows 98/Me.)
   - Find all protected files on local drives: Searches for and displays the names of all local deleted files that are protected by Norton Protection or the Windows Recycle Bin.
   - Find any recoverable files matching your criteria: Prompts you for search criteria.
   - Find all Norton Protected Users files: Searches for other users' protected files as well as your own. (This option is available in Windows NT/2000/XP.)
5. Click **Next**.

   UnErase Wizard displays a list of the most recently deleted files.
6. Select the file that you want to recover.
7. Click **Recover**.
8. If your deleted file is not listed (Windows 98/Me only), click **Next**.

   UnErase Wizard guides you through the process of creating a more complete list of deleted files from which to select.
9. Select the file you want to recover. Click **Recover**.
10. To close UnErase Wizard, click **Finish**.

    When you have recovered a file, you can preview its contents.

Note: You must have Quick View installed to preview a recovered file.

To preview a recovered file's contents

1. In a search results list, select a file name.
2. Click **Quick View**.
3. In the Name column of the search results list, right-click a file name, then click **Quick View**.

If you delete a file on a floppy disk from a DOS prompt by specifying file name letters after a wildcard (such as DEL *ILENAME.TXT as opposed to DEL FILENAME.TXT or DEL *.TXT), the file is listed as unrecoverable on the Recently Deleted Files page.

To see if a file is actually recoverable

1. Right-click in the center of the file list, then click **Show Unrecoverable Files**.
2. Click **Next**.
3. Use the subsequent UnErase Wizard pages to search the floppy disk.

CHAPTER 7

Eliminating data permanently

Wipe Info lets you remove selected files or folders from your hard drive.

Note: If you are running a recovery application such as System Restore or GoBack, you must erase your history before running Wipe Info to ensure that the data is completely wiped.

About Wipe Info

The Wipe Info Wizard erases files or folders from your hard drive so that they cannot be recovered.

- When you wipe a file, Wipe Info wipes the file and attempts to wipe any free space associated with the file and the file's directory entry.
- When you wipe a folder, Wipe Info wipes all of the files in the folder, and then if the folder is empty, it attempts to wipe the directory entry for the folder.

You cannot recover files that have been wiped. Windows Me/XP System Restore can restore files that have been wiped if they are one of the protected file types. By default, many document types, such as .doc and .xls files in My Documents are protected. Windows Me/XP System Restore maintains a copy of protected files. Wiping the original file does not wipe the copy that Windows Me/XP System Restore maintains.

About hexadecimal values

Wipe Info uses hexadecimal values to wipe files. Hexadecimal refers to the base 16 number system. This system is used to represent numbers in the

binary system, which uses the zero and one symbols in combinations to represent any number. Hexadecimal numbers are used by programmers because they are easier to write than zeros and ones.

The hexadecimal system consists of the numbers 0 to 9 and the letters A to F, used in combinations. For example, the decimal number 14 is represented as the letter E in the hexadecimal system.

In Wipe Info options, you can specify values from 00 to FF, representing numbers from 0 to 255 respectively. You can type the value using a number or a character from A to F.

About the Government Wipe process

When you select Government Wipe, Wipe Info does the following:

- Overwrites the data with 00s
- Verifies the 00 overwrite
- Overwrites with FFs
- Verifies the FF overwrite
- Writes a random value, or a value that you choose from 00 to FF
- Verifies the random overwrite
- Reverifies the random overwrite to ensure that it was written correctly
- Repeats as many times as you specify, up to 100

File names vs. file data

Wipe Info eliminates a file's contents from the disk, but does not remove the file name. While the file name remains on disk, it is no longer visible in Windows Explorer, and there is no data stored with it.

Warning: Never store sensitive information in a file name or attribute. This data can be replicated throughout your system without your knowledge, for example, in a list of most recently used files, or a file name search. This type of embedded information can be very difficult to remove from your computer.

Set Wipe Info options

You can specify how Wipe Info handles hidden, read-only, and system files. You can also specify the type of wipe to use. There are two types of wipes available:

- Fast Wipe overwrites the data being wiped with the hexadecimal value of your choice.
- Government Wipe is a 7-step procedure that conforms to the method specified in DoD (Department of Defense) document 5220-22-M, National Industrial Security Program Operating Manual, for the ultimate security level when eliminating data from a hard drive.

To change Wipe Info options

1. In the Norton AntiVirus Professional Edition main window, click **Advanced Tools**.
2. On the Wipe Info line, click **Start Tool**.
3. Click **Options**.
4. On the General tab, select the options for Read-only, System, and Hidden file types.

   This tells Wipe Info how to handle these types of files.
5. On the Wipe Type tab, select one of the following:
   - Fast Wipe
   - Government Wipe
6. Select the values for Wipe Info to use when overwriting the selected files.
7. Click **Apply**.

Wipe files or folders

To wipe a file or folder, add it to the Wipe Info window, then wipe it from within the window.

To wipe files or folders

1. In the Norton AntiVirus Professional Edition main window, click **Advanced Tools**.
2. On the Wipe Info line, click **Start Tool**.
3. In the Wipe Info window, click **Browse**.
4. Do one of the following:
   - Click **Folders**.
   - Click **Files**.
5. Select the folder or file to wipe.
6. Click **Open**.
7. With the Wipe Info window open, locate a folder or file on your hard disk.
8. Drag the selected item into the Wipe Info file list.
9. Continue to drag all of the files and folders that you want to wipe into the Wipe Info list.

   If you add an item to the list by mistake, select the item, then click **Remove Item(s) from list**.
10. Click **Wipe All**.
11. Click **Yes** to confirm the warning.

    All of the files in the list are wiped.

4

What to do if a virus is found

CHAPTER 8

What to do if a virus is found on your computer

If Norton AntiVirus Professional Edition finds a virus on your computer, there are three possible resolutions to the problem:

- Repair the file: Removes the virus from the file.
- Quarantine the file: Makes the file inaccessible by any programs other than Norton AntiVirus. You cannot accidentally open the file and spread the virus, but you can still evaluate it for possible submission to Symantec. For more information, see "If you have files in Quarantine" on page 95.
- Delete the file: Removes the virus from your computer by deleting the file that contains the virus. It should be used only if the file cannot be repaired or quarantined.

Viruses can be found when you run a scan or by Auto-Protect when you perform an action with an infected file. The way that you handle a virus differs depending on whether a scan or Auto-Protect found the virus.

If a virus is found during a scan

If a scan that you request finds a virus, you either receive a summary of the repair results, or you have to use the Repair Wizard to resolve the problem.

Review the repair details

If you have set your manual scan options so that Norton AntiVirus Professional Edition repairs files automatically, and all infected files could be repaired, the Scan Summary lists the number of files infected and repaired. This information is presented for status purposes only; you don't need to take further action to protect your computer. If you want to know

more, you can check the repair details to see which files were infected and with what viruses.

To review the repair details

1 In the the scanner window, in the Summary pane, click **More Details**.

2 When you are done reviewing the results, click **Finished**.

Use the Repair Wizard

If there are files that could not be repaired, or if you have set your manual scan options so that Norton AntiVirus Professional Edition asks you what to do when a virus is found, the Repair Wizard opens. If Norton AntiVirus Professional Edition did not attempt a repair, the Repair Wizard opens in the Repair pane. Otherwise, it opens in the Quarantine pane.

To use the Repair Wizard

1 If the Repair Wizard opens in the Repair pane, uncheck any files that you don't want Norton AntiVirus Professional Edition to repair.

All files are checked by default. This is the recommended action.

2 Click **Repair**.

3 If any files cannot be repaired, the Quarantine pane opens.

All files are checked to be added to the Quarantine by default. This is the recommended action.

In the Quarantine pane, uncheck any files that you do not want to quarantine, then click **Quarantine**.

4 If any files could not be quarantined, the Delete pane opens.

If you do not delete the infected files, the virus remains on your computer and can cause damage or be transmitted to others.

Uncheck any files that you do not want to be deleted, then click **Delete**.

5 Once all of the files have been repaired, quarantined, or deleted, the Summary pane of the scanner window opens. When you are done reviewing the summary, click **Finished**.

Note: After repairing a boot virus on your hard drive, restart your computer.

If a virus is found by Auto-Protect

Auto-Protect scans files for viruses when you perform an action with them, such as moving, copying, or opening them. If it detects a virus or virus-like activity, in most cases you receive an alert telling you that a virus was found and repaired. How you proceed depends on the operating system that you are using.

If you are using Windows 98/98SE/Me

If a virus is found and repaired by Auto-Protect in Windows 98/98SE/Me, you receive an alert telling you which file was repaired.

To close the alert

- Click **Finish**.

If you have set your options so that Auto-Protect asks you what to do when it finds a virus, the alert asks you to choose an action. The recommended action is always preselected.

Action	Result
Repair the infected file	Eliminates the virus and repairs the infected item. When a virus is found, Repair is always the best choice.
Quarantine the infected file	Isolates the virus-infected file, but does not remove the virus. Select Quarantine if you suspect that the infection is caused by an unknown virus and you want to submit the virus to Symantec for analysis.
Delete the infected file	Erases both the virus and the infected file. Select Delete if Repair is not successful. Replace the deleted file with the original program file or backup copy. If the virus is detected again, your original copy is infected.
Do not open the file, but leave the problem alone	Stops the current operation to prevent you from using an infected file. This action does not solve the problem. You will receive an alert the next time that you perform the same activity.

Action	Result
Ignore the problem and do not scan this file in the future	Adds the file that is suspected of containing a virus to the Exclusions list. When you add a file to the Exclusions list, the file is excluded from any future virus scans, unless you remove it from the list. Select this option only if you know that the file does not contain a virus.
Ignore the problem and continue with the infected file	Continues the current operation. Select this option only if you are sure that a virus is not at work. You will receive an alert again. If you are not sure what to do, select Do not open the file, but leave the problem alone.

If a file cannot be repaired, you receive an alert telling you that the repair was not made and recommending that you quarantine the file. You have the same options as those listed in the table, with the exception of Repair the infected file.

If you are using Windows NT/2000/XP

If a virus is found and repaired by Auto-Protect in Windows NT/2000/XP, you receive an alert telling you which file was repaired and which virus was infecting the file. If you have an active Internet connection, clicking the virus name opens the Symantec Web page that describes the virus.

To close the alert

- Click **OK**.

If the file cannot be repaired, you receive two alerts, one telling you that Auto-Protect was unable to repair the file, and another telling you that access to the file was denied.

You can set your Auto-Protect options to try to quarantine any infected files that it cannot repair. If you do this, you are informed if any files are quarantined. For more information, see "If you have files in Quarantine" on page 95.

To resolve problems with unrepaired files

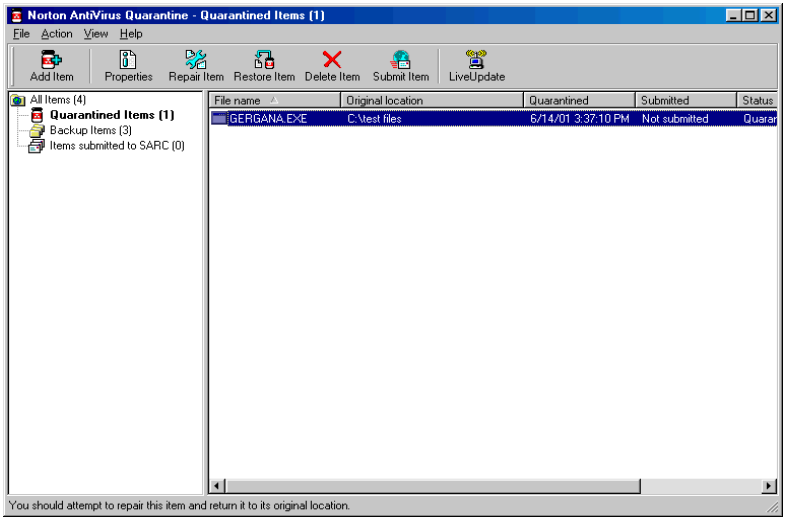
1. Run a manual scan on your computer to ensure that no other files are infected. For more information, see "Perform a full system scan" on page 64.
2. Follow the recommended actions in the Repair Wizard to protect your computer from the infected files. For more information, see "If a virus is found during a scan" on page 91.

If you have files in Quarantine

Once a file has been placed in Quarantine, you have several options. All actions that you take on files in Quarantine must be performed in the Quarantine window.

To open the Quarantine window

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus Professional Edition main window, click **Norton AntiVirus > Reports**.
3. In the Reports pane, on the Quarantined items line, click **View Report**.



The toolbar at the top of the Quarantine window contains all of the actions that you can perform on Quarantined files.

Action	Result
Add Item	Adds files to Quarantine. Use this action to quarantine a file that you suspect is infected. This action has no effect on files that are already in Quarantine.
Properties	Provides detailed information about the selected file and the virus that is infecting it.
Repair Item	Attempts to repair the selected file. Use this action if you have received new virus definitions since the file was added to Quarantine.
Restore Item	Returns the selected file to its original location without repairing it.
Delete Item	Deletes the selected file from your computer.
Submit Item	Sends the selected file to Symantec. Use this option if you suspect that a file is infected even if Norton AntiVirus did not detect a virus, or if you suspect that the virus was newly released.
LiveUpdate	Runs LiveUpdate to check for new protection and program updates. Use this if you haven't updated your virus protection for a while and want to try to repair the files in Quarantine.

To perform an action on a file in Quarantine

1. Select the file on which you want to perform the action.
2. In the toolbar, select the action that you want to perform.
3. When you are finished, on the File menu, click **Exit**.

If Norton AntiVirus Professional Edition cannot repair a file

One of the most common reasons that Norton AntiVirus Professional Edition cannot repair a file is that you do not have the most up-to-date virus protection. Update your virus protection with LiveUpdate and scan again. For more information, see "Keep current with LiveUpdate" on page 47.

If that does not work, read the information in the report window to identify the types of items that cannot be repaired, and then match it to one of the following types:

- Infected files have .exe, .doc, .dot, or .xls file name extensions. Any file can be infected. Use the Repair Wizard to solve the problem. For more information, see "Use the Repair Wizard" on page 92.
- Hard disk master boot record, boot record, or system files (such as IO.SYS or MSDOS.SYS) and floppy disk boot record and system files. Replace using the Rescue Disks or your operating system disks. For more information, see "About Rescue Disks" on page 45 and "Create Emergency Disks" on page 22.

If your computer does not start properly

If you have a virus on your computer and need to start the computer from an uninfected disk to remove the virus, or if you need to restore a boot record, use your Rescue Disks. If you do not have Rescue Disks, you can use your Emergency Disks to start the computer and remove the virus. If you need to restore boot records and do not have Rescue Disks, or if you need to restore system files, you must reinstall Windows. For more information, see "About Rescue Disks" on page 45 and "Create Emergency Disks" on page 22.

If you need to use Rescue Disks

Sometimes a virus infection prevents your computer from starting normally. Some viruses can only be removed if the computer is started from a clean disk, not the infected hard disk. Often, a Norton AntiVirus Professional Edition alert tells you when to use your Rescue Disks.

You first need to determine if your Rescue Disks are current. This means that you have created or updated your Rescue Disks since you did any of the following:

- Added, modified, or removed internal hardware
- Added, modified, or removed hard disk partitions
- Upgraded your operating system

If your Rescue Disks are not current, you can still use them to remove viruses from your computer. When the Rescue Disk window appears, use only the Norton AntiVirus Professional Edition task.

To use your Rescue Disks

1. Insert the Basic Rescue Boot floppy disk into drive A and restart your computer.

   The Rescue program runs in DOS.

2. Use the arrow keys to select the program that you want to run.

   A description of the selected program appears in the right panel of the Rescue program. Your choices are:

   - Norton AntiVirus: Scans your computer for viruses and repairs any infected files
   - Rescue Recovery: Checks and restores boot and partition information

3. Press **Enter** to run the selected program.
4. Follow the on-screen instructions for inserting and removing the Rescue Disks.
5. When the Rescue program is done, remove the Rescue Disk from drive A and restart your computer.

If you need to use Emergency Disks

If you have not created Rescue Disks, you can use Emergency Disks to restart your computer and scan for viruses. For more information, see "Create Emergency Disks" on page 22.

To use Emergency Disks

1. Insert Emergency Disk 1 into drive A and restart your computer.

   The Emergency program runs in DOS.

2. Ensure that Antivirus is selected, then press **Enter** to begin the Norton AntiVirus Emergency program.
3. Follow the on-screen instructions for inserting and removing the Emergency Disks.

   The Emergency program automatically scans your computer and removes viruses.

4. When the Emergency program is done, remove the Emergency Disk from drive A and restart your computer.

If you are using the CD as an Emergency Disk

If you are using the Norton AntiVirus Professional Edition CD as an Emergency Disk, you can ignore all of the instructions to change disks, as all necessary information is on the CD.

Note: You may need to change your computer's BIOS Setup options to start from the CD-ROM drive. For more information, see "I cannot start from drive A" on page 110.

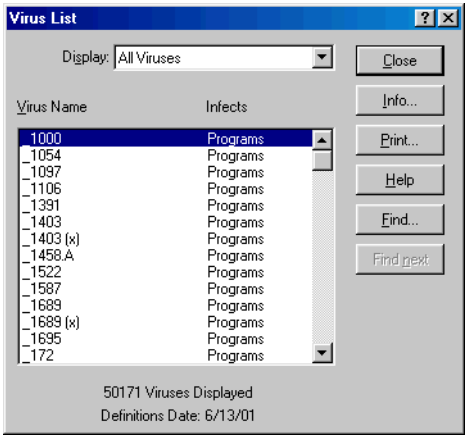
To use the CD as an Emergency Disk

1. Insert the Norton AntiVirus Professional Edition CD into the CD-ROM drive.
2. Restart your computer.

   The Emergency program scans your computer and removes viruses.

Look up virus names and definitions

You can look up a virus name from within Norton AntiVirus Professional Edition. The Virus List dialog box lists the viruses in the current virus definition service files.



To ensure that you have the latest virus definitions, run LiveUpdate. For more information, see "Keep current with LiveUpdate" on page 47.

To look up virus names and definitions

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus Professional Edition main window, click **Norton AntiVirus > Reports**.
3. In the Reports pane, on the Virus List line, click **View Report**.

You can print the list.

To print the list

- In the Virus List dialog box, click **Print**.

You can also use the list to get more information about a specific virus.

To get more information about a specific virus

1. In the Virus List dialog box, select the virus about which you want more information.
2. Click **Info**.
3. In the Virus Information window, click **Close** when you are done viewing the virus information.
4. When you are done viewing the list, in the Virus List dialog box, click **Close**.

Look up viruses on the Symantec Web site

Because of the large number of viruses, the Virus List file does not include descriptions of each virus. The Symantec Web site contains a complete list of all known viruses and related malicious code, along with descriptions. You must be connected to the Internet to look up viruses.

To look up viruses

1. Start Norton AntiVirus Professional Edition.
2. In the Norton AntiVirus Professional Edition main window, click **Norton AntiVirus > Reports**.
3. In the Reports pane, on the Online Virus Encyclopedia line, click **View Report**.

   The Symantec Web site opens in your Internet browser.
4. Use the links on the Web page to access the virus information for which you are looking.

CHAPTER 9

What to do if a threat is found on your handheld device

Threats can be found when you run a scan or by Auto-Protect when you use an infected file. The way that you handle a threat differs depending on whether a scan or Auto-Protect found it.

If a threat is found by Auto-Protect

Auto-Protect scans files and data for threats when you perform some action with them, such as copying, opening, or beaming.

If it detects a virus or *virus-like activity*, that is, an action that Symantec AntiVirus for Palm OS perceives as the work of a possible unknown virus, you receive an alert telling you that a virus was found, in most cases. An *alert* appears in a graphical user interface (GUI) to signal that an error has occurred, or to provide a warning.

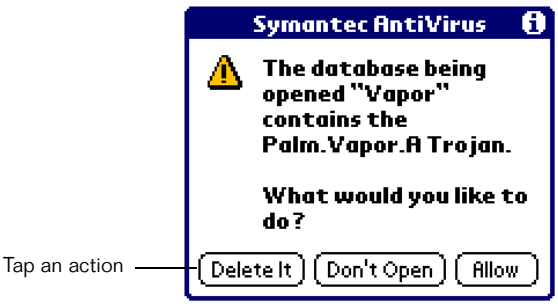
If Auto-Protect finds a virus on your handheld device, there are three possible resolutions to the problem:

- Remove the threat: This action deletes the infected file. Replace or resynchronize the file from the original program or backup copy. If the virus is detected again, your original copy is infected.
- Not open the file: This action does not open the infected file and stops the current activity to prevent you from using an infected file. This action does not solve the problem. You will receive an alert the next time you perform the same activity.
- Allow the file to open: This action continues the current activity. Select this action only if you are sure that a virus is not at work. You will

receive an alert each time that you open the file. If you are not sure what to do, do not open the file.

If you don't delete a known threat, it could destroy information on your Palm OS device, and possibly spread to other devices.

If Auto-Protect finds a threat, it displays an alert.



To delete a threat in Auto-Protect

1 On the Alert screen, tap **Delete It**.

This is the recommended action. After you tap Delete it, a message appears telling you to reset your Palm OS device.

2 Tap **Reset**.

Resetting your device does not affect any uninfected data on your device. For more information, see "If a threat is deleted" on page 105.

3 To verify that the threat has been deleted, view the Activity Log. For more information, see "Check recent antivirus activity" on page 43.

If you choose not to delete the infected file, choose a different action.

To stop the current activity due to a threat in Auto-Protect

- Tap **Don't Open**.

  Because threats don't harm your device unless they are activated, tapping Don't Open lets you bypass the threat and stop the current activity. However, it is highly recommended that you delete the threat.

To allow a threat in Auto-Protect

- Tap **Allow**.

  This continues the activity that triggered the alert. If you think the Auto-Protect alert was triggered by a harmless activity, you can proceed with caution.

Warning: If you open an infected file, you risk damaging your Palm OS data.

If a threat is found by a scan

If a threat is found while scanning, it appears in the Scan Summary screen.

To respond to a threat found while scanning

1. Tap **Delete** to delete the threat.

   This is the recommended action. Deleted threats appear with an asterisk in the Activity Log.
2. Tap **OK** to confirm that the threat was deleted.
3. When the threat has been deleted, perform a soft reset on your Palm OS device.
4. Tap **Continue** to proceed with the activity when you know the activity is safe.

View information about threats

The Threat List shows the list of threats that Symantec AntiVirus for Palm OS detects. It lists the threat name and the type.

The Threat Information screen describes a few details about a specific threat. The following facts appear:

- Name: The name of the threat.
- Size: The file size, in bytes.
- Threat type: Whether the threat is a Trojan horse, worm, or other threat type. For more information, see "How viruses work" on page 12.
- Likelihood: The frequency of occurrence in the computing community.

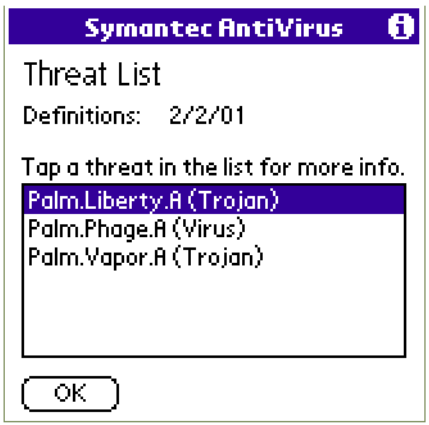
There is much more information about threat types, specific threats, and mobile computing security issues on the Symantec Web site at:

http://www.symantec.com

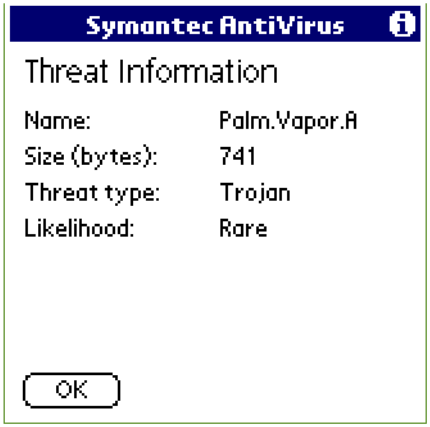
For more information, see "Norton AntiVirus Professional Edition on the Web" on page 59.

To view threat information

1. Start Symantec AntiVirus for Palm OS on your handheld device.
2. On the main screen, tap **Threats**.



3 To display the information about a threat, tap it.



4 Tap **OK** to close the Threat Information screen.

5 Tap **OK** to close the Threat List screen.

If a threat is deleted

When a threat is deleted, it is completely removed from your handheld device. Most often, the threat is an infected program and the entire program is deleted.

To be completely certain that no other threats exist or that multiple threats have been detected at one time, rescan after a threat has been deleted.

If a program is deleted

If you delete a program from your handheld device due to a threat, you can replace the deleted files. Reinstall your program files by synchronizing your handheld device to your computer or beaming the program from the original source.

5

Appendix

APPENDIX A

Troubleshooting

The information in this chapter will help you solve the most frequent problems that you may experience. If you can't find the solution to your problem here, there is a wealth of information on the Symantec Web site. You can find a troubleshooter, updates, patches, online tutorials, knowledge base articles, and virus removal tools. Point your browser to:

www.symantec.com/techsupp/

Use these suggestions to help solve problems encountered while running antivirus tools for your computer in Norton AntiVirus Professional Edition.

My Rescue Disk does not work

Due to the number of product-specific technologies used by manufacturers to configure and initialize hard drives, the Rescue program cannot always create a bootable disk automatically. If your Rescue Boot Disk does not work properly, do one of the following:

- If you have a special startup disk for your computer, add it to your Rescue Disk set. In an emergency, start from that disk. Remove the disk and insert your Rescue Boot Disk. At the DOS prompt, type A:RSHELL, press Enter, then follow the on-screen instructions.
- Use the Disk Manager or similarly named program that came with your computer to make your Rescue Boot Disk bootable. Make sure to test your modified Rescue Boot Disk.

Sometimes, your Rescue Boot Disk does not work properly because you have more than one operating system installed, such as Windows NT and Windows 98.

To modify your Rescue Boot Disk

1. Start up from your hard drive.
2. Insert your Rescue Boot Disk into drive A.
3. At the DOS prompt, type **SYS A:**
4. Press **Enter**.

   This transfers the operating system to the Rescue Boot Disk. Be sure to retest your Rescue Disks.

The alert tells me to use my Rescue Disks, but I did not create them

With your Norton AntiVirus Professional Edition CD you can create Emergency Disks. Although they are not as powerful as the Rescue Disks you create, you can use the Emergency Disks to recover from most common emergencies. For more information, see "Create Emergency Disks" on page 22.

You can use the CD that contains Norton AntiVirus Professional Edition as an Emergency Disk if your computer can start from the CD-ROM drive. For more information, see "If you are using the CD as an Emergency Disk" on page 99.

Once you have created the Emergency Disks, use them to solve the problem.

I cannot start from drive A

If your computer does not check drive A first on startup, use your computer's Setup program to change settings.

Be careful when making changes using your computer's Setup program. If you have never used it before, you may want to refer to your computer manufacturer's documentation.

To change your computer's settings

1. Restart your computer.

   A message appears telling you the key or keys to press to run SETUP, such as Press <DEL> if you want to run SETUP.
2. Press the key or keys to launch the Setup program.

3 Set the Boot Sequence to boot drive A first and drive C second.

   Setup programs vary from one manufacturer to the next. If you cannot find the Boot Sequence option, use the Setup program's Help system, refer to the documentation that came with your system, or contact your system's manufacturer.

4 Save the changes, then exit the Setup program.

You may need to use a special boot disk rather than the Rescue Boot Disk. In this case, use the boot disk or startup disk that came with your computer.

If your computer is set up with more than one operating system, such as Windows 2000 and Windows 98, you may need to modify the Rescue Boot Disk. For more information, see "My Rescue Disk does not work" on page 109.

Norton AntiVirus Professional Edition Auto-Protect does not load when I start my computer

If the Norton AntiVirus Professional Edition Auto-Protect icon does not appear in the lower-right corner of the Windows taskbar, Auto-Protect is not loaded. There are three likely reasons this is happening.

You may have started Windows in safe mode. Windows restarts in safe mode if the previous shutdown did not complete successfully. For example, you may have turned off the power without choosing Shut Down on the Windows Start menu.

To restart Windows

1 On the Windows taskbar, click **Start > Shut Down**.

2 In the Shut Down Windows dialog box, click **Restart**.

3 Click **OK**.

Norton AntiVirus Professional Edition may not be configured to start Auto-Protect automatically.

To set Auto-Protect to start automatically

1 In the Norton AntiVirus Professional Edition main window, click **Options**.

2 Click **Norton AntiVirus**.

3 In the Options dialog box, under System, click **Auto-Protect**.

4 Ensure that Start Auto-Protect when Windows starts up is checked.

Norton AntiVirus Professional Edition may not be configured to show the Auto-Protect icon in the tray.

To show the Auto-Protect icon in the tray

1 In the Norton AntiVirus Professional Edition main window, click **Options**.

2 Click **Norton AntiVirus**.

3 In the Options dialog box, under System, click **Auto-Protect**.

4 Ensure that Show the Auto-Protect icon in the tray is checked.

I have scanned and removed a virus, but it keeps infecting my files

There are four possible reasons a virus could be reappearing.

The virus might be in a program file with an unusual extension for which Norton AntiVirus Professional Edition is not configured to look.

To reset Norton AntiVirus scanning options

1 In the Norton AntiVirus Professional Edition main window, click **Options**.

2 Click **Norton AntiVirus**.

3 In the Options dialog box, under System, click **Manual Scan**.

4 Under Which file types to scan for viruses, click **Comprehensive file scanning**.

5 Click **Manual Scan > Bloodhound**.

6 Ensure that Enable Bloodhound heuristics is checked, then click **Highest level of protection**.

7 Click **OK**.

8 Scan all of the disks that you use and repair all infected files.

The source of the infection could also be a floppy disk. Scan all of the floppy disks that you use to ensure that they are free of viruses.

Another reason could be that the virus is remaining in memory after you remove it from the boot record. It then reinfects your boot record. Use

your Rescue Disks to remove the virus. For more information, see "If you need to use Rescue Disks" on page 97.

If the problem is a Trojan horse or worm that was transmitted over a shared network drive, you must disconnect from the network or password protect the drive to let Norton AntiVirus Professional Edition delete the problem.

Norton AntiVirus Professional Edition cannot repair my infected files

The most common reason that Norton AntiVirus Professional Edition cannot repair your infected files is that you do not have the most current virus protection on your computer. Update your virus protection regularly to protect your computer from the latest viruses. For more information, see "Keep current with LiveUpdate" on page 47.

If after using LiveUpdate the virus still cannot be repaired, the file may be corrupted, or contain a new virus. There are two additional options:

- Quarantine the file and submit it to Symantec. For more information, see "If you have files in Quarantine" on page 95.
- If a non-infected copy of the file exists, delete the infected file and replace it with the non-infected file.

I get an error when testing basic Rescue Disks

If you get the message Non-system disk, replace disk and press any key when testing your Rescue Disks, the Rescue program may not have prepared the floppy boot files correctly.

To repair the Rescue Boot Disk without having to reformat the disk and create a new Rescue Disk set

1. Remove the Rescue Boot Disk and restart your computer.
2. Insert the Rescue Boot Disk into the floppy disk drive.
3. On the Windows taskbar, click **Start > Run**.
4. In the Run dialog box, type **SYS A:**
5. Click **OK**.

I can't receive email

There are three possible solutions to this problem.

Temporarily disable email protection. This might allow the problem email to be download so that you can once again enable email protection. You are protected by Auto-Protect and Script Blocking while email protection is disabled.

To temporarily disable incoming email protection

1. In the Norton AntiVirus Professional Edition main window, click **Options**.
2. Click **Norton AntiVirus**.
3. In the Options dialog box, under Internet, click **Email**.
4. Uncheck **Scan incoming Email**.
5. Click **OK**.
6. Download your email.
7. Reenable incoming email protection.

Your email client may have timed out. Make sure time-out protection is enabled. For more information, see "Enable time-out protection" on page 69.

If you continue to experience problems downloading email, disable email protection.

To disable email protection

1. In the Norton AntiVirus Professional Edition main window, click **Options**.
2. Click **Norton AntiVirus**.
3. In the Options dialog box, under Internet, click **Email**.
4. Uncheck **Scan incoming Email**.
5. Uncheck **Scan outgoing Email**.
6. Click **OK**.

I can't send email

If you get the message, Norton AntiVirus was unable to send your email message because the connection to your email server was disconnected, your email client may be set to automatically disconnect after sending and receiving mail.

For Norton AntiVirus Professional Edition to scan outgoing email for viruses, it intercepts and scans the message before it is sent to your email provider. To resolve this issue, turn off this option within your email client. Consult your email client manual for instructions on how to do this. Or, disable Norton AntiVirus Professional Edition outgoing email scanning.

To disable outgoing email scanning

1. Start Norton AntiVirus Professional Edition.
2. Click **Options**.
3. Click **Email**.
4. Uncheck **Scan outgoing Email**.
5. Click **OK**.

Service and support solutions

Service and support information is available from the Help system of your Symantec product. Click the Service and Support topic in the Help index.

Technical support

Symantec offers two technical support options:

- Online Service and Support

  Connect to the Symantec Service & Support Web site at http://service.symantec.com, select your user type, and then select your product and version. This gives you access to current hot topics, knowledge bases, file download pages, multimedia tutorials, contact options, and more.

- PriorityCare telephone support

  PriorityCare fee-based telephone support services are available to all registered customers.You can access the PriorityCare number for your product through the Service & Support Web site. You'll be led through the online options first, and then to the telephone contact options available for your product and version.

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 old version for up to twelve months after the release of the new version. Technical information may still be available through the Service & Support Web site (http://service.symantec.com).

When Symantec announces that a product will no longer be marketed or sold, telephone support will be discontinued 60 days later. Support will be available for discontinued products from the Service & Support Web site only.

Customer service

Access customer service options through the Service & Support Web site at http://service.symantec.com. From this site, you can receive assistance with non-technical questions, and for information on how to do the following:

- Subscribe to the Symantec Support Solution of your choice.
- Obtain product literature or trialware.
- Locate resellers and consultants in your area.
- Replace missing or defective CD-ROMS, disks, manuals, and so on.
- Update your product registration with address or name changes.
- Get order, return, or rebate status information.
- Access customer service FAQs.
- Post a question to a Customer Service representative.

For upgrade orders, visit the online upgrade center at:
http://www.symantecstore.com

Worldwide service and support

Technical support and customer service solutions vary by country. For information on Symantec and International Partner locations outside of the United States, please contact one of the service and support offices listed below, or connect to http://service.symantec.com and select your region under the Global Service and Support.

Service and support offices

North America

Symantec Corporation
555 International Way
Springfield, OR 97477
U.S.A.

http://www.symantec.com/

Argentina and Uruguay

Symantec Region Sur
Cerrito 1054 - Piso 9
1010 Buenos Aires
Argentina

http://www.service.symantec.com/mx
+54 (11) 5382-3802

Asia/Pacific Rim

Symantec Australia
Level 2, 1 Julius Avenue
North Ryde, NSW 2113
Sydney
Australia

http://www.symantec.com/region/reg_ap/
+61 (2) 8879-1000
Fax: +61 (2) 8879-1001

Brazil

Symantec Brasil
Market Place Tower
Av. Dr. Chucri Zaidan, 920
12° andar
São Paulo - SP
CEP: 04583-904
Brasil, SA

http://www.service.symantec.com/br
+55 (11) 5189-6300
Fax: +55 (11) 5189-6210

Europe, Middle East, and Africa

Symantec Customer Service Center
P.O. Box 5689
Dublin 15
Ireland

http://www.symantec.com/region/reg_eu/
+353 (1) 811 8032

Mexico

Symantec Mexico
Blvd Adolfo Ruiz Cortines,
No. 3642 Piso 14
Col. Jardines del Pedregal
Ciudad de México, D.F.
C.P. 01900
México

http://www.service.symantec.com/mx
+52 (5) 661-6120

Other Latin America

Symantec Corporation
9100 South Dadeland Blvd.
Suite 1810
Miami, FL 33156
U.S.A.

http://www.service.symantec.com/mx

Subscription policy

If your Symantec product includes virus, firewall, or web content protection, you might be entitled to receive protection updates via LiveUpdate. The length of the subscription could vary by Symantec product.

When you near the end of your subscription, you will be prompted to subscribe when you start LiveUpdate. Simply follow the instructions on the screen. After your initial subscription ends, you must renew your subscription before you can update your virus, firewall, or web content protection. Without these updates, your vulnerability to attack increases. Renewal subscriptions are available for a nominal charge.

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.

January 15, 2002

G L O S S A R Y

access rights — The types of operations and files a user or group can access and what the user or group is permitted to do with those directories and files.

administrator — 1. A person who oversees the operation of a network. 2. A person responsible for installing programs on a network and configuring them for distribution to workstations. This person may also update security settings on workstations.

alert — A dialog box that appears in a graphical user interface (GUI) to signal that an error has occurred, or to provide a warning.

beam — To transfer data by infrared transmission.

browser — A software application that makes navigating the Internet easy by providing a graphical user interface. This lets the user click menus, icons, or buttons rather than learn difficult computer commands. Also called a Web client.

compressed file — A file that has been compressed using a special data storage format in order to save space on your disk.

compression — Using a mathematical algorithm to process data from a file or disk, such that the resulting data occupies less physical space on the disk. Individual files or entire disks can be compressed by various types of utility software.

disk icon — An icon representing a disk.

document file — A file that is created by, or associated with, a program and contains no executable code. Examples include word processing documents, databases, and spreadsheets.

download To transfer a file from one computer system to another, through a modem or network. Download usually refers to the act of transferring a file from the Internet, a BBS (bulletin board system), or a service such as America Online.

download directory The directory in which files received during file transfer are stored.

email (electronic mail) A method of exchanging messages and files with other people via computer networks. A popular protocol for sending email is SMTP (Simple Mail Transfer Protocol). Popular protocols for receiving email are POP3 (Post Office Protocol 3) and IMAP4 (Internet Message Access Protocol 4). Web-based email services use HTTP (HyperText Transfer Protocol) for sending and receiving email.

executable file A file containing program code that can be launched. Generally includes any file that is a program, extension, or a system file.

file server A storage device connected to a network that provides network users access to shared programs and data files.

file type The four-character code, stored along with a creator code in each file, that identifies its type. Programs use this code to determine if a file is in a format that can be read by the program.

hard disk A device that reads data from, and writes data onto, a disk.

icon A graphic symbol used to represent a file, folder, disk, or other entity.

infected file A file that contains a virus.

Internet A decentralized global network connecting millions of computers.

IR Infrared. Infrared transmission communicates through an IR port without cables. IR ports are typically found on handheld devices and laptop computers.

known virus Any virus that Norton AntiVirus Professional Edition can detect and identify by name.

LAN (Local Area Network) A group of computers connected for the purpose of sharing resources. The computers on a local area network are typically located within a defined physical space, such as a single building, or section of a building.

local A term that refers to your computer, as opposed to a remote computer.

locked disk *See* write-protect.

locked file A file that can be viewed, but cannot be written to or deleted. Also referred to as read-only.

log A record of actions and events that take place on a computer or handheld device.

network A set of computers and associated hardware connected together in a work group for the purpose of sharing information and hardware among users.

newsgroups A discussion forum on the Internet that provides articles and posting opportunities for its members. A newsgroup is typically focused on a particular subject or range of subjects.

operating system A program that ties the capabilities of computer hardware and software to input/output devices such as disks, keyboards, and mice.

password A character sequence entered by users to verify their identities to a network or program. The most secure passwords are difficult to guess or find in a dictionary, and contain a combination of capital letters, lowercase letters, numbers, and symbols.

program A set of instructions that can be executed by a computer, and are written for a specific purpose such as word processing or creating a spreadsheet. Also called software.

read-only A 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 those that cannot. Some examples of removable media are floppy disks, disk cartridges (such as SyQuest and Bernoulli, for example), CDs, and Zip disks.

script A list of instructions that can be executed without user interaction. Unlike other types of programs, scripts can be opened with text editors or word processing programs, so they are very easy to change. Examples of scripts include Visual Basic programs and network login scripts.

startup disk A disk that contains the system files necessary to start your computer. Startup disk usually refers to a floppy disk or CD that can be used to start the computer in an emergency.

synchronize The process by which the handheld device and computer compare files to ensure that they contain the same data. During synchronization, information can be copied to your computer from your handheld or vice versa.

Trojan horse A destructive program often designed to cause damage or do something malicious to a system, while disguised as something useful or interesting. Unlike viruses, Trojan horses don't make copies of themselves. Some Trojan horse programs perform malicious actions on the computer on which they are run, while others, such as Back Orifice, provide remote-control capabilities for hackers.

unknown virus A virus for which Norton AntiVirus Professional Edition does not contain a definition. *See also* virus definitions file.

virus A self-replicating program intentionally written 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. Self-replication differentiates viruses from other virus-like computer infections such as Trojan horse programs and worms. *See also* virus-like activity.

virus definition Virus information that lets an antivirus program recognize and alert you to the presence of a specific virus. *See also* unknown virus.

virus definitions file A file used by Norton AntiVirus to find and repair viruses. The virus definitions files must be updated regularly. LiveUpdate automates the process of downloading updated virus definitions files.

Virus List A list that shows all of the viruses for which Norton AntiVirus has a virus definition. It is important to update this list regularly.

virus-like activity An activity or action that Norton AntiVirus Professional Edition 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.

Web page A single document on the World Wide Web that is identified by a unique URL. A Web page can contain text, hyperlinks, and graphics.

Web site A group of Web pages managed by a single company, organization, or individual. A Web site may include text, graphics, audio and video files, and hyperlinks to other Web pages.

World Wide Web The collection of hypertext documents that are stored on Web servers around the world. Also called WWW or simply the Web. The Web allows universal access to a vast collection of documents stored in HTML format as Web pages.

worm A 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 a computer down. So far, worms do not exist in the Macintosh world.

write-protect 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.

INDEX

T

U

V

W

Norton AntiVirus™ Professional Edition

CD Replacement Form

CD REPLACEMENT: After your 60-Day Limited Warranty, if your CD becomes unusable, fill out and return 1) this form, 2) your damaged CD, and 3) your payment (see pricing below, add sales tax if applicable), to the address below to receive replacement CD. *DURING THE 60-DAY LIMITED WARRANTY PERIOD, THIS SERVICE IS FREE.* You must be a registered customer in order to receive CD replacements.

FOR CD REPLACEMENT

Please send me: ___ CD 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 distributor.

Briefly describe the problem:_____

_____

CD Replacement Price	$ 10.00
Sales Tax (See Table)	_____
Shipping & Handling	$ 9.95
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 CD REPLACEMENT ORDER TO:

Symantec Corporation
Attention: Order Processing
555 International Way
Springfield, OR 97477 (800) 441-7234

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

symantec™