

Norton AntiVirusTM Corporate Edition

Norton AntiVirusTM Corporate Edition 7.0

INTELLIGENT SOLUTIONS TO PROTECT YOUR ORGANIZATION

Norton AntiVirus™ Corporate Edition

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Copyright Notice

Copyright © 1999 Symantec Corporation.

Documentation Version 1.0

All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS, and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make change without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, Peter Norton Group, 10201 Torre Avenue, Cupertino, CA 95014.

Trademarks

Symantec, the Symantec logo, Norton AntiVirus, LiveUpdate, Striker, Bloodhound, and Symantec AntiVirus Research Center (SARC) are trademarks of Symantec Corporation.

Microsoft, Windows, and Windows logo are registered trademarks, and Microsoft Exchange is a trademark of Microsoft Corporation. NetWare is a registered trademark of Novell, Inc. Mac and Mac OS are trademarks of Apple Computer, Inc. Other brands and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

SYMANTEC LICENSE AND WARRANTY

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

LICENSE AND WARRANTY:

The software which accompanies this license (the "Software") is the property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, you will have certain rights to use the Software after your acceptance of this license. Except as may be modified by a license addendum which accompanies this license, your rights and obligations with respect to the use of this Software are as follows:

You may:

- (i) use only one copy of one version of the various versions of the Software contained on the enclosed CD-ROM on a single computer;
- (ii) make one copy of the Software for archival purposes, or copy the software onto the hard disk of your computer and retain the original for archival purposes;
- (iii) use the Software on a network, provided that you have a licensed copy of the Software for each computer that can access the Software over that network;
- (iv) after written notice to Symantec, transfer the Software on a permanent basis to another person or entity, provided that you retain no copies of the Software and the transferee agrees

to the terms of this agreement; and

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

You may not:

- (i) copy the documentation which accompanies the Software;
- (ii) sublicense, rent or lease any portion of the Software;
- (iii) reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software; or
- (iv) use a previous version or copy of the Software after you have received a disk replacement set or an upgraded version as a replacement of the prior version, unless you donate a previous version of an upgraded version to a charity of your choice, and such charity agrees in writing that it will be the sole end user of the product, and that it will abide by the terms of this agreement. Unless you so donate a previous version of an upgraded version, upon upgrading the Software, all copies of the prior version must be destroyed.

Sixty Day Money Back Guarantee:

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

Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to you. Your sole remedy in the event of a breach of this warranty

will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money you paid for the Software. Symantec does not warrant that the Software will meet your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE.

Disclaimer of Damages:

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

SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

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

U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in

Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c) (1) and (2) of the Commercial Computer Software-Restricted Rights clause at 48 CFR 52.227-19, as applicable, Symantec Corporation, 10201 Torre Avenue, Cupertino, CA 95014.

General:

This Agreement will be governed by the laws of the State of California. This Agreement may only be modified by a license addendum which accompanies this license or by a written document which has been signed by both you and Symantec. Should you have any questions concerning this Agreement, or if you desire to contact Symantec for any reason, please write: Symantec Customer Sales and Service, 10201 Torre Avenue, Cupertino, CA 95014.

SYMANTEC LICENSE AND WARRANTY

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

C O N T E N T S

Chapter 1 Introducing Norton AntiVirus

How does Norton AntiVirus prevent infections?	7
What is SARC?	8

Chapter 2 Managing Norton AntiVirus

Benefits of a managed solution	11
Setting antivirus policy	12
What to scan	13
What to do if a virus is detected	13
Migrating from standalone to managed protection	13
Clients	13
Servers	14

Chapter 3 Using Norton AntiVirus

What you do	15
Standalone vs. managed installations	16
Opening Norton AntiVirus	16
Getting around in Norton AntiVirus	16
Getting help	19
Keeping virus protection current	20
Using LiveUpdate	20
Updating without LiveUpdate	21
Managing Realtime Protection	22
Turning File System Realtime Protection off temporarily	22
Increasing File System Realtime Protection	23
Scanning for viruses	23
On-demand scans	24
Scheduled scans	25
Startup scans	26
Custom scans	27
Interpreting scan results	28
Managing the Quarantine	29
Treating files in the Quarantine	30
Clearing Backup Items	31
Submitting a potentially infected file to SARC for analysis	31
Setting an exclusion	32

Symantec Service and Support Solutions

CD Replacement Form

Index

Introducing Norton AntiVirus

This Norton AntiVirus Corporate Edition guide is designed for two audiences:

- Administrators
- Client users

For administrators, Chapter 2, “Managing Norton AntiVirus,” presents a few issues that relate to standalone clients and managed clients. For client users, Chapter 3, “Using Norton AntiVirus,” presents basic procedures to perform everyday tasks and maintain complete virus protection.

The same Norton AntiVirus Corporate Edition client program is installed on all Win32 machines for standalone protection (Windows 9x, Windows NT Workstation and Server, and Windows 2000). A separate client program, not discussed in this guide, protects Windows 3.x and DOS computers.

How does Norton AntiVirus prevent infections?

A virus is simply a computer program designed in such a way that, when run, it attaches a copy of itself to another computer program or document. Thereafter, whenever the infected program is run or document is opened, the attached virus program is activated and attaches itself to yet other programs and documents. In addition to replicating, viruses are generally programmed to deliver a payload. Most viruses simply display a message on a particular trigger date. Some, however, are programmed specifically to damage data by corrupting programs, deleting files, or reformatting disks.

Symantec engineers track reported outbreaks of computer viruses to identify new viruses. Once a virus is identified, information about the virus (a virus signature) is stored in a virus definitions file, which contains the

necessary information to detect and eliminate the virus. When Norton AntiVirus scans for viruses, it is searching for these telltale virus signatures.

The Norton AntiVirus LiveUpdate feature makes sure your virus protection remains current. Updated virus definitions files are available from Symantec regularly. With LiveUpdate, Norton AntiVirus connects automatically to a special Symantec site, determines if your files need updating, downloads the proper files, and installs them in the proper location.

Virus infections can be easily avoided. Viruses that are quickly detected and removed from your computer cannot spread to other files and cause damage. Norton AntiVirus uses a variety of methods to detect file, boot, and macro viruses early:

- **File System Realtime Protection:** Constantly monitors activity on your computer by looking for virus signatures when a file is executed or opened, and when modifications have been made to a file, such as renaming, saving, moving, or copying a file to and from folders.

To supplement detection of known viruses, Norton AntiVirus includes a powerful component called Bloodhound. With this advanced heuristic technology, Norton AntiVirus can detect a high percentage of new or unknown viruses not yet analyzed by antivirus researchers.

- **Signature-based scanning:** Norton AntiVirus relies on signature or pattern-based scanning to detect viruses. Norton AntiVirus searches for residual virus signatures in infected files. This search is called a scan. If a virus signature is detected, Norton AntiVirus notifies you that one or more of your files is infected.

What is SARC?

The strength behind the Norton AntiVirus Corporate Edition protection lies in the Symantec AntiVirus Research Center (SARC). The increasing number of computer viruses, currently over 40,000 are known, requires effort to track, identify, and analyze new viruses and virus technologies. SARC researchers disassemble each virus sample to discover its identifying features and behavior. With this information, they develop a virus definition that Symantec products use to detect and eliminate the new virus during scans. At least weekly, and whenever a destructive new virus threatens, Symantec makes updated definitions available.

Because of the speed at which new viruses spread, particularly over the Internet, SARC is developing automated software analysis tools. With direct submissions over the Internet of infected files from your Norton AntiVirus

Quarantine to SARC, the time from discovery, analysis, and return cure by email is shrinking from days to hours, and in the near future, to minutes.

Managing Norton AntiVirus

This chapter is intended primarily for network administrators who manage Norton AntiVirus Corporate Edition on client computers. It discusses the benefits of a managed solution, the default install settings on client computers and how they relate to antivirus policy, and the migration path from standalone clients and servers to managed clients and servers.

Benefits of a managed solution

Norton AntiVirus network-level virus protection adds an additional layer of security for computers attached to a Norton AntiVirus server. These computers, running in connected mode, join a group of managed computers monitored by a network administrator. Managed computers can be more closely monitored, and virus intrusion points can be detected and then better protected against future attacks. Some of the specific benefits of network protection include:

- Added protection at the server level: Norton AntiVirus scans the network servers containing the essential data, email, and program resources that keep your network running efficiently.
- Centralized virus scanning of networked computers: Managed computers can be scanned from a Symantec System Center console at specific, scheduled times of the day. This is a convenient solution for network users who do not have the time to regularly scan their computer for viruses, and ensures network administrators that the network remains protected against virus attacks.
- Quarantine Server for virus infected files: Copies of infected items are forwarded from the Quarantine on the client machine to the centralized Quarantine. An administrator submits the item to SARC and receives a virus definitions update by email. After applying the update

on the centralized Quarantine to test and confirm the update, the updates are rolled out to client machines. The client machine, upon receiving the update, performs a selected preset operation, such as repairing the infected item and releasing it from the client Quarantine automatically.

- Convenient update options for networked computers: Save time and effort for both network administrators and network users. Virus definitions files should be updated frequently to ensure that every computer has current virus protection. As part of a network installation, computers attached to a Norton AntiVirus server receive updates seamlessly.

Administrators remotely control Norton AntiVirus settings through a console application, the Symantec System Center. Tasks for clients include the following:

- Starting and stopping File System Realtime Protection.
- Starting and stopping Lotus Notes, Lotus cc:Mail, or Microsoft Exchange Realtime Protection, if installed.
- Creating and running scheduled scans.
- Creating and running on-demand scans.
- Changing scan options for all types of scans.
- Updating virus definitions files throughout the network.

Administrators can standardize virus protection settings over the network by locking configuration settings on the Norton AntiVirus clients. Network users cannot change settings for locked items. By standardizing virus protection settings, an administrator can turn the network into a fortress against virus invasions without slowing the normal performance of the network.

Setting antivirus policy

Norton AntiVirus provides two types of protection: File System Realtime Protection, which constantly monitors files for infection as they are accessed or modified, and scans, that can be initiated on demand, scheduled to run unattended, or invoked automatically at system startup. In both cases, there are two basic configuration components:

- What to scan
- What to do if a virus is detected

What to scan

By default, Norton AntiVirus File System Realtime Protection scans files identified by file extension. The default list of extensions includes all files commonly at risk of infection. Norton AntiVirus completes scans faster by scanning only files with the selected extensions.

Consider changing this setting to All Types in a high-risk environment or after a series of virus incidents. At a small resource cost, you can effectively block infection from files with non-standard extensions as well.

All other scans—on demand, scheduled, custom, or startup—examine All Types by default.

What to do if a virus is detected

Norton AntiVirus responds to infected files with actions and backup actions. By default, when a virus is detected by either Realtime Protection or during a scan, Norton AntiVirus attempts to clean the virus from the infected file. If Norton AntiVirus cannot clean the file, then the backup action is to move the infected file to the Quarantine so that the virus cannot spread.

Depending on your antivirus policy, you can change these settings to delete on detection or leave alone (log only). Further, you can set different actions for macro and non-macro viruses for each scan type separately.

Migrating from standalone to managed protection

The following topics briefly summarize the procedure to migrate standalone clients to managed protection. For complete information, refer to the *Norton AntiVirus Corporate Edition 7.0 Implementation Guide*.

Clients

Norton AntiVirus Corporate Edition standalone clients for Windows 95, 98, NT 4.0, and 2000 can be migrated to managed protection by copying a single file, GRC.DAT, to each client machine. GRC.DAT contains data for communication between the server and client.

GRC.DAT is created automatically when rolling out the Norton AntiVirus Enterprise Solution. The Norton AntiVirus server installation includes the creation of the following folders on each management server:

Using Norton AntiVirus

Norton AntiVirus safeguards computers from virus infection, no matter what the source. Computers are protected from viruses that spread from hard drives, floppy disks, email attachments, and others that travel across networks. Files within compressed files are scanned and cleaned. No separate programs or options changes are necessary for the Internet-borne viruses—File System Realtime Protection scans program and document files automatically as they are downloaded.

Norton AntiVirus responds to infected files with actions and backup actions. When a virus is detected during a scan, Norton AntiVirus, by default, attempts to clean the virus from the infected file. If the file is cleaned, the virus is successfully and completely removed from the file. If for some reason Norton AntiVirus cannot clean the file, then Norton AntiVirus attempts the backup action, moving the infected file to the Quarantine so that the virus cannot spread.

For more information about Norton AntiVirus preset options, see [“Setting antivirus policy”](#) on page 12.

What you do

Norton AntiVirus tasks that you initiate or configure from the workstation include the following:

- Get help online (see page 19).
- Keep virus protection current (see page 20).
- Increase Realtime Protection (see page 23).
- Scan for viruses (see page 23).
- Schedule unattended or startup scans (see page 25 and page 26).
- Manage the Quarantine of infected files (see page 29).

Standalone vs. managed installations

Your Norton AntiVirus Corporate Edition virus protection may be either a standalone or an administrator-managed installation. The procedures that follow in this chapter assume a standalone installation with the preset or default option settings. If your installation is part of a network-wide installation managed by the Symantec System Center, some options may be locked, dimmed, or not appear at all, depending upon your administrator's antivirus policy.

Opening Norton AntiVirus

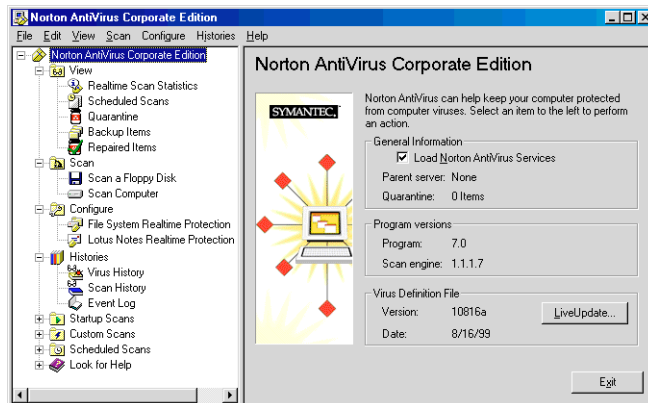
To open Norton AntiVirus, do one of the following:



- On the Windows taskbar, double-click the Norton AntiVirus Corporate Edition icon.
- Click Start, point to Programs, point to Norton AntiVirus Corporate Edition, and click Norton AntiVirus Corporate Edition

Getting around in Norton AntiVirus

Most of the work you do in Norton AntiVirus will be in its two-paneled window. The left pane groups activities you can perform into categories. For example, Scan a Floppy Disk and Scan Computer are tasks in the Scan category. Individual icons represent each category in the left pane. When you click categories and other items in the left pane, the window to the right responds with the information you need to perform a task.



- Click a plus sign in the left pane to open a folder

- Click a minus sign in the left pane to close a folder
- Click an item in the left pane to access the information in the right pane.

View

Realtime Scan Statistics	View statistics about the status of realtime scans, including the last file that was scanned (even if it wasn't infected).
Scheduled Scans	View the list of all scheduled scans created to run on your computer, including the name of the scan, when it is scheduled to run, and who created it.
Quarantine	Manage virus-infected files that have been isolated to prevent their spread (see page 30).
Backup Items	Delete backup copies of infected files. As a data safety precaution, Norton AntiVirus makes a backup copy of infected items before attempting a repair. After verifying that Norton AntiVirus cleaned an infected item of viruses, you should delete the copy in Backup Items (see page 31).
Repaired Items	Release items that have been cleaned of viruses whose original locations are not known. For example, an infected attachment may have been stripped from an email and quarantined. After the item is cleaned in the Quarantine and then moved to Repaired Items, you must restore the item from Repaired Items and specify the location where to restore it.

Scan

Scan a Floppy Disk	Scan floppy disks and other removable media.
Scan Computer	Scan a file, folder, drive, or entire computer at any time (see page 24).

Configure

- File System Realtime Protection** Whenever you access, copy, save, move, or open a file, it is examined to make sure it is not infected (see page 23).
- Email Realtime Protection** For groupware email clients, Norton AntiVirus includes additional protection for email attachments (Lotus Notes, Lotus cc:Mail, and Microsoft Exchange clients).

Histories

- Virus History** View a list of the viruses that have infected your computer with additional relevant information about the infection.
- Scan History** Keep track of the scans that have occurred on your computer over time. Scans are displayed with additional relevant information about the scans.
- Event Log** View a log of virus protection-related activities on your computer, including configuration changes, errors, and virus definitions file information.

Startup Scans

- New Startup Scan** Some users supplement a scheduled scan with an automatic scan whenever they start their computer. Often, a Startup Scan is restricted to critical, high-risk folders, such as the Windows folder and folders that store Word and Excel templates (see page 24).

Custom Scans

- New Custom Scan** If you regularly scan the same set of files or folders, you can create a Custom Scan restricted to just those items. At any time, you can quickly verify that the specified files and folders are virus free (page 27).

Scheduled Scans

New Scheduled Scan

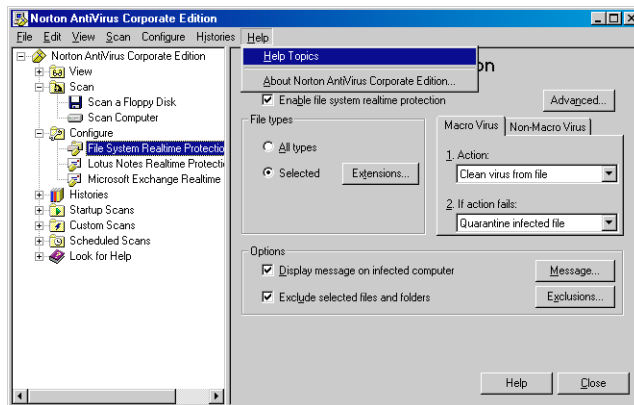
Schedule a scan of your hard disks that runs at least once per week. A scheduled scan confirms that your computer remains virus-free (see page 25).

Getting help

The Norton AntiVirus online help system has general information and step-by-step procedures to help you keep your computer safe from viruses.

To get help using Norton AntiVirus, do one of the following:

- In any Norton AntiVirus pane, click the Help button.
- From the Help menu, choose Help Topics.



If you are connected to the Internet, you can visit the Symantec AntiVirus Research Center (SARC) to view the Virus Encyclopedia, which contains information about all known viruses, find out about virus hoaxes, and read white papers about viruses and virus threats in general.

To visit the Symantec AntiVirus Research Center:

- On the Windows taskbar, click Start, point to Programs, point to Norton AntiVirus Corporate Edition, and click Symantec AntiVirus Research Center.

Keeping virus protection current

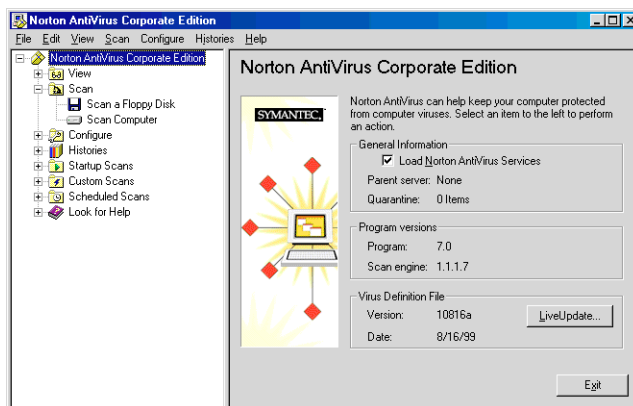
Norton AntiVirus relies on up-to-date information to detect and eliminate viruses. One of the most common reasons virus problems occur is that virus definitions files are not updated after installation. Symantec supplies updated virus definitions files that contain the necessary information about all newly discovered viruses at least weekly. Make it a practice to update virus definitions once per month at a minimum. Scheduling LiveUpdate to run automatically is the easiest way not to forget. Always update immediately if a new virus scare is reported.

Using LiveUpdate

With LiveUpdate, Norton AntiVirus connects automatically to a special Symantec Internet site and determines if virus definitions need updating. If so, it downloads the proper files and installs them in the proper location. LiveUpdate also checks for and downloads program patches to Norton AntiVirus Corporate Edition, if available. Generally, you do not have to do anything to configure LiveUpdate. The only requirement is an Internet connection.

To update virus protection immediately:

- 1 Open Norton AntiVirus.
- 2 In the left pane, click Norton AntiVirus Corporate Edition.
- 3 In the right pane, click the LiveUpdate button.

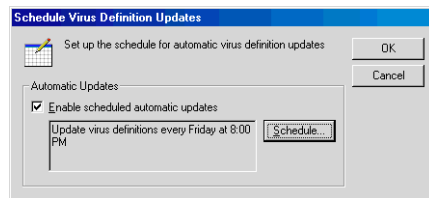


- 4 Click Next to start the automatic update.

Note: If necessary, you can configure the LiveUpdate Internet connection or specify a proxy server. Click Options in the LiveUpdate panel or open Settings >Control Panel >LiveUpdate from the Windows Start menu.

To schedule automatic LiveUpdates:

- 1 Open Norton AntiVirus.
- 2 From the File menu, choose Schedule Updates.
- 3 Check Enable Scheduled Automatic Updates.



- 4 Click Schedule to specify the frequency, day, and time for the LiveUpdate to run.

Note: In a centrally managed network, your administrator may roll out updated virus definitions to workstations. In this case, you do not have to do anything.

Updating without LiveUpdate

Symantec supplies a special program called Intelligent Updater if you cannot use LiveUpdate. You can download the updates from the SARC Web site (see “[To visit the Symantec AntiVirus Research Center:](#)” on page 19). If you don’t have a modem or Internet connection, you can get the updates by mail. Information is included in the Service and Support Solutions in this guide.

To install the latest virus definitions:

- 1 Do one of the following:
 - Download the Intelligent Updater program to any folder on your computer.
 - Insert the disk you received from Symantec in the A: drive.

- 2 From a My Computer or Windows Explorer window, locate and then double-click the Intelligent Updater program.
- 3 Follow all prompts displayed by the update program.
The Intelligent Updater program searches your computer for Norton AntiVirus, then installs the new virus definitions files in the proper folder automatically.
- 4 Scan your disks to make sure newly discovered viruses are detected.

Managing Realtime Protection

File System Realtime Protection is your best defense against virus attack. Whenever you access, copy, save, move, or open a file, Realtime Protection scans the file to ensure that a virus has not attached itself.

To supplement File System Realtime Protection if you use a groupware email client, Norton AntiVirus detects it at install and includes Realtime Protection for email attachments as well. Protection is provided for the following email clients:

- Lotus Notes 4.5x and 4.6
- Lotus cc:Mail 8.0 and 8.01
- Microsoft Exchange 5.0, Microsoft Outlook 97, and Microsoft Outlook 98 (MAPI only, not Internet)

Norton AntiVirus scans only the attachments associated with email. There is no need to scan the message itself, as mail messages are not subject to computer viruses.

Turning File System Realtime Protection off temporarily

Every time you start your computer, File System Realtime Protection makes sure your computer remains virus free. Sometimes, however, you are told to disable your antivirus software when you are installing new computer programs. In this case, you disable File System Realtime Protection temporarily and then turn it back on again.

To turn off File System Realtime Protection temporarily:



- On the taskbar in the lower-right corner of your Windows desktop, right-click the Norton AntiVirus icon, then click to uncheck Enable File System Realtime Protection.

To turn on File System Realtime Protection:

- On the taskbar in the lower-right corner of your Windows desktop, right-click the Norton AntiVirus icon, then click to check Enable File System Realtime Protection.

In some configurations, the Norton AntiVirus icon is not displayed on the taskbar in the lower-right corner of your Windows desktop. In this case, open Norton AntiVirus (see [“Opening Norton AntiVirus”](#) on page 16), click Configure in the left pane, click File System Realtime Protection in the right pane, and check or uncheck Enable File System Realtime Protection.

Increasing File System Realtime Protection

Norton AntiVirus File System Realtime Protection is preset to scan only files commonly at risk of infection. Norton AntiVirus completes scans faster by scanning only files with selected extensions, such as .EXE, .COM, .DLL, .DOC, and .XLS. This is an efficient way to scan because viruses affect only certain file types.

In a high-risk environment or after you’ve been subjected to a virus attack, you may decide to increase File System Realtime Protection to scan all files, regardless of extension.

To change File System Realtime Protection settings:

- 1 Open Norton AntiVirus.
- 2 In the left pane, click Configure.
- 3 In the right pane, click File System Realtime Protection.
- 4 In the File Types group box, select All Types.
- 5 Click Close to save your settings.

Scanning for viruses

In addition to File System Realtime Protection, which is your most powerful defense against virus infection, Norton AntiVirus supplies several different types of scans to provide additional protection:

- On-demand scans: Scan a file, folder, drive, or entire computer at any time.
- Scheduled scans: Run unattended at a specified frequency.

- Startup scans: Run every time you start your computer and Windows loads.
- Custom scans: Scan specified file sets at any time.

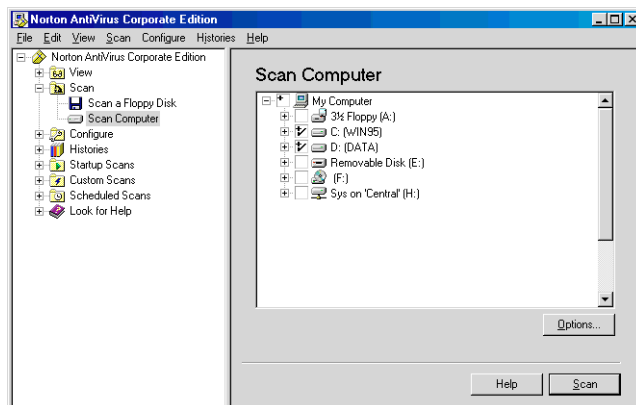
A single, weekly Scheduled Scan of all files is generally sufficient protection, as long as File System Realtime Protection is always running. If your computer is victimized by viruses, consider adding a Startup Scan or daily Scheduled Scan. Another good habit is to always scan floppy disks when first used, particularly if they have been circulating.

On-demand scans

You can scan for viruses at any time. Select anything from a single file to a floppy disk to your entire computer.

To initiate a scan:

- 1 Open Norton AntiVirus.
- 2 In the left pane, click Scan and choose one of the following:
 - Scan A Floppy Disk
 - Scan Computer



- 3 Check boxes in the tree control specify where to scan. You can check anything from the entire computer to a single file.
 - Double-click to open or close a drive or folder.

- Click the check box to select or deselect items. The symbols mean the following:



The file, drive, or folder is not selected. If the item is a drive or folder, the folders and files in it are also not selected.



The individual file or folder is selected.



The individual folder or drive is selected. All items within the folder or drive are also selected.



The individual folder or drive is not selected, but one or more items within the folder or drive is selected.

- 4 If desired, click Options to change to default settings for what is scanned and how to respond if a virus is detected.

Generally, it is not necessary to change any of these settings. The preset options are to scan all files, clean the virus from an infected file, and to Quarantine the infected file if the virus cannot be removed.

- 5 Click Scan.

Norton AntiVirus begins the scan and reports the results.

Note: If you change settings, they only apply to the current scan. If you want the settings to apply to all future scans, click the Save Settings button.

If desired, you can easily scan a single file without opening the Norton AntiVirus program.

To scan a single item:

- 1 From a My Computer or Explorer window, right-click a file, folder, or drive.
- 2 Choose Scan For Viruses from the popup menu.

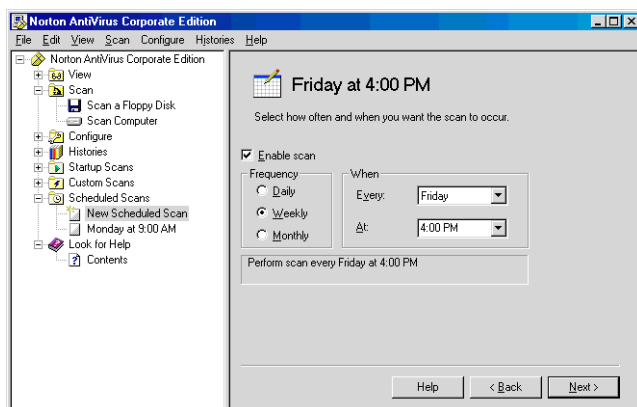
Scheduled scans

A scheduled scan is an important component of virus protection. At the very least, schedule a scan to run once per week to ensure that your computer remains virus-free.

To schedule a scan:

- 1 Open Norton AntiVirus.
- 2 In the left pane, click Scheduled Scans.

- 3 In the right pane, click New Scheduled Scan.
- 4 Enter a name and description for the scan, then click Next.
For example, call the scan “Friday at 4.”
- 5 Specify the frequency for the scan, then click Next.



- 6 Check boxes in the tree control to specify where to scan. You can check anything from the entire computer to a single file. See [“On-demand scans”](#) on page 24 for directions.
- 7 If desired, click Options to change to default settings for what is scanned and how to respond if a virus is detected.

Generally, it is not necessary to change any of these settings. The preset options are to scan all files, clean the virus from an infected file, and to Quarantine the infected file if the virus cannot be removed.

Note: If you change settings, they apply only to the scan you are scheduling.

- 8 Click Save.
Your computer must be turned on when the scan is scheduled to take place.

Startup scans

Some users supplement a scheduled scan with an automatic scan whenever they start their computer. Often, a Startup Scan is restricted to critical, high-risk folders, such as the Windows folder and folders that store Word and Excel templates.

To configure a Startup Scan:

- 1 Open Norton AntiVirus.
- 2 In the left pane, click Startup Scans then click New Startup Scan.
- 3 Enter a name and description for the scan, then click Next.
- 4 Check boxes in the tree control to specify where to scan. You can check anything from the entire computer to a single file. See [“On-demand scans”](#) on page 24 for directions.
- 5 If desired, click Options to change to default settings for what is scanned and how to respond if a virus is detected.

Generally, it is not necessary to change any of these settings. The preset options are to scan all files, clean the virus from an infected file, and to Quarantine the infected file if the virus cannot be removed.

Note: If you change settings, they apply only to the scan you are configuring.

- 6 Click Save.
The scan will run every time you start your computer and Windows loads.

Custom scans

If you regularly scan the same set of files or folders, you can create a Custom Scan restricted to just those items. At any time, you can quickly verify that the specified files and folders are virus free.

To configure a Custom Scan:

- 1 Open Norton AntiVirus.
- 2 In the left pane, click Custom Scans then click New Custom Scan.
- 3 Enter a name and description for the scan, then click Next.
- 4 Check boxes in the tree control to specify where to scan. You can check anything from the entire computer to a single file. See [“On-demand scans”](#) on page 24 for directions.
- 5 If desired, click Options to change to default settings for what is scanned and how to respond if a virus is detected.

Generally, it is not necessary to change any of these settings. The preset options are to clean the virus from file and to Quarantine the infected file if the virus cannot be removed.

Note: If you change settings, they apply only to the scan you are configuring.

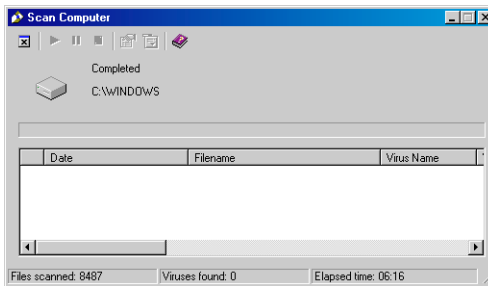
- 6 Click Save.

To run a Custom Scan:

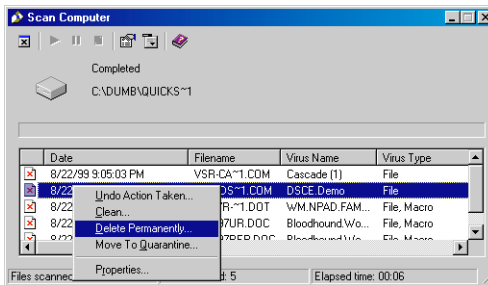
- 1 Open Norton AntiVirus.
- 2 Click Custom Scans and double-click the saved Custom Scan.

Interpreting scan results

Whenever a scan runs—on-demand, scheduled, startup, or custom—Norton AntiVirus displays a dialog to report progress. You can pause, restart, or stop the scan. At the completion of the scan, results are reported. If no viruses were detected, the list box is blank and the status is, simply, Completed.



If viruses are detected during the scan, the dialog includes the name of the infected file, the name of the virus, and the action taken. An alert is also generated, by default, whenever a virus is detected.



In addition to the preset actions set when you configured the scan, you can act on any infected files directly in the scan results dialog box.

To act on an infected file:

- 1 Right-click a file to display the actions popup menu.
- 2 Choose one of the following actions:
 - Undo Action Taken: If possible, reverses the preset action response.
 - Clean: Removes the virus from the file.
 - Delete Permanently: Deletes the infected file.
 - Move To Quarantine: Places the infected file in the Quarantine.
 - Properties: Displays information about the virus.

Depending on the preset action for a virus detection, your selection may not be able to be performed.

Note: In a managed network, the scan dialog may not appear for an administrator-scheduled scan. Similarly, your administrator may choose not to display alerts when a virus is detected.

Managing the Quarantine

Sometimes Norton AntiVirus detects an unknown virus that can't be eliminated with the current set of virus definitions. Or, you have a file you think is infected that is not being detected. The Norton AntiVirus Quarantine safely isolates virus-infected files on your computer. A virus in a quarantined item cannot spread.

Files are placed in the Quarantine in one of two ways:

- Norton AntiVirus is configured to move infected items detected during Realtime Protection or a scan to the Quarantine.
- You manually select a file and add it to the Quarantine.

The Norton AntiVirus preset options for Realtime Protection and all scan types are to clean a virus from an infected file on detection, but to place the file in the Quarantine if it cannot be cleaned.

To manually add a file to the Quarantine:

- 1 Open Norton AntiVirus.
- 2 In the left pane, click View.



- 3 In the right pane, click Quarantine.
- 4 Click the Move To Quarantine button.
- 5 Locate the file and click Add.

Treating files in the Quarantine

If a file is placed in the Quarantine, the first step is to update your virus definitions and scan again. If the virus still can't be removed, the infected file should be submitted to the Symantec AntiVirus Research Center for analysis. The unique Scan and Deliver technology makes this task effortless. New virus definitions files will be developed to detect and clean the virus from the file and returned to you by email. After the new definitions are installed, you can scan the file once more.

To rescan a file isolated in the Quarantine:

- 1 Open Norton AntiVirus.
- 2 Update your virus definitions.
See ["Keeping virus protection current"](#) on page 20.
- 3 In the left pane, click View.
- 4 In the right pane, click Quarantine.
- 5 Select the file in the Quarantine listing and do one of the following:
 - Right-click the file and choose Clean from the popup menu.
 - Click the Clean button.
- 6 Click Start Clean.



The file is scanned again with the new definitions and replaced at its original location.

Note: In a managed network, virus definitions updates are usually rolled out by your network administrator. Your local Quarantine will be aware when updated virus definitions arrive and will take an automatic action configured by your administrator. For example, the action may be to silently scan, clean, and restore files from your Quarantine.

Occasionally, a clean file does not have a location to be returned to. For example, an infected attachment may have been stripped from an email and placed in the Quarantine. In this special circumstance, the cleaned file is placed in Repaired Items instead. You must release the file and specify a location.

To release a cleaned file from Repaired Items:

- 1 Open Norton AntiVirus.
- 2 In the left pane, click View.
- 3 In the right pane, click Repaired Items.
- 4 Right-click the file and choose Restore from the popup menu.
- 5 Specify the location for the cleaned file.

Clearing Backup Items

As a data safety precaution, Norton AntiVirus is configured to make a backup copy of an infected item before attempting a repair. After an infected item has been successfully cleaned, you should delete it from Backup Items because the backup is still infected.

To clear Backup Items:

- 1 Open Norton AntiVirus.
- 2 In the left pane, click View.
- 3 In the right pane, click Backup Items.
- 4 Select the file in the Backup Items listing and do one of the following:
 - Right-click the file and choose Delete Permanently from the popup menu.
 - Click the Delete button.



Submitting a potentially infected file to SARC for analysis

Sometimes, Norton AntiVirus cannot clean a virus from a file. Or, you suspect a file is infected and is not being detected. The Symantec AntiVirus Research Center (SARC) will analyze your file to make sure it is not infected. If a new virus is discovered in your submission, SARC will create and send you special updated virus definitions to detect and eliminate the new virus. You must have an Internet connection to submit a sample and an email address to receive a reply.

Note: In a managed network, submissions to SARC are usually handled by your network administrator from a centralized network Quarantine. In this case, the Submit To SARC button will not appear in your workstation version of Norton AntiVirus.

To submit a file to SARC from the Quarantine:

- 1 Open Norton AntiVirus.
- 2 In the left pane, click View.
- 3 In the right pane, click Quarantine.
- 4 Select the file in the list of quarantined items and click the Submit To SARC button.



Follow the directions in the wizard to collect the necessary information and submit the file for analysis.

You are notified by email with the results of the analysis, and, if appropriate, updated virus definitions.

Setting an exclusion

Rarely, a file that does not contain a virus is detected as infected. A false positive occurs when Norton AntiVirus detects remnants of virus code in files that have been partially cleaned, for example, by other virus protection programs. The virus signatures remain in a partially cleaned file, but the harmful virus code has been removed and rendered harmless. However, Norton AntiVirus continues to detect the virus signature in the clean file, and notifies you each time the file is scanned that the file is infected.

Exclusions are items that you don't want or need to include in a scan. Excluding files from a scan is useful when you suspect that a scan is detecting false positives on your computer.

You set exclusions separately for type of scan: Realtime Protection, On-demand Scans, Scheduled Scans, Startup Scans, or Customs Scans. The procedure, however, is the same.

To exclude a file from a scan:

- 1 Do one of the following:
 - For Realtime Protection, click Configure in the left pane and then click File System Realtime Protection in the right pane.
 - For all other scan types, click Options in the pane where you specify what to scan.
- 2 Check the Exclude Files And Folders option.
- 3 Click the Exclusions button to specify the file to exclude.

Be careful with exclusions. If you exclude a file from a scan, no action will be taken to clean it if the file later becomes infected. This could be a potential risk to the security of your computer.

Symantec Service and Support Solutions

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

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

Registering your Symantec product

You can register your Symantec product in the following ways:

- Complete the registration card included with your package and drop the card in the mail.
- Register via modem during the installation process (if your software offers this feature).
- Visit the Symantec web site at:
<http://www.symantec.com/>
- Fax your registration to (800) 800-1438 or (541) 984-8020.

Virus definitions update disk

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

To order, do one of the following:

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

Technical support

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

World Wide Web

The Symantec World Wide Web site (<http://service.symantec.com>) is the portal to an array of customer-centered solutions. These solutions include the services listed below.

Product knowledge bases

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

Ask Symantec

Ask Symantec discussion groups provide a forum where you can ask questions and receive answers from Symantec online Customer and Technical Support Specialists.

File downloads

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

Other technical support options

Other Symantec support options include the following:

Automated fax retrieval system To receive general product information, fact sheets and product upgrade order forms directly to your fax machine, please call our Customer Service fax retrieval system at (800) 554-4403 or (541) 984-2490.

For technical application notes, please call our Technical Support fax retrieval system at (541) 984-2490 and select option 2.

StandardCare Support If you can't access the Internet, take advantage of your 90 days of free telephone technical support (from the date of your first call) at no charge to all registered users of Symantec software.

Please see the back of this manual for the support telephone number for your product.

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

Support for old and discontinued versions

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

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

Customer Service

You can contact Customer Service online at:

<http://service.symantec.com/>

Customer Service can assist you with non-technical questions, such as:

- Subscribing to the Symantec Support Solution of your choice.
- Obtaining product literature or trialware.
- Locating resellers and consultants in your area.
- Replacing missing or defective CD-ROMs, disks, manuals, and so on.
- Updating your product registration with address or name changes.
- Getting order, return, or rebate status information.

- Accessing Frequently Asked Questions, or FAQs.
- Posting questions to the Customer Service newsgroup.

You can also call Customer Service at (800) 441-7234.

Upgrade Orders

For upgrade orders, please call the Customer Service Order Desk at (800) 568-9501.

Or, you can visit the upgrade center online at:

<http://www.symantec.com/upgrades/>

Worldwide Service and Support

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

Or, you can get more information at <http://www.symantec.com/>.

Service and Support offices

NORTH AMERICA

Symantec Corporation
175 W. Broadway
Eugene, OR 97401

<http://www.symantec.com/>

(800) 441-7234 (USA & Canada)
(541) 334-6054 (all other locations)
Fax: (541) 984-8020

Automated Fax Retrieval

(800) 554-4403
(541) 984-2490

EUROPE, MIDDLE EAST, AFRICA

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

http://www.symantec.com/region/reg_eu/
+353 (1) 811 8032
Fax: +353 (1) 811 8033

Automated Fax Retrieval +31 (71) 408 3782

ASIA/PACIFIC RIM

Symantec Australia Pty. Ltd.
408 Victoria Road
Gladesville, NSW 2111
Australia

http://www.symantec.com/region/reg_ap/
+61 (2) 9850 1000
Fax: +61 (2) 9850 1001

Automated Fax Retrieval +61 (2) 9817 4550

LATIN AMERICA

Symantec América Latina
Oficina principal
2500 Broadway, Suite 200
Santa Monica, CA 90404

<http://www.symantec.com/region/mx/>
(310) 449-7086
Fax: (310) 449-7576

BRAZIL

Symantec Brazil
Av. Juruca, 302 - cj 11
São Paulo - SP
04080 011
Brazil

<http://www.symantec.com/region/br/>
+55 (11) 5561 0284
Fax: +55 (11) 5530 8869

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

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

Norton AntiVirus™ Corporate Edition

CD Replacement Form

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

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: _____

Disk 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
175 West Broadway
Eugene, OR 97401-3003

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



I N D E X

A

antivirus policy, setting 12-13

B

Backup Items folder
about 31
clearing 31

C

clients, migrating 13
custom scans
about 23
configuring 27-28

E

excluding a file from a scan 32
exclusions
about 32
setting 32

L

LiveUpdate
immediate update 20
scheduled update 21
Lotus ccMail Realtime Protection 22
Lotus Notes Realtime Protection 22

M

managed clients
benefits 11
differences from standalone clients 16
Microsoft Exchange Realtime Protection 22
migrating
clients 13
servers 14

N

Norton AntiVirus
how it works 7
opening 16

O

on-demand scans
about 23
initiating 24-25
opening Norton AntiVirus 16

Q

Quarantine
about 29
manually adding files 29
rescanning files 30
treating files 30

R

Realtime Protection
about 22
antivirus policy 13
disabling temporarily 22
groupware email clients 22
increasing 23
Repaired Items folder
about 30
releasing items 31
rescanning files in Quarantine 30

S

SARC
about 8
accessing 19
submitting files to 31-32
scan results, interpreting 28-29

- scanning
 - custom 27-28
 - on-demand 24-25
 - quick scan of single items 25
 - scheduled 25-26
 - startup 26-27
- scheduled scans
 - about 23
 - scheduling 25-26
- servers, migrating 14
- setting antivirus policy 12-13
- standalone clients
 - benefits of managed clients 11
 - differences from managed clients 16
- startup scans
 - about 23
 - configuring 26-27
- submitting files to SARC 31-32
- Symantec AntiVirus Research Center. *See* SARC

U

- updating virus protection
 - immediately 20
 - scheduling 21
 - without LiveUpdate 21

V

- viruses
 - about 7
 - keeping protection current 20-21