Norton AntiVirus™ Corporate Edition User's Guide

Norton AntiVirus™ Corporate Edition

Norton AntiVirus™ Corporate Edition User's Guide

Copyright Notice

Trademarks

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

SYMANTEC LICENSE AND WARRANTY

NOTICE:

Symantec licenses the accompanying 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 continuing installation, as pressing the "Yes" button will indicate your assent to them. If you do not agree to these terms, please press the "No" button to exit install as 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 licensers 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 one copy of the Software 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:

All Symantec products and documentation are commercial in nature. The Software and documentation are "Commercial Items", as that term is defined in 48 C.F.R. §2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms are defined in 48 C.F.R. §252.227-7014(a)(5) and 48 C.F.R. §252.227-7014(a)(1), and used in 48 C.F.R. §12.212 and 48 C.F.R. 227.7202, as applicable. Consistent with 48 C.F.R. §12.212, 48 C.F.R. §252.227-7015, 48 C.F.R. §227.7202 through 227.7202-4, 48 C.F.R. §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 Boulevard, 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, 20330 Stevens Creek Boulevard, Cupertino, CA 95014.

C O N T E N T S

Index

CHAPTER 1

Introducing Norton AntiVirus Corporate Edition

This chapter includes the following:

- How the User's Guide is organized
- How Norton AntiVirus prevents infections
- About Symantec Security Response

How the User's Guide is organized

The *Norton AntiVirus Corporate Edition User's 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 for Desktops client program is installed on all Win32 computers for standalone protection (Windows 9x/Me/NT 4.0/2000/XP computers). A separate program, not discussed in this guide, protects Windows 3.x and DOS computers.

How Norton AntiVirus prevents infections

A virus is a computer program designed so that, when run, it attaches a copy of itself to another computer program or document. Thereafter, whenever the infected program is run or a document containing a macro virus 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 Web 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 anti-virus 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.

About Symantec Security Response

The strength behind Norton AntiVirus Corporate Edition is Symantec Security Response, formerly known as 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. Symantec Security Response 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, Symantec Security Response has developed automated software analysis tools. With direct submissions over the Internet of infected files from your Norton AntiVirus Quarantine to Symantec Security Response, the time from discovery, analysis, and return cure by email is shrinking from days to hours, and in the near future, to minutes.

CHAPTER 2

Managing Norton AntiVirus Corporate Edition

This chapter is intended primarily for network administrators who manage Norton AntiVirus Corporate Edition for Desktops on client computers.

This chapter includes the following:

- Benefits of a managed solution
- Setting anti-virus policy
- Changing a client from unmanaged to managed protection
- Changing a client from managed to unmanaged protection

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 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 scheduled times of the day. They can also be scanned when a virus sweep is run. Centralized virus scanning provides a convenient

solution for network users who do not have time to regularly scan their computers for viruses, and for network administrators who are assured that their networks remain protected against virus attacks.

- Symantec Central Quarantine for virus-infected files: This benefit provides an automated response to heuristically detected new or unrecognized viruses. Copies of infected items are forwarded automatically from the Quarantine on the client computer to the Central Quarantine. Either Internet-based or Email-based Scan and Deliver transports the infected items from the Central Quarantine to Symantec Security Response, which develops and returns updated virus definitions.

  The Internet-based method provides a fully automated, closed-loop virus submission and definitions delivery system; new virus definitions are produced and returned for immediate deployment to the infected computer or the whole organization without IT intervention. Additionally, realtime status of virus submissions to Symantec and definitions deployment to infected endpoints is available from the Central Quarantine console.

- Convenient update options for networked computers: These options 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 if the administrator has selected the Virus Definition Transport Method to update computers.

  For more information, see the *Norton AntiVirus Corporate Edition Implementation Guide*.

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

- Enabling and disabling File System Realtime Protection
- Enabling and disabling Lotus Notes, or Microsoft Exchange Realtime Protection, if installed
- Creating and running scheduled scans
- Creating and running manual scans and virus sweeps
- 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 protect the network against virus invasions without slowing the normal performance of the network.

Setting anti-virus 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

Choosing what to scan

Norton AntiVirus File System Realtime Protection scans all file types by default. Manual, scheduled, custom, and startup scans also examine all file types by default. You can choose to scan files by file extension or by type of file (documents and programs) but your protection from viruses is reduced.

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, the backup action is to move the infected file to the Quarantine so that the virus cannot spread.

Depending on your anti-virus policy, you can change these settings to delete on detection or leave alone (log only). For File System Realtime Protection, you can also choose to deny access. In addition, you can set different actions for macro and nonmacro viruses for each scan type separately.

Changing a client from unmanaged to managed protection

For Windows 9x/Me/NT 4.0/2000/XP computers, do one of the following to convert unmanaged Norton AntiVirus Corporate Edition clients to managed clients:

- Copy the Grc.dat file from the parent server to each client computer that you want the parent server to manage.

  Grc.dat contains data for communication between the server and client.
- Reinstall Norton AntiVirus Corporate Edition over the existing client installations by whatever mechanism you use to manage your network Norton AntiVirus rollout.

The Norton AntiVirus Corporate Edition standalone client for Windows 3.x/DOS is a different program than the managed client. You must uninstall the standalone client for Windows 3.x/DOS before rolling out the managed client.

If the Norton AntiVirus Corporate Edition standalone client is installed on a server that you want to migrate to management capabilities, you must first uninstall the standalone client. You can then install the server version of Norton AntiVirus as part of your Norton AntiVirus Corporate Edition rollout. You cannot install the server version over an existing standalone client installation.

For more information, see the *Norton AntiVirus Corporate Edition Implementation Guide*.

Changing a client from managed to unmanaged protection

There are two ways to convert managed clients to unmanaged clients:

- Uninstall and reinstall Norton AntiVirus Corporate Edition.
- Use a text editor (such as Notepad) to edit the client's Grc.dat file.

For more information, see the *Norton AntiVirus Corporate Edition Implementation Guide*.

C H A P T E R 3

Using Norton AntiVirus Corporate Edition

This chapter is intended for users of Norton AntiVirus Corporate Edition for Desktops on Windows 9x/Me/NT 4.0/2000/XP computers.

This chapter includes the following:

- What Norton AntiVirus Corporate Edition does
- Getting started
- Keeping virus protection current
- Managing Realtime Protection
- Scanning for viruses
- Managing the Quarantine

What Norton AntiVirus Corporate Edition does

Norton AntiVirus Corporate Edition 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 Internet-borne viruses—File System Realtime Protection scans program and document files automatically as they are downloaded.

Norton AntiVirus Corporate Edition responds to infected files with actions and backup actions. When a virus is detected during a scan, Norton AntiVirus Corporate Edition, 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 Corporate Edition cannot clean the file, Norton AntiVirus Corporate Edition attempts the backup action, moving the infected file to the Quarantine so that the virus cannot spread.

For more information, see "Setting anti-virus policy" on page 13.

Getting started

Your Norton AntiVirus Corporate Edition virus protection may be either a standalone or an administrator-managed installation. The procedures in this chapter assume a standalone installation with the preset or default option settings. Your network administrator will advise you as to what tasks you should perform using Norton AntiVirus Corporate Edition.

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 anti-virus policy.

Opening Norton AntiVirus Corporate Edition

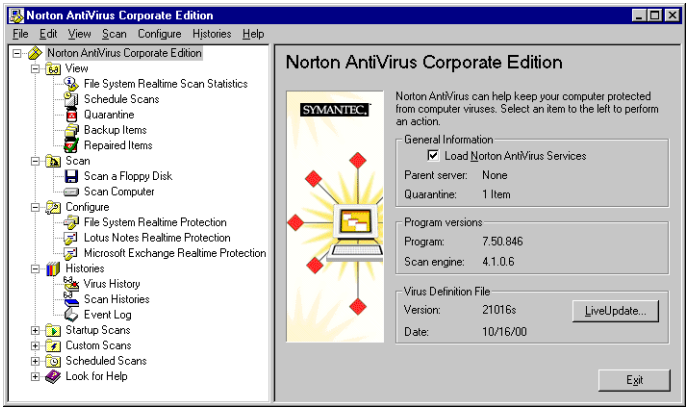
You can open Norton AntiVirus Corporate Edition several ways.

To open Norton AntiVirus Corporate Edition

- Do one of the following:
  - On the Windows taskbar, double-click **Norton AntiVirus Corporate Edition**.
  - On the Windows taskbar, click **Start** > **Programs** > **Norton AntiVirus Corporate Edition** > **Norton AntiVirus Corporate Edition**.

Navigating in Norton AntiVirus Corporate Edition

The Norton AntiVirus Corporate Edition main window is divided into two panes. 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 right pane responds with the information you need to perform a task.



To navigate in the left pane, do any of the following:

- Click a plus sign to expand a folder.
- Click a minus sign to collapse a folder.
- Click an item to access the information in the right pane.

View

File System Realtime Scan Statistics	View statistics about the status of realtime scans, including the last file that was scanned (even if it wasn't infected).
Schedule 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. For more information, see "Rescanning files in the Quarantine" on page 34.
Backup Items	Delete backup copies of infected files. As a data safety precaution, Norton AntiVirus Corporate Edition makes a backup copy of infected items before attempting a repair. After verifying that Norton AntiVirus Corporate Edition cleaned an infected item of viruses, you should delete the copy in Backup Items. For more information, see "Clearing Backup Items" on page 36.
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 moved to Repaired Items, you must restore the item from Repaired Items and specify the location to which 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. For more information, see "Using on-demand scans" on page 26.

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. For more information, see "Modifying File System Realtime Protection" on page 25.
Lotus Notes Realtime Protection and Microsoft Exchange Realtime Protection	For groupware email clients, Norton AntiVirus Corporate Edition includes additional protection for email attachments (Lotus Notes 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 Histories	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 computers. Often, a Startup Scan is restricted to critical, high-risk folders, such as the Windows folder and folders that store Word and Excel templates. For more information, see "Using on-demand scans" on page 26.

Custom Scans

New Custom Scan

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

For more information, see "Configuring Custom Scans" on page 31.

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.

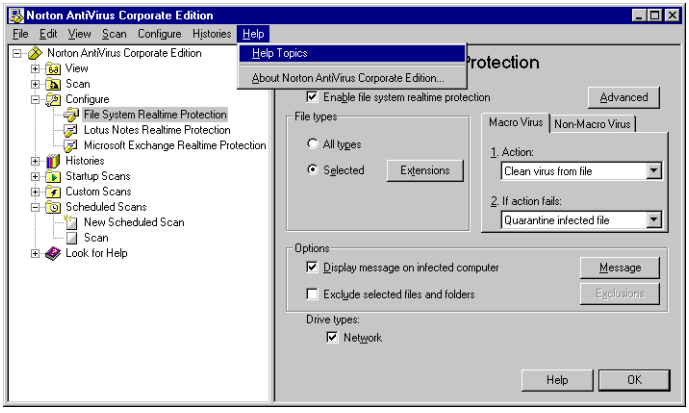
For more information, see "Scheduling scans" on page 28.

Getting help

The Norton AntiVirus Corporate Edition 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 Corporate Edition

- Do one of the following:
  - In the Norton AntiVirus Corporate Edition main window, click **Help**.
  - On the Help menu, click **Help Topics**.



If you are connected to the Internet, you can visit the Symantec Security Response (formerly known as Symantec AntiVirus Research Center) Web site 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 Security Response Web site

- In your Internet browser, type the following Web address:

  securityresponse.symantec.com

Keeping virus protection current

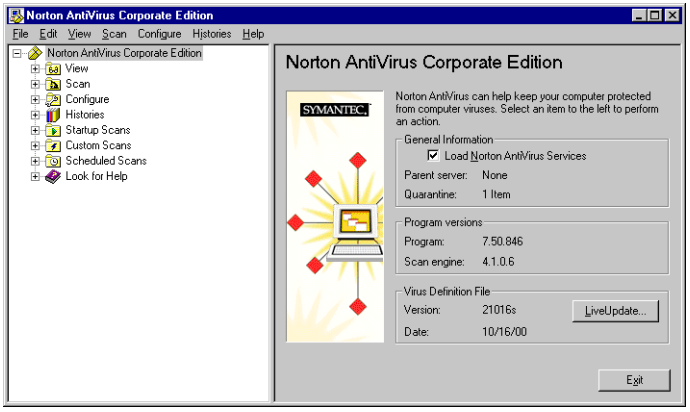
Norton AntiVirus Corporate Edition relies on up-to-date information to detect and eliminate viruses. One of the most common reasons virus problems occur is that virus definitions files are not updated after installation. Symantec supplies updated virus definitions files that contain the necessary information about all newly discovered viruses at least weekly. Make it a practice to update virus definitions once per week 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.

Updating virus protection with LiveUpdate

With LiveUpdate, Norton AntiVirus Corporate Edition connects automatically to a special Symantec Web 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 Corporate Edition.
2. In the left pane, click **Norton AntiVirus Corporate Edition**.
3. In the right pane, click **LiveUpdate**.

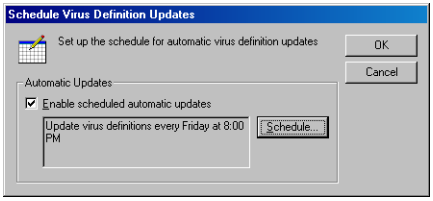


4. If necessary, select the method by which you want to connect to the LiveUpdate server.
5. Click **Next** to start the automatic update.

Note: If necessary, you can configure the LiveUpdate Internet connection or specify a proxy server. To do so, open LiveUpdate from the Windows Start menu and change the options as appropriate in the LiveUpdate panel.

To schedule LiveUpdates

1. Open Norton AntiVirus Corporate Edition.
2. On the File menu, click **Schedule Updates**.
3. Check **Enable scheduled automatic updates**.



4. Click **Schedule** to specify the frequency, day, and time that you want LiveUpdate to run.

5 Click **Advanced**.

6 To set up Norton AntiVirus Corporate Edition so that scheduled LiveUpdate events that are missed run at a later time, check **Handled Missed Events Within** and set the days.

7 To set up Norton AntiVirus Corporate Edition so that scheduled LiveUpdate events run within a specified time range rather than at a set time, check the type of randomization method that you want to use and set the minute, day of the week, or day of the month.

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 Symantec Security Response Web site.

For more information, see "To visit the Symantec Security Response Web site" on page 21.

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 User's 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 into drive A.

2 In 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 Corporate Edition, 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 Corporate Edition 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, 4.6, and 5.0
- Microsoft Exchange 5.0 and 5.5, Microsoft Outlook 97, Microsoft Outlook 98 (MAPI only, not Internet), and Microsoft Outlook 2000

Norton AntiVirus Corporate Edition scans only the attachments associated with email. There is no need to scan the message itself.

Turning File System Realtime Protection off temporarily

Every time you start your computer, File System Realtime Protection makes sure your computer is virus-free. Sometimes, however, you are told to disable your anti-virus software when you are installing new computer programs. In this case, 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 the Windows Desktop, right-click **Norton AntiVirus Corporate Edition**, then uncheck **Enable File System Realtime Protection**.

To turn on File System Realtime Protection

- On the taskbar in the lower-right corner of the Windows Desktop, right-click **Norton AntiVirus Corporate Edition**, then check **Enable File System Realtime Protection**.

In some configurations, the Norton AntiVirus Corporate Edition icon is not displayed on the taskbar in the lower-right corner of your Windows Desktop.

To turn File System Realtime Protection on or off when the Norton AntiVirus Corporate Edition icon is not displayed in the taskbar

1. Open Norton AntiVirus Corporate Edition

   For more information, see "Opening Norton AntiVirus Corporate Edition" on page 16.
2. Click **Configure** in the left pane.
3. Click **File System Realtime Protection** in the right pane.
4. Check or uncheck **Enable File System Realtime Protection**.

Modifying File System Realtime Protection

Norton AntiVirus Corporate Edition File System Realtime Protection is preset to scan all files. Scanning all files offers the most protection from viruses.

However, Norton AntiVirus Corporate Edition completes scans faster by scanning only files with selected extensions, such as .exe, .com, .dll, .doc, and .xls. Although this method offers less protection, it is an efficient way to scan because viruses affect only certain file types. The default list of extensions represents those files that are commonly at risk of infection.

To modify File System Realtime Protection

1. Open Norton AntiVirus Corporate Edition.
2. In the Norton AntiVirus main Window, in the left pane, click **Configure**.
3. In the right pane, click **File System Realtime Protection**.
4. In the File Types group box, do one of the following:
   - Click **All Types** to instruct Norton AntiVirus Corporate Edition to scan all files.
   - Click **Selected Extensions** to instruct Norton AntiVirus Corporate Edition to scan only those files that match the listed file extensions. Click **Extensions** to change the default list of file extensions.
5. Click **OK** 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 Corporate Edition supplies several different types of scans to provide additional protection. Scan types include the following:

- 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.

Using on-demand scans

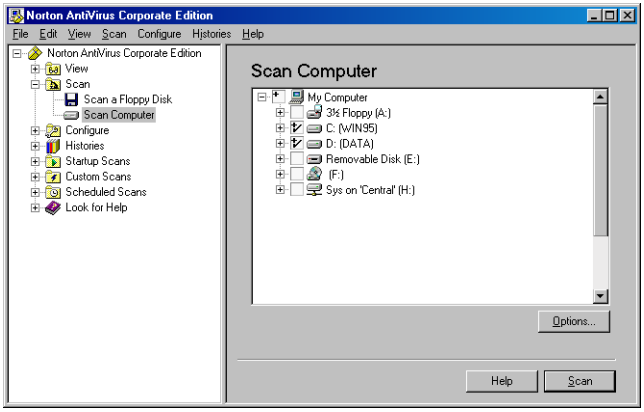
You can scan for viruses at any time. Select anything from a single file to a floppy disk to your entire computer.

To initiate an on-demand scan

1. Open Norton AntiVirus Corporate Edition.
2. In the Norton AntiVirus Corporate Edition main window, in the left pane, click **Scan**.

3 Select one of the following:

- Scan A Floppy Disk (This option is available only when a floppy disk drive is present.)
- Scan Computer



Check boxes in the tree control specify where to scan. You can check anything from the entire computer to a single file.

4 Do one of the following:

- Double-click a drive or folder to open or close it.
- 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 are selected.

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 quarantine the infected file if the virus cannot be removed.

Note: Modified settings only apply to the current scan. To apply the settings to all future scans, click **Save Settings**.

---

6 Click **Scan**.

Norton AntiVirus Corporate Edition begins the scan and reports the results.

You can scan a single file without opening the Norton AntiVirus Corporate Edition program.

To scan a single item

- In a My Computer or Explorer window, right-click a file, folder, or drive, then click **Scan For Viruses**.

Scheduling 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 Corporate Edition.

2 In the Norton AntiVirus Corporate Edition main window, in the left pane, click **Scheduled Scans**.

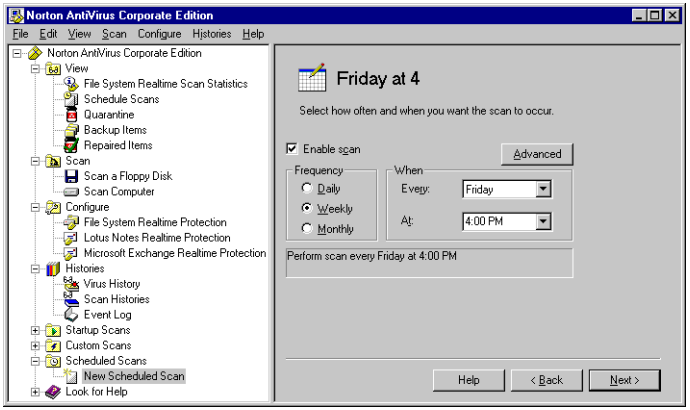
3 In the right pane, click **New Scheduled Scan**.

4 Type a name and description for the scan.

For example, call the scan “Friday at 4.”

5 Click **Next**.

6 Specify the frequency for the scan.



7 Click **Next**.

8 In the tree control, check boxes to specify where to scan.

You can check anything from the entire computer to a single file. For more information, see "Using on-demand scans" on page 26.

9 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 quarantine the infected file if the virus cannot be removed.

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

---

10 Click **Save**.

Your computer must be turned on and Norton AntiVirus Services must be loaded when the scan is scheduled to take place. (By default, Norton AntiVirus Services are loaded when you start your computer.)

To delete a Scheduled Scan

1 Open Norton AntiVirus Corporate Edition.

2 In the Norton AntiVirus Corporate Edition main window, in the left pane, expand the **Scheduled Scans** folder.

3 Right-click the scan that you want to remove, then click **Delete**.

Configuring Startup Scans

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

Note: If you create more than one Startup Scan, the scans will run sequentially in the order that they were created.

To configure a Startup Scan

1. Open Norton AntiVirus Corporate Edition.
2. In the Norton AntiVirus Corporate Edition main window, in the left pane, click **Startup Scans**.
3. Click **New Startup Scan**.
4. Type a name and description for the scan.
5. Click **Next**.
6. In the tree control, check boxes to specify where to scan.

   You can check anything from the entire computer to a single file.

   For more information, see "Using on-demand scans" on page 26.
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: Modified settings apply only to the scan you are configuring.

   ---
8. Click **Save**.

   The scan will run every time you start your computer and Windows loads.

To delete a Startup Scan

1. Open Norton AntiVirus Corporate Edition.
2. In the Norton AntiVirus Corporate Edition main window, in the left pane, expand the **Startup Scans** folder.
3. Right-click the scan that you want to remove, then click **Delete**.

Configuring 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 Corporate Edition.
2. In the Norton AntiVirus Corporate Edition main window, in the left pane, click **Custom Scans**.
3. Click **New Custom Scan**.
4. Type a name and description for the scan.
5. Click **Next**.
6. In the tree control, check boxes to specify where to scan.

   You can check anything from the entire computer to a single file.

   For more information, see "Using on-demand scans" on page 26.
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 clean the virus from an infected file and quarantine the infected file if the virus cannot be removed.

   Note: Modified settings apply only to the scan you are configuring.
8. Click **Save**.

To run a Custom Scan

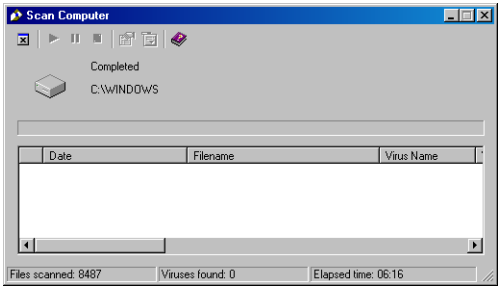
1. Open Norton AntiVirus Corporate Edition.
2. Click **Custom Scans**.
3. Double-click the saved Custom Scan.

To delete a Custom Scan

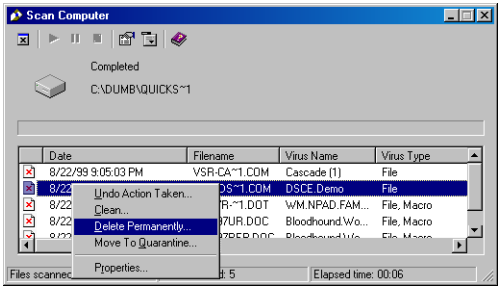
1. Open Norton AntiVirus Corporate Edition.
2. In the Norton AntiVirus Corporate Edition main window, in the left pane, expand the **Custom Scans** folder.
3. Right-click the scan that you want to remove, then click **Delete**.

Interpreting scan results

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



If viruses are detected during the scan, the dialog box 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 pop-up menu.
2. Select 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 box 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 Corporate Edition 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 Corporate Edition 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 Corporate Edition 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 Corporate Edition 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 Corporate Edition.
2. In the Norton AntiVirus Corporate Edition main window, in the left pane, click **View**.
3. In the right pane, click **Quarantine**.
4. Click **Move To Quarantine**.
5. Locate the file, then click **Add**.

Rescanning files in the Quarantine

If a file is placed in the Quarantine, update your virus definitions. After updating the definitions, all files in the Quarantine are scanned automatically. If the virus still can't be removed, submit the infected file to Symantec Security Response for analysis. A new virus definitions file is developed to detect and clean the virus and the file is sent to you by email. After the new definitions file is installed, the files are scanned.

For more information, see "Submitting a potentially infected file to Symantec Security Response for analysis" on page 36.

To rescan a file isolated in the Quarantine

1. Update your virus definitions.

   For more information, see "Keeping virus protection current" on page 21.
2. In the Norton AntiVirus Corporate Edition main window, in the left pane, click **View**.
3. In the right pane, click **Quarantine**.
4. Select the file in the Quarantine listing.
5. Do one of the following:
   - Right-click the file, then on the pop-up menu, click **Clean**.
   - Click **Clean**.
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 the Quarantine.

Occasionally, a clean file does not have a location to which to be returned. 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 Corporate Edition.
2. In the Norton AntiVirus Corporate Edition main window, in the left pane, click **View**.
3. In the right pane, click **Repaired Items**.
4. Right-click the file, then on the pop-up menu, click **Restore**.
5. Specify the location for the cleaned file.

Clearing Backup Items

As a data safety precaution, Norton AntiVirus Corporate Edition 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 Corporate Edition.
2. In the Norton AntiVirus Corporate Edition main window, in the left pane, click **View**.
3. In the right pane, click **Backup Items**.
4. Select the file in the Backup Items listing.
5. Do one of the following:
   - Right-click the file, then on the pop-up menu, click **Delete Permanently**.
   - Click **Delete**.
6. Click **Start Delete**.

Submitting a potentially infected file to Symantec Security Response for analysis

Sometimes, Norton AntiVirus Corporate Edition cannot clean a virus from a file. Or, you suspect a file is infected and is not being detected. Symantec Security Response (formerly known as Symantec AntiVirus Research Center) analyzes your file to make sure it is not infected. If a new virus is discovered in your submission, Symantec Security Response creates and sends 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 Symantec Security Response are usually handled by your network administrator from the Symantec Central Quarantine. In this case, the Submit To SARC button is not available in your workstation version of Norton AntiVirus Corporate Edition. Also, the Submit To SARC button is not available if the administrator configures an unmanaged client to not allow submissions to Symantec Security Response.

To submit a file to Symantec Security Response from the Quarantine

1. Open Norton AntiVirus Corporate Edition.
2. In the Norton AntiVirus Corporate Edition main window, in the left pane, click **View**.
3. In the right pane, click **Quarantine**.
4. Select the file in the list of quarantined items.
5. Click **Submit To SARC**.

   Follow the on-screen instructions 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 Corporate Edition 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 Corporate Edition 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.

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, in the left pane, click **Configure**, then, in the right pane, click **File System Realtime Protection**.
   - For all other scan types, in the pane where you specify what to scan, click **Options**.
2. Check **Exclude Files And Folders**.
3. Click **Exclusions** to specify the file to exclude.
4. To enable prescan exclusions, check **Check File For Exclusion Before Scanning**.

   Different situations determine how this option affects performance. For example:
   - If you copy a large folder that is in the exclusions list and prescan exclusions is enabled, the copying process is shorter since the folder contents are excluded prior to scanning.
   - If you copy over a large folder that is not in the exclusions list, disabling prescan exclusions improves performance.
5. Click **Extensions**.
6. Specify the file types that you want to exclude.

   You can use the ? wildcard to specify any character. For example, XL? excludes .xls, .xlt, .xlw, and .xla files.
7. Click **Files/Folders**.
8. Specify what to exclude.
9. Click **OK**.

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.

I N D E X

R

S

U

V