

Norton AntiVirus™ Corporate Edition Implementation Guide

Norton AntiVirus™ Corporate Edition

Norton AntiVirus™ Corporate Edition Implementation Guide

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.

Documentation version: 7.6

PN: 07-30-00473

Copyright Notice

Copyright © 1999-2001 Symantec Corporation.

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 changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Symantec, the Symantec logo, Symantec AntiVirus, Norton AntiVirus, Norton AntiVirus Corporate Edition, LiveUpdate, Striker, Bloodhound, and Symantec Security Response are trademarks of Symantec Corporation.

Microsoft, Windows, and Windows logo are registered trademarks of Microsoft Corporation.

NetWare is a registered trademark of Novell, Inc. Mac and Mac OS are trademarks of Apple Computer, Inc. OS/2 is a registered trademark of IBM Corporation in the United States and other countries. 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 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 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 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

Section 1 Getting started

Chapter 1 Introduction to Norton AntiVirus Corporate Edition

What's new in Norton AntiVirus Corporate Edition 7.6	21
About Norton AntiVirus Corporate Edition	22
How Norton AntiVirus Corporate Edition works	24
Symantec System Center	24
Alert Management System	24
Server protection	25
Client protection	25
Parent server issues	26
Client configuration types	26
About scanning	28
What you can do with Norton AntiVirus Corporate Edition	28
Establish policies and enforce them	28
Verify protection	28
Manage virus definitions file updates	29
Control live viruses	29
Manage virus protection using virus history, scan history, and event log data	29
Manage groups of computers	30
Manage scanning	30
Virus History, Scan History, and Event Log data	31

Chapter 2 Server groups

About server groups	34
How you can see server groups	34
Primary, secondary, master primary, and parent servers	35
Considerations in server group planning	40
Server group passwords	41
What options are applied when set at the server group level	41

Chapter 3 **Roaming Client Support**

About Roaming Client Support	43
When to use Roaming Client Support	44
How Roaming Client Support works	45
Roaming client management limitations	48
Implementation tasks	48
Requirements	49
Analyzing your network and creating server list text files	49
Using RoamAdmn.exe to set up the roaming servers	52
Load balancing and marking primary and backup servers	53
Specifying a primary server with a list of backup servers	54
Specifying other types of parent servers	55
Rolling out RoamAdmn.exe and the server list text files to administrator computers	56
Setting up Roaming Client Support on each client	57
Running Roaming Client Support as a command line utility	58
Command line switches	58
Related Registry keys	61

Chapter 4 **Other information you need to know before installing**

Planning for network traffic	64
Symantec System Center traffic	64
Server-to-server traffic	65
Client traffic	66
Other sources of traffic	67
The scalability of Norton AntiVirus Corporate Edition	68
How Norton AntiVirus handles scalability issues	69
Where to get more information for scalability planning	70
Required protocols	71
Configuring options and running operations	71
Windows NT/2000 cluster server protection	72
NetWare cluster server protection	73
Product installation order	74
Staged installations	74
Learning about Norton AntiVirus Corporate Edition in a lab setting	75
Procedures for evaluating server components	75
Procedures for evaluating client components	77
Scanning configuration trade offs	78

What to scan	78
Scans based on file type	78
When to scan	80
Default virus handling actions	82
Client email scans	82
Management policy planning	83
Server group locking	83
Event management	83
What else do I need to plan for?	83
How Terminal Servers are protected	84
Viewing Terminal Servers from the console	84
Terminal Server and Terminal Services limitations	84
Preventing user-launched scans	85
Installing AppSec	85
Limiting access to the Norton AntiVirus Corporate Edition	
registry key on Windows NT 4.0 computers	87
Trade-off considerations for the Reset ACL tool	87
Central Quarantine	88
Submit new viruses and get a rapid solution	88
Customer profiles	89
Profile 1: Medium-sized organization	89
Profile 2: Large organization	92
Profile 3: Enterprise-sized organization	98

Chapter 5 **Installing the Norton AntiVirus Corporate Edition server program, management snap-in, and console add-ons**

System requirements	106
System requirements for Windows NT/2000 servers	106
System requirements for NetWare servers	108
Other NetWare requirements and considerations	108
System requirements for the Norton AntiVirus management	
snap-in	110

Preparing for installation	110
Installation order for Citrix Metaframe on Terminal Server	110
Which computer should I use to run the server installation program?	110
Locating servers during installation	111
Creating a text file with IP addresses to import	111
Verifying network access and privileges	112
Rights to install to Windows NT/2000 servers	113
Installing to NetWare servers	113
From what operating systems can I run the installation program?	114
Locating servers during installation	114
Required restarts	115
Understanding server installation options	116
Initializing virus protection for Windows NT servers	116
Installing the Norton AntiVirus Corporate Edition server program	116
Installing both the Norton AntiVirus Corporate Edition server program and Alert Management System	117
Restarting a Windows NT/2000 server with automatic or manual startup	127
Configuring automatic installations of Norton AntiVirus Corporate Edition on NetWare servers without Symantec System Center	129
Installing the Norton AntiVirus Corporate Edition management snap-in	130
Installing the Symantec System Center console add-ons	131
Uninstalling	131
Uninstalling the Norton AntiVirus Corporate Edition management snap-in	131
Uninstalling Norton AntiVirus Corporate Edition from a Windows NT/2000 server	132
Uninstalling Norton AntiVirus Corporate Edition from NetWare primary servers	132
Uninstalling Norton AntiVirus Corporate Edition from NetWare secondary servers	133
Reboot required before reinstalling	133

Chapter 6 **Installing Norton AntiVirus Corporate Edition to clients**

System requirements	135
System requirements for the Windows 9x/Me/NT	
4.0/2000/XP client	136
System requirements for the Windows 3.x client	136
System requirements for the DOS client	137
Requirement for clients running IPX only	137
Preparing for client installation	137
Rights to install to client computers	137
Client does not install to Terminal Servers	138
When a restart is required	138
Installing email support	138
Disabling the installation of the email plug-in and	
LiveUpdate for the Norton AntiVirus Corporate Edition	
client	139
Installing Norton AntiVirus Corporate Edition to client	
computers	140
Installing the Norton AntiVirus Corporate Edition client	
from an internal Web server	141
Installing from the client disk image on the server	163
Installing Norton AntiVirus Corporate Edition to Windows	
NT/2000/XP clients	164
Installing the Norton AntiVirus Corporate Edition client	
locally	168
Installing with logon scripts	169
Installing from floppy disks or a self-extracting .exe	175
Rolling out custom Grc.dat and LiveUpdate .hst files	
during client installs	180
Rolling out clients using third party products	181
Rolling out SMS package definition files	181
Rolling out with the Novell ManageWise ZENworks	
Application Launcher	184
Rolling out with Microsoft IntelliMirror	185
Configuring automatic installations of Norton AntiVirus	
Corporate Edition using NetWare servers without	
Symantec System Center	186
Creating Norton AntiVirus Emergency and Rescue Disk sets	
for client computers	187
Creating and using the Norton AntiVirus Emergency	
Disk set	188
Creating a Norton AntiVirus Rescue Disk set	188

Uninstalling Norton AntiVirus Corporate Edition on Windows NT clients	189
Reboot required before reinstalling	189

Chapter 7 **Updating Norton AntiVirus Corporate Edition**

Planning your migration	192
Pilot your rollout first	192
Minimize unprotected clients	192
Plan your definitions update strategy	192
Get definitions updating working immediately	193
Match management snap-in version to client version	193
Train your support staff and end users as part of the rollout	193
Automatic migration of servers and clients	194
Custom settings may be lost	195
Quarantine/Virus Bin items are automatically migrated	196
How automatic migration works	196
Migrating from Norton System Center	197
Migrating from the LANDesk Virus Protect /Norton AntiVirus Corporate Edition 6.x console to Symantec System Center	198
Migrating an existing LiveUpdate server	198
Migrating servers	199
Migrating Windows NT servers	199
Migrating from Norton AntiVirus for NetWare	201
Migrating from LANDesk Virus Protect/Norton AntiVirus Corporate Edition 6.x	202
Migrating from other server anti-virus products	203
Migrating clients to Norton AntiVirus Corporate Edition	203
Determining parent servers and policy	203
Migrating Windows NT clients	204
Migrating Windows 9x/Me clients	205
Migrating 16-bit clients	206
Migrating unmanaged Norton AntiVirus Corporate Edition clients	207
Migrating remote clients	208
Migrating clients from other anti-virus products	209
Checksum scanning is unsupported	210
Troubleshooting the update	210
Cannot see server to update	210
New viruses everywhere	210
An update failed or did not complete	211
Updating Norton AntiVirus server fails if Symantec System Center Console is running on the server	211

Section 2 Using Norton AntiVirus Corporate Edition

Chapter 8 Controlling servers and clients

Managing server groups	216
Filtering the server group view	217
Grouping servers into server groups	217
Selecting a primary server for a server group	219
Changing a server group password	219
Locking and unlocking server groups	220
What happens when you move a server to a different server group	223
Selecting from the tree or the right console pane	223
Applying policies at the server group, server, and client level	224
Changing a client's management status	225
Changing a client from unmanaged to managed	225
Editing the Grc.dat file to control clients	226
Changing a client from managed to unmanaged	227
Changing the client check-in interval	229
An in-depth look at Grc.dat	231
The role of the primary server	231
The role of the ClientConfig key	232
Where changes are recorded	232
What causes Grc.dat to be written	233
How changes are made	233
Changing the Debug value	234
Editing the Grc.dat file	234
The structure of Grc.dat	237
Enabling the Norton AntiVirus Corporate Edition icon in the Windows system tray	249
Deleting clients	249
Changing the client expiration level	250
Centralized client scanning control	251
Default communications port	251

Chapter 9 **Keeping your protection current**

What are virus definitions file updates?	254
Controlling virus definitions file rollouts	254
Viewing the virus list for a server or client	255
Verifying the dates of virus definitions files	255
Warning icon appears when definitions are out-of-date	256
Which update method should I use?	257
Virus Definition Transport Method	257
LiveUpdate	258
Intelligent Updater	259
Using the Virus Definition Transport Method	259
Updating servers	262
Testing updates and delivering them to the primary master server	262
If you don't test virus definitions updates	263
Downloading virus definitions files from the Symantec FTP site or LiveUpdate server using LiveUpdate	263
Configuring primary servers to retrieve from the master primary server	264
Updating servers individually	266
Setting advanced scheduled LiveUpdate options	267
Updating NetWare servers	270
Using LiveUpdate	273
Configuring servers to retrieve from the Symantec FTP site or LiveUpdate server	273
Configuring clients to retrieve from the Symantec FTP site or LiveUpdate server	274
Scheduling LiveUpdate for clients	274
Setting LiveUpdate usage policies	275
Using LiveUpdate with an internal LiveUpdate server	276
Rolling back a virus definitions file	282
Updating with Intelligent Updater	283
Updating servers and clients with Norton AntiVirus Corporate Edition product updates	283
Updating products and virus definitions files with Package.exe ...	284
Update examples	285

Chapter 10 Scanning for viruses

What kinds of scans are available	289
Virus sweeps	290
Manual scans	291
Scheduled scans	291
Realtime scans	291
About console tree objects and scanning	292
Understanding server scans	292
Understanding client scans	293
Understanding scans on multiple selected computers	294
About configuring manual, scheduled, and realtime scan options	295
Assigning actions and backup actions for detected viruses	296
Setting options that control interaction with users	296
Setting options that exclude files from scanning	301
Setting options that include files for scanning	304
Setting CPU utilization	310
Configuring manual scans	311
Understanding realtime protection	313
File caching for realtime scans	313
If your email program is not supported	314
Remote scans of email data	314
Setting client realtime protection options at the server or server group level	314
Locking realtime protection options	315
Resetting realtime protection options	315
Changing realtime protection options without clicking Reset All	316
Configuring realtime protection for files	317
Configuring server realtime protection for your file system	317
Configuring client realtime protection for your file system	318
Setting file system realtime protection advanced options	319
Selecting drive types to scan	319
Configuring realtime protection for mail applications	323

Configuring scheduled scans	324
Scheduling scans for server groups	325
Scheduling server scans	327
Scheduling scans for clients	330
Scheduling multiple scans	333
Setting options for missed scheduled scans	333
Understanding the hierarchy for scheduling scans	334
Editing, deleting, or disabling a scheduled scan	334
Running a scheduled scan on demand	335
Logon scanning options	336
Selecting file types to scan	336
Selecting locations to scan	337
Assigning actions for detected viruses during a logon scan ...	337
Preventing users from canceling a logon scan	338
Setting command-line scan options	338
Configuring logon scans for clients	339
Enabling and configuring NetWare logon scanning	339
Enabling and configuring Windows NT/2000 logon scanning	340
Enabling disk cache to speed logon scans	342

Chapter 11 Working with notifications, history, and events

Notification mechanisms	343
Customizable message box	344
Virus histories	344
Viewing histories	344
Sorting columns of data	346
Filtering items by date	346
Viewing a history of viruses found	347
Understanding Virus History icons	348
Taking additional actions on items in the Virus History	349
Viewing a history of scans performed	350
Understanding Scan History icons	351
Viewing Event Log information	351
Understanding Event Log icons	352
Using the Event Log	352
Clearing items from the Event Log	353
Deleting histories	353
How data is collected for Event Log and history views	354

Chapter 12 Managing virus infections

Symantec Central Quarantine	356
Symantec Security Response	357
Creating a Central Quarantine	357
Enabling the Central Quarantine	358
Configuring client forwarding to the Quarantine Server	359
Using Internet-based Scan and Deliver	360
Configuring Internet-based Scan and Deliver	361
Managing virus definitions updates	364
Reviewing sample submission status	368
Overriding automatic operation	370
Sending alerts	371
Using Email-based Scan and Deliver	374
Configuring Email-based Scan and Deliver	374
Configuring the Quarantine Server	374
Submitting files for analysis	375
Managing quarantined files	376
Updating Central Quarantine virus definitions	378
Testing the virus definitions update	379
Responding to virus outbreaks	380
Alert Management System	380
Built-in notification	380
Filtering Virus Found alerts	382
Taking action on viruses	383
Running a virus sweep	384
What if a client computer is turned off during the virus sweep?	385
Using the Norton AntiVirus Rescue Disk set to recover from a boot sector infection	385
Cleaning the virus	385
Restoring the computer's boot sector	386
What if my floppy disks become infected by a boot virus?	387

Section 3 Reference

Appendix A Scalability planning information

Planning questions	391
Ideal client-to-server ratios	392
Practical limits for Norton AntiVirus Corporate Edition	
client-to-server ratios	393
Trade-off considerations	394
Optimal number of threads for update operations	394
Recommendations on number of threads for key	
operations	395
Virus definitions file updating	396
Virus definitions update performance	396
Client configuration updates	399
Client and server installations and updates	399
Trade-off considerations	400
Additional thread configuration guidelines	401
Norton AntiVirus Corporate Edition server specifications	401
Typical Norton AntiVirus Corporate Edition servers	402
Client check-in interval	403
The Virus Definition Transport Method versus LiveUpdate	403
Virus Definition Transport Method operations	403
LiveUpdate operations	404
Using both the Virus Definition Transport Method and	
LiveUpdate	404
Operations that do not affect scalability	405

Appendix B Troubleshooting

Installation issues	407
Third party rollout and error 0x20000046E	407
NDS errors when installing Norton AntiVirus Corporate	
Edition to a NetWare 4.x server running an outdated	
Clib.nlm	408
Windows Installer Service error	409
Windows 2000 client installs that use interactive logon	
scripts	410
The Norton AntiVirus Corporate Edition server program	
install stops responding	410
Locating servers during installation	410

What settings apply when server group, server, and client settings differ?	416
Windows NT Workstation limitations	416
Difficulty configuring or running scans	418
Performance issues	420
My computer runs much slower since I installed Norton AntiVirus Corporate Edition client	420
Initial memory usage drops after running a scan under Windows 2000	420
As RTVscan sits with no activity, the page fault value in Task Manager slowly increases	420
Virus definitions file updating issues	421
LiveUpdate does not run	421
NetWare server not running TCP/IP can't get an update from Windows NT server in another server group	422
Some Norton AntiVirus Corporate Edition servers weren't updated	423
Incomplete discovery process	423
Other issues	423
Norton AntiVirus Corporate Edition and Microsoft Exchange server issue	424
Norton AntiVirus Corporate Edition and Microsoft Outlook Express issue	424
Viruses in System Restore folder on computers running Windows Me	424
LiveUpdate and the Windows Me/XP System Restore feature	425

Appendix C Norton AntiVirus Corporate Edition for Windows NT/2000 Services

Appendix D Events written to the Windows NT/2000 Event Log

Appendix E Understanding viruses

What is a virus?	431
File infector viruses	432
Boot sector viruses	432
Master boot record viruses	432
Multi-partite viruses	433
Macro viruses	433
What is a Trojan horse?	433

What is a worm?	434
What is a virus hoax?	434

Appendix F Definition Updater

System requirements for Definition Updater	435
Distribution Console (server) requirements	435
Definition Updater Agent (client) requirements	436
Location of Definition Updater install program	436
Additional Definition Updater install tasks	437
Installing an Agent	437
Administrator install tasks	437
User install tasks	439
Setting Agent email options	439
Setting the Agent monitoring schedule	440
Uninstalling Definition Updater	441
Uninstalling the Mobile Update Distribution Console	441
Uninstalling a Definition Updater Agent	441
Updating mobile computers with Definition Updater	442
How Definition Updater works	442
Administrator activities	443
User activities	444
Using LiveUpdate to update Definition Updater	445
Getting started with Definition Updater	445
Starting and exiting Definition Updater	445
Setting administrator email options	446
Sending virus definitions update packages	447
The Definition Updater Result Log	449
Viewing the Result Log	450
Deleting entries from the Result Log	450
Definition Updater troubleshooting	452

Appendix G Virus Scan for DOS

Understanding Virus Scan for DOS	455
Configuring command-line scans	456
Vscand.exe DOS error levels and error messages	459
Sample batch file	462

CD Replacement Form

Index

1

G e t t i n g s t a r t e d

Introduction to Norton AntiVirus Corporate Edition

This chapter includes the following:

- What's new in Norton AntiVirus Corporate Edition 7.6
- About Norton AntiVirus Corporate Edition
- How Norton AntiVirus Corporate Edition works
- What you can do with Norton AntiVirus Corporate Edition

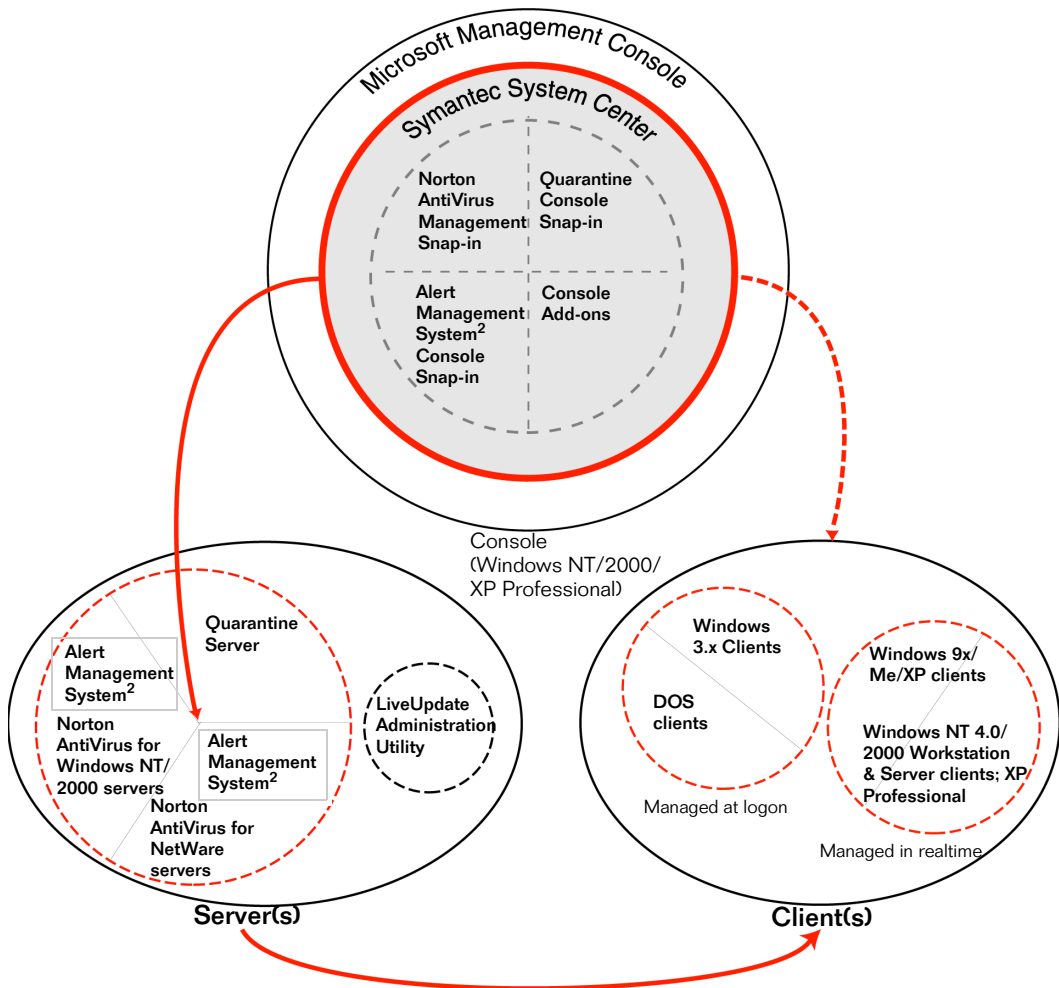
What's new in Norton AntiVirus Corporate Edition 7.6

The following features are new to Norton AntiVirus Corporate Edition 7.6:

- Client compatibility with Windows Me.
- Client compatibility with Windows XP.
- Compatibility with Microsoft Windows NT Server 4.0, Terminal Server Edition, and Windows 2000 Terminal Services.
- Ability to import a list of computers located in non-WINS environments during roll out.
- Support for mobile clients.
- Virus Found alert filtering capability.

For more information, see [“How Terminal Servers are protected”](#) on page 84, [“Creating a text file with IP addresses to import”](#) on page 111, [“Roaming Client Support”](#) on page 43, and [“Filtering Virus Found alerts”](#) on page 382.

About Norton AntiVirus Corporate Edition



Norton AntiVirus Corporate Edition includes the following products and tools:

- Symantec System Center (console and Alert Management System²), which you use to centrally manage Symantec products and alerting.
- Norton AntiVirus Corporate Edition management snap-in, which extends the Symantec System Center console so you can manage Norton AntiVirus Corporate Edition on servers and clients.
- Norton AntiVirus Corporate Edition 7.6 for Windows NT/2000 Servers
- Norton AntiVirus Corporate Edition 7.6 for NetWare Servers
- Norton AntiVirus Corporate Edition 7.6 for Windows NT/2000 Desktops
- Norton AntiVirus Corporate Edition 7.6 for Windows 9x/Me/XP Desktops
- Norton AntiVirus Corporate Edition 7.6 Windows 3.x/DOS Desktops
- LiveUpdate Administration Utility, which you can use to download updates to your intranet FTP server or other internal server. Servers and clients then retrieve updates from the designated server.
- Central Quarantine, which you can use to centrally manage infected files detected on servers and clients.
- Norton AntiVirus Corporate Edition includes a Microsoft Management Console snap-in. Use this snap-in to manage Norton AntiVirus Corporate Edition from the Symantec System Center console.
- Importer tool, which you can use to import computers located in non-WINS environments.
- Roaming Client Support, which you can use to ensure that Norton AntiVirus Corporate Edition clients (including mobile clients) are assigned to the best servers based on speed and proximity.
- ACL Fix Tool, which limits registry writes on a Windows NT platform to administrators.

Note: Symantec Corporation is also a provider of firewall, gateway, groupware, and other security products that are not discussed in this guide.

How Norton AntiVirus Corporate Edition works

Norton AntiVirus Corporate Edition consists of several distinct functional modules.

Symantec System Center

Symantec System Center is a program that plugs into the Microsoft Management Console framework on a Windows NT/2000/XP Professional computer. Symantec System Center lets you configure all server protection options and many client protection options for Windows clients. Although only one installation is necessary, you can install Symantec System Center on as many computers as you want. No administrator configuration console is available for DOS or Windows 3.1x.

From any Symantec System Center console with the Norton AntiVirus Corporate Edition management snap-in installed, you can view and configure any Win32 Norton AntiVirus Corporate Edition clients and servers that are visible on the network through IP or IPX.

Alert Management System

The Alert Management System (AMS²) is an alerting system that allows virus events to generate alerts through pagers, email, and other means.

AMS² is comprised of two separate components:

- Programs that run on each server
- Programs that run on the computer used as the Symantec System Center console

Server protection

The server setup program lets you select the servers that you want to protect, and then copies the required files to each server. NetWare servers run Norton AntiVirus Corporate Edition for NetWare Servers NLMs; Windows NT/2000 servers run Norton AntiVirus Corporate Edition for Windows NT/2000 Servers services.

For more information, see [“Preparing for installation”](#) on page 110.

You can scan servers with the Norton AntiVirus Corporate Edition client programs by mapping a drive to the server and then scanning the network drive. However, unless you install the Norton AntiVirus Corporate Edition server or client program on each server, your network is not fully protected. You should protect file servers so that they do not act as a central distribution point for viruses that will infect the clients.

Server protection does not rely on any other Norton AntiVirus Corporate Edition components, but to configure the protection options for NetWare servers, you must use the Symantec System Center console. For Windows NT servers, you can also configure options from Norton AntiVirus Corporate Edition.

Client protection

You can protect DOS and Windows computers by installing Norton AntiVirus Corporate Edition onto each computer that you want to protect (NAVEX for DOS, and Norton AntiVirus Corporate Edition for Windows 3.11 and 95/98/Me/NT/2000/XP clients).

For more information, see [Chapter 4, “Other information you need to know before installing”](#) on page 63.

The only client protection available without installing software onto each client is a DOS-level scan from a logon script or similar method.

To function properly, client protection should reside locally. By default, the server setup program creates a client installation folder on each server so that clients can be installed directly from the servers. You can also automate client installation with logon scripts.

For more information, see [“Installing Norton AntiVirus Corporate Edition to client computers”](#) on page 140.

Once you install the client to a computer, it has all the necessary elements for complete virus protection even if it is not managed.

Managed clients connected to the LAN can receive virus definitions file updates from the server. Also, each Windows client program has the capability to download the latest virus definitions file update from the Internet, allowing unmanaged computers to keep their own protection up-to-date. Norton AntiVirus Corporate Edition is compatible with both the Microsoft client for NetWare and the Novell client for NetWare networks.

Note: We recommend running the Novell client for NetWare on the computer from which Norton AntiVirus Corporate Edition is rolled out to NetWare servers.

Parent server issues

Once 32-bit clients are installed, the Norton AntiVirus Corporate Edition realtime protection service handles communication to the parent server. Symantec System Center delivers changes to clients and updates cached client settings in the server's registry.

A 32-bit client does not need to log on or map a drive to the parent server in order to send alerts or get virus definitions file updates and configuration data. A 16-bit client does need to be logged on to the parent server to communicate.

Client configuration types

Norton AntiVirus Corporate Edition classifies the client computers in four ways: managed, sometimes managed, lightly managed, and unmanaged. Though there is some overlap in these classifications, you should understand the distinction among the client types.

Managed clients

Managed clients are those that attach and log on to the network on a regular basis. Managed clients can:

- Communicate with a parent server and download configuration and virus definitions file updates as often as necessary.
- Be seen from Symantec System Center under their parent server.
- Immediately send alerts if Norton AntiVirus Corporate Edition detects a virus. Client log information is also available from Symantec System Center.
- Have their configuration settings locked from Symantec System Center so that the user cannot change them.
- Automatically install to a user's hard drive through logon scripts. This is useful for new installations and for program updates.

Sometimes managed clients

Sometimes managed clients share most of the managed client characteristics. However, when they are not connected, the icon representing that client in Symantec System Center is dimmed. If the parent server does not communicate with that client for three days, the icon representing the client is removed from the Symantec System Center display. Any setting you have chosen to lock down remains locked even if the client computer is not connected to the network or becomes disconnected. The next time these clients log on to the network, they will receive any new configuration data and the latest virus definitions file. Any virus events that occurred while offline will be communicated to the server during the client logon.

Lightly managed clients

Lightly managed clients are managed without using the Symantec System Center console. They are configured by editing a configuration file, called Grc.dat. You can include Grc.dat as part of the client installation files. You can perform configuration changes by rolling out a new Grc.dat to clients using your own third-party software.

Unmanaged clients

Unmanaged clients are not connected to the network and have no parent server with which to communicate. They will not appear in the Symantec System Center view even if later connected to the network. These clients need to download their own program and definition updates. LiveUpdate is built into each of the Windows clients so they can automatically get new virus definitions file updates.

About scanning

Norton AntiVirus Corporate Edition uses several anti-virus technologies and scanning methods to provide comprehensive network file scanning. Scans look for known viruses by comparing files with known virus strings. These strings are contained in a virus definitions file that resides on each computer. To protect yourself from new viruses, you can configure regular virus definitions file updates.

What you can do with Norton AntiVirus Corporate Edition

You can complete key administrative tasks using Norton AntiVirus Corporate Edition.

Establish policies and enforce them

You can lock configuration settings such as real time scanning to ensure that your clients remain protected from viruses at all times. You can also password protect server groups so that changes to settings for servers and clients can be made only by authorized staff.

Verify protection

From the Symantec System Center console, you can select and view the current protection settings for any managed clients. All managed clients that are running Norton AntiVirus Corporate Edition appear in the right pane of the console when their parent server is selected in the tree. Without leaving your desk, you can verify which clients are protected.

Manage virus definitions file updates

You must update virus protection frequently on all of your servers and clients to guard against the latest virus threats. Norton AntiVirus Corporate Edition includes several methods for getting the latest virus definitions files and updating your servers and clients.

You can automate the update process and specify when it runs.

Control live viruses

Set up your servers and clients so that infected files are automatically forwarded to a central Quarantine Server. You can then choose to submit the file to Symantec Security Response, formerly known as Symantec AntiVirus Research Center, for a rapid turnaround solution.

You can use the new Internet-based Scan and Deliver, an automated virus sample submission and definition delivery system that provides realtime protection against heuristically detected new viruses.

Alternatively, you can use the older Email-based Scan and Deliver, a virus sample submission and virus definitions delivery system that includes the Scan and Deliver Wizard to simplify sending items to Symantec Security Response for analysis. If a new virus is found, updated virus definitions are returned by email.

Manage virus protection using virus history, scan history, and event log data

You can analyze the data for infection trends, and then take appropriate action such as setting tighter configuration options for higher risk clients. Virus history and event log data is exportable to many third-party reporting systems.

Manage groups of computers

A server group is a container of servers and clients that share communication channels. You organize servers and clients into server groups. Server group members can share the same Symantec product configuration settings. You can also run a Symantec product operation on all members of a server group at once. For example, you can apply Norton AntiVirus Corporate Edition configuration settings to all of the members of a server group simultaneously.

Server groups are independent of Windows NT/2000 domains and are not dependent on any other products.

For more information about server groups, see [Chapter 2, “Server groups”](#) on page 33.

Manage scanning

Using Symantec System Center as a single point of administration, you can manage scanning as follows:

- Set scanning options and run virus scans for individual servers and client computers.
- Set global scanning options and run scans for computers that are members of the same server group.

You can use Norton AntiVirus Corporate Edition scanning technologies with the different types of scans described below:

- Manual or on-demand scans: Inspect selected files and folders on selected computers. Manual scans are ideal for providing immediate results from a scan on a small area of the network, or a local hard drive.
- Real time scans: Inspect files for known virus definitions on a continuous basis as files are read from or written to a server or client computer. You can also configure 32-bit client computers to scan the following applications:
 - Lotus Notes
 - Microsoft Exchange
 - Microsoft Outlook

- **Scheduled scans:** Inspect selected files and folders on selected computers at a predetermined time. Scheduled scans are ideal for large areas of the network because the scans can run during off hours when network traffic is low. For example, you may want to scan all files with a new virus definitions file that you recently downloaded.
- **Logon scans:** This is for Windows 3.1 and DOS clients only. Inspect client computers as they log on to the network. You set the same logon scanning options for all clients that connect to a server running Norton AntiVirus Corporate Edition. You can configure logon scans at the server group level.

Note: Unmanaged clients also have a configurable startup scan.

A virus sweep is another type of scan launched from Symantec System Center. It causes all managed clients to immediately start scanning. Managed and sometimes managed clients will also display your predefined message when they encounter a virus. This message can be as many as 512 characters and include event-specific variables. You can custom tailor this message for single users or groups.

Virus History, Scan History, and Event Log data

Virus and status information is available from the Symantec System Center console at all times in the following formats:

- **Virus History:** Lists all detected viruses for selected computers or server groups. You can select an item in the list and perform additional actions, such as Delete or Move File To Quarantine. Virus History shows many details about each infection such as the name and location of the infected file, the name of the infected computer, the primary and secondary actions that were configured for the detected virus, and whether those actions succeeded.
- **Scan History:** Use Scan History to view scans that have run or are running on selected computers or server groups.
- **Event Log:** Contains all other logged information that does not fall into the previous two categories. For example, the Event Log would contain messages about the virus definitions file or Symantec program updates for specific computers.

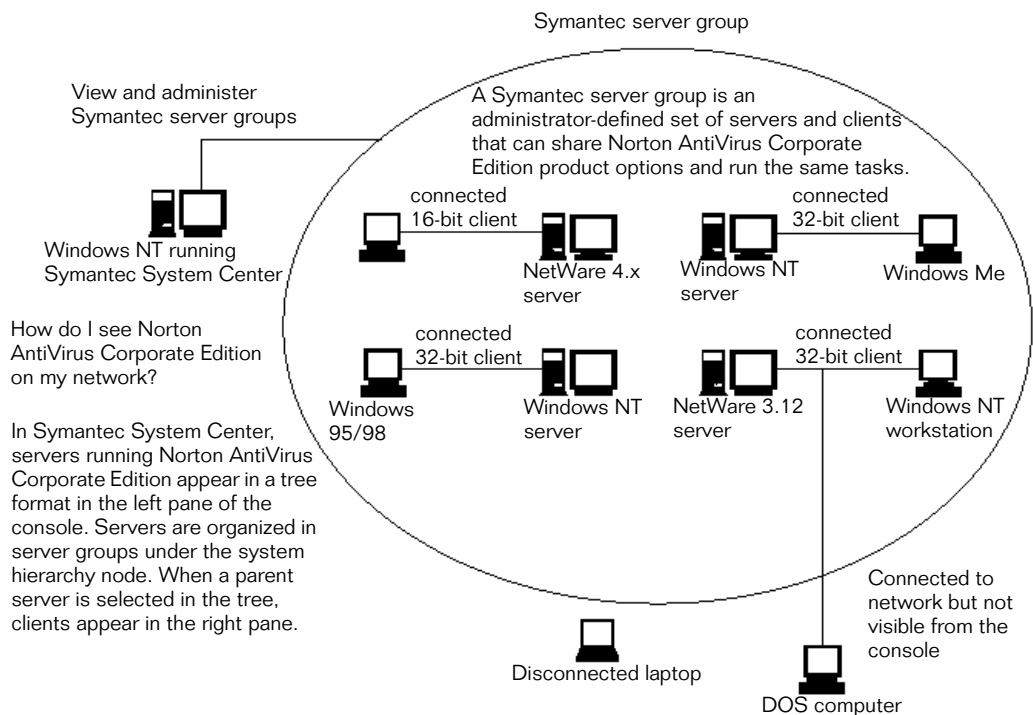
You can specify a time range to filter the view. For example, you might want to view only those scans that ran within the last 7 days.

These reports are server group based. If you want a report that includes multiple server groups, export the data, then manipulate it using a third-party reporting tool, such as Crystal Reports. Symantec System Center provides you with a comma delimited file that can be exported for use with your preferred third-party reporting tool.

Server groups

This chapter covers the following topics:

- About server groups
- Considerations in server group planning



About server groups

A server group is a container of servers and clients that share communications channels. Server groups are independent of Windows NT/2000 domains and are not dependent on any other products.

Server group members can share the same Norton AntiVirus Corporate Edition policies. You can also run a Norton AntiVirus Corporate Edition operation (such as a virus sweep) on all members of a server group.

The first time that you run Install Norton AntiVirus To Servers from Disk 2, the Setup Wizard prompts you to create a server group. From the Symantec System Center console, you can create new server groups and manage their membership. You can create as many server groups as you need to manage your servers and clients efficiently.

Servers can be a member of only one server group at a time, but you can easily move servers from one server group to another using drag and drop. All clients of the server that you move are also moved to the new server group.

For administrators who have used Norton AntiVirus Corporate Edition 6.0 or LANDesk Virus Protect 5.01 or higher until recently: Server groups are identical in functionality to your old Virus Protect or Norton AntiVirus domains. You must migrate your old domains to server groups before you can manage them. The migration can be performed automatically during installation.

For more information about updating from these products, see [Chapter 7, “Updating Norton AntiVirus Corporate Edition”](#) on page 191.

How you can see server groups

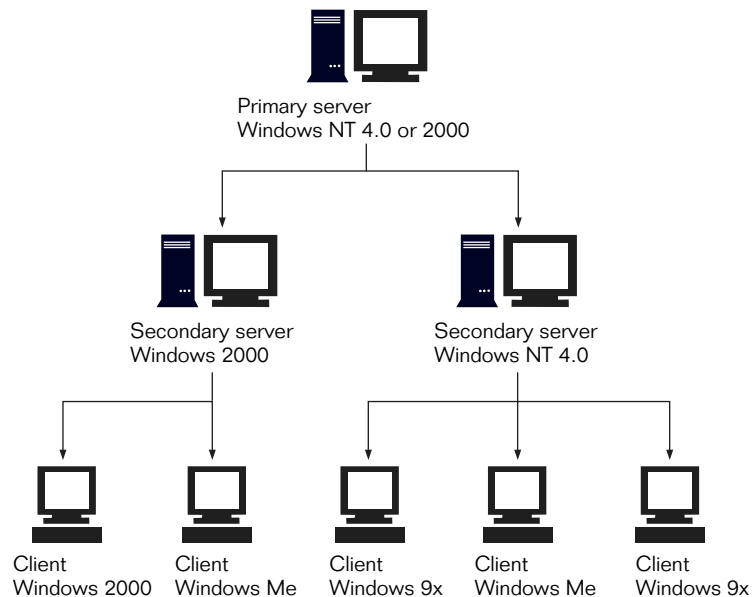
When you run the Symantec System Center console, you see servers that are running managed Symantec products in a tree format. Servers are grouped under server groups. You can define as many server groups as you need. When a server is selected in the tree, its clients appear in the right pane of the console.

Primary, secondary, master primary, and parent servers

When you manage with Symantec System Center, servers assume the following roles:

- Primary server
- Secondary server
- Master primary server
- Parent server

Primary server



Each server group has an administrator-designated primary server. The primary server is responsible for configuration functions in the server group. It can also be responsible for new virus definitions file updates.

From the Symantec System Center console, when you launch a task at the server group level, the task runs on the server group's primary server. The primary server also forwards the task on to all other servers in the server group.

If you are using Alert Management System², the primary server also processes all notifications.

Computers running any of the following operating systems can be made primary servers:

- Windows 2000 Server, Advanced Server, or Professional
- Windows NT 4.0 Server or Workstation
- NetWare 3.x, 4.x, or 5.x

How the registry is affected

When you modify server options, you directly modify the registries of the selected servers. The modification is made through a communication method named Transman (Transman.dll).

The primary server acts as the repository of all server options on a group level. If you modify on a group level, the changes are recorded first in the registry of the primary server for that group in the

HKLM\Software\Intel\LAN Desk\VirusProtect6\CurrentVersion\DomainData key.

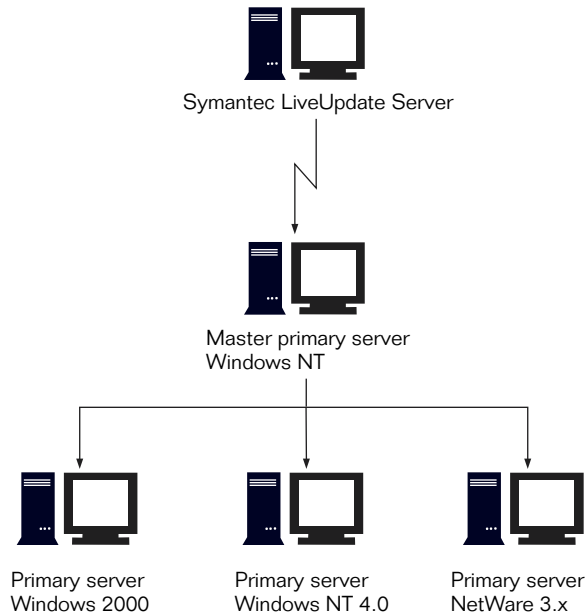
Then they are recorded in each of the other servers.

Secondary server

Servers that are not assigned primary server status are called secondary servers. Secondary servers are children of primary servers. They retrieve information from the primary server and share it with clients.

All servers in a server group are secondary servers until you assign one as the primary server. You must designate the primary server before you can perform most tasks at the server group level.

Master primary server



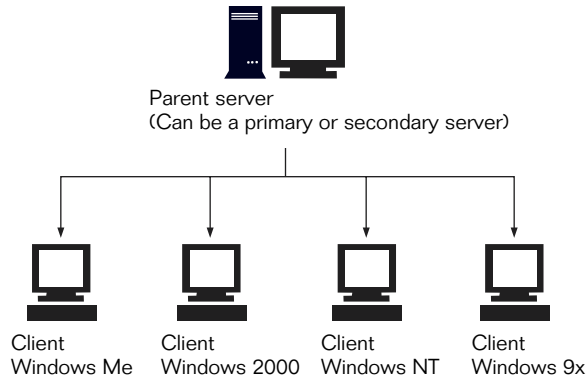
A master primary server is a primary server from which other primary servers retrieve LiveUpdate information, such as virus definitions files and product updates. For example, when you manage Norton AntiVirus Corporate Edition using Symantec System Center, you can download virus definitions file updates to a master primary server. You can then set up all of your other primary servers to retrieve virus definitions file updates from the master primary server.

When you set up a master primary server, a single designated server goes to the Symantec Web site for new virus definitions files. This limits your organization's exposure to the Web.

Once you set up the primary servers to retrieve virus definitions file updates from the master primary server, the master primary server is fully designated. No other task is required.

Note: Symantec product configuration changes cannot be managed at a level higher than the server group.

Parent server



A parent server is the server that a connected client communicates with to get configuration updates and to send alerts.

Parent versus primary servers

The management features of Norton AntiVirus Corporate Edition allow some servers to handle additional administrative responsibilities. Some servers may act as parent servers; others may act as primary servers. These two functions are not mutually exclusive. A primary server may also act as a parent server.

Changing primary and parent servers

You can change primary servers and parent servers easily.

To change a primary server

- 1 In the Symantec System Center console tree, double-click the server group.
- 2 In the right pane, right-click the secondary server you are designating as a primary server, then click **Make Server A Primary Server**.

To change a parent server

- 1 Copy the Grc.dat file from the one of the following folders of the intended parent server (based on the target client's platform):
 - NAV\Clt-inst\Win32
 - NAV\Clt-inst\Win16
 - NAV\Clt-inst\DOS
- 2 Paste the Grc.dat file into one of the following folders on the client:
 - For Windows 9x\Me: C:\Program Files\Norton AntiVirus
 - For Windows NT: C:\Winnt\Profiles\All Users\Application Data\Symantec\Norton AntiVirus Corporate Edition\7.5
 - For Windows 2000\XP: C:\Documents and Settings\All Users\Application Data\Symantec\Norton AntiVirus Corporate Edition\7.5

Clients

Clients interact with their parent server when they check in with status information and help determine whether new updates and configuration settings files are needed. If you are using the Alert Management System², they also send event notifications to parent servers. Parent servers may be either primary or secondary servers.

Note: Norton AntiVirus Corporate Edition clients running IPX only will not check in with their parent server and will not show up under the Symantec System Center console. They must either have IP installed on the server and client or run Microsoft File and Print Services for NetWare on the Server.

Considerations in server group planning

When planning server groups, consider the following:

- You can combine both NetWare and Windows NT servers into the same server groups, which allows simultaneous remote configuration of either or both types of systems. Because all configuration parameters are nearly identical for both server types, configuring servers is easy.
- You should place multiple NetWare servers that reside in the same NDS container into the same server group. This will simplify client installation with logon scripts.
- You should place multiple Windows NT domain controllers that reside in the same Windows NT domain into the same server group. This will simplify client installation with logon scripts.
- Because you can protect each server group with a unique password, separating server groups based on administrative responsibility is a logical option.
- Fewer server groups will reduce the overall effort required to maintain and configure client and server protection.
- All server group members can share the same product configuration settings. For example, clients and servers that are at greater risk of viruses should be grouped together so that a common, more secure configuration can be used. Clients and servers that require less protection or restrictions (for example, software development environments) should also be grouped together.
- Server groups should not be set up to span WAN links. If you set up server groups to span slow WAN links, they can slow down Symantec System Center and needlessly increase network traffic over these links.
- You can easily create or delete server groups, and you can drag and drop servers from one server group to another at any time.

Server group passwords

The default password used to unlock the server group created during install is:

symantec

When you create a new server group, you type the password that you want to assign to it. You can change the password as necessary. Empty passwords are allowed. You cannot change the password of an empty server group, or lock/unlock it.

For more information about server group passwords, see [“Changing a server group password”](#) on page 219.

What options are applied when set at the server group level

You can set the same options on the server or client level that you set at the server group level. If you do this, the individual computers' settings will be overwritten by the server group settings. If an option is not changed at the server group level, the option remains unchanged on servers and clients.

Note: Realtime scan options must be locked at the server group or server level before they will be propagated to clients. If they are not locked, the options will be applied to new clients only.

Roaming Client Support

This chapter covers the following topics:

- About Roaming Client Support
- When to use Roaming Client Support
- How Roaming Client Support works
- Roaming client management limitations
- Implementation tasks
- Load balancing and marking primary and backup servers
- Specifying a primary server with a list of backup servers
- Specifying other types of parent servers
- Rolling out RoamAdmn.exe and the server list text files to administrator computers
- Setting up Roaming Client Support on each client
- Running Roaming Client Support as a command line utility

About Roaming Client Support

Roaming Client Support dynamically connects computers on a Windows NT-based network with the parent server that provides the best performance based on speed and proximity.

As an alternative to identifying parent servers based on response time, you can use Roaming Client Support to balance the load among a pool of servers that are equal in connection speed and proximity based on the client load on the computers.

Roaming Client Support includes two tools:

Administrative tool (RoamAdmn.exe):	This sets up servers for roam detection. These servers act as guide posts in the network tree.
Agent (NAVRoam.exe):	This runs as a service on roam managed clients. It checks periodically to determine whether a different parent server needs to be assigned to the client.

When to use Roaming Client Support

You can use Roaming Client Support for the following purposes:

- Connect any computer, including a laptop used by a mobile user, to the best parent server. When Roaming Client Support detects changes to the client's network address, it designates a new best parent server if necessary.

For example, when a mobile user based in New York travels to California, Roaming Client Support detects the new location and reassigns the user's laptop to the best parent server.

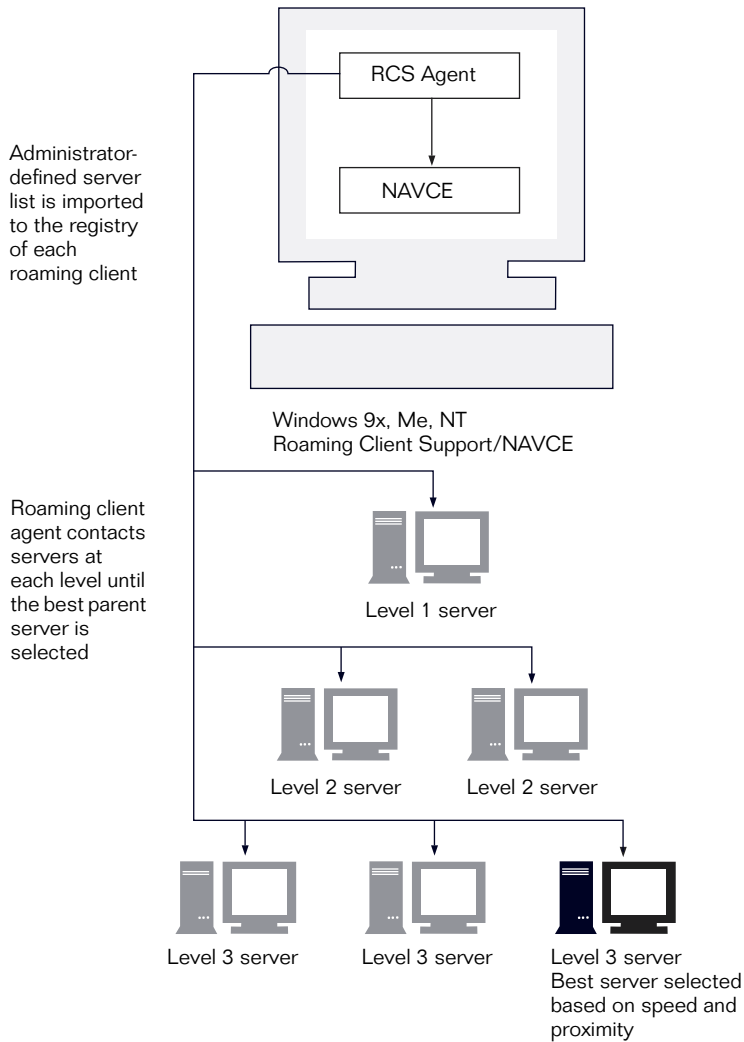
- Locate the best parent server to manage a previously unmanaged computer when it connects to the network.

For example, a corporation may have a distribution center for new computers. Administrators set up Roaming Client Support on the computers before they are sent out to branch offices. As part of setting up Roaming Client Support, the administrators specify all possible parent servers for the new computers. When end users connect the new computers to the network, Roaming Client Support assigns the best parent server automatically.

Once it becomes a client of the best parent server, the computer receives upgrades, virus definitions file updates, and configuration updates.

You can also configure Roaming Client Support to connect with other types of parent servers, such as alert servers or Quarantine servers.

How Roaming Client Support works



Roaming Client Support works in the following manner:

Action	Description
MIS creates a server list.	<p>A server list is a text file containing potential parent servers located throughout the network. The servers in the list are structured hierarchically from a general geographic area to a specific area.</p> <p>The servers are organized into levels that range from Level 1, the broadest geographic area, to the most specific. For example, a server in New York locates the United States at Level 1. At Level 2, it locates East Coast United States servers. At Level 3, it locates the New York server.</p> <p>Medium-sized networks may require only one or two levels while enterprise-sized networks may require five or more levels.</p>
The server list and the agent (NAVRoam.exe) are rolled out to clients.	NAVRoam.exe installs to the client as part of Norton AntiVirus Corporate Edition.
The server list is imported to the registry of each client.	NAVRoam.exe imports the server list on the client.
The server list is imported to the registry of remote servers.	RoamAdmn.exe sets the appropriate registry keys on remote servers.
NAVRoam.exe is launched on each client.	<p>NAVRoam.exe locates the best server when:</p> <ul style="list-style-type: none">■ Windows starts up and loads its services■ The computer's network address changes■ A parent server becomes unavailable; by default, this check runs every two hours <p>NAVRoam.exe also locates the best server at a regular interval, to detect and adjust for changes in the environment; for example, the parent server may change when the current parent server can no longer be contacted.</p>

Action	Description
The agent contacts the nearest server and requests the next level of servers from it.	
The servers in the list become structured hierarchically, locating the general area of the network and identifying the server that is closest to the agent.	This continues until the fastest responding server has no level beneath it.
The parent server is assigned.	<p>The parent server is selected based on:</p> <ul style="list-style-type: none"> ■ Connection speed between the server and client ■ Proximity of the server to the client <p>If the client was previously assigned to a different parent, it attempts to delete itself from that parent when it checks in with the new parent.</p>
Roaming Client Support continually performs a set of checks.	<p>Roaming Client Support checks:</p> <ul style="list-style-type: none"> ■ That any parent to which the client has been attached is still valid. If not, it connects the computer with the closest available parent on the network. ■ Whether the computer's network address has changed. If so, it connects you with the closest available parent. ■ The computer's Clients registry key to determine if the computer is a parent. If so, it determines if the number of clients has changed.

Roaming client management limitations

A roaming client is managed in the sense that it has a parent server from which it can receive upgrades, virus definitions files, and configuration updates.

Management of a managed client is dependent on its logical association with a parent server in a Norton AntiVirus Corporate Edition server group. Administration of the client is possible because of that association.

Management of a roaming client is based on which server is assigned as the parent server. The roaming client is not administered as it moves from one parent server to another based on server load.

Implementation tasks

To use Roaming Client Support, complete the following tasks:

- Analyze your network and create server list text files as needed.
For more information, see [“Analyzing your network and creating server list text files”](#) on page 49.
- Roll out RoamAdmn.exe and the server list text files to the administrator computers that MIS will use to import server lists into the registry on remote servers.
For more information, see [“Rolling out RoamAdmn.exe and the server list text files to administrator computers”](#) on page 56.
- Roll out Norton AntiVirus Corporate Edition and the server list text files to clients.
NAVRoam.exe is automatically rolled out to clients when you roll out Norton AntiVirus Corporate Edition. It is copied to the same directory in which Norton AntiVirus Corporate Edition is installed.
- Set up Roaming Client Support on each client. This includes importing server list contents to the registry and installing NAVRoam.exe as a service on each client.
For more information, see [“Setting up Roaming Client Support on each client”](#) on page 57.

Requirements

Roaming clients must be running Norton AntiVirus Corporate Edition under any of the following operating systems:

- Windows 9x
- Windows NT 4.0
- Windows 2000
- Windows XP

Analyzing your network and creating server list text files

You will need to analyze your network and organize servers, as well as the clients on which the agent is to be installed. Planning can limit unnecessary server-client communication. For example, if you have already narrowed the search to the West Coast for a server in Los Angeles, you would not include servers in its lists that are located on the East Coast. This could generate unnecessary traffic.

The roaming servers should be logically associated in a tree structure. Servers at the top level should cover the widest geographic area. At each subsequent level, use more specific locations.

The only limit to the number of levels that you can define is determined by the text file size limit of 512 characters.

You can create the server list text file using a text file editor such as Notepad.

Import files contain text lines in the following format:

<computer>,<type of server>,<level>,<server list>

where:

<computer> is the name of the server.

<type of server> is the server type (for example, primary server, parent server, Quarantine server, Grc.dat server, or Alert server).

<level> is the level as specified in the server list text file.

<server list> is the name given to the server list.

For example:

<local> Parent 0 USASvr,EuropeSvr,AsiaSvr

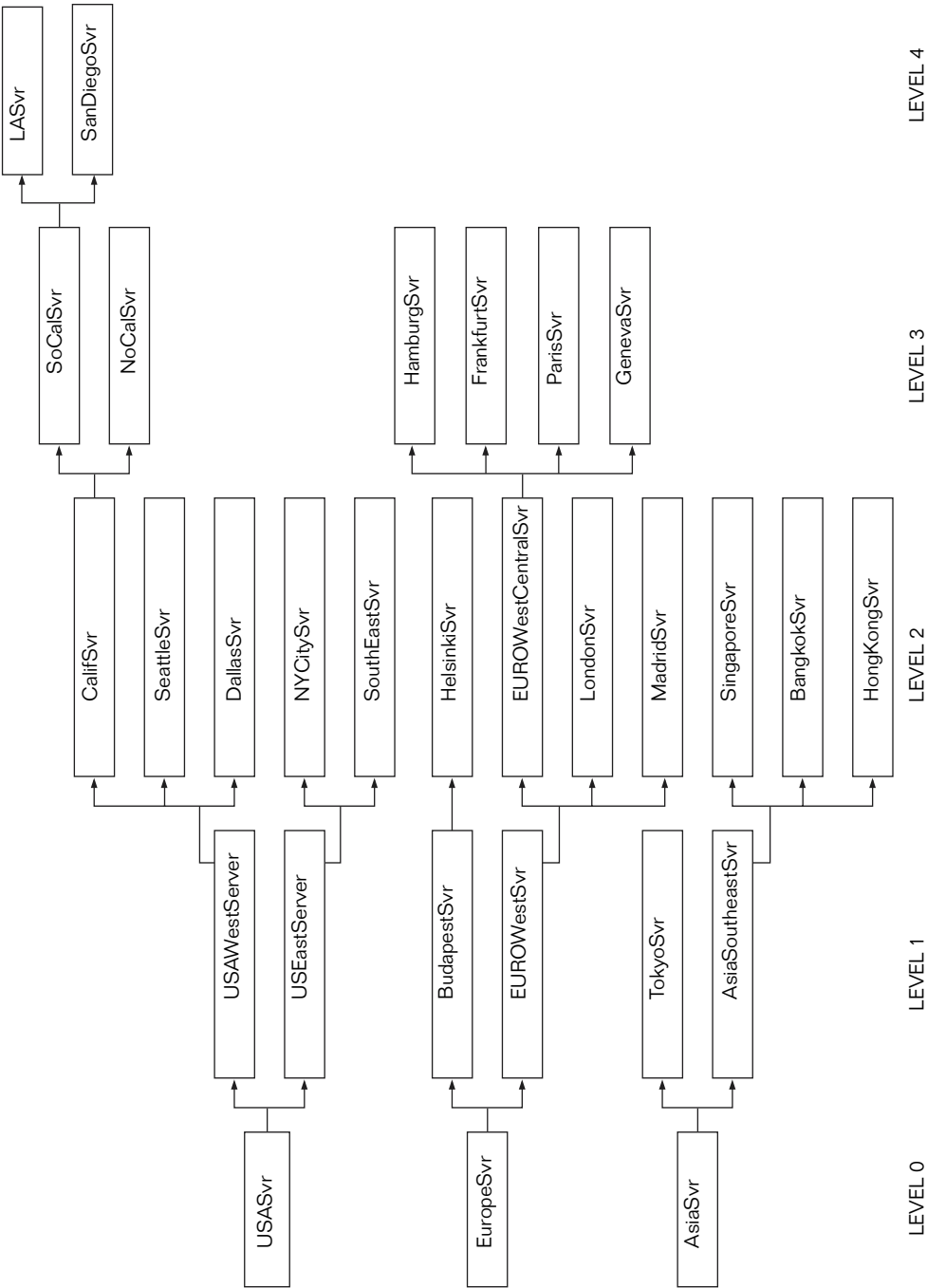
Note: In the server list for the client, you must include the <local> parameter in front of Parent 0. <local> points to the first level of servers that NavRoam should attempt to contact. If you omit <local> from the Parent 0 line, the first level of servers will not be located.

Importing this text line in the file creates a value under the HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion\ProductControl registry key as follows:

Registry Value Name	Data
RoamManagingParentLevel0	USASvr,EuropeSvr,AsiaSvr

Server list text file example

A corporation has a total of 32 roam servers that are available to serve as parents located in the United States, Europe, and Asia. MIS has grouped the servers as shown in the following illustration.



Each server contains a list of the servers the next level down on its branch. In this example, the registry values under the ProductControl key for USASvr, USEastSvr, and SouthEastSvr would be set up as follows:

Server Name	Registry Value Name	Data
USASvr	RoamManagingParentLevel1	USWestServer,USEastServer
USEastServer	RoamManagingParentLevel2	NYCitySvr, SouthEastSvr
SouthEastSvr	RoamManagingParentLevel3	MiamiSvr,AtlantaSvr,RichmondSvr

For more information, see [“Related Registry keys”](#) on page 61.

To set up a client to roam on this network, you would import a server list file.

The servers are imported into the registry using the /import command.

To import the server list on clients

- At the command prompt, type the following:
NAVRoam /import serverlist.txt
where serverlist.txt represents the name of the server list you created.

Using RoamAdmn.exe to set up the roaming servers

You can use RoamAdmn.exe to set up the roaming servers.

To set up the roaming servers

- At the command prompt, type the following:
RoamAdmn /import serverlist.txt
where serverlist.txt represents the name of the server list you created.

Example

A corporation has a computer from which all of the North American roaming servers are visible.

The serverlist.txt file includes the following lines:

```
USASvr Parent 1 USWestServer,USEastServer
USWestServer Parent 2 CalifSvr,SeattleSvr,DallasSvr
USEastServer Parent 2 NYCitySvr,SouthEastSvr
CalifSvr Parent 3 SoCalSvr,NoCalSvr
SouthEastSvr Parent 3 MiamiSvr,AtlantaSvr,RichmondSvr
SoCalSvr Parent 4 LASvr,SanDiegoSvr
```

When imported to the registry, the data appears as follows:

Server Name	Registry Value Name	Data
USASvr	RoamManagingParentLevel1	USWestServer,USEastServer
USWestServer	RoamManagingParentLevel2	CalifSvr,SeattleSvr,DallasSvr
USEastServer	RoamManagingParentLevel2	NYCitySvr,SouthEastSvr
CalifSvr	RoamManagingParentLevel3	SoCalSvr,NoCalSvr
SouthEastSvr	RoamManagingParentLevel3	MiamiSvr,AtlantaSvr,RichmondSvr
SoCalSvr	RoamManagingParentLevel4	LASvr,SanDiegoSvr

Load balancing and marking primary and backup servers

When you create a server list text file, you can allow for load balancing by instructing servers to be treated as equals regardless of how long it takes to contact them. To do this, use an equals sign (=) instead of commas between the servers in the list. For example:

```
SouthEastSvr Parent 4 MiamiSvr=AtlantaSvr=RichmondSvr
```

The equals signs signify that the client load must be balanced equally among the servers.

The servers must be running NAVRoam.exe or RoamAdmn.exe. These programs count the number of clients and create a ClientCount key under the ProductControl key. The server with the lowest client count is selected for the client. If one or more of the servers does not have a ClientCount key, the parent is chosen randomly from the servers in the list.

If the fastest response is from a server surrounded by equals signs, each server in the list is contacted. If those servers are running the agent then they have a ClientCount key that counts the number of clients in ProductControl. The agent reads this key, then selects the server from the list that has the smallest number of clients to become the parent server.

If some of the servers marked with the equals sign are not running the agent, then the client count is not available, and the agent selects one of these servers at random. This spreads the clients among the servers but not as equally as when the ClientCount key is available.

Servers must be prevented from roaming and searching for parents.

To prevent the servers from roaming

- Set the RoamClient registry key value to 0.

Specifying a primary server with a list of backup servers

You can specify a primary server with a list of backup servers by separating the servers by a forward arrow sign (>). For example:

```
SouthEastSvr Parent 4 MiamiSvr>AtlantaSvr>RichmondSvr
```

Each server specified must be running NAVRoam.exe or RoamAdmn.exe.

The response time is checked only for the first server in the list that answers. Subsequent servers are used if the preceding servers in the list do not respond.

There is no load balancing. If the first server goes down, then the clients migrate to the next server on the list when they check their parent.

Specifying other types of parent servers

Roaming Client Support can connect a roaming computer to more than one type of parent. On startup and whenever the network address changes, the computer can be paired with the nearest type of parent for:

- Norton AntiVirus Corporate Edition
- Quarantine
- Alerts (AMS²)
- Grc.dat (specifies a server to provide the client with Grc.dat settings)

Note: A Quarantine server must have the Norton AntiVirus Corporate Edition server program installed for Roaming Client Support to find it. A Quarantine server on which Norton AntiVirus Corporate Edition for desktops is installed will not be found.

The corresponding registry values must be set to 1. Corresponding server types must also be specified in the server list text file, then imported into the registry.

Note: For Windows NT/2000/XP computers, you must have Admin rights to write to the registry.

At the command line prompt, you can type any of the following:

```
NAVRoam /nearest_parent
NAVRoam /nearest_quarantine
NAVRoam /nearest_GRC
NAVRoam /nearest_alerts
NAVRoam /nearest_primary
```

Registry values are named appropriately. For example, for a Level 3 list:

- The value for Quarantine servers is RoamManagingQuarantineLevel3
- The value for Alert servers is RoamManagingAlertsLevel3
- The value for Grc.dat servers is RoamManagingGRCLevel3
- The value for the nearest primary server is RoamManagingPrimaryLevel3

Roaming servers may contain more than one server list. For example, USWestSvr may also function as a Level 2 Quarantine server, and as a Level 1 Alerts server.

When there are corresponding server lists in the registry for each parent type, the computer is connected with each parent.

Note: A client cannot connect with multiple parents of the same type.

The basic tasks and actions that occur when a client is connected with each type of parent are as follows:

Task	Action(s)
Setting a client parent	<ul style="list-style-type: none">■ Disconnects from the old parent■ Connects to the new parent■ Updates the Grc.dat file■ Updates the LiveUpdate host file if necessary
Setting a quarantine parent	Copies quarantine registry key values from parent to client
Setting a GRC parent	Copies the Grc.dat file from the GRC parent and processes it
Setting an Alerts parent	Lets the client registry values identifying the AMS ² server and runs AMS ²
Setting a Primary parent	Copies the Grc.dat file from the GRC parent and processes it

Rolling out RoamAdmn.exe and the server list text files to administrator computers

Roamadm.exe is located on Disk 1 in the AdminTools folder. You must copy Roamadm.exe to servers from which you want to import a server list to remote server registries, then run it.

Setting up Roaming Client Support on each client

Roaming Client Support (NAVRoam.exe) is rolled out to a client automatically whenever Norton AntiVirus Corporate Edition is rolled out to a client. NAVRoam is copied to the folder in which Norton AntiVirus Corporate Edition is installed.

To set up Roaming Client Support on each client, you must import the server list to the client's registry and install NAVRoam as a service.

To accomplish this, you can create a batch file or logon script that includes the following commands:

```
NAVRoam /import <servers.txt>
```

```
NAVRoam /install
```

where:

/import imports the server list contents into the registry of the local computer.

<servers.txt> represents the name of the text file that contains the server list.

/install loads Roaming Client Support as a service.

Note: You must have Admin rights to use command line options.

Once Roaming Client Support is registered as a service, it starts. The service also starts automatically and runs in the background whenever the computer is turned on.

Running Roaming Client Support as a command line utility

Roaming Client Support can also run as a command line utility. However, running Roaming Client Support as a service provides more control over scheduled runs than when it is run as a command line utility. Running Roaming Client Support as a service also allows for continued monitoring.

To run Roaming Client Support as a command line utility

- At the command line prompt, type:
NAVRoam
Following the NAVRoam command, add any necessary command line switches.

Command line switches

You can use the following command line switches with NAVRoam and Roamadm.

Switch	Description
/h	Displays a list of the switches with descriptions of their usages.
/import <server list>	<server list> is the text file in which the list of potential parent servers is specified. Sets up client or server registry keys. When using Roamadm.exe, you can import the server list to remote servers. When using NAVRoam.exe, you can import the server list to the registry of the local computer.

Switch	Description
/export <file>	<p><file> is the name of the file to which the information is written.</p> <p>Reports all the roaming servers that the client can find at all levels and for all parent types (primary server, parent server, Quarantine server, alert server, and Grc.dat server).</p> <p>You can use the file created with the export command as the server list for import.</p>
/install <path> <new service name> <new exe name>	<p><path> is the pathname for the folder to which you want to copy NAVRoam.</p> <p><new service name> is NAVRoam.</p> <p><new exe name> is NAVRoam.exe.</p> <p>Registers Roaming Client Support as a service, then starts it. The service runs until the computer is shut down.</p>
/remove <new service name>	Stops and removes NAVRoam.exe.
/nearest	<p>Finds and sets nearest appropriate parent (for the primary, parent, Quarantine, alert, or Grc.dat server).</p> <p>Requires that the parent GRC path be set manually in the registry.</p> <p>For more information, see “Related Registry keys” on page 61.</p>
/nearest_parent	Finds and sets the nearest client parent server.
/nearest_primary	<p>Finds and sets the nearest primary server for clients running NAVRoam.</p> <p>Requires that the parent GRC path be set manually in the registry.</p> <p>For more information, see “Related Registry keys” on page 61.</p>

Switch	Description
/nearest_quarantine	Finds and sets the nearest Quarantine parent server.
/nearest_GRC	<p>Finds and applies the Grc.dat file from the nearest Grc.dat parent server.</p> <p>Requires that the parent GRC path be set manually in the registry.</p> <p>For more information, see “Related Registry keys” on page 61.</p>
/nearest_alerts	Finds and sets the nearest Alert (AMS ²) server.
/check_parent	Verifies that the parent server is running.
/shutdown	Disconnects the client from the parent server.
/time-network <elapsed-time-in-seconds> <delta-time-in-milliseconds> <servers>	<p>Provides the average amount of time it takes to contact each specified server.</p> <p><elapsed-time-in-seconds>: Specify the number of seconds to allow the process to run.</p> <p><delta-time-in-milliseconds>: Specify in milliseconds how often to contact the server. For example, 10000 contacts the server every 10 seconds.</p> <p><servers>: Specify the servers to be contacted. Separate server names with commas. Do not include spaces between server names or commas.</p>

Related Registry keys

You can edit the registry to change Roaming Client Support registry values using a registry editor such as Regedit or Regedt32.

The agent behavior is controlled by registry keys under:

HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\
CurrentVersion\ProductControl

The keys are as follows:

Key name	Description
CheckForNewParentIntervalInSeconds	If a computer cannot find the nearest parent when it first starts, then it periodically checks to see if the network is up. The interval is set by this registry key. The default value is 30 seconds.
CheckParentIntervalInMinutes	Determines how often the computer checks to see if its parent is available. If the parent is not available, then it tries to find a new parent. The default value is 120 minutes.
RoamClient	Instructs the agent to make this computer a child of the nearest parent. The default value is 1. Set this value to 0 if you do not want the computer to become a child of the nearest parent.
RoamQuarantine	If the value is set to 1, then Quarantine forwarding is set to the nearest server found from the Quarantine search keys. The default value is 0.
RoamAlerts	If the value is set to 1, then AMS ² alert forwarding is set to the nearest server found from the Alerts search keys. The default value is 0.
RoamGRC	If the value is set to 1, then the client roams to the server from which it should receive policy file (Grc.dat) updates. The default value is 0.

Key name	Description
RoamServer	If the value is set to 1, then the client roams to the best primary server. The default value is 0.
ParentGRCPATH	Set the ParentGRCPATH value to GRC.dat. The agent copies Grc.dat to the local computer and applies it. See information for RoamGRC above.
ParentLiveUpdateHstPath	<p>Defines the directory underneath the NAV home directory; for example, \Myliveupdatehost\Liveupdt.hst</p> <p>(Do not specify the full pathname.)</p> <p>The agent copies the LiveUpdate host file here. This applies when roaming a client.</p>

Note: If both the RoamClient and RoamGRC keys are set to 1, NAVRoam copies the Grc.dat from the parent. NAVRoam then copies the Grc.dat from the GRC parent and overwrites the copy that originated on the parent.

Other information you need to know before installing

This chapter covers the following topics:

- Planning for network traffic
- The scalability of Norton AntiVirus Corporate Edition
- Required protocols
- Configuring options and running operations
- Windows NT/2000 cluster server protection
- NetWare cluster server protection
- Product installation order
- Staged installations
- Learning about Norton AntiVirus Corporate Edition in a lab setting
- Scanning configuration trade offs
- What to scan
- Management policy planning
- How Terminal Servers are protected
- Limiting access to the Norton AntiVirus Corporate Edition registry key on Windows NT 4.0 computers
- Central Quarantine
- Submit new viruses and get a rapid solution
- Customer profiles

Planning for network traffic

This section helps you understand the types and quantity of network traffic Symantec System Center and Norton AntiVirus Corporate Edition generated by the following:

- Alerts
- Updated virus definitions file transfers
- Configuration file transfers
- Clients checking in with their statuses
- Discovery service
- Refreshing

The amount of traffic generated depends on the number and type of configuration parameters you change, as well as your Discovery settings.

Symantec System Center traffic

Symantec System Center can communicate with all NetWare servers, Windows NT/2000 servers, and Windows clients. The communication protocol can be IP or IPX and might switch automatically from one to the other depending on throughput. The initial view of servers and clients that displays in the Symantec System Center console originates from the local registry and is then updated by retrieving information from each server. The client lists are gathered from each server rather than from each individual client.

Whenever server configuration parameters change, Symantec System Center sends the updates to each server in the server group directly, rather than through the primary server. Global client changes are sent through the parent server; individual client changes go directly to each client. In each case, an IP-to-IP or IPX-to-IPX path must exist for each leg of the communication.

For example, if the computer running Symantec System Center only has IP loaded, the servers have IP and IPX, but clients have only IPX, you could send updates to servers and clients through the server. Because there is no common protocol between individual clients and Symantec System Center, no updates can be sent directly to the individual clients.

Because the servers have both IP and IPX loaded, Symantec System Center communicates to the servers through IP and then the servers send the updates to the clients through IPX. To configure clients in this scenario, highlight the server and not individual clients. Highlighting individual clients causes Symantec System Center to attempt direct communication with the client, which is not possible in this case.

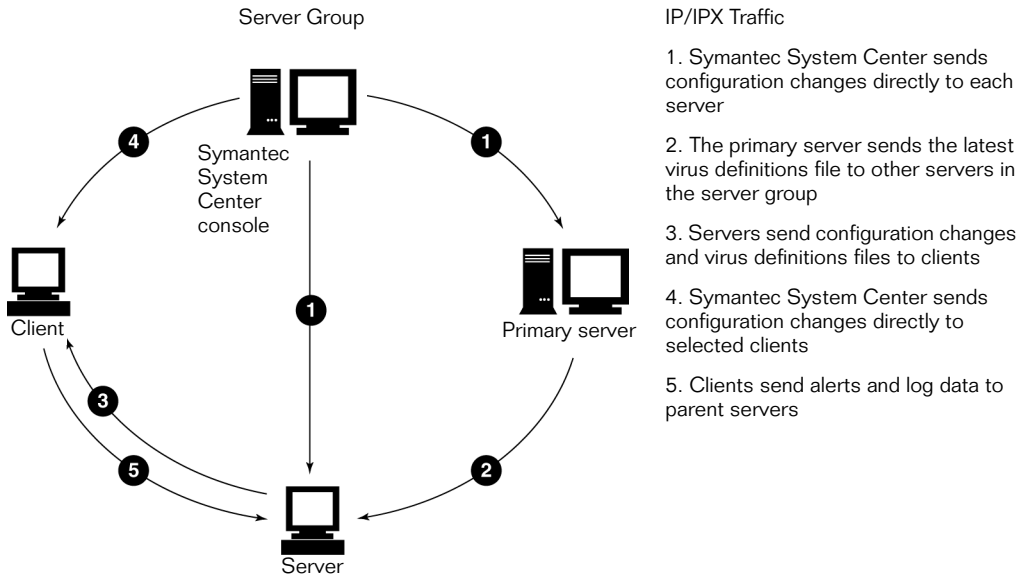
Server-to-server traffic

Using either IP or IPX, Norton AntiVirus Corporate Edition servers can communicate with each other to send virus definitions file updates and to forward alerts.

Only the primary server sends virus definitions file updates to the other servers in the server group (assuming definition sharing is enabled). Placing a newer virus definitions file on a server other than the primary server lets that server use the new virus definitions file. However, no other servers will automatically receive that virus definitions file unless a server-to-server download is scheduled. No network traffic is generated between servers until there is a new virus definitions file to send.

Other servers in the server group can receive updates from the primary server. Placing a newer update on a server other than the primary server allows that server to use the update. However, no other servers will automatically receive that update (unless a server-to-server download is scheduled). No network traffic is generated between servers until there is a new update to send.

Whenever a secondary server detects an event that triggers an alert notification to the primary server, the Alert Management System² on the primary server then processes the alert. No AMS²-related network traffic is generated when there are no notifications to forward.



Client traffic

Clients running Norton AntiVirus Corporate Edition communicate with servers to send notifications and receive updates and configuration data pushed from the parent server.

Clients send notifications to their parent server only when an event is generated. Otherwise, the alerting system does not generate any traffic. Windows clients periodically check with their parent server to provide their status.

Clients also check in to the parent server to provide the status information that is displayed in the Symantec System Center console.

For Windows NT/2000 and Windows 9x/Me/XP, only a single (1 KB) packet is sent from the client to the server to provide status information. The server does not respond if the status indicates that no action is necessary.

Note: Packets are transmitted using UDP. For this reason, there should be no routers between a client and its parent.

For Windows 3.1 clients, several packets may be exchanged at each interval.

Note: If you use the Virus Definition Transport Method to update servers and clients, avoid configuring a large number of servers and clients to update at the same time. See [“Using the Virus Definition Transport Method”](#) on page 259 for more information about the Virus Definition Transport Method.

Other sources of traffic

The Discovery Service, Find feature, and Refresh feature can also generate network traffic:

- Local Discovery broadcasts to the Symantec System Center console’s local subnet. Servers then respond immediately with information about themselves and their clients. Intense Discovery serially pings every server in the Network Neighborhood. The amount of traffic generated depends upon the number of minutes set for the discovery cycle interval and the number of discover threads set to run at once.
- A Network Discovery using the Find feature generates a small amount of traffic.
- The Refresh feature generates a small amount of traffic when run at the server group or server level. When a server group is refreshed, Symantec System Center pings all members of the group. When a server is refreshed, Symantec System Center pings the server and its clients.

For more information, see the *Symantec System Center Implementation Guide*.

The scalability of Norton AntiVirus Corporate Edition

For Norton AntiVirus Corporate Edition and all enterprise anti-virus solutions, most scalability problems involve the following operations. These are major scalability issues because of the large number of protected computers involved, the frequency of these operations, their high priority, the requirement for timely execution, and the amount of data involved.

- Virus definitions file updates: Virus definitions file updates involve a large volume of data that must be frequently distributed to every protected computer on the network. The update operation must be quick.

Updating can be expensive in terms of shared resource usage. It can affect the level of service provided to users negatively.

- Protected computer visibility: Protected computers on the network must be visible to the management console. Connections and locations must be confirmed periodically. Whether initiated by the protected computers or by a management computer, the process used to meet this management requirement can be expensive and problematic.
- Distribution of configuration updates: Distributing changes in anti-virus policy or operations quickly to a large number of protected computers can present a problem in terms of shared resource usage and time-to-completion. It can also result in lower service levels to other applications.
- Software installation and updates: Each time a new computer or server is added to the network, anti-virus software must be installed and the management console alerted to the new protected computer. In addition, because the types of virus attacks change frequently, anti-virus software must be updated more frequently than most other applications. The time and resources needed to manage and execute anti-virus software installation and updates across the network pose big scalability issues.

How Norton AntiVirus handles scalability issues

Scalability issues have been addressed in Norton AntiVirus Corporate Edition through the following design and implementation principles:

- The protected computers initiate and execute Norton AntiVirus Corporate Edition operations, including virus scanning and virus definitions file updating. There is no dependence on services from other computers to complete such operations. This occurs without compromising centralized control and configuration.
- When centralized initiation of an operation is necessary, Norton AntiVirus Corporate Edition minimizes the time required to start the operation on the affected computers. This maximizes parallel execution among protected computers.
- Norton AntiVirus Corporate Edition provides enterprise management functions that make it possible to define and configure virus protection across hundreds or thousands of protected computers through a single interface. This includes organizing protected computers into groups that can logically share virus protection policies and configuration settings.
- Norton AntiVirus Corporate Edition minimizes processing time and dependencies for all frequently and widely distributed operations.

The following scalability features address the design and implementation principles:

- Multithreading of virus definitions updates: You can run multiple virus update distribution processes simultaneously on a single server. Multithreading reduces the time-to-completion for virus definitions updates to large groups.
- Independent, server-driven client configuration updates: Client configuration updating used to be initiated by client check-in processing. In Norton AntiVirus Corporate Edition, it is driven intelligently from the server when configuration updates are received from the management console. In addition, client configuration updates are multithreaded.

- Smart server task queue management: The Norton AntiVirus Corporate Edition task queue for each server is now checked for redundant tasks before new tasks are added. This change, combined with server-driven configuration updating, makes client configuration updating faster. It also eliminates server update processing spikes that occurred when a client configuration update could not be initiated before the client checked in again.
- 3,000 workstation clients per Norton AntiVirus Corporate Edition server: It is now possible on a typical 100 MB network to connect up to 3,000 clients to a single Norton AntiVirus Corporate Edition server and still meet time-to-completion requirements for critical server-initiated operations. This includes virus definitions updates.

Not every installation will achieve the 3,000-clients-per-server ratio. However, virtually every installation will provide significantly higher client-to-server ratios and better performance.

Where to get more information for scalability planning

Plan your implementation of Norton AntiVirus Corporate Edition on your network to ensure that you take full advantage of scalability features.

For more information, see [“Scalability planning information”](#) on page 391.

The following issues are addressed:

- How to get optimum performance and scalability from Norton AntiVirus Corporate Edition
- Client-to-server ratios
- Number of threads for update operations
- Virus definitions updating
- Client configuration (Grc.dat) updates
- Remote Windows NT/2000 client installation and updates
- Additional thread configuration guidelines
- Norton AntiVirus Corporate Edition server specifications
- Typical Norton AntiVirus Corporate Edition servers
- Client check-in interval
- Scalability of other Norton AntiVirus Corporate Edition operations

Required protocols

Norton AntiVirus Corporate Edition uses an adaptive communication method that handles both IP and IPX communication at any time. Two benefits of this new method are that Norton AntiVirus Corporate Edition does not require or create NetWare SAPs, and Norton AntiVirus Corporate Edition is compatible with IP-only networks. Though this new communication method is flexible, certain combinations of mixed protocols prevent proper client or server communication.

If you are managing computers running Norton AntiVirus Corporate Edition on both Windows NT and NetWare operating systems, you need the following protocols installed on the computer that is running Symantec System Center:

- TCP/IP
- IPX

Configuring options and running operations

You can configure options and run Norton AntiVirus Corporate Edition operations for a server group, single server, multiple servers, or one or more clients.

To apply to a server group

- 1 In the console tree, right-click the server group icon, then click **All Tasks > Norton AntiVirus**.
- 2 Click a specific menu item.

To apply to a single primary or secondary server

- 1 In the console tree, click the server group.
- 2 In the right pane, right-click the server and click **All Tasks > Norton AntiVirus**.
- 3 Click a specific menu item.

To apply to one or more servers

- 1 In the console tree, click the server group icon.
- 2 In the right pane, shift-click to select multiple servers.
- 3 Right-click the highlighted servers and click **All Tasks > Norton AntiVirus**.
- 4 Click a specific menu item.

To apply to one or more clients

- 1 Double-click the server group icon.
- 2 In the console tree, click the server.
- 3 In the right pane, shift-click to select multiple clients.
- 4 Right-click the highlighted clients and click **All Tasks > Norton AntiVirus**.
- 5 Click a specific menu item.

Windows NT/2000 cluster server protection

You can protect and manage Windows NT/2000 cluster servers with Norton AntiVirus Corporate Edition.

To protect cluster servers, you complete the following tasks:

- Install the Norton AntiVirus Corporate Edition client to each local computer that is part of the cluster server.
Do not install the client to the shared drives.
- Roll out clients using the local server names rather than the shared cluster name.

Each client is managed separately and provides protection in the event of a fail over. You can synchronize the manageability of the clients if they point to the same Norton AntiVirus Corporate Edition server and configuration is performed at the server level.

The shared drives are protected in realtime by each computer's Realtime File System Protection when the computer has control of the drives. When control of the shared drives is passed to another computer, that computer's realtime file scanning automatically takes over the protection.

If a manual scan of the shared drives is being performed when a fail over occurs, the scan does not restart on the new computer. You must initiate a new scan.

If one client in the cluster is down temporarily, it receives the latest virus definitions when RTVScan starts and the client checks in with the parent.

Logging and alerting include the name of the local computer and not the cluster server name. This helps to identify which computer had the event.

Note: Problems might occur if the Norton AntiVirus Corporate Edition server or client is installed to the shared drive. For example, only one client and the shared drives will be protected. Also, manageability is lost after a fail over.

NetWare cluster server protection

You can protect and manage NetWare cluster servers with Norton AntiVirus Corporate Edition.

To protect cluster servers

- Launch Norton AntiVirus Corporate Edition after all volumes have been mounted and cluster services have been started in the Autoexec.ncf file.

Launching Norton AntiVirus Corporate Edition once these other tasks are completed ensures that all volumes are detected.

Product installation order

Install products in the following order:

- Install Symantec System Center before you install the Norton AntiVirus Corporate Edition management snap-in.
- Install the Norton AntiVirus Corporate Edition management snap-in before you attempt to manage Norton AntiVirus Corporate Edition from the Symantec System Center console.
- Roll out Norton AntiVirus Corporate Edition to servers before you roll out Norton AntiVirus Corporate Edition to clients. If you install to clients first, they will not be able to connect to a Norton AntiVirus Corporate Edition server and will run in unmanaged mode.

For an explanation of managed mode versus unmanaged mode, see [“Managed clients”](#) on page 27 and [“Unmanaged clients”](#) on page 28.

- Install other products and utilities in the order that works best for you.

Staged installations

A staged installation method is common for larger organizations and involves first installing the Norton AntiVirus Corporate Edition to a test server, then expanding to additional groups of servers in stages over a period of time so that any potential issues within your environment are discovered prior to a full-scale deployment.

Start installing managed clients after you install the Norton AntiVirus Corporate Edition to one or more servers, or install all servers first and then all clients.

Variations of the staged installation method include installing to Windows NT/2000 servers, then NetWare servers, or just to Windows clients. You can then include other operating systems to work out any issues on a per-platform basis.

Learning about Norton AntiVirus Corporate Edition in a lab setting

Before you perform a full-scale installation, install Norton AntiVirus Corporate Edition to a non-production lab environment for a learning and evaluation period. This lets you address any issues before full enterprise deployment.

You can plan and install Norton AntiVirus Corporate Edition to a limited-lab environment, or plan and roll out Norton AntiVirus Corporate Edition to your production network.

Procedures for evaluating server components

To get the most out of a trial run when testing Norton AntiVirus Corporate Edition on servers, install to at least two servers, mixing Windows NT and NetWare if needed. The communication protocols in your test environment should match those in your production environment. Include routers in your test environment (particularly for mixed protocol environments). Perform a complete install to each server, including AMS². Install Symantec System Center to at least one 32-bit client. Create at least one server group that contains two or more servers.

If you are migrating from Intel LANDesk Virus Protect, see [Chapter 7, “Updating Norton AntiVirus Corporate Edition”](#) on page 191.

Windows NT Workstation limitations

The maximum number of other computers that can simultaneously connect over the network to Windows NT Workstation 3.5, 3.51, and 4.0 is 10. This limit includes all transports and resource sharing protocols combined. This limit is also the number of simultaneous sessions from other computers that the system is permitted to host and does not apply to the use of administrative tools that attach to the system from a remote computer.

This limitation applies only to inbound connections to Windows NT Workstation 3.5, 3.51, and 4.0. When you use Windows NT Workstation 3.5, 3.51, and 4.0, unlimited outbound connections can be established to other computers.

Any file, print, named pipe, or mail slot session that does not have any activity on it will be disconnected after the AutoDisconnect time has expired. The time expires after 15 minutes, by default. Once the session is

disconnected, one of the 10 connections will be available so that another user can connect to the Windows NT Workstation computer.

Lower the AutoDisconnect time to reduce the issues users might encounter with the 10-connection limit on a computer that is not used heavily for server purposes.

To avoid losing the server service's self-tuning capability, change the AutoDisconnect time using the Registry Editor rather than from a command line or from Control Panel Network.

After installing to the servers

After you have installed to the servers, take the following steps:

- Configure all the different scans for maximum protection (all files, all drives, and so on).
- Test virus definitions file downloads and server-to-server updates.
- Create a virus test file (not a real virus) to see how the virus-catching mechanisms work without introducing a real virus on your computer.

For more information, see [“Creating a virus test file”](#) on page 76.

- Let scheduled scans and other automated functions run for several days.
- Verify that Symantec System Center can view servers on both sides of routers.

For more information, see [“Required protocols”](#) on page 71.

- Verify that log files and reports accurately reflect the expected data.

Creating a virus test file

To create a text file that will be detected as a virus, which you can use to verify detection of viruses, logging, and alert functioning, copy the following line into a separate file, saving it as Trigger.com This file is not a virus, but will be detected as the EICAR Test String.⁷⁰ Disable realtime file protection temporarily before saving the file.

```
X5O!P%@AP[4\PZX54(P^)^7CC)7)$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Do not include spaces above, below, in front of, or behind this string. Spaces might prevent the string from being detected.

Procedures for evaluating client components

Test client programs in a nonproduction environment to locate any potential problems that might interfere with productivity. Perform tests in a nonproduction environment with a hardware and software setup that matches the production environment closely.

- Install to all operating systems that you expect to use.
- Install to connected and standalone clients if necessary.
- Match all IP/IPX protocol combinations that exist in your environment.
- Match client to server OS combinations (for example, Windows NT workstation logging onto NetWare servers, and so on).
- Hardware setup should reflect minimum and maximum configurations.

If you're migrating from Intel LANDesk Virus Protect, see [Chapter 7](#), "Updating Norton AntiVirus Corporate Edition" on page 191.

After installing to client computers

After you have installed Norton AntiVirus Corporate Edition to the computers in your lab environment, complete the following tasks:

- Configure all of the different scans for maximum protection (all files, all drives, and so on).
- Test virus definitions file downloads.
- Use a virus test file that you create to trigger the alerting system.
For more information, see ["Creating a virus test file"](#) on page 76.
- Let scheduled scans and other automated functions run for several days.
- Verify that Symantec System Center can view clients on both sides of routers.
For more information, see ["Required protocols"](#) on page 71.
- Verify that connected clients appear in the Symantec System Center view under the correct parent server.
- Lock some client scanning parameters using Symantec System Center and verify that clients cannot change these settings.
- Launch a virus sweep and verify that the client scans take place.
- Verify that log files and reports reflect the expected data.

Scanning configuration trade offs

This section describes some of the main configuration options available in Norton AntiVirus Corporate Edition and provides additional information about security implications and network overhead.

For details on how to enable configuration options, see [“Scanning for viruses”](#) on page 289.

What to scan

As you create your anti-virus policy, decide which types of files to scan.

Scans based on file type

In theory, you should only need to scan files infected by viruses. However, there is no sure way to know which files are infected. Continuously scanning all files is the most secure approach, but is not practical. The best approach is to layer your scanning and target those files or system areas that are most likely to contain viruses. To know what should be scanned, you must understand what the threats are and how likely you are to encounter them. Viruses fall into three general categories: boot sector, .com and .exe, and macro viruses.

Boot sector viruses

Boot sector viruses reside in system areas of hard and floppy disks. This category also includes master boot record, or partition sector viruses. This type of virus only spreads from floppy disk to hard drive when a computer attempts to start from the floppy disk. Once the virus is memory resident, some or all floppy disks accessed become infected.

Boot sector viruses were the most common virus type and accounted for about 22 of the 25 most common viruses reported. These viruses thrived on DOS and Windows 3.1 computers. Since the growth of computers running Windows 95 and Windows NT, the growth rate of boot sector viruses has declined because many of these viruses cannot spread on these operating systems. In addition, users are generally warned by the operating system when one of these viruses is present, either by a warning message or system malfunction.

.com and .exe viruses

.com and .exe viruses infect any files containing executable code. File types that contain executable code can be difficult to identify by their file extensions, but typically they are .bin, .com, .dll, .doc, .dot, .exe, .sys, and .xls. The growth rate of these viruses is declining for some of the same reasons that boot sector viruses are in decline. Many of the older common viruses cannot spread under some of the new operating systems. However, these viruses still present a significant threat and can spread quickly.

Macro viruses

Macro viruses represent the newest virus category and are spreading faster than any previous category of viruses. Macro viruses use the macro language of an application so that the application environment is in a sense the operating system for the macros. Macro viruses are becoming increasingly deviant and can jump from the application environment to the operating system.

The majority of macro viruses are targeted at Microsoft Word. Macro viruses for Microsoft Excel are also becoming common. Though no other applications are currently being targeted, macro viruses can spread under any application that supports the Visual Basic programming language. In addition, any application that supports a macro or scripting language is a target for virus writers. Macro viruses have complicated the task of configuring anti-virus programs because the number of file extensions that might need to be scanned is infinite. Unless you know that all of your users maintain the default file extensions (for example, .doc, .xls), you might need to scan all extensions, which can increase the overhead associated with scanning.

Scans for compressed files

The contents of compressed files are scanned, by default, with on-demand scans on servers and on-demand, scheduled custom, and startup scans on clients. Email realtime protection scans within compressed files.

Because of the processing overhead, file system realtime protection does not scan files within the compressed files. File system realtime protection does, however, scan files as they are extracted from compressed files.

Scans of drives

Scan all drives on a regular basis because any drive might contain a virus. If users don't have write access to some drives, scan these drives less often (for example, weekly instead of daily). CDs should also be scanned at least once. There are cases in which viruses have shipped on commercial CDs from both large and small companies.

Exclusions

Exclusions let you further customize your protection. You can exclude by folder, file name, or file extension.

Norton AntiVirus Corporate Edition can check for specified exclusions before or after the scan runs.

For more information about exclusions, see [“Setting options that exclude files from scanning”](#) on page 301.

When to scan

As you create your anti-virus policy, you must decide when to scan files. Norton AntiVirus Corporate Edition provides you with opportunities to scan servers and clients for viruses. Protect your servers by enabling realtime scanning and performing a nightly full-server scan.

Client protection is not as simple as server protection because there are many computing environments and requirements. Norton AntiVirus Corporate Edition provides a wide range of overlapping options that let you select the scanning method that works best for your environment.

A layered approach lets you use several scan types to achieve a satisfactory protection level without imposing too much overhead or delay at any one time. You can do a complete drive scan at start-up or program start-up for all computers, and at logon time for Windows 3.1 and DOS computers. You also can rely on a scheduled client scan to do a complete or partial drive scan.

Note: Startup scans are not managed or configured from the Symantec System Center console. You can configure startup scans directly from Norton AntiVirus Corporate Edition. For more information, see the Norton AntiVirus Corporate Edition help system. Use the keyword startup to find related topics.

- Run VSCAND from Autoexec.bat to scan memory and the boot sector only. This ensures that you are free from boot sector viruses and other system viruses before other programs load while imposing very little delay to system start-up. This should allow users quick access to their computers and reduce the urge to circumvent their local protection.
For more information about VSCAND, see [“Virus Scan for DOS”](#) on page 455.
- Run VSCAND from the logon script to perform a full or partial drive scan using the selected extension list. You can configure the scan to run once a day, once a week, or at another interval that you specify.
- You can also run a limited scan of directories and use a lunch time scheduled scan to perform a complete drive scan. The realtime scanning detects any viruses encountered between complete drive scans.
- If you rely on scan methods that users cannot defeat, your options are logon scan, a start-up scan from the Norton AntiVirus Corporate Edition 16-bit or 32-bit clients, scheduled scan, virus sweep, and realtime scan.

Scan files being modified

The scan files being modified option alerts you any time a virus attempts to infect a file. Because there are fewer files being modified on a regular basis, you might want to select all files to be scanned or make a more inclusive selected extension list.

Scan files being accessed and modified

The scan files being accessed and modified option detects viruses before they load into memory. However, scanning all files accessed imposes more overhead than scanning only files being modified as fewer files are modified than accessed. If possible, use the selected extension list for this option to minimize the impact. You might need to add .tmp or similar extensions to let the realtime scanner detect viruses in files that are first written to temporary files.

Default virus handling actions

Norton AntiVirus Corporate Edition provides the following default virus handling actions:

- When a virus is detected, Norton AntiVirus Corporate Edition cleans it. If the clean operation fails, the infected file is moved to Quarantine on the local computer.
- For each type of scan, all files are scanned.

You might want to handle infected files differently. For example, you might want Norton AntiVirus Corporate Edition to fix macro viruses automatically but ask you what action to take when a program file virus is detected. This gives you greater control over the repair.

For information about configuring actions on detection of a virus, see [“Assigning actions and backup actions for detected viruses”](#) on page 296.

Client email scans

This version of Norton AntiVirus Corporate Edition supports scanning of email attachments on client computers. Norton AntiVirus Corporate Edition protects the following products:

- 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

For more information, see [“Installing email support”](#) on page 138.

Management policy planning

You may want to establish some policies related to managing with Symantec System Center. Consider the following issues.

Server group locking

You can lock a server group with a password to prevent unauthorized administrators from making configuration changes. What server groups do you want to lock? Who will have the password?

For more information, see [Chapter 8, “Locking and unlocking server groups”](#) on page 220.

Event management

What types of alert actions do you want to configure for events?

Do you want to set up a single centralized alert server per site, or do you want alerts to go to more than one administrator?

For more information, see the *Symantec System Center Implementation Guide*.

What else do I need to plan for?

If you are installing Symantec products to be managed by Symantec System Center, you may have additional planning considerations. For example, how will you and other administrators roll out, administer, and maintain the products? What settings do you want to lock for the products?

Some additional considerations:

- Although Symantec System Center is a good WAN management tool, it is not designed for use as a WAN distribution tool. The NT Client Install option available from the Symantec System Center Tools menu should not be used to distribute across a WAN.
- Plan server groups around WAN links so that the client/server and server/server communication is all kept within the LAN.

How Terminal Servers are protected

Norton AntiVirus Corporate Edition 7.6 for Windows NT/2000 Servers runs on Terminal Servers in much the same way that Norton AntiVirus Corporate Edition works on Windows NT/2000 file servers. Only alerting differs.

Alerts work for users who are logged on to the server console. Users who are connected through a terminal client session do not receive alerts.

Viewing Terminal Servers from the console

Terminal Servers appear the same as file servers in the console from which they are managed. Both types of servers are represented with the same icon in the Symantec System Center console.

Terminal Server and Terminal Services limitations

The following limitations apply to Terminal Server and Terminal Services protection:

- Norton AntiVirus Corporate Edition does not protect mapped drives on clients that can be accessed by applications running during a session on the Terminal Server.
- The realtime file system protection running on the Terminal Server does not detect virus events, such as saving an infected file, that occur on local client drives.
- Norton AntiVirus Corporate Edition does not provide functionality to Terminal Server clients. For example, Norton AntiVirus Corporate Edition does not route alerts to the proper client session, or allow for Symantec System Center to run within a session.
- Vpstray.exe is the program that displays Norton AntiVirus Corporate Edition Realtime Protection status in the system tray. Launching Vpstray.exe per session is not feasible when scaling to a large user base due to the large footprint required for each session. Vpstray.exe does not run if the session is remote but it does run on the Terminal Server console.

- When a user logs off of a remote terminal session, and the realtime setting to check floppy disks on computer shutdown is enabled, an unnecessary access is made to the floppy disk drive on the console. This setting is disabled by default.
- Session-specific information is not logged or included in virus alerts.

Preventing user-launched scans

Manual scans of servers running Windows NT version 4.0 Terminal Server Edition or Windows 2000 Terminal Services are not supported. These scans cannot be blocked.

To address this issue, you can do the following:

- Restrict the Windows Start menu icon display and directories for Norton AntiVirus Corporate Edition to prevent users from running manual scans.
- Use the Application security registration utility (AppSec) to restrict non-administrator users to running only the programs that are included in an administrator-defined list of applications.

Installing AppSec

You can install AppSec for the Windows NT 4.0 Terminal Server Edition or for Windows 2000 Terminal Services.

For Windows NT 4.0 Terminal Server Edition, AppSec installs automatically when you install Windows NT version 4.0 Terminal Server Edition.

For Windows 2000 Terminal Services, AppSec is included in the Windows 2000 Server Resource Kit.

You must install both AppSec and the AppSec hotfix.

You can find information about installing AppSec and the hotfix at:

<http://www.microsoft.com/windows2000/library/resources/reskit/tools/hotfixes/appsec-o.asp>

Preventing users from launching a scan via a terminal session on the server

You can prevent users from scanning in a terminal session on a Windows NT 4.0 Terminal Server Edition server or a Windows 2000 Terminal Services server.

To prevent users from launching a scan from a Windows NT Terminal Server

- 1 On the Terminal Server, click **Start > Programs > Administrative Tools > Application Security**.

The Authorized Applications dialog box appears.

- 2 In the Security group box, click **Enabled**.

Users are denied access to all programs that are not included in the Authorized Applications list, including the Norton AntiVirus Corporate Edition scanner.

To prevent users from launching a scan from a Windows 2000 terminal server

- 1 On the Terminal Server, click **Start > Programs > Windows 2000 Resource Kit > Tools**.
- 2 Double-click **Alphabetized List of Tools**.
- 3 Click **Application Security**.

The Authorized Applications dialog box appears.

- 4 In the Security group box, click **Enabled**.

Users are denied access to all programs that are not included in the Authorized Applications list, including the Norton AntiVirus Corporate Edition scanner.

Limiting access to the Norton AntiVirus Corporate Edition registry key on Windows NT 4.0 computers

With default permissions set on a Windows NT 4.0 computer, all users can modify the data stored in the registry for any application, including Norton AntiVirus Corporate Edition.

To resolve this security problem, remove the permissions that give users open access to the registry. The Reset ACL tool (ResetACL.exe) removes the permissions that allow full access by all users to the following Norton AntiVirus Corporate Edition registry key and subkeys:

HKLM\SOFTWARE\Intel\LANDesk\VirusProtect6\CurrentVersion

To use the Reset ACL tool, complete the following tasks:

- Roll out Resetacl.exe, which is located on Disk 1 in the Admttools folder, to Windows NT 4.0 computers that are not secure.
- Run Resetacl.exe on each Windows NT 4.0 computer.

After running Resetacl.exe, only users with Admin rights can change the keys.

Trade-off considerations for the Reset ACL tool

While the Reset ACL tool boosts security for Norton AntiVirus Corporate Edition on Windows NT 4.0 computers, several trade-off considerations exist.

In addition to losing access to the registry, users without Admin rights cannot run the following operations:

- Start or stop the Norton AntiVirus Corporate Edition service.
- Run LiveUpdate.
- Schedule LiveUpdate.
- Configure Norton AntiVirus Corporate Edition. For example, they cannot set realtime protection or email scanning options.

The options associated with these operations are dimmed in the Norton AntiVirus Corporate Edition interface.

In addition, users can modify scan options, but the changes are not saved in the registry nor are they processed. Users can also save manual scan options as the default set but the options are not written to the registry.

Central Quarantine

The Quarantine is a key component of anti-virus policy. By default, Norton AntiVirus Corporate Edition clients are configured to isolate infected items that cannot be repaired in the Quarantine. Any suspect file can be quarantined manually. From the Quarantine, these items can be submitted to Symantec Security Response via email or the Internet for analysis. If a new virus is identified, updated virus definitions are returned to you.

With a centralized Quarantine, infected files on client computers are forwarded to the Quarantine server with no user intervention. When new virus definitions arrive, they are tested in the Quarantine before they are distributed to clients.

You can set up a Quarantine server and enable Quarantine forwarding on servers and clients to copy infected files to your centralized Quarantine server. The file is isolated safely in the client's local Quarantine. A copy of the file is sent to the Quarantine server.

For more information about Central Quarantine, see [Chapter 12, “Managing virus infections”](#) on page 355.

Submit new viruses and get a rapid solution

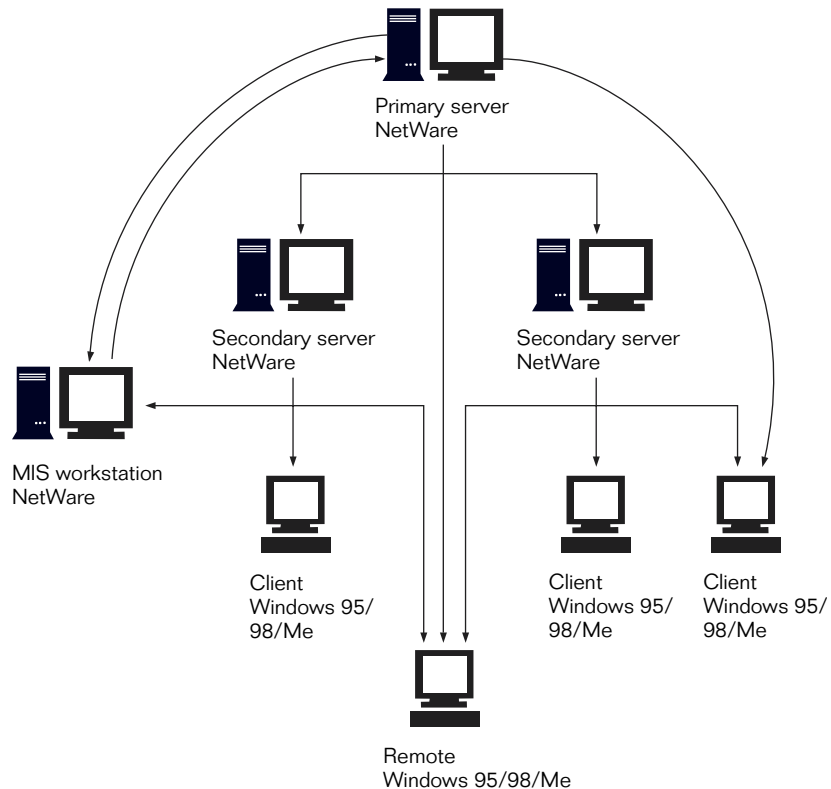
Use the Scan and Deliver feature to submit infected files to Symantec Security Response via the Internet feature, or by email. Symantec AntiVirus Research Automation (SARA) provides automatic virus sample analysis and virus definitions creation. This ensures that you receive a rapid solution to your virus infection problem.

For information on Scan and Deliver and SARA, see [Chapter 12, “Managing virus infections”](#) on page 355.

Customer profiles

The following profiles demonstrate how Norton AntiVirus Corporate Edition protection is implemented and managed in different organizations.

Profile 1: Medium-sized organization



This organization has one main office and several remote users. The organization's environment includes the following:

- The organization has a total of 600 workstations, 98% of which are Windows 95/98/Me. MIS uses Windows NT for personal desktop workstations.
- Several users work remotely from their home computers, which run Windows 95/98/Me.

- There are no Windows NT servers in the organization. Currently, 100% of the organization's servers are NetWare.
- Microsoft Word and Microsoft Excel are in wide use.

How they roll out Norton AntiVirus Corporate Edition

- Norton AntiVirus Corporate Edition is silently installed to each workstation from a logon script. The logon script identifies the operating system running on each computer and installs Norton AntiVirus Corporate Edition if it has not already been installed.
- Remote users are given a CD to install an unmanaged Norton AntiVirus Corporate Edition.

How they manage alerting

- AMS² is installed on the primary server. An email is sent to an administrator's account when a virus is found.
- AMS² logs are monitored from the Symantec System Center for events or viruses that might require extra attention.

How they protect their environment from viruses

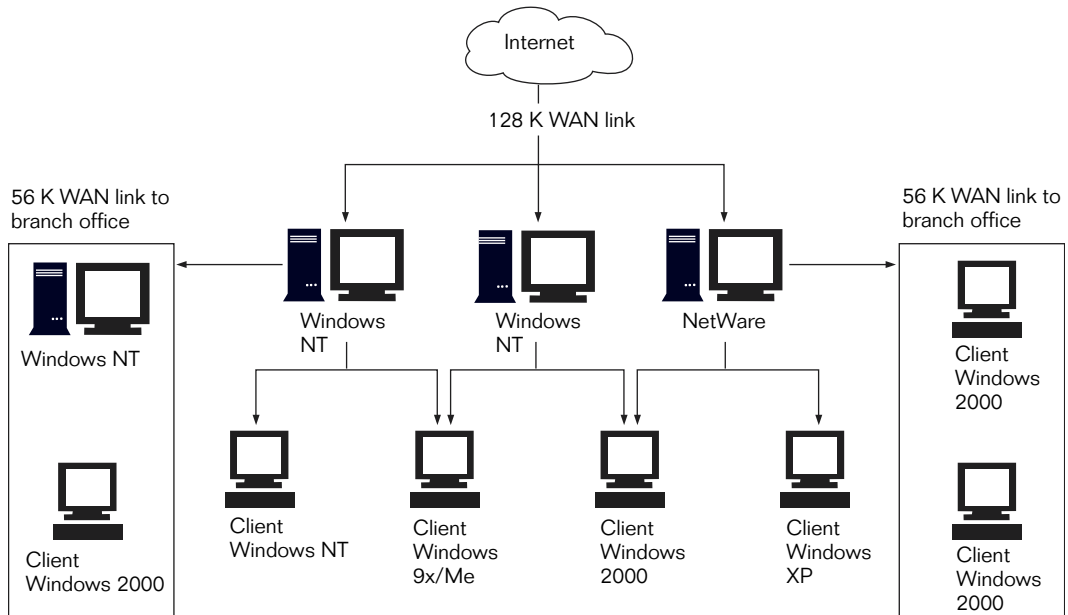
- The Norton AntiVirus Corporate Edition server program is installed on NetWare servers.
- All workstations are protected by Norton AntiVirus Corporate Edition for desktops. The workstations use the Norton AntiVirus Corporate Edition options defined by MIS. MIS locks Norton AntiVirus Corporate Edition options to prevent users from changing how Norton AntiVirus Corporate Edition protects their computers from viruses.
- MIS has installed Symantec System Center on a Windows NT Workstation for anti-virus administration.
- All workstations are managed by a single parent server. One nonproduction NetWare server was selected to be a parent server in order to save resources on the production servers.
- Remote workstations are unmanaged. These users are responsible for keeping their virus protection current. These users can change the way Norton AntiVirus Corporate Edition protects their computers from viruses.
- Virus alerts and definitions updates are monitored regularly from the Symantec System Center console. The administrator regularly checks the Event Log and Virus History for any events or viruses that might require extra attention.

- Most of the NetWare servers are file and application servers. Users access files on these servers often. To save resources, Norton AntiVirus Corporate Edition realtime scanning only scans files when they are modified. This decreases the impact of Norton AntiVirus Corporate Edition on a server with limited resources.
- The administrator has scheduled a Server Group Scan to scan all Norton AntiVirus Corporate Edition servers during nonproduction hours. The anti-virus scan is scheduled to run at a different time than the scheduled nightly backup so that they do not interfere with each other.
- The administrator has scheduled a weekly Client Scan.

How virus definitions are updated

- The NetWare servers cannot use the automatic virus definitions update method because they are not configured for FTP connections. The administrator uses a scheduled batch file to run twice a week. The batch file downloads the definitions file from the Symantec FTP site and copies it to the NAV directory on the primary server.
- Secondary servers automatically retrieve updates from the primary server.
- Most Norton AntiVirus Corporate Edition clients automatically receive virus definitions from their parent server using the Virus Definition Transport Method. When the parent server receives new virus definitions, it immediately begins sending the clients definitions updates. The parent server is able to update multiple clients at a time, and simultaneously updates one client on each subnet to reduce network traffic.
- Remote clients retrieve definitions updates from Symantec by running LiveUpdate.

Profile 2: Large organization

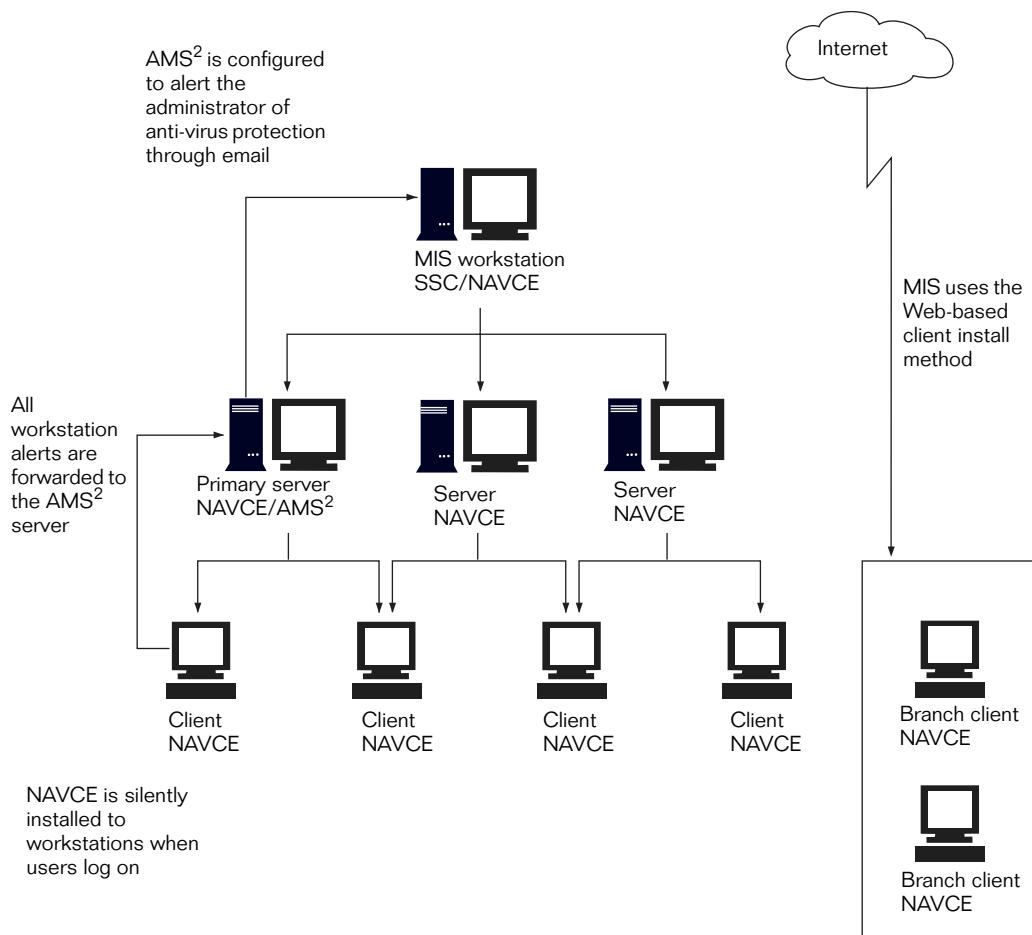


This organization has one corporate office and 50 branch offices scattered across the New England states. The organization's environment includes the following:

- The corporate office has 1,000 workstations. Each of the branch offices averages about 20 workstations.
- There are 120 servers in the organization, 95% of which are Windows NT and 5% are NetWare. Most of the servers are located at the corporate office, so many branch offices do not have a local server.
- The organization has a total of 2,000 workstations, 20% of which are Windows NT/2000 and 80% are Windows 95/98/Me.
- The branch offices are connected to the corporate office through a 56K WAN link, and the corporate office has a 128K link to the Internet. Because of limited bandwidth, it is important to keep network traffic on these links to a minimum.
- Microsoft Exchange, Microsoft Word, and Microsoft Excel are in wide use. The organization's workstations are highly susceptible to macro viruses and viruses spread through email.

How they roll out client installations

- The corporate office uses a logon script installation to local workstations. Norton AntiVirus Corporate Edition is silently installed on each workstation when the user logs on. The logon script identifies the operating system running on each computer and installs Norton AntiVirus Corporate Edition if it has not already been installed.
- The branch offices are unable to use a logon script installation because the bandwidth to the corporate office is limited. Users at the branch offices use a Web-based install method to install Norton AntiVirus Corporate Edition for desktops. MIS sent these users an email with instructions and a URL link to the Web-based installer.



How they manage alerting

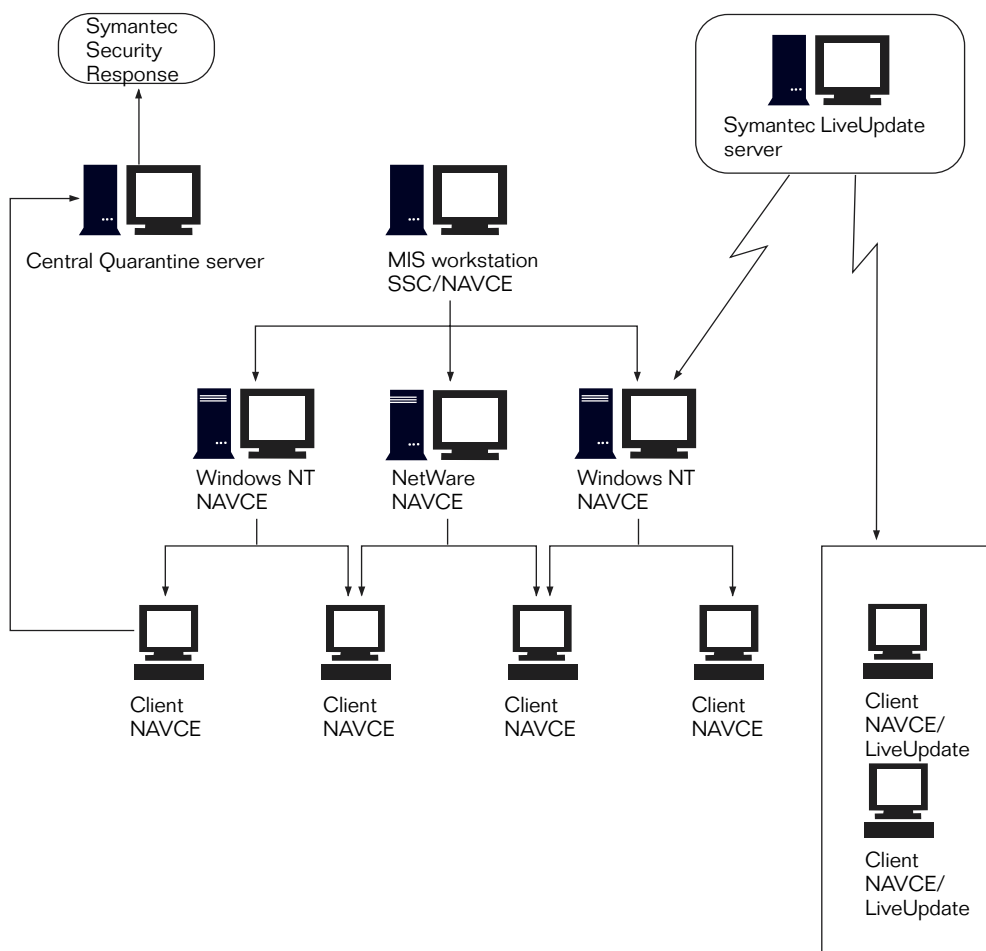
- The primary server is also an AMS² server. All workstation alerts are forwarded to this server.
- When a virus is found, AMS² emails the administrator in charge of anti-virus protection.
- AMS² logs are monitored from the Symantec System Center for events or viruses that might require extra attention.

How they protect their environment from viruses

- To guard their site from infections originating on the Internet, MIS runs Norton AntiVirus for Firewalls in conjunction with a CVP-compliant firewall program.
- The Microsoft Exchange server is protected by Norton AntiVirus for Microsoft Exchange.
- All NetWare servers are protected by Norton AntiVirus Corporate Edition.
- All Windows NT servers are protected by the Norton AntiVirus Corporate Edition server or client programs.
- All workstations are protected by the Norton AntiVirus Corporate Edition client program. The workstations use the Norton AntiVirus Corporate Edition options defined by the MIS group. Email is scanned by the Norton AntiVirus Corporate Edition email plug-in. MIS locks Norton AntiVirus Corporate Edition options to prevent users from changing the way their computers are protected from viruses.

- All workstations at the corporate office share one parent server, and all workstations located at branch offices share a different parent server. There are 1,000 clients attached to each parent server. These clients check in with their parent server every 100 minutes, averaging about ten clients checking in with the parent server every minute. Local and remote clients are separated into different client groups because they use different virus definitions updating methods.
- Windows NT Servers that do not act as parent servers are installed as Norton AntiVirus Corporate Edition clients under a special parent server. Users access files on these servers often. To save resources, Norton AntiVirus Corporate Edition realtime scanning only scans files when they are modified. This decreases the impact of Norton AntiVirus Corporate Edition on a server with limited resources.
- Norton AntiVirus Corporate Edition is configured to forward infected files that cannot be repaired to a Central Quarantine Server. The administrator submits suspicious files to Symantec Security Response for analysis. Symantec Security Response analyzes the file submissions and reports back to the administrator with new virus definitions or other solutions.
- All Norton AntiVirus Corporate Edition servers are under one server group. One of the Windows NT parent servers is designated as the primary server.
- Symantec System Center is installed at the corporate office so the administrators can configure anti-virus settings from a central location.

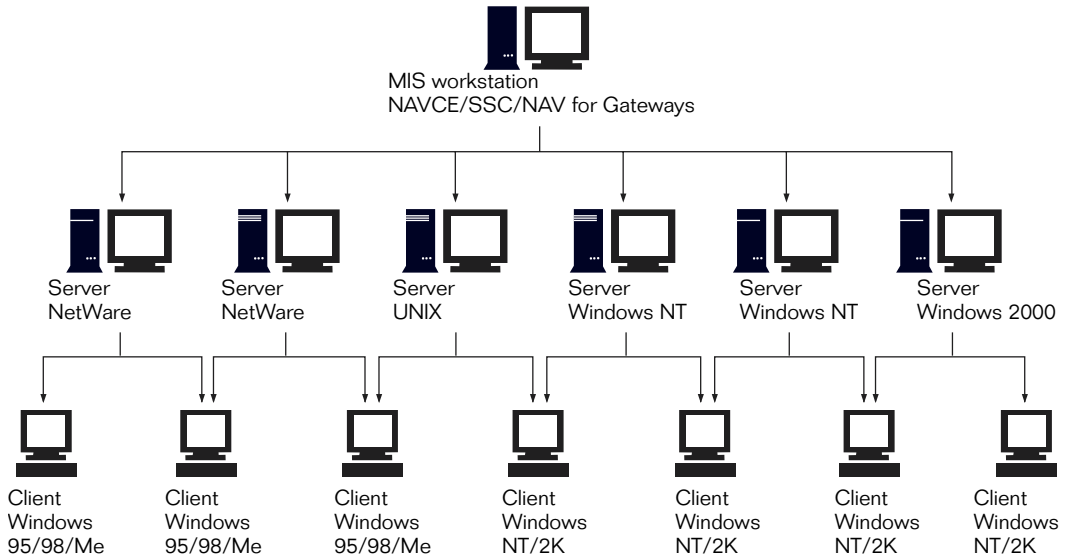
- The administrator has scheduled a Server Group Scan to scan all Norton AntiVirus Corporate Edition servers during nonproduction hours. The anti-virus scan is scheduled to run at a different time than the scheduled nightly backup so that they do not interfere with each other.
- The administrator has scheduled a weekly client Scan.



How virus definitions are updated

- The administrator has selected a Windows NT file server to act as a LiveUpdate server. The LiveUpdate Administration Utility pulls Norton AntiVirus Corporate Edition product updates and virus definitions files from the Symantec FTP site to the server in the corporate office. The local LiveUpdate server reduces traffic to the Internet.
- The LiveUpdate Administration Utility is scheduled to download new packages twice a week.
- The primary server retrieves definitions updates from the internal LiveUpdate server.
- Secondary servers retrieve definitions updates from the primary server.
- Clients at the corporate office retrieve virus definitions from their local parent server using the Virus Definition Transport Method. When the parent server receives new virus definitions, it immediately sends the clients definitions updates. The parent server updates multiple clients at a time, and simultaneously updates one client on each subnet to reduce network traffic.
- Clients at branch offices retrieve definitions from a LiveUpdate server at the corporate office instead of using the Virus Definition Transport Method. LiveUpdate retrieves a smaller definitions package, so network traffic between the branch and corporate offices is minimized.
- MIS has configured LiveUpdate to run nightly during nonproduction hours, at a randomly scheduled time. Users can also initiate a LiveUpdate from the Norton AntiVirus Corporate Edition interface.

Profile 3: Enterprise-sized organization



This organization has offices around the world. The organization has 150 offices in the United States, ranging from 20 to 3,000 employees. The organization's environment includes the following:

- 2,500 servers, of which 30% run NetWare, 45% Windows NT, 20% Windows 2000, and 5% Unix.
- The organization has a total of 35,000 workstations in the United States, of which 40% run Windows 9x/Me/XP and 60% run Windows NT/2000.
- Many Windows NT/2000 users do not have administrative rights to their workstations.
- Many of the Windows computers are laptops.
- MIS uses a software distribution utility to install software on all workstations.
- Lotus Notes, Microsoft Exchange, Microsoft Word, and Microsoft Excel are in wide use.

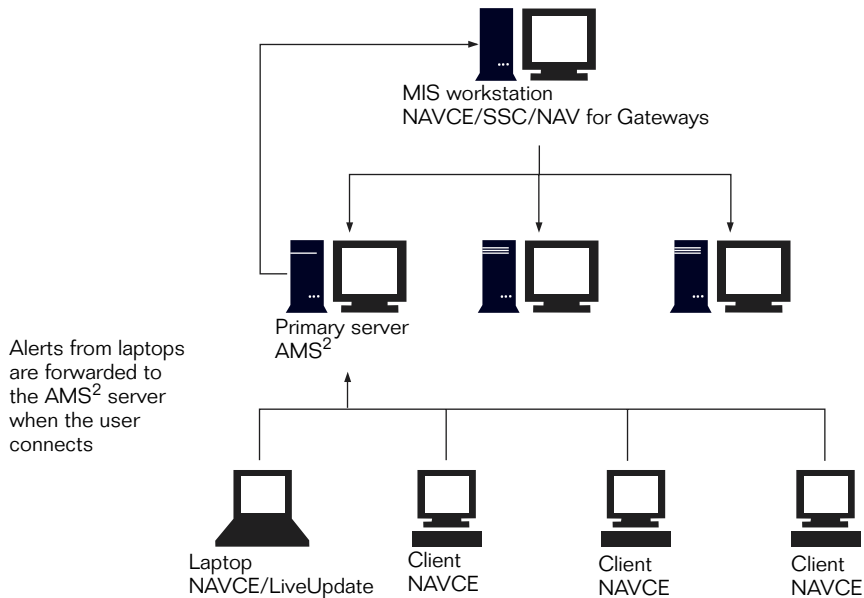
This organization uses Tivoli SecureWay Risk Manager 3.7, which ships with an adapter for Norton AntiVirus Corporate Edition. This adapter allows Tivoli SecureWay Risk Manager to read the Norton AntiVirus Corporate Edition event log. Information gathered and displayed by Tivoli SecureWay Risk Manager includes the following:

- Status of virus definition updates
- Historical information on scans
- Statistics regarding the number of infections within the organization

How they roll out Norton AntiVirus Corporate Edition

- MIS manages software distribution using a software distribution utility. MIS has created a Norton AntiVirus Corporate Edition installation package to silently install managed clients on every connected workstation. Different packages from different parent servers are distributed to each client group, depending on the location and special needs of those clients.
- MIS has created a special Norton AntiVirus Corporate Edition installation CD for laptop users containing a similar installation package.
- Small branch offices that do not utilize the software distribution utility use a Web-based install method to distribute the installation packages.

MIS sent these users an email with instructions and a URL link to the Web-based installer.



How they manage alerting

- The primary server in each server group is also an AMS² server. (Alert servers do not generate a lot of traffic.) All workstation alerts are forwarded to this server.
- When a virus is found, AMS² pages the local administrator in charge of anti-virus protection.
- Alerts from laptop users are forwarded to the AMS² server when the user connects to the network.

How they protect their environment from viruses

To guard their site from infections originating in Internet email, MIS runs Norton AntiVirus for Gateways.

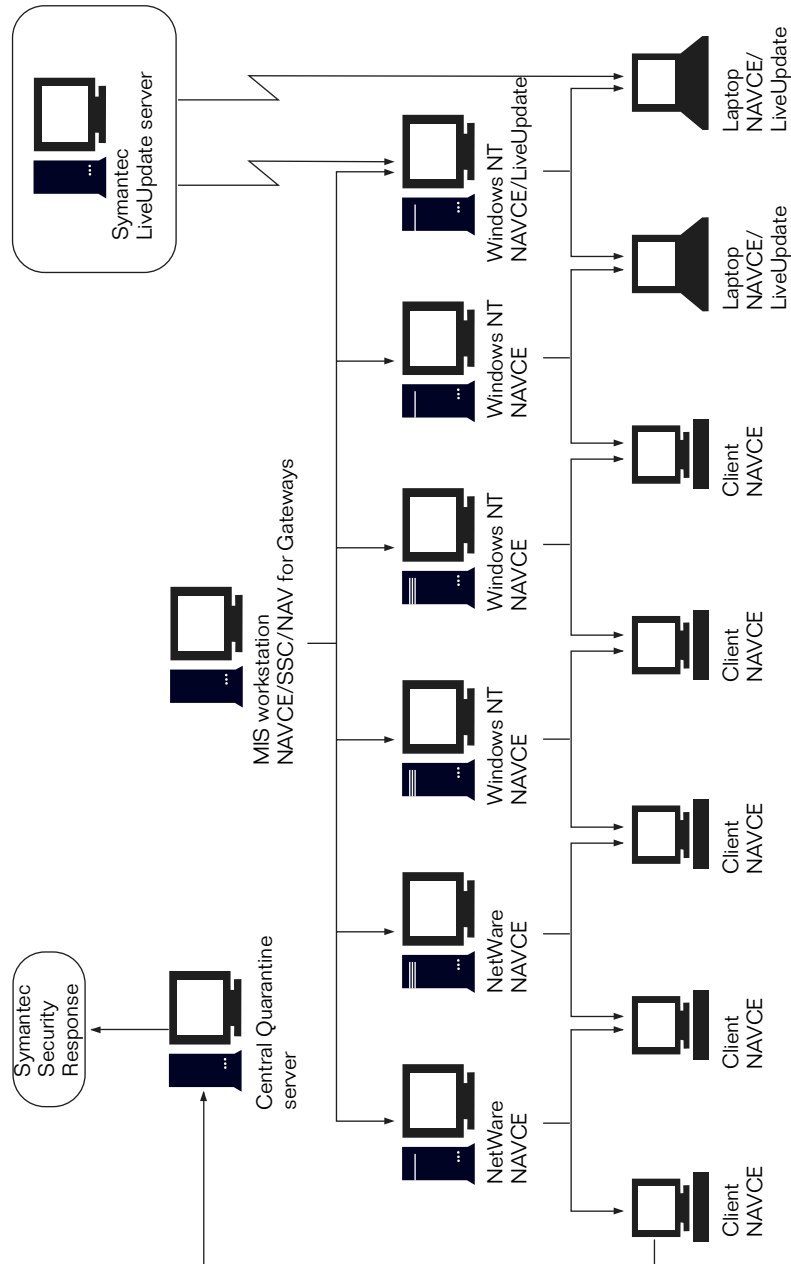
- Lotus Notes servers are protected by Norton AntiVirus for Lotus Notes.
- Microsoft Exchange servers are protected by Norton AntiVirus for Microsoft Exchange.
- All NetWare servers are protected by the Norton AntiVirus Corporate Edition server program.
- All Windows NT servers are protected by the Norton AntiVirus Corporate Edition server or client programs.
- All workstations are protected by the Norton AntiVirus Corporate Edition client program. The workstations use the Norton AntiVirus Corporate Edition options defined by MIS, including email client protection. MIS locks Norton AntiVirus Corporate Edition options to prevent users from changing the way Norton AntiVirus Corporate Edition protects their computers from viruses. Special anti-virus configurations are assigned to client groups with special needs, such as those where risk of viral infection is high or low.
- Each branch office is under a separate server group. The administrator at each site is responsible for the anti-virus protection at that site. Administrators at each office have the passwords for the server groups they are responsible for.
- Workstations at each branch office are managed by a parent server at the site where the workstations are located.
- Symantec System Center is installed at each office so the local administrators can configure anti-virus settings for the computers for which they are responsible.
- The development team is under a separate parent server because they have special needs. Their anti-virus options are less restrictive so they can disable anti-virus protection when necessary (for example, when compiling a program).
- Windows NT Servers not acting as parent servers are installed as Norton AntiVirus Corporate Edition clients under a special parent server. Users access files on these servers often. To save resources, Norton AntiVirus Corporate Edition realtime scanning only scans files when they are modified. This decreases the impact of Norton AntiVirus Corporate Edition on a server with limited resources.

- Laptop users share a parent server because they need specific options. These clients check in with their parent server frequently because they do not stay connected to the network for long. Checks in intervals of ten minutes ensure that these clients receive updated anti-virus configurations. When they do connect to the internal network via modem, Norton AntiVirus Corporate Edition checks for updates and receives a small settings file to update options.
- Workstations that do not fall into a special-needs category share a parent server. There are no more than 2,000 clients attached to each parent server. These clients check in with their parent server every 200 minutes, which averages to about 10 clients checking in with the parent server every minute.
- Norton AntiVirus Corporate Edition forwards unrepairable infected files to a Central Quarantine Server. The administrator submits suspicious files to Symantec Security Response for analysis. Symantec Security Response analyzes the file submissions and reports back to the administrator with new virus definitions or other solutions.
- The administrator has scheduled a Server Group Scan to scan all computers running the Norton AntiVirus Corporate Edition server program during nonproduction hours. The anti-virus scan is scheduled to run at a different time than the scheduled nightly backup so they do not interfere with each other.
- The administrator has scheduled a weekly Client Scan.

How virus definitions are updated

- One Windows NT Server in the central office is designated as a master primary server. This server receives definition updates from Symantec via a scheduled LiveUpdate.
- Primary servers in each server group retrieve definitions from the master primary server on a scheduled basis.
- In each server group, secondary servers retrieve definitions from the primary server.
- Most Norton AntiVirus Corporate Edition clients obtain virus definitions from their parent server using the Virus Definition Transport Method. When the parent server receives new virus definitions, it immediately sends the clients definitions updates. The parent server updates multiple clients at a time, and simultaneously updates one client on each subnet to reduce network traffic.
- Laptop users do not receive virus definitions from their parent server because the definitions file is large and can take a long time to transfer

across a dial-up connection. Laptop users can run LiveUpdate to the Symantec server so that they can update virus definitions when necessary.



Installing the Norton AntiVirus Corporate Edition server program, management snap-in, and console add-ons

This chapter includes the following:

- System requirements
- Preparing for installation
- Installing the Norton AntiVirus Corporate Edition server program
- Installing the Norton AntiVirus management snap-in
- Installing the Symantec System Center console add-ons
- Uninstalling

System requirements

This section contains information about system requirements for the following platforms or components:

- Norton AntiVirus Corporate Edition 7.6 for Windows NT/2000 Servers
- Norton AntiVirus Corporate Edition 7.6 for NetWare Servers
- Norton AntiVirus Corporate Edition management snap-in

Note: The Norton AntiVirus Corporate Edition server program cannot be installed to Windows XP. You must install the Norton AntiVirus Corporate Edition client program.

System requirements for Windows NT/2000 servers

- Windows NT Server 4.0 with Service Pack 3 or higher, Windows 2000 Server and Advanced Server; Windows NT Workstation 4.0 with Service Pack 3 or higher, Windows 2000 Professional.
- 32 MB RAM (64 MB or higher recommended)
- Intel Pentium processor (Pentium Pro or higher recommended)
- 62 MB free disk space for Norton AntiVirus Corporate Edition server files and 55 MB free disk space for the Norton AntiVirus Corporate Edition client disk image
- 10 MB free disk space for AMS² server files

For information about cluster server support, see [“Windows NT/2000 cluster server protection”](#) on page 72.

Windows Terminal Server compatibility

Norton AntiVirus Corporate Edition 7.6 for Windows NT/2000 Servers protects servers within your organization that are running Windows NT Server 4.0, Terminal Server Edition, and Windows 2000 Terminal Services.

Norton AntiVirus Corporate Edition client software does not install to servers running Windows NT Server 4.0, Terminal Server Edition or Windows 2000 Terminal Services.

Norton AntiVirus Corporate Edition runs under several platforms and clients.

Terminal Server and Terminal Services platforms

- Windows NT 4.0 Terminal Server Edition (with Service Pack 4 and above)
- Windows 2000 Server
- Windows 2000 Advanced Server

Thin clients

- Microsoft Terminal Server RDP (Remote Desktop Protocol) Client
- Citrix Metaframe (ICA) Client v. 1.8 and above

Thin client platforms

- Windows 95
- Windows 95 OSR2
- Windows 95 OSR2.1 (USB support)
- Windows 98
- Windows 98 SE
- Windows Me
- Windows NT 4.0 Workstation (Service Pack 4 and above)
- Windows NT 4.0 Server (Service Pack 4 and above)
- Windows NT 4.0 Server Enterprise Edition (Service Pack 4 and above)
- Windows 2000 Professional
- Windows 2000 Server
- Windows 2000 Advanced Server
- Windows XP Home Edition
- Windows XP Professional

MAC volumes not supported

Norton AntiVirus Corporate Edition does not support the scanning of MAC volumes on Windows NT 4.0 servers for Macintosh viruses.

System requirements for NetWare servers

- NetWare 3.12, 3.2, 4.11, 4.2, or NetWare 5.x
- 3 MB RAM (above standard NetWare requirements) for Norton AntiVirus Corporate Edition NLMs
- Required with NetWare 3.12: Streams.nlm v3.12 (or later), After311.nlm v4.12, and Clib.nlm v3.12g (or later)
- Required with NetWare 4.11 and 4.2: Support Pack 9
- 70 MB of free disk space for Norton AntiVirus Corporate Edition server files and 46 MB free disk space for the Norton AntiVirus Corporate Edition client disk image
- 10 MB free disk space for AMS² files (20 MB during installation)

Note: We recommend running the Novell client for NetWare on the computer from which Norton AntiVirus Corporate Edition is rolled out to NetWare servers.

NetWare SFT III not supported

Norton AntiVirus Corporate Edition is not supported on NetWare servers running SFT III.

Other NetWare requirements and considerations

Possible issue with Maple drivers

If you use the Microsoft 32-bit NetWare client (also known as Maple) driver on the computer you use to run the server Setup program, you cannot browse an NDS tree and install the Norton AntiVirus Corporate Edition server program to a NetWare container. You must select the server object, which installs Norton AntiVirus Corporate Edition in bindery mode.

You do not need to set a bindery context if you install into NDS.

NDS errors when installing to a NetWare 4.x server running an outdated Clib.nlm

If you install Norton AntiVirus Corporate Edition to a NetWare 4.x server with an outdated version of the Clib.nlm file, you will see these error messages:

Error importing NWDSCreateContextHandle

Error (0xa0000014)(-1610612716) initializing DS in DS Preliminaries

Error

Error: 0xa0000014(-1610612716) in line 255: [DSPROFILE]

Error

Error: Not authenticated with Novell Directory Services in line 278: [DSOBJECTS]

Use the latest Novell Clib.nlm file. This file is contained in the latest version of the NetWare update patch (LIBUPF or newer), which you can download from the Novell Support Web site:

<http://support.novell.com>

Install this patch on your NetWare 4.x server and reinstall Norton AntiVirus Corporate Edition to resolve this problem.

Requirements for forwarding infected files from NetWare servers to Quarantine servers

- For NetWare 3.12, Quarantine forwarding is not supported.
- For NetWare 4.x, Quarantine forwarding requires that Winsock 2.0 or later is installed on the NetWare server.

Temporary space required on the SYS volume

When scanning compressed archives (such as .zip and .arj files) on a NetWare server, Norton AntiVirus Corporate Edition first makes a call to NetWare to decompress one NetWare file at a time from the archive into a temporary directory on the SYS volume. Allocate enough free space in your SYS volume to accommodate the largest single compressed file (not the entire compressed archive) on your server.

System requirements for the Norton AntiVirus management snap-in

- The snap-in must be installed on the computer on which you installed the Symantec System Center console.
- 6 MB hard disk space.

Preparing for installation

You can roll out the Norton AntiVirus Corporate Edition server program to:

- Windows 2000 Professional or Windows 2000 Server
- Windows NT Server or Windows NT Workstation
- NetWare servers

Before you begin installing, you may want to review the topics that follow the installation procedure for information such as required rights and when restarts are necessary.

Installation order for Citrix Metaframe on Terminal Server

Norton AntiVirus Corporate Edition does not support drive remapping for Citrix Metaframe. If you plan to use Citrix Metaframe and remap your drives, complete these tasks in the following order:

- Install Citrix Metaframe.
- Remap the drives.
- Install Norton AntiVirus Corporate Edition 7.6 for Windows NT/2000 Servers.

Which computer should I use to run the server installation program?

You can run the installation program on computers running a Windows NT-based system.

Locating servers during installation

When you run the server installation program, you can browse for the servers to which you want to install. However, servers that are across routers might be difficult to locate. To verify that you can see a server when you run the server installation program, try mapping a drive to the server using Windows Explorer. If you can see a server in Windows Explorer, you should see the server when you run the server installation program.

Server browsing requires the use of the WINS (Windows Internet Name Service) protocol. For computers that are located in a non-WINS environment (such as a native Windows 2000 network that uses the LDAP or DNS protocol), you must create a text file with IP addresses, then import it to add servers to which you want to install.

For more information, see [“Creating a text file with IP addresses to import”](#) on page 111.

Creating a text file with IP addresses to import

You can create a text file that includes IP addresses that you want to import. During installation, you can import the contents of the text file to add the computers to the list of computers that you have selected for installation. This feature is useful for adding computers that are located in a non-WINS Windows NT or Windows 2000 environment.

Note: The Import feature is designed for use with Windows NT 4.0 and Windows 2000 servers only. It is not intended for use with NetWare.

To create a text file with IP addresses to import

- 1 Create a new text file using a text editor (such as Notepad).
- 2 Type the IP address of each server that you want to import on a separate line.
For example:
127.0.0.1
127.0.0.2
127.0.0.3
- 3 Save the file to a location that you can access when you run the server install program.

For more information about importing the text file contents, see [“Installing both the Norton AntiVirus Corporate Edition server program and Alert Management System”](#) on page 117.

Note: When necessary, you can comment out IP addresses that you do not want to import with a semi-colon (;) or colon (:). For example, if you included addresses in your list for computers that are on a subnet you know to be down, you can comment them out to eliminate errors.

Verifying network access and privileges

The computer you use to run the server installation program should have the appropriate network clients and protocols (IP and IPX/SPX) running so that you can see all the NetWare and Windows NT servers where you want to install Norton AntiVirus Corporate Edition.

The rights you need to install to server and client computers depend on the server platform and version.

Rights to install to Windows NT/2000 servers

During the installation, if you select a server to which you are not currently logged on, the installation program prompts you to log on. Log on as an administrator because the server installation program launches a second installation program at the server to create and start services and to modify the registry. You must have administrator rights for the server or for the Windows NT domain to which the server belongs.

Sharing must also be enabled on the Windows NT server where you install the Norton AntiVirus Corporate Edition server program. The installation program uses the default NT shares such as c\$ and admin\$. When you install Windows NT, these shares are enabled by default. If you changed the share names or disabled sharing to the default shares, the installation program cannot complete the server installation.

If you log on to a Windows NT/2000 domain and are put into a regular domain group without administrator rights over the local computer, you cannot install.

To reestablish the credential with the local computer

- From a DOS box, type the following command:
net use \\machinename\ipc\$/user:username password
Use this command to install if you are a local administrator with a different password than the domain administrator.

Installing to NetWare servers

The server installation program copies NLMs and other files to one or more NetWare servers that you select. Before you begin installation, log on to all servers to which you want to install. To install to NDS or bindery you need administrator or supervisor rights.

After running the server installation program, go to the server console (or have rights to run RCONSOLE) to load the Norton AntiVirus Corporate Edition NLMs. You only need to do this manually the first time if you select the automatic startup option during Setup.

To load the Norton AntiVirus Corporate Edition NLMs

- At the server console, type the following:
Load sys:\nav\vpstart.nlm /install

Installing to NetWare 4.x and 5.x servers

If you are installing to any NetWare 4.x or 5.x servers, the installation program prompts you to enter a username and password for the NDS container that you choose to hold logon scripts. Using Symantec System Center and your network administration tools, you can enable the logon scripts to automate client installation. You must have administrator equivalent rights to the container you designate.

Installing into NDS

If you browse to an NDS object to which you are not authenticated, the installation program would normally prompt you to log on. However, some versions of the Novell client might not return a logon request, and in this case the installation program will time out or stop responding. To avoid this problem, log on to the NDS tree before running the installation program.

From what operating systems can I run the installation program?

You can run the installation program only on computers running Windows 2000 or Windows NT 4.x (Workstation or Server).

Locating servers during installation

When you run the server installation program, you can browse for the servers to which you want to install. However, servers that are across routers and bridges might be difficult to locate. To verify that you will see a server when you run the server installation program, map a drive to the server using Windows Explorer. If you can see a server in Windows Explorer, you should see the server when you run the server installation program.

If you cannot see a NetWare server, have someone run the server installation program at another location where the server is visible. If you cannot see a Windows NT server, you can run the server installation program on the server.

Required restarts

This section describes the situations when a restart is required.

Windows NT server restart may be required after installation or update

As you install or update Norton AntiVirus Corporate Edition, the installation program displays a status for each server to report the progress of the installation or update, to alert you to any errors, and to prompt you for any required action. After an installation or update, the status is “Restart necessary for Windows NT servers” if the installation program needs to replace any files that are in use.

Specific cases where restart is required

There are a few instances where a restart is necessary:

- When installing AMS² to a Windows NT server, you must restart the computer after the installation program has completed in order for AMS² to run.
- When updating Norton AntiVirus Corporate Edition files on a Windows NT server (for example, when applying a service release), some files might be in use. In this case, you must restart the server to replace the older files.
- NetWare 3.12 servers require a restart if the Norton AntiVirus Corporate Edition installation program must update the version on CLIB on the server.

Understanding server installation options

The installation program lets you install Norton AntiVirus Corporate Edition server and administration software.

During the installation process, you will choose the computers to which you want to install. They will also be added to a single server group. Later, from Symantec System Center console, you can create new server groups and use drag and drop to populate them with the servers to which you installed.

When you install Norton AntiVirus Corporate Edition, the installation program installs Norton AntiVirus Corporate Edition NLMs to the NetWare servers (3.12, 3.2, 4.11, 4.2, and 5.x) that you select and installs services to the computers running Windows NT 4.x Server or Workstation that you select.

Initializing virus protection for Windows NT servers

The server Setup program copies files to the selected Windows NT servers. After the files are on each server, a second Setup program (Vpremove.exe), which requires no user input, must run on the server to create and start Norton AntiVirus Corporate Edition services and modify the registry.

Installing the Norton AntiVirus Corporate Edition server program

You can install the Norton AntiVirus Corporate Edition server program to:

- Windows 2000 Professional or Windows 2000 Server
- Windows NT Workstation or Windows NT Server
- NetWare servers

Before you begin installing, see [“System requirements”](#) on page 106 and [“Preparing for installation”](#) on page 110 for information that is needed for a successful installation, such as required rights and when restarts are necessary.

The instructions for installing the Norton AntiVirus Corporate Edition server program are presented in two separate procedures—for Windows NT/2000 servers and NetWare servers. You might, however, choose to install to both operating systems during the same installation process by selecting the appropriate servers.

Installing both the Norton AntiVirus Corporate Edition server program and Alert Management System

When installing Norton AntiVirus Corporate Edition to Windows NT/2000 servers or workstations, or NetWare servers, you can also install the Alert Management System² (AMS²) program that runs on every primary server.

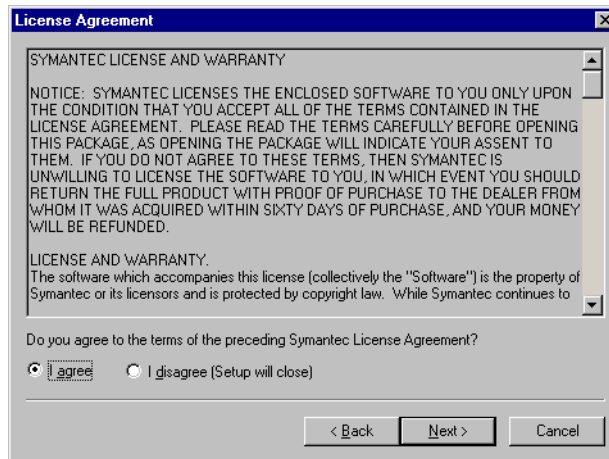
While AMS² is only required on the primary server to configure and view alerts, install AMS² to computers on which you install the Norton AntiVirus Corporate Edition server program. This lets you make any of these computers a primary server. If a secondary server needs to be made primary, AMS² events will not be lost.

For many of the actions that AMS² can take, you select the computer that will take that action. AMS² is required for some of the actions to run. Installing AMS² server on more computers allows you flexibility in choosing the computers that can take more advanced alert actions, such as sending pages.

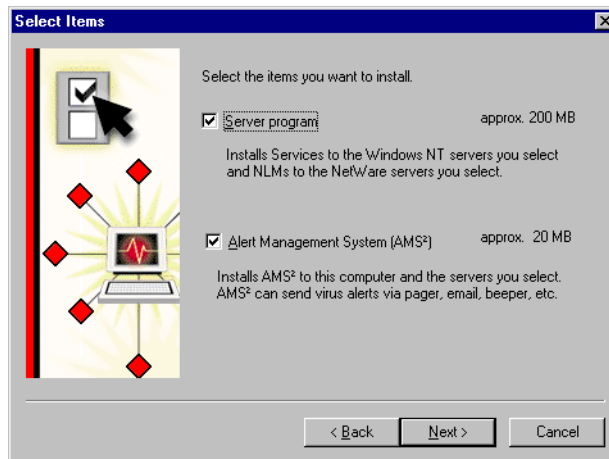
To install Norton AntiVirus and AMS² to Windows NT/2000 servers

- 1 Do one of the following:
 - From Disk 2, click **Install Norton AntiVirus To Servers**, then ensure that Install Norton AntiVirus **Server** is selected.
 - If you installed the Symantec System Center add-ons, from the Symantec System Center Tools menu, click **AV Server Rollout**.
- 2 Click **Next**.

- 3 Read the Symantec License and Warranty, then click **I agree**, and click **Next**.



- 4 Ensure that **Server program** and **Alert Management System (AMS²)** are checked, then click **Next**.



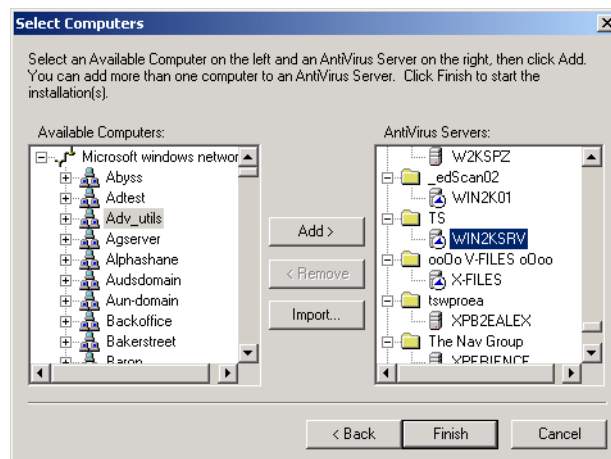
Only the primary server uses the AMS² files. If you select the AMS² option during setup, the service is installed on each server where you install the Norton AntiVirus Corporate Edition server program during that installation session. This lets you change primary servers without reinstalling AMS² on the new primary server. If you do not plan to change your primary server, uninstall the AMS² files from nonprimary servers.

Configure AMS² on the server using Symantec System Center and the AMS² programs that are loaded on the Symantec System Center server. If you do not select the AMS² option when installing Symantec System Center, you cannot configure alert actions on that server.

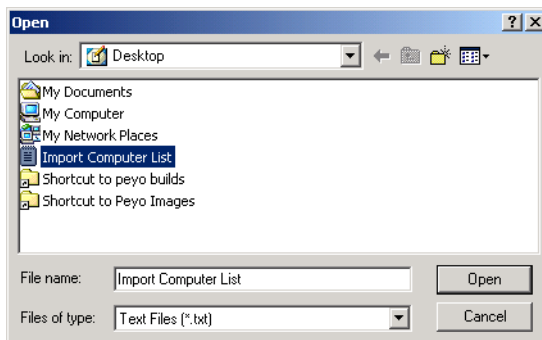
- 5 Double-click **Microsoft Windows Network**.
- 6 Select a server on which to install, then click **Add**.
- 7 Repeat this step until servers to which you are installing are added.
- 8 Do one of the following:
 - If you created a text file containing IP addresses to import computers located in non-WINS environments, continue to step 9.
 - If you did not create a text file containing IP addresses to import computers located in non-WINS environments, skip steps 9 through 12, and continue with step 13.

Note: See [“Creating a text file with IP addresses to import”](#) on page 111 for information about importing from a text file. Also note that the Import feature is designed for use with Windows NT-bases systems only. It is not intended for use with NetWare.

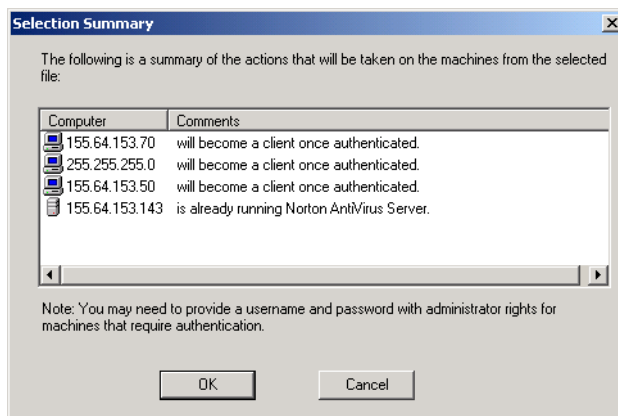
- 9 Click Import to import the list of servers.



- 10 Locate and double-click the text file that contains the computer names.



A summary list of computers to be added to the Available Computers list appears.



During the authentication process, you may need to provide a username and password for computers that require authentication.

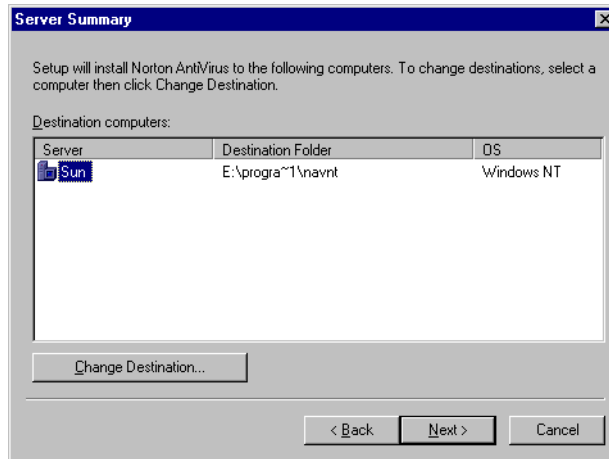
- 11 Click **OK**.

During the authentication process, Setup checks for different error conditions. You are prompted to view this information interactively on an individual computer basis or to write the information to a log file for later viewing.

If you create a log file, it is located at **C:\Winnt\Navcesrv.txt**.

- 12 Click **Yes** to write to a log file, **No** to display the interactive information.

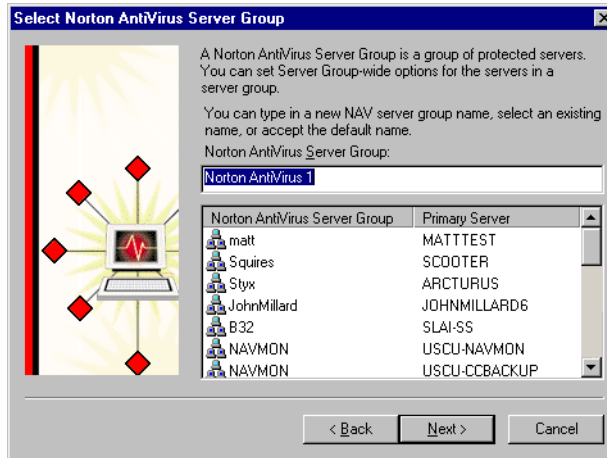
- 13 Click **Next**.



- 14 Accept the default Norton AntiVirus Corporate Edition install path or change it as necessary (select a computer and click **Change Destination**), then click **Next**.

15 Do one of the following:

- Type a name for a new server group, then click **Next**.
You will be prompted to confirm the creation of the new server group.
- Select an existing server group to join, then click **Next** and type the server group password when prompted.



For information about planning server groups, see [“About server groups”](#) on page 34.

For information about planning for optimal server-client ratios, see [“Scalability planning information”](#) on page 391.

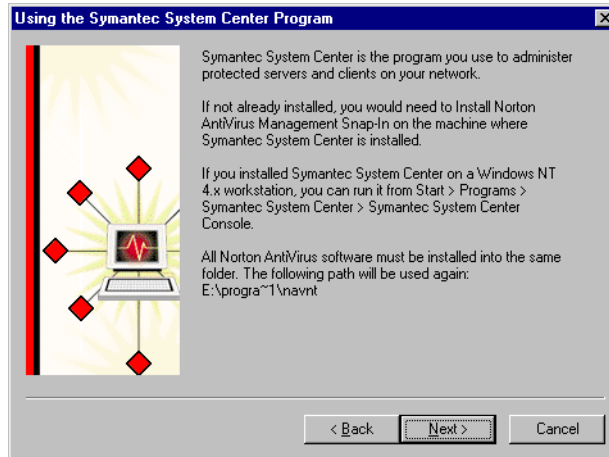
16 Click **Automatic or Manual** startup.

If you click Automatic, the Norton AntiVirus Corporate Edition services (and AMS² services, if you installed AMS²) will start automatically if you need to restart a Windows NT server running Norton AntiVirus Corporate Edition.

If you click Manual, you will have to start these services manually when you restart a Windows NT server running Norton AntiVirus Corporate Edition.

17 Click **Next.**

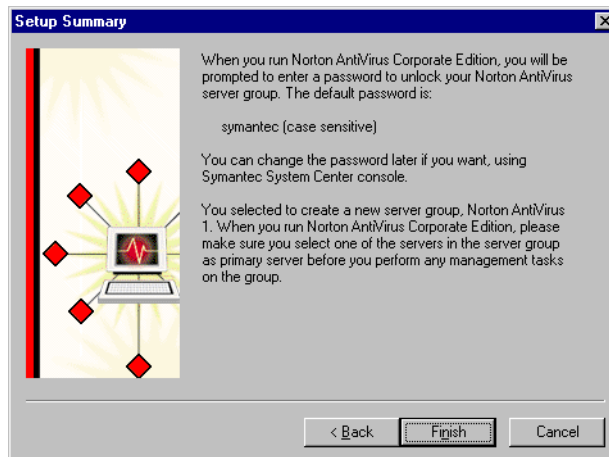
The Using the Symantec System Center Program screen appears.



18 Click **Next.**

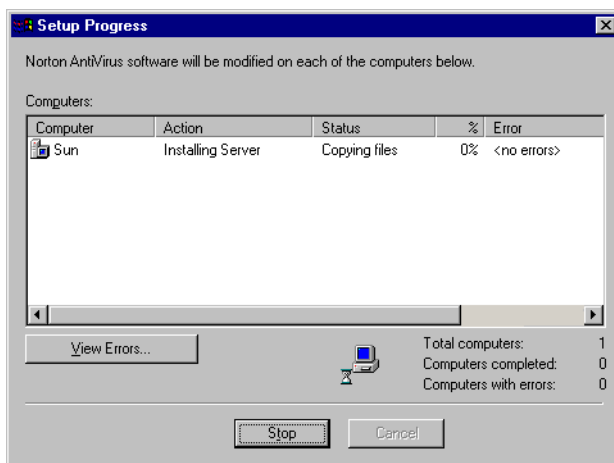
The Setup Summary screen appears indicating that the default password used to unlock the server group is:

symantec



19 Click **Finish**.

The Setup Progress screen shows the status of server installations.



20 When Norton AntiVirus Corporate Edition is installed to all of the servers you specified, check to see if any errors were reported. Select a server and click **View Errors** for more information.

21 Click **Close** when completed.

To install Norton AntiVirus Corporate Edition to NetWare servers

When installing Norton AntiVirus Corporate Edition to NetWare Directory Services (NDS), it is recommended that the computer performing the installation use the Novell Client for NetWare. If you encounter problems installing to NDS with the Microsoft Client for NetWare, install the Novell Client for NetWare and try again.

- 1 Log on to all NetWare servers on which you want to install Norton AntiVirus Corporate Edition.
- 2 Do one of the following:
 - From Disk 2, click **Install Norton AntiVirus To Servers**.
 - From the Symantec System Center console, click **Tools > AV Server Rollout**. (This is available only if you installed the Symantec System Center add-ons.)
- 3 Ensure that **Install Norton AntiVirus To Servers** is selected, then click **Next**.
- 4 Read the Symantec License and Warranty, click **I agree**, then click **Next**.

- 5 Ensure that Server Program is checked, then click **Next**.
- 6 Do one of the following:
 - If you are using the Novell Client for NetWare, double-click **NetWare Services**.
 - If you are using the Microsoft Client for NetWare, double-click **NetWare Or Compatible Network**.
- 7 Do one of the following:
 - Novell Client for NetWare: To install to a bindery server, double-click **NetWare Servers** and select a server (indicated by a server icon).
 - Novell Client for NetWare: To install to NDS, double-click **Novell Directory Services**, then select the SYS volume object where you want to install Norton AntiVirus Corporate Edition. (To locate a SYS volume object, double-click the tree object, and continue expanding the organizational objects until you reach the organization unit that contains the SYS volume object.)
 - Microsoft Client for NetWare: To install to a bindery server, select a server (indicated by a server icon).
 - Microsoft Client for NetWare: To install to NDS, select the SYS volume object where you want to install Norton AntiVirus Corporate Edition. (To locate a SYS volume object, double-click the tree object, and continue expanding the organizational objects until you reach the organization unit that contains the SYS volume object.)
- 8 Click **Add**.

If you are installing to NDS, you are prompted to enter a container, user name, and password. If you enter an incorrect user name or password at this stage, installation will continue normally. However, when you attempt to start Norton AntiVirus Corporate Edition on the NetWare server, you will receive an authentication error and will be prompted for the correct user name and password.
- 9 Repeat steps 7 and 8 until volumes for all servers you are installing to are added.
- 10 Click **Next**.
- 11 Accept the default Norton AntiVirus Corporate Edition install path or change it as necessary, then click **Next**.

- 12 Do one of the following:
 - Type a name for a new server group, then click **Next**, then click **Yes** to confirm.
 - Select an existing server group to join, then click **Next** and provide the server group password when prompted.
- 13 Click **Automatic Startup** or **Manual Startup**, then click **Next**.
 - If you click Automatic Startup, Vpstart.nlm starts automatically each time the server starts. (You must perform step 15 before this takes effect.)
 - If you click Manual Startup, run Vpstart.nlm each time you start the server.
- 14 Click **Next** until you reach the final screen, then click **Close**. Read each screen carefully.
- 15 After the install is complete, run Vpstart.nlm on each NetWare server to which you installed. You can do this at the server console or you can use RConsole if you have rights. The first time that you load Vpstart.nlm after installation, you must use the /Install switch. For example:

Load Sys:Nav\Vpstart.nlm /Install

For information about planning server groups, see [“About server groups”](#) on page 34.

I need to install AMS to Windows NT/2000 computers where I have already installed Norton AntiVirus for servers

If you have already installed the Norton AntiVirus Corporate Edition server program to your Windows NT/2000 computers without installing AMS², and you now want to install AMS², you must run a manual AMS² install.

To install AMS to Windows NT/2000 computers manually

- 1 Insert Disk 2 in your CD-ROM drive.
- 2 Run the Setup.exe program located in the following directory:
Cd2\Navcorp\Rollout\Ams2\Winnt

I need to install AMS to NetWare servers where I have already installed the Norton AntiVirus Corporate Edition server program

If you have already installed the Norton AntiVirus Corporate Edition server program to NetWare servers without installing AMS², and you now want to install AMS², the action you take depends on whether you have valuable configuration information you do not want to lose. For example, if you have made many NetWare servers primary servers, they store information that will be lost if you uninstall the Norton AntiVirus Corporate Edition server program.

Restarting a Windows NT/2000 server with automatic or manual startup

On a Windows NT/2000 server, the Norton AntiVirus Corporate Edition services (and AMS² services, if you installed AMS²) start automatically if you selected the automatic startup option during installation.

If necessary, you can also manually start the services.

If you selected the manual startup option during the installation, you must manually start these services in the order shown (click Control Panel > Services) each time you restart a protected Windows NT server:

- Norton AntiVirus Server
- DefWatch
- Intel PDS
- Intel Alert Handler (if you installed AMS²)
- Intel Alert Originator (if you installed AMS²)
- Intel File Transfer (if you installed AMS²)

To have the services load automatically

- Click **Startup > Automatic > OK**.

To restart a Windows NT/2000 server with manual Norton AntiVirus Corporate Edition startup

- 1 On the Windows taskbar, click **Start > Settings > Control Panel**.
- 2 Double-click **Services**.
- 3 Click **Norton AntiVirus Server**.
- 4 Click **Start**.
- 5 If you installed AMS², click **Intel Alert Handler**.
- 6 Click **Start**.
- 7 If you installed AMS², click **Intel Alert Originator**.
- 8 Click **Start**.
- 9 If you installed AMS², click **Intel File Transfer**.
- 10 Click **Start** if it is not already started.
- 11 If you installed AMS², click **Intel PDS**.
- 12 Click **Start** if it is not already started.

To have services start automatically in the future

- 1 On the Windows taskbar, click **Start > Settings > Control Panel**.
- 2 Double-click **Services**.
- 3 Select the service, then click **Startup > Automatic**.
- 4 Click **OK**.

Configuring automatic installations of Norton AntiVirus Corporate Edition on NetWare servers without Symantec System Center

If you have a Novell NetWare server but no Windows NT servers on which to run Symantec System Center, you can configure Norton AntiVirus Corporate Edition to install automatically on your Windows clients. To do this, complete the following tasks:

- Install Norton AntiVirus Corporate Edition on your NetWare server.
For installation instructions, see [“To install Norton AntiVirus Corporate Edition to NetWare servers”](#) on page 124.
- Configure automated installation of Norton AntiVirus Corporate Edition Windows clients.
- Configure automatic updates of virus definitions to servers.
For more information, see [“Updating NetWare servers”](#) on page 270.

To configure the automatic installations

- 1 Load Vpstart.nlm on the server using the /Install switch (Load Sys:Nav\Vpstart.nlm /Install).
This switch creates logon script modifications on NDS servers or to Sys:\Public\Net\$log.dat on bindery servers.
- 2 Add users to the NAVUSERS group using NWADMIN or SYSCON.
- 3 Load Vpregedt.nlm on the server console.
- 4 Click **(O)pen**.
- 5 Click **VirusProtect6**.
- 6 Press **Enter**.
- 7 Click **(O)pen** again, click **LoginOptions**, then press **Enter**.
- 8 In the left pane of the window, click **(E)dit** to edit values.
- 9 Scroll to and click **DoInstallOnWin95**, **DoInstallOnWinNT**, and/or **DoInstallOn16Bit**, depending on your environment.
Your choices are: OPTIONAL (the installation requires user input), FORCE (silent install, no user input required), and NONE (do not install). These entries are case sensitive.
- 10 If you previously installed clients and need to force a new update, increment the WinNTClientVersion, Win95ClientVersion, and/or 16BitClientVersion to a higher number.
- 11 Unload the Norton AntiVirus NLM from the console.

- 12 Type the following command to reload the Norton AntiVirus Corporate Edition NLM:
(LOAD VPSTART)
- 13 Test the client installation.

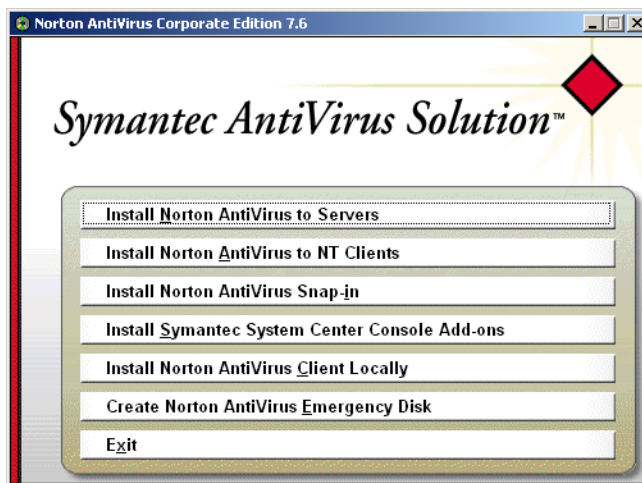
Note: The client must be a member of the NortonAntiVirusUser group.

Installing the Norton AntiVirus Corporate Edition management snap-in

You can use the Norton AntiVirus Corporate Edition management snap-in to manage computers on which you install Norton AntiVirus Corporate Edition. Install the snap-in on a computer where Symantec System Center has already been installed.

To install the Norton AntiVirus Corporate Edition management snap-in

- 1 Insert Disk 2 into your CD-ROM drive.
- 2 On the main installation screen, click **Install Norton AntiVirus Snap-in**.



- 3 Follow on-screen instructions.

Installing the Symantec System Center console add-ons

Symantec System Center console add-ons include the Remote NT Client Installation and Norton AntiVirus Server Rollout options. Once you install these options, they are added to the Symantec System Center Tools menu. You must have installed Symantec System Center before you can install the add-ons.

To install the add-ons

- 1 Insert Disk 2 into your CD-ROM drive.
- 2 On the main installation screen, click **Install Symantec System Center console add-ons**.
- 3 Follow the on-screen instructions.

Uninstalling

This section describes how you can uninstall the Norton AntiVirus Corporate Edition management snap-in and how you can uninstall from servers.

Uninstalling the Norton AntiVirus Corporate Edition management snap-in

To uninstall the Norton AntiVirus Corporate Edition management snap-in

- 1 On the Windows taskbar, click **Start > Settings > Control Panel**.
- 2 Double-click **Add/Remove Programs**.
- 3 Double-click **Norton AntiVirus Snap-In**.
- 4 Click **Yes**.

Uninstalling Norton AntiVirus Corporate Edition from a Windows NT/2000 server

To uninstall Norton AntiVirus Corporate Edition

- 1 From the Start menu, click **Settings > Control Panel > Add/Remove Programs**.
- 2 Click **Norton AntiVirus Corporate Edition**.
- 3 Click **Remove**.

Uninstalling Norton AntiVirus Corporate Edition from NetWare primary servers

You can avoid losing valuable information when you uninstall Norton AntiVirus Corporate Edition from a primary server running under NetWare.

To uninstall Norton AntiVirus Corporate Edition

- 1 Switch to the Norton AntiVirus screen on the server by pressing **Ctrl** and **Esc** at the same time, then click **Norton AntiVirus**.
- 2 On the NetWare console where you are running Norton AntiVirus, press **Esc**.
- 3 When the confirmation dialog box appears, click **Yes**, then press **Enter**.
- 4 Type the password, then press **Enter**.
- 5 Using a text editor, open Server.inf. This file is located in the NAV folder on the NetWare server. Add the following lines to the [COPYUPDATEFILES] section:

```
$Home$\Vpams.inf=$Updatepath$\Vpams.inf  
$Home$\Ams2\Ams2dbp.nlm=$Updatepath$\Ams2\Netware\  
Ams2dbp.nlm  
$Home$\Ams2\Amslib.nlm=$Updatepath$\Ams2\Netware\  
Amslib.nlm  
$Home$\Ams2\Bcsthdl.nlm=$Updatepath$\Ams2\Netware\  
Bcsthndl.nlm  
$Home$\Ams2\Hndlrsvc.nlm=$Updatepath$\Ams2\Netware\  
Hndlrsvc.nlm  
$Home$\Ams2\Iao.nlm=$Updatepath$\Ams2\Netware\Iao.NLM
```

```
$Home$\Ams2\Msgsys.Nlm=$Updatepath$\Ams2\Netware\
Msgsys.nlm
$Home$\Ams2\Nlmxhndl.nlm=$Updatepath$\Ams2\Netware\
Nlmxhndl.nlm
$Home$\Ams2\Pds.nlm=$Updatepath$\Ams2\Netware\Pds.nlm
$Home$\Ams2\Snmphndl.nlm=$Updatepath$\Ams2\Netware\
Snmphndl.nlm
```

- 6 Using a text editor, open Vpdata.var.
This file is located in the NAV folder on the NetWare server.
- 7 In the [VARIABLES] section, set INCLUDE_AMS2=1073741824
- 8 In the \Navcorp\Rollout folder on Disk 2, copy Vpams.inf to the NAV folder on the NetWare server.
- 9 Create a folder named AMS2 under the NAV folder on the NetWare server.
- 10 Copy all the files from the \Navcorp\Rollout\Ams2\Netware\ folder on Disk 2 to the AMS2 subfolder that you created.
- 11 On the NetWare server console, type the following command:
load Sys:Nav\Vpstart.nlm /Remove
If you installed to a different directory, substitute the default install directory with the directory to which you installed.
- 12 Press **Enter**.

Uninstalling Norton AntiVirus Corporate Edition from NetWare secondary servers

To uninstall from secondary servers running under NetWare

- 1 Uninstall the Norton AntiVirus Corporate Edition server program.
- 2 When reinstalling, install both the Norton AntiVirus Corporate Edition server program and AMS² at the same time.

Reboot required before reinstalling

If you uninstall Norton AntiVirus Corporate Edition, you must reboot the computer before reinstalling.

Installing Norton AntiVirus Corporate Edition to clients

This chapter includes the following:

- System requirements
- Preparing for client installation
- Installing Norton AntiVirus Corporate Edition to client computers
- Rolling out clients using third party products
- Configuring automatic installations of Norton AntiVirus Corporate Edition using NetWare servers without Symantec System Center
- Creating Norton AntiVirus Emergency and Rescue Disk sets for client computers

System requirements

This section contains information about system requirements for the following platforms or components:

- Windows 9x/Me/NT 4.0/2000/XP clients
- Windows 3.x clients
- DOS clients

System requirements for the Windows 9x/Me/NT 4.0/2000/XP client

The requirements are as follows:

- Windows 9x, Windows Me, Windows NT 4.0 with Service Pack 3 or higher, Windows 2000, or Windows XP.
- 32 MB RAM minimum.
- Intel 486 processor (Pentium or faster recommended).
- 43 MB of free disk space (80 MB during installation).
- WINSOCK 2.0 or later.

Additional requirement for rollout to Windows XP clients

You must enable the setting that allows network logons using non-Guest accounts before rolling out Norton AntiVirus Corporate Edition to Windows XP.

To allow network logons using non-Guest accounts

- 1 On the Windows taskbar, click **Start > Administrative Tools > Local Security Policy**.
- 2 In the left pane, double-click **Local Policies**.
- 3 Click **Security Options**.
- 4 In the right pane, double-click **Network Access Sharing and security model for local accounts**.
- 5 Change the setting to Classic - local users authenticate as themselves.
- 6 Click **OK**.
- 7 Exit the Local Security Policy snap-in.

System requirements for the Windows 3.x client

The requirements are as follows:

- Intel 486 processor or higher
- Windows 3.1 or later, enhanced mode (Windows 3.11 and Windows for Workgroups are supported)
- 16 MB of RAM minimum
- 640 KB of system memory
- 23 MB of free disk space (35 MB during installation)

System requirements for the DOS client

The requirements are as follows:

- Intel 386™ 33 MHz processor (Pentium or faster recommended)
- 640 KB of system memory
- 2 MB of extended memory
- Extended memory manager, such as EMM386
- 8 MB of free disk space (10 MB during installation)
- MS-DOS 5.0 or later

Requirement for clients running IPX only

When installing Norton AntiVirus Corporate Edition interactively on clients running IPX only, the parent server to which you are connecting must have Microsoft File and Print Services for NetWare installed. If installing from a network share on the parent server, or using a Grc.dat file that contains the IPX address of the parent server, Microsoft File and Print Services for NetWare is not required on the server.

Preparing for client installation

Before you read this section, be sure to review [“System requirements”](#) on page 135.

Install Norton AntiVirus Corporate Edition on one or more servers before you install to clients. If you install to clients first, they cannot connect to a Norton AntiVirus server and will run in unmanaged mode.

For an explanation of managed mode versus unmanaged mode, see [“Managed clients”](#) on page 27 and [“Unmanaged clients”](#) on page 28.

Rights to install to client computers

Users who are installing to Windows NT/2000/XP clients must have administrator rights on their own computers and must be logged on with administrator rights to install the Norton AntiVirus Corporate Edition client.

If you do not want to provide users with administrative rights to their own computers, use the NT Client Install utility to install the Windows NT client program to Windows NT/2000/XP workstations remotely. To run the

Windows NT Client Install utility must have local administrative rights on any client to which the installation is to be pushed.

The NT Client Install utility is available from the Symantec System Center console Tools menu.

For more information, see [“Installing Norton AntiVirus Corporate Edition to client computers”](#) on page 140.

Client does not install to Terminal Servers

You cannot install the Norton AntiVirus Corporate Edition client program to a Terminal Server. You must install the Norton AntiVirus Corporate Edition server program instead.

For more information, see [“Windows Terminal Server compatibility”](#) on page 106.

When a restart is required

When running a silent install on Windows 9x/Me clients, clients are forced to restart by default.

Installing email support

The client installation program automatically detects the email programs on client computers and installs the appropriate files.

If the client computers are running Microsoft Exchange or Lotus Notes, users do not need to provide additional information to the client installation program.

Lotus Notes should be closed until five minutes after Norton AntiVirus Corporate Edition is installed and the Norton AntiVirus service starts. (actually it is 5 minutes after the service starts, so if the Norton AntiVirus Corporate Edition install reboots, it would be 5 minutes after Windows restarts).

If Lotus Notes is open when Norton AntiVirus Corporate Edition is installed, anti-virus protection will not begin until after Notes is restarted.

Disabling the installation of the email plug-in and LiveUpdate for the Norton AntiVirus Corporate Edition client

The client installs of Norton AntiVirus can interface with email clients. This is an extra level of anti-virus protection that works in conjunction with Norton AntiVirus for Notes, Norton AntiVirus for Microsoft Exchange, Norton AntiVirus for Internet Email Gateways or for Firewalls, not to replace them. However, you might not want or need this extra layer of protection.

LiveUpdate is also included in the client installation of Norton AntiVirus Corporate Edition. If you use realtime updating of definitions, you might want to remove the LiveUpdate option from client computers.

To prevent Norton AntiVirus Corporate Edition from installing email plug-ins

- 1 Open Windows Explorer on the primary server.
- 2 Navigate to C:\Program Files\Nav\Clt-inst\Win32\Setup.wis.
- 3 Open Setup.wis and set the values to 0, where appropriate.

For example, if you do not want Norton AntiVirus Corporate Edition to plug into your Notes mail client, change 1 to 0 in the following line:

Notes=1

- 4 Save the changes and close the file.

Now if you run setup from Vplogon.bat, it calls the Setup.wis file but does not plug in to that mail client.

Note: The Setup.wis file is read only during a fresh install. On an overinstall or upgrade, the custom settings in setup.wis are not read.

If you are running setup from the Clt-inst directory, run the following to ensure that the Setup.wis file is processed:

Setup.exe /S /V /Qn

Installing Norton AntiVirus Corporate Edition to client computers

You can provide users with any of the following installation options:

- Download the client installation program from an internal Web server, then run it. This option is available for Windows 9x/Me/XP and Windows NT/2000 clients.

For more information, see [“Installing the Norton AntiVirus Corporate Edition client from an internal Web server”](#) on page 141.

- Run the client installation program from the client disk image on a server.

Note: MSI Administrative Installation is not supported.

For more information, see [“Installing from the client disk image on the server”](#) on page 163.

- Run the Install Norton AntiVirus to NT Clients option directly from Disk 2.

For more information, see [“Installing Norton AntiVirus Corporate Edition to Windows NT/2000/XP clients”](#) on page 164.

- Run the Install Norton AntiVirus Client Locally option directly from Disk 2.

For more information, see [“Installing the Norton AntiVirus Corporate Edition client locally”](#) on page 168.

- Fully automate both 32-bit and 16-bit client installations and updates by using logon scripts.

For more information, see [“Installing with logon scripts”](#) on page 169.

- Run the client installation program directly from floppy disks or a self-extracting .exe. This option is ideal for users who want to install Norton AntiVirus Corporate Edition on a home computer that does not connect to a Norton AntiVirus Corporate Edition server.

For more information, see [“Installing from floppy disks or a self-extracting .exe”](#) on page 175.

- From the console Tools menu, use the NT Client Install option to remotely install the Norton AntiVirus Corporate Edition client to computers running Windows NT/2000. This utility lets you install on Windows NT/2000 computers without giving users administrative rights to their computers. The installation procedure is the same as that for the Install Norton AntiVirus to NT Clients option that is available directly from Disk 2.

For more information, see [“Installing Norton AntiVirus Corporate Edition to Windows NT/2000/XP clients”](#) on page 164.

Installing the Norton AntiVirus Corporate Edition client from an internal Web server

This section includes the following topics:

- About installing from an internal Web server
- Setting up Norton AntiVirus Corporate Edition client install images on the Web server
- Where you can get Internet Information Server or Apache Server?
- Installing Apache Web Server as a service
- Configuring for an Internet Information Server
 - Windows NT/2000/XP installs
 - Windows 9x/Me installs
 - If you do not want to install the Norton AntiVirus Corporate Edition server program
 - Windows NT/2000/XP installs
 - Windows 9x/Me installs
- Configuring for an Apache Server
 - If you do not want to install the Norton AntiVirus Corporate Edition server program
 - Windows NT/2000/XP installs
 - Windows 9x/Me installs

- Running Apache HTTP Server services
- Updating Grc.dat files to assign parent servers
- Assigning clients to different parent servers
- Notifying users to download Norton AntiVirus Corporate Edition

Note: To use the Web install for clients running under Windows NT/2000 or XP, the user who launches the installation must have local Admin rights.

About installing from an internal Web server

You can set up Web-based client installs on an internal Microsoft Internet Information Server (IIS) version 4.0 or 5.0, or an Apache HTTP Server version 1.3.12.

Client installs are available for Windows 9x, Me, and NT/2000 computers.

Users who are installing to Windows NT/2000 clients must have administrator rights on their own computers and must be logged on with administrator rights to install the Norton AntiVirus Corporate Edition client.

Note: The client-based Web-install program is not configured to install versions of Norton AntiVirus Corporate Edition prior to version 7.5.

To download the client install program, users must have Internet Explorer 4.0 or higher on their computers. The Internet Explorer security level for the local intranet must be set to Medium so that Symantec ActiveX controls can be downloaded to the client. When the installation is complete, the security level can be restored to its original setting.

To set up the Web-based client install, you complete the following tasks:

- Set up Norton AntiVirus Corporate Edition client disk images on the Web server.
- Configure the Internet Information Server or Apache server.
- Update the Grc.dat files for the client disk images to assign clients to parent servers.
- Email users with the URL to which they point to download the Norton AntiVirus Corporate Edition client install.

Setting up client install images on the Web server

The procedure you complete to set up client images differs depending upon the following:

- The Web server type (IIS or Apache).
- Whether the Norton AntiVirus Corporate Edition server program is installed on the internal Web server. If it is installed on the internal Web server, the clients will be managed automatically by that server.

Where you can get Internet Information Server or Apache Server?

- Internet Information Server 5.0 installs by default during a Windows 2000 Professional, Server, or Advanced Server installation. If this option was unchecked when Windows 2000 was installed, you need the Windows 2000 installation CD to add this service.
- Internet Information Server 4.0 can be installed to Windows NT 4.0 from the Microsoft Option Pack for Windows NT 4.0.
- Apache Web Server 1.3.12 for Windows NT 4.0 and Windows 2000 can be downloaded from the Apache Software Foundation Web site:
<http://www.apache.org>
See the Apache Web site for the most up-to-date information about Apache Web Server releases.

Installing Apache Web Server as a service

After the Apache Web Server is installed, you must install it as a service.

To install Apache Web Server as a service

- On the Windows taskbar, click **Start > Programs > Apache Web Server > Install Apache As A Service**.

Configuring for an Internet Information Server

When the Norton AntiVirus Corporate Edition server program is installed on the internal Web server, clients will be managed automatically with that server as the parent server.

For information about assigning different parent servers to clients, see [“Updating Grc.dat files to assign parent servers”](#) on page 160 and [“Assigning clients to different parent servers”](#) on page 161.

To configure for a server where the Norton AntiVirus Corporate Edition server program is installed

- 1 Do one of the following to start Internet Services Manager:
 - If you are running IIS version 4.0, on the Windows taskbar, click **Start > Programs > Windows NT 4.0 Option Pack > Microsoft Internet Information Server > Internet Service Manager**.
 - If you are running IIS version 5.0, on the Windows taskbar, click **Start > Programs > Administrative Tools > Internet Services Manager**.
- 2 Double-click the **Web server** icon.
- 3 Right-click the **Default Web Site**, then click **New > Virtual Directory**.
- 4 Click **Next**.
- 5 In the Alias textbox, type the name of the directory (for example, NAVCEClientInstall), then click **Next**.
- 6 Select the location where Norton AntiVirus Corporate Edition is installed on the server, then click the **Clt-inst** folder.
- 7 Click **Next**.
- 8 Assign Read access rights only.
- 9 Do one of the following:
 - For IIS 4.0, click **Finish**.
 - For IIS 5.0, click **Next**, then click **Finish**.

Windows NT/2000/XP installs

For Windows NT/2000/XP installs, use a text editor such as Notepad to edit Startnt.htm located in the Clt-inst\Webinst folder on the server.

To edit Startnt.htm

- 1 Replace the Enter_Server_Name value with the name of the Web server.
- 2 Replace the Enter_Virtual_Homedirectory_Name value with the name of the virtual home directory you created (for example, NAVCEClientInstall).
- 3 To run silent installs, edit Files_nt.ini, located in the Clt-inst\Webinst folder. In the [General] section, remove the semicolons that appear at the beginning of the following lines:

InstallOptions=/s /v"/qn /li Webinst.log"

MSILogFileName=Webinst.log

Windows 9x/Me installs

For Windows 9x/Me installs, use a text editor to edit Start9x.htm located in the Clt-inst\Webinst folder on the server.

To edit Start9x.htm

- 1 Replace the Enter_Server_Name value with the name of the Web server.
- 2 Replace the Enter_Virtual_Homedirectory_Name value with the name of the virtual home directory you just created (for example, NAVCEClientInstall).
- 3 To run silent installs, edit Files_9x.ini, located in the Clt-inst\Webinst folder. In the [General] section, remove the semicolons that appear at the beginning of the following lines:

InstallOptions=/s /v"/qn /li Webinst.log"

MSILogFileName=Webinst.log

If you do not want to install the Norton AntiVirus Corporate Edition server program

If you do not want to install the Norton AntiVirus Corporate Edition server program, you can create regular or silent installs. Silent installs can be managed or unmanaged.

To create regular installs

- 1 Create a folder named Nav\Clt-inst on the Web server.
- 2 Insert Disk 2 into your CD-ROM drive.
- 3 Copy the following folders and their contents to the Nav\Clt-inst folder you created:
 - Navcorp\Rollout\Avserver\Clients\Win32
 - Navcorp\Rollout\Avserver\Clients\Webinst
- 4 Do one of the following to launch Internet Services Manager:
 - If you are running IIS version 4.0, on the Windows taskbar, click **Start > Programs > Windows NT 4.0 Option Pack > Microsoft Internet Information Server > Internet Service Manager**.
 - If you are running IIS version 5.0, on the Windows taskbar, click **Start > Programs > Administrative Tools > Internet Services Manager**.
- 5 Double-click the **Web server** icon.

- 6 Right-click the **Default Web Site**, then click **New > Virtual Directory**.
- 7 Click **Next**.
- 8 In Alias, type the name of the directory (for example, NAVCEClientInstall), then click **Next**.
- 9 Locate and click the **Clt-inst** folder you created in step 1, then click **Next**.
- 10 Assign Read access rights only.
- 11 Do one of the following:
 - For IIS 4.0, click **Finish**.
 - For IIS 5.0, click **Next**, then click **Finish**.

Windows NT/2000/XP installs

For Windows NT/2000/XP installs, use a text editor such as Notepad to edit Startnt.htm located in the Clt-inst\Webinst folder.

To edit Startnt.htm

- 1 Replace the Enter_Server_Name value with the name of the Web server.
- 2 Replace the Enter_Virtual_Homedirectory_Name value with the name of the virtual home directory you created (for example, NAVCEClientInstall).

Windows 9x/Me installs

For Windows 9x/Me installs, use a text editor to edit Start9x.htm, located in the Clt-inst\Webinst folder on the server.

To edit Start9x.htm

- 1 Replace the Enter_Server_Name value with the name of the Web server.
- 2 Replace the Enter_Virtual_Homedirectory_Name value with the name of the virtual home directory you just created (for example, NAVCEClientInstall).

To create silent managed client Web installs

- 1 Create a folder named Nav\Clnt-inst on the Web server.
- 2 Insert Disk 2 into your CD-ROM drive.
- 3 Copy the following folders and their contents to the Nav\Clnt-inst folder you created:
 - Navcorp\Rollout\Avserver\Clients\WIN32
 - Navcorp\Rollout\Avserver\Clients\Webinst
- 4 Do one of the following to start Internet Services Manager:
 - If you are running IIS version 4.0, on the Windows taskbar, click **Start > Programs > Windows NT 4.0 Option Pack > Microsoft Internet Information Server > Internet Service Manager**.
 - If you are running IIS version 5.0, on the Windows taskbar, click **Start > Programs > Administrative Tools > Internet Services Manager**.
- 5 Double-click the **Web server** icon.
- 6 Right-click the **Default Web Site**, then click **New > Virtual Directory**.
- 7 Click **Next**.
- 8 In Alias, type the name of the directory (for example, NAVCEClientInstall), then click **Next**.
- 9 Locate and click the **Clnt-inst** folder you created in step 1, then click **Next**.
- 10 Assign Read access rights only.
- 11 Do one of the following:
 - For IIS 4.0, click **Finish**.
 - For IIS 5.0, click **Next**, then click **Finish**.

Windows NT/2000/XP installs

Use a text editor such as Notepad to edit the Grc.dat file, the Files_nt.ini file, and the Startnt.htm file.

To edit the files

- 1 Insert the following line at the end of the Grc.dat file, located in the Clt-inst\Win32 folder:

PARENT=S<SERVERNAME>

where <SERVERNAME> is the name of the intended parent server.
(Don't include the brackets.)
- 2 To run silent installs, edit Files_nt.ini, located in the Clt-inst\Webinst folder. In the [General] section, remove the semicolons that appear at the beginning of the following lines:

InstallOptions=/s /v"/qn /li Webinst.log"
MSILogFileName=Webinst.log
- 3 Edit Startnt.htm, located in the Clt-inst\Webinst folder as follows:
 - Replace the Enter_Server_Name value with the name of the Web server.
 - Replace the Enter_Virtual_Homedirectory_Name value with the name of the virtual home directory you created (for example, NAVCEClientInstall).

Windows 9x/Me installs

Use a text editor such as Notepad to edit the Grc.dat file, the Files_9x.ini file, and the Start9x.htm file.

To edit the files

- 1 Use a text editor to open Grc.dat, located in the Clt-inst\Win32 folder and insert the following line at the end of the file:

PARENT=S<SERVERNAME>

where <SERVERNAME> is the name of the intended parent server.
(Don't include the brackets.)
- 2 To run silent installs, edit Files_9x.ini, located in the Clt-inst\Webinst folder. In the [General] section, remove the semicolons that appear at the beginning of the following lines:

InstallOptions=/s /v"/qn /li Webinst.log"
MSILogFileName=Webinst.log
- 3 Edit Start9x.htm, located in the Clt-inst\Webinst folder on the server as follows:
 - Replace the Enter_Server_Name value with the name of the Web server.
 - Replace the Enter_Virtual_Homedirectory_Name value with the name of the virtual home directory you just created (for example, NAVCEClientInstall).

To create silent unmanaged client Web installs

- 1 Create a folder named Nav\Clt-inst on the Web server.
- 2 Insert Disk 2 into your CD-ROM drive.
- 3 Copy the following folders and their contents to the Nav\Clt-inst folder you created:
 - Navcorp\Rollout\Avserver\Clients\Win32
 - Navcorp\Rollout\Avserver\Clients\Webinst
- 4 Do one of the following to start Internet Services Manager:
 - If you are running IIS version 4.0, on the Windows taskbar, click **Start > Programs > Windows NT 4.0 Option Pack > Microsoft Internet Information Server > Internet Service Manager**.
 - If you are running IIS version 5.0, on the Windows taskbar, click **Start > Programs > Administrative Tools > Internet Services Manager**.

- 5 Double-click the **Web server** icon.
- 6 Right-click the **Default Web Site**, then click **New > Virtual Directory**.
- 7 Click **Next**.
- 8 In Alias, type the name of the directory (for example, NAVCEClientInstall), then click **Next**.
- 9 Locate and click the **Clt-inst** folder you created in step 1, then click **Next**.
- 10 Assign Read access rights only.
- 11 Do one of the following:
 - For IIS 4.0, click **Finish**.
 - For IIS 5.0, click **Next**, then **Finish**.

Windows NT/2000/XP installs

Use a text editor such as Notepad to edit Startnt.htm and Files_nt.ini.

To edit the files

- 1 Edit Startnt.htm, located in the Clt-inst\Webinst folder as follows:
 - Replace the Enter_Server_Name value with the name of the Web server.
 - Replace the Enter_Virtual_Homedirectory_Name value with the name of the virtual home directory you created (for example, NAVCEClientInstall).
- 2 To run silent installs, edit Files_nt.ini, located in the Clt-inst\Webinst folder. In the [General] section, remove the semicolons that appear at the beginning of the following lines:
`InstallOptions=/s /v"/qn /li Webinst.log"`
`MSILogFileName=Webinst.log`

Windows 9x/Me installs

Use a text editor such as Notepad to edit Start9x.htm and Files_9x.ini.

To edit the files

- 1 Edit Start9x.htm, located in the Clt-inst\Webinst folder on the server as follows:
 - Replace the Enter_Server_Name value with the name of the Web server.
 - Replace the Enter_Virtual_Homedirectory_Name value with the name of the virtual home directory you just created (for example, NAVCEClientInstall).
- 2 If you want the installs to run silently, edit Files_nt.ini, located in the Clt-inst\Webinst folder. In the [General] section, remove the semicolons that appear at the beginning of the following lines:
`InstallOptions=/s /v"/qn /li Webinst.log"`
`MSILogFileName=Webinst.log`

Configuring for an Apache Server

When the Norton AntiVirus Corporate Edition server program is installed on the internal Web server, clients are managed automatically with that server as the parent server.

For information about assigning parent servers to clients, see [“Updating Grc.dat files to assign parent servers”](#) on page 160 and [“Assigning clients to different parent servers”](#) on page 161.

To configure for a server where the Norton AntiVirus Corporate Edition server program is installed

- 1 Use a text editor such as Notepad to open the Srm.conf file that is installed by default in C:\Program Files\Apache Group\Apache\Conf.
- 2 Add the following five lines to the end of the Srm.conf file:

```
DirectoryIndex default.htm
<VirtualHost 111.111.111.111>
#ServerName Machinename
DocumentRoot "C:\Program Files\Nav\Clt-inst"
</VirtualHost>
```

Replace 111.111.111.111 with the IP address of the computer where Apache HTTP Server is installed. Replace Machinename with the name of the server. The DocumentRoot line must include the directory to which Norton AntiVirus Corporate Edition was installed on the server followed by \Clt-inst. "C:\Program Files\Nav\Clt-inst" is the default. Quotation marks are required for the root directory. If they are not included, Apache services might not start.

- 3 For Windows NT/2000/XP installs, use a text editor such as Notepad to edit Startnt.htm located in the Clt-inst\Webinst folder as follows:

- Replace the Enter_Server_Name value with the name of the Web server computer.
- Delete the words Enter_Virtual_Homedirectory_Name from the VirtualHomeDirectory value. When deleted, the value appears as follows:

value = ""

- To run silent installs, edit Files_nt.ini, located in the Clt-inst\Webinst folder. In the [General] section, remove the semicolons that appear at the beginning of the following lines:

```
InstallOptions=/s /v"/qn /li Webinst.log"
MSILogFileName=Webinst.log
```


- 4 For Windows 9x installs, use a text editor to edit Start9x.htm located in the Clt-inst\Webinst folder as follows:
 - Replace the Enter_Server_Name value with the name of the Web server machine.
 - Delete the words Enter_Virtual_Homedirectory_Name from the VirtualHomeDirectory value. When deleted, the value appears as follows:
value = ""
 - To run silent installs, edit Files_9x.ini, located in the Clt-inst\Webinst folder. In the [General] section, remove the semicolons that appear at the beginning of the following lines:
InstallOptions=/s /v"/qn /li Webinst.log"
MSILogFileName=Webinst.log

If you do not want to install the Norton AntiVirus Corporate Edition server program

If you do not want to install the Norton AntiVirus Corporate Edition server program, you can create regular or silent installs. Silent installs can be managed or unmanaged.

To create regular installs

- 1 On the Web server computer, create a folder named Nav\Clt-inst.
- 2 Insert Disk 2 into your CD-ROM drive.
- 3 Copy the following folders and their contents to the Nav\Clt-inst folder you created:
 - Navcorp\Rollout\Avserver\Clients\Win32
 - Navcorp\Rollout\Avserver\Clients\Webinst
- 4 Use a text editor such as Notepad to open the Srm.conf file that is installed by default in C:\Program Files\Apache Group\Apache\Conf.

- 5 Add the following five lines to the end of the Srm.conf file:
DirectoryIndex default.htm
<VirtualHost 111.111.111.111>
#ServerName Machinename
DocumentRoot "C:\Nav\Clt-inst"
</VirtualHost>

Replace 111.111.111.111 with the IP address of the computer where Apache HTTP Server is installed. Replace Machinename with the name of the server. The DocumentRoot line must include the directory of the folder you created in step 1 (for example, "C:\Nav\Clt-inst"). Quotation marks are required for the root directory. If they are not included, Apache services might not start.
- 6 For Windows NT/2000/XP installs, use a text editor such as Notepad to edit Startnt.htm located in the Clt-inst\Webinst folder as follows:
 - Replace the Enter_Server_Name value with the name of the Web server computer.
 - Delete the words Enter_Virtual_Homedirectory_Name from the VirtualHomeDirectory value. When deleted, the value appears as follows:
value = ""
- 7 For Windows 9x/Me installs, use a text editor to edit Start9x.htm, located in the Clt-inst\Webinst folder as follows:
 - Replace the Enter_Server_Name value with the name of the Web server computer.
 - Delete the words Enter_Virtual_Homedirectory_Name from the VirtualHomeDirectory value. When deleted, the value appears as follows
value = ""

To create silent managed client installs

- 1 On the Web server computer, create a folder named Nav\Clt-inst.
- 2 Insert Disk 2 into your CD-ROM drive.
- 3 Copy the following folders and their contents to the Nav\Clt-inst folder you created:
 - Navcorp\Rollout\Avserver\Clients\Win32
 - Navcorp\Rollout\Avserver\Clients\Webinst
- 4 Use a text editor such as Notepad to open the Srm.conf file that is installed by default in C:\Program Files\Apache Group\Apache\Conf.
- 5 Add the following five lines to the end of the Srm.conf file:

```
DirectoryIndex default.htm  
<VirtualHost 111.111.111.111>  
#ServerName Machinename  
DocumentRoot "C:\Nav\clt-inst"  
</VirtualHost>
```

Replace 111.111.111.111 with the IP address of the computer where Apache HTTP Server is installed. Replace Machinename with the name of the server. The DocumentRoot line must include the directory of the folder you created in step 1 (for example, "C:\Nav\Clt-inst"). Quotation marks are required for the root directory. If they are not included, Apache services might not start.

Windows NT/2000/XP installs

Use a text editor such as Notepad to edit Grc.dat, Files_nt.ini, and Startnt.htm.

To edit the files

- 1 Open the Grc.dat file, located in the Clt-inst\Win32 folder and search for the following line:

PARENT=

- 2 Add the letter S and the name of the parent server as follows:

PARENT=S<Servername>

where <Servername> is the name of the intended parent server. (Don't include the brackets.)

- 3 To run silent installs, edit Files_nt.ini, located in the Clt-inst\Webinst folder. In the [General] section, remove the semicolons that appear at the beginning of the following lines:

InstallOptions=/s /v"/qn /li Webinst.log"

MSILogFileName=Webinst.log

- 4 Use a text editor to edit Startnt.htm located in the Clt-inst\Webinst folder as follows:

- Replace the Enter_Server_Name value with the name of the Web server.
- Delete the words Enter_virtual_homedirectory_name from the VirtualHomeDirectory value. When deleted, the value appears as follows:

value = ""

Windows 9x/Me installs

Use a text editor such as Notepad to edit Grc.dat, Files_9x.ini, and Start9x.htm.

To edit the files

- 1 Open the Grc.dat file, located in the Clt-inst\Win32 folder and search for the following line:

PARENT=

- 2 Add the letter S and the name of the parent server as follows:

PARENT=S<Servername>

where <Servername> is the name of the intended parent server. (Don't include the brackets.)

- 3 To run silent installs, edit Files_9x.ini, located in the Clt-inst\Webinst folder. In the [General] section, remove the semicolons that appear at the beginning of the following lines:

InstallOptions=/s /v"/qn /li Webinst.log"

MSILogFileName=Webinst.log

- 4 Use a text editor to edit Start9x.htm, located in the Clt-inst\Webinst folder on the server as follows:

- Replace the Enter_Server_Name value with the name of the Web server.
- Delete the words Enter_Virtual_Homedirectory_Name from the VirtualHomeDirectory value. When deleted, the value appears as follows:

value = ""

To create silent unmanaged client installs

- 1 Create a folder named Nav\Clnt-inst on the Web server computer.
- 2 Insert Disk 2 into your CD-ROM drive.
- 3 Copy the following folders and their contents to the Nav\Clnt-inst folder you created:
 - Navcorp\Rollout\Avserver\Clients\Win32
 - Navcorp\Rollout\Avserver\Clients\Webinst
- 4 Use a text editor such as Notepad to open the Srm.conf file that is installed by default in C:\Program Files\Apache Group\Apache\Conf.
- 5 Add the following five lines to the end of the Srm.conf file:

```
DirectoryIndex default.htm  
<VirtualHost 111.111.111.111>  
#ServerName Machinename  
DocumentRoot "C:\Nav\clnt-inst"  
</VirtualHost>
```

Replace 111.111.111.111 with the IP address of the computer where Apache HTTP Server is installed. Replace Machinename with the name of the server. The DocumentRoot line must include the directory of the folder you created in step 1 (for example, "C:\Nav\Clnt-inst").

Quotation marks are required for the root directory. If they are not included, Apache services might not start.

Windows NT/2000/XP installs

Use a text editor such as Notepad to edit Files_nt.ini and Startnt.htm.

To edit the files

- 1 To run silent installs, edit Files_nt.ini, located in the Clt-inst\Webinst folder. In the [General] section, remove the semicolons that appear at the beginning of the following lines:
`InstallOptions=/s /v"/qn /li Webinst.log"`
`MSILogFileName=Webinst.log`
- 2 Edit Startnt.htm, located in the Clt-inst\Webinst folder as follows:
 - Replace the Enter_Server_Name value with the name of the Web server.
 - Delete the words Enter_Virtual_Homedirectory_Name from the VirtualHomeDirectory value. When deleted, the value appears as follows:
value = ""

Windows 9x/Me installs

Use a text editor such as Notepad to edit Files_9x.ini and Start9x.htm.

To edit the files

- 1 To run silent installs, edit Files_9x.ini, located in the Clt-inst\Webinst folder. In the [General] section, remove the semicolons that appear at the beginning of the following lines:
`InstallOptions=/s /v"/qn /li Webinst.log"`
`MSILogFileName=Webinst.log`
- 2 Edit Start9x.htm located in the Clt-inst\Webinst folder on the server as follows:
 - Replace the Enter_Server_Name value with the name of the Web server.
 - Delete the words Enter_Virtual_Homedirectory_Name from the VirtualHomeDirectory value. When deleted, the value appears as follows:
value = ""

Running Apache HTTP Server services

To edit any of the Norton AntiVirus Corporate Edition client files (for example, Grc.dat), stop Apache HTTP Server before you make the changes, then restart Apache HTTP Server for the changes to take effect.

To start Apache HTTP Server

- On the Windows taskbar on the server computer, click **Start > Programs > Apache Web Server > Start Apache**.

To stop Apache HTTP Server

- On the Windows taskbar on the server computer, click **Start > Programs > Apache Web Server > Stop Apache**.

Updating Grc.dat files to assign parent servers

The Grc.dat file contains an entry that defines the parent server. When you copy the Grc.dat file from a server running the Norton AntiVirus Corporate Edition server program to a client, that server then becomes the client's parent. A client restart is required for this change to take effect.

If the Norton AntiVirus Corporate Edition server program is installed on the Web server, the Grc.dat file includes the entry that assigns the server as the parent for client installs.

If the Norton AntiVirus Corporate Edition server program is not installed on the Web server and you copied the Windows 95/98/Me/XP and Windows NT/2000 client images from Disk 2, the Grc.dat file does not include an entry to assign the parent server.

Take the following actions based on your needs:

- Edit the Grc.dat files in the install directories on the Web server to include required parent server entries.
- Copy the Grc.dat file from an intended parent server to the install directories on the Web server, then restart the client.
- Make no changes to the Grc.dat file, causing clients to be unmanaged.

To edit the Grc.dat file

- Use a text editor such as Notepad to edit the [KEYS] section as follows:
Connected=D1
AlertDirectory=S\\<Servername>\Vpalerts
RemoteHomeDirectory=S\\<Servername>\Vphome
Parent=S<Servername>
where <Servername> is the name of the intended parent server. (Don't include the brackets.)

To copy the Grc.dat file from the intended parent server

- Copy the Grc.dat from the directory to which the Norton AntiVirus Corporate Edition server program was installed on the intended parent server to the Nav\Clt-inst\Win32 folder on the Web server.
By default, the Norton AntiVirus Corporate Edition server program is installed to C:\Program files\Nav.
A client restart is required for this change to take effect.

Assigning clients to different parent servers

If Norton AntiVirus Corporate Edition is to be installed to clients that are to be managed by different parent servers, you can create multiple install images. Each install image can include a Grc.dat file that points to a different parent server.

To complete the following procedure, you must already have created a Norton AntiVirus Corporate Edition client install image.

See [“Setting up client install images on the Web server”](#) on page 143 and [“Updating Grc.dat files to assign parent servers”](#) on page 160.

To create multiple install images that point to different parent servers using IIS

- 1 From the Norton AntiVirus Corporate Edition client install image, copy the Clt-inst folder, then paste and rename the copy (for example, Clt-inst2).

Repeat this step to create as many copies as needed.

- 2 Create a new unique virtual home directory that points to the appropriate Clt-inst folder for the intended parent server, then update Startnt.htm and Start9x.htm with the new virtual home directory.
- 3 Update the parent server name in Grc.dat in each of the platform subdirectories.

For more information, see [“Updating Grc.dat files to assign parent servers”](#) on page 160.

Note: If you add or delete files when manually updating the Virdefs folder, update the Filecount= line in the [General] group and Filexx= lines in the [Files] group in Webinst\Files_nt.ini and Webinst\Files_9x.ini. For example, if you increased the number of files from 84 to 85, you would change the FileCount= line to 85.

Notifying users to download Norton AntiVirus Corporate Edition

You can email users instructions to download the Web-based Norton AntiVirus Corporate Edition.

For silent Windows 9x client installs, the computer restarts at the end of Setup. Notify users that they should save their work and close applications before they begin the installation.

Include a URL in your email message that points to the client install as follows:

- For Internet Information Server:

`http://Server_name/Virtual_home_directory/Webinst/`

where `Server_name` is the name of the Web-based server, `Virtual_home_directory` is the name of the Alias you created, and `Webinst` is the folder you created on the Web server under `\Clt-inst`. (For example, `http://Server_name/Navceclientinstall/Webinst/`)

When the URL points to an internal Web server to which Norton AntiVirus Corporate Edition is installed, the clients are managed by this server. If you want some clients to be managed by a different server, see [“Assigning clients to different parent servers”](#) on page 161.

- For Apache Web Server:

`http://Server_name/Webinst/`

where `Server_name` is the name of the computer where Apache Web Server is installed. The IP address of that server computer can also be used in place of the `Server_name`.

When the URL points to an internal Web server to which Norton AntiVirus Corporate Edition is installed, the clients are managed by this server. If you want some clients to be managed by a different server, see [“Assigning clients to different parent servers”](#) on page 161.

Installing from the client disk image on the server

When you install Norton AntiVirus Corporate Edition to servers, the server Setup program creates a client disk image (or installation folder) on each protected server. Client users can then run the Norton AntiVirus Corporate Edition Setup program from the servers to which they connect. The Norton AntiVirus Corporate Edition client will install in managed mode and display in the right pane of the Symantec System Center when its associated server is selected in the console tree. When the client runs in managed mode, you can configure automatic definitions file updates for the client and administer them from Symantec System Center.

On Windows NT/2000 servers, the default shared folder is `\\Server\Vphome\Clt-inst`, and everyone has read permissions. On NetWare servers, the default shared directory is `\\Server\Sys\Nav\Clt-inst`. Setup also creates a group called NORTONANTIVIRUSUSER. If you add users to this group, they will have the rights they need (Read and File Scan) to run the client installation program from the client disk image on the server.

If you make Disk 2 available on a shared network drive, users will need to map that drive on their workstations to ensure successful installation of all components.

To install from the client disk image on a server

- 1 Verify that users have rights to the client disk image on the server.
- 2 Give the user the path and, if necessary, a drive mapping to the client disk image.

For NetWare servers, the default path is `\\Server\Sys\Nav\Clt-inst`. For Windows NT servers, the default share path is `\\Server\Vphome\Clt-inst`.

- 3 Make sure the user knows which platform to install. These installation folders and Setup programs are available under the Clt-inst folder on each server:

`Clt-inst\Win32\Setup.exe`

`Clt-inst\Win16\Setup.exe`

`Clt-inst\Dos\Install.bat`

Installing Norton AntiVirus Corporate Edition to Windows NT/2000/XP clients

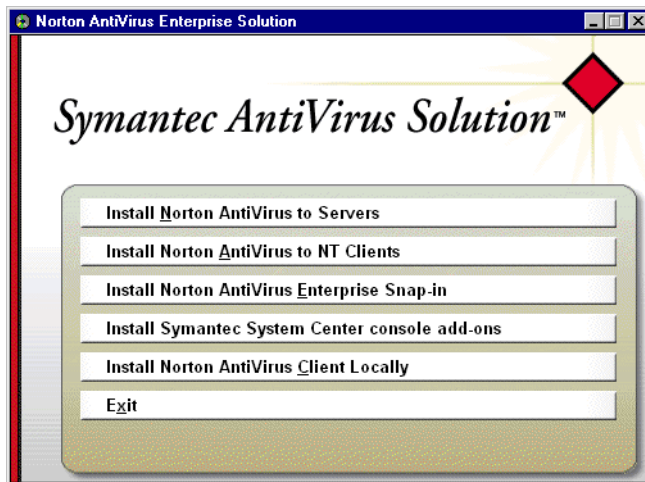
You can remotely install the Norton AntiVirus Corporate Edition 32-bit client onto any Windows NT computer connected to the network, and you can install to multiple clients at the same time without having to physically go to each workstation.

The client application can be rolled out to all clients attached to either Windows NT/2000 or NetWare servers running Norton AntiVirus Corporate Edition.

Another advantage to remote installation is that users do not need to log on to their computers as administrators prior to the installation if you have administrator rights to the domain to which the client computers belong.

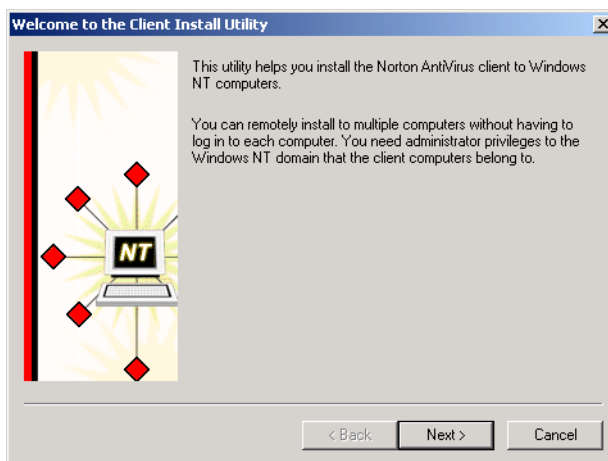
To install Norton AntiVirus Corporate Edition to Windows NT/2000/XP clients

- 1 From Disk 2, click **Install Norton AntiVirus To NT Clients**.

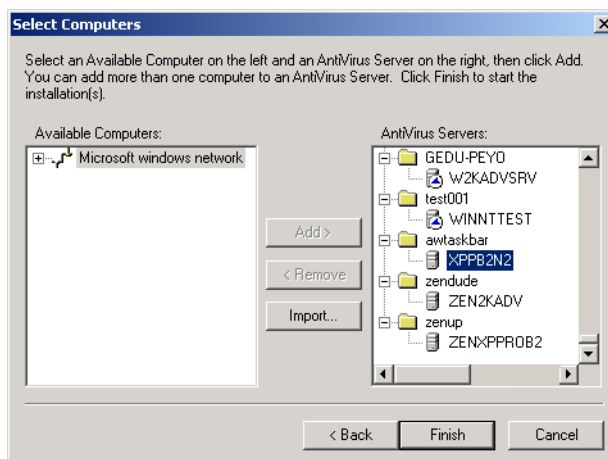


The Welcome screen appears.

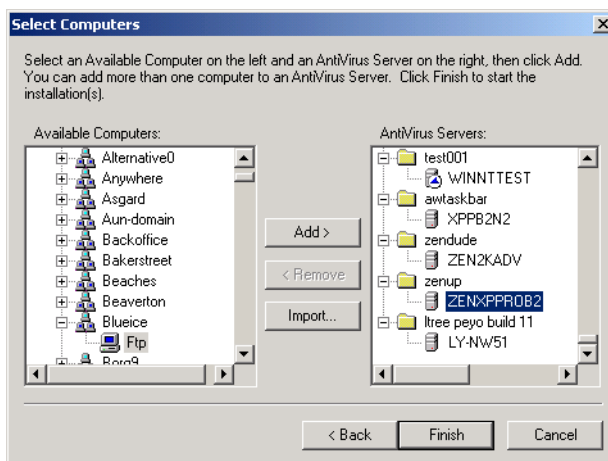
- 2 Click **Next**.



3 Double-click **Microsoft Windows NT Network**.



4 Select a computer on the left and a server running Norton AntiVirus Corporate Edition on the right, then click **Add**.



5 Repeat this step until clients that you want to manage are added.

Note: You can reinstall to computers that are already running Norton AntiVirus Corporate Edition.

You can also import a text file to add Windows NT/2000/XP clients.

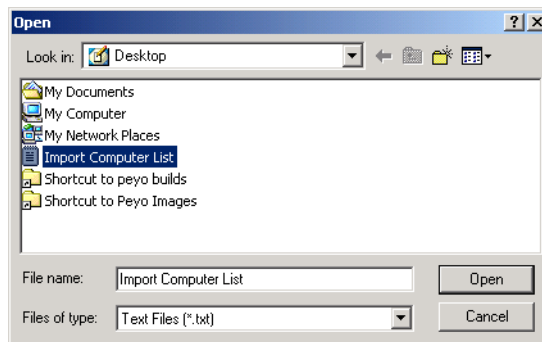
- 6 Do one of the following:

If you created a text file containing IP addresses to import computers located in non-WINS environments, continue to step 7.

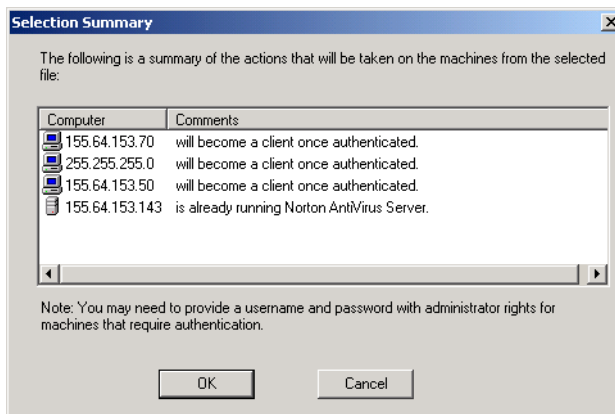
If you did not create a text file containing IP addresses to import computers located in non-WINS environments, skip steps 7 through 10, and continue with step 11.

Note: See [“Creating a text file with IP addresses to import”](#) on page 111 for information about importing from a text file. Also note that the Import feature is designed for use with Windows NT/2000/XP only. It is not intended for use with NetWare.

- 7 Click Import to import the list of computers.
- 8 Locate and double-click the text file that contains the computer names.



A summary list of computers to be added to the Available Computers list appears.



During the authentication process, you may need to provide a username and password for computers that require authentication.

9 Click **OK**.

During the authentication process, Setup checks for different error conditions. You are prompted to view this information interactively on an individual computer basis or to write the information to a log file for later viewing.

If you create a log file, it is located at **C:\Winnt\Navcecln.txt**.

10 Click **Yes** to write to a log file, **No** to display the interactive information.

11 Click **Finish**.

Installing the Norton AntiVirus Corporate Edition client locally

If the client computer is connected to the network, installing directly from Disk 2 is the least preferred option because the disk might get damaged or lost, and only one user can install at a time. Also, to install the Norton AntiVirus Corporate Edition client in managed mode is more difficult because the user must specify a Norton AntiVirus Corporate Edition server to connect to when installing from the CD.

If users do not specify a Norton AntiVirus Corporate Edition server to connect to when installing from Disk 2, the Norton AntiVirus Corporate Edition client is installed in unmanaged mode. This means that users are responsible for getting their own virus definitions files and program updates through an Internet connection.

To changed the client's status to managed, use one of the following methods:

- Reinstall the client from the server or use one of the other installation methods.
- Copy the Grc.dat file from the intended parent server to the client. (This method is faster and requires fewer resources.)

Note: If you make Disk 2 available on a shared network drive, users will need to map that drive on their workstations to ensure successful installation of all components.

To install from Disk 2

- 1 If users will run the client in managed mode, tell users the Norton AntiVirus Corporate Edition server to which they connect.
The installation program prompts them for this information.
- 2 Give users access to Disk 2.
- 3 Have users run the client Setup program for their platform.
For example, if the CD-ROM drive is E, users could run the Setup program from one of the following paths:
E:\Navcorp\Rollout\Avserver\Clients\Win32\Setup.exe
E:\Navcorp\Rollout\Avserver\Clients\Win16\Setup.exe
E:\Navcorp\Rollout\Avserver\Clients\Dos\Install.bat

To copy Grc.dat to the client

- 1 Copy the Grc.dat file from the one of the following folders (based on the target client's platform) of the intended parent server:
 - NAV\Clt-inst\Win32
 - NAV\Clt-inst\Win16
 - NAV\Clt-inst\DOS
- 2 Paste the Grc.dat file to one of the following folders on the client:
 - For Windows 9x\Me: C:\Program Files\Norton AntiVirus
 - For Windows NT: C:\Winnt\Profiles\All Users\Application Data\Symantec\Norton AntiVirus Corporate Edition\7.5
 - For Windows 2000\XP: C:\Documents and Settings\All Users\Application Data\Symantec\Norton AntiVirus Corporate Edition\7.5
- 3 Restart the client.
The Grc.dat file disappears after it is used to update the client.

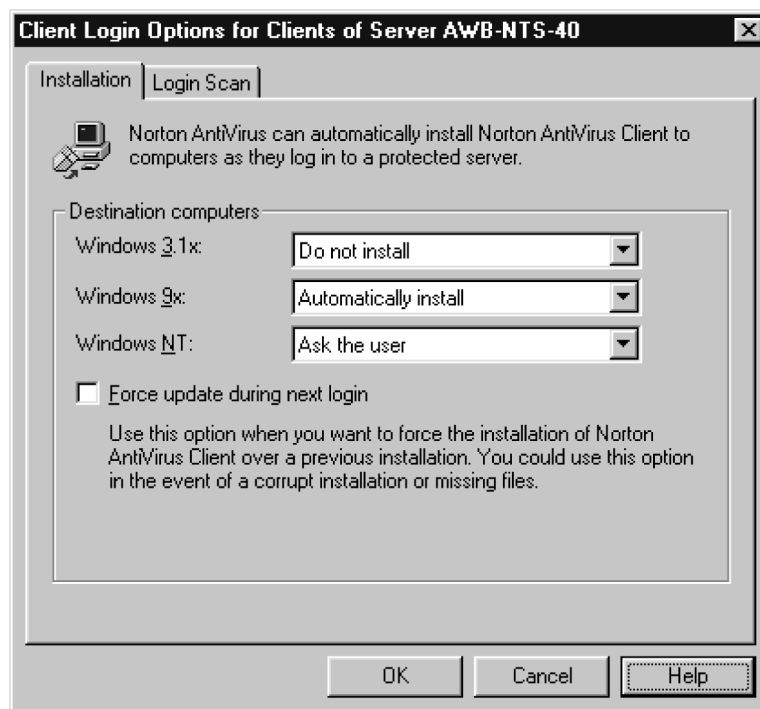
Installing with logon scripts

You can automate client installation using logon scripts that the server Setup program copies to each protected NetWare server and Windows NT server.

When users who are enabled to run the script log on to a protected server, the script calls a program to check the version number of the client that is currently available on the server. If the client version on the server is newer

than the client version on the user's hard disk, or if the client is not installed on the user's hard disk, the client Setup program runs for the platforms you specify.

You can set options to force the client installation or to prompt the user to run the installation. (The Windows NT setting also applies to Windows 2000.)



16-bit clients need a Temp directory specified in their Autoexec.bat

The logon script installation to a 16-bit client will not work unless the 16-bit client has a Temp directory specified in the Autoexec.bat file. For example:

```
set temp = C:\Temp
```

Any valid directory can be used for the temp variable. It does not have to be C:\Temp.

Configuring client installation while logging on

To configure client installation at logon:

- Use Symantec System Center to set update options and enable updates.
- Use your network administration tools to associate users with the logon script.

Because the server Setup program creates a logon group (NORTONANTIVIRUSUSER) on NetWare servers and a netlogon share on Windows NT/2000 servers, setting up users to run the scripts is simple.

Using automatically created groups on NetWare servers

The server Setup program creates a user group called NORTONANTIVIRUSUSER on each NetWare server. When you add a user to the group, the logon script runs according to the options you set in Symantec System Center the next time the user logs on to the server.

Using automatically created shares on Windows NT servers

When you use User Manager to assign the Vplogon.bat logon script to a user, the client computer runs the script from the netlogon share on the server, which launches the client installation according to the options you set in Symantec System Center.

To install using a logon script for NetWare

- 1 In the Symantec System Center console, right-click the server, then click **All Tasks > Norton AntiVirus > Client Login Scan And Installation**.
- 2 Click **Installation**.
- 3 Set client logon installation options for each computer type:
(The Windows NT setting is also used for Windows 2000.)
 - Automatically install: User has no option to cancel the installation at logon.
 - Ask the user: User enters Yes or No to receive the installation at logon.
 - Do not install: No changes are made to the client computer at logon.
- 4 To force an update of Norton AntiVirus Corporate Edition when the client next logs on, check **Force Update During Next Login**.
This option is useful if installing over an installation that is corrupt or missing files.
- 5 Click **OK**.
- 6 Add each user that you want to receive a logon client installation to the NORTONANTIVIRUSUSER group.
The procedure for adding users varies depending on whether you are using NetWare 3.2 or NetWare 4.x/5.x.

How the Force Update During Next Login option works

The Force Update During Next Login does not stay checked once you click OK in the **Client Login Scan And Installation dialog box**.

Checking Force Update During Next Login increments a counter under [ClientNumber] in the Vp_login.ini on the Norton AntiVirus Corporate Edition server. When the client logs on, it looks for this value and compares it with the value in its registry under

HKEY_LOCAL_MACHINE\Software\Intel\VirusProtect6\CurrentVersion\
ClientNumber

Each time you check the Force Update During Next Login box, the value under ClientNumber in the Vp_login.ini increases. If the value does not match, then the client is updated.

Associating users with logon scripts

You can add users to groups in NetWare 3.2, 4.x, or 5.x

To add a user to a group in NetWare 3.2

- 1 On the protected NetWare server, in the Sys:Public directory, type **SYSCON** to start the NetWare system console.
- 2 Select the **Group Information** using the arrow keys, then press **Enter**.
- 3 Under Group Names, select **NORTONANTIVIRUSUSER**, then press **Enter**.
- 4 Under Group Information, select **Member List**, then press **Enter**.
- 5 Under Group Members, press the **Insert** key to add a user to the group.
- 6 A list of all users who are not members of this group appears.
- 7 Select the user you want to receive the logon installation or logon scan, then press **Enter** to add the user to the NORTONANTIVIRUSUSER group.
- 8 Press **Escape** four times, then press **Enter** to confirm that you want to close the system console.

The user has been added to the group, and the change takes place the next time the user logs on.

To add a user to a group in NetWare 4.x or 5.x

- 1 From a client, open the NetWare Administrator utility (Nwadmin32.exe or Nwadm95.exe).
- 2 Double-click the **NORTONANTIVIRUSUSER** group.
- 3 In the Group dialog box, click **Members**.
- 4 Click **Add** to add a user to the group.
- 5 Select the user you want to add, then click **OK**.
- 6 Click **OK** to close the Group dialog box.

The user has been added to the NORTONANTIVIRUSUSER group. The configured logon installation or logon scan occurs the next time the user logs on to the protected server.

- 7 Close the NetWare Administrator utility.

Note: Logon scans are available for Windows 3.1 and DOS clients only.

Installing using a logon script for Windows NT

To install using a logon script for Windows NT

- 1 Copy the following files from the Program Files\Nav\Logon directory on the protected server to the netlogon share (By default, this is C:\Winnt\System32\Repl\Import\Scripts for Windows NT and C:\Winnt\Sysvol\Sysvol\Domainname\Scripts for Windows 2000.):
 - Vplogon.bat
 - Nbpshpop.exe

If this share has been changed, copy the files to the custom directory that you set up as the netlogon share.
- If you are installing to a Windows domain that has both PDC and BDC, copy Vplogon.bat and Nbpshpop.exe to all PDC and BDC locations, or set up replication.

This prevents a file not found error when Windows authenticates to other servers.
- 2 In the Symantec System Center console, select a Norton AntiVirus Corporate Edition server to set logon installation and update options for all client computers that connect to that server.
- 3 Right-click the server, then click **All Tasks > Norton AntiVirus > Client Login Scan And Installation.**
- 4 Click **Installation.**
- 5 Set client logon installation options for each computer type:
(The Windows NT setting is also used for Windows 2000.)
 - Automatically install: User has no option to cancel the installation at logon.
 - Ask the user: User enters Yes or No to receive the installation at logon.
 - Do not install: No changes are made to the client computer at logon.
- 6 Click **OK.**

- 7 On the Windows taskbar, click **Start > Programs > Administrative Tools > User Manager**.
- 8 In the User Manager window, double-click the Username you want to receive a client logon installation.
- 9 In the User Properties dialog box, click **Profile**.
- 10 In the logon Script Name area of the User Environment Profile, type **Vplogon.bat**.
- 11 Click **OK** twice, then close the User Manager dialog box.

Installing from floppy disks or a self-extracting .exe

You can run the Package.exe utility to create installation disks or a self-extracting .exe. Distribute the disks or self extracting .exe to users so that they can install the Norton AntiVirus Corporate Edition client on computers that do not connect to a Norton AntiVirus Corporate Edition server (such as their home computers).

When users run the client installation using this method, the Norton AntiVirus Corporate Edition client is installed by default in unmanaged mode. This means that users must be responsible for getting their own virus definitions files and program updates through an Internet connection. If you want to manage the client, click Managed, then specify a server name during the installation.

Using Package.exe

The Norton AntiVirus Corporate Edition Client Packager (Package.exe) is located in the Navcorp\Rollout\Avserver\Clients folder on Disk 2. The Norton AntiVirus Corporate Edition Client Packager helps you create one of the following:

- A single self-extracting executable for client installation that you can distribute to users on the Web or via email
- A set of floppy disks for client installation that you can distribute to users

During installation, decide whether the client will be managed or unmanaged. By default, the client is unmanaged.

You must create separate installation packages for Windows 9x/NT/2000, Windows 3.1, and DOS. If creating floppy disks, be sure to have plenty of high density floppy disks on hand. For example, a Windows 9x/NT/2000 installation package requires 20 disks.

To create installation disks

- 1 Using File Manager or Windows Explorer, locate and run Package.exe from the Navcorp\Rollout\Avserver\Clients folder on Disk 2.
- 2 Select a target operating system from the list.
- 3 Check **Create A Silent Installation Package** to create an installation that requires no user interaction when the installation program is launched on the client.
- 4 Check **Accept Setup.wis Options For Silent Install** to create an installation that includes switches specified in the Setup.wis file.
A description of each switch is included in the Setup.wis file.
Windows 9x clients will be forced to restart by default.
- 5 Click **Floppy disk**.
- 6 Accept Temp as the default destination folder where the floppy disk files will be created, or change as necessary.

Note: The Setup.wis file is read only during a fresh install. On an overinstall or upgrade, the custom settings in setup.wis are not read.

The amount of free disk space you will need on your computer depends on the operating system for which you are creating installation disks:

Operating system	Required free disk space
Windows 9x/NT/2000	21 MB (75 MB for install)
Windows 3.1	5 MB (10 MB for install)
DOS	4 MB (5 MB for install)

- 7 Click **Create**.
Package.exe copies the files to the folder you designated. This might take a few minutes.
- 8 When package creation is complete, click **OK**, then click **Close**.

- 9 Using File Manager or Windows Explorer, locate one of the following subfolders in the destination folder you chose:

Operating system	Subfolder name
Windows 9x/NT/2000	Nav32flp
Windows 3.1	Nav16flp
DOS	Navdsflp

- 10 Insert a formatted floppy disk into the disk drive, then copy one of the following files to the disk, depending on the operating system for which you are creating installation disks.

Operating system	File name
Windows 9x/NT/2000	Nav732.exe
Windows 3.1	Nav731.exe
DOS	Nav7dos.exe

- 11 Remove the disk from the floppy drive and label it Disk 1.
- 12 Copy the remaining compressed files to floppy disks in sequential order, and label each accordingly.
- For example, for DOS, copy Disk2.cab to a floppy disk and label it Disk 2, then copy Disk3.cab to a floppy disk and label it Disk 3.

To create a self-extracting .exe

- 1 Using File Manager or Windows Explorer, locate and run Package.exe from the Navcorp\Rollout\Avserver\Clients folder on Disk 2.
- 2 Select a target operating system from the list.
- 3 Check **Create A Silent Installation Package** to create an installation that requires no user interaction when the installation program is launched on the client.
- 4 Click **Web or email**.
- 5 Enter the destination folder where you want the package to be created.
The amount of free disk space you will need on your computer depends on the operating system for which you are creating the self-extracting executable:

Operating system	Required free disk space
Windows 9x/NT/2000	21 MB (75 MB for install)
Windows 3.1	5 MB (10 MB for install)
DOS	4 MB (5 MB for install)

- 6 Click **Create**.
Package.exe copies the installation package to the folder you designated. This might take a few minutes.
- 7 When package creation is complete, click **OK**, then click **Close**.

To install from floppy disks

- 1 Insert the floppy disk labeled Disk 1 into the floppy disk drive.
- 2 Do one of the following:
 - For Windows 9x/NT/2000, on the Windows taskbar, click **Start > Run**. Type **A:\Nav732.exe**, then click **OK**.
 - For Windows 3.1x, open File Manager, then click **File > Run**. Type **A:\Nav731.exe**, then click **OK**.
 - For DOS, at the DOS prompt, type
A:\Nav7dos.exe
where A: represents the letter of the floppy disk drive.
- 3 Follow the installation instructions.

By default, Norton AntiVirus Corporate Edition will be unmanaged. To manage the client, specify a server name during the installation.
- 4 Click **Yes** to restart your computer.

To install from a self-extracting file

- 1 Locate the appropriate file in the folder created by Package.exe:

Operating system	File name
Windows 9x/NT/2000	Nav732.exe
Windows 3.1	Nav731.exe
DOS	Nav7dos.exe

- 2 Email or copy this file to a temporary directory on the computer to which you are installing, such as C:\Temp.
- 3 In File Manager or Windows Explorer, double-click the executable file.

This launches the Setup program.
- 4 Read and follow the installation instructions.
- 5 Click **Yes** to restart your computer.

Rolling out custom Grc.dat and LiveUpdate .hst files during client installs

During client rollout, you can install custom Grc.dat and LiveUpdate .hst files.

To roll out custom Grc.dat files

- 1 Do one of the following:
 - For Windows 9x/Me: Create a new folder named To Nav under the folder in which the client setup files are located.
 - For Windows NT/2000/XP: Create a new folder named To App under the folder in which the client setup files are located.

By default, the client setup files are located on Disk 2 under \NAVCorp\Rollout\AVServer\Clients\Win32. You can copy the contents of this directory to a hard disk, then create the To Nav and To App folders.

- 2 Copy the Grc.dat file to the folder that you created.

When Setup runs, it copies the contents of the newly created folder to the directory in which Norton AntiVirus Corporate Edition is installed:

- Windows 9x/Me: C:\Program Files\Norton AntiVirus
- Windows NT 4.0: C:\Winnt\Profiles\All Users\Application Data\Symantec\Norton AntiVirus Corporate Edition\7.5
- Windows 2000/XP: C:\Documents and Settings\All Users\Application Data\Symantec\Norton AntiVirus Corporate Edition\7.5

Note: Files that are normally copied during installation are not written over by files in the To NAV, To LU, or To App directories. For example, a copy of Rtvscan.exe stored in the To Nav directory will not override the Rtvscan.exe file copied during installation.

To roll out custom LiveUpdate .hst files

- 1 Create a new folder named To LU under the folder in which the setup files are located.

By default, the client setup files are located on Disk 2 under \NAVCorp\Rollout\AVServer\Clients\Win32. You can copy the contents of this directory to a hard disk, then create the To LU folder.

- 2 Copy the custom .hst file to the new folder.

Files in the To LU directory are copied to the LiveUpdate directory on the client.

Rolling out clients using third party products

You can roll out Norton AntiVirus Corporate Edition using a variety of third party products, including Microsoft Systems Management Server (SMS) and Novell ManageWise ZENworks.

Rolling out SMS package definition files

Microsoft SMS administrators can use a package definition file (.pdf) to distribute Norton AntiVirus Corporate Edition to clients. For your convenience, Symantec has included a package definition file (.pdf) for the following products on Disk 2 in the Navcorp\Rollouts\Avserver\Clients\Win32 folder:

Package definition file name	Norton AntiVirus Corporate Edition product name
Navce.pdf	Norton AntiVirus Corporate Edition for Windows 95/98/Me, Windows NT (Workstation and Server) and Windows 2000 (Professional, Server, and Advanced Server)

To distribute Norton AntiVirus Corporate Edition with Microsoft Systems Management Server (SMS), you typically complete the following tasks:

- Create source directories to store each Norton AntiVirus Corporate Edition version that you plan to distribute.
- Create a query to identify clients that have sufficient free disk space to install the application.
- Create a workstation package to distribute the software.
- Generate an SMS job to distribute and install the workstation package on clients.

In a workstation package you define the files that comprise the software application to be distributed, and define package configuration and identification information.

The .pdf has its package configuration and identification information already defined. Import the file into your workstation package.

Edit the Grc.dat file

For silent (managed) installs on Disk 2 to work properly, you must edit the Grc.dat file in the corresponding operating system folder (for example, Win32 for Windows 9x/NT/2000).

To edit the Grc.dat file

- 1 Open the appropriate copy of Grc.dat with a text editor, such as Notepad.
- 2 Locate the line that begins with Parent=
- 3 After the = sign, add the following:
S<Servername>
where <Servername> is the name of your server.
- 4 Save and close the text file.

The install folder must be copied locally and Grc.dat must be changed and saved before you run the rollout using SMS.

Using Setup.wis to customize silent installs

Setup.wis allows customization of silent installations. Edit Setup.wis using a text editor such as Notepad.

You can edit Setup.wis as follows:

- [DestinationFolder] can have the values:
InstallDir=
Set to the word Default for the normal installation directory, or specify a valid path to a new directory for installation.
- [RunOptions] can have the values:
StartAutoProtect=
StartAutoProtect refers to File System Realtime Protection. Valid values are 1 for true and 0 for false.
- [SetupCompleteSuccess] can have the values:
BootOption= 1 to stop the forced reboot under 9x (Windows NT does not need to reboot after install).
DisplaySilentMsg=1 to display a dialog box during silent install for Windows 9x and Windows NT. Under 9x this will display a message warning of the impending reboot. 0= do not display dialog box.
- [SnapIns] can have the values:
ForceInstall= 1 to force the install or 0 to not force the install.
Notes= 1 to install the snap-in or 0 to not install the snap-in.
Exchange=1 to install the snap-in or 0 to not install the snap-in.
For example, if ForceInstall = 1 and Notes = 1, the Notes snap-in is installed even when Notes is not installed on the computer. If ForceInstall=0 and Notes=1, the Notes snap-in is installed if Notes is found on the computer. If ForceInstall=0 and Notes=0, the Notes snap-in is not installed even when Notes is found on the computer.

The install folder must be copied locally to save and make these changes.

For more information about using SMS or creating a query, refer to your Microsoft Systems Management Server documentation.

Rolling out with the Novell ManageWise ZENworks Application Launcher

You can use Novell's ManageWise ZENworks Application Launcher to distribute Norton AntiVirus Corporate Edition to Windows 3.x, 9x, NT, and 2000 clients. With minimal configuration effort, you can create a package specific to the target operating system.

Creating a Norton AntiVirus Corporate Edition install package

After ZENworks is installed on the NetWare server and rolled out to clients via a logon script, complete the following tasks:

- From Network Administrator, locate an Organization Unit and create an Application Object that points to the location of the Norton AntiVirus Corporate Edition installation files on the server (for example, Sys:\Nav\Clnt-inst\Win32\Setup.exe for a Windows 9x/NT/2000 client install).
- Configure the Application Object. When setting options:
 - Associate the Application Object to an Organization Unit, group of users, or individual users.
 - When setting system requirements, select the operating system that matches the location of the Norton AntiVirus Corporate Edition install files on the server.
- Set the Application Object install style. For example, select Show Distribution Progress or Prompt User For Reboot If Needed.

After the preparation is completed, ZENworks pushes the Application Object to the client and launches Setup when the client logs on. No steps are required on the client side.

Rolling out with Microsoft IntelliMirror

You can set up IntelliMirror to roll out the Norton AntiVirus Corporate Edition client to Windows 2000 computers in a specified domain or domain subset.

You must have Active Directory set up in your environment.

Note: Client upgrades from previous versions of Norton AntiVirus Corporate Edition are not supported. Also note that IntelliMirror cannot be used to roll out the Norton AntiVirus Corporate Edition server program.

To roll out using IntelliMirror

- 1 On the Windows taskbar, click **Start > Programs > Administrative Tools > Active Directory Users and Computers**.
- 2 Decide whether Norton AntiVirus Corporate Edition is to be installed on all computers in the domain or a subset of computers, then do one of the following:
 - To install to all computers in the domain, right-click the domain and click **Properties**.
 - To install to a subset of computers, right-click the Organization Unit that contains the computers and click **Properties**.
- 3 On the Group Policy tab, select an existing group policy object or create a new policy by clicking **New**.
- 4 Click **Edit**.
- 5 In the Group Policy window, expand **Computer Configuration > Software Settings > Software Installation**.
- 6 Right-click **Software Installation**, then click **New > Package**.
- 7 In the browse window, select the UNC share where the Norton AntiVirus Corporate Edition client files are located.
- 8 Click the **Navce.msi** file and click **Open**.
- 9 Click **Assign**, then click **OK**.

Norton AntiVirus Corporate Edition appears. Norton AntiVirus Corporate Edition will install to the clients in the specified domain or Organization Unit the next time that they are restarted.

Configuring automatic installations of Norton AntiVirus Corporate Edition using NetWare servers without Symantec System Center

If you have a Novell NetWare server but no Windows NT workstations on which to run Symantec System Center, you can configure Norton AntiVirus Corporate Edition to install automatically on your Windows clients. Complete the following tasks:

- Install Norton AntiVirus Corporate Edition on your NetWare server.
For installation instructions, see page 105.
- Configure automated installation of Norton AntiVirus Corporate Edition Windows clients.
- Configure automatic update of virus definitions to servers.
For more information, see [“Updating NetWare servers”](#) on page 270.

To configure the automatic installations

- 1 Load Vpstart.nlm on the server with the /INSTALL switch (LOAD SYS:NAV\VPSTART.NLM /INSTALL).

This switch creates logon script modifications on NDS servers or to SYS:\PUBLIC\NET\$LOG.DAT on Bindery servers.
- 2 Add users to the NortonAntiVirusUser group using NWADMIN or SYSCON.
- 3 Unload the Norton AntiVirus NLM from the console.
- 4 Load Vpregedt.nlm at the server console.
- 5 Select **(O)pen**.
- 6 Select **VirusProtect6**.
- 7 Press **Enter**.
- 8 Select **(O)pen** again, select **LoginOptions**, then press **Enter**.
- 9 Select **(E)dit** to edit values in the left pane of the window.
- 10 Scroll to and select **DoInstallOnWin95**, **DoInstallOnWinNT** and/or **DoInstallOn16Bit**, depending on your environment.

Your choices are: OPTIONAL (the installation requires user input), FORCE (silent install, no user input required), and NONE (do not install). These entries are case sensitive.

- 11 If you previously installed clients and need to force a new update, increment the WinNTClientVersion, Win95ClientVersion, and/or 16BitClientVersion to a higher number.
- 12 Type the following command to reload the Norton AntiVirus NLM:
(LOAD VPSTART)
- 13 Test the client installation.

Note: The client must be a member of the NortonAntiVirusUser group.

Creating Norton AntiVirus Emergency and Rescue Disk sets for client computers

You can create Norton AntiVirus Emergency and Rescue Disk sets:

- Rescue Disks are created for a specific Windows 9x computer. They contain information about the computer's BIOS, partition and boot record. The disk set contains NAVDX, the Symantec command line scanner, and virus definitions files.

The Rescue Disk must be updated whenever the BIOS, partition, or boot record information changes. The Rescue Disk set can then be used to restore the partition and boot record on the computer if they are destroyed by a virus.

- The Norton AntiVirus Emergency Disk set allows you to create a bootable floppy disk set from which you can scan all Windows 9x computers and Windows NT computers with FAT system drives. This disk set does not contain any BIOS, partition, and boot record information. It contains NAVDX and virus definitions files.

The virus definitions files on the Norton AntiVirus Emergency Disks will only be used if the virus definitions files on the local computer are corrupt or not accessible.

Note: The Norton AntiVirus Emergency Disk cannot scan NTFS system drives. Also, the creation of Rescue Disks for the Sony VAIO laptops is not supported.

Creating and using the Norton AntiVirus Emergency Disk set

You will need three disks to create a Norton AntiVirus Emergency Disk set.

To create the Norton AntiVirus Emergency Disk set

- 1 Insert Disk 2 into your CD-ROM drive.
- 2 On the main installation menu, click **Create Norton AntiVirus Emergency Disk**.
- 3 Insert the first 1.44MB floppy into drive A and follow the on-screen prompts to create the Norton AntiVirus Emergency Disks.

To use the Norton AntiVirus Emergency Disk set

- 1 Turn off the power to the computer.
- 2 Insert the first Norton AntiVirus Emergency Disk into drive A.
- 3 Turn on the power to the computer.
- 4 Follow the on-screen instructions.

Creating a Norton AntiVirus Rescue Disk set

You will need five disks to create a Norton AntiVirus Rescue Disk set.

To create a Norton AntiVirus Rescue Disk set

- 1 On the Windows 9x taskbar, click **Start > Programs > Norton AntiVirus Corporate Edition > Rescue Disk**.
- 2 Follow the on-screen instructions.

When complete, test the Norton AntiVirus Rescue Disk set.

To test the Norton AntiVirus Rescue Disk set

- 1 Insert the Norton Rescue Boot Disk in drive A.
- 2 Restart the computer.
- 3 Follow the on-screen instructions.

For information about using the Norton AntiVirus Rescue Disk set, see [“Using the Norton AntiVirus Rescue Disk set to recover from a boot sector infection”](#) on page 385.

Uninstalling Norton AntiVirus Corporate Edition on Windows NT clients

To uninstall Norton AntiVirus Corporate Edition

- 1 From the Start menu, click **Settings > Control Panel > Add/Remove Programs**.
- 2 Click **Norton AntiVirus Corporate Edition**.
- 3 Click **Remove**.

Reboot required before reinstalling

If you uninstall Norton AntiVirus Corporate Edition, you must reboot the computer before reinstalling.

Updating Norton AntiVirus Corporate Edition

This chapter includes the following:

- Planning your migration
- Automatic migration of servers and clients
- Custom settings might be lost
- Quarantine/Virus Bin items are automatically migrated
- How automatic migration works
- Migrating from Norton System Center
- Migrating from the LANDesk Virus Protect /Norton AntiVirus Corporate Edition 6.x console to Symantec System Center
- Migrating an existing LiveUpdate server
- Migrating servers
- Migrating clients to Norton AntiVirus Corporate Edition
- Checksum scanning is unsupported in Norton AntiVirus Corporate Edition 7.5 and higher
- Troubleshooting the update

Planning your migration

In general, the flow of a migration starts with the migration of the management console, followed by the servers, and ending with the migration of the clients. However, the actual sequence of events varies depending on the existing environment. Following are general guidelines to help you plan your migration.

Pilot your rollout first

Do a small scale rollout to identify issues that are likely to occur in the larger migration. For instance, if a particular software configuration that is prevalent in your organization causes problems with the rollout or operation of the client, the pilot should expose this.

A good pilot candidate is the IS or support department. These departments usually have advanced users who will need to be familiar with the client at the start of the rollout.

Minimize unprotected clients

If the migration entails the removal of existing anti-virus software (other than Norton AntiVirus 4.x or 5.x, or LANDesk Virus Protect), there will be a short period of time when some clients are unprotected. You can minimize your exposure by staging the migration/rollout, and by trying to roll out as soon as possible after the previous anti-virus removal. Also, make sure that all of your servers, including GroupWare servers, are protected during this period. This way, incidents will be isolated to a single computer.

Plan your definitions update strategy

Since there are several ways of getting virus definitions file updates to clients and servers, it is essential to decide how this will function before the rollout, and to test your update strategy during the pilot.

Decide how to handle remote and sometimes connected clients as part of your plan.

Unless you are migrating from Norton AntiVirus Corporate Edition 7.0, the update mechanism and schedule established for an earlier version of Norton AntiVirus or LANDesk Virus Protect will not be migrated automatically. You will need to reconfigure when you install or update Norton AntiVirus Corporate Edition and Symantec System Center.

Get definitions updating working immediately

Set the update policy on migrated computers immediately after the rollout, and test it immediately after each stage of the rollout.

Match management snap-in version to client version

You should always use the same version of the management snap-in to manage your clients. For example, to manage Norton AntiVirus Corporate Edition version 7.6 clients use a Symantec System Center console to which you have installed the Norton AntiVirus Corporate Edition version 7.6 management snap-in.

Note: When upgrading from Norton AntiVirus Corporate Edition 7.x to 7.6, all components on the same computer must be updated.

Moving servers between server groups

Although it is best to plan your server group structure before you begin the migration, you do have the flexibility to move servers around later. Unlike servers, you cannot drag and drop clients from parent server to parent server in the Symantec System Center console.

Train your support staff and end users as part of the rollout

Designate time spent training end users and staff as a milestone of your rollout project. This minimizes downtime as a result of end user confusion.

Automatic migration of servers and clients

In many cases, the Norton AntiVirus Corporate Edition Setup program can detect earlier versions of Norton AntiVirus or LANDesk Virus Protect and automatically migrate those versions to Norton AntiVirus Corporate Edition.

The Norton AntiVirus Corporate Edition Setup program will automatically migrate the following products:

- Norton AntiVirus for Win95/98, NT Workstation, NT Server version 4.0x

Note: After migrating from Norton AntiVirus for Win95/98, NT Workstation, NT Server version 4.0x, the computers must be restarted before they will be protected by Norton AntiVirus Corporate Edition.

- Norton AntiVirus for Win95/98, NT Workstation, NT Server version 5.0x
- Norton AntiVirus 2000 Retail, all platforms
- Norton AntiVirus Corporate Edition 7.x (Migrate servers before clients)
- Norton AntiVirus Corporate Edition 6.x, all Wintel platforms except 16-bit
- Norton AntiVirus Corporate Edition 6.x for NetWare servers
- Intel LanDesk Virus Protect 5.01 and higher, all platforms except 16-bit (Virus Bins are not migrated; they are deleted)

Note: When migrating from Norton AntiVirus Corporate Edition version 7.0x to Norton AntiVirus Corporate Edition version 7.5, migrate servers before you migrate clients. When clients are migrated first, but are connected to a parent server running 7.0x, the 7.0x client software attempts to install over the 7.5 client software.

The following products are not migrated by Norton AntiVirus Corporate Edition and must be uninstalled manually before the installation of Norton AntiVirus Corporate Edition:

- Norton AntiVirus for NetWare, all versions
- Norton AntiVirus for DOS/Windows 3.1, all versions
- Intel LANDesk Virus Protect on DOS/Windows 3.1 clients, all versions
- IBM AntiVirus, all versions
- Norton AntiVirus as a part of Norton SystemWorks
- Earlier versions of Norton AntiVirus or LANDesk Virus Protect
- AntiVirus products from other vendors

If Norton SystemWorks is detected when the Norton AntiVirus Corporate Edition Setup program runs, Norton AntiVirus Corporate Edition will not install.

Versions of Norton AntiVirus older than 4.0 or LANDesk Virus Protect earlier than 5.01 will be detected, but the uninstall of those versions will fail, and Norton AntiVirus Corporate Edition will attempt to install anyway. Antivirus products from other vendors will not be detected and Norton AntiVirus Corporate Edition will attempt to install alongside them.

Custom settings may be lost

If you are migrating from Norton AntiVirus Corporate Edition 7.0 or 7.0x, custom settings on clients and servers will be preserved during migration.

If you are migrating from an earlier version of Norton AntiVirus Corporate Edition or LANDesk Virus Protect, custom settings on clients and servers will not be preserved during migration. This includes, but is not limited to:

- Scheduled scans and LiveUpdate sessions
- All scan options
- All realtime protection options
- Custom exclusions and file extensions to scan
- LiveUpdate host files
- Norton AntiVirus activity logs
- Quarantine forwarding information

Some settings for Norton AntiVirus Corporate Edition 6.x will be preserved during migration:

- Client/Parent relationships
- Domains (migrated to Symantec System Center server groups)

During the migration of connected client computers, they adopt the set of client options that have been set at the client's parent server level.

Quarantine/Virus Bin items are automatically migrated

If there are any items in Quarantine on Norton AntiVirus 5.0x clients or servers, or items in Norton AntiVirus Corporate Edition 6.x, they will be migrated automatically to the Norton AntiVirus Corporate Edition Quarantine. However, if any items in Quarantine are determined by Norton AntiVirus Corporate Edition to be uninfected, they are deleted rather than migrated.

How automatic migration works

When Setup.exe for Norton AntiVirus Corporate Edition executes, it completes the following process during the migration:

- Setup calls Pmig.dll, the migration .Dll.
- The .Dll checks registry keys to determine if Norton AntiVirus, LANDesk Virus Protect, or Norton SystemWorks is installed and checks the version.
- The .Dll gets the product uninstall key.
- If Norton SystemWorks is found, the Norton AntiVirus Corporate Edition setup ends.
- If a correct version of Norton AntiVirus is found, any items in Quarantine or Virus Bin are moved to Program Files\Symantec\Conversion.
- The product uninstall is launched using its registry uninstall value.
- After the uninstall completes, the Norton AntiVirus Corporate Edition install starts.

- Near the end of the Norton AntiVirus Corporate Edition install, any items in the Conversion folder are scanned. If they are infected, they are converted to Norton AntiVirus Corporate Edition Quarantine items. If they are uninfected, they are deleted.
- The Norton AntiVirus Corporate Edition install completes.

Migrating from Norton System Center

When migrating from Norton System Center to Symantec System Center, install Symantec System Center and the Norton AntiVirus management snap-in on a different computer than the one on which you are running Norton System Center.

You can continue to use Norton System Center to manage your Norton AntiVirus 4.x and 5.x clients while you are installing Symantec System Center and rolling out the Norton AntiVirus Corporate Edition server program. After you migrate the clients to Norton AntiVirus Corporate Edition, any pre-existing Norton System Center agents remain on those clients.

The decision to uninstall Norton System Center and remove Norton System Center agents from clients depends on whether you are using Norton System Center to manage products other than Norton AntiVirus.

To remove Norton System Center agents from the clients

- 1 Create a Norton System Center job that deletes the agents.
- 2 Execute agtinst.exe /u from a login script.
- 3 Use your own preferred method for compelling clients to run programs.

To remove Norton System Center

- 1 On the Windows taskbar, click **Start > Settings > Control Panel**.
- 2 Double-click **Add/Remove programs**.
- 3 Remove Norton System Center, then Norton Event Manager.

Migrating from the LANDesk Virus Protect / Norton AntiVirus Corporate Edition 6.x console to Symantec System Center

Migrate all installations of LANDesk Virus Protect Administrator to Symantec System Center. To do this, click Install Symantec System Center from Disk 1, then click Install Norton AntiVirus Snap-ins from Disk 2.

If you attempt to install Symantec System Center to a computer that has LANDesk Virus Protect Administrator or LANDesk Virus Protect for NT Server installed, you will be prompted to remove them. Symantec System Center will not install until you remove these products. After you uninstall LANDesk Virus Protect Administrator and LANDesk Virus Protect for NT Server, you can install Symantec System Center.

Before updating servers, run an intense discovery to ensure that all servers you want to update are discovered.

For information about discovery, see the *Symantec System Center Implementation Guide*.

Note: Symantec System Center must run on a Windows NT computer. For more information, see the *Symantec System Center Implementation Guide*.

Migrating an existing LiveUpdate server

If you have already set up LiveUpdate FTP servers or UNC paths, there is no need to modify them. They will continue to be used the same way with Norton AntiVirus Corporate Edition.

When Symantec System Center is installed, you will have the option to install LiveUpdate Administrator as well. To continue to use internal LiveUpdate, install LiveUpdate Administrator to at least one of your Windows NT servers. This lets you schedule LiveUpdate Administration Utility's retrieval of packages directly from Symantec System Center by choosing the server to which LiveUpdate Administration Utility is installed, clicking Properties, and choosing the LiveUpdate Administration Utility property page.

Migrating servers

This section describes how you can migrate servers.

Note: When upgrading from Norton AntiVirus Corporate Edition 7.x to 7.6, all components on the same computer, including Symantec System Center 4.6, must be updated.

Migrating Windows NT servers

This section describes how to migrate from the following:

- Norton AntiVirus 4.x and 5.x to Norton AntiVirus Corporate Edition
- Norton AntiVirus 5.x Quarantine Server
- Norton AntiVirus Corporate Edition 6.x and 7.x

Migrating from Norton AntiVirus 4.x and 5.x to Norton AntiVirus Corporate Edition

If the Norton AntiVirus Corporate Edition install routine detects Norton AntiVirus version 4.x or 5.x on the target computer, it uninstalls that version of Norton AntiVirus before upgrading it to Norton AntiVirus Corporate Edition. This removes the necessity of uninstalling manually.

To migrate Windows NT servers

- 1 On Disk 2 under the Install Norton AntiVirus to Servers option, run the AntiVirus Server rollout tool.
- 2 When prompted to install or update Norton AntiVirus, click **Install**.
The Update selection is used if the targets are already running Norton AntiVirus Corporate Edition 6.x or 7.x.
- 3 Select the server groups for the servers you are rolling out.
You can move servers between server groups later.
- 4 When the install starts, it uninstalls Norton AntiVirus 4.x or 5.x if either is detected.

The migration requires a restart of the Windows NT server.

All custom options from the previous version of Norton AntiVirus will be lost. This includes custom extensions to scan, any exclusions, alerting options, scheduled scans, LiveUpdate sessions, or custom LiveUpdate HST files. Any local activity logs will also be lost.

- 5 Reset the custom options at the Symantec System Center Console as soon as possible after the servers are migrated.

Note: Run LiveUpdate on Norton AntiVirus 4.x for NT Server installations to get the latest update before migrating them to ensure that the migration completes successfully.

Migrating a Norton AntiVirus 5.x Quarantine Server

If you attempt to install Norton AntiVirus Corporate Edition over a Windows NT computer that is acting as a Norton AntiVirus Quarantine server, the install warns you that it will disable the Quarantine Server as it performs the migration. If you let the migration continue, it converts and moves the quarantined items to local Quarantine in the new installation of Norton AntiVirus Corporate Edition. However, you will no longer have an active Quarantine Server if you haven't set one up during the install of the Symantec System Center Console. As soon as you set up the Symantec System Center Quarantine Console, you can either configure the previous server to remain the Quarantine Server, or move the items over to the new Quarantine Server.

Set the identity of the Quarantine Server either at the domain level or the parent server level so that the clients receive this configuration as they are migrated.

Note: Any quarantined items to be automatically converted by the Norton AntiVirus Corporate Edition migration are scanned for viruses. If they are not infected, they are deleted rather than converted. For this reason, you might want to manually move items from your existing Quarantine Server before you migrate it.

Migrating from Norton AntiVirus Corporate Edition 6.x and 7.x

Norton AntiVirus Corporate Edition provides for easy migration from previous versions.

To migrate servers from Norton AntiVirus Corporate Edition 6.x and 7.x

- 1 On Disk 2, run the AntiVirus Server rollout tool.
- 2 Click **Update**.
This preserves your existing domain/server group structure.
- 3 After the server is updated, it might need to be restarted if files that were in use need to be replaced.
Migrate clients of updated parent servers as soon as possible, as they will not get new pattern files from their parent until they have been migrated to Norton AntiVirus Corporate Edition.

Migrating from Norton AntiVirus for NetWare

Since the Norton AntiVirus Corporate Edition install will not detect Norton AntiVirus for NetWare, you must first manually uninstall Norton AntiVirus for NetWare from the servers to be migrated.

To migrate from Norton AntiVirus for NetWare

- 1 On the servers running Norton AntiVirus for NetWare that you want to migrate, unload Norton AntiVirus from the Norton AntiVirus console on the server.
If you do not unload the Norton AntiVirus NLM and you try to install Norton AntiVirus Corporate Edition, the install fails when you try to load Vpstart /Install.
- 2 Remove the Norton AntiVirus for NetWare files from the server.
- 3 Use the NetWare Administrator (Nwadmin32.exe or Nwadm95.exe) to remove the Norton AntiVirus server object from the NDS tree.
- 4 Remove the Norton AntiVirus for NetWare load line from Autoexec.ncf, if necessary.
- 5 From the AntiVirus server rollout tool on Disk 2, install Norton AntiVirus Corporate Edition to your NetWare servers.

- 6 When prompted to choose Install or Update, click **Install**.
- 7 Select the server groups for the NetWare servers (you can move the servers around between server groups later).

All settings from the previous version of Norton AntiVirus are lost and must be reset on the Symantec System Center Console after Norton AntiVirus Corporate Edition is installed.

You can uninstall the Norton AntiVirus for NetWare client console program at your convenience by running its uninstall item from the Norton AntiVirus for NetWare program group on the client computer.

Migrating from LANDesk Virus Protect/Norton AntiVirus Corporate Edition 6.x

LANDesk Virus Protect 5.01 and higher, and Norton AntiVirus Corporate Edition 6.x can automatically be updated to Norton AntiVirus Corporate Edition from Disk 2. For Norton AntiVirus Corporate Edition 6.x, all parent/client relationships will be maintained during the migration.

To migrate from LANDesk Virus Protect/Norton AntiVirus Corporate Edition 6.x

- 1 From Disk 2, click **Install Norton AntiVirus to Servers**.
- 2 Click **Update**.

A list of servers already running a version of LANDesk Virus Protect or Norton AntiVirus Corporate Edition appears.
- 3 Select your target servers from the list.

The migration will complete unattended.
- 4 After the migration, go back to the Symantec System Center Console to reset policy on the server.

If the server has clients, migrate those clients as soon as possible. The clients will not receive new virus definitions files until they are migrated.

Migrating from other server anti-virus products

The Norton AntiVirus Corporate Edition install requires all products that are not automatically uninstalled to be removed from the servers prior to installation.

For more information, see [“Automatic migration of servers and clients”](#) on page 194.

After the anti-virus program is uninstalled, the servers are treated like any other servers to which Norton AntiVirus Corporate Edition is rolled out.

Migrating clients to Norton AntiVirus Corporate Edition

This section describes the following:

- How to determine parent servers and policy
- How to migrate:
 - Windows NT clients
 - Windows 9x clients
 - 16-bit clients
 - Unmanaged Norton AntiVirus Corporate Edition clients
 - Remote clients
 - Clients from other anti-virus products

Determining parent servers and policy

When Norton AntiVirus is installed to servers, each server receives a full set of installation files for all supported platforms in the folder Program Files\Nav\Clt-inst on a Windows NT/2000 server and SYS:NAV\clt-inst on a NetWare server.

Note: If you have servers running Norton AntiVirus that you know will never serve as parents, you can remove the \Clt-inst directory and its sub-directories to reclaim approximately 50 MB of hard disk space.

When anti-virus policy is set on the server, the policy settings are saved in the Grc.dat file. This file exists in all of the install sets and is updated any

time policy is changed. When Norton AntiVirus Corporate Edition is then installed to clients from these install sets, the policy is carried to the clients with this file, along with the identification of the parent server.

When clients are migrated from earlier versions of Norton AntiVirus or LANDesk Virus Protect, the folder to which that version is installed is used.

Note: When migrating from Norton AntiVirus Corporate Edition version 7.0x to Norton AntiVirus Corporate Edition version 7.6, migrate servers before you migrate clients. When clients are migrated first, but are connected to a parent server running 7.0x, the 7.0x client software attempts to install over the 7.6 client software.

Migrating Windows NT clients

There are three recommended methods for migrating NT clients:

- By use of logon script. If this method is used, the users will need to have local administrator rights to the Windows NT computer with which they are logging on.
- By use of the NT Client Install utility. The NT Client Install utility removes the necessity of users having local administrator rights and logging on. The administrator running the NT Client Install utility must have administrator rights to the domain to which the client computers belong. To run NT Client Install utility, on the Tools menu of the Symantec System Center Console, click NT Client Install or run Ntremote.exe directly from the path Navcorp\Rollout\Ntclient on Disk 2.
- Have your users execute Setup.exe (or Setup.exe /s /v /qn for a silent install) directly from the Vphone\Clnt-inst\Win32 folder on their destined parent server. If this method is used, the users will need to have local administrator rights to the NT machine to which they're installing.

In each case, automatic migration from earlier versions of Norton AntiVirus or LANDesk Virus Protect occurs. Also, the clients inherit the policy that was set on the parent server.

You can also migrate Windows NT clients using the program Package.exe, which creates either a self-extracting executable or an install disk set. This method is recommended for remote users.

For more information, see [“Migrating remote clients”](#) on page 208.

Note: If the Norton AntiVirus user interface (Vpc32.exe) is open when the Norton AntiVirus Corporate Edition install is attempted, the migration and install exits on the client.

Migrating Windows 9x/Me clients

There are two recommended methods for migrating Win95/98/Me clients:

- By use of logon script.
- Have your users execute Setup.exe (or Setup.exe /s /v/qn for a silent install) directly from the Vphome\Clt-inst\Win32 folder on their destined parent server.

In each case, automatic migration from earlier versions of Norton AntiVirus or LANDesk Virus Protect occurs. Also, the clients inherit the policy that was set on the parent server immediately.

You can also migrate Windows 9x clients using the program Package.exe, which creates either a self-extracting executable or an install disk set. This method is recommended for remote users.

For more information, see [“Migrating remote clients”](#) on page 208.

Note: If the Norton AntiVirus user interface (Vpc32.exe) is open when the Norton AntiVirus Corporate Edition install is attempted, the migration and install exits on the client.

Migrating 16-bit clients

This sections describes how to migrate from the following:

- Norton AntiVirus 4.x
- LANDesk Virus Protect/Norton AntiVirus Corporate Edition 6.x

Migrating from Norton AntiVirus 4.x

Since these clients are not automatically migrated, the earlier versions of Norton AntiVirus must be removed prior to migration. To uninstall Norton AntiVirus version 4.x for DOS/Windows 3.1, run Setup.exe, which is located in the directory to which Norton AntiVirus was installed with the uninstall command line switch. For example:

```
C:\Nav\Setup.exe /u
```

Uninstalling in DOS can be accomplished via a batch file.

You can then install the Norton AntiVirus Corporate Edition clients using the install instructions.

Migrating from LANDesk Virus Protect/Norton AntiVirus Corporate Edition 6.x

Since these clients are not automatically migrated, the earlier versions of LANDesk Virus Protect/Norton AntiVirus Corporate Edition 6.x must be removed prior to migration. To uninstall LANDesk Virus Protect/Norton AntiVirus Corporate Edition 6.x for DOS/Windows 3.1, run Vpremove.exe, which is located in the original install directory. Uninstalling in DOS can be accomplished via a batch file.

Migrating unmanaged Norton AntiVirus Corporate Edition clients

Unmanaged clients do not communicate with any parent server.

To migrate an unmanaged version of Norton AntiVirus Corporate Edition client to the managed version

- 1 Decide which server is going to be the parent server of each client.
- 2 Copy the Grc.dat file from the Norton AntiVirus folder of the server to the Application Data folder of the client.

After the client is restarted, Rtvscan.exe detects the presence of this file, processes it, and begins communication with the parent server. You can then manage the client from the Symantec System Center Console, as with any other client. This process can be automated with logon scripts or another distribution tool.

Treat the client as any other client that is going to be migrated automatically. The Norton AntiVirus Corporate Edition setup will migrate these clients automatically as described in [“Automatic migration of servers and clients”](#) on page 194. Select the Force Update option from the parent server.

Migrating remote clients

Norton AntiVirus Corporate Edition includes the program Package.exe, which creates a self-extracting executable or an install disk set for remote users. The install set created with Package.exe migrates clients from earlier versions of Norton AntiVirus or LANDesk Virus Protect automatically, in the same manner that a normal install migrates clients.

You can use Package.exe to create install sets for clients to run in either managed or unmanaged mode. Before creating the install packages for remote clients, decide how you want to manage the remote clients:

- Decide if the remote clients should be considered unmanaged clients or managed clients. If they are to be managed, then decide which will be the parent servers of the remote clients. You might want to create a server group specifically to manage the remote clients, as it will be easy to set policy for the group separately if the policy will differ from that for normal connected clients. For example, you will want to let the remote clients launch LiveUpdate on their own for virus definitions updates (in addition to scheduling a LiveUpdate session for them), which you might not want to do for always connected clients.
- Determine and set the anti-virus policy and definitions update process for the remote clients before you run Package.exe to create the installation set. This way, the installation set installs with the policy you have determined.

To create an install set for remote clients that will be managed

- 1 Determine a parent server or server group for the remote clients.
- 2 On the parent server, set the policy exactly as you want it for the remote clients.

This causes Package.exe to package the install set with the policy settings. You can see this by noting that all instances of Grc.dat in the Nav\Clt-inst folder on the parent server reflect the new policy settings.

- 3 If you want Norton AntiVirus Corporate Edition to install in a folder other than its default folder (for instance, Program Files\Norton AntiVirus in the case of Win95/98/Me installs), and if you want to control whether or not a restart occurs after a silent install (it occurs by default on Win95/98/Me, but not on Win NT/2000), you can edit the Setup.wis file that appears in the Clt-inst\Win32 folder on the parent server. In the [DestinationFolder] section of Setup.wis, find the InstallDir=Default line and replace Default with the location where the application is to be installed.

- 4 With the proper Grc.dat file in the install sets in the Clt-inst folders, you can now run Package.exe in the Clt-inst folder of the parent server.
- 5 Select the media type, silent install option, and client platform.
Package.exe creates the install set.

To create an install set for clients that will be unmanaged

- 1 Using File Manager or Windows Explorer, locate and run Package.exe from the Navcorp\Rollout\Avserver\Clients folder on Disk 2.
- 2 Select a target operating system from the list.
- 3 Check **Create A Silent Installation Package** to create an installation that requires no user interaction when the installation program is launched on the client.
- 4 Click **Web or email** to create a self-extracting executable, or click the floppy disk option.
- 5 Distribute the install set to your remote clients.

If the remote clients that you want to migrate are running an anti-virus product from another vendor, the Norton AntiVirus Corporate Edition install will not automatically uninstall the product.

For more information about using Package.exe, see [“Installing from floppy disks or a self-extracting .exe”](#) on page 175.

Migrating clients from other anti-virus products

Since the Norton AntiVirus Corporate Edition install will not recognize the presence of other anti-virus products, they must be removed prior to the rollout.

Checksum scanning is unsupported

Following migration from Norton AntiVirus Corporate Edition version 7.0x to 7.5 or higher, the checksum feature will be enabled but is not supported.

Troubleshooting the update

Some common issues can be resolved quickly.

Cannot see server to update

If you run the Setup program, click Update, then cannot see the server that you want to update:

- Verify that you can see the server in Network Neighborhood. If you cannot, the server might be down or you might have some other network issue.
- If the server is on a network that does not use WINS name resolution, you will need to create a text file that names this server, then import it. For more information see, [“Locating servers during installation”](#) on page 111.
- On the Select Servers To Update dialog box, click Find Computer.
- If that does not work, verify that Norton AntiVirus Corporate Edition is installed and running on the server.

New viruses everywhere

If you find many new viruses on your network that you have not seen before after updating to Norton AntiVirus, this might be because Norton AntiVirus Corporate Edition uses a new scan engine that might detect viruses under a different name. Norton AntiVirus Corporate Edition also has improved detection capabilities, especially for macro viruses.

An update failed or did not complete

If you clicked Cancel part way through an upgrade, the power went out, or one or more servers failed to update, use the following procedure to complete the update.

To complete the update

- 1 If you do not already know which servers failed to update, launch Symantec System Center.
 - a In the console tree, select the server group to which the servers were added.
 - b On the View menu, click **NAV Corporate Edition**.
The version numbers for each server appear in the right pane.
- 2 Make a list of servers that are running Virus Protect 5.01 or higher and label it List 1.
- 3 Make another list of servers that should appear in the domain list but do not (or are dimmed). Label this List 2.
- 4 Rerun Setup.
- 5 Click **Update**.
- 6 Select the servers from List 1 that did not update, then update them.
- 7 For each server in List 2, manually uninstall Virus Protect from the server.
- 8 Install Norton AntiVirus on the servers in List 2.

Updating Norton AntiVirus server fails if Symantec System Center Console is running on the server

If you try to update a remote server while it is running the Symantec System Center Console, the update fails. Close the Symantec System Center Console on your Norton AntiVirus servers before updating them.

If you run the Norton AntiVirus Update program from your workstation, close the Symantec System Center Console so that it can be updated. Run the Update program on each computer where you run the Symantec System Center Console to ensure that all installations are updated.

2

U s i n g N o r t o n A n t i V i r u s
C o r p o r a t e E d i t i o n

Controlling servers and clients

This chapter covers the following topics:

- Managing server groups
- Selecting from the tree or the right console pane
- Applying policies at the server group, server, and client level
- Changing a client's management status
- Changing the client check-in interval
- An in-depth look at Grc.dat
- Enabling the Norton AntiVirus Corporate Edition icon in the Windows system tray
- Deleting clients
- Changing the client expiration level
- Centralized client scanning control
- Default communications port

Managing server groups

Server group members can share the same Symantec product policies. You can also run a Symantec product operation on all members of a server group.

The first time that you roll out a manageable Symantec product to servers, you create a server group. (For example, the first time that you run the Install Norton AntiVirus to Server or NT Clients option from Disk 2, you create a server group.)

From the Symantec System Center console, you can create new server groups and manage their membership. You can create as many server groups as you need to manage your servers and clients efficiently. Servers can be members of only one server group at a time, but they can be moved from one server group to another.

You can create and populate server groups to separate configurations and to separate communications across WAN links. Avoid creating server groups that span WAN links.

For administrators who have used Norton AntiVirus Corporate Edition 6.0 or LANDesk Virus Protect 5.x until recently: Server groups are identical in functionality to your old Virus Protect or Norton AntiVirus domains. You must migrate your old domains to server groups before you can manage them. The migration can be performed automatically during installation.

For more information, see [“Automatic migration of servers and clients”](#) on page 194.

Filtering the server group view

You can filter which server groups display in the Symantec System Center server group list. You can monitor and administer only the server groups that display in the list. By default, the Symantec System Center console displays all server groups. To remove server groups from your console, filter the view.

You receive notifications for displayed server groups only. If you filter a server group, you will not receive notifications from that server group.

To filter the server group view

- 1 On the Symantec System Center console tree, right-click **System Hierarchy**, then click **View > Filter Server Group View**.
- 2 Uncheck the server groups that you want to filter from the server group list.
All server groups display by default.
- 3 Click **OK**.

To view a single server group

- On the Symantec System Center console tree, right-click the server group, then click **New Window From Here**.

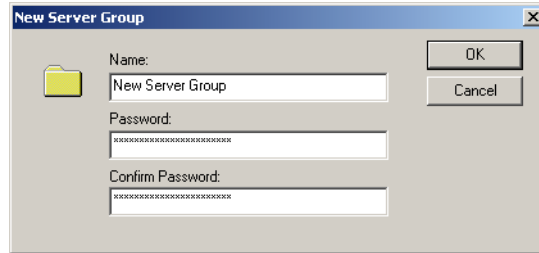
Grouping servers into server groups

The installation program groups all of the servers that you select into one server group. This might be adequate if you want all of your file servers to use the same settings for the manageable Symantec product. However, if you want to make global configuration changes for groups of servers, you can create new server groups and easily drag and drop (or cut and paste) servers from one server group to another. When you move a server, all connected client computers move with it.

For example, you might have some servers that require higher levels of protection. In this case, place all of them in the same server group and set special options to protect the server group.

To create a new server group

- 1 On the Symantec System Center console tree, right-click **System Hierarchy**, then click **New > Server Group**.



- 2 Type the name for the new server group.
The name cannot have more than 47 characters.
- 3 In the Password text box, type a password for the server group.
- 4 In the Confirm Password text box, retype the password.
- 5 Click **OK**.

Note: A server can belong to only one server group. You can move a server between groups using a drag and drop operation.

To rename a server group

- 1 Unlock the server group that you want to rename, if necessary.
- 2 Right-click the server group, then click **Rename**.
- 3 Enter the new server group name.

To delete a server group

- 1 Unlock the server group that you want to delete, if necessary.
- 2 From the server group you will delete, cut any existing servers and paste them into another server group.
You can only delete a server group if it is empty.
- 3 Right-click the empty server group, then click **Delete**.
- 4 Right-click **System Hierarchy**, then click **Refresh**.

Selecting a primary server for a server group

When you select a server group object in Symantec System Center and set options, the settings are saved to the primary server in the server group. Other servers in the same server group will then use the new configuration.

You must specify which server in the server group is the primary server. No server is specified as the primary server by default. Until you designate a primary server, you cannot perform some Symantec product management operations.

Computers running any of the following operating systems can be primary servers:

- Windows 2000 Server, Advanced Server, or Professional
- Windows NT 4.0 Server or Workstation
- NetWare Server

The primary server plays an important role, so select a stable server that is always running.

To assign the primary server for an existing server group

- Right-click the server that you want to be the primary server, then click **Make Server A Primary Server**.

Note: When changing primary servers, you will lose the AMS² alerts you have set up. You can reconfigure the alerts on the new primary server, or export the alerts to the new server before you change primary servers. For more information, see the *Symantec System Center Implementation Guide*.

Changing a server group password

The default password used to unlock the server group created during install is:

symantec

Note: Passwords are case sensitive.

When you create a new server group, you enter the password that you want to assign to it.

You can change the password as necessary. To do so, the server group must have a primary server assigned to it. Empty passwords are allowed.

To change the password

- 1 Right-click the server group.
- 2 Click **Configure Server Group Password**.



- 3 Type the old password.
- 4 Press Tab, then type the new password.
- 5 Press Tab, then retype the password.
- 6 Click OK.

Locking and unlocking server groups

You can lock a server group with a password to prevent unauthorized administrators from making configuration changes. You can add or change passwords at any time. The default password for the server group created during install is:

symantec

Note: Passwords are case sensitive.

To lock a server group

- Right-click the server group that you want to lock, then click **Lock Server Group**.

To unlock a server group

- 1 Right-click the server group, then click **Unlock Server Group**.
- 2 Type the password to unlock the server group.
- 3 Check **Save This Password** if you do not want to retype the password in future sessions or for other server groups that may have the same password.

If the password is correct, it will be saved. When you attempt to unlock a server group in the future, Symantec System Center will try all saved passwords. You will be prompted for a password only if none of the saved passwords works.

To prevent server groups from locking when you exit the console

- 1 On the Symantec System Center console, right-click **System Hierarchy**, then click **Properties**.
- 2 Uncheck **Lock All Server Groups When Exiting Console**.

Saving and changing server group passwords

When entering a password, click **Save This Password** if you do not want to reenter the password in future sessions. Saved passwords are DES encrypted and are stored in the registry of the local computer.

Once the password is saved, you will not need to enter it when opening any server group that uses the same password.

To save a password

- 1 On the Symantec System Center console tree, right-click a locked server group, then click **Unlock Server Group**.
- 2 Type the password for the server group.
- 3 Check **Save This Password**.
- 4 Click **OK**.

To change a server group password

- 1 Right-click the server group, then click **Configure Server Group Password**.
- 2 Type the old password.
- 3 Type the new password, then type it again for confirmation.
- 4 Click **OK**.

If you do not save server group passwords

If you do not save passwords, all server groups are automatically locked by default each time Symantec System Center runs, even if you unlocked them the last time that you ran the program.

If you unchecked the Lock All Server Groups When Exiting Console box on the System Hierarchy properties page, the server group will remain unlocked when the Symantec System Center console is reopened.

Changing primary and parent servers

You can change primary servers and parent servers easily.

To change a primary server

- 1 In the Symantec System Center console tree, double-click the server group icon.
- 2 Right-click the secondary server that you are designating as a primary server, then click **Make Server A Primary Server**.

To change a parent server

- 1 Copy the Grc.dat file from the one of the following folders of the intended parent server (based on the target client's platform):
 - NAV\Clnt-inst\Win32
 - NAV\Clnt-inst\Win16
 - NAV\Clnt-inst\DOS
- 2 On the client, paste the Grc.dat file to one of the following folders:
 - For Windows 9x\Me: C:\Program Files\Norton AntiVirus
 - For Windows NT: C:\Winnt\Profiles\All Users\Application Data\Symantec\Norton AntiVirus Corporate Edition\7.5
 - For Windows 2000\XP: C:\Documents and Settings\All Users\Application Data\Symantec\Norton AntiVirus Corporate Edition\7.5
- 3 Restart the client.

What happens when you move a server to a different server group

When you move a server from one group to another, a Grcsrv.dat file is created on the server automatically. The Grcsrv.dat file synchronizes the new server group settings to the server. The new server group must have a primary server.

Grcsrv.dat is located in the same directory to which Norton AntiVirus Corporate Edition was installed on the server. It has the same format as a Grc.dat file. It is created only when synchronizing a server to a new server group's settings.

Grcsrv.dat only works for servers running Norton AntiVirus Corporate Edition version 7.5 or later. For older servers, the topology service copies registry settings from the primary server to the server that is being moved.

Selecting from the tree or the right console pane

If you select a client or server from the right console pane, you communicate directly with that computer through a proprietary protocol. The options you set apply immediately and directly to the registry of the target computer.

If you select a server or server group from the console tree, you do not communicate directly with that computer or server group. Rather, the options you set are applied to the Grc.dat file.

The Grc.dat file stores important information, such as parent server identity and Norton AntiVirus Corporate Edition configuration settings. Clients read the Grc.dat file and then modify the registry to apply the options listed there. Once processed on the client, the Grc.dat is deleted.

The Grc.dat file always overwrites and supersedes changes made through direct communication.

Applying policies at the server group, server, and client level

You can set Norton AntiVirus Corporate Edition policies and apply them at the server group, server, or client level.

To apply to a server group

- 1 In the console tree, right-click the server group icon, then click **All Tasks > Norton AntiVirus**.
- 2 Click a specific menu item.

To apply to a single primary or secondary server

- 1 In the console tree, click the server group.
- 2 In the right pane, right-click the server and click **All Tasks > Norton AntiVirus**.
- 3 Click a specific menu item.

To apply to one or more servers

- 1 In the console tree, click the server group icon.
- 2 In the right pane, shift-click to select multiple servers.
- 3 Right-click the highlighted servers and click **All Tasks > Norton AntiVirus**.
- 4 Click a specific menu item.

To apply to one or more clients

- 1 Double-click the server group icon.
- 2 In the console tree, click the server.
- 3 In the right pane, shift-click to select multiple clients.
- 4 Right-click the highlighted clients and click **All Tasks > Norton AntiVirus**.
- 5 Click a specific menu item.

Changing a client's management status

You can change a client's management status from:

- Unmanaged to managed
- Managed to unmanaged

Changing a client from unmanaged to managed

You can assign an unmanaged client to a parent server whenever necessary. Once connected to a Norton AntiVirus Corporate Edition server, the Norton AntiVirus Corporate Edition client runs in managed mode and can be administered and configured centrally.

You can also reassign a parent server when necessary.

To assign a new parent server, do one of the following:

- Copy the Grc.dat file from the server to the client.
- Use logon scripts to detect and reinstall the clients automatically so that they run in managed mode. However, if the unmanaged version is the same as the version that you are installing, you will need to force an install when the client next logs on.

For more information about forcing an installation at logon, see [“Installing with logon scripts”](#) on page 169.

To copy Grc.dat to the client

- 1 Copy the Grc.dat file from the one of the following folders (based on the target client's platform) of the intended parent server:
 - NAV\Clnt-inst\Win32
 - NAV\Clnt-inst\Win16
 - NAV\Clnt-inst\DOS
- 2 Paste the Grc.dat file to one of the following folders on the client:
 - For Windows 9x\Me: C:\Program Files\Norton AntiVirus
 - For Windows NT: C:\Winnt\Profiles\All Users\Application Data\Symantec\Norton AntiVirus Corporate Edition\7.5
 - For Windows 2000\XP: C:\Documents and Settings\All Users\Application Data\Symantec\Norton AntiVirus Corporate Edition\7.5
- 3 Restart the client.

The Grc.dat file disappears after it is used to update the client.

Editing the Grc.dat file to control clients

If you do not want to manage a client-server application in order to protect your desktop computers from viruses or give up bandwidth on your network to the Norton AntiVirus Corporate Edition managed solution, you might prefer to control clients by editing the Grc.dat file. Editing Grc.dat lets you control clients when you want to without having them check in with parent servers.

For more information about the Grc.dat, see [“An in-depth look at Grc.dat”](#) on page 231.

Warning: If you choose to edit the Grc.dat file, use a text editor such as Notepad only. Edit very carefully. Symantec Corporation does not provide support for editing the Grc.dat file.

Changing a client from managed to unmanaged

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.

Uninstalling and reinstalling Norton AntiVirus Corporate Edition ensures that no settings are retained from the managed installation. To let users change configuration options, remove the HKEY_LOCAL_MACHINE\Software\Intel\Landesk\VirusProtect6 subkey.

To remove the subkey

- 1 Uninstall Norton AntiVirus Corporate Edition from the client workstation.
- 2 Open the Registry Editor.
- 3 Delete the HKEY_LOCAL_MACHINE\Software\Intel\Landesk\VirusProtect6 subkey.
- 4 Reinstall Norton AntiVirus Corporate Edition to the client.
- 5 When prompted to make the client Managed or Unmanaged, click **Unmanaged**.

Using a text editor (such as Notepad), edit the client's Grc.dat file as follows to bring the client to an unmanaged state:

[KEYS]

!KEY!= \$REGROOT\$

ClientType=D2

Add this to the Grc.dat file to change this to an unmanaged client.

Connected=D0

Do not initialize the transport layer.

Parent=S

No parent server.

AlertDirectory=S

This was formerly a directory on the server.

RemoteHomeDirectory=S

This was formerly a directory on the server.

!KEY!= \$REGROOT\$\AdministratorOnly

!KEY!= \$REGROOT\$\AdministratorOnly\
General

ShowVPIcon=D1

Enable the virus protect icon in the system tray.

!KEY!= \$REGROOT\$\AdministratorOnly\
Security

LockUnloadServices=D0

Reenable the option to load/unload services from the main UI.

UseScanNetDrivePassword=D0

Do not prompt for a password to scan network drives.

UseVPUninstallPassword=D0

Do not prompt for a password when uninstalling the client.

VPUninstallPassword=S

Delete uninstall password.

NetScanPassword=S

Delete network drive scan password.

!KEY!= \$REGROOT\$\PatternManager

EnableProductUpdates=D1

LiveUpdate will download product patches if available.

LockUpdatePattern=D0	Reenable the option to LiveUpdate manually from the main UI.
LockUpdatePatternScheduling=D0	Reenable the option to schedule LiveUpdate from the main UI.
UpdateClients=D0	Do not request definitions from a parent server.

Note: The changes will not take effect fully until the Norton AntiVirus Client service is restarted (on Windows NT/2000/XP) or the computer is restarted (on Windows 9x/Me).

Changing the client check-in interval

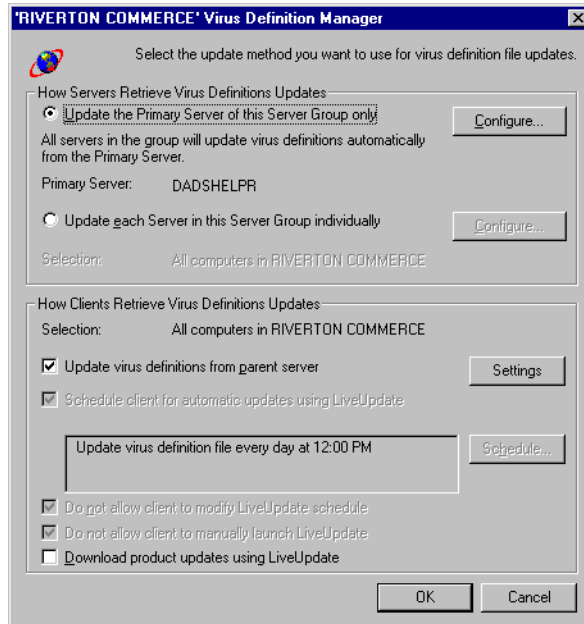
Norton AntiVirus Corporate Edition client configuration updates are not triggered by client check-in as they were prior to version 7.5. Check-in intervals can be lengthened from the default of 60 minutes when necessary. Longer client check-in intervals help reduce traffic and server processing.

For mobile clients, a check-in interval of one hour should be adequate. For very stable groups of clients, longer check-in intervals of 24 hours or more may better meet operating requirements.

Note: Make sure that the period for dropping nonreporting clients from the parent server's list of connected clients is longer than the new, longer client check-in intervals.

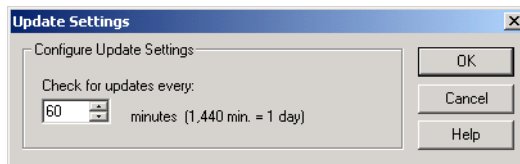
To change the client check-in interval

- 1 In the console tree, right-click the server group, server, or client icon, then click **All Tasks > Norton AntiVirus > Virus Definition Manager**.



- 2 Click **Settings**.

The Update Settings dialog box appears.



- 3 Change the update frequency as necessary.
For example, you can change the interval to 1440 minutes if you want the client to check in once every 24 hours.

An in-depth look at Grc.dat

The Grc.dat file is a text format file that acts as a repository of changes being made to a group of clients.

There are several versions of the Grc.dat file on a parent server. One appears in \Program Files\NAV (or for Windows 2000 computers in \Documents and Settings\All Users\Application Data\Symantec\Norton AntiVirus Corporate Edition\7.5). This version of Grc.dat gets copied to the client to initiate options changes at the client level. Another Grc.dat file appears in each of the \CLT-INST directories. These are copied to the client during installation. A third Grc.dat file is in the rollout directory of Disk 2. It is a simplified version, with commented lines that let you turn LiveUpdate on and off, or to specify a parent server.

Any time you modify client options from the Symantec System Center console at the server group level or server level, this information is updated on the client's parent server.

When you modify server options, you directly modify the registries of the selected servers via the Transman communication method. Transman uses dynamic libraries that include CBA (Common Base Agent) and NTS (Network Transport System).

Note: It is not necessary for a port to be open to each of the servers to write the changes.

The role of the primary server

The primary server acts as the repository of all server options on a server group level. If you modify at the server group level, the changes are recorded in two places:

- In the registry of the primary server for that server group in the CurrentVersion\DomainData key.
- In all of the other servers.

The CurrentVersion\DomainData key contains all the entries found under CurrentVersion, including the ClientConfig key.

HKEY_LOCAL_MACHINE\Software\Intel\Landesk\VirusProtect6\CurrentVersion is the root of all entries for Norton AntiVirus Corporate Edition. Client and server settings appear under the root.

Scan information for scans set through Symantec System Center console is located under HKEY_LOCAL_MACHINE.

Scan information is located under HKEY_CURRENT_USER for scans that were created on the computer using the Norton AntiVirus Corporate Edition user interface.

The role of the ClientConfig key

The ClientConfig key on the CurrentVersion\ClientConfig level contains all of the option changes for the clients of the server that is being selected for action.

The ClientConfig key under the CurrentVersion\DomainData\ClientConfig key (on the primary server) contains the client options for all of the clients of all the servers in the server group. Note that the options are recorded here only if you have changed the options at the server group level.

If you make a client configuration change at the server group level, the ClientConfig key at the CurrentVersion level on the primary server will change, affecting the options of its children. The ClientConfig key under CurrentVersion\DomainData will also change, affecting the clients of all the secondary servers in that group as they get the registry changes from the console.

Where changes are recorded

The process changes if you modify client options at the server level. The options changes are written to the registry of the server under CurrentVersion\ClientConfig. The options are then bundled into a Grc.dat file and sent to the clients. RTVSCAN on the client then converts the options to registry keys in the client's registry, and deletes the Grc.dat file.

The contents of Grc.dat are parsed into the registry of 32-bit clients and the VPCCC16.ini on Win3x clients.

If you modify client options at the server group level, all changes are written to the registry of the primary server. The changes are written to CurrentVersion\ClientConfig for the benefit of the primary server's children. The options are written to the \Nav\Grc.dat file on the primary server and pushed to the primary server's children.

The changes are also written to CurrentVersion\DomainData\ClientConfig. They are then written to the secondary servers' registries, and then a \Nav\Grc.dat is written and pushed to the clients of each of the secondary servers.

What causes Grc.dat to be written

When you make a change to client options on a group level, the changes are recorded in the ClientConfig key. They are then written to \Nav\Grc.dat and pushed to the client, which incorporates the changes into its registry.

On the Symantec System Center console, when you accept changes on the server group level, the ProcessGRCNow key under CurrentVersion\ProductControl on the affected server moves from 0 to 1. RTVScan on the server has a thread monitoring this key. When RTVScan sees the move from 0 to 1, it rebuilds the Grc.dat file. Another thread then feeds the Grc.dat file to all of its clients where the local RTVScan can find it. Every 60 seconds the local RTVScan runs a CheckGRC call (configurable in the registry). When it finds one, it converts it to one or more registry entries and deletes the Grc.dat file.

How changes are made

When you click OK to options changes the first time, the ProcessGRCNow value is changed to 1. RTVScan processes the changes into the Grc.dat file, and pushes it out to its clients. Each time you click OK subsequently, the ProcessGRCNow value is checked. If the value is already 1, it stays 1. If it is 0, it is incremented to 1. RTVScan has finished pushing out the Grc.dat file with the first OK change. Now it returns to the ProcessGRCNow key. The value is 1 again, and the process starts over. However, RTVScan has all the accumulated changes going into the new Grc.dat file. It is processed normally, pushing it out to its clients, and checks one more time for the value of ProcessGRCNow. If it is still 0, it continues to watch for changes. If the value is 1, the process starts over until it returns to 0.

Changing the Debug value

Under the CurrentVersion\ProductControl key, change the Debug key to a value of verbose. A DOS box appears and all RTVScan actions are recorded here. If you make a client option change at a server or server group level, the entire process scrolls on-screen.

To capture the data in a file, type logging after the verbose setting. Both settings might slow your computer.

If you close one of these windows, you terminate the process that opened it. You will need to restart the server and set the debug value back to none.

Editing the Grc.dat file

You can add a line to the registry during rollout if necessary by editing the Grc.dat file. For example, the following line:

Warning: If you choose to edit the Grc.dat file, use a text editor such as Notepad only. Edit carefully as Symantec Corporation does not provide support for editing the Grc.dat file.

```
!KEY!=$REGROOT$\AdministratorOnly
```

creates a key called AdministratorOnly under HKLM\Software\Intel\LANDesk\VirusProtect6\CurrentVersion. Any additional lines of text (up to the next !KEY!) are key values.

You could then create the following section:

```
!KEY!=$REGROOT$\AddressCache\GUESTROOM
```

Below this line, you could add a line such as test=D1.

If you then copy this Grc.dat into one of the following locations, the Grc.dat file will convert to a registry entry:

- For Windows 9x\Me: C:\Program Files\Norton AntiVirus
- For Windows NT: C:\Winnt\Profiles\All Users\Application Data\Symantec\Norton AntiVirus Corporate Edition\7.5
- For Windows 2000\XP: C:\Documents and Settings\All Users\Application Data\Symantec\Norton AntiVirus Corporate Edition\7.5

The key and value you defined will be created.

Formatting rules

Formatting rules are as follows:

- The first line of Grc.dat must be [KEYS]
- Any registry key can be created under HKLM by following the format !KEY!=<Regkey path minus HKLM>
- For example:
 - You create the registry key HKLM/Software/Symantec
!KEY!=Software/Symantec
 - You create the following registry key:
HKLM\Software\Intel\LANDesk\VirusProtect6\CurrentVersion\Patternmanager
!KEY!=\$REGROOT\$\PatternManager :
!KEY!=Software\Intel\LANDesk\VirusProtect6\CurrentVersion\PatternManager
- To add registry values, the following formatting rules apply:
<registry value name>=<B,S,D><Regvalue>
B: Binary: For this code letter, each byte is represented by two hexadecimal values. The first four hexadecimal should equal the total number of hexadecimal values.
S: String code letter.
D: DWORD code letter.
- Every entry made after the code letter must be in all caps.

- For realtime scan options, if an option is to be locked the corresponding registry value name must be preceded by an exclamation point (!).

For example:

The following registry key enables realtime scanning and disables the checkbox on the client's user interface:

! OnOff=D1 writes two registry values, OnOff=1 and OnOff-L=0.

- Comments can be added by using one of the following characters at the beginning of the line: 0, #, ;, \, or //.
- The following keyword can be used as part of the value (the information to the right of the equal sign) for registry keys and values:
\$FILE_SERVERS: Resolves to computer name

\$REGROOTS: resolves to

Software\Intel\LANDesk\VirusProtect6\CurrentVersion

\$_CHOMES: Resolves to the path of the home directory (target directory)

\$CHOMES: Resolves to \$-CHOME\$ (hard coded)

The following lines would write the registry key

HKLM\Software\Intel\LANDesk\VirusProtect6\CurrentVersion\Legacy
and the registry value OldLogsDirectory with the value C:\Program
files\Navnt\Logs on a computer with Norton AntiVirus Corporate
Edition installed in the default directory:

[KEYS]

!KEY!=\$REGROOT\$\Legacy

OldLogsDirectory=S\$_CHOMES\$\logs

- The registry value GRC-State-Counter will cause all the registry values in the associated registry key to be cleared if the value it is equal to is different from the value on the client processing from the Grc.dat file.

The structure of Grc.dat

The following table describes Grc.dat file entries.

Key Name and Sample Options Settings	Description
[KEYS]	
!KEY!=\$REGROOT\$	\$REGROOT\$ is the root of the following name.
[HKEY_LOCAL_MACHINE\Software\Intel\LanDesk\VirusProtect6\CurrentVersion]	
FullGRCUpdateCounter=D1	Client only. This value is compared with the Grc.dat file on the server to see if a full Grc.dat update is needed.
LicenseNumber=Sxxxxxx	License number.
Connected=D1	D0= No, D1=Yes. Determines whether to load the transport layer in RTVScan. For managed servers and clients, the transport layer should always be initialized.
AlertDirectory=S\\[path...]\$	UNC path to server where alerts should be sent.
RemoteHomeDirectory=S\\[path...]	Client only. UNC path to server from which client software was installed.
Parent=S[SERVERNAME]	Replace [SERVERNAME] with the name of the parent server. If no server is specified, the client is unmanaged.
GRCUpdateTime=B00081E061E1001060000	Client only. This value is compared with the Grc.dat file on the server to see if a regular Grc.dat update should occur.
!KEY!=\$REGROOT\$\AddressCache	

Key Name and Sample Options Settings	Description
!KEY!=\$REGROOT\$\AddressCache\SUN	Address_0 & Address_1 represent the parent server's IP and IPX addresses. Lines under \AddressCache record parent server information and must not be modified.
Address_0=B002000C020000B9700009B409CEF000 00	
Protocol=SAddress_1	
Address_1=B002000202000824100000000015600609 79842DA000000000000000000000000000000001	
good=D1	D0=Discovery was not able to communicate with the server. D1=Discovery was able to communicate with the server on its last attempt.
!KEY!=\$REGROOT\$\AdministratorOnly	
!KEY!=\$REGROOT\$\AdministratorOnly\General	
DisplayOutdatedMessage=D0	Determines whether to display the outdated pattern file message.
RunBrowser=D0	Activates the option to run a Web browser when a virus is found.
ShowVPIcon=D0	D0=Do not show the Norton AntiVirus Corporate Edition icon in the system tray. D1=Show the Norton AntiVirus Corporate Edition icon in the system tray.
WarnAfterDays=D90	Specifies how old the pattern file must be before a warning message appears.
!KEY!=\$REGROOT\$\AdministratorOnly\Security	

Key Name and Sample Options Settings	Description
VPUninstallPassword=S	Clears the uninstall password.
UseVPUninstallPassword=D1	D0=Do not prompt for a password when uninstalling the client. D1=Prompt for password when uninstalling the client.
UseScanNetDrivePassword=D1	D0=Do not prompt for a password to scan network drives. D1=Prompt for a password to scan network drives.
NetScanPassword=S	Clears the network scan password.
LockUnloadServices=D1	D0=Enable the option to load/unload services in the Norton AntiVirus Corporate Edition interface. D1= Disable the option to load/unload services in the Norton AntiVirus Corporate Edition interface.
!KEY!=\$REGROOT\$\Common	
NTEventLog=D1	Controls whether or not to write events to the NT Event log. D0=Don't write to Event log. D1=Write to Event log.
ForwardLogs=D0	Forwards general logging to the parent server. General logging includes scan starts and scan stops. D0=Disable forwarding. D1=Enable forwarding.

Key Name and Sample Options Settings	Description
AlertParent=D	This controls whether or not a local machine forwards an alert to its parent server when a virus is detected. For servers, this means the alert is forwarded to the domain's primary server. For primary servers, this means the alert is forwarded to the computers listed under the Consoles key. D0=No. D1=Yes.
RenameExt=SVIR	This is the extension applied to infected files.
LDVPEventLog=D1	Controls whether or not to write events to LDVP log files. D0=Don't write to log file. D1=Write to log file.
MessageBox=D0	Display message. D0=Disabled. D1=Enabled.
!KEY!=\$REGROOT\$\LocalScans	
!KEY!=\$REGROOT\$\LocalScans\ManualScan	
SecondMacroAction=D1	Second action taken for macro viruses if first action fails. D1=Quarantine. D3=Delete. D4=Leave alone. D5=Clean.
ZipExts=.sarj, .lha, .zip, .mme, .izh, .uue	Extensions that will be scanned as archived files. These files are decompressed and the files inside are scanned.
ScanBootSector=D1	This controls whether or not to scan the boot sector on all local drives. D0=No. D1=Yes.
FirstAction=D5	D1=Quarantine. D3=Delete. D4=Leave Alone. D5=Clean.

Key Name and Sample Options Settings	Description
DisplayStatusDialog=D0	When set to 1, the scan status dialog appears during the scan.
NeededFreeDiskSpace=D30720000	This specifies the minimum disk space (in bytes) required for a manual scan to start. 30720000=30 MB. This is the default value in absence of this value.
Types=D6	Determines the types of files to scan if FileType is set to 2. D1=Archived files. D2=Program files. D4=Document files. D6=Both document and program files.
FirstMacroAction=D5	D1=Quarantine. D3=Delete. D4=Leave Alone. D5=Clean.
ScanMemory=D1	Controls whether or not to scan memory. D0=No. D1=Yes.
FileType=D1	Files being scanned. D0=All. D1=Selected extensions. D2=Selected types.
ScanAllDrives=D1	Scan all drives on the system. D0=Disabled. D1=Enabled.
MessageBox=D0	Display message. D0=Disabled. D1=Enabled.
ZipFile=D1	Scan a file in compressed files. D0=Enabled. D1=Enabled.

Key Name and Sample Options Settings	Description
Logger=D1	Specifies the event type to be used in event logs. D0=Scheduled scan. D1=Manual scan. D2=Realtime scan. D6=Console. D7=VpDown. D8=System. D9=Startup. D10=Idle. D100=Client. D101=Local end. D102=Forward.
ZipDepth=D3	D1=Only files in archive. D2=Files and archives in archive. D9=Files are archives inside archive up to nine levels deep.
SecondAction=D1	D1=Quarantine. D3=Delete. D4=Leave Alone. D5=Clean. If first action fails.
Softmice=D1	Controls whether or not files are scanned for mutation viruses. This is always set to 1. D0=No. D1=Yes.
Exts=.sdot, .doc, .html, .htt, .htm, .vbs, .js, .shs, .ppt, .mso, .pot, .rtf, .mdb, .jtd, .hlp, .inf, .ini, .hta, .mp?, .obd, .obt, .pps, .smm, .vsd, .vst, .xl?, .vss, .exe, .com, .bin, .sys, .dll, .ocx, .vxd, .bat, .btm, .csc, .pif, .386, .cla, .ov?, .drv, .scr, .acm, .acv, .adt, .ax, .cpl, .csh, .jse, .pl, .pm, .sh, .shb, .vbe, .wsf, .wsh	
REGROOT\$\ManualScan	
!KEY!=\$REGROOT\$\PatternManager	
LockUpdatePatternScheduling=D1	D0=Enable the option to schedule LiveUpdate from the Norton AntiVirus Corporate Edition user interface. D1=Disable the option to schedule LiveUpdate from the Norton AntiVirus Corporate Edition user interface.

Key Name and Sample Options Settings	Description
SetClientFromServer=D1	Client only. If set to one, this will allow the client to be configured from the server.
EnableProductUpdates=D0	D1=LiveUpdate will download product patches if available. D0=LiveUpdate will not download product patches.
LockUpdatePattern=D1	D0=Enable the option to run LiveUpdate manually from the Norton AntiVirus Corporate Edition user interface. D1=Disable the option to run LiveUpdate manually from the Norton AntiVirus Corporate Edition user interface.
UpdateClients=D1	D0=Do not request virus definitions from parent server. D1=Request virus definitions from parent server.
CheckConfigMinutes=D3	Client only. Number of minutes before the client checks in with the server (to maintain status information and display accurate information at the console).
!KEY!=\$REGROOT\$\ProductControl	
ManageThisComputer=D0	Tells transport system whether or not this computer can be managed. D0=Can't be managed (NT client). D1=Can be managed (NT server).
!KEY!=\$REGROOT\$\Quarantine	
ForwardingEnabled=D1	Used to enable or disable forwarding of infected items to the Quarantine Server. D0=Disable. D1=Enable.

Key Name and Sample Options Settings	Description
ForwardingServer=S[Server name]	Server name, Server IP address, or Server IPX address.
ForwardingPort=D3579	Server port number. (The port on which the Quarantine Server listens.)
ForwardingProtocol=D0	The protocol used to communicate with the Quarantine Server. D0=IP. D1=IPX.
ForwardingServerRetryTimer=D600	Number of seconds to wait between retries to the server when a server or communications error occurs.
ScanDeliverEnabled=D0	Used to enable or disable Scan and Deliver. D0=Disable. D1=Enable.
DefWatchMode=D2	D0=Silent mode. D1=Repair/leave in Quarantine. D2=Prompt. D3=Manual/notify Quarantine.
!KEY!=\$REGROOT\$\Storages	
!KEY!=\$REGROOT\$\Storages\FileSystem	
!KEY!=\$REGROOT\$\Storages\FileSystem\RealTimeScan	
HoldOnClose=D1	Controls whether or not to block a kernel closed until done scanning. D0=Don't block. D1=Block.
DriveList=S	Contains a list of drives that are protected with realtime scan. If the data is blank, all non-removable drives are protected.

Key Name and Sample Options Settings	Description
DoCompressed=D0	When files are flagged as OS compressed files (for example, NT compression), this controls whether the file is skipped or scanned. D0=Skip. D1=Scan.
SecondMacroAction=D1	Second action taken for macro viruses if first action fails. D1=Quarantine. D3=Delete. D4=Leave alone. D5=Clean.
ZipExts=.sarj, .lha, .zip, .mme, .lzh, .uue	Extensions that will be scanned as archived files. These files are decompressed and the files inside are scanned.
Writes=D1	The Scan Files Being Modified option. D0=Off. D1=On.
FirstAction=D5	D1=Quarantine. D3=Delete. D4=Leave Alone. D5=Clean.
CDRoms=D0	Controls whether or not files being accessed from CD-ROMs are scanned. D0=No. D1=Yes. (Only for Windows 3.x.)
HaveExceptionDirs=D0	This signals whether or not there are exception directories. (You can find exception directories under the subkey NoScanDir.) D0=No. D1=Yes.
Types=D6	Determines the types of files to scan if FileType is set to two. D1=Archived files. D2=Program files. D4=Document files. D6=Both document and program files.

Key Name and Sample Options Settings	Description
FirstMacroAction=D5	D1=Quarantine. D3=Delete. D4=Leave Alone. D5=Clean.
FileType=D0	Files being scanned. D0=All. D1=Selected extensions. D2=Selected types.
Reads=D1	Along with ExecsValue, represents the Scan Files When Accessed option. D0=Off. D1=On.
ClientDir=\$\$_CHOME\$\Alert	Path to the client directory that contains files that DOS and Win16 clients copy to when a virus is detected.
CheckRemovable=D1	Scan boot records of removable drives. D0=Disabled. D1=Enabled.
Floppys=D1	Controls whether or not files accessed on floppy disks are scanned. D0=No. D1=Yes. (Only for Windows 3.x.)
Trap=D0	Controls whether or not the Realtime Virus Behavior monitor is on. D0=Off. D1=On.
MessageBox=D0	Display message. D0=Disabled. D1=Enabled.
ZipFile=D0	Scan a file in compressed files. D0=Enabled. D1=Enabled.
OnOff=D1	Shows whether or not the realtime scan driver is working (hooked). D0=Unhooked. D1=Hooked.
Networks=D1	Controls whether or not files accessed on network drives are scanned. D0=No. D1=Yes.

Key Name and Sample Options Settings	Description
DenyAccess=D1	D0=Don't deny access. D1=Always deny access. D2=Deny access only if Clean fails. (If action is not Clean, access is denied.)
Logger=D2	Specifies the event type to be used in event logs. D0=Scheduled scan. D1=Manual scan. D2=Realtime scan. D6=Console. D7=VPDown. D8=System. D9=Startup. D100=Client. D101=Local end. D102=Forwarded.
ZipDepth=D3	D1=Only files in archive. D2=Fles and archives in archive. D9=Files are archives inside archive up to nine levels deep.
HardDisks=D1	Controls whether or not files accessed on hard drives are scanned. D0=No. D1=Yes.
Execs=D1	Controls whether or not files are scanned when executed. D0=No. D1=Yes.
Cache=D1	Turns cache on or off. Files in the cache are not scanned.
SecondAction=D1	D1=Quarantine. D3=Delete. D4=Leave Alone. D5=Clean. If first action fails.
Softmice=D1	Controls whether or not files are scanned for mutation viruses. This is always set to D1. D0=No. D1=Yes.

Key Name and Sample Options Settings	Description
Exts=.sdot, .doc, .html, .htt, .htm, .vbs, .js, .shs, .ppt, .mso, .pot, .rtf, .mdb, .jtd, .hlp, .inf, .ini, .hta, .mp?, .obj, .obt, .pps, .smm, .vsd, .vst, .xl?, .vss, .exe, .com, .bin, .sys, .dll, .ocx, .vxd, .bat, .btm, .csc, .pif, .386, .cla, .ov?, .drv, .scr, .acm, .acv, .adt, .ax, .cpl, .csh, .jse, .pl, .pm, .sh, .shb, .vbe, .wsf, .wsh	
HaveExceptionFiles=D0	This indicates whether or not there are exception files. Exception files are under the subkey FileExceptions. D0=No. D1=Yes.
AccessCounter=D3	The value increments from 0 up. If there is a failure to read this registry value, it could be set at -1. Tracks how many times a registry value is set through Transman.
ScanFloppyBRonAccess=D1	Scan floppy disks for boot record viruses. D0=Disabled. D1=Enabled.
BackupToQuarantine=D1	This option is used to turn on/off the creation of a backup copy stored in Quarantine before an infected file is repaired. D0=No. D1=Backup to Quarantine.
RemoveAlert=D0	Enable or disable the display of Alerts that are generated when monitoring virus-like activity. D0=Disabled. D1=Enabled.
RemoveAlertSeconds=D1	The alerts displayed when monitoring virus-like activities will be displayed for a duration specified by this value (0-99 seconds).

Enabling the Norton AntiVirus Corporate Edition icon in the Windows system tray

By default, the Norton AntiVirus Corporate Edition icon does not appear in the Windows system tray on the client computer.

To make the Norton AntiVirus Corporate Edition icon appear in the Windows System tray

- 1 From the Symantec System Center console, right-click the server group, then click **All Tasks > Norton AntiVirus > Client Administrator Only**.
- 2 Click **Show Norton AntiVirus Icon On Desktop**.

Deleting clients

You can delete clients from the Symantec System Center console. The client is deleted from the console and from the registry of its server.

Deleting clients from the console is useful if you have uninstalled Norton AntiVirus Corporate Edition from the clients. If the clients are uninstalled but not deleted from the console, they remain in the console until they are deleted from the registry of the former parent servers. This might not happen for several days. When you delete clients from the console, they are removed from the console view immediately.

By default, active clients check in with the parent server every 60 minutes. If the clients are still active when deleted, they reappear on the right pane of the console once they check back in with the parent server.

To delete a client

- 1 From the Symantec System Center console, click the server.
- 2 In the right panel, right-click the client and click **Delete**.

Changing the client expiration level

Servers are responsible for keeping an updated list of their clients. The Symantec System Center console only lists clients that it has received from querying parent servers. No discovery of clients nor any cached information is kept for clients on the console computer. If you remove a client from the Clients key on the parent server, the client no longer appears in the console under its parent server.

If a client is down (for example, because it was turned off for a week), when it is restarted, it checks in with its parent server. The client is then added to the server's Clients key, and appears in the console on the next update. The expiration interval must be greater than the client check-in interval (how often the client checks with the server) or the client key is deleted and added continually and the client does not appear in the console. By default, the client check-in interval is set to 60 minutes. The interval may be changed with the CheckConfigMinutes registry value.

You can add a registry key DWORD value that determines the number of hours before a parent server discards a deleted client. The new DWORD value determines the number of hours before the client is removed from the console.

To add the DWORD value

- 1 On the parent server, launch the Windows Registry Editor, then locate the following key:
HKEY_LOCAL_MACHINE\Software\Intel\LanDesk\VirusProtect6\CurrentVersion directory
- 2 On the Edit menu, click **New > DWORD Value**.
- 3 Name the value as follows:
ClientExpirationTimeout
- 4 Right-click the new key, then click **Modify**.
- 5 In the Value Data text box, replace the 0 with a number greater than 0.
Without the use of the ClientExpirationTimeout value, the default time is 60 minutes. Use a smaller value to decrease the time it takes for the client to be removed from the console, or use a larger value to increase the time. For example, if a large number of your client computers are being removed from the console because people are away from the office and their computers are turned off, you can specify a larger number.

- 6 Click **OK**, then exit the Registry Editor.

Once every hour, the parent server reviews its client registry entries. It checks the LastCheckinTime registry value to see if it is older than the configured ClientExpirationTimeout value. If it is, the server deletes that registry key. The next time that the console queries the server for a list of its clients, that client will not appear.

No restart is required.

Centralized client scanning control

You can preconfigure realtime scanning options on managed computers. All of the client installation methods, except installing directly from Disk 2, let you install the clients with preset parameters that can be locked. You can centrally configure scheduled scans for managed and sometimes managed clients. Users do not have the ability to prevent this scan from running unless the administrator checks the Show Stop Button On Progress Window box when configuring the scan. (To prevent Windows 3.x and DOS client logon scans from being cancelled, the Don't Allow User To Cancel Login Scan box must be checked.)

Default communications port

The default port number for client/server communications is 2967 for IP and 33345 for IPX. In the rare event that the port number is already in use, a random port is obtained for use during the communications session.



Keeping your protection current

This chapter includes the following topics:

- What are virus definitions file updates?
- Controlling virus definitions file rollouts
- Viewing the virus list for a server or client
- Verifying the dates of virus definitions files
- Which update method should I use?
- Using the Virus Definition Transport Method
- Using LiveUpdate
- Using LiveUpdate with an internal LiveUpdate server
- Rolling back a virus definitions file
- Updating with Intelligent Updater
- Updating servers and clients with Norton AntiVirus Corporate Edition product updates
- Updating products and virus definitions files with Package.exe
- Update examples

What are virus definitions file updates?

One way that Norton AntiVirus Corporate Edition finds viruses is by comparing segments of your files to the sample code inside of a virus definitions file. The virus definitions file contains nonmalicious bits of code, or virus definitions, for thousands of viruses. If Norton AntiVirus Corporate Edition finds a match, the file is infected.

To speed scanning, each computer that runs Norton AntiVirus Corporate Edition has a copy of the virus definitions file. However, the local copy on each computer can become outdated as new viruses are discovered. Virus definitions files are updated regularly (about once a week, or more frequently when needed). The updated file is available for download through a number of methods, such as over the Web.

Controlling virus definitions file rollouts

You can use a previous virus definitions file network-wide. For example, if a new virus definitions file is causing a false positive or other problem, you can select an earlier definition set from the Symantec System Center console. All servers and clients in that server group will roll back to the specified signature file. Because of the simplicity of undoing a new virus definitions file rollout, you can release new virus definitions files in less time.

When you roll out previous virus definitions files, the files that are newer than the date of the previous files are deleted.

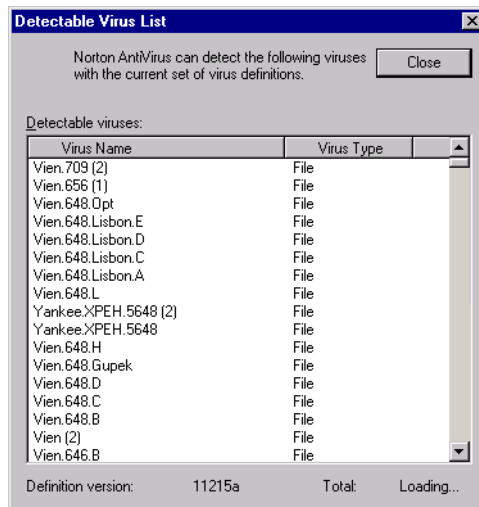
You can control the version of the virus definitions file used on all servers and clients in a server group. Users who have downloaded a virus definitions file that has not yet been approved for company use can be forced to use the virus definitions file that you specify.

Viewing the virus list for a server or client

You can view a list of viruses that are detectable on a selected server or client.

To view the remote virus list

- Right-click the server or client, then click **All Tasks > Norton AntiVirus > View Virus List**.



Details about viruses are available only when the virus list is opened on a computer. The remote virus list provides a means of ensuring that the selected computer is protected from a particular virus.

Verifying the dates of virus definitions files

When the Norton AntiVirus Corporate Edition view is selected on the Symantec System Center console, you can view the name of the virus definitions file on each protected computer. You can also see the current virus definitions file version for a server or server group.

To view the current virus definitions file version

- 1 On the Symantec System Center console, right-click the server group or server, then click **All Tasks > Norton AntiVirus > Virus Definition Manager**.

- 2 Click **Configure**.

The file name appears in the Current Version field. The higher the number, the more recent the file. The file naming convention is as follows:

YMMDDR

where:

Y = Number of years since 1998 (when this convention was established)

M = Month

D = Day

R = Revision (a sequential alpha value)

For example, 20419b means 04/19/2000 Revision 2.

Once virus definitions files are updated on a computer, it may take several minutes before the information is available from the console.

Warning icon appears when definitions are out-of-date

When the NAV Corporate Edition view is selected from the Symantec System Center console, a warning icon displays if a virus definitions file is out-of-date on one or more clients or servers within a server group. The icon looks like this:



If a client computer has an outdated virus definitions file, the warning icon also displays at the server and server group level. To find the computer or computers with the outdated definitions, expand the server group and servers as necessary and look for more warning icons.

Which update method should I use?

There are various methods available for downloading virus definitions and setting up servers and clients to retrieve them:

- Virus Definition Transport Method
- LiveUpdate
- Intelligent Updater

This section compares these technologies.

For more information, see [“The Virus Definition Transport Method versus LiveUpdate”](#) on page 403.

Virus Definition Transport Method

The main advantage of this method is that you can roll out virus definitions files to clients. This provides more control when you need to update definitions quickly. You can use this method to automate the process of distributing virus definitions updates to all servers and clients on your network.

The Virus Definition Transport Method employs a virus definitions file with a .vdb extension.

- For Norton AntiVirus Corporate Edition servers, the Virus Definition Transport Method passes a full package (*.vdb) from the primary server to all secondary servers in the server group. This file is extracted and the proper definitions placed in the appropriate directory on the server. The .vdb file is required by the server to pass on to its clients.
- For Norton AntiVirus Corporate Edition clients, the .vdb file is passed from the parent server. The file is extracted and the proper definitions placed in the appropriate directory. The .vdb file is discarded. It is not required for proper functionality.

For detailed information about setting up and using the Virus Definition Transport Method, see [“Using the Virus Definition Transport Method”](#) on page 259.

LiveUpdate

The main advantage of LiveUpdate is the small size of the microdefs file that is rolled out to clients. Norton AntiVirus Corporate Edition determines which virus definitions already reside on the client. Only the portion of the file that contains new data is retrieved by the computer.

Decide which of the following ways you want servers and clients to download virus definitions when using LiveUpdate:

- Connect directly to the LiveUpdate site.
- Connect to an internal LiveUpdate server.

About connecting to the Symantec LiveUpdate site

You can set up LiveUpdate on servers and clients to connect directly to the Symantec LiveUpdate site for updates.

- For Norton AntiVirus Corporate Edition servers, LiveUpdate downloads the full package rather than a microdefs file. The full package is necessary so that the .vdb file can be transmitted via the Virus Definition Transport Method to other parent servers and clients.
- For Norton AntiVirus Corporate Edition clients, LiveUpdate uses the microdefs file. The microdefs file updates the appropriate directory on the client with the required update. LiveUpdate will not create a .vdb file. A .vdb file is not necessary for the client to be updated.

About connecting to an internal LiveUpdate server

You can set up an internal LiveUpdate server to which virus definitions files are downloaded. You can then point your managed servers and clients to download from the LiveUpdate server. This type of setup is referred to as Central LiveUpdate.

You might create a Central LiveUpdate for the following reasons:

- To control the version of virus definitions files your servers and clients are using.
- To limit the number of connections made outside of your firewall.

The LiveUpdate Administration Utility, which is used to set up an internal LiveUpdate server, is ideally suited for sites with 1000 or more nodes. If you manage a smaller number of nodes, you might want to use the Virus Definition Transport Method.

When you use an internal LiveUpdate server:

- For Norton AntiVirus Corporate Edition servers, a package that includes a .vdb file is downloaded, then used for Virus Definition Transport Method distribution.
- For Norton AntiVirus Corporate Edition clients (Windows9x/Windows NT/Windows 2000), the appropriate LiveUpdate microdef packages are downloaded for clients.

For detailed information about using LiveUpdate, see [“Using LiveUpdate”](#) on page 273.

For more information about setting up a LiveUpdate server with LiveUpdate Administration Utility, see [“Using LiveUpdate with an internal LiveUpdate server”](#) on page 276.

Intelligent Updater

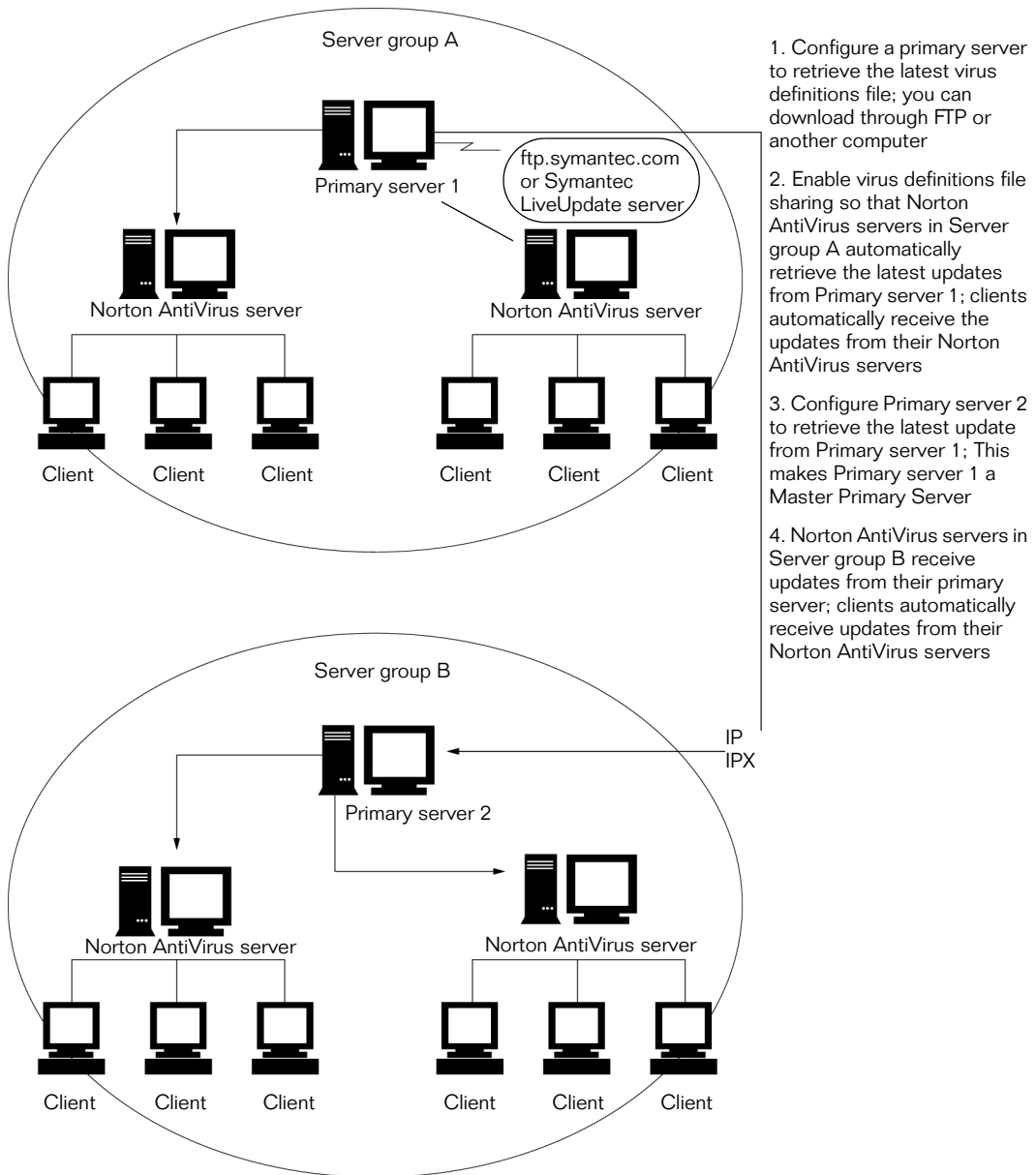
Intelligent Updater files are self-extracting executables. They are available for download from the Symantec Security Response Web site at <http://securityresponse.symantec.com>. This method is used by Symantec Security Response to deliver custom virus definitions files to you.

For more information, see [“Updating with Intelligent Updater”](#) on page 283.

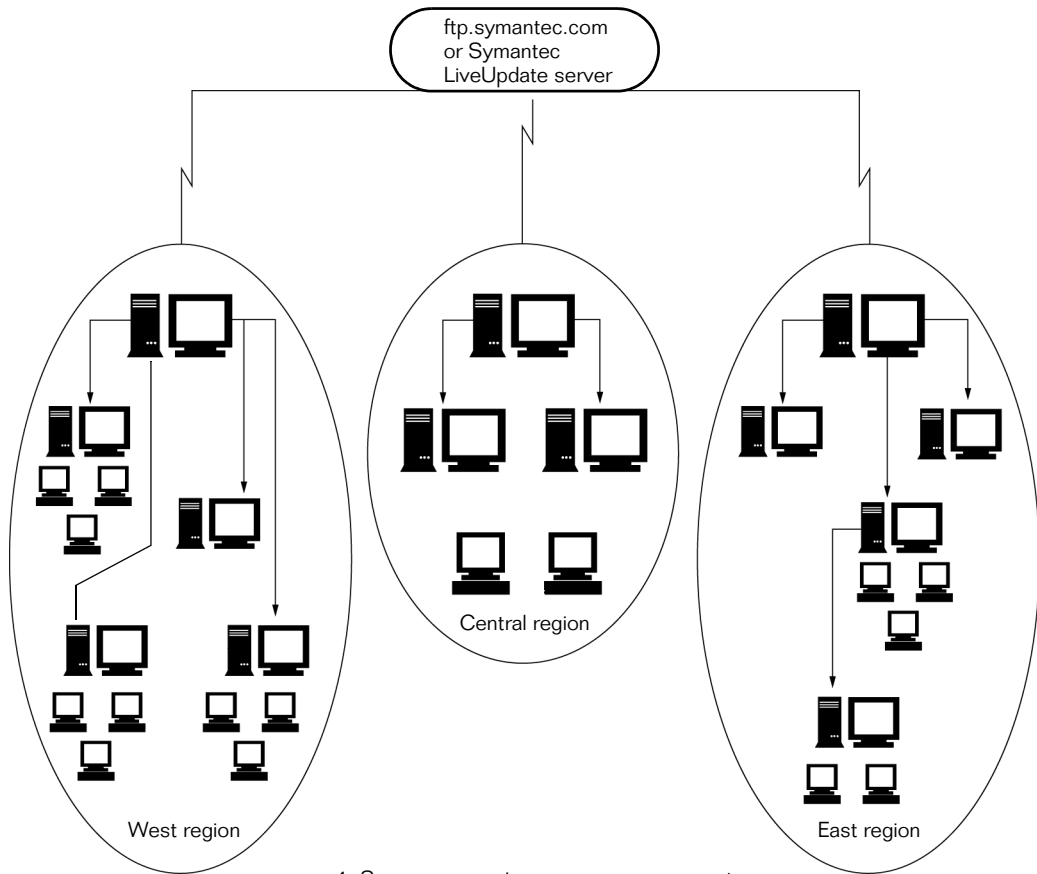
Using the Virus Definition Transport Method

You can use the Virus Definition Transport Method to automate the task of distributing a new virus definitions file to each computer on your network.

Configure only one computer on your network to retrieve the latest virus definitions file from the Symantec FTP site or Symantec LiveUpdate server. Then configure all other computers on the network to share this virus definitions file. For example, if you have a small network of six file servers divided into two server groups, the following diagram shows one way you could configure definitions file updates for your computer.



The diagram below illustrates how you might configure virus definitions file updates if your organization has multiple sites linked over a wide area network.



1. Server group primary servers on separate wide area networks retrieve the update from the Symantec FTP site or LiveUpdate server
2. Primary servers distribute the update to primary servers in other server groups in their local networks
3. The primary servers distribute the update to other protected servers and clients in their server group

Updating servers

To anticipate new viruses, you can configure automatic virus definitions file updates for servers. New virus definitions files are available when you run LiveUpdate and connect to the Symantec FTP site or LiveUpdate server.

The Virus Definition Transport Method employs a virus definitions file with a .vdb extension. When the .vdb file is posted on a primary server, it can flow to other primary servers, as well as to secondary servers and clients.

Testing updates and delivering them to the primary master server

Many administrators prefer to test virus definitions files on a test network before making them available on a production server.

To test virus definitions files, complete the following tasks:

- Install the Norton AntiVirus Corporate Edition server program to a primary server on the test network.
- From the primary server on your test network, run LiveUpdate to download the virus definitions file.
- Test the virus definitions file.

Once testing is complete, copy the virus definitions file from the test server to a primary server on your production network. The virus definitions file has a .vdb extension and downloads to \Program files\Nav on the test server. You copy this file to \Program files\Nav on the master primary server on the production network.

The master primary server is the primary server on the production network to which you copy tested virus definitions files and from which other primary servers retrieve virus definitions files.

Configure all other primary servers in the network to retrieve the virus definitions file from the master primary server to which you copied the virus definitions file.

Once the virus definitions files are on the primary servers, they will flow to other servers in the server group.

For information about downloading virus definitions files using LiveUpdate, see [“Downloading virus definitions files from the Symantec FTP site or LiveUpdate server using LiveUpdate”](#) on page 263.

If you don't test virus definitions updates

If you don't test virus definitions files, you can configure the master primary server to retrieve the latest virus definitions file from the Symantec FTP site or LiveUpdate server.

The master primary server is the primary server on the production network to which you download virus definitions files and from which other primary servers retrieve virus definitions files.

You can then configure all other primary servers to retrieve the virus definitions file from the master primary server.

Once the virus definitions files are on the primary servers, they will flow to other servers in the server group.

For information about downloading virus definitions files using LiveUpdate, see the next section.

Downloading virus definitions files from the Symantec FTP site or LiveUpdate server using LiveUpdate

You can download virus definition updates from the Symantec FTP site or from a LiveUpdate server.

To download a virus definitions file from the Symantec FTP site or LiveUpdate server

- 1 Right-click a server or server group, then click **All Tasks > Norton AntiVirus > Virus Definition Manager**.
- 2 Do one of the following:
 - To update all servers in the group automatically from the primary server, click **Update The Primary Server Of This Server Group Only**.
 - To update servers individually, click **Update Each Server In This Server Group Individually**.

The option that you select affects all servers in the server group, whether you right-clicked a server group or an individual server.

- 3 Click **Configure**.

- 4 Click **Update Now**.

A message appears with information about how you can view the date of the new virus definitions file.

- 5 Read the information that appears, then click **OK**.

To schedule the virus definitions file update

- 1 Right-click a server group or server, then click **All Tasks > Norton AntiVirus > Virus Definition Manager**.
- 2 Do one of the following:
 - To update all servers in the group automatically from the primary server, click **Update The Primary Server Of This Server Group Only**.
 - To update servers individually, click **Update Each Server In This Server Group Individually**.

The option that you select affects all servers in the server group, whether you right-clicked a server group or an individual server.

- 3 Click **Configure**.
- 4 Ensure that the Schedule For Automatic Updates box is checked, then click **Schedule**.
- 5 Select options to determine when the virus definitions file will update (for example, every Tuesday at 10:00 pm).
- 6 To configure how Norton AntiVirus Corporate Edition handles missed events or randomize the date or time when the definitions files are downloaded, click **Advanced** and set the corresponding options.

Configuring primary servers to retrieve from the master primary server

You can configure all primary servers to retrieve virus definitions files from a master primary server.

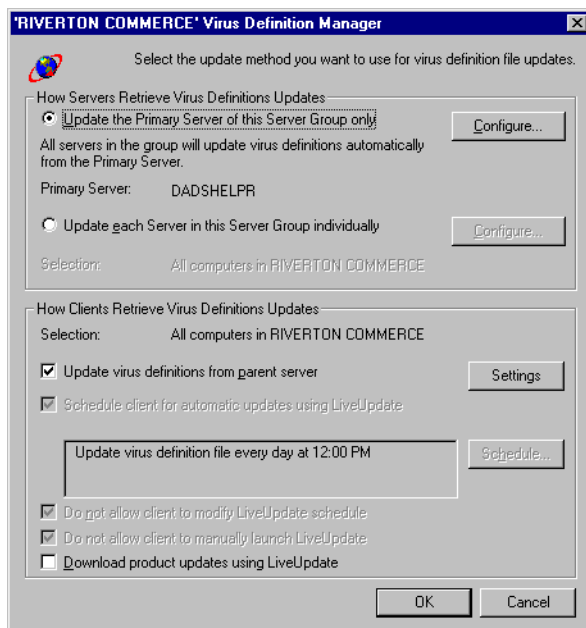
By default, virus definitions files then flow to other computers in your network.

Once the virus definitions files are retrieved by the primary server, they flow to secondary servers.

Clients are configured to automatically retrieve virus definitions from their parent servers if the Update Virus Definitions From Parent Server option in the Virus Definition Manager dialog box is enabled.

To configure primary servers to update from your master primary server

- 1 Right-click the server, then click **All Tasks > Norton AntiVirus > Virus Definition Manager**.



- 2 Click **Update the Primary Server of this Server Group only**.
- 3 Click **Configure**.
- 4 Click **Source**.
- 5 Click **Another Protected Server**, then click **Configure**, if necessary.
- 6 If you have used the Another Protected Server option before, you must click **Configure** to choose a different server.
- 7 Select the master primary server from the list of servers that appears.
- 8 Click **OK** twice.

- 9 Do one of the following:
 - Click **Update Now** to retrieve the virus definitions files from the master primary server immediately.
 - Check **Schedule For Automatic Updates**, then click **Schedule** and set a frequency and time when the server will check for updates on the master primary server.
- 10 Click **OK** until the Virus Definition Manager dialog box closes.

Repeat this procedure for each primary server that will retrieve virus definitions files from the master primary server.

To configure clients to retrieve virus definitions files from their parent server

- 1 In the Symantec System Center console, right-click the server group, then click **All Tasks > Norton AntiVirus > Virus Definition Manager**.
- 2 Check **Update Virus Definitions From Parent Server**.
- 3 Click **OK**.

Updating servers individually

You can choose to update virus definitions files on servers individually. You might want to do this, for example, if you experience a network problem with your designated primary server. Servers can be configured to do one of the following:

- Run LiveUpdate and download virus definitions files directly from the Symantec FTP site, Symantec LiveUpdate server, or an internal LiveUpdate server.
- Retrieve virus definitions files from another protected server.

To configure a server to download using LiveUpdate

- 1 In the Symantec System Center console, right-click the server group, then click **All Tasks > Norton AntiVirus > Virus Definition Manager**.
- 2 Click **Update Each Server In This Server Group Individually**.
- 3 Click **Configure**.
- 4 Click **Source**.

- 5 Click **LiveUpdate (Win32)/FTP (NetWare)**, then click **OK**.

Note: Make sure that your NetWare server is running FTP.

- 6 Do one of the following:
 - Click **Update Now** to launch a LiveUpdate session immediately.
 - Click **Schedule For Automatic Updates**, then click **Schedule** and set a frequency and time when the server will run a LiveUpdate session.
- 7 Click **OK** until the Virus Definition Manager dialog box closes.

To configure a server to download from another protected server

- 1 Right-click the server, then click **All Tasks > Norton AntiVirus > Virus Definition Manager**.
- 2 Click **Update Each Server In This Server Group Individually**.
- 3 Click **Configure**.
- 4 Click **Source**.
- 5 Click **Another Protected Server**.
- 6 Select the server from which to retrieve virus definitions files from the list of servers that appears, then click **OK**.
- 7 Do one of the following:
 - Click **Update Now** to retrieve the virus definitions files from the other protected server immediately.
 - Check **Schedule For Automatic Updates**, then click **Schedule** and set a frequency and time when the server will retrieve the virus definitions files from the other protected server.
- 8 Click **OK** until the Virus Definition Manager dialog box closes.

Setting advanced scheduled LiveUpdate options

When setting options for scheduled LiveUpdate sessions for servers and clients, you can specify advanced settings.

- Randomize LiveUpdate schedules for multiple computers to minimize the impact on network traffic.
- Determine how missed LiveUpdate events will be handled.

Randomizing scheduled LiveUpdate sessions

You can set options so that servers or clients that are configured to run LiveUpdate at the same scheduled time will run LiveUpdate within a specified time range rather than at a set time. This can result in better managed network traffic.

You can randomize on the following:

- Plus or minus a specified number of minutes of the scheduled time. For example, 45 minutes plus or minus the scheduled time of 3:00 P.M.
- Any day of the week within a specified interval of days. For example, any day between Tuesday and Friday.
- Any day of the month plus or minus a specified number of days of the scheduled date. For example, 10 days before or after the scheduled date of January 3rd.

To randomize the LiveUpdate schedule for servers

- 1 Right-click the server or server group, then click **All Tasks > Norton AntiVirus > Virus Definition Manager**.
- 2 Click **Configure**.
- 3 Check **Schedule For Automatic Updates**.
- 4 Click **Schedule**.
- 5 Set the frequency and time when the server will check for updates.
- 6 Click **Advanced**.
- 7 Under Randomization Options, check **Options**, then set the minutes, day of the week, or day of the month options.
- 8 Click **OK** until you return to the Symantec System Center main window.

To randomize the LiveUpdate schedule for clients

- 1 Right-click the server or server group, then click **All Tasks > Norton AntiVirus > Virus Definition Manager**.
- 2 Check **Schedule Client For Automatic Virus Definition Updates Using LiveUpdate**.
- 3 Click **Schedule**.
- 4 Set the frequency and time when the clients will check for updates.
- 5 Click **Advanced**.

- 6 Under Randomization Options, check **Options**, then set the minutes, day of the week, or day of the month options.
- 7 Click **OK** until you return to the Symantec System Center main window.

Configuring for missed LiveUpdate events

You can set options so that scheduled LiveUpdate events that were missed run at a later time. For example, an event might be missed if a computer is turned off when the LiveUpdate session is scheduled to run. You can set the session to run if the computer is restarted within a specified time parameter.

To configure for missed LiveUpdate events for servers

- 1 Right-click the server group or server, then click **All Tasks > Norton AntiVirus > Virus Definition Manager**.
- 2 Click **Configure**.
- 3 Click **Schedule for Automatic Updates**.
- 4 Click **Schedule**.
- 5 Click **Advanced**.
- 6 Check **Handled Missed Events Within**.
- 7 Set the time limit within which you want the scan to run.
For example, you might want a weekly LiveUpdate to run only if it is within three days after the scheduled time for the missed event.
- 8 Click **OK** until you return to the Symantec System Center main window.

To configure for missed LiveUpdate events for clients

- 1 Right-click the server group or server, then click **All Tasks > Norton AntiVirus > Virus Definition Manager**.
- 2 Click **Schedule Client For Automatic Virus Definition Updates Using LiveUpdate**.
- 3 Click **Schedule**.
- 4 Click **Advanced**.
- 5 Click **Handled Missed Events Within**.

- 6 Set the time limit within which you want the scan to run.
For example, you may want a weekly LiveUpdate to run only if it is within three days after the scheduled time for the missed event.
- 7 Click **OK** until you return to the Symantec System Center main window.

Updating NetWare servers

For a NetWare environment, you can choose among several update methods:

- If you have an exclusive NetWare environment with a single Windows NT computer on which you run the Symantec System Center console, you can designate a NetWare server as the primary server. The NetWare server must have the TCP/IP protocol running and must be able to connect to the Internet.
- If you have a mixed NetWare and Windows NT environment, install the Norton AntiVirus Corporate Edition server program to a Windows NT computer and designate it as your primary server. You can then set up the NetWare servers to pull the virus definitions updates from the primary server.
- Schedule a batch file to download the definitions for Norton AntiVirus Corporate Edition and copy them to the correct location on your primary server.

To use the scheduled batch file download method, the managed client that you use to connect to the Symantec FTP site must have TCP/IP support.

You can use any scheduler program that can run an external batch file.

To use the batch file method

- 1 Use a text editor such as Notepad to create the following script:

```
open ftp.symantec.com
anonymous
test@net.com
cd public/english_us_canada/antivirus_definitions/norton_antivirus/
static
lcd c:\temp
bin
hash
prompt
get Sarcx86.exe
quit
```

- 2 Save the file as Cescrypt.txt.

- 3 Use a text editor to create the following batch file:

```
ftp -s:cescrypt.txt
c:\temp\sarcx86.exe /q /dump /vdb c:\temp
copy c:\temp\*.vdb <path>
del /q c:\temp\*.vdb
del /q c:\temp\sarcx86.exe
```

- 4 Save the file as Cegetter.bat.

For Cegetter.bat to work correctly, you must modify it so that it copies the definitions to the Norton AntiVirus directory on the primary server.

- 5 Right-click **Cegetter.bat**, then click **Edit**.

- 6 Find the following line in the Cegetter.bat file:

```
copy c:\temp\*.vdb <path>
```

Change <path> to the location of the Norton AntiVirus directory on the primary server.

<path> can be either a directory on the local computer or a UNC path to another server. You must use short file names. For example: copy c:\temp*.vdb c:\progra~1\nav or copy c:\temp*.vdb \\servername\vphome.

- 7 If you are running Windows 9x, remove the /q from the following lines:

```
del /q c:\temp\*.vdb  
del /q c:\temp\sarcx86.exe
```
- 8 Test Cegetter.bat by running the batch file from a DOS prompt.
You will see a DOS window showing the progress of the download.
- 9 Schedule Cegetter.bat to run once a week to get regular virus definitions updates.

NetWare servers not running TCP/IP cannot get updates from a Windows NT server in another server group

If your NetWare server is not running TCP/IP and is not using a domain naming system (DNS) server, you might have difficulty updating a NetWare server from a Windows NT server that resides in a different server group. This is because the NetWare server does not store the address of the Windows NT server in its address cache.

If you do not run TCP/IP on your NetWare server and still want to update it from a Windows NT server in another server group, you can work around this problem. Temporarily move the NetWare server into a server group that has a Windows NT server running the IPX protocol. After one day, you can move the NetWare server back to its original server group. This adds the Windows NT server address to the NetWare server's address cache, letting the NetWare server locate the Windows NT server to obtain the updated virus definitions file.

Using LiveUpdate

When you use LiveUpdate, you can choose how clients and servers get new virus definitions file and product updates:

- Allow your managed servers and clients to connect to the Symantec FTP site or Symantec LiveUpdate server to download.

For information about implementing this method, see [“Configuring servers to retrieve from the Symantec FTP site or LiveUpdate server”](#) on page 273 and [“Configuring clients to retrieve from the Symantec FTP site or LiveUpdate server”](#) on page 274.

- Set up a LiveUpdate server, download updates to that server, and have your managed servers and clients retrieve updates from this internal LiveUpdate server.

For information about implementing this method, see [“Using LiveUpdate with an internal LiveUpdate server”](#) on page 276.

Configuring servers to retrieve from the Symantec FTP site or LiveUpdate server

You can configure servers to retrieve virus definitions file updates from the Symantec FTP site or from a LiveUpdate server.

To configure servers to connect to the Symantec FTP site or LiveUpdate server

- 1 In the Symantec System Center console, right-click the server group, then click **All Tasks > Norton AntiVirus > Virus Definition Manager**.
- 2 Click **Update The Primary Server Of This Server Group Only**.
- 3 Click **Configure**.
- 4 Verify that LiveUpdate appears in the Update Source Field. Click **Source**, then click **LiveUpdate**, if it does not.

Note: The server must have a valid Internet connection to connect to the Symantec FTP site.

Configuring clients to retrieve from the Symantec FTP site or LiveUpdate server

Clients can be configured to connect to the Symantec FTP site or LiveUpdate server.

To configure clients to connect to the Symantec FTP site or LiveUpdate server

- 1 In the Symantec System Center console, right-click the server group, then click **All Tasks > Norton AntiVirus > Virus Definition Manager**.
- 2 Verify that the following check boxes are unchecked:
 - Update Virus Definitions From Parent Server
 - Do Not Allow Client To Manually Launch LiveUpdate

Note: The client must have a valid Internet connection or modem to connect to the Symantec FTP site.

Scheduling LiveUpdate for clients

You can schedule clients to run LiveUpdate. You can also schedule client LiveUpdate sessions to run after hours.

To schedule LiveUpdate for clients

- 1 In the Symantec System Center console, right-click the server group, then click **All Tasks > Norton AntiVirus > Virus Definition Manager**.
- 2 Click **Schedule Client For Automatic Updates Using LiveUpdate**.
- 3 Click **Schedule**.
- 4 Select the frequency, day, and time that you want the update to occur.

Note: If LiveUpdate is configured to connect to a UNC share on an internal server, the system account must have full rights to network resources. If LiveUpdate is configured to download updates from a UNC share, then LiveUpdate will fail. The system account has no network credentials and must connect to other resources using a null session. For more information, see [“LiveUpdate does not run”](#) on page 421.

Setting LiveUpdate usage policies

You can set LiveUpdate usage policies for your managed clients. The policies determine if the following activities can be performed at the client level:

- LiveUpdate schedule can be changed
- LiveUpdate can be manually launched

To set LiveUpdate policies for clients

- 1 In the Symantec System Center console, right-click the server group, then click **All Tasks > Norton AntiVirus > Virus Definition Manager**.
- 2 Click **Download Product Updates Using LiveUpdate**.
- 3 To prevent the LiveUpdate schedule from being modified on the client, click **Do Not Allow Client To Modify LiveUpdate Schedule**. (**Schedule Client For Automatic Updates Using LiveUpdate** must be checked or this box is dimmed.)
- 4 To prevent LiveUpdate from being manually launched on the client, click **Do Not Allow Client To Manually Launch LiveUpdate**.

When these options are checked, they appear dimmed on the client.

Note: When the Do Not Allow Client To Modify LiveUpdate Schedule check box or Do Not Allow Client To Manually Launch LiveUpdate check box is not checked, LiveUpdate can run on the client at any time.

Using LiveUpdate with an internal LiveUpdate server

If you manage 1000 or more nodes, use the LiveUpdate Administration Utility to update virus definitions files and the Norton AntiVirus Corporate Edition program.

To set up a LiveUpdate Server with the LiveUpdate Administration Utility and to set up servers to retrieve updates from the LiveUpdate Server, you complete the following tasks:

- Install LiveUpdate Administration Utility on a computer. Install on a Windows NT computer running the Norton AntiVirus Corporate Edition server program. This lets you configure LiveUpdate Administration Utility scheduling from the Symantec System Center console to download updates from Symantec.

For the LiveUpdate Administration Utility installation procedure, see the *Symantec System Center Implementation Guide*.

- Configure LiveUpdate Administration Utility, specifying the packages to download, and the directory to which the packages will download.

If you have workstations connected to a UNC network location, the user logged on to the network must have access rights to the network resource. The user name and password supplied in the host file are ignored. One option available with a Windows NT server is to create a shared resource that all users are authorized to access (a NULL share). For information about creating a NULL share, refer to your Microsoft Windows NT server documentation.

- Make sure that your FTP server, Web server, or UNC share is configured to share files from the download directory that you specified.
- On the Symantec System Center console, do the following:
 - Configure LiveUpdate for the internal LiveUpdate server.
 - Configure other servers and clients to download from the internal LiveUpdate server.
 - Schedule the intervals when you want LiveUpdate sessions to run.

Many administrators prefer to test virus definitions files on a test network before making them available on a production server. If you test your virus definitions files, test them on your test network. Once testing is complete, run LiveUpdate from your production network.

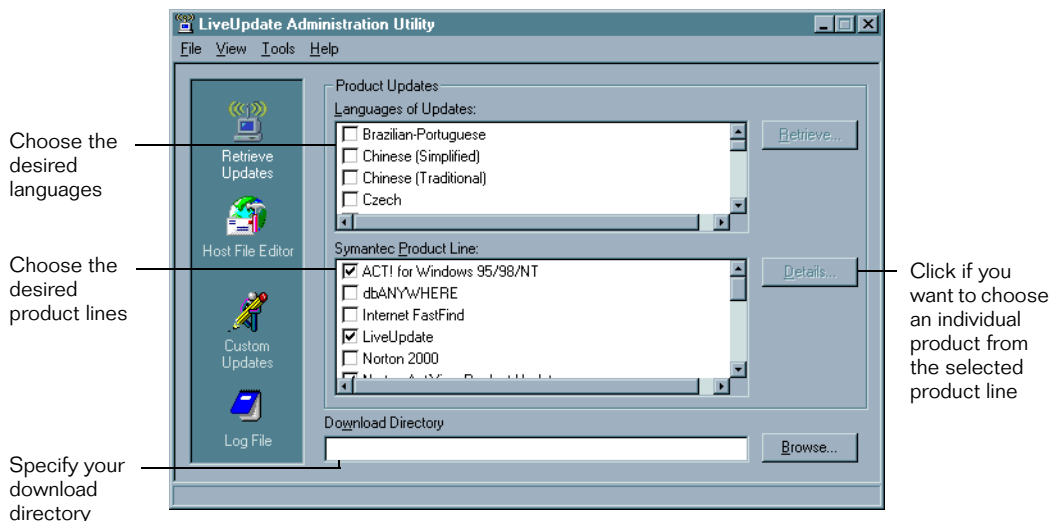
To install the LiveUpdate Administration Utility

- 1 Insert the Symantec System Center CD 1 into your CD-Rom drive.
- 2 Click **Install LiveUpdate Administration Utility**.
- 3 Follow the on-screen instructions.

To configure the LiveUpdate Administration Utility

- 1 On the Windows taskbar, click **Start > Programs > LiveUpdate Administration Utility > LiveUpdate Administration Utility**.
- 2 Click **Retrieve Updates**.
- 3 Specify the Download Directory on your LiveUpdate server.

This is the location where the update packages and support files will be stored once they are downloaded from Symantec. (Files first download to a temporary directory that is created by the LiveUpdate Administration Utility. Once the file is downloaded fully, it is moved to the specified Download Directory.) The Download Directory can be any directory on your server.



- 4 Select the languages for download packages.
- 5 Check the Symantec product lines that will be supported.

Because all installed Symantec products that use LiveUpdate now point to your Intranet server, it is safer to download full product lines rather than individual products.

If you want to select individual product components from a particular Symantec product line, check the Product Line box, click **Details** button, then check both the Languages and Products to download.

When you select individual product components to update, you risk missing other available updates. For example, new virus definitions files for Norton AntiVirus Corporate Edition might require an engine update that is also available for download.

In addition to the downloaded packages, LUADMIN retrieves index files called Symtri.zip, Livetri.zip, and Symtri16.zip, as well as products.xml. These files are required by different versions of LiveUpdate.

To retrieve update packages

- 1 On the Windows taskbar, click **Start > Programs > LiveUpdate Administration Utility > LiveUpdate Administration Utility**.

- 2 Click **Retrieve Updates**.

- 3 Click **Retrieve** to begin the administrator LiveUpdate.

- 4 Follow the instructions in each panel to retrieve the packages.

If the LiveUpdate Administration Utility does not successfully download all of the packages that you originally selected, none of the packages will appear in your specified download directory.

- 5 Check the log file for details about the download activity.

To view the log file, in the LiveUpdate Administration Utility main window, click **Log File**.

- 6 If you did not specify a directory on your FTP server as your download directory, copy the contents of the download directory to the directory you specified in the LiveUpdate properties page for the URL Or IP Address textbox.

You must configure LiveUpdate to update from the internal LiveUpdate server. Once configured, the next time users click LiveUpdate from their workstations, they will receive the packages from your internal server, not Symantec's external server.

Unlock the server group, if necessary.

To unlock the server group

- On the Symantec System Center console, right-click the server group, then click **Unlock Server Group**.

To configure LiveUpdate to update from the internal LiveUpdate server

- 1 Right-click the server group, then click **Properties**.
- 2 On the LiveUpdate tab, click **Internal LiveUpdate Server**.

The screenshot shows the 'Riverton Commerce Properties' dialog box with the 'LiveUpdate' tab selected. The 'General' tab is also visible. The 'LiveUpdate' section contains the following fields and options:

- Select the LiveUpdate source for this machine.**
 - ☒ **Symantec LiveUpdate Server**
LiveUpdate will obtain updates from the Symantec server.
 - ☐ **Internal LiveUpdate Server**
 - Description:**
 - Name:** [Text box]
 - Location:** [Text box]
 - Login:**
 - Name:** [Text box]
 - Password:** [Text box]
 - Connection:**
 - URL or IP Address:** [Text box]
 - Type:** [Dropdown menu showing 'FTP']
- ☒ **Apply settings to all clients.**

At the bottom of the dialog are buttons for **OK**, **Cancel**, and **Apply**.

3 Complete the following fields:

Name	Type the name of the server. This name will appear when you run LiveUpdate.
Location	This text box is optional. You can enter descriptive information related to the server. For example, the name of the site.
Login Name	The login name associated with the server. Leave this field blank so that users can log on and retrieve the files without entering information.
Login Password	The login password associated with the server. Leave this field blank so that users can log on and retrieve the files without entering information.
URL or IP Address	<p>If you are using the FTP method (recommended), select FTP in Type and enter the FTP address for the server. For example: ftp.myliveupdateserver.com.</p> <p>If you are using the HTTP method, select HTTP in Type and enter the Universal Resource Locator for the server. Examples: http:\\myliveupdateserver.com</p> <p>or</p> <p>155.66.133.11\\Export\\Home\\Ludepot</p> <p>If you are using the LAN method, select LAN in Type and enter the server UNC path name. For example: \\Myserver\\LUDepot</p> <p>In the Login field, enter the name and password to access the server.</p>

4 Click **OK**.

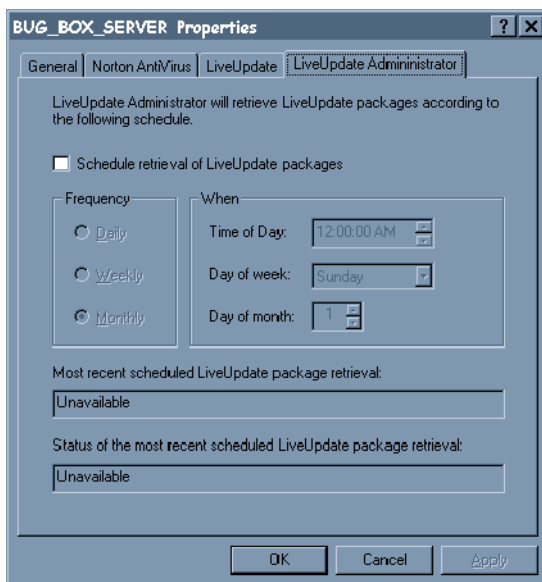
When you leave the Login Name and Login Password text boxes empty, an anonymous logon will be used. This requires that anonymous logons be enabled on the FTP server. If your policy prohibits anonymous logons on FTP servers, enter the logon and password for the FTP server and directory that will be accessed.

To configure LiveUpdate to update from the Symantec LiveUpdate server

- 1 In the Symantec System Center console, right-click the server group, then click **Properties**.
- 2 On the LiveUpdate tab, click **Symantec LiveUpdate server**.
When LiveUpdate is run from the server, it retrieves virus definitions from the Symantec LiveUpdate server.

To schedule LiveUpdate sessions

- 1 In the Symantec System Center console, right-click a server on which both the Norton AntiVirus Corporate Edition server program and LiveUpdate Administration Utility are installed, then click **Properties**.
- 2 On the LiveUpdate Administrator tab, click **Schedule retrieval of LiveUpdate packages**.



The LiveUpdate Administrator tab is available only if you have installed both the LiveUpdate Administrator Utility and the Norton AntiVirus Corporate Edition server program to the server.

- 3 Select the frequency with which you want LiveUpdate to run.
- 4 Specify the Time Of Day, Day Of Week, and Day Of Month when LiveUpdate will run.

Note: From the LiveUpdate Administrator property page, you can determine the LiveUpdate package most recently retrieved. You can also determine the status of this package.

Rolling back a virus definitions file

You can roll back a virus definitions file to a server group if necessary. For example, you might do this if the most recent file generated false positive virus detections.

To roll back virus definitions files

- 1 Click the server group or server.
- 2 Click **All Tasks > Norton AntiVirus > Virus Definition Manager**.
- 3 Ensure that **Update The Primary Server Of This Server Group Only** is checked, then click **Configure**.
- 4 Click **Definition File**.
- 5 Select the virus definitions file you want to use, then click **Apply**.
- 6 Click **Yes** to change the current file.
- 7 Click **Close > OK > OK**.

The previous virus definitions file loads immediately.

Note: When you roll back virus definitions files, virus definitions that are newer than those included in the rolled back version are deleted.

Updating with Intelligent Updater

Intelligent Updater is a self-extracting executable file that contains virus definitions files. Intelligent Updater can be downloaded from the Symantec Security Response Web site (<http://securityresponse.symantec.com>).

To distribute updated virus definitions, download a new Intelligent Updater, then use your preferred distribution mechanism to deliver the updates to your managed servers and clients.

You might also want unmanaged clients to use Intelligent Updater as their virus definitions update mechanism.

Updating servers and clients with Norton AntiVirus Corporate Edition product updates

The Virus Definitions Transport Method updates virus definitions files only. Use the Virus Definitions Transport Method for virus definitions file updating, then use LiveUpdate to update Norton AntiVirus Corporate Edition on your managed servers and clients.

To update managed servers and clients

- 1** Install LiveUpdate Administration Utility on a computer.
Install to the same computer to which you installed the Norton AntiVirus Corporate Edition server program. This lets you configure LiveUpdate Administration Utility scheduling from the Symantec System Center console.
- 2** Configure LiveUpdate Administration Utility, specifying the packages to download, and the directory to which the packages will be downloaded.
- 3** Make sure that your FTP server is configured to share files from the download directory that you specified.
- 4** On the Symantec System Center console:
 - Configure LiveUpdate for the internal LiveUpdate server.
 - Configure other servers and clients to download from the internal LiveUpdate server.
 - Schedule the intervals when you want LiveUpdate sessions to run.

- 5 On the Symantec System Center console, right-click the server group or server in the console tree, or a client in the right pane, then click **All Tasks > Norton AntiVirus > Virus Definition Manager**.
- 6 Click **Download Product Updates Using LiveUpdate**.
- 7 Click **OK**.

To complete the tasks required to update Norton AntiVirus Corporate Edition with LiveUpdate

- 1 Complete all of the procedures under [“Using LiveUpdate with an internal LiveUpdate server”](#) on page 276.
- 2 On the Symantec System Center console, right-click the server group, then click **All Tasks > Norton AntiVirus > Virus Definition Manager**.
- 3 Uncheck **Do Not Allow Client To Manually Launch LiveUpdate**.
- 4 Uncheck **Do Not Allow Client To Modify LiveUpdate Schedule**.
- 5 Check **Download Product Updates Using LiveUpdate**.
- 6 Check **Schedule Client For Automatic Updates Using LiveUpdate**.
- 7 Click **Schedule**.
- 8 Select the frequency and date/time when LiveUpdate will run.
- 9 Click **OK**.

Updating products and virus definitions files with Package.exe

Use Package.exe to create a file for distribution that includes both Symantec product updates and new virus definitions files.

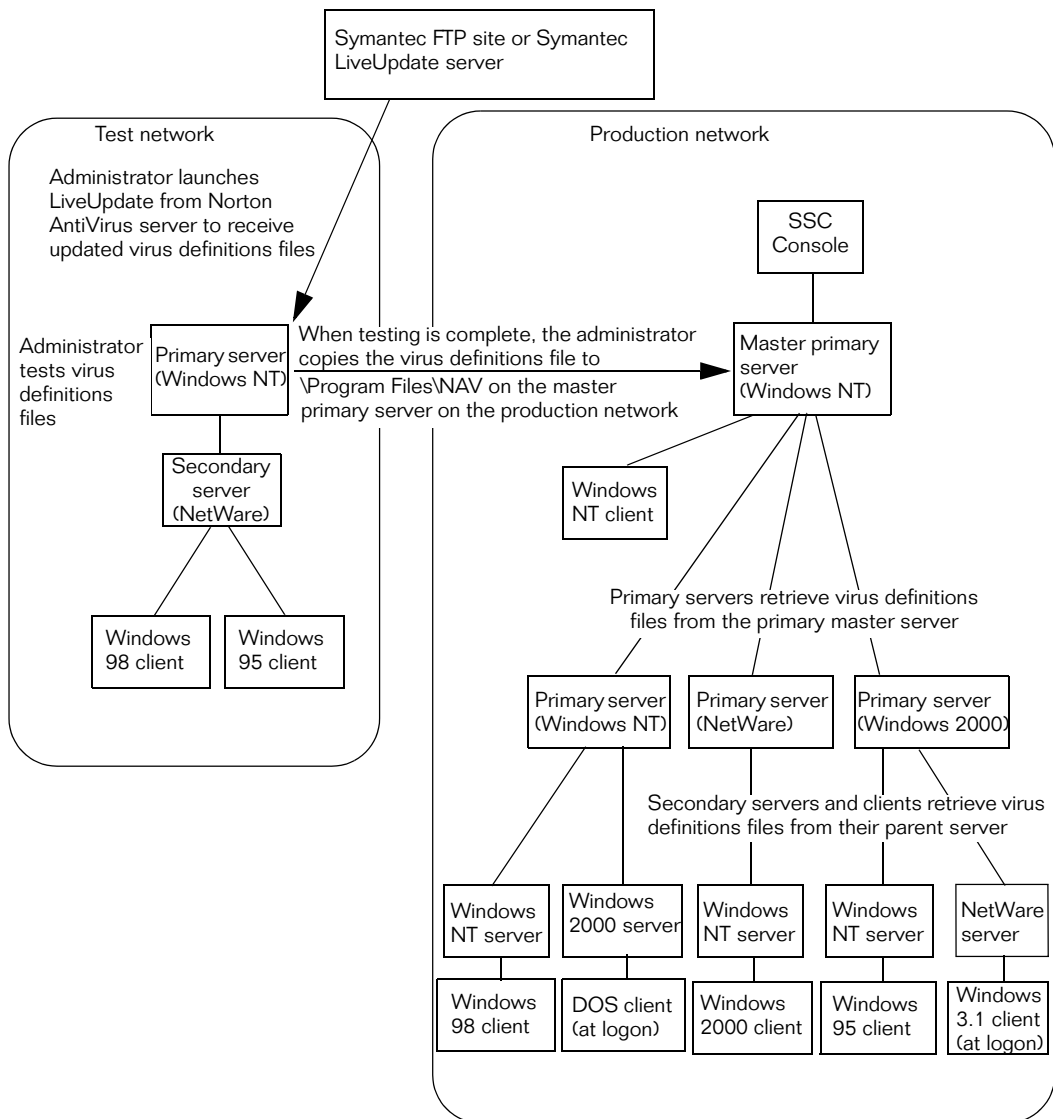
For more information, see [“Using Package.exe”](#) on page 175.

Update examples

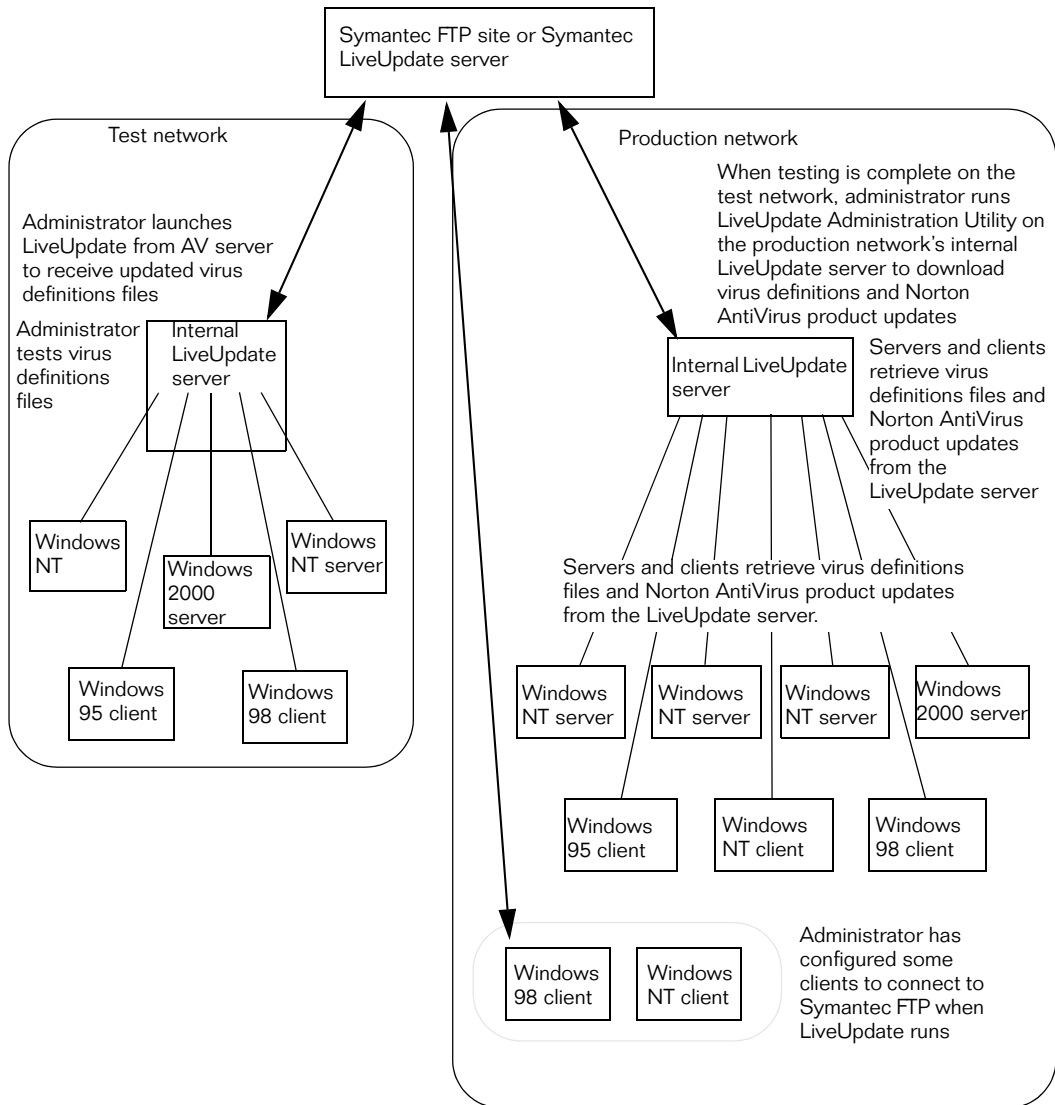
The following illustrations show how administrators at two different companies perform updates.

At Company A, the administrator downloads the new virus definitions file from the Symantec FTP site or Symantec LiveUpdate server to a primary server on the test network. He tests the virus definitions file. When testing is completed, he copies the virus definitions file to the master primary server on his production network. He has configured other primary servers so that they retrieve the update from the master primary server. All other connected computers use the Virus Definition Transport Method. Secondary servers retrieve the update from their primary server. Clients retrieve the update from their parent server. (Windows 3.1 and DOS clients receive the updates when they next log on to the computer.)

At Company B, the administrator downloads the new virus definitions file from the Symantec FTP site or Symantec LiveUpdate server to her test network. She tests the virus definitions file. When testing is completed, she downloads the new virus definitions file from the Symantec FTP site or Symantec LiveUpdate server to the internal LiveUpdate server on her production network. Some low risk users are allowed to go outside the firewall. When LiveUpdate runs on their computers, virus definitions files are downloaded directly from the Symantec FTP site or Symantec LiveUpdate server. All other protected servers and clients are configured and scheduled to retrieve virus definitions file updates from the LiveUpdate server.



Company A updates with Virus Definition Transport Method



Company B updates with LiveUpdate and LiveUpdate Administration Utility

Scanning for viruses

This chapter includes the following:

- Configuring manual, scheduled, and realtime scan options
- Configuring manual scans
- Scanning in realtime
- Configuring realtime protection for files
- Configuring realtime protection for mail applications
- Configuring scheduled scans
- Using logon scanning options
- Configuring logon scans for clients

What kinds of scans are available

From the Symantec System Center console, you can set up the following scans for servers and clients:

- **Virus sweeps:** Inspect all drives on all servers and clients belonging to the selected object. Virus sweeps provide immediate results from a scan on large areas of the network.
- **Manual or on-demand scans:** Inspect selected folders and drives on selected computers. Manual scans provide immediate results from a scan on a small area of the network, or a local hard drive.
- **Scheduled scans:** Inspect selected folders and drives on selected computers at a predetermined time. Scheduled scans are ideal for large areas of the network because you can run the scans during off hours when network traffic is low.
- **Realtime scans:** Inspect files as they are read from or written to a server or client computer. You can also configure native email scanning for 32-bit client computers.

You can set up manual, scheduled, and realtime scans on the Norton AntiVirus Corporate Edition client. On the client interface you can select individual files to scan. For security reasons, you can select individual files to scan only from the Norton AntiVirus Corporate Edition client interface. On the Symantec System Center console, you can select folders and drives to scan.

The Norton AntiVirus Corporate Edition client interface includes two additional types of scans:

- Custom scans: Save a scan that can be run manually at a later time.
- Startup scans: Save a scan to run automatically when the computer starts. (If you create more than one startup scan, they run sequentially in the order created.)

This chapter only covers setting up scans from the Symantec System Center console. For information on using the client interface, see the *Norton AntiVirus Corporate Edition User's Guide*.

Virus sweeps

From the Symantec System Center console, you can launch an immediate scan of both servers and clients with a single button. You can perform a virus sweep by selecting the System Hierarchy, one or more server groups, or one or more servers in the Symantec System Center console tree.

After starting a virus sweep on the System Hierarchy, you'll know within minutes that your entire network is virus-free. You do not have to send messages that ask users to scan their computers to ensure that the network is clean. The virus sweep ensures that there are no viruses on servers or workstations.

For more information, see [“Running a virus sweep”](#) on page 384.

Note: You cannot interrupt or stop a virus sweep after it has started. You must let it finish.

Manual scans

From the Symantec System Center console, you can launch an immediate scan of one or more Norton AntiVirus Corporate Edition servers in the same server group, or one or more Norton AntiVirus Corporate Edition clients managed by the same Norton AntiVirus Corporate Edition server.

A manual scan quickly gives you the status of a targeted area of your network. Unlike the virus sweep, which scans all files on all drives, you can configure a manual scan to narrow the scope of your scans.

Scheduled scans

From the Symantec System Center console, you can set up a scan to run at a specific time of day using daily, weekly, or monthly intervals. Scheduled scans must be created separately for servers and clients:

- Schedule server scans by selecting server groups or a server in the Symantec System Center console tree.
- Schedule client scans by selecting a server or a client in the Symantec System Center Console tree.

Time your scheduled scans to closely follow your schedule for updating virus definitions files so that any newly introduced viruses are handled efficiently.

Realtime scans

From the Symantec System Center console, you can set up file system realtime protection on both Norton AntiVirus Corporate Edition servers and Norton AntiVirus Corporate Edition clients. You can set up mail data realtime protection for supported mail applications installed on the Norton AntiVirus Corporate Edition client. You configure server and client realtime protection separately.

After you configure realtime protection, you only need to change it if your network environment or security policy changes.

About console tree objects and scanning

The objects that you select in the console tree (and in the right pane for multiple selected objects) determine the types of scans that are available, where scans are performed, and the scan options that are available.

Understanding server scans

You can scan or configure one or more Norton AntiVirus Corporate Edition servers. The number of servers that you scan or configure depends on the object that you select:

- All servers in the network: If you select the System Hierarchy object in the Symantec System Center console tree, you can run a virus sweep to scan all Norton AntiVirus Corporate Edition servers in the network. (A virus sweep scans not only the Norton AntiVirus Corporate Edition server but any Norton AntiVirus Corporate Edition clients managed by the server.)
- All servers in selected server groups: If you select the System Hierarchy object in the Symantec System Center console tree, then select multiple server groups in the right pane, you can run either a virus sweep or configure a scheduled scan. A virus sweep scans all the Norton AntiVirus Corporate Edition servers and their clients in the selected server groups, while a scheduled scan scans only the servers.
- All servers in a server group: If you select a server group object, you can run a virus sweep or configure a scheduled scan for all servers in the server group.
- Some servers in a server group: If you select the server group object, then select multiple servers in the right pane, you can perform either a virus sweep or manual scan on all selected servers. (You cannot select multiple servers to configure scheduled scans.)
- A single server: If you select a single server object, you can run a virus sweep to scan the server and all of its clients, scan just the server by performing a manual scan, or configure a scan of the server or its clients using a scheduled scan.

Understanding client scans

Use Symantec System Center to scan or configure one or more Norton AntiVirus Corporate Edition client computers. The level of configuration depends on the object that is selected:

- All clients in the network: If you select the System Hierarchy object in the Symantec System Center console tree, you can run a virus sweep to scan all 32-bit and 16-bit Norton AntiVirus Corporate Edition clients in the network. (A virus sweep also scans all the Norton AntiVirus Corporate Edition servers that manage the clients.) For more information, see [“Running a virus sweep”](#) on page 384.
- All clients in selected server groups: If you select the System Hierarchy object in the Symantec System Center console tree, then select multiple server groups in the right pane, you can run a virus sweep. The virus sweep scans all Norton AntiVirus Corporate Edition servers and their 32-bit and 16-bit clients in the selected server groups.
- All clients in a single server group: If you select the server group object, you can run a virus sweep to scan all 32-bit and 16-bit clients in a single server group.
- All clients connected to a single server: If you select a server object, you can run a virus sweep or configure a scheduled scan. The virus sweep scans all 32-bit and 16-bit clients that are managed by the server. The scheduled scan scans only the 32-bit clients that are managed by the server.
- Selected 32-bit clients that connect to the same server: If you select a server in the console tree, then select multiple 32-bit client computers in the right pane, you can perform a manual scan.
- A single 32-bit client: If you select a 32-bit client object, you can perform a manual scan or set up a scheduled scan for only that computer.
- 16-bit clients: You cannot individually configure or scan 16-bit client computers. However, 16-bit computers are included in virus sweeps, and you can set realtime protection options for 16-bit clients at the server or server group level.

Note: Clients’ settings must be locked before realtime options configured at the Symantec System Center console can be propagated to them. For more information, see [“Locking realtime protection options”](#) on page 315.

Understanding scans on multiple selected computers

On the Symantec System Center console, you can select and configure multiple servers or client computers for specific scan types.

- **Multiple server groups:** When you select the System Hierarchy object in the Symantec System Center console tree, all server groups display in the right pane. In the right pane, select multiple server groups by holding down the Ctrl key and clicking the server groups. You can then perform a virus sweep or scheduled scan.
- **Multiple servers:** When you select a server group in the Symantec System Center console tree, all servers for the selected server group display in the right pane. In the right pane, select multiple servers by pressing Ctrl and clicking the servers. You can then perform a virus sweep or manual scan. You can also configure client realtime protection options and server realtime protection options.
- **Multiple client computers:** When you select a server in the Symantec System Center console tree, all Norton AntiVirus client computers that connect to the server display in the right pane. In the right pane, select multiple client computers by pressing Ctrl and clicking the client computers. You can then perform a manual scan. You can also configure client realtime protection options.

When you look at realtime protection, virus sweep, or manual scan options for multiple selected computers, the configuration check boxes and options have a tri-state feature that is apparent only when the computers have different options configured. Click the same option multiple times to see the different states.

- A solid black check mark in a check box or a solid black bullet in an option means that the option is selected for all computers in that group. Setting an option to a state other than the dimmed state resets that option for selected computers.
- A blank check box means the option is not selected for any computer in that group. Setting an option to a state other than the dimmed state resets that option for selected computers.
- A dimmed check mark in a dimmed box, a completely blank series of options, or a blank field means that some of the computers in the group have that option selected and some do not. Setting an option to a state other than the dimmed state resets that option for selected computers.

Dimmed or missing options

Some options, such as excluding files and folders, are not available when you select multiple computers because the option applies only to a specific computer.

Scan options set at the server group level

If you set the same scan options on the server or client level and at the server group level, the individual computers' settings are overwritten by the server group settings. If the same option is not changed at the server group level, the option remains unchanged on servers and clients.

Note: Realtime protection options work differently from the other scan options. Realtime protection options must be locked at the server group or server level before they can be propagated to clients. For more information, see [“Understanding realtime protection”](#) on page 313.

About configuring manual, scheduled, and realtime scan options

Many of the same scan options are available in different types of scans. For example, you can assign actions and backup actions when configuring manual, scheduled, or realtime scans.

Logon scanning options are unique (not shared between scan types) and are explained under a separate heading.

For more information, see [“Logon scanning options”](#) on page 336.

If you do not want details about scanning options and are ready to configure scans now, see the following major sections:

- See [“Configuring manual scans”](#) on page 311.
- See [“Configuring realtime protection for files”](#) on page 317.
- See [“Configuring logon scans for clients”](#) on page 339.

Assigning actions and backup actions for detected viruses

You can assign an action (and a backup action in case your first choice is not possible) that Norton AntiVirus takes when it discovers a virus. You can assign separate actions for macro and nonmacro viruses. Following are the actions and backup actions you can assign to detected viruses:

- **Clean Virus From File:** Attempts to clean an infected file upon detection.
- **Quarantine Infected File:** Attempts to move the infected file to Quarantine on the infected computer as soon as it is detected. After an infected file is moved to Quarantine, no user can execute it until you take an action (for example, clean or delete) and move the file back to its original location.
- **Delete Infected File:** Attempts to delete the file. Use this option only if you can replace the infected file with a virus-free backup copy because the file is permanently deleted and cannot be recovered from the Recycle Bin.
- **Leave Alone (Log Only):** Notifies you of the virus and logs the event but does not perform any other action.

By default, Norton AntiVirus first attempts to clean the file. If it cannot be cleaned, Norton AntiVirus moves the file to Quarantine on the infected computer.

To control how a virus is handled, choose the Leave Alone (log only) option. When you are notified of the virus, open the Virus History for the computer, right-click the name of the infected file and select one of the following actions: Clean, Delete Permanently, or Move To Quarantine.

Setting options that control interaction with users

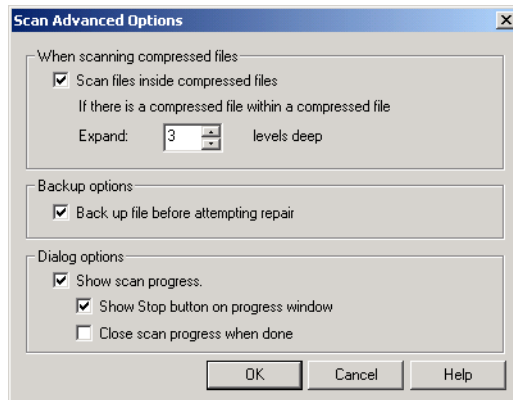
This section describes how to do the following:

- Display a scan progress window on the computer being scanned.
- Display a warning message on an infected computer.
- Add an infection warning to an email message with an infected attachment.
- Notify the sender of the infected attachment.
- Notify others about the receipt of an infected attachment.

Displaying or turning off a scan progress window on the client computer being scanned

If you want users to know that Norton AntiVirus is remotely scanning their computers (during an administrator-initiated manual or scheduled scan), set an option to display a scan progress window on client computers as they are scanned. Other options include:

- Show a Stop button on the scan progress window that lets a user cancel a scan in progress.
- Close the scan progress window automatically when a scan completes. This option is useful for unattended computers.



Displaying a warning message on an infected computer

When you run a remote scan on a user's computer, you can immediately notify the user of a problem by displaying a warning message on the infected computer's screen. If you display a warning, you can customize the message by including information such as the name of the virus, the name of the infected file, the status of the infection, and so on.

The default warning message contains message variables and text. The message variable is in brackets. Everything outside of the square brackets is text. You can change the text and message variables included in the

warning message to suit your needs. The message variables are defined below.

Variable	Text
[LoggedBy]	Type of scan that logged the event: Realtime, scheduled, or manual scan
[Event]	Type of event, such as Virus Found
[VirusName]	Name of detected virus
[PathAndFilename]	Full path and file name
[Location]	Drive location on the infected computer
[Computer]	Name of computer
[User]	Network logon name of user
[ActionTaken]	Action taken on infected file (such as cleaned, moved to the Quarantine, deleted, or left alone)
[DateFound]	Date and time the virus was found
[Status]	State of the file: Infected, Not Infected, or Deleted
	This message variable is not used by default. If you want to display this information, you must manually add the message variable to the warning message

For example, a warning message might look like this:

Scan type: Scheduled Scan

Event: Virus Found

VirusName: Stoned-C

File: C:\Autoexec.bat

Location: C:

Computer: ACCTG-2

User: JSmith

Action taken: Cleaned

Adding an infection warning to an email message

You can configure Lotus Notes and Microsoft Exchange realtime protection to automatically insert a warning into the body of an email message that contains an infected attachment. You can do this only if you have installed the email plug-in support for the following applications:

- 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

If you receive an infected attachment, you are warned when you read the email message.

This type of warning can be important if Norton AntiVirus is unable to clean the virus from the email attachment, and the attachment file is moved, left alone, deleted, or renamed. The warning message tells you which virus was found and explains the action that was taken.

Norton AntiVirus appends this text to the top of the email message associated with the infected attachment:

Norton AntiVirus found a virus in an attachment from [EmailSender].

For each infected file, the following information is also added to the email message:

- Name of the file attachment
- Name of the virus
- Action taken (such as cleaned, moved to the Quarantine, deleted, or left alone)
- File status (infected or not infected)

If the default message is not adequate for your organization, you can customize the subject and body of the message.

The email message contains a field, called [EmailSender]. All fields in brackets contain variable information. You can customize the default message by right-clicking the body of the message and selecting a field to insert into the message.

The message would look like this to the recipient:

Norton AntiVirus found a virus in an attachment from
John.Smith@mycompany.com.

Notifying the sender of the infected attachment

You can configure Lotus Notes and Microsoft Exchange realtime protection to respond automatically to the sender of an email message that contains an infected attachment.

Norton AntiVirus sends a reply email message with the subject:

Virus Found in message "[EmailSubject]"

The body of the message tells the sender to whom the infected attachment was sent:

Norton AntiVirus found a virus in an attachment you ([EmailSender]) sent to [EmailRecipientList].

For each infected file, the following information is also added to the email message:

- Name of the file attachment
- Name of the virus
- Action taken (such as cleaned, moved to the Quarantine, deleted, or left alone)
- File status (infected or not infected)

Notifying others about the receipt of an infected attachment

You can configure Lotus Notes and Microsoft Exchange realtime protection to notify others whenever an email message that contains an infected attachment is opened.

Norton AntiVirus sends to the selected recipients an email message with the subject:

Virus Found in message "[EmailSubject]"

The body of the message tells who sent the infected attachment:

Norton AntiVirus found a virus in an attachment from [EmailSender].

For each infected file, the following information is also added to the email message:

- Name of the file attachment
- Name of the virus
- Action taken (such as cleaned, moved to the Quarantine, deleted, or left alone)
- File status (infected or not infected)

Setting options that exclude files from scanning

Exclusions let you further customize your protection. When setting up what files to scan, exclusions help you balance the amount of protection your network requires and the amount of time and resources required to provide that protection. For example, when scanning all file types, you may want to exclude certain folders that contain only data files that are not subject to viruses. This decreases the overhead associated with needlessly scanning files.

On Windows-based computers, you can exclude files from any type of scan by specifying the file extension (using wildcards). On NetWare servers, you can exclude files only by drives and folders; you cannot exclude files by file extension.

From SSC, you can exclude files from a scan by drives and folders when you select the following objects and scan types:

- Client object: Manual scan, scheduled scan, and client realtime protection
- Server object: Manual scan, scheduled server scan, and server realtime protection (Windows only)

When excluding files directly from the Norton AntiVirus Corporate Edition client or server user interface, you can exclude files by drive, folder, or file name for all available types of scans, except for email scans.

From the client or server user interface, you may want to exclude files that trigger false positive alerts. For example, if you used another virus scanning program to clean infected files and the program did not completely remove the virus code, the file may be harmless but the disabled virus code might cause Norton AntiVirus to register a false positive. Check with Symantec Technical Support if you are not sure if a file is infected.

Setting exclusions

Norton AntiVirus Corporate Edition checks for specified exclusions before or after the scan runs. When it applies exclusions after the scan runs, information is presented for viruses found only if the file has not been excluded. When it applies exclusions before the scan runs, the excluded items are not scanned at all.

When Realtime Protection is enabled and a file is accessed (for example, it is opened, read, or written to), Norton AntiVirus Corporate Edition scans the file. If Norton AntiVirus Corporate Edition finds a virus, it checks to see if it is on the exclusions list, then acts as follows:

- If the file is on the exclusions list, no further action is taken.
- If the file is not on the exclusions list, it is handled appropriately based on all the scan option settings.

In a manual scan, virus sweep, or scheduled scan, all files are scanned. If a file is not infected, no action is taken. If the file is infected, Norton AntiVirus Corporate Edition checks to see if it is excluded. If the file is excluded, Norton AntiVirus Corporate Edition does not produce an alert notification. If the file is not excluded, an alert notification appears.

Norton AntiVirus keeps a count of the number of files scanned. Excluded files are included in this count, but Norton AntiVirus does not perform any action (such as clean or move) on the excluded files.

When the Check file for exclusion before scanning setting is enabled and a file is accessed (for example, it is opened, read, or written to), Norton AntiVirus Corporate Edition checks to see if the file is excluded. If the file is not excluded, it is then scanned. Because each file must be compared to the prescan exclusion list before it is scanned, scans may take longer to complete.

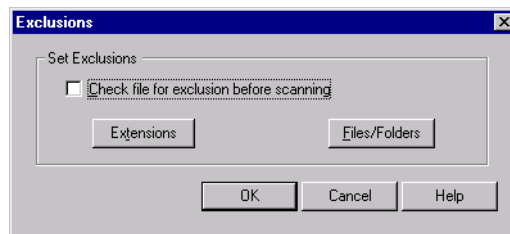
When the prescan exclusions setting is disabled, the file is scanned.

Both enabling and disabling prescan exclusions can improve performance in different situations. For example:

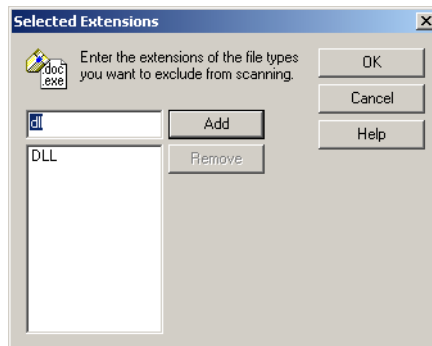
- If you copied a large folder that was in the exclusions list and prescan exclusions was enabled, the copying process would not take as long since the folder contents would be excluded prior to scanning.
- If you copied a large folder not in the exclusions list, disabling prescan exclusions would improve performance.

To set exclusions

- 1 In the Scan Options dialog box, click **Exclusions**.



- 2 To enable prescan exclusions, check **Check file for exclusion before scanning**.
- 3 Click **Extensions**, then specify the file types to exclude before scanning occurs.



- 4 Click **OK**.

- 5 Click **Files/Folders**, then specify the drives or folders (and their contents) to exclude before scanning occurs.

As a security precaution, when you set these options from the Symantec System Center console, folder names are visible but file names are not.

- 6 Click **OK**.

Excluding files on single and multiple computers

When configuring an individual computer, you can specify files for exclusion by file extension and by folder. As a security measure, files cannot be viewed from the Symantec System Center console. You can select individual files only while configuring Norton AntiVirus Corporate Edition from the computer that stores those files.

When configuring multiple computers, specify files for exclusion only by file extension. This is because files and folders are specific for each computer.

If you enable exclusions when scanning or configuring multiple computers, Norton AntiVirus uses any exclusions that you previously configured for the individual computers.

Setting options that include files for scanning

This section describes how to complete the following tasks:

- Select file types and extensions to scan.
- Select folders to scan.
- Scan or configure a single computer.
- Set options for scanning compressed files.

Selecting file types and extensions to scan

When configuring manual, scheduled, or realtime scans, you can set options for Norton AntiVirus to scan all file types, or you can limit the scope of the scan by:

- Scanning only certain file types, such as documents or programs. When scanning by file type, Norton AntiVirus reads each file header to determine the file type. For example, if you enable document scanning, Norton AntiVirus scans all documents even if you name them with a nonstandard extension, such as Document3.mlt instead of Document3.doc. This option doesn't apply to NetWare servers; it applies only to Windows-based computers.
- Scanning by file extension. When scanning by file extension, Norton AntiVirus does not read the file header to determine the file type and scans only files with the extensions that you specify.

Norton AntiVirus Corporate Edition scans all file types and selected extensions. Recommended extensions appear in the list below.

Extension	Description
386	Driver
ACM	Driver; audio compression manager
ACV	Driver; audio compression/decompression manager
ADT	ADT file; fax
AX	AX file
BAT	Batch
BTM	Batch
BIN	Binary
CLA	Java Class
COM	Executable
CPL	Applet Control Panel for Microsoft Windows
CSC	Corel Script
DLL	Dynamic Link Library

Extension	Description
DOC	MS-Word
DOT	MS-Word
DRV	Driver
EXE	Executable
HLP	Help File
HTA	HTML application
HTM	HTML
HTML	HTML
HTT	HTML
INF	Install script
INI	Initialization file
JS	JavaScript
JSE	JavaScript Encoded
JTD	Ichitaro
MDB	MS-Access
MP?	MS-Project
MSO	MS-Office 2000
OBD	MS-Office binder
OBT	MS-Office binder
OCX	MS-object linking and embedding custom control
OV?	Overlay
PIF	Program information file
PL	PERL program source code (UNIX)
PM	Presentation Manager Bitmaps Graphics
POT	MS-PowerPoint
PPT	MS-PowerPoint

Extension	Description
PPS	MS-PowerPoint
RTF	Rich Text Format document
SCR	Fax/screensaver/snapshot, script for Faxview/MS Windows
SH	Shell Script (UNIX)
SHB	Corel Show Background file
SHS	Shell scrap file
SMM	AmiPro
SYS	Device driver
VBE	VESA BIOS (Core Functions)
VBS	VBScript
VSD	Visio
VSS	Visio
VST	Visio
VXD	Virtual device driver
WSF	Windows Script File
WSH	Windows Script Host Settings File
XL?	MS-Excel

Selecting folders to scan

The default is to scan all files and folders. However, you can restrict the scan to selected folders only.

As a security measure, files cannot be viewed from the Symantec System Center console.

Scanning or configuring a single computer

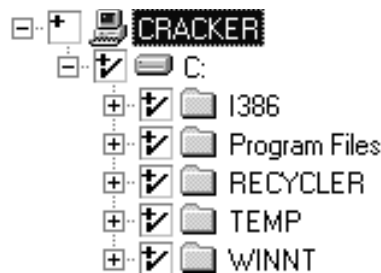
When running a manual scan or configuring a scheduled scan for a single computer, you can select folders to scan. If you want Norton AntiVirus to remember your selection for future scans, click Save Settings.

Making the selection

Select folders to scan from the tree view. The computer name appears as the highest level object, and the local fixed drives display under the computer name. For example, when running a manual scan from the SSC console for the computer CRACKER, you would see:



If you expand the C drive on CRACKER, you see:



As you select folders or items in the tree view, the icons next to each folder or item change among the following states.

Icon	Icon description
	Norton AntiVirus scans all files in this folder and also scans all files in subfolders.
	Norton AntiVirus scans one or more items that you've selected in the folder or one of the subfolders.
	Norton AntiVirus scans the selected file. This is available only from the client or server interface of Norton AntiVirus Corporate Edition.
	Norton AntiVirus does not scan the folder or subitems.

Setting options for scanning compressed files

For Windows 32-bit computers, options for scanning within compressed files apply only to manual scans or scheduled scans. Because of the significant processing overhead, file system realtime protection does not scan files within compressed files on Windows computers; however, the files are scanned as they are extracted from compressed files.

For NetWare servers, options for scanning within compressed files apply only to realtime and scheduled scans. In order to scan the contents of a compressed file, Norton AntiVirus extracts each file, one file at a time, from the container and copies it to the SYS volume where it is scanned. The SYS volume must have enough space available on the volume to accommodate the largest file in the container.

If you have compressed files within compressed files, set options to scan multiple layers. If you set this option, Norton AntiVirus scans the container (such as Files.zip) and also the contents of the container, which are the individual, compressed files.

You cannot stop a scan in progress on a compressed file. If you click Stop Scan, Norton AntiVirus stops the scan only after it has finished scanning the compressed file.

The following options also affect compressed file scanning.

Option	Description
Scan All Files:	If this option is enabled, compressed files are scanned if the Scan Inside Compressed Files option in the Advanced dialog box is also enabled.
Scan By Extension:	If this option and the Scan Inside Compressed files option are enabled, compressed files are scanned regardless of whether the extension is in the list of specified extensions. The extension check is applied to the files inside the compressed files. For example, if you have chosen to scan only .com using the extensions list, and you have enabled Scan Inside Compressed Files, then a file named Test.zip that contains .com and .doc files is scanned, only the .com files inside Test.zip are scanned.

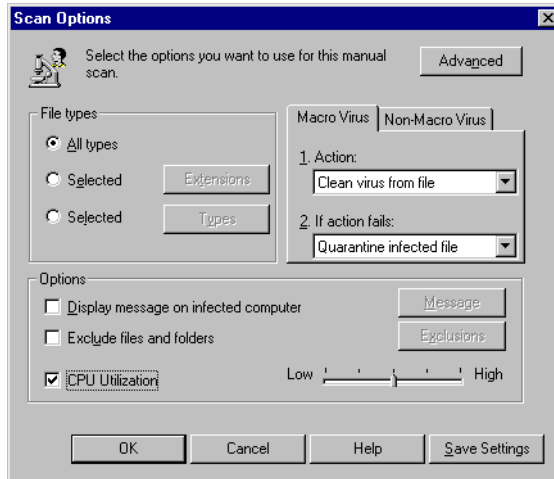
Setting CPU utilization

You can limit the amount of processor resources that Norton AntiVirus uses during a scan. The more you limit CPU utilization, the longer the scan takes. You may want to set lower CPU utilization in some situations. For example, if you have scans running at lunch time during the work week, you might want to lower CPU utilization to minimize impact on user productivity.

You can set CPU utilization when running a manual scan or when configuring a scheduled scan. By default, this option is not selected.

Configuring manual scans

Manual or on-demand scans inspect selected files and folders on selected computers. Manual scans are ideal for providing immediate results from a scan on a small area of the network or on a local hard drive.



To configure a manual scan

- 1 In the Symantec System Center console, do one of the following:
 - Right-click a server or client computer.
 - Select one or more servers in the same server group, then right-click the servers.
 - Select one or more clients managed by the same server, then right-click the clients.

Note: If you want to scan all servers and clients in a server group, run a virus sweep instead of a manual scan. For more information, see [“Running a virus sweep”](#) on page 384.

- 2 Click **All Tasks > Norton AntiVirus > Start Manual Scan**.
- 3 Select the folders to scan.

If you are scanning multiple computers, this option is not available. Go to step 5.

- 4 Click **Save Settings** if you want Norton AntiVirus to remember your selections for future manual scans on this computer.

Norton AntiVirus also remembers these settings for future scans when multiple computers are selected.

- 5 Click **Options**.

You can:

- Select file types and extensions to scan.
- Display a warning message on infected computers.
- Exclude files and folders from the scan. (Not available for multiple clients or servers.)
- Set CPU utilization.
- Assign actions and backup actions for detected viruses.

- 6 Click **Advanced**.

You can:

- Determine whether compressed files are scanned. If enabled, you can determine how deeply compressed levels are scanned. The default scan setting is three levels in a compressed file.
- Back up files before attempting to repair them as a data safety precaution. The files will be encrypted and backed up to the Quarantine directory. Once backed up, the file must be restored before it can be accessed again.
- Determine whether a progress dialog box appears on the computer while the scan runs. You can configure the progress dialog box to close automatically when the scan has completed. You can also display or hide a Stop button on the remote computer. When this option is disabled, the scan cannot be stopped from the remote machine.
- Enable scans of files using NetWare compression.

- 7 Click **OK** to save advanced options.

- 8 In the Scan Options window, click **Save Settings** if you want Norton AntiVirus to remember these options for future manual scans on this computer.

Norton AntiVirus will also remember these settings for future scans when multiple computers are selected.

- 9 Click **OK** to continue with these options.

- 10 Click **Start**.

Understanding realtime protection

If you enable realtime protection, Norton AntiVirus scans both files and email data as they're read from or written to a client computer. Realtime protection scans all files by default. Configure realtime protection for servers at the server group or server level. Configure clients at either the server group, server, or client level.

For more information, see [“Setting client realtime protection options at the server or server group level”](#) on page 314.

Norton AntiVirus provides native email scanning on 32-bit client computers for these data formats:

- 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

With native email scanning, Norton AntiVirus intercepts messages with infected attachments before the attachments are opened.

When you access an infected file inside a compressed file using Windows Explorer or a compression application (such as WinZip), Norton AntiVirus displays an alert and provides status on the infected item. However, this status is for the temporary files created by Windows Explorer or the compression application. The virus remains in the compressed file. To act directly on the infected file inside of the compressed file, you must perform a manual scan.

File caching for realtime scans

Norton AntiVirus Corporate Edition includes a file caching feature that optimizes realtime scan performance. When Windows 9x/NT/2000/Me/XP computers are scanned in realtime, a list of files that have been scanned and are known to be uninfected is cached.

A file is added to the cache once it has been scanned and determined to be clean. Once added to the cache, it is not rescanned until it is removed from the cache. A file is removed from the cache when:

- A system event, such as a delete or write, acts on the file.
- The computer is restarted.
- Realtime protection is disabled.
- Virus definitions are updated.

If your email program is not supported

If your email system is not one of the supported data formats, you can still protect your network by enabling realtime protection on your file system. For example, if you are running a Novell GroupWise email system and one of your users receives a message with an infected attachment, Norton AntiVirus can detect the virus as soon as the user double-clicks the attachment to open it. This is because most email programs (such as GroupWise) save attachments to a temporary directory when users launch the attachments from the email client program. If you enable realtime protection on your file system, Norton AntiVirus detects the virus as it is written to the temporary directory. Norton AntiVirus also detects the virus if the user tries to save the infected attachment to a local or network drive.

Remote scans of email data

Norton AntiVirus cannot remotely scan client email data. This is because the email application may not be running on the local computer, and an email password is required to access the email data. Norton AntiVirus cannot store or discover local email passwords.

Use Symantec System Center to remotely set and lock realtime protection options on client computers. Users can run realtime scans of email data on their own computers.

Setting client realtime protection options at the server or server group level

When you change client realtime protection options at the server or server group level, you must lock the option and click OK to propagate that setting. Changes made at the server group level are propagated to all clients belonging to the server group. Changes at the server level are propagated to all clients belonging to the server.

When you click Reset All at the server group level, any scan options that were previously set at the server and client level are overwritten by the server group settings. When you click Reset All at the server level, any scan options that were previously set at the client level are overwritten by the server settings.

Changes made at the server group level are sent immediately to the primary server, which in turn updates the other servers in the server group. Each server then updates its clients. When you configure client realtime

protection options at the server level, the server pushes the changes to its clients. The update process takes several minutes.

If the new client configuration is not immediately received by the parent server or by the client, the information is updated during the server/client check-in. The default client check-in interval is set to 60 minutes.

Locking realtime protection options

If you configure and lock a client realtime protection option at the server group or server level, connected client computers read and use the new configuration from the server to which they connect.

If you configure but do not lock a client realtime protection option at the server group or server level, the currently connected client computers do not read or use the new server or server group configuration. These changes will be propagated to future client installations.

If you select multiple clients for a server and the clients have different realtime protection options, a question mark (?) is displayed over the Lock button. When you lock or unlock the setting, the change is propagated to the selected clients.

Resetting realtime protection options

If you want to be sure that all computers are using the same realtime scanning configuration, click Reset All when configuring the options. This propagates realtime protection options on all opened configuration pages to the affected computers.

Only opened configuration pages are propagated. For example, when configuring client realtime protection options:

- You view the file system realtime protection options.
- You do not view the client email configuration options, which are located in a separate configuration tab.
- You click Reset All.

In this example, only the file system realtime protection options are propagated.

Resetting servers to accept the server group-level configuration

If you configure server realtime protection options for a server group, then click Reset All, you are propagating all realtime protection options to all of the servers that belong to the server group.

Resetting clients to accept the server group-level configuration

If you configure client realtime protection options for a server group, then click Reset All, you are propagating all file system realtime protection options and any other viewed property pages to all of the clients that connect to any of the servers in the server group.

Resetting clients to accept the server-level configuration

If you configure client realtime protection options for a server, then click Reset All, you are propagating all file system realtime protection options and any other viewed property pages to all of the clients that connect to the server.

Changing realtime protection options without clicking Reset All

If you are configuring server realtime protection options at the server group level, Norton AntiVirus propagates any options that you change to all of the servers that belong to the server group when you click OK. Options that you do not change at the server group level are not propagated and may remain different on individual servers.

If you are configuring client realtime protection options at the server or server group level, Norton AntiVirus propagates only those options that are locked when you click OK.



This is an unlocked option.



This is a locked option.

If you change an option but do not lock it, the existing clients will not pick up the change. These changes also will not be propagated to future client installations.

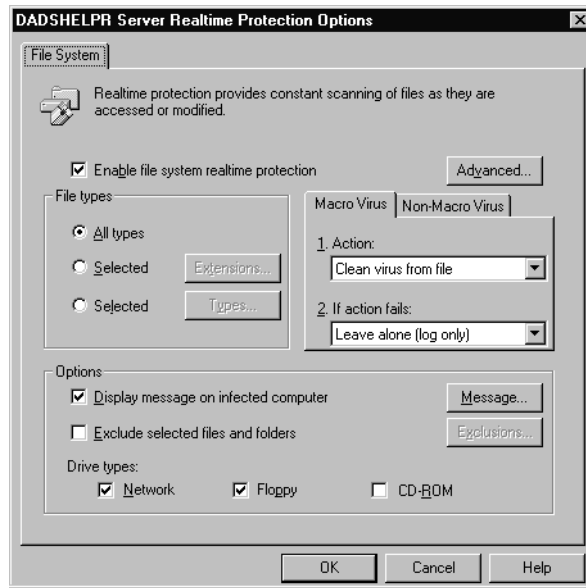
If you select an individual 32-bit client computer in Symantec System Center to set a realtime protection option, the client computer will pick up the change whether the item is locked or unlocked. This makes it possible to lock or unlock an option for a single user without resetting all options on all clients.

Configuring realtime protection for files

Realtime scans can inspect files for known viruses on a continuous basis as the files are read from or written to a computer. Realtime protection is enabled on your file system by default.

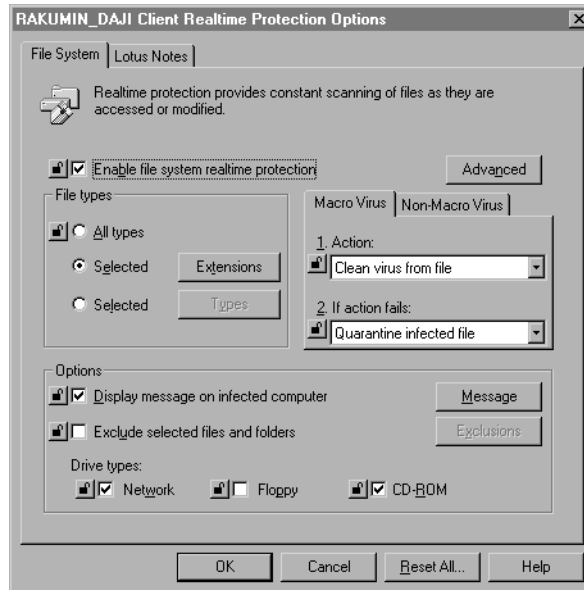
Configuring server realtime protection for your file system

When you configure realtime protection for your file system, the configuration pages look slightly different depending on whether you are setting options for servers or clients. This is what the configuration page looks like when you configure server realtime protection:



Configuring client realtime protection for your file system

When you configure realtime protection for your clients, you might see additional configuration pages depending on the email system that you use. For example, the following screen shot shows a configuration tab for Lotus Notes.



For more information, see [“Configuring realtime protection for mail applications”](#) on page 323.

You can also lock realtime protection options on clients if you want to enforce a virus policy. Users cannot change options that you lock.

Setting file system realtime protection advanced options

Two file system advanced realtime protection options determine the file operations that realtime protection monitors.

- **Modified (scan on create):** Whenever a file is written or modified, or if a file is copied to a computer, Norton AntiVirus scans the file. This permits faster performance because the number of file processes that realtime protection monitors is limited. However, the trade-off is protection; some viruses will not be detected when using this option.
- **Accessed or modified (scan on create, open, move, copy, or run):** Whenever a file is written to or modified, or if a file is copied to a computer, Norton AntiVirus scans the file. In addition, Norton AntiVirus scans the file whenever it is read or executed. This provides slower performance but is more thorough. This option provides the best protection against viruses at a small resource cost.

Selecting drive types to scan

When configuring realtime protection options for files, specify which drive types you want Norton AntiVirus to scan.

The network drive option applies to all computers. The floppy disk and CD-ROM drive options apply only to Windows 3.x computers. If you are configuring protection for computers running Windows 9x/NT/2000/Me/XP or NetWare, these options do not apply.

- **Floppy:** Norton AntiVirus can scan files as they are read from or written to floppy disks. Floppy disks are common sources of virus infections because users may bring infected disks from home.
- **CD-ROM:** On occasion, some software companies ship CD-ROMs with infected files on them.
- **Network:** If you enable realtime protection on network drives, Norton AntiVirus can scan files as they're written from a client computer to a server (or from a server to another server). This option is not necessary if you enable realtime protection on your servers. For example, suppose that you enable scanning of network drives on Client A and also have realtime protection enabled on Server B. When Client A writes a file to a network drive on Server B, Norton AntiVirus scans the file on Client A and then scans the file again on Server B. This could reduce network performance on the client computer.

To configure realtime protection for files

1 Do one of the following:

- Right-click the server group or servers that you want to configure, then click **All Tasks > Norton AntiVirus > Server Realtime Protection Options**.

If you select a server group object, Symantec System Center assumes you want to configure all servers in the server group.

- Right-click individual or multiselect servers, then click **All Tasks > Norton AntiVirus > Client Realtime Protection Options**.
- Right-click the server group or servers with clients that you want to configure, then click **All Tasks > Norton AntiVirus > Client Realtime Protection Options**.

Symantec System Center assumes you want to configure all clients associated with the server or server group.

- Right-click individual or multiselect clients for a server, then click **All Tasks > Norton AntiVirus > Client Realtime Protection Options**.

2 Ensure that Enable File System Realtime Protection is checked.

3 Set realtime protection options.

You can:

- Select file types and extensions to scan.
- Assign actions and backup actions for detected viruses.
- Display a warning message on the infected computer.
- Exclude files and folders from the scan. (Available only when you select an individual server for Server Realtime Protection Options or an individual client for Client Realtime Protection Options.)
- Select drive types to scan.

4 Click **Advanced**.

You can:

- Scan files when they are modified or accessed/modified.
For more information, see [“Setting file system realtime protection advanced options”](#) on page 319.
- Back up files before attempting to repair them as a data safety precaution. The files are encrypted and backed up to the Quarantine directory. Once backed up, the file must be restored before it can be accessed again.
- For servers, determine whether compressed files are scanned. Compressed files are not scanned on servers by default. If enabled, you can determine how deeply compressed levels are scanned. The default scan setting is three levels in a compressed file.

5 Click **Heuristics** to change the level of protection provided by Bloodhound Heuristic Scanning.

Bloodhound can detect a high percentage of unknown viruses by isolating and locating the logical regions of a file. Bloodhound then analyzes the program logic for virus-like behavior.

6 Click **OK** once you’ve established the setting you want.

7 Click **Floppies** if you want to change the current setting for floppy disk scanning.

You can:

- Select **Check floppies for boot viruses upon access** to have Norton AntiVirus scan the floppy disk in the floppy drive for a boot virus when the drive is first accessed. From **When a boot virus is found**, you must select whether to clean a virus from the boot record or leave it alone.

If you select **Leave Alone (Log Only)**, an alert is sent when a virus is detected but no action is taken. Use this option if you want to take direct control over the virus cleaning and handling process. For example, after you receive the alert, you can decide what course of action to take.

- Select **Do not check floppies upon system shutdown** to have Norton AntiVirus skip the scan of any floppy disk in the floppy drive when the computer is shut down normally.

- 8 (Windows 9x only): Click **Monitor** to disable protection monitors for virus-like activities.

Virus-like activities are activities that viruses perform when attempting to infect your files. Any of these activities might occasionally be legitimate in your work context. The following activities can be excluded from monitoring:

- Low-Level Format Of Hard Disk: All information on the drive is erased and cannot be recovered. This type of format is generally performed at the factory only. If this activity is detected, it usually indicates an unknown virus at work. (This is not an option for NEC PC98xx computers.)
 - Write To Hard Disk Boot Records: Very few programs write to hard disk boot records. If this activity is detected, it could indicate an unknown virus at work.
 - Write To Floppy Disk Boot Records: Only a few programs (such as the operating system Format command) write to floppy disk boot records. If this activity is detected, it could indicate an unknown virus at work.
- 9 Lock or unlock any client realtime protection options that you want to propagate to clients.
- For more information, see [“Locking realtime protection options”](#) on page 315.
- 10 If you are configuring realtime protection options for a server group, click **Reset All** if you want to be sure that all computers are using the realtime scanning configuration you set at this level.
- For more information, see [“Resetting realtime protection options”](#) on page 315.
- 11 Click **OK**.

For more information, see [“About configuring manual, scheduled, and realtime scan options”](#) on page 295.

Configuring realtime protection for mail applications

Realtime scans can inspect email data for the following applications:

- 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

Data is inspected for known virus definitions on a continuous basis as the data is read from or written to a computer. With native email scanning, Norton AntiVirus scans messages for infected attachments when the message is opened.

For more information, see [“Understanding realtime protection”](#) on page 313.

To configure realtime protection options for email data

- 1 In the Symantec System Center console, right-click the server group or servers to configure, then click **All Tasks > Norton AntiVirus > Client Realtime Protection Options**.
- 2 On the Lotus Notes or Microsoft Exchange tab, check **Enable Realtime Protection**.

The tab is only present if at least one of your clients has the email application installed. You can use the Microsoft Exchange tab to configure both Microsoft Exchange and Microsoft Outlook.

- 3 Set realtime protection options.

You can:

- Select file types and extensions to scan.
 - Assign actions and backup actions for detected viruses.
 - Display a warning message on infected computers.
 - Insert a warning into the email message.
 - Send email to the sender of the infected attachment.
 - Send email to selected recipients when a virus is detected.
- 4 Click **Advanced** to configure scanning of compressed files.
 - 5 Set the options, then click **OK**.

- 6 Lock or unlock options as desired.
For more information, see [“Locking realtime protection options”](#) on page 315.
- 7 Click **Reset All** if you want to be sure that all computers are using the realtime scanning configuration you set at a higher level.
For more information, see [“Resetting realtime protection options”](#) on page 315.

Configuring scheduled scans

Scheduled scans are ideal for scanning large areas of the network. For example, after you download the latest definitions file, you may want to scan all files with it. It is a good idea to schedule scans during off hours when network traffic is low.

From the Symantec System Center console, you can schedule scans for servers or clients. Users can also schedule scans for their computers using the Norton AntiVirus client, but they cannot change or disable any scans that you schedule for their client computers.

When you create and save a scheduled scan, Norton AntiVirus remembers which server group, server, or computer on which to run the scan and also remembers the settings that you chose for that scan.

If a 32-bit computer is turned off during a scheduled scan, the scan will not run unless the computer has been configured to run missed scan events.

For more information, see [“Setting options for missed scheduled scans”](#) on page 333.

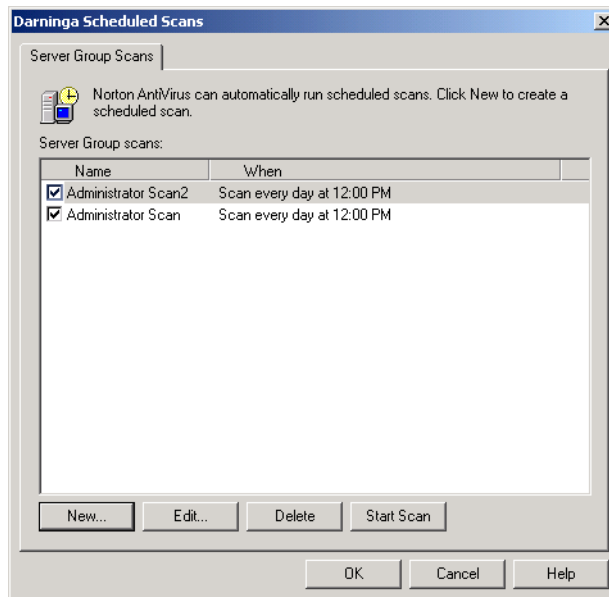
For a scheduled scan to run on a 16-bit computer, the computer must be turned on and the computer's user must be logged on.

Scheduling scans for server groups

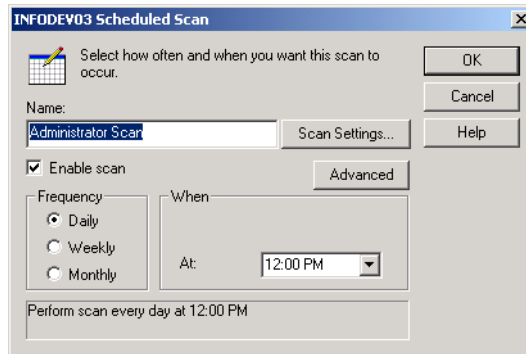
You can schedule scans for one or more server groups. The scheduled scan runs on all servers in the server group.

To schedule a scan for a server group

- 1 In the Symantec System Center console, do one of the following:
 - In the console tree, click **System Hierarchy**. In the right pane, Shift+click or Ctrl+click to select multiple server groups, then right-click the selection.
 - Right-click a server group.
- 2 Click **All Tasks > Norton AntiVirus > Scheduled Scans**.



3 Click **New**.



4 Type a name for the scan.

5 Set a frequency for the scan.

6 Set a time for the scan.

You can enter any time in increments of 1 minute or use the drop down list to select a time in 15-minute increments.

7 Click **Advanced**.

8 Check **Handle Missed Events Within**, then set the time limit within which you want the scan to run.

For example, you may want a weekly scan to run only if it is within three days after the scheduled time for the missed event.

9 Click **OK** to close the Advanced Schedule Options dialog box.

10 Click **Scan Settings**.

11 Click **Options**.

You can:

- Select file types and extensions to scan.
- Display a warning message on the infected computer.
- Exclude files from the scan by file extension.
- Set CPU utilization.
- Assign actions and backup actions for detected viruses.

12 Click **Advanced.**

You can:

- Display a scan progress window on a computer being scanned.
- Close a Scan Progress window on a computer when the scan completes.
- Back up files before attempting to repair them as a data safety precaution. The files are encrypted and backed up to the Quarantine directory. Once backed up, the file must be restored before it can be accessed again.
- Set options for scanning compressed files.

13 Click **OK until you return to the main screen in Symantec System Center.**

For more information, see [“About configuring manual, scheduled, and realtime scan options”](#) on page 295.

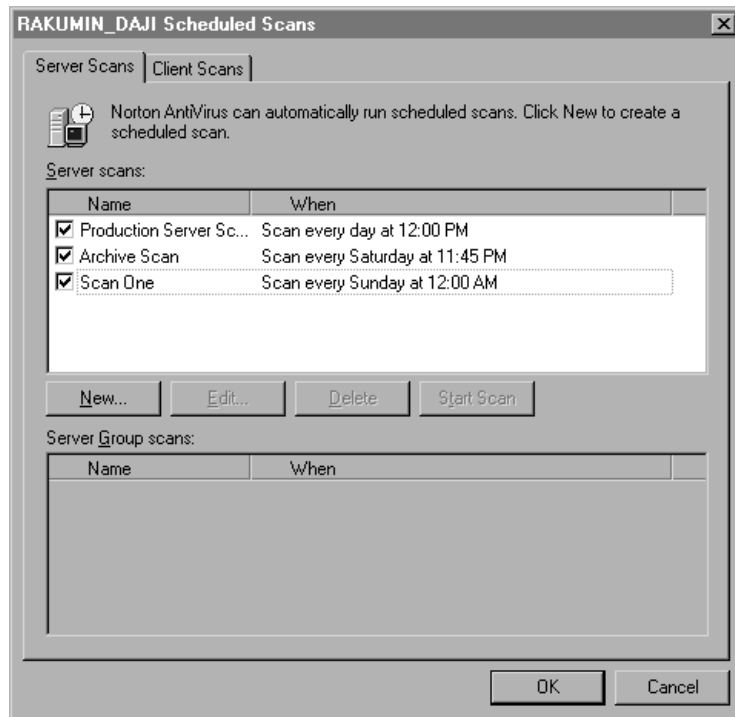
Scheduling server scans

You can schedule scans at the server level.

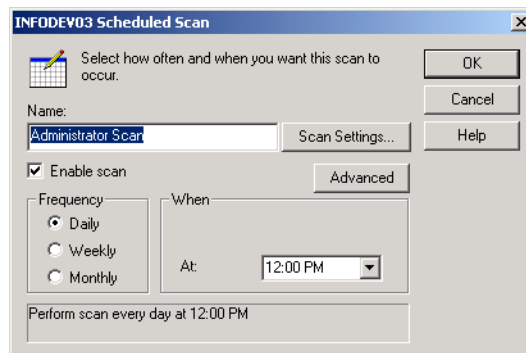
To schedule server scans

- 1** In the Symantec System Center console, right-click a server.
- 2** Click **All Tasks > Norton AntiVirus > Scheduled Scans**.

- 3 On the **Server Scans** tab, click **New**.



- 4 Type a name for the scan.



- 5 Set a frequency for the scan.

- 6 Set a time for the scan.

You can enter any time in increments of 1 minute or use the drop down list to select a time in 15-minute increments.

- 7 Click **Advanced**.
- 8 Check **Handle Missed Events Within**, then set the time limit within which you want the scan to run.

For example, you may want a weekly scan to run only if it is within three days after the scheduled time for the missed event.

- 9 Click **OK** to close the Advanced Schedule Options dialog box.
- 10 Click **Scan Settings**.
- 11 Select folders to scan.
- 12 Click **Options**.

You can:

- Select file types and extensions to scan.
- Display a warning message on the infected computer.
- Exclude files from the scan by file extension or by drive and folder.
- Set CPU utilization.
- Assign actions and backup actions for detected viruses.

- 13 Click **Advanced**.

You can:

- Display a scan progress window on a computer being scanned.
- Close a Scan Progress window on a computer when the scan completes.
- Back up files before attempting to repair them as a data safety precaution. The files are encrypted and backed up to the Quarantine directory. Once backed up, the file must be restored before it can be accessed again.
- Set options for scanning compressed files.

- 14 Click **OK** until you return to the main screen in Symantec System Center.

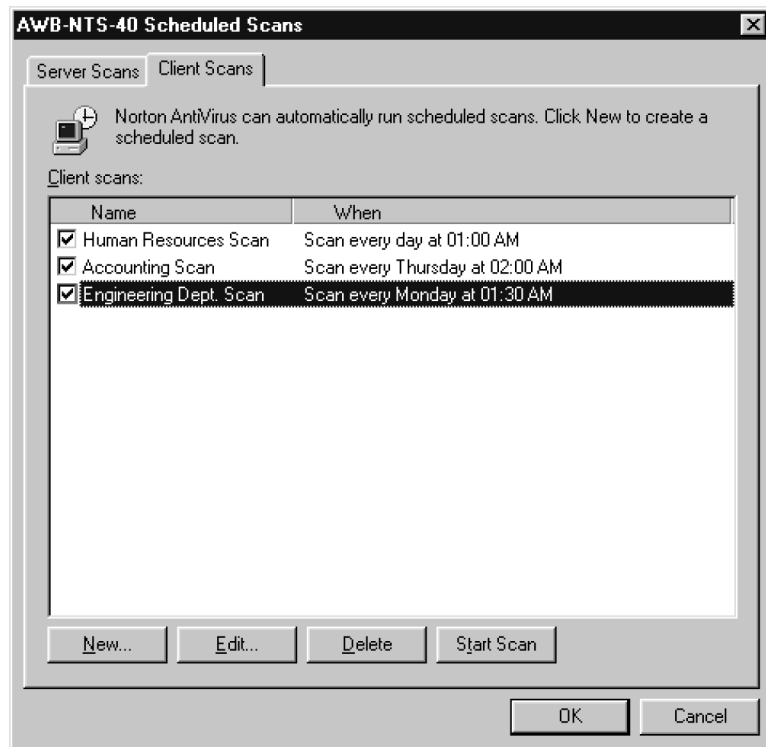
For more information, see [“About configuring manual, scheduled, and realtime scan options”](#) on page 295.

Scheduling scans for clients

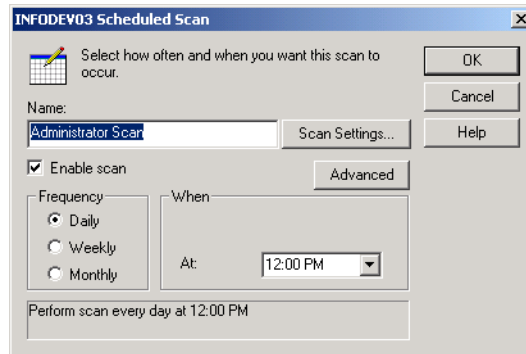
You can schedule client scans at the server or client level.

To schedule client scans at the server level

- 1 In the Symantec System Center console, right-click a server.
- 2 Click **All Tasks > Norton AntiVirus > Scheduled Scans**.
- 3 On the Client Scans tab, click **New**.



- 4 Type a name for the scan.



- 5 Set a frequency for the scan.
- 6 Set a time for the scan.
You can enter any time in increments of 1 minute or use the drop down list to select a time in 15-minute increments.
- 7 Click **Advanced**.
- 8 Check **Handle Missed Events Within**, then set the time limit within which you want the scan to run.
For example, you may want a weekly scan to run only if it is within three days after the scheduled time for the missed event.
- 9 Click **OK** to close the Advanced Schedule Options dialog box.
- 10 Click **Scan Settings**.
- 11 Click **Options**.

You can:

- Select file types and extensions to scan.
- Display a warning message on the infected computer.
- Exclude files from the scan by file extension.
- Set CPU utilization.
- Assign actions and backup actions for detected viruses.

12 Click **Advanced.**

You can:

- Display a scan progress window on a computer being scanned.
- Close a Scan Progress window on a computer when the scan completes.
- Back up files before attempting to repair them as a data safety precaution. The files are encrypted and backed up to the Quarantine directory. Once backed up, the file must be restored before it can be accessed again.
- Set options for scanning compressed files.

13 Click **OK until you return to the main screen in Symantec System Center.**

To schedule client scans at the client level

- 1** In the Symantec System Center console, right-click a client.
- 2** Click **All Tasks > Norton AntiVirus > Scheduled Scans**.
- 3** Click **New**.
- 4** Type a name for the scan.
- 5** Set a frequency for the scan.
- 6** Set a time for the scan.

You can enter any time in increments of 1 minute or use the drop down list to select a time in 15-minute increments.

- 7** Click **Advanced**.
- 8** Check **Handle Missed Events Within**, then set the time limit within which you want the scan to run.

For example, you may want a weekly scan to run only if it is within three days after the scheduled time for the missed event.

- 9** Click **OK** to close the Advanced Schedule Options dialog box.
- 10** Click **Scan Settings**.
- 11** Select the folders to scan.

This option is not available if you are scanning multiple computers because folders are specific to each computer.

12 Click **Options.**

You can:

- Select file types and extensions to scan.
- Display a warning message on the infected computer.
- Exclude files from the scan by file extension or by drive and folder.
- Set CPU utilization.
- Assign actions and backup actions for detected viruses.

13 Click **Advanced.**

You can:

- Display a scan progress window on a computer being scanned.
- Close a Scan Progress window on a computer when the scan completes.
- Back up files before attempting to repair them as a data safety precaution. The files are encrypted and backed up to the Quarantine directory. Once backed up, the file must be restored before it can be accessed again.
- Set options for scanning compressed files.

14 Click **OK until you return to the main screen in Symantec System Center.**

For more information, see [“About configuring manual, scheduled, and realtime scan options”](#) on page 295.

Scheduling multiple scans

Norton AntiVirus lets only one scheduled scan run on a computer. If more than one scan is scheduled at the same time, they will run sequentially.

Setting options for missed scheduled scans

When you create or edit scheduled scans, you can ensure that scan events that were missed will run at a later time. For example, a computer may be turned off at the time when a scan is scheduled to run. Enabling the Handle Missed Events option lets the scan run if the computer is turned on within a specified time parameter.

Understanding the hierarchy for scheduling scans

The number and types of computers that you can schedule depend on the object you select before entering the scheduling configuration dialog box.

- **Server group:** If you select a server group, you can schedule scans for all servers in the server group.
- **Server:** If you select a server, you can schedule a scan for that server only, or for all clients that connect to that server. When scheduling a scan for an individual server, you can also see server group-level scans in which the server is scheduled. This avoids creating redundant scans.
- **Client:** If you select a client, you schedule a scan only for that client.

Note: You cannot configure scheduled scans for multiselect servers. You must configure them at the server group or server level.

Editing, deleting, or disabling a scheduled scan

If you want to stop a previously scheduled scan from occurring, you can delete or disable it. If you want to modify the properties of an existing scheduled scan, you can edit it.

To edit or delete a scheduled scan

- 1 In the Symantec System Center console, right-click the object (one or more server groups, a server, or a client) for which you want to edit or delete the scheduled scan.

- 2 Click **All Tasks > Norton AntiVirus > Scheduled Scans**.

The scans that you can schedule or edit depend on the object that you select.

For more information, see [“Understanding the hierarchy for scheduling scans”](#) on page 334.

- 3 Select one of the following:
 - **Server Scans:** Edit or delete scans for servers. This option is not available if you selected a 32-bit client computer in step 1.
 - **Client Scans:** Edit or delete scans for clients. This option is not available if you selected a server group in step 1.

- 4 Do one of the following:
 - Select an existing scan, then click **Edit**. Change any properties that you want, then click **OK** until you return to the Symantec System Center main window.
 - Select an existing scan, then click **Delete**.

To disable a previously scheduled scan

- 1 In the Symantec System Center console, right-click the object (one or more server groups, a server, or a client) for which you want to disable the scheduled scan.

The scans that you can disable depend on the object you select.

For more information, see [“Understanding the hierarchy for scheduling scans”](#) on page 334.

- 2 Click **All Tasks > Norton AntiVirus > Scheduled Scans**.
- 3 Select one of the following:
 - **Server Scans**: Disable scans for servers. This option is not available if you selected a 32-bit client computer in step 1.
 - **Client Scans**: Disable scans for clients. This option is not available if you selected a server group in step 1.
- 4 Uncheck the previously scheduled scan.
- 5 Click **OK**.

Running a scheduled scan on demand

When you create and save a scheduled scan, Norton AntiVirus remembers which server group, server, or computer on which to run the scan and also remembers all of the settings that you chose for that specific scan.

After configuring a scheduled scan (with all of its scan properties), you might want to run it on demand at some time other than when you originally scheduled it. This can save you the effort of configuring and running a manual scan with similar properties.

To run a scheduled scan on demand

- 1 In the Symantec System Center console, right-click a server group or a server.
For more information, see [“Understanding the hierarchy for scheduling scans”](#) on page 334.
- 2 Click **All Tasks > Norton AntiVirus > Scheduled Scans**.
- 3 Select one of the following:
 - Server Scans: Run a server scan on demand.
 - Client Scans: Run a client scan on demand. This option is not available if you selected a server group in step 1.
- 4 Select an existing scheduled scan.
- 5 Click **Start Scan**.

Logon scanning options

Logon scanning is available for Windows 3.1 and DOS computers only.

When configuring logon scans, you may want more detailed information about:

- Selecting file types to scan
- Selecting locations to scan
- Assigning actions for detected viruses
- Preventing users from canceling a logon scan
- Setting command-line scan options

Selecting file types to scan

You can set one or more options to scan the following types of files on a Windows 3.1 or DOS computer at logon:

- All files: This option includes system compressed files, such as files compressed using a disk compression program such as Stacker. When the scanner requests these types of files, the operating system uncompresses them. However, the All files option does not include compressed executables (such as *.ex_ files) or compressed archives (such as .zip files), which are available as separate items.
- Compressed executables: This includes compressed files such as *.ex_.
- Compressed archives: This includes *.zip, *.lha, and *.lzh.

Selecting locations to scan

You can set options to scan any of the following locations on the client computer at logon:

- Memory
- Boot sector and partition table
- All local drives (includes hard drives, CD drives, and floppy disk drives)

Scanning memory and the boot sector typically takes just a few seconds. Scanning files on all local drives might take longer, depending on the sizes of the drives and the speed of the computer.

Assigning actions for detected viruses during a logon scan

You can assign an action for Norton AntiVirus to take when it discovers a virus during a logon scan of a Windows 3.1 or DOS computer. Following are the actions you can assign to detected viruses:

- Clean Virus From File: Norton AntiVirus attempts to clean an infected file as soon as it is detected.
- Quarantine Infected File: Norton AntiVirus attempts to move the infected file to the Quarantine on the infected computer as soon as it is detected. After an infected file is moved to the Quarantine, no user can execute it until you take an action (for example, clean or delete) and move the file back to its original location. If you have set up a Quarantine server, the file is also forwarded to the server. The file also remains on the local computer. Virus definitions must be updated on the local computer.
- Delete Infected File: Norton AntiVirus attempts to delete the file. Use this option only if you can replace the infected file with a virus-free backup copy because the file is permanently deleted and cannot be recovered from the Recycle Bin.
- Leave Alone (log only): Norton AntiVirus will notify you of the virus and log the event but will not perform any other action.

Preventing users from canceling a logon scan

When configuring logon scans for Windows 3.1 and DOS computers, you can check an option to enforce a virus scan at logon. This prevents users from canceling the scan.

To prevent users from canceling a logon scan

- 1 In the Symantec System Center console, right-click a server group, multiple servers, or a server.
- 2 Click **All Tasks > Norton AntiVirus > Client Login Scan And Installation**.
- 3 Click **Login Scan**.
- 4 Ensure that Enable Client Login Scan is checked.
- 5 Check **Don't Allow User To Cancel Login Scan**.

Setting command-line scan options

Vscand.exe is the program that scans Windows 3.1 and DOS client computers as they log on to the network. Vscand.exe is a DOS program that accepts command-line parameters.

When configuring a logon scan, you can check options in the File Types or File Locations group boxes, and the corresponding command-line parameter is added to the list that displays from the dialog box where you are configuring the scan. If you uncheck a box, the corresponding command-line parameter is automatically removed from the list.

Many other command-line parameters are available for Vscand.exe that are not available in check box format on the Login Scan page. You can manually add command-line parameters to the list that displays at the bottom of the Login Scan page.

For more information, see [“Configuring command-line scans”](#) on page 456.

Configuring logon scans for clients

You can scan Windows 3.1 and DOS client computers as they log on to the network. The logon scanning options for all clients that connect to the same Norton AntiVirus server are identical. You can configure logon scans at the server group level or when selecting one or more servers in the same server group.

Enabling and configuring NetWare logon scanning

To set up logon scans for Windows 3.1 and DOS clients that connect to NetWare servers:

- Use Symantec System Center to enable logon scans.
- Use NetWare Administrator (for 4.x networks) or SYSCON (for 3.2 networks) to associate users with the logon script that performs the scan. To facilitate this association, the server Setup program creates a NORTONANTIVIRUSUSER group on NetWare servers.

To enable and configure NetWare login scanning

- 1 In the Symantec System Center console, right-click a server group, multiple servers, or a server.
- 2 Click **All Tasks > Norton AntiVirus > Client Login Scan And Installation**.
- 3 Click **Login Scan**.
- 4 Ensure that Enable Client Login Scan is checked.
- 5 Change any of the logon scan options or accept the defaults.
- 6 Click **OK**.
- 7 Using your network administration tools, add each user whose computer you want scanned while logging on to the NORTONANTIVIRUSUSER group.

You can:

- Add a user to a group in NetWare 3.2.
- Add a user to a group in NetWare 4.x.

For more information, see [“Associating users with logon scripts”](#) on page 173 and [“Logon scanning options”](#) on page 336.

Enabling and configuring Windows NT/2000 logon scanning

To set, enable, and configure logon scans for Windows 3.1 and DOS clients that connect to Windows NT/2000 servers:

- Use Symantec System Center to enable logon scans.
- Use your Windows network administration tools to associate users with the script that performs the scan. To facilitate this, the server Setup program creates a netlogon share (VPLOGON) on Windows NT/2000 servers.

To enable and configure Windows NT/2000 logon scanning

- 1 In the Symantec System Center console, right-click a server group, multiple servers, or a server.
- 2 Click **All Tasks > Norton AntiVirus > Client Login Scan And Installation**.
- 3 Click **Login Scan**.
- 4 Ensure that Enable Client Login Scan is checked.
- 5 Change any of the logon scan options or accept the defaults.
For more information, see [“Logon scanning options”](#) on page 336.
- 6 Click **OK**.
- 7 Using Windows Explorer or a command prompt, copy the following two files from the Nav\Logon directory on the protected server:
 - Vplogon.bat
 - Nbpshpop.exe
- 8 Do one of the following:
 - In Windows NT, paste the files into the following directory:
C:\Winnt\System32\Repl\Import\Scripts
 - In Windows 2000, paste the files into the following directory:
C:\Winnt\Sysvol\Domain Name\Scripts
where Domain Name is the name of your domain controller.
If this share has been changed, paste the files into the custom directory that you set up as the netlogon share.

- 9 If you are installing to a Windows domain that has both a Primary Domain Controller (PDC) and a Backup Domain Controller (BDC), you must either copy and paste Vplogon.bat and Nbpshpop.exe to all PDC and BDC locations, or you must set up replication.

This prevents a file not found error when Windows authenticates to other servers.

- 10 Run User Manager in Windows NT or Active Directory Users and Computers in Windows 2000 to assign the Vplogon.bat script to each user whose computer you want scanned at logon.

For more information, see [“To assign a script to a user in Windows NT”](#) on page 341.

To assign a script to a user in Windows NT

- 1 On the Windows taskbar, click **Start > Programs > Administrative Tools > User Manager**.
- 2 In the User Manager window, double-click the Username of the user you want to receive a client logon installation.
- 3 In the User Properties dialog box, click **Profile**.
- 4 Under Login Script Name, in the User Environment Profile, type **Vplogon.bat**.
- 5 Click **OK** twice, and close the User Manager dialog box.

The logon script is added to the user's profile.

To assign a script to a user in Windows 2000

- 1 On the Windows taskbar, click **Start > Programs > Administrative Tools > Active Directory Users and Computers**.
- 2 In the console tree, click **Users**.
- 3 Double-click the name of the user you want to receive a client logon installation.
- 4 Click **Profile**.
- 5 In Logon script, type **Vplogon.bat**.
- 6 Click **OK** and close the Active Directory Users and Computers window.

The logon script is added to the user's profile.

Enabling disk cache to speed logon scans

When Windows 3.1 and DOS clients scan at logon, Vscand.exe runs on the client computers. Vscand.exe is a DOS program and may take a long time to run unless the client computer has a disk cache enabled. For example, you may need to add the following line to the Autoexec.bat of all client computers that run logon scans:

```
C:\Your_Path\Smartdrv.exe /X
```

Working with notifications, history, and events

This chapter includes the following:

- Notification mechanisms
- Viewing histories
- Viewing a history of viruses found
- Viewing a history of scans performed
- Viewing Event Log information
- Deleting histories
- How data is collected for Event Log and history views

Notification mechanisms

Symantec System Center includes the Alert Management System² (AMS²). See the *Symantec System Center Administrator's Guide* for information about using AMS² alerting. If you choose not to use AMS², the Norton AntiVirus Corporate Edition management snap-in has the following built in notification mechanisms that do not require AMS²:

- Customizable message box
- Virus histories

Customizable message box

When configuring scans, you can click an option to cause a customizable message to appear on the screen of the computer (Windows NT/2000 server, NetWare console, or client computer) where the virus was detected.

For more information about creating customized messages, see [“Displaying a warning message on an infected computer”](#) on page 297.

Virus histories

Information about detected viruses can be viewed in Virus History, which is available when you select a server group or server, then select Logs > Virus History from the Tools menu. You can view information about detected viruses for an entire server group or for a selected server within a server group. If you select a server group, Virus History lists information about viruses detected on all computers throughout the server group, including connected clients. If you select a server, Virus History lists information about viruses detected on the selected server and clients that connect to that server.

Viewing histories

From the Symantec System Center console you can centrally view virus activity and scanning on your network. You can also view histories for selected server groups, for a single server group, or for selected computers within a server group.

If you select a server group, Virus History lists information about viruses detected on all computers throughout the server group, including connected clients. If you select a server, Virus History lists information about viruses detected on the selected server and clients that connect to that server.

- **Virus History:** Lists all detected viruses for selected computers or server groups. You can select an item in the list and perform additional actions, such as Delete or Move To Quarantine. Virus History shows many details about each infection such as the name and location of the infected file, the name of the infected computer, the primary and secondary actions that were configured for the detected virus, and what action was taken on the virus.
- **Virus Sweep History:** Use Virus Sweep History to display information about previous virus sweeps for server groups.

- **Scan History:** Use Scan History to view scans that have run or are running on selected computers or server groups. Specify a time range to filter the view. For example, you might want to view only those scans that ran within the last 7 days.
- **Event Log:** Contains all other logged information that does not fall into the previous two categories. For example, the Event Log would contain messages about virus definitions file or configuration changes for specific computers.

To view the Virus History

- 1 In the Symantec System Center console, select an unlocked server group.
- 2 On the Tools menu, click **Logs > Virus History**.
For details about actions you can take when viewing virus histories, see [“Viewing a history of viruses found”](#) on page 347.

To view the Virus Sweep History

- 1 In the Symantec System Center console, select an unlocked server group.
- 2 On the Tools menu, click **Logs > Virus Sweep History**.
Virus sweeps appear by name, date, and server group.
- 3 Click **View Results** to examine the results of previous sweeps.

To run a new Virus Sweep

- 1 In the Symantec System Center console, select an unlocked server group.
- 2 On the Tools menu, click **Logs > Virus Sweep History**.
- 3 Click **New Sweep**.
- 4 Type a name for the virus sweep or accept the default name.
- 5 Click **Start**.

To view the Scan History

- 1 In the Symantec System Center console, select an unlocked server group.
- 2 On the Tools menu, click **Logs > Scan History**.
For details about actions you can take when viewing scan histories, see [“Viewing a history of scans performed”](#) on page 350.

To view the Event Log

- 1 In the Symantec System Center console, select an unlocked server group.
- 2 On the Tools menu, click **Logs > Event Log**.

Sorting columns of data

When viewing histories and event logs, sort the data from any column by clicking the column header. The ascending sort icon appears within a column header button the first time you click it. The descending sort icon appears the next time you click the column header.

Filtering items by date

When viewing the Virus History, Virus Sweep History, Scan History, and Event Log, you can filter items by date.

Norton AntiVirus Corporate Edition does not delete the information from the Virus History when you change the date range. For example, if you change the information displayed to Today, the other information will continue to exist, but it will not be displayed. You can limit the information displayed in the Virus History to:

- Today
- Past 7 days
- This month
- All items
- A selected range of days

To filter items by date

- 1 In the Symantec System Center Console, select the server group or server.
- 2 On the Tools menu, click **Logs**, then one of the following:
 - Event Log
 - Scan History
 - Virus History
 - Virus Sweep History
- 3 In the list box, click one of these options:
 - Today
 - Past 7 Days
 - This Month
 - All Items
 - Selected Range
- 4 If you clicked Selected Range, select a start date and an end date, then click **OK**.

Viewing a history of viruses found









The Virus History displays a list of viruses that have infected your computer and additional relevant information about the infections. Viewing the Virus History helps you determine which viruses have most frequently infected your computer, which types of scans have been most effective on your computer, and whether files are still infected.

You can view the virus history for a selected computer.

For details about actions you can take when viewing Virus Histories, see [“Viewing histories”](#) on page 344.

Understanding Virus History icons

In the Virus History window, you can perform several additional actions such as saving the data as a comma separated value (.CSV) file or changing the time for which Norton AntiVirus Corporate Edition shows data.

Icon	Description
	The file is infected.
	The file is not infected. The file was never infected, or it has been cleaned. See the action taken on the file for more information.
	An error occurred in association with this file.
	Closes the Virus History window.
	View item properties such as the virus name, the infected filename and path, the computer and user logged on when the scan occurred, the date the virus was found, and the action taken.
	Shows additional actions you can take on a selected item. For more information, see “Taking additional actions on items in the Virus History” on page 349.
	Saves the data shown in the Virus History window as a comma separated value (.Cvs) file.
	Displays Help for Virus History.

Taking additional actions on items in the Virus History

You can take additional actions on files displayed in the Virus History. For example, you could clean a file that is listed as infected, or delete an infected file permanently. You cannot perform additional actions on email data and only limited actions on compressed files. The following actions are available for files:

- **Undo Action Taken:** Norton AntiVirus Corporate Edition can undo the last action taken on an infected file, including removing a file from the Quarantine, and removing the .Vbn extension from a renamed file. Norton AntiVirus Corporate Edition cannot restore a file that has been permanently deleted. You cannot undo actions on compressed files.
- **Clean:** Norton AntiVirus Corporate Edition virus definitions files are frequently updated. A file that you could not clean yesterday or a few weeks ago might become cleanable when the virus definitions file is updated. You cannot perform this action on compressed files.
- **Delete Permanently:** You can permanently delete any infected file (including compressed files) that is stored in the Quarantine or Virus History. Permanently deleted files cannot be recovered.
- **Move To Quarantine:** If you determine that Norton AntiVirus Corporate Edition has left an infected file alone, it is a good idea to move the file to the Quarantine, where the virus will be unable to spread to other files on your computer. You can move compressed files to Quarantine.

To undo the action taken

- 1 Right-click the file, then click **Undo Action Taken**.
- 2 Click **Start Undo**.

To clean the infected file

- 1 Right-click the file, then click **Clean**.
- 2 Click **Start Clean**.

To delete the infected file permanently

- 1 Right-click the file, then click **Delete Permanently**.
- 2 Click **Start Delete**.

Warning: Permanently deleted files cannot be recovered.

To move the file to the Quarantine

- 1 Right-click the file, then click **Move To Quarantine**.
- 2 Click **Quarantine**.

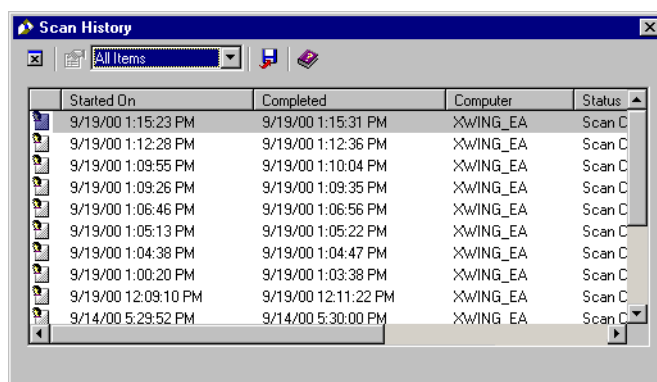
Viewing a history of scans performed

Norton AntiVirus Corporate Edition not only provides constant protection against virus invasions, it also tracks the scans that have occurred on your computer. The Scan History uses data from the Event Log to provide a complete picture of the scans performed on your computer. Scans are displayed with additional relevant information. The Scan History includes information about how frequently a computer has been scanned, which types of scans are running on a computer, and which computer is running the scans.

This data enables you to notice virus infection trends, to which you can respond with better virus detection tactics. For example, someone who uses their computer during the week for business and during the weekend to surf the Internet might notice that virus infections occur most often on Sunday night or Monday morning. In response, that person could schedule a thorough scheduled scan to occur every Monday morning at 8:00 A.M.

You can change the amount of information in the Scan History by date or save the data to comma separated value (.Csv) format, and then import it into another program.





You can view a server's scan history as shown in the dialog box below.



For details about actions you can take when viewing scan histories, see [“Viewing a history of scans performed”](#) on page 350.

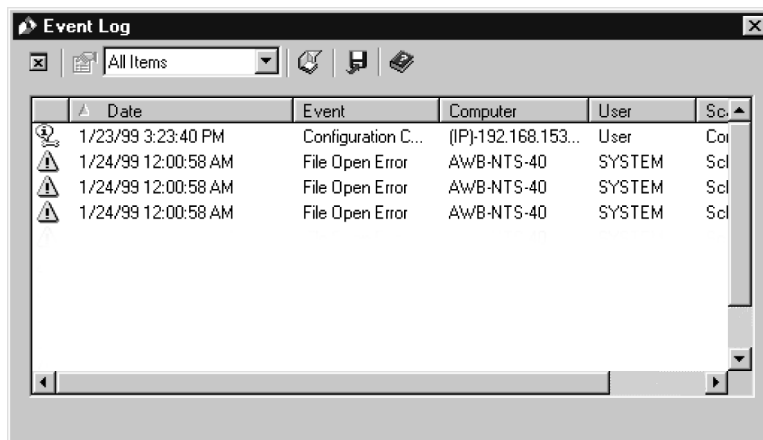
Understanding Scan History icons

In the Scan History window, you can perform several additional actions such as saving the data as a comma separated value (.Csv) file and changing the date range of data shown.

Icon	Description
	Closes the Scan History window.
	Views item properties.
	Saves the current data shown in the Scan History as a comma separated value (.Csv) file.
	Displays Help for Scan History.








Viewing Event Log information

The Event Log contains daily records of virus protection-related activities on your computer, including configuration changes, errors, and virus definitions file information. These records, called events, are displayed along with additional relevant information in a list format.



Understanding Event Log icons

In the Event Log, you can perform several additional actions such as saving the data as a comma separated value (.Csv) file and filtering the data by event type.

Icon	Description
	Describes an information event.
	Describes an error event, such as a File Open error or a File Checksum error.
	Closes the Event Log window.
	Views item properties.
	Saves the data shown in the Event Log window as a comma separated value (.Csv) file.
	Filters the Event Log by the following categories: Configuration change, Norton AntiVirus Corporate Edition startup/shutdown, Virus definitions file, Scan Omissions, Forward to Quarantine, Deliver to Symantec Security Response.
	Displays Help for the Event Log.

Using the Event Log

Norton AntiVirus Corporate Edition enables you to sort events in the Event Log by Date, Event Name, Computer, User, or Scan Type.

Information in the Event Log can also be filtered by date or by categories of events, letting you view information for a few days or for up to 999 days. Once you have displayed the information you want to view in the Event Log, you can send the information to a comma separated value (.Csv) file.

Clearing items from the Event Log

You cannot permanently remove event records from the Event Log from within Norton AntiVirus Corporate Edition. However, you can filter events by date.

To permanently delete Event Log records, delete the .log files containing the event records. Events are recorded in .log files for each day of the week in a Nav\Logs directory. These files are named according to the day they were created.

Warning: Do not permanently delete .log files as you will lose the historical virus protection data they contain.

Deleting histories

You can set options that determine the frequency with which Virus History, Scan History, and the Event Log are deleted.

To set the delete history frequency

- 1 In the Symantec System Center Console, select a server group or server.
- 2 On the Tools menu, click **Logs > Configure History**.
- 3 Select the time period after which the histories will be purged.
- 4 Click **OK**.

How data is collected for Event Log and history views

When you view a server group's Event Log, Scan History, Virus History, or Virus Sweep History, Norton AntiVirus Corporate Edition collects data from the server group's primary server. The log on the primary server contains:

- All events for the primary server
- The following event types that are forwarded from clients to parent servers:
 - Scan Start
 - Scan Stop
 - Scan Abort
 - Virus Found

The client event types are stored in the parent server Event Log as soon as they are forwarded from clients. The parent server forwards these events to the primary server immediately. (In some cases, the primary server is the parent server.)

The log on the primary server does not contain:

- Events for parent servers
- Event types that are not forwarded from clients to parent servers

If you are interested in events for parent servers or event types that are not forwarded, you will need to view logs at the server level.

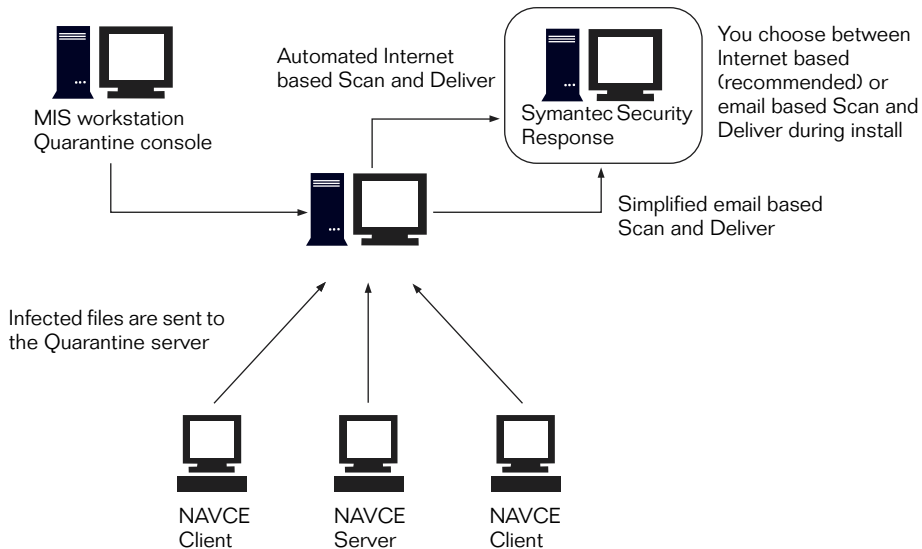
Managing virus infections

This chapter includes the following:

- Symantec Central Quarantine
- Creating a Central Quarantine
- Using Internet-based Scan and Deliver
- Using Email-based Scan and Deliver
- Responding to virus outbreaks
- Taking action on viruses
- Filtering Virus Found Alerts
- Running a virus sweep
- Using the Norton AntiVirus Rescue Disk set to recover from a boot sector infection

Note: You must install Quarantine Server and Quarantine Console before you can use Central Quarantine. For system requirements and installation instructions, see the *Symantec System Center Implementation Guide*.

Symantec Central Quarantine



By default, Symantec and Norton AntiVirus products are configured to isolate infected items that cannot be repaired with their current sets of virus definitions. These items are forwarded to the Central Quarantine.

From the Central Quarantine, the infected samples are submitted to Symantec Security Response (formerly known as Symantec AntiVirus Research Center) for analysis. One of two transport technologies selected at install is used to submit samples:

- Internet-based Scan and Deliver: An automated virus sample submission and definition delivery system that provides realtime protection against heuristically detected new viruses.
- Email-based Scan and Deliver: A virus sample submission and virus definitions delivery system that includes the Scan and Deliver Wizard to simplify sending items to Symantec Security Response for analysis. If a new virus is found, updated virus definitions are returned by email.

Symantec Security Response

Symantec Security Response is committed to providing swift, global responses to computer virus threats, proactively researching and developing technologies that eliminate such threats, and educating the public on safe computing practices.

At Symantec Security Response, a team of virus experts develops identification and detection technology to find and eliminate computer viruses. Aiding the researchers is Symantec AntiVirus Research Automation (SARA). With SARA, a high percentage of virus sample submissions can be analyzed automatically. The virus definitions to remove the viruses are created and distributed to customers without human intervention. This technology stops newly discovered viruses before they can spread.

Creating a Central Quarantine

The Central Quarantine has two components:

- Quarantine Server that is installed on any Windows NT/2000 computer to store infected samples and communicate with Symantec Security Response
- Quarantine Console that snaps into MMC to perform management tasks

To use the Central Quarantine:

- Enable the Quarantine Server.
- Configure server and client forwarding to the Quarantine Server.
- Configure Scan and Deliver to transport samples to Symantec Security Response and receive virus definitions updates.

Email-based Scan and Deliver or Internet-based Scan and Deliver is selected during the Quarantine Server install. To change from one to the other, reinstall the Quarantine Server.

Enabling the Central Quarantine

Configure the Quarantine Server to act as a centralized repository for infected files that could not be repaired on client computers. Then, configure clients to forward copies of the files contained in their local Quarantines.

For more information on configuring forwarding copies of quarantined files, see [“Configuring client forwarding to the Quarantine Server”](#) on page 359.

Note: If you are selecting Symantec Central Quarantine for the first time, follow the procedure in [“To select an initial Quarantine Server to manage”](#) on page 358. If you have already attached to a Quarantine server, follow the instructions in [“To change the Quarantine Server to which Central Quarantine attaches”](#) on page 358.

To select an initial Quarantine Server to manage

- 1 In the left pane, click **Symantec Central Quarantine**. If you are opening Symantec Central Quarantine for the first time, you are prompted to attach to This Computer or Another Computer.
- 2 Do one of the following:
 - To use the local computer as the Quarantine Server, click **This Computer**. The word Local is displayed at the end of Symantec Central Quarantine.
 - To use another computer as the Quarantine Server, click **Another Computer**. Type the server name or click **Browse** to locate the computer. Type the username and password for the computer and the domain name, if part of a domain.

To change the Quarantine Server to which Central Quarantine attaches

- 1 In the left pane, right-click **Symantec Central Quarantine** and click **Attach to server**.
- 2 Do one of the following:
 - To attach to the local computer, type the server name and click **OK**.
 - To attach to another Quarantine Server, type the server name, enter the username and password to log on to the server, and enter the domain name, if part of a domain.

Configuring client forwarding to the Quarantine Server

Two types of Central Quarantine clients can forward virus samples to the Quarantine Server:

- Managed, such as Norton AntiVirus Corporate Edition clients and servers managed with Symantec System Center
- Nonmanaged, such as Norton AntiVirus for Microsoft Exchange, Norton AntiVirus for Gateways, or Norton AntiVirus for Lotus Notes

A key difference between the two types of clients is how virus definitions updates are returned. Under Email-based Scan and Deliver, virus definitions updates are returned by email for all specified platforms and applied under administrator control.

Under Internet-based Scan and Deliver, virus definitions updates are returned and installed automatically only on computers that are running a managed product. For nonmanaged products, administrators must download and apply updated virus definitions when notified.

For more information about Internet-based Scan and Deliver virus definitions updates, see [“Managed and nonmanaged products”](#) on page 366.

To configure managed clients to forward to the Quarantine Server

- 1 Right-click clients, servers, or server groups in the Symantec System Center and click **All Tasks > Norton AntiVirus > Quarantine Options**.

- 2 Click **Enable Quarantine or Scan And Deliver**.

- 3 Click **Allow Forwarding To Quarantine Server**.

By selecting forwarding, clients cannot submit items directly to Symantec Security Response from the Quarantine on the client.

- 4 Under Server Name, enter the server name, IP address, or SPX address of the Quarantine Server.

- 5 Enter the port and protocol specified when setting the Quarantine Server properties.

See [“Configuring the Quarantine Server”](#) on page 361 for Internet-based Scan and Deliver. See [“Configuring the Quarantine Server”](#) on page 374 for Email-based Scan and Deliver.

- 6 Select an automatic operation to run on the client Quarantine when virus definitions updates arrive.

To configure nonmanaged products to forward to the Quarantine Server

- 1 Locate the Quarantine Forwarding settings of the product.
Refer to the documentation or online help of the product.
- 2 Enter the server name or IP address where the Quarantine Server is running.
- 3 Enter the port and protocol specified when setting the Quarantine Server properties.
- 4 Enter the **Retry** interval in seconds.

See [“Configuring the Quarantine Server”](#) on page 361 for Internet-based Scan and Deliver. See [“Configuring the Quarantine Server”](#) on page 374 for Email-based Scan and Deliver.

Using Internet-based Scan and Deliver

Internet-based Scan and Deliver is an automated virus sample submission and definition delivery system that provides realtime protection against heuristically detected new viruses. All computers worldwide that run Symantec and Norton AntiVirus products are connected to Symantec Security Response.

Samples of files or boot sectors that might be infected with a new virus are captured on protected computers and sent through the network to the analysis center, which collects and automatically analyzes the samples. If a new virus is found, the center produces and returns new virus definitions, the signatures used to detect, verify, and remove the virus.

New definitions are packaged as updates to Symantec and Norton AntiVirus products and distributed immediately to any customer that reports the new virus. The signatures are later distributed to all other customers to prevent the new virus from spreading further.

Configuring Internet-based Scan and Deliver

Internet-based Scan and Deliver requires two items of information for Central Quarantine operation:

- The folder location to store files on the Quarantine Server
- The appropriate protocols for your network and the port on which to listen

Other settings, including Web communication, sample submission policy, and definition return policy, have default settings carried from install that may be appropriate without modification.

Configuring the Quarantine Server

The Quarantine Server receives virus samples from computers running Symantec and Norton AntiVirus products. The Quarantine Server is the centralized repository for infected files that could not be repaired on client machines. After the Quarantine Server is configured, configure clients to send copies of the files contained in their local Quarantines.

For more information on configuring clients to forward copies of quarantined files, see [“Configuring client forwarding to the Quarantine Server”](#) on page 359.

To configure the Quarantine Server

- 1 In the left pane, right-click **Symantec Central Quarantine** and click **Properties**.
- 2 On the General tab, enter the folder location for the Central Quarantine.
- 3 Specify the maximum size for the Quarantine.
- 4 Select the appropriate protocols for your network and specify the port on which to listen.

Do not use another application's reserved port. Generally, ports over 1025 are not reserved.

Communicating with the gateway

Web Communication settings determine how the Central Quarantine communicates with the gateway to the Symantec Security Response analysis center. Generally, the default gateway is supplied when the Quarantine Server is installed.

The sample submission and definitions return transactions can be secured over the Web using Secure Socket Layer (SSL) encryption technology. The encryption level (40-bit or 128-bit) is determined by the version of Internet Explorer installed on the Quarantine Server computer.

To specify Web Communication settings

- 1 In the left pane, right-click **Symantec Central Quarantine** and click **Properties**.
- 2 On the Web Communication tab, specify settings:
 - Name: Gateway computer that communicates with the analysis center
 - Secure submission: Check to use SSL for submissions
 - Secure download: Check to use SSL for returned virus definitions

Specifying an HTTP firewall proxy

Many sites install the Central Quarantine behind a proxy firewall. Because all transactions with the analysis center gateway are sent by HTTP and secured by SSL, they must be authenticated. To enable communication between the Central Quarantine and the gateway, supply a user name and password for the firewall proxy, as well as its address and port.

To specify the HTTP firewall proxy

- 1 In the left pane, right-click **Symantec Central Quarantine** and click **Properties**.
- 2 On the Firewall tab, enter the firewall proxy information:
 - Firewall name: IP address or name of the firewall
 - Firewall port: Port on which to communicate with the firewall
 - Firewall User name: User name
 - Firewall password: Password

Setting a sample submission policy

Sample Policy settings determine whether or not virus samples are submitted automatically to the gateway. If automatic sample submission is not selected, samples in the Quarantine must be released to the gateway individually.

For additional security, specify that user data be stripped from samples before submission.

Policy submission settings can be superseded on an item-by-item basis when viewing the Actions tab for a selected item in the Quarantine.

To set sample policy

- 1 In the left pane, right-click **Symantec Central Quarantine** and click **Properties**.
- 2 On the Sample Policy tab, set sample policy:
 - Automatic sample submission: If checked, virus samples are automatically queued for analysis
 - Queue check interval: Frequency at which the Quarantine is checked for new items
 - Strip user data from sample: For data security, only the virus portion of the infected file is sent to the gateway
 - Status query interval: Frequency at which the gateway is polled for status changes about submitted samples

Entering Customer Information

Customer Information is included in all messages (virus samples) from customers to gateways. It identifies the customer making the request and is used for authorization and tracking. The information is entered at install, but can be modified if necessary.

To specify Customer Information

- 1 In the left pane, right-click **Symantec Central Quarantine** and click **Properties**.
- 2 On the Customer Information tab, specify customer information:
 - Company name: Name of company
 - Account number: Symantec support plan account number
 - Contact name: Administrator contact at company
 - Contact telephone: Telephone number with area code
 - Contact email: Required should correspondence be necessary

Managing virus definitions updates

Symantec Security Response provides both certified and noncertified virus definitions files.

Once a virus definition has been tested and certified, it is added to standard virus definitions set. Noncertified virus definitions are automatically generated and downloaded by the analysis center in response to a newly discovered virus, according to the installing definitions policy.

To manage virus definitions updates, set the following policies:

- Definition Policy: How frequently the Central Quarantine polls the Symantec Security Response gateway for updated, certified virus definitions
- Install Definitions: Which computers receive certified or noncertified virus definitions automatically in response to newly discovered viruses from sample submissions

Virus definitions updates for nonmanaged clients must be downloaded manually.

Setting Definition Policy

Definition Policy determines how frequently the gateway is polled to download updated certified virus definitions. Certified virus definitions are tested by the analysis center before general release.

To set Definition Policy

- 1 In the left pane, right-click **Symantec Central Quarantine** and click **Properties**.
- 2 On the Definition Policy tab, set definition policy:
 - Active sequence number: The sequence number of the currently installed definitions on the Quarantine Server. Definitions can be certified or noncertified.
 - Certified definitions interval: In minutes, how frequently the gateway is polled for updated certified definitions. The default setting is once per day.

Installing definitions

Install Definitions policy determines which computers receive updated virus definitions automatically in response to virus detections.

Separate policies can be set for certified and noncertified virus definitions. Certified virus definitions are tested by the analysis center before distribution. Noncertified virus definitions are automatically generated by the analysis center in response to a newly discovered virus.

If virus definitions are delivered for a virus detected on a computer that is not selected to receive virus definitions automatically, you can manually queue the computer for virus definitions delivery.

To set Install Definitions policy

- 1 In the left pane, right-click **Symantec Central Quarantine** and click **Properties**.
- 2 On the Install Definitions tab, set the Install Definitions policy:
 - Certified definitions
 - Install on selected targets: If checked, certified virus definitions are automatically installed on the selected servers. Click **Select** to specify the servers.
 - Definitions that are not yet certified
 - Install on infected clients: If checked, noncertified virus definitions are automatically installed on the computers on which the virus was detected.
 - Install on servers of infected clients: If checked, noncertified virus definitions are installed on the parent server of the infected client.
 - Install on selected servers: If checked, noncertified virus definitions are automatically installed on the selected servers. Click **Select** to specify the servers.
 - Delivery
 - Retry interval: In minutes, how frequently virus definitions updates are attempted when targets are disconnected.

To manually queue a computer for definitions delivery

- 1 In the right pane, right-click a quarantined item and click **Properties**.
- 2 On the Actions tab, click **Queue item for definition delivery**. If the item is not eligible for a definitions update, the Queue item for definition delivery button is not available.

Managed and nonmanaged products

Two types of Central Quarantine clients can forward items to the Quarantine Server:

- Managed, such as Norton AntiVirus Corporate Edition clients managed with Symantec System Center
- Nonmanaged, such as Norton AntiVirus for Microsoft Exchange, Norton AntiVirus for Gateways, or Norton AntiVirus for Lotus Notes

The key difference between the two is how virus definitions updates are returned. Virus definitions updates can be installed automatically only on computers that are running a managed product.

Nonmanaged products must be updated manually when virus definitions are created in response to a newly discovered virus. For these products, an alert is generated that contains the location of FTP sites from which to download the virus definitions.

If a nonmanaged product runs under Windows NT/2000, you can install a managed version of Norton AntiVirus Corporate Edition on the same computer. Since both Central Quarantine clients share the same set of virus definitions, the nonmanaged product can forward infected items to the Central Quarantine and the managed product will receive the virus definitions update.

When definitions are available for nonmanaged products, a “Cannot install definitions on target machines” alert is generated. The alert includes the locations of FTP sites from which to download the definitions.

To locate updated virus definitions for nonmanaged products

- 1 Right-click the infected item in the Quarantine and click **Properties**.
- 2 On the Errors tab, note the FTP sites from which to download updated definitions.

To configure an alert that includes FTP locations

- 1 Right-click **Symantec Central Quarantine** and click **Properties**.
- 2 On the Alerting tab, configure to send events to AMS² or Write to Event Log alert for the Cannot install definitions on target machines event.
An event is sent to AMS² or an entry is written to the NT event log, respectively.

Reviewing sample submission status

A sample's status within the system can be determined by reviewing the actions performed and attributes set during communications between the Quarantine Server and the gateway.

Viewing a list of quarantined items

Files are added to the Central Quarantine when client machines are configured to forward infected items to the Quarantine Server. The status entry in the table reports the processing state of the sample within the system.

Status	Meaning
Quarantined	Sample has been received by the Central Quarantine.
Submitted	Sample has been submitted to Symantec Security Response for analysis.
Released	Sample has been queued for analysis.
Held	Sample is withheld from submission.
Unneeded	New virus definitions are not required for the sample.
Needed	New virus definitions are required for the sample.
Available	New virus definitions are held for delivery to the submitting computer.
Distribute	New virus definitions are queued for delivery to the submitting computer.
Distributed	New virus definitions have been delivered to the submitting computer.
Installed	New virus definitions have been installed on the submitting computer.
Attention	Sample requires intervention from technical support.
Error	Processing error occurred.
Not installed	Virus definitions could not be delivered to the submitting computer.
Restart	Sample processing will begin again.

To view a list of quarantined items

- In the left pane, click **Symantec Central Quarantine**.
Quarantined items are listed in the right pane.

To get detailed information about a quarantined item

- Right-click an item in the Quarantine and click **Properties**.

Interpreting attributes of submissions

Request and response messages exchanged between clients and servers contain numerous attributes that describe a sample and its status within the system. These proprietary attributes always start with the X- characters.

To view attributes for a sample

- 1 In the left pane, right-click **Symantec Central Quarantine**.
- 2 In the right pane, right-click an item and click **Properties**.
- 3 On the Sample Attributes tab, double-click a displayed attribute for a brief definition.

Reviewing actions on samples

The actions taken on a sample include a selected sample's submission and virus definition delivery status.

You can override the default sample submission policy settings for the selected sample. You can manually queue a sample for submission to the analysis center, as well as query for updated virus definitions files for the selected sample.

To view sample actions

- 1 In the left pane, click **Symantec Central Quarantine**.
- 2 In the right pane, right-click a quarantined item and click **Properties**.
- 3 On the Actions tab, review actions taken on the sample.

Reviewing submission errors

Submission errors, if any, are reported for each sample. Review the entries to determine the action required for the sample.

To review submission errors

- 1 In the left pane, right-click **Symantec Central Quarantine**.
- 2 In the right pane, right-click an item and click **Properties**.
- 3 On the Errors tab, review submission errors.

Overriding automatic operation

Policy settings for automatic sample submission and virus definitions install can be overridden.

Generally, samples are submitted manually only after a submission error or a change to the queue priority of selected samples is desired. Similarly, if virus definitions are available for a computer that is not selected to receive virus definitions automatically, you can manually queue the computer for virus definitions delivery.

Submitting files manually

Suspect files can be manually submitted for virus analysis. To be eligible for manual submission:

- The sample cannot already be eligible for automatic submission. The X-Sample-Priority must be 0.
- To manually set the priority for a sample, right-click an item in the Quarantine, click Properties, and set the Submission priority on the Actions tab.
- The sample has not been submitted (X-Date-Submitted is missing or 0).
- The sample has not been analyzed (X-Date-Analysis-Finished is not present or 0).

To manually submit items to the analysis center

- 1 In the Quarantine, select one or more files.
- 2 Right-click the selection and choose **All Tasks > Queue item for automatic analysis**.

Requesting virus definitions updates manually

A target machine that does not receive virus definitions updates automatically can be queued for delivery of new virus definitions. For these machines, the sample status is Available. To be eligible for manual definitions delivery:

- The sample cannot already be eligible for automatic delivery of virus definitions (X-Signatures-Priority is 0).
- The sample requires virus definitions (X-Signatures-Sequence > 0).
- The sample has not yet been disinfected (X-Date-Sample-Finished is missing or 0).

To request virus definitions updates

- 1 In the Quarantine, select one or more files.
- 2 Right-click and choose **All Tasks > Queue for automatic delivery of new definitions**.

Sending alerts

In addition to entries in the Quarantine Log, alerts triggered by Central Quarantine events can be sent in the following ways:

- Message box
- Page
- Email
- Run program and send SNMP trap
- Broadcast
- Written to NT event log

For nonmanaged clients that do not receive virus definitions updates automatically, the “Cannot install definitions on target machines” alert is generated. The alert is posted automatically to the Error tab of the infected item with the locations of FTP sites to download the definitions and the Quarantine Log. If enabled, the Send Internet Mail and Write to Event Log alerts also include this information.

Configuring alerting

Alerting settings determine the events at the Quarantine that trigger alerts and where to send them. Each event can be enabled or disabled individually.

Event	Meaning
Unable to connect to the gateway	Cannot connect to the Immune System gateway.
Defcast error	Defcast is the service that distributes new virus definitions from the Quarantine Server to target machines.
Cannot install definitions on target machines	Distribution of new virus definitions failed. Also indicates that virus definitions are available for nonmanaged clients.
Unable to access definition directory	Quarantine Server cannot find the virus definitions directory.
Cannot connect to Quarantine Scanner svc	Samples cannot be scanned in the Quarantine and will not be forwarded to the gateway.
The Quarantine Agent service has stopped	Quarantine will not be able to communicate with the gateway.
Waiting for needed definitions	Virus definitions have not yet arrived from the gateway.
New Certified definitions arrived	New certified virus definitions have arrived on the Quarantine Server.
New non-certified definitions arrived	New noncertified virus definitions have arrived on the Quarantine Server in response to a sample submission.
Disk quota remaining is low for Quarantine dir	The Quarantine folder is becoming full.
Disk free space is less than Quarantine max size	The Quarantine folder is set to a maximum size greater than the available free disk space.
Sample: was not repaired	Either a sample wasn't repaired or a repair wasn't necessary.

Event	Meaning
Sample: unable to install definitions	New virus definitions could not be installed, usually due to a corrupted virus definitions set.
Sample: processing error	There was an error processing this sample.
Sample: needs attention from Tech Support	Sample could not be processed automatically. Contact Tech Support for help with the sample.
Sample: held for manual submission	Sample is being held on the Quarantine Server instead of being automatically submitted.
Sample: too long without installing new defs	New virus definitions should have been installed (status is available), but were not.
Sample: too long with Distributed Status	New virus definitions have arrived from the gateway, but confirmation that they were installed on the client has not yet been received at the Quarantine.
Sample: too long with Needed status	Virus definitions have not yet been pulled from the gateway.
Sample: too long with Released status	Gateway has not yet responded.
Sample: too long with Submitted status	Sample has not yet been accepted by the gateway.
Sample: too long with Quarantined status	Sample has not yet been scanned initially at the Quarantine.
Sample: new definitions held for delivery	New virus definitions are being held on the Quarantine Server instead of being delivered.

After identifying the AMS² server, specify who receives the alert for each event. After the recipients are configured, each event can be enabled or disabled separately on the Alerting tab.

To configure alerting

- 1 In the left pane, right-click **Symantec Central Quarantine** and click **Properties**.
- 2 On the Alerting tab, configure alerts.

To specify who receives an alert and by what method

- 1 On the Alerting tab, click **Configure**.
- 2 Select an event and click **Configure**.
- 3 Click **Help** on each panel of the wizard for more information.

Using Email-based Scan and Deliver

Email-based Scan and Deliver is a virus sample submission and virus definitions delivery system that protects against heuristically detected new viruses. It includes the Scan and Deliver Wizard to simplify sending items to Symantec Security Response for analysis.

If a new virus is found, updated virus definitions are returned by email, where they can be applied first in the Central Quarantine to test and confirm operation. The updated virus definitions are then applied to clients and servers throughout the network.

Configuring Email-based Scan and Deliver

Email-based Scan and Deliver requires two items of information for Central Quarantine operation:

- The folder location to store files on the Quarantine Server
- The appropriate protocols for your network and the port on which to listen

Configuring the Quarantine Server

Configure the Quarantine Server as a centralized repository for infected files that could not be repaired on client computers. Once this is done, you can configure clients to send copies of the files contained in their local Quarantines.

For more information on configuring clients to forward copies of quarantined files, see [“Configuring client forwarding to the Quarantine Server”](#) on page 359.

To configure the Quarantine Server

- 1 Right-click **Symantec Central Quarantine** and click **Properties**.
- 2 On the General tab, enter the Quarantine folder location.
- 3 Specify the maximum size for the Quarantine.
- 4 Select the appropriate protocols for your network and specify the port on which to listen.

Do not use another application's reserved port. Generally, ports over 1025 are not reserved.

Submitting files for analysis

Quarantine includes the Scan and Deliver Wizard to simplify sending items to Symantec Security Response for analysis. Your personal data can be stripped from the file copies that are sent to Symantec Security Response to ensure privacy.

Once you receive the virus definitions update by email you can apply it in the Central Quarantine to test and confirm its effectiveness. Next, apply the update to the client computer (where the original infected file remains quarantined). The client computer then performs a selected preset operation such as repairing the infected item and releasing it from the client Quarantine automatically.

Sending files to Symantec Security Response

The Scan And Deliver Wizard simplifies sending items to Symantec Security Response for analysis. Scan and Deliver emails the virus strain to Symantec for analysis and immediate virus definition creation.

When you click Submit Item, the Scan And Deliver Wizard analyzes the file and may recommend an action other than delivering it to Symantec Security Response. For example, the virus might be eliminated with your current set of virus definitions. You can override the recommended action and submit it.

You must have an Internet connection and an email address to submit files to Symantec Security Response.

To submit a file to Symantec Security Response

- 1 Open the Symantec Central Quarantine.
- 2 Right-click a file in the list of Quarantined items and click **Submit Item to SARC**.
- 3 Follow the directions in the Scan And Deliver Wizard to collect information and submit the file to Symantec Security Response for analysis.
- 4 When the wizard runs, there are two settings to cover special circumstances:
 - Strip File Content: If selected, only the portion of a file that can be infected is sent to Symantec Security Response. Any confidential data is stripped from the document before it is submitted. The complete file remains in Quarantine.
 - Specify Custom SMTP Server: This setting applies to corporate environments to route items from Quarantine to Symantec Security Response through your custom SMTP server.

Managing quarantined files

By default, Symantec and Norton AntiVirus clients are configured to isolate infected items that cannot be repaired with their current sets of virus definitions. Clients that have been configured to forward these infected files automatically send copies to the Central Quarantine Server.

Once the files are in the Central Quarantine, the following administrative actions are possible:

- View a list of quarantined files
- Repair files
- Restore files
- Delete files
- Submit files to Symantec Security Response for analysis

Viewing a list of quarantined items

Files are added to the Central Quarantine when client computers are configured to forward infected items to the Central Quarantine. You can view a list of the files contained in the Quarantine Server.

To view a list of quarantined items

- In the left pane, click **Symantec Central Quarantine**.

To get detailed information about a quarantined item

- In the right pane, right-click an item and click **Properties**.

Deleting quarantined files

Although you can delete any item in the Central Quarantine, reserve this option for files you no longer need. After confirming that updated virus definitions detect and eliminate the virus, it is safe to delete the quarantined item.

To delete files

- 1 In the left pane, click **Symantec Central Quarantine**.
- 2 In the right pane, select one or more files in the list of quarantined items.
- 3 Right-click the selection and click **Delete**.

Repairing and restoring quarantined files

When you click Restore, no attempt is made to repair the file. Use this option with discretion to avoid infecting your system. For example, only use Restore when Symantec Security Response notifies you that a submitted file is not infected. Restoring a potentially infected file is not safe. Restored files are copied to the Quarantine Console computer.

When you click Repair, an attempt is made to repair the file. You are prompted for a location to store a successful repair. With new virus definitions, you can test the repair in the Central Quarantine before distributing the definitions.

To repair an infected file

- 1 In the left pane, click **Symantec Central Quarantine**.
- 2 In the right pane, select one or more files in the list of quarantined items.
- 3 Right-click the selection and click **Repair**.

Updating Central Quarantine virus definitions

Because the Quarantine itself performs virus scanning and repairs, you must have current virus definitions. For Email-based Scan and Deliver, the virus definitions reside on the computer where the Quarantine Console is installed.

If Symantec Security Response returns updated virus definitions by email in response to a submitted virus sample, apply them to the computer where the Quarantine Console is installed. For Email-based Scan and Deliver, you can test the updated virus definitions in the Central Quarantine before applying them to other supported Symantec and Norton AntiVirus products.

If a client version of Norton AntiVirus is installed on the same computer as the Quarantine Console computer, the client version of LiveUpdate will update the Quarantine as well. If not, you must manually apply updated virus definitions.

Symantec supplies updated virus definitions on the Symantec Security Response Web site.

To download updated virus definitions

- 1 Go to the Symantec Security Response Web site:
<http://securityresponse.symantec.com>
- 2 Click **Definition Updates**.
- 3 Click **Download Virus Definition Updates**.
- 4 Select the virus definitions update for Norton AntiVirus Corporate Edition.

To manually install the latest virus definitions

- 1 Do one of the following:
 - Detach the virus definitions package emailed from Symantec Security Response and copy it to any folder on the Quarantine Console computer.
 - Download the virus definitions update and copy it to any folder on the Quarantine Console computer.
- 2 From a My Computer or Windows Explorer window, locate and double-click the virus definitions update.
- 3 Follow all prompts displayed by the update program.
The update is installed in the proper folder automatically.

Testing the virus definitions update

You should test the virus definitions update.

To test updated virus definitions files

- 1 In the list of Quarantined items, select one or more files.
- 2 Right-click the selection and click **All Tasks > Repair Item**.

After you've confirmed that the new virus definitions eliminate the viruses from files in the Quarantine, apply the definitions to other supported Symantec and Norton AntiVirus products. The same package can be used for Windows NT clients. Additional packages are sent in appropriate formats for other platforms that were specified at the time of submission to Symantec Security Response. For example, script packages are returned for the Solaris platform.

Responding to virus outbreaks

Norton AntiVirus Corporate Edition can notify you of a virus problem in several ways.

Alert Management System

Symantec System Center ships with a snap-in notification system called Alert Management System² (AMS²). When a virus problem occurs, AMS² can send alerts through a pager, an email, and other means.

For more information, see the *Symantec System Center Implementation Guide*.

Built-in notification

Norton AntiVirus also has built-in notification capabilities that can be used instead of or in addition to the AMS² notification.

Built-in notification, which does not require AMS², includes:

- Customizable message box
- Virus histories

Customizable message box

When configuring manual, scheduled, or realtime scans for your file system, you can cause a customizable message to appear on the screen of the computer where the virus was detected.

For more information, see [“Displaying a warning message on an infected computer”](#) on page 297.

When configuring realtime scan options for email data, you can insert a warning into an email message.


For more information, see [“Notifying others about the receipt of an infected attachment”](#) on page 300.

Virus histories

Information about detected viruses can be viewed in Virus History, which is available when you select a server group, server, or client, then select Norton AntiVirus > Virus History from the Tools menu. Information about detected viruses can be viewed for an entire server group, a selected server within a server group, or a selected client. If you select a server group, Virus History lists information about viruses detected on all computers throughout the server group, including connected clients. If you select a server, Virus History lists information about viruses detected on the selected server and all clients that connect to that server.

For more information on viewing virus histories, see [“Viewing histories”](#) on page 344.

Warning icon in Symantec System Center Console

This warning icon  is imposed on a server group icon if a virus is found on one or more servers or clients within the server group. (This same icon appears when other issues need to be resolved in a server group.)

To find the specific computer or computers with the virus, expand the server group and servers as necessary and look for “Virus Found!” in the status column for any infected server or workstation.

After fixing the problem, remove the warning icon.

To remove the warning icon

- From the Symantec System Center Console, right-click the affected computers, then click **All Tasks > Norton AntiVirus > Clear Virus Status**.

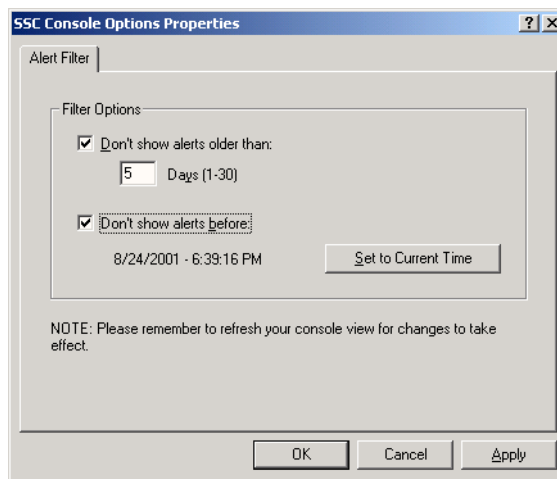
Filtering Virus Found alerts

From the Symantec System Center console, you can filter the Virus Found alerts that appear when servers or workstations become infected. By default, Virus Found alerts appear for the past three days.

You can change the number of days for which Virus Found alerts appear.

To change the number of days for which Virus Found alerts appear

- 1 From the Symantec System Center console Tools menu, click **SSC Console Options**.



- 2 Make sure the **Don't Show Alerts Older Than box is checked**.
- 3 Type the number of days for which you want to see Virus Found alerts.

The minimum is 1 and the maximum is 30.

- 4 Click OK.

You will need to refresh the console before the change takes effect.

You can filter all Virus Found alerts up to the current date and time.

To filter all Virus Found alerts up to the current date and time

- 1 From the Symantec System Center console Tools menu, click **SSC Console Options**.
- 2 Make sure the **Don't Show Alerts Before box is checked**.
- 3 Click **Set To Current Time**.
- 4 Click **OK**.

You will need to refresh the console before the change takes effect.

Taking action on viruses

Using Symantec System Center to configure scans for servers and for 16-bit and 32-bit clients, you can specify an action (and a backup action in case your first choice is not possible) that Norton AntiVirus will take on any viruses that it detects during the scan. You can specify a separate action for each type of scan.

For more information, see [“Scanning for viruses”](#) on page 289.

Use command-line options to clean files if you run scans on DOS-only computers.

The following actions are available for detected viruses:

- Clean Virus From File: Norton AntiVirus attempts to clean an infected file as soon as it is detected.
- Quarantine Infected File: Norton AntiVirus attempts to move the infected file to the Quarantine on the infected computer as soon as it is detected. After an infected file is moved to the Quarantine, no user can execute it until you take an action (for example, clean or delete) and move the file back to its original location.
- Delete Infected file: Norton AntiVirus attempts to delete an infected file as soon as it is detected.
- Leave Alone (Log Only): Norton AntiVirus notifies you of the virus and logs the event but does not perform any other action.

Running a virus sweep

If you discover several viruses, you might not know if the problem is localized to the computer or server where the viruses were detected or if the problem has spread to other areas of the network. You might want to begin a virus sweep using Symantec System Center.

The number of computers that you scan depends on how you start the sweep.

To sweep your entire system

- On the Symantec System Center Console, right-click **System Hierarchy**, then click **All Tasks** > **Norton AntiVirus** > **Start Virus Sweep**.

Norton AntiVirus then scans all servers and connected client computers in all server groups.

To sweep a server group

- On the Symantec System Center Console, right-click the server group, then click **All Tasks** > **Norton AntiVirus** > **Start Virus Sweep**.

Norton AntiVirus then scans all servers and connected client computers in the server group.

To sweep a server

- On the Symantec System Center Console, right-click the server, then click **All Tasks** > **Norton AntiVirus** > **Start Virus Sweep**.

Norton AntiVirus then scans the selected server and all client computers that connect to that server.

Note: A virus sweep can create considerable network traffic, the amount and duration of which depend upon the size of your network. Once you start a virus sweep it must complete; you cannot stop it.

What if a client computer is turned off during the virus sweep?

If a client computer is turned off during a virus sweep, Norton AntiVirus scans it in this way:

- 32-bit computers: Norton AntiVirus scans the computer as soon as it is turned on. The computer does not have to log on to the network.
- 16-bit computers: Norton AntiVirus scans the computer as soon as it is turned on and logged on to the network.

Using the Norton AntiVirus Rescue Disk set to recover from a boot sector infection

If you suspect your computer has been damaged by a boot sector virus (because you are unable to start your computer), you can use the Norton AntiVirus Rescue Disk set to clean the virus or restore the boot sector of your computer's drive.

To learn more about responding to infected floppy disks, see [“What if my floppy disks become infected by a boot virus?”](#) on page 387.

For information about creating the Norton AntiVirus Rescue Disk set, see [“Creating a Norton AntiVirus Rescue Disk set”](#) on page 188.

Cleaning the virus

Attempt to scan and clean the boot sector virus from the computer. Cleaning removes the virus from the computer's boot sector and partition tables. To clean an infected boot sector, use the Norton AntiVirus Rescue Boot Disk to start your computer, then follow the instructions on the screen.

To clean a boot virus

- 1 Turn off the computer for 15 seconds, then insert the Norton AntiVirus Rescue Boot Disk into the floppy disk drive.
- 2 Restart the computer.
After the computer has started, instructions appear and the prompt displays (A:\>).
- 3 Remove the Norton AntiVirus Rescue Boot Disk from the floppy drive, then insert the Norton AntiVirus Program Disk.
- 4 Type **Go**.
- 5 Press **Enter**.
- 6 Follow the on-screen instructions to clean the virus or leave it alone.
- 7 If the boot sector was successfully cleaned, remove the disk then restart the computer without any disks.

What if the boot virus could not be cleaned?

If Norton AntiVirus is unable to clean a boot virus with the NAVDX utility, remove the virus by replacing the infected boot sector with a clean copy of the boot sector stored on the Norton AntiVirus Emergency Disk.

Warning: Do not use another computer's Norton AntiVirus Emergency Disk for this procedure. Each disk contains unique information about that computer's boot sector.

Restoring the computer's boot sector

Some boot viruses cannot be cleaned. If this is the case, attempt to restore the boot sector using the Norton Emergency disk. The disk replaces the infected boot sector with a clean, uninfected version of the boot sector stored on the Norton Emergency disk. This process destroys the virus and prevents it from spreading.

To restore an infected computer's boot sector

- 1 Turn off the computer for 15 seconds, then insert the Norton Emergency disk and restart the computer.
- 2 After the computer has booted and you are at the A: prompt, type **Rescue**.
- 3 Press **Enter**.
- 4 Press the Tab key until the cursor appears in **Boot Records**, then press the spacebar to select the option.
- 5 Press the Tab key to move the cursor to **Partition Tables**, then press the spacebar to select the option.
- 6 Press the Tab key to select **Restore**, then press **Enter**.
- 7 Follow the prompts.

The Norton Emergency program will copy the uninfected boot sector and partition table from the Norton Emergency disk onto the computer. This process overwrites the virus and keeps it from spreading.

What if my floppy disks become infected by a boot virus?

Boot viruses damage computers by making them unable to start. When you cannot start a computer, you cannot access your files and applications. Boot viruses can copy themselves onto the boot sectors of floppy disks, then transfer from the floppy disk to a computer.

Usually, boot viruses infect the boot sector of a floppy disk, but do not infect the files stored on that disk.

Although your files may not be harmed, an infected floppy disk is a threat to the well-being of your computer. To avoid spreading a boot virus from a floppy disk to your computer's boot sector and partition tables, enable file system realtime protection and copy the files from the infected floppy disk to a disk that is not infected, then throw away the infected disk.

Scan the files on the new floppy disk to ensure that it has not become infected.

3

R e f e r e n c e



Scalability planning information

This appendix provides guidelines and tools for planning your implementation. There are important trade-off issues to consider when planning your Norton AntiVirus Corporate Edition implementation.

By following the guidelines included in this appendix, you can:

- Lower capital and operating costs.
- Reduce administrative effort.
- Maximize the speed at which new virus threats are addressed.
- Lower server CPU and network usage.

Planning questions

To take advantage of Norton AntiVirus Corporate Edition scalability benefits, answer the following questions:

- What is your ideal client-to-server ratio?
For more information, see [“Ideal client-to-server ratios”](#) on page 392.
- What is the optimum number of threads for virus definitions updates and for configuration file distribution?

For more information, see [“Optimal number of threads for update operations”](#) on page 394, [“Virus definitions file updating”](#) on page 396, and [“Client configuration updates”](#) on page 399.

- What level and kind of server is needed to achieve the target client-to-server ratio and meet performance requirements?

For more information, see [“Norton AntiVirus Corporate Edition server specifications”](#) on page 401.

- What is the optimum client check-in interval?

For more information, see [“Client check-in interval”](#) on page 403.

Ideal client-to-server ratios

If you are running a typical 100 MB network, you can connect 3,000 or more workstation clients to a single Norton AntiVirus Corporate Edition server and still meet key performance standards. You can achieve this client-to-server ratio on typical network servers running Windows NT/2000/XP and using the IP protocol to communicate with clients. A typical network server has two or more Intel-based processors and typical network server memory, disk, and network interface resources.

With this network and server configuration, you can deliver new virus definitions files from a single server and install them on 3,000 workstations in 35-50 minutes under moderate network loading conditions. You can distribute and install new Norton AntiVirus Corporate Edition client configurations on all 3,000 clients in two minutes or less.

You can connect 1,000 clients to a single NetWare server. Likewise, servers using the IPX protocol to communicate with clients can handle up to 1,000 clients. Performance on a 10 MB LAN is slower, but it is still possible to connect up to 800 clients to a single server.

Practical limits for Norton AntiVirus Corporate Edition client-to-server ratios

The following table shows the client-to-server ratios that you can expect for different combinations of servers, networks, and protocols.

	100 MB LAN		10 MB LAN	
Server type/configuration	IP	IPX	IP	IPX
Enterprise server running NT	3,000	1,500	800	800
Enterprise server running NetWare	1,000	1,000	800	800
Workgroup server running NT	1,200	600	600	600
Workgroup server running NetWare	600	600	600	600

For more information about Enterprise and Workgroup server categories, see [“Norton AntiVirus Corporate Edition server specifications”](#) on page 401.

The criteria used to establish these ratios include:

- Stable, reliable, and consistent performance for all client-server operations.
- Completion of virus definitions updates on all connected clients in less than one hour from the time that new virus definitions files are received by the parent Norton AntiVirus Corporate Edition server.

This is based on the most demanding operational goals that Symantec has encountered among its larger customers for completing virus definitions updates across their enterprises. One hour to update virus definitions is not necessarily the ideal. For this critical operation, faster is always better.

Performance on a 100 megabit network is limited by the speed of the server. You can improve performance on faster networks by using more powerful servers. On a 10 megabit network, performance is limited by the network capacity itself. It may be possible to use a less powerful workgroup-type server and still meet performance requirements.

Trade-off considerations

While the server/client ratios listed in the preceding table are realistic, other rules exist for grouping clients together for connection to the same server. Consider the following factors when determining how to group clients:

- For administrative purposes, group clients that can share common Norton AntiVirus Corporate Edition configuration settings and options on the same server. Otherwise, you cannot administer all of the clients on a server as if they were a single client.
- Follow subnet boundaries and avoid mixing segments with differing LAN performance characteristics when grouping clients together on a single Norton AntiVirus Corporate Edition server.

Optimal number of threads for update operations

Norton AntiVirus Corporate Edition includes the following time and resource intensive operations:

- Virus definitions updating
- Client configuration updating
- Remote client installation and updating

These operations use multithreading so that a Norton AntiVirus Corporate Edition server can initiate and perform them for multiple clients simultaneously.

By default, Norton AntiVirus Corporate Edition starts five threads for each of these operations. This default setting yields significant improvements in performance, but even better performance may be achieved on faster networks by raising the number of threads.

As you raise the number of threads, the rate at which client updates are completed increases. However, more server and network resources are used. This is to be expected since a multithreaded operation works on multiple clients at a time.

For each network, server, and type of operation, there is an optimal number of threads. When you exceed this number, performance will, at best, stay flat. Performance may decline while resource usage continues to increase. There may also be an increase in the incidence of process failures as threads are increased beyond the optimal level.

Recommendations on number of threads for key operations

The following table indicates the number of threads that yields optimum results for the Norton AntiVirus Corporate Edition operations in which multithreading is of greatest benefit.

LAN speed	Protocol	Network OS	Server category	Optimal thread range for:		
				Virus definition update	Client configuration update	NT Remote installs
100 MB	IP	Windows NT	Enterprise	10-15	5-10	10-20
			Workgroup	5-8	4-7	10-20
		NetWare	Enterprise	6-10	5-10	10-20
			Workgroup	5-8	4-7	10-20
		IPX	Enterprise	6-10	5-10	10-20
			Workgroup	5-8	4-7	10-20
		NetWare	Enterprise	6-10	5-10	10-20
			Workgroup	5-8	4-7	10-20
			Enterprise	6-10	5-10	5-10
			Workgroup	5-8	4-7	5-10
10 MB	IP	NT	Enterprise	6-10	5-10	5-10
			Workgroup	5-8	4-7	5-10
		NetWare	Enterprise	6-10	5-10	5-10
			Workgroup	5-8	4-7	5-10
		IPX	Enterprise	6-10	5-10	5-10
			Workgroup	5-8	4-7	5-10
		NetWare	Enterprise	7-10	5-10	5-10
			Workgroup	5-8	4-7	5-10
			Enterprise	7-10	5-10	5-10
			Workgroup	5-8	4-7	5-10

For an explanation of Enterprise and Workgroup server categories, see [“Norton AntiVirus Corporate Edition server specifications”](#) on page 401.

Virus definitions file updating

This section assumes that you are using the Virus Definition Transport Method. For more information about virus definitions file updating methods, see [“The Virus Definition Transport Method versus LiveUpdate”](#) on page 403 and [“Which update method should I use?”](#) on page 257.

The primary factor in setting client-to-server ratios for most large networks is virus definitions file updating performance. Using typical enterprise type servers, performance is processor-bound on 100 megabit networks and network-bound on 10 megabit networks.

Virus definitions update performance

The following table shows key performance and resource usage estimates for virus definitions file updating on an enterprise server running Windows NT.

Network speed	100 Megabit		10 Megabit	
Protocol	IP	IPX	IP	IPX
Optimum number of threads	10-15	6-10	6-10	6-10
Update rate-seconds/client	0.90	1.80	3.20	3.20
Max client-to-server ratio	3,000	1,500	800	800
Server CPU usage (%)	92-98%	88-96%	24-26%	48-52%
Network usage (%)	32-38%	16-19%	85-93%	85-93%

The following table shows key performance and resource usage estimates for virus definitions file updating on a workgroup server running Windows NT.

Network speed	100 Megabit		10 Megabit	
Protocol	IP	IPX	IP	IPX
Optimum number of threads	5-8	5-8	5-8	5-8
Update rate-seconds/client	2.25	4.50	3.20	4.50
Max client-to-server ratio	1,200	600	800	600
Server CPU usage (%)	92-98%	88-96%	43-46%	88-96%
Network usage (%)	12-18%	6-10%	85-93%	65-72%

The following table shows key performance and resource usage estimates for virus definitions file updating on an enterprise server running NetWare.

Network speed	100 Megabit		10 Megabit	
Protocol	IP	IPX	IP	IPX
Optimum number of threads	6-10	6-10	6-10	6-10
Update rate-seconds/client	2.70	2.70	3.20	3.20
Max client-to-server ratio	1,000	1,000	800	800
Server CPU usage (%)	38-42%	40-45%	30-35%	32-37%
Network usage (%)	10-15%	10-15%	85-93%	85-93%

The following table shows key performance and resource usage estimates for virus definitions file updating on a workgroup server running NetWare.

Network speed	100 Megabit		10 Megabit	
Protocol	IP	IPX	IP	IPX
Optimum number of threads	5-8	5-8	5-8	5-8
Update rate-seconds/client	4.50	4.50	4.50	5.60
Max client-to-server ratio	600	600	600	600
Server CPU usage (%)	56-62%	60-65%	56-62%	60-65%
Network usage (%)	6-10%	6-10%	65-72%	65-72%

For information about Enterprise and Workgroup server categories, see [“Norton AntiVirus Corporate Edition server specifications”](#) on page 401.

To increase threads for virus definitions updating

- Add (modify) the following registry value:
\\hklm\software\intel\landesk\virusprotect6\currentversion\
ClientUpdateThreadPool

The default is five threads if this value is not there. The minimum value that the server will accept is 1 and the maximum is 40. If you specify values beyond this range, the default value will be used.

Note: This same value is used for client configuration updates.

Client configuration updates

In Norton AntiVirus Corporate Edition, client configuration is server-driven and multithreadable. This results in fast performance. Using the optimal threads provided above, 3,000 clients can receive and apply updates in two to five minutes depending on the server and network speeds.

Several other key operations use Grc.dat updates as the means of transmission from servers to their clients. These operations include:

- Virus definitions rollbacks
- Client software updates
- Virus sweeps
- On-demand virus scans initiated from the console by administrators

To increase threads for client configuration updating

- Add or modify the following registry value:
`\\hklm\software\intel\landesk\virusprotect6\currentversion\
ClientUpdateThreadPool`

The default is five threads if this value does not exist. The minimum value that the server will accept is 1 and the maximum is 40. If you specify values beyond this range, the default is used.

Note: This same value is used for virus definitions files updating.

Client and server installations and updates

Client and server installations and updates are scalability issues even though they would not normally be applied to more than a few hundred workstations in any one instance. On a nonbusy 100 megabit network using a single enterprise type server and 15 to 25 threads, Norton AntiVirus Corporate Edition 7.6 for desktops can be installed or updated on 250 Windows NT/2000/XP workstations in about one hour.

To increase threads for client or server installations and updates

- Edit the following registry keys:
HKLM\SOFTWARE\Intel\LANDesk\VirusProtect6\CurrentVersion:
NAVClientRollout_ThreadCount for NTRemote
NAVServerRollout_ThreadCount for Server Rollout
The default values are 3 for server rollout and 10 for client rollout.

Trade-off considerations

There are several factors to consider when determining how many threads to use for each server and operation.

- Network speed and loading: The number of threads should be lower for a 10 MB network or for a faster network that carries heavy, high-priority traffic. However, for a typical 100 MB network, increasing the number of threads from the default setting may improve performance without creating network traffic problems.
- Server speed and loading: If you are using a less powerful server, or the server is providing services to other important applications, you may want to try fewer threads.
You will need to select servers carefully. For guidelines on selecting servers, see [“Norton AntiVirus Corporate Edition server specifications”](#) on page 401.
- Client-to-server ratio: If you choose to connect a lower number of clients to a Norton AntiVirus Corporate Edition server, you may find that a lower number of threads works well.
- Performance requirements: If minimizing distribution of virus definitions and client configuration response time is the highest priority for your network, or for a portion of it, you can reduce the number of clients connected to each server and increase the number of threads for virus definitions and client configuration update operations.

After considering these trade-offs, you may have two identical Norton AntiVirus Corporate Edition servers in your installation, each with a different number of clients connected and each running a different number of threads for the same operations.

Additional thread configuration guidelines

Norton AntiVirus Corporate Edition sorts clients connected to a server by subnet and thread. Each thread that is processing the update queue updates all of the clients on one subnet before starting on another subnet. This improves network load distribution. Only one or two threads are slowed down by updating clients on slower subnets. The other threads can update computers on fast subnets quickly. This reduces the time to update most clients, assuming that the majority are on fast connections to the server.

For enterprise-class servers on a fast network, configuring threads to work on several subnets at the same time better balances the network load, making better use of the high-speed network near the central server. This specifically limits the load on slower subnets, and avoids the possibility of having multiple threads updating computers on the same subnet, which raises the traffic level on that subnet.

Norton AntiVirus Corporate Edition server specifications

Norton AntiVirus Corporate Edition servers must be matched to your target client-to-server ratio. On a 100 MB network, performance is related directly to the power of the server. More powerful servers can support more clients. Fewer servers are needed to support Norton AntiVirus Corporate Edition operations. However, an extremely powerful server could saturate the network, or be forced to work at a rate below its capacity, when performing more resource intensive operations such as virus definitions updating. You will need to determine the appropriate balance.

For 10-megabit networks, the network is the limiting factor in performance. Using a more powerful server may have little or no impact on actual Norton AntiVirus Corporate Edition server performance.

Typical Norton AntiVirus Corporate Edition servers

The following table includes two server profiles that represent the two ends of the spectrum of computer systems that are typically used as Norton AntiVirus Corporate Edition servers. These guidelines indicate the requirements for Norton AntiVirus Corporate Edition servers in your installation.

	Enterprise	Workgroup
	Most powerful	Least powerful
Server CPU	Dual-600 MHz Pentium III	Single-450 MHz Pentium II
Server memory	1 GB	256 MB
Server disk sub-system	Dual high-speed SCSI controllers	EIDE-ATA controller
	60-100 GB RAID array	2-20 GB drives
Server network interface	One 100 megabit NIC	One 100 megabit NIC
Reasons for selecting this type of server	100 megabit network	10 megabit network
	Thousands of workstation clients that can share configurations (high client-to-server ratio)	Fragmented workstation groups each needing separate configurability (lower client-to-server ratio)
	Other applications running on the server	Server dedicated to Norton AntiVirus Corporate Edition
	Moderate network traffic	Heavy network traffic
	High performance standards for anti-virus update operations	Lower priority on speed of anti-virus update operations

Client check-in interval

Norton AntiVirus Corporate Edition client configuration updates are not triggered by client check-in as they were prior to version 7.5. You can lengthen check-in intervals from the default of 60 minutes when necessary. Longer client check-in intervals help reduce traffic and server processing.

For mobile clients, a check-in interval of one hour should be adequate. For stable groups of clients, longer check-in intervals of 24 hours or more may better meet operating requirements. Make sure that the time period for dropping nonreporting clients from the parent server's list of connected clients is longer than the new client check-in intervals.

For more information, see [“Changing the client check-in interval”](#) on page 229.

The Virus Definition Transport Method versus LiveUpdate

At the server level, you must make a choice between using the Virus Definition Transport Method or LiveUpdate for distributing virus definitions updates among servers.

Properly implemented, both the Virus Definition Transport Method and LiveUpdate are scalable and practical for use in large and very large networks for distributing virus definitions updates among servers. However, they work very differently.

Virus Definition Transport Method operations

The Virus Definition Transport Method is a push operation that is started when new virus definitions are received by one server. The server then notifies an administrator-defined set of other servers of the request for the new definitions. When these servers receive the new definitions, they send them out to a number of servers. New definitions are distributed to all of the servers on the network. The servers begin immediately to distribute the new definitions to their clients.

Overall, the Virus Definition Transport Method is more suitable from a scalability perspective. Because it is event-driven, there is no polling traffic and processing. The Virus Definition Transport Method does not overburden any one computer and is very fast and effective at distributing

new updates to a large number of Norton AntiVirus Corporate Edition servers.

The only drawback to the Virus Definition Transport Method is the large amount of data to transmit. With the Virus Definition Transport Method, a complete new virus definitions file is transmitted to each server. With LiveUpdate, only new and modified definitions are distributed.

LiveUpdate operations

LiveUpdate is a pull operation. Each client or server on which LiveUpdate is being used initiates the update operation by requesting new definitions on a scheduled, periodic basis. LiveUpdate may be configured on each computer to request the update from a designated LiveUpdate server or directly from the Symantec LiveUpdate Web site.

Using both the Virus Definition Transport Method and LiveUpdate

Some installations use both the Virus Definition Transport Method and LiveUpdate. LiveUpdate is used as the normal update mechanism. It is scheduled to run on a weekly basis. The Virus Definition Transport Method is used as the emergency system for getting new virus definitions files distributed quickly when the network is threatened by a new virus.

While the Virus Definition Transport Method is used more often, some large networks depend on LiveUpdate. These installations do not permit direct access to the Symantec site by a large number of servers and clients. One or more servers acts as a LiveUpdate server to all of the other servers on the network, and in some installations, to all clients.

Randomized Scheduling

Randomized Scheduling automatically spreads requests for new definitions over a defined period of time among the computers that share the same update schedule. Virtually all servers and clients on a network can share the same LiveUpdate schedule without creating unmanageable spikes in demand for network and LiveUpdate server resources.

Operations that do not affect scalability

The following Norton AntiVirus Corporate Edition operations are not scalability concerns.

Operation	Why it is not a scalability concern
Scheduled virus scans	While you can mandate and configure scheduled scans centrally, they are executed on each protected computer independently and without dependency on the parent server or administrative console at runtime.
Virus sweeps	Grc.dat files initiate and supply the options and settings for virus sweep operations. The sweep operations take place on each protected computer.
On-demand virus scans	Grc.dat files initiate and supply the options and settings for manual virus scans. The scan operations take place on each protected computer.
Virus definitions rollback	Grc.dat files initiate and supply the settings for definitions rollback operations. Once the Grc.dat file has been processed by a client, it searches for the designated virus definitions file. If it has the file, it applies the file and signals the parent server. If it does not have the file, it requests and applies it. While not completed as quickly as multithreaded virus definitions updates, rollback execution time is acceptable in relation to its frequency of use. Rollbacks use modest levels of network and server resources.
Client software automated install-on-logon	Grc.dat files distribute the command to the clients to update the client software on next log-on. The software updates are spread out over time because they occur when each client logs on again.

Most of these operations use the Grc.dat file for initiation and configuration. Grc.dat distribution is fast and multithreaded. After Grc.dat has been received, clients proceed independently. Except for rollbacks and automated client installs, these operations are executed on the clients without depending on the parent server.

For rollbacks, clients almost always have the rollback virus definitions files and can complete rollbacks quickly and without depending on the parent server. However, when a large number of clients do not have the file that is being rolled back, the operation takes longer to complete and uses more server and network resources. You can avoid this situation by keeping the last five virus definitions files on each protected computer and by not rolling back to earlier files.

For automated client installations, the client must receive the new software from the parent server. However, because these updates do not take place until the next logon for each client, the associated server processing and network traffic are spread out over time.

Troubleshooting

This appendix includes the following topics:

- Installation issues
- Performance issues
- Virus definitions file updating issues
- Issues related to Norton AntiVirus Corporate Edition and Microsoft Exchange, Microsoft Outlook Express, and the Windows Me/XP System Restore feature

Installation issues

This section provides information about some common issues that may arise during installation, and how to resolve them.

Note: Third party rollout via modifications to Navce.msi, or running the Norton AntiVirus Corporate Edition server program install via Navce.msi, are not supported.

Third party rollout and error 0x20000046E

If you roll out Norton AntiVirus Corporate Edition with an installation method not provided in the product and receive error 0x20000046E when attempting manual or scheduled scans, check the Norton AntiVirus Service and ensure that the checkbox to interact with Desktop is checked.

NDS errors when installing Norton AntiVirus Corporate Edition to a NetWare 4.x server running an outdated Clib.nlm

If you install Norton AntiVirus Corporate Edition to a NetWare 4.x server with an outdated version of the Clib.nlm file, you will see the following error messages:

Error importing NWDSCreateContextHandle

Error (0xa0000014)(-1610612716) initializing DS in DS Preliminaries

Error

Error: 0xa0000014(-1610612716) in line 255: [DSPROFILE]

Error

Error: Not authenticated with Novell Directory Services in line 278: [DSOBJECTS]

You must use the latest Novell Clib.nlm file. This file is contained in the latest version of the NetWare update patch, which you can download from the Novell Support Web site:

<http://support.novell.com>

Install this patch on your NetWare 4.x server and reinstall Norton AntiVirus Corporate Edition to resolve this issue.

Dealing with an Unable to load Listview.ocx error

If Norton AntiVirus Corporate Edition displays an Unable to load Listview.ocx error, one or more of the following files were not registered during installation: Clntcon.ocx, Srvcon.ocx, or Ldvpocx.ocx. This situation might occur if the installation was not complete when you exited the Setup program, or if Transman.dll is missing from the directory where you installed Norton AntiVirus Corporate Edition.

To correct this error

- Copy Transman.dll to:

C:\Program Files\Common Files\Symantec Shared\SSC

If Transman.dll is already there, uninstall Norton AntiVirus Corporate Edition, then reinstall it.

Specifying a container for logon scripts on NetWare 4.x or 5.x servers

If you're installing to a NetWare 4.x or 5.x server, the Setup program prompts you to provide a username, password, and an NDS container. The container you specify will hold sample logon scripts that automatically install the client to users' computers. The Setup program stores this information for later use but does not authenticate the information you enter.

What happens if I enter an invalid container name or password during installation?

The only clean way to resolve this issue is to let the install complete, then immediately run `Load sys:\nav\vpstart.nlm /remove`

You can then reinstall using the correct information.

I entered an incorrect user name and password when rolling out Norton AntiVirus Corporate Edition to NetWare servers

The easiest way to resolve this issue is to let the install complete, then immediately run `Load sys:\nav\vpstart.nlm /remove`

Windows Installer Service error

When this error occurs, the following message appears in a Windows Installer dialog box:

This installation package cannot be installed by the Windows Installer service. You must install a Windows service pack that contains a newer version of the Windows Installer service.

To resolve this issue

- Run `Instmsia.exe` which is located on Disk 2 at:
`Navcorp\Rollout\Avserver\Clients\Win32`

Windows 2000 client installs that use interactive logon scripts

When a Windows 2000 client installs Norton AntiVirus Corporate Edition via logon scripts that are run interactively, the dialog box where the questions are asked is minimized.

To run batch files in a maximized window

- Set the value for the following registry key to 1:
HKLM\Software\Microsoft\Windows NT\
CurrentVersion\WinLogon:RunLoginScriptSync

The Norton AntiVirus Corporate Edition server program install stops responding

If the Norton AntiVirus Corporate Edition server install program appears to stop responding, or hang, close it, then restart the install program.

Locating servers during installation

When you run the server Setup program, you can browse for the servers to which you want to install. However, servers that are across routers and bridges may be difficult to locate. To verify that you'll be able to see a server when you run the server Setup program, map a drive to the server using Windows Explorer. If you can see a server in Windows Explorer, you should be able to see the server when you run the server Setup program.

If you cannot see a NetWare server, you can attempt to resolve the issue by performing the following tasks:

- Verify that you have the Novell client installed, preferably the most recent version.
- Ensure that the server is logged into the NDS tree.
- Have someone else run the server Setup program at another location where the server is visible.

If you cannot see a Windows NT/2000 server, run the server Setup program on the server.

Server or client missing from tree view of Symantec System Center console

When you run the Symantec System Center console, you see virus-protected servers and connected client computers displayed as objects in an expandable/collapsible tree format. Servers are grouped under server groups, and connected client computers are grouped under the server to which they connect. This is called the server group view.

At startup, Symantec System Center pings every server running Norton AntiVirus Corporate Edition. As soon as the servers respond, they and connected client computers that are running Norton AntiVirus Corporate Edition display in the server group view.

If you start virus-protected servers or add connected clients while Symantec System Center is already running, you might need to either discover or find the new computer so that it will display in the server group view.

Discover

You can click Tools > Discovery Service to perform a new discovery of all servers and connected clients. An intense discovery may take a while.

For more information, see the *Symantec System Center Implementation Guide*.

Find

You can click Tools > Find Computer to search specifically for the computer you added. This does not take very long. Norton AntiVirus Corporate Edition adds the computer to the server group view after finding it (if it was not already there).

For more information, see the *Symantec System Center Implementation Guide*.

Refresh

You can right-click at the system hierarchy, server group, or server level, then select Refresh to validate active communication with the list of currently displayed servers. However, the refresh feature does not find servers or server groups that may have been added since the current session of Symantec System Center started. If the refresh determines that a server or client that previously displayed in the server group view is no longer communicating, it will dim the object in the server group view.

For more information, see the *Symantec System Center Implementation Guide*.

Startup issues after Norton AntiVirus Corporate Edition is installed

The information in this section may help you if you experience startup issues after installing Norton AntiVirus Corporate Edition on your Windows clients. A yellow exclamation point may appear on the shield in the system tray. The exclamation point appears after you restart, and realtime protection is not enabled. On Windows 95/98 computers, you may see the following error message:

RTVSCN95 caused a General Protection Fault in Module Krnl386.exe.

These problems are usually caused by a timing conflict between Norton AntiVirus Corporate Edition and another program or service loading at startup.

- To resolve the issue on Windows NT/2000 computers, change the load order of the Norton AntiVirus Corporate Edition Client service by creating a dependency on another service.

For instructions on creating a dependency, please see the Microsoft Knowledge Base Article Q193888, "How to Delay Loading of Specific Services."

Shutdown issues after Norton AntiVirus Corporate Edition is installed

The information in this section may help you if you experience shutdown issues after installing Norton AntiVirus Corporate Edition on your Windows clients. When you attempt to shut down or restart the computer, it may stop responding, or you may see the following error message:

The application cannot respond to the End Task request.

Norton AntiVirus Corporate Edition Auto-Protect scans the A drive during restart or shutdown to prevent your computer from becoming infected by a boot sector virus. On some computers, the shutdown floppy disk drive scan causes timing problems during shutdown.

Note: Back up the system registry before making any changes. Incorrect changes to the registry can result in permanent data loss or corrupted files. Modify only the keys specified.

To back up the Windows 95/98/NT registry

- 1 Click **Start**.
- 2 Click **Run**.
The Run dialog box appears.
- 3 Type **Regedit**.
- 4 Click **OK**.
The Registry Editor opens.
- 5 On the Registry menu, click **Export Registry File**.
- 6 Verify the following items in the Export Registry File dialog box:
 - Save in: Desktop
 - File name: Registry Backup
 - Save as type: Registration Files
 - Export range: All
- 7 Click **Save**.
- 8 Exit the Registry Editor and verify that the file Registry Backup.reg is on the Desktop.

To disable the shutdown floppy disk drive scan within the registry

- 1 On the Windows Start menu, click **Run**.
The Run dialog box appears.
- 2 Type **Regedit**.
- 3 Click **OK**.
The Registry Editor opens.
- 4 Navigate to the following subkey:
HKEY_LOCAL_MACHINE\Software\Intel\LanDesk\VirusProtect6\
CurrentVersion

- 5 In the right pane, right-click and click **New > DWORD Value**.
- 6 Name the value Skipshutdownfloppycheck.
- 7 Right-click the new Skipshutdownfloppycheck and click **Modify**.
- 8 In the Value Data text box, type **1**.
- 9 Repeat steps 4 through 7 to create a new value named Skipshutdownscan with a value of 1.
- 10 To re-enable the shutdown floppy disk drive scan, set the Skipshutdownfloppycheck and Skipshutdownscan values to 0.
- 11 On the Registry menu, click **Exit** to save the changes.

The same 16-bit client displays twice in the console after an update

When you update a Norton AntiVirus Corporate Edition 16-bit client, you initially see two copies of the same client computer displayed in Symantec System Center. This is because the old client still exists in the Norton AntiVirus Corporate Edition server's client list. When the server refreshes its client list, it clears the old copy of the Norton AntiVirus Corporate Edition 16-bit client. Afterwards, only the updated Norton AntiVirus Corporate Edition 16-bit client displays in Symantec System Center.

Can't see server to update

If you can't see the server to update, use the following methods to resolve the issue:

- The server might be down or you might have some other network issue. Use the Find Computer button from the Select servers to update the dialog box.
- Verify that Norton AntiVirus Corporate Edition is installed and running on the server. If your server is not currently running Norton AntiVirus Corporate Edition, it will not display in the list of updateable servers.

- Stop then restart the following Symantec System Center and Norton AntiVirus Corporate Edition services:
 - Norton AntiVirus Server
 - Defwatch
 - Intel PDS
 - Intel File Transfer
 - Intel Alert Originator
 - Intel Alert Handler
 - Symantec System Center Discovery Service

Can't see client to update

Norton AntiVirus Corporate Edition clients running IPX only will not check in with their parent server and thus, not show up under the Symantec System Center console. They must either have IP installed on the server and client or run Microsoft File and Print Services for NetWare on the Server.

An update failed or did not complete

Try to resolve the issue using any of the following methods:

- Reboot the workstation or server that didn't get updated.
- Stop, then restart the Norton AntiVirus service.
- Apply the definitions from within Symantec System Center.

To apply the definitions from within Symantec System Center

- 1 In the console tree, right-click the server group, then click **All Tasks > Norton AntiVirus > Virus Definition Manager**.
- 2 Click **Configure**.
- 3 Click **Definition File**.
- 4 Click **Apply**.

Silent uninstall of the Norton AntiVirus Corporate Edition program for desktops

The Norton AntiVirus Corporate Edition user interface must be closed before the product can be uninstalled successfully.

How do I use the LiveUpdate Administration Utility?

The LiveUpdate Administration Utility, which is used to set up an internal LiveUpdate Server, is ideally suited for sites with 1000 or more nodes. If you manage a smaller number of nodes, you may prefer to use the Virus Definition Transport Method.

For more information, see [“Which update method should I use?”](#) on page 257 and [“Using the Virus Definition Transport Method”](#) on page 259.

What settings apply when server group, server, and client settings differ?

When server group, server, and client settings differ, settings are applied in the following manner:

- If you change options at the client level for a feature that cannot be locked, such as a scheduled scan, the settings are overwritten by those set at the server level.
- For client realtime protection, client settings must be locked before the realtime options configured on the Symantec System Center console can be propagated to them.
- If you set options at the server group level, change them for a specific server, then reset options at the server group level, the settings apply to all servers in the group.
- Options set at the server group level apply to all servers in the group.
- If you use Reset All, options at the server group level take effect immediately.
- Local options take effect immediately until server group options are pushed out. Server group options always override local options.

Windows NT Workstation limitations

The maximum number of computers that are permitted to simultaneously connect over the network to Windows NT Workstation 4.0 is 10. This limit includes all transports and resource sharing protocols combined. This limit is also the number of simultaneous sessions from other computers the system is permitted to host and does not apply to the use of administrative tools that attach to the system from a remote computer.

This limitation only applies to inbound connections to Windows NT Workstation 4.0. When you use Windows NT Workstation 4.0, unlimited outbound connections can be established to other systems.

Any file, print, named pipe, or mail slot session that does not have any activity on it will be automatically disconnected after the AutoDisconnect time has expired; by default, the time expires at 15 minutes. Once the session is disconnected, one of the 10 connections will be available so that another user can connect to the Windows NT Workstation computer.

A workaround

Lowering the AutoDisconnect time can help to reduce some of the issues users may encounter with the 10-connection limit on a computer that is not used heavily for server purposes. To avoid losing the Server service's self-tuning capability, change the AutoDisconnect time using the Windows Registry Editor rather than from a command line or Control Panel Network.

To configure the AutoDisconnect time

- Run the following command from a command prompt:
`net config server /autodisconnect:time_before_autodisconnect`
replacing `time_before_autodisconnect` with a number in minutes.

The Windows NT Server service is self-tuning. Server configuration parameters are calculated and set automatically each time you start Windows NT. If you run Net Config Server in conjunction with the `/Autodisconnect`, `/Servcomment` or `/Hidden` switches, the current values for the automatically tuned parameters are displayed and written to the registry. Once written, you cannot tune the Server service using Control Panel Networks. If you changed any of the Server service settings, Windows NT cannot automatically tune the Server service for your new configuration. To avoid losing the Server service's self-tuning capability, make the change using the Registry Editor rather than from a command line or Control Panel Network.

Difficulty configuring or running scans

This section describes issues related to configuring scanning or running scans.

Difficulty loading Norton AntiVirus Corporate Edition for NetWare (RTVSCAN issue)

If you receive the following error message when loading Norton AntiVirus Corporate Edition for NetWare:

RTVSCAN could not load NDS function.

You may be using an outdated Dsapi.nlm. Update your Dsapi.nlm by downloading the latest version from Novell at www.novell.com, and reinstall Norton AntiVirus Corporate Edition.

You may want to use Config Reader to identify any outdated NLMs. Config Reader can take input from a CONFIG.TXT file and present it in a way that provides you with more options than viewing it through a text editor. Config Reader is available from the Novell Website.

Issues configuring a group of selected clients

If you select a group of 32-bit clients and you include a 16-bit client in this group, Symantec System Center client configuration options are not available. To resolve this issue, check the client group for any selected 16-bit clients. While pressing the Ctrl key, click the 16-bit client to remove it from a selection in Symantec System Center.

Issues configuring 16-bit clients

You can't remotely configure individual or multiple-selected groups of 16-bit clients. Configure 16-bit clients by configuring the server group or server to which the 16-bit clients connect.

The configuration changes I made to the client software did not work

Changes you make to Norton AntiVirus Corporate Edition clients take effect after several minutes.

If, for any reason, the new client configuration is not immediately received by the parent server or by the client, the information will be updated during the server/client check-in. By default, the client check-in interval is set to 60 minutes.

To set the update frequency

- 1 Right-click a server group or server.
- 2 Click **All Tasks > Norton AntiVirus > Virus Definition Manager**.
- 3 Click **Settings**.

Stopping a scan in progress on a compressed file

You cannot stop a scan in progress on a compressed file. If you click Stop Scan, Norton AntiVirus Corporate Edition stops the scan only after it has finished scanning the compressed file.

Performance issues

This section presents some common performance issues.

My computer runs much slower since I installed Norton AntiVirus Corporate Edition client

You can take the following actions:

- Make sure that the computer meets the Norton AntiVirus Corporate Edition system requirements as specified in page 106 for servers and on page 135 for clients.
- Limit the programs launched on startup to only those that are required. Each program can consume a significant amount of system resources.

Note: Avoid changing Norton AntiVirus Corporate Edition realtime scan settings to minimize system resource usage. For example, changing scans to check for modified files only may consume fewer resources, but the affected computer would be more vulnerable to virus infection.

Initial memory usage drops after running a scan under Windows 2000

The memory is allocated when the main user interface for Norton AntiVirus Corporate Edition is displayed. In Windows 2000, when a scan is started, the Results View dialog is displayed and the main user interface is minimized. When the main user interface is minimized, memory that was allocated is then released.

As RTVscan sits with no activity, the page fault value in Task Manager slowly increases

The MainTimer loop of RTVscan queries the registry for values about once each minute. There is enough time between the calls for the operating system to page the memory to disk so that when the query is made again, a page fault will occur. This behavior is not uncommon, but can impact performance.

Virus definitions file updating issues

This sections presents some issues related to updating virus definitions file updates, and how to resolve them.

LiveUpdate does not run

You may find that you can run LiveUpdate from the Norton AntiVirus Corporate Edition user interface. However, when you attempt to run LiveUpdate from the Symantec System Center console, or when LiveUpdate is scheduled, it does not run.

If LiveUpdate is connecting to the Internet

If LiveUpdate is connecting to the Internet, this problem may occur because the system account does not have rights to the firewall or proxy server. To correct the problem, allow the Norton AntiVirus service to use an Administrator account rather than the system account.

Note: If your firewall has validation rules that are independent of user accounts, then LiveUpdate will not work.

To allow the NAV service to use a different account

- 1 Open the NT Services list, and then double-click the Norton AntiVirus service.
The Service window appears.
- 2 Check This Account, and then click the button to the right (“...”) under Log On As.
The Add User window appears. By default, the service logs in with the System account.
- 3 Choose any account that has Administrator rights to the affected computer, click Add, and then click OK.
- 4 Type the passwords, and then click OK.
- 5 Stop and then restart the Norton AntiVirus service.

If LiveUpdate connects to a UNC share on an internal server

If LiveUpdate connects to a UNC share on an internal server, a problem may occur because the system account does not have full rights to network resources. If LiveUpdate is configured to download updates from a UNC share, then LiveUpdate fails. The system account has no network credentials and must connect to other resources using a null session.

One solution for this problem is to allow the Norton AntiVirus service to use a different account. This must be performed on each Windows NT/2000 computer that is experiencing this problem.

Alternatively, you can configure the internal server to allow null sessions. Rather than configuring the Norton AntiVirus service to use a different account on all Windows NT computers that experience this problem, you can configure the server to allow connections from the system account.

For more information, see [“To allow the NAV service to use a different account”](#) on page 421.

NetWare server not running TCP/IP can't get an update from Windows NT server in another server group

If your NetWare server is not running TCP/IP and is not using a domain naming services (DNS) server, you may have difficulty updating a NetWare server from a Windows NT server that resides in a different server group. This is because the NetWare server does not store the address of the Windows NT server in its address cache.

If you choose not to run TCP/IP on your NetWare server and still want to update it from a Windows NT server in another domain, you can work around this issue by temporarily moving the NetWare server into a server group that has a Windows NT server in it. After one day, you can then move the NetWare server back to its original domain. This action adds the Windows NT server address to the NetWare server's address cache, and the NetWare server can locate the Windows NT server to obtain the updated virus definitions file.

Some Norton AntiVirus Corporate Edition servers weren't updated

When you update a server group, you find several Norton AntiVirus Corporate Edition servers in the server group that were not updated. This can occur in two cases.

Incomplete discovery process

If the discovery process is slow to find all Norton AntiVirus Corporate Edition servers, select a server for update before the primary server has been discovered. The update process tries to automatically add all servers in the server group to the update process. If the primary server in the server group isn't located, the update can't check for other server group servers. In this case, only the discovered servers would be located and updated.

To avoid this, allow the discovery process to complete before selecting servers, or check to see that all servers in the server group are selected before updating the server group.

Other issues

Other issues that may occur include:

- Issues between Norton AntiVirus Corporate Edition and Microsoft Exchange server
- Issues between Norton AntiVirus and Microsoft Outlook Express
- Viruses in System Restore folder on computers running Windows Me
- Issues between LiveUpdate and the Windows Me/XP System Restore feature

Norton AntiVirus Corporate Edition and Microsoft Exchange server issue

When Norton AntiVirus Corporate Edition for Windows NT/2000 is running on the same server as Microsoft Exchange, Norton AntiVirus Corporate Edition can detect the components of a virus such as Vbs.Loveletter.worm in the Edb.log file. Norton AntiVirus Corporate Edition either quarantines or deletes the file. Microsoft Exchange might then stop responding.

To resolve this, exclude both the temporary directory used by Microsoft Exchange and the Microsoft Exchange database folder from scanning.

If Microsoft Exchange has already stopped responding, run Isinteg and Eseutil to repair it.

For more information on Eseutil and Microsoft Exchange repair, see the Microsoft Knowledge Base Article Q219419, "XADM: Information Store Stops Unexpectedly and Cannot Be Repaired."

Norton AntiVirus Corporate Edition and Microsoft Outlook Express issue

When Norton AntiVirus Corporate Edition is running on a computer that is using Outlook Express and some other third party email applications, Norton AntiVirus Corporate Edition can detect the components of a virus, such as the Vbs.loveletter worm, in the Inbox file. Norton AntiVirus Corporate Edition either quarantines or deletes the Inbox file.

To resolve this issue, exclude the folder containing the Inbox file from realtime and manual scans.

Viruses in System Restore folder on computers running Windows Me

When you perform a scan using Norton AntiVirus Corporate Edition, you may receive alerts indicating that one or more files in the _Restore\Temp or the _Restore\Archive folders contain a virus or are infected with a virus. Alerts report that the virus cannot be cleaned. This is due to the design of Microsoft Windows Me.

For more information, see Microsoft Knowledge Base article Q263455 at:

<http://support.microsoft.com/support/kb/articles/Q263/4/55.ASP>

LiveUpdate and the Windows Me/XP System Restore feature

An issue may arise when you use the System Restore feature to restore to an earlier date after running LiveUpdate to get the latest virus definitions. After restarting, the following situations may exist:

- Norton AntiVirus services fail to load.
- A yellow exclamation point appears on the shield icon in the system tray.
- Virus detection no longer works.

Try this method first

- 1 Modify the CurDefs= value in C:\Program Files\Common Files\Symantec Shared\VirusDefs\definfo.dat to the date of the LastDefs= value.

For example, if the Definfo.dat file contains the following:

```
[DefDates]
CurDefs=20010725.005
LastDefs=20001219.002
```

you would modify the file to read:

```
[DefDates]
CurDefs=20001219.002
LastDefs=20001219.002
```

- 2 Save the file.
- 3 Modify the value in brackets [] in C:\Program Files\Common Files\Symantec Shared\VirusDefs\Usage.dat to the same value as the LastDefs= value in step 1.

For example, if Usage.dat contains the following:

```
[20010725.005]
DEFWATCH_10=1
NAVCORP_70=1
```

you would modify the file to read:

```
[20001219.002]
DEFWATCH_10=1
NAVCORP_70=1
```

- 4 Save the file.

- 5 Restart the Norton AntiVirus Client service from the Services Control Panel.

(Alternatively, from the Norton AntiVirus Corporate Edition user interface, you can check the box labeled Load Norton AntiVirus Services.

- 6 Run LiveUpdate to download the latest virus definitions.

If the above procedure does not resolve the issue

- 1 Copy the contents of the virus definitions folder from your source media, usually
NAVCORP\ROLLOUT\AVSERVER\CLIENTS\WIN32\VirDefs on Disk 2,
into the C:\Program Files\Common Files\Symantec
Shared\VirusDefs\INCOMING directory.
- 2 Restart the Norton AntiVirus Client service by using the Services Control Panel or using the checkbox labeled “Load Norton AntiVirus Services” in the NAV User Interface.

If none of the above steps restore the product functionality, please consult the Symantec Online Support Knowledge Base or Symantec Technical Support.



Norton AntiVirus Corporate Edition for Windows NT/2000 Services

This chapter includes names and descriptions for Norton AntiVirus Corporate Edition server and client services:

Service Name	Binary Name	Description
Norton AntiVirus Corporate Edition Server		
Norton AntiVirus Server	Rtvscan.exe	Main Norton AntiVirus Service. Most Norton AntiVirus Server related tasks are performed in this service.
Defwatch	Defwatch.exe	Service that watches for newly arriving virus definitions.
Intel PDS	Pds.exe	Intel Ping Discovery Service. Allows for discovery of products on the computer. Applications register with this service, along with an APP ID (such as LDVP), and a packet to return in response to ping requests (Pong Packet).

Service Name	Binary Name	Description
Norton AntiVirus Corporate Edition Client		
Norton AntiVirus Client	Rtvscan.exe	Main Norton AntiVirus Service. Most Norton AntiVirus client related tasks are performed in this service.
Defwatch	Defwatch.exe	Service to watch for new definitions arriving.

Events written to the Windows NT/2000 Event Log

The following table lists events written by Norton AntiVirus Corporate Edition to the Windows NT/2000 Event Log.

Event	Event number	Description
Event_Scan_Stop	2	Occurs when scanning completes.
Event_Scan_Start	3	Occurs when scanning starts.
Event_Pattern_Update	4	Occurs when a parent server sends a .Vdb file to a secondary server.
Event_Infection	5	Occurs when scanning detects a virus.
Event_File_Not_Open	6	Occurs when scanning fails to gain access to a file or directory.
Event_Load_Pattern	7	Occurs when Norton AntiVirus Corporate Edition loads a new .Vdb file.
Event_Trap	11	Used by Realtime Protection email scanning when handling email attachments.

Event	Event number	Description
Event_Config_Change	12	Occurs when a server updates its configurations according to the changes made from the console, excluding configurations changes made in the PRODUCTCONTROL or DOMAINDATA registry keys.
Event_Shutdown	13	Occurs when the Norton AntiVirus service is unloaded.
Event_Startup	14	Occurs when the Norton AntiVirus service is loaded.
Event_Pattern_Download	16	Occurs when new definitions are downloaded by a scheduled definitions update.
Event_Too_Many_Viruses	17	Occurs when Norton AntiVirus Corporate Edition has deleted or quarantined more than 5 infected files within the last minute. The number of files quarantined/ deleted and the time interval are configurable from the registry. The defaults are 5 files in 60 seconds.
Event_Fwd_To_Qserver	18	Occurs when quarantined files are sent to a Quarantine server.
Event_Backup_Restore_Error	20	Occurs when Norton AntiVirus Corporate Edition fails to back up a file or restore a file from Quarantine.
Event_Scan_Abort	21	Occurs when a scan is stopped before it completes.

Understanding viruses

The term virus is often used as a generic reference to any malicious code that is not, in fact, a true computer virus. This document discusses viruses, Trojan horses, worms, and hoaxes and ways to prevent them.

New forms of malicious code appear on the scene unpredictably. For the most recent information on viruses, worms, and hoaxes, visit the Symantec Security Updates site at:

<http://securityresponse.symantec.com>

Note that the Reference Area includes many more details about virus technologies and specific viruses than are included in this appendix.

What is a virus?

A computer virus is a small program written to alter the way a computer operates, without the permission or knowledge of the user. A virus must meet two criteria: It must execute itself. It will often place its own code in the path of execution of another program. It must replicate itself. For example, it may replace other executable files with a copy of the virus infected file. Viruses can infect desktop computers and network servers alike.

Some viruses are programmed to damage the computer by damaging programs, deleting files, or reformatting the hard disk. Others are not designed to do any damage, but simply to replicate themselves and make their presence known by presenting text, video, and audio messages. Even these benign viruses can create problems for the computer user. They take up computer memory used by legitimate programs. As a result, they often cause erratic behavior and can result in system crashes. In addition, many viruses are bug-ridden, and these bugs may lead to system crashes and data loss.

There are five recognized types of viruses.

File infector viruses

File infector viruses infect program files. These viruses normally infect executable code, such as .com and .exe files. They can infect other files when an infected program is run from a floppy disk, hard drive, or from the network. Many of these viruses are memory resident. After memory becomes infected, any noninfected executable that runs becomes infected. Examples of known file infector viruses include Jerusalem and Cascade.

Boot sector viruses

Boot sector viruses infect the system area of a disk—that is, the boot record on floppy disks and hard disks. All floppy disks and hard disks (including disks containing only data) contain a small program in the boot record that is run when the computer starts up. Boot sector viruses attach themselves to this part of the disk and activate when the user attempts to start up from the infected disk. These viruses are always memory resident in nature. Most were written for DOS, but all PCs, regardless of the operating system, are potential targets of this type of virus. All that is required to become infected is to attempt to start up your computer with an infected floppy disk. While the virus remains in memory, all floppy disks that are not write protected will become infected when the floppy disk is accessed. Examples of boot sector viruses are Form, Disk Killer, Michelangelo, and Stoned.

Master boot record viruses

Master boot record viruses are memory resident viruses that infect disks in the same manner as boot sector viruses. The difference between these two virus types is the location of the viral code. Master boot record infectors normally save a legitimate copy of the master boot record in a different location. Windows NT computers that become infected by either boot sector viruses or master boot sector viruses will not start. This is due to the difference in how the operating system accesses its boot information, as compared to Windows 95/98. If your Windows NT system is formatted with FAT partitions you can usually remove the virus by starting to DOS and using anti-virus software. If the boot partition is NTFS, the system must be recovered by using the three Windows NT Setup disks. Examples of master boot record infectors are NYB, AntiExe, and Unashamed.

Multi-partite viruses

Multi-partite (also known as polypartite) viruses infect both boot records and program files. They are particularly difficult to repair. If the boot area is cleaned, but the files are not, the boot area will be reinfected. The same holds true for cleaning infected files. If the virus is not removed from the boot area, any files that you have cleaned will be reinfected. Examples of multi-partite viruses include One_Half, Emperor, Anthrax and Tequila.

Macro viruses

Macro viruses infect data files. They are the most common and have cost corporations the most time and money. With the advent of Visual Basic in Microsoft's Office 97, a macro virus can be written that not only infects data files, but can also infect other files. Macro viruses infect Microsoft Office Word, Excel, PowerPoint and Access files. Newer strains are turning up in other programs as well. These viruses use another program's internal programming language, which was created to allow users to automate certain tasks within that program. Because of the ease with which these viruses can be created, there are now thousands of them in circulation. Examples of macro viruses include W97M.melissa, wm.niceday and W97M.groov.

What is a Trojan horse?

Trojan horses are impostors—files that claim to be something desirable but are actually malicious. An important distinction from true viruses is that they do not replicate themselves. Trojan horses contain malicious code, that, when triggered, causes loss, or even theft, of data. In order for a Trojan horse to spread, you must invite these programs onto your computers, for example, by opening an email attachment. The PWSteal.trojan is an example of a Trojan horse.

What is a worm?

Worms are programs that replicate themselves from computer to computer without the use of a host file. This is in contrast to viruses, which require the spreading of an infected host file. Although worms generally exist inside of other files, such as Word or Excel documents, there is a difference between how worms and viruses use the host file. The worm will release a document that already has the worm macro inside the document. The entire document will travel from computer to computer, so the entire document should be considered the worm. PrettyPark.worm is a particularly prevalent example.

What is a virus hoax?

Virus hoaxes are messages, almost always sent by email, that are similar to chain letters. Some of the common phrases used in these hoaxes are: If you receive an email titled [email virus hoax name here], do not open it! Delete it immediately! It contains the [hoax name] virus. It will delete everything on your hard drive and [extreme and improbable danger specified here]. This virus was announced today by [reputable organization name here]. Forward this warning to everyone you know!

Most virus hoax warnings do not deviate much from this pattern. If you are unsure if a virus warning is legitimate, additional information is available at:

<http://www.symantec.com/avcenter/hoax.html>

Definition Updater

You can use Definition Updater to update virus definitions on unmanaged machines that have access to email.

Note: Definition Updater is provided to you as unsupported software only.

System requirements for Definition Updater

This section lists system requirements for the Distribution Console and the Definition Updater agent.

Distribution Console (server) requirements

- Windows NT 4.x (Workstation or Server) with Service Pack 3 or higher, or Windows 2000
- Intel 486-66 MHz processor (or higher)
- Mouse
- CD-ROM drive
- VGA (SVGA recommended) graphics display
- Minimum 16 MB (32 MB recommended) available memory
- 21 MB free disk space (26 MB during installation)
- Norton AntiVirus must be installed

- A dedicated server email account. Definition Updater works with the following email programs:
 - Microsoft Outlook 97/98/2000
 - Microsoft Outlook Express
 - Microsoft Exchange Client 4.0 or higher
 - Lotus cc:Mail 6.x
 - Lotus Notes 4.x or higher
 - Eudora Pro 4.1 or higher

Definition Updater Agent (client) requirements

- Windows 9x, Windows NT Workstation/Server version 4.x (with Service Pack 3)
- Intel 486-66 MHz processor (or higher)
- Mouse
- VGA (SVGA recommended) graphics display
- Minimum 16 MB of RAM (32 MB recommended)
- 4 MB available hard disk space (depending on mail server type)
- Norton AntiVirus 5.0 for Windows 9x, or workstation installation
- An email account on a compatible email system. Definition Updater works with the following email programs:
 - Microsoft Outlook 97/98/2000
 - Microsoft Outlook Express
 - Microsoft Exchange Client 4.0 or higher
 - Lotus cc:Mail 6.x
 - Lotus Notes 4.x or higher
 - Eudora Pro 4.1 or higher

Location of Definition Updater install program

The Definition Updater install program is located on Disk 1 in the following directory:

Prodmgmt\Nosuprt\Mobileup

Additional Definition Updater install tasks

Definition Updater requires multiple Agent (client) components (one on each update recipient machine). You must install the Agent component to the machines on which you plan to update virus definitions files via corporate email.

Installing an Agent

Each user machine to which you want to send updates must have the Definition Updater Agent installed. The Agent detects, reassembles, and processes virus definitions file updates as they are received. The administrator uses the Distribution Console to send the Agent installation executables to each user via email. Please review the system requirements for the Agent prior to installation.

Installing an Agent is a two part procedure. First, the Administrator distributes the Agent installation package to the required users. Then, each user runs the Agent installation executable to perform the setup.

Administrator install tasks

To install an Agent

- 1 Review the system requirements for the Agent prior to proceeding with the installation.
- 2 From the Symantec System Center console Tools menu, click **Norton AntiVirus > Definition Updater** to start the Distribution Console.
- 3 On the Send tab, under Type, click **Mobile Update Agent Install**.
- 4 Click **Add**.
- 5 In the Mobile Update Agent Install dialog box, select the appropriate install packages, depending on the email type you and persons in your company use, then click **OK**.

They are added to the list.

- 6 Specify the people or groups to which you want to send the Agent installation by doing one of the following:
 - Click **Address Book**. Under Show Names From The, select the address book you want to use.

In the address list, click the names or groups to which you want to send the Agent installation, then click **Add**. The names or groups are added to the list.
 - Click **Manual Add**. Under Email Address, type the email address of the person or group to whom you want to send the Agent installation, then click **OK**. The name or group is added to the list.

For some email types, you must include the gateway when you manually enter an email address.

For more information, see “About your email options” in the online help.

- 7 To change the email message subject line or body text, click **Message Body**.
 - Under Subject, type the subject line you want to appear in the Agent installation emails.
 - Under Text, type the main message you want to appear in the Agent installation emails, then click **OK**.

This subject line and message text appear in each Agent installation email you send.

In your email message, include basic information instructing the recipient on how to deal with the Agent installation executable.

- 8 Click **Send**.

The Agent installation executables are sent, and the Send tab fields are cleared.

The users will receive the Agent installation executable in their email inboxes. They must run the executable to install the Agent (instructions follow).

User install tasks

To install an Agent

- 1 When you receive the Agent installation email message, close all programs except for your email system.
- 2 In your email inbox, open the Agent installation email message.
- 3 Save the attached executable (.exe) file to your hard disk.
- 4 Run the executable (.exe) file.
- 5 In the WinZip self-extraction dialog box, click **Setup**.
The installation files self-extract and an InstallShield wizard message appears.
- 6 Follow any directions on your screen as the setup process proceeds.
- 7 When the Setup Is Finished dialog box appears, click **Launch Mobile Update Agent**.
- 8 Click **Finish**.

The dialog box closes. The Definition Updater Agent icon appears in your Windows system tray. You can proceed to set your Agent email options and monitoring schedule.

Setting Agent email options

After you install Agents, they must check and verify that their email settings are correct. Later, if they switch email systems or addresses, their email settings can also be changed here.

To set Agent email options

- 1 In the Windows system tray, right-click **Mobile Update Agent**.
- 2 Click **Email**.
- 3 In the Mail Settings dialog box, under Email, click the email program you want to use.
- 4 Enter information into each of the fields that appear.

Each email program type displays slightly different entry fields.

For more information on the field information required for each email type, see “About your email options” in the online help.

- 5 Click **Test Settings** to validate the email setting information.
- 6 Click **OK**.

The email settings for this Agent are established. You can now begin to receive updates.

Setting the Agent monitoring schedule

Update recipients can set their Definition Updater Agents to monitor their email systems, that is, to process updates at specific times only, or around the clock (the default). For example, you may want to process updates only during certain business hours.

To set Agent scheduling options

- 1 In the Windows system tray, right-click **Mobile Update Agent**, then click **Schedule**.
- 2 In the Monitoring Schedule dialog box, under Monitor During This Time Period, do one of the following:
 - Click **Always Monitor** to have your updates monitored 24 hours every day.
 - Click **Monitor During The Following Days**. Select a From time and a To time, between which monitoring will occur, and enable the days on which you want monitoring to occur.
- 3 Under Monitor Once Every, select an increment (number) and measure of time (minutes or hours) to specify how often the updates should be monitored within the monitoring period chosen above.
- 4 Click **OK**.

Uninstalling Definition Updater

This section presents information about uninstalling all Definition Updater components.

Uninstalling the Mobile Update Distribution Console

To uninstall the Distribution Console

- 1 On the Windows taskbar, click **Start > Settings > Control Panel**.
- 2 Double-click **Add/Remove Programs**.
- 3 In the Add/Remove Programs Properties dialog box, under the program list, click **Mobile Update Distribution Console**.
- 4 Click **Add/Remove**, then **Yes** to confirm.
The Mobile Update Uninstall program starts.
- 5 Follow the on-screen instructions.

Uninstalling a Definition Updater Agent

At some point you might want to uninstall a Definition Updater Agent (for example, some employees have changed jobs and you no longer need to send updates to them).

To uninstall a Definition Updater Agent

- 1 On the Windows taskbar, click **Start > Settings > Control Panel**.
- 2 Double-click **Add/Remove Programs**.
- 3 In the Add/Remove Programs Properties dialog box, in the program list, click **Mobile Update Agent**.
- 4 Click **Add/Remove**.
The Mobile Update Uninstall program starts.
- 5 Follow the on-screen instructions.

Updating mobile computers with Definition Updater

Definition Updater works with Norton AntiVirus to automatically update virus definitions files over your company's email system. It lets you perform updates quickly and easily for mobile professionals or telecommuters who are frequently away from your network.

Using your current email system and corporate email directories, Definition Updater makes the most of your existing technology to ensure that the update process is seamless and easy. You use a single interface dialog box to select and send update files to anyone in your company, wherever they are. Definition Updater segments the virus definitions files into small, administrator-defined chunks and sends them in multiple email messages to each recipient's email inbox. The recipient's Definition Updater Agent software then detects, rebuilds, and processes the updates automatically, without the need for user intervention.

How Definition Updater works

Definition Updater is composed of two components: a main Distribution Console from which updates are distributed, and a client Agent that is installed on every computer you want to send updates to. The Distribution Console is run by an administrator, who selects the files that need to be distributed for updating, and sends them to your employees. The Agents receive and process the email update packages and provide feedback to the Distribution Console so that the process may be closely monitored.

To offset the problem of delivering the typically large virus definitions files by email, the administrator sets a maximum size (for example, 100K) for the update files. Definition Updater breaks down virus definitions files selected for distribution into manageable chunks of the specified size and sends them in multiple email messages to the chosen persons within your company. When received, the Agent component of Definition Updater automatically detects and reassembles the files, and updates the virus definitions on the Agent computer. If any problems occur during the update process, the Agent automatically generates a "failed update" message and sends it through the user's email to the Distribution Console's Result Log.

Administrator activities

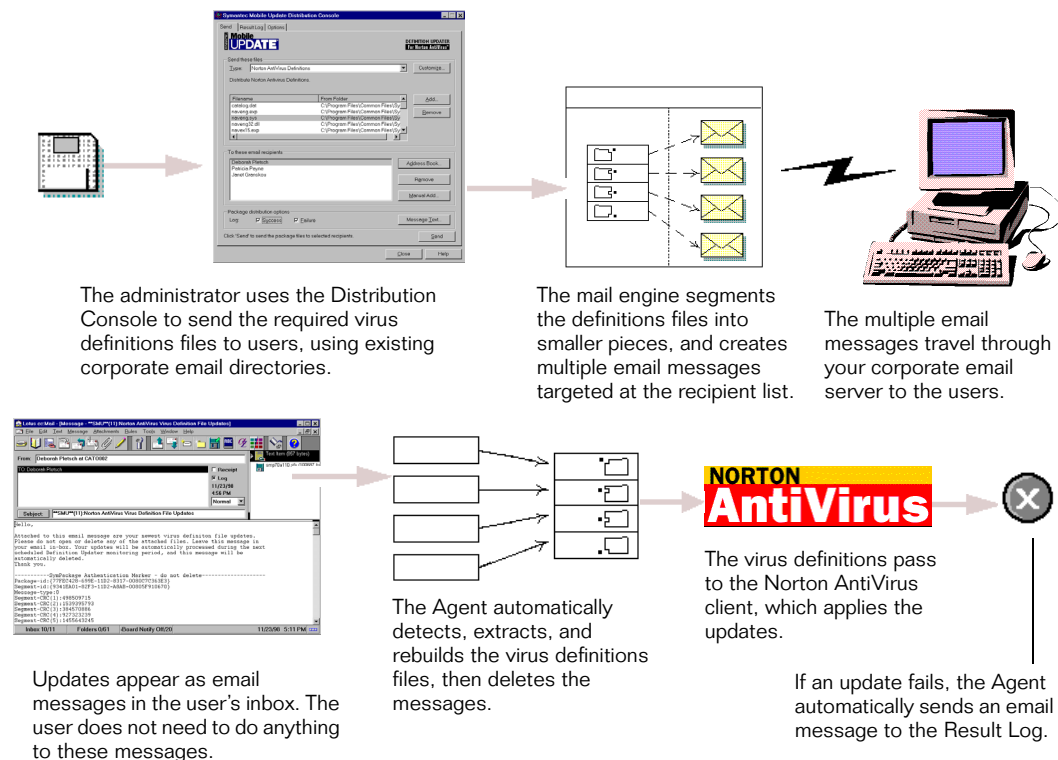
The Distribution Console is set up and run by your Norton AntiVirus administrator. The administrator installs the Distribution Console on a Windows NT 4.0 Workstation or Server and configures the console to use a particular corporate email account to send the updates, and to break down the update files to a more manageable size (for example, 100K). The administrator then sends the selected Agent installation program by email to the desired members of your company.

Note: Definition Updater does not segment the Agent installation package before it sends it to the users. The Agent package is sent at full size.

The administrator uses the LiveUpdate feature on the Distribution Console to ensure that your company has the latest version of Definition Updater. When virus definitions updates are available, the administrator selects the files to be sent and chooses the persons (or email groups) who will receive the updates. The administrator then composes the subject and body text that will appear in each message, and emails the updates to the chosen recipients.

After sending the update packages, the administrator reviews the results of the update in the Result Log on the Distribution Console. If the Result Log records any failed updates, the administrator can manually resend the update packages to the necessary persons.

The following diagram illustrates how Definition Updater processes virus definitions file updates:



User activities

Definition Updater was designed to be almost transparent to the user (the update recipient). After initial installation of the Distribution Console and Agent (see [“Installing an Agent”](#) on page 437), users receive updates through their email inboxes. Update messages wait in the user's inbox until the Agent next performs its monitoring activity, at which time the Agent detects the update messages, reassembles them (as necessary), and applies them to the relevant Norton AntiVirus definitions files. The Agent then automatically deletes the messages and enters an update status message into the user's outbox to be sent to the Distribution Console's Result Log. The user is often unaware that an update has taken place.

If users access their inboxes while update messages are waiting to be processed, they need do nothing with them. The messages exist for information purposes only, and will be deleted automatically. Users simply leave them in their inboxes for future processing.

Using LiveUpdate to update Definition Updater

The LiveUpdate feature allows you to ensure that you are always using the most up-to-date version of Definition Updater available.

To use LiveUpdate to update Definition Updater

- 1 Start the Distribution Console.
- 2 On the Options tab, click **LiveUpdate**.
- 3 In the LiveUpdate Welcome dialog box, follow the on-screen instructions.

LiveUpdate checks if you are running a previous version of Definition Updater, and automatically updates it for you.

Getting started with Definition Updater

This section describes how to start and exit the Definition Updater Distribution Console, how to configure your email and file size settings, and how to use Definition Updater to send virus definitions file update packages to people in your company.

Starting and exiting Definition Updater

The Definition Updater administrator's interface consists of a single, easy to use Distribution Console. The administrator sets the options for virus definitions file update distribution through the Distribution Console.

To start the Definition Updater Distribution Console

- In the Symantec System Center console Tools menu, click **Norton AntiVirus > Definition Updater**.

To exit the Definition Updater Distribution Console

- Click **Close**.

Setting administrator email options

After installing the Distribution Console, specify the email settings you want to use to send email updates to your users. Specify email settings only once. Settings need to be changed only if you want to use a new or different email setup in the future.

To set administrator email options

- 1 Start the Distribution Console.
- 2 On the Options tab, click **Email**.

The screenshot shows the 'Mail Settings' dialog box. It has a title bar with a question mark and a close button. The 'Email program:' dropdown is set to 'Lotus cc:Mail 6.x'. Below it, a note says: 'To login to Lotus cc:Mail 6.x, you need to enter a login name, password, and postoffice path. Your cc:Mail login dialog provides the postoffice path.' The 'Login:' field contains 'Deborah Pletsch'. The 'Password:' field is masked with asterisks. The 'Post office:' field contains 'M:\CCDATA02' and has a 'Browse' button next to it. The 'Maximum attachment size:' is set to '100' KB. At the bottom are 'OK', 'Cancel', and 'Test Settings' buttons. Three annotations with lines pointing to the dialog are on the left: 'Indicate the type of email system you use' points to the 'Email program:' dropdown; 'Enter relevant information about your email account' points to the 'Login:', 'Password:', and 'Post office:' fields; 'Set the maximum file size for your virus definitions update emails' points to the 'Maximum attachment size:' field.

- 3 In the Mail Settings dialog box, under Email program, click the email program you want to use.
- 4 Enter information into each of the fields that appears.
Each email program type will display slightly different entry fields.
For complete details on the field information required for each email type, see “About your email options” in the online help.
- 5 In the Maximum attachment size field, type the maximum segment size (in K) you want to allow for your email update file attachments. The default maximum size is 4096K.

Definition Updater segments all files that are larger than your specified maximum file attachment size into smaller chunks.

- 6 Click **Test Settings** to validate the email setting information.
- 7 Click **OK**.

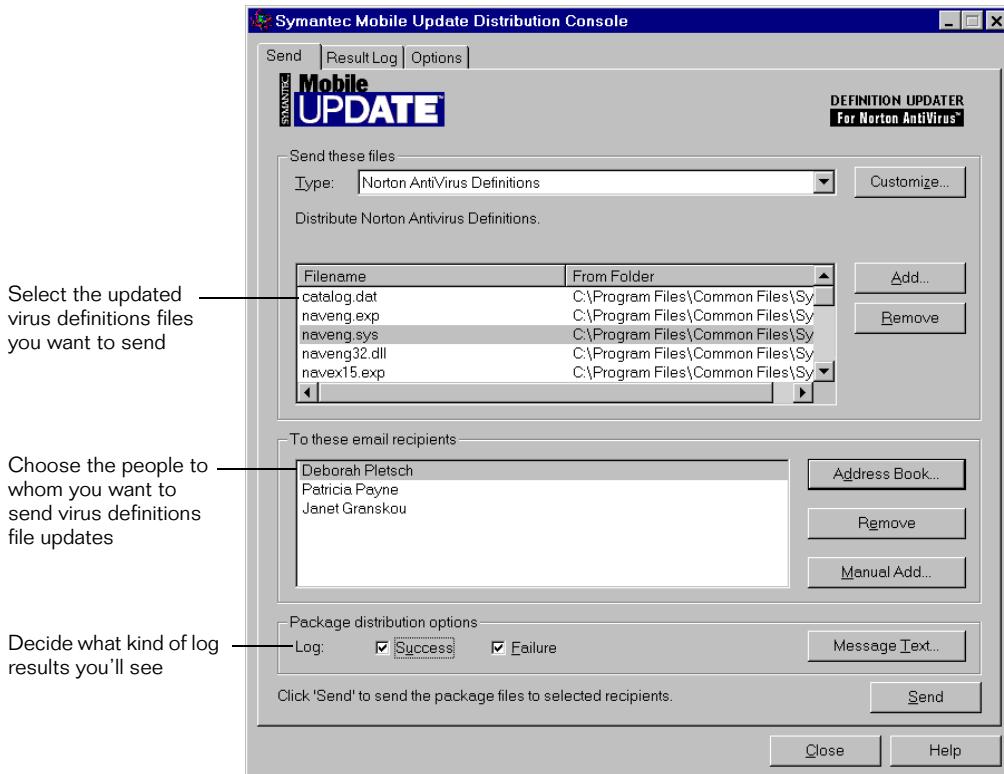
Your email settings are established and you can begin to send updates.

Sending virus definitions update packages

Each time you send virus definitions updates, you must first select the files or folders you want to send, and the people or groups to whom you want to send them.

To send virus definitions update packages

- 1 Start the Distribution Console.
- 2 Click the **Send** tab.



- 3 Under Type, click **Norton AntiVirus Definitions**.
- 4 Click **Customize**.

- 5 In the Norton AntiVirus dialog box, use the browse feature to specify the default directory you want to use as a starting point from which to select virus definitions files, then click **OK**.
- 6 Click **Add**.
- 7 In the Browse For Folder dialog box, select the files or folders you want to send, then click **OK**.

The files are added to the list.

- 8 Specify which people or groups to whom you want to send the updates by doing one of the following:
 - Click **Address Book**. Under Show Names From, select the address book you want to use. In the address list, click the names or groups to whom you want to send updates, then click **Add**.

The names or groups are added to the list.

- Click **Manual Add**. Under Email Address, type the email address of the person or group to whom you want to send updates. Click **OK**.

The name or group is added to the list.

For some email types, you must include the gateway when you manually enter an email address.

See “About your email options” in the online help for details.

- 9 To change the email message subject line or body text, click **Message**.
 - Under Subject, type the subject line you want to appear in the update emails.
 - Under Body, type the main message you want to appear in the update emails, then click **OK**.

This subject line and message will now appear in each update email you send.

In your email message, include basic information instructing the recipient on how to deal with the update email. Recipients should not delete or move an update message, nor try to open the attached files. The email notification messages are for informational purposes only; they are automatically deleted after the updates have been completed.

- 10 Under Package Distribution Options Log, click to check options for the type of feedback you want to receive in the Result Log.

If you want the log to report on successful updates, click **Success**. If you want the log to include failed updates, click **Failure**. You can enable one, both, or neither of the check boxes.

11 Click **Send**.

A message appears stating that the virus definitions update packages have been successfully sent, and the Send tab fields are cleared for the next update.

Note: If you are using Outlook Express to send update packages and have entered an invalid email address, an Outlook Express error message appears. Note the email address involved and close the Outlook Express error dialog box. A message appears stating that the virus definitions update packages have been successfully sent. This applies to the packages sent to valid email addresses only. The packages sent to the invalid address will not be sent or processed; they remain in your Outlook Express outbox until deleted.

The Definition Updater Result Log

The Result Log receives email messages from each Agent following update package processing. The types of messages you receive are determined by the log options you selected before you sent the updates. You can choose to receive log messages for both successfully processed updates and failed updates, or for failed updates only.

Use the Result Log to track the virus definitions file update process, and to ensure that all intended recipients are correctly receiving updates. Remember that some recipients might have their monitoring schedule set for certain days only, so it may be several days before you receive feedback from all recipients following an update package distribution.

The Result Log runs in conjunction with the administrator's email inbox. Log result messages appear in both the inbox and the Result Log simultaneously. If a log entry is deleted from one place, it is deleted from both places.

Viewing the Result Log

The Result Log displays feedback email messages as they are received from each recipient Agent installation of Definition Updater. Entries remain in the Result Log until you delete them.

To view the Result Log

- 1 Start the Distribution Console.
- 2 On the Result Log tab, under Type, click **NAV Virus Definition Files**.
- 3 Click **Refresh** to ensure that you are viewing the most up-to-date log entries.

In the log list, status messages for all updates that have been processed will be displayed by date and time sent, recipient, and status.

Only those updates having the status types specified in the Package Distribution Options Log section will be displayed (see step 10 on page 448).

Deleting entries from the Result Log

All entries remain in the Result Log until you delete them from the list.

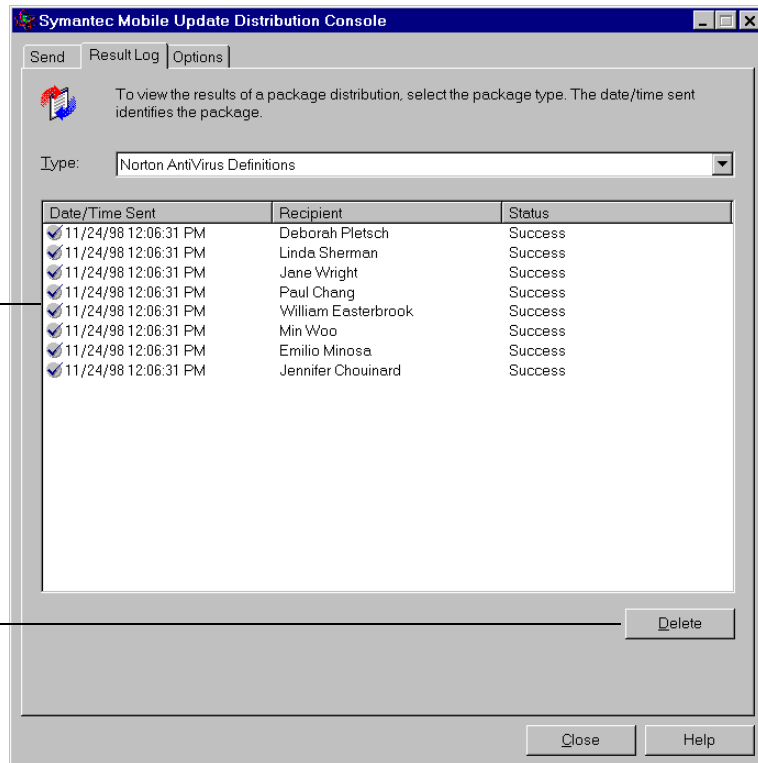
The Result Log runs in conjunction with the administrator's email inbox. Log result messages appear in both the inbox and the Result Log simultaneously. If a log entry is deleted from one place, it is deleted from both places.

To delete log entries

- 1 Start the Distribution Console.
- 2 On the Result Log tab, in the list of log entries, click the log entry you want to delete, then click **Delete**.

Track the results of recent virus definitions update packages

Delete log entries after viewing and responding to them



The entry is deleted from the list.

Definition Updater troubleshooting

This section offers hints for solving common problems, and answers to questions frequently asked by Definition Updater users.

I sent updates to several people earlier today, but there are no items listed in the Result Log. Why not?

There are two important things to remember when viewing the Result Log. The first is that you must enable one or both of the Success and Failure check boxes in the Package Distribution Options Log section of the Send tab before sending update emails in order to receive log messages (see step 9 of [“Sending virus definitions update packages”](#) on page 447).

Secondly, remember that some of your users may have set their monitoring schedules so that updates are only performed at certain times, on certain days of the week (see [“Setting the Agent monitoring schedule”](#) on page 440). Until the updates are actually performed, no log messages will be received.

I sent a virus definitions file update to 30 people two days ago, and have received confirmation of all these updates in the Result Log. One of them is listed as Failed. What should I do?

When a Result Log message shows that an update has failed, it indicates that something has gone wrong with the update process. This can be any one of a number of things, such as a corrupt original or update file, a problem with the user's email system, a transmission error, and so on.

The best thing to do if an update registers as failed is to simply resend the same files to the affected users a second time. Wait to see if the resent updates are processed successfully.

If all of your updates register as failed, then the problem is most likely with your email setup or system. Check that your Distribution Console email options have been set correctly. Next check that your corporate email server is functioning properly; a server crash might affect an entire update package transmission. Resend updates as soon as possible.

The updates that I send to a particular person repeatedly fail. What can I do to solve this problem?

If you repeatedly encounter problems when sending updates to a particular email address, check that both your Distribution Console and the relevant Agent installation are correctly set up for the email type and account involved in the message transaction. Have the affected recipient check his or her Agent email setup (see [“Setting Agent email options”](#) on page 439). Then check that the Distribution Console is set to function with that user’s email system. If both components appear to be correctly set up, the problem may be with the user’s email server or system. Investigate as required and resend updates as soon as possible.

A user accidentally deleted an update message. What impact will this have on the update process?

When users receive update messages in their email inboxes, they must not move, delete, or open the messages or any of the attached files. If a user alters, moves, or deletes an update message before it has been detected, the Agent will not be able to process the update correctly, and the virus definitions file update will fail.

Remember to instruct your users on these issues in the email message that accompanies each update package (see step 8 of [“Sending virus definitions update packages”](#) on page 447).



Virus Scan for DOS

Vscand.exe is a DOS scanner that you can run in batch mode with one or more command-line options.

Understanding Virus Scan for DOS

Norton AntiVirus uses Vscand.exe for scanning Windows 3.1 and DOS computers during logon. For Windows 3.1 and DOS computers that are not connected to the network, you can add Vscand.exe to the Autoexec.bat file so that it automatically runs at startup.

If you run Vscand.exe on a network drive, you might need to enter a password. The default password is:

symantec

You can change the password by running Vscand.exe with the /W option.

Remove or overwrite older copies of Vscand.exe from earlier versions of Intel LANDesk Virus Protect, LANProtect, or LANDesk Manager. Otherwise, if a user runs Vscand.exe without specifying the full path, the computer might use an older version of Vscand.exe.

Configuring command-line scans

Many command line options have long name switches that you can use instead of the letter code. For example, you could enter either the /A or the /Allnozip option to scan all files in the directory except compressed files. Both options have the same function. Run Vscand.exe with the /? option to see the long names for the switches if you want to use them.

The /W option does not display in the onscreen list, but it is functional.

Option	Description
/?	Displays a list of Vscand.exe command line switches.
Drive:[path]	Required for Vscand.exe to know which directories/files to scan.
/A	Scans all files except compressed files in the current directory on the specified drive.
/AZ	Scans all files in the current directory on the specified drive, instead of using *.*. To scan a different directory, type the full directory path on the command line with the /A option. For example, enter Vscand C:\Temp /A to scan all files in the TEMP directory.
/C	Cleans infected files automatically. This switch does not work if the /NC switch is used.
/CM	Cleans infected Word macro files automatically.
/D	Deletes all infected files found, instead of prompting you for confirmation to delete each infected file as it is found. Any files deleted with the /D option are not placed in the Recycle Bin. These files can only be retrieved with an undelete utility.
/DZ=x	Decompress layers. If a compressed file is nested inside another compressed file, by default Vscand will not scan that nested file. Use this switch to force the scan into x levels of nested layers. The switch default is to scan two levels deep.
/HE	Displays error (return code) help screen.

Option	Description
/L=filename	Records all the events of the current scan to the specified file, not on-screen. If you do not specify a file name, an auto-incrementing file (Vplog\$.rpt) is opened and written to the current directory.
/LA=	Specifies a three-character language code for Vscand to use.
/M	Scans the memory only. No disk files are scanned.
/NA	Does not create alert files even if a virus is found.
/NB	Cancels scanning of the boot sector and partition area of the hard drive.
/NC	Cancels the option prompts (Clean, Delete, and Leave Alone) while Vscand.exe is run. Vscand.exe reports any detected viruses to the Norton AntiVirus master log file, or the file specified by the /L filename option.
/NL	Does not create a log file when viruses are found.
/NM	Cancels scanning of the computer's memory. Verify that memory is clean before using this option.
/NS	Cancels scanning of subdirectories below the current directories of the specified drives.
/P	Scans hard drive partition only. Specify the drive you want to scan with this option. For instance, use Vscand C: /P to scan the C drive partition.
/Q	Does not display file names as they are scanned.
/RP	Restores the original partition table if Vscand.exe was unable to clean it correctly.
/S=[dd]	Schedules Vscand.exe to scan one day of the month ([dd] stands for the date). In cases where the date is only one digit, only enter one digit. 0 tells Vscand.exe to scan daily. Use this option if you add Vscand.exe to the system logon script.
/S=[www]	Schedules Vscand.exe to scan once a week ([www] represents an abbreviation of the day of the week). Acceptable abbreviations are Sun, Mon, Tue, Wed, Thu, Fri, and Sat. Use this option if you add Vscand.exe to the system logon script.

Option	Description
/SE	Scans files with default extensions: .com, .exe, .sys, .bin, .xls, .dll, .doc, .dot, .ovl, .htm, .htt, .vps, .js, .shs, .ppt, and .mso.
/SE=xxx,yyy,zzz	Scans files with specified extensions.
/U	Prevents users from interrupting Vscand.exe. With this option enabled, users cannot stop the scan by pressing Ctrl+C at their computers.
/V	<p>Scans all local volumes (both floppy and hard drives). You can specify file types to be scanned across all volumes. For example, to scan only .doc and .dot files in all volumes, enter:</p> <pre>Vscand *.doc *.dot /V</pre> <p>This option scans all .dot and .doc files on all local drives. Do not specify a drive letter when you use the /V option. For example, Vscand C: * .doc /V scans only the .doc files on the C drive, not on all local drives.</p>
/W	Configures whether Vscand.exe requires users without supervisory rights to enter a password before they can scan network drives. The default password is symantec. This option does not display with the /? option.
/WT	If Word macro viruses are found, the alert times out after 10 seconds and continues.
/WT=x	You can set the time the computer waits for a response with the /WT option. The alert times out after x seconds and continues.

Vscand.exe DOS error levels and error messages

There are several DOS error levels that Vscand.exe returns if a virus is found or if an error was made in executing Vscand.exe. If more than one error occurs, the sum indicates which errors occurred. For example, errors 4 and 8 return a DOS error of 12.

Use the error levels shown in the table below to prepare a batch file that automates virus scanning on your network.

In addition to the DOS error levels, Virus Scan for DOS displays a limited number of error messages to the user.

DOS error level	Meaning
0x00	No error.
0x01	Error in the command-line option.
0x02	Vscand.exe was unable to locate a valid virus definitions file. Copy the virus definitions file to the Vscand.exe folder, or map a drive to the server where Norton AntiVirus was installed.
0x04	A virus was found in the computer's memory. Remove the virus by turning off the workstation and starting from a clean system disk.
0x08	A boot or file virus was found on the scanned drive. Review the scan report to find out which file is infected.
0x10	Vscand.exe was unable to locate the specified drive.
0x20	Vscand.exe was canceled by the user by pressing Esc. A message stating that the user stopped the scan is recorded in Vplog.rpt.
0x40	Self Check error occurred, or an internal consistency check error occurred.

In addition to the DOS error levels, Virus Scan for DOS also displays a limited number of error messages to the user.

Error displayed	Meaning
-1	Definitions file is corrupted. To fix this problem, re-expand a copy of the definitions file.
-2	Out of memory error occurred during definitions file loading. Vscand uses and requires 425 KB of RAM. To fix this problem, free more DOS memory. Drivers and TSR programs in Config.sys and Autoexec.bat all utilize memory, possibly not leaving enough for Vscand to run. One option is to load some programs and drivers into upper memory, which will free up conventional memory. You could also increase the amount of RAM on the workstation.
-3	<p>CRC error during definitions load. This probably means that the definitions file is corrupted. To fix this problem, get a new definitions file that does not fail a CRC check.</p> <p>A CRC is a number that is stored in the definitions file when it is created. When Vscand loads a definitions file, it runs some calculations to recreate this number. If the stored number and generated number do not match, Vscand assumes that the definitions file has changed and is corrupted.</p>
-94	<p>This definitions file version does not match the file extension number. To fix this problem, copy/download the definitions file again to ensure that it has the correct name and internal definitions number.</p> <p>Vscand returns this error when it detects an inconsistency between the virus definition number in the definitions file's file name (for example, lpt\$vpn.286) and the number stored inside the virus definitions file. This error would occur if you changed a virus definitions file's name from lpt\$vpn.286 to lpt\$vpn.300. This is a self check to ensure that Vscand uses the correct definitions file.</p>

Error displayed	Meaning
-95	Cannot find new definitions file structure; need old definitions file. To fix this problem, use the latest version of Vscand. Definitions files come in two formats, one old and one new. The latest version of Vscand requires a definitions file stored in the new format to run.
-96	Open definitions file failed. The file might be locked against more than one program reading it at a time. To fix this problem, make sure that Vscand is not trying to run more than one copy at the same time. For example, two DOS boxes in Windows could be trying to run Vscand at the same time. Since DOS does not multitask, it generally cannot handle this. If both copies of Vscand attempt to read the definitions file at the same time, this error could result.
-97	Cannot read new definitions file headers. The definitions files might be corrupted or outdated. This error is similar to error -95. To fix the problem, get a new definitions file.
-98	Cannot find definitions file in current directory. To fix this problem, make sure a copy of the definitions file exists in the directory from which Vscand was run. When Vscand runs, it checks for a definitions file in the directory from which it was run. If a definitions file cannot be found, this error results.

Sample batch file

The sample batch file below shows how you might use error codes to automate virus scans using Vscand:

```
vscand rbs\*.vom /nc
if errorlevel 8 goto l8
if errorlevel 7 goto l7
if errorlevel 6 goto l6
if errorlevel 5 goto l5
if errorlevel 4 goto l4
if errorlevel 3 goto l3
if errorlevel 2 goto l2
if errorlevel 1 goto l1
echo bad value
goto end
:l1
echo errorlevel = 1
goto end
:l2
echo errorlevel = 2
goto end
:l3
echo errorlevel = 3
goto end
:l4
echo errorlevel = 4
goto end
:l5
echo errorlevel = 5
goto end
:l6
echo errorlevel = 6
goto end
```

```
:l7  
echo errorlevel = 7  
goto end  
:l8  
echo errorlevel = 8  
:end
```


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, 2) your damaged CD, and 3) your payment (see pricing below, add sales tax if applicable), to the address below to receive replacement CD. *DURING THE 60-DAY LIMITED WARRANTY PERIOD, THIS SERVICE IS FREE.* You must be a registered customer in order to receive CD replacements.

FOR CD REPLACEMENT

Please send me: ☐ CD Replacement

Name

Company Name

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

City State Zip/Postal Code

Country* Daytime Phone

Software Purchase Date

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

Briefly describe the problem:

CD Replacement Price \$ 10.00
Sales Tax (See Table) \$ 9.95
Shipping & Handling
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 (800) 441-7234

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

Symantec and Norton AntiVirus are trademarks of Symantec Corporation.
Other brands and products are trademarks of their respective holder/s.
© 2001 Symantec Corporation. All rights reserved. Printed in the U.S.A.



I N D E X

A

- Alert Management System 24
- AppSec 85
- automatic startup for Windows NT server 127

B

- boot viruses 78
 - cleaning with rescue disk 385
 - infecting floppy disks 387

C

- cache, enabling to speed logon scans 342
- cached server group passwords 221
- Central LiveUpdate 258
- Central Quarantine
 - client forwarding 359
 - creating 357
 - enabling 358
 - updating definitions 378
- changing
 - client expiration level 250
 - client management status 225
- cleaning infected files 349
- client configuration updates 399
- ClientConfig key 232
- clients
 - changing management status 225
 - configuration types 26
 - creating installation disks 176
 - deleting 249
 - evaluating during testing 77
 - expiration level, changing 250
 - forwarding for Central Quarantine 359
 - installing to 137, 140
 - interaction with parent server 39
 - lightly managed 27
 - managed 27
 - managing with Roaming Client Support 43

- clients (*continued*)

- overview of centralized scanning
 - control 251
 - protection for 25
 - scans 293
 - sometimes managed 27
 - sometimes unmanaged 27
 - traffic 66
 - understanding client scans 293
 - unmanaged 28
 - viewing virus list for 255
- client-to-server ratios 392
- cluster servers, protecting 72
- Command-line switches for Roaming Client Support 58
- communications port, default 251
- compressed files, scanning 79
- configuration trade offs for scanning 78
- configuring
 - automatic installations on NetWare servers
 - without Symantec System Center 129
 - client forwarding for Quarantine 359
 - logon scan options 336
 - manual scans 311
 - manual, scheduled, and realtime scan
 - options 295
 - options to exclude files from scanning 301
 - options to include files for scanning 304
 - realtime protection for email
 - applications 323
 - resetting clients to accept server group-level configuration 316
 - resetting clients to accept server-level configuration 316
 - resetting servers to accept server group-level configuration 316
 - scan options 295
 - on multiple selected computers 294
 - scheduled scans 324

- configuring (*continued*)
 - settings that apply when server group, server, and client settings differ 416
 - single computer 307
- console, selecting from right console pane 223
- CPU utilization, setting 310
- creating server group 218
- customer profiles
 - enterprise-sized organization 98
 - large organization 92
 - medium-sized organization 89

D

- dates of virus definitions files, verifying 255
- Definition Updater (unsupported software) 435
- Defwatch.exe 427, 428
- deleting
 - clients 249
 - files from Quarantine 377
 - histories 353
 - infected files 349
 - scheduled scans 334
 - server groups 218
- disk image on the server, installing from 175
- distributing Norton AntiVirus with SMS Package
 - Definition Files 181
- DOS scanning 455

E

- email
 - installing support 138
 - Lotus Notes, configuring scans for 323
 - scanning 82
- Email-based Scan and Deliver 374
- Emergency Disk
 - cleaning boot viruses 385
 - recovering from boot virus 385
 - restoring infected boot sector 387
- enabling and configuring 339
- error levels and error messages for
 - Vscand.exe 459
- evaluating client components 76

- Event Log 351
 - clearing items 353
 - filtering items by date 346
 - sorting columns 346
 - working with Event Log data 31
- events written to Windows NT Event Log 429
- excluding
 - files from scanning 301
 - files on single and multiple computers 304
- expiration level, client
 - changing 250

F

- file exclusions 302
- files
 - cleaning infected 349
 - deleting infected 349
 - moving to Quarantine 350
 - scanning compressed 79
 - undoing action taken 349
- filtering
 - Event Log items by date 346
 - server group view in the console 217
 - Virus Found alerts 382
- floppy disk infection 387

G

- Grc.dat file 223
 - annotated 237
 - editing 226, 234
 - structure 237
- Grcsrv.dat 223
- grouping servers into server groups 217

H

- history, viruses and scans 31

I

- icons
 - in Windows System Tray, enabling 249
 - Scan History 351
 - Virus History 348
- idle scans, configuring for clients 342
- importing IP addresses during install 119

- incomplete update, resolving 415
- infections, managing 355
- initializing virus protection for Windows NT servers 116
- installing
 - 16-bit clients need TEMP directory in Autoexec.bat 170
 - AMS to computers where Norton AntiVirus is already installed 126
 - both Norton AntiVirus for Servers and Alert Management System 117
 - client installation methods 140
 - configuring automatic installations on NetWare servers without Symantec System Center 129
 - configuring client installation at logon 171
 - email support 138
 - from client disk image on the server 175
 - from floppy disks or self-extracting .exe 175
 - how to create text file with IP addresses to import 111
 - into NDS 114
 - locating servers when 111
 - Norton AntiVirus Corporate Edition 33, 63, 105
 - system requirements for clients 135
 - Norton AntiVirus Corporate Edition management snap-in 130
 - order of product installation 74
 - preparing for client installation 137
 - required restarts 115
 - restarting Windows NT server with automatic or manual startup 127
 - server 116
 - staged installations 74
 - troubleshooting issues 407
 - uninstalling
 - from NetWare primary servers 132
 - from NetWare secondary servers 133
 - from Windows NT Server manually 132
 - Norton AntiVirus management snap-in 131
 - with logon scripts 169
- Intelligent Updater 259

- Internet-based Scan and Deliver 360
- IP addresses, creating a text file for install 111

L

- lab testing Norton AntiVirus Corporate Edition 75
- lightly managed clients 27
- live viruses, handling 82
- LiveUpdate 258
 - configuring
 - clients to retrieve from Symantec FTP site or LiveUpdate server 274
 - servers to retrieve from Symantec FTP site 273
 - configuring for missed events 269
 - scheduling for clients 274
 - setting advanced scheduled options 267
 - setting client policy for 275
 - using UNC share on an internal server 422
 - using with internal LiveUpdate server 276
- locking
 - server groups 220
- locking realtime options 315
- log type comparisons 344
- logon scans 31
 - enabling disk cache to speed up 456
 - enabling on NetWare 341
 - options 336
 - preventing users from canceling 338
 - selecting file types to scan 339
 - setting command line options 340
- logon scripts, installing with 169
- Lotus Notes, configuring scans for 323

M

- macro viruses 79
- managed clients 27
- managing server groups 216
- manual scans 30
 - configuring 311
 - options 313
- manual startup for Windows NT server 127
- Maple drivers and NetWare 108
- master primary server 37

- Microsoft Exchange server and Norton AntiVirus 424
- Microsoft Management Console 23
- Microsoft Systems Management Server SMS packages 181
- migration
 - automatic 194
 - for clients 203
 - for servers 197
 - from an existing LiveUpdate server 198
 - from LANDesk Virus Protect 198
 - from Norton System Center 197
 - when custom settings are lost 195
- migration, planning 192
- missed LiveUpdate events, configuring for 269
- mobile clients, managing 43
- moving
 - files to Quarantine 350
 - servers from one server group to another 34
- moving a server to a different server group 223

N

- NDS errors 408
- NetWare
 - logon scanning 339
 - Quarantine forwarding requirements 109
 - required rights to install to servers 113
- NetWare primary servers, uninstalling from 132
- NetWare secondary servers, uninstalling from 133
- network traffic
 - client 83
 - planning for 64
- Norton AntiVirus Corporate Edition
 - how it works 24
 - new features in version 7.6 21
 - scalability planning information 391
 - server specifications 401
 - Terminal Server protection 84
 - what you can do with 28
- Norton AntiVirus Corporate Edition
 - overview 22, 24
- notification mechanisms
 - customizable message box 344
 - virus histories 344

O

- on-demand scans 30
- overview of Norton AntiVirus Corporate Edition 22

P

- Package.exe 175
- parent server 38
- parent vs. primary servers 38
- password, saving and changing 221
- Pds.exe 427
- performance issues, troubleshooting 420
- planning
 - alert management 83
 - client installation 137
 - management policy 83
 - migration 192
 - questions 391
 - server groups 33, 40
- port, default 251
- primary server 35
 - uninstalling from NetWare primary server 132
- profiles
 - enterprise-sized organization 98
 - large organization 92
 - medium-sized organization 89
- program viruses 79
- protocols
 - required 64
 - supported 71

Q

- Quarantine
 - alert settings 372
 - Central Quarantine
 - client forwarding 359
 - creating 357, 358
 - deleting files from 377
 - Email-based Scan and Deliver 374
 - Internet-based Scan and Deliver 360
 - NetWare requirements 109
 - repairing and restoring files 377

R

- randomizing virus definitions file updates 268
- realtime scanning 30, 313, 317
 - configuring for mail applications 323
 - denying access to infected files 318
 - email support issues 314
 - file caching for 313
 - locking options 315
 - resetting options 315
- repairing files in Quarantine 377
- requirements. *See* system requirements.
- Rescue Disk set 187
- restarting Windows NT server with automatic or manual startup 127
- restarts, required 115
- restoring files in Quarantine 377
- rights
 - to install to NetWare servers 113
 - to install to Windows NT clients 137
- Roaming Client Support 43
 - command line switches 58
 - creating server list text files 49
 - how it works 45
 - implementation tasks 48
 - load balancing and marking primary and backup servers 53
 - management limitations 48
 - requirements 49
 - running as a command line utility 58
 - specifying parent server types 55
 - specifying primary server with a list of backup servers 54
 - using Roamadmin 52
 - when to use it 44
- rolling back a virus definitions file 282
- rolling out
 - clients using third party products 181
 - SMS Package Definition Files 181
 - virus definitions files 254
 - with Microsoft IntelliMirror 185
- Rtvsan.exe 427, 428
- Rtvsan95 caused General Protection Fault in Module Kernal386.exe 412

S

- saving server group password 221
- scalability
 - operations that do not affect scalability 405
 - planning information 391
- Scan and Deliver
 - Email-based 374
 - Internet-based 360
- scan history 31, 350
 - creating a report 351
 - data format 350
 - filtering items by date 346
 - icons 351
 - sorting columns 346
- scanning
 - assigning actions 296
 - by file type 78
 - clients 293
 - compressed files 79, 309
 - configuration trade offs 78
 - configuring manual scans 309
 - dimmed or missing options 295
 - displaying warning message on client 297
 - DOS 455
 - drives 80
 - email 314
 - on client computers 82
 - excluding files and folders 304
 - files
 - being accessed 81
 - being modified 81
 - for viruses 289
 - locking realtime options 315
 - manual, scheduled, and realtime scan options 295
 - options 295
 - assigning actions 296
 - displaying scan progress 297
 - logon scan 336
 - manual 309
 - NetWare logon 339
 - realtime protection for files 317
 - resetting for realtime protection 315
 - scheduled scans 324
 - selecting drive types to scan 319
 - Windows NT logon scanning 340
 - realtime 313

scanning (*continued*)

- recommended extensions to scan 305
 - remote scans of email data 314
 - scheduled scans 31
 - deleting 334
 - disabling 334
 - editing 334
 - running on demand 335
 - selecting
 - file types and extensions 305
 - files and folders to scan 307
 - servers 289
 - setting
 - client realtime protection options at server or server group level 314
 - CPU utilization 310
 - options on multiple selected computers 294
 - realtime protection for files 317
 - single computer 307
 - troubleshooting 418
 - when to scan 80
- scenarios 89
- secondary server 36
- self-extracting .exe, creating 178
- server groups 34
- cached passwords 221
 - changing password 219
 - creating 218
 - deleting 218
 - description 34
 - filtering views 217
 - grouping servers 217
 - how to view 34
 - including both Windows NT and NetWare servers 40
 - locking 83
 - locking and unlocking 220
 - managing 216
 - options applied at the server group level 41
 - planning 33, 40
 - renaming 218
 - selecting primary server for 219
 - unlocking 221
 - viewing 34
 - what happens when you move server to a new server group 223

servers

- changing primary and parent servers 222
 - evaluating during testing 75
 - installation 116
 - enabled sharing requirement 113
 - procedure 114
 - restart may be required 115
 - restarting Windows NT server with automatic or manual startup 127
 - rights required for Windows NT 113
 - rights to install 113
 - verifying network access 112
 - locating during installation 114
 - master primary 37
 - moving from one server group to another 34
 - parent 38
 - parent server issues 26
 - primary 35
 - protecting cluster servers 72
 - protection for 25
 - scans 289
 - secondary 36
 - types
 - master primary server 37
 - parent server 38
 - primary server 35, 231
 - secondary server 36
 - understanding installation options 116
 - viewing virus list for 255
- services
- Norton AntiVirus Corporate Edition 342, 455
 - Symantec System Center and Alert Management System 427
- Shutdown 412
- SMS PDF files for distributing Norton AntiVirus 181
- sometimes managed clients 27
- staged installations 74
- sweep, virus 31, 290
 - running 384
- Symantec Security Response 357
- Web site 431
- Symantec System Center 24

- system requirements
 - clients 136
 - DOS client 137
 - management snap-in 110
 - NetWare servers 108
 - required protocols 64
 - Windows 3.x client 136
 - Windows 95/98/NT 4.0/2000 client 136
 - Windows NT servers 106

T

- Terminal Server 84
 - compatibility 106
- testing Norton AntiVirus Corporate Edition in lab 75
- third party products for rollout, using 181
- traffic
 - client 66
 - server-to-server 65
 - Symantec System Center 64
- tree, selecting from 223
- troubleshooting
 - can't see NetWare server to update 414
 - cannot stop a scan on compressed file 419
 - changes during an update 414
 - computer runs slower after client installed 420
 - configuration changes do not work 419
 - configuring 16-bit clients 418
 - difficulty configuring or running scans 418
 - how to use LiveUpdate Administration Utility 416
 - incomplete discovery process 423
 - initial memory usage drop when scanning under Windows 2000 420
 - invalid container name or password entered during installation 409
 - issues configuring group of selected clients 418
 - locating servers during install 410
 - Maple drivers and NetWare 108
 - NDS errors when installing to a NetWare 4.x server running an outdated Clib.nlm 109
 - NetWare server can't update from Windows NT server in another group 422

troubleshooting (*continued*)

- Norton AntiVirus and Microsoft Exchange server 424
- outdated Clib.nlm 408
- page fault value increase when Rtvscan has no activity 420
- pattern file updates 421
- performance issues 420
- Quarantine and NetWare 109
- Rtvscan issues 418
- same 16-bit client displays twice in console after update 414
- server or client missing from tree view of Symantec System Center Console 411
- settings that apply when server group, server, and client settings differ 416
- shutdown issues after Norton AntiVirus Corporate Edition is installed 412
- some servers not updated 423
- specifying a container for logon scripts on NetWare 409
- startup issues after Norton AntiVirus Corporate Edition is installed 412
- temporary space required on the SYS volume 109
- Unable to load Listview.ocx error 408
- update failed or did not complete 415
- virus scans 418
- Windows NT Workstation limitations 416

U

- Unable to load Listview.ocx error 408
- UNC share, using with LiveUpdate internal server 422
- uninstalling
 - from NetWare primary servers 132
 - from NetWare secondary servers 133
 - from Windows NT Server manually 132
 - Norton AntiVirus management snap-in 131
 - Norton AntiVirus program for desktops 415
- unlocking server groups 220
- unmanaged clients 28
 - how to make managed 225

- updating
 - optimal number of threads for update
 - operations 394
 - products and virus definitions files with Package.exe 284
 - servers and clients with Norton AntiVirus
 - product updates 283
 - testing updates 262
 - to Norton AntiVirus Corporate Edition 7.5 191
 - troubleshooting 210
 - virus definitions files
 - choosing a method 257
 - examples 285
 - Intelligent Updater 283
 - LiveUpdate 273
 - Virus Definition Transport Method 259
 - virus definitions files with Package.exe 284

V

- viewing
 - client protection settings from the console 28
 - histories 344
 - virus list for server or client 255
- Virus Definition Transport Method 259
 - implementation examples 261
 - testing updates 262
 - updating
 - NetWare servers 266, 270
 - servers 262
 - updating NetWare servers not running TCP/IP 272
 - versus LiveUpdate 403
- virus definitions files 254
 - rolling back 282
 - rollouts 254
 - troubleshooting updates 421
 - update methods 257
 - update performance 396
 - updating on Central Quarantine 378
 - verifying dates 255
- Virus Found alerts, filtering 382
- virus handling actions 82

- Virus History 31
 - filtering items by date 346
 - icons 348
 - procedures 349
 - sorting columns of data 346
 - viewing 344
- virus list 255
- virus protection for Windows NT server,
 - initializing 116
- Virus Scan for DOS 455
- virus sweeps 31, 290
 - running 384
- viruses
 - .com and .exe 79
 - boot 78
 - boot sector 432
 - creating a test file 76
 - file infector 432
 - handling 82
 - hoaxes 434
 - macro 79, 433
 - master boot record 432
 - multi-partite 433
 - removing a warning icon 381
 - Trojan horse 433
 - worms 434
- Vscand.exe 81
 - command line options 456
 - error levels and error messages 459
 - sample batch file 459, 462

W

- warning icon, clearing 381
- warning message, displaying on an infected computer 297
- What's new in Norton AntiVirus Corporate Edition 7.6 21
- Windows NT
 - server restart may be required after
 - installation or update 115
 - Workstation limitations 75
- Windows NT/2000
 - logon scanning, enabling and configuring 340
 - protecting cluster servers 72