

"Whether you are managing an existing NAVCE 7.6 configuration or implementing SAVCE version 8.x, this book will help you get the most out of your software installation..."

—David Banes, Symantec Security Response, Asia Pacific Regional Manager

SYNGRESS®

1 YEAR UPGRADE
BUYER PROTECTION PLAN



CONFIGURING SymantecTM AntiVirus Corporate Edition

Develop an Effective Enterprise AntiVirus Solution!

- Complete Coverage of Symantec System Center (SSC) Console
- Prepare for the Symantec Product Specialist (SPS) Certification Exam 250-011
- Master the "Three Cs" of Virus Response: Containment, Cleanup, and Communication

Laura E. Hunter

Athar A. Kahn

James Stanger, Ph.D.

Jay Cee Taylor

Robert J. Shimonski Technical Editor

With more than 1,500,000 copies of our MCSE, MCSD, CompTIA, and Cisco study guides in print, we continue to look for ways we can better serve the information needs of our readers. One way we do that is by listening.

Readers like yourself have been telling us they want an Internet-based service that would extend and enhance the value of our books. Based on reader feedback and our own strategic plan, we have created a Web site that we hope will exceed your expectations.

Solutions@syngress.com is an interactive treasure trove of useful information focusing on our book topics and related technologies. The site offers the following features:

- One-year warranty against content obsolescence due to vendor product upgrades. You can access online updates for any affected chapters.
- “Ask the Author” customer query forms that enable you to post questions to our authors and editors.
- Exclusive monthly mailings in which our experts provide answers to reader queries and clear explanations of complex material.
- Regularly updated links to sites specially selected by our editors for readers desiring additional reliable information on key topics.

Best of all, the book you’re now holding is your key to this amazing site. Just go to **www.syngress.com/solutions**, and keep this book handy when you register to verify your purchase.

Thank you for giving us the opportunity to serve your needs. And be sure to let us know if there’s anything else we can do to help you get the maximum value from your investment. We’re listening.

www.syngress.com/solutions

CONFIGURING

Symantec

AntiVirus

Corporate
Edition

Laura E. Hunter

Athar A. Khan

JayCee Taylor

James Stanger, Ph.D.

Robert J. Shimonski, Technical Editor

Syngress Publishing, Inc., the author(s), and any person or firm involved in the writing, editing, or production (collectively “Makers”) of this book (“the Work”) do not guarantee or warrant the results to be obtained from the Work.

There is no guarantee of any kind, expressed or implied, regarding the Work or its contents. The Work is sold AS IS and WITHOUT WARRANTY. You may have other legal rights, which vary from state to state.

In no event will Makers be liable to you for damages, including any loss of profits, lost savings, or other incidental or consequential damages arising out from the Work or its contents. Because some states do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

You should always use reasonable care, including backup and other appropriate precautions, when working with computers, networks, data, and files.

Syngress Media®, Syngress®, “Career Advancement Through Skill Enhancement®,” “Ask the Author UPDATE®,” and “Hack Proofing®,” are registered trademarks of Syngress Publishing, Inc. “Syngress: The Definition of a Serious Security Library”™, “Mission Critical™,” and “The Only Way to Stop a Hacker is to Think Like One™” are trademarks of Syngress Publishing, Inc. Brands and product names mentioned in this book are trademarks or service marks of their respective companies.

KEY	SERIAL NUMBER
001	PK9EV4NV43
002	TQMM7T6CVF
003	8J9H4NDREA
004	ZMATTNH89Y
005	U8MPTST3V3
006	KA7HYC4ES6
007	G8JA5QNCAK
008	9J3NNY6RD7
009	T3QULAV6FH
010	5BVF7TNZEL

PUBLISHED BY
Syngress Publishing, Inc.
800 Hingham Street
Rockland, MA 02370

Configuring Symantec AntiVirus Enterprise Edition

Copyright © 2003 by Syngress Publishing, Inc. All rights reserved. Printed in the United States of America. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

Printed in the United States of America

1 2 3 4 5 6 7 8 9 0

ISBN: 1-931836-81-7

Technical Editor: Robert J. Shimonski
Acquisitions Editors: Catherine B. Nolan,
Andrew Williams

Cover Designer: Michael Kavish
Page Layout and Art by: Patricia Lupien
Copy Editor: Mike McGee
Indexer: J. Edmund Rush

Distributed by Publishers Group West in the United States and Jaguar Book Group in Canada.



Acknowledgments

We would like to acknowledge the following people for their kindness and support in making this book possible.

Karen Cross, Lance Tilford, Meaghan Cunningham, Kim Wylie, Harry Kirchner, Kevin Votel, Kent Anderson, Frida Yara, Jon Mayes, John Mesjak, Peg O'Donnell, Sandra Patterson, Betty Redmond, Roy Remer, Ron Shapiro, Patricia Kelly, Kristin Keith, Jennifer Pascal, Doug Reil, David Dahl, Janis Carpenter, and Susan Fryer of Publishers Group West for sharing their incredible marketing experience and expertise.

The incredibly hard working team at Elsevier Science, including Jonathan Bunkell, AnnHelen Lindeholm, Duncan Enright, David Burton, Rosanna Ramacciotti, Robert Fairbrother, Miguel Sanchez, Klaus Beran, and Rosie Moss for making certain that our vision remains worldwide in scope.

David Buckland, Wendi Wong, Daniel Loh, Marie Chieng, Lucy Chong, Leslie Lim, Audrey Gan, and Joseph Chan of STP Distributors for the enthusiasm with which they receive our books.

Kwon Sung June at Acorn Publishing for his support.

Jackie Gross, Gayle Voycey, Alexia Penny, Anik Robitaille, Craig Siddall, Darlene Morrow, Iolanda Miller, Jane Mackay, and Marie Skelly at Jackie Gross & Associates for all their help and enthusiasm representing our product in Canada.

Lois Fraser, Connie McMenemy, Shannon Russell, and the rest of the great folks at Jaguar Book Group for their help with distribution of Syngress books in Canada. David Scott, Tricia Wilden, Marilla Burgess, Annette Scott, Geoff Ebbs, Hedley Partis, Bec Lowe, and Mark Langley of Woodslane for distributing our books throughout Australia, New Zealand, Papua New Guinea, Fiji Tonga, Solomon Islands, and the Cook Islands.

Winston Lim of Global Publishing for his help and support with distribution of Syngress books in the Philippines.

A special thanks to Robert J. Shimonski for his continuing help and dedication to so many Syngress titles.



Contributors

James Stanger (Ph.D., Symantec Technology Architect, Convergence Technology Professional, CIW Master Administrator, MCP, Linux+, A+) is co-author of Syngress Publishing's *E-mail Virus Protection Handbook* (ISBN: 1-928994-23-7) and *Hack Proofing Linux: A Guide to Open Source Security* (ISBN: 1-928994-34-2). A network security consultant and writer, James' specialties include virus management, mail server administration, intrusion detection, and network auditing. Currently Senior Course Director for ProsoftTraining, James consults with Symantec to enable security professionals to deploy virus protection, vulnerability management, and firewall/VPN solutions in enterprise networks. James has also consulted for companies and organizations such as IBM, Securify, Brigham Young University, ITM Technology, and the William Blake Archive. James is the Chairperson of the Linux Professional Institute (LPI) Advisory Council and sits on the CompTIA Linux+ and Server+ cornerstone committees. In addition to authoring books for Syngress, James has also authored security books and courses for Sybex, Osborne/McGraw-Hill, and ComputerPREP. James resides in Washington.

Chris Mosby (Symantec Product Specialist) is a Senior Network Specialist at Bechtel Hanford, Inc. He currently manages the System Management Server and Virus Protection systems for the Environmental Restoration Contract at the United States Department of Energy's Hanford Nuclear Reservation. At the time of this writing, Chris' implementation of Symantec AntiVirus Corporate Edition, and the use of other antivirus methods, has allowed his company to have zero network downtime due to virus infection, since January of 2000. He was also awarded a Gold Award Certificate by Bechtel Hanford, Inc. for his efforts during the Nimda virus outbreak, where it was calculated that the company was saved one million dollars in potential lost work. Chris is also a columnist for the myITforum.com Web site, where he has written articles on Systems Management Server and antivirus topics. Chris holds an associate's degree in Physics, and lives in Kennewick, WA with his wife, Debbie.

Athar A. Khan (Symantec Product Specialist NAVCE, MCSE, MCSA,CCA) is a Wintel (Windows Systems on Intel Platforms) Systems Engineer at a high tech company in southern California. Athar solely architected, implemented and supported a global, enterprise-wide Norton AntiVirus Corporate Edition solution using 10 NAVCE servers for 4,000+ systems in over 30 office locations and numerous home offices. As the NAVCE Administrator, Athar devised incident response strategies to prevent, contain, and counter virus threats and outbreaks including Nimda and Code Red. Currently, Athar is architecting, implementing, and supporting an enterprise-wide data backup and disaster recovery solution that will ultimately protect over 10 Terabytes of data using Connected TLM software. In addition to these responsibilities, Athar performs advanced technical support and Windows domain administration with a scope of responsibility that encompasses 500+ servers and 3,500+ clients in over 60 locations worldwide. Athar holds a bachelor's degree in Electrical Engineering from the Illinois Institute of Technology.

Scott Dentler (CISSP, CCSE, CCSA, MCSE, CCNA) is an IT consultant who has served with companies such as Sprint and H&R Block, giving him exposure to large enterprise networks. Scott's background includes a broad range of IT facets, including Cisco routers and switches, Microsoft NT/2000, Check Point firewalls and VPNs, Red Hat Linux, network analysis and enhancement, network design and architecture, and network IP allocation and addressing. He has also prepared risk assessments and used that information to prepare business continuity and disaster recovery plans for knowledge-based systems. Scott is a contributor to *Snort 2.0 Intrusion Detection* (Syngress Publishing, ISBN: 1-931836-74-4).

Jay Cee Taylor (CNA/CNE-4.11, CNA/CNE-5.0, CNA/CNE-6.0, CNS, MCP) is the Senior Network Administrator for Thomson Industries, a branch of the Danaher Corporation's Motion Group. Danaher is a leading industrial company, which designs, manufactures, and markets innovative products. Thomson is a leading manufacturer and provider of linear motion products and engineering. Jay Cee currently supports a large Novell NetWare and Windows environment, managing enterprise-wide accounts, file systems, backup solutions, and virus

protection. His specialties include Novell/Microsoft administration, design, implementation, upgrades and migrations, Computer Associate's ARCserve/BrightStor products, and Symantec's NAVCE. Jay Cee has successfully performed a migration to NAVCE 7.6, and he will soon begin a NetWare 6.0 upgrade and a full migration to SAVCE 8.0. Jay Cee is a Licensed Technical Instructor who worked for several years as a Senior Instructor and Training Coordinator for Computer Career Center of Garden City, NY teaching NetWare administration and engineering, and Windows-based courses. Jay Cee is a member of NUI and currently resides in Hempstead, NY with his two best friends: his younger brother, Peter Schork, and his fiancée, Jennifer Caffiero.

Laura E. Hunter (MCSE, MCT, MCDBA, MCP, MCP+I, CCNA, A+, Network+, iNet+, CNE-4, CNE-5) is a Senior IT Specialist with the University of Pennsylvania, where she provides network planning, implementation and troubleshooting services for various business units and schools within the University. Her specialties include Microsoft Windows NT/2000 design and implementation, troubleshooting, and security topics. As an "MCSE Early Achiever" on Windows 2000, Laura was one of the first in the country to renew her Microsoft credentials under the Windows 2000 certification structure. Laura's previous experience includes a position as the Director of Computer Services for the Salvation Army and as the LAN Administrator for a medical supply firm. She also operates as an independent consultant for small businesses in the Philadelphia metropolitan area and is a regular contributor to the TechTarget family of Web sites. Laura holds a bachelor's degree from the University of Pennsylvania and is a member of the Network of Women in Computer Technology, the Information Systems Security Association, and InfraGard, a cooperative undertaking between the United States Government and other participants dedicated to increasing the security of United States critical infrastructures.

Jason E. Genser (MCP, A+) is a computer consultant specializing in systems management, antivirus and software deployment solutions, and technologies for small- and medium-sized businesses. Jason has more than ten years of extensive hands-on experience with personal computers and net-

works and has designed and implemented the infrastructure of a multi-site, Microsoft SMS 2.0 environment for a subsidiary of Cingular Wireless. Jason is a columnist on www.myitforum.com, a leading Web site for IT professionals and system administrators. He is the technical editor of *TCP/IP Unleashed, Second Edition*, *Microsoft Windows 2000 Professional Unleashed*, and *Microsoft Windows 2000 Server Unleashed*. He is also a contributing author and editor on *Peter Norton's Complete Guide to Windows 2000 Server*. A native and life-long resident of central New Jersey, Jason is a member of the Internet Society and the North American Association of Technology Professionals.



Technical Editor and Contributor

Robert J. Shimonski (TruSecure TICSAs, Cisco CCDP, CCNP, Symantec SPS, NAI Sniffer SCP, Nortel NNCSS, Microsoft MCSE, MCP+I, Novell Master CNE, CIP, CIBS, IWA CWP, DCSE, Prosoft MCIW, SANS.org GSEC, GCIH, CompTIA Server+, Network+, Inet+, A+, e-Biz+, Security+, HTI+) is a Lead Network and Security Engineer for the leading manufacturing company, Danaher Corporation. At Danaher, Robert is responsible for leading the IT department within his division into implementing new technologies, standardization, upgrades, migrations, high-end project planning, and designing infrastructure architecture. Robert is also part of the corporate security team responsible for setting guidelines and policy for the entire corporation worldwide. In his role as a Lead Network Engineer, Robert has designed, migrated, and implemented very large scale Cisco and Nortel based networks.

Robert has held positions as a Network Architect for Cendant Information Technology and worked on accounts ranging from the IRS, to AVIS Rent a Car, and was part of the team that rebuilt the entire Avis worldwide network infrastructure to include the Core, and all remote locations. Robert maintains a role as a part time technical trainer at a local computer school to deliver classes on networking and systems administration whenever possible.

Robert is also a part-time author who has worked on over 20 book projects as an author and editor. He has written and edited books on a plethora of topics with a strong emphasis on network security. Robert has designed and worked on some brand new topics for Syngress Publishing to include the only book dedicated to the Sniffer Pro protocol analyzer. Robert has worked on the following Syngress Publishing titles: *Security+ Study Guide & DVD Training System* (ISBN: 1-931836-72-8); *Sniffer Pro Network Optimization & Troubleshooting Handbook* (ISBN: 1-931836-57-4); *Configuring and Troubleshooting Windows XP Professional* (ISBN: 1-928994-80-6); *BizTalk Server 2000 Developer's Guide for .NET*

(ISBN: 1-928994-40-7); *SSCP Study Guide & DVD Training System* (ISBN: 1-931836-80-9); *Nokia Network Security Solutions Handbook* (ISBN: 1-931836-70-1); and *MCSE Implementing and Administering Security in a Windows 2000 Network Study Guide & DVD Training System* (ISBN: 1-931836-84-1). Robert is also a contributor to the forthcoming *Building DMZs for Enterprise Networks* (ISBN: 1-931836-88-4) and *MCSA/MCSE Exam 70-292 Study Guide & DVD Training System: Managing and Maintaining a Windows Server 2003 Environment for an MCSA Certified on Windows 2000* (ISBN: 1-932266-56-9).

Robert's specialties include network infrastructure design with the Cisco product line, systems engineering with Windows 2000/2003 Server, NetWare 6, Red Hat Linux and Apple OSX. Robert's true love is in network security design and management utilizing products from the Nokia, Cisco, and Check Point arsenal. Robert is also an advocate of Network Management and loves to 'sniff' networks with Sniffer-based technologies. When not doing something with computer related technology, Robert enjoys spending time with Erika and snowboarding wherever the snow may fall and stick.

Contents

Foreword	xxxi
Chapter 1 Introduction To Norton AntiVirus Corporate Edition (NAVCE)	1
Introduction	2
A Brief History of Computer Viruses	2
Malware	3
Viruses	3
Worms	5
Macro Viruses	5
Trojan Horses	6
Other Miscellaneous Malicious Programs	7
Fighting Back with Antivirus Programs	9
Commercial Antivirus Programs	10
Computer Associates	11
Network Associates	11
Panda Software	11
Freeware Antivirus Programs	11
Antivirus Solutions and the Enterprise	13
What's New in NAVCE v7.6	15
Introducing Norton Antivirus Extensible (NAVEX)	
Engine Technology	16
Centralizing Antivirus Administration	16
The NAVCE Client/Server Architecture	17
NAVCE Communication Methods	18
Server-to-Server Communication	19
Server-to-Client Communication	19
Introducing Symantec Security Response	20
Symantec Scan and Deliver	22
	xiii

Symantec AntiVirus Research Automation (SARA)	22
Symantec Support for Operating Systems and Networks	23
Supported Operating Systems for Clients	23
DOS PCs	23
Windows 3.x	24
The Remaining Windows Family	24
Supported Operating Systems for Servers	25
Windows NT 4.0 and Windows 2000	25
Novell NetWare	26
Support for Cluster Servers, Terminal Servers, and More...	26
Windows NT 4.0/2000 Cluster Servers	27
Novell NetWare Cluster Servers	27
Windows NT 4.0/2000 Terminal Servers	27
Citrix MetaFrame 1.8	28
Supported Networking Protocols	28
Symantec AntiVirus Corporate Edition 8.0	29
Windows Client Support	30
Windows Server Support	30
NetWare Server Support	31
Symantec Product Specialist Certification Information	31
Exam Objectives	32
Topic 1: Symantec AntiVirus Solution	33
Topic 2: Installation	33
Topic 3: The Discovery Process	33
Topic 4: Updating Virus Definitions	33
Topic 5: Scanning and Configuring Client E-mail	34
Topic 6: Virus Scans	34
Topic 7: Client/Server Communication	34
Topic 8: Central Quarantine and Quarantine Server	34
Topic 9: Alert Management System (AMS ²)	35
Summary	36
Solutions Fast Track	37
Frequently Asked Questions	39

Chapter 2 Designing a Managed Antivirus Infrastructure	41
Introduction	42
Understanding NAVCE Server Groups	44
Server Group Planning Considerations	45
Choosing Servers to Be Part of a Group	46
NAVCE for Windows NT/2000	47
NAVCE for NetWare	47
Creating a NAVCE Server Group	48
Creating or Changing a Server Group Password	49
Planning NAVCE Server Roles	52
Primary Servers	52
Secondary Servers	53
Master Primary Server	54
Parent Servers	57
Determining NAVCE Client Configurations	57
Managed Clients	58
Sometime Managed	59
Lightly Managed	59
Unmanaged	60
NAVCE Licensing	61
The Symantec Value Program	64
Symantec Elite Program	66
The Commit Option	67
The Forecast Option	67
Support for Decentralized Purchasing	67
Product Offerings	68
Summary	70
Solutions Fast Track	71
Frequently Asked Questions	72
Chapter 3 Implementing Symantec System Center and Alert Management System² (AMS²)	77
Introduction	78
Understanding the Symantec System Center	79
SSC Minimum Requirements	81
Additional Requirements for SSC Snap-ins	83
Recommended Configurations	83

Exploring SSC Features	85
Discovery Services	86
Server Groups Administration	86
Task Initiation	87
Managing Alerts	87
Remote Capabilities	88
Symantec Snap-ins for SCC	88
AMS ² Snap-in	88
The Norton AntiVirus Corporate Edition	
Management Snap-in	89
Symantec System Center Console Add-ons	89
Implementing SSC	90
Uninstalling Legacy NAVCE and LANDesk Products	90
Installing SSC	91
Installing the AMS ² Snap-in	93
Installing the Norton AntiVirus Corporate Edition	
Management Snap-in	93
Installing Symantec System Center Console Add-ons	94
Understanding SSC Services Running on	
Windows NT/2000 Servers	95
Troubleshooting: The SSC Does Not Retain	
Configuration Settings	95
Troubleshooting: If You Don't See Clients in the SSC	96
Uninstalling SSC	96
Uninstalling the Norton AntiVirus Corporate Edition	
Management Snap-in	97
Manually Uninstalling the SSC and Its Snap-ins	97
The SSC Discovery Process	112
The Discovery Cycle	113
Load from Cache Only	114
Local Discovery	114
Intense Discovery	114
IP Discovery	115
Adding Clients on LANs without WINS	116
Considering Network Bandwidth Utilization	119
SSC Console Traffic	119

Server-to-Server Traffic	119
Discovery Cycle Traffic	120
NAVCE Client/Server Traffic	120
NAVCE Server/Client Traffic	120
Manually Generated Traffic: NAVCE Client Enumeration	121
Manually Generated Traffic: Server Role Reassignment	121
Manually Generated Traffic: Moving NAVCE	
Servers between Groups	122
Manually Generated Traffic: Refreshing SSC Console	122
Introducing Alert Management System ²	123
Processing Alert Management	123
Compatible AMS ² Alerts for each Operating System	124
Implementing Alert Management System ²	125
Uninstalling Alert Management System ²	127
Configuring AMS ² Alerts	129
Configuring Alert Messages	130
Configuring Default Alert Messages	132
Configuring AMS ² Message Box Alerts	133
Configuring AMS ² Broadcast Alerts	134
Configuring AMS ² Alerts to Run Programs	134
Configuring the Load an NLM Alert	135
Configuring the Send E-mail Alert	135
Configuring the Send Page Alert	136
Configuring for a Known Paging Service	137
Configuring for an Unknown Paging Service	137
Configuring Alerts for SNMP	138
Configuring the Send SNMP Trap Alert	138
Configuring Alerts for the Windows NT/2000/XP	
Event Log	141
Managing Configured Alerts	141
Testing Configured Alerts	142
Exporting Alerts to Other Systems	142
Introducing NAVCE Notification Methods Not	
Requiring AMS ²	143
Customizable Messages	143
Histories and the Event Log	143

Understanding Scan Histories	143
Understanding Virus Histories	143
Understanding Virus Sweep Histories	144
Understanding the Event Log	144
Summary	146
Solutions Fast Track	147
Frequently Asked Questions	150
Chapter 4 Implementing Central Quarantine 2.01	153
Introduction	154
Introducing Central Quarantine 2.01	155
Implementing Quarantine Console 2.01	156
Quarantine Console 2.01 System Requirements	156
Recommended Configuration	157
Installing Quarantine Console 2.01	157
Uninstalling Quarantine Console 2.01	159
Implementing Quarantine Server 2.01	160
Quarantine Server 2.01 System Requirements	161
Recommended Configuration	161
Installing Quarantine Server 2.01	161
Understanding the Quarantine Server Services	
Running on NT/2000 Servers	164
Uninstalling Quarantine Server 2.01	165
Configuring Central Quarantine 2.01	166
Configuring Quarantine Server for Internet-Based	
Scan and Deliver	169
Configuring Quarantine Server for Email-Based	
Scan and Deliver	181
Configuring Submissions of Suspected Viruses to SSR	182
Receiving and Testing Updated Fingerprints from SSR	183
Configuring Managed Client PCs to Route Suspected	
Viruses to the Quarantine Server	184
Troubleshooting Central Quarantine 2.01	185
Summary	190
Solutions Fast Track	191
Frequently Asked Questions	193

Chapter 5 Implementing NAVCE 7.6 to Servers	195
Introduction	196
Understanding NAVCE 7.6 Servers	196
Windows NT / 2000 Server System Minimum Requirements	198
Utilizing Windows NT 4.0 Workstation or Windows 2000 Professional Systems as NAVCE Servers	199
Novell NetWare Server System Minimum Requirements	200
Implementing NAVCE 7.6 to Servers	201
Developing a Deployment Plan	201
Windows NT/2000 NAVCE Server Installation Considerations	201
Installing NAVCE 7.6 to Windows NT/2000 Servers	202
Configuring NAVCE 7.6 Servers	208
Uninstalling NAVCE 7.6 from Windows NT/2000 Servers	208
Uninstalling NAVCE Using the Command Line	209
Manual Uninstall	209
Understanding NAVCE 7.6 Registry Keys on NT/2000 Servers	212
NAVCE Registry Components	212
AddressCache Registry Key	213
ClientConfig Registry Key	213
DomainData Registry Key	214
Clients Registry Key	215
Children Registry Key	215
Understanding NAVCE 7.6 Services	
Running on NT/2000 Servers	217
Norton AntiVirus Server (rtvscan.exe)	217
DefWatch (defwatch.exe)	218
Intel Ping Discovery Service (pds.exe)	218
Introducing the grc.dat File	218
The grc.dat File	219
Summary	220
Solutions Fast Track	220
Frequently Asked Questions	223

Chapter 6 Implementing NAVCE 7.6 to Client PCs	225
Introduction	226
Understanding NAVCE 7.6 Client PCs	227
Check-in Intervals	228
Intel Ping Discovery Service	230
Communication Tools	232
NAVCE 7.6 Client PC System Requirements	233
MS-DOS Client PC System Requirements	233
Windows 3.x Client PC System Requirements	233
Windows 9x/Me/NT/2000/XP Client PC System Requirements	233
Implementing NAVCE 7.6 to Client PCs	235
Developing a Deployment Plan	236
Installing NAVCE 7.6 to Client PCs	237
Installing from an Internal Web Server	239
IIS Web Server Client Installations	240
Apache Web Server Client Installations	246
Installing from a Client Disk Image on a NAVCE Server	251
Remotely Installing NAVCE Client to NT/2000/XP Client PCs	252
Installing the NAVCE Client Locally	259
Installing the NAVCE Client through Logon Scripts	264
Installing the NAVCE Client from Floppy Disks or a Self-Extracting Deliverable Package	267
Understanding Third-Party Installation Methods	273
Using Microsoft IntelliMirror to Deploy the NAVCE Client	274
Using Microsoft Systems Management Server to Deploy the NAVCE Client	275
Using Novell ZENworks for Desktops to Deploy the NAVCE Client	276
Uninstalling NAVCE from Client PCs	276
Understanding NAVCE 7.6 Registry Keys on NT/2000/XP Client PCs	277
Windows 9x/NT/2000/XP	277

Understanding NAVCE 7.6 Services Running on NT/2000/XP	
Client PCs	279
Norton AntiVirus Server (RTVScan.exe)	280
DefWatch (defwatch.exe)	281
vpexrt.exe	281
vp trays.exe	281
Testing Your Deployment	282
Summary	284
Solutions Fast Track	284
Frequently Asked Questions	287

Chapter 7 Upgrading from Prior Versions 289

Introduction	290
NAVCE Upgrade Considerations	291
Testing Your Deployment	292
Developing an Upgrade Plan	293
Testing Your Rollout	293
Planning Virus Definition Update Methods	295
Upgrading from NAVCE 7.0 and 7.5	297
Upgrading from NAVCE 6.x	298
Upgrading the Norton System Center	299
Exploring Automatic Migration Options	299
Upgrading from NAV for NetWare	300
Automatically Migrating NAVCE Client PCs	301
Upgrading 16-Bit Windows Client PCs	302
Upgrading Windows 9x/Me Client PCs	302
Upgrading Windows NT Client PCs	304
Upgrading Unmanaged NAVCE Client PCs	305
Upgrading Remote Client PCs	306
Migrating from Third-Party LAN Antivirus Products	309
Sample Project Plan for NAVCE Upgrade	310
Identifying Project Resources and Major Tasks	311
Determining Timelines	318
Identifying Task Dependencies	320
Summary	323
Solutions Fast Track	323
Frequently Asked Questions	326

Chapter 8 Configuring Your NAVCE 7.6 Environment	329
Introduction	330
Configuring NAVCE 7.6 Clients	330
Installing a NAVCE Client in Unmanaged Mode	331
Exploring and Configuring the NAVCE Client	339
Configuring NAVCE Services Load Options	339
File System Realtime Protection Options	340
Enable/Disable File System Realtime Protection	340
Configuring File System Realtime Protection	
Advanced Options	341
Configuring File System Realtime Protection File	
Types Options	344
Configuring File System Realtime Protection Actions	347
Configuring File System Realtime Protection Virus	
Notification Message Options	349
Configuring File and Folder Exclusions for File System	
Realtime Protection	351
Configuring Drive Types for File System Realtime	
Protection	354
Other Types of Scans and Clients	356
Configuring Windows NT 4.0/2000 Cluster	
Server Protection	356
Configuring Windows NT 4.0 Terminal Server Protection	357
Configuring Windows 2000 Terminal Services Protection	357
Enabling Terminal Services on a Windows 2000 Server	358
Switching from Application Server to Remote	
Administration Mode	360
Installing NAVCE on Windows 2000 Terminal Server	361
Configuring NAVCE 7.6 Servers	366
Configuring Multiple NAVCE Clients and Servers	367
Configuring Roaming for NAVCE 7.6 Clients	367
Features of Roaming Client Support	368
Roaming Client Support Requirements	368
Implementing Roaming Client Support	369
Summary	370
Solutions Fast Track	370
Frequently Asked Questions	372

Chapter 9 Securing Your NAVCE 7.6 Environment	375
Introduction	376
Evaluating Security Requirements for Your Organization	377
Determining Your Security Policies	378
Writing It All Down: Drafting Your Network Security Policy	381
Acceptable Use Policy	381
Internet Usage	382
Disaster Recovery Policy	382
Antivirus Policy	383
Identifying Threats to Network Security	383
Natural Disasters	384
Hackers	384
Social Engineering	384
Internal Threats	385
Viruses/Trojans/Worms	385
Network-Based Attacks	386
Developing a Security Solution for NAVCE 7.6	386
Designating a Server	387
Selecting a Network Protocol	388
Implementing Your Security Solution for NAVCE 7.6	391
Installing Central Quarantine Server	391
Configuring Central Quarantine Server	392
Configuring Firewall Settings	394
Enabling NAVCE Communication	394
Configuring LiveUpdate Access	395
Allowing Access for AMS ²	396
Configuring Quarantine Server Ports	397
Securing NAVCE 7.6 Windows NT/2000 Servers	397
Locking Down the NAVCE Installation	397
Creating or Changing a Server Group Password	398
Hardening the Windows Operating System	399
Providing Physical Security for Your Windows NT/2000 Server	399
Configuring the Operating System for Maximum Security	400
Protecting Terminal Servers	403

Restricting Virus Scans on Terminal Servers	403
Managing Access to the NAVCE 7.6 Registry Keys on NT/2000 Servers	405
Auditing Access to the Windows Registry	406
Securing NAVCE 7.6 Novell NetWare Servers	409
Enabling NetWare Servers to Forward to Quarantine Server Using the IPX Protocol	409
Configuring FTP Downloads of Antivirus Updates for NetWare Servers	410
Testing the FTP Function in Novell NetWare	410
Securing Your NetWare Servers	411
Securing NAVCE 7.6 Client PCs	412
Monitoring NAVCE Client Definitions	413
Preventing a User from Canceling a Virus Scan	414
Managing Access to the NAVCE 7.6 Registry Keys on NT/2000/XP Client PCs	415
Introducing the Reset ACL (resetacl.exe) Tool	416
Special Considerations When Using the Reset ACL Tool	417
Undoing resetacl.exe Changes	418
Summary	420
Solutions Fast Track	420
Frequently Asked Questions	423
Chapter 10 Updating Virus Protection	431
Introduction	432
Introducing the Virus Definition Transport Method (VDTM)	434
The RTVScan Timer Loop	435
Features of the Virus Definition Transport Method	436
Configuring a Server to Use VDTM	436
Introducing Symantec LiveUpdate	439
LiveUpdate versus VDTM	439
Considerations for Configuring LiveUpdate	442
Configuring External LiveUpdate	442
Configuring Internal LiveUpdate	445
LiveUpdate Administration Utility Introduction and System Requirements	446

Installing Symantec LiveUpdate 1.5.3.21	
Administration Utility	447
Configuring LiveUpdate Using the LiveUpdate	
Administration Utility	450
Configuring Servers and Clients to Connect to the	
Internal LiveUpdate Server	451
Introducing Intelligent Updater	453
Summary	456
Solutions Fast Track	456
Frequently Asked Questions	458

Chapter 11 Troubleshooting Your NAVCE 7.6 Environment 461

Introduction	462
Troubleshooting Basics	462
DNS Issues	463
Reverse Zones	466
DNS Configuration Notes	468
DNS Troubleshooting Applications	470
Dynamic DNS and the NAVCE Environment	478
Alternative Forms of Name Resolution	479
DHCP Issues	482
Directory Services Issues	483
Firewalls and the NAVCE Environment	483
Troubleshooting Servers	486
Windows NT/2000 Servers	486
Installation Errors	486
Configuring a Primary NAVCE Server	487
Verifying Check-in Frequency and keepalive Packets	487
Verifying Client/Server Communication	488
Inability to Communicate with Clients through the SSC	489
Setting the Preferred Protocol	490
Configuring Clients	491
Combining 16-Bit and 32-Bit Clients	492
Failed Notifications	492
NAVCE Server Installation Issues	493
Uninstalling NAVCE Server	496
LiveUpdate Issues	500

DUAL NIC Systems	502
Additional Fixes	504
Novell NetWare Servers	505
Installation Issues	505
Debugging NAVCE in NetWare	506
NetWare Servers and Windows NT/2000	508
Configuring a Preferred Protocol for a NetWare Server	508
Problems Conducting Scans in NetWare Servers	510
Troubleshooting Client PCs	510
Solving Hard-Drive Issues	510
Printing Problems	511
Problems Creating a Rescue Disk	512
Scanning for Additional Files	513
vptray Issues	514
Placing a Shortcut in the Windows Startup Folder	515
Exchange Server Issues	515
Outlook Express Issues	516
Windows Me and the Restore\Temp and	
_Restore\Archive Folders	516
NAVCE Fails after Using the Windows Me/XP System	
Restore Feature	517
Modifying Files	517
Obtaining and Installing Old Definition Files	518
NAVCE Installation Issues	518
Registry Permissions	518
NTFS Permissions	519
Verifying Distributed Component Object Model	
Configuration	520
Uninstalling Client Versions of NAVCE	523
Uninstalling NAVCE from Windows NT/2000/XP	
Client Systems	523
Uninstalling NAVCE from Windows 9x and Me Client	
Systems	526
Troubleshooting Roaming Client Support	528
Server List File Size Limits	528
File Syntax	528

DNS Issues	528
Fully Qualified Domain Names versus Host Names	528
DNS and Duplicate Host Names	529
Addressing Performance Issues	529
Problems after Using LiveUpdate	530
Maximum Number of Clients and the Registry Size Value	530
Slow Client Logoff in Terminal Services	531
Achieving Balance	532
Page Faults and RTVScan	532
Tracking Performance	532
Improving Performance	533
Accessing Information Databases	534
Additional Symantec Search Engines	535
Third-Party Search Engines	536
Search Techniques	536
Summary	537
Solutions Fast Track	537
Frequently Asked Questions	540

Chapter 12 Scanning for Viruses and Handling Virus Outbreaks 545

Introduction	546
Virus Scanning Methods	547
Real-Time Scans	547
Scheduled Scans	549
Manual Scans	550
Configuring Computer Virus Scans	550
Configuring Manual Scans	550
Configuring Manual Scans from Symantec System Center	550
Configuring Manual Scans from the Client	556
Symantec Bloodhound Heuristics	557
Symantec Striker	558
Configuring Real-Time Scans	559
File Systems	559
Messaging Systems	563
Locking Real-Time Scanning Options	565
Configuring Scheduled Scans for Servers	566

Scheduling Scans for Specific Servers	566
Scheduling Scans for Server Groups	568
Configuring Scheduled Scans for Client PCs	568
Configuring Logon Scans	568
Configuring Startup Scans	571
Configuring Custom Scans	572
Analyzing the Results of Computer Virus Scans	572
Understanding Computer Virus Outbreaks	573
Identifying Computer Virus Outbreaks	574
Responding to Computer Virus Outbreaks	574
Communicating the Outbreak	575
Containing a Virus Outbreak	576
Using Virus Sweeps	577
Cleaning up a Virus Outbreak	580
Understanding Alert Management Server ²	580
Using Built-in Notifications	580
Displaying Notification Messages to End Users	580
Using the Virus History Feature	582
Taking Actions Against Infected Files	582
Recovering from Boot Sector Viruses	582
Managing the Virus Outbreak Process	585
Summary	588
Solutions Fast Track	589
Frequently Asked Questions	591
Chapter 13 Backup and Disaster Recovery	595
Introduction	596
Basic Principles of Backup and Disaster Recovery	596
Creating a Baseline of Your Network	597
Leaving Room for Growth	598
Planning for Data Retention	598
Creating a Workable Backup Schedule	599
Creating a Tape Rotation Scheme	599
Providing an Offsite Storage Location	601
Striking a Balance Between Cost and Convenience	604
Training Your Staff	604
Involving Your Users in the Disaster Recovery Process	604

Testing Your Backups	605
Designing a Disaster Recovery Plan	606
Defining Mission-Critical Criteria for Your Organization	607
Identifying Vulnerabilities	609
Implementing a Backup Strategy	610
Choosing Backup Software	610
Selecting Hardware and Media	611
Floppy Disks	612
Hard Drives and Disks	613
CD-R/CD-RW/DVD-R	613
Iomega Drives	613
Magnetic Tapes	614
Jukeboxes, Stack Loaders, and the Like	615
Magneto-Optical and Floptical Disks	615
Creating a Backup Schedule	616
Defining Support and Service Levels for Your Organization	620
Backing Up Dedicated NAVCE 7.6 Servers	622
Using NTBackup in Windows 2000	622
Using the Command Line to Schedule Backups	629
Testing NAVCE Server Backup Jobs	631
Restoring Dedicated NAVCE 7.6 Servers	633
Summary	637
Solutions Fast Track	638
Frequently Asked Questions	640

Appendix A Norton AntiVirus 2003 and 2003 Professional Edition **643**

Introducing NAV 2003 and NAV 2003 Professional Edition	643
System Requirements	644
NAV 2003 System Requirements	645
NAV 2003 Professional Edition System Requirements	646
Installing NAV 2003	646
Preparing for the Installation	646
Beginning the Installation	648
First-Time Use	652
Troubleshooting the Installation	657
Configuring NAV 2003 LiveUpdate	657

Interactive versus Express Mode	658
Configuring Auto-Protect	659
Configuring SmartScan	660
Configuring Bloodhound	661
The Auto-Protect Advanced Window	662
The Auto-Protect Exclusions List Window	662
Configuring Script Blocking	662
Configuring Manual Scan Options	663
Configuring E-mail Protection	664
Protecting Instant Messenger Traffic	665
Configuring The Miscellaneous Section	666
Password Protection for NAV 2003	667
Viewing Log Files	667
Saving Your Changes: The Options File	668
Troubleshooting NAV 2003	668
Uninstalling NAV 2003	669
Installing NAV 2003 Professional Edition	670
Post-Install Tasks	672
Configuring NAV 2003 Professional Edition	675
Conducting a Full Scan	676
Configuring the Norton Protected Recycle Bin	679
Troubleshooting NAV 2003 Professional Edition	681
Troubleshooting the Installation	682
Troubleshooting the Configuration	682
Uninstalling NAV 2003 Professional Edition	682

Index**685**

Foreword

We have all become accustomed to using computers for e-mail, writing, financial modeling, and data storage, as well as retrieving many types of data both at home and at work. These computers are typically connected to company networks and the Internet, normally 24 hours a day, 365 days a year. These same computers and networks, though designed to be accessible, were not necessarily designed to be secure—in other words, data security was not a primary focus during their development.

Unfortunately, the security of online computing resources has been an issue since the early days of computer networks. It didn't take long before the first computer worm appeared, and from that day forward, computers, and the networks they run, have needed protection against viruses, Trojan horses, and worms, whether automated or driven by unscrupulous users.

This struggle between companies/users and malicious coders raises many concerns, such as:

- Who is using your computer?
- How secure is your data?
- Are your corporate marketing plans or customers' credit card numbers being copied across an unsecured network by a computer worm, or via a backdoor Trojan while you work?
- Is Greyware (such as Spyware or Adware) infiltrating your corporate users' computers via spam and causing the leakage of information by way of surfing and purchasing habits?

Many of these threats can be delivered by malicious code via corporate e-mail systems, public networks, Web sites, or shared corporate network resources. They can use either known or unpublished software vulnerabilities to exploit badly designed

software, all for the purpose of gaining control of a user's computer. However, with all of the advancements in user education, antivirus software, and information security in general, we are still a long way from the trusted and secure computing services currently on the drawing board.

The aforementioned problems are just some of the privacy and data security issues malicious code is connected with. A sound security policy encompassing software solutions, security policies, and employee work practices is essential in effectively combating these types of threats. But, as you likely know, relying on individual computer users to protect their own computers simply does not work.

Antivirus software has been helping users protect themselves against malicious code since the first worms and viruses appeared on desktop computers in the late 80s and early 90s. Many vendors in the antivirus software industry have come and gone in the fight against viruses. Over the years, the Symantec Corporation has acquired several smaller antivirus and data security vendors for their unique technologies, culminating in the acquisition of IBM and Intel's antivirus business in the latter part of the 1990s. Both of these acquisitions were to have a significant impact on Symantec's approach to its enterprise software solutions; resulting in the birth of Norton AntiVirus Corporate Edition (NAVCE).

NAVCE breathed new life into Norton AntiVirus, and the consumer and enterprise editions headed in different directions to satisfy two distinct needs: those of the average home user, and those of the corporate network administrator. The technologies acquired from Intel and IBM—enterprise antivirus software management and automated virus handling, respectively—were the keystones of this divergence. There are, however, several common components shared by the home and enterprise products, including the core virus scanning engine and the interfaces to the Digital Immune System (DIS), where new viruses are processed and updated virus definitions are created and distributed.

These key components, along with comprehensive network management features, are the backbone of an effective enterprise antivirus software solution, and differentiate NAVCE in a highly competitive marketplace. NAVCE 7.6 gives network administrators control over the client side of the antivirus scanning product, enabling planned and controlled rollouts of product upgrades and virus definition updates.

Clients can be locked down so users cannot turn off the antivirus protection or alter the settings of the antivirus software. PC administrators can run regularly scheduled virus scans to supplement on-access scanning, and view virus activity on their client base using centralized reporting and quarantine tools.

NAVCE continues to evolve with Symantec AntiVirus Corporate Edition (SAVCE) versions 8, 8.1, and 8.5, offering additional functionality that provides comprehensive virus protection for workstations and network servers enterprise wide

Version 8.5 not only improves the speed of virus scanning as well as the delivery speed of virus definitions to workstations, but also reduces the size of these updates, and adds digital signatures to them. All this with an enhanced protection of configuration settings which offers such valuable features as the ability to re-enable real-time virus protection. It also provides improved manageability and deployment while simultaneously requiring fewer servers.

These are all improvements on the tried and tested NAVCE 7.6, which *Configuring Symantec AntiVirus Enterprise Edition* teaches you how to implement, upgrade, and configure in a diverse network environment. The authors of *Configuring Symantec AntiVirus Enterprise Edition* have experience implementing and managing NAVCE installations in enterprises that range from 50 to 5000 users with multiple servers, and have hands-on experience with the day-to-day operation of NAVCE, from installation to troubleshooting to infection recovery.

Whether you are managing an existing NAVCE 7.6 configuration or implementing SAVCE version 8.x, this book will help you get the most out of your software installation, allowing you to maximize your virus protection while minimizing both the cost of ownership and your own workload.

—David Banes
Symantec Security Response
Asia Pacific Regional Manager

Introduction To Norton AntiVirus Corporate Edition (NAVCE)

Solutions in this chapter:

- A Brief History of Computer Viruses
 - Fighting Back with Antivirus Programs
 - Antivirus Solutions and the Enterprise
 - Centralizing Antivirus Management
 - Introducing Symantec Security Response
 - Symantec Support for Operating Systems and Networks
 - Symantec AntiVirus Corporate Edition 8.0
 - Symantec Product Specialist Certification Information
-
- ☑ Summary
 - ☑ Solutions Fast Track
 - ☑ Frequently Asked Questions

Introduction

At some time in the last 15 years many of us blinked, and upon opening our eyes we found the world on the verge of becoming one large network. Public and private networks were interconnected both far and near, and now in your corner of this interconnected puzzle, virus protection for the network has become your responsibility.

With numerous unforeseeable viruses attempting to infiltrate your network, providing reliable and secure virus protection should be one of your top concerns. Norton AntiVirus Corporate Edition 7.6 (NAVCE) propels the terms “reliable” and “secure” to an exceedingly higher level. NAVCE can help protect your network, both servers and clients alike, with the most up-to-date protection in a completely automated environment.

With a well-designed and implemented deployment of NAVCE, worrying about virus protection for your network will be history. NAVCE provides a truly proactive approach to your virus protection needs that won’t leave you scrambling for answers when a virus threat arises.

Understanding computer viruses, and what they are capable of, can provide you with a clearer understanding of why a product such as NAVCE should be introduced into your network structure.

NOTE

This book is intended to introduce you to the NAVCE 7.x AntiVirus software. It will provide you with the finer particulars to help you utilize the software to proactively *and* reactively guard your network from virus threats. Additionally, this book provides information necessary for you to pass the Symantec Product Specialist certification Exam 250-011.

A Brief History of Computer Viruses

As computers became more popular in the home and workplace, viruses followed them in through the door. Viruses are nothing more than moderately small programs designed to disrupt and alter the functionality of a computer.

The word *malicious* is defined by Merriam-Webster’s Collegiate Dictionary as: *given to, marked by, or arising from malice*. Additionally, *malice* is defined as: *The desire*

to cause pain, injury, or distress to another—or—the intent to commit an unlawful act or cause harm without legal justification or excuse. There are thousands of viruses floating around the networks of the world, and a great percentage of them fall into this definition.

However, not all viruses are malicious, some are just disruptive. Others, however, are not only disruptive, but destructive at heart, designed to destroy the recipient's system.

Malware

Malware comes from the phrase “*malicious software*.” The term is functional in covering an entire scope of aggressive software such as Trojan horses and worms. Though malware's definition may vary, it basically describes any software or code that is specifically designed to damage and/or disrupt a system. The overall problem with this generic definition boils down to a simple issue: how one receives the malware, and whether the sender's intentions were malicious.

Hypothetically, in order to better understand malware, let's say we have constructed a secure networked lab environment so we can write, test, and study such programs. In our excitement of breaking a code we have been studying and reinventing a specific malware program, we send our findings along with the program itself to all of our co-authors, *and forget to add an appropriate subject line to the e-mail warning the recipients of the e-mail's content.* Surely, our intent was to share our findings with our peers, and not to cause any destruction to their systems. However, upon opening the e-mail and watching their entire system being formatted before their eyes, others might not perceive the issue in the same manner as we did. The program itself was purely malicious, but our intent was not. Does that make it malware? What if we had clearly warned the recipients of the e-mail's attachment and they chose to open it in an unsecured environment? Is it *then* considered malware? This is a very tricky question, with no clear-cut answer.

No matter how you perceive the generic definition offered in the previous paragraph, it is fair to say that most viruses—worms, Trojan horses, and macro viruses alike—are malware.

Viruses

For viruses to efficiently perform the devious functions their creators intend, they somehow need to be executed. Once executed, most viruses will attempt to replicate themselves throughout the computer and ultimately (if interconnected to other computers) onto the network. Viruses are activated when an infected program is loaded into memory and executed either by its own code or by the