

# Contents

<b>Foreword</b>	<b>xxxi</b>
<b>Chapter 1 Introduction To Norton AntiVirus Corporate Edition (NAVCE)</b>	<b>1</b>
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 <sup>2</sup> )	35
Summary	36
Solutions Fast Track	37
Frequently Asked Questions	39

<b>Chapter 2 Designing a Managed Antivirus Infrastructure</b>	<b>41</b>
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
<b>Chapter 3 Implementing Symantec System Center and Alert Management System<sup>2</sup> (AMS<sup>2</sup>)</b>	<b>77</b>
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 <sup>2</sup> 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 <sup>2</sup> 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 <sup>2</sup>	123
Processing Alert Management	123
Compatible AMS <sup>2</sup> Alerts for each Operating System	124
Implementing Alert Management System <sup>2</sup>	125
Uninstalling Alert Management System <sup>2</sup>	127
Configuring AMS <sup>2</sup> Alerts	129
Configuring Alert Messages	130
Configuring Default Alert Messages	132
Configuring AMS <sup>2</sup> Message Box Alerts	133
Configuring AMS <sup>2</sup> Broadcast Alerts	134
Configuring AMS <sup>2</sup> 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 <sup>2</sup>	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
<b>Chapter 4 Implementing Central Quarantine 2.01</b>	<b>153</b>
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

<b>Chapter 5 Implementing NAVCE 7.6 to Servers</b>	<b>195</b>
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

<b>Chapter 6 Implementing NAVCE 7.6 to Client PCs</b>	<b>225</b>
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

<b>Chapter 8 Configuring Your NAVCE 7.6 Environment</b>	<b>329</b>
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

<b>Chapter 9 Securing Your NAVCE 7.6 Environment</b>	<b>375</b>
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 <sup>2</sup>	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
<b>Chapter 10 Updating Virus Protection</b>	<b>431</b>
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 <sup>2</sup>	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
<b>Chapter 13 Backup and Disaster Recovery</b>	<b>595</b>
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
<b>Index</b>	<b>685</b>