

# VISIT US AT

www.syngress.com

Syngress is committed to publishing high-quality books for IT Professionals and delivering those books in media and formats that fit the demands of our customers. We are also committed to extending the utility of the book you purchase via additional materials available from our Web site.

## **SOLUTIONS WEB SITE**

To register your book, visit [www.syngress.com/solutions](http://www.syngress.com/solutions). Once registered, you can access our [solutions@syngress.com](mailto:solutions@syngress.com) Web pages. There you may find an assortment of value-added features such as free e-books related to the topic of this book, URLs of related Web sites, FAQs from the book, corrections, and any updates from the author(s).

## **ULTIMATE CDs**

Our Ultimate CD product line offers our readers budget-conscious compilations of some of our best-selling backlist titles in Adobe PDF form. These CDs are the perfect way to extend your reference library on key topics pertaining to your area of expertise, including Cisco Engineering, Microsoft Windows System Administration, CyberCrime Investigation, Open Source Security, and Firewall Configuration, to name a few.

## **DOWNLOADABLE E-BOOKS**

For readers who can't wait for hard copy, we offer most of our titles in downloadable Adobe PDF form. These e-books are often available weeks before hard copies, and are priced affordably.

## **SYNGRESS OUTLET**

Our outlet store at [syngress.com](http://syngress.com) features overstocked, out-of-print, or slightly hurt books at significant savings.

## **SITE LICENSING**

Syngress has a well-established program for site licensing our e-books onto servers in corporations, educational institutions, and large organizations. Contact us at [sales@syngress.com](mailto:sales@syngress.com) for more information.

## **CUSTOM PUBLISHING**

Many organizations welcome the ability to combine parts of multiple Syngress books, as well as their own content, into a single volume for their own internal use. Contact us at [sales@syngress.com](mailto:sales@syngress.com) for more information.



SYNGRESS®

MICROSOFT®

# Vista

for

# IT Security

## Professionals

**Anthony Piltzecker** Technical Editor

Larry Chaffin  
Scott Granneman  
Laura E. Hunter  
Alun Jones  
Jan Kanclirz  
Marc Perez

Daniel Sheperd  
Matt Sheperd  
Robert J. Shimonski  
Henrik Walther

Elsevier, 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 Elsevier, 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 Elsevier, Inc. Brands and product names mentioned in this book are trademarks or service marks of their respective companies.

**KEY SERIAL NUMBER**

001	HJIRTCV764
002	PO9873D5FG
003	829KM8NJH2
004	8932KLPERN
005	CVPLQ6WQ23
006	VBP965T5T5
007	HJJJ863WD3E
008	2987GVTWMK
009	629MP5SDJT
010	IMWQ295T6T

**PUBLISHED BY**

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

**Microsoft Vista for IT Security Professionals**

Copyright © 2007 by Elsevier, Inc. All rights reserved. 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-10: 1-59749-139-X

ISBN-13: 978-1-59749-139-6

Publisher: Andrew Williams  
Acquisitions Editor: Gary Byrne  
Technical Editor: Tony Piltzecker  
Cover Designer: Michael Kavish

Page Layout and Art: Patricia Lupien  
Copy Editor: Audrey Doyle  
Indexer: Richard Carlson

For information on rights, translations, and bulk sales, contact Matt Pedersen, Commercial Sales Director; email [m.pedersen@elsevier.com](mailto:m.pedersen@elsevier.com).



# Technical Editor

**Tony Piltzecker** (CISSP, MCSE, CCNA, CCVP, Check Point CCSA, Citrix CCA), author and technical editor of Syngress Publishing's *MCSE Exam 70-296 Study Guide and DVD Training System*, is a Consulting Engineer for Networked Information Systems in Woburn, MA. He also contributed to *How to Cheat at Managing Microsoft Operations Manager 2005* (Syngress, ISBN: 1597492515).

Tony's specialties include network security design, Microsoft operating system and applications architecture, as well as Cisco IP Telephony implementations. Tony's background includes positions as IT Manager for SynQor Inc.; Network Architect for Planning Systems, Inc.; and Senior Networking Consultant with Integrated Information Systems. Along with his various certifications, Tony holds a bachelor's degree in Business Administration. Tony currently resides in Leominster, MA, with his wife, Melanie, and his daughters, Kaitlyn and Noelle.



# Contributors

**Larry Chaffin** is the CEO/Chairman/Founder of Pluto Networks, a virtual worldwide network consulting company spanning 23 countries and specializing in book authoring, VoIP, WLAN, and security. He is an accomplished author. He was a contributor to *Managing Cisco Secure Networks* (Syngress, ISBN: 1931836566), *Skype Me!* (Syngress, ISBN: 1597490326), *Practical VoIP Security* (Syngress, ISBN: 1597490601), *Configuring Check Point NGX VPN-1/Firewall-1* (ISBN: 1597490318) and author of *Building a VoIP Network with Nortel's Multimedia Communication Server 5100* (Syngress, ISBN: 1597490784). He has also coauthored or ghostwritten 11 other technology books about VoIP, WLAN,

security and optical technologies. Larry has over 29 vendor certifications from companies such as Avaya, Cisco HP, IBM, isc2, Juniper, Microsoft, Nortel, PMI, and VMware. Larry has been a Principal Architect designing VoIP, security, WLAN, and optical networks for many Fortune 100 companies in 22 countries. He is viewed by his peers as one of the most well-respected experts in the field of VoIP and Security in the world. Larry has spent countless hours teaching and conducting seminars/workshops around the world in the field of Voice/VoIP, security and wireless networks. Larry is currently working on a follow-up to *Building a VoIP Network with Nortel's Multimedia Communication Server 5100* as well as new books on Cisco VoIP networks, Microsoft Vista, and Practical VoIP case studies.

*Larry cowrote Chapter 1.*

**Scott Granneman** is an author, teacher, and consultant. A monthly columnist for both *SecurityFocus* and *Linux Magazine*, Scott has also authored three books on open source technologies, each of which focuses on security issues in a different way: *Don't Click on the Blue E!: Switching to Firefox*; *Hacking Knoppix*; and *Linux Phrasebook*. As an adjunct professor at Washington University in St. Louis and Webster University, Scott teaches a variety of popular courses about security, technology, and the Internet. As a Principal of WebSanity, he manages the firm's UNIX-based server environment and helps develop the company's Content Management System, which is used nationally by educational, business, and nonprofit clients.

*Scott wrote Appendix A and Appendix B.*

**Laura E. Hunter** (CISSP, MCSE: Security, MCDBA, Microsoft MVP) is an Active Directory architect with a publicly held engineering and staffing firm, where she provides network planning, implementation, and troubleshooting services for Active Directory and other Microsoft technologies. Her specialties include Windows 2000 and 2003 Active Directory design and implementation, trou-

bleshooting, and security topics. Laura has more than a decade of experience with Windows computers; her previous experience includes a position as an IT Project Leader with the University of Pennsylvania and as the Director of Computer Services for the Salvation Army. She is a contributor to the TechTarget family of Web sites and to *Redmond Magazine* (formerly *Microsoft Certified Professional Magazine*).

Laura has previously contributed to the Syngress Windows Server 2003 MCSE/MCSA DVD Guide & Training System series as a DVD presenter, author, and technical reviewer. Laura is the author of the *Active Directory Consultant's Field Guide* (ISBN: 1-59059-492-4) from APress, and the coauthor of the *Active Directory Cookbook, Second Edition* (ISBN: 059610202X) from O'Reilly Media. Laura is a four-time recipient of the prestigious Microsoft MVP award in the area of Windows Server—Networking. Laura holds a Master's Degree in Computer Science from the University of Pennsylvania and also works as a freelance writer, trainer, speaker and consultant.

*Laura wrote Chapter 6.*

**Alun Jones** (MVP, MCP) is the President of Texas Imperial Software. Texas Imperial Software develops secure networking software and provides security engineering consulting services. Texas Imperial Software's flagship product is WFTPD Pro, a secure FTP server for Windows, written entirely by Alun.

Alun entered the security engineering field as more and more of WFTPD's support needs indicated that few companies were trying to meet their needs for security on the Internet. His current day job is as an Information Systems Security Engineer at Premera Blue Cross, a health insurance provider based in the Pacific Northwest of the USA.

Alun has attended, but not completed, University at Corpus Christi College, Cambridge, and Bath University, and now lives in Seattle, Washington, with his wife, Debbie, and son, Colin.

*Alun wrote Chapter 5.*

**Jan Kanclirz Jr.** (CCIE #12136–Security, CCSP, CCNP, CCIP, CCNA, CCDA, INFOSEC Professional, Cisco WLAN Support/Design Specialist) is currently a Senior Network Information Security Architect at IBM Global Services. Jan specializes in multivendor designs and post-sale implementations for several technologies such as VPNs, IPS/IDS, LAN/WAN, firewalls, content networking, wireless, and VoIP. Beyond network designs and engineering, Jan’s background includes extensive experience with open source applications and Linux. Jan has contributed to several Syngress book titles: *Managing and Securing Cisco SWAN*, *Practical VoIP Security*, and *How to Cheat at Securing a Wireless Network*.

In addition to Jan’s full-time position at IBM G.S., Jan runs a security portal, [www.MakeSecure.com](http://www.MakeSecure.com), where he dedicates his time to security awareness and consulting. Jan lives in Colorado, where he enjoys outdoor adventures. Jan would like to thank his family, slunicko, and friends for all of their support.

*Jan wrote Chapter 7.*

**Marc Perez** (MCSE:Security, Security+) is a senior consultant at Networked Information Systems in Boston, MA. Representing Network Information Systems’ Microsoft practice, he provides strategic and technical consulting services to midsize and enterprise-level clients located throughout the Northeast. Focusing on securely integrating directory services with messaging and collaboration solutions, he provides the guidance necessary for enterprises to leverage their technology investments toward more effective communication with an emphasis on presence.

Educated at the University of Southern Maine, Marc has consulted privately for several organizations in the Boston area and has held roles throughout New England, including four years as an Information Security Manager for MBNA America Bank. He currently lives on the North Shore with his wife, Sandra, and his two sons, Aidan and Lucas.

*Marc wrote Chapter 8.*



**Daniel Shepherd** (MCP, GSEC) is IT Manager for an oil and gas trade association, headquartered in Washington, D.C. Dan provides the association with a full range of IT services, including designing, administering, and troubleshooting the corporate network. The small staff of roughly 30 employees supports more than 40,000 individual association members. The projects Dan has designed and implemented for the organization range from a whole office VoIP implementation, a network infrastructure upgrade, a complete overhaul of aging server hardware and software, and virtualization of the server environment for increased resource utilization and security through role isolation.

Dan's background includes positions as the Network Administrator for the fastest-growing restaurant point-of-sale company in the southeast and as a Consultant for Faith Based Design Inc., where he provided training, technical writing, and field engineering services for the U.S. Military.

*Daniel wrote Chapter 9 and cowrote Chapter 1.*

**Matt Shepherd** (CISSP, MCSE, GCFW, GSEC, CEH) is a consultant for Project Performance Corporation of McLean, VA. Project Performance Corporation synthesizes its capabilities in security architecture, engineering, and compliance with best-of-breed tools to provide effective security solutions to customers in the public and private sectors. Matt uses his experience as a network administrator, IT manager, and security architect to deliver high-quality solutions for Project Performance Corporation's clients. Matt holds bachelor's degrees from St. Mary's College of Maryland, and he is currently working on his Master's of Science in Information Assurance.

Matt would like to thank his wife, Leena, for her wonderful support during this project, and throughout their relationship. He thanks his family for a lifetime of love and support and Olive for making every day special. Matt also thanks his brother Daniel for tackling this project with him.

Matt thanks Mike Nigro, Martin Wright, and Jan Hill at PPC for supporting him on this project, and he also sends thanks to Shon

Eizenhoefer at Microsoft for taking the time to provide clear, timely answers when he needed them.

*Matt wrote Chapter 4.*

**Robert J. Shimonski** (MCSE) is an Entrepreneur and best-selling author and editor of hundreds of published books and thousands of magazine and industry articles. Rob consults within today's most challenging business and technology environments and brings front-line industry knowledge to the reader in every page he writes. Rob is always on top of the latest trends and reporting the state of the business and technology industry from a real-world perspective. As of the writing of this book, Rob is currently on assignment testing and developing secure Vista images and designing a Longhorn upgrade for a large global firm.

For Syngress, Rob has written many cutting-edge "in demand" titles, including *The (ISC)2 SSCP Study Guide and DVD Training System* (ISBN 1931836809), *The Best Damn Firewall Book Period!* (ISBN 1931836906), *Designing and Building Enterprise DMZs* (ISBN 1597491004), *Nokia Network Security Solutions Handbook* (ISBN 1931836701), *Sniffer Pro Network Optimization and Troubleshooting Handbook* (ISBN 1931836574), *Configuring and Troubleshooting Windows XP Professional with CD-ROM* (ISBN 1928994806), *Configuring Symantec Antivirus Corporate Edition* (ISBN 1931836817), and the *Network+ Study Guide & Practice Exams: Exam N10-003* (ISBN 1931836426). Rob also helped to develop the first DVD video with Syngress for the launch of *The Security + Study Guide and DVD Training System* (ISBN 1931836728), which has become a best seller.

Rob owns and operates Sound Room Studios Inc, a media development company in Long Island, NY. His role there is to produce and engineer audio and video content for TV, radio, and digital distribution.

*Rob wrote Chapters 2 and 3.*

**Henrik Walther** (Exchange MVP, MCSE Messaging/Security) is a senior consultant working for Interprise Consulting A/S (a Microsoft Gold Partner) based in Copenhagen, Denmark. Henrik has more than 14 years of experience in the IT business, where he primarily works with Microsoft Exchange, ISA Server, MOM, IIS, clustering, Active Directory, and virtual server technologies.

In addition to his job as an Exchange System specialist, Henrik also runs the Danish Web site Exchange-faq.dk. He also is the primary content creator, forums moderator, and newsletter editor at the leading Microsoft Exchange site, MExchange.org. Henrik is the author of *CYA: Securing Exchange Server 2003 & Outlook Web Access* (Syngress, 2004), and he has been a reviewer on several other messaging books (including another Exchange 2007 book).

*Henrik wrote Chapter 10.*



# Foreword Contributor

**Brien Posey** is Relevant Technologies' Vice President of Research and Development ([www.relevanttechnologies.com](http://www.relevanttechnologies.com)). Brien has previously served as the Director of Information Systems for a large nationwide chain of healthcare facilities and as the Department of Defense's senior network engineer at Fort Knox. He has also served as Editor in Chief of several technical publications and also as a network administrator for one of the country's largest insurance companies.

Brien is an award-winning technology author, a Microsoft Certified Systems Engineer (MCSE), and a Microsoft MVP. He has written or contributed material to 28 books and published more than 3,000 articles for a variety of Web sites and printed publications, including *CNET*, *Jupiter Media*, *Microsoft's TechNet Magazine*, *Windows Magazine*, *Windows Networking*, *TechTarget*, and *ZDNet*.

# Contents

<b>Foreword</b> . . . . .	<b>xxv</b>
<b>About the CD</b> . . . . .	<b>xxvii</b>
<b>Chapter 1 Microsoft Vista: An Overview</b> . . . . .	<b>1</b>
Introduction . . . . .	.2
The User Interface . . . . .	.7
The Welcome Center . . . . .	.10
The Start Menu . . . . .	.11
User Accounts . . . . .	.13
Internet Explorer 7 . . . . .	.15
Internet Explorer 7 Features . . . . .	.15
RSS Feeds . . . . .	.16
Pop-up Blocker . . . . .	.20
Phishing Filter . . . . .	.20
Summary . . . . .	.22
Solutions Fast Track . . . . .	.22
Frequently Asked Questions . . . . .	.23
<b>Chapter 2 Microsoft Vista: The Battle Against Malware Lives On</b> . . . . .	<b>25</b>
Introduction . . . . .	.26
Malware Fundamentals . . . . .	.27
Viruses, Worms, and Trojan Horses . . . . .	.28
Viruses . . . . .	.30
Worms . . . . .	.32
Trojan Horses . . . . .	.35
Spyware and Adware . . . . .	.37
Botnets . . . . .	.39
Prevention and Response . . . . .	.39
Incident Response . . . . .	.41
Microsoft Vista and Security . . . . .	.42
Windows Service Hardening (WSH) . . . . .	.43
Network Access Protection (NAP) . . . . .	.45
Improvements in Internet Explorer 7 . . . . .	.45
Basic Browser Behavior . . . . .	.46

Browser Exploits . . . . .	.46
Web Spoofing . . . . .	.46
Configuring Internet Explorer Securely . . . . .	.47
Protected Mode . . . . .	.48
ActiveX Opt-In . . . . .	.48
Fix My Settings . . . . .	.49
Security Status Bar . . . . .	.50
Windows Defender . . . . .	.50
Setting Internet Zones . . . . .	.50
Configuring Privacy . . . . .	.52
Advanced Security Settings . . . . .	.55
Configuring the Microsoft Phishing Filter . . . . .	.56
Windows Security Center . . . . .	.59
Configuring a Firewall . . . . .	.60
Using Windows Update . . . . .	.63
Using the Malicious Software Removal Tool . . . . .	.65
Configuring Malware Protection . . . . .	.65
Other Security Settings . . . . .	.69
User Account Control . . . . .	.69
Windows Defender . . . . .	.71
Using Windows Defender . . . . .	.72
How to Use the Windows Defender Software Explorer . . . . .	.75
Using Software Explorer . . . . .	.76
Other Related Tools . . . . .	.76
Using Microsoft SpyNet . . . . .	.77
Summary . . . . .	.78
Solutions Fast Track . . . . .	.79
Frequently Asked Questions . . . . .	.83
<b>Chapter 3 Microsoft Vista: Securing User Access . . . . .</b>	<b>87</b>
Introduction . . . . .	.88
Access Control Fundamentals . . . . .	.88
Limiting Exposure . . . . .	.89
Understanding Attacks . . . . .	.90
Password Cracking . . . . .	.90
Rootkits . . . . .	.92
Using Encryption . . . . .	.92

Secure Protocols . . . . .	93
Kerberos . . . . .	93
SSH . . . . .	94
Authentication Devices . . . . .	94
Smart Card Authentication . . . . .	95
Biometrics Authentication . . . . .	96
Keeping Workstations Secure . . . . .	97
Improving the Logon Architecture . . . . .	98
Session 0 . . . . .	100
User Account Control . . . . .	102
Using User Access Control . . . . .	103
Marking an Application . . . . .	104
Using the Local Security Policy to Configure UAC . . . . .	105
Disabling UAC When Installing Applications . . . . .	107
Changing the Prompt for UAC . . . . .	107
Remote Assistance . . . . .	108
Using Remote Assistance . . . . .	111
Sending an Invitation . . . . .	112
Network Access Protection . . . . .	113
Summary . . . . .	115
Solutions Fast Track . . . . .	115
Frequently Asked Questions . . . . .	119

<b>Chapter 4 Microsoft Vista: Trusted Platform Module Services . . . . .</b>	<b>123</b>
Introduction . . . . .	124
Understanding the TPM . . . . .	124
Trusted Platform Features . . . . .	127
Trusted Platform Architecture . . . . .	128
The TCG Trusted Platform . . . . .	128
Your Windows Vista PC . . . . .	133
The Role of the TBS . . . . .	138
Configuring and Managing the TPM on a Stand-Alone System . . . . .	139
Configuring BIOS Settings . . . . .	141
Using the TPM Microsoft Management Console . . . . .	142
Initializing the TPM . . . . .	143
Turning the TPM On . . . . .	145

Turning the TPM Off . . . . .	148
Clearing the TPM . . . . .	149
Changing the Owner Password . . . . .	153
Blocking and Allowing Commands . . . . .	155
Configuring and Managing the	
TPM in an Enterprise Environment . . . . .	163
Using GPOs and Active Directory . . . . .	165
Preparing Your Pre-Longhorn Domain Controllers . . . . .	165
Preparing Your Longhorn Domain Controllers . . . . .	170
Blocking Commands . . . . .	171
Deploying TPM-Equipped Devices with Scripting . . . . .	173
Your TPM WMI Primer . . . . .	173
Scripting the TPM Deployment . . . . .	175
TPM Applications . . . . .	178
Digital Rights Management . . . . .	178
Microsoft Applications . . . . .	179
Third-Party Applications . . . . .	180
Understanding the Security Implications of the TPM . . . . .	181
Encryption as a Countermeasure . . . . .	181
Can I Really Trust These People? . . . . .	185
The TPM Only Enables Technical Security Controls . . . . .	186
Existing Attacks . . . . .	187
Summary . . . . .	189
Solutions Fast Track . . . . .	190
Frequently Asked Questions . . . . .	192
<b>Chapter 5 Microsoft Vista: Data Protection . . . . .</b>	<b>195</b>
Introduction . . . . .	196
USB Devices . . . . .	196
ReadyBoost: Plug In to Speed . . . . .	197
USB Group Policy Settings . . . . .	198
Controlling Device Installation . . . . .	199
A Real-World Scenario of Device Installation . . . . .	203
Controlling Device Use . . . . .	206
Real-World Usage: Our Road Warrior Returns . . . . .	209
Rights Management . . . . .	209
Rights Management Is Bad—No, Good—No, Bad... . . . .	210
Rights Management Is Doomed to Failure . . . . .	211



Rights Management Can Only Succeed . . . . .211

Encrypting File System . . . . .214

    A Little Crypto Theory . . . . .214

    Ancient History: What You Should Already Know . . . .215

        Enabling Encryption on a File or Folder . . . . .216

        Exporting Your EFS Encryption Keys . . . . .219

        Adding Users to EFS-Protected Files . . . . .220

        Creating a Nondefault EFS Policy . . . . .220

        Exporting and Deleting EFS Private Keys . . . . .223

        Recovering EFS-Protected Files . . . . .225

        New EFS Features with Windows Vista . . . . .227

Whole-Disk Encryption . . . . .227

    It's Been a While Coming . . . . .229

        Preparing a New Installation of Vista for BitLocker 232

        Preparing an Upgrade of Vista for BitLocker . . . .234

        Preparing an Existing

        Installation of Vista for BitLocker: The Hard Way . .234

        Preparing an Existing

        Installation of Vista for BitLocker: The Easy Way . .236

        Enabling BitLocker to

        Protect Your Laptop's Data in Case of Loss . . . . .236

        Using manage-bde.wsf

        to Protect Volumes other Than the Boot Volume . . .243

        Recovering a BitLocker

        System after Losing Your Startup Key or PIN . . . . .248

        Removing BitLocker Protection

        Temporarily to Install a BIOS or System Update . . .249

    BitLocker with TPM: What Does It Give You? . . . . .251

    BitLocker with EFS: Does It Make Sense? . . . . .252

    BitLocker for Servers . . . . .253

    Using BitLocker to Decommission a System . . . . .253

PatchGuard . . . . .254

    What Is PatchGuard? . . . . .255

        Why Only 64-Bit? . . . . .257

    Why Third-Party Security

    Companies Don't Want to Use PatchGuard . . . . .257

Summary . . . . .	260
Solutions Fast Track . . . . .	260
Frequently Asked Questions . . . . .	263
<b>Chapter 6 Microsoft Vista: Networking Essentials . . .</b>	<b>267</b>
Introduction . . . . .	268
Not Your Father's TCP/IP Stack . . . . .	268
Limitations of IPv4 . . . . .	269
Limited Address Space . . . . .	269
Security and Quality of Service . . . . .	273
Host and Router Configuration . . . . .	274
Introduction to IPv6 and Dual Layer . . . . .	274
Increased Address Space . . . . .	275
Built-in Security and QoS . . . . .	276
Windows Vista Support for IPv6 . . . . .	276
Understanding the Dual-Layer Architecture . . . . .	277
Configuring IPv6 Using the GUI . . . . .	278
Configuring IPv6 from the Command Line . . . . .	281
Using the Network and Sharing Center . . . . .	282
Working with Network Sharing and Discovery . . . . .	283
Network Discovery . . . . .	283
Working with File and Printer Sharing . . . . .	286
Introducing Public Folder Sharing . . . . .	287
Password-Protected Sharing . . . . .	288
Media Sharing . . . . .	289
Working with Network Locations . . . . .	289
Using the Network Map . . . . .	291
Troubleshooting with the Network Map . . . . .	292
Working with the Windows Firewall . . . . .	295
Configuring the Windows Firewall . . . . .	296
Working with Built-In Firewall Exceptions . . . . .	299
Creating Manual Firewall Exceptions . . . . .	302
Advanced Configuration of the Windows Firewall . . . . .	305
Modifying IPSec Defaults . . . . .	309
Creating Connection Security Rules . . . . .	317
Creating Firewall Rules . . . . .	325
Monitoring the Windows Firewall . . . . .	338

Summary	340
Solutions Fast Track	340
Frequently Asked Questions	342
<b>Chapter 7 Microsoft Vista: Wireless World</b>	<b>345</b>
Introduction	346
What's New with Wireless in Vista?	346
Native Wireless Architecture	347
UI Improvements	348
Wireless Group Policy	350
Wireless Auto Configuration	350
WPA2 Support	353
Integration with NAP When Using 802.1x	353
EAP Host Infrastructure	354
Microsoft Vista Network Diagnostics Framework	354
Command-Line Support	356
Network Location Awareness and Profiles	358
Next-Generation TCP/IP Stack	358
Single Sign-on	358
Wireless Security	358
Wireless Ranges	359
Why We Need Security	360
The Two Main Security Threats: Access and Privacy	360
Access	361
Privacy	368
WPA and WPA2 Modes	372
Attacks against WPA	374
Rogue Access Points	375
Detecting and Protecting against Rogue Access Points	376
Security Enhancements Using 802.1x/EAP	378
EAP	378
802.1x	379
Network Group Policy Enhancements	380
Mixed Security Mode	381
Allow and Deny Lists for Wireless Networks	381
Extensibility	382
Wired LAN Settings	383

Network Awareness . . . . .	383
Error Messages and Troubleshooting Improvements . . .	383
Configuring Wireless Security in Vista . . . . .	384
Configuring Wireless Security	
Using the Connect to a Network Dialog Box . . . . .	385
Configuring Wireless Security from the Command Line	391
Summary . . . . .	394
Solutions Fast Track . . . . .	394
Frequently Asked Questions . . . . .	396
<b>Chapter 8 Microsoft Vista: Windows Mail. . . . .</b>	<b>399</b>
Introduction . . . . .	400
Comparing WindowsMail with Outlook Express . . . . .	400
Database Architecture . . . . .	402
Loss Prevention and Identities . . . . .	405
Phishing Filter . . . . .	414
Scanning from the Start . . . . .	415
Working with Filtered Mail . . . . .	417
Junk Mail Filter . . . . .	422
SmartScreen . . . . .	422
Configuring Junk E-Mail Options . . . . .	423
Instant Search . . . . .	429
Basic Functionality . . . . .	430
Searching from within Instant Mail . . . . .	432
Summary . . . . .	437
Solutions Fast Track . . . . .	437
Frequently Asked Questions . . . . .	439
<b>Chapter 9 Microsoft Vista: Update and Monitoring Services . . . . .</b>	<b>441</b>
Introduction . . . . .	442
Using Windows Update . . . . .	444
Windows Update Settings . . . . .	445
Installing Updates Automatically . . . . .	447
Choosing Whether to Install Downloaded Updates	448
Checking for Updates but Choosing	
Whether to Download and Install Them . . . . .	449
Never Checking for Updates . . . . .	450
Using Microsoft Update . . . . .	451

Installing Microsoft Update . . . . .	451
Enabling and Disabling Microsoft Update . . . . .	452
Managing Updates . . . . .	452
Checking for Updates . . . . .	452
Installing Updates . . . . .	453
Viewing the Update History . . . . .	455
Restoring Hidden Updates . . . . .	456
Uninstalling Updates . . . . .	457
Scripting Windows Update Settings . . . . .	460
Enabling and Scheduling Automatic Updates . . . . .	461
Opt-In to Microsoft Update . . . . .	463
Using Windows Server Update Services (WSUS) and Vista	463
Windows Server Update Services 2 . . . . .	464
WSUS 2 Stand-Alone Installation . . . . .	466
WSUS 2 Active Directory Integration . . . . .	472
Administering WSUS . . . . .	473
Windows Server Update Services 3 . . . . .	481
WSUS 3 Stand-Alone and Active Directory Installations . . . . .	481
WSUS 3 MMC 3.0 Administrative Interface . . . . .	481
Using Systems Management Server and Vista . . . . .	491
SMS 2003 and Vista . . . . .	491
System Center Configuration Manager 2007 Beta 1 and Vista . . . . .	492
Using Microsoft Operations Manager and Vista . . . . .	493
System Center Operations Manager 2007 RC2 . . . . .	494
Monitoring Clients and Servers . . . . .	495
System Center Essentials 2007 Beta 2 . . . . .	497
Using Third-Party Tools with Vista . . . . .	497
Altiris . . . . .	498
Installing the Altiris Client Management Suite . . . . .	499
Managing Vista Clients . . . . .	500
Software Delivery Methods . . . . .	504
Managing Software Updates . . . . .	505
Other Third-Party Tools . . . . .	506
Summary . . . . .	507
Solutions Fast Track . . . . .	508
Frequently Asked Questions . . . . .	510

<b>Chapter 10 Disaster Recovery with Exchange Server 2007</b> . . . . .	<b>513</b>
Introduction . . . . .	514
Backing Up Exchange 2007 Using Windows 2003 Backup	514
Backing Up an Exchange 2007 Mailbox Server . . . . .	514
Backing Up an Exchange 2007 Hub Transport Server . . . . .	518
Backing Up an Exchange 2007 Client Access Server . . . . .	519
Backing Up an Exchange 2007 Unified Messaging Server . . . . .	522
Backing Up an Exchange 2007 Edge Transport Server	523
Restoring Exchange 2007 Storage Groups and Databases Using Windows 2003 Backup . . . . .	523
Repairing a Corrupt or Damaged Exchange 2007 Database Using Eseutil . . . . .	527
Restoring Mailbox Data Using the Recovery Storage Group Feature . . . . .	533
Managing Recovery Storage Groups Using the Exchange Troubleshooting Assistant . . . . .	534
Managing Recovery Storage Groups Using the Exchange Management Shell . . . . .	543
Recovering an Exchange 2007 Server Using the RecoverServer Switch . . . . .	547
Restoring and Configuring the Operating System . . . . .	548
Installing Exchange 2007 Using the RecoverServer Switch . . . . .	549
Recovering an Exchange 2007 Cluster Using the RecoverCMS Switch . . . . .	551
Restoring Mailbox Databases Using the Improved Database Portability Feature . . . . .	552
Summary . . . . .	556
Solutions Fast Track . . . . .	556
Frequently Asked Questions . . . . .	560
<b>Appendix A Microsoft Vista: The International Community</b> . . . . .	<b>563</b>
Microsoft vs. The World: What's the Issue? . . . . .	564
Microsoft Vista: The EU Fixes . . . . .	564

The 2004 Ruling . . . . .564  
     August 2003: A Preliminary Decision . . . . .565  
     March 2004: The Ruling . . . . .565  
     March 2004: The Punishment . . . . .569  
     The March 2004 Ruling in Practice . . . . .570  
 Vista . . . . .572  
     Problems Begin . . . . .572  
     Threats and a Response . . . . .574  
     Four Areas of Concern . . . . .574  
     October 2006: Microsoft’s Concessions . . . . .576  
     Immediate Results of the October Press Conference . . . . .578  
     Putting Out Fire with Gasoline . . . . .579  
     Initial Release of the PatchGuard APIs . . . . .581  
 Microsoft and Japan . . . . .581  
     The Raid in Tokyo . . . . .582  
     The JFTC’s Recommendation  
     and Microsoft’s Response . . . . .582  
 Microsoft Vista: The Korean Fixes . . . . .583  
     The Complaint . . . . .583  
     The KFTC’s Decision . . . . .584  
     Two Versions of XP . . . . .584  
     Two Versions of Vista . . . . .584  
 Notes and Sources . . . . .585  
     Microsoft Vista: The EU Fixes . . . . .585  
         The March 2004 Ruling . . . . .585  
         Vista . . . . .586  
         The October Concessions . . . . .587  
         Squabbling over Security . . . . .587  
     Microsoft and Japan . . . . .589  
     Microsoft Vista: The Korean Fixes . . . . .589  
         Changes to XP . . . . .590  
         Vista . . . . .590  
 Summary . . . . .591

**Appendix B Microsoft Vista: The EULA . . . . . 593**  
     Introduction . . . . .594  
     Criticism and Change . . . . .594

Benchmark Testing . . . . .	.595
Rigging the Tests . . . . .	.596
Virtualization . . . . .	.597
Virtualization Controls . . . . .	.598
DRM and Virtualization . . . . .	.600
Notes and Sources . . . . .	.601
EULA Overview . . . . .	.601
Benchmarking . . . . .	.601
Virtualization . . . . .	.602
Summary . . . . .	.602
<b>Index. . . . .</b>	<b>603</b>



# Foreword

In 2001, the IT community was celebrating the long-awaited release of Microsoft's Windows XP. The release of Windows XP was a major milestone for Microsoft because it was the first time that the company had created an NT kernel-based operating system intended for both businesses and consumers. Windows XP was designed to render DOS-based operating systems such as Windows 9x and Windows ME obsolete forever. Sadly, the celebration was short-lived, though, as it became apparent that Windows XP and Internet Explorer were both plagued with security problems.

At first these security problems were mostly a concern for businesses. It wasn't long, however, before consumers began to feel the consequences of these security holes as well. Nuisances such as Trojans, spyware, pop-ups, and browser hijackers quickly went from existing in relative obscurity to becoming an almost overnight epidemic.

In 2003, Microsoft was hard at work on Service Pack 2 for Windows XP, which was originally intended to consist of a set of critical security patches and hotfixes that had been rolled up into a service pack. But everything changed when the Slammer worm hit.

The development team in Redmond was already hard at work on a new desktop operating system, code-named Longhorn (now known as Windows Vista). Longhorn was slated to include code that would prevent Slammer-type worms from being effective, but the new operating system was still years away from being ready to be released.

Fearing another Slammer-type attack, Microsoft Vice President Jim Allchin made the decision to halt the development of Longhorn and mandated that much of the Longhorn code be adapted to Windows XP and included in Service Pack 2.

Service Pack 2 was released on August 6, 2004. However, the service pack didn't fix all of Windows XP's security problems, although it did help to some extent. In retrospect it was probably good that Microsoft created Service Pack 2 from Longhorn code. This strategy gave the company the chance to see that the code was not completely secure, thus providing Microsoft with a chance to rewrite the code prior to Vista's release.

All this hard work apparently has paid off, though. Windows Vista is the first desktop operating system released under Microsoft's Trustworthy Computing Initiative, and it is without a doubt the most secure OS that Microsoft has released to date.

Even so, Vista isn't completely secure right out of the box. Like every previous Windows operating system, Vista is highly customizable, and the settings that you configure Vista to use play a role in how secure the operating system really is. For example, there will undoubtedly be security updates released for Vista as new security threats are discovered. If Vista isn't configured to receive these updates, though, then it will be less secure than an updated version of Vista.

That's where *Microsoft Vista for IT Security Professionals* is helpful. This book discusses all of the enhanced security mechanisms that are present in Vista. It also shows you how to configure these mechanisms for optimal security.

—Brien M. Posey  
Vice President of Research and Development,  
Relevant Technologies  
[www.relevanttechnologies.com](http://www.relevanttechnologies.com)

# About the CD



The CD icon that appears beside certain sections of the chapters in this book indicates that this material is available on the CD. The CD also includes scripts and other adjunct material. We hope this material is helpful to you.