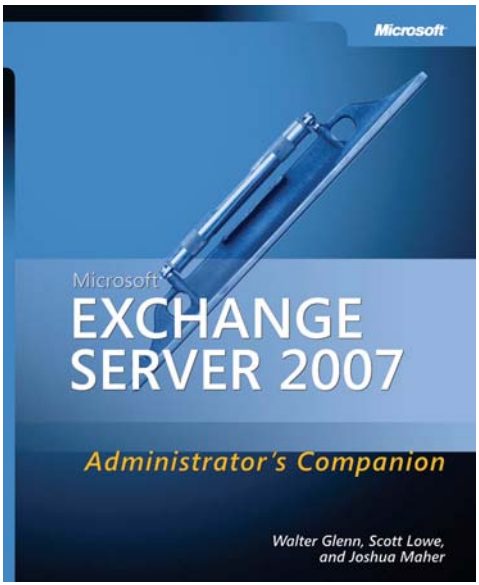


Microsoft® Exchange Server 2007 Administrator's Companion

Walter Glenn, Scott Lowe, and Joshua Maher

To learn more about this book, visit Microsoft Learning at
http://www.microsoft.com/MSPress/books/9545.aspx

9780735623507

Microsoft Press

Resources for IT Professionals

Published and Forthcoming Titles from Microsoft Press

Windows Server

Microsoft® Windows Server® 2003 *Resource Kit*
Microsoft MVPs and Partners with Microsoft Windows Server Team
978-0-7356-2232-6

Microsoft Windows Server 2003 *Administrator's Companion* Second Edition
Charlie Russel, Sharon Crawford, and Jason Gerend
978-0-7356-2047-6

Microsoft Windows Server 2003 *Inside Out*
William R. Stanek
978-0-7356-2048-3

Microsoft Windows Server 2003 *Administrator's Pocket Consultant* Second Edition
William R. Stanek
978-0-7356-2245-6

Windows Client

Windows Vista™ *Resource Kit*
Tulloch, Northrup, Honeycutt, Russel, and Wilson with the Microsoft Windows Vista Team
978-0-7356-2283-8

Windows Vista *Administrator's Pocket Consultant*
William R. Stanek
978-0-7356-2296-8

Microsoft Windows® XP Professional *Resource Kit* Third Edition
The Microsoft Windows Team with Charlie Russel and Sharon Crawford
978-0-7356-2167-1

Microsoft Windows XP Professional *Administrator's Pocket Consultant* Second Edition
William R. Stanek
978-0-7356-2140-4

Microsoft Windows Command-Line *Administrator's Pocket Consultant*
William R. Stanek
978-0-7356-2038-4

SQL Server 2005

Microsoft SQL Server™ 2005 *Administrator's Pocket Consultant*
William R. Stanek
978-0-7356-2107-7

Microsoft SQL Server 2005 *Administrator's Companion*
Whalen, Garcia, et al.
978-0-7356-2198-5

Inside Microsoft SQL Server 2005: The Storage Engine
Kalen Delaney
978-0-7356-2105-3

Inside Microsoft SQL Server 2005: T-SQL Programming
Itzik Ben-Gan, Dejan Sarka, and Roger Wolter
978-0-7356-2197-8

Exchange Server 2007

Microsoft Exchange Server 2007 *Administrator's Companion*
Walter Glenn and Scott Lowe
978-0-7356-2350-7

Microsoft Exchange Server 2007 *Administrator's Pocket Consultant*
William R. Stanek
978-0-7356-2348-4

Scripting

Microsoft Windows PowerShell™ *Step by Step*
Ed Wilson
978-0-7356-2395-8

Microsoft VBScript *Step by Step*
Ed Wilson
978-0-7356-2297-5

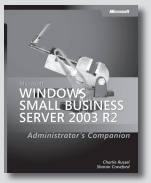
Microsoft Windows Scripting with WMI: Self-Paced Learning Guide
Ed Wilson
978-0-7356-2231-9

Advanced VBScript for Microsoft Windows Administrators
Don Jones and Jeffery Hicks
978-0-7356-2244-9

RELATED TITLES

Microsoft Office SharePoint® Server 2007 *Administrator's Companion*
Bill English with the Microsoft SharePoint Community Experts
978-0-7356-2282-1

Microsoft Windows Security *Resource Kit* Second Edition
Ben Smith and Brian Komar with the Microsoft Security Team
978-0-7356-2174-9



Microsoft Windows Small Business Server 2003 R2 *Administrator's Companion*
Charlie Russel and Sharon Crawford
978-0-7356-2280-7

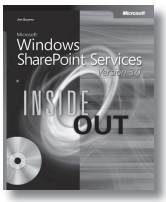
Microsoft Internet Security and Acceleration (ISA) Server 2004 *Administrator's Pocket Consultant*
Bud Ratliff and Jason Ballard with the Microsoft ISA Server Team
978-0-7356-2188-6

2007 Microsoft® Office System Resources for Developers and Administrators

Microsoft Office SharePoint® Server 2007 Administrator's Companion

Bill English with the Microsoft SharePoint Community Experts
ISBN 9780735622821

Get your mission-critical collaboration and information management systems up and running. This comprehensive, single-volume reference details features and capabilities of SharePoint Server 2007. It delivers easy-to-follow procedures, practical workarounds, and key troubleshooting tactics—for on-the-job results.



Microsoft Windows SharePoint Services Version 3.0 Inside Out

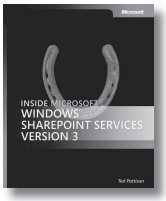
Errin O'Connor
ISBN 9780735623231

Conquer Microsoft Windows SharePoint Services—from the inside out! This ultimate, in-depth reference packs hundreds of time-saving solutions, troubleshooting tips, and workarounds. You're beyond the basics, so now learn how the experts tackle information sharing and team collaboration—and challenge yourself to new levels of mastery!

Microsoft SharePoint Products and Technologies Administrator's Pocket Consultant

Ben Curry
ISBN 9780735623828

Portable and precise, this pocket-sized guide delivers immediate answers for the day-to-day administration of Sharepoint Products and Technologies. Featuring easy-to-scan tables, step-by-step instructions, and handy lists, this book offers the straightforward information you need to get the job done—whether you're at your desk or in the field!



Inside Microsoft Windows® SharePoint Services Version 3

Ted Pattison and Daniel Larson
ISBN 9780735623200

Get in-depth insights on Microsoft Windows SharePoint Services with this hands-on guide. You get a bottom-up view of the platform architecture, code samples, and task-oriented guidance for developing custom applications with Microsoft Visual Studio® 2005 and Collaborative Application Markup Language (CAML).

Inside Microsoft Office SharePoint Server 2007

Patrick Tisseghem
ISBN 9780735623682

Dig deep—and master the intricacies of Office SharePoint Server 2007. A bottom-up view of the platform architecture shows you how to manage and customize key components and how to integrate with Office programs—helping you create custom enterprise content management solutions.

Microsoft Office Communications Server 2007 Resource Kit

Microsoft Office Communications Server Team
ISBN 9780735624061

Your definitive reference to Office Communications Server 2007—direct from the experts who know the technology best. This comprehensive guide offers in-depth technical information and best practices for planning, designing, deploying, managing, and optimizing your systems. Includes a toolkit of valuable resources on CD.

Programming Applications for Microsoft Office Outlook® 2007

Randy Byrne and Ryan Gregg
ISBN 9780735622494

Microsoft Office Visio® 2007 Programming Step by Step

David A. Edson
ISBN 9780735623798

See more resources at **microsoft.com/mspress** *and* **microsoft.com/learning**

Microsoft Press® products are available worldwide wherever quality computer books are sold. For more information, contact your bookseller, computer retailer, software reseller, or local Microsoft Sales Office, or visit our Web site at **microsoft.com/mspress**. To locate a source near you, or to order directly, call 1-800-MSPRESS in the United States. (In Canada, call **1-800-268-2222**.)

Microsoft® Press

Windows Vista™ Resources for Administrators

Windows Vista Administrator's Pocket Consultant

William Stanek
ISBN 9780735622968

Portable and precise, this pocket-sized guide delivers immediate answers for the day-to-day administration of Windows Vista. Featuring easy-to-scan tables, step-by-step instructions, and handy lists, this book offers the straightforward information you need to solve problems and get the job done—whether you're at your desk or in the field!

Windows Vista Resource Kit

Mitch Tulloch, Tony Northrup, Jerry Honeycutt, Ed Wilson, Ralph Ramos, and the Windows Vista Team
ISBN 9780735622838

Get the definitive reference for deploying, configuring, and supporting Windows Vista—from the experts who know the technology best. This guide offers in-depth, comprehensive technical guidance on automating deployment; implementing security enhancements; administering group policy, files folders, and programs; and troubleshooting. Includes an essential toolkit of resources on DVD.

MCTS Self-Paced Training Kit (Exam 70-620): Configuring Windows Vista Client

Ian McLean and Orin Thomas
ISBN 9780735623903

Get in-depth preparation plus practice for Exam 70-620, the required exam for the new Microsoft Certified Technology Specialist (MCTS): Windows Vista Client certification. This 2-in-1 kit focuses on installing client software and configuring system settings, security features, network connectivity, media applications, and mobile devices. Ace your exam prep—and build real-world job skills—with lessons, practice tests, evaluation software, and more.

MCITP Self-Paced Training Kit (Exam 70-622): Installing, Maintaining, Supporting, and Troubleshooting Applications on the Windows Vista Client – Enterprise

Tony Northrup and J.C. Mackin
ISBN 9780735624085

Maximize your performance on Exam 70-622, the required exam for the new Microsoft® Certified IT Professional (MCITP): Enterprise Support Technician certification. Comprehensive and in-depth, this 2-in-1 kit covers managing security, configuring networking, and optimizing performance for Windows Vista clients in an enterprise environment. Ace your exam prep—and build real-world job skills—with lessons, practice tests, evaluation software, and more.

MCITP Self-Paced Training Kit (Exam 70-623): Installing, Maintaining, Supporting, and Troubleshooting Applications on the Windows Vista Client – Consumer

Anil Desai with Chris McCain of GrandMasters
ISBN 9780735624238

Get the 2-in-1 training kit for Exam 70-623, the required exam for the new Microsoft Certified IT Professional (MCITP): Consumer Support Technician certification. This comprehensive kit focuses on supporting Windows Vista clients for consumer PCs and devices, including configuring security settings, networking, troubleshooting, and removing malware. Ace your exam prep—and build real-world job skills—with lessons, practice tests, evaluation software, and more.

See more resources at **microsoft.com/mspress** *and* **microsoft.com/learning**

Microsoft® Press

Table of Contents

Introduction . . . . . *xxi*

Part I
Introduction

1 Overview of Microsoft Exchange Server 2007 3

What Is Exchange Server? 3
Editions of Exchange Server 2007 4
Exchange Server 2007 Standard Edition 4
Exchange Server 2007 Enterprise Edition 5
Understanding Basic Concepts 5
Messaging Systems 5
The Organization of an Exchange Environment 8
Exchange Server Storage 11
What's New in Exchange Server 2007 13
Active Directory Site Routing 14
Split Permissions Model 14
Exchange Server 2007 Setup Wizard 14
Exchange Management 14
Exchange Server Roles 15
Unified Messaging 15
Messaging Policy and Compliance 15
Anti-Spam and Antivirus 15
64-Bit Architecture 16
Outlook Web Access 16
Summary 17

2 Active Directory for Exchange Administrators 19

Brief Overview of Active Directory 19
Directory Structure in Active Directory 20
Logical Structure of Active Directory 20
Groups 25
Other Active Directory Components 27
Naming Partitions 27
Sites 28
Location Service Providers 28
Global Catalog Servers 28
Client Authentication 29
Active Directory Names 30
Exchange Server 2007 and Active Directory 31
Exchange Server 2007 and Active Directory Site Topology 31
Storing Exchange Server 2007 Data in Active Directory 33
Exchange Server 2007 and Forest Boundaries 36
Configuration Partition and Directory Data 37
DNS Configuration 37
Summary 38

3 Exchange Server 2007 Architecture 39

The Role of Exchange Server 2007 Roles 39
Mailbox Server Role 40
Client Access Server Role 41
Hub Transport Server Role 42
Unified Messaging Server Role 43
Edge Transport Server Role 44
Storage Design Goals in Exchange Server 2007 45
Stores and Storage Groups 46
Increased User Support 48
Individual Backup and Restore 49
Database File Structure 50
On-Demand Content Conversion 50
Single-Instance Message Store 50

Data Recovery and Transaction Logs 51
The Extensible Storage Engine 51
Transaction Log Files 57
The Web Folder Client 62
Public Folders 63
Multiple Public Folder Trees 64
Indexing 64
Index Catalogs 66
Index Size 67
Exchange Server Storage Design 67
Supported Storage Technologies 67
Choosing a RAID Level 68
Planning for Disk Space 69
Logical Unit Number (LUN) Layout 70
Other Storage Notes 71
Testing Your Storage Architecture 72
Transport Architecture 73
SMTP Connectors 73
Creating SMTP Connectors 74
Message Routing 74
Message Transport Scenarios 78
Transport Protocols 81
Summary 83

Part II
Planning Your Deployment

4 Assessing Needs 87

Defining User Needs 88
Messaging 88
Public Folders 89
Connections to Other Systems 90
Remote Access 91
Custom Applications 91
Training and Support Services 91

Assessing Current Resources 92
Defining Your Geographic Profile 92
Defining Your Software Environment 92
Defining Your Network Topology 93
Defining Your Active Directory Model 96
Defining Administrative Needs 98
Summary 98

5 Planning for Deployment 99

Planning the Organization 99
Establishing a Naming Convention 99
Planning Public Folders 102
Planning Gateways 103
Planning Servers 104
Disk Considerations 104
Processor Considerations 106
Memory Considerations 108
Network Considerations 108
Ways to Add Fault Tolerance 109
Summary 109

Part III
Installation and Deployment

6 Installing Exchange Server 2007 113

Preparing for the Installation 114
Gathering Information 114
Verifying Hardware Requirements 116
Getting Service Packs 117
Defining the Role of Your Server 118
Optimizing Hardware through Configuration 119
Verifying System Requirements 120
Creating the Exchange Administrator's Account 124
Playing It Safe 125
Performing the Installation 125
Preparing the Active Directory Environment 126

Installing Exchange Server 2007 in a New Organization 128
The Role of Roles 130
Installing in an Existing Organization 135
Verifying Your Installation 136
Finalizing Exchange Server 2007 Deployment 138
Keeping Exchange Healthy 142
Summary 143

7 Coexisting with Previous Versions of Exchange Server 145

Chapter Background 146
Terminology 146
Exchange Server 2007 Coexistence Deployment Considerations 147
Exchange Server 2003 Native Mode 147
Automatic Coexistence Tasks 148
Global Settings 149
Installing Exchange Server 2007 into an Existing Exchange Server 2003 Organization 150
Coexistence Administration Issues 152
Creating Additional Routing Group Connectors 153
Coexistence Issue: Version-Specific Administration 155
SMTP Connectors and Internet E-Mail 156
Handling Internet E-Mail 157
Adding an SMTP Connector to Your Legacy Exchange Organization . . . 158
Public Folders 162
Public Folder Replication 163
Handling Public Folder Referrals 164
Administering Public Folders 166
Recipient Update Service 167
Complete Coexistence Notes 168
Summary 181

8 Transitioning to Exchange Server 2007 183

The Example Scenario 184
Transition Options 185
Transition Limitations 185
Move Internet Mail to Exchange Server 2007 186

Allow Mail to Flow to the Internet . . . 187
Allow Incoming Mail from the Internet . . . 190
Moving Mailboxes to Exchange Server 2007 . . . 192
The Decommissioning Process . . . 199
Re-Home Client Services . . . 200
Remove SMTP Connectors from Your Legacy Exchange Organization . . . 200
Re-Home Public Folders . . . 201
Move the Offline Address Book to Exchange Server 2007 . . . 203
Move the Recipient Update Service to Exchange Server 2007 . . . 204
Remove Legacy Connectors . . . 205
Uninstall Exchange from Legacy Exchange Servers . . . 207
Remove Legacy Exchange Routing Groups . . . 207
Summary . . . 208

9 High Availability in Exchange Server 2007 . . . 209

Continuous Replication and Transaction Logs . . . 210
Local Continuous Replication . . . 213
Preparing for LCR . . . 214
Enabling Local Continuous Replication . . . 215
Cluster Continuous Replication . . . 223
CCR Terminology . . . 224
Preparing for CCR . . . 226
Enabling Continuous Cluster Replication . . . 227
Establishing the Cluster . . . 229
Configure the MNS Quorum to Use the File Share Witness . . . 233
Installing Exchange Server 2007 on Your Cluster . . . 233
Verifying the Status of Your CCR . . . 236
Verifying That a Server Can Handle a Failover . . . 236
Configuring the Transport Dumpster . . . 237
Closing Thoughts on CCR . . . 238
Single Copy Clusters . . . 239
Summary . . . 242

Part IV
Management

10 Managing Exchange Server 2007 245

Microsoft Management Console 246
The MMC User Interface 246
How MMC Works 249
Using the Exchange Management Console 251
Major Areas of the Exchange Management Console 252
Examining the Exchange Hierarchy 254
Using the Exchange Management Shell 260
Understanding Cmdlets 262
Getting Help 263
Summary 265

11 Creating and Managing Recipients 267

Understanding Recipient Types 268
Users 269
Mailbox Users 269
Mail-Enabled Users 286
Mailbox Resources 288
Mail Contacts 289
Creating a Mail Contact 289
Configuring a Mail Contact 291
Distribution Groups 291
Creating a Distribution Group 292
Configuring a Group 293
Creating Dynamic Distribution Groups 296
Filtering Recipients 297
Templates 298
Address Lists 299
Summary 302

12 Using Public Folders 303

Understanding Public Folder Storage 304
Using Public Folders in Outlook 2007 305
Creating a Public Folder in Outlook 305
Managing Public Folders in Outlook 305
Managing Public Folder Databases in the Exchange Management Console . . . 307
Creating a New Public Folder Database 308
Removing a Public Folder Database 309
Creating and Managing Public Folders in the Exchange Management Shell . . . 311
Creating a Public Folder 311
Removing a Public Folder 311
Getting Information about a Public Folder 312
Managing Settings for a Public Folder 312
Summary 314

13 Creating and Managing Storage Groups 315

Review of Exchange Server 2007 Storage Architecture 315
Benefits of Using Storage Groups 317
Increased User Support 318
Individual Backup and Restore 319
Hosting of Multiple Businesses 319
Support for Special Mailboxes 320
Planning Storage Groups 320
Planning for Disk Space 321
Planning for Multiple Storage Groups 324
Planning for Backup and Restore Throughput 325
Managing Storage Groups 326
Creating Storage Groups 326
Modifying Storage Group Configuration 329
Removing Storage Groups 332
Managing Stores 333
Creating a Mailbox Store 333
Modifying Mailbox Database Configuration 335
Summary 343

14 Unified Messaging 345

Unified Messaging Overview 346

Unified Messaging Features 346
Exchange Server 2007 Unified Messaging Objects 348
Creating and Managing Unified Messaging Objects 350
Unified Messaging Dial Plans 350
Unified Messaging Mailbox Policy 357
Unified Messaging IP Gateways 363
Associating Servers with Dial Plans 366
Enabling Unified Messaging for Individual Mailboxes 367
Summary 370

Part V
Maintenance

15 Troubleshooting Exchange Server 2007 373
Using Troubleshooting Tools 373
Using Event Viewer 373
Using Diagnostics Logging 375
Inbox Repair Tool 379
RPing Utility 380
Eseutil.exe Offline Tool 383
Best Practices Analyzer 385
Mail Flow Troubleshooter 387
Performance Troubleshooter 389
Other Useful Utilities 390
Finding Help 390
Product Documentation 391
Microsoft TechNet 391
Internet Newsgroups 391
Summary 392

16 Disaster Recovery 393
Backup and Restore Technologies 393
The Exchange Database 394
Volume Shadow Copy Service 399
Exchange Streaming Backup API 401
Other Exchange Server Components 405

Backup and Restore Strategies 406
Recovering an Exchange Mailbox Server 410
Recovering an Exchange Mailbox Database 414
Recovering a Single Exchange Mailbox 414
Backing up an Exchange Mailbox Server 416
Backing up an Exchange Mailbox Database 417
Backing up a Single Exchange Mailbox 418
Planning for Corruption 419
Implementing Backup Strategies 420
Operational Best Practices 425
Summary 426

17 Tuning Exchange Server 2007 Performance 427

Understanding How the Performance Snap-in Works 427
Performance Monitoring Concepts 428
Collecting Data with the Performance Snap-In 429
Viewing Collected Data 430
Evaluating the Four Main Subsystems in Windows 431
Evaluating Memory Usage 432
Evaluating Processor Usage 433
Evaluating Disk Usage 434
Evaluating Network Usage 436
Using the Performance Snap-in to Tune Exchange Server 2007 437
SMTP System Monitor Counters 437
Outlook Web Access 438
Unified Messaging Counters 439
Using Other Exchange Performance Tools 442
Microsoft Exchange Server Jetstress Tool 442
Exchange Load Generator 444
Summary 445

Part VI
Security

18 Security Policies and Exchange Server 2007 449

Why Are Information Security Policies Important? 450

Information Security Policies and Electronic Policies 452
Information Security Policies for Exchange Server 2007 453
Password Policies 453
Logon Policies 454
Acceptable Use Policies 455
Computer Viruses, Trojans, and Worms 456
Schema Extensions by Exchange Server 2007 457
Data Security 459
Legal Exposure to Unwanted E-Mail Content 460
Backing Up and Archiving Exchange Databases 461
E-Mail Integrity 462
Miscellaneous Elements to Consider 463
Related Resources 464
Summary 465

19 Exchange Server Security Basics 467

The Scope of Security 468
Motivations of a Criminal Hacker 469
How Hackers Work 470
Physical Security 474
Administrative Security 474
The Built-in Exchange Administrative Groups 475
The Add Exchange Administrator Wizard 477
SMTP Security 480
Computer Viruses 485
What Is a Virus? 485
Trojans 486
Worms 486
Junk E-Mail 487
Security Tools Provided by Microsoft 488
Summary 489

20 Antivirus and Anti-Spam 491

The Edge Transport Server at a Glance 491
Edge Transport Server Deployment 493
Verify the Edge Transport Server's DNS Suffix 493

Configure Firewalls to Pass Edge Traffic 494
Install Active Directory Application Mode 495
Install the Exchange Server 2007 Edge Transport Server Role 495
Subscribe the Edge Transport Server to the Exchange Server 2007 Organization 497
Managing Anti-Spam Features 502
Content Filtering 502
Connection Filtering: IP Allow List 506
Connection Filtering: IP Allow List Providers 508
Connection Filtering: IP Block List 509
Connection Filtering: IP Block List Providers 511
Recipient Filtering 514
Sender Filtering 515
Sender ID 517
Attachment Filtering 520
Managing Antivirus with Microsoft Forefront Security for Exchange Server . . . 524
About Microsoft Forefront Security for Exchange Server 525
Installing Microsoft Forefront Security for Exchange Server 525
Managing Microsoft Forefront Security for Exchange Server 527
Other Microsoft Forefront Security for Exchange Server Benefits 529
Summary 530

21 Securing Exchange Server 2007 Messages 531

Windows Server 2003 Security Protocols 531
Understanding the Public Key Infrastructure in Windows Server 2003 532
Encryption and Keys 532
Encryption Schemes 533
Certificate Services in Windows Server 2003 534
Managing the Public Key Infrastructure 540
Installing and Configuring Certificate Services 540
Installing Web Enrollment Support 545
Using the Web Enrollment Pages 546
Viewing Information About Certificates 551
Securing Messaging in Outlook 2007 555
Initially Trusting a Certificate 556

Encryption and Outlook 2007 . . . 556
Digital Signatures and Outlook 2007 . . . 557
S/MIME and Outlook 2007 . . . 557
Configuring Outlook 2007 for Secure Messaging . . . 558
Installing Exchange Certificate Templates . . . 560
Understanding How Exchange Server 2007 Integrates with Windows Server 2003 Security . . . 561
Summary . . . 564

Part VII
Clients

22 Overview of Exchange Clients . . . 567
Microsoft Office Outlook 2007 . . . 568
Windows Mail and Microsoft Outlook Express . . . 570
Outlook Web Access . . . 572
Standard Internet E-Mail Clients . . . 573
Non-Windows Platforms . . . 573
UNIX Clients . . . 574
Macintosh Clients . . . 574
Choosing a Client for Exchange Server . . . 574
Summary . . . 575

23 Deploying Microsoft Office Outlook 2007 . . . 577
Installing Outlook 2007 . . . 577
Standard Outlook Installation . . . 578
Installing Outlook 2007 by Using the Office Customization Tool . . . 579
Supporting Outlook 2007 . . . 579
Using Cached Exchange Mode . . . 580
Enabling Multiple Users in Outlook 2007 . . . 586
Outlook Anywhere . . . 590
Summary . . . 593

24 Supporting Outlook Web Access . . . 595
Features of OWA . . . 595
Deploying OWA . . . 596

Single-Server Scenario . . . 596
Multiserver Scenario . . . 597
ISA Server 2006 and OWA . . . 600
Authentication Options . . . 601
Configuring OWA Properties and Features . . . 610
Managing Access to UNC Shares and SharePoint Document Repositories . . . 611
OWA Segmentation . . . 617
OWA User Features . . . 622
Summary . . . 624

25 Supporting Other Clients . . . 625

Post Office Protocol Version 3 . . . 625
Enabling POP3 . . . 627
Administering POP3 . . . 627
Internet Messaging Access Protocol 4 . . . 632
Enabling IMAP4 . . . 633
Administering IMAP4 . . . 634
POP3/IMAP4 Considerations . . . 639
Summary . . . 640

Part VIII

Appendices

A Default Directory Structure for Exchange Server 2007 . . . 643

B Delivery Status Notification Codes . . . 645

C Default Log File Locations . . . 649

D Default Diagnostic Logging Levels for Exchange Processes . . . 651

Glossary . . . 657

Index . . . 669

Chapter 19

Exchange Server Security Basics

The Scope of Security **468**
Motivations of a Criminal Hacker **469**
How Hackers Work **470**
Physical Security **474**
Administrative Security **474**
SMTP Security **480**
Computer Viruses **485**
Junk E-Mail **487**
Security Tools Provided by Microsoft **488**
Summary **489**

Security incidents, including hacking, virus attacks, spyware outbreaks, and identity theft, have rocked the computing world. Due to the e-mail server's reliance on access to the outside world, e-mail has become a target for miscreants everywhere, who try to use this medium to gain access to an organization. As such, security has become so central to the administrator's role that a large portion of this book is devoted to a discussion of it.

This chapter offers ideas about how to add complexity and create hindrances to those who wish to attack your network over port 25. It is never fool-proof, but the more you invest in security, the more secure your e-mail server will be. However, if you have good strategies in place and adequate tools to assist you, you can anticipate and thwart most attacks.

Think Globally When Diagnosing a Security Problem

Recently, a United States firm with national visibility in its industry was attacked by a group based outside of the U.S. The attacking group used its Exchange server to send out spam messages (in its own language) to addresses all over the world. At first, this problem looked like a virus, but then the company realized the attackers had planted a program on the Exchange server that was launching the outgoing e-mails.

By the time the firm figured out the problem, outbound SMTP queues had nearly 100,000 messages sitting in them, ready to be sent. Besides the obvious concern that the people receiving the spam would be unhappy, there were also a multitude of other negative possible consequences that could have occurred as a result of this problem:

- **A tarnished reputation** By "allowing" this activity to take place, the company proved to those that received the spam that inadequate security measures were being taken. Whether this statement actually reflected reality would be a moot point to those who's perceptions of this company changed.
- **Lawsuits** By sending out spam, the company opened itself up to lawsuit that could prove to be costly and further harm the company's reputation.

The Scope of Security

Everyone has heard the old phrase "a chain is only as strong as its weakest link." You can easily apply that thinking to security: a network is only as secure as its least secured component. Always consider e-mail to be one of those weak links on your network because it is an obvious entry point. Attackers use e-mail to wreak havoc because it's easy: no matter how well you secure your network, chances are good that you have port 25 open on your firewall and that a Simple Mail Transport Protocol (SMTP) server is ready to work with e-mail when it comes in.

When you begin thinking about security strategies, always answer the following question: What am I securing Exchange Server 2007 against? The answers to this question are varied and can be grouped into four categories:

1. Social engineering attempts
2. Physical security
3. Administrative security
4. SMTP security

You learned about social engineering in depth in Chapter 18, "Security Policies and Exchange Server 2007." In this chapter, the other three security categories are covered.

Motivations of a Criminal Hacker

Although a lot of literature has been written about the technical aspects of securing a network, not much is available about who your enemies are and what motivates them to attack. Before you can determine how to protect your organization, you must learn to think like a hacker, figure out where you're vulnerable, and then develop a game plan to reduce your exposure. If you can understand who would want to do you harm and what can be gained from such harm, you can better protect your company and your information. Make the following assumptions:

- You do have professional adversaries.
- You are on their target list.
- You will be attacked some day.
- You cannot afford to be complacent.

One of the most difficult realities for an organization to accept is the presence of adversaries who might attempt to harm it by using technology. It's also possible that you really do not have adversaries in this traditional sense. Today, attackers look for any system that has an exploitable weakness that they can turn to their advantage. Often, attackers look at weakly secured systems as bases from which to launch more sophisticated attacks.

The motivations of attackers can be varied and complex. Hackers are often motivated, in part, by their invisibleness. Today's more sophisticated hackers are often also motivated by the prospect of a big payday. On the Internet, a hacker can "peek" into a company's private world—its network—and learn a lot while remaining anonymous.

Some individuals are just curious to see what they can learn about your company or individuals within your company. These hackers often don't have any malicious intent and are unaware that their actions violate security policy or criminal codes. That does not mean that these casual hackers are any less dangerous, however.

Other hackers are simply trying to help. You've probably been in this category once or twice yourself. In your zeal to be helpful, you bypass security policies to fix problems or accomplish emergency assignments. You might even believe that your efforts are more efficient than following established guidelines and policies. Nevertheless, the bypassing of known security policies is one element of hacking a network.

Some individuals act with malicious intent, engaging in acts of sabotage, espionage, or other criminal activities. They can become moles, stealing information to sell to competitors or foreign groups. Some simply enjoy destroying the work of others as well as their own work. Others act out of revenge for a real or perceived wrong committed against them, or believe they are acting in line with a strongly held belief system. Still others are

more methodical and hardened and turn hacking into a career; they might even take employment just to do your company harm.

How Hackers Work

Hackers start by learning that an e-mail server exists, which generic scanning tools can tell them. Coupled with the public information of your Domain Name System (DNS) records, hackers can quickly know a lot about your network.

Finding company information is easy for anyone. You can do it. Simply open a command prompt and type **nslookup**. Set the type of the record you're looking for to a mail exchanger (MX) record by typing **set type=mx**. Type a domain name. This example uses Microsoft.com. Figure 19-1 shows the results.

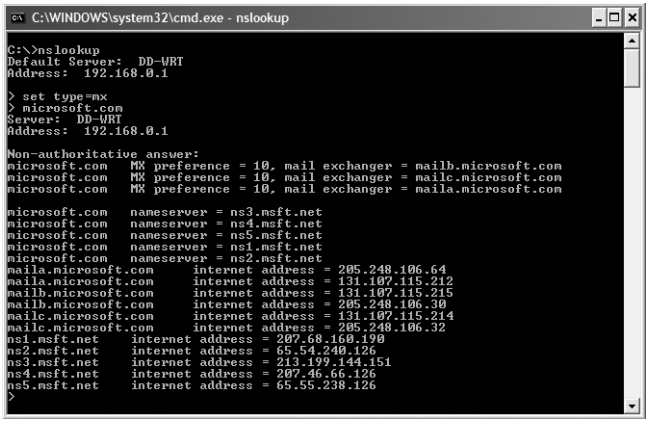


Figure 19-1 Using the NSLookup tool to find the public MX records for Microsoft.com

Next, the hacker determines the platform of your SMTP server in one of two ways. In the first approach, the hacker can use Telnet to open a session to your server over port 25 and then read the banner. Under Exchange Server 2007, the banner no longer identifies the version of Exchange Server being run, but does still indicate that the server is running the Microsoft ESMTP service. By removing the version number, Microsoft makes it harder for hackers to determine the exact version of Exchange that you are using. Note, of course, that because Exchange Server 2007 is the only version that, by default, lacks this identifying information, there are methods to achieve the same goal in older versions. However, a hacker can still figure out what he wants to know. It will take a couple of service packs and another major version of Exchange before this default omission really begins to bear fruit. Figure 19-2 gives you a look at an ESMTP conversation that takes place with an Exchange Server 2007 server.

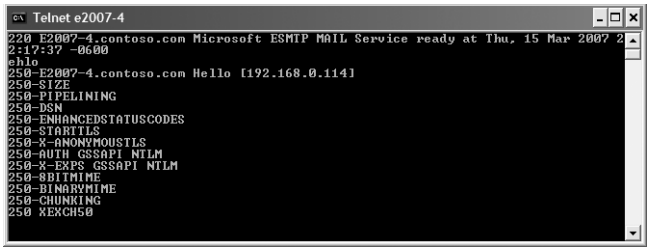


Figure 19-2 Opening a Telnet session to a server running Exchange Server 2003

Under older versions of Exchange Server, the exact version of the Exchange server being run is displayed (see Figure 19-3). The main version number, 6.0, means Exchange Server 2003. An Exchange 2000 Server registers with a main version number of 5.0. A SendMail server has its name and the version of SendMail software used by the company displayed in the header as well as the operating system (OS). Using this kind of information, a hacker can target his efforts by looking for exploits that will work for your specific system.

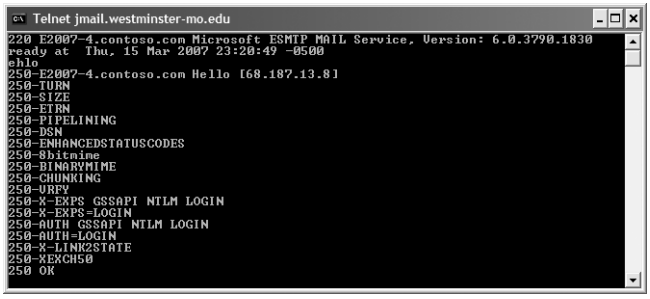


Figure 19-3 Opening a Telnet session to a server running Exchange Server 2007

> **More Info** Although Exchange Server 2007 is the first version of Exchange Server that, by default, does not display versioning information in a telnet window, you can manually configure older versions of Exchange Server to act the same way. Refer to *http://support.microsoft.com/kb/281224/en-us* for more information..

The second way to determine your e-mail server platform is to send a bogus e-mail to your server. This is accomplished by sending a message to an unlikely e-mail address such as pancake@contoso.com. The nondelivery report (NDR) that is returned has the e-mail server information located somewhere in the NDR. The following sample is a message header sent to the lab Exchange server at contoso.com. Notice that the Exchange server version is included right in the Sent by line:

```
Delivery has failed to these recipients or distribution lists:

pancake@contoso.com
This recipient e-mail address was not found in the recipient e-mail system.
Microsoft Exchange will not try to redeliver this message for you. Please
check the recipient e-mail address and try resending this message, or provide
the following diagnostic text to your system administrator.
------------------------------------------------------------------------------
Sent by Microsoft Exchange Server 2007
Diagnostic information for administrators:
Generating server: E2007-4.contoso.com
pancake@contoso.com
#550 5.1.1 RESOLVER.ADR.RecipNotFound; not found ##
Original message headers:
Received: from E2007-4.contoso.com ([192.168.0.22]) by E2007-4.contoso.com
 ([192.168.0.22]) with mapi; Thu, 15 Mar 2007 22:31:42 -0600
Content-Type: application/ms-tnef; name="winmail.dat"
Content-Transfer-Encoding: binary
From: Francis Cat <cat.francis@contoso.com>
To: "pancake@contoso.com" <pancake@contoso.com>
Date: Thu, 15 Mar 2007 22:31:37 -0600
Subject: Test message
Thread-Topic: Test message
Thread-Index: AQHHZ4P8FQkU6/4hJka2OY89GG0rfg==
Message-ID: <48B260B970217342AAFBCD9BD19B2E5D20A39D1C1B@E2007-4.contoso.com>
Accept-Language: en-US
Content-Language: en-US
X-MS-Has-Attach:
X-MS-TNEF-Correlator: <48B260B970217342AAFBCD9BD19B2E5D20A39D1C1B@E2007-4
       .contoso.com>
MIME-Version: 1.0
```

Now that the hacker knows which e-mail server software you run, he or she checks known databases to find vulnerabilities to exploit. The known vulnerabilities for Exchange Server 2007 are listed in Microsoft's Security Bulletins and can be found at www.microsoft.com/security/ default.mspx. On older versions of Exchange, some of the vulnerabilities could involve Microsoft Internet Information Services (IIS) because IIS managed the SMTP service for Exchange. In Exchange Server 2007, SMTP is a core part of Exchange itself, which helps to reduce the attack potential on your server. Other vulnerabilities may involve Microsoft Outlook Web Access (OWA), again because of the involvement of IIS managing the HTTP connectivity to the Exchange server. At a minimum, be aware of any vulnerabilities that exist for Exchange Server 2007 and test and install the patches when they are released.

Generally speaking, the e-mail administrator can expect the following kinds of attacks:

- **Buffer overflows** Buffer overflows send a larger quantity of data to the server than is anticipated. Depending on how the overflow is executed, it could cause the server to stop working or it might run malicious code from the attacker.

- **Data processing errors** These are not common currently, but the concept is that a small program is sent directly to the server, and the server runs it. More common today is sending these programs to a network though e-mail as attachments. Depending on their function and purpose, these programs can be viruses, Trojans, or worms (discussed at length later in this chapter).
- **HTML viruses** These do not require user intervention to run unattended scripts.
- **Custom programs written to run against port 25 (SMTP)** The more common types of programs that attack port 25 include e-mail–flooding programs or programs that contain their own SMTP engine that use the port for their own malicious purposes.
- **Denial of Service (DoS)** A Denial of Service attack is an attack on a network that is undertaken in an effort to disrupt the services provided by a network or server.
- **Cross-site scripting** Cross-site scripting is a vulnerability whereby an attacker places malicious code into a link that appears to be from a trusted source.
- **Spam and phishing expeditions** Spam, or junk mail, is a well-known e-mail malady and affects just about everyone that uses the communication medium. A particular type of spam, called a phishing e-mail, attempts to lure unsuspecting users into clicking on unsafe web links. These links point to web forms that ask the user to provide sensitive personal information.

Here are some broad actions you can take to guard against the attacks just described, plus others:

- **Physical access to the server** Lock the doors and use some type of biotech authentication.
- **Viruses, Trojans, and worms** Use antivirus software and regularly scan your servers and workstations. Use the Exchange Server 2007 Edge Transport server role on at least one Exchange server.
- **Loss of data** Perform regular backups.
- **Unauthorized use of user accounts** Conduct user training on information security policies and require complex passwords.
- **Denial of service attack** Harden the TCP/IP stack and the router.
- **Platform vulnerabilities** Install all software patches and engage in service that offers minimization. Microsoft has released excellent free software for updating its patches on your servers. This software is called Windows Server Update Services (WSUS).

More Info A discussion of WSUS is outside the scope of this chapter, but you can learn more about WSUS on Microsoft's Web site at *http://www.microsoft.com/windowsserversystem/updateservices/default.mspx*.

The rest of this chapter is intended to help you secure Exchange Server 2007 against these types of attacks. However, a brief discussion of physical security of your Exchange server is in order.

Physical Security

Physical security is a topic not often mentioned in many security books, particularly in books only about Exchange, but it is a topic worth mentioning. Servers can be left on desks running in a corner cubicle or in an unlocked server room. However, it is always best practice to store your servers in a secure location using door locks and, in some instances, motion detectors and/or other physical security measures.

When you limit physical access to a server, you limit who can log on locally to the server, who can use portable storage to introduce a new virus or malicious program on your network, and who can retrieve information directly from the server. Limiting physical access is one of the easiest and most elementary methods of securing your server against internal attacks that exist.

Most administrators reading this book already have these physical security measures in place. Those who haven't physically secured your servers should do so at their earliest opportunity. Limiting physical access to a server can go a long way toward protecting your information from would-be attackers.

Administrative Security

In previous versions of this book, this section talked extensively about the use of administrative groups as a way to achieve some semblance of administrative security for your Exchange organization. In Exchange Server 2007, however, Microsoft has mostly done away with administrative groups, leaving only a single administrative group named Exchange Administrative Group (FYDIBOHF23SPDLT) in which only Exchange Server 2007 servers reside. This administrative group is present only to support coexistence with legacy Exchange servers.

Note The name of the Exchange administrative group, Exchange Administrative Group (FYDIBOHF23SPDLT), is pretty convoluted. Likewise, Exchange Server 2007's legacy routing group, named Exchange Routing Group (DWBGZMFD01QNBJR), is also fairly convoluted. Have you wondered at all why Microsoft chose these particular names? First, Microsoft had to be careful that it didn't choose a name that already exists in a customer's legacy Exchange organization. Second, the Exchange team decided that a little creativity was in order. Look carefully at the two names. Both have the same number of characters with each letter and number occupying the same positions. To make a long story short, if you look at the administrative

group's name, you find you can go to the previous letter (or number) in the alphabet for each character in the name and spell "EXCHANGE12ROCKS." Likewise, for the routing group, go to the next letter of the alphabet for each letter in the routing group name and you also get "EXCHANGE12ROCKS." It's really nice to see the product team having so much fun with a product that is generally considered all business!

Why did the Exchange team eliminate administrative groups from the Exchange equation? With the complete overhaul of the management interface and its new "area of responsibility" focus, administrative groups simply aren't necessary and can add to the overall complexity of managing Exchange. Figure 19-4 gives you a side-by-side look at the legacy Exchange System Manager and the Exchange Server 2007 Exchange Management Console. With their absence in Exchange Server 2007, you need to use a way other than administrative groups to achieve administrative security. In this section, you learn two methods by which you can add users to act in various Exchange administrative capacities.

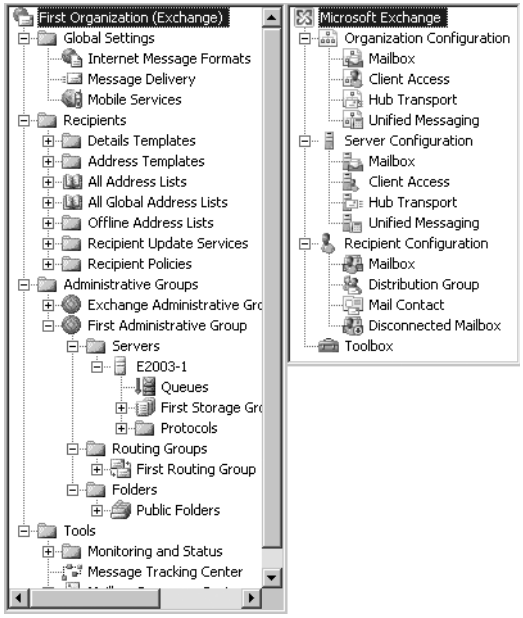


Figure 19-4 The Exchange Server 2003 Exchange System Manager is on the left and the Exchange Server 2007 Exchange Management Console is on the right.

The Built-in Exchange Administrative Groups

When you run the initial installation of Exchange Server 2007, five Active Directory universal security groups are created, each with specific rights to various parts of the Exchange organization. Four of the five groups, shown in Figure 19-5 inside Active Directory Users

and Computers, pertain directly to management of the Exchange organization and are as follows:

- **Exchange View-Only Administrators** This role allows you to view configurations on all Exchange objects, but not to make any changes to those configurations.
- **Exchange Servers** This role provides the following rights:
  - Members of this group have all of the rights of Exchange View-Only Administrators.
  - Members of this group have access to server-based Exchange configuration information and to the Active Directory objects that are server-related.
  - Members of this group may perform server-based administration but cannot perform operations at the global Exchange organization level.
  - Members of this group are also members of the local Administrators group on each server on which Exchange Server 2007 is installed.
- **Exchange Recipient Administrators** This role provides the following rights:
  - Members of this group have all of the rights of Exchange View-Only Administrators.
  - Members of the group are also allowed to configure any object related to recipients and public folders, including contacts, groups, public folder objects, Unified Messaging mailbox settings, Client Access mailbox settings, and any other recipient Exchange property found in Active Directory.
- **Exchange Organization Administrators** This role provides the following rights:
  - Members of this group have all of the rights of Exchange Recipient Administrators, plus more.
  - Users assigned to this group are allowed to view and administer all aspects of the Exchange organization, including servers, and organizational configuration.
  - Members of the role are considered the owners of all Exchange-related Active Directory objects.
  - During Exchange Server 2007 installation, this group is added to the membership of the server's local Administrators group. If you install Exchange Server 2007 on a domain controller, which is not recommended, Exchange Organization Administrators have additional rights by virtue of the local Administrators group having more rights on a domain controller.

If you want to add a full Exchange administrator to your organization, all you have to do is add the appropriate user account to the Exchange Organization Administrators group. The same holds true for the other security groups.

Figure 19-5 The Exchange Server 2007 built-in security group

The Add Exchange Administrator Wizard

Exchange Server 2007 also provides an easy way to add Exchange administrators with each administrator role having responsibility for only a specific part of the Exchange organization, such as a single server, a group of servers, or only able to manage recipients. You will find that this administrative delegation method is far more flexible and effective than administrative groups were in the past.

The best way to demonstrate how the Add Exchange Administrator operation works is to see it in action. To start the process, open the Exchange Management Console and select the Organization Configuration option, as shown in Figure 19-6.

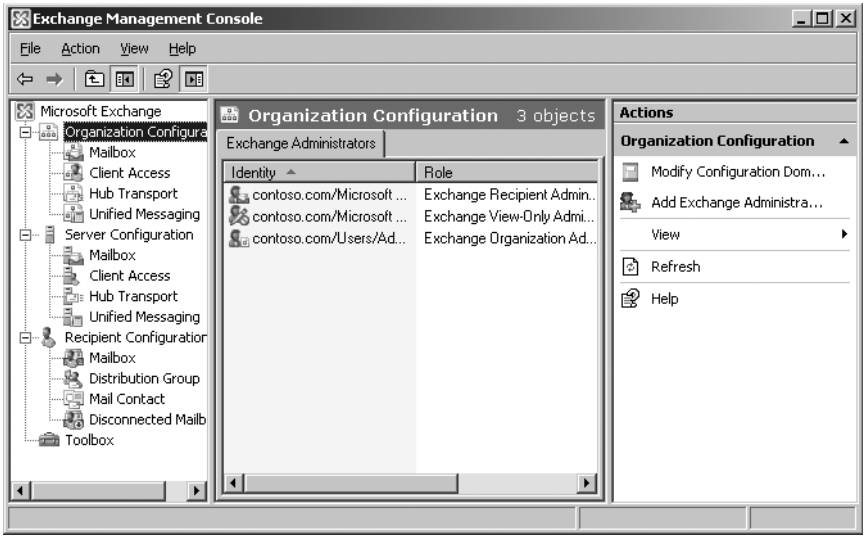


Figure 19-6 The Organization Configuration window

Note that the work pane shown in Figure 19-6 shows you the groups that already have some level of permission to the Exchange organization. To add Exchange administrators, from the Action pane, choose Add Exchange Administrator. This selection displays a one-page wizard, shown in Figure 19-7.

Figure 19-7 The Add Exchange Administrator Wizard

There are three selections that you must make in order to complete this wizard.

First, select the user or group to which you want to grant Exchange administrative rights. Next, select the role and scope that should apply to the new Exchange administrator. Finally, if you've selected the Exchange Server Administrator role, select at least one server to which this new user or group has access. Click Add, and from the Select Exchange Server window, choose the desired servers. Figure 19-8 shows what the screen looks like after you select the Exchange Server Administrator role and add a managed server.

> **Note** When you add someone to the Exchange Server Administrator role, you must manually add that user or group to each managed server's local Administrators group.

In reality, when you run the Add Exchange Administrator wizard, the resulting command simply adds the selected users to one of the groups that you learned about in the section "The Built-in Exchange Administrative Groups." The only role for which this does not hold true is for the Exchange Server Administrator role. When users or groups are assigned to this role, the user or group is assigned Full Control permission on the specified server object and all child objects.

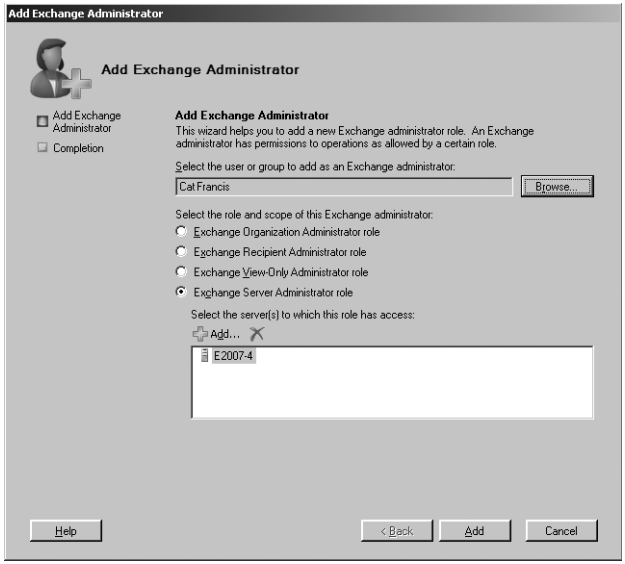


Figure 19-8 Selecting the Exchange Server Administrator role

Management Shell

You can also manage administrative roles through the Exchange Management Shell.

The following command adds a user account that can manage the Exchange Server 2007 server named E2007-4:

```
Add-ExchangeAdministrator -Identity 'contoso.com/Users/David So'
  -Role 'ServerAdmin' -Scope 'E2007-4'
```

If you add someone using Exchange Server Administrator role, you need to manually add the selected user or group to the built-in local administrators group on the target server.

This command adds a user to the Exchange Recipient Administrators role:

```
Add-ExchangeAdministrator -Identity 'contoso.com/Users/David So'
  -Role 'RecipientAdmin'
```

This command adds a user to the Exchange View-Only Administrators role:

```
Add-ExchangeAdministrator -Identity 'contoso.com/Users/David So'
  -Role 'ViewOnlyAdmin'
```

This command adds a user to the Exchange OrganizationAdministrators role:

```
Add-ExchangeAdministrator -Identity 'contoso.com/Users/David So'
  -Role 'OrgAdmin'
```

Table 19-1 comes from Microsoft's documentation on the role of roles in Exchange Server 2007 and provides a concise look at exactly what each administrative role accomplishes.

Table 19-1 Exchange Server Administrative Roles

Role	Members	Member of	Exchange permissions
Exchange Organization Administrators	Administrator, or the account that was used to install the first Exchange 2007 server	Exchange Recipient Administrator, Administrators local group of *<Server Name>*	Full control of the Microsoft Exchange container in Active Directory
Exchange Recipient Administrators	Exchange Organization Administrators	Exchange View-Only Administrators	Full control of Exchange properties on Active Directory user object
Exchange Server Administrators	Exchange Organization Administrators	Exchange View-Only Administrators, Administrators local group of *<Server Name>*	Full control of Exchange *<Server Name>*
Exchange View-Only Administrators	Exchange Recipient Administrators, Exchange Server Administrators (*<Server Name>*)	Exchange Recipient Administrators, Exchange Server Administrators	Read access to the Microsoft Exchange container in Active Directory. Read access to all the Windows domains that have Exchange recipients.

SMTP Security

By default, an SMTP server attempts to make a TCP port 25 connection to your Exchange server via an anonymous connection. Anonymous does not mean that a user account set up in your Active Directory proxies the connection request, as is the case with the IIS Anonymous user account, IUSR_<machinename>. In the SMTP world, anonymous means that no user name or password is required for the remote SMTP service to make a port 25 connection. Hence, any SMTP server on the Internet can make, by default, a port 25 connection to your Exchange server.

To make SMTP more secure, you could require either Basic or Integrated Windows Authentication (IWA) before the SMTP Virtual Server (VS) could accept an inbound connection. But this configuration isn't practical on the Internet because you can't predict who will be connecting to your Exchange server in the future and thus can't assume that the user has an appropriate user name and password to make a connection. Moreover, not

many messaging administrators are interested in implementing such a security measure at their end. So even though an anonymous connection to port 25 on your Exchange server represents a vulnerability, it is one that must be managed using a different approach than removing anonymous connections.

How do you protect against these kinds of attacks? With Exchange Server 2007, you can use an Edge Transport server that offloads the security burden from your primary Exchange servers. You learn about implementing the Edge Transport server in Chapter 20, "Antivirus and Anti-Spam." This chapter also discusses how the Edge Transport server can help improve the overall security of your Exchange infrastructure. However, more traditional ways of protecting Exchange also apply even when Edge Transport servers are used.

Perhaps the most common way to protect an Exchange infrastructure is through the use two firewalls. A dual firewall topology allows you to protect your internal Exchange servers while also filtering incoming e-mail against potential attacks. The area between the two firewalls is called the *perimeter network* (also known as DMZ or demilitarized zone). The philosophy is to put up a line of defense against potential attacks. Hence, you're willing to sacrifice your Exchange servers in the perimeter network, but not willing to sacrifice your Exchange servers on the internal network. Because the Exchange servers in the perimeter network do not host any important information—no mailboxes or public folders—they can be both sacrificed during an attack and easily rebuilt. And because they act only as relay servers, they can be used to sanitize incoming e-mail over port 25.

Take a look at Figure 19-9. Note that there are three network levels. Starting from the top, each network becomes more trusted, with the External, or Internet, zone being completely untrusted. The perimeter network is more trusted as it resides behind at least one organizational firewall and generally houses servers that can be considered "expendable." In this diagram, the external firewall has port 25 open in order to facilitate incoming SMTP traffic. Mail is routed to the Exchange Server 2007 Edge Transport server where it is processed for viruses, checked using various spam filters, and run through various incoming transport rules. Your external MX records must point to this Edge Transport server. There is another important note in this diagram. Note that the external firewall also provides the ability to scan incoming content for viruses and spyware. When possible, always run your e-mail through a similarly configured firewall even before that mail hits the Edge Transport server's content-scanning engines. Many of today's security appliances, such as the Cisco ASA and Sonicwall's family of firewalls, provide this additional protection.

From a software perspective, also consider running Microsoft Forefront Security for Exchange Server. Forefront has the ability to scan every incoming message with up to five

completely separate virus scanners. By instituting this multilayer security infrastructure, all incoming mail is scanned by many different virus scanning engines, some hardware-based and some software-based, which results in a much higher likelihood you will be protected against even the newest viruses.

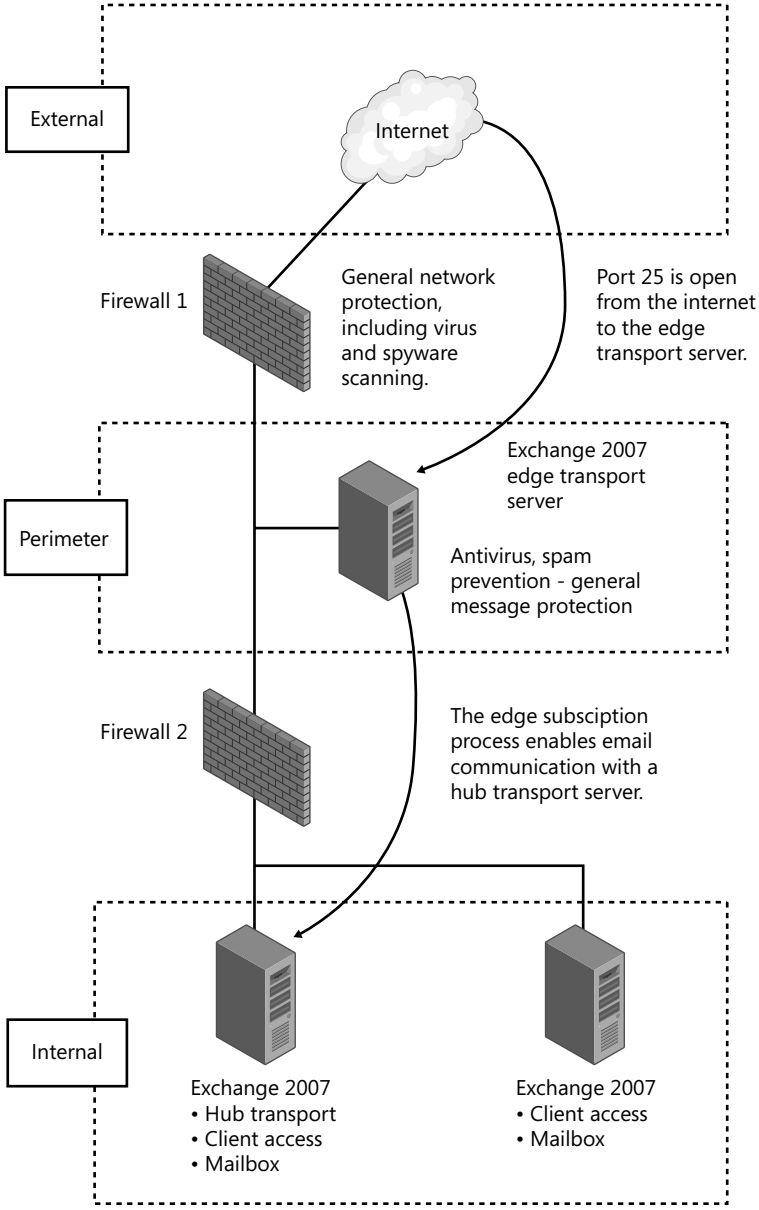


Figure 19-9 One way to secure your Exchange infrastructure

However, even the best virus-scanning infrastructure on the planet does not always protect you. Think back to some of the major viruses in the last few years, which were able to spread worldwide very quickly, usually in a matter of hours. It is almost impossible for any antivirus company to get the virus, study it, write a definition for it, and then push out the new definition for that virus before it spreads worldwide. You can tell an Edge Transport server, however, to quarantine or delete any message that contains certain types of attachments and, in effect, block most viruses based on their type of content rather than on a comparison to a virus definition file.essent.

Note Be aware of two issues regarding traditional antivirus servers. First, many products offered by the major antivirus vendors perform content scanning at the same time as the virus scanning. While there may be no problem with this method of scanning e-mail, be aware of a distinction between content scanning and antivirus scanning, which highlights the need to perform both types of scanning in the perimeter network, a capability enabled through the use of Exchange Server 2007's Edge Transport server. Second, everyone may not be able afford to purchase everything required in order to achieve the configuration outlined in this chapter—namely, a separate Exchange server running Edge Transport as well as firewalls/security appliances that perform virus scanning functions. These ideas are presented to highlight the concepts being discussed. Other, less expensive (and potentially less secure) options include:

- Using a single firewall with multiple interfaces and creating a perimeter network using firewall rules
- Using a single firewall and running the Edge Transport server on the internal interface alongside your other Exchange servers
- Skipping the installation of the Edge Transport server and delivering mail directly to an internal Hub Transport server

Once scanned and approved, the e-mail is sent to an internal Hub Transport server. The internal Exchange Server 2007 Hub Transport server should be configured to accept inbound e-mail only from the perimeter network's Edge Transport server. Inbound mail that has been approved by the Edge Transport server also rides on the standard SMTP TCP port 25, so you need to open this port on your internal firewall as well. To do this in the most secure way possible, create a firewall rule that only allows port 25 traffic specifically between the Edge Transport server and one of your internal Hub Transport servers. Then, secure the communication tunnel using IPsec, which is discussed further in Chapter 21. The internal Exchange server should also be running its own antivirus software, preferably from a vendor that is different from the one the servers are using in the perimeter network. The whole point of implementing this model is to ensure that port 25 traffic is as well protected as possible.

In order to use an Edge Transport server, subscribe the Edge Transport server to the Active Directory domain. The subscription process establishes one-way replication of

recipient and configuration information from your Active Directory into an Active Directory Application Mode (ADAM) instance running on your Edge Transport server. Further, the Edge Subscription process creates the SMTP Send connectors required to enable mail flow from your Exchange servers to the Internet through an Edge Transport server. If you are using the recipient lookup or safe list aggregation features of the Edge Transport server, subscribe the Edge Transport server to the organization.

More Info The complete process for installing, configuring, and subscribing the Edge Transport services is covered in Chapter 20, "Antivirus and Anti-Spam."

No system is foolproof, but this dual firewall topology has multiple advantages:

- By passing incoming e-mail through the Edge Transport servers content filtering services, you filter for code types that virus scanners don't.
- By passing your e-mail through a virus scanner, you do your best to ensure that all known viruses are cleaned out. Not passing your e-mail through an updated antivirus scanner after running it through a content scanner is unwise because older viruses might not be caught by the content scanner.
- By passing all of your outgoing e-mail through the Exchange Server 2007 Edge Transport server, the IP address (private or public) of the internal Exchange Server 2007 server does not need to be published in the public DNS records. This means that an attacker attempting to Telnet into your server is never able to reach it directly. Also, if you configure the internal Exchange Server 2007 server to accept e-mail only from DMZ-based Exchange servers, any attempts to make port 25 connections to the internal Exchange server from any other IP address will fail.

If a hacker decides to bring down your perimeter Exchange servers, you've really lost nothing of value other than your time in getting the servers functioning again. Your company might lose some money due to the inability to communicate via e-mail, but it hasn't lost any current data. This is an important point. The server that hosts your data is the one most protected. And the ones most exposed do not host important data. If those servers are lost, at least all the business-critical data is saved on the internal Exchange Server 2007 server. For many companies, this is an acceptable level of risk to assume. This is the beginning stage of a defense that provides multiple layer of protection, starting with expendable services with the really important data protected in a variety of different ways.

As explained throughout this chapter, no answer is perfect, and this security scenario does have a few major holes, such as doing nothing to protect against messages sent to the Exchange server via Outlook Web Access. Port 25 is well protected, but port 80 access to your Exchange server is wide open. If you want to learn more about OWA, refer to Chapter 24, "Supporting Outlook Web Access."

The second major hole in this model is one that cannot be plugged: messages are continuing to flow to your internal Exchange server. As long as a packet can reach your internal Exchange server, there is always the potential for harm. So remember the 80-percent rule: you can make your data only about 80-percent secure. But don't let that discourage you from implementing appropriate security strategies.

Computer Viruses

This section expands on computer viruses in general and discusses some implications for viruses on Exchange Server 2007.

What Is a Virus?

A *virus* is a piece of code that attaches itself to other programs or files. When these files run, the code is invoked and begins replicating itself. The replication occurs over the network. Viruses can now exploit the vulnerabilities of nearly every platform.

Some viruses reside in memory after the original program is shut down. When other programs are executed, the virus attaches itself to these new programs until the computer is shut down or turned off. Some viruses have a "dormant" phase and appear only at certain times or when certain actions are performed.

There are many types of viruses. Some overwrite existing code or data. Others include the ability to recognize whether an executable file is already infected. *Self-recognition* is required if the virus is to avoid multiple infections of a single executable, which can cause excessive growth in size of infected executables and corresponding excessive storage space, contributing to the detection of the virus.

Resident viruses install themselves as part of the operating system upon execution of an infected host program. The virus remains resident until the system is shut down. Once installed in memory, a resident virus is available to infect all suitable hosts that are accessed.

A *stealth virus* is a resident virus that attempts to evade detection by concealing its presence in infected files. For example, a stealth virus might remove the virus code from an executable when it is read (rather than executed) so that an antivirus software package sees only the noncompromised form of the executable.

Computer viruses can spread by the use of e-mail and usually appear in e-mail attachments. If the virus can find its way into the messaging stream, it uses the client capability to send and receive e-mail to replicate itself quickly and do its damage as fast as possible.

An essential aspect of protecting your messaging system against viruses is user education. Users should learn to be guarded about which attachments they are allowed to open.

Your information security policies should also outline the types of e-mails and attachments that users are allowed to open. For example, users should be forbidden to open attachments in two instances: when they were not expecting the attachments, and when the attachments arrive from unrecognizable aliases.

Finally, whenever possible, consider a centralized antivirus service that updates the distributed clients from a centrally managed server. Most such solutions provide you with ways to more granularly manage each client and proactively fix problems that may take place.

Trojans

A *Trojan* (also known as a Trojan horse) is a malicious program embedded inside a normal, safe-looking program. The difference between a virus and a Trojan is that the Trojan is embedded and the virus is attached to the file or executable.

When the normal program runs, the malicious code runs as well and can cause damage or steal critical information. An example of a Trojan is a word-processing program that, when executed, allows the user to compose a document while, in the background, malicious code is running that deletes files or destroys other programs.

Trojans generally are spread through e-mail or *worms*, which are programs that run by themselves. The damage that Trojans can cause is similar to that of a virus: from nominal to critical. Trojans are particularly frightening because in most cases, users are unaware of the damage the Trojan is causing. The malicious work is being masked by the Trojan effect of the program.

Worms

As just mentioned, worms are programs that run by themselves. They do not embed or attach themselves to other programs nor do they need to do this to replicate. They can travel from computer to computer across network connections and are self-replicating. Worms might have portions of themselves running on many different computers, or the entire program might run on a single computer. Typically, worms do not change other programs, although they might carry other code that does.

The first network worms were intended to perform useful network management functions by taking advantage of operating system properties. Malicious worms exploit system vulnerabilities for their own purposes. Release of a worm usually results in brief outbreaks, shutting down entire networks.

The damage that worms can cause, like Trojans and viruses, ranges from the nominal to the critical. The type and extent of damage must be assessed individually for each worm. However, worms can install viruses and Trojans that then run their own code.

An attack that combines a worm, Trojan, and/or virus can be a very difficult attack to survive without significant damage. The impact of viruses, Trojans, and worms on your

messaging system and network should not be underestimated. Because they use e-mail to exploit system vulnerabilities, installing antivirus software is simply not enough. You must also ensure that known vulnerabilities in all your operating systems are patched. Don't focus only on your servers. Every device should be updated with the most recent patches from each vendor as soon as possible. Most environments will want to test these patches before installing them. But after they have been tested, install them.

Junk E-Mail

Junk e-mail is a huge issue. One client with whom this author recently worked installed its first e-mail filtering software and found that it had 46 percent fewer inbound e-mails.

Exchange Server 2007's new Edge Transport role has new capabilities that can help to significantly reduce the amount of junk e-mail that enters your environment. The Edge Transport Role server has the following agents that help to protect your e-mail infrastructure. The information in Table 19-2 is right from Microsoft's Edge Transport server documentation.

Table 19-2 Edge Transport Agents

Agent name	Description
Connection Filtering Agent	Performs host IP address filtering based on IP Allow Lists, IP Allow List providers, IP Block Lists, and IP Block List providers.
Address Rewriting Inbound Agent	Modifies recipient SMTP addresses in inbound messages based on predefined address alias information. Address rewriting can be useful in scenarios which an organization wants to hide internal domains.
Edge Rule Agent	Processes all messages received over SMTP to enforce transport rules defined on the Edge Transport server.
Sender ID Agent	Determines whether the sending SMTP host is authorized to send messages for the SMTP domain of the message originator.
Recipient Filter Agent	Verifies that the recipients specified during the SMTP session through the `RCPT TO:` command are valid and not on the list of blocked SMTP addresses and domains.
Sender Filter Agent	Verifies that the sender specified in the `MAIL FROM:` command and in the message header is valid and not on the list of blocked SMTP addresses and domains.
Content Filter Agent	Uses Microsoft SmartScreen technology to assess the contents of inbound messages in order to assign an SCL rating for junk e-mail processing based on transport and store thresholds.
Protocol Analysis Agent	Interacts with Connection Filtering, Sender Filtering, Recipient Filtering, and Sender ID agents to determine Sender Reputation Level (SRL) rating and to take action based on rating thresholds.

Table 19-2 Edge Transport Agents (Continued)

Agent name	Description
Attachment Filtering Agent	Filters messages based on attachment file name, file name extension, or MIME content type to block potentially harmful messages or remove critical attachments.
Address Rewriting Outbound Agent	Modifies sender SMTP addresses in outbound messages based on predefined address alias information. Address rewriting can be useful in scenarios where an organization wants to hide internal domains.
Forefront Security for Exchange Routing Agent	Responsible for connecting into the Transport stack to ensure that the scanning process scans messages prior to delivery to Hub Transport servers.

Many of these features are discussed in the next Chapter 20, "Antivirus and Anti-Spam," and Chapter 21, "Messaging Security."

Security Tools Provided by Microsoft

In order to help you deploy and maintain the most secure Exchange infrastructure possible, Microsoft provides a number of tools designed to remove malware, make sure that your environment is properly configured, and to help you configured a multitude of security settings.

- **Malicious Software Removal Tool** The Microsoft Windows Malicious Software Removal Tool checks computers running Windows XP, Windows 2000, and Windows Server 2003 for infections by specific, prevalent malicious software—including Blaster, Sasser, and Mydoom—and helps remove any infection found. When the detection and removal process is complete, the tool displays a report describing the outcome, including which, if any, malicious software was detected and removed. Microsoft releases an updated version of this tool on the second Tuesday of each month, and as needed to respond to security incidents. On a regular basis, run the Malicious Software Removal Tool on your Exchange server to make sure your system is free of threats.

  More Info To download the Microsoft Software Removal Tool, visit *http://www.microsoft.com/security/malwareremove/default.mspx*.

- **Microsoft Baseline Security Analyzer** The Microsoft Baseline Security Analyzer (MBSA) is a tool that analyzes your existing environment and, in particular, analyzes how you have configured a number of Microsoft products, including Windows 2000 SP3; Windows XP and Windows Server 2003; Office XP, 2003 and 2007; Exchange 2000, 2003 and 2007; SQL Server 2000 SP4; and SQL Server 2005. With this information, Microsoft compares your configuration against a list

of best practices and provides you with a report of action items that you can take to improve the security of your environment.

> **More Info** To download the Microsoft Baseline Security Analyzer, visit *http://www.microsoft.com/technet/security/tools/mbsa2/default.mspx*.

- **Security Configuration Wizard** Windows Server 2003 Service Pack 1 includes the Security Configuration Wizard (SCW), a tool designed to reduce the attack surface of your Windows servers. SCW helps administrators to create security policies that are consistent with the practice of least privilege. In this case, that means running the fewest possible services on a server in order to reduce the number of services that can be used to attack the computer.

Summary

This chapter discussed how hackers think, how to secure incoming SMTP e-mail, and how to secure Administrator access to your Exchange server. Also discussed were the differences between a virus, a Trojan, and a worm, and a method was outlined for securing inbound SMTP traffic. Two other areas in this book were also referenced that discuss sender filtering and securing OWA. The next chapter discusses how to secure e-mail messages using encryption and certificates.